FORMAL GROUPS AND APPLICATIONS

Michiel Hazewinkel

Department of Mathematics
Erasmus Universiteit
Rotterdam, The Netherlands



ACADEMIC PRESS New York San Francisco London 1978

A Subsidiary of Harcourt Brace Jovanovich, Publishers

COPYRIGHT © 1978, BY ACADEMIC PRESS, INC.
ALL RIGHTS RESERVED.
NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, INCLUDING PHOTOCOPY, RECORDING, OR ANY INFORMATION STORAGE AND RETRIEVAL SYSTEM, WITHOUT PERMISSION IN WRITING FROM THE PUBLISHER.

ACADEMIC PRESS, INC.
111 Fifth Avenue, New York, New York 10003

United Kingdom Edition published by
ACADEMIC PRESS, INC. (LONDON) LTD.
24/28 Oval Road, London NW1 7DX

Library of Congress Cataloging in Publication Data

Hazewinkel, Michiel.
Formal groups and applications.

(Pure and applied mathematics, a series of monographs and textbooks ;)
Bibliography: p.
Includes index.
1. Groups, Formal. I. Title. II. Series.
QA3.P8 [QA171] 510'.8s [512'.22] 77-82414
ISBN 0-12-335150-2

AMS (MOS) 1970 Subject Classifications: 14L05, 14K15, 12B25, 55B20, 55G25

PRINTED IN THE UNITED STATES OF AMERICA

To Marijke, Maarten, and Annette

CONTENTS

Preface xi
Leitfaden and Indicien xiii
Introduction xvii

Chapter I Methods for Constructing One Dimensional Formal Groups

1 Definition and Elementary Properties of Formal Groups. Survey of the Results of Chapter I 1
2 The Functional Equation–Integrality Lemma 8
3 The Formal Group Laws $F_V(X, Y)$, $F_{V,T}(X, Y)$, and $F_S(X, Y)$ 16
4 Some Binomial Coefficient Arithmetic 20
5 A Universal One Dimensional Commutative Formal Group Law 24
6 Most One Dimensional Formal Group Laws Are Commutative 38
7 Honda's Method for Constructing Formal Group Laws 42
8 The Lubin–Tate Formal Group Laws 43

Chapter II Methods for Constructing Higher Dimensional Formal Group Laws

9 Definitions and Elementary Properties. Survey of the Results of Chapter II 51
10 The Higher Dimensional Functional Equation Lemma 59
11 The Universal n-Dimensional Commutative Formal Group Laws $H_U(X, Y)$ 63
12 Curvilinear Formal Group Laws 68
13 Higher Dimensional Honda Formal Group Laws and Higher Dimensional Lubin–Tate Formal Group Laws 73
14 Lie Theory 79
E.1 Bibliographical and Other Notes 87

Chapter III Curves, p-Typical Formal Group Laws, and Lots of Witt Vectors

15 Definitions. Survey of Results 91
16 Curves and p-Typical Formal Groups 102
17 Lots of Witt Vectors 115
E.2 Bibliographical and Other Notes 144

Chapter IV Homomorphisms, Endomorphisms, and the Classification of Formal Groups by Power Series Methods

18	Definitions and Preliminary Elementary Results. Survey of Chapter IV	147
19	Universal Isomorphisms	162
20	Existence and Nonexistence of Homomorphisms and Isomorphisms	173
21	Formal A-Modules	199
22	Lifting and Reducing Formal Group Laws. Formal Moduli	230
23	Rings of Endomorphisms of Formal Group Laws	245
24	Classification of One Dimensional Formal Group Laws over Finite Fields	253
25	Rings of Curves and Artin–Hasse-Like Exponential Mappings	269
E.3	Bibliographical and Other Notes	310

Chapter V Cartier–Dieudonné Modules

26	Basic Definitions and Reminders. Survey of the Results of Chapter V	312
27	Cartier–Dieudonné Modules for Formal Group Laws	320
28	On the Classification of Commutative Formal Group Laws over an Algebraically Closed Field of Characteristic $p > 0$	354
29	Cartier–Dieudonné Theory for Formal A-Modules	374
30	"Le Tapis de Cartier" for Formal A-Modules, or Lifting Formal Group Laws and Formal A-Modules Revisited	395
E.4	Bibliographical and Other Notes	422

Chapter VI Applications of Formal Groups in Algebraic Topology, Number Theory, and Algebraic Geometry

31	Basic Definitions and Survey of the Results of Chapter VI	427
32	Local Class Field Theory	433
33	Zeta Functions of Elliptic Curves over Q and Atkin–Swinnerton–Dyer Conjectures	441
34	On Complex Cobordism and Brown–Peterson Cohomology	446
35	Tate Modules (for One Dimensional Formal Group Laws)	460
E.5	Bibliographical and Other Notes	475

Chapter VII Formal Groups and Bialgebras

36	Basic Definitions and Survey of the Results of Chapter VII	478
37	Formal Groups and Bialgebras	485
38	Curves in Noncommutative Formal Groups	504
E.6	Bibliographical and Other Notes	514

Appendix A On Power Series Rings

A.1	Power Series Rings	517
A.2	Filtration and Topology	518
A.3	Formal Weierstrass Preparation Theorem	519
A.4	Homomorphisms and Isomorphisms. Formal Inverse Function and Implicit Function Theorems	520

Appendix B Brief Notes on Further Applications of Formal Group (Law) Theory

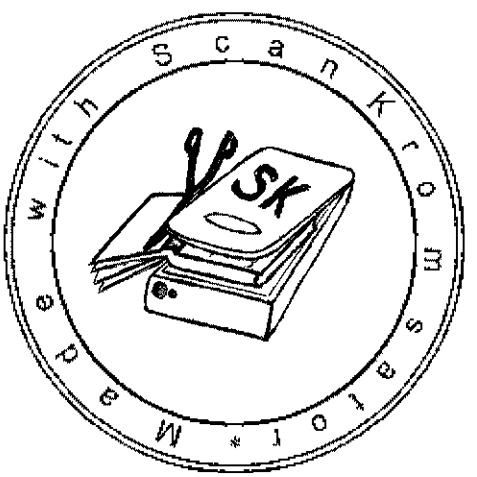
B.1 More on Formal Groups in Number Theory 523
B.2 More on Formal Groups in Algebraic Geometry 524
B.3 More on Formal Groups in Arithmetical Algebraic Geometry 525
B.4 More on Formal Groups in Algebraic Topology 527

Bibliography 531

Notation 551

Index 567

This page intentionally left blank



PREFACE

This is a book on formal groups from the naïve or power series point of view. That is, it is really about formal group *laws*.

The theory of formal groups has found a number of rather spectacular applications in recent years in number theory, arithmetical algebraic geometry, algebraic geometry, and algebraic topology, ranging from congruences for the coefficients of modular forms and local class field theory to extraordinary K-theories and (indirectly) results on the homotopy groups of spheres.

Originally I intended to try to organize in the form of a coherent set of lecture notes those parts of the theory of formal groups leading up to the various applications and those parts which seemed to me to be in imminent danger of becoming applicable. It was Eilenberg who suggested casually over a glass of grappa in Udine, that, in that case, I had better try to make a proper job of it. To him, many thanks.

The result is, I hope, a book, which, starting from no more than a reasonable acquaintance with the more elementary facts concerning commutative rings and modules, takes the reader through most of the known results on formal groups and which also presents those applications which do not require too much extra apparatus.

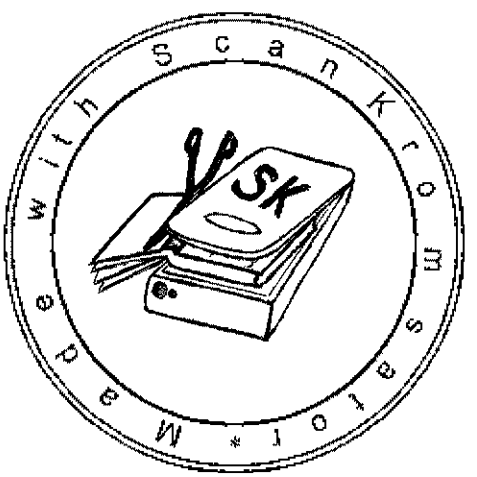
This last restriction caused, inevitably, a number of casualties. Notably, the applications to algebraic geometry (abelian varieties), which are only present in the form of some brief, mainly bibliographical, notes.

Quite a number of people helped directly or indirectly in making this book possible (e.g., by inviting me to lecture on parts of it). To all of them also many thanks. Special thanks are due to Marijke, Maarten, and Annette (they know what for) and to my secretary, Hannie Oosthout, who did a splendid job of typing on the basis of a set of notes which were a perfect mess of addenda, corrections, and emendations, so that, at times, the script ran in three distinct yet intersecting directions.

The computer calculations which briefly occur in the introduction were done by Ir. G. J. v.d. Steen of our department of Automatische Informatie Verwerking.

MICHIEL HAZEWINKEL, Krimpen a/d Yssel, January 1977

This page intentionally left blank



LEITFADEN AND INDICIEN

L.1 On the Organization of the Book

The first section of each of the seven chapters of the book is an introduction plus survey of the material treated in that chapter. I have tried to write these sections in such a way that they can, in principle, be read consecutively without referring to the rest of the book. Thus, assuming some stamina and reasonable powers of absorption, recollection, and belief on the part of the reader, he can obtain a very fair idea of the theory of formal groups and their applications by reading these introductory survey sections only; he will even have seen some proofs.

The text itself contains few bibliographical remarks and references. Most of these have been collected in six sections (E.1–E.6) placed at the ends of Chapters II–VII. These "bibliographical and other notes" sections often also contain some additional comments on related mathematical matters.

Finally, there are two appendices. The first one is purely for the convenience of the reader who is not acquainted with the more elementary facts concerning power series algebras. In the second appendix I have tried to give a sort of bibliographical guide to those applications of the theory of formal group laws which, for lack of space–time or a lack of competence on the part of the author, could not be treated in detail in the main text.

L.2 Bibliography, Indexes and Referencing System

The bibliography is fairly extensive. In addition to those papers and books actually referred to it also contains all those papers and books that I know of which use or treat formal groups and those papers which treat of closely related (author's opinion) material. Between brackets ( ) behind each bibliographical item are listed the sections of the book where this particular item is referred to; thus I hoped to make it easier for other authors to rebuke the present writer for misrepresenting their results.

In the index of notations I have distinguished between incidental, generic, and standard notations. Thus, e.g., $\mathbf{Z}$ for the integers is a standard notation and so is (in this book) $\Psi_G(x)$ for the characteristic polynomial of a one dimensional formal group law over a finite field; the Greek letter ϕ is generically used

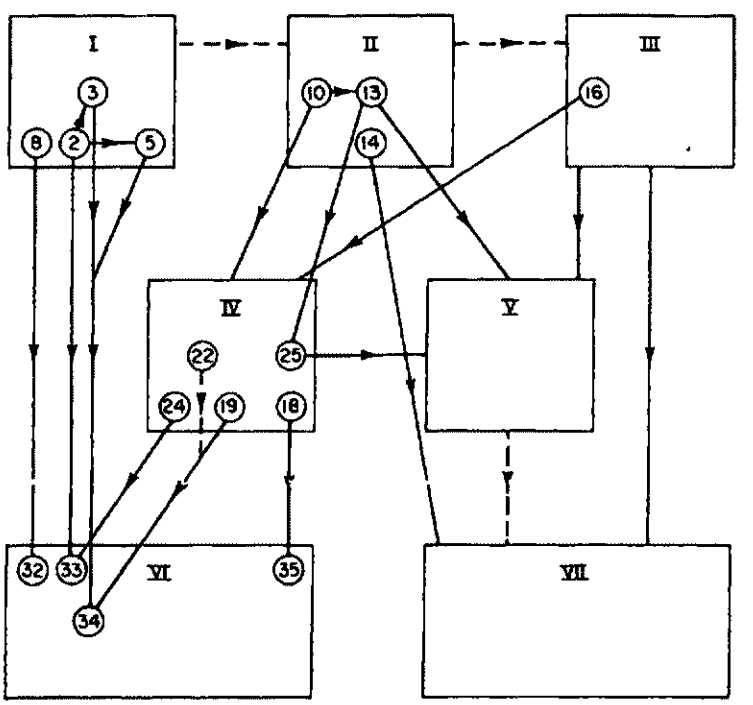
to denote a homomorphism of rings or algebras and an example of an incidental notation is $\mathscr{E}_m$ which is used in Section 20.4 to denote a certain noncommutative ring. Also, for each standard notation, I have tried to indicate its meaning in the notations listing itself instead of merely giving the place where the notation is first used.

The index itself is meant to be not only an index of definitions but also an index of examples, theorems, and constructions. Thus, e.g., under "formal group law, universal, one-dimensional" the reader will find D: 1.5, C: 5.2, T: 5.3, 5.5 meaning that the concept is defined in Section 1.5, a construction can be found in Section 5.2, and two important theorems concerning these objects can be found in 5.3 and 5.5. In this connection E stands for "example."

Finally, all sections, subsections, theorems, definitions, diagrams, scholia, formulas, addenda, propositions, lemmas, ... are numbered by means of one subset of $(\mathbf{N} \cup \{0\})^3$, lexicographically ordered, for the whole book; we have used the abbreviations *a* and *a.b* for (*a*.0.0) and (*a.b*.0). The beginning of a new subsection (*a.b.c*) is marked with a square in the left margin. A subsection (*a.b.c*) continues until the next lexicographically larger number occurs with a square in the left margin (as a ((sub)sub) section heading, not as a see below reference). Cross referencing within a chapter is done by giving the appropriate element of $(\mathbf{N} \cup \{0\})^3$. When referring to a result or formula in another chapter we occasionally indulge in a bit of redundancy by listing the chapter number as well.

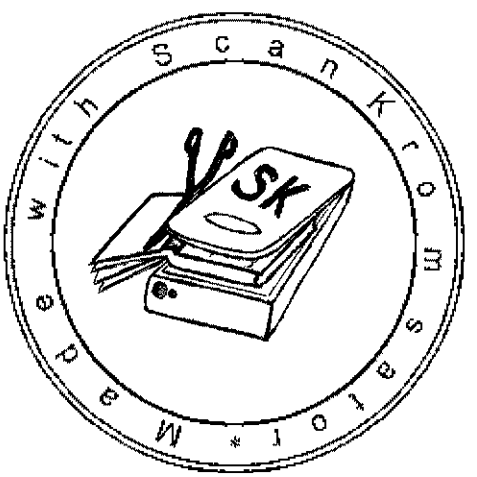
L.3 Interdependence of Chapters and Sections

A rough indication of the interdependence of chapters and sections is given by the following diagram. The encircled numbers are the sections that are mainly relevant for the dependence arrow in question.



Personally, I feel that the dependencies suggested by the diagram are too strong rather than too weak. For instance, for a course on formal groups in algebraic topology, one certainly does not need all of 2, 3, 5, 10, 16, 19, 22. Especially of 16 and 19, 22 only selected bits are needed, and 10 is not needed at all.

This page intentionally left blank



INTRODUCTION

An n-dimensional formal group law over a ring A is an n-tuple of power series $F(X, Y)$ in $X_1, \ldots, X_n; Y_1, \ldots, Y_n$ with coefficients in A such that

$$F(X, 0) = X, \qquad F(0, Y) = Y, \qquad F(X, F(Y, Z)) = F(F(X, Y), Z)$$

(where X and Y are short for the vectors $(X_1, \ldots, X_n)$, $(Y_1, \ldots, Y_n)$). If moreover $F(X, Y) = F(Y, X)$, the formal group law is said to be commutative. Three most important examples are $\hat{\mathbf{G}}_a(X, Y) = X + Y$, $\hat{\mathbf{G}}_m(X, Y) = X + Y + XY$ (both one dimensional) and the infinite dimensional formal group law $\hat{W}_{p^\infty}(X, Y)$ defined by the addition polynomials $\Sigma_0(X; Y)$, $\Sigma_1(X; Y)$, ... over $\mathbf{Z}$ of the Witt vectors, which in turn are defined by

$$w_{p^n}(\Sigma_0, \ldots, \Sigma_n) = w_{p^n}(X) + w_{p^n}(Y)$$

where

$$w_{p^n}(X) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$$

One way to view formal group laws is as recipes for manufacturing ordinary groups (by substituting, say, topologically nilpotent elements for the X_i and Y_i).

There are at least three ways in which formal group laws arise naturally:

(a) Let G be an n-dimensional analytic Lie group. Let $e \in G$ be the identity element of G. Take analytic coordinates in a neighborhood V of e such that e has coordinates $(0, 0, \ldots, 0)$. Let $x, y \in V$ have coordinates $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, respectively. If x and y are close enough to e, we have $z = xy \in V$. Let $z_1, \ldots, z_n$ be the coordinates of z. Now since G is analytic, the z_i are analytic in the $x_1, \ldots, x_n; y_1, \ldots, y_n$; and taking a power series development around $(0, 0, \ldots, 0)$, we have for x, y close enough to e n power series

$$z_i = f_i(x_1, \ldots, x_n; y_1, \ldots, y_n)$$

These n power series define a formal group law $\hat{G}(x, y)$ in the sense of the definition above. They constitute so to speak the infinitesimal group structure of order ∞ at e of G. In particular the Lie algebra $\mathfrak{g}$ of G is recoverable from $\hat{G}$, and thus $\hat{G}$ is an intermediate object between $\mathfrak{g}$ and G.

Now much the same construction can be performed for a smooth algebraic group G defined, say, over a field k of characteristic $p > 0$. In this case the Lie

algebra of G carries very little information about G, and it was as a possibly good substitute for Lie theory in the case of characteristic $p > 0$ that the theory of formal groups found its first vigorous development in the hands of Dieudonné.

In particular, in the case of abelian varieties A, the associated formal group law $\hat{A}$ has since been found to carry much information on the arithmetic of A.

(b) Let $L(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be a Dirichlet series with coefficients in $\mathbf{Z}$. One associates to $L(s)$ the power series $f_L(X) = \sum_{n=1}^{\infty} n^{-1}a(n)X^n \in \mathbf{Q}[\![X]\!]$ and $F_L(X, Y) = f_L^{-1}(f_L(X) + f_L(Y))$ where $f_L^{-1}(X)$ is defined by $f_L^{-1}(f_L(X)) = X$. Then the coefficients of $F_L(X, Y)$ are in $\mathbf{Z}_{(p)}$ precisely when $L(s)$ has an Euler factor for the prime p in the sense that

$$L(s) = (1 + e_1 p^{-s} + e_2 p^{1-2s} + e_3 p^{2-3s} + \cdots)^{-1} \sum_{n=1}^{\infty} b(n)n^{-s}$$

with $b(n) \equiv 0 \bmod p^r$ if $p^r \mid n$, $e_i \in \mathbf{Z}_p$. These two ways in which formal group laws arise in nature are not independent. Indeed, it is precisely the connection between (a) and (b) which, e.g., in the case of elliptic curves E over $\mathbf{Q}$, gives some beautiful results concerning the zeta function of E.

(c) Let h^* be a multiplicative extraordinary cohomology theory which has first Chern classes in a suitable technical sense. Then (because $\mathbf{CP}^{\infty}$ is classifying for line bundles) there is a universal formula

$$c_1(\xi \otimes \eta) = \sum_{i,j} a_{ij} c_1(\xi)^i c_1(\eta)^j$$

which gives the first Chern class of a tensor product of two complex line bundles in terms of the first Chern classes of the factors. The power series $F_h(X, Y) = \sum a_{ij} X^i Y^j$ is then a one dimensional formal group law over $h(pt)$, the ring of coefficients of h^*; and, as it turns out, $F_h(X, Y)$ carries a good deal of information about h^*.

These three classes of examples make it reasonable to study formal group laws more deeply (even if one did not know about other applications, for example to local class field theory and global class field theory for function fields).

Now in any case for the class of examples arising from analytic Lie groups, the formal group laws are intermediate between Lie groups and Lie algebras. So there ought to be "formal Lie theory," that is, Lie theory without convergence. And indeed, specializing to the one dimensional case, one has: let $F(X, Y)$ be a one dimensional commutative formal group law over a $\mathbf{Q}$-algebra R, then there is a unique power series $f(X) \in R[\![X]\!]$ such that $f(X) = X + \cdots$ and $f(F(X, Y)) = f(X) + f(Y)$. This $f(X)$ is called the logarithm of $F(X, Y)$. So if $F(X, Y)$ is, e.g., a formal group law over $\mathbf{Z}$, then over $\mathbf{Q}$ there exists a power series $f(X) \equiv X \bmod(\text{degree } 2)$ such that $F(X, Y) = f^{-1}(f(X) + f(Y))$. Thus

the problem of finding all one dimensional formal group laws over $\mathbf{Z}$ becomes, What power series $f(X)$ over $\mathbf{Q}$ are such that $f^{-1}(f(X)+f(Y))$ has integral coefficients? In (b) above we have seen an example of this. Roughly the condition is that $f(X)$ must exhibit the kind of regularity exemplified by the splitting off of an Euler factor in the sense indicated in (b).

The precise answer is given by what I call the functional equation lemma, which is, without a doubt the most important tool in this book. The precise statement of the functional equation lemma takes more space than one should use in an introduction, so let us try to see by means of examples what kind of lemma it is.

(d) Let $f(X), g(X) \in \mathbf{Q}[\![X]\!]$ be two power series in one variable X such that $f(X) \equiv g(X) \equiv X \mod(\text{degree } 2)$ and $f(X) - p^{-1}f(X^p) \in \mathbf{Z}_{(p)}[\![X]\!]$, $g(X) - p^{-1}g(X^p) \in \mathbf{Z}_{(p)}[\![X]\!]$. Then $F(X, Y) = f^{-1}(f(X)+f(Y))$ and $g^{-1}(f(X))$ have their coefficients in $\mathbf{Z}_{(p)}$ (not just $\mathbf{Q}$). Thus, for example, Hasse's lemma that $\exp(X + p^{-1}X^p + p^{-2}X^{p^2} + \cdots)$ has its coefficients in $\mathbf{Z}_{(p)}$ is an application of the functional equation lemma. This is of course related to the statement made under (b). The Euler factor in this case is $1 - p^{-s}$.

(e) Let $f(X) \in \mathbf{Q}[T][\![X]\!]$ be the power series

$$f(X) = X + p^{-1}TX^{p^h} + p^{-2}TT^{p^h}X^{p^{2h}} + p^{-3}TT^{p^h}T^{p^{2h}}X^{p^{3h}} + \cdots$$

then $f^{-1}(f(X)+f(Y))$ has its coefficients in $\mathbf{Z}[T]$. This actually gives us quite a few different formal group laws over $\mathbf{Z}$ by substituting $h = 1, 2, \ldots$ and, e.g., $T = 1$. (These are, incidentally, the formal group laws associated to the so-called extraordinary K-theories.)

(f) Consider the Witt polynomials $w_{p^n}(X) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^nX_n$. It is obvious that they satisfy $w_{p^n}(X) \equiv w_{p^{n-1}}(X^p) \bmod p^n$. And, given this, the functional equation lemma says that the polynomials $\Sigma_0, \Sigma_1, \ldots$ determined by $w_{p^n}(\Sigma_0, \ldots, \Sigma_n) = w_{p^n}(X) + w_{p^n}(Y)$, $n = 0, 1, 2, \ldots$, have coefficients in $\mathbf{Z}$.

(g) Let $L(s)$ be a Dirichlet series with Euler factor $1 + e_1p^{-s} + e_2p^{1-2s} + \cdots$ as in (b). Let $h(X)$ be any power series with coefficients in $\mathbf{Z}$ and let $f_L(h(X)) = g(X) = \sum_{n=1}^{\infty} n^{-1}d(n)X^n$. Then

$$\sum d(n)n^{-s} = (1 + e_1p^{-s} + e_2p^{1-2s} + \cdots)^{-1} \sum c(n)n^{-s}$$

with $c(n) \equiv 0 \bmod p^r$ if $p^r \mid n$. That is, the same Euler factor splits off. And this is how we shall prove the Atkin–Swinnerton–Dyer conjectures in Section 33.2.

(h) Let R be a ring in which all prime numbers $\neq p$ are invertible and suppose that R is torsion free. Let $F(X, Y)$ be a formal group law over R and let $f(X) \in R \otimes \mathbf{Q}[\![X]\!]$ be the logarithm of $F(X, Y)$. Write $f(X) = \sum a_nX^n$ and let $\hat{f}(X) = \sum a_{p^m}X^{p^m}$. Then via the functional equation lemma one finds that $\hat{F}(X, Y) = \hat{f}^{-1}(\hat{f}(X)+\hat{f}(Y))$ has its coefficients in R. (Note that the relation

between $f(X)$ and $\hat{f}(X)$ is the same as between the ordinary logarithm, $-\log(1-X) = X + 2^{-1}X^2 + 3^{-1}X^3 + \cdots$ and Hasse's p-logarithm $H(X) = X + p^{-1}X^p + p^{-2}X^{p^2} + \cdots$.) Now this so-called p-typification operation can be applied in topology to split off from complex cobordism cohomology $MU^*_{(p)}$ (localized at (p)) a factor BP^* (Brown–Peterson cohomology) which so to speak involves only the prime number p.

The formal group laws of MU^* and BP^* have the following logarithms

$$\log_{MU}(X) = \sum_{n=0}^{\infty} \frac{[\mathbf{CP}^n]}{n+1} X^{n+1}, \qquad \log_{BP}(X) = \sum_{n=0}^{\infty} \frac{[\mathbf{CP}^{p^n-1}]}{p^n} X^{p^n}$$

where $[\mathbf{CP}^m]$ is the class of complex projective space of complex dimension m. Now $F_{MU}(X, Y)$ turns out to be a universal one dimensional formal group law, and it follows that $F_{BP}(X, Y)$ is universal for formal group laws whose logarithms involve only the X^{p^n} and no other powers of X.

Now let $f_V(X)$ over $\mathbf{Q}[V_1, V_2, \ldots]$ be the power series

$$(*) \qquad f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}$$

$$a_0(V) = 1, \qquad p a_n(V) = a_{n-1}(V) V_1^{p^{n-1}} + \cdots + a_1(V) V_{n-1}^p + a_0(V) V_n$$

and let $F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y))$. Then, again, the functional equation lemma gives us that $F_V(X, Y)$ has its coefficients in $\mathbf{Z}[V]$. And one finds another formal group law which is universal for formal group laws whose logarithms involve only the powers X^{p^n} of X. It follows that $BP(pt)$ and $\mathbf{Z}_{(p)}[V]$ are identifiable in such a way that $a_n(V)$ corresponds to $p^{-n}[\mathbf{CP}^{p^n-1}] = m_n \in BP(pt)$. Then because we have formulas for the V_n in terms of the $a_n(V)$, we find polynomial generators $v_1, v_2, \ldots$ of $BP(pt)$ related to m_n by

$$p m_n = m_{n-1} v_1^{p^{n-1}} + \cdots + m_1 v_{n-1}^p + v_n$$

These generators $v_1, v_2, \ldots$ have proved to be useful for calculations on a number of occasions (e.g., to prove that certain elements in the stable homotopy groups of the spheres are nonzero).

(i) A further contribution of the functional equation lemma to our understanding of formal group laws is that it practically dictates how the logarithm of a universal formal group law should look. It must be (in a certain sense) of the form

$$f_U(X) = \sum a_n(u) X^n$$

$$a_n(u) = \sum_{(i_1, \ldots, i_s)} d(i_1, \ldots, i_s) U_{i_1} U_{i_2}^{i_1} \cdots U_{i_s}^{i_1 \cdots i_{s-1}}$$

where the sum is over all sequences $(i_1, \ldots, i_s)$, $i_j \in \mathbf{N}$, such that $i_1 \cdots i_s = n$ and where the $d(i_1, \ldots, i_s)$ are certain coefficients which can be specified recursively.

In this connection let me remark that to the human eye at least all the

regularity in a universal formal group law sits in its logarithm not in the formal group law itself—maybe understandably, as the differential $f'(X)\,dX$ of the logarithm $f(X)$ can easily be interpreted as the unique (up to a scalar factor) invariant differential on the formal group law $F(X, Y)$.

To illustrate this remark I have written at the end of this introduction the first few terms of the "3-typical" universal formal group law $F_V(X, Y)$, whose logarithm (cf. (*) above) is certainly eminently regular and also the first few terms of the universal formal group law $F_U(X, Y)$. (The calculations were done by computer to degree 23 for $F_V(X, Y)$ and degree 11 for $F_U(X, Y)$.)

In this introduction I have not tried to give a short description of the contents of the book. For that, the curious reader is invited to glance at the table of contents which is reasonably detailed. Instead, I have tried to give the flavor of some of the more important constructions and results, and I have tried to give some small indication of how diverse and sometimes surprising the applications of the theory of formal groups are.

> Nobody who falls down stairs like that can be all bad. (R. A. Lafferty, *Fourth Mansions*)

The first few terms of the one dimensional universal formal group law $F_U(X, Y)$

$$
\begin{aligned}
F_U(X, Y) = {} & X + Y + XY(-U_2) + (XY^2 + X^2Y)(-U_3 + U_2^2) \\
& + (XY^3 + X^3Y)(-2U_4 + 2U_2U_3 + 2U_2^3) \\
& + X^2Y^2(-3U_4 + 4U_2U_3 - 4U_2^3) \\
& + (XY^4 + X^4Y)(-U_5 + 4U_2U_4 - 3U_2^2U_3 + 3U_2^3 + U_3^2) \\
& + (X^2Y^3 + X^3Y^2) \\
& \times (-2U_5 + 11U_2U_4 - 11U_2^2U_3 + 10U_2^3 + 3U_3^2) \\
& + (XY^5 + X^5Y) \\
& \times (-6U_6 + 2U_5U_2 - 6U_2U_3^2 \\
& \qquad + 4U_3U_4 - 6U_2^2U_4 + 2U_2^3U_3 - 4U_2^5) \\
& + (X^2Y^4 + X^4Y^2) \\
& \times (-15U_6 + 7U_5U_2 - 22U_2U_3^2 \\
& \qquad + 15U_3U_4 - 28U_2^2U_4 + 21U_2^3U_3 - 21U_2^5) \\
& + X^3Y^3 \\
& \times (-20U_6 + 10U_5U_2 - 33U_2U_3^2 + 22U_3U_4 \\
& \qquad - 43U_2^2U_4 + 37U_2^3U_3 - 34U_2^5) \\
& + \cdots
\end{aligned}
$$

By the time one reaches degree 11 the coefficient of X^5X^6 involves 42 different monomials in the U's with coefficients like 78447.

The first few terms of the one dimensional universal p-typical formal group law $F_V(X, Y)$ (for the prime $p = 3$).

$$
\begin{aligned}
F_V(X, Y) = {} & X + Y + (XY^2 + Y^2X)(-V_1) \\
& + (XY^4 + X^4Y)(V_1^2) + (X^2Y^3 + X^3Y^2)(3V_1^2) \\
& + (XY^6 + X^6Y)(-V_1^3) + (X^3Y^5 + X^5Y^2)(-6V_1^3) \\
& + (X^3Y^4 + X^4Y^3)(-13V_1^3) \\
& + (XY^8 + X^8Y)(-3V_2) + (X^2Y^7 + X^7Y^2)(-12V_2 + 6V_1^4) \\
& + (X^3Y^6 + X^6Y^3)(-28V_2 + 27V_1^4) \\
& + (X^4Y^5 + X^5Y^4)(-42V_2 + 52V_1^4) \\
& + (XY^{10} + X^{10}Y)(6V_1V_2 + V_1^5) + (X^2Y^9 + X^9Y^2)(45V_1V_2) \\
& + (X^3Y^8 + X^8Y^3)(163V_1V_2 - 27V_1^5) \\
& + (X^4Y^7 + X^7Y^4)(362V_1V_2 - 106V_1^5) \\
& + (X^5Y^6 + X^6Y^5)(532V_1V_2 - 192V_1^5) \\
& + \cdots \\
& + (X^{10}Y^{13} + X^{13}Y^{10}) \\
& \times (-105024048V_1^3V_2^2 + 95416130V_1^7V_2 + 21339672V_1^{11}) \\
& + \cdots
\end{aligned}
$$

FORMAL GROUPS AND APPLICATIONS

CHAPTER I

METHODS FOR CONSTRUCTING ONE DIMENSIONAL FORMAL GROUPS

1 Definition and Elementary Properties of Formal Groups Survey of the Results of Chapter I

Let A be a ring. A ring will always mean a commutative associative ring A with identity element $1 \in A$. All algebras over A will be unitary and commutative.

1.1 Definition and examples

A one dimensional formal group law over a ring A is a formal power series in two variables $F(X, Y) \in A[\![X, Y]\!]$ of the form

$$F(X, Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j \tag{1.1.1}$$

such that the following associativity condition holds

$$F(X, F(Y, Z)) = F(F(X, Y), Z) \tag{1.1.2}$$

If one has in addition

$$F(X, Y) = F(Y, X) \tag{1.1.3}$$

the formal group is said to be *commutative.*

(Note that condition (1.1.2) makes sense because $F(X, Y)$ has no constant term.)

■ (1.1.4) **Lemma** Let $F(X, Y)$ be a formal group law over a ring A. Then there exists a power series $\imath(X) = -X + b_2 X^2 + \cdots$ with coefficients in A such that $F(X, \imath(X)) = 0$.

Proof Exercise, or see Appendix (A.4.7).

■(1.1.5) **Examples** Some examples of one dimensional formal group laws are

(1.1.6) $\hat{\mathbf{G}}_a(X, Y) = X + Y$ (the additive formal group law)

(1.1.7) $\hat{\mathbf{G}}_m(X, Y) = X + Y + XY$ (the multiplicative formal group law)

Both these formal group laws are commutative. To obtain a noncommutative example, let A be a ring that contains an element $\varepsilon \neq 0$ such that $\varepsilon^2 = 0$ and $p\varepsilon = 0$ for some prime number p. For example, $A = k[\varepsilon]/(\varepsilon^2)$ where k is a field of characteristic p. Let

(1.1.8) $$F(X, Y) = X + Y + \varepsilon X Y^p$$

One checks relatively easily that then $F(F(X, Y), Z) = F(X, F(Y, Z))$, so that (1.1.8) does define a formal group law.

None of these examples can be considered typical. On one hand, we have the exercise: suppose A is a ring with no nilpotents and $F(X, Y)$ is a polynomial over A of the form $F(X, Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j$ such that $F(F(X, Y), Z) = F(X, F(Y, Z))$, then $F(X, Y)$ is of the form $X + Y + cXY$; and on the other hand, we have the theorem that if A does not contain elements $a \neq 0$ that are nilpotent and such that $na = 0$ for some $n \in \mathbf{N}$, then every one dimensional formal group law over A is commutative. This will be proved in Section 6.

(To do the exercise mentioned above suppose that the degree in X in $F(X, Y)$ is ≥ 2; now consider the degree in X of $F(X, F(Y, Z))$ and $F(F(X, Y), Z)$ to obtain a contradiction; to prove that the degree in Y in $F(X, Y)$ is ≤ 1 consider the degree in Z of $F(F(X, Y), Z)$ and $F(X, F(Y, Z))$.)

1.2 Curves

The power series $F(X, Y)$ over A can be viewed as a recipe for manufacturing ordinary groups. Consider for instance power series in one variable without constant term $\gamma(t) = b_1 t + b_2 t^2 + \cdots$ with coefficients in A. Given two such power series $\gamma_1(t)$, $\gamma_2(t)$ the expression $F(\gamma_1(t), \gamma_2(t))$ makes sense, and we can define an addition on the set of all such power series by means of the formula

(1.2.1) $$\gamma_1(t) +_F \gamma_2(t) = F(\gamma_1(t), \gamma_2(t))$$

This turns the set of all power series without constant term into a group, which we shall denote $\mathscr{C}(F)$. This group is commutative if $F(X, Y)$ is commutative. The zero element of $\mathscr{C}(F)$ is the zero power series and for $\gamma(t) \in \mathscr{C}(F)$ we have $\gamma(t) +_F \iota(\gamma(t)) = 0$, where $\iota(X)$ is the power series of (1.1.4). This group, when enriched with further structure, will be most important for the classification of formal groups. To whet the appetite we remark at this point that $\mathscr{C}(\hat{\mathbf{G}}_m)$ turns out to be the underlying additive group of the ring of Witt vectors $W(A)$ (Witt

vectors for all primes simultaneously; cf. Section 17 for more details on Witt vectors and this particular connection with formal groups).

1.3 Formal group laws and formal groups

Let B be a (commutative) A-algebra and let $\mathfrak{n}(B)$ be the ideal of nilpotent elements of B. Then the addition $x +_F y = F(x, y)$ defines a (new) group structure on $\mathfrak{n}(B)$. Thus a formal group law $F(X, Y)$ defines a functor F: $\mathbf{Alg}_A \to \mathbf{Group}$, where $\mathbf{Alg}_A$ denotes the category of (commutative) unitary algebras over A and **Group** denotes the category of groups. This functor F is the *formal group* (or occasionally *formal group scheme*) associated to the formal group law $F(X, Y)$. This functorial point of view will not play a large role in this book, and the reader uninured to or intolerant of categorical matters has nothing to worry about.

More generally, let B be a complete topological algebra over A where the topology on B is defined by means of an ideal I of B such that $\bigcap_n I^n = \{0\}$ (so that the topology on B is Hausdorff). Then $F(x, y)$ is a convergent series for all $x, y \in I$ and defines an element of I, which gives us a group structure on I. The construction of 1.2 is an instance of this.

1.4 Homomorphisms and isomorphisms

Let $F(X, Y)$, $G(X, Y)$ be two formal group laws over A. A *homomorphism* (over A) $F(X, Y) \to G(X, Y)$ is a power series $\alpha(X) = b_1 X + b_2 X^2 + \cdots$ with coefficients in A without constant term such that

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y)) \tag{1.4.1}$$

This condition means precisely that α induces homomorphisms between the various ordinary groups that one can manufacture out of $F(X, Y)$, $G(X, Y)$ as in 1.2 and 1.3. The homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is an *isomorphism* if there exists a homomorphism $\beta(X)$: $G(X, Y) \to F(X, Y)$ such that $\alpha(\beta(X)) = X = \beta(\alpha(X))$. Exercise: the homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is an isomorphism if and only if $b_1 \in U(A)$, the group of units of A.

These notions of homomorphism and isomorphism fit with the functorial point of view of 1.3 in that two formal groups $F(X, Y)$, $G(X, Y)$ are isomorphic if and only if their associated functors F and G are isomorphic (as functors $\mathbf{Alg}_A \to \mathbf{Group}$). This is easily seen by considering the element X in the A-algebras $A[X]/(X^n)$ for $n = 1, 2, \ldots$. Similarly, every morphism between the group-valued functors F and G "comes from" a power series $\alpha(X) = b_1 X + b_2 X^2 + \cdots$.

An isomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$, $\alpha(X) = b_1 X + b_2 X^2 + \cdots$ is called a *strict* isomorphism if $b_1 = 1$.

■ (1.4.2) **Example of an isomorphism** Let $E(X)$ and $\log(1+X)$ be the power series

$$E(X)=\sum_{n=1}^{\infty}\frac{X^n}{n!},\qquad \log(1+X)=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n} \tag{1.4.3}$$

and consider the formal group laws $\hat{\mathbf{G}}_m(X, Y)$ and $\hat{\mathbf{G}}_a(X, Y)$ of (1.1.5) over $\mathbf{Q}$, the field of rational numbers. Then $E(X)$ and $\log(1+X)$ define mutually inverse strict isomorphisms over $\mathbf{Q}$:

$$E(X)\colon \hat{\mathbf{G}}_a(X, Y)\to\hat{\mathbf{G}}_m(X, Y),\qquad \log(1+X)\colon \hat{\mathbf{G}}_m(X, Y)\to\hat{\mathbf{G}}_a(X, Y) \tag{1.4.4}$$

On the other hand, let k be a field of characteristic $p>0$. The power series $\hat{\mathbf{G}}_m(X, Y)$ and $\hat{\mathbf{G}}_a(X, Y)$ can also be seen as power series with coefficients in k. These two formal group laws are definitely not isomorphic as formal group laws over k.

To see this we first define the power series $[n]_F(X)$, $n\in\mathbf{Z}$, for every commutative one dimensional formal group law $F(X, Y)$ over a ring A.

These are defined as follows

(1.4.5)

$$[1]_F(X)=X,\qquad [n]_F(X)=F(X,[n-1]_F(X))\quad\text{if } n\geq 2,\quad [0]_F(X)=0$$
$$[-1]_F(X)=\imath(X),\quad [-n]_F(X)=\imath([n]_F(X))\qquad\text{if } n\geq 2$$

For the formal groups $\hat{\mathbf{G}}_a(X, Y)$, $\hat{\mathbf{G}}_m(X, Y)$, one easily checks that if $n\geq 0$,

$$[n]_{\hat{\mathbf{G}}_a}(X)=nX,\qquad [n]_{\hat{\mathbf{G}}_m}(X)=(1+X)^n-1 \tag{1.4.6}$$

Now if $\hat{\mathbf{G}}_a(X, Y)$ and $\hat{\mathbf{G}}_m(X, Y)$ were isomorphic over a characteristic $p>0$ field k, then there would be a power series over k $\alpha(X)=b_1X+b_2X^2+\cdots$ with $b_1\neq 0$ such that $[p]_{\hat{\mathbf{G}}_a}(\alpha(X))=\alpha([p]_{\hat{\mathbf{G}}_m}(X))=\alpha(X^p)$, which is a contradiction.

1.5 Change of rings and universal formal group laws

Let $F(X, Y)$ be a formal group law over a ring A and let $\phi\colon A\to B$ be a homomorphism of rings. Suppose $F(X, Y)=X+Y+\sum c_{ij}X^iY^j$, then by applying ϕ to the coefficients of $F(X, Y)$ we obtain a formal group law

$$\phi_*F(X, Y)=X+Y+\sum\phi(c_{ij})X^iY^j \tag{1.5.1}$$

over the ring B.

■ (1.5.2) **Definition** (universal formal group laws) A (one dimensional commutative) formal group law $F(X, Y)$ over a ring L (the L stands for Lazard) is a *universal* (one dimensional commutative) formal group law iff for every formal group law $G(X, Y)$ over a ring A there is a unique ring homomorphism $\phi\colon L\to A$ such that $\phi_*F(X, Y)=G(X, Y)$.

The ring L is (up to isomorphism) uniquely determined by this definition. Indeed, if $F(X, Y)$ over L and $F'(X, Y)$ over L' are two universal one dimensional commutative formal group laws, then by the requirements of the definition there are unique homomorphisms ϕ: $L \to L'$, ψ: $L' \to L$ such that $\phi_* F(X, Y) = F'(X, Y)$, $\psi_* F'(X, Y) = F(X, Y)$; and by uniqueness we must have $\phi\psi = id_{L'}$, $\psi\phi = id_L$, so that L and L' are isomorphic.

■ (1.5.3) **Existence of universal formal group laws** It is a trivial matter to show that there exists a universal one dimensional commutative formal group law over some ring L. Indeed, let $\tilde{L} = \mathbf{Z}[\ldots, C_{ij}, \ldots; i, j = 1, 2, \ldots]$ where the C_{ij} are indeterminates and consider the formal power series

$$F_C(X, Y) = X + Y + \sum_{i,j \geq 1} C_{ij} X^i Y^j$$

We write

$$(1.5.4) \qquad F_C(F_C(X, Y), Z) - F_C(X, F_C(Y, Z)) = \sum_{i,j,k} P_{ijk}(C) X^i Y^j Z^k$$

where the $P_{ijk}(C)$, $i, j, k = 0, 1, 2, \ldots$, are certain polynomials in the C_{lm}. Let $\mathfrak{A}$ in $\tilde{L}$ be the ideal generated by the elements

$$C_{ij} - C_{ji}, \quad i, j = 1, 2, \ldots; \qquad P_{ijk}(C), \quad i, j, k = 0, 1, 2, \ldots$$

and let $L = \tilde{L}/\mathfrak{A}$ and let $F(X, Y) = \chi_* F_C(X, Y)$ where χ: $\tilde{L} \to L$ is the natural projection. Then $F(X, Y)$ over L is clearly a universal one dimensional commutative formal group law.

It is a totally different matter to determine the structure of the ring L. It is one of the main goals of this chapter to show that L is (isomorphic to) $\mathbf{Z}[U_2, U_3, U_4, \ldots]$, where the U_i, $i = 2, 3, 4, \ldots$, are indeterminates, and to exhibit a (more or less) explicit universal one dimensional commutative formal group over $\mathbf{Z}[U]$.

1.6 Survey of some of the results of Chapter I

To prove that $L = \mathbf{Z}[U]$ and to construct an explicit universal formal group over $\mathbf{Z}[U]$ we first discuss a general (and powerful) method for constructing formal group laws over characteristic zero rings. Here a characteristic zero ring is defined to be a ring A such that the natural map $A \to A \otimes \mathbf{Q}$ is injective; i.e., A has no (additive) torsion. This method of constructing one dimensional formal group laws is as follows. Let A be a characteristic zero ring and let $f(X) = X + a_2 X^2 + \cdots$ be a power series with coefficients in $A \otimes \mathbf{Q}$. Let $f^{-1}(X)$ be the inverse function power series of $f(X)$; i.e., $f^{-1}(X)$ is a power series over $A \otimes \mathbf{Q}$ such that $f^{-1}(f(X)) = X = f(f^{-1}(X))$. (To prove existence of $f^{-1}(X)$ is an easy exercise; cf. also Appendix (A.4.6).) Now define

$$(1.6.1) \qquad F(X, Y) = f^{-1}(f(X) + f(Y))$$

Then one trivially has $F(X, Y) = F(Y, X)$ and $F(F(X, Y), Z) = F(X, F(Y, Z))$, so the power series (1.6.1) is in any case a one dimensional commutative formal group law over $A \otimes \mathbf{Q}$ (albeit not a very interesting one since it is isomorphic (via $f(X)$) over $A \otimes \mathbf{Q}$ to the additive formal group law $\hat{\mathbf{G}}_a(X, Y)$ over $A \otimes \mathbf{Q}$). However, if $f(X)$ satisfies a certain type of functional equation (one for every prime number p that is not invertible in A) or, equivalently, if $f(X)$ is obtainable by means of a certain type of recursive procedure, then $F(X, Y)$ actually has its coefficients in $A \subset A \otimes \mathbf{Q}$ and then (1.6.1) defines a one dimensional commutative formal group law over A (which, as a rule, is definitely not isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ over A). This functional equation–integrality lemma is the subject of Section 2 below. This lemma is very much related to integrality statements of the following sort: let $H(X) = X + p^{-1}X^p + p^{-2}X^{p^2} + \cdots$ and $\exp(X) = \sum (n!)^{-1}X^n$ be the usual exponential series, then $\exp(H(X))$ has no denominators divisible by p. That is, the integrality statements of Section 2 are of the Witt vector type and there are Artin–Hasse exponentials floating around.

We use this method of constructing formal group laws to construct a number of interesting formal group laws in Sections 3 and 5. One of these (the one constructed in Section 5) turns out to be a universal one dimensional commutative formal group law. It is defined over $\mathbf{Z}[U] = \mathbf{Z}[U_2, U_3, \ldots]$. To prove this one needs a bit of binomial coefficient arithmetic (Section 4).

At this point a number of theorems appear as fairly easy corollaries of the work that has been done so far. They are the following:

■ (1.6.2) **Theorem** Every one dimensional commutative formal group law over a $\mathbf{Q}$-algebra A is strictly isomorphic over A to the additive one dimensional formal group law over A.

Two elements in a power series ring $A[\![X_1, \ldots, X_n]\!]$ are said to be congruent mod(degree m) if they are congruent modulo the closed ideal of $A[\![X_1, \ldots, X_n]\!]$ generated by the monomials $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ with $i_1 + i_2 + \cdots + i_n \geq m$.

A polynomial of total degree $\leq m$, $F_m(X, Y) = X + Y + \sum_{i,j\geq 1} c_{ij}X^iY^j$ is called a commutative one dimensional formal group law chunk of order m if $F_m(X, F_m(Y, Z))$ and $F_m(F_m(X, Y), Z)$ are congruent mod(degree $m + 1$) and $F_m(X, Y) = F_m(Y, X)$. With this terminology one has:

■ (1.6.3) **Theorem** Every one dimensional commutative formal group law chunk of order m, $m \geq 1$, comes from a one dimensional commutative formal group. That is, if $F_m(X, Y)$ is a one dimensional commutative formal group law chunk over a ring A, then there is a one dimensional commutative formal group $F(X, Y)$ over A such that $F_m(X, Y) \equiv F(X, Y)$ mod(degree $m + 1$).

For each $n \in \mathbf{N}$, we define $\nu(n)$ as

$$(1.6.4)\quad \nu(n) = \begin{cases} 1 & \text{if } n \text{ is not a power of a prime number or } n = 1 \\ p & \text{if } n = p^r, \quad r \in \mathbf{N}, \quad \text{where } p \text{ is a prime number} \end{cases}$$

and we define a polynomial $C_n(X, Y)$ as

$$C_n(X, Y) = v(n)^{-1}\{-(X + Y)^n + X^n + Y^n\} \tag{1.6.5}$$

Note that $C_n(X, Y)$ is a polynomial with coefficients in $\mathbf{Z}$. The third useful corollary is now:

■ (1.6.6) **Lemma** If $F(X, Y)$, $G(X, Y)$ are two commutative one dimensional formal group laws over a ring A and $F(X, Y) \equiv G(X, Y)$ mod(degree m), $m \geq 2$, then there is an element $b \in A$ such that $F(X, Y) \equiv G(X, Y) + bC_m(X, Y)$ mod(degree $m + 1$).

All these results have their higher dimensional analogues. In Section 6 we deal with a phenomenon that is special for dimension 1, viz.:

■ (1.6.7) **Theorem** Every one dimensional formal group law over a ring A is commutative if and only if A contains no elements $a \neq 0$ that are both torsion and nilpotent. (That is, there must be no elements $a \in A$, $a \neq 0$, for which there are $n, m \in \mathbf{N}$ such that $na = a^m = 0$.)

The chapter closes with two more methods of constructing formal group laws. One (due to Honda) uses (essentially) the same functional equation lemma as used to construct the formal group laws of Sections 3 and 5. The second one (due to Lubin and Tate) is essentially a special case, but merits separate treatment because of elegance and various applications.

The simplest example of such a Lubin–Tate formal group law is obtained as follows. Let A be a nontrivial discrete valuation ring with residue field k of q elements. Choose a uniformizing element π. Let K be the quotient field of A and let $f(X) \in K[\![X]\!]$ be the power series

$$f(X) = X + \pi^{-1}X^q + \pi^{-2}X^{q^2} + \cdots$$

and define

$$F(X, Y) = f^{-1}(f(X) + f(Y)), \quad [a]_F(X) = f^{-1}(af(X)) \quad \text{for } a \in A \tag{1.6.8}$$

where $f^{-1}(X)$ is the inverse power series; i.e., $f^{-1}(f(X)) = f(f^{-1}(X)) = X$; cf. Appendix (A.4.5).

■ (1.6.9) **Theorem** $F(X, Y)$ is a formal group law over A, and $[a]_F(X)$ is an endomorphism over A of $F(X, Y)$ for all $a \in A$.

The essential fact, which sees to it that the power series $F(X, Y)$ and $[a]_F(X)$ have their coefficients in A, is that $f(X)$ satisfies

$$f(X) - \pi^{-1}f(X^q) \in A[\![X]\!] \tag{1.6.10}$$

(and we need $f(X) \equiv X$ mod(degree 2) or at least $f(X) \equiv uX$ mod(degree 2) where u is a unit of A). This is another instance of the functional equation lemma already mentioned.

2 The Functional Equation–Integrality Lemma

In this section we discuss our main tool for proving integrality statements.

2.1 Ingredients and constructions

The basic ingredients for the constructions in this section are

(2.1.1) $\quad A \subset K, \qquad \sigma\colon K \to K, \qquad \mathfrak{A} \subset A, \qquad p, \quad q, \quad s_1, \quad s_2, \quad \ldots$

where A is a subring of a ring K, $\sigma\colon K \to K$ is a ring homomorphism, $\mathfrak{A}$ is an ideal of A, p is a prime number, q a power of p, and $s_1, s_2, \ldots$ are elements of K.

These ingredients are supposed to satisfy the following conditions:

(2.1.2) $\quad \sigma(A) \subset A; \qquad \sigma(a) \equiv a^q \bmod \mathfrak{A} \qquad$ for all $\quad a \in A$

(2.1.3) $\quad p \in \mathfrak{A}; \qquad s_i\mathfrak{A} = \{s_i b \mid b \in \mathfrak{A}\} \subset A, \quad i = 1, 2, \ldots$

We note that $\sigma(a) \equiv a^q \bmod \mathfrak{A}$ for all $a \in A$ implies that $\sigma(A) \subset A$ and also that $\sigma(\mathfrak{A}) \subset \mathfrak{A}$.

In addition we require the property

(2.1.4) $\quad \mathfrak{A}^r b \subset \mathfrak{A} \quad \Rightarrow \quad \mathfrak{A}^r \sigma(b) \subset \mathfrak{A}$

for all $r \in \mathbf{N}$, $b \in K$. This property is, e.g., automatically satisfied if $\mathfrak{A}$ is principal, $\mathfrak{A} = (c)$, with $c \in A$ such that $\sigma(c) = uc$ for some unit $u \in A$. This is the case in all the examples below; cf. also Remark (2.4.15).

Examples of this type of situation are, e.g.,

(2.1.5) $\quad A = \mathbf{Z}, \quad K = \mathbf{Q}, \quad \sigma = id, \quad p = q, \quad s_i \in p^{-1}\mathbf{Z} \subset \mathbf{Q}, \quad \mathfrak{A} = p\mathbf{Z}$

(2.1.6) $\quad A = \mathbf{Z}_{(p)}[V_1, V_2, \ldots; W_1, W_2, \ldots], \quad K = A \otimes \mathbf{Q}$

$$\sigma(b(V_1, V_2, \ldots; W_1, W_2, \ldots)) = b(V_1^p, V_2^p, \ldots; W_1^p, W_2^p, \ldots)$$

$$\mathfrak{A} = pA, \quad p = q, \quad s_i \in p^{-1}A$$

(2.1.7) K a local field with finite residue field k, A the ring of integers of K, $p = \mathrm{char}(k)$, $q = p$, $\mathfrak{A} = \mathfrak{m}$, the maximal ideal of A, $\sigma\colon K \to K$ the unique (Frobenius) endomorphism such that $\sigma(a) \equiv a^p \bmod \mathfrak{m}$ for all $a \in A$, and $s_i \in \pi^{-1}A$ where π is a uniformizing element of A.

Now let $g(X) = \sum_{i=1}^{\infty} b_i X^i$ be a power series in one variable with coefficients in A, then, given the ingredients (2.1.1), we construct a new power series $f_g(X)$ by means of the recursion formula (or functional equation)

$$f_g(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i f_g(X^{q^i}) \tag{2.1.8}$$

where $\sigma_*^i f_g(X)$ is the power series obtained from $f_g(X)$ by applying the endomorphism σ^i to the coefficients of $f_g(X)$.

The power series $f_g(X)$ depends of course not only on $g(X)$ but also on σ, q, and especially $s_1, s_2, \ldots$.

Equation (2.1.8) is in fact a recursion formula for the coefficients of $f_g(X)$. Indeed, let

$$g(X) = \sum_{i=1}^{\infty} b_i X^i, \qquad f_g(X) = \sum_{i=1}^{\infty} d_i X^i$$

then the d_n, $n = 1, 2, \ldots$, are recursively determined as follows. Write $n = q^r m$ where m is such that q does not divide m. Then we have

$$d_n = b_n + s_1 \sigma(d_{n/q}) + \cdots + s_r \sigma^r(d_{n/q^r}) \tag{2.1.9}$$

(If q does not divide n, we have of course $d_n = b_n$.)

Two examples of power series that are of the form $f_g(X)$ are

$$H(X) = X + p^{-1}X^p + p^{-2}X^{p^2} + \cdots \tag{2.1.10}$$

$$l(X) = \log(1 + X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n} \tag{2.1.11}$$

To obtain $H(X)$ one takes $A = \mathbf{Z}_{(p)}$, $K = \mathbf{Q}$, $\sigma = id$, $q = p$, $\mathfrak{A} = p\mathbf{Z}_{(p)}$, $s_1 = p^{-1}$, $s_2 = s_3 = \cdots = 0$, and $g(X) = X$. To obtain $l(X)$ we also take $A = \mathbf{Z}_{(p)}$, $K = \mathbf{Q}$, $\sigma = id$, $q = p$, $\mathfrak{A} = p\mathbf{Z}_{(p)}$, $s_1 = p^{-1}$ and $s_2 = s_3 = \cdots = 0$; but if $p = 2$, then we take

$$g(X) = \sum_{(2,n)=1} n^{-1}(X^n - X^{2n})$$

and if $p > 2$ we must take

$$g(X) = \sum_{(n,p)=1} (-1)^{n+1} n^{-1} X^n.$$

We can now state the functional equation–integrality lemma

2.2 Functional equation lemma

Let A, K, σ, $\mathfrak{A}$, p, q, s_1, s_2, ... be as in 2.1, let $g(X) = \sum_{i=1}^{\infty} b_i X^i$, $\bar{g}(X) = \sum_{i=1}^{\infty} \bar{b}_i X^i$ be two power series in one variable over A, and suppose that b_1 is invertible in A. Then we have:

(i) the power series $F_g(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$ has its coefficients in A;

(ii) the power series $f_g^{-1}(f_{\bar{g}}(X))$ has its coefficients in A;

(iii) if $h(X) = \sum_{n=1}^{\infty} c_n X^n$ is a power series with coefficients in A, then there is a power series $\hat{h}(X) = \sum_{n=1}^{\infty} \hat{c}_n X^n$ with $\hat{c}_n \in A$, $n = 1, 2, \ldots$, such that $f_g(h(X)) = f_{\hat{h}}(X)$;

(iv) if $\alpha(X) \in A[\![X]\!]$, $\beta(X) \in K[\![X]\!]$ are two power series with coefficients in A and K respectively and $r \in \mathbf{N} = \{1, 2, \ldots\}$, then we have

$$\alpha(X) \equiv \beta(X) \mod \mathfrak{A}^r A[\![X]\!] \iff f_g(\alpha(X)) \equiv f_g(\beta(X)) \mod \mathfrak{A}^r A[\![X]\!]$$

If $f_g(X)$ and $f_{\bar{g}}(X)$ are power series obtained by the recursion equation (2.1.8) with everything the same except possibly $g(X) \neq \bar{g}(X)$, then we shall say that $f_g(X)$ and $f_{\bar{g}}(X)$ satisfy *the same type of functional equation*. Thus, so the speak, the type of a functional equation is given by the data $s_1, s_2, \ldots, q, \sigma$ (and A, K, $\mathfrak{A}$).

Parts (ii) and (iii) now say, e.g., that if $f(X), \bar{f}(X)$ satisfy functional equations and $f(X) \equiv \bar{f}(X) \equiv X$ mod(degree 2), then the formal group laws $F(X, Y) = f^{-1}(f(X)+f(Y))$, $\bar{F}(X, Y) = \bar{f}^{-1}(\bar{f}(X)+\bar{f}(Y))$ are strictly isomorphic if and only if $f(X)$ and $\bar{f}(X)$ satisfy functional equations of the same type.

2.3 Some applications

Before proving the lemma let us give a number of applications. First take $A = \mathbf{Z}_{(p)}$, $\mathbf{Q} = K$, $\sigma = id$, $\mathfrak{A} = p\mathbf{Z}_{(p)}$, $q = p$, $s_1 = p^{-1}$, $s_2 = s_3 = \cdots = 0$, $g(X) = X$, and $\bar{g}(X) = \sum_{(n,2)=1} n^{-1}(X^n - X^{2n})$ if $p = 2$ and $\bar{g}(X) = \sum_{(n,p)=1} (-1)^{n+1} n^{-1} X^n$ if $p > 2$. Then we have $H(X) = f_g(X)$ and $l(X) = f_{\bar{g}}(X)$. Now if $\exp(X)$ is the usual exponential series, $\exp(X) = \sum_{n=0}^{\infty} (n!)^{-1} X^n$, then $\exp(X) - 1 = l^{-1}(X)$ so that part (ii) of the functional equation lemma implies

■ (2.3.1) **Lemma** [162] The power series $\exp(H(X))$ has p-integral coefficients.

With the same basic ingredients we consider some more general Artin–Hasse–Whaples–Witt exponential series. Let

$$d(X) = d_0 X + d_1 X^p + d_2 X^{p^2} + \cdots$$

with $d_i \in \mathbf{Q}$ and write

$$\exp(d(X)) = \sum_{n=0}^{\infty} c_n X^n \tag{2.3.2}$$

Then we have

■ (2.3.3) **Proposition** [113, Proposition 1] All the coefficients c_n, $n = 0, 1, 2, \ldots$, in (2.3.2) are p-integral (i.e., in $\mathbf{Z}_{(p)}$) if and only if there are $b_i \in \mathbf{Z}_{(p)}$ such that $d_i = p^{-1} d_{i-1} + b_i$ for all $i = 0, 1, 2, \ldots$ (where d_{-1} is taken to be equal to 0).

This is proved as follows. If there are $b_i \in \mathbf{Z}_{(p)}$ such that $d_i = p^{-1} d_{i-1} + b_i$ for all i, then $d(X) = f_{\bar{g}}(X)$ with $\bar{g}(X) = \sum_{i=0}^{\infty} b_i X^{p^i}$. Let $g(X) = \sum_{(n,2)=1} n^{-1}(X^n + X^{2n})$ if $p = 2$ and $g(X) = \sum_{(n,p)=1} (-1)^{n+1} n^{-1} X^n$ if $p > 2$, then $l(X) = f_g(X)$; part (ii) of the functional equation lemma now implies that all the c_n are p-integral. Conversely, if all the c_n are p-integral, then by part (iii) of the functional equation lemma there exists an $\hat{h}(X)$ with coefficients in $\mathbf{Z}_{(p)}$ such that $d(X) = f_{\hat{h}}(X)$. It follows immediately from this that $\hat{h}(X)$ must be of the form $\hat{h}(X) = \sum_{i=0}^{\infty} b_i X^{p^i}$, which then implies that $d_i = p^{-1} d_{i-1} + b_i$ for all i.

■ (2.3.4) **Dwork's integrality lemma** In a similar vein one proves Dwork's integrality lemma 1 of [137]. It says the following. Let T be the completion of the maximal unramified extension field of $\mathbf{Q}_p$ and let $\sigma \in \mathrm{Gal}(T/\mathbf{Q}_p)$ be the (continuous extension of the) Frobenius automorphism of T over $\mathbf{Q}_p$. Let A be the ring of integers of T. Then $h(X) = 1 + a_1 X + a_2 X^2 + \cdots \in T[\![X]\!]$ is in $A[\![X]\!]$ iff $\sigma_* h(X^p)/h(X)^p \in 1 + pXA[\![X]\!]$. This is proved as follows. We have seen above that $\log(1+X) - p^{-1}\log(1+X^p) \in X + X^2 A[\![X]\!]$. By parts (ii) and (iii) of the functional equation lemma it follows that $h(X)$ is integral iff $\log(h(X)) - p^{-1}\sigma_* \log(h(X^p)) \in A[\![X]\!]$. Multiplying with $-p$ and taking exponentials, we see that this is equivalent to $\sigma_* h(X^p)/h(X)^p \in 1 + pXA[\![X]\!]$.

■ (2.3.5) **Construction of some formal group laws** For the third application we take $A = \mathbf{Z}[V_1, V_2, \ldots; T_1, T_2, \ldots] = \mathbf{Z}[V; T]$, $K = \mathbf{Q}[V; T]$, $\sigma\colon K \to K$ is the $\mathbf{Q}$-homomorphism defined by $T_i \mapsto T_i^p$, $V_j \mapsto V_j^p$ for all $i, j \in \mathbf{N}$, $q = p$, $\mathfrak{A} = pA$, $s_i = p^{-1} V_i$, $i \in \mathbf{N}$. Let

$$g(X) = X, \qquad \bar{g}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i}$$

so that, writing $f_V(X)$ and $f_{V,T}(X)$ for the corresponding power series $f_g(X)$ and $f_{\bar{g}}(X)$, we have

$$f_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{p} f_V^{(p^i)}(X^{p^i}) \tag{2.3.6}$$

$$f_{V,T}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i} + \sum_{i=1}^{\infty} \frac{V_i}{p} f_{V,T}^{(p^i)}(X^{p^i})$$

where we have used the notation $f^{(p^i)}(X)$ for $(\sigma^i)_* f(X)$, as we shall usually do whenever σ is an endomorphism of the particular kind we are dealing with here. (Note that $f_V(X)$ is in fact a power series over $\mathbf{Q}[V]$; i.e., it involves no T's.) The first few terms of

$$f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}, \qquad f_{V,T}(X) = \sum_{n=0}^{\infty} a_n(V, T) X^{p^n}$$

are

$$a_0(V) = 1, \qquad a_1(V) = p^{-1} V_1, \qquad a_2(V) = p^{-2} V_1 V_1^p + p^{-1} V_2$$

$$a_3(V) = p^{-3} V_1 V_1^p V_1^{p^2} + p^{-2} V_1 V_2^p + p^{-2} V_2 V_1^{p^2} + p^{-1} V_3$$

$$a_0(V, T) = 1, \qquad a_1(V, T) = p^{-1} V_1 + T_1,$$

$$a_2(V, T) = p^{-2} V_1 V_1^p + p^{-1} V_2 + p^{-1} V_1 T_1^p + T_2$$

We define

$$F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y)) \tag{2.3.7}$$

$$F_{V,T}(X, Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y)) \tag{2.3.8}$$

$$\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X)) \tag{2.3.9}$$

An application of parts (i) and (ii) of the functional equation lemma now shows that the power series $F_V(X, Y)$, $F_{V,T}(X, Y)$, $\alpha_{V,T}(X, Y)$ have their coefficients in $\mathbf{Z}[V]$, $\mathbf{Z}[V; T]$, and $\mathbf{Z}[V; T]$, respectively. Because $f_V(X) \equiv f_{V,T}(X) \equiv X \mod(\text{degree } 2)$, we have $F_V(X, Y) \equiv F_{V,T}(X, Y) \equiv X + Y \mod(\text{degree } 2)$ and $\alpha_{V,T}(X) \equiv X \mod(\text{degree } 2)$. Moreover, it is trivially clear from (2.3.7) and (2.3.8) that

$$F_V(X, Y) = F_V(Y, X)$$

$$F_{V,T}(X, Y) = F_{V,T}(Y, X)$$

$$F_V(F_V(X, Y), Z) = F_V(X, F_V(Y, Z))$$

$$F_{V,T}(F_{V,T}(X, Y), Z) = F_{V,T}(X, F_{V,T}(Y, Z))$$

so that we have proved

■ (2.3.10) **Theorem** $F_V(X, Y)$ and $F_{V,T}(X, Y)$ are one dimensional commutative formal group laws over $\mathbf{Z}[V]$ and $\mathbf{Z}[V, T]$, respectively. Moreover, $\alpha_{V,T}(X)$ is a strict isomorphism over $\mathbf{Z}[V, T]$ from $F_V(X, Y)$ to $F_{V,T}(X, Y)$.

■ (2.3.11) **Remark** These two formal group laws $F_V(X, Y)$ and $F_{V,T}(X, Y)$ and the isomorphism $\alpha_{V,T}(X)$ between them will play an important role in the remainder of this book. In part this is caused by the fact that every one dimensional commutative formal group law over a $\mathbf{Z}_{(p)}$-algebra is up to strict isomorphism obtainable from $F_V(X, Y)$ by ring change, i.e., by specifying the V_i suitably (cf. 1.8). This is proved in Section 16.4. The importance of $\alpha_{V,T}(X)$ and $F_{V,T}(X, Y)$ lies in the fact that the isomorphism $\alpha_{V,T}(X)$ is in a certain sense "the most general strict isomorphism possible." (Cf. Theorem (19.2.6).) In Section 3 we shall study $F_V(X, Y)$ and $F_{V,T}(X, Y)$ in more detail. One of the things one can get out of $F_V(X, Y)$ is a reasonable supply of nonisomorphic formal group laws over $\mathbf{Z}$ and $\mathbf{Z}/(p)$; cf. Section 3.2 and Remark (3.3.11).

2.4 Proof of the functional equation lemma

We shall do our calculations in the ring $K[\![X, Y]\!]$. If G, H are two elements in this ring, then $G \equiv H \mod(\mathfrak{A}^r, \text{degree } m)$ means that if $G - H = \sum b_{ij} X^i Y^j$, then $b_{ij} \in \mathfrak{A}^r$ for all i, j such that $i + j < m$. By definition $\mathfrak{A}^0 = A$. We shall need a number of lemmas.

■ (2.4.1) **Lemma** Write $f_g(X) = \sum_{n=1}^{\infty} a_n X^n$ and let $n = q^r m$ where m is not divisible by q. Then $a_n \mathfrak{A}^r \subset A$.

Proof This follows by induction (with respect to r) from (2.1.9) because $s_i \mathfrak{A} \subset A$ for all $i = 1, 2, \ldots$.

■ (2.4.2) **Lemma** Let $G(X, Y) \in A[\![X, Y]\!]$ and let $n = q^r m$, $l > 0$; we have

$$G(X, Y)^{nq^l} \equiv [\sigma_*^l G(X^{q^l}, Y^{q^l})]^n \mod \mathfrak{A}^{r+1} \tag{2.4.3}$$

Proof Because $\sigma(a) \equiv a^q \bmod \mathfrak{A}$ for all $a \in A$ and because $p \in \mathfrak{A}$, we have that

$$G(X, Y)^{q^l} \equiv \sigma_*^l G(X^{q^l}, Y^{q^l}) \mod \mathfrak{A}$$

An easy induction with respect to r then shows that for all $r = 0, 1, 2, \ldots,$

$$G(X, Y)^{q^{l+r}} \equiv (\sigma_*^l G(X^{q^l}, Y^{q^l}))^{q^r} \mod \mathfrak{A}^{r+1}$$

and (2.4.3) follows immediately from this last congruence.

We now proceed to prove part (i) of the functional equation lemma. We write $F(X, Y)$ and $f(X)$ for $F_g(X, Y)$ and $f_g(X)$, respectively. Let

$$F(X, Y) = F_1(X, Y) + F_2(X, Y) + \cdots \tag{2.4.4}$$

where $F_i(X, Y)$ is homogeneous of degree i in X, Y. Because $f(X) \equiv b_1 X$ mod(degree 2), we have $f^{-1}(X) \equiv b_1^{-1} X$ mod(degree 2) and hence $F(X, Y) \equiv X + Y$ mod(degree 2), hence $F_1(X, Y)$ has its coefficients in A. We now proceed by induction to prove that $F_n(X, Y)$ has its coefficients in A for all $n = 1, 2, \ldots$. Assume therefore that $F_1(X, Y), \ldots, F_{n-1}(X, Y)$ have their coefficients in A. Because $F(X, Y) \equiv 0$ mod(degree 1), we have for all $r \geq 2$,

$$(F_1(X, Y) + \cdots + F_{n-1}(X, Y))^r \equiv (F(X, Y))^r \mod(\text{degree } n+1) \tag{2.4.5}$$

Combining this with (2.4.3) we have

$$F(X, Y)^{q^i n} \equiv \sigma_*^i F(X^{q^i}, Y^{q^i}))^n \mod(\mathfrak{A}^{r+1}, \text{degree } n+1) \tag{2.4.6}$$

where $n = q^r m$, $q \nmid m$. Now by the definition of $F(X, Y)$ we have

$$f(F(X, Y)) = f(X) + f(Y) \tag{2.4.7}$$

and because σ is a homomorphism it follows from this that

$$\sigma_*^i f(\sigma_*^i F(X, Y)) = \sigma_*^i f(X) + \sigma_*^i f(Y) \tag{2.4.8}$$

Now $f(X)$ satisfies a functional equation

$$f(X) = g(X) + \sum_{n=1}^{\infty} s_n \sigma_*^n f(X^{q^n}) \tag{2.4.9}$$

Substituting $F(X, Y)$ for X in (2.4.9) and writing $f(X) = \sum_{n=1}^{\infty} a_n X^n$, we obtain

$$f(F(X, Y)) = g(F(X, Y)) + \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n)(F(X, Y))^{q^{in}} \tag{2.4.10}$$

Now by (2.4.6), Lemma (2.4.1), and property (2.1.4) we know that

$$(2.4.11)\quad s_i\sigma^i(a_n)F(X, Y)^{q^{in}} \equiv s_i\sigma^i(a_n)(\sigma^i_* F(X^{q^i}, Y^{q^i}))^n \mod(A, \text{degree } n+1)$$

Substituting this in (2.4.10) and using (2.4.8), (2.4.9), we obtain mod(A, degree $n+1$)

$$\begin{aligned}(2.4.12)\quad f(F(X, Y)) &\equiv g(F(X, Y)) + \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n)(\sigma^i_* F(X^{q^i}, Y^{q^i}))^n \\ &\equiv g(F(X, Y)) + \sum_{i=1}^{\infty} s_i\sigma^i_* f(\sigma^i_* F(X^{q^i}, Y^{q^i})) \\ &\equiv g(F(X, Y)) + \sum_{i=1}^{\infty} s_i(\sigma^i_* f(X^{q^i}) + \sigma^i_* f(Y^{q^i})) \\ &\equiv g(F(X, Y)) + f(X) + f(Y) - g(X) - g(Y)\end{aligned}$$

However, because $g(X) \equiv b_1 X$ mod(degree 2) and $F(X, Y) \equiv F_n(X, Y)$ mod(A, degree $n+1$), we have

$$(2.4.13)\qquad g(F(X, Y)) \equiv b_1 F_n(X, Y) \mod(A, \text{degree } n+1)$$

Now combine (2.4.13), (2.4.12), and (2.4.7) to obtain that

$$b_1 F_n(X, Y) \equiv 0 \mod(A, \text{degree } n+1)$$

which proves that $F_n(X, Y)$ has its coefficients in A because b_1 is an invertible element of A. This concludes the proof of part (i) of Lemma 2.2.

The proof of part (ii) is practically identical and is left to the reader.

To prove part (iii) write $\hat{f}(X) = f(h(X))$. Then we have, because $h(X) \equiv 0$ mod(A),

$$\begin{aligned}\hat{f}(X) - \sum_{i=1}^{\infty} s_i\sigma^i_* \hat{f}(X^{q^i}) &= f(h(X)) - \sum_{i=1}^{\infty} s_i\sigma^i_* f(\sigma^i_* h(X^{q^i})) \\ &= f(h(X)) - \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n)(\sigma^i_* h(X^{q^i}))^n \\ &\equiv f(h(X)) - \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(a_n)(h(X)^{q^{in}}) \\ &= f(h(X)) - \sum_{i=1}^{\infty} s_i\sigma^i_* f(h(X)^{q^i}) \\ &= g(h(X)) \equiv 0\end{aligned}$$

where all the congruences are mod(A). This proves part (iii) of Lemma 2.2.

The implication $\Rightarrow$ of part (iv) of the functional equation lemma is easy. Indeed, we have already seen that $a_n\mathfrak{C}^t \subset A$ if $f(X) = \sum_{i=1}^{\infty} a_i X^i$ and $n = q^t m$,

$q \nmid m$. Now if $\beta(X) = \alpha(X) + \gamma(X)$ with $\gamma(X) \in \mathfrak{C}^r A[\![X]\!]$ then as in the proof of Lemma (2.4.2)

$$\beta(X)^{q^i} \equiv \alpha(X)^{q^i} \mod \mathfrak{C}^{r+t}$$

and

$$\beta(X)^n \equiv \alpha(X)^n \mod \mathfrak{C}^{r+t}$$

Hence $a_n \beta(X)^n \equiv a_n \alpha(X)^n \bmod \mathfrak{C}^r$, and $f(\alpha(X)) \equiv f(\beta(X)) \bmod \mathfrak{C}^r$.

To prove the inverse implication of part (iv) we first show that

$$\alpha(X) \equiv 0 \mod \mathfrak{C}^r \quad \Rightarrow \quad f^{-1}(\alpha(X)) \equiv 0 \mod \mathfrak{C}^r \tag{2.4.14}$$

To see this write $f^{-1}(\alpha(X)) = \gamma(X)$ and $\alpha(X) = f(\gamma(X))$. Certainly $\gamma(X) \equiv 0$ mod($\mathfrak{C}^r$, degree 2) because $f(X) \equiv b_1 X$ mod(degree 2) with b_1 a unit. Suppose now we have proved that $\gamma(X) \equiv 0$ mod($\mathfrak{C}^r$, degree n). Then we have mod($\mathfrak{C}^r$, degree $n+1$)

$$\alpha(X) \equiv f(\gamma(X)) \equiv g(\gamma(X)) + \sum_{i=1}^{\infty} s_i \sigma_*^i f(\gamma(X)^{q^i}) \equiv 0$$

because $\gamma(X)^{q^i} \equiv 0$ mod($\mathfrak{C}^{r+1}$, degree $n+1$) and hence $f(\gamma(X)^{q^i}) \equiv 0$ mod($\mathfrak{C}^{r+1}$, degree $n+1$) by the $\Rightarrow$ part of (iv) of the functional equation lemma, which we have already proved. By induction this proves (2.4.14).

Now let $f(\alpha(X)) \equiv f(\beta(X)) \bmod \mathfrak{C}^r$ (note that neither $f(\alpha(X))$ nor $f(\beta(X))$ need have its coefficients in A). Let

$$\delta(X) = f^{-1}(f(\beta(X)) - f(\alpha(X)))$$

then $\delta(X) \equiv 0 \bmod \mathfrak{C}^r$ by (2.4.14). Now $f(\delta(X)) + f(\alpha(X)) = f(\beta(X))$, hence

$$\beta(X) = f^{-1}(f(\delta(X)) + f(\alpha(X))) = F(\delta(X), \alpha(X))$$

and it follows that $\beta(X) \equiv \alpha(X) \bmod \mathfrak{C}^r$ because $F(X, Y)$ has coefficients in A and because $F(0, Y) = Y$ and $\delta(X) \equiv 0 \bmod \mathfrak{C}^r$.

This proves part (iv) of the functional equation lemma. Q.E.D.

■ (2.4.15) **Remark** Suppose that instead of (2.1.2)–(2.1.4) the functional equation ingredients satisfy (2.1.2) and

$$p \in \mathfrak{C} \quad \text{and} \quad \sigma^j(s_i)\mathfrak{C} \subset A \quad \text{for all} \quad i, j \in \mathbf{N} \tag{2.4.16}$$

Then the functional equation lemma 2.2 holds. This is usually a somewhat weaker hypothesis. The only difference in the proof is that Lemma (2.4.1) gets replaced by the lemma that $\sigma^i(a_n)\mathfrak{C}^r \subset A$ for all $i \in \mathbf{N}$ if $n = q^r m$, $q \nmid m$, which also follows immediately from (2.1.9) (by induction).

3 The Formal Group Laws $F_V(X, Y)$, $F_{V,T}(X, Y)$, and $F_S(X, Y)$

In this section we discuss in somewhat more detail the formal groups laws $F_V(X, Y)$ and $F_{V,T}(X, Y)$ which were introduced in 2.3, and we also construct and discuss a third formal group law $F_S(X, Y)$. We start by defining this third formal group law. Fix a prime number p for this whole section. The results of this section do not play an important role in the remainder of Chapter I (except by way of suggestion and motivation) but will be important later.

3.1 The formal group law $F_S(X, Y)$

To define this formal group law we apply the functional equation lemma 2.2 with $A = \mathbf{Z}[S_2, S_3, \ldots] = \mathbf{Z}[S]$, $K = \mathbf{Q}[S]$, $\mathfrak{A} = pA$, $\sigma: K \to K$ raises each S_j to its pth power, $q = p$, $s_i = p^{-1}S_{p^i}$ for all $i = 1, 2, \ldots$, and

$$g(X) = X + \sum_{n=2}^{\infty} S_n X^n - \sum_{i=1}^{\infty} S_{p^i} X^{p^i} \tag{3.1.1}$$

We write $f_S(X)$ for the corresponding power series $f_g(X)$ and we define

$$F_S(X, Y) = f_S^{-1}(f_S(X) + f_S(Y)) \tag{3.1.2}$$

An application of part (i) of the functional equation lemma shows that $F_S(X, Y)$ has its coefficients in $\mathbf{Z}[S]$, so $F_S(X, Y)$ is a one dimensional formal group law over $\mathbf{Z}[S]$.

Let $\phi: \mathbf{Z}[V_1, V_2, \ldots] \to \mathbf{Z}[S_2, S_3, \ldots]$ be the embedding $\phi(V_i) = S_{p^i}$. Then part (ii) of the functional equation lemma shows that the formal groups $\phi_* F_V(X, Y)$ and $F_S(X, Y)$ are strictly isomorphic over $\mathbf{Z}[S]$.

We write

$$f_S(X) = \sum_{n=1}^{\infty} c_n X^n \tag{3.1.3}$$

$$g(X) = \sum_{n=1}^{\infty} b_n X^n \tag{3.1.4}$$

then, according to (2.1.9), the coefficients c_n satisfy the equation

$$c_n = \frac{S_p}{p} c_{n/p}^{(p)} + \cdots + \frac{S_{p^r}}{p} c_{n/p^r}^{(p^r)} + b_n \tag{3.1.5}$$

where $n = p^r m$, $(p, m) = 1$, and where we have written $c^{(p^l)}$ for $\sigma^l(c)$, $l = 1, 2, \ldots$.

Combining this with (3.1.1) we see that for $n = 2, 3, \ldots$,

$$c_n \equiv v_p(n)^{-1} S_n \mod(S_2, \ldots, S_{n-1}) \tag{3.1.6}$$

where $v_p(n)$ is defined as

$$v_p(n) = \begin{cases} 1 & \text{if } n = 1 \text{ or } n \text{ not a power of } p \\ p & \text{if } n = p^r, \quad r \in \mathbf{N} \end{cases} \tag{3.1.7}$$

It follows immediately from (3.1.6) (and (3.1.2)) that

(3.1.8) $$F_S(X, Y) \equiv X + Y + S_n v_p(n)^{-1} B_n(X, Y) \mod(S_2, \ldots, S_{n-1}, \text{degree}(n+1))$$

where $B_n(X, Y)$ is the polynomial

(3.1.9) $$B_n(X, Y) = X^n + Y^n - (X + Y)^n$$

3.2 Construction of a number of nonisomorphic formal group laws

We construct a number of formal group laws over $\mathbf{Z}$ by means of the functional equation 2.2, one for every $n \in \mathbf{N}$. To do this we take $A = \mathbf{Z}$, $K = \mathbf{Q}$, $\mathfrak{A} = p\mathbf{Z}$, $\sigma = id$, $p = q$, $s_i(n) = 0$ if $i \neq n$, $s_n(n) = 1$, $g(X) = X$. The resulting formal power series $f_g(X)$ will be denoted $f_{\Delta_n}(X)$. These power series then satisfy the functional equation

(3.2.1) $$f_{\Delta_n}(X) = X + p^{-1} f_{\Delta_n}(X^{p^n})$$

so that

(3.2.2) $$f_{\Delta_n}(X) = X + p^{-1} X^{p^n} + p^{-2} X^{p^{2n}} + \cdots$$

We let

(3.2.3) $$F_{\Delta_n}(X, Y) = f_{\Delta_n}^{-1}(f_{\Delta_n}(X) + f_{\Delta_n}(Y))$$

and a now familiar application of the functional equation lemma shows that the $F_{\Delta_n}(X, Y)$ are one dimensional commutative formal group laws over $\mathbf{Z}$. Furthermore, if $\bar{F}_{\Delta_n}(X, Y)$ denotes the formal group law over $\mathbf{Z}/(p)$ obtained by reducing all the coefficients of $F_{\Delta_n}(X, Y)$ modulo p, then the formal groups $\bar{F}_{\Delta_n}(X, Y)$ are all nonisomorphic over $\mathbf{Z}/(p)$.

To see this we calculate $[p]_{F_{\Delta_n}}(X)$ modulo p for all $n = 1, 2, \ldots$.

■ (3.2.4) **Lemma** $[p]_{F_{\Delta_n}}(X) \equiv X^{p^n} \mod(p)$.

Proof For convenience of notation let us write $f_n(X)$ for $f_{\Delta_n}(X)$ and $[p]_n(X)$ for $[p]_{F_{\Delta_n}}(X)$. We know that

(3.2.5) $$f_n^{-1}(p f_n(X)) = [p]_n(X)$$

Hence, using (3.2.1) we see that

(3.2.6) $$f_n([p]_n(X)) = p f_n(X) = pX + f_n(X^{p^n}) \equiv f_n(X^{p^n}) \mod(p)$$

and the lemma follows by part (iv) of the functional equation lemma.

■ (3.2.7) **Exercise** Prove Lemma (3.2.4) directly by induction, starting with the observation that obviously

(3.2.8) $$[p]_n(X) \equiv X^{p^n} \mod(p, \text{degree } p^n + 1)$$

because

$$f_n(X) \equiv X + p^{-1}X^{p^n} \mod(\text{degree } p^n + 1) \tag{3.2.9}$$

■ (3.2.10) **Corollary** If $n, m \in \mathbf{N}$, $n \neq m$, then there are no nonzero homomorphisms $\alpha(X)$: $\bar{F}_{\Delta_n}(X, Y) \to \bar{F}_{\Delta_m}(X, Y)$ (over any field of characteristic p).

Proof If $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is a homomorphism, then $\alpha([p]_F(X)) = [p]_G(\alpha(X))$. In view of Lemma (3.2.4) this proves the corollary.

■ (3.2.11) **Remark** Let $F(X, Y)$ be a one dimensional commutative formal group law over a field k of characteristic p. Then, as we shall see later in (18.3.2), if $[p]_F(X) \neq 0$, then the first nonzero coefficient in $[p]_F(X)$ occurs at degree p^h for a certain $h \in \mathbf{N}$. This h is called the *height* of the formal group law $F(X, Y)$. Thus the formal group law $\bar{F}_{\Delta_n}(X, Y)$ defined above has height n. The phenomenon signaled in Corollary (3.2.10) is a general one: there are no nonzero homomorphisms between one dimensional commutative formal group laws of different heights over fields of characteristic $p > 0$. The argument is the same as in (3.2.10) above; cf. also (18.3.4).

3.3 Some results concerning the formal group laws $F_V(X, Y)$, $F_{V,T}(X, Y)$

Let $F_{V,T}(X, Y)$, $F_V(X, Y)$ be the formal group laws defined in 2.3. Recall that

$$F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y)) \tag{3.3.1}$$

$$F_{V,T}(X, Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y))$$

where $f_V(X)$ and $f_{V,T}(X)$ satisfy the functional equations

$$f_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{p} f_V^{(p^i)}(X^{p^i}) \tag{3.3.2}$$

$$f_{V,T}(X) = X + T_1 X^p + T_2 X^{p^2} + \cdots + \sum_{i=1}^{\infty} \frac{V_i}{p} f_{V,T}^{(p^i)}(X^{p^i}) \tag{3.3.3}$$

where, again, we have written $f_V^{(p^i)}(X)$ for $\sigma_*^i f_V(X)$. We shall always use this notation when σ is a homomorphism of the type

$$\sigma: R[W_1, W_2, \ldots] \to R[W_1, W_2, \ldots],$$

$$b(W_1, W_2, \ldots) \mapsto b(W_1^p, W_2^p, \ldots)$$

Writing

$$f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n} \tag{3.3.4}$$

$$f_{V,T}(X) = \sum_{n=0}^{\infty} a_n(V, T) X^{p^n} \tag{3.3.5}$$

(it is obvious from (3.3.2) and (3.3.3) that all non-p-power coefficients in $f_V(X)$ and $f_{V,T}(X)$ are zero), we see that the $a_n(V)$ and $a_n(V, T)$ satisfy the recursion relations (cf. also (2.1.9))

$$(3.3.6)\qquad a_n(V) = p^{-1}V_1 a_{n-1}(V)^{(p)} + \cdots + p^{-1}V_{n-1}a_1(V)^{(p^{n-1})} + p^{-1}V_n, \qquad a_0(V) = 1$$

$$(3.3.7)\qquad a_n(V, T) = p^{-1}V_1 a_{n-1}(V, T)^{(p)} + \cdots + p^{-1}V_{n-1}a_1(V, T)^{(p^{n-1})} + p^{-1}V_n + T_n, \qquad a_0(V, T) = 1$$

From (3.3.6) by a straightforward induction one obtains

$$(3.3.8)\qquad a_n(V) = \sum_{i_1+\cdots+i_r=n} \frac{V_{i_1}V_{i_2}^{p^{i_1}}\cdots V_{i_r}^{p^{i_1+\cdots+i_{r-1}}}}{p^r}$$

where the sum is over all sequences $(i_1, \ldots, i_r)$, i_j, $r \in \mathbf{N}$ such that $i_1 + \cdots + i_r = n$.

Now consider all terms in the expression (3.3.8) for a_n for which $i_r = j$ for some fixed j, $1 \leq j \leq n$. Then it is clear that these terms of the sum in (3.3.8) sum to

$$p^{-1}a_{n-j}(V)V_j^{p^{n-j}}$$

So (3.3.8) implies that

$$(3.3.9)\qquad pa_n(V) = a_{n-1}(V)V_1^{p^{n-1}} + a_{n-2}(V)V_2^{p^{n-2}} + \cdots + a_1(V)V_{n-1}^{p} + V_n$$

From (3.3.6) and (3.3.7) together we obtain, again by a straightforward induction,

$$(3.3.10)\qquad a_n(V, T) = a_n(V) + a_{n-1}(V)T_1^{p^{n-1}} + \cdots + a_1(V)T_{n-1}^{p} + T_n$$

The two formulas (3.3.9) and (3.3.10) will have a large number of applications later in this book; they have, e.g., to do with isomorphisms of formal group laws, generators for the coefficient ring of Brown–Peterson cohomology, operations in Brown–Peterson cohomology, and Cartier–Dieudonné modules of formal group laws.

■ (3.3.11) **Remark** Let ϕ_n: $\mathbf{Z}[V] \to \mathbf{Z}$ be the ring homomorphism defined by $\phi_n(V_i) = 0$ if $i \neq n$ and $\phi_n(V_n) = 1$. Then we have

$$(3.3.12)\qquad (\phi_n)_* F_V(X, Y) = F_{\Delta_n}(X, Y)$$

This explains (we hope) the notation F_{Δ_n}; Δ_n is short for the sequence of integers $\Delta_n = (0, 0, \ldots 0, 1, 0, 0, \ldots)$ with the 1 in the nth spot.

4 Some Binomial Coefficient Arithmetic

To prove universality properties of various formal group laws (e.g., $F_S(X, Y)$ and the formal group law $F_U(X, Y)$ which we shall construct in Section 5) we shall need some properties of the binomial coefficients.

4.1 Preliminary remarks

For each $n \in \mathbf{N}$ we define (gcd means greatest common divisor)

$$v(n) = \gcd\left\{\binom{n}{1}, \ldots, \binom{n}{n-1}\right\} \tag{4.1.1}$$

Then we have

$$v(n) = \begin{cases} 1 & \text{if } n = 1 \text{ or } n \text{ is not a power of a prime number} \\ p & \text{if } n = p^r, \quad r \in \mathbf{N} \text{ for a certain prime number } p \end{cases} \tag{4.1.2}$$

We include a proof for completeness sake. First, let n not be a power of a prime. Let p be any prime number. Then $n = p^r m$ with $m > 1$ and $(m, p) = 1$. Now suppose that $p \mid v(n)$. Then we would have modulo p

$$(X^{p^r} + Y^{p^r})^m \equiv (X + Y)^{p^r m} \equiv X^{p^r m} + Y^{p^r m} \equiv (X^{p^r})^m + (Y^{p^r})^m$$

so that $(X + Y)^m \equiv X^m + Y^m \bmod(p)$, which is clearly false because $\binom{m}{1} = m$ and $(m, p) = 1$.

Now let n be a power of a prime number p. We clearly have $(X + Y)^p \equiv X^p + Y^p$, and hence by induction $(X + Y)^{p^r} \equiv X^{p^r} + Y^{p^r}$, proving that $p \mid v(n)$ if n is a power of p. Conversely, we have $\binom{n}{1} = n = p^r$, so that p is the only prime that divides $v(n)$. Now suppose that $p^2 \mid v(n)$. Then substituting $X = Y = 1$ in $(X + Y)^n - X^n - Y^n$ we find $2^n \equiv 2 \bmod(p^2)$ and by induction $m^n \equiv m \bmod(p^2)$ for all $m \in \mathbf{N}$, which is clearly false as is shown by taking $m = p$.

We shall need the following key lemma in Section 5.

4.2 Binomial coefficient lemma

Lemma Let $X_1, \ldots, X_{n-1}$ be indeterminates, $X_i = X_{n-i}$, $i = 1, 2, \ldots, n-1$, $n \geq 2$. Let $\lambda_1, \ldots, \lambda_{n-1}$ be integers such that $\lambda_1 \binom{n}{1} + \cdots + \lambda_{n-1}\binom{n}{n-1} = v(n)$. Then every X_i can be written as an integral linear combination of the expressions

$$\lambda_1 X_1 + \cdots + \lambda_{n-1} X_{n-1} \tag{4.2.1}$$

$$\binom{i+j}{i} X_{i+j} - \binom{k+j}{j} X_{k+j}, \qquad i, j, k \geq 1, \quad i + j + k = n \tag{4.2.2}$$

Proof We claim that it suffices to prove for every prime number p that every X_i can be written modulo p as a linear combination of the expressions (4.2.1), (4.2.2).

■ (4.2.3) **Proof of the claim** To see this let M be the free abelian group generated by $X_1, \ldots, X_m$ where $m = 2^{-1}n$ if $(2, n) = 2$ and $m = 2^{-1}(n-1)$ if $(2, n) = 1$. Let N be the free abelian group generated by a generator y_0, and one generator y_{ijk} for every triple (i, j, k) with $i, j, k \geq 1$ and $i + j + k = n$. Define ϕ: $N \to M$ by

$$\phi(y_0) = \lambda_1 X_1 + \cdots + \lambda_{n-1} X_{n-1}$$

$$\phi(y_{ijk}) = \binom{i+j}{i} X_{i+j} - \binom{k+j}{j} X_{k+j}$$

(where we use (as a notational convenience) $X_i = X_{n-i}$). Then what we have to prove is that ϕ is surjective. Let C be the cokernel of ϕ. Then because $\otimes$ is right exact we have for every prime number p an exact sequence $N \otimes \mathbf{Z}/(p) \to M \otimes \mathbf{Z}/(p) \to C \otimes \mathbf{Z}/(p) \to 0$. But by hypothesis $N \otimes \mathbf{Z}/(p) \to M \otimes \mathbf{Z}/(p)$ is surjective for every p, hence $C \otimes \mathbf{Z}/(p) = 0$ for every p, which proves that $C = 0$ because C is a finitely generated abelian group. It therefore remains to prove the modulo p version of Lemma 4.2 for every prime number p.

■ (4.2.4) **The modulo p case with $n = p$ or $(n, p) = 1$** If $n = p$ or $(p, n) = 1$, then for every $i = 1, 2, \ldots, n-1$ we have $(i, p) = 1$ or $(n - i, p) = 1$. For each $i = 1, \ldots, n-1$, let $a(i) \in \{i, n-i\}$ be such that $(a(i), p) = 1$. Using $X_i = X_{n-i}$, we can assume that $\lambda_i = 0$ if $i \neq a(i)$; we take $a(1) = 1$. Now take $i = 1, j = a(2) - 1, \ldots, a(m) - 1, k = n - a(2), \ldots, n - a(m)$ in (4.2.2) to obtain the matrix of coefficients

$$\begin{pmatrix} \lambda_1 & \lambda_{a(2)} & \lambda_{a(3)} & \cdots & \lambda_{a(m)} \\ \binom{n-1}{a(2)-1} & \binom{a(2)}{1} & 0 & \cdots & 0 \\ \binom{n-1}{a(3)-1} & 0 & \binom{a(3)}{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \binom{n-1}{a(m)-1} & 0 & \cdots & 0 & \binom{a(m)}{1} \end{pmatrix} = A'$$

where $m = 2^{-1}n$ if $(n, 2) = 2$ and $m = 2^{-1}(n-1)$ if $(2, n) = 1$. One finds

$$\det(A') = \sum_{i=1}^{m} \frac{a(1) \cdots a(m)}{n} \binom{n}{a(i)} \lambda_{a(i)} = \left(\frac{1}{n} \prod_{i=1}^{m} a(i) \right) \left(\sum_{i=1}^{m} \binom{n}{a(i)} \lambda_{a(i)} \right)$$

$$= n^{-1} v(n) \prod_{i=1}^{m} a(i)$$

because $\lambda_i = 0$ if $i \notin \{a(1), \ldots, a(m)\}$. It follows that $\det(A') \not\equiv 0 \bmod p$ if $(n, p) = 1$ or $n = p$. Indeed, if $(n, p) = 1$, then also $(v(n), p) = 1$, and we had chosen $a(i)$ such that $(a(i), p) = 1$ for $i = 1, 2, \ldots, m$; and if $n = p$, then $v(n) = p$, so $\det(A') \not\equiv 0 \bmod(p)$ also in this case.

■ (4.2.5) **The modulo p case with $n = pm$ and $m > 1$** Taking $j = 1$ in (4.2.2) and using $X_{k+j} = X_i$, we find the expressions

(4.2.6) $$-(pm - i)X_i + (i+1)X_{i+1}$$

Now take $i = pl$ in (4.2.6) to see that all X_k with j of the form $p+1, 2p+1, \ldots, (m-1)p+1$ can modulo p be written as linear combinations of the expressions (4.2.2). Then taking $i = lp+1, \ldots, (l+1)p-1$ we see from (4.2.6) that also the X_j with j of the form $j = lp+r$, $l = 1, \ldots, m-1$; $r = 1, \ldots, p-1$ can be written modulo p as linear combinations of the expressions (4.2.2). Now take $i = p-1$ in (4.2.6) to obtain X_{p-1} as a linear combination modulo p of the expressions (4.2.2) and then take $i = p-2, \ldots, 2$ to obtain also the X_j with $j = 1, \ldots, p-1$ as linear combinations of the expressions (4.2.2). We have now obtained every X_j with $(j, p) = 1$ as a linear combination of the expressions (4.2.2).

To write the X_{pi}, $i = 1, \ldots, m$, as linear combinations of (4.2.1) and (4.2.2) we use induction. The induction hypothesis is:

> if $\lambda_1, \ldots, \lambda_{n-1}$ are such that $\sum \lambda_i \binom{n}{i} \equiv v(n) \mod(p)$ if $v(n) \neq p$ and $\sum \lambda_i \binom{n}{i} \equiv v(n) \mod p^2$ if $v(n) = p$, then each X_i can be written modulo p as a linear combination of the expressions (4.2.1), (4.2.2).

The induction starts because the proof given in (4.2.4) for $n = p$ or $(n, p) = 1$ still works under the somewhat weaker conditions on $\lambda_1, \ldots, \lambda_{n-1}$ stated in the induction hypothesis.

Let Y, Z be indeterminates, then we have

$$(4.2.7)\quad (Y^p + Z^p)^m \equiv (Y+Z)^{pm} \mod(p)$$

$$(4.2.8)\quad (Y^p + Z^p)^{p^r} \equiv (Y+Z)^{p^{r+1}} \mod(p^2) \quad \text{if} \quad r \geq 1$$

It follows that

$$(4.2.9)\quad \binom{pm}{pi} \equiv \binom{m}{i} \mod(p), \qquad \binom{p^{r+1}}{pi} \equiv \binom{p^r}{i} \mod(p^2) \qquad \text{if} \quad r \geq 1$$

$$(4.2.10)\quad \binom{pm}{i} \equiv 0 \mod(p) \qquad \text{if} \quad (i, p) = 1$$

$$(4.2.11)\quad \binom{p^{r+1}}{i} \equiv 0 \mod(p^2) \qquad \text{if} \quad (i, p) = 1 \text{ and } r \geq 1$$

Hence if $n = pm$, $v(n) \neq p$, $m > 1$, we find from (4.2.9) and (4.2.10)

$$(4.2.12)\quad v(n) = \sum_{i=1}^{n-1} \lambda_i \binom{n}{i} \equiv \sum_{i=1}^{m-1} \lambda_{ip} \binom{m}{i} \mod(p)$$

and if $n = pm$, $m = p^r$, $r \geq 1$, we obtain from (4.2.9) and (4.2.11) that

$$(4.2.13)\quad p = \sum_{i=1}^{n-1} \lambda_i \binom{n}{i} \equiv \sum_{i=1}^{m-1} \lambda_{ip} \binom{m}{i} \mod(p^2)$$

By induction it follows from (4.2.12) and (4.2.13) that we can write the X_{pl} modulo p as linear combinations of the expressions (4.2.2) for those i, j, k with $(p, i) = (p, j) = (p, k) = p$ and the expression

$$v(m)v(n)^{-1}(\lambda_p X_p + \cdots + \lambda_{n-p} X_{n-p}) \tag{4.2.14}$$

if $v(n) \neq p$, *respectively the expression*

$$\lambda_p X_p + \cdots + \lambda_{n-p} X_{n-p} \tag{4.2.15}$$

if $v(n) = p$. Now $(v(m), p) = 1 = (v(n), p)$ if m is not a power of p and because we have already written all the X_i with $(i, p) = 1$ as linear combinations modulo p of (4.2.1) and (4.2.2), we can write (4.2.14), respectively (4.2.15), as linear combinations modulo p of (4.2.1) and the expressions (4.2.2). This concludes the proof of the modulo p case with $n = pm$ and $m > 1$, and hence also concludes the proof of Lemma 4.2.

4.3 Connection with Lazard's comparison lemma

We define a polynomial in n indeterminates $X_1, \ldots, X_n$ over an abelian group A as an element of $A \otimes \mathbf{Z}[X_1, \ldots, X_n]$. Then the lemma proved above is equivalent to the following cocycle lemma.

■ (4.3.1) **Lemma** Let $\Gamma(X, Y)$ be a homogeneous polynomial of degree n in two indeterminates such that $\Gamma(X, Y) = \Gamma(Y, X)$ and $\Gamma(X, Y) - \Gamma(X, Y + Z) + \Gamma(X + Y, Z) - \Gamma(Y, Z) = 0$. Then there is an $a \in A$ such that $\Gamma(X, Y) = aC_n(X, Y)$ where $C_n(X, Y)$ is the polynomial

$$C_n(X, Y) = v(n)^{-1}(X^n + Y^n - (X + Y)^n)$$

The equivalence of Lemmas 4.2 and (4.3.1) combined with Lemma (1.6.6) (which we have not yet proved) shows why one can expect that Lemma 4.2 will play a role.

■ (4.3.2) **Proof of the equivalence of Lemmas 4.2 and (4.3.1)** Let M be the abelian group generated by $X_1, \ldots, X_{n-1}$ subject to the relations $X_i = X_{n-i}$, $i = 1, \ldots, n-1$, and $\binom{i+j}{j} X_{i+j} - \binom{j+k}{k} X_{j+k}$ for all triples (i, j, k), $i, j, k \in \mathbf{N}$, $i + j + k = n$. We define a homomorphism $\phi\colon \mathbf{Z} \to M$ as follows

$$\phi\colon \mathbf{Z} \to M, \qquad 1 \mapsto \sum_{i=1}^{n} \lambda_i X_i \tag{4.3.3}$$

Then, clearly, Lemma 4.2 is equivalent to the statement

$$\phi \text{ is surjective} \tag{4.3.4}$$

We also define a homomorphism

$$\psi\colon M \to \mathbf{Z}, \qquad X_i \mapsto v(n)^{-1} \binom{n}{i} \tag{4.3.5}$$

(Note that ψ is well defined.) We have $\psi\phi = id$, so ϕ is also injective, so Lemma 4.2 is equivalent to the statement

(4.3.6) ϕ is an isomorphism and ψ is its inverse

We now show that (4.3.6) implies Lemma (4.3.1). Let $\Gamma(X, Y) = c_0 X^n + c_1 XY^{n-1} + \cdots + c_{n-1} XY^{n-1} + c_n Y^n$ be a polynomial over A such that $\Gamma(X, Y) = \Gamma(Y, X)$ and

$$\Gamma(X, Y) - \Gamma(X + Y, Z) + \Gamma(X, Y + Z) - \Gamma(Y, Z) = 0;$$

then $c_0 = c_n = 0$ and $\binom{i+j}{j} c_{i+j} = \binom{k+j}{k} c_{j+k}$, as is easily checked. It follows that $X_i \mapsto c_i$ defines a homomorphism (of abelian groups) $\chi: M \to A$. By (4.3.6) we know that $X_i = \nu(n)^{-1}\binom{n}{i}(\lambda_1 X_1 + \cdots + \lambda_{n-1} X_{n-1})$ so that $c_i = \nu(n)^{-1} \times \binom{n}{i}\chi(\lambda_1 X_1 + \cdots + \lambda_{n-1} X_{n-1})$.

Conversely, assume we have proved Lemma (4.3.1). Then there is an element $a \in M$ such that $X_i = \nu(n)^{-1}\binom{n}{i} a$ for all i. Multiplying with λ_i and summing over i then gives $a = \lambda_1 X_1 + \cdots + \lambda_{n-1} X_{n-1}$ so that $X_i = \nu(n)^{-1}\binom{n}{i} \times (\lambda_1 X_1 + \cdots + \lambda_{n-1} X_{n-1})$, which shows that $\phi\psi = id$, proving (4.3.6).

5 A Universal One Dimensional Commutative Formal Group Law

In this section we construct a universal one dimensional commutative formal group law $F_U(X, Y)$ over $\mathbf{Z}[U] = \mathbf{Z}[U_2, U_3, U_4, \ldots]$.

5.1 A priori properties of $F_U(X, Y)$ which motivate the construction

This section is meant to give the reader some idea why one has to construct a universal formal group law more or less as we shall do it below. To this end we first remark that the formal group $F_S(X, Y)$ of 3.1 is a universal commutative one dimensional formal group law for one dimensional commutative formal group laws defined over $\mathbf{Z}_{(p)}$-algebras; i.e., if $G(X, Y)$ is a one dimensional commutative formal group law over a $\mathbf{Z}_{(p)}$-algebra A, then there is a unique homomorphism $\phi: \mathbf{Z}[S] \to A$ such that $\phi_* F_S(X, Y) = G(X, Y)$. We have not yet proved this fact, nor shall we do so until after we have constructed $F_U(X, Y)$ and proved the universality of $F_U(X, Y)$. It can, however, also be proved at this stage by virtually the same arguments that we shall use below in 5.3 to prove the universality of the (yet to be constructed) formal group law $F_U(X, Y)$.

Now if $F(X, Y)$ over L is a universal one dimensional commutative formal group law, then $F(X, Y)$ over $L \otimes \mathbf{Z}_{(p)}$ and $F_S(X, Y)$ over $\mathbf{Z}_{(p)}[S]$ are both formal group laws over $\mathbf{Z}_{(p)}$-algebras and both are universal for one dimensional commutative formal group laws over $\mathbf{Z}_{(p)}$-algebras. It follows that there is an isomorphism $\phi_p: \mathbf{Z}_{(p)}[S] \to L \otimes \mathbf{Z}_{(p)}$ such that $\phi_{p*} F_S(X, Y) = F(X, Y)$. Such a statement holds for all prime numbers p.

This suggests first that L is a ring of the form $\mathbf{Z}[U] = \mathbf{Z}[U_2, U_3, \ldots]$ and suggests moreover that $F(X, Y)$ is a formal group law of the type $F(X, Y) = f^{-1}(f(X) + f(Y))$ with $f(X)$ a power series over $\mathbf{Z}[U]$ satisfying a functional equation of type

$$f(X) = g_p(X) + \sum_{i=1}^{\infty} \frac{s(p, i)}{p} \sigma_{p*}^i f(X^p) \tag{5.1.1}$$

for all prime numbers p simultaneously, where $g_p(X)$ is required to be p-integral. The most simple choices for σ_p, etc. are of course σ_p: $\mathbf{Z}[U] \to \mathbf{Z}[U]$, $U_j \mapsto U_j^p$ and $s(p, i) = U_{p^i}$. Then, starting with $f(X) \equiv X$ mod(degree 2), the first thing one writes is

$$X + \frac{U_2}{2} X^2 + \frac{U_3}{3} X^3 + \left(\frac{U_2 U_2^2}{4} + \frac{U_4}{2}\right) X^4 + \frac{U_5}{5} X^5 + \left(\frac{U_3 U_2^3}{6} + \frac{U_2 U_3^2}{6}\right) X^6 + \cdots \tag{5.1.2}$$

However, it now appears that the prime numbers 2 and 3 interfere with one another: the term $6^{-1} U_3 U_2^3$, which has to be present because of (5.1.1) with $p = 3$, prevents (5.1.1) from holding for $p = 2$, and vice versa with respect to the term $6^{-1} U_2 U_3^2$. The solution is to insert suitable coefficients. Thus

$$X + \frac{U_2}{2} X^2 + \frac{U_3}{3} X^3 + \left(\frac{U_2 U_2^2}{4} + \frac{U_4}{2}\right) X^4 + \frac{U_5}{5} X^5 + \left(\frac{2U_3 U_2^3}{3} + \frac{U_2 U_3^2}{2} + U_6\right) X^6 + \cdots \tag{5.1.3}$$

does satisfy (5.1.1) for all p modulo (degree 7) (for suitable $g_p(X)$ which depend on p). (There has to be something like U_6 in the coefficient of X^6 because S_6 occurs in the coefficient of X^6 in $F_S(X, Y)$.) Thus the only problem in constructing a universal formal group law appears to lie in showing that one can always find suitable coefficients. This readily leads to a power series $h(X) = \sum_{n=1}^{\infty} a_n(U)$ where each $a_n(U)$ is a sum of expressions

$$k(q_1, \ldots, q_t, d) U_{q_1} U_{q_2}^{q_1} \cdots U_{q_t}^{q_1 \cdots q_{t-1}} U_d^{q_1 \cdots q_t} \tag{5.1.4}$$

where the q_i are prime powers, $q_1 q_2 \cdots q_t d = n$ and the $k(q_1, \ldots, q_t, d)$ are suitable rational numbers. The universal formal group law constructed in [178] is of this type.

There is however some lack of elegance in allowing only factorizations of n of type $(q_1, \ldots, q_t, d)$ with the q_i prime powers; it would be more elegant to use all possible sequences $(i_1, \ldots, i_s)$ such that $i_1 \cdot \cdots \cdot i_s = n$. It is indeed possible to do this in a nice way, and the formal group law $F_U(X, Y)$ to be constructed below is obtained in this manner.

5.2 Construction of the universal formal one dimensional commutative group law $F_U(X, Y)$

We now proceed to construct a universal one dimensional commutative formal group law $F_U(X, Y)$ over $\mathbf{Z}[U_2, U_3, \ldots]$. The first thing to do is the

■ (5.2.1) **Choice of coefficients** For each $s \in \mathbf{N}$ and each sequence $(i_1, \ldots, i_s)$ with $i_j \in \mathbf{N}\backslash\{1\}$, $j = 1, \ldots, s$, let $n(i_1, \ldots, i_s)$ be an integer such that the following conditions are satisfied:

(5.2.2) $$n(i_1, \ldots, i_s) = 1 \quad \text{if} \quad s = 1$$

and for $s \geq 2$

(5.2.3) $$n(i_1, \ldots, i_s) \equiv 1 \bmod p^r$$

if $i_1, \ldots, i_r$ are powers of a prime number p and i_{r+1} is not a power of p

(5.2.4) $$n(i_1, \ldots, i_s) \equiv 0 \bmod p^{r-1}$$

if $i_2, \ldots, i_r$ are powers of a prime number p and i_1 and i_{r+1} are not powers of p

(If $s = r$ in (5.2.3) and (5.2.4), then the conditions on i_{r+1} are supposed to be vacuously satisfied; thus (5.2.3) requires that $n(p, p) \equiv 1 \bmod(p^2)$, and (5.2.4) requires that $n(p_1, p_2, p_2) \equiv 0 \bmod(p_2^2)$ if p_1 and p_2 are two different prime numbers.) Note that there are many sets of integers $n(i_1, \ldots, i_s)$ satisfying these conditions; the integer $n(i_1, i_2, \ldots, i_s)$ has to satisfy two different congruences at the same time if and only if i_1 and i_2 are powers of two different prime numbers. In Section 5.6 we shall discuss a particular choice for the integers $n(i_1, \ldots, i_s)$ which will be useful later.

■ (5.2.5) **Definition of $F_U(X, Y)$** We now define the power series $f_U(X)$ over $\mathbf{Q}[U] = \mathbf{Q}[U_2, U_3, \ldots]$ by the formula

(5.2.6) $$f_U(X) = \sum_{n=1}^{\infty} m_n(U) X^n$$

where

(5.2.7) $$m_n(U) = \sum_{(i_1, \ldots, i_s)} \frac{n(i_1, \ldots, i_s)}{\nu(i_1)} \cdot \frac{n(i_2, \ldots, i_s)}{\nu(i_2)} \cdot \ldots \cdot \frac{n(i_s)}{\nu(i_s)} U_{i_1} U_{i_2}^{i_1} \cdot \ldots \cdot U_{i_s}^{i_1 i_2 \cdots i_{s-1}}$$

where the sum is over all sequences $(i_1, \ldots, i_s)$, $s \in \mathbf{N}$, $i_j \in \mathbf{N}\backslash\{1\}$, $j = 1, \ldots, s$, such that $i_1 i_2 \cdots i_s = n$.

The power series $F_U(X, Y)$ is now defined by

(5.2.8) $$F_U(X, Y) = f_U^{-1}(f_U(X) + f_U(Y))$$

5.3 The universality theorem

■ (5.3.1) **Theorem** $F_U(X, Y)$ has its coefficients in $\mathbf{Z}[U]$ and the formal group law $F_U(X, Y)$ over $\mathbf{Z}[U]$ is a universal one dimensional commutative formal group law.

This is proved in several steps. The first step is to prove that $F_U(X, Y)$ is integral, i.e., that $F_U(X, Y)$ has its coefficients in $\mathbf{Z}[U]$. This will be done by means of the functional equation lemma 2.2.

■ (5.3.2) **Proof of the integrality of** $F_U(X, Y)$ Let p be a prime number, and let $A_p = \mathbf{Z}_{(p)}[U]$, $K = \mathbf{Q}[U]$, σ_p: $K \to K$ the homomorphism $U_j \mapsto U_j^p$, $j = 2, 3, \ldots$, $\mathfrak{a} = pA_p$, $q = p$, $s_i = p^{-1}U_{p^i}$, $i = 1, 2, \ldots$. As usual we write $g^{(p^i)}(X)$ for $(\sigma_p^i)_* g(X)$. We want to prove that

$$f_U(X) - \sum_{i=1}^{\infty} \frac{U_{p^i}}{p} f_U^{(p^i)}(X^{p^i}) \in A_p[\![X]\!] \tag{5.3.3}$$

To prove this we first prove some congruences concerning the coefficients that occur in (5.2.7). Let

$$d(i_1, \ldots, i_s) = \frac{n(i_1, i_2, \ldots, i_s)}{v(i_1)} \cdot \frac{n(i_2, \ldots, i_s)}{v(i_2)} \cdot \ldots \cdot \frac{n(i_s)}{v(i_s)}$$

■ (5.3.4) **Lemma**

(i) If $1 \neq v(i_1) = \cdots = v(i_r) \neq v(i_{r+1})$, $r \leq s$, then $p^r d(i_1, \ldots, i_s) \in \mathbf{Z}$, where $p = v(i_1) = \cdots = v(i_r)$. (If $r = s$, then $v(i_r) \neq v(i_{r+1})$ is taken to be automatically fulfilled.)

(ii) If $v(i_1) = 1$, then $d(i_1, \ldots, i_s) \in \mathbf{Z}$.

Proof We prove both parts of the lemma simultaneously by induction on s. The case $s = 1$ is trivial. If $s > 1$, we distinguish four cases:

(a) $v(i_1) = 1 = v(i_2)$. Then $d(i_2, \ldots, i_s) \in \mathbf{Z}$ by induction hypothesis and hence $d(i_1, \ldots, i_s) = v(i_1)^{-1} n(i_1, \ldots, i_s) d(i_2, \ldots, i_s) \in \mathbf{Z}$.

(b) $v(i_1) = 1 \neq v(i_2) = p$. Let $v(i_2) = \cdots = v(i_t) \neq v(i_{t+1})$. Then by induction hypothesis $p^{t-1} d(i_2, \ldots, i_s) \in \mathbf{Z}$ and hence $d(i_1, \ldots, i_s) = v(i_1)^{-1} n(i_1, \ldots, i_s) d(i_2, \ldots, i_s) \in \mathbf{Z}$ because $n(i_1, i_2, \ldots, i_s) \equiv 0 \bmod p^{t-1}$ by (5.2.4) in this case.

(c) $1 \neq v(i_1) = v(i_2) = p$. Then $p^{r-1} d(i_2, \ldots, i_s) \in \mathbf{Z}$ by induction hypothesis and hence $p^r d(i_1, \ldots, i_s) = v(i_1)^{-1} n(i_1, \ldots, i_s) p^r d(i_2, \ldots, i_s) = n(i_1, \ldots, i_s) p^{r-1} d(i_2, \ldots, i_s) \in \mathbf{Z}$.

(d) $1 \neq p_1 = v(i_1) \neq v(i_2) = p_2 \neq 1$. Let $v(i_2) = \cdots = v(i_t) \neq v(i_{t+1})$. Then by induction hypothesis $p_2^{t-1} d(i_2, \ldots, i_s) \in \mathbf{Z}$ and hence $p_1 d(i_1, \ldots, i_s) = n(i_1, \ldots, i_s) d(i_2, \ldots, i_s) \in \mathbf{Z}$ because $n(i_1, \ldots, i_s) \equiv 0 \bmod p_2^{t-1}$, in this case by (5.2.4).

■ (5.3.5) **Lemma** If $1 \neq v(i_1) = p$, then

$$d(i_1, \ldots, i_s) - p^{-1} d(i_2, \ldots, i_s) \in \mathbf{Z}_{(p)}$$

Proof We distinguish three cases:

(a) $v(i_2) = 1$. Then $d(i_2, \ldots, i_s) \in \mathbf{Z}$ by Lemma (5.3.4) and hence $d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) = p^{-1}((n(i_1, \ldots, i_s) - 1)d(i_2, \ldots, i_s) \in \mathbf{Z}$ because $n(i_1, \ldots, i_s) \equiv 1 \bmod(p)$ by (5.2.3) as $v(i_1) = p$.

(b) $1 \neq v(i_2) = p_2 \neq p$. Then $d(i_2, \ldots, i_s) \in \mathbf{Z}_{(p)}$ by Lemma (5.3.4) and we find $d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) \in \mathbf{Z}_{(p)}$, again because $n(i_1, \ldots, i_s) \equiv 1 \bmod(p)$.

(c) $v(i_2) = p$. Let $v(i_2) = v(i_3) = \cdots = v(i_r) \neq v(i_{r+1})$. Then $p^{r-1}d(i_2, \ldots, i_s) \in \mathbf{Z}$ by Lemma (5.3.4) and hence

$$d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) = p^{-1}(n(i_1, \ldots, i_s) - 1)d(i_2, \ldots, i_s) \in \mathbf{Z}$$

because we have $n(i_1, \ldots, i_s) \equiv 1 \bmod p^r$ in this case according to (5.2.3).

■ (5.3.6) **Proof of (5.3.3)** Let $n = p^r m$, $(m, p) = 1$. The coefficient of X^n in (5.3.3) is then equal to

$$m_n(U) - p^{-1}U_p m_{n/p}^{(p)}(U) - \cdots - p^{-1}U_{p^r} m_{n/p^r}^{(p^r)}(U) \tag{5.3.7}$$

We split up the sum (5.2.7) as

$$m_n(U) = m_{n,0}(U) + m_{n,1}(U) + \cdots + m_{n,r}(U) \tag{5.3.8}$$

where $m_{n,0}(U)$ is the sum of those terms of $m_n(U)$ for which $v(i_1) \neq p$, and $m_{n,j}(U)$ is the sum of those terms of $m_n(U)$ for which $i_1 = p^j$, $j = 1, \ldots, r$.

We now claim

$$m_{n,0}(U) \in \mathbf{Z}_{(p)}[U] \tag{5.3.9}$$

$$m_{n,j}(U) - p^{-1}U_{p^j} m_{n/p^j}^{(p^j)}(U) \in \mathbf{Z}_{(p)}[U] \tag{5.3.10}$$

Statement (5.3.9) follows immediately from Lemma (5.3.4); and statement (5.3.10) follows from Lemma (5.3.5). This concludes the proof of (5.3.3).

■ (5.3.11) **Proof of the integrality of $F_U(X, Y)$** (conclusion) Because (5.3.3) holds, we know by the functional equation lemma that $F_U(X, Y) \in A_p[\![X, Y]\!] = \mathbf{Z}_{(p)}[U][\![X, Y]\!]$. This holds for all prime numbers p, hence $F_U(X, Y) \in \mathbf{Z}[U][\![X, Y]\!]$.

■ (5.3.12) **Proof of the universality of $F_U(X, Y)$** To prove the universality $F_U(X, Y)$ we first remark that

$$f_U(X) \equiv X + v(n)^{-1}U_n \quad \bmod(U_2, \ldots, U_{n-1}, \text{degree}(n+1)) \tag{5.3.13}$$

(This follows immediately from the definition of $f_U(X)$; cf. (5.2.6), (5.2.7).) It follows that

$$F_U(X, Y) \equiv X + Y + U_n C_n(X, Y) \quad \bmod(U_2, \ldots, U_{n-1}, \text{degree}(n+1)) \tag{5.3.14}$$

where, as always, $C_n(X, Y) = v(n)^{-1}(X^n + Y^n - (X + Y)^n)$. Choose $\lambda_1^{(n)}, \ldots, \lambda_{n-1}^{(n)}$ such that $\lambda_1^{(n)}\binom{n}{1} + \cdots + \lambda_{n-1}^{(n)}\binom{n}{n-1} = v(n)$ for all $n \in \mathbf{N}\backslash\{1\}$. Let

$$F_U(X, Y) = X + Y + \sum_{i,j \geq 1} e_{ij} X^i Y^j \tag{5.3.15}$$

We now define new elements $y_2, y_3, \ldots \in \mathbf{Z}[U]$ as follows:

$$y_n = \sum_{i=1}^{n-1} \lambda_i^{(n)} e_{i,n-i} \tag{5.3.16}$$

■ (5.3.17) **Lemma** The $y_2, y_3, \ldots$ are a free polynomial basis for $\mathbf{Z}[U]$, i.e., every element of $\mathbf{Z}[U]$ can uniquely be written as a polynomial in the $y_2, y_3, \ldots$.

Proof This follows immediately from (5.3.14) because (5.3.14) says that

$$y_n \equiv U_n \mod(U_2, \ldots, U_{n-1})$$

■ (5.3.18) **Proof of the universality of** $F_U(X, Y)$ (continued) Now let $G(X, Y)$ be an arbitrary one dimensional formal group law over a ring A. Write

$$G(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j$$

We define a homomorphism $\phi: \mathbf{Z}[U] \to A$ by requiring that

$$\phi(y_n) = \sum_{i=1}^{n-1} \lambda_i^{(n)} a_{i,n-i} \tag{5.3.19}$$

This is well defined because of Lemma (5.3.17). Certainly ϕ is the only possible homomorphism $\mathbf{Z}[U] \to A$ such that $\phi_* F_U(X, Y) = G(X, Y)$. It remains to prove that ϕ actually does take $F_U(X, Y)$ into $G(X, Y)$, i.e., that $\phi(e_{ij}) = a_{i,j}$ for all $i, j \geq 1$. This is done by induction with respect to $i + j$, starting with the case $i = 1 = j$, which is trivial because $\lambda_1^{(2)} = 1$, hence $y_2 = e_{1,1}$. Now suppose that $\phi(e_{i,j}) = a_{i,j}$ for all i, j with $i + j < n$. Now because $F_U(X, Y)$ and $G(X, Y)$ are commutative one dimensional formal group laws, we have that the coefficients satisfy certain conditions, viz.

$$a_{ij} = a_{ji}, \qquad e_{ij} = e_{ji} \tag{5.3.20}$$

$$P_{ijk}(e_{l,m}) = 0 = P_{ijk}(a_{l,m}) \tag{5.3.21}$$

where the P_{ijk} are certain universal polynomials expressing associativity. (Cf. also (1.5.3); there is one such polynomial for each triple (i, j, k), $i, j, k \in \mathbf{N}$.) One easily checks that these polynomials are of the form

$$\binom{i+j}{i} C_{i+j,k} - \binom{j+k}{j} C_{i,j+k} - Q_{ijk}(C_{l,m}) \tag{5.3.22}$$

where the Q_{ijk} are certain polynomials with coefficients in $\mathbf{Z}$ involving only the $C_{l,m}$ with $l+m<i+j+k$. Cf. (6.1.6)–(6.1.9) for more details on the $P_{ijk}(C)$. By the induction hypothesis we therefore know that

$$\phi\left(\binom{i+j}{i}e_{i+j,k}-\binom{j+k}{j}e_{i,j+k}\right)=\binom{i+j}{i}a_{i+j,k}-\binom{j+k}{j}a_{i,j+k},\qquad i+j+k=n \tag{5.3.23}$$

We also have by the definition of ϕ that

$$\phi(\lambda_1^{(n)}e_{1,n-1}+\cdots+\lambda_{n-1}^{(n)}e_{n-1,1})=\lambda_1^{(n)}a_{1,n-1}+\cdots+\lambda_{n-1}^{(n)}a_{n-1,1} \tag{5.3.24}$$

and by the binomial coefficient lemma 4.2 we know that (5.3.20), (5.3.23), (5.3.24) together imply that $\phi(e_{ij})=a_{i,j}$ for $i+j=n$. This concludes the proof of the universality of $F_U(X, Y)$.

5.4 Logarithms

Let A be a characteristic zero ring, i.e., $A\to A\otimes\mathbf{Q}$ is injective or, equivalently, A has no additive torsion. Let $F(X, Y)$ be a one dimensional commutative formal group law over A. Then, because $F_U(X, Y)$ over $\mathbf{Z}[U]$ is a universal one dimensional commutative formal group law, there is a unique homomorphism ϕ: $\mathbf{Z}[U]\to A$ such that $\phi_*F_U(X, Y)=F(X, Y)$. Tensoring with $\mathbf{Q}$ gives us a homomorphism (also denoted ϕ) ϕ: $\mathbf{Q}[U]\to A\otimes\mathbf{Q}$. Let

$$f(X)=\log_F(X)=\phi_*f_U(X) \tag{5.4.1}$$

Then $f(X)$ is a power series with coefficients in $A\otimes\mathbf{Q}$ such that

$$F(X, Y)=f^{-1}(f(X)+f(Y)) \tag{5.4.2}$$

(because $A\to A\otimes\mathbf{Q}$ is injective) and such that

$$f(X)\equiv X \mod(\text{degree } 2) \tag{5.4.3}$$

Moreover, again because $A\to A\otimes\mathbf{Q}$ is injective, there is precisely one power series $f(X)$ such that (5.4.2) and (5.4.3) hold. This power series $f(X)$ is called the *logarithm* of the formal group law $F(X, Y)$ and is occasionally denoted $\log_F(X)$.

The name comes from the fact that the logarithm of the one dimensional multiplicative group $\hat{\mathbf{G}}_m(X, Y)$ is equal to

$$\log_{\hat{\mathbf{G}}_m}(X)=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n}=\log(1+X)$$

If A is not a characteristic zero ring, then the logarithm $\log_F(X)$ of a one dimensional commutative formal group law does as a rule not exist.

■ (5.4.4) **Corollary** Every one dimensional commutative formal group law over a $\mathbf{Q}$-algebra is strictly isomorphic to the one dimensional additive formal group law.

Indeed, if $F(X, Y)$ is a one dimensional commutative formal group law over a $\mathbf{Q}$-algebra A, then $\log_F(X)$ is the (unique) strict isomorphism $F(X, Y) \to \hat{\mathbf{G}}_a(X, Y)$. In case A is something like the ring of integers of a local field of characteristic zero (and residue characteristic $p > 0$) there is an occasionally quite useful formula for the logarithm of a formal group law.

■ (5.4.5) **Proposition** Let A be a $\mathbf{Z}_{(p)}$-algebra of characteristic zero such that $\bigcap_n p^n A = \{0\}$. Let $F(X, Y)$ be a one dimensional formal group law over A. Then we have (in $A \otimes \mathbf{Q}[\![X]\!]$)

$$\log_F(X) = \lim_{n \to \infty} p^{-n}[p^n]_F(X) \tag{5.4.6}$$

(Here the topology of $A \otimes \mathbf{Q}[\![X]\!]$ is the natural one defined by $\lim_{n\to\infty} g_n(X) = f(X)$, $g_n(X) = \sum c_{in} X^i, f(X) = \sum d_i X^i \Leftrightarrow \forall\, k, \forall\, m, \exists\, r$ such that $c_{kn} - d_k \in p^m A$ for all $n \geq r$; i.e., for every k the coefficients of X^k in $g_n(X)$ converge p-adically to the coefficient of X^k in $f(X)$ as $n \to \infty$.)

Proof It suffices to prove the proposition in the special case that $A = \mathbf{Z}_{(p)}[U]$ and $F(X, Y) = F_U(X, Y)$ the one dimensional universal formal group law over $\mathbf{Z}[U] \subset \mathbf{Z}_{(p)}[U]$ constructed in Section 5.2 above. Let $f(X) = f_U(X)$. Then we have

$$f(X) = \sum_{n=1}^{\infty} a_n X^n, \qquad a_1 = 1, \qquad a_n \in p^{-v_p(n)}\mathbf{Z}_{(p)}[U] \tag{5.4.7}$$

where $v_p(n) = k$ if $p^k \mid n$ and $p^{k+1} \nmid n$, $k \in \mathbf{N} \cup \{0\}$. Choose $m \in \mathbf{N}$ and let $k = \max_{i=1,\ldots,m}\{v_p(i)\}$. Then for $n > 3k$ we have

$$p^n f(X) \equiv 0 \mod(\text{degree } m+1,\ p^{n-k})$$

and hence, using (5.4.7)

$$f(p^n f(X)) \equiv p^n f(X) \mod(\text{degree } m+1,\ p^{2n-3k})$$

So, for $2n > 3k$, we have by Part (iv) of the functional equation lemma

$$p^n f(X) \equiv f^{-1}(p^n f(X)) = [p^n]_F(X) \mod(\text{degree } m+1,\ p^{2n-3k})$$

and $f(X) \equiv p^{-n}[p^n]_F(X) \mod(\text{degree } m+1,\ p^{n-3k})$ proving (5.4.6).

■ (5.4.8) **Remark** Somewhat related to formula (5.4.6) is the sometimes useful observation that for any (one dimensional) commutative formal group

law over a $\mathbf{Z}_{(p)}$-algebra A there exist for every n power series $\beta_0(X), \ldots, \beta_n(X) \in A[\![X]\!]$, $\beta_0(X) \equiv X \bmod(\text{degree } 2)$ such that

$$(5.4.9)\quad [p^n]_F(X) = p^n\beta_0(X) + p^{n-1}\beta_1(X^p) + \cdots + p\beta_{n-1}(X^{p^{n-1}}) + \beta_n(X^{p^n})$$

(Of course the power series $\beta_i(X)$, $i = 0, \ldots, n$, may depend on n.) This is proved in a rather similar manner as Proposition (5.4.5) as follows. Again it suffices to treat only the special case $A = \mathbf{Z}_{(p)}[U]$, $F(X, Y) = F_U(X, Y)$. Now by (5.4.7) there exists a power series $\gamma(X) \in \mathbf{Q}[U][\![X]\!]$ such that

$$(5.4.10)\qquad p^n f(X) \equiv \gamma(X^{p^{k+1}}) \quad \bmod(p^{n-k}\mathbf{Z}_{(p)}[U][\![X]\!])$$

We proceed to prove (5.4.9) by induction. Suppose we have already found $\beta_0(X), \ldots, \beta_n(X)$ such that (5.4.9) holds mod(degree m). We write

$$(5.4.11)\quad [p^n]_F(X) \equiv p^n\beta_0(X) + \cdots + \beta_n(X^{p^n}) + bX^m \quad \bmod(\text{degree } m+1)$$

Let $k = v_p(m)$, then we have to show that $b \in p^{n-k}\mathbf{Z}_{(p)}[U]$. We can assume $k < n$ (otherwise we are through). Using $f(X) \equiv X \bmod(\text{degree } 2)$ and applying Part (iv) of the functional equation lemma we obtain from (5.4.11)

$$(5.4.12)\quad p^n f(X) \equiv f([p^n]_F(X)) \equiv f(p^{n-k-1}\beta_{k+1}(X^{p^{k+1}}) + \cdots + \beta_n(X^{p^n})) + bX^m$$

$\bmod(p^{n-k}\mathbf{Z}_{(p)}[U][\![X]\!]$, degree $m+1)$. Using (5.4.10) we see that bX^m is a power series in $X^{p^{k+1}} \bmod p^{n-k}\mathbf{Z}_{(p)}[U][\![X]\!]$ proving that $b \in p^{n-k}\mathbf{Z}_{(p)}[U]$ because $v_p(m) = k$.

5.5 Universality properties of $F_S(X, Y)$

Let $F_S(X, Y)$ be the one dimensional commutative formal group law over $\mathbf{Z}[S_2, S_3, \ldots] = \mathbf{Z}[S]$ constructed in Section 3.1. Because $F_U(X, Y)$ over $\mathbf{Z}[U]$ is universal, there exists a unique homomorphism $\phi\colon \mathbf{Z}[U] \to \mathbf{Z}[S]$ such that $\phi_* F_U(X, Y) = F_S(X, Y)$. Now by (3.1.8) we have $F_S(X, Y) \equiv X + Y + S_n v_p(n)^{-1} B_n(X, Y) \bmod(S_2, \ldots, S_{n-1}, \text{degree } n+1)$, and by (5.3.14) we have that $F_U(X, Y) \equiv X + Y + v(n)^{-1} U_n B_n(X, Y) \bmod(U_2, \ldots, U_{n-1}, \text{degree } n+1)$. It follows that

$$(5.5.1)\qquad \phi(U_n) \equiv v_p(n)^{-1} v(n) S_n \quad \bmod(S_2, \ldots, S_{n-1})$$

where $v_p(n) = v(n)$ if $v(n) = p$ and $v_p(n) = 1$ if $v(n) \neq p$. It follows that ϕ induces an isomorphism

$$(5.5.2)\qquad \phi \otimes \mathbf{Z}_{(p)}\colon \mathbf{Z}_{(p)}[U] \to \mathbf{Z}_{(p)}[S]$$

and this proves:

(5.5.3) **Theorem** The formal group law $F_S(X, Y)$ over $\mathbf{Z}_{(p)}[S]$ is universal for one dimensional commutative formal group laws over $\mathbf{Z}_{(p)}$-algebras. (The same statement holds for $F_S(X, Y)$ considered as a formal group law over $\mathbf{Z}[S]$.)

■ (5.5.4) **Remark** If one identifies $\mathbf{Z}_{(p)}[S]$ with $\mathbf{Z}_{(p)}[U]$ by means of $U_i = S_i$, $i = 2, 3, \ldots$, then the formal group laws $F_U(X, Y)$ and $F_S(X, Y)$ become strictly isomorphic. Note that this is not the identification given by $\phi \otimes \mathbf{Z}_{(p)}$. The strict isomorphism is given by $f_S^{-1}(f_U(X))$ which is seen to be p-integral by the functional equation lemma (2.2). (Cf. (5.3.2) and 3.1.)

■ (5.5.5) **Caveat** Let $F(X, Y)$ and $F_U(X, Y)$ be two universal one dimensional commutative formal group laws over $\mathbf{Z}[U]$, then $F(X, Y)$ and $F_U(X, Y)$ need not be isomorphic as formal groups over $\mathbf{Z}[U]$. An example is $F(X, Y) = \phi_* F_U(X, Y)$ where ϕ: $\mathbf{Z}[U] \to \mathbf{Z}[U]$ is the automorphism $U_2 \mapsto U_2 + U_3$, $U_i \mapsto U_i$ for $i \geq 3$. Indeed, there is not even a power series $\alpha(X) = aX + a_2 X^2 + \cdots$ with a a unit in $\mathbf{Z}[U]$, i.e., $a = \pm 1$, such that $\alpha(F(X, Y)) \equiv F_U(\alpha(X), \alpha(Y))$ mod(degree 3).

Conversely, if $F(X, Y)$ is strictly isomorphic over $\mathbf{Z}[U]$ to $F_U(X, Y)$, then $F(X, Y)$ over $\mathbf{Z}[U]$ need not be a universal commutative one dimensional formal group law. To see this, let $F(X, Y) = \alpha^{-1} F_U(\alpha(X), \alpha(Y))$ where $\alpha(X) = X + U_3 X^2$. Then we have that

$$\text{(5.5.6)} \quad \log_F(X) = f_U(\alpha(X)) \equiv X + U_3 X^2 + \frac{U_2}{2} X^2 + \left(U_2 U_3 + \frac{U_3}{3}\right) X^3 \quad \text{mod(degree 4)}$$

Now if $F(X, Y)$ over $\mathbf{Z}[U]$ were universal, there must be a homomorphism ϕ: $\mathbf{Z}[U] \to \mathbf{Z}[U]$ such that $\phi_* \log_F(X) = \log_{F_U}(X)$, which means that there must be elements $b_2 = \phi(U_2)$ and $b_3 = \phi(U_3)$ in $\mathbf{Z}[U]$ such that

$$\text{(5.5.7)} \qquad b_2 + 2b_3 = U_2, \qquad b_3 + 3b_2 b_3 = U_3$$

which is not possible.

5.6 A special choice for the coefficients

In this subsection we discuss a special choice for the integers $n(i_1, \ldots, i_s)$ which will be useful later.

■ (5.6.1) **Definition of the** $n(i_1, \ldots, i_s)$ For each prime number p and each $i \in \mathbf{N}\backslash\{1\}$, let $c(p, i)$ be an integer such that

$$\text{(5.6.2)} \qquad c(p, i) = 1 \quad \text{if} \quad v(i) = 1$$

$$\text{(5.6.3)} \qquad c(p, p^r) = 1 \quad \text{for all } r \in \mathbf{N}$$

$$\text{(5.6.4)} \qquad c(p, i) \equiv \begin{cases} 1 & \bmod(p) \\ 0 & \bmod(q) \end{cases} \quad \text{if} \quad 1 \neq v(i) = q \neq p$$

We now define integers $b(i_1, \ldots, i_s)$ for all sequences $(i_1, \ldots, i_s)$ with $s \in \mathbf{N}$, $i_j \in \mathbf{N}\backslash\{1\}$, $j = 1, \ldots, s$, by the formula

$$\text{(5.6.5)} \qquad b(i_1) = \prod_{p \mid i_1} c(p, i_1)$$

if $s = 1$, and the recursion formula

$$b(i_1, \ldots, i_s) = \prod_{p \mid i_1 \cdots i_s} c(p, i_s) b(i_1, \ldots, i_{s-1}) \tag{5.6.6}$$

if $s \geq 2$. Here the product is over all prime numbers p that divide $i_1 i_2 \cdot \cdots \cdot i_s$, so that the factor $c(p, i_s)$ occurs once irrespective of how high a power of p divides $i_1 i_2 \cdot \cdots \cdot i_s$.

Finally, we define

$$n(i_1, \ldots, i_s) = \frac{b(i_1, \ldots, i_s)}{b(i_2, \ldots, i_s)} \quad \text{if} \quad s \geq 2, \quad n(i_1) = 1 \tag{5.6.7}$$

With induction we obtain from (5.6.6) that

$$b(i_1, \ldots, i_s) = \prod_{p \mid i_1 \cdots i_s} c(p, i_s) \prod_{p \mid i_1 \cdots i_{s-1}} c(p, i_{s-1}) \cdots \prod_{p \mid i_1} c(p, i_1) \tag{5.6.8}$$

so that $n(i_1, \ldots, i_s)$ is equal to

(5.6.9)

$$n(i_1, \ldots, i_s) = \prod_{\substack{p \nmid i_2 \cdots i_s \\ p \mid i_1}} c(p, i_s) \prod_{\substack{p \nmid i_2 \cdots i_{s-1} \\ p \mid i_1}} c(p, i_{s-1}) \cdots \prod_{\substack{p \nmid i_2 \\ p \mid i_1}} c(p, i_2) \prod_{p \mid i_1} c(p, i_1)$$

■ (5.6.10) **Proof that the $n(i_1, \ldots, i_s)$ defined by (5.6.7) (or (5.6.9)) satisfy the conditions (5.2.2)–(5.2.4)** Condition (5.2.2) is clearly satisfied by definition. Suppose that $1 \neq p = v(i_1) = \cdots = v(i_r) \neq v(i_{r+1})$. First suppose that $r \geq 2$. The only prime number dividing i_1 is p, and p also divides $i_2, i_2 i_3, \ldots, i_2 i_3 \cdot \cdots \cdot i_s$, so that (5.6.9) and (5.6.3) say that $n(i_1, \ldots, i_s) = 1$ in this case. Next suppose that $r = 1$. The only prime number dividing i_1 is p and $c(p, i) \equiv 1 \bmod(p)$ for all i according to (5.6.2) and (5.6.4). Therefore (5.6.9) says that $n(i_1, \ldots, i_s) \equiv 1 \bmod(p)$ in this case. This proves condition (5.2.3). Now let $v(i_1) \neq p = v(i_2) = \cdots = v(i_r) \neq v(i_{r+1})$. Then there is a prime number q that divides i_1 but which does not divide $i_2, \ldots, i_r$ and hence does not divide $i_2, i_2 i_3, \ldots, i_2 i_3 \cdot \cdots \cdot i_r$. It now follows from (5.6.9) that $n(i_1, \ldots, i_s)$ contains the factor $c(q, i_2)c(q, i_3) \cdot \cdots \cdot c(q, i_r)$. But $c(q, i_2) \equiv c(q, i_3) \equiv \cdots \equiv c(q, i_r) \equiv 0 \bmod(p)$ according to (5.6.4) because $1 \neq v(i_2) = v(i_3) = \cdots = v(i_r) = p \neq q$. Hence $n(i_1, \ldots, i_s) \equiv 0 \bmod p^{r-1}$ in this case, which proves condition (5.2.4).

■ (5.6.11) **Convention** Fix a choice for the $c(p, i)$ so that (5.6.2)–(5.6.4) are satisfied and let $F_U(X, Y)$ and $f_U(X)$ be the power series defined by (5.2.6)–(5.2.8) with the $n(i_1, \ldots, i_s)$ as specified by (5.6.5)–(5.6.7). From now on unless otherwise stated $F_U(X, Y)$ and $f_U(X)$ will denote precisely these formal power series.

■ (5.6.12) **A formula or U_n in terms of the $m_k(U)$** In the case of these particular choices of $n(i_1, \ldots, i_s)$ there are "reasonable" formulas for the U_n in

terms of the $m_k(U)$. These formulas will later be useful in complex cobordism cohomology.

As before let

$$d(i_1, \ldots, i_s) = \frac{n(i_1, \ldots, i_s)}{v(i_1)} \cdot \cdots \cdot \frac{n(i_s)}{v(i_s)} \tag{5.6.13}$$

then (5.6.7) and (5.6.6) imply that for $s \geq 2$

$$\frac{d(i_1, \ldots, i_s)}{d(i_1, \ldots, i_{s-1})} = v(i_s)^{-1} \prod_{p | i_1 \cdots i_s} c(p, i_s) \tag{5.6.14}$$

Note that this number depends only on the product $i_1 \cdot \cdots \cdot i_s$ and i_s but not on the individual factors $i_1, i_2, \ldots, i_{s-1}$. We define for all $n, l \in \mathbf{N}\backslash\{1\}$

$$\mu(n, l) = \prod_{p | n} c(p, l) \tag{5.6.15}$$

■ (5.6.16) **Theorem**

$$v(n) m_n(U) = U_n + \sum_{\substack{l | n \\ l \neq 1, n}} \frac{\mu(n, l) v(n)}{v(l)} m_{n/l}(U) U_l^{n/l}$$

Proof We have according to (5.2.7), (5.6.13), (5.6.14), and (5.6.15)

$$\begin{aligned} m_n(U) &= \sum d(i_1, \ldots, i_s) U_{i_1} U_{i_2}^{i_1} \cdot \cdots \cdot U_{i_s}^{i_1 \cdots i_{s-1}} \\ &= v(n)^{-1} U_n + \sum_{s \geq 2} \frac{\mu(n, i_s)}{v(i_s)} (d(i_1, \ldots, i_{s-1}) U_{i_1} U_{i_2}^{i_1} \cdot \cdots \\ &\quad \cdot U_{i_{s-1}}^{i_1 \cdots i_{s-2}}) U_{i_s}^{n/i_s} \\ &= v(n)^{-1} U_n + \sum_{\substack{l | n \\ l \neq 1, n}} \frac{\mu(n, l)}{v(l)} m_{n/l}(U) U_l^{n/l} \end{aligned}$$

5.7 Group law chunks and the comparison lemma

■ (5.7.1) **Definition** A commutative one dimensional formal group law chunk of order m over a ring A is a polynomial of total degree $\leq m$ in two indeterminates $F_m(X, Y)$ of the form $F_m(X, Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j$ such that $F_m(X, Y) = F_m(Y, X)$ and $F_m(F_m(X, Y), Z) \equiv F_m(X, F_m(Y, Z))$ mod(degree $m + 1$).

■ (5.7.2) **Example** If $F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^i$ is a one dimensional formal group law over a ring A, then setting $a_{ij} = 0$ for all $i, j \in \mathbf{N}$ such that $i + j > m$ yields a commutative one dimensional formal group law chunk which we shall denote $F_{(m)}(X, Y)$.

■ (5.7.3) **Theorem** $(F_U)_{(m)}(X, Y)$ over $\mathbf{Z}[U_2, \ldots, U_m]$ is a universal commutative formal group law chunk.

Proof This proof is practically identical with that of the universality of $F_U(X, Y)$.

■ (5.7.4) **Corollary** Every one dimensional commutative formal group law chunk comes from a formal group. That is, if $F_m(X, Y)$ over A is a one dimensional commutative formal group law chunk, then there exists a one dimensional commutative formal group law $F(X, Y)$ over A such that $F(X, Y) \equiv F_m(X, Y)$ mod(degree $m + 1$).

■ (5.7.5) **Corollary** (Lazard's comparison lemma) Let $F_m(X, Y)$ and $G_m(X, Y)$ be one dimensional commutative formal group law chunks of order m over a ring A and suppose that $F_m(X, Y) \equiv G_m(X, Y)$ mod(degree m). Then there exists an $a \in A$ such that $F_m(X, Y) \equiv G_m(X, Y) + aC_m(X, Y)$ where $C_m(X, Y) = v(m)^{-1}(X^m + Y^m - (X + Y)^m)$.

Proof This follows immediately from Theorem (5.7.3) and the fact that $F_U(X, Y) \equiv X + Y + U_m C_m(X, Y)$ mod$(U_2, \ldots, U_{m-1}$, degree $m + 1)$.

■ (5.7.6) **Corollary** Let $F(X, Y)$ be a commutative one dimensional formal group law over a ring A. Then $F(X, Y)$ is (strictly) isomorphic to the additive one dimensional formal group law over A if and only if $[p]_F(X) \in pA[\![X]\!]$ for all prime numbers p.

Proof The condition is clearly necessary because if $\alpha(X)$: $F(X, Y) \to \hat{\mathbf{G}}_a(X, Y)$ is an isomorphism, then $\alpha([p]_F(X)) = p\alpha(X)$. Conversely, suppose that the condition is satisfied, and suppose that $\alpha_m(X)$ is a power series such that $\alpha_m(X) \equiv X$ mod(degree 2) and $F(X, Y) \equiv \alpha_m^{-1}(\alpha_m(X) + \alpha_m(Y))$ mod(degree m) with $m \geq 2$. (The induction starts became $\alpha_2(X) = X$ works for $m = 2$.) Then by the comparison lemma we have

$$F(X, Y) \equiv \alpha_m^{-1}(\alpha_m(X) + \alpha_m(Y)) + aC_m(X, Y) \quad \text{mod(degree}(m + 1)) \tag{5.7.7}$$

If $v(m) = 1$, then $\alpha_{m+1}(X) = \alpha_m(X) - aX^m$ is such that $F(X, Y) \equiv \alpha_{m+1}^{-1}(\alpha_{m+1}(X) + \alpha_{m+1}(Y))$ mod(degree $m + 2$). If $v(m) = p$, we have $[p]_F(X) \in pA[\![X]\!]$, $\alpha_m^{-1}(p\alpha_m(X)) \in pA[\![X]\!]$, so that (5.7.7) then implies that

$$a(p^{-1}(pX^m - (pX)^m)) \in pA[\![X]\!]$$

so that there is a $b \in A$ such that $a = pb$. In this case take $\alpha_{m+1}(X) = \alpha(X) - bX^m$ to obtain a power series such that $F(X, Y) \equiv \alpha_{m+1}^{-1}(\alpha_{m+1}(X) + \alpha_{m+1}(Y))$ mod(degree $m + 1$).

■ (5.7.8) **Example** Let k be a ring of characteristic $p > 0$ (i.e., $pa = 0$ for all $a \in A$) where p is a prime number. Let

$$F(X, Y) = X + Y + aX^{p^n}Y^{p^m} + bX^{p^m}Y^{p^n} \tag{5.7.9}$$

Then $F(X, Y)$ is a one dimensional formal group law chunk of order p^{n+m}. If k is a field and $a \neq b$, $n \neq m$, then $F(X, Y)$ does not come from a one dimensional formal group law because, as we shall see in Section 6, every one dimensional formal group law over a field is commutative.

5.8 Invariant differential forms on a one dimensional formal group law

To conclude this section we give Honda's remarkably elegant proof (cf. [188, 189]) that a one dimensional formal group over a characteristic zero ring A is (i) commutative and (ii) admits a logarithm (defined over $A \otimes \mathbf{Q}$). Statement (i) will be proved again in the next section (in a more general context but in a much more cumbersome fashion) and, given (i), (ii) follows (cf. 5.4).

Let $F(X, Y)$ be a one dimensional formal group law over a characteristic zero ring A. By taking partial derivatives with respect to X in the associativity relation $F(F(X, Y), Z) = F(X, F(Y, Z))$ we find

$$\frac{\partial F}{\partial X}(X, F(Y, Z)) = \frac{\partial F}{\partial X}(F(X, Y), Z) \cdot \frac{\partial F}{\partial X}(X, Y) \tag{5.8.1}$$

Let $g(X)$ be the formal power series (with coefficients in A) defined by

$$g(X) \cdot \frac{\partial F}{\partial X}(0, X) = 1 \tag{5.8.2}$$

and let $f(X)$ be the unique formal power series (with coefficients in $A \otimes \mathbf{Q}$) such that

$$\frac{\partial}{\partial X} f(X) = g(X), \qquad f(X) \equiv X \mod(\text{degree } 2) \tag{5.8.3}$$

Then it follows from (5.8.1) (with $X = 0$, $Y = X$, $Z = Y$) and (5.8.2) that

$$\frac{\partial}{\partial X} f(F(X, Y)) = \frac{\partial}{\partial X} f(X) \tag{5.8.4}$$

It follows that

$$f(F(X, Y)) - f(X) \in A \otimes \mathbf{Q}[\![Y]\!] \tag{5.8.5}$$

We write

$$f(F(X, Y)) - f(X) = h(Y) \tag{5.8.6}$$

and substitution of $X = 0$ in (5.8.6) then gives $h(Y) = f(Y)$ so that

$$f(F(X, Y)) = f(X) + f(Y) \tag{5.8.7}$$

which proves that $F(X, Y)$ is commutative and at the same time that $F(X, Y)$ admits a logarithm over $A \otimes \mathbf{Q}$.

The expression $g(X)\,dX$ can be interpreted as a right invariant differential form on $F(X, Y)$. The invariance property is in fact (5.8.4).

6 Most One Dimensional Formal Group Laws Are Commutative

Practically all the formal group laws constructed so far have been commutative. This is no accident, as is shown by Theorem (1.6.7) which we shall prove in this section. The theorem in question says:

6.1 Commutativity theorem

Theorem Let A be a ring that has no elements $a \neq 0$ that are torsion and nilpotent simultaneously (i.e., there do not exist $a \neq 0, a \in A$, and $n, m \in \mathbf{N}$ such that $na = a^m = 0$). Then every one dimensional formal group law is commutative. Conversely, if every one dimensional formal group law over A is commutative, then A has no nonzero torsion nilpotents.

■ (6.1.1) **Proof of necessity of the condition on A** The example is (1.1.8). Suppose $0 \neq a \in A$ and suppose that $n, m \in \mathbf{N}$ are such that $na = a^m = 0$. Let $n \in \mathbf{N}$ be the smallest natural number such that $na = 0$, then $n > 1$; hence there exists a prime number p such that $p \mid n$, let $b = p^{-1}na$, then $b \neq 0$ and $pb = 0$. Also clearly $b^m = 0$; let m be minimal such $b^m = 0$, then $m > 1$. Let $c = b^{m-1}$, then $c \neq 0$, $c^2 = 0$, $pc = 0$. Now let $F(X, Y)$ be the power series (cf. (1.1.8))

$$F(X, Y) = X + Y + cXY^p \tag{6.1.2}$$

It is easy to check that $F(F(X, Y), Z) = F(X, F(Y, Z))$ so that $F(X, Y)$ is a noncommutative formal group law.

■ (6.1.3) **Proof of sufficiency in case A is a characteristic zero ring** Now suppose that A is a characteristic zero ring, i.e., $na = 0$, $a \in A$, $n \in \mathbf{N}$, implies $a = 0$; or, equivalently, the canonical homomorphism $A \to A \otimes \mathbf{Q}$ is injective. Let

$$F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j \tag{6.1.4}$$

be a formal group law over A.

We have

$$F(F(X, Y), Z) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j + Z + \sum_{l,k \geq 1} a_{l,k} \left(X + Y + \sum_{r,s \geq 1} a_{ij} X^r Y^s \right)^l Z^k$$

$$F(X, F(Y, Z)) = X + Y + Z + \sum_{l,k \geq 1} a_{l,k} Y^l Z^k + \sum_{i,m \geq 1} a_{i,m} X^i \left(Y + Z + \sum_{t,s \geq 1} a_{s,t} Y^s Z^t \right)^m$$

so that the associativity condition becomes

$$P_{ijk}(a_{l,m}) = 0, \qquad i, j, k \geq 1 \tag{6.1.5}$$

where $P_{ijk}(C)$ is the polynomial in the $C_{l,m}$, $l + m \leq i + j + k$,

$$P_{ijk}(C) = C_{i+j,k} \binom{i+j}{i} + \sum C_{l,k} \binom{l}{r_0 s_0 i_1 \cdots i_n} C_{r_1,s_1}^{i_1} \cdots C_{r_n,s_n}^{i_n} - C_{i,j+k} \binom{j+k}{k} + \sum C_{i,m} \binom{m}{s_0 t_0 i_1 \cdots i_n} C_{s_1,t_1}^{i_1} \cdots C_{s_n,t_n}^{i_n} \tag{6.1.6}$$

where the first sum is over all $l, n, r_1, \ldots, r_n, s_1, \ldots, s_n, i_1, \ldots, i_n \in \mathbf{N}$, and r_0, $s_0 \in \mathbf{N} \cup \{0\}$ such that

$$\begin{aligned} r_0 + r_1 i_1 + \cdots + r_n i_n &= i \\ s_0 + s_1 i_1 + \cdots + s_n i_n &= j \\ r_0 + s_0 + i_1 + \cdots + i_n &= l \end{aligned} \tag{6.1.7}$$

and the second sum is over all $m, n, s_1, \ldots, s_n, t_1, \ldots, t_n, i_1, \ldots, i_n \in \mathbf{N}$, and s_0, $t_0 \in \mathbf{N} \cup \{0\}$ such that

$$\begin{aligned} s_0 + s_1 i_1 + \cdots + s_n i_n &= j \\ t_0 + t_1 i_1 + \cdots + t_n i_n &= k \\ s_0 + t_0 + i_1 + \cdots + i_n &= m \end{aligned} \tag{6.1.8}$$

Note that conditions (6.1.7) and (6.1.8) imply that

$$P_{ijk}(C) \equiv \binom{i+j}{i} C_{i+j,k} - \binom{j+k}{k} C_{i,j+k} \mod(\ldots, C_{l,m}, \ldots; \quad l + m < i + j + k) \tag{6.1.9}$$

a fact which we have used before.

Now suppose that $a_{r,s} = a_{s,r}$ for all $r + s < t$. Take i, j, k such that $i = k$, $i + j + k = t$. Then $P_{iji}(a) = 0$ implies that

$$\binom{i+j}{i} a_{i+j,i} = \binom{i+j}{i} a_{i,j+i} \tag{6.1.10}$$

(A one–one correspondence between the remaining terms of $P_{iji}(a)$ is given by taking $l = m$, $r_0 = t_0$, $r_1 = t_1, \ldots, r_n = t_n$ in the two sums in (6.1.6).) But A is a

characteristic zero ring, hence $a_{i+j,i} = a_{i,i+j}$, thus giving us an inductive proof that $a_{ij} = a_{j,i}$ for all $i, j \geq 1$.

6.2 Proof that one dimensional formal group laws over integral domains are commutative

■ (6.2.1) **Lemma** Let $F(X, Y)$ be a noncommutative one dimensional formal group law over a ring A. Then there is a nonzero homomorphism of $F(X, Y)$ into $\hat{\mathbf{G}}_m(X, Y)$ or into $\hat{\mathbf{G}}_a(X, Y)$.

Proof We write $X \cdot Y$ for $F(X, Y)$ and $X^{[-1]}$ for $\iota(X) = [-1]_F(X)$. Let $H(X, Y) = X \cdot Y \cdot X^{[-1]}$, i.e., $H(X, Y) = F(X, F(Y, \iota(X)))$. Then $H(0, Y) = Y$, so we can write

$$H(X, Y) = Y + \sum_{n=1}^{\infty} r_n(X)Y^n \tag{6.2.2}$$

where the $r_n(X)$ are elements of $A[\![X]\!]$ such that $r_n(0) = 0$. Because $F(X, Y)$ is noncommutative, there is an $n \in \mathbf{N}$ such that $r_n(X) \neq 0$. Let m be the smallest element of $\mathbf{N}$ such that $r_m(X) \neq 0$. We distinguish two cases.

■ (6.2.3) **Case A**: $m = 1$ In this case one has

$$H(X, Y) \equiv Y(1 + r_1(X)) \mod(Y^2) \tag{6.2.4}$$

and the identity

$$(X \cdot X') \cdot Y \cdot (X \cdot X')^{[-1]} = X \cdot (X' \cdot Y \cdot X'^{[-1]}) \cdot X^{[-1]}$$

which follows from the associativity of $F(X, Y)$, shows that

$$H(X \cdot X', Y) = H(X, H(X', Y)) \tag{6.2.5}$$

And this gives $\mod(Y^2)$

$$Y(1 + r_1(X \cdot X')) \equiv Y(1 + r_1(X'))(1 + r_1(X)) \tag{6.2.6}$$

which means that

$$r_1(X \cdot X') = r_1(X) + r_1(X') + r_1(X)r_1(X') \tag{6.2.7}$$

and (6.2.7) says that $r_1(X)$ is a homomorphism of $F(X, Y)$ into $\hat{\mathbf{G}}_m(X, Y)$.

■ (6.2.8) **Case B**: $m > 1$ In this case one has

$$H(X, Y) \equiv Y + r_m(X)Y^m \mod(Y^{m+1}) \tag{6.2.9}$$

and using (6.2.5) again one finds $\mod(Y^{m+1})$, using $m \geq 2$,

$$\begin{aligned} Y + r_m(X \cdot X')Y^m &\equiv H(X', Y) + r_m(X)H(X', Y)^m \\ &\equiv Y + r_m(X')Y^m + r_m(X)(Y + r_m(X')Y^m)^m \\ &\equiv Y + r_m(X')Y^m + r_m(X)Y^m \end{aligned}$$

which shows that

$$r_m(X \cdot X') = r_m(X) + r_m(X') \tag{6.2.10}$$

i.e., that r_m is a homomorphism of $F(X, Y)$ into $\hat{G}_a(X, Y)$.

■ (6.2.11) **Lemma** Let A be an integral domain and let $F(X, Y)$, $F'(X, Y)$ be one dimensional formal group laws over A. Suppose that $F'(X, Y)$ is commutative and that there exists a nonzero homomorphism $\alpha(X)$: $F(X, Y) \to F'(X, Y)$. Then $F(X, Y)$ is commutative.

Proof We write

$$\alpha(X) = \sum_{n \geq r} a_n X^n, \qquad a_r \neq 0 \tag{6.2.12}$$

Let

$$C(X, Y) = X \cdot Y \cdot X^{[-1]} \cdot Y^{[-1]} = F(X, F(Y, F(\imath(X), \imath(Y)))) \tag{6.2.13}$$

be the commutator of X and Y with respect to the group law $F(X, Y)$. Because $F'(X, Y)$ is commutative and $\alpha(X)$ is a homomorphism we must have

$$\alpha(C(X, Y)) = 0 \tag{6.2.14}$$

Suppose that $C(X, Y) \neq 0$, then $C(X, Y) = D_m(X, Y)$ mod(degree $m + 1$) with $D_m(X, Y) \neq 0$ a homogeneous polynomial of degree m in X, Y. Relations (6.2.12) and (6.2.14) now say that

$$a_r D_m(X, Y) \equiv 0 \quad \text{mod(degree } mr + 1) \tag{6.2.15}$$

which, because A is an integral domain and $a_r \neq 0$, implies the contradiction that $D_m(X, Y) = 0$. This proves the lemma.

6.3 Proof of Theorem 6.1 (conclusion)

Let A be a ring with no elements $a \neq 0$ that are simultaneously torsion and nilpotent. Let $F(X, Y)$ be a one dimensional formal group law over A. We write

$$F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j \tag{6.3.1}$$

For each prime ideal $\mathfrak{p}$ of A let ϕ: $A \to A/\mathfrak{p}$ be the natural projection. In addition let ϕ_∞: $A \to A \otimes \mathbf{Q}$ be the natural homomorphism $a \mapsto a \otimes 1$. Lemmas (6.2.1) and (6.2.11) imply that the formal groups $(\phi)_* F(X, Y)$ are all commutative, which means that the elements $a_{ij} - a_{ji}$ are in $\mathfrak{p}$ for every prime ideal $\mathfrak{p}$, so that the elements $a_{ij} - a_{ji}$ are nilpotents. But $(\phi_\infty)_* F(X, Y)$ is also commutative by (6.1.3) (or 5.8), therefore $a_{ij} - a_{ji}$ is also in $\mathrm{Ker}(\phi_\infty)$, i.e., $a_{ij} - a_{ji}$ is also a torsion element for all i, j. Because of the hypothesis on A this means that $a_{ij} = a_{ji}$ for all i, j, i.e., that $F(X, Y)$ is commutative.

7 Honda's Method for Constructing Formal Group Laws

7.1 The setting

In this whole section K will be a discrete valuation field of characteristic 0 (not necessarily complete) with ring of integers A and maximal ideal $\mathfrak{m}$ such that the residue field $k = A/\mathfrak{m}$ is of characteristic $p > 0$. In addition we require that there exists an endomorphism $\sigma\colon K \to K$ and a power q of p such that

$$\sigma(a) \equiv a^q \mod(\mathfrak{m}) \qquad \text{for all} \quad a \in A \tag{7.1.1}$$

Examples of such fields K are, e.g., all fields $A \otimes \mathbf{Q}$ with $\mathbf{Z}_{(p)} \subset A \subset \mathbf{Z}_p$ and all finite extensions of the p-adic numbers $\mathbf{Q}_p$.

We fix a prime element π of A.

7.2 The constructions

Let K be a field as in 7.1. Then $K_\sigma[\![T]\!]$ denotes the noncommutative ring of power series in T over K with the multiplication rule $Ta = \sigma(a)T$; $A_\sigma[\![T]\!]$ is the subring of $K_\sigma[\![T]\!]$ consisting of all power series with coefficients in A.

Now let $u(T) \in A_\sigma[\![T]\!]$ be an element such that $u(T) \equiv \pi \mod(\text{degree } 1)$, where π is the (fixed) prime element of A. We set

$$u^{-1}\pi = 1 + \sum_{i=1}^{\infty} b_i T^i, \qquad b_i \in K \tag{7.2.1}$$

and

$$f(X) = X + \sum_{i=1}^{\infty} b_i X^{q^i}, \qquad F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{7.2.2}$$

7.3 Honda formal group laws

■ **Theorem** Let $F(X, Y)$ be obtained as in (7.2.1)–(7.2.3). Then $F(X, Y)$ has its coefficients in A and hence defines a commutative one dimensional formal group law over A.

Proof From the relation (7.2.1) we have $u(1 + \sum_{i=1}^{\infty} b_i T^i) = \pi$. Writing $u(T) = \pi + a_1 T + a_2 T^2 + \cdots$, we obtain

$$\pi b_n = -a_1 \sigma(b_{n-1}) - a_2 \sigma^2(b_{n-2}) - \cdots - a_{n-1}\sigma^{n-1}(b_1) - a_n \tag{7.3.1}$$

so that $f(X)$ satisfies the functional equation

$$f(X) = X + \sum_{i=1}^{\infty} s_i \sigma_*^i f(X^{q^i}) \tag{7.3.2}$$

with $s_i = -\pi^{-1}a_i$. To prove Theorem 7.3 it now suffices to apply the functional equation lemma 2.2.

7.4 Remark

Again let $u(T) = \pi + a_1 T + a_2 T^2 + \cdots$, and now consider

$$\pi u^{-1} = 1 + \sum_{i=1}^{\infty} \bar{b}_i T^i \tag{7.4.1}$$

and set

$$\bar{f}(X) = X + \sum_{i=1}^{\infty} \bar{b}_i T^i, \qquad \bar{F}(X, Y) = \bar{f}^{-1}(\bar{f}(X) + \bar{f}(Y)) \tag{7.4.2}$$

then the $\bar{b}_i$ satisfy the equation

$$\bar{b}_n \sigma^n(\pi) + \bar{b}_{n-1}\sigma^{n-1}(a_1) + \cdots + \bar{b}_1 \sigma(a_{n-1}) + a_n = 0 \tag{7.4.3}$$

From this (by means of the reverse argument of 3.3) we find

$$\bar{b}_n = \sum_{i_1 + \cdots + i_r = n} c_{i_1} \sigma^{i_1}(c_{i_2}) \cdots \sigma^{i_1 + \cdots + i_{r-1}}(c_{i_r}) \tag{7.4.4}$$

where $c_i = -\sigma^i(\pi)^{-1} a_i$. It follows (still reversing 3.3) that

$$\bar{b}_n = c_1 \sigma(\bar{b}_{n-1}) + \cdots + c_{n-1}\sigma^{n-1}(\bar{b}_1) + c_n \tag{7.4.5}$$

which proves that $\bar{f}(X)$ satisfies the functional equation

$$\bar{f}(X) = X + \sum_{i=1}^{\infty} c_i \sigma_*^i \bar{f}(X^{q^i}) \tag{7.4.6}$$

which proves that $\bar{F}(X, Y)$ is also a formal group law over A. The formal group laws $\bar{F}(X, Y)$ and $F(X, Y)$ are generally not isomorphic over A. (Except when $\sigma(\pi) = \pi$, then $F(X, Y) = \bar{F}(X, Y)$.)

8 The Lubin–Tate Formal Group Laws

An occasionally extremely useful and a certainly very elegant construction of formal group laws has been given by Lubin and Tate [264]. The formal group laws so obtained are special cases of the ones obtainable by means of the functional equation lemma 2.2 (just as were the Honda formal group laws of the previous section), but they deserve specific mention all the same.

8.1 The setting and statement of the theorem

Let A be the ring of integers of a discretely valued complete local field K with finite residue field k of q elements. Let π be a uniformizing element, i.e., the maximal ideal of A is (π). Let $\mathscr{E}_\pi$ be the set of all power series $e(X)$ in $A[\![X]\!]$ such that

$$e(X) \equiv \pi X \mod(\text{degree } 2), \qquad e(X) \equiv X^q \mod(\pi) \tag{8.1.1}$$

The simplest example of such a power series is $e(X) = \pi X + X^q$.

■ (8.1.2) **Lemma** Let $e(X)$ and $\bar{e}(X)$ be in $\mathscr{E}_\pi$ and let $L(X_1, \ldots, X_n) = a_1 X_1 + \cdots + a_n X_n$ be a linear form in $X_1, \ldots, X_n$ with coefficients in A. Then there is a unique power series $\Phi(X_1, \ldots, X_n) \in A[\![X_1, \ldots, X_n]\!]$ such that

(8.1.3) $\quad \Phi(X_1, \ldots, X_n) \equiv L(X_1, \ldots, X_n) \mod(\text{degree } 2)$

(8.1.4) $\quad e(\Phi(X_1, \ldots, X_n)) = \Phi(\bar{e}(X_1), \ldots, \bar{e}(X_n))$

The proof of this lemma is not difficult and will be given in Section 8.2. First we use the lemma to construct formal group laws. Given $e(X) \in \mathscr{E}_\pi$, let $F_e(X, Y)$ be the unique power series in $A[\![X, Y]\!]$ such that $F_e(X, Y) \equiv X + Y$ mod(degree 2) and $e(F_e(X, Y)) = F_e(e(X), e(Y))$; given $a \in A$ and a second power series $\bar{e}(X) \in \mathscr{E}_\pi$, we let $[a]_{e,\bar{e}}(X)$ be the unique power series such that $[a]_{e,\bar{e}}(X) \equiv aX$ mod(degree 2) and $e([a]_{e,\bar{e}}(X)) = [a]_{\bar{e},\bar{e}}(\bar{e}(X))$. We shall write $[a]_e(X)$ for $[a]_{e,e}(X)$. With these notations we have

■ (8.1.5) **Theorem** (Lubin–Tate [264, Theorem 1])

(i) The power series $F_e(X, Y)$ is a one dimensional commutative formal group law over A.

(ii) $[a]_e(X)$ is an endomorphism of $F_e(X, Y)$ for all $a \in A$.

(iii) $[\pi]_e(X) = e(X)$.

(iv) $[1]_{\bar{e},e}(X)$ is a strict isomorphism over A from $F_e(X, Y)$ to $F_{\bar{e}}(X, Y)$.

(v) $[a]_e([b]_e(X)) = [ab]_e(X)$.

(vi) $F_e([a]_e(X), [b]_e(X)) = [a + b]_e(X)$.

(vii) $[1]_{\bar{e},e}([a]_e(X)) = [a]_{\bar{e}}([1]_{\bar{e},e}(X))$.

Proof All these statements are proved by applications of the uniqueness statement of Lemma (8.1.2). For example, the associativity of $F_e(X, Y)$ is proved by observing that by definition

$$e(F_e(X, F_e(Y, Z))) = F_e(e(X), e(F_e(X, Y))) = F_e(e(X), F_e(e(Y), e(Z)))$$

$$F_e(X, F_e(Y, Z)) \equiv X + Y + Z \mod(\text{degree } 2)$$

$$e(F_e(F_e(X, Y), Z)) = F_e(e(F_e(X, Y)), e(Z)) = F_e(F_e(e(X), e(Y)), e(Z))$$

$$F_e(F_e(X, Y), Z) \equiv X + Y + Z \mod(\text{degree } 2)$$

The uniqueness part of Lemma (8.1.2) now says that $F_e(F_e(X, Y), Z) = F_e(X, F_e(Y, Z))$. Commutativity of $F_e(X, Y)$ and statements (ii)–(vii) of the theorem are proved in the same way.

■ (8.1.6) **Corollary** The map $a \mapsto [a]_e(X)$ is an injective homomorphism from A into the endomorphism ring of the formal group law $F_e(X, Y)$.

Proof This follows from (v) and (vi), and the fact that $[a]_e(X) \equiv aX$ mod(degree 2).

This means that $F_e(X, Y)$ has a rather large endomorphism ring. Indeed, as we shall see, if the characteristic of K is zero, this endomorphism ring is maximally large. (Cf. Chapter IV, Proposition (23.2.6).)

8.2 Proof of Lemma (8.1.2)

This lemma is proved by constructing a series of polynomials $\Phi_r(X_1, \ldots, X_n)$ of (total) degree r in $X_1, \ldots, X_n$ and with coefficients in A such that (8.1.3) and (8.1.4) hold mod(degree $r+1$) and by showing that these $\Phi_r(X_1, \ldots, X_n)$ are unique (mod(degree $r+1$)). This is done by induction, the case $r = 1$ being trivial: we must take $\Phi_1(X_1, \ldots, X_n) = L(X_1, \ldots, X_n)$. Now suppose we have already found $\Phi_r(X_1, \ldots, X_n)$ and proved its uniqueness. Write

$$\Phi_{r+1}(X_1, \ldots, X_n) = \Phi_r(X_1, \ldots, X_n) + E_{r+1}(X_1, \ldots, X_n) \tag{8.2.1}$$

where $E_{r+1}(X_1, \ldots, X_n)$ is a yet to be determined homogeneous polynomial of degree $r+1$. Suppose that

$$\begin{aligned} &\Phi_r(\bar{e}(X_1), \ldots, \bar{e}(X_n)) \\ &\quad \equiv e(\Phi_r(X_1, \ldots, X_n)) + D_{r+1}(X_1, \ldots, X_n) \mod(\text{degree } r+2) \end{aligned} \tag{8.2.2}$$

where $D_{r+1}(X_1, \ldots, X_n)$ is homogeneous of degree $r+1$ with coefficients in A. We have mod(degree $r+2$)

$$\Phi_{r+1}(\bar{e}(X_1), \ldots, \bar{e}(X_n)) \equiv \Phi_r(\bar{e}(X_1), \ldots, \bar{e}(X_n)) + \pi^{r+1}E_{r+1}(X_1, \ldots, X_n) \tag{8.2.3}$$

$$e(\Phi_{r+1}(X_1, \ldots, X_n)) \equiv e(\Phi_r(X_1, \ldots, X_n)) + \pi E_{r+1}(X_1, \ldots, X_n) \tag{8.2.4}$$

Equations (8.2.3)–(8.2.4) show that if $\Phi_{r+1}(X_1, \ldots, X_n)$ is to satisfy (8.1.3)–(8.1.4) mod(degree $r+2$), then $\Phi_{r+1}(X_1, \ldots, X_n)$ must be equal to $\Phi_r(X_1, \ldots, X_n) + E_{r+1}(X_1, \ldots, X_n)$ with $E_{r+1}(X_1, \ldots, X_n)$ given by

$$E_{r+1}(X_1, \ldots, X_n) \equiv (\pi - \pi^{r+1})^{-1}D_{r+1}(X_1, \ldots, X_n) \tag{8.2.5}$$

This takes care of the uniqueness assertion of the lemma, and it remains only to prove that $E_{r+1}(X_1, \ldots, X_n)$ as determined by (8.2.5) is integral; i.e., since $r \geq 1$ we have to show that $D_{r+1}(X_1, \ldots, X_n) \equiv 0 \bmod \pi$. To see this remember that $e(X) \equiv \bar{e}(X) \equiv X^q \bmod(\pi)$. So that, because $a^q \equiv a \bmod(\pi)$ for all $a \in A$ (the residue field k has q elements),

$$\begin{aligned} \Phi_r(\bar{e}(X_1), \ldots, \bar{e}(X_n)) &\equiv \Phi_r(X_1^q, \ldots, X_n^q) \\ &\equiv (\Phi_r(X_1, \ldots, X_n))^q \equiv e(\Phi_r(X_1, \ldots, X_n)) \end{aligned}$$

where all congruences are mod(π). In view of (8.2.2) this shows that indeed $D_{r+1}(X_1, \ldots, X_n) \equiv 0 \bmod(\pi)$. This concludes the proof. (The power series $\Phi(X_1, \ldots, X_n)$ is the unique power series such that $\Phi(X_1, \ldots, X_n) \equiv \Phi_r(X_1, \ldots, X_n)$ mod(degree $r+1$) for all $r = 1, 2, 3, \ldots$.)

8.3 The Lubin-Tate formal group laws and the functional equation lemma. Isomorphism results

We apply the functional equation lemma 2.2 with A, K, q as in 8.1 and with $\mathfrak{A} = (\pi)$, $s_1 = \pi^{-1}$, $s_2 = s_3 = \cdots = 0$, σ the identity automorphism of K, and $g(X) = X$. This gives a power series $f(X)$ that satisfies the recursion equation

$$f(X) = X + \pi^{-1} f(X^q) \tag{8.3.1}$$

Let

$$F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{8.3.2}$$

$$[\pi]_F(X) = f^{-1}(\pi f(X)) \tag{8.3.3}$$

Now $\pi^{-1}(\pi f(X^q)) - \pi f(X) = \pi^{-1}\pi f(X^q) - \pi f(X) = f(X^q) - \pi f(X) = \pi f(X) - \pi X - \pi f(X) = -\pi X$. It follows that $\pi f(X)$ satisfies a functional equation similar to (8.3.1) (with X replaced by πX), so that by parts (i) and (ii) of the functional equation lemma we have that $F(X, Y)$ and $[\pi]_F(X)$ have integral coefficients, so that $F(X, Y)$ is a one dimensional commutative formal group law over A having $[\pi]_F(X)$ as an endomorphism.

We claim that

$$[\pi]_F(X) \equiv X^q \mod(\pi) \tag{8.3.4}$$

This is obviously true modulo (degree$(q + 1)$) by the definition of $[\pi]_F(X)$; cf. (8.3.3). So suppose that (8.3.4) has been proved mod(degree m) with $m > q$. Then we have mod(π, degree$(m + 1)$)

$$f([\pi]_F(X)) \equiv [\pi]_F(X) + \pi^{-1} f([\pi]_F(X)^q) \equiv [\pi]_F(X) + \pi^{-1} f(X^{q^2})$$

$$\pi f(X) \equiv \pi X + f(X^q) \equiv \pi X + X^q + \pi^{-1} f(X^{q^2})$$

and it follows that $[\pi]_F(X) \equiv X^q$ mod(π, degree $m + 1$), which proves (8.3.4). (Alternative proof: apply part (iv) of the functional equation lemma.)

The power series $[\pi]_F(X)$ is therefore in $\mathscr{E}_\pi$, so by the uniqueness part of the Lubin–Tate lemma (8.1.2) we have that $F(X, Y) = F_e(X, Y)$ with $e(X) = [\pi]_F(X)$. Now if $F_{\bar{e}}(X, Y)$ is any other Lubin–Tate formal group law over A, then $F_{\bar{e}}(X, Y)$ is strictly isomorphic to $F_e(X, Y)$ by part (iv) of the theorem, so

$$F_{\bar{e}}(X, Y) = \bar{f}^{-1}(\bar{f}(X) + \bar{f}(Y)) \tag{8.3.5}$$

with $\bar{f}(X) = f([1]_{e,\bar{e}}(X))$. But by part (iii) of the functional equation lemma $\bar{f}(X)$ satisfies a functional equation of the same type as $f(X)$. Conversely, part (ii) of the functional equation lemma says that power series that satisfy the same type of functional equation (i.e., everything the same except possibly $g(X)$, $g(X) \equiv X$ mod(degree 2)) yield strictly isomorphic formal groups. And if $\alpha(X) \in A[\![X]\!]$, $\alpha(X) \equiv X$ mod(degree 2), then one has mod(π)

$$\alpha^{-1}([\pi]_F(\alpha(X))) \equiv \alpha^{-1}(\alpha(X)^q) \equiv \alpha^{-1}(\alpha(X^q)) \equiv X^q$$

so that if $\bar{F}(X, Y)$ is isomorphic to $F(X, Y)$, where $F(X, Y)$ is as in (8.3.2), then

$$[\pi]_{\bar{F}}(X) \equiv [\pi]_F(X) \equiv X^q \mod(\pi)$$

We have proved:

■ (8.3.6) **Proposition** The Lubin-Tate formal group laws $F_e(X, Y)$ obtained from power series $e(X) \in \mathscr{E}_\pi$ are in one-one correspondence with formal group laws obtained by means of the functional equation lemma with A, K, q as in 8.1, $\mathfrak{A} = (\pi)$, $\sigma = id$, $s_1 = \pi^{-1}$, $s_2 = s_3 = \cdots = 0$ (and varying $g(X)$). The correspondence is given by

$$g(X) \mapsto f_g^{-1}(\pi f_g(X)) \in \mathscr{E}_\pi \tag{8.3.7}$$

Let $\hat{A}_{nr}$ be the ring of integers of the completion $\hat{K}_{nr}$ of the maximal unramified extension K_{nr} of K. Then if $F(X, Y)$ and $\bar{F}(X, Y)$ are Lubin-Tate formal group laws over A corresponding to different uniformizing elements π, $\bar{\pi}$, they become isomorphic over $\hat{A}_{nr}$. More precisely, if $\bar{\pi} = u\pi$, $u \in U(A)$, let $\varepsilon \in \hat{A}_{nr}$ be such that $\sigma(\varepsilon) = u\varepsilon$ where σ is the Frobenius automorphism of K_{nr}/K extended (by continuity) to $\hat{K}_{nr}$. (NB: such an ε always exists; cf. remark (8.3.15)(ii).) Then we have

■ (8.3.8) **Proposition** There is a power series $\alpha(X) \in \hat{A}_{nr}[\![X]\!]$ such that $\alpha(X) \equiv \varepsilon X$ mod(degree 2) and such that

$$\sigma_* \alpha(X) = \alpha([u]_e(X)) \tag{8.3.9}$$

$$\alpha(F(X, Y)) = \bar{F}(\alpha(X), \alpha(Y)) \tag{8.3.10}$$

$$\alpha([a]_e(X)) = [a]_{\bar{e}}(\alpha(X)) \tag{8.3.11}$$

where $e(X) \in \mathscr{E}_\pi$ and $\bar{e}(X) \in \mathscr{E}_{\bar{\pi}}$ are such that $F_e(X, Y) = F(X, Y)$, $F_{\bar{e}}(X, Y) = \bar{F}(X, Y)$.

Proof By Proposition (8.3.6) (and parts (iv), (vii) of Theorem (8.1.5), or, alternatively, part (ii) of the functional equation lemma 2.2) we can assume that $F(X, Y) = f^{-1}(f(X) + f(Y))$, $\bar{F}(X, Y) = \bar{f}^{-1}(\bar{f}(X) + \bar{f}(Y))$ where $f(X)$ and $\bar{f}(X)$ satisfy the functional equations

$$f(X) = X + \pi^{-1} f(X^q) \tag{8.3.12}$$

$$\bar{f}(X) = X + \bar{\pi}^{-1} \bar{f}(X^q) \tag{8.3.13}$$

Now we can also view $\bar{f}(X)$ as obtained from a functional equation situation $A = \hat{A}_{nr}$, $K = \hat{K}_{nr}$, q, $\sigma = \text{Frobenius} \in \text{Aut}(\hat{K}_{nr}/K)$, $\mathfrak{A} = \bar{\pi}\hat{A}_{nr}$, $s_1 = \bar{\pi}^{-1}$, $s_2 = s_3 = \cdots = 0$, $g(X) = X$. Now consider $\varepsilon f(X)$. We have

$$\begin{aligned} \varepsilon f(X) - \bar{\pi}^{-1}\sigma_*(\varepsilon f(X^q)) &= \varepsilon f(X) - \bar{\pi}^{-1}\sigma(\varepsilon) f(X^q) = \varepsilon f(X) - \bar{\pi}^{-1}\varepsilon u f(X^q) \\ &= \varepsilon f(X) - \varepsilon\pi^{-1} f(X^q) = \varepsilon X \in \hat{A}_{nr}[\![X]\!] \end{aligned}$$

So, $\varepsilon f(X)$ satisfies the same type of functional equation (over $\hat{A}_{nr}$) as $\bar{f}(X)$, so that by part (ii) of the functional equation lemma we have that

$$\alpha(X) = \bar{f}^{-1}(\varepsilon f(X)) \tag{8.3.14}$$

is a power series with coefficients in $\hat{A}_{nr}$.

Equations (8.3.11) and (8.3.10) are now immediate (if one remembers that $[a]_e(X) = f^{-1}(af(X))$ and $[a]_{\bar{e}}(X) = \bar{f}^{-1}(a\bar{f}(X))$). As to (8.3.9), we have

$$\sigma_*(\alpha(X)) = \bar{f}^{-1}(\sigma_*(\varepsilon f)(X)) = \bar{f}^{-1}(\sigma(\varepsilon)f(X)) = \bar{f}^{-1}(\varepsilon u f(X))$$
$$= \bar{f}^{-1}(\varepsilon f([u]_e(X))) = \alpha([u]_e(X)).$$

This proves the proposition.

■ (8.3.15) **Remarks**

(i) Proposition (8.3.8) will be important in the application of formal group laws to local class field theory (cf. Section 32).

(ii) Let $u \in \hat{A}_{nr}$ be a unit. Then there exists an ε such that $\sigma(\varepsilon) = u\varepsilon$. This can be proved via first Galois cohomology groups and a generalized version will be proved later (Chapter IV, Proposition (24.1.7)). Here is a direct proof. The residue field k_{sc} of $\hat{A}_{nr}$ is an algebraic closure of k. Let $U^n(\hat{A}_{nr})$ be the subgroup of $U(\hat{A}_{nr}) = \hat{A}_{nr}^*$ of elements $x \in \hat{A}_{nr}$ such that $x \equiv 1 \bmod \pi^n$. Now let $u \in \hat{A}_{nr}$, because $\sigma(x) \equiv x^q \bmod \pi$ and because k_{sc} is algebraically closed (so that we can solve $y^{q-1} = \bar{a}$ for all $\bar{a} \in k_{sc}$) there is an $y_1 \in U(\hat{A}_{nr})$ such that $y_1^{-1}\sigma(y_1) \equiv u \bmod \pi$. Let $u_1 = y_1\sigma(y_1)^{-1}u$, then $u_1 = 1 + \pi a_2$ for a certain $a_2 \in \hat{A}_{nr}$. Again because $\sigma(x) \equiv x^q \bmod \pi$ and because k_{sc} is algebraically closed (so that we can solve $y^q - y = \bar{a}$ for all $\bar{a} \in k_{sc}$), there is an $z_2 \in \hat{A}_{nr}$ such that $a_2 \equiv z_2 - \sigma(z_2)$. Let $y_2 = 1 + \pi z_2$, then $y_2 u_1 \sigma(y_2)^{-1} \equiv 1 \bmod \pi^2$ so that $y_2 y_1 \sigma(y_2 y_1)^{-1} u = 1 + \pi^2 a_3$ for a certain $a_3 \in \hat{A}_{nr}$. Continuing in this way we find a series of elements $y_1, y_2, y_3, \ldots, y_i \in U^{i-1}(\hat{A}_{nr})$ such that

$$(y_i y_{i-1} \cdots y_2 y_1)\sigma(y_i y_{i-1} \cdots y_2 y_1)^{-1} u \equiv 1 \mod \pi^i$$

Because $U(\hat{A}_{nr})$ is complete the limit $\lim_{i\to\infty}(y_i y_{i-1} \cdots y_2 y_1) = y$ exists and is in $U(\hat{A}_{nr})$. Because $U(A_{nr})$ is Hausdorff (and σ is continuous), we have $y\sigma(y)^{-1}u = 1$. Q.E.D.

■ (8.3.16) Let $F_e(X, Y)$ be a Lubin–Tate formal group law over A, with $e(X) \equiv \pi X$ mod(degree 2). Then according to Proposition (8.3.6) we know that the logarithm $f_e(X)$ of $F_e(X, Y)$ satisfies a functional equation

$$f_e(X) - \pi^{-1} f_e(X^q) \in A[\![X]\!] \tag{8.3.17}$$

We claim that the uniformizing element π of A is uniquely determined by condition (8.3.17). To see this let $b_i \in K$ be the coefficient of X^{q^i} in $f_e(X)$. Then (8.3.17) implies that

$$b_i - \pi^{-1} b_{i-1} = c_i \in A \qquad \text{for all} \quad i \in \mathbf{N} \tag{8.3.18}$$

and hence inductively

(8.3.19) $$v(b_i) = -i$$

where v is the normalized exponential valuation on K. Now let $\hat{\pi}$ be a second element of A and suppose that $f_e(X) - \hat{\pi}^{-1} f_e(X^q) \in A[\![X]\!]$. Then

(8.3.20) $$b_i - \hat{\pi}^{-1} b_{i-1} = \hat{c}_i \qquad \text{for all} \quad i \in \mathbf{N}, \quad v(\hat{\pi}) = 1$$

Multiplying (8.3.18) and (8.3.20) respectively with πb_i^{-1} and $\hat{\pi} b_i^{-1}$ we find

(8.3.21) $$\pi = c_i \pi b_i^{-1} + b_{i-1} b_i^{-1}, \qquad \hat{\pi} = \hat{c}_i \hat{\pi} b_i^{-1} + b_{i-1} b_i^{-1}$$

so that $\pi \equiv \hat{\pi} \bmod \pi^{i+1}$ for all $i \in \mathbf{N}$. Hence $\pi = \hat{\pi}$. So every Lubin-Tate formal group law $F(X, Y)$ determines uniquely a uniformizing element of A which we shall denote $\pi(F)$.

■ (8.3.22) **Proposition** The two Lubin-Tate formal group laws $F(X, Y)$ and $G(X, Y)$ are isomorphic over A if and only if $\pi(F) = \pi(G)$ and then $F(X, Y)$ and $G(X, Y)$ are strictly isomorphic over A.

Proof If $\pi(F) = \pi(G)$, then the logarithms $f(X)$, $g(X)$ of $F(X, Y)$ and $G(X, Y)$ both satisfy functional equations $f(X) - \pi^{-1} f(X^q) \in A[\![X]\!]$, $g(X) - \pi^{-1} g(X^q) \in A[\![X]\!]$ which according to the part (iii) of the functional equation lemma 2.2 means that $F(X, Y)$ and $G(X, Y)$ are strictly isomorphic.

Conversely, suppose that $F(X, Y)$ and $G(X, Y)$ are isomorphic over A. Let the isomorphism be $\alpha(X) = uX + \cdots$, then we have $uf(X) = g(\alpha(X))$ and part (ii) of the functional equation lemma says that $g(\alpha(X)) - \pi(G)^{-1} g(\alpha(X^q)) \in A[\![X]\!]$ so that $uf(X) - \pi(G)^{-1} uf(X^q) \in A[\![X]\!]$ hence $f(X) - \pi(G)^{-1} f(X^q) \in A[\![X]\!]$ which implies $\pi(F) = \pi(G)$ by (8.3.16).

■ (8.3.23) **Remarks**

(i) Later (Chapter IV, (21.8.9) or (24.5.3)) we shall see that the Lubin-Tate formal group laws are precisely the formal group laws over A that (a) admit A as a ring of endomorphisms (more precisely there must be a ring homomorphism $\rho: A \to \mathrm{End}_A(F(X, Y))$ such that $\rho(a) \equiv aX \bmod(\text{degree } 2)$) and (b) are such that $[p]_F(X) \equiv uX^{p^n} \bmod(\text{degree } p^n + 1, \pi)$ with $u \in U(A)$ and $n = [K : \mathbf{Q}_p]$.

(ii) Let A_n be the ring of integers of the unramified extension of degree n of A and let A_{nr} be the ring of integers of K_{nr}. A slight extension of the argument of the proof of Proposition (8.3.22) then gives that $F(X, Y)$ and $G(X, Y)$ are strictly isomorphic over $\hat{A}_{nr}$ if and only if $\pi(F) = \pi(G)$ (and then they are strictly isomorphic over A) and that $F(X, Y)$ and $G(X, Y)$ are isomorphic over A_n (resp. A_{nr}, resp. $\hat{A}_{nr}$) if and only if there is a unit $u \in U(A_n)$ (resp. $U(A_{nr})$, resp. $U(\hat{A}_{nr})$) such that $u^{-1}\sigma(u) = \pi(F)^{-1}\pi(G)$.

(iii) Completeness of A is unnecessary for Section 8.1 through (8.3.6) and

(8.3.16)–(8.3.22). But completeness of A is used for (8.3.23)(i) and Proposition (8.3.8).

(iv) Proposition (8.3.22) also shows that there are very many nonisomorphic formal group laws over $\mathbf{Z}_p$; and since every formal group law over $\mathbf{Z}_p$ is strictly isomorphic over $\mathbf{Z}_p$ to a formal group law over $\mathbf{Z}$, we obtain (by varying p as well) a fair collection of nonisomorphic formal group laws over $\mathbf{Z}$.

CHAPTER II

METHODS FOR CONSTRUCTING HIGHER DIMENSIONAL FORMAL GROUP LAWS

9 Definitions and Elementary Properties. Survey of the Results of Chapter II

Most of the topics treated in Chapter I have higher dimensional analogues. In particular, there is a higher dimensional functional equation lemma, there are higher dimensional universal formal groups, and there are higher dimensional Honda and Lubin–Tate formal groups.

9.1 Definitions

An n-dimensional formal group law over a ring A is an n-tuple of power series $F(X, Y) = (F(1)(X, Y), \ldots, F(n)(X, Y))$ in $2n$ indeterminates $X_1, \ldots, X_n$; $Y_1, \ldots, Y_n$ such that

$$F(i)(X, Y) \equiv X_i + Y_i \mod(\text{degree } 2), \qquad i = 1, \ldots, n \tag{9.1.1}$$

$$F(i)(F(X, Y), Z) = F(i)(X, F(Y, Z)), \qquad i = 1, \ldots, n \tag{9.1.2}$$

and if one has in addition that

$$F(i)(X, Y) = F(i)(Y, X), \qquad i = 1, \ldots, n \tag{9.1.3}$$

then the group law is said to be commutative.

We shall usually write $F(X, Y)$ for the *column* vector with components $F(1)(X, Y), \ldots, F(n)(X, Y)$, and we shall write X and Y for the *column* vectors with components $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$. With these notations conditions (9.1.1)–(9.1.3) are written

$$F(X, Y) \equiv X + Y \mod(\text{degree } 2)$$

$$F(F(X, Y), Z) = F(F(Y, Z)), \qquad F(X, Y) = F(Y, X)$$

It is again an easy exercise to check that there is an n-tuple of power series $\iota(X)$ in $X_1, \ldots, X_n$ such that $F(X, \iota(X)) = 0$. (Or cf. Appendix (A.4.5).)

9.2 Examples

Some examples of n-dimensional formal group laws are

$$\hat{G}_a^n(X, Y) = X + Y \tag{9.2.1}$$

the n-dimensional additive formal group law, and the formal group law

$$\begin{aligned} F(1)(X, Y) &= X_1 + Y_1 + X_1 Y_1 + X_2 Y_3 \\ F(2)(X, Y) &= X_2 + Y_2 + X_1 Y_2 + X_2 Y_4 \\ F(3)(X, Y) &= X_3 + Y_3 + X_3 Y_1 + X_4 Y_3 \\ F(4)(X, Y) &= X_4 + Y_4 + X_3 Y_2 + X_4 Y_4 \end{aligned} \tag{9.2.2}$$

a set of formulas that becomes a good deal less mysterious if one observes that it results from calculating

$$\begin{bmatrix} 1 + X_{11} & X_{12} \\ X_{21} & 1 + X_{22} \end{bmatrix} \begin{bmatrix} 1 + Y_{11} & Y_{12} \\ Y_{21} & 1 + Y_{22} \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and writing X_1 for X_{11}, X_2 for X_{12}, X_3 for X_{21}, and X_4 for X_{22} and similarly for Y.

9.3 Formal group laws and formal groups. Curves

As in the one dimensional case (cf. 1.5) a formal group law can be seen as a recipe for manufacturing ordinary groups. More precisely, if B is an A-algebra and $\mathfrak{n}(B)$ is the ideal of nilpotent elements of B and $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ with $x_i, y_i \in \mathfrak{n}(B)$, $i = 1, \ldots, n$, then $F(x, y)$ is an n-tuple of elements in $\mathfrak{n}(B)$, and the addition $x +_F y = F(x, y)$ turns $\mathfrak{n}(B)^n$ into an ordinary group. This addition is compatible with the maps $\mathfrak{n}(B)^n \to \mathfrak{n}(C)^n$ induced by an A-algebra homomorphism $B \to C$; and thus the formal group law $F(X, Y)$ defines a functor F: $\mathbf{Alg}_A \to \mathbf{Group}$, which is called the formal group associated to $F(X, Y)$.

More generally, $F(x, y)$ has meaning for x_i, y_i topologically nilpotent, just as in Section 1.5 of Chapter I.

Define a *curve* $\gamma(t)$ in $F(X, Y)$ as an n-tuple of power series in one indeterminate t such that $\gamma(t) \equiv 0$ mod(degree 1). Then two curves can be added by the formula

$$\gamma_1(t) +_F \gamma_2(t) = F(\gamma_1(t), \gamma_2(t))$$

and this turns the set of all curves into a group which is denoted $\mathscr{C}(F)$.

9.4 Homomorphisms and isomorphisms

Let $F(X, Y)$ be an n-dimensional formal group law over a ring A and $G(X, Y)$ an m-dimensional formal group law over A. A *homomorphism over* A, $F(X, Y) \to G(X, Y)$ is an m-tuple of power series $\alpha(X)$ in n indeterminates such that $\alpha(X) \equiv 0$ mod(degree 1) and

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y)) \tag{9.4.1}$$

Just as in the one dimensional case there is a one-one correspondence between such m-tuples of power series $\alpha(X)$ and functor morphisms $F \to G$ between the corresponding formal groups. The homomorphism $\alpha(X)$ is an isomorphism if there exists a homomorphism $\beta(X)$: $G(X, Y) \to F(X, Y)$ such that $\alpha(\beta(X)) = X$, $\beta(\alpha(X)) = X$. This is equivalent to the condition that the induced morphism of functors $F \to G$ be an isomorphism. It is an easy exercise to show that $\alpha(X)$ is an isomorphism if and only if the Jacobian matrix $J(\alpha)$ of $\alpha(X)$ is invertible. Here $J(\alpha)$ is the matrix

$$J(\alpha) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

if $\alpha(1)(X) \equiv a_{11}X_1 + \cdots + a_{1n}X_n, \ldots, \alpha(m)(X) = a_{m1}X_1 + \cdots + a_{mn}X_n$ mod(degree 2). The morphism $\alpha(X)$ is said to be a *strict* isomorphism if $J(\alpha) = I_n$, the $n \times n$ identity matrix, i.e., if $\alpha(X) \equiv X$ mod(degree 2).

One defines the endomorphisms $[n]_F(X)$: $F(X, Y) \to F(X, Y)$ as in the one dimensional case, i.e.,

$$\begin{array}{llll} [1]_F(X) = X, & [n]_F(X) = F(X, [n-1]_F(X)) & \text{if} & n \geq 2 \\ [0]_F(X) = 0, & [n]_F(X) = \iota([-n]_F(X)) & \text{if} & n < 0 \end{array} \tag{9.4.2}$$

9.5 Change of rings and universal formal group laws

Let $F(X, Y)$ be a formal group law over a ring A and let ϕ: $A \to B$ be a homomorphism of rings. Then by applying ϕ to the coefficients of the power series $F(1)(X, Y), \ldots, F(n)(X, Y)$, one obtains a formal group law $\phi_* F(X, Y)$ over B.

An n-dimensional (commutative) formal group law $F(X, Y)$ over a ring L is said to be *universal* for n-dimensional (commutative) formal group laws if for every n-dimensional (commutative) formal group law $G(X, Y)$ over a ring A, there is a unique homomorphism of rings ϕ: $L \to A$ such that $G(X, Y) = \phi_* F(X, Y)$. It is, again, a trivial matter to show that universal formal group laws exist. For example, to obtain a universal n-dimensional commutative formal group law one proceeds as follows. If $\mathbf{k} = (k_1, \ldots, k_n)$, $k_j \in \mathbf{N} \cup \{0\}$, is a multi-index of length n, we use $|\mathbf{k}|$ to denote the sum $k_1 + \cdots + k_n$. Now take

indeterminates $C_{\mathbf{k},\mathbf{l}}(i)$ for all $i = 1, \ldots, n$ and multi-indices $\mathbf{k}, \mathbf{l}$ with $|\mathbf{k}| \geq 1$ and $|\mathbf{l}| \geq 1$. Let $L' = \mathbf{Z}[\ldots, C_{\mathbf{k},\mathbf{l}}(i), \ldots; i = 1, \ldots, n, |\mathbf{k}|, |\mathbf{l}| \geq 1]$ and let

$$F(i)(X, Y) = X_i + Y_i + \sum_{|\mathbf{k}|, |\mathbf{l}| \geq 1} C_{\mathbf{k},\mathbf{l}}(i) X^{\mathbf{k}} Y^{\mathbf{l}} \tag{9.5.1}$$

where $X^{\mathbf{k}}$ is short for $X_1^{k_1} \cdot \cdots \cdot X_n^{k_n}$, and $Y^{\mathbf{l}}$ is similarly defined.

We write

$$F(i)(F(X, Y), Z) - F(i)(X, F(Y, Z)) = \sum_{\mathbf{j},\mathbf{k},\mathbf{l}} P_{\mathbf{j},\mathbf{k},\mathbf{l},i}(C) X^{\mathbf{j}} Y^{\mathbf{k}} Z^{\mathbf{l}} \tag{9.5.2}$$

By the way, one easily checks that the polynomials $P_{\mathbf{j},\mathbf{k},\mathbf{l},i}(C)$ are of the form

$$C_{\mathbf{j}+\mathbf{k},\mathbf{l}}(i) \binom{\mathbf{j}+\mathbf{k}}{\mathbf{j}} - C_{\mathbf{j},\mathbf{k}+\mathbf{l}}(i) \binom{\mathbf{k}+\mathbf{l}}{\mathbf{l}} - Q_{\mathbf{j},\mathbf{k},\mathbf{l},i}(C) \tag{9.5.3}$$

where the $Q_{\mathbf{j},\mathbf{k},\mathbf{l},i}$ are polynomials in the $C_{\mathbf{s},\mathbf{t}}(m)$ with $|\mathbf{s} + \mathbf{t}| < |\mathbf{j} + \mathbf{k} + \mathbf{l}|$. Here $\mathbf{s} + \mathbf{t} = (s_1 + t_1, \ldots, s_n + t_n)$ and $\binom{\mathbf{k}}{\mathbf{l}} = \binom{k_1}{l_1} \cdots \binom{k_n}{l_n}$.

Now let $\mathfrak{A} \subset L'$ be the ideal generated by the polynomials $P_{\mathbf{j},\mathbf{k},\mathbf{l},i}$ and the polynomials $C_{\mathbf{s},\mathbf{t}}(i) - C_{\mathbf{t},\mathbf{s}}(i)$, and put $L = L'/\mathfrak{A}$, then $\pi_* F(X, Y)$ is a universal formal group over L where $\pi: L' \to L$ is the natural projection and $F(X, Y)$ is given by (9.5.1).

9.6 Infinite dimensional formal group laws

Let $(X_i)_{i \in I}$ be a set of indeterminates indexed by an arbitrary index set I. The formal power series ring $A[\![X_i, i \in I]\!]$ is now defined as the ring of all formal (infinite) sums $\sum c_{\mathbf{n}} X^{\mathbf{n}}$ where $\mathbf{n}$ runs through all functions $\mathbf{n}: I \to \mathbf{N} \cup \{0\}$ with finite support (i.e., for every $\mathbf{n}$ there are only finitely many $i \in I$ such that $\mathbf{n}(i) \neq 0$). Here $X^{\mathbf{n}}$ is short for $\prod_{i \in \operatorname{supp}(\mathbf{n})} X_i^{\mathbf{n}(i)}$, where $\operatorname{supp}(\mathbf{n}) = \{i \in I \mid \mathbf{n}(i) \neq 0\}$.

One can now consider elements $F(i)(X, Y) \in A[\![X_i, Y_i; i \in I]\!]$, and at first sight one could define an infinite dimensional formal group law as a set of power series $F(i)(X, Y) \in A[\![X_i, Y_i; i \in I]\!]$ indexed by I such that

$$F(i)(X, Y) \equiv X_i + Y_i \bmod(\text{degree } 2)$$

and such that

$$F(i)(X, F(Y, Z)) = F(i)(F(X, Y), Z) \qquad \text{for all } i \in I$$

However, for arbitrary sets of power series $F(i)(X, Y)$, $i \in I$, this second condition makes no sense because the calculation of the coefficient of a monomial $X^{\mathbf{l}} Y^{\mathbf{m}} Z^{\mathbf{n}}$ in $F(i)(X, F(Y, Z))$ or $F(i)(F(X, Y), Z)$ will in general involve infinite sums of elements of A.

The right definition is:

■ (9.6.1) **Definition** An (infinite) dimensional formal group law with (infinite) index set I over a ring A consists of elements $F(i)(X, Y) \in A[\![X_i, Y_i; i \in I]\!]$, one for each $i \in I$,

$$F(i)(X, Y) = \sum_{\mathbf{m},\mathbf{n}} c_{\mathbf{m},\mathbf{n}}(i) X^{\mathbf{m}} Y^{\mathbf{n}}$$

such that the following conditions are satisfied

(9.6.2) $\quad F(i)(X, Y) \equiv X_i + Y_i \mod(\text{degree } 2) \quad$ for all $i \in I$

(9.6.3) For every $\mathbf{m}$, $\mathbf{n}$ there are only finitely many $i \in I$ such that $c_{\mathbf{m},\mathbf{n}}(i) \neq 0$.

(9.6.4) $\quad F(i)(F(X, Y), Z) = F(i)(X, F(Y, Z)) \quad$ for all $i \in I$

Observe that condition (9.6.4) makes sense if condition (9.6.3) is satisfied. The formal group law is commutative if in addition

(9.6.5) $\quad F(i)(X, Y) = F(i)(Y, X) \quad$ for all $i \in I$

The condition (9.6.3) also fits in well with the functorial point of view; cf. 9.3 and [256, 64, 65].

■ (9.6.6) **Example** Let A be a ring. We consider the elements

$$1 + \sum_{i=1}^{\infty} X_i t^i, \qquad 1 + \sum_{i=1}^{\infty} Y_i t^i$$

in $A[X_i, Y_i; i \in I][\![t]\!]$. Multiplying these two formal power series in t we find a power series

(9.6.7) $$1 + \sum_{i=1}^{\infty} F(i)(X, Y) t^i$$

where $F(i)(X, Y)$ is a polynomial in $X_1, \ldots, X_i; Y_1, \ldots, Y_i$. We claim that the sequence of polynomials $F(i)(X, Y)$, $i \in \mathbf{N}$ constitutes an infinite dimensional commutative formal group law in the sense of Definition (9.6.1). This is most easily seen as follows. If we give each X_i and Y_i weight i (and t weight -1), then it follows immediately that $F(i)(X, Y)$ is homogeneous (or isobaric) of total weight i. It follows immediately from this that

$$c_{\mathbf{m},\mathbf{n}}(i) = 0 \quad \text{if} \quad i > \sum_{j \in \operatorname{supp}(\mathbf{m})} j\mathbf{m}(j) + \sum_{j \in \operatorname{supp}(\mathbf{n})} j\mathbf{n}(j)$$

so that condition (9.6.3) is satisfied. Conditions (9.6.4) and (9.6.5) are satisfied because multiplication of power series in t is associative and commutative, and condition (9.6.2) is immediate from the definition.

As we shall see later, this example has a lot to do with the rings of Witt vectors (for all primes simultaneously).

■ (9.6.8) **Remarks on "infinite dimensional universal formal group laws"** There cannot exist a universal formal group law (in the sense of (9.6.1)) for formal group laws with index set I if I is infinite because there is no predicting which finitely many $c_{\mathbf{m},\mathbf{n}}(i)$ will be nonzero. There does exist however a ring $\mathbf{Z}[\![U(i, \mathbf{n}); X_i, Y_i]\!]$ where $\mathbf{n}$ runs through all functions $I \to \mathbf{N} \cup \{0\}$ with finite support and $i \in I$ and there exists an I-vector $F_U(X, Y)$ of elements of $\mathbf{Z}[\![U; X; Y]\!]$ with the following properties

(9.6.9) for every monomial $U(i_1, \mathbf{n}_1)^{r_1} \cdots U(i_t, \mathbf{n}_t)^{r_t} X^{\mathbf{k}} Y^{\mathbf{l}}$ in U's, X's, and Y's, there are only finitely many $i \in I$ such that this monomial occurs with nonzero coefficient in the ith component of $F_U(X; Y)$.

$$\begin{aligned} &F_U(X, Y) \equiv X + Y \mod(\text{degree 2 in } X \text{ and } Y), \\ &F_U(X, Y) = F_U(Y, X) \end{aligned} \tag{9.6.10}$$

$$F_U(F_U(X, Y), Z)) = F_U(X, F_U(Y, Z)) \tag{9.6.11}$$

where we note that condition (9.6.11) makes sense again because of property (9.6.9). But $F(X, Y)$ is not a formal group law over $\mathbf{Z}[U]$ or even $\mathbf{Z}[\![U]\!]$ because it does not satisfy the "monomials in X and Y have finite support" condition (9.6.3).

However, the I-vector $F_U(X, Y)$ does yield many formal group laws as follows:

(9.6.12) For every $\mathbf{n}$, let $\kappa(\mathbf{n})$ be a finite subset of I. Now set $U(\mathbf{n}, i) = 0$ in $F(X, Y)$ for all $i \notin \kappa(\mathbf{n})$, all $\mathbf{n}$. The resulting I-vector $F_{U,\kappa}(X; Y)$ is a formal group law with index set I over $\mathbf{Z}[U(\mathbf{n}, i) \mid i \in \kappa(\mathbf{n})]$.

Moreover, the I-vector $F_U(X, Y)$ has the following universality property.

(9.6.13) For every formal group law $G(X, Y)$ with index set I over any ring A there exists a unique map $\phi: \{U(\mathbf{n}, i)\} \to A$ such that for every $\mathbf{n}$, $\phi(U(\mathbf{n}, i)) = 0$ for almost all i and such that $\phi_* F_U(X, Y) = G(X, Y)$. (Note that $\phi_* F(X, Y)$ makes sense because of (9.6.12).)

Now $F_U(X, Y)$ is defined as $f_U^{-1}(f_U(X) + f_U(Y))$ where $f_U(X)$ is an I-vector of elements in $\mathbf{Q}[\![U; X; Y]\!]$ which also satisfies (9.6.9).

In fact, running slightly ahead of our story, for each finite subset κ of I let

$$f_\kappa(X) \in \mathbf{Q}[U(\mathbf{n}, i) \mid \operatorname{supp}(\mathbf{n}) \subset \kappa, i \in \kappa]$$

be the finite dimensional universal formal group law with index set κ constructed in Section 11.1. Then $f_U(X)$ is the unique I-vector of elements of $\mathbf{Q}[\![U; X]\!]$ such that

$$f_U(X) \equiv f_\kappa(X) \mod(U(\mathbf{n}, i), \operatorname{supp}(\mathbf{n}) \cup \{i\} \not\subset \kappa; X_i, i \notin \kappa)$$

for all finite subsets $\kappa \subset I$.

This means in particular that all the formal group laws constructed as in (9.6.12) have logarithms, so that we obtain as consequences:

(9.6.14) Every formal group law $F(X, Y)$ with index set I can be lifted to characteristic zero.

(9.6.15) Every formal group law $F(X, Y)$ with index set I over a torsion free ring A has a unique logarithm.

Occasionally it is useful to observe that the formal group laws $F_{U,\kappa}(X, Y)$ of (9.6.12) are functional equation formal group laws in the sense that their logarithms satisfy certain obvious (cf. Section 11) functional equations.

Thus, though $F_U(X, Y)$ described above is not a universal formal group law with index set I, it is a very useful substitute. We shall not prove the results sketched above in the book, nor use them since our interests in this book are mainly finite dimensional (except for Witt vector type formal group laws; cf. Chapter III, Section 17; Chapter IV, Sections 25.1 and 25.2; and Chapter V). In fact, as far as applications are concerned, one dimensional formal group laws are (for the moment) by far the most important. The reader interested in the infinite dimensional constructions outlined above is referred to [184].

9.7 Survey of some of the results of Chapter II

We have seen that, e.g., a universal n-dimensional commutative formal group law exists. It is of course a totally different matter to determine the structure of the corresponding ring L. It is one of the main goals of this chapter to prove that L is isomorphic to the ring of polynomials in countably infinite indeterminates over $\mathbf{Z}$, and to exhibit an explicit example of a universal commutative formal group law over this ring. To do this we proceed exactly as in the one dimensional case; that is, we first do a multidimensional version of the functional equation lemma, then do a bit of higher dimensional binomial coefficient arithmetic, construct a candidate for a universal formal group law, and prove that it is actually universal. This is the subject matter of Sections 10, 11. In Section 12 we encounter a new phenomenon: curvilinear commutative formal group laws. In dimension 1 every formal group law is curvilinear, but that is not true in dimension > 1. Every commutative formal group law is strictly isomorphic to a curvilinear one, and curvilinear group laws are usually much easier to handle when doing calculations.

Then, in Section 13, we discuss the higher dimensional versions of the Honda formal group laws of Section 7 and the higher dimensional analogues of the Lubin–Tate formal group laws of Section 8. These are obtained as follows. Let A be a discrete valuation ring (to simplify things a bit) with residue field k of characteristic $p > 0$. Let π be a uniformizing element of A, let K be the quotient

field of A, and let $\sigma: K \to K$ be an endomorphism such that $\sigma(a) \equiv a^q \bmod \pi$ for all $a \in A$. Let B be any $n \times n$ matrix with coefficients in A. We define

$$g_B(X) = X + \pi^{-1} B\sigma_* g_B(X^q), \qquad G_B(X, Y) = g_B^{-1}(g_B(X) + g_B(Y))$$

Then $G_B(X, Y)$ is an n-dimensional formal group law over A, called a generalized Lubin–Tate formal group law. If k has q elements and we take $\sigma = id$, then $g_B^{-1}(ag_B(X)) = [a](X)$ has its coefficients in A for all $a \in A$, so that we find endomorphisms $[a](X)$ of $G_B(X, Y)$ for all $a \in A$.

As a by-product of the construction of a universal higher dimensional commutative formal group in Section 11 we obtain the "**Q**-theorem," that over a **Q**-algebra every commutative n-dimensional formal group law is strictly isomorphic to the n-dimensional additive formal group law $\hat{\mathbf{G}}_a^n$. But what about the noncommutative ones? In dimension 1 there are hardly any noncommutative formal group laws. But that is definitely not true in dimension > 1 as is suggested, e.g., by Example (9.2.2). Let $F(X, Y)$ be an n-dimensional formal group law over A. We write

$$F(X, Y) \equiv X + Y + B(X, Y) \quad \text{mod(degree 3)} \tag{9.7.1}$$

then $B(X, Y)$ is an n-tuple of quadratic polynomials in the $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ of the form

$$B(i)(X, Y) = \sum_{j,k=1}^{n} \gamma_{jk}^i X_j Y_k \tag{9.7.2}$$

We now define a Lie algebra structure on A^n by means of the formula

$$[e_j, e_k] = \sum_{i=1}^{n} \gamma_{jk}^i e_i - \sum_{i=1}^{n} \gamma_{kj}^i e_i \tag{9.7.3}$$

where e_i is the canonical ith basis vector of A^n.

This Lie algebra is called the Lie algebra of the formal group law $F(X, Y)$ and is denoted $L(F)$.

This construction is functorial. One easily checks that if $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is a morphism of formal group laws, then $J(\alpha)$: $A^n \to A^m$ induces a homomorphism of Lie algebras $J(\alpha)$: $L(F) \to L(G)$.

In Section 14 we shall show that the functor L from formal group laws over A to Lie algebras over A that are free as A-modules is an equivalence of categories if A is a **Q**-algebra. This means in particular that given a Lie algebra L over, e.g., **R**, there is a formal group law $F(X, Y)$ over **R** such that $L(F) = L$. One can then show that $F(X, Y)$ converges for X, Y small enough, so that we actually obtain a neighborhood of the identity of an analytic Lie group with the given Lie algebra as Lie algebra. This gives a method of proving Lie's theorem, and in fact formal group laws were defined in 1946 by Bochner with exactly this purpose in mind; cf. [40].

10 The Higher Dimensional Functional Equation Lemma

In this section we discuss the higher dimensional analogues of Sections 2 and 3.

10.1 Ingredients and constructions

The basic ingredients for the constructions of the n-dimensional functional equation lemma are practically the same as in the one dimensional case, viz.,

$$(10.1.1) \qquad A \subset K, \qquad \sigma: K \to K, \qquad \mathfrak{A} \subset A, \qquad p, \quad q, \quad s_1, \quad s_2, \ldots$$

where A, K, σ, p, q are as in the one dimensional case, i.e., A is a subring of a ring K, σ is an endomorphism of K, $\mathfrak{A}$ is an ideal of A, p is a prime number, and q is a power of p. But the $s_1, s_2, \ldots$ are now supposed to be $n \times n$ matrices with coefficients in K, $s_1 = (s_1(i, j))$, $s_2 = (s_2(i, j))$, ... The conditions that these ingredients have to satisfy are the obvious analogues of (2.1.2)–(2.1.4), viz. $\sigma(a) \equiv a^q \bmod \mathfrak{A}$ for all $a \in A$, $s_k(i, j)\mathfrak{A} \subset A$ for all $k = 1, 2, \ldots; i, j = 1, \ldots, n$, and (2.1.4) (or $\sigma^l(s_k(i, j))\mathfrak{A} \subset A$ for all l, k, i, j; cf. Remark (2.4.15)).

Now let $g(X)$ be an n-tuple of power series in $X_1, \ldots, X_m$ with coefficients in A without constant terms. Then given the ingredients (10.1.1) we construct a new n-tuple of power series by means of the recursion formula (or functional equation)

$$(10.1.2) \qquad f_g(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i f_g(X^{q^i})$$

where $\sigma_*^i f_g(X)$ is the n-tuple of power series obtained from $f_g(X)$ by applying the endomorphism σ^i to the coefficients of the n-tuple of power series $f_g(X)$, and where X^{q^i} is short for $(X_1^{q^i}, \ldots, X_m^{q^i})$. In (10.1.2) $f_g(X)$ and $g(X)$ are taken to be column vectors and the s_i are matrices, so that (10.1.2) makes sense.

As in the one dimensional case, we note that (10.1.2) is really a recursion equation for the coefficients of the n-tuple of power series $f_g(X)$.

If $f(X)$ is an n-tuple of power series without constant terms over A such that the Jacobian matrix $J(f)$ is invertible (cf. 9.4 for the definition of $J(f)$), then there is a unique n-tuple of power series $f^{-1}(X)$ such that $f(f^{-1}(X)) = f^{-1}(f(X)) = X$. (Cf. Appendix (A.4.5).)

The n-dimensional functional equation lemma can now be stated as follows.

10.2 Functional equation lemma

Let A, K, $\mathfrak{A}$, σ, p, q, s_1, s_2, ... be as in 10.1. Let $g(X)$ and $\bar{g}(\bar{X})$ be two n-tuples of power series in $X = (X_1, \ldots, X_n)$ and $\bar{X} = (\bar{X}_1, \ldots, \bar{X}_m)$, respectively, with coefficients in A such that $g(X) \equiv 0 \bmod(\text{degree } 1)$, $\bar{g}(\bar{X}) \equiv 0 \bmod(\text{degree } 1)$. Suppose moreover that the Jacobian matrix $J(g)$ is invertible. Then we have

(i) the n-tuple of power series $F_g(X, Y) = f_g^{-1}(f_g(X) + f_g(Y))$ in $X_1, \ldots, X_n; Y_1, \ldots, Y_n$ has its coefficients in A;

(ii) the n-tuple of power series $f_g^{-1}(f_{\bar{g}}(\bar{X}))$ in $\bar{X}_1, \ldots, \bar{X}_m$ has its coefficients in A;

(iii) if $h(\bar{X})$ is any n-tuple of power series in $\bar{X}_1, \ldots, \bar{X}_m$ over A such that $h(\bar{X}) \equiv 0 \mod(\text{degree } 1)$, then there is an n-tuple of power series $\bar{h}(\bar{X})$ in $\bar{X}_1, \ldots, \bar{X}_m$ such that $f_g(h(\bar{X})) = f_{\bar{h}}(\bar{X})$;

(iv) if $\alpha(\hat{X})$, $\beta(\hat{X})$ are n-tuples of power series in $\hat{X}_1, \ldots, \hat{X}_l$ with coefficients in A and K, respectively, then for all $r = 1, 2, 3, \ldots$

$$\alpha(\hat{X}) \equiv \beta(\hat{X}) \mod \mathfrak{a}^r \quad \Leftrightarrow \quad f_g(\alpha(\hat{X})) \equiv f_g(\beta(\hat{X})) \mod \mathfrak{a}^r$$

The proof of this lemma is virtually identical with the proof of the corresponding one dimensional version; cf. Chapter I, Section 2.4. The various formulas are the same, but the symbols occurring in them must now be interpreted as matrices and vectors.

10.3 The higher dimensional formal group laws $F_V(X, Y)$, $F_{V,T}(X, Y)$

We apply the functional equation lemma 10.2 to obtain the higher dimensional analogues of the one dimensional formal group laws $F_V(X, Y)$, $F_{V,T}(X, Y)$ which we constructed in 2.3 and studied in more detail in Section 3 of Chapter I.

Choose $n \in \mathbf{N}$ and let $\mathbf{Z}[V]$ be short for $\mathbf{Z}[V_i(j, k); i = 1, 2, \ldots; j, k = 1, \ldots, n]$ and let $\mathbf{Z}[V, T]$ be short for $\mathbf{Z}[V_i(j, k), T_i(j, k); i = 1, 2, \ldots; j, k = 1, \ldots, n]$. We write V_i for the $n \times n$ matrix $(V_i(j, k))$, T_i for the $n \times n$ matrix $(T_i(j, k))$, X for the column vector $(X_1, \ldots, X_n)$ and X^m for the column vector $(X_1^m, \ldots, X_n^m)$. Choose a prime number p. We are now going to apply the functional equation lemma 10.2 with the ingredients: $A = \mathbf{Z}[V]$ or $\mathbf{Z}[V, T]$, $K = \mathbf{Q}[V]$ or $\mathbf{Q}[V, T]$, $\mathfrak{a} = pA$, $q = p$, $s_i = p^{-1}V_i$, $i = 1, 2, \ldots$, σ: $K \to K$ the homomorphism defined by

$$\sigma(V_i(j, k)) = V_i(j, k)^p, \qquad \sigma(T_i(j, k)) = T_i(j, k)^p$$

$$g(X) = X, \qquad \bar{g}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i}$$

As usual, for this type of endomorphism σ we shall write $a^{(p)}$ for $\sigma^* a$, $a \in K$ and $h^{(p)}(X)$ for $\sigma_* h(X)$. If $h(X)$ is a vector or matrix of power series, then $\sigma_* h(X) = h^{(p)}(X)$ is the vector or matrix obtained by applying σ_* to all the entries of $h(X)$. Thus $V_i^{(p)}$ denotes the matrix with entries $V_i(j, k)^p$. We shall write $f_V(X)$ and

$f_{V,T}(X)$ for the n-tuples of power series defined à la (10.1.2) by means of the ingredients listed above. Thus

$$f_V(X) = X + \sum_{i=1}^{\infty} p^{-1} V_i f_V^{(p^i)}(X^{p^i}) \tag{10.3.1}$$

$$f_{V,T}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i} + \sum_{i=1}^{\infty} p^{-1} V_i f_{V,T}^{(p^i)}(X^{p^i}) \tag{10.3.2}$$

Let

$$F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y)) \tag{10.3.3}$$

$$F_{V,T}(X, Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y))$$

$$\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X)) \tag{10.3.4}$$

Then the functional equation lemma says:

■ (10.3.5) **Theorem** $F_V(X, Y)$ and $F_{V,T}(X, Y)$ are n-dimensional formal group laws over $\mathbf{Z}[V]$ and $\mathbf{Z}[V, T]$, respectively, and $\alpha_{V,T}(X)$ is a strict isomorphism over $\mathbf{Z}[V, T]$ from $F_V(X, Y)$ to $F_{V,T}(X, Y)$.

Later, in Chapter III, we shall see that $F_V(X, Y)$ is universal for a certain kind of formal group law, viz. the p-typical ones, and that the isomorphism $\alpha_{V,T}(X)$ is in a certain sense the most general isomorphism possible between p-typical formal group laws.

10.4 Some more results on $F_V(X, Y)$ and $F_{V,T}(X, Y)$

It is immediately clear from the defining formulas (10.3.1), (10.3.2) that $f_V(X)$ and $f_{V,T}(X)$ are of the form

$$f_V(X) = \sum_{i=0}^{\infty} a_i(V) X^{p^i}, \qquad a_0(V) = I_n, \text{ the } n \times n \text{ identity matrix} \tag{10.4.1}$$

$$f_{V,T}(X) = \sum_{i=0}^{\infty} a_i(V, T) X^{p^i}, \quad a_0(V, T) = I_n \tag{10.4.2}$$

where the $a_i(V)$, $a_i(V, T)$ are certain $n \times n$ matrices with coefficients in $\mathbf{Q}[V]$, $\mathbf{Q}[V, T]$. The following formulas are now proved exactly as in the one dimensional case; cf. Section 3.3 of Chapter I:

$$a_m(V) = p^{-1} V_1 a_{m-1}(V)^{(p)} + \cdots + p^{-1} V_{m-1} a_1(V)^{(p^{m-1})} + p^{-1} V_m \tag{10.4.3}$$

$$a_m(V) = \sum_{i_1 + \cdots + i_r = m} p^{-r} V_{i_1} V_{i_2}^{(p^{i_1})} \cdots V_{i_r}^{(p^{i_1 + \cdots + i_{r-1}})} \tag{10.4.4}$$

where the sum is over all sequences $(i_1, \ldots, i_r)$, $i_1, \ldots, i_r$, $r \in \mathbf{N}$ such that $i_1 + \cdots + i_r = m$,

$$(10.4.5) \qquad pa_m(V) = a_{m-1}(V)V_1^{(p^{m-1})} + \cdots + a_1(V)V_{m-1}^{(p)} + V_m$$

$$(10.4.6) \qquad a_m(V, T) = a_m(V) + a_{m-1}(V)T_1^{(p^{m-1})} + \cdots + a_1(V)T_{m-1}^{(p)} + T_m$$

Note that these formulas specialize to the ones given in 3.3, Chapter I ((3.3.6), (3.3.8)–(3.3.10)) if $n = 1$. We stress that $V_i^{(p^r)}$ is the matrix with entries $V_i(j, k)^{p^r}$ and not the matrix power $(V_i)^{p^r}$; but, e.g., $a_1(V)V_{m-1}^{(p)}$ is the matrix product of the matrices $a_1(V)$ and $V_{m-1}^{(p)}$.

The formulas given above will be useful in Chapter IV when we shall take up the study of isomorphisms of (higher dimensional) formal group laws.

10.5 An example (the formal group law of Witt vectors of length n associated to the prime number p)

Let $\phi\colon \mathbf{Z}[V] \to \mathbf{Z}$ be the ring homomorphism defined by the conditions $\phi(V_2) = \phi(V_3) = \cdots = 0$ and

$$\phi(V_1) = \begin{pmatrix} 0 & \cdots & 0 \\ 1 & & \\ 0 & \ddots & \vdots \\ \vdots & \ddots & \\ 0 & \cdots\ 0\ 1\ 0 & \end{pmatrix} = M$$

Using (10.4.5) we see that

$$a_1 = p^{-1}M, \quad a_2 = p^{-2}M^2, \quad \cdots, \quad a_{n-1} = p^{-n+1}M^{n-1}$$

$$a_n = a_{n+1} = \cdots = 0$$

Let $\hat{W}_{p^n}(X, Y)$ denote the n-dimensional formal group law $\phi_* F_V(X, Y)$ over $\mathbf{Z}$. Its logarithm is then equal to

$$(10.5.1) \qquad \log_{\hat{W}_{p^n}}(X_1, \ldots, X_n) = \begin{pmatrix} X_1 \\ X_2 + p^{-1}X_1^p \\ \vdots \\ X_n + p^{-1}X_{n-1}^p + \cdots + p^{-n+1}X_1^{p^{n-1}} \end{pmatrix}$$

Now the first n addition polynomials of the ring of Witt vectors associated to the prime p are given by the formulas

$$(10.5.2) \qquad w_{p,i}(S_0(\bar{X}, \bar{Y}), \ldots, S_i(\bar{X}, \bar{Y})) = w_{p,i}(\bar{X}) + w_{p,i}(\bar{Y}) \qquad i = 0, \ldots, n-1$$

where $w_{p,i}(Z_0, \ldots, Z_i) = Z_0^{p^i} + pZ_1^{p^{i-1}} + \cdots + p^i Z_i$, $i = 0, 1, \ldots, n-1$, and $\bar{X}$, $\bar{Y}$ are short for $(\bar{X}_0, \ldots, \bar{X}_{n-1})$, $(\bar{Y}_0, \ldots, \bar{Y}_{n-1})$. Multiplying (10.5.2) with p^{-i} on both sides and substituting X_i for $\bar{X}_{i-1}$, Y_i for $\bar{Y}_{i-1}$, $i = 1, \ldots, n$, we see that

the $\hat{W}_{p^n}(i)(X, Y)$ are in fact the first n addition polynomials of the ring of Witt vectors associated to the prime p.

11 The Universal n-Dimensional Commutative Formal Group Laws $H_U(X, Y)$

In this section we construct a universal commutative n-dimensional formal group law $H_U(X, Y)$ for each $m \in \mathbf{N}$. All formal group laws in this section will be commutative.

11.1 The constructions

For each sequence $(q_1, \ldots, q_t)$, $t \in \mathbf{N}$, of powers of prime numbers, $q_i = p_i^{s_i}$, $s_i \in \mathbf{N}$, p_i a prime number, choose an integer $n(q_1, \ldots, q_t)$ such that the following congruences are satisfied

(11.1.1)

$$n(q_1, \ldots, q_t) \equiv 1 \mod p_1^r \quad \text{if } p_1 = p_2 = \cdots = p_r \neq p_{r+1}, \quad 1 \leq r \leq t$$

$$n(q_1, \ldots, q_t) \equiv 0 \mod p_2^{r-1} \quad \text{if } p_1 \neq p_2 = \cdots = p_r \neq p_{r+1}, \quad 2 \leq r \leq t$$

(If $r = t$, then the condition $p_r \neq p_{r+1}$ is supposed to be vacuously satisfied.)

These are precisely the same conditions as those in (5.2.1) which we used to construct a one dimensional universal formal group law in 5.2. The only difference is that we now consider only sequences of prime powers.

■ (11.1.2) **Some notation** Fix $m \in \mathbf{N}$; m is the dimension of the formal group law $F_U(X, Y)$ that we are going to construct. We use a boldface letter $\mathbf{n}$ to denote a multi-index $\mathbf{n} = (n_1, \ldots, n_m)$, $n_i \in \mathbf{N} \cup \{0\}$. We set $\mathbf{0} = (0, 0, \ldots, 0)$, $\mathbf{e}(i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the ith place. If $\mathbf{n}$ is a multi-index and $i \in \mathbf{N} \cup \{0\}$, then $i\mathbf{n}$ is the multi-index $(in_1, \ldots, in_m)$; and if $\mathbf{k}$, $\mathbf{l}$ are two multi-indices, then $\mathbf{k} + \mathbf{l}$ denotes the multi-index $(k_1 + l_1, \ldots, k_m + l_m)$. The symbol $\mathbf{I}$ denotes the set of all multi-indices $\mathbf{n}$; i.e., $\mathbf{I} = \{(n_1, \ldots, n_m) \mid n_1, \ldots, n_m \in \mathbf{N} \cup \{0\}\}$; for $\mathbf{n} \in \mathbf{I}$, $|\mathbf{n}|$ denotes the number $|\mathbf{n}| = n_1 + \cdots + n_m$. Finally, we define $\mathbf{D} \subset \mathbf{I}$ as the set of all multi-indices $\mathbf{n} \in \mathbf{I}$ for which $|\mathbf{n}| \geq 1$ and such that $\mathbf{n} \neq p^r\mathbf{e}(i)$ for all prime numbers $p, r \in \mathbf{N}$, $i = 1, \ldots, m$. Note that the indices $\mathbf{e}(i)$ themselves, $i = 1, \ldots, m$, are in $\mathbf{D}$.

We write X for $(X_1, \ldots, X_m)$; and if $\mathbf{n} \in \mathbf{I}$, then $X^{\mathbf{n}}$ is short for $X_1^{n_1} \cdots X_m^{n_m}$. This is not to be confused with X^n, which denotes the vector $(X_1^n, \ldots, X_m^n)$. If $a = (a_1, \ldots, a_m)$ is a vector, then $aX^{\mathbf{n}}$ is of course the vector $(a_1 X^{\mathbf{n}}, \ldots, a_m X^{\mathbf{n}})$.

Let $\mathbf{Z}[U]$ be short for $\mathbf{Z}[U(i, \mathbf{n})$; $\mathbf{n} \in \mathbf{I}$ and $|\mathbf{n}| \geq 2$, $i = 1, \ldots, m]$. We also define $U(i, \mathbf{e}(j)) = 0$ if $i \neq j$ and $U(i, \mathbf{e}(i)) = 1$, $i, j = 1, \ldots, m$. If $q = p^s$, $s \in \mathbf{N} \cup \{0\}$, p a prime number, then we use U_q to denote the $m \times m$ matrix $(U(i, q\mathbf{e}(j))_{i,j}$; and if $\mathbf{d} \in \mathbf{I} \backslash \{\mathbf{0}\}$, we use $U_{\mathbf{d}}$ to denote the column vector $(U(1, \mathbf{d}), \ldots, U(m, \mathbf{d}))$.

Using all this notation we now define for each $\mathbf{n} \in \mathbf{I}$, $|\mathbf{n}| \geq 1$ a column vector $a_{\mathbf{n}}$ with coordinates in $\mathbf{Q}[U] = \mathbf{Q} \otimes \mathbf{Z}[U]$ by means of the formula

$$(11.1.3) \qquad a_{\mathbf{n}} = \sum_{(q_1, \ldots, q_t, \mathbf{d})} \frac{n(q_1, \ldots, q_t)}{p_1} \cdot \ldots \cdot \frac{n(q_{t-1}, q_t)}{p_{t-1}} \frac{n(q_t)}{p_t} U_{q_1} U_{q_2}^{(q_1)} \ldots U_{q_t}^{(q_1 \cdots q_{t-1})} U_{\mathbf{d}}^{(q_1 \cdots q_t)}$$

where the sum is over all sequences $(q_1, \ldots, q_t, \mathbf{d})$, $t \in \mathbf{N} \cup \{0\}$, $q_i = p_i^{s_i}$, $s_i \in \mathbf{N}$, p_i a prime number, $\mathbf{d} \in \mathbf{D}$ such that $q_1 \cdots q_t \mathbf{d} = \mathbf{n}$. Here, as usual, if M is a matrix or vector with coefficients in $\mathbf{Q}[U]$, then $M^{(r)}$ is the matrix of vector obtained from M by applying the endomorphism $U(i, \mathbf{d}) \mapsto U(i, \mathbf{d})^r$ to the entries of M. If $M = U_q$ or $U_{\mathbf{d}}$, this is the same as raising each of the entries of M to the rth power.

We now define

$$(11.1.4) \qquad h_U(X) = \sum_{|\mathbf{n}| \geq 1} a_{\mathbf{n}} X^{\mathbf{n}}, \qquad H_U(X, Y) = h_U^{-1}(h_U(X) + h_U(Y))$$

(Note that $a_{\mathbf{e}(i)}$ is the column vector $(0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the ith place, so that $h_U(X) \equiv X$ mod(degree 2) so that $h_U^{-1}(X)$ is well defined.)

■ (11.1.5) **Theorem** $H_U(X, Y)$ is a power series with coefficients in $\mathbf{Z}[U]$ and it is in fact a universal commutative m-dimensional formal group law over $\mathbf{Z}[U]$.

■ (11.1.6) **Corollary** (Q-theorem) If $F(X, Y)$ is an m-dimensional commutative formal group law over a $\mathbf{Q}$-algebra A, then there is a unique strict isomorphism $\alpha(X)$: $F(X, Y) \to \hat{\mathbf{G}}_{\mathrm{a}}^m$.

This isomorphism $\alpha(X)$ is denoted $\log_F(X)$ and is called the logarithm of $F(X, Y)$. More generally, if $F(X, Y)$ is an m-dimensional commutative formal group law over a characteristic zero ring A, then we use $\log_F(X)$ to denote the unique m-tuple of power series $f(X)$ with coefficients in $A \otimes \mathbf{Q}$ such that $F(X, Y) = f^{-1}(f(X) + f(Y))$ and $f(X) \equiv X$ mod(degree 2).

As in the one dimensional case we have a formula

$$(11.1.7) \qquad \log_F(X) = \lim_{n \to \infty} p^{-n}[p^n]_F(X)$$

for $F(X, Y)$ a commutative formal group law over a characteristic zero $\mathbf{Z}_{(p)}$-algebra A such that $\bigcap_n p^n A = \{0\}$. The proof is virtually the same as in the one dimensional case; cf. Proposition (5.4.5) of Chapter I. Remark (5.4.8) also generalizes to the more dimensional case.

■ (11.1.8) **Remark** If $m = 1$ then $H_U(X, Y)$ does not coincide with the one dimensional universal formal group law $F_U(X, Y)$ which we constructed in Section 5 of Chapter I. Cf., however, also Section 12 below.

11.2 Proof of the integrality of $H_U(X, Y)$

Let $(q_1, \ldots, q_t)$ be a sequence of powers of prime numbers. We define

$$d(q_1, \ldots, q_t) = \frac{n(q_1, \ldots, q_t)}{p_1} \cdot \ldots \cdot \frac{n(q_{t-1}, q_t)}{p_{t-1}} \cdot \frac{n(q_t)}{p_t} \tag{11.2.1}$$

where $q_i = p_i^{s_i}$, p_i a prime number, $s_i \in \mathbf{N}$. Then one has

$$d(q_1, \ldots, q_t) - p_1^{-1} d(q_2, \ldots, q_t) \in \mathbf{Z}_{(p_1)} \tag{11.2.2}$$

and

$$d(q_1, q_2, \ldots, q_t) \in \mathbf{Z}_{(p)} \quad \text{for all prime numbers } p \neq p_1. \tag{11.2.3}$$

Statements (11.2.2) and (11.2.3) are just special cases of lemmas (5.3.5) and (5.3.4), respectively. The next step is:

■ (11.2.4) **Lemma** The n-tuple of power series $h_U(X, Y)$ satisfies a functional equation of the form

$$h_U(X) = g_p(X) + \sum_{i=1}^{\infty} p^{-1} U_{p^i} h_U^{(p^i)}(X^{p^i})$$

with $g_p(X) \in \mathbf{Z}_{(p)}[U][\![X]\!]^m$ and $g_p(X) \equiv X$ mod(degree 2) for every prime number p.

Proof This is proved in almost exactly the same way as we proved Lemma (5.3.3) in (5.3.6). Choose a prime number p. Let $\mathbf{n} = p^r\mathbf{k}$ where $\mathbf{k} = (k_1, \ldots, k_m)$ is such that at least one of the k_i is prime to p. Now write $a_{\mathbf{n}}$ as a sum

$$a_{\mathbf{n}} = a_{\mathbf{n}}(0) + a_{\mathbf{n}}(1) + \cdots + a_{\mathbf{n}}(r) \tag{11.2.5}$$

where $a_{\mathbf{n}}(0)$ is the sum over all terms in the right-hand side of (11.1.3) for which $(q_1, p) = 1$ and where $a_{\mathbf{n}}(j)$ is the sum over all terms in the right-hand side of (11.1.3) for which $q_1 = p^j$. It now follows from (11.2.3) and (11.2.2) that

$$a_{\mathbf{n}}(0) \in \mathbf{Z}_{(p)}[U][\![X]\!]^m \tag{11.2.6}$$

$$a_{\mathbf{n}}(j) - p^{-1} U_{p^j} a_{p^{-j}\mathbf{n}}^{(p^j)} \in \mathbf{Z}_{(p)}[U][\![X]\!]^m, \qquad j = 1, \ldots, r$$

Formulas (11.2.5) and (11.2.6) together prove Lemma (11.2.4).

■ (11.2.7) By the functional equation lemma 10.2 we see from Lemma (11.2.4) that the coefficients of the n-tuple of power series $H_U(X, Y)$ are in $\mathbf{Z}_{(p)}[U]$ for every prime number p, which means that all those coefficients are in $\mathbf{Z}[U]$. This concludes the proof of the integrality of $H_U(X, Y)$.

11.3 Some multidimensional binomial coefficient arithmetic

In order to prove the universality of $H_U(X, Y)$ we first do the higher dimensional version of the binomial coefficient arithmetic of Section 4 of Chapter I.

■(11.3.1) Let $\mathbf{n}$ be a multi-index of length m. We write $\mathbf{k} \leq \mathbf{n}$ if $k_i \leq n_i$ for all $i = 1, 2, \ldots, m$, and $\mathbf{k} < \mathbf{n}$ if $\mathbf{k} \leq \mathbf{n}$ and $|\mathbf{k}| < |\mathbf{n}|$. If $\mathbf{k} \leq \mathbf{n}$, we define

$$\binom{\mathbf{n}}{\mathbf{k}} = \binom{n_1}{k_1} \cdots \binom{n_m}{k_m} \tag{11.3.2}$$

$$v(\mathbf{n}) = \begin{cases} p & \text{if } n = p^r \mathbf{e}(i) \text{ for some prime number } p,\ r \in \mathbf{N},\ i \in \{1, \ldots, m\} \\ 1 & \text{otherwise} \end{cases}$$

(11.3.3)

Then one has for $|\mathbf{n}| \geq 2$

$$v(\mathbf{n}) = \gcd\left\{\binom{\mathbf{n}}{\mathbf{k}} \mid 0 < \mathbf{k} < \mathbf{n}\right\} \tag{11.3.4}$$

This is clear from the corresponding one dimensional situation if $\mathbf{n}$ is of the form $\mathbf{n} = n\mathbf{e}(j)$ for some $n \in \mathbf{N}, j \in \{1, \ldots, m\}$ (cf. 4.1); and if $\mathbf{n} = (n_1, n_2, \ldots, n_m)$ has at least two $n_i \neq 0$, let i_1 be the smallest number such that $n_{i_1} \neq 0$, take $\mathbf{k} = n_{i_1}\mathbf{e}(i_1)$, then $\binom{\mathbf{n}}{\mathbf{k}} = 1$.

■(11.3.5) For each $n \in \mathbf{N}$, $n \geq 2$ choose integers $\lambda_{n,1}, \ldots, \lambda_{n,n-1}$ such that $\lambda_{n,1}\binom{n}{1} + \cdots + \lambda_{n,n-1}\binom{n}{n-1} = v(n)$. Now let $\mathbf{n}$ be a multi-index. If $\mathbf{n}$ is of the form $n = n\mathbf{e}(j)$ and $\mathbf{k} < \mathbf{n}$, then $\mathbf{k} = k\mathbf{e}(j)$ for some $k < n$. In this case we define $\lambda(\mathbf{n}, \mathbf{k}) = \lambda_{n,k}$. If $\mathbf{n}$ is not of the form $n\mathbf{e}(j)$, let i_1 be the smallest index such that $n_{i_1} \neq 0$. Let $\mathbf{k} \leq \mathbf{n}$. For these $\mathbf{n}$, we set $\lambda(\mathbf{n}, \mathbf{k}) = 1$ if $\mathbf{k} = n_{i_1}\mathbf{e}(i_1)$ and $\lambda(\mathbf{n}, \mathbf{k}) = 0$ if $\mathbf{k} \neq n_{i_1}\mathbf{e}(i_1)$. We then have of course that

$$\sum_{0 < \mathbf{k} < \mathbf{n}} \lambda(\mathbf{n}, \mathbf{k}) \binom{\mathbf{n}}{\mathbf{k}} = v(\mathbf{n}) \tag{11.3.6}$$

■(11.3.7) **Lemma** Let $\mathbf{n}$ be a multi-index, $|\mathbf{n}| \geq 2$. For each $0 < \mathbf{k} < \mathbf{n}$ let $X(\mathbf{k})$ be an indeterminate and let $X(\mathbf{k}) = X(\mathbf{n} - \mathbf{k})$. Then every $X(\mathbf{k})$ can be written as a linear expression with coefficients in $\mathbf{Z}$ of the expressions

$$\sum_{0 < \mathbf{k} < \mathbf{n}} \lambda(\mathbf{n}, \mathbf{k}) X(\mathbf{k}) \tag{11.3.8}$$

$$\binom{\mathbf{j} + \mathbf{k}}{\mathbf{k}} X(\mathbf{j} + \mathbf{k}) - \binom{\mathbf{k} + \mathbf{l}}{\mathbf{l}} X(\mathbf{k} + \mathbf{l}), \qquad \mathbf{j} + \mathbf{k} + \mathbf{l} = \mathbf{n},\ \mathbf{j}, \mathbf{k}, \mathbf{l} > \mathbf{0}. \tag{11.3.9}$$

where the $\lambda(\mathbf{n}, \mathbf{k})$ are as above in (11.3.5).

Proof If $\mathbf{n}$ is of the form $\mathbf{n} = n\mathbf{e}(j)$, this is the binomial coefficient lemma 4.2. If $\mathbf{n}$ is not of the form $\mathbf{n} = n\mathbf{e}(j)$, let i be the smallest index such that $n_i \neq 0$. Then (11.3.8) is equal to $X(n_i\mathbf{e}(i))$. For all $0 < j < n_i$, take $\mathbf{j} = j\mathbf{e}(i)$, $\mathbf{k} = (n_i - j)\mathbf{e}(i)$, $\mathbf{l} = \mathbf{n} - \mathbf{j} - \mathbf{k}$. Then $X(\mathbf{j} + \mathbf{k}) = X(n_i\mathbf{e}(i))$, $X(\mathbf{k} + \mathbf{l}) = X(\mathbf{j}) = X(j\mathbf{e}(i))$, and $\binom{\mathbf{k}+\mathbf{l}}{\mathbf{l}} = 1$, so that we have obtained all $X(\mathbf{k})$ with $\mathbf{k} = j\mathbf{e}(i)$, $0 < j \leq n_i$ as a linear combination of (11.3.8) and (11.3.9). Now let

$\mathbf{r} = (r_1, \ldots, r_m)$, $\mathbf{r} \neq re(i)$ be a multi-index with $\mathbf{0} < \mathbf{r} < \mathbf{n}$ and $0 < r_i \leq n_i$. We take $\mathbf{j} = r_i\mathbf{e}(i)$, $\mathbf{k} = \mathbf{r} - \mathbf{j}$, $\mathbf{l} = \mathbf{n} - \mathbf{j} - \mathbf{k}$. Then $\binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} = 1$, $X(\mathbf{j} + \mathbf{k}) = X(\mathbf{r})$, $X(\mathbf{k} + \mathbf{l}) = X(\mathbf{j}) = X(r_i\mathbf{e}(i))$, so that we have also obtained all $X(\mathbf{r})$ with $\mathbf{r}$ as described above as linear combinations of (11.3.8) and (11.3.9). But if $\mathbf{r} < \mathbf{n}$ and $\mathbf{r} \neq re(i)$, then either $\mathbf{r}$ of $\mathbf{n} - \mathbf{r}$ has its ith component > 0 and $X(\mathbf{r}) = X(\mathbf{n} - \mathbf{r})$. This concludes the proof of the lemma.

11.4 Proof of the universality of $H_U(X, Y)$

Let $n \in \mathbf{N}$. We write $h_{U(n)}(X)$ and $H_{U(n)}(X, Y)$ for the m-tuples of formal power series obtained from $h_U(X)$ and $H_U(X, Y)$ by substituting 0 for all $U(i, \mathbf{d})$, $\mathbf{d} \in \mathbf{I}$, $i \in \{1, \ldots, m\}$, with $|\mathbf{d}| > n$. Then we have

$$h_U(X) \equiv h_{U(n)}(X) + \Gamma_{n+1}(X) \quad \text{mod(degree } n + 2) \tag{11.4.1}$$

where $\Gamma_{n+1}(X)$ is the following m-tuple of homogeneous forms of degree $n + 1$ in $X_1, \ldots, X_m$:

$$\Gamma_{n+1}(X) = \sum_{|\mathbf{d}| = n+1} v(\mathbf{d})^{-1} U_{\mathbf{d}} X^{\mathbf{d}} \tag{11.4.2}$$

where the notation is as in (11.1.2). It follows that for $H_U(X, Y)$

$$H_U(X, Y) \equiv H_{U(n)}(X, Y) + \Gamma_{n+1}(X) + \Gamma_{n+1}(Y) - \Gamma_{n+1}(X + Y) \quad \text{mod(degree } n + 2) \tag{11.4.3}$$

We write

$$H_U(X, Y) = (H_U(1)(X, Y), \ldots, H_U(m)(X, Y)) \tag{11.4.4}$$

$$H_U(i)(X, Y) = X_i + Y_i + \sum_{|\mathbf{k}|, |\mathbf{l}| \geq 1} e_{\mathbf{k},\mathbf{l}}(i) X^{\mathbf{k}} Y^{\mathbf{l}} \tag{11.4.5}$$

Now for each $\mathbf{d} \in \mathbf{I}$ with $|\mathbf{d}| \geq 2$ and $i \in \{1, \ldots, m\}$, define

$$y(i, \mathbf{d}) = \sum_{\mathbf{0} < \mathbf{k} < \mathbf{d}} \lambda(\mathbf{d}, \mathbf{k}) e_{\mathbf{k}, \mathbf{d}-\mathbf{k}}(i) \tag{11.4.6}$$

where the $\lambda(\mathbf{d}, \mathbf{k})$ are as in (11.3.5).

■ (11.4.7) **Lemma** The $y(i, \mathbf{d})$, $\mathbf{d} \in \mathbf{I}$, $|\mathbf{d}| \geq 2$, $i \in \{1, \ldots, m\}$ are a polynomial basis for $\mathbf{Z}[U]$.

That is, every element of $\mathbf{Z}[U]$ can be written uniquely as a polynomial in the $y(i, \mathbf{d})$. The proof of Lemma (11.4.7) is not difficult; it follows directly from (11.4.3) and (11.3.6).

■ (11.4.8) **Proof of the universality of $H_U(X, Y)$** Now let $G(X, Y)$ be any m-dimensional commutative formal group law over a ring A. We write $G(X, Y) = (G(1)(X, Y), \ldots, G(m)(X, Y))$, and

$$G(i)(X, Y) = X_i + Y_i + \sum_{|\mathbf{k}|, |\mathbf{l}| \geq 1} a_{\mathbf{k},\mathbf{l}}(i) X^{\mathbf{k}} Y^{\mathbf{l}} \tag{11.4.9}$$

We now define a homomorphism ϕ: $\mathbf{Z}[U] \to A$ by setting

$$\phi(y(i, \mathbf{d})) = \sum_{\mathbf{0}<\mathbf{k}<\mathbf{d}} \lambda(\mathbf{d}, \mathbf{k}) a_{\mathbf{k},\mathbf{d}-\mathbf{k}}(i) \tag{11.4.10}$$

Note that this is well defined because of Lemma (11.4.7). Also ϕ is certainly the only possible homomorphism $\mathbf{Z}[U] \to A$ such that $\phi_* H_U(X, Y) = G(X, Y)$. It remains to prove that $\phi(e_{\mathbf{k},\mathbf{l}}(i)) = a_{\mathbf{k},\mathbf{l}}(i)$ for all $|\mathbf{k}|, |\mathbf{l}| > 1, i \in \{1, \ldots, m\}$. The case $|\mathbf{k} + \mathbf{l}| = 2$ follows directly from (11.4.10) because in that case $y(i, \mathbf{k} + \mathbf{l}) = e_{\mathbf{k},\mathbf{l}}(i)$ by (11.4.6) and $\phi(y(i, \mathbf{k} + \mathbf{l})) = a_{\mathbf{k},\mathbf{l}}(i)$ by (11.4.10).

Commutativity of $H_U(X, Y)$ and $G(X, Y)$ means that we have relations

$$a_{\mathbf{k},\mathbf{l}}(i) = a_{\mathbf{l},\mathbf{k}}(i), \qquad e_{\mathbf{k},\mathbf{l}}(i) = e_{\mathbf{l},\mathbf{k}}(i) \tag{11.4.11}$$

and the associativity of $H_U(X, Y)$, $G(X, Y)$ means that the $e_{\mathbf{k},\mathbf{l}}(i)$ and $a_{\mathbf{k},\mathbf{l}}(i)$ satisfy certain universal relations of the form

$$\binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} e_{\mathbf{j}+\mathbf{k},\mathbf{l}}(i) - \binom{\mathbf{k}+\mathbf{l}}{\mathbf{l}} e_{\mathbf{j},\mathbf{k}+\mathbf{l}}(i) = Q_{\mathbf{j},\mathbf{k},\mathbf{l},i}(e_{\mathbf{s},\mathbf{t}})$$

$$\binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} a_{\mathbf{j}+\mathbf{k},\mathbf{l}}(i) - \binom{\mathbf{k}+\mathbf{l}}{\mathbf{l}} a_{\mathbf{j},\mathbf{k}+\mathbf{l}}(i) = Q_{\mathbf{j},\mathbf{k},\mathbf{l},i}(a_{\mathbf{s},\mathbf{t}})$$

where $Q_{\mathbf{j},\mathbf{k},\mathbf{l},i}(e_{\mathbf{s},\mathbf{t}})$ involves only those $e_{\mathbf{s},\mathbf{t}}$ with $|\mathbf{s} + \mathbf{t}| < |\mathbf{j} + \mathbf{k} + \mathbf{l}|$; cf. 9.5. One now proves that $\phi(e_{\mathbf{k},\mathbf{l}}(i)) = a_{\mathbf{k},\mathbf{l}}(i)$ for all $|\mathbf{k}|, |\mathbf{l}| \geq 1$ by an easy induction with respect to $|\mathbf{k} + \mathbf{l}|$, using the binomial coefficient lemma (11.3.7). This concludes the proof of the universality of $H_U(X, Y)$ and hence concludes the proof of Theorem (11.1.5).

(11.4.12) **Corollary** (Lazard's comparison lemma) Let $F(X, Y)$ and $G(X, Y)$ be two m-dimensional formal group laws over a ring A and suppose that $F(X, Y) \equiv G(X, Y)$ mod(degree n). Then there exist an m-tuple of homogeneous forms Γ of degree n with coefficients in A and an $m \times m$ matrix M with coefficients in A such that

$$\begin{aligned} F(X, Y) \equiv G(X, Y) + \Gamma(X) + \Gamma(Y) - \Gamma(X + Y) \\ + M(\nu(n)^{-1}(X^n + Y^n - (X + Y)^n)) \end{aligned} \tag{11.4.13}$$

If one adds the restriction that $\Gamma(X)$ may contain no terms of the form aX_i^n, $a \in A$, $i \in \{1, \ldots, m\}$, then the Γ and M in (11.4.13) are unique.

12 Curvilinear Formal Group Laws

All formal group laws in this section are commutative.

The m-dimensional universal formal group law $H_U(X, Y)$ of Section 11 does not coincide with the one dimensional formal group law $F_U(X, Y)$ constructed in Section 5 if $m = 1$. In fact it seems that there is no higher dimensional

analogue of $F_U(X, Y)$ that is universal. However, there does exist a higher dimensional analogue for $F_U(X, Y)$ that is universal for a certain class of formal group laws, the so-called curvilinear formal group laws. This m-dimensional version of $F_U(X, Y)$ is obtained from $F_U(X, Y)$ by replacing everywhere in $f_U(X)$ and $F_U(X, Y)$ the indeterminates $U_i, i = 2, 3, \ldots$, by $m \times m$ matrices of indeterminates $U_i = (U_i(j, k))_{j,k}$.

12.1 Definition and characterization of curvilinear formal group laws

Let $\mathbf{k}$, $\mathbf{l}$ be multi-indices of length m, then $\mathbf{kl}$ denotes the multi-index $\mathbf{kl} = (k_1 l_1, \ldots, k_m l_m)$. An m-dimensional formal group law

$$F(X, Y) = (F(1)(X, Y), \ldots, F(m)(X, Y))$$
$$F(i)(X, Y) = X_i + Y_i + \sum_{|\mathbf{k}|, |\mathbf{l}| \geq 1} a_{\mathbf{k},\mathbf{l}}(i) X^{\mathbf{k}} Y^{\mathbf{l}}$$

is said to be *curvilinear* if the following condition is satisfied:

(12.1.1) If $|\mathbf{k}|, |\mathbf{l}| \geq 1$, $\mathbf{kl} = \mathbf{0}$, then $a_{\mathbf{k},\mathbf{l}}(i) = 0$ for all $i = 1, 2, \ldots, m$.

■ (12.1.2) **Lemma** (criterion for curvilinearity) Let A be a characteristic zero ring and $F(X, Y)$ an m-dimensional formal group law over A. Then $F(X, Y)$ is curvilinear if and only if $\log_F(X)$ is of the form

$$\log_F(X) = X + \sum_{n=2}^{\infty} a_n X^n$$

where the a_n are $n \times n$ matrices with coefficients in $A \otimes \mathbf{Q}$.

For the moment we shall prove only the "if" part of this criterion. The "only if" part will follow from the construction of a universal curvilinear formal group law later in this section.

■ (12.1.3) **Proof of the "if" part of Lemma (12.1.2)** Let $g(X) = \sum_{n=1}^{\infty} a_n X^n$, $a_1 = I_n$ and $G(X, Y) = g^{-1}(g(X) + g(Y))$. Write

$$G(i)(X, Y) = X_i + Y_i + \sum a_{\mathbf{k},\mathbf{l}}(i) X^{\mathbf{k}} Y^{\mathbf{l}}$$

Suppose that there are $a_{\mathbf{k},\mathbf{l}} \neq 0$ with $\mathbf{kl} = \mathbf{0}$ and $|\mathbf{k}|, |\mathbf{l}| \geq 1$. Choose such an $a_{\mathbf{k},\mathbf{l}} \neq 0$ with $|\mathbf{k} + \mathbf{l}|$ minimal. Now consider the coefficient of $X^{\mathbf{k}} Y^{\mathbf{l}}$ on both sides of

(12.1.4) $$g(G(X, Y)) = g(X) + g(Y)$$

Because the coefficient of $X^{\mathbf{k}} Y^{\mathbf{l}}$ in the right-hand side of (12.1.4) is zero, we see from $g(X) = \sum a_n X^n$ that we must have a relation of the form

(12.1.5) $$a_{\mathbf{k},\mathbf{l}}(i) X^{\mathbf{k}} Y^{\mathbf{l}} = \{\sum b_{\ldots} (a_{\mathbf{k}_{i_1},\mathbf{l}_{i_1}}(j_1))^{r_1} \cdot \cdots \cdot (a_{\mathbf{k}_{i_s},\mathbf{l}_{i_s}}(j_s))^{r_s}\} X^{\mathbf{k}} Y^{\mathbf{l}}$$

with $j_1 = \cdots = j_s = j$. Here the sum is over all $\mathbf{k}_{i_1}, \ldots, \mathbf{k}_{i_s}, \mathbf{l}_{i_1}, \ldots, \mathbf{l}_{i_s}, j, r_1, \ldots, r_s$ such that $r_1, \ldots, r_s \in \mathbf{N}$,

$$r_1\mathbf{k}_{i_1} + \cdots + r_s\mathbf{k}_{i_s} = \mathbf{k}, \quad r_1\mathbf{l}_{i_1} + \cdots + r_s\mathbf{l}_{i_s} = \mathbf{l}, \quad 1 \leq |\mathbf{k}_{i_j} + \mathbf{l}_{i_j}| < |\mathbf{k} + \mathbf{l}|$$

and the $b\ldots$ are certain multinomial coefficients. Now $\mathbf{kl} = 0$; it follows that also $\mathbf{k}_{i_t}\mathbf{l}_{i_t}$ is zero for all $t = 1, \ldots, s$, so that by induction $a_{\mathbf{k}_{i_t}, \mathbf{l}_{i_t}} = 0$ unless $|\mathbf{k}_{i_t} + \mathbf{l}_{i_t}| = 1$, i.e.,

$$\mathbf{k}_{i_t} = \mathbf{e}(j) \quad \text{and} \quad \mathbf{l}_{i_t} = \mathbf{0} \qquad \text{or} \qquad \mathbf{l}_{i_t} = \mathbf{e}(j) \quad \text{and} \quad \mathbf{k}_{i_t} = \mathbf{0}$$

So the sum (12.1.5) reduces to a sum

$$a_{\mathbf{k},\mathbf{l}}(i)X^{\mathbf{k}}Y^{\mathbf{l}} = \sum b\ldots X_j^{r_1}Y_j^{r_2} \tag{12.1.6}$$

which shows that $a_{\mathbf{k},\mathbf{l}}(i) = 0$ because $\mathbf{kl} = 0$ and $|\mathbf{k}| \geq 1$, $|\mathbf{l}| \geq 1$.

12.2 Construction of some curvilinear formal group laws

For each sequence of integers $(i_1, \ldots, i_s)$, $s \in \mathbf{N}$, $i_j \in \mathbf{N}\backslash\{1\}$ let $n(i_1, \ldots, i_s)$ be the integer defined in 5.6 and let

$$d(i_1, \ldots, i_s) = v(i_1)^{-1}v(i_2)^{-1} \cdots v(i_s)^{-1}n(i_1, \ldots, i_s)n(i_2, \ldots, i_s) \cdots \times n(i_{s-1}, i_s)n(i_s)$$

as in (5.3.3). Let $\mathbf{Z}[R]$ be short for $\mathbf{Z}[R_i(j, k); i = 2, 3, \ldots; j, k = 1, \ldots, m]$. We now define the $m \times m$ matrices $b_i(R)$, $i = 2, 3, \ldots$, as

$$b_i(R) = \sum_{(i_1, \ldots, i_s)} d(i_1, \ldots, i_s)R_{i_1}R_{i_2}^{(i_1)} \cdots R_{i_s}^{(i_1 \cdots i_{s-1})} \tag{12.2.1}$$

Let

$$f_R(X) = X + \sum_{i=2}^{\infty} b_i(R)X^i, \qquad F_R(X, Y) = f_R^{-1}(f_R(X) + f_R(Y)) \tag{12.2.2}$$

Then one shows as in 5.3 and 11.2 that $f_R(X)$ satisfies a functional equation of type

$$f_R(X) = g_p(X) + \sum_{j=1}^{\infty} p^{-1}R_{pj}f_R^{(pj)}(X^{pj})$$

with $g_p(X) \in \mathbf{Z}_{(p)}[R][\![X]\!]$ so that $F_R(X, Y)$ has its coefficients in $\mathbf{Z}[R]$ by the functional equation lemma 10.2. Hence $F_R(X, Y)$ is a curvilinear formal group law over $\mathbf{Z}[R]$ by (the "if" part of) Lemma (12.1.2).

A second curvilinear formal group law $H_R(X, Y)$ is obtained as follows. Let ϑ: $\mathbf{Z}[U] \to \mathbf{Z}[R]$ be the homomorphism $U(i, \mathbf{d}) \mapsto 0$ unless $\mathbf{d}$ is of the form $\mathbf{d} = d\mathbf{e}(j)$, $U(i, d\mathbf{e}(j) \mapsto R_d(i, j)$. We define

$$H_R(X, Y) = \vartheta_* H_U(X, Y) \tag{12.2.3}$$

Then $H_R(X, Y)$ is a curvilinear formal group law over $\mathbf{Z}[R]$ with logarithm $h_R(X) = \vartheta_* h_U(X)$, which satisfies the same type of functional equation as $f_R(X)$ so that the formal group laws $F_R(X, Y)$ and $H_R(X, Y)$ are strictly isomorphic by the functional equation lemma 10.2.

12.3 Universality of the curvilinear formal group laws $F_R(X, Y)$, $H_R(X, Y)$

First a definition:

■ (12.3.1) **Definition** A curvilinear m-dimensional formal group law $F(X, Y)$ over a ring L is said to be a *universal* curvilinear m-dimensional formal group law if for every curvilinear m-dimensional formal group law $G(X, Y)$ over a ring A there is a unique homomorphism ϕ: $L \to A$ such that $\phi_* F(X, Y) = G(X, Y)$.

■ (12.3.2) **Theorem** The formal group laws $F_R(X, Y)$ and $H_R(X, Y)$ of 12.2 are universal curvilinear m-dimensional formal group laws.

Proof We have already seen that $F_R(X, Y)$ and $H_R(X, Y)$ are curvilinear formal group laws. So it remains to prove the universality. Let $F_{R(n)}(X, Y)$, $H_{R(n)}(X, Y)$ be the formal group laws obtained from $F_R(X, Y)$ and $H_R(X, Y)$ by substituting 0 for all $R_d(i, j)$ with $d > n$. Then we have from (12.2.1), (12.2.2) and (11.4.2), (11.4.3)

$$\begin{aligned} F_R(X, Y) &\equiv F_{R(n)}(X, Y) + R_{n+1}(\nu(n+1)^{-1} \\ &\qquad \times (X^{n+1} + Y^{n+1} - (X + Y)^{n+1})) \quad \text{mod(degree } n+2) \\ H_R(X, Y) &\equiv H_{R(n)}(X, Y) + R_{n+1}(\nu(n+1)^{-1} \\ &\qquad \times (X^{n+1} + Y^{n+1} - (X + Y)^{n+1})) \quad \text{mod(degree } n+2) \end{aligned} \tag{12.3.3}$$

Let $G(X, Y)$ be a curvilinear formal group law over a ring A. We are going to show by induction that there are homomorphisms ϕ_n, ψ_n: $\mathbf{Z}[R] \to A$ such that $G(X, Y) \equiv \phi_{n*} F_R(X, Y) \equiv \psi_{n*} H_R(X, Y)$ mod(degree $n+1$), and that the restriction of such ϕ_n, ψ_n to $\mathbf{Z}[R(n)] = \mathbf{Z}[R_d(i, j) \mid d \leq n] \subset \mathbf{Z}[R]$ is unique. This is obvious for $n = 1$. So suppose we have already found ψ_n, ϕ_n for some $n \geq 1$. By the comparison lemma (11.4.12) it follows that there are homogeneous m-tuples of polynomials $\Gamma_1(X)$, $\Gamma_2(X)$ of degree $n+1$ not involving any terms of the form aX_i^{n+1} and $m \times m$ matrices with coefficients in A, M_1, M_2 such that

$$\begin{aligned} G(X, Y) &\equiv \phi_{n*} F_R(X, Y) + \Gamma_1(X) + \Gamma_1(Y) - \Gamma_1(X + Y) \\ &\qquad + M_1(\nu(n+1)^{-1}(X^{n+1} + Y^{n+1} - (X + Y)^{n+1}) \\ G(X, Y) &\equiv \psi_{n*} H_R(X, Y) + \Gamma_2(X) + \Gamma_2(Y) - \Gamma_2(X + Y) \\ &\qquad + M_2(\nu(n+1)^{-1}(X^{n+1} + Y^{n+1} - (X + Y)^{n+1})) \end{aligned}$$

But $G(X, Y)$, $\psi_{n*}H_R(X, Y)$, $\phi_{n*}F_R(X, Y)$ are all curvilinear formal group laws. It follows directly from the definition of curvilinear that

$$\Gamma_1(X) + \Gamma_1(Y) - \Gamma_1(X + Y) = 0 = \Gamma_2(X) + \Gamma_2(Y) - \Gamma_2(X + Y)$$

Now define ϕ_{n+1}, ψ_{n+1}: $\mathbf{Z}[R] \to A$ as follows: $\psi_{n+1}(R_d) = \psi_n(R_d)$ if $d \leq n$, $\psi_{n+1}(R_{n+1}) = M_2$, $\psi_{n+1}(R_d) = 0$ if $d > n + 1$; $\phi_{n+1}(R_d) = \phi_n(R_d)$ if $d \leq n$, $\phi_{n+1}(R_{n+1}) = M_1$, $\phi_{n+1}(R_d) = 0$ if $d > n + 1$. Then we have that

$$G(X, Y) \equiv (\phi_{n+1})_* F_R(X, Y) \equiv (\psi_{n+1})_* H_R(X, Y) \mod(\text{degree } n + 2)$$

because of (11.3.3). Moreover the ϕ_{n+1}, ψ_{n+1} are unique on $\mathbf{Z}[R(n + 1)] \subset \mathbf{Z}[R]$ because M_1 and M_2 are unique. This concludes the proof of Theorem (12.3.2).

■ (12.3.4) **Corollary** ("only if" part of Lemma (12.1.2)) If A is a characteristic zero ring and $G(X, Y)$ is a curvilinear m-dimensional formal group law over A, then $\log_G(X)$ is of the form $\log_G(X) = \sum_{n=1}^{\infty} a_n X^n$ for certain $m \times m$ matrices a_n with coefficients in $A \otimes \mathbf{Q}$.

■ (12.3.5) Let ψ: $\mathbf{Z}[R] \to \mathbf{Z}[U]$ be the natural embedding $R_i(j, k) \mapsto U(j, ie(k))$. Then $\psi_* h_R(X)$, the logarithm of $\psi_* H_R(X, Y)$, and $h_U(X)$, the logarithm of $H_U(X, Y)$, satisfy the same type of functional equation for all prime numbers p. (In fact $\psi_* h_R(X)$ is obtained from $h_U(X)$ by substituting 0 for all $U(i, \mathbf{d})$ with $\mathbf{d} \in \mathbf{D}$.) It now follows from the functional equation lemma that $H_U(X, Y)$ and $\psi_* H_R(X, Y)$ are strictly isomorphic. Since $H_U(X, Y)$ is universal, we have proved

■ (12.3.6) **Proposition** Every commutative formal group law over a ring A is strictly isomorphic over A to a curvilinear formal group law over A.

In fact the isomorphism $H_U(X, Y) \xrightarrow{\sim} \psi_* H_R(X, Y)$ gives a functorial way of making formal group laws curvilinear. Over characteristic zero rings the procedure is as follows: let $\log_F(X) = f(X)$ be the logarithm of an m-dimensional formal group law over a characteristic zero ring A; write

$$f(X) = \sum_{\mathbf{n}} a_{\mathbf{n}} X^{\mathbf{n}}, \qquad a_{\mathbf{n}} \in (A \otimes \mathbf{Q})^m$$

define

$$\bar{f}(X) = \sum_{i=1}^{m} \sum_{n=1}^{\infty} a_{ne(i)} X_i^n$$

then $\bar{F}(X, Y) = f^{-1}(\bar{f}(X) + \bar{f}(Y))$ is a curvilinear formal group law over A that is strictly isomorphic to $F(X, Y)$ over A. So the procedure is simply "cross out in $\log_F(X)$ all coefficients that one does not want."

13 Higher Dimensional Honda Formal Group Laws and Higher Dimensional Lubin–Tate Formal Group Laws

All formal group laws in this section will be commutative.

13.1 The higher dimensional Honda formal groups

■(13.1.1) In this section (13.1) K will be a discretely valued field of characteristic zero (not necessarily complete) with ring of integers A, maximal ideal $\mathfrak{m}$, and residue field $k = A/\mathfrak{m}$ of characteristic $p > 0$. In addition we require that there exists an endomorphism $\sigma\colon K \to K$ and a power q of p such that

$$\sigma(a) \equiv a^q \mod(\mathfrak{m}) \quad \text{for all} \quad a \in A \tag{13.1.2}$$

■(13.1.3) Choose a uniformizing element π of A. Let $K_\sigma((T))$ be the noncommutative ring of Laurent series in one variable T with the multiplication rule $Ta = \sigma(a)T$ for $a \in K$. Let $u = \sum_{i=0}^{\infty} c_i T^i$ be an $m \times m$ matrix with its elements in $A_\sigma((T))$, such that $u(T) \equiv \pi I_n \mod(\text{degree } 1)$. Now let $u^{-1}\pi = I_n + \sum_{i=1}^{\infty} B_i T^i$ and let $f(X_1, \ldots, X_m) = f(X)$ and $F(X, Y)$ be defined by

$$f(X) = X + \sum_{n=0}^{\infty} B_i X^{q^i} \tag{13.1.4}$$

$$F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{13.1.5}$$

■(13.1.6) **Proposition** The m-tuple of power series $F(X, Y)$ defined above is a formal group law over A.

Proof From $u^{-1}\pi = I_n + \sum_{i=1}^{\infty} B_i T^i$ we find $u(I_n + \sum_{i=1}^{\infty} B_i T^i) = \pi$. Writing $u = \pi I_n + a_1 T + a_2 T^2 + \cdots$, where the a_i are $m \times m$ matrices, we obtain

$$\pi B_n + a_1 \sigma(B_{n-1}) + a_2 \sigma^2(B_{n-2}) + \cdots + a_{n-1}\sigma^{n-1}(B_1) + a_n = 0$$

so that $f(X)$ satisfies the functional equation

$$f(X) = X + \sum_{i=1}^{\infty} s_i \sigma_*^i f(X^{q^i})$$

with $s_i = -\pi^{-1}a_i$. To prove Proposition (13.1.6) it therefore suffices to apply the functional equation lemma 10.2.

13.2 Generalized Lubin-Tate formal laws and Cartier's semilinear trick

■(13.2.1) **Generalized Lubin–Tate formal group laws** Suppose we are in the standard functional equation type situation. That is, $\mathfrak{A}$ is an ideal in $A \subset K$, $\sigma\colon K \to K$, $p \in \mathfrak{A}$, q a power of p, $\sigma(a) \equiv a^q \mod \mathfrak{A}$ for all $a \in A$. Now let

$s_1 = b \in K^{m\times m}$ be such that $\mathfrak{a}b \subset A^{m\times m}$ and take $s_2 = s_3 = \cdots = 0$. Taking $g(X) = X$ and (hence)

$$f_b(X) = X + b\sigma_* f(X^q), \qquad F_b(X, Y) = f_b^{-1}(f_b(X) + f_b(Y)) \tag{13.2.2}$$

we find, by the functional equation lemma 10.2, an m-dimensional formal group law over A. We shall call these formal group laws *generalized Lubin–Tate formal group laws.*

Note that even in the case that $m = 1$ and A a discrete valuation ring these are more general than the Lubin–Tate formal group laws of Section 8 of Chapter I, owing to the possibility of a twist σ, which may be nontrivial if q is unequal to the number of elements of the residue field of A.

The price one pays for this generality is that in general if $a \in A$, then $f_b^{-1}(af_b(X))$ is not integral (i.e., in $A[\![X]\!]$), so that we do not have endomorphisms $[a]$ for all $a \in A$; cf., however, Proposition (13.2.7).

More generally, one can of course consider m-tuples of power series in $X_1, X_2, \ldots, X_m$ defined by

$$f(X) = g(X) + b\sigma_* f(X^q), \qquad g(X) \in A[\![X]\!]^m \tag{13.2.3}$$

$$g(X) \equiv X \mod(\text{degree } 2)$$

Then by the functional equation lemma $F(X, Y) = f^{-1}(f(X) + f(Y))$ is a formal group law over A that is strictly isomorphic over A to $F_b(X, Y)$, and conversely all formal group laws over A that are strictly isomorphic over A to $F_b(X, Y)$ have logarithms of the form (13.2.3).

■ (13.2.4) **Twisted Lubin–Tate formal group laws** In the case $m = 1$ $\mathfrak{a} = \pi A$ a principal ideal of A with $\pi^{-1} \in K$ and $b = \pi^{-1}u$ for some unit $u \in A$, we shall call the one dimensional formal group law $F_b(X, Y)$ defined by (13.2.2) a *twisted Lubin–Tate formal group law.*

■ (13.2.5) **Homomorphisms** Let A, K, p, q, σ, $\mathfrak{a}$ be as in (13.2.1). Let $b \in K^{m\times m}$, $\hat{b} \in K^{n\times n}$ be such that $b\mathfrak{a} \subset A^{m\times m}$, $\hat{b}\mathfrak{a} \subset A^{n\times n}$, and let $c \in A^{n\times m}$ be an $n \times m$ matrix with coefficients in A such that

$$\hat{b}\sigma_*(c) = cb \tag{13.2.6}$$

Then we have

$$\begin{aligned} cf_b(X) &= cX + cb\sigma_* f_b(X^q) = cX + \hat{b}\sigma_*(c)\sigma_*(f_b(X^q)) \\ &= cX + \hat{b}\sigma_*(cf_b(X^q)) \end{aligned}$$

showing that $cf_b(X)$ satisfies the same kind of functional equation as $f_{\hat{b}}(X)$ so that the functional equation lemma says that $f_{\hat{b}}^{-1}(cf_b(X))$ has its coefficients in A. In other words, we have a homomorphism of formal group laws over A

$$f_{\hat{b}}^{-1}(cf_b(X)) \colon F_b(X, Y) \to F_{\hat{b}}(X, Y)$$

for every matrix $c \in A^{n \times m}$ satisfying (13.2.6). In particular we have

■ (13.2.7) **Proposition** Let A, K, $\mathfrak{A}$, p, q, σ, b be as in (13.2.1). Suppose that $\sigma = id$. Then $[a](X) = f_b^{-1}(af_b(X))$ is an endomorphism over A of $F_b(X, Y)$ for every $a \in A$.

■ (13.2.8) **Remarks**

(i) More generally, one always has an endomorphism $[a](X)$ of $F_b(X, Y)$ if $\sigma(a) = a$, $a \in A$.

(ii) Sometimes one can prove that all homomorphisms between generalized Lubin-Tate formal group laws $F_b(X, Y) \to F_b(X, Y)$ are of the form $f_b^{-1}(cf_b(X))$ where c is a matrix satisfying (13.2.6); cf. (20.1.24) of Chapter IV.

■ (13.2.9) **Cartier's semilinear trick** In [68] and [72] Cartier constructs certain higher dimensional formal group laws in the following situation:

(i) A is a local ring with maximal ideal $\mathfrak{m}$ and residue field k of characteristic $p > 0$;

(ii) there are an automorphism σ of A and a power q of p such that $\sigma(a) \equiv a^q \bmod \mathfrak{m}$ for all $a \in A$;

(iii) $pa = 0$, $a \in A \Rightarrow a = 0$.

Given this Cartier constructs an h-dimensional formal group law given the following data:

(iv) a free module M over A of finite rank h together with a semilinear endomorphism η: $M \to M$ such that $\eta(\mathfrak{m}M) \subset pM$. (Here semilinear means of course $\eta(m_1 + m_2) = \eta(m_1) + \eta(m_2)$, $\eta(am) = \sigma(a)\eta(m)$ for all m, m_1, $m_2 \in M$, $a \in A$.)

These constructions are important for the so-called *tapis de Cartier*, which has to do with liftings of formal group laws and cristalline cohomology; cf. Section 30 of Chapter V for details.

Here is how to obtain a formal group law out of (M, η) as above. Let $K = A[p^{-1}] = A \otimes \mathbf{Q}$. Then σ extends uniquely to an automorphism σ of K (by (iii)). Choose a basis $e_1, \ldots, e_h$ for M over A.

Let $D = D(\eta) = (d_{ij})$ be the matrix of η, i.e.,

$$\eta(e_i) = \sum_{j=1}^{h} d_{ji} e_j$$

Then the condition $\eta(\mathfrak{m}M) \subset pM$ means that $(p^{-1}D)\mathfrak{m} \subset A^{n \times n}$. Taking

$$b = p^{-1}D(\eta)$$

we can apply formula (13.2.2) to define a formal group law $G(M, \eta)(X, Y)$ with logarithm

$$g(M, \eta)(X) = X + p^{-1}D(\eta)\sigma_* g(M, \eta)(X^q) \tag{13.2.10}$$

This is the formal group law constructed by Cartier in [68] and [72] from the data (M, η). For more details, cf. Section 30.1 of Chapter V.

■ (13.2.11) **Isomorphisms** The question naturally arises, Does $G(M, \eta)(X, Y)$ as constructed above depend on the choice of the basis $e_1, \ldots, e_h$? And of course it does, but only within isomorphism.

Let ϕ: $(M, \eta) \to (\hat{M}, \hat{\eta})$ be a homomorphism of pairs (M, η); i.e., ϕ is a homomorphism of A-modules ϕ: $M \to \hat{M}$ such that the following diagram commutes

(13.2.12)
$$\begin{array}{ccc} M & \xrightarrow{\phi} & \hat{M} \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\hat{\eta}} \\ M & \xrightarrow[\phi]{} & \hat{M} \end{array}$$

Let $e_1, \ldots, e_h$ be a basis of M and $\hat{e}_1, \ldots, \hat{e}_l$ a basis of $\hat{M}$. Let c be the matrix of ϕ with respect to the bases $\{e_1, \ldots, e_h\}$, $\{\hat{e}_1, \ldots, \hat{e}_l\}$. Then the commutativity of (13.2.12) says that

$$D(\hat{\eta})\sigma_*(c) = cD(\eta)$$

so that by (13.2.5) we have a homomorphism of formal group laws

$$g(\hat{M}, \hat{\eta})^{-1}(cg(M, \eta)(X))\colon G(M, \eta)(X, Y) \to G(\hat{M}, \hat{\eta})(X, Y)$$

(which induces the original ϕ: $M \to \hat{M}$ on the Lie algebra level. $(L(G(M, \eta)) = M; L(G(\hat{M}, \hat{\eta})) = \hat{M})$.)

In particular, it follows that $G(M, \eta)(X, Y)$ does not depend up to isomorphism on the choice of the basis $\{e_1, \ldots, e_h\}$ of M.

■ (13.2.13) **Remark** It is clear now that the semilinear construction can be generalized. The following case will be important for us in Section 30 of Chapter V when we are doing a generalization for formal A-modules of the *tapis de Cartier*.

B is a discrete valuation ring with uniformizing element π and residue characteristic $p > 0$, σ a power of a Frobenius-like endomorphism of B (i.e., $\sigma(a) \equiv a^q \bmod \pi$ for all $a \in B$), and M a free B-module of finite rank with a σ-semilinear endomorphism η: $M \to M$. In this case one takes $b = \pi^{-1}D(\eta)$ where $D(\eta)$ is a matrix of η.

13.3 The higher dimensional Lubin-Tate formal groups

■ (13.3.1) In this subsection (13.3) K is a *complete* discretely valued field with ring of integers A, maximal ideal $\mathfrak{m}$, residue field $k = A/\mathfrak{m}$. We suppose that k has q elements, $q = p^r$, $p = \text{char}(k)$. (We do not require that K has characteristic 0.) Choose a prime element π of A and an integer $m \in \mathbf{N}$.

Let M be an $m \times m$ matrix such that $\pi^{-1}M$ is an invertible matrix with

coefficients in A. Choose a $t \in \mathbf{N}$. We use $\mathscr{E}_{M,t}$ to denote the set of all m-tuples of power series $d(X)$ in $(X_1, \ldots, X_m) = X$ such that

(13.3.2) $\quad d(X) \equiv MX \mod(\text{degree } 2), \qquad d(X) \equiv X^{q^t} \mod(\pi)$

■(13.3.3) **Theorem** For each $d(X) \in \mathscr{E}_{M,t}$, there is precisely one m-dimensional formal group law $F_d(X, Y)$ over A such that $F_d(d(X), d(Y)) = d(F_d(X, Y))$. If $d(X)$, $\bar{d}(X) \in \mathscr{E}_{M,t}$, then $F_d(X, Y)$ and $F_{\bar{d}}(X, Y)$ are strictly isomorphic over A.

The proof of this theorem (as well as some more results on endomorphisms and homomorphisms which we shall discuss in Chapter IV, Section 20.1) can be based on the following generalization of the fundamental Lubin–Tate lemma (8.1.2).

■(13.3.4) **Lemma** Let M be an $m \times m$ matrix with coefficients in A, N an $n \times n$ matrix with coefficients in A such that $\pi^{-1}M$ and $\pi^{-1}N$ are invertible matrices over A. Let $d(X_1, \ldots, X_m) \in \mathscr{E}_{M,t}$ and $e(X_1, \ldots, X_n) \in \mathscr{E}_{N,t}$. Let $k \in \mathbf{N}$ and let L be an n-tuple of linear forms in km indeterminates $(Z_{1,1}, \ldots, Z_{k,m})$ with coefficients in A. We shall write Z_1 for $(Z_{1,1}, \ldots, Z_{1,m})$, $\ldots$, Z_k for $(Z_{k,1}, \ldots, Z_{k,m})$. Suppose that

(13.3.5) $\quad e(L(Z_1, \ldots, Z_k)) \equiv L(d(Z_1), \ldots, d(Z_k)) \mod(\text{degree } 2)$

Then there exists a unique n-tuple of power series $\Phi(Z)$ in $Z_{1,1}, \ldots, Z_{k,m}$ such that

(13.3.6) $\quad \Phi(Z_1, \ldots, Z_k) \equiv L(Z_1, \ldots, Z_k) \mod(\text{degree } 2)$

(13.3.7) $\quad e(\Phi(Z_1, \ldots, Z_k)) = \Phi(d(Z_1), \ldots, d(Z_k))$

(Note that (13.3.6) and (13.3.7) together imply (13.3.5) and that if $n = m = 1$ (13.3.5) always holds if $N = M$ and never if $N \neq M$.)

We shall not give the proof of this lemma in detail. The structure of the proof is identical with the proof of Lemma (8.1.2) in 8.2. That is with induction one constructs unique n-tuples of polynomials $\Phi_r(Z_1, \ldots, Z_k)$ such that (13.3.6) holds and such that (13.2.7) holds mod(degree $r + 1$). To get the next approximation one must find $E_{r+1}(Z_1, \ldots, Z_k)$ homogeneous of degree $r + 1$ such that

$$NE_{r+1}(Z_1, \ldots, Z_k) - E_{r+1}(MZ_1, \ldots, MZ_k) = D_{r+1}(Z_1, \ldots, Z_k)$$

where $D_{r+1}(Z_1, \ldots, Z_k)$ is a given homogeneous polynomial which is $\equiv 0 \bmod \pi$. Here some technical difficulties due to higher dimensionality arise because one cannot simply "move M outside of E_{r+1}." One constructs E_{r+1} by means of successive approximation and here the completeness of A is used in an essential way. A detailed proof can be found in [226].

■(13.3.8) **Proof of Theorem (13.3.3)** Given the lemma the proof of Theorem (13.3.3) is exactly as the proof of Theorem (8.1.5) in Chapter I.

13.4 The higher dimensional Lubin-Tate formal group laws as special cases of the functional equation lemma formal group laws

■ (13.4.1) **The endomorphism** $[\pi]$ Let A, K, $\mathfrak{A}$, p, q, σ be as in (13.2.1). Suppose in addition that $\mathfrak{A}$ is a principal ideal $\mathfrak{A} = \pi A$, that $\pi^{-1} \in K$ and that $\sigma(\pi) = \pi$. Let D be any $m \times m$ matrix with coefficients in A such that $\sigma_*(D) = D$ and take $b = \pi^{-1}D$.

By remark (13.2.8)(i) we then have an endomorphism

$$[\pi](X)\colon F_b(X, Y) \to F_b(X, Y)$$

We claim that

(13.4.2) $$[\pi](X) \equiv DX^q \mod \pi$$

To see this first observe that because $\sigma_*(D) = D$,

(13.4.3) $$(DX)^{q^r} \equiv (DX^q)^{q^{r-1}} \mod \pi^r$$

Now to prove (13.4.2) it suffices by part (iv) of the functional equation lemma to show that

$$f_b([\pi](X)) = \pi f_b(X) \equiv f_b(DX^q) \mod \pi$$

which follows readily from (13.4.3), again because $\sigma_*(D) = D$.

■ (13.4.4) **The endomorphism** $[M](X)$ Now let A, K, p, q, π, M be as in (13.3.1) and let $F_b(X, Y)$ be the generalized Lubin–Tate formal group law with $b = M^{-1} = \pi^{-1}\bar{M}$ where $\bar{M}$ is the inverse of $\pi^{-1}M$ (here one takes $\sigma = id$ and q^t instead of q). By (13.2.5) we have an endomorphism

$$[M](X) = f_b^{-1}(Mf_b(X))\colon F_b(X, Y) \to F_b(X, Y)$$

over A because $M^{-1}\sigma_*(M) = M^{-1}M = I = MM^{-1}$. Exactly as in (13.4.1) one now shows easily that

(13.4.5) $$[M](X) \equiv X^{q^t} \mod \pi, \qquad [M](X) \equiv MX \mod(\text{degree } 2)$$

(The completeness of A is of course not necessary for this.) Thus we see that $F_b(X, Y)$ is a higher dimensional Lubin–Tate formal group law as in 13.3. Exactly as in Section 8 Chapter I, we can now set up a bijective correspondence between higher dimensional Lubin–Tate formal group laws corresponding to elements $d(X) \in \mathscr{E}_{M,t}$ and generalized Lubin–Tate formal group laws with logarithms

$$f(X) = g(X) + bf(X^{q^t}), \qquad g(X) \in A[\![X]\!], \qquad g(X) \equiv X \mod(\text{degree } 2)$$

where $b = M^{-1}$ $(= \pi^{-1}\bar{M})$.

14 Lie Theory

In this section A is supposed to be a $\mathbf{Q}$-algebra. We shall start to show that the functor L, which assigns to every n-dimensional formal group law $F(X, Y)$ over A its Lie algebra $L(F)$, is an equivalence of categories.

14.1 The Lie-algebra of an n-dimensional formal group law

Let $F(X, Y) = (F(1)(X, Y), F(2)(X, Y), \ldots, F(n)(X, Y))$ be an n-dimensional formal group law over A. We write

$$F(i)(X, Y) = X_i + Y_i + \sum_{l,k=1}^{n} \gamma_{lk}^{i} X_l Y_k \quad \text{mod(degree 3)} \tag{14.1.1}$$

The elements $\gamma_{jk}^{i} \in A$ can then be used to define a Lie algebra structure on A^n as follows:

$$[e_j, e_k] = \sum_{i=1}^{n} (\gamma_{jk}^{i} - \gamma_{kj}^{i}) e_i \tag{14.1.2}$$

(NB the "multiplication" $e_j e_k = \sum_{i=1}^{n} \gamma_{jk}^{i} e_i$ does *not* as a rule define an associative algebra structure on A^n.)

(14.1.3) **Proof that (14.1.2) defines a Lie algebra structure** It is immediate that $[e_j, e_j] = 0$ for all j and that $[e_j, e_k] = -[e_k, e_j]$ for all j, k. It remains to check the Jacobi identity $[[e_i, e_j], e_k] + [[e_j, e_k], e_i] + [[e_k, e_i], e_j] = 0$ for all i, j, k. This can be seen, e.g., by means of a fairly messy calculation using $F(X, F(Y, Z)) \equiv F(F(X, Y), Z)$ mod(degree 4). We follow Serre [363, LG, Chapter IV, No. 7]. Write

$$F(X, Y) = X + Y + B(X, Y) \quad \text{mod(degree 3)} \tag{14.1.4}$$

where $B(X, Y)$ is an n-tuple of bilinear forms in X, Y.

Let $X^{[-1]}$ be short for $\iota(X) = [-1]_F(X)$, i.e., $\iota(X) = X^{[-1]}$ is the unique n-tuple of power series such that $F(X, X^{[-1]}) = 0$. We then have

$$X^{[-1]} \equiv -X + B(X, X) \quad \text{mod(degree 3)} \tag{14.1.5}$$

as is easily checked. Now, as we have seen in 9.3, an n-dimensional formal group law $F(X, Y)$ can be used to define a group structure on, e.g., the set of all n-tuples of topologically nilpotent elements of $A[\![X, Y]\!]$. We denote this multiplication with a dot $\cdot$ so that, e.g., $X \cdot Y$ stands for $F(X, Y)$. Using this notation we have

$$X \cdot Y \cdot X^{[-1]} \equiv Y + [X, Y] \quad \text{mod(degree 3)} \tag{14.1.6}$$

where $[X, Y]$ is short for $B(X, Y) - B(Y, X)$.

Similarly, one has

$$Y^{[-1]} \cdot X \cdot Y \equiv X + [Y, X] \quad \text{mod(degree 3)} \tag{14.1.7}$$

and

$$X^{[-1]} \cdot Y^{[-1]} \cdot X \cdot Y \equiv [X, Y] \quad \text{mod(degree 3)} \tag{14.1.8}$$

Finally, one has the Jacobi identity (for the n-tuples X, Y, Z in $A[\![X, Y, Z]\!]^n$)

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0 \tag{14.1.9}$$

which is proved as follows. In any group G let (x, y) be short for $x^{-1}y^{-1}xy$ and x^y for $y^{-1}xy$. Then one has in any group G the identity of P. Hall

$$(x^y, (y, z))(y^z, (z, x))(z^x, (x, y)) = e \tag{14.1.10}$$

as is easily checked by writing everything out. We apply this to the group defined by $F(X, Y)$ on all n-tuples of topologically nilpotent elements of $A[\![X, Y, Z]\!]$. Now we have

$$\begin{aligned} (X^Y, (Y, Z)) &\equiv [X, [Y, Z]] \quad \text{mod(degree 4)} \\ (Y^Z, (Z, X)) &\equiv [Y, [Z, X]] \quad \text{mod(degree 4)} \\ (Z^X, (X, Y)) &\equiv [Z, [X, Y]] \quad \text{mod(degree 4)} \end{aligned} \tag{14.1.11}$$

Indeed, by symmetry, it suffices to prove the first of these formulas. Now $X^Y \equiv X$ mod(degree 2) and $(X, Y) \equiv [X, Y]$ mod(degree 3) by (14.1.7) and (14.1.8). Plugging this into (14.1.8) again we find the first formula of (14.1.11). The Jacobi identity (14.1.9) now follows from (14.1.11) and the P. Hall formula (14.1.10) because $[X, [Y, Z]]$, $[Y, [Z, X]]$, $[Z, [X, Y]]$ are all homogeneous of degree 3. It is trivial to see that (14.1.9) implies that (14.1.2) defines a Lie algebra structure on A^n.

■ (14.1.12) **Remark** The foregoing is precisely how one proves that the commutator (x, y) defines a Lie product on the associated graded group of a filtered group $G = G_1 \supset G_2 \supset \cdots$. The Lie algebra $L(F)$ constructed above is in fact the Lie algebra $\mathrm{gr}_1(G)$ where G is the group induced by F on the set of all n-tuples of topologically nilpotent elements of $A[\![T]\!]$, filtered by degree in T, where T is one indeterminate.

14.2 The main theorem of formal Lie theory

Let $F(X, Y)$ and $G(X, Y)$ be two finite dimensional formal group laws over a ring A and let $\alpha(X)$ be a homomorphism from $F(X, Y)$ to $G(X, Y)$. Let $J(\alpha)$ be the Jacobian matrix of $\alpha(X)$, i.e.,

$$\alpha(X) \equiv J(\alpha)X \quad \text{mod(degree 2)} \tag{14.2.1}$$

Then by (14.1.8) we have

$$\begin{aligned} \alpha(X)^{[-1]} \cdot \alpha(Y)^{[-1]} \cdot \alpha(X) \cdot \alpha(Y) &\equiv [J(\alpha)X, J(\alpha)Y]_G \quad \text{mod(degree 3)} \\ \alpha(X^{[-1]} \cdot Y^{[-1]} \cdot X \cdot Y) &\equiv J(\alpha)[X, Y]_F \quad \text{mod(degree 3)} \end{aligned} \tag{14.2.2}$$

which implies that $J(\alpha)$ induces a homomorphism of Lie algebras $J(\alpha)$: $L(F) \to L(G)$. We shall also use $L(\alpha)$ to denote this homomorphism of Lie algebras. We have thus defined a functor L from the category of finite dimensional formal groups over A to the category of Lie algebras over A that are free of finite rank as modules over A.

(14.2.3) **Theorem** (formal Lie theory theorem) Let A be a $\mathbf{Q}$-algebra. The functor L from finite dimensional formal group laws over A to Lie algebras over A that are free of finite rank as modules over A is an equivalence of categories.

Let $\mathbf{FG}_A$ denote the category of finite dimensional formal group laws over A and let $\mathbf{LA}_A$ be the category of Lie algebras over A whose underlying modules are free of finite rank over A. Then Theorem (14.2.3) says two things:

(14.2.4) For $F(X, Y)$, $G(X, Y) \in \mathbf{FG}_A$, the map $\mathbf{FG}_A(F(X, Y), G(X, Y)) \to \mathbf{LA}_A(L(F), L(G))$ is a bijection.

(14.2.5) Given $L \in \mathbf{LA}_A$, there is an $F(X, Y) \in \mathbf{FG}_A$ such that $L(F)$ is isomorphic to L.

In this section we shall prove only (14.2.5), which is the formal version of Lie's third theorem. To do this we use some results concerning the universal enveloping algebra of a Lie algebra and some results concerning free Lie algebras, which is what 14.3 and 14.4 below are about. The second half of Theorem (14.2.3) (statement (14.2.4)) will be proved later in Chapter VII, Section 37.4. There we shall also give a second proof of (14.2.5) which does not use the Campbell–Hausdorff formula.

14.3 The universal enveloping algebra of a Lie algebra

Let B be an associative algebra over A. Then the bracket $[b_1, b_2] = b_1 b_2 - b_2 b_1$ defines a Lie algebra structure on the underlying A-module of B. This Lie algebra is denoted $L(B)$. We shall say that an A-module homomorphism ϕ: $\mathfrak{g} \to B$ of an A Lie algebra $\mathfrak{g}$ to an associative algebra B over A is a *Lie homomorphism* iff $\phi[x, y] = \phi(x)\phi(y) - \phi(y)\phi(x)$ for all $x, y \in \mathfrak{g}$, i.e., iff ϕ induces a Lie algebra homomorphism $\mathfrak{g} \to L(B)$.

All associative algebras over A are supposed to be unitary, and homomorphisms of associative algebras preserve the unit elements. The category of associative algebras over A is denoted $\mathbf{Ass}_A$.

■ (14.3.1) **Definition** (universal enveloping algebra of a Lie algebra) Let $\mathfrak{g} \in \mathbf{LA}_A$. A universal enveloping algebra of $\mathfrak{g}$ is an associative algebra with unit $U\mathfrak{g}$ over A together with a homomorphism of Lie algebras $\varepsilon: \mathfrak{g} \to U\mathfrak{g}$ such that the following universal property is satisfied:

(14.3.2) For every Lie homomorphism $\phi: \mathfrak{g} \to B$ into an associative algebra B, there exists a unique homomorphism of associative algebras $\tilde{\phi}: U\mathfrak{g} \to B$ such that $\phi = \tilde{\phi}\varepsilon$.

It follows directly from the universality property (14.3.2) that $U\mathfrak{g}$ (if it exists) is unique up to isomorphism.

■ (14.3.3) **Construction of** $U\mathfrak{g}$ Let $\mathfrak{g} \in \mathbf{LA}_A$. The tensor algebra $T\mathfrak{g} \in \mathbf{Ass}_A$ of $\mathfrak{g}$ has as underlying module the direct sum

$$T\mathfrak{g} = \bigoplus_{n=0}^{\infty} T_n\mathfrak{g}$$

where $T_0\mathfrak{g} = A$, $T_n\mathfrak{g} = \mathfrak{g} \otimes \mathfrak{g} \otimes \cdots \otimes \mathfrak{g}$ (n times) where all tensor products are over A. There is an obvious associative multiplication on $T\mathfrak{g}$ defined by

$$(x_1 \otimes \cdots \otimes x_m, y_1 \otimes \cdots \otimes y_n) \mapsto x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n \in T_{n+m}\mathfrak{g}$$

For any $B \in \mathbf{Ass}_A$ one has

$$\mathbf{Mod}_A(\mathfrak{g}, B) \simeq \mathbf{Ass}_A(T\mathfrak{g}, B) \tag{14.3.4}$$

where $\mathbf{Mod}_A$ is the category of A-modules. Now let I be the ideal of $T\mathfrak{g}$ generated by the elements of the form $[x, y] - x \otimes y + y \otimes x \in T\mathfrak{g}$ for $x, y \in \mathfrak{g}$. Let $U\mathfrak{g} = T\mathfrak{g}/I$ and let $\varepsilon: \mathfrak{g} \to U\mathfrak{g}$ be the composed map $\mathfrak{g} = T_1\mathfrak{g} \subset T\mathfrak{g} \to U\mathfrak{g}$. Then $\mathfrak{g} \to U\mathfrak{g}$ is a universal enveloping algebra. Indeed if $\phi: \mathfrak{g} \to B$ is a Lie homomorphism, then ϕ extends naturally and uniquely to a homomorphism of associative algebras $T\mathfrak{g} \to B$ (14.3.4) and because ϕ is a Lie homomorphism $\phi(I) = 0$ so that ϕ factors (uniquely) through $U\mathfrak{g}$ to define $\tilde{\phi}$.

Consider $U\mathfrak{g} \otimes U\mathfrak{g}$ (tensor product over A). Then $x \mapsto x \otimes 1 + 1 \otimes x$ defines a Lie homomorphism $\mathfrak{g} \to U\mathfrak{g} \otimes U\mathfrak{g}$ (to check this simply calculate $(x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x)$), which by the universality property of $U\mathfrak{g}$ extends to a homomorphism of associative algebras

$$\Delta: U\mathfrak{g} \to U\mathfrak{g} \otimes U\mathfrak{g}, \qquad \mathfrak{g} \ni x \mapsto 1 \otimes x + x \otimes 1 \tag{14.3.5}$$

which is called the diagonal map or the comultiplication on $U\mathfrak{g}$. An element $y \in U\mathfrak{g}$ is called *primitive* if $\Delta y = 1 \otimes y + y \otimes 1$.

■ (14.3.6) **Structure of** $U\mathfrak{g}$ (Poincaré–Birkhoff–Witt theorem) First we have

(14.3.7) $\varepsilon: \mathfrak{g} \to U\mathfrak{g}$ is injective (P-B-W)

We shall accordingly view $\mathfrak{g}$ as embedded in $U\mathfrak{g}$ via ε. (This has already been used more or less in the writing down of (14.3.5).) Let $x_1, \ldots, x_n$ be a basis for $\mathfrak{g}$. As usual we shall use boldface letters $\mathbf{k}$ to denote n-tuples of elements in $\mathbf{N} \cup \{0\}$ and $x^{\mathbf{k}}$ is short for $x_1^{k_1} \cdots x_n^{k_n} \in U\mathfrak{g}$, $x_i^0 = 1$. We have

(14.3.8) $U\mathfrak{g}$ is a free module over A with basis $\{x^{\mathbf{k}}\}_{\mathbf{k}}$.

That is, a basis for $U\mathfrak{g}$ is formed by all finite products $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ with the x_i *in that order*. The multiplication in $U\mathfrak{g}$ satisfies

$$x^{\mathbf{k}} x^{\mathbf{l}} = x^{\mathbf{k}+\mathbf{l}} + \sum_{0 < \mathbf{j} < \mathbf{k}+\mathbf{l}} a_{\mathbf{j}} x^{\mathbf{j}} \tag{14.3.9}$$

for certain $a_{\mathbf{j}} \in A$. And the comultiplication in $U\mathfrak{g}$ is given by

$$\Delta(x^{\mathbf{k}}) = \sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} \binom{\mathbf{k}}{\mathbf{i}} x^{\mathbf{i}} \otimes x^{\mathbf{j}} \tag{14.3.10}$$

Finally,

(14.3.11) If A is torsion free (as a $\mathbf{Z}$-module, i.e., $a \in A$, $na = 0$, $n \in \mathbf{N} \Rightarrow a = 0$), then $\mathfrak{g} \subset U\mathfrak{g}$ coincides with the set of primitive elements of $U\mathfrak{g}$. I.e., $\mathfrak{g} = \{y \in U\mathfrak{g} \mid \Delta y = y \otimes 1 + 1 \otimes y\}$.

We shall not prove these results on the structure of $U\mathfrak{g}$. The proofs are rather long; cf., e.g., [363, LA, Chapter III] for (14.3.7), (14.3.8), and (14.3.11).

■ (14.3.12) **Remark** The comultiplication $\Delta: U\mathfrak{g} \to U\mathfrak{g} \otimes U\mathfrak{g}$ is coassociative and cocommutative. There is also a counit (or augmentation) $U\mathfrak{g} \to A$. All this turns $U\mathfrak{g}$ into a so-called bialgebra, a type of structure very much related to formal groups, which we shall discuss in more detail in Chapter VII.

14.4 Free Lie algebras

Let X be a set. We shall first recall the constructions of the free magma on X, the free algebra on X, the free associative algebra on X, and the free Lie algebra on X.

■ (14.4.1) **The free magma M_X** A *magma* is a set M with a map $M \times M \to M$, $(x, y) \mapsto xy$. Given a set X we construct inductively a family of sets X_n, $n \in \mathbf{N}$, as follows:

$$X_1 = X, \; X_n = \coprod_{p+q=n} X_p \times X_q, \qquad p, q \in \mathbf{N}$$

where $\coprod$ stands for disjoint union. Now let $M_X = \coprod_{n=1}^{\infty} X_n$. There is a natural multiplication $M_X \times M_X \to M_X$ defined by the maps $X_n \times X_m \subset X_{n+m} \subset M_X$. If $w \in M_X$, $w \in X_n$, then the length of w is defined as $l(w) = n$. Every "word" $w \in M_X$ of length > 1 can be uniquely written as a product $w'w'' = w$. One easily checks the freeness property of M_X:

(14.4.2) Let N be any magma and $f\colon X \to N$ any map, then there is a unique homomorphism of magmas $\tilde{f}\colon M_X \to N$ that extends f.

■ (14.4.3) **The free algebra** Al_X An *algebra* over a ring A is just an A-module B together with a multiplication map $B \times B \to B$ which is A-bilinear. There are no conditions such as commutativity, associativity, existence of a unit element.

Let X be a set. We define Al_X, the free algebra on X over A as follows: an element $\alpha \in Al_X$ is a finite sum $\sum a_m m$, $a_m \in A$, $m \in M_X$. The multiplication $Al_X \times Al_X \to Al_X$ extends A-linearly the multiplication $M_X \times M_X \to M_X$. The freeness property of Al_X is:

(14.4.4) Let B be an algebra over A and let $f\colon X \to B$ be a map. Then there is a unique map of A-algebras $\tilde{f}\colon Al_X \to B$ that extends f.

The length function on M_X defines a grading on Al_X making Al_X a graded algebra: $Al_X = \oplus_{n=1}^{\infty} Al_X^n$ where Al_X^n is the free module over $X_n \subset M_X$.

■ (14.4.5) **The free associative algebra** Ass_X An associative algebra over a ring A is an algebra B over A such that the multiplication $B \times B \to B$ is associative and such that there is a unit element in B. Let X be a set then the free associative algebra over A is defined as follows.

$A \oplus Al_X$ has a natural structure of a graded A-algebra with unit element. Let $J \subset A \oplus Al_X$ be the ideal of generated by all the elements $(ab)c - a(bc)$. Let $Ass_X = A \oplus Al_X/J$. There is a natural map $X \simeq X_1 \subset M_X \subset Al_X \subset A \oplus Al_X \to Ass_X$. The freeness property of Ass_X is now the obvious one:

(14.4.6) Let B be an associative algebra over A and let $f\colon X \to B$ be any map. Then there is a unique homomorphism of associative algebras $\tilde{f}\colon Ass_X \to B$ that extends f. The ideal J is a homogeneous ideal of the graded algebra $A \oplus Al_X$, so that Ass_X is a graded associative algebra $Ass_X = \oplus_{n=0}^{\infty} Ass_X^n$. A basis of the free A-module Ass_X^n is given by the associative (but noncommutative) words of length n in the elements of X. The associative algebra can be also be seen as the tensor algebra (cf. (14.3.3)) of the free A-module over X.

■ (14.4.7) **The free Lie algebra** L_X The free Lie algebra L_X over A on X is constructed as follows. Let $I \subset Al_X$ be the ideal generated by all elements of the form aa, $a \in Al_X$ and $a(bc) + b(ca) + c(ab) = J(a, b, c)$. We define $L_X = Al_X/I$. The freeness property of L_X is:

(14.4.8) Let L be a Lie algebra over A and $f\colon X \to L$ any map. Then there exists a unique morphism of A Lie algebras $\tilde{f}\colon L_X \to L$ that extends f.

The free Lie algebra L_X is also free as an A-module but is not of finite rank if X has two or more elements. We shall not use nor prove these facts; cf., e.g., [44, Chapter 2].

The ideal I is generated by homogeneous elements of the graded algebra Al_X so that L_X is a graded Lie algebra $L_X = \oplus_{n=1}^{\infty} L_X^n$.

■ (14.4.9) **Relation between L_X and Ass_X** Let $L(Ass_X)$ be the Lie algebra structure on Ass_X. (Cf. 14.3.) $X \to Ass_X$ then defines by (14.4.8) a Lie homomorphism $L_X \to Ass_X$ and hence by the universality property of UL_X a homomorphism of associative algebras Φ: $UL_X \to Ass_X$. We claim that Φ is an isomorphism. This is seen as follows. Ψ': $X \to L_X \to UL_X$ is a map of X into an associative algebra. Hence by (14.4.6) there is a unique homomorphism of associative algebras Ψ: $Ass_X \to UL_X$ extending Ψ'. An easy argument using the uniqueness parts of (14.3.2), (14.4.6), and (14.4.8) now proves that $\Psi\Phi$ and $\Phi\Psi$ are the identity homomorphisms.

■ (14.4.10) **Campbell–Hausdorff formula** Now suppose that A is a $\mathbf{Q}$-algebra. The associative algebra Ass_X on X comes equipped with a diagonal map $Ass_X \to Ass_X \otimes Ass_X$ defined by the map $X \to Ass_X \otimes Ass_X$, $x \mapsto x \otimes 1 + 1 \otimes x$. Under the identification $UL_X \xrightarrow{\sim} Ass_X$ this diagonal map coincides with the diagonal map Δ: $UL_X \to UL_X \otimes UL_X$ defined in 14.3. Because A is a $\mathbf{Q}$-algebra and therefore torsion free, this means by (14.3.9) that we can identify L_X with the set of primitive elements of Ass_X. This inclusion $L_X \subset Ass_X$ respects the grading, i.e., $L_X^n \subset Ass_X^n$.

The elements of Ass_X are noncommutative (but associative) polynomials in the elements of X. Let Ass_X^n be the free A-module generated by all words in the elements of X of length n. We define $\widehat{Ass}_X$ as $\prod_{n=0}^{\infty} Ass_X^n$, this is the completion of Ass_X with respect to the topology induced by the "degree of noncommutative polynomials." Let $\hat{L}_X$ be the closure of L_X in $\widehat{Ass}_X$. I.e., $\hat{L}_X = \prod_{n=1}^{\infty} L_X^n$. Define the completed tensor product $\widehat{Ass}_X \mathbin{\widehat{\otimes}} \widehat{Ass}_X$ as $\prod_{p,q=0}^{\infty} Ass_X^p \otimes Ass_X^q$. The diagonal morphism Δ: $Ass_X \to Ass_X \otimes Ass_X$ then extends to a diagonal morphism Δ: $\widehat{Ass}_X \to \widehat{Ass}_X \mathbin{\widehat{\otimes}} \widehat{Ass}_X$. We claim:

(14.4.11) The primitive elements of $\widehat{Ass}_X$ are precisely the elements of $\hat{L}_X$. This is proved as follows. Write $y \in \widehat{Ass}_X$ as an infinite sum $y = \sum_{n=0}^{\infty} y_n$ where y_n is homogeneous of degree n. Because Δ is homogeneous, we have $\Delta y = y \otimes 1 + 1 \otimes y$ if and only if $\Delta(y_n) = 1 \otimes y_n + y_n \otimes 1$ for all n. Now $y_n \in Ass_X$ for all n so that $y_n \in L_X$ for all n, hence $y \in \hat{L}_X$.

■ (14.4.12) Let $\hat{\mathfrak{m}}_X \subset \widehat{Ass}_X$ be the ideal generated by $X \subset \widehat{Ass}_X$. We define exp: $\hat{\mathfrak{m}}_X \to 1 + \hat{\mathfrak{m}}_X$ and log: $1 + \hat{\mathfrak{m}}_X \to \hat{\mathfrak{m}}_X$ by means of the usual formulas

$$\exp(y) = \sum_{n=0}^{\infty} \frac{y^n}{n!}, \qquad \log(1+y) = \sum_{n=1}^{\infty} (-1)^n \frac{y^n}{n}$$

Then one has $\exp(\log(1+y)) = 1 + y$ and $\log(\exp(y)) = y$, as usual. (These are formal identities.)

■ (14.4.13) **Lemma** The map exp induces a bijection from the set $\{y \in \hat{\mathfrak{m}}_X \mid \Delta y = y \otimes 1 + 1 \otimes y\}$ onto the set $\{z \in 1 + \hat{\mathfrak{m}}_X \mid \Delta z = z \otimes z\}$.

Proof Because Δ is continuous and an algebra homomorphism, it commutes with exp. Therefore, if $y \in \hat{\mathfrak{m}}_X$ and $\Delta y = y \otimes 1 + 1 \otimes y$, we have

$$\begin{aligned}\Delta(\exp(y)) &= \exp(\Delta y) = \exp(1 \otimes y + y \otimes 1) \\ &= \exp(1 \otimes y)\exp(y \otimes 1) = \exp(y) \otimes \exp(y)\end{aligned}$$

because $1 \otimes y$ and $y \otimes 1$ commute with one another.

■ (14.4.14) **Theorem** (Campbell–Hausdorff) Let $X = \{x, y\}$ be a set with two (different) letters. Then there is a $z \in \hat{L}_X$ such that $\exp(x)\exp(y) = \exp(z)$.

Proof Because $\exp(x), \exp(y) \in 1 + \hat{\mathfrak{m}}_X$ we have $\exp(x)\exp(y) \in 1 + \hat{\mathfrak{m}}_X$ so that by (14.2.12) there is a unique $z \in \hat{\mathfrak{m}}_X$ such that $\exp(z) = \exp(x)\exp(y)$. Now Δ is a homomorphism of associative algebras and $x, y \in X \subset L_X$ so that by (14.4.13)

$$\begin{aligned}\Delta(\exp(x)(\exp(y)) &= \Delta(\exp(x))\,\Delta(\exp(y)) \\ &= (\exp(x) \otimes \exp(x))(\exp(y) \otimes \exp(y)) \\ &= \exp(z) \otimes \exp(z),\end{aligned}$$

so again by (14.4.13) $z \in \hat{L}_X$.

It is not difficult to calculate the first few terms of $z \in \hat{L}_X$ explicitly. One finds

$$\begin{aligned}(14.4.15)\qquad z = z(x, y) \equiv x + y + \tfrac{1}{2}[x, y] + \tfrac{1}{12}[x, [x, y]] \\ + \tfrac{1}{12}[y, [y, x]] \mod(\text{degree } 4)\end{aligned}$$

Note also that

$$(14.4.16)\quad z(x, 0) = x, \qquad z(0, y) = y, \qquad z(z(x, w), y) = z(x, z(w, y))$$

14.5 Proof of the formal version of Lie's third theorem

We are now in a position to prove part of Theorem (14.2.3), viz., statement (14.2.5): let A be a $\mathbf{Q}$-algebra, $L \in \mathbf{LA}_A$, then there is an $F(X, Y) \in \mathbf{FG}_A$ such that $L(F)$ is isomorphic to L.

The proof goes in several steps. First let $x_1, \ldots, x_n$ be a basis for L (over A). The bracket multiplication is then given by "structure constants"

$$(14.5.1)\qquad [x_i, x_j] = \sum_{k=1}^{n} c_{ij}^k x_k, \qquad c_{ij}^k \in A$$

Now let $E = A[\![X, Y]\!]^n$ and let $(f_i), (g_i)$ be elements of E. We can use (14.5.1) to define a bracket multiplication on E as

$$(14.5.2)\qquad [(f_i), (g_i)] = \left(\left(\sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^k f_i g_j\right)_k\right)$$

We also use E to denote this Lie algebra; E is so to speak the Lie algebra $L \otimes A[\![X, Y]\!]$ over $A[\![X, Y]\!]$ obtained by extending the scalars from A to $A[\![X, Y]\!]$. An element $(f_i) \in E$ is said to be homogeneous of degree m if each f_i is a homogeneous polynomial (in $X_1, \ldots, X_n, Y_1, \ldots, Y_n$) of degree m. As usual we write X for $(X_i) \in E$ and Y for $(Y_i) \in E$.

■ (14.5.3) **Lemma** If $(f_i) \in E$ is homogeneous of degree m, then $[X, (f_i)]$ and $[Y, (f_i)]$ are homogeneous of degree $m + 1$.

This is immediately obvious from (14.5.2). Now consider the free Lie algebra L_S on the two element set $S = \{u, v\}$ and its completion $\hat{L}_S$; cf. (14.4.10) above.

Let $\phi\colon L_S \to E$ be the Lie algebra homomorphism defined by $u \mapsto X$, $v \mapsto Y$. We then have

■ (14.5.4) **Lemma** For all $m \in \mathbf{N}$, $\phi(L_S^m) \subset \mathfrak{m}^m E$ where $\mathfrak{m}$ is the maximal ideal of $A[\![X, Y]\!]$.

This follows immediately from Lemma (14.5.3).

Lemma (14.5.4) implies that ϕ extends (uniquely) to a Lie algebra homomorphism $\phi\colon \hat{L}_S \to E$. Now let $z \in \hat{L}_S$ be the unique element such that $\exp(z) = \exp(u)\exp(v)$ (cf. (14.4.14)) and let $F(X, Y) \in E = A[\![X, Y]\!]^n$ be the element $\phi(z)$. Then because $z \equiv u + v + \frac{1}{2}[u, v]$ mod(degree 3) (cf. (14.4.15)) we have (using (14.5.4))

$$F(X, Y) \equiv X + Y + \tfrac{1}{2}[X, Y] \quad \text{mod(degree 3)} \tag{14.5.5}$$

and (14.4.16) implies that $F(X, Y)$ is associative, so that $F(X, Y)$ is a formal group law of dimension n over A such that the degree two part of $F(X, Y)$ is equal to

$$(\tfrac{1}{2}[X, Y])_i = \left(\tfrac{1}{2}\sum_{j=1}^{n}\sum_{k=1}^{n} c_{jk}^i X_j X_k\right)_i \tag{14.5.6}$$

Using $c_{jk}^i = -c_{kj}^i$ we see that the Lie algebra of $F(X, Y)$ is indeed $\mathfrak{g}$; cf. (14.1.1), (14.1.2), (14.5.1), (14.5.2). This concludes the proof of the formal version of Lie's third theorem.

■ (14.5.7) **Remark** If $A = \mathbf{R}$, $\mathbf{C}$, or a nonarchimedean characteristic zero field, then one can show that the power series $F(X, Y)$ actually converge for small enough X, Y. Thus one obtains a "Lie group chunk" from which a full simply connected analytic Lie group with the given Lie algebra as Lie algebra can be obtained; cf. [363] for more details.

E.1 Bibliographical and Other Notes

(E.1.1) **Historical note on formal groups** Formal group laws were first defined by Bochner [40], who used them to separate, so to speak, Lie theory into a "formal"

part and a "convergence" part, thus making the classical proofs more lucid. Of course the formal part of the theory worked over any field of characteristic zero.

The study of formal group laws in characteristic $p > 0$ began in the early 1950s when the work of Chevalley [75] showed that the correspondence Lie algebras–Lie groups breaks down completely in characteristic $p > 0$. Thus the search for a good substitute for the Lie algebra of an algebraic group was on.

Now of course in characteristic zero the formal group law of an analytic group is an intermediate object between the Lie algebra and the analytic group itself, and so is the universal enveloping algebra of the Lie algebra. Guided by this (cf. the introduction of [114]) and using another intermediate notion peculiar to characteristic $p > 0$: left invariant semiderivations (cf. [99]), Dieudonné tackled the question systematically and by 1958, when the last of his formidable series of papers [102–109, 100, 101, 110–113] appeared, he had created a full-fledged theory of formal groups from the hyperalgebra point of view, which is and was of considerable importance in algebraic geometry, not least because the Dieudonné modules which turned up in the classification results turned out to be an exceedingly important and versatile kind of objects.

Meanwhile at about the same time (somewhat later) Lazard [250, 251, 252] started studying formal groups from the formal power series point of view, relying heavily on some quite tough computations. Among the results he obtained are Theorem (1.6.3) (= (5.7.4)): group law chunks can be extended), the comparison lemma (1.6.6) (= (5.7.5)), and the theorem that one dimensional formal group laws over a ring without nilpotents are commutative (cf. Theorem (1.6.7); the strengthened version (1.6.7) is due to Connell [79]). Even more important was Lazard's result that the ring over which a universal formal group law is defined is free polynomial. But it took quite a while before this last result was appreciated and used (cf. in this connection the last lines of the introduction of [277]). There is, therefore, something pleasing about the fact that some of the more recent applications of the theory of formal groups (notably to complex cobordism theory) are applications of formal group *laws* and various kinds of universal formal group laws rather than applications of formal groups.

(E.1.2) **On the origins of the functional equation lemma** The functional equation lemma (10.2 and 2.2) as stated here has not appeared in print before. It has two immediate precursors however. These are:

(i) The case K a discrete valuation field of characteristic zero, A its ring of integers, k its residue field of characteristic $p > 0$, and $\sigma\colon K \to K$ an endomorphism such that $\sigma(a) \equiv a^q \bmod(\pi A)$ for all $a \in A$. This case is essentially contained in Honda [189], albeit only for special power series $g(X)$, $h(X)$, $\bar{g}(X)$, $\bar{h}(X)$. In particular parts (i), (ii) of the functional equation lemma correspond to Theorem 2 of [189]; Proposition 2.5 more or less corresponds to part (iii); and part (iv) corresponds to Lemmas 4.1 and 4.2 of [189]. (Cf. Section 20.3 below for details on the noncommutative power series calculation methods that Honda developed in this connection.)

(ii) The case $K = \mathbf{Q}[U]$, $A = \mathbf{Z}[U]$, $\sigma\colon U_i \mapsto U_i^p$; cf. the author's papers [170, 171, 173]; and a generalization in [177].

These two precursors of the functional equation lemma were found independently. The simplest example of a functional equation logarithm of type (i) is

$$X + \pi^{-1}X^q + \pi^{-2}X^{q^2} + \cdots$$

(and this particular logarithm of a Lubin–Tate formal group law already appears in [188]; cf. in this connection also the introduction of [72]). The simplest example of a functional equation logarithm of type (ii) is

$$X + \frac{T}{p}X^q + \frac{TT^q}{p^2}X^{q^2} + \frac{TT^qT^{q^2}}{p^3}X^{q^3} + \cdots$$

an example which dates from December 1969/January 1970 (Moscow). There is a somewhat disturbing similarity yet dissimilarity about these examples.

Given the functional equation lemma as stated above in 2.2 and 10.2 one recognizes more precursors (all for the case $s_2 = s_3 = \cdots = 0$), viz. Dieudonné's Proposition 1 in [113], Dwork's Lemma 1 in [137], a lemma of Cartier [68] which we shall meet in (17.6.1) (these three are very closely related), and also of course the various integrality statements concerning the Witt vectors which all come from the functional equation type relation

$$w_{pn}(X) \equiv w_n(X^p) \bmod p^{v_p(pn)}$$

or, better,

$$(pn)^{-1}w_{pn}(X) \equiv p^{-1}(n^{-1}w_n(X^p)) \bmod (\mathbf{Z}_{(p)}[X])$$

(E.1.3) **Note on the universal formal group law theorems** As we remarked before the important theorem that the ring over which a universal formal group is defined is free polynomial is due to Lazard. He first proved the comparison lemma (cocycle lemma; (5.7.5) and (11.4.12)) and then with this as his main tool constructed the universal formal group laws by successive approximation by taking in each degree the generic extension.

The proof of universality which we have given comes from [170, 171, 173] and is an adaption to the algebraic and higher dimensional case of a proof of Buhštaber and Novikov of the universality of the formal group law of complex cobordism [58] (with the missing binomial coefficient lemma filled in).

In both cases this method works essentially because one has a good candidate for a universal formal group law which has already been proved to be integral.

In turn, this bit of binomial coefficient arithmetic which is needed (Section 4 above) is the core of Fröhlich's more conceptual proof [144] of Lazards comparison lemma (one dimensional case). Lazard's original proof of the comparison lemma was exceedingly tough and computational, even in the one dimensional case; and in the higher dimensional case the combinatorial difficulties were severe enough that the present author for instance never quite managed to read the paper in question [252] entirely. Recently using curvilinear coordinates (cf. also Section 12 above) Lazard essentially reduced the higher dimensional comparison lemma to the one dimensional case; cf. [254, 256]; cf. also [255].

The various explicit universal formal group laws $F_V(X, Y)$, $F_{V,T}(X, Y)$, $F_S(X, Y)$, $F_R(X, Y)$, $H_U(X, Y)$ first appeared in [170, 171, 173, 178].

(E.1.4) **Note on generalizations** When studying formal groups from the hyperalgebra point of view, there is no a priori reason to limit oneself to smooth ones; and thus, e.g., finite group schemes creep easily in. Conversely, a formal group law of finite height can be seen as an inductive limit of finite ones; cf. also E.4.1(d) below. See

Chapter VII below for some material on these more general formal groups; see also Appendix B.2 (p-divisible groups). Finally, [257] contains some preliminaries on formal group *laws* from a more general point of view than (truncated power series) algebras.

(E.1.5) **Notes on Sections 5.8 and 6** The theorem that a formal group law over a ring without nilpotents is commutative is due to Lazard [250]. A proof via hyperalgebra methods was given by Dieudonné [112]. The strengthened form, Theorem 6.1, is due to Connell [79]. The proof follows Serre [366], and I have also made use of [69]. The proof over a characteristic zero ring of section 5.8 is, as was mentioned in the text, due to Honda [188, 189].

(E.1.6) **Notes on Section 8** The fundamental Lemma (8.1.2), Theorem (8.1.5), and Proposition (8.3.9) are all due to Lubin and Tate [264].

(E.1.7) **Notes on Section 12** The notion of a curvilinear formal group law is due to Lazard [256]. The explicit universal curvilinear formal group law $F_R(X, Y)$ first appeared in [173].

(E.1.8) **Notes on Section 13** Generalized Lubin–Tate formal group laws were defined by Cartier in [63] (cf. also [72]) using curves. Koch in [226] defined higher dimensional formal Lubin–Tate formal group laws and used them to give some (counter) examples concerning the relation between finite height formal group laws and p-divisible groups. The higher dimensional Honda formal group laws were constructed first in [189].

(E.1.9) **Notes on Section 14** For Section 14 (formal Lie theory), I have made use of Fröhlich [144], Bourbaki [44], and especially Serre [363].

(E.1.10) **Note on logarithms** The existence and uniqueness of logarithms of commutative formal group laws is an immediate consequence of the comparison lemma and is due to Lazard, [251, 252]. I know of no printed reference for formulas (5.4.6) and (11.1.7), except the closely related formula on page 168 of [404]. But of course (5.4.6) and (11.1.7) are known. The author heard about them from J. Lubin.

CHAPTER III

CURVES, p-TYPICAL FORMAL GROUP LAWS, AND LOTS OF WITT VECTORS

In this chapter all formal group laws will be commutative formal group laws over a ring A, unless noncommutativity is expressly specified.

15 Definitions. Survey of Results

15.1 Curves

Let $F(X, Y)$ be an n-dimensional (commutative) formal group law over a ring A. A *curve* in $F(X, Y)$ is simply an n-tuple of power series $\gamma(t)$ in one variable t with coefficients in A and without constant term, i.e., $\gamma(0) = 0$. As was remarked in 1.4 and 9.3 one can use the "group recipe" $F(X, Y)$ to define an addition of curves

$$\gamma_1(t) +_F \gamma_2(t) = F(\gamma_1(t), \gamma_2(t)) \tag{15.1.1}$$

The resulting ordinary group is denoted $\mathscr{C}(F)$, or $\mathscr{C}(F; A)$ if we want to stress that we are considering curves with coefficients in A; it is of course a commutative group if F is commutative as we shall assume from now on.

The group $\mathscr{C}(F)$ admits a number of operators $\mathbf{V}_m$, $\mathbf{f}_m$, $\langle a \rangle$, $m \in \mathbf{N}$, $a \in A$. The words attached to the $\mathbf{V}_m$, $\mathbf{f}_m$, and $\langle a \rangle$ are respectively Verschiebung operators, Frobenius operators, and homothety operators. These are defined as

$$\mathbf{V}_m\gamma(t) = \gamma(t^m) \tag{15.1.2}$$

$$\langle a \rangle\gamma(t) = \gamma(at) \tag{15.1.3}$$

These two definitions do not involve the group law $F(X, Y)$. The definition of the $\mathbf{f}_m$ is slightly more involved. Choose additional variables $Z_1, \ldots, Z_m$. We write

$$\gamma(Z_1 t^{1/m}) +_F \gamma(Z_2 t^{1/m}) +_F \cdots +_F \gamma(Z_m t^{1/m}) = \beta(Z_1, \ldots, Z_m; t^{1/m}) \tag{15.1.4}$$

This is a power series in $t^{1/m}$ with coefficients in $A[Z_1, \ldots, Z_m]$. Because $F(X, Y)$ is commutative and associative, we see from (15.1.4) that the

coefficients of $t^{i/m}$ in (15.1.4) are homogeneous symmetric polynomials in the $Z_1, \ldots, Z_m$ of degree i. This means that we can write

$$\beta(Z_1, \ldots, Z_m; t^{1/m}) = \beta'(\sigma_1, \ldots, \sigma_m; t^{1/m}) \tag{15.1.5}$$

where $\sigma_1, \ldots, \sigma_m$ are the elementary symmetric polynomials in the $Z_1, \ldots, Z_m$. Now substitute $\sigma_1 = \cdots = \sigma_{m-1} = 0$, $\sigma_m = (-1)^{m-1}$ in $\beta'(\sigma_1, \ldots, \sigma_m; t^{1/m})$. Because the coefficient of $t^{i/m}$ is homogeneous of degree i and σ_j has weight j, we see that $\beta'(0, \ldots, 0, (-1)^{m-1}; t^{1/m})$ is in fact a power series in t (and not just a power series in $t^{1/m}$). We now define

$$\mathbf{f}_m\gamma(t) = \beta'(0, 0, \ldots, 0, (-1)^{m-1}; t^{1/m}) \tag{15.1.6}$$

Formally one can write

$$\mathbf{f}_m\gamma(t) = \gamma(\zeta_m t^{1/m}) +_F \gamma(\zeta_m^2 t^{1/m}) +_F \cdots +_F \gamma(\zeta_m^m t^{1/m}) \tag{15.1.7}$$

where ζ_m is a primitive mth root of unity; and if the ring A is such that it makes sense to talk about the m (different) mth roots of unity over A, then (15.1.7) is a perfectly good definition of $\mathbf{f}_m$.

There are a number of relations among the operators $\mathbf{V}_m$, $\mathbf{f}_n$, $\langle a \rangle$ which we shall describe and prove later; see 16.2. The only one that we need for the moment is

$$\mathbf{f}_k\mathbf{V}_m = \mathbf{V}_m\mathbf{f}_k \qquad \text{if} \quad (k, m) = 1 \tag{15.1.8}$$

To prove this relation and also several others the following is often useful. Suppose that A is a characteristic zero ring; i.e., that $A \to A \otimes \mathbf{Q}$ is injective. Let $f(X)$ be the logarithm of $F(X, Y)$, and let $\gamma(t) \in \mathscr{C}(F; A)$ be a curve. Then we have

$$f(\gamma(t)) = \sum_{i=1}^{\infty} x_i t^i \quad \Rightarrow \quad f(\mathbf{f}_m\gamma(t)) = \sum_{i=1}^{\infty} m x_{mi} t^i \tag{15.1.9}$$

Indeed, we have

$$\begin{aligned} f(\mathbf{f}_m\gamma(t)) &= f(\gamma(\zeta_m t^{1/m}) +_F \cdots +_F \gamma(\zeta_m^m t^{1/m})) \\ &= f(\gamma(\zeta_m t^{1/m})) + \cdots + f(\gamma(\zeta_m^m t^{1/m})) \\ &= \sum_{i=1}^{\infty} \sum_{j=1}^{m} x_i(\zeta_m^{ij}) t^{i/m} \\ &= \sum_{m|i} m x_i t^{i/m} = \sum_{i=1}^{\infty} m x_{im} t^i \end{aligned}$$

15.2 p-typical formal group laws

Choose a prime number p.

Let $F_V(X, Y)$ over $\mathbf{Z}[V]$ be the m-dimensional formal group law constructed

in Section 3 (in case $m = 1$) and Section 10 (for all $m \in \mathbf{N}$). Recall that $F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y))$ where $f_V(X) = \sum_{n=1}^{\infty} a_n(V)X^{p^n}$ with

$$X^{p^n} = (X_1^{p^n}, \ldots, X_m^{p^n})$$

and the $a_n(V)$ are $m \times m$ matrices with coefficients in $\mathbf{Q}[V]$ that satisfy $pa_n(V) = a_{n-1}(V)V_1^{(p^{n-1})} + \cdots + a_1(V)V_{n-1}^{(p)} + V_n$; cf. 10.3. Note in particular that $f_V(X) = \log_{F_V}(X)$ has the very special property that the coefficients of all monomials $X^{\mathbf{n}}$ are zero except possibly for $\mathbf{n} = p^r\mathbf{e}(i)$, $r \in \mathbf{N} \cup \{0\}$, $i \in \{1, \ldots, m\}$. Such formal group laws will be called p-typical formal group laws.

More precisely, we define:

■ (15.2.1) **Definition** A formal group law $F(X, Y)$ over a ring A is called *p-typical* if and only if there exists a homomorphism $\phi\colon \mathbf{Z}[V] \to A$ such that $\phi_* F_V(X, Y) = F(X, Y)$.

This, of course, is not a very nice or operational definition. Much more useful is the criterion (15.2.3) below. To formulate it we need one more definition

■ (15.2.2) **Definition** A curve $\gamma(t)$ in a formal group law $F(X, Y)$ is called p-typical if and only if $\mathbf{f}_q\gamma(t) = 0$ for all prime numbers $q \neq p$.

■ (15.2.3) **Theorem** (criterion for p-typicality) Let A be a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra and $F(X, Y)$ an m-dimensional formal group law over A. Then $F(X, Y)$ is p-typical if and only if all the curves $\gamma(t) = (t^{p^{r_1}}, t^{p^{r_2}}, \ldots, t^{p^{r_m}})$, $r_i \in \mathbf{N} \cup \{0\}$, $i = 1, \ldots, m$, are p-typical. In particular, if $m = 1$, a formal group law $F(X, Y)$ over such a ring A is p-typical if and only if the curve $\gamma(t) = t$ is p-typical.

The last statement of (15.2.3) follows from the earlier parts of (15.2.3) because of (15.1.8). (More generally, the criterion (15.2.3) holds if A has no q-torsion for all prime numbers q different from p; e.g., the ring $A = \mathbf{Z}[X]/(pX)$ is of this type but is not a characteristic zero ring nor a $\mathbf{Z}_{(p)}$-algebra.)

In the case of a characteristic zero ring we can characterize p-typicality in terms of logarithms as follows.

■ (15.2.4) **Proposition** Let $\gamma(t)$ be a curve in an m-dimensional formal group law $F(X, Y)$ over a characteristic zero ring A. Then $\gamma(t)$ is p-typical if and only if $\log_F(\gamma(t))$ is of the form

$$\log_F(\gamma(t)) = \sum_{n=0}^{\infty} a_n t^{p^n} \tag{15.2.5}$$

where the a_n are m-vectors with coordinates in $A \otimes \mathbf{Q}$.

■ (15.2.6) **Proposition** An m-dimensional formal group law $F(X, Y)$ over a characteristic zero ring A is p-typical if and only if $\log_F(X)$ is of the form

$$\log_F(X) = \sum_{n=0}^{\infty} a_n X^{p^n} \tag{15.2.7}$$

where the a_n are $m \times m$ matrices with coordinates in $A \otimes \mathbf{Q}$ and $X^{p^n} = (X_1^{p^n}, \ldots, X_m^{p^n})$ as usual.

Given the definition of p-typical, the following proposition should come as no surprise.

■ (15.2.8) **Proposition** The m-dimensional formal group law $F_V(X, Y)$ is p-typical and is universal for p-typical formal group laws of dimension m.

That is, for every p-typical m-dimensional formal group law over a ring A, there is a unique homomorphism ϕ: $\mathbf{Z}[V] \to A$ such that $\phi_* F_V(X, Y) = F(X, Y)$. Indeed, given Definition (15.2.1) the only thing to prove is that ϕ is unique, which is not difficult. In spite of its apparent triviality the universality of $F_V(X, Y)$ will be extremely useful. The reason lies of course in Theorem (15.2.3) and Proposition (15.2.6) and also in

■ (15.2.9) **Theorem** Every formal group law over a $\mathbf{Z}_{(p)}$-algebra A is strictly isomorphic over A to a p-typical formal group law over A.

15.3 Witt vectors and Artin-Hasse exponentials

In this subsection $F(X, Y)$ is a one dimensional formal group law over a characteristic zero ring A. Let $\log_F(X)$ be given by

$$\log_F(X) = \sum_{i=1}^{\infty} a_i X^i, \qquad a_1 = 1, \quad a_i \in A \otimes \mathbf{Q} \tag{15.3.1}$$

We now define polynomials $\bar{w}_n^F(Z)$ in $Z_1, \ldots, Z_n$ as

$$\bar{w}_n^F(Z) = \sum_{d|n} a_{n/d} Z_d^{n/d} \tag{15.3.2}$$

For example, we can take $F(X, Y) = F_{\Delta_1}(X, Y)$ over $\mathbf{Z}$; cf. 3.2. This formal group has the power series

$$X + p^{-1}X^p + p^{-2}X^{p^2} + \cdots$$

for its logarithm. The polynomials $n\bar{w}_n^F(Z)$ for $n = 1, p, p^2, p^3, \ldots$ then become respectively

$$Z_1, \qquad Z_1^p + pZ_p, \qquad Z_1^{p^2} + pZ_p^p + p^2 Z_{p^2}, \qquad \ldots$$

Writing Y_i for Z_{p^i}, $i = 0, 1, 2, \ldots$, these become

$$Y_0, \quad Y_0^p + pY_1, \quad Y_0^{p^2} + pY_1^p + p^2 Y_2, \quad Y_0^{p^3} + pY_1^{p^2} + p^2 Y_2^p + p^3 Y_3, \quad \ldots$$

which are the familiar Witt polynomials that one uses to define the ring of Witt vectors associated to the prime number p.

Now take $F(X, Y) = \hat{G}_m^-(X, Y) = X + Y - XY$. The logarithm of this formal group law is

$$X + \frac{X^2}{2} + \frac{X^3}{3} + \frac{X^4}{4} + \cdots$$

so that its associated polynomials

$$n\bar{w}_n^{\hat{G}_m^-}(Z_1, Z_2, \ldots, Z_n) = w_n(Z_1, \ldots, Z_n) = \sum_{d|n} dZ_d^{n/d} \tag{15.3.3}$$

are the polynomials underlying the definition of the (generalized) ring of Witt vectors for all prime numbers simultaneously; cf. [308, Lecture 26; 64].

Now let $F(X, Y)$ be again an arbitrary one dimensional formal group over a characteristic zero ring A. We define polynomials $\Sigma_n^F(x_1, \ldots, x_n; y_1, \ldots, y_n)$ by the conditions

$$\bar{w}_n^F(\Sigma_1^F(x; y), \ldots, \Sigma_n^F(x; y)) = \bar{w}_n^F(x) + \bar{w}_n^F(y) \tag{15.3.4}$$

■ (15.3.5) **Lemma** The $\Sigma_n^F(x; y)$ are polynomials with their coefficients in A (not just $A \otimes \mathbf{Q}$).

We can therefore use the $\Sigma_n^F(x; y)$ to define a new addition on the set of vectors of infinite length with coordinates in A as follows:

$$(a_1, a_2, a_3, \ldots) +_{W^F(A)} (b_1, b_2, \ldots) = (\Sigma_1^F(a; b), \Sigma_2^F(a; b), \ldots)$$

This defines an abelian group which we shall denote $W^F(A)$. We define a (reduced) Artin–Hasse type exponential mapping associated to the formal group $F(X, Y)$ by the formula

$$\bar{E}^F(x, t) = \log_F^{-1}\left(\sum_{n=1}^{\infty} \bar{w}_n^F(x)t^n\right) \tag{15.3.6}$$

where x is short for $(x_1, x_2, \ldots)$. $\bar{E}^F(x, t)$ is a power series in t with coefficients in $A \otimes \mathbf{Q}[x_1, x_2, \ldots]$.

■ (15.3.7) **Lemma** $\bar{E}^F(x, t)$ is a power series in t with coefficients in $A[x_1, x_2, \ldots]$.

■ (15.3.8) **Proposition** $a = (a_1, a_2, \ldots) \mapsto \bar{E}^F(a, t)$ defines an isomorphism of abelian groups $W^F(A) \to \mathscr{C}(F; A)$.

In particular, we see that we can view the abelian group $\mathscr{C}(\hat{G}_m^-; A)$ (where $\hat{G}_m^-(X, Y) = X + Y - XY$) as the abelian group underlying the ring of generalized Witt vectors $W(A)$.

Section 17 below is concerned with a detailed study of the ring functor W

and various quotient functors like $W_{p^\infty}(A)$, the ring of Witt vectors of infinite length associated to the prime number p. We pay particular attention to the Artin–Hasse exponential map which can be seen as a multiplication preserving, additive morphism of functors

$$W_{p^\infty}(A) \to W(W_{p^\infty}(A))$$

(This is not however a functor homomorphism of ring functors since it does not preserve unit elements.) This Artin–Hasse exponential map is but one of a whole family of transformations of which the nicest one is a functor homomorphism of ring-valued functors

$$\Delta_A\colon W(A) \to W(W(A))$$

A precise and characterizing definition of W and Δ are given by the theorem:

■ (15.3.9) **Theorem** There is a unique functor W: **Ring** $\to$ **Ring** which satisfies the following properties: (i) as a functor **Ring** $\to$ **Set**, W satisfies $W(A) = \{(a_1, a_2, a_3, \ldots) \mid a_i \in A\}$ and $W(\phi)(a_1, a_2, \ldots) = (\phi(a_1), \phi(a_2), \ldots)$ for a ring homomorphism $\phi\colon A \to B$; (ii) $w_{n,A}\colon W(A) \to A$ is a (functorial) homomorphism of rings for every A and $n \in \mathbf{N}$.

The functor W: **Ring** $\to$ **Ring** admits functorial ring endomorphisms $\mathbf{f}_n$: $W \to W$ for every $n \in \mathbf{N}$ that are uniquely characterized by the property $w_m \mathbf{f}_n = w_{nm}$ for every $m \in \mathbf{N}$.

Finally, there is a functorial homomorphism $\Delta\colon W(-) \to W(W(-))$ that is uniquely characterized by the property $w_{n,W(A)}\Delta_A = \mathbf{f}_{n,A}$ for all $n \in \mathbf{N}$ and $A \in$ **Ring**.

The "one prime number version" of Theorem (15.3.9) is

■ (15.3.10) **Theorem** There is a unique functor W_{p^∞}: **Ring** $\to$ **Ring** that satisfies the following properties: (i) as a functor **Ring** $\to$ **Set**, W_{p^∞} satisfies $W_{p^\infty}(A) = \{(a_0, a_1, \ldots) \mid a_i \in A\}$ and $W_{p^\infty}(\phi)(a_0, a_1, a_2, \ldots) = (\phi(a_0), \phi(a_1), \ldots)$ for a ring homomorphism $\phi\colon A \to B$; (ii) for every $n \in \mathbf{N} \cup \{0\}$, $w_{p^n,A}$: $W_{p^\infty}(A) \to A$ is a functorial homomorphism of rings, where $w_{p^n,A}(a_0, a_1, a_2, \ldots) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$; i.e., we have silently written $(a_0, a_1, \ldots)$ instead of $(a_{p0}, a_{p1}, \ldots)$.

The functor $W_{p^\infty} \to W_{p^\infty}$ admits a functorial ring homomorphism $\mathbf{f}_p$: $W_{p^\infty} \to W_{p^\infty}$ that is uniquely characterized by the property $w_{p^n}\mathbf{f}_p = w_{p^{n+1}}$ for every $n \in \mathbf{N} \cup \{0\}$.

Finally, there is functorial homomorphism $\Delta_{p^\infty,p^\infty}\colon W_{p^\infty}(-) \to W_{p^\infty}(W_{p^\infty}(-))$, characterized by $w_{p^n}\Delta_{p^\infty,p^\infty} = \mathbf{f}_p^n$ for all $n \in \mathbf{N} \cup \{0\}$.

The connections between $W(-)$, $W_{p^\infty}(-)$, Δ, $\Delta_{p^\infty,p^\infty}$ and the "Artin–Hasse" map $W_{p^\infty}(A) \to W(W_{p^\infty}(A))$ are given by

■ (15.3.11) **Theorem**

(i) ε_p: $(a_1, a_2, \dots) \to (a_{p^0}, a_{p^1}, a_{p^2}, \dots)$ defines a homomorphism of ring valued functors $W(-) \to W_{p^\infty}(-)$, and the following diagram of homomorphisms of ring valued functors is commutative:

$$\begin{array}{ccc} W(A) & \xrightarrow{\Delta_A} & W(W(A)) \\ \| & & \downarrow{\scriptstyle \varepsilon_{p,W(A)}} \\ W(A) & \longrightarrow & W_{p^\infty}(W(A)) \\ \downarrow{\scriptstyle \varepsilon_{p,A}} & & \downarrow{\scriptstyle W_{p^\infty}(\varepsilon_{p,A})} \\ W_{p^\infty}(A) & \xrightarrow{\Delta_{p^\infty,A,p^\infty}} & W_{p^\infty}(W_{p^\infty}(A)) \end{array}$$

where the middle horizontal arrow is simply defined as the composite $\varepsilon_{p,W(A)}\Delta_A$.

(ii) There is a multiplication preserving additive morphism E'_p: $W_{p^\infty}(-) \to W(W_{p^\infty}(-))$ between the ring-valued functors $W_{p^\infty}(-)$, $W(W_{p^\infty}(-))$ considered as functors $\mathbf{Alg}_p \to \mathbf{Ring}$ characterized by $w_n E'_p = 0$ if n is not a power of p and $w_{p^r} E'_p = \mathbf{f}_p^r$ for all $r \in \mathbf{N} \cup \{0\}$. Of the two diagrams of functor morphisms below the right one is commutative and the left one is *not*:

$$\begin{array}{ccc} W(A) & \xrightarrow{\Delta_A} & W(W(A)) \\ \downarrow{\scriptstyle \varepsilon_{p,A}} & & \downarrow{\scriptstyle W(\varepsilon_{p,A})} \\ W_{p^\infty}(A) & \xrightarrow{E'_{A,p}} & W(W_{p^\infty}(A)) \end{array} \qquad \begin{array}{ccc} W_{p^\infty}(A) & \xrightarrow{E'_{A,p}} & W(W_{p^\infty}(A)) \\ \downarrow & & \downarrow{\scriptstyle \varepsilon_{p,W_{p^\infty}(A)}} \\ W_{p^\infty}(A) & \xrightarrow{\Delta_{p^\infty,A,p^\infty}} & W_{p^\infty}(W_{p^\infty}(A)) \end{array}$$

The functor morphism $E'_{A,p}$ is a functor morphism of group-valued functors and also preserves multiplication; it does not preserve unit elements, however, and therefore (just barely) misses being a functor homomorphism of ring-valued functors.

Of course, classically the Artin–Hasse map maps $W_{p^\infty}(A)$ into $\Lambda(W_{p^\infty}(A))$ where for $B \in \mathbf{Ring}$, $\Lambda(B)$ is the group of all power series $1 + b_1 t + b_2 t^2 + \cdots$, $b_i \in B$ under multiplication of power series. One has

■ (15.3.12) **Proposition** The maps $(a_1, a_2, a_3, \dots) \to \prod_{i=1}^{\infty} (1 - a_i t^i)$ define an isomorphism of group-valued functors $\bar{E}$: $W(-) \to \Lambda(-)$.

Composing $E'_{A,p}$ with $\bar{E}_{W_{p^\infty}(A)}$, one obtains a morphism of functors $E_{A,p}$: $W_{p^\infty}(A) \to \Lambda(W_{p^\infty}(A))$ which in the case of a perfect field of characteristic p coincides with the Artin–Hasse exponential map as defined, e.g., in [11, 162, 438].

The proof of these theorems and various related facts is the subject matter of Section 17.

All this generalizes to a considerable extent. True, it is a fairly rare phenomenon that the group of curves $\mathscr{C}(F; -)$ admits a functorial nontrivial ring structure (compatible with the $c_n \bar{w}_{n,F}$ for suitable constants c_n). Still there are quite a number of formal group laws for which the group of curves and/or selected subgroups such as the group of p-typical curves admit a natural Witt-vector-like ring structure. Among these are the (local) Lubin–Tate formal

group laws defined over the ring of integers A of a complete local field with finite residue field k of q elements. The "q-typical" curves of such a formal group F have a natural ring structure, and in fact $\mathscr{C}_q(F; k)$ is isomorphic to A itself. One could speak of "ramified Witt vectors." There are also, so to speak, global Lubin–Tate formal group laws defined over the rings of integers A of global fields K. In this case one even has Artin–Hasse-like maps $A_v \to \mathscr{C}(F; A_v)$ for all discrete valuations v where A_v is the discrete complete valuation ring attached to the valuation v. And if the class number of K is 1, there even exists an Artin–Hasse-like functorial homomorphism of ring functors $\Delta^F: \mathscr{C}(F; -) \to \mathscr{C}(F; \mathscr{C}(F; -))$ of which $\Delta: W(-) \to W(W(-))$ is the special case $F = \hat{\mathbf{G}}_m^-$.

The proofs of all this rely heavily on the functional equation lemma and give in the case of $F = \hat{\mathbf{G}}_m^-$ new proofs of, e.g., Theorems (15.3.9)–(15.3.11). These generalizations thus make Section 17 largely superfluous. Still Witt vectors are of such importance that a double treatment is amply justified. And also, to do all these generalizations, it is convenient to have some more technical tools available, especially concerning "formal A-modules" and the classification of one dimensional formal group laws over finite fields. This is the reason that the treatment of the general results indicated above and also of (15.3.5)–(15.3.8) is postponed until Chapter IV.

15.4 $W_{p^\infty}(\mathbf{Z}_p)$, $W_{p^\infty}(\mathbf{F}_p)$, and $\Delta_{p^\infty, p^\infty}: \mathbf{Z}_p \to W_{p^\infty}(\mathbf{Z}_p)$

As a partial illustration of the way formal group and functional equation techniques can be used in dealing with Witt vectors, we offer in this section a quick proof of the fact that $W_{p^\infty}(\mathbf{F}_p) = \mathbf{Z}_p$ where $\mathbf{F}_p$ is the field of p elements and a quick treatment of $\Delta_{p^\infty, p^\infty}: W_{p^\infty}(\mathbf{F}_p) \to W_{p^\infty}(W_{p^\infty}(\mathbf{F}_p))$.

Consider the formal group law $F(X, Y) = F_{\Delta_1}(X, Y)$ over $\mathbf{Z}$ of Chapter I, Section 3.2 defined by

$$F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{15.4.1}$$

$$f(X) = X + p^{-1}X^p + p^{-2}X^{p^2} + \cdots = X + p^{-1}f(X^p)$$

■ (15.4.2) **Lemma** Every curve $\gamma(t) \in \mathscr{C}(F; \mathbf{Z}_p)$ can be uniquely written as a sum

$$\sum_{i=1}^{\infty} {}^F c_i t^i, \qquad c_i \in \mathbf{Z}_p$$

The curve is p-typical if and only if

$$\gamma(t) = \sum_{n=0}^{\infty} {}^F b_n t^{p^n}, \qquad b_n \in \mathbf{Z}_p$$

Proof The first statement is immediate from the fact that $F(X, Y) \equiv X + Y$ mod(degree 2). The second follows by Proposition (15.2.4) because $f(X)$ involves only pth powers of X.

We now define for all $n \in \mathbf{N} \cup \{0\}$ a map $w_{p^n}^F: \mathscr{C}_p(F; \mathbf{Z}_p) \to \mathbf{Z}_p$ by the formula

$$w_{p^n}^F(\gamma(t)) = p^n \text{ times (coefficient of } t^{p^n} \text{ in } f(\gamma(t))) \tag{15.4.3}$$

■ (15.4.4) **Lemma** The map $\bar{E}^F: \mathbf{Z}_p^{\mathbf{N} \cup \{0\}} \to \mathscr{C}_p(F; \mathbf{Z}_p)$ defined by $(a_0, a_1, a_2, \ldots) \mapsto \sum^F a_i t^{p^i}$ is a bijection and $w_{p^n}^F \bar{E}^F = w_{p^n}$.

Proof We first calculate

$$\begin{aligned} w_{p^n}^F \bar{E}^F(a_0, a_1, \ldots) &= w_{p^n}^F\left(\textstyle\sum^F a_i t^{p^i}\right) \\ &= p^n(\text{coefficient of } t^{p^n} \text{ in } f\left(\textstyle\sum^F a_i t^{p^i}\right)) \\ &= p^n\left(\text{coefficient of } t^{p^n} \text{ in } \sum_{i=0}^{\infty} f(a_i t^{p^i})\right) \\ &= p^n\left(\text{coefficient of } t^{p^n} \text{ in } \sum_{i=0}^{\infty} \sum_{l=0}^{\infty} p^{-l}(a_i t^{p^i})^{p^l}\right) \\ &= p^n\left(\text{coefficient of } t^{p^n} \text{ in } \sum_{r=0}^{\infty}\left(\sum_{l=0}^{r} p^{-l} a_{r-l}^{p^l}\right) t^{p^r}\right) \\ &= w_{p^n}(a_0, a_1, a_2, \ldots) \end{aligned}$$

The injectivity of $\bar{E}^F$ follows from this because if $(a_0, a_1, \ldots)$ and $(b_0, b_1, \ldots)$ are such that $w_{p^n}(a) = w_{p^n}(b)$ for all n, then $a_i = b_i$ for all i because $\mathbf{Z}_p$ is torsion free. Finally, the fact that $\operatorname{Im}(\bar{E}^F) \subset \mathscr{C}_p(F; \mathbf{Z}_p) \subset \mathscr{C}(F; \mathbf{Z}_p)$ and the surjectivity of $\dot{E}^F$ follow from Lemma (15.4.2). Q.E.D.

Now by the definition of the addition in $\mathscr{C}_p(F; \mathbf{Z}_p)$ we have that

$$w_{p^n}^F(\gamma(t) +_F \delta(t)) = w_{p^n}^F(\gamma(t)) + w_{p^n}^F(\gamma(t))$$

So transferring the addition of $\mathscr{C}_p(F; \mathbf{Z}_p)$ to $\mathbf{Z}_p^{\mathbf{N} \cup \{0\}}$ via the bijection $\bar{E}^F$, we find a group structure on $\mathbf{Z}_p^{\mathbf{N} \cup \{0\}}$ that satisfies

$$w_{p^n}((a_0, a_1, \ldots) + (b_0, b_1, \ldots)) = w_{p^n}(a_0, a_1, \ldots) + w_{p^n}(b_0, b_1, \ldots)$$

This group structure is necessarily unique because $\mathbf{Z}_p$ has no torsion.

The next thing to do is to define a suitable ring structure on $\mathscr{C}_p(F; \mathbf{Z}_p)$. Let $\gamma(t), \delta(t) \in \mathscr{C}_p(F; \mathbf{Z}_p)$. Write $f(\gamma(t)) = \sum c_i t^{p^i}$, $f(\delta(t)) = \sum d_i t^{p^i}$. We define

$$\gamma(t) \cdot \delta(t) = f^{-1}\left(\sum_{i=0}^{\infty} p^i c_i d_i t^{p^i}\right) \tag{15.4.5}$$

■ (15.4.6) **Lemma** Formula (15.4.5) defines a multiplication on $\mathscr{C}_p(F; \mathbf{Z}_p)$ and turns the abelian group $\mathscr{C}_p(F; \mathbf{Z}_p)$ into a commutative ring with unit element. The unit element is the curve $\gamma_0(t) = t$, and $w_{p^n}^F(\gamma(t) \cdot \delta(t)) = w_{p^n}^F(\gamma(t)) w_{p^n}^F(\delta(t))$.

Proof By the functional equation lemma 2.2 we know that the c_i and d_i satisfy the properties

$$c_i = p^{-1}c_{i-1} + \text{integral}, \qquad d_i = p^{-1}d_{i-1} + \text{integral} \tag{15.4.7}$$

$$p^i c_i \in \mathbf{Z}_p, \qquad p^i d_i \in \mathbf{Z}_p \tag{15.4.8}$$

(of which (15.4.8) follows from (15.4.7)). It follows that $p^i c_i d_i = p^{-1}(p^{i-1}c_{i-1}d_{i-1}) + \text{integral}$ so that, again by the functional equation lemma, $\gamma(t) \cdot \delta(t)$ has its coefficients in $\mathbf{Z}_p$. This proves that $\gamma(t) \cdot \delta(t) \in \mathscr{C}_p(F; \mathbf{Z}_p)$. The various identities that go into the definition of ring follow immediately from (15.4.5), as does the formula for $w_{p^n}^F$. Q.E.D.

Transferring the multiplication on $\mathscr{C}_p(F; \mathbf{Z}_p)$ to $\mathbf{Z}^{\mathbf{N} \cup \{0\}}$ via the bijection $\bar{E}^F$, we now have a ring structure on $\mathbf{Z}_p^{\mathbf{N} \cup \{0\}}$ for which the maps $w_{p^n}: \mathbf{Z}_p^{\mathbf{N} \cup \{0\}} \to \mathbf{Z}_p$ are ring homomorphisms. This means that $\mathbf{Z}_p^{\mathbf{N} \cup \{0\}}$ with this ring structure is $W_{p^\infty}(\mathbf{Z}_p)$.

We now proceed to define a ring homomorphism $\Delta^F: \mathbf{Z}_p \to \mathscr{C}_p(F; \mathbf{Z}_p)$. For each $a \in \mathbf{Z}_p$, we set

$$\Delta^F(a) = f^{-1}(af(t)) \tag{15.4.9}$$

■ (15.4.10) **Lemma** Formula (15.4.9) defines a ring homomorphism $\mathbf{Z}_p \to \mathscr{C}_p(F; \mathbf{Z}_p)$ such that $w_{p^n}^F \Delta^F(a) = a$ for all $n \in \mathbf{N}$ and $a \in \mathbf{Z}_p$.

Proof Because we have that $af(t) - p^{-1}(af(t^p)) = at$ and $a \in \mathbf{Z}_p$, the functional equation lemma gives us that $\Delta^F(a)$ has its coefficients in $\mathbf{Z}_p$ and hence is an element of $\mathscr{C}_p(F; \mathbf{Z}_p)$. The remainder of the lemma is immediate from the definitions of addition and multiplication in $\mathscr{C}_p(F; \mathbf{Z}_p)$ and the definition of $w_{p^n}^F$. (NB: formula (15.4.9) gives something with integral coefficients only if $a \in \mathbf{Z}_p$; for if $a \notin \mathbf{Z}_p$, then in $\mathbf{Z}_p[a]$ the congruence $b \equiv b^p \bmod(p)$ does no longer hold; cf. Chapter I, Section 2 for details as to why this is relevant.) Q.E.D.

Let $\rho: \mathscr{C}_p(F; \mathbf{Z}_p) \to \mathscr{C}_p(F; \mathbf{F}_p)$ be the projection induced by the canonical map $\mathbf{Z}_p \to \mathbf{F}_p$. Suppose that $\gamma(t) \in \operatorname{Ker}(\rho)$. Write

$$\gamma(t) = \sum_{i=0}^{\infty} {}^F c_i t^{p^i}$$

It follows that $p \mid c_i$ for all i, which in turn implies that if $f(\gamma(t)) = \sum b_i t^{p^i}$, then $b_i \in p\mathbf{Z}_p$ for all i. Conversely, if $b_i \in p\mathbf{Z}_p$ for all i, then if $\sum b_i t^{p^i} = f(\sum^F c_i t^{p^i})$, we have $c_i \in p\mathbf{Z}_p$ as is easily checked by induction (or use part (iv) of the functional equation lemma). It follows that $\operatorname{Ker} \rho$ is an ideal in $\mathscr{C}_p(F; \mathbf{Z}_p)$ so that $\mathscr{C}_p(F; \mathbf{F}_p)$ inherits a ring structure from $\mathscr{C}_p(F; \mathbf{Z}_p)$, which then identifies $\mathscr{C}_p(F; \mathbf{F}_p)$ with $W_{p^\infty}(\mathbf{F}_p)$, the ring of vectors $(a_0, a_1, a_2, \ldots)$, $a_i \in \mathbf{F}_p$ (with addition and multiplication defined by first lifting vectors $(\tilde{a}_0, \tilde{a}_1, \ldots)$ to vectors $(\tilde{a}_0, \tilde{a}_1, \ldots)$, $\tilde{a}_i \in \mathbf{Z}_p$, then adding and multiplying in $W_{p^\infty}(\mathbf{Z}_p)$, and then reducing the coordinates of the results modulo p).

■ (15.4.11) **Theorem** The composed map

$$\mathbf{Z}_p \xrightarrow{\Delta^F} \mathscr{C}_p(F; \mathbf{Z}_p) \xrightarrow{\rho} \mathscr{C}_p(F; \mathbf{F}_p)$$

is an isomorphism of rings.

Proof Because Δ^F is a homomorphism of rings, as is ρ, we have to show only that $\rho\Delta^F$ is bijective. To this end we first remark that

$$\Delta^F(p) \equiv t^p \mod p$$

by Lemma (3.2.4). Now write $a \in \mathbf{Z}_p$ as $a = p^r u$ with u a unit in $\mathbf{Z}_p$, then by its definition (15.4.9) and part (iv) of the functional equation lemma

$$\Delta^F(a) \equiv u t^{p^r} \mod(p, \text{degree } p^r + 1) \tag{15.4.12}$$

The injectivity of $\rho\Delta^F$ follows from this. To see that $\rho\Delta^F$ is surjective we filter the group $\mathbf{Z}_p$ by the subgroups $p^n\mathbf{Z}_p$ and $\mathscr{C}_p(F; \mathbf{F}_p)$ by the subgroups $\mathscr{C}_p^{(n)}(F; \mathbf{F}_p)$ of all p-typical curves $\gamma(t) = \sum^F c_i t^{p^i}$ with $c_0 = c_1 = \cdots = c_{n-1} = 0$.

Note that the map

$$\mathscr{C}_p^{(n)}(F; \mathbf{F}_p) \to \mathbf{F}_p, \qquad \sum^F c_i t^{p^i} \mapsto c_n$$

induces an isomorphism $\mathscr{C}_p^{(n)}(F; \mathbf{F}_p)/\mathscr{C}_p^{(n+1)}(F; \mathbf{F}_p) \xrightarrow{\sim} \mathbf{F}_p$. From (15.4.12) we see that $\rho\Delta^F$ maps $p^n\mathbf{Z}_p$ into $\mathscr{C}_p^{(n)}(F; \mathbf{F}_p)$ and that the induced homomorphisms $p^n\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p \to \mathscr{C}_p^{(n)}(F; \mathbf{F}_p)/\mathscr{C}_p^{(n+1)}(F; \mathbf{F}_p)$ are bijective. Because the groups $\mathbf{Z}_p$ and $\mathscr{C}_p(F, \mathbf{F}_p)$ are both complete and Hausdorff with respect to the topology defined by the subgroups $p^n\mathbf{Z}_p$ and $\mathscr{C}_p^{(n)}(F; \mathbf{F}_p)$, it follows that $\rho\Delta^F$ is also surjective.

■ (15.4.13) **Corollary** $\mathbf{Z}_p \xrightarrow{\sim} W_{p^\infty}(\mathbf{F}_p)$.

The last thing to do is to show that also the Frobenius morphisms in $\mathscr{C}_p(F; \mathbf{Z}_p)$, $\mathscr{C}_p(F; \mathbf{F}_p)$, $\mathbf{Z}_p$, correspond.

■ (15.4.14) **Lemma** $w_{p^n}^F(\mathbf{f}_p(\gamma(t)) = w_{p^{n+1}}^F(\gamma(t))$ for all $\gamma(t) \in \mathscr{C}_p(F; \mathbf{Z}_p)$.

Proof Immediate from the definition of the $w_{p^n}^F$ and the definition of $\mathbf{f}_p$ via formula (15.1.9).

Transferring $\mathbf{f}_p$ to $W_{p^\infty}(\mathbf{Z}_p)$ via the isomorphism $\bar{E}^F$ we find an endomorphism $\mathbf{f}_p$ of $W_{p^\infty}(\mathbf{Z}_p)$ that satisfies $w_{p^n}\mathbf{f}_p = w_{p^{n+1}}$ for all $n \in \mathbf{N} \cup \{0\}$ (and $\mathbf{f}_p$ is uniquely characterized by this property because $\mathbf{Z}_p$ is torsion free).

■ (15.4.15) **Lemma** If $\mathbf{f}_p(a_0, a_1, \ldots) = (b_0, b_1, b_2, \ldots) \in W_{p^\infty}(\mathbf{Z}_p)$, then $a_i \equiv b_i \mod p$ for all $i = 0, 1, 2, \ldots$.

Proof We have $w_1(b) = w_p(a)$ so $a_0^p + pa_1 = b_0$ which gives $b_0 \equiv a_0^p \equiv a_0 \mod p$. Using induction, and $(c \equiv d \mod(p^r) \Rightarrow c^p \equiv d^p \mod(p^{r+1}))$ we see that $a_i^p \equiv a_i \equiv b_i \mod(p)$ for $i = 0, 1, \ldots, n-1$ and $w_n(b) = w_{n+1}(a)$ imply $p^n b_n \equiv p^n a_n^p \mod(p^{n+1})$ so that $a_n \equiv a_n^p \equiv b_n \mod(p)$.

■ (15.4.16) **Corollary** $\mathbf{f}_p(\operatorname{Ker}\bar{\rho}) \subset \operatorname{Ker}\bar{\rho}$ where $\bar{\rho}$ is the canonical projection $W_{p^\infty}(\mathbf{Z}_p) \to W_{p^\infty}(\mathbf{F}_p)$, and the induced homomorphism $\mathbf{f}_p$: $W_{p^\infty}(\mathbf{F}_p) \to W_{p^\infty}(\mathbf{F}_p)$ is the identity.

So we see that Δ^F and ρ are also compatible with the Frobenius morphisms $\mathbf{f}_p$ and that Δ^F has the property $w_p\Delta^F = \mathbf{f}_p$, which according to Theorem (15.3.10) it must have to qualify as the "Artin–Hasse-like" homomorphism $\Delta_{p^\infty,p^\infty}$: $W_{p^\infty}(\mathbf{F}_p) \to W_{p^\infty}(W_{p^\infty}(\mathbf{F}_p))$. (Cf. Corollary (15.4.16) and Lemma (15.4.10).)

16 Curves and p-Typical Formal Groups

In 15.1 we defined the abelian group $\mathscr{C}(F; A)$ of curves over A in a formal group law $F(X, Y)$ over A. This section first studies $\mathscr{C}(F; A)$ and its subgroup $\mathscr{C}_p(F; A)$ in somewhat more detail and then proceeds to the proofs of the various results mentioned in 15.2.

16.1 Generalities on $\mathscr{C}(F; A)$ and its operators

■ (16.1.1) **Filtration** Let $\gamma(t)$ be a curve in an m-dimensional formal group law $F(X, Y)$. Write $\gamma(t) = \sum_{n=1}^{\infty} c_n t^n$, $c_n \in A^m$. We let $\mathscr{C}^n(F; A)$ be the subset of all curves such that $c_i = 0$, $i = 1, \ldots, n-1$. Because $F(X, Y) \equiv X + Y$ mod(degree 2), we see easily that $\mathscr{C}^n(F; A)$ is in fact a subgroup of $\mathscr{C}(F; A)$. This defines a filtration

$$\mathscr{C}(F; A) = \mathscr{C}^1(F; A) \supset \mathscr{C}^2(F; A) \supset \cdots \supset \mathscr{C}^n(F; A) \supset \cdots$$

of $\mathscr{C}(F; A)$ by subgroups. It is clear that $\bigcap_n \mathscr{C}^n(F; A) = 0$. This filtration defines a topology on $\mathscr{C}(F; A)$, and it is also clear that $\mathscr{C}(F; A)$ is complete with respect to this topology.

■ (16.1.2) **Change of rings** Now let ϕ: $A \to B$ be a ring homomorphism and let $\gamma(t)$ be a curve in $F(X, Y)$ over A. Then $\phi_*\gamma(t)$ is an m-tuple of power series with coefficients in B and hence can be interpreted as a curve in $\phi_*F(X, Y)$. This defines a map ϕ_*: $\mathscr{C}(F; A) \to \mathscr{C}(\phi_*F; B)$ which is clearly a continuous homomorphism. In fact $\phi_*\mathscr{C}^n(F; A) \subset \mathscr{C}^n(\phi_*F; B)$. It is also immediately clear from the definitions that ϕ_* commutes with the various operators that we have defined in 15.1. That is, we have

$$\phi_* \circ \langle a \rangle = \langle \phi(a) \rangle \circ \phi_*, \qquad a \in A \tag{16.1.3}$$

$$\phi_* \circ \mathbf{V}_n = \mathbf{V}_n \circ \phi_*, \qquad n \in \mathbf{N} \tag{16.1.4}$$

$$\phi_* \circ \mathbf{f}_n = \mathbf{f}_n \circ \phi_*, \qquad n \in \mathbf{N} \tag{16.1.5}$$

Note that in (16.1.5) the $\mathbf{f}_n$ on the left-hand side is defined using $F(X, Y)$, and the $\mathbf{f}_n$ on the right-hand side is defined using $\phi_*F(X, Y)$. The proofs of (16.1.3)–(16.1.5) are immediate from the definitions.

■ (16.1.6) **Functoriality** Now let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism from the m-dimensional formal group law $F(X, Y)$ to the n-dimensional formal group law $G(X, Y)$. Recall that $\alpha(X)$ is an n-tuple of power series in m-variables such that $\alpha(X) \equiv 0$ mod(degree 1) and $\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$. Now let $\gamma(t)$ be a curve in $F(X, Y)$, i.e., $\gamma(t)$ is an m-tuple of power series in one indeterminate t. Then $\alpha(\gamma(t))$ is an n-tuple of power series in one indeterminate t such that $\alpha(\gamma(t)) \equiv 0$ mod(degree 1). So we can view $\alpha(\gamma(t))$ as a curve in $G(X, Y)$. This defines a map $\alpha_* = \mathscr{C}(\alpha) = \mathscr{C}(\alpha; A)$: $\mathscr{C}(F; A) \to \mathscr{C}(G; A)$. The map α_* is clearly a homomorphism; moreover $\alpha_*(\mathscr{C}^n(F; A)) \subset \mathscr{C}^n(G; A)$ so that α_* is continuous; and finally α_* also commutes with the operators $[a]$, $\mathbf{V}_n$, $\mathbf{f}_n$ in that we have

$$\alpha_* \circ \langle a \rangle = \langle a \rangle \circ \alpha_* \tag{16.1.7}$$

$$\alpha_* \circ \mathbf{V}_n = \mathbf{V}_n \circ \alpha_* \tag{16.1.8}$$

$$\alpha_* \circ \mathbf{f}_n = \mathbf{f}_n \circ \alpha_* \tag{16.1.9}$$

where of course in the last formula the $\mathbf{f}_n$ on the left-hand side is calculated by means of $F(X, Y)$ and the $\mathbf{f}_n$ on the right-hand side is calculated by means of $G(X, Y)$. Thus (16.1.9) should really be written as $\alpha_* \circ \mathbf{f}_n^F = \mathbf{f}_n^G \circ \alpha_*$. The proofs of (16.1.7)–(16.1.9) are immediate from the definitions. (For (16.1.9) one needs that $\alpha(X)$ is a homomorphism.)

■ (16.1.10) **V-basis** Let $\delta_i(t)$, $i = 1, \ldots, m$, be the curve $\delta_i(t) = (0, 0, \ldots, 0, t, 0, \ldots, 0)$ with the t in the ith spot in the m-dimensional formal group law $F(X, Y)$. Then every curve in $F(X, Y)$ over A can be uniquely written as a convergent sum

$$\gamma(t) = \sum_{n=1}^{\infty} \sum_{i=1}^{m} \mathbf{V}_n \langle a_{n,i} \rangle \delta_i(t) \tag{16.1.11}$$

Indeed, let $\gamma(t) = \sum c_n t^n$ with $c_n \in A^m$. Write $c_n = (c_{n,1}, \ldots, c_{n,m})$. Take $a_{1,i} = c_{1,i}$, $i = 1, \ldots, m$. Then we have

$$\gamma(t) \equiv \sum_{i=1}^{m} \mathbf{V}_1 \langle a_{1,i} \rangle \delta_i(t) \quad \text{mod(degree 2)}$$

and the $a_{1,i}$ are uniquely determined by this condition. Now let

$$\gamma(t) - \sum_{i=1}^{m} \mathbf{V}_1 \langle a_{1,i} \rangle \delta_i(t) \equiv c_2' t^2 \quad \text{mod(degree 3)}$$

Write $c_2' = (c_{2,1}', \ldots, c_{2,m}')$ and let $a_{2,i} = c_{2,i}'$, $i = 1, \ldots, m$. Then, because $F(X, Y) \equiv X + Y$ mod(degree 2), we have

$$\gamma(t) \equiv \sum_{n=1}^{2} \sum_{i=1}^{m} \mathbf{V}_n \langle a_{n,i} \rangle \delta_i(t) \quad \text{mod(degree 3)}$$

and this determines the $a_{2,i}$ uniquely.

Continuing in this way, we find unique $a_{n.i}$ for all $n = 1, 2, \ldots$ such that

$$\gamma(t) \equiv \sum_{n=1}^{k} \sum_{i=1}^{m} \mathbf{V}_n\langle a_{n.i}\rangle \delta_i(t) \quad \text{mod(degree } k+1)$$

$$\equiv \sum_{n=1}^{\infty} \sum_{i=1}^{m} \mathbf{V}_n\langle a_{n.i}\rangle \delta_i(t) \quad \text{mod(degree } k+1)$$

for all k, which is equivalent to (16.1.11) because $\mathscr{C}(F; A)$ is Hausdorff.

A set of m curves like $\{\delta_i(t); i = 1, \ldots, m\}$ such that every curve can be uniquely written in the form (16.1.11) is called a V-basis for $\mathscr{C}(F; A)$.

16.2 Relations among the Frobenius, Verschiebung, and homothety operators

In 15.1 we defined a number of operators on $\mathscr{C}(F; A)$. These operators are not independent. The relations among them are

(16.2.1) $$\langle a\rangle\langle a'\rangle = \langle aa'\rangle$$

(16.2.2) $$\langle 1\rangle = \mathbf{V}_1 = \mathbf{f}_1 = id$$

(16.2.3) $$\mathbf{V}_m\mathbf{V}_n = \mathbf{V}_{mn}$$

(16.2.4) $$\mathbf{f}_m\mathbf{f}_n = \mathbf{f}_{mn}$$

(16.2.5) $$\langle a\rangle\mathbf{V}_n = \mathbf{V}_n\langle a^n\rangle$$

(16.2.6) $$\text{if } (n, m) = 1, \quad \text{then } \mathbf{f}_n\mathbf{V}_m = \mathbf{V}_m\mathbf{f}_n$$

(16.2.7) $$\mathbf{f}_n\langle a\rangle = \langle a^n\rangle\mathbf{f}_n$$

(16.2.8) $$\langle a\rangle + \langle b\rangle = \sum_{n=1}^{\infty} \mathbf{V}_n\langle r_n(a, b)\rangle\mathbf{f}_n$$

(16.2.9) $$\mathbf{f}_n\mathbf{V}_n = [n]$$

In (16.2.9) $[n]$ is the operator that sends a curve $\gamma(t)$ into its n-fold sum in $\mathscr{C}(F; A)$, $\gamma(t) \mapsto \gamma(t) +_F \gamma(t) +_F \cdots +_F \gamma(t)$, i.e., $[n] = [n]_{F\bullet}$. This operation must not be confused with the operator $\langle n\rangle$ which sends $\gamma(t)$ to $\gamma(nt)$. Further, in (16.2.8) the $r_n(a, b) \in A$ are obtained by substituting a and b for Z_1 and Z_2 in the universal polynomials $r_d(Z_1, Z_2)$ which are defined by

$$Z_1^n + Z_2^n = \sum_{d|n} d r_d(Z_1, Z_2)^{n/d}$$

The $r_d(Z_1, Z_2)$ are polynomials with integral coefficients as we shall prove below in (16.2.10).

The infinite sum (16.2.8) makes sense when interpreted as

$$\left(\sum_{n=1}^{\infty} \mathbf{V}_n\langle r_n(a, b)\rangle\mathbf{f}_n\right)\gamma(t) = \sum_{n=1}^{\infty} ((\mathbf{V}_n\langle r_n(a, b)\rangle\mathbf{f}_n)\gamma(t))$$

because $\mathscr{C}(F; A)$ is complete in the topology defined by the subgroups $\mathscr{C}^n(F; A)$ and because $V_n\delta(t) \subset \mathscr{C}^n(F; A)$ for any curve $\delta(t)$.

■ (16.2.10) **Proof that the $r_n(X, Y)$ are polynomials with integral coefficients** We consider the power series $(1 - Xt)(1 - Yt)$ in $\mathbf{Z}[X, Y][\![t]\!]$. We can write

$$(1 - Xt)(1 - Yt) = \prod_{i=1}^{\infty} (1 - r_i(X, Y)t^i)$$

where the $r_i(X, Y)$ are certain elements of $\mathbf{Z}[X, Y]$. We claim that these $r_i(X, Y)$ do in fact satisfy the relation $X^n + Y^n = \sum_{d|n} dr_d(X, Y)^{n/d}$. To see this one applies the operator $-t(d/dt)\log$ to the equality above. One finds (using that $-t(d/dt)\log(f(t)) = tf'(t)/f(t)$ and

$$-t\frac{d}{dt}\log(f(t)g(t)) = -t\frac{d}{dt}\log(f(t)) - t\frac{d}{dt}\log(g(t))$$

for all power series $f(t)$ and $g(t)$)

$$-t\frac{d}{dt}\log(1 - Xt)(1 - Yt) = \frac{Xt}{1 - Xt} + \frac{Yt}{1 - Yt} = \sum_{n=1}^{\infty} (X^n + Y^n)t^n$$

and

$$\begin{aligned} -t\frac{d}{dt}\log\left(\prod_{i=1}^{\infty} (1 - r_i(X, Y)t^i\right) &= \sum_{i=1}^{\infty} \frac{ir_i(X, Y)t^i}{1 - r_i(X, Y)t^i} \\ &= \sum_{i=1}^{\infty}\sum_{j=1}^{\infty} i(r_i(X, Y)t^i)^j \\ &= \sum_{n=1}^{\infty}\left(\sum_{i|n} ir_i(X, Y)^{n/i}\right)t^n \end{aligned}$$

The desired relation follows by comparing the coefficients of t^n. Q.E.D.

Of the relations (16.2.1)–(16.2.9), (16.2.1), (16.2.2), (16.2.3), and (16.2.5) are immediate from the definitions. The remaining relations are proved by the following reduction method.

■ (16.2.11) It suffices to prove (16.2.1)–(16.2.9) for the case of formal group laws $F(X, Y)$ defined over a characteristic zero ring A.

Indeed, let $F(X, Y)$ be an m-dimensional formal group law over a ring A. Let $\tilde{A}$ be any characteristic zero ring such that there exists a surjective ring homomorphism $\phi\colon \tilde{A} \to A$. Let $\psi\colon \mathbf{Z}[U] \to A$ be the unique ring homomorphism such that $\psi_* F_U(X, Y) = F(X, Y)$ where $F_U(X, Y)$ is the universal m-dimensional formal group law. For each $U(\mathbf{d}, i)$, $|\mathbf{d}| \geq 2$, let $\tilde{\psi}(U(\mathbf{d}, i)) \in \tilde{A}$ be any element such that $\phi(\tilde{\psi}(U(d, i))) = \psi(U(d, i))$. Then $\tilde{\psi}_* F_U(X, Y) = \tilde{F}(X, Y)$ is such that $\phi_* \tilde{F}(X, Y) = F(X, Y)$. Now suppose that, e.g., (16.2.4) holds in $\mathscr{C}(\tilde{F}; \tilde{A})$. Take

any curve $\gamma(t) \in \mathscr{C}(F; A)$, let $\tilde{\gamma}(T)$ be such that $\phi_* \tilde{\gamma}(t) = \gamma(t)$. Such a $\tilde{\gamma}(t)$ exists because $\phi\colon \tilde{A} \to A$ is surjective. We have $\mathbf{f}_l \mathbf{f}_n \tilde{\gamma}(t) = \mathbf{f}_{ln} \tilde{\gamma}(t)$ by hypothesis in $\mathscr{C}(\tilde{F}; \tilde{A})$. Now apply (16.1.5) to obtain $\mathbf{f}_l \mathbf{f}_n \gamma(t) = \mathbf{f}_{ln} \gamma(t)$ in $\mathscr{C}(F; A)$. The remaining formulas are treated in the same way except for (16.2.8) where one also uses the fact that ϕ_* preserves the filtration, i.e., $\phi_* \mathscr{C}^n(\tilde{F}; \tilde{A}) \subset \mathscr{C}^n(F, A)$ and the fact that $\mathscr{C}(F; A)$ is Hausdorff, i.e., $\bigcap_n \mathscr{C}^n(F, A) = 0$.

■ (16.2.12) It suffices to prove (16.2.1)–(16.2.9) for the case of additive formal group laws $F(X, Y)$ over a characteristic zero ring.

Indeed, by (16.2.11) it suffices to prove (16.2.1)–(16.2.9) for the case of formal group laws $F(X, Y)$ over a characteristic zero ring A. Then we have available the logarithm $f(X)$ of $F(X, Y)$. The logarithm $f(X)$ defines an isomorphism of formal group laws over $A \otimes \mathbf{Q}$ $f(X)\colon F(X, Y) \to \hat{\mathbf{G}}_{\mathrm{a}}^m(X, Y)$. Now to prove that, e.g., $\mathbf{f}_l \mathbf{f}_n = \mathbf{f}_{ln}$ holds one proceeds as follows. Let $\gamma(t) \in \mathscr{C}(F; A)$. By assumption we know that $\mathbf{f}_l \mathbf{f}_n(f(\gamma(t)) = \mathbf{f}_{ln}(f(\gamma(t)))$. By (16.1.9) this means that $f_*(\mathbf{f}_l \mathbf{f}_n(\gamma(t)) = f_*(\mathbf{f}_{ln}(\gamma(t))$. But f is an isomorphism over $A \otimes \mathbf{Q}$ between $F(X, Y)$ and $\hat{\mathbf{G}}_{\mathrm{a}}^n(X, Y)$. It follows that $\mathbf{f}_l \mathbf{f}_n \gamma(t) = \mathbf{f}_{ln} \gamma(t)$ in $\mathscr{C}(F; A \otimes \mathbf{Q})$. But A is of characteristic zero, so that $\mathscr{C}(F; A) \to \mathscr{C}(F; A \otimes \mathbf{Q})$ is injective. It follows that $\mathbf{f}_l \mathbf{f}_n \gamma(t) = \mathbf{f}_{ln} \gamma(t)$ also in $\mathscr{C}(F; A)$ itself.

■ (16.2.13) **Proof of relations (16.2.1)–(16.2.9) in the case $F(X, Y) = \hat{\mathbf{G}}_{\mathrm{a}}^n(X, Y)$** Let $F(X, Y) = \hat{\mathbf{G}}_{\mathrm{a}}^m(X, Y)$. In this case it is easy to calculate the various operators explicitly.

Let $\gamma(t) = \sum_{k=1}^{\infty} a_k t^k$, $a_k \in A^m$. We then have

$$\mathbf{V}_n \gamma(t) = \sum_{k=1}^{\infty} a_k t^{nk}, \qquad \langle a \rangle \gamma(t) = \sum_{k=1}^{\infty} a_k a^k t^k \tag{16.2.14}$$

$$\mathbf{f}_l \gamma(t) = \sum_{k=1}^{\infty} l a_{kl} t^k \tag{16.2.15}$$

The last relation is easily proved by using formula (15.1.7), remembering that $\sum_{i=1}^{l} \zeta_l^{ri} = 1$ if l divides r and $= 0$ otherwise (where ζ_l is a primitive lth root of unity). (Note that formula (15.1.7) makes sense because A is of characteristic zero.) We now proceed to check the formulas (16.2.1)–(16.2.9). Of these (16.2.1)–(16.2.3) and (16.2.5) are of course still trivial. As to (16.2.4), we have

$$\mathbf{f}_l(\mathbf{f}_n \gamma(t)) = \mathbf{f}_l\left(\sum_{k=1}^{\infty} n a_{kn} t^k\right) = \sum_{k=1}^{\infty} l n a_{kln} t^k = \mathbf{f}_{ln} \gamma(t)$$

For formula (16.2.6), we write

$$\mathbf{f}_l \mathbf{V}_n \gamma(t) = \mathbf{f}_l\left(\sum_{k=1}^{\infty} a_k t^{kn}\right) \tag{16.2.16}$$

Now because $(l, n) = 1$ we know that l divides kn if and only if l divides k. It follows that

$$\mathbf{f}_l\left(\sum_{k=1}^{\infty} a_k t^{kn}\right) = \sum_{k=1}^{\infty} l a_{lk} t^{kn} \tag{16.2.17}$$

and on the other hand

$$\mathbf{V}_n\mathbf{f}_l\left(\sum_{k=1}^{\infty} a_k t^k\right) = \mathbf{V}_n\left(\sum_{k=1}^{\infty} l a_{kl} t^k\right) = \sum_{k=1}^{\infty} l a_{kl} t^{nk}$$

Comparing this last formula with (16.2.16) and (16.2.17), we see that we have proved (16.2.6).

Now consider (16.2.7). We have

$$\mathbf{f}_l\langle a\rangle\gamma(t) = \mathbf{f}_l\left(\sum_{k=1}^{\infty} a_k a^k t^k\right) = \sum_{k=1}^{\infty} l a_{kl} a^{kl} t^k$$

$$\langle a^l\rangle\mathbf{f}_l\gamma(t) = \langle a^l\rangle\left(\sum_{k=1}^{\infty} l a_{lk} t^k\right) = \sum_{k=1}^{\infty} l a_{lk} a^{kl} t^k$$

which takes care of (16.2.7). We now proceed to prove (16.2.8). We have because $F(X, Y) = X + Y$ that

$$(\langle a\rangle + \langle b\rangle)\gamma(t) = \left(\sum_{k=1}^{\infty} a_k a^k t^k\right) +_F \left(\sum_{k=1}^{\infty} b_k a^k t^k\right) = \sum_{k=1}^{\infty} a_k (a^k + b^k) t^k$$

$$= \sum_{k=1}^{\infty} a_k \left(\sum_{d|k} d r_d(a, b)^{k/d}\right) t^k$$

and on the other hand

$$\left(\sum_{k=1}^{\infty} \mathbf{V}_k\langle r_k(a, b)\rangle\mathbf{f}_k\right)(\gamma(t)) = \sum_{k=1}^{\infty} (\mathbf{V}_k\langle r_k(a, b)\rangle\mathbf{f}_k\gamma(t))$$

$$= \sum_{k=1}^{\infty} \mathbf{V}_k\langle r_k(a, b)\rangle\left(\sum_{i=1}^{\infty} k a_{ki} t^i\right)$$

$$= \sum_{i,k=1}^{\infty} k r_k(a, b)^i a_{ki} t^{ki}$$

$$= \sum_{n=1}^{\infty} \sum_{d|n} d r_d(a, b)^{n/d} a_n t^n$$

which proves (16.2.8). Finally, (16.2.9) is a triviality because

$$\mathbf{f}_n\mathbf{V}_n\gamma(t) = \mathbf{f}_n\left(\sum_{k=1}^{\infty} a_k t^{nk}\right) = \sum_{k=1}^{\infty} n a_k t^k = n\gamma(t) = [n]\gamma(t)$$

because n always divides kn. This concludes the proof of relations (16.2.1)-(16.2.9).

■ (16.2.18) **Remark** (caveat) Note that in general $\mathbf{V}_n\mathbf{f}_n \neq [n]$.

16.3 p-Typical curves

Choose a prime number p. Recall that a curve $\gamma(t) \in \mathscr{C}(F; A)$ is p-typical if $\mathbf{f}_q\gamma(t) = 0$ for all prime numbers $q \neq p$. Suppose that A is a characteristic zero ring. The first thing to prove is Proposition (15.2.4), i.e.,

■ (16.3.1) A curve $\gamma(t)$ in a formal group law $F(X, Y)$ over a characteristic zero ring A is p-typical if and only if $\log_F(\gamma(t))$ is of the form

$$\log_F(\gamma(t)) = \sum_{n=1}^{\infty} a_n t^{p^n} \tag{16.3.2}$$

where the a_n are m-vectors with coefficients in $A \otimes \mathbf{Q}$.

Proof Because we have $\log_F$ available and because A is of characteristic zero, we have (cf. (15.1.9))

$$\log_F(\mathbf{f}_q\gamma(t)) = \sum_{k=1}^{\infty} qb_{qk}t^k \qquad \text{if} \quad \log_F(\gamma(t)) = \sum_{k=1}^{\infty} b_k t^k$$

so that $\mathbf{f}_q\gamma(t) = 0$ is equivalent to $b_n = 0$ for all multiples n of q. This proves the lemma.

■ (16.3.3) We shall use $\mathscr{C}_p(F; A)$ to denote the set of p-typical curves in $\mathscr{C}(F; A)$. Because $\mathbf{f}_q$: $\mathscr{C}(F; A) \to \mathscr{C}(F; A)$ is a homomorphism of groups, we have that $\mathscr{C}_p(F; A)$ is a subgroup of $\mathscr{C}(F; A)$. Further, $\mathbf{V}_p\mathscr{C}_p(F; A) \subset \mathscr{C}_p(F; A)$ and $\mathbf{f}_p\mathscr{C}_p(F; A) \subset \mathscr{C}_p(F; A)$, $\langle c\rangle\mathscr{C}_p(F; A) \subset \mathscr{C}_p(F; A)$ because of relations (16.2.6), (16.2.4), and (16.2.7).

Let ϕ: $A \to B$ be a ring homomorphism. Then ϕ_*: $\mathscr{C}(F; A) \to \mathscr{C}(F; B)$ maps $\mathscr{C}_p(F; A)$ into $\mathscr{C}_p(\phi_* F; B)$ because of (16.1.5). Finally, if $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is a homomorphism of formal group laws, then also α_*: $\mathscr{C}(F; A) \to \mathscr{C}(G; A)$ maps $\mathscr{C}_p(F; A)$ into $\mathscr{C}_p(G; A)$.

■ (16.3.4) **Lemma** Let $F(X, Y)$ be an m-dimensional formal group law over a ring A and suppose that A is a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra. Let $\gamma(t)$ and $\hat{\gamma}(t)$ be two p-typical curves in $F(X, Y)$ and suppose that $\gamma(t) \equiv \hat{\gamma}(t)$ mod(degree n), then $\gamma(t) \equiv \hat{\gamma}(t)$ mod(degree p^k) where k is the smallest element of $\mathbf{N} \cup \{0\}$ such that $p^k \geq n$.

Proof Suppose $n < p^k$ (otherwise there is nothing to prove) and suppose we have already proved that $\gamma(t) \equiv \hat{\gamma}(t)$ mod(degree r) with $n \leq r < p^k$. Write $\gamma(t) \equiv \hat{\gamma}(t) + ct^r$ with $c \in A^m$. Because k is minimal such that $n < p^k$, there is a prime number q different from p that divides r. Applying $\mathbf{f}_q$ to $\gamma(t) \equiv \hat{\gamma}(t) + ct^r$, we obtain $\mathbf{f}_q\gamma(t) \equiv \mathbf{f}_q\gamma(t) + qct^{r/q}$ mod(degree $r/q + 1$). But $\gamma(t)$ and $\hat{\gamma}(t)$ are both p-typical. Hence $qc = 0$ which implies that $c = 0$ because A is a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra. Q.E.D.

■ (16.3.5) Now suppose that $F(X, Y)$ is an m-dimensional p-typical formal group law over a ring A. As in (16.1.10) let $\delta_i(t)$, $i = 1, \ldots, m$, be the curves $\delta_i(t) = (0, \ldots, 0, t, 0, \ldots, 0)$ with the t in the ith spot. In case $A = \mathbf{Z}[V]$ and $F_V(X, Y) = F(X, Y)$ it follows from (16.3.1) that the $\delta_i(t)$ are p-typical curves. It now follows from the definition of p-typical formal groups and (16.3.3) above that the $\delta_i(t)$ are p-typical curves in $\mathscr{C}(F; A)$ for any p-typical formal group law $F(X, Y)$ over any ring A.

We now claim that all the curves of the form

$$\sum_{k=1}^{\infty} \sum_{i=1}^{m} \mathbf{V}_p^k \langle a_{k,i} \rangle \delta_i(t) \tag{16.3.6}$$

are p-typical. (NB we have used $\mathbf{V}_p^k = \mathbf{V}_{p^k}$; cf. (16.2.3).) This follows immediately from (16.2.6) and (16.2.7).

Now let $\gamma(t)$ be any curve in $F(X, Y)$. Using the fact that all curves of the form (16.3.6) are p-typical, it follows from (16.1.10) above that $\gamma(t)$ can be written as a sum

$$\gamma(t) = \sum_{n \in I(p)} \mathbf{V}_n \gamma_n(t) \tag{16.3.7}$$

with $\gamma_n(t) \in \mathscr{C}_p(F; A)$ for all $n \in I(p)$ and $I(p) = \{n \in \mathbf{N} \mid (n, p) = 1\}$.

■ (16.3.8) **Lemma** Let $F(X, Y)$ be a p-typical formal group law over a ring A that is a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra. Then every curve $\gamma(t) \in \mathscr{C}(F; A)$ can be uniquely written in the form (16.3.7).

Proof We have already seen that any curve $\gamma(t)$ can be written in the form (16.3.7). Because the $\mathbf{V}_n$ are group homomorphisms, it suffices to prove that $\sum_{n \in I(p)} \mathbf{V}_n \gamma_n(t) = 0$, $\gamma_n(t) \in \mathscr{C}_p(F; A)$, implies $\gamma_n(t) = 0$ for all $n \in I(p)$. To see this we prove that $\mathbf{V}_n \gamma_n(t) = 0$ for all $n \in I(p)$. This suffices because by its definition $\mathbf{V}_n$ is clearly injective. Suppose we have already shown that $\mathbf{V}_n \gamma_n(t) \equiv 0 \bmod(\text{degree } r)$ for all $n \in I(p)$. Write $r = p^k s$ with $(s, p) = 1$. Suppose that $\mathbf{V}_n \gamma_n(t) \not\equiv 0 \bmod(\text{degree } r + 1)$. Then since $\mathbf{V}_n \gamma_n(t)$ involves only powers of t^n, we must have $n \mid r$ and $\gamma_n(t) \not\equiv 0 \bmod(\text{degree } n^{-1}r + 1)$ by induction hypothesis. Hence by Lemma (16.3.4) we must have $n^{-1}r = p^l$ for some l. As $n \in I(p)$ this means that $n = s$ and $l = k$. So there is at most one n such that $\mathbf{V}_n \gamma_n(t) \not\equiv 0 \bmod(\text{degree } r + 1)$, a contradiction with $\sum \mathbf{V}_n \gamma_n(t) = 0$.

■ (16.3.9) **Lemma** Let $F(X, Y)$ be an m-dimensional p-typical formal group over a ring A that is a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra. Then every p-typical curve in $F(X, Y)$ can be uniquely written in the form (16.3.6).

Proof Let $\gamma(t)$ be a p-typical curve. By (16.1.10) we can write $\gamma(t)$ uniquely in the form

$$\gamma(t) = \sum_{n=1}^{\infty} \sum_{i=1}^{m} \mathbf{V}_n \langle a_{n,i} \rangle \delta_i(t) \tag{16.3.10}$$

To prove the lemma we show that $a_{n,i} = 0$ unless $n = p^l$, $l \in \mathbf{N} \cup \{0\}$. Suppose this is not the case and let r be the smallest integer such that $a_{r,i} \neq 0$ for some i and $r \neq 1$ or a power of p. Let

$$\hat{\gamma}(t) = \sum_{k=1}^{\infty} \sum_{i=1}^{m} \mathbf{V}_p^k \langle a_{p^k,i} \rangle \delta_i(t)$$

Then we have

$$\gamma(t) \equiv \hat{\gamma}(t) + a_r t^r \mod(\text{degree } r+1)$$

but $\gamma(t)$ and $\hat{\gamma}(t)$ are both p-typical and r is not a power of p, hence by Lemma (16.3.4) $\gamma(t) \equiv \hat{\gamma}(t)$ mod(degree $r+1$) and it follows that $a_r = 0$, a contradiction. Q.E.D.

■ (16.3.11) Let A be a $\mathbf{Z}_{(p)}$-algebra. Then there is a natural projection ε_p^F: $\mathscr{C}(F; A) \to \mathscr{C}_p(F; A)$ defined as follows

(16.3.12) $$\gamma(t) \mapsto \sum_{n \in I(p)} n^{-1} \mu(n) \mathbf{V}_n \mathbf{f}_n \gamma(t)$$

where $I(p) = \{n \in \mathbf{N} \mid (n, p) = 1\}$ and $\mu(n)$: $\mathbf{N} \to \mathbf{Z}$ is the Möbius function defined by the property $\sum_{d|n} \mu(d) = 1$ if $n = 1$ and $\sum_{d|n} \mu(d) = 0$ if $n > 1$. (Because $n^{-1} \in A$ for $n \in I(p)$, multiplication by n^{-1} is defined in $\mathscr{C}(F; A)$; this operation must not be confused with $\langle n^{-1} \rangle$.)

If A is also a characteristic zero ring and $f(X)$ is the logarithm of $F(X, Y)$, then we claim that $\varepsilon_p \gamma(t) = f^{-1}(\varepsilon_p^{\mathbf{G}_a} f(\gamma(t)))$ and that $\varepsilon_p^{\mathbf{G}_a}$ of a curve $\gamma(t)$ is the curve

$$\sum_{n=0}^{\infty} a_{p^n} t^{p^n}$$

if $\gamma(t)$ is the curve $\gamma(t) = \sum_{k=1}^{\infty} a_k t^k$. This is quite easy to check. Indeed

$$f(\varepsilon_p \gamma(t)) = \sum_{n \in I(p)} n^{-1} \mu(n) \mathbf{V}_n \mathbf{f}_n f(\gamma(t))$$

where the right-hand sum is in $\mathscr{C}(\hat{\mathbf{G}}_a^m; \mathbf{Q} \otimes A)$. Writing $f(\gamma(t)) = \sum_{k=1}^{\infty} b_k t^k$, we have

$$n^{-1} \mu(n) \mathbf{V}_n \mathbf{f}_n f(\gamma(t)) = \sum_{n \in I(p)} \sum_{k=1}^{\infty} \mu(n) b_{nk} t^{nk}$$

so that the coefficient of t^r in $f(\varepsilon_p \gamma(t))$ is equal to

$$\sum_{n|r, n \in I(p)} \mu(n) b_r = \begin{cases} 0 & \text{if } r \text{ is not a power of } p \\ b_r & \text{if } r \text{ is a power of } p \end{cases}$$

(The explicit definition of $\mu(n)$ is: $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by a square; $\mu(p_1 p_2 \cdots p_r) = (-1)^r$ if $p_1, \ldots, p_r$ are r different prime numbers.)

■ (16.3.13) **Remarks** If $F(X, Y)$ is not a p-typical formal group law, then there need not exist p-typical curves $\delta_i(t)$ such that $\delta_i(t) \equiv (0, \ldots, 0, t, 0, \ldots, 0)$ mod(degree 2). It is easy to check that this is the case, e.g., for the universal one dimensional formal group law $F_U(X, Y)$ (take $p > 2$).

The condition "A of characteristic zero or a $\mathbf{Z}_{(p)}$-algebra" in (16.3.8), (16.3.11), (16.3.12) cannot be removed. Take, e.g., $F(X, Y) = \hat{\mathbf{G}}_a(X, Y)$ over a field of characteristic $q \neq p$. The curve $t + t^q$ is then p-typical and so is the curve t.

16.4 p-Typical formal group laws and the criterion for being p-typical

We are now in a position to prove Theorem (15.2.3) (the criterion for p-typicality of a formal group law). We fix a prime number p.

■ (16.4.1) **Proof of the "only if" part of Theorem (15.2.3)** Consider the curve $\gamma(t) = (t^{p^{r_1}}, \ldots, t^{p^{r_m}})$ in the m-dimensional p-typical formal group law $F_V(X, Y)$. These curves in $\mathscr{C}(F_V(X, Y); \mathbf{Z}[V])$ are p-typical by Proposition (15.2.4) (which has been proved in (16.3.1)). It now follows from the definition of p-typical formal group and (16.3.3) that the $\gamma(t) = (t^{p^{r_1}}, \ldots, t^{p^{r_m}})$ are p-typical for any p-typical formal group law $F(X, Y)$ over any ring A. Alternatively, one uses that all curves of the form (16.3.6) are p-typical.

■ (16.4.2) **Start of the proof of the "if" part of Theorem (15.2.3)** Let $\rho\colon \mathbf{Z}[U] \to \mathbf{Z}[V]$ be the projection $\rho(U(i, n)) = 0$ if $\mathbf{n}$ is not of the form $\mathbf{n} = p^r\mathbf{e}(i)$, $i \in \{1, \ldots, m\}$, $r \in \mathbf{N} \cup \{0\}$, and $\rho(U(i, p^r\mathbf{e}(j)) = V_r(i, j)$. Let $H_U(X, Y)$ be the m-dimensional universal formal group law constructed in 11.1 and assume that the $n(q_1, \ldots, q_t)$ have been chosen in such a way that $n(q_1, \ldots, q_t) = 1$ if $v(q_1) = \cdots = v(q_t)$. (This can be done; cf. (11.1.1).) We then have that $\rho_* H_U(X, Y) = F_V(X, Y)$ by the definitions of $H_U(X, Y)$ and $F_V(X, Y)$ (cf. (11.1.3)–(11.1.4) and (10.3.1), (10.3.3), and (10.4.1), (10.4.4)). Because $H_U(X, Y)$ is a universal m-dimensional formal group law, there is a unique homomorphism $\psi\colon \mathbf{Z}[U] \to A$ such that $\psi_* H_U(X, Y) = G(X, Y)$. We are going to prove that $\psi(U(i, \mathbf{n})) = 0$ if $\mathbf{n}$ is not of the form $\mathbf{n} = p^r\mathbf{e}(i)$, $i \in \{1, \ldots, m\}$. Suppose we have proved this. Then ψ factors uniquely through ρ, i.e., there is a unique homomorphism $\phi\colon \mathbf{Z}[V] \to A$ such that $\psi = \phi\rho$. Because $\rho_* H_U(X, Y) = F_V(X, Y)$, it follows that $\phi_* F_V(X, Y) = G(X, Y)$. This proves the existence of ϕ.

It therefore remains to prove that $\psi(U(i, \mathbf{n})) = 0$ for $\mathbf{n}$ not of the form $p^r\mathbf{e}(i)$, $r \in \mathbf{N}$, $i \in \{1, \ldots, m\}$. To do this we first do two universal calculations.

■ (16.4.3) **Lemma** Let $n \in \mathbf{N}$ and suppose that $v(n) \neq p$. Let $h_n(X)$ and $H_n(X, Y)$ be the power series over $\mathbf{Q}[U]$ and $\mathbf{Z}[U]$ obtained by substituting

zero for all $U_i(j, k) = U(j, ie(k))$ with $i < n$, $j, k \in \{1, \ldots, m\}$ and $v(i) \neq p$. Then for all primes $q \neq p$ that divide n, we have in $\mathscr{C}(H_n; \mathbf{Z}[U])$

$$\mathbf{f}_q \delta_i(t) \equiv q v(n)^{-1} U_{ne(i)} t^{n/q} \mod(\text{degree } n/q + 1)$$

where, as always, $\delta_i(t)$ is the curve $(0, \ldots, 0, t, 0, \ldots, 0)$ with the t in the ith spot.

(Note that none of the $U(i, \mathbf{d})$ for which $\mathbf{d} = (d_1, \ldots, d_m)$ has two or more $d_j \neq 0$ is set equal to zero.)

Proof It follows immediately from the definition of $h_U(X)$ in (11.1.3) and (11.1.4) that $h_n(\delta_i(t))$ is of the form

$$h_n(\delta_i(t)) \equiv \sum b_l t^{p^l} + v(n)^{-1} U_{ne(i)} t^n \mod(\text{degree } n + 1) \tag{16.4.4}$$

because the coefficients of the $X^{\mathbf{n}}$ for $\mathbf{n}$ of the form $ne(j)$ do not involve any $U(i, \mathbf{d})$ with $\mathbf{d} = (d_1, \ldots, d_m)$ such that more than one of the d_j is nonzero. The lemma follows immediately from (16.4.4).

The second universal calculation that we need involves lexicographic degrees.

■ (16.4.5) **Lexicographic degree** Let $\mathbf{n}, \mathbf{k}$ be two multi-indices of length m. We shall write $\mathbf{n} <_l \mathbf{k}$ if and only if $n_1 < k_1$ or ($n_1 = k_1$ and $n_2 < k_2$) or ... or ($n_1 = k_1$ and ... and $n_{m-1} = k_{m-1}$ and $n_m < k_m$).

Let $\mathbf{n}$ be a multi-index of length m and suppose that at least two of the n_j are nonzero. Then there exist $r_1, \ldots, r_m \in \mathbf{N}$ such that:

(16.4.6) $\hat{n} = n_1 p^{r_1} + n_2 p^{r_2} + \cdots + n_m p^{r_m}$ is divisible by a prime number different from p;

(16.4.7) if $\mathbf{n} <_l \mathbf{k}$, then $\hat{n} < k_1 p^{r_1} + \cdots + k_m p^{r_m}$.

(To see to it that (16.4.7) holds it suffices to take $r_1, \ldots, r_m$ such that

$p^{r_{m-1}} > p^{r_m} d_m, \quad p^{r_{m-2}} > p^{r_m} d_m + p^{r_{m-1}} d_{m-1}, \quad \ldots, \quad p^{r_1} > p^{r_m} d_m + \cdots + p^{r_2} d_2$.)

■ (16.4.8) **Lemma** Let $\mathbf{n} = (n_1, \ldots, n_m)$ be a multi-index such that at least two of the n_j are nonzero. Let $h_{\mathbf{n}}(X)$ and $H_{\mathbf{n}}(X, Y)$ be the formal power series obtained from $h_U(X)$ and $H_U(X, Y)$ by substituting zero for all the $U_i(j, k) = U(j, ie(k))$ with $j, k \in \{1, \ldots, m\}$ and $v(i) \neq p$ and by also substituting zero for all $U(j, \mathbf{d})$, $j \in \{1, \ldots, m\}$, for which $\mathbf{d} <_l \mathbf{n}$, $|\mathbf{d}| > 1$, and $v(\mathbf{d}) \neq p$. Let $r_1, \ldots, r_m \in \mathbf{N}$ be such that (16.4.6) and (16.4.7) hold. Then we have in $\mathscr{C}(H_{\mathbf{n}}; \mathbf{Z}[U])$ for all prime numbers $q \neq p$ that divide $\hat{n}$

$$\mathbf{f}_q(t^{p^{r_1}}, \ldots, t^{p^{r_m}}) \equiv q U_{\mathbf{n}} t^{\hat{n}/q} \mod(\text{degree } \hat{n}/q + 1)$$

Proof It follows immediately from the definition of $h_U(X)$ in (11.1.3) and (11.1.4) that if $\mathbf{k} <_l \mathbf{n}$ and $\mathbf{k} \neq p^r \mathbf{e}(j)$ for all $r \in \mathbf{N}$, $j \in \{1, \ldots, m\}$, then

$$a_{\mathbf{k}}(U) \equiv 0 \mod(U_i(j, k), U(l, \mathbf{d}) \mid v(i) \neq p, v(\mathbf{d}) \neq p, \mathbf{d} <_l \mathbf{n}, |\mathbf{d}| > 1)$$

and also that

$$a_{\mathbf{n}}(U) \equiv U_{\mathbf{n}} \mod(U_i(j, k), U(l, \mathbf{d}) \mid v(i) \neq p, v(\mathbf{d}) \neq p, \mathbf{d} <_l \mathbf{n}, |\mathbf{d}| > 1)$$

It follows that $h_{\mathbf{n}}(t^{p^{r_1}}, \ldots, t^{p^{r_m}})$ is of the form

$$(16.4.9) \qquad h_{\mathbf{n}}(t^{p^{r_1}}, \ldots, t^{p^{r_m}}) \equiv \sum b_i t^{p^i} + U_{\mathbf{n}} t^{\hat{n}} \mod(\text{degree } \hat{n} + 1)$$

and the lemma follows immediately from (16.4.9).

■ (16.4.10) **Remark** It is not true that if $\mathbf{k} <_l \mathbf{n}$ and $\mathbf{k} \neq p^r \mathbf{e}(j)$ for all $r \in \mathbf{N}$ and $j \in \{1, \ldots, m\}$ then

$$a_{\mathbf{k}}(U) \equiv 0 \mod(U(j, \mathbf{d}) \mid \mathbf{d} <_l \mathbf{n}, v(\mathbf{d}) \neq p, |\mathbf{d}| > 1)$$

For instance, if $m = 2$ and $\mathbf{n} = (0, 7)$, $\mathbf{k} = (0, 6)$ and $p = 3$, then $a_{\mathbf{k}}(U)$ involves a term $U_2(1, 1)U_3(1, 2)^2 = U(1, 2\mathbf{e}(1))U(1, 3\mathbf{e}(2))^2$.

■ (16.4.11) **Proof of Theorem (15.2.3) (conclusion)** It is now an easy matter to finish the proof of Theorem (15.2.3). We first show that $\psi(U_n(j, k)) = 0$ for all $n \in \mathbf{N}$, $j, k \in \{1, \ldots, m\}$, for which $v(n) \neq p$. One proceeds by induction. Suppose that we have already shown that $\psi(U_r(j, k)) = 0$ for all $r < n$, $j, k \in \{1, \ldots, m\}$ for which $v(r) \neq p$. If $v(n) = p$, the induction step is trivial. If $v(n) \neq p$, let $q \neq p$ be a prime number dividing n. Let $i \in \{1, \ldots, m\}$. Then by Lemma (16.4.3) we have in $\mathscr{C}(G; A)$

$$\mathbf{f}_q \delta_i(t) \equiv qv(n)^{-1} \psi(U_{n\mathbf{e}(i)})\, t^{n/q} \mod(\text{degree } n/q + 1)$$

But by hypothesis $\mathbf{f}_q \delta_i(t) = 0$, and hence $\psi(U_{n\mathbf{e}(i)}) = 0$ because A is a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring.

Next we show that also $\psi(U(i, \mathbf{d})) = 0$ for all $\mathbf{d} = (d_1, \ldots, d_m)$ for which two or more of the d_j are nonzero. Suppose this is not the case. Let $\mathbf{n}$ be the lexicographically smallest multi-index among these $\mathbf{d}$ for which $\psi(U_{\mathbf{d}}) \neq 0$. Choose $r_1, \ldots, r_m$ such that (16.4.6) and (16.4.7) hold. Let q be a prime number $\neq p$ that divides $\hat{n}$. Then we have by Lemma (16.4.8)

$$\mathbf{f}_q(t^{p^{r_1}}, \ldots, t^{p^{r_m}}) \equiv q\psi(U_{\mathbf{n}}) t^{\hat{n}/q} \mod(\text{degree } \hat{n}/q + 1)$$

But by hypothesis $\mathbf{f}_q$ of these curves is zero; this is a contradiction because A is a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra. Q.E.D.

■ (16.4.12) **Corollary** (of the proof) Let $G(X, Y)$ be a curvilinear formal group law over a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring. Then $G(X, Y)$ is p-typical if and only if the standard V-basis curves $\delta_1(t), \ldots, \delta_m(t)$ are p-typical.

■ (16.4.13) **Corollary** (= Proposition (15.2.6)) An m-dimensional formal group law $F(X, Y)$ over a characteristic zero ring A is p-typical if and only if its logarithm is of the form

$$\log_F(X) = \sum_{n=1}^{\infty} a_n X^{p^n}$$

Proof The "only if" part follows directly from the definition of p-typical. The "if" part follows from the criterion (15.2.3) because all curves $\gamma(t) = (t^{p^{r_1}}, \ldots, t^{p^{r_m}})$ are p-typical, in this case by Proposition (15.2.4).

■ (16.4.14) **Theorem** (= Theorem (15.2.9)) Let A be a $\mathbf{Z}_{(p)}$-algebra. Then every m-dimensional formal group law over A is strictly isomorphic to a p-typical formal group law over A.

Proof Let $H_U(X, Y)$ and $F_V(X, Y)$ be the m-dimensional universal group law over $\mathbf{Z}[U]$ and the m-dimensional p-typical universal formal group law over $\mathbf{Z}[V]$. We identify $\mathbf{Z}[V]$ with a subring of $\mathbf{Z}[U]$ by the embedding $\kappa(V_r(i, j)) = U(i, p^r\mathbf{e}(j))$. Now the logarithms $h_U(X)$ and $f_V(X)$ satisfy functional equations

$$h_U(X) = g_p(X) + \sum_{i=1}^{\infty} \frac{U_{p^i}}{p} h_U^{(p^i)}(X^{p^i}), \qquad f_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{p} f_V^{(p^i)}(X^{p^i})$$

Identifying V_i and U_{p^i} by means of κ, it follows that the power series $\alpha(X) = f_V^{-1}(h_U(X))$ has coefficients in $\mathbf{Z}[U]$ and hence defines a strict isomorphism $H_U(X, Y) \simeq \kappa_* F_V(X, Y)$. This proves the proposition because $H_U(X, Y)$ is universal and because $\phi_* F_V(X, Y)$ is p-typical by definition for all ϕ: $\mathbf{Z}[V] \to A$. Q.E.D.

■ (16.4.15) We note that the isomorphism $H_U(X, Y) \simeq \kappa_* F_V(X, Y)$ defines in fact a universal way of making a formal group p-typical. Assuming that in the definition of $H_U(X, Y)$ we have taken $n(q_1, \ldots, q_t) = 1$ if $v(q_1) = \cdots = v(q_t)$, the logarithm of $\kappa_* F_V(X, Y)$ is obtained from $h_U(X)$, the logarithm of $H_U(X, Y)$, by simply setting all $U(i, \mathbf{d}) = 0$ for $\mathbf{d}$ not of the form $p^r\mathbf{e}(j)$, $r \in \mathbf{N}$, $j \in \{1, \ldots, m\}$, or in other words by simply striking out all terms in $h_U(X)$ that should not occur in the logarithm of a p-typical formal group law.

■ (16.4.16) **Remark** The restriction "over rings A that are characteristic zero rings or $\mathbf{Z}_{(p)}$-algebras" cannot be left out of Theorem (15.2.3) (= Theorem (16.4.1)). To see this let k be a field of characteristic 2 and consider the one dimensional formal group law $F(X, Y) = f^{-1}(f(X) + f(Y))$ over k where $f(X) = X + X^6$. One easily checks that the curve $t + t^6$ is 3-typical in $\mathscr{C}(\hat{\mathbf{G}}_a; k)$. It follows that the curve t is 3-typical in $\mathscr{C}(F; k)$ (cf. (16.3.3)). A simple calculation gives

$$F(X, Y) \equiv X + Y + X^4Y^2 + Y^4X^2 \mod(\text{degree } 7)$$

Now let $F_V(X, Y)$ be the one dimensional 3-typical formal group law of Section 3. Then

$$F_V(X, Y) \equiv X + Y - V_1(XY^2 + X^2Y) \mod(\text{degree } 4)$$

so that if ϕ: $\mathbf{Z}[V] \to k$ is such that $\phi_* F_V(X, Y) = F(X, Y)$, then we must have $\phi(V_1) = 0$. But

$$F_V(X, Y) \equiv X + Y \mod(\text{degree } 9, V_1)$$

so that there is no homomorphism ϕ: $\mathbf{Z}[V] \to k$ such that $\phi_* F_V(X, Y) = F(X, Y)$.

■ (16.4.17) **Proof of Proposition (15.2.8)** (universality of $F_V(X, Y)$) Let $F(X, Y)$ be a p-typical formal group over a ring A. By definition there exists a ϕ: $\mathbf{Z}[V] \to A$ such that $\phi_* F_V(X, Y) = F(X, Y)$. It remains to show that ϕ is unique. Suppose that ψ: $\mathbf{Z}[V] \to A$ is a second homomorphism such that $\psi_* F_V(X, Y) = F(X, Y)$. Let $H_U(X, Y)$ and ρ: $\mathbf{Z}[U] \to \mathbf{Z}[V]$ be as in (16.4.2). Then $(\psi\rho)_* H_U(X, Y) = (\phi\rho)_* H_U(X, Y) = F(X, Y)$, hence $\phi\rho = \psi\rho$ by the universality of $H_U(X, Y)$, and $\phi = \psi$ because ρ is surjective.

■ (16.4.18) **Proposition** Let $F(X, Y)$ be a formal group law over a $\mathbf{Z}_{(p)}$-algebra A. Then every curve $\gamma(t) \in \mathscr{C}(F; A)$ can be uniquely written as a sum

$$\gamma(t) = \sum_{n \in I(p)} \mathbf{V}_n \gamma_n(t)$$

with $\gamma_n(t) \in \mathscr{C}_p(F; A)$ for all $n \in I(p)$.

Proof Combine Lemma (16.3.8) with Theorem (16.4.14) and the fact that α_* commutes with the operators $\mathbf{V}_n$ and $\mathbf{f}_n$ if $\alpha(X)$ is a homomorphism of formal group laws.

17 Lots of Witt Vectors

17.1 The rings of Witt vectors $W(A)$

Let $X_1, X_2, \ldots$ be a series of indeterminates. We define a series of polynomials $w_n(X_1, \ldots, X_n)$ with coefficients in $\mathbf{Z}$ as follows:

$$(17.1.1) \qquad w_1(X) = X_1, \qquad w_2(X) = X_1^2 + 2X_2, \qquad \ldots,$$
$$w_n(X) = \sum_{d|n} dX_d^{n/d}, \qquad \ldots$$

Now let Φ be any polynomial in two variables (one or both of which may, of course, be dummies) with integral coefficients. For example, $\Phi(Z_1, Z_2) = Z_1 + Z_2$ or $Z_1 Z_2$ or $-Z_1$ or 0 or 1.

We now define polynomials $\phi_i(X_1, \ldots, X_i; Y_1, \ldots, Y_i)$ by the condition

$$(17.1.2) \qquad \Phi(w_n(X_1, \ldots, X_n), w_n(Y_1, \ldots, Y_n))$$
$$= w_n(\phi_1(X_1; Y_1), \ldots, \phi_n(X_1, \ldots, X_n; Y_1, \ldots, Y_n))$$

which we shall also write $\Phi(w_n(X), w_n(Y)) = w_n(\phi(X; Y))$. It is obvious from (17.1.1) that there exist $\phi_i(X_1, \ldots, X_i; Y_1, \ldots, Y_i)$ with coefficients in $\mathbf{Q}$ such that (17.1.2) holds (because X_n can be written as a polynomial in the $w_1(X), \ldots, w_n(X)$ with coefficients in $\mathbf{Q}$).

■ (17.1.3) **Lemma** The $\phi_n(X; Y)$ have their coefficients in $\mathbf{Z}$.

To prove this lemma we use a sublemma:

(17.1.4) **Sublemma** Let A be any ring, $n \in \mathbf{N}$. Let $x = (x_1, x_2, \ldots)$, $y = (y_1, y_2, \ldots) \in A^{\mathbf{N}}$ and suppose that $x_i \equiv y_i \bmod(pA)$ for all $i \in \mathbf{N}$ and let $p^k \mid n$. Then $w_n(x) \equiv w_n(y) \bmod(p^{k+1}A)$.

Proof If $x_d \equiv y_d \bmod(pA)$, then $dx_d^{n/d} \equiv dy_d^{n/d} \bmod(p^{k+1}A)$ because $a \equiv b \bmod(p^rA) \Rightarrow a^p \equiv b^p \bmod(p^{r+1}A)$. This proves the sublemma.

■ (17.1.5) **Proof of Lemma (17.1.3)** We proceed by induction, the case $n = 1$ being trivial. Assume therefore that $\phi_i(X; Y)$ has integral coefficients for all $i < n$ with $n \geq 2$. Choose a prime number p and write $n = p^k m$ with $(p, m) = 1$. We are going to prove that $\phi_n(X; Y) \in \mathbf{Z}_{(p)}[X; Y]$. If $k = 0$, this follows directly from $\Phi(w_n(X), w_n(Y)) = w_n(\phi(X; Y))$ because to write X_n in terms of the $w_1(X), \ldots, w_n(X)$ one needs only denominators that are products of divisors of n. So suppose that $k \geq 1$. We note that

(17.1.6) $\quad w_n(X) = w_{n/p}(X^p) + p^k(mX_n + \text{terms involving lower } X\text{'s})$

where, as usual, X^p is short for $(X_1^p, X_2^p, \ldots)$. Indeed

$$w_n(X) = \sum_{d \mid n} dX_d^{n/d} = \sum_{d \mid p^{-1}n} dX_d^{n/d} + \sum_{d \mid n, d \nmid p^{-1}n} dX_d^{n/d}$$

$$= w_{n/p}(X^p) + \sum_{d \mid n, d \nmid p^{-1}n} dX_d^{n/d}$$

But if $d \mid n$ and $d \nmid p^{-1}n$, we must have $d = p^k d'$ with $d' \mid m$. This proves (17.1.6).

From $\Phi(w_n(X), w_n(Y)) = w_n(\phi(X; Y))$ we obtain, using (17.1.6),

(17.1.7) $\quad n\phi_n(X; Y) + p^k(\text{terms involving lower } \phi\text{'s}) + w_{n/p}(\phi^p(X; Y))$

$$= \Phi(w_n(X), w_n(Y))$$

Now because the lower ϕ's have integral coefficients, we have $\phi_r^p(X; Y) \equiv \phi_r(X^p; Y^p) \bmod p$ for all $r < n$ so that using the sublemma (17.1.4)

(17.1.8) $\qquad w_{n/p}(\phi^p(X; Y)) \equiv w_{n/p}(\phi(X^p; Y^p)) \quad \bmod(p^k)$

On the other hand, substituting (17.1.6) in $\Phi(w_n(X), w_n(Y))$ we find (because Φ has integral coefficients)

(17.1.9) $\qquad \Phi(w_n(X), w_n(Y)) \equiv \Phi(w_{n/p}(X^p); w_{n/p}(Y^p)) \quad \bmod(p^k)$

Further, we have of course

(17.1.10) $\qquad \Phi(w_{n/p}(X^p); w_{n/p}(Y^p)) = w_{n/p}(\phi(X^p; Y^p))$

Combining (17.1.7)–(17.1.10) we see that $n\phi_n(X; Y) \equiv 0 \bmod(p^k)$ which proves that $\phi_n(X; Y)$ is in $\mathbf{Z}_{(p)}[X; Y]$. This holds for all p. Hence $\phi_n(X; Y) \in \mathbf{Z}[X; Y]$, which concludes the proof of the lemma.

■ (17.1.11) **Remark** The interested reader has probably detected some sort of similarity between this proof and the proof of the functional equation lemma in Section 2. This is no accident as we shall see later; cf. Section 25.1 of Chapter IV.

We now define the polynomials $\Sigma_1, \Sigma_2, \ldots; \Pi_1, \Pi_2, \ldots; \iota_1, \iota_2, \ldots$ by the equations

$$(17.1.12)\quad w_n(\Sigma) = w_n(X) + w_n(Y), \quad w_n(\Pi) = w_n(X)w_n(Y), \quad w_n(\iota) = -w_n(X)$$

■ (17.1.13) **Construction of $W(A)$, the ring of generalized Witt vectors over A** Let A be any ring and let $W(A)$ be the set of all infinite sequences $(a_1, a_2, \ldots)$, $a_i \in A$. We define an addition and multiplication on $W(A)$ by the rules

$$(17.1.14)\quad (a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (\Sigma_1(a; b_1), \Sigma_2(a_1, a_2; b_1, b_2), \ldots)$$

$$(a_1, a_2, \ldots) \cdot (b_1, b_2, \ldots) = (\Pi_1(a_1; b_1), \Pi_2(a_1, a_2; b_1, b_2), \ldots)$$

■ (17.1.15) **Theorem** The set $W(A)$ with the addition and multiplication defined by (17.1.14) is a commutative ring. The zero element is $(0, 0, \ldots)$ and the unit element is $(1, 0, 0, \ldots)$, and

$$(a_1, a_2, \ldots) + (\iota_1(a_1), \iota_2(a_1, a_2), \ldots) = (0, 0, 0, \ldots)$$

Moreover, if $\phi\colon A \to B$ is a homomorphism of rings, then

$$W(\phi)(a_1, a_2, \ldots) = (\phi(a_1), \phi(a_2), \ldots)$$

is a homomorphism of rings $W(A) \to W(B)$. Finally, the $w_n\colon W(A) \to A$ are ring homomorphisms.

Proof To prove that $W(A)$ is indeed a ring we have to show that various identities like $(a + b)c = ac + bc$ hold. To do this we first observe that if A is a $\mathbf{Q}$-algebra, then $w\colon W(A) \to A^{\mathbf{N}}$, $(a_1, a_2, \ldots) \mapsto (w_1(a), w_2(a), \ldots)$ is a bijection that takes addition and multiplication in $W(A)$ into coordinatewise addition and multiplication in $A^{\mathbf{N}}$. But $A^{\mathbf{N}}$ with coordinatewise addition and multiplication is a ring. It follows that $W(A)$ is also ring. Also $w(0, 0, 0, \ldots)) = (0, 0, 0, \ldots)$, $w((1, 0, 0, \ldots)) = (1, 1, 1, \ldots)$, and $w((\iota_1(a), \iota_2(a), \ldots) = (-a_1, -a_2, -a_3, \ldots)$, which proves the statements concerning zero, unit element, and opposite element in the case that A is a $\mathbf{Q}$-algebra. Now let A be a characteristic zero ring and $\phi\colon A \to A \otimes \mathbf{Q}$ the natural embedding. Then $W(\phi)\colon W(A) \to W(A \otimes \mathbf{Q})$ is injective. Further, because addition and multiplication for Witt vectors are defined by "universal" polynomials with coefficients in $\mathbf{Z}$, it is obvious that $W(\phi)$ preserves addition and multiplication.

But the various identities that go into the definition of "ring" hold in $W(A \otimes \mathbf{Q})$; hence, because $W(\phi)$ is injective, preserves multiplication, addition, and opposites, and takes $(0, 0, \ldots)$ into $(0, 0, \ldots)$ and $(1, 0, 0, \ldots)$ into

$(1, 0, 0, \ldots)$, it follows that $W(A)$ is also a ring. Finally, if A is any ring, then there is a characteristic zero ring $\tilde{A}$ with a surjective homomorphism $\phi: \tilde{A} \to A$. Now $W(\tilde{A})$ is a ring, $W(\phi)$ preserves everything in sight, and it follows that $W(A)$ is also a ring. The last two statements of the theorem are obvious from the definitions of addition and multiplication in $W(A)$. Q.E.D.

■ (17.1.16) **Addendum** We have defined a functor W: **Ring** $\to$ **Ring** with the properties:

(i) as a set $W(A) = \{(a_1, a_2, \ldots) \mid a_i \in A\}$;
(ii) as a map of sets $W(\phi)$: $W(A) \to W(B)$ takes $(a_1, a_2, \ldots)$ into $(\phi(a_1), \phi(a_2), \ldots)$;
(iii) the w_n: $W(A) \to A$, $a \mapsto w_n(a)$ are ring homomorphisms for all $n \in \mathbf{N}$.

It follows from the proof given above that W is the unique functor **Ring** $\to$ **Ring** with these properties.

The functor W: **Ring** $\to$ **Ring** is representable, i.e., there is a ring R such that $W(A) = \mathbf{Ring}(R, A)$ functorially. In fact, $R = \mathbf{Z}[X_1, X_2, \ldots]$ clearly does the job. The addition formulas $\Sigma_1(X; Y)$, $\Sigma_2(X; Y)$, ... now define a homomorphism

$$(17.1.17)\quad \mathbf{Z}[X_1, X_2, \ldots] \to \mathbf{Z}[X_1, X_2, \ldots] \otimes \mathbf{Z}[X_1, X_2, \ldots]$$
$$X_i \mapsto \Sigma_i(X_1 \otimes 1, \ldots, X_i \otimes 1; 1 \otimes X_1, \ldots, 1 \otimes X_i)$$

defining a coassociative, cocommutative comultiplication on $\mathbf{Z}[X_1, X_2, \ldots]$. Taking Spec we find an affine group scheme $W = \mathrm{Spec}(\mathbf{Z}[X_1, X_2, \ldots])$. The points of this group scheme with values in a ring A are of course precisely the elements of $W(A)$.

■ (17.1.18) **The formal group law $\hat{W}(X, Y)$** The sequence of power series:

$$\Sigma_1(X, Y), \quad \Sigma_2(X, Y), \quad \Sigma_3(X, Y), \quad \ldots$$

(which are in reality polynomials) defines an infinite dimensional formal group law in the sense of Definition (9.6.1). To see this we first remark that if we give X_i and Y_i weight i, then $w_n(X)$ and $w_n(Y)$ are homogeneous of weight n. Using $w_n(\Sigma_n(X; Y)) = w_n(X) + w_n(Y)$, it follows from this that $\Sigma_n(X; Y)$ is homogeneous of weight n, which implies that the coefficient of $X^{\mathbf{k}}Y^{\mathbf{l}}$ in $\Sigma_n(X; Y)$ is zero if

$$n > \sum_{j \in \mathrm{supp}(\mathbf{k})} j\mathbf{k}(j) + \sum_{j \in \mathrm{supp}(\mathbf{l})} j\mathbf{l}(j)$$

so that condition (9.6.3) is satisfied. Also $w_n(X) \equiv nX_n \mod(X_1, \ldots, X_{n-1})$, $\Sigma_i(X; Y) \equiv 0 \mod(X_1, \ldots, X_{n-1}; Y_1, \ldots, Y_{n-1})$ if $i < n$ so that $\Sigma_n(X; Y) \equiv X_n + Y_n \mod(X_1, \ldots, X_{n-1}; Y_1, \ldots, Y_{n-1})$ which because $\Sigma_n(X; Y)$ is homogeneous of weight n implies that $\Sigma_n(X; Y) \equiv X_n + Y_n \mod(\text{degree } 2)$. Finally, (9.6.4) and (9.6.5) (associativity and commutativity) are satisfied because Witt vector addition is associative and commutative. We shall use

$\hat{W}(X, Y)$ to denote this formal group law and $\hat{W}$ to denote the associated formal group.

17.2 The universal λ-ring $\Lambda(A)$

Let A be a ring, and let $\Lambda(A)$ denote the set of all power series $f(t)$ in one indeterminate t of the form

$$f(t) = 1 + a_1 t + a_2 t^2 + \cdots, \qquad a_i \in A$$

(Instead of $\Lambda(A)$ one also often finds $1 + tA[\![t]\!]$ in the literature.) Multiplication of power series defines an addition on $\Lambda(A)$ which turns $\Lambda(A)$ into an abelian group with as zero element the element $1 \in \Lambda(A)$. We are going to define also a multiplication on $\Lambda(A)$ which will make $\Lambda(A)$ into a ring. To do so we first define some universal polynomials.

■ (17.2.1) **Intermezzo concerning symmetric functions** Let $\xi_1, \xi_2, \ldots, \xi_r; \eta_1, \ldots, \eta_s$ be indeterminates. We define X_i and Y_i by the equations

$$(1 + X_1 t + X_2 t^2 + \cdots) = \prod_i (1 - \xi_i t),$$

$$(1 + Y_1 t + Y_2 t^2 + \cdots) = \prod_i (1 - \eta_i t)$$

In other words the X_i and Y_i are up to sign the elementary symmetric functions in the ξ_j and η_j. Now consider the symmetric expressions

$$\prod_{i,j} (1 - \xi_i \eta_j t) = 1 + P_1 t + P_2 t^2 + \cdots$$

$$\prod_i (1 - \xi_i^n t) = 1 + Q_{n,1} t + Q_{n,2} t^2 + \cdots$$

By the fundamental theorem on symmetric functions P_i can be written as a polynomial $P_i(X_1, \ldots, X_i; Y_1, \ldots, Y_i)$ in the $X_1, \ldots, X_i; Y_1, \ldots, Y_i$ and $Q_{n,i}$ can be written as a polynomial $Q_{n,i}(X_1, \ldots, X_{ni})$ in the $X_1, X_2, \ldots, X_{ni}$. Moreover, these polynomials $P_i(X; Y)$, $Q_{n,i}(X)$ are independent of r and s (the number of ξ's and the number of η's) provided $r, s \geq i$ for $P_i(X; Y)$ and $r \geq ni$ for $Q_{n,i}(X)$.

This means that we can write formally

$$\prod_{i=1}^{\infty} (1 - \xi_i t) = 1 + X_1 t + X_2 t^2 + \cdots$$

$$\prod_{i=1}^{\infty} (1 - \eta_i t) = 1 + Y_1 t + Y_2 t^2 + \cdots$$

$$\prod_{i,j=1}^{\infty} (1 - \xi_i \eta_j t) = 1 + P_1(X_1; Y_1)t + P_2(X_1, X_2; Y_1, Y_2)t^2 + \cdots$$

$$\prod_{i=1}^{\infty} (1 - \xi_i^n t) = 1 + Q_{n,1}(X_1, \ldots, X_n)t + Q_{n,2}(X_1, \ldots, X_{2n})t^2 + \cdots$$

(symmetric functions in an infinity of indeterminates).

The polynomials P_n will be used below to define the multiplication on $\Lambda(A)$; the polynomials $Q_{n,i}$ will be used later to define Frobenius operators.

■ (17.2.2) **Multiplication on $\Lambda(A)$** We now define a multiplication on $\Lambda(A)$ by means of the formula

$$(17.2.3)\qquad (1 + a_1 t + a_2 t^2 + \cdots) * (1 + b_1 t + b_2 t^2 + \cdots) = 1 + P_1(a; b)t + P_2(a; b)t^2 + \cdots$$

To show that this multiplication and the addition defined above do indeed turn $\Lambda(A)$ into a ring we define a number of functions s_n: $\Lambda(A) \to A$, as follows

$$(17.2.4)\qquad s_1 t + s_2 t^2 + \cdots = -\frac{tf'(t)}{f(t)} = -t\frac{d}{dt}\log(f(t))$$

■ (17.2.5) **Lemma** For all $f(t)$, $g(t) \in \Lambda(A)$, we have

$$s_n(f(t)g(t)) = s_n(f(t)) + s_n(g(t))$$
$$s_n(f(t) * g(t)) = s_n(f(t))s_n(g(t))$$

Proof The first statement of the lemma is immediate from (17.2.4). To prove the second statement we write formally

$$f(t) = \prod_{i=1}^{\infty} (1 - \xi_i t), \qquad g(t) = \prod_{i=1}^{\infty} (1 - \eta_i t)$$

By formula (17.2.4) we then see that the $s_n(f(t))$, $s_n(g(t))$ can be expressed as

$$s_n(f(t)) = \sum_{i=1}^{\infty} \xi_i^n, \qquad s_n(g(t)) = \sum_{i=1}^{\infty} \eta_i^n$$

and $s_n(f(t) * g(t))$ is equal to the coefficient of t^n in

$$-t\frac{d}{dt}\log\left(\prod_{i,j=1}^{\infty} (1 - \xi_i\eta_j t)\right) = \sum_{i,j=1}^{\infty} \frac{\xi_i\eta_j t}{1 - \xi_i\eta_j t} = \sum_{i,j=1}^{\infty} (\xi_i\eta_j t + (\xi_i\eta_j t)^2 + \cdots)$$

This proves the second statement of the lemma.

■ (17.2.6) **Proposition** $\Lambda(A)$ with the addition and multiplication defined above is a ring, and the s_n: $\Lambda(A) \to A$ are ring homomorphisms. Moreover, if ϕ: $A \to B$ is a homomorphism of rings, then $\Lambda(\phi)$: $\Lambda(A) \to \Lambda(B)$, $1 + a_1 t + a_2 t^2 + \cdots \mapsto 1 + \phi(a_1)t + \phi(a_2)t^2 + \cdots$ is a ring homomorphism. We have thus defined a functor Λ: **Ring** $\to$ **Ring**.

Proof That $\Lambda(\phi)$ is compatible with the addition and multiplication defined above follows immediately from the fact that addition and mult

plication are defined by means of (universal) polynomials with coefficients in $\mathbf{Z}$. The rest of the proof is exactly analogous to the proof that $W(A)$ is a ring (Theorem (17.1.15)); the role of the w_n in the proof of (17.1.15) is here played by the s_n.

■ (17.2.7) **The exponential map $W(A) \to \Lambda(A)$** For every ring A, we define a map $\bar{E}_A\colon W(A) \to \Lambda(A)$ by the formula

$$\bar{E}_A((a_1, a_2, \ldots)) = \prod_{i=1}^{\infty} (1 - a_i t^i) \tag{17.2.8}$$

■ (17.2.9) **Proposition** The map $\bar{E}_A$ is bijective for all rings A; and, moreover, $\bar{E}_A(a + b) = \bar{E}_A(a)\bar{E}_A(b)$, $\bar{E}_A(ab) = \bar{E}_A(a) * \bar{E}_A(b)$, and $\bar{E}_A$ is an isomorphism of rings. In addition if $\phi\colon A \to B$ is a homomorphism of rings, then $\Lambda(\phi)\bar{E}_A = \bar{E}_B W(\phi)$ so that the $\bar{E}_A$ define an isomorphism of ring-valued functors $\bar{E}\colon W \to \Lambda$. Finally, we have $s_n \bar{E}_A = w_n$.

Proof That $\bar{E}_A$ is bijective is immediate, and $\Lambda(\phi)\bar{E}_A = \bar{E}_B W(\phi)$ also follows immediately from the definitions. Having this, to prove that $\bar{E}_A$ is a homomorphism it suffices (by the now familiar trick used in the proof of Theorem (17.1.15) (and Proposition (17.2.6)) to show that

$$s_n(\bar{E}_A(ab)) = s_n(\bar{E}_A(a) * \bar{E}_A(b))$$

and

$$s_n(\bar{E}_A(a + b)) = s_n(\bar{E}_A(a)) \dotplus s_n(\bar{E}_A(b))$$

for all $n \in \mathbf{N}$. And this in turn follows from $s_n \bar{E}_A = w_n$ because s_n and w_n are both ring homomorphisms. Thus it remains to show only that $s_n(\bar{E}_A(a)) = w_n(a)$ for all A and $a \in W(A)$. We have

$$-t\frac{d}{dt}\log(\bar{E}_A(a)) = \sum_{i=1}^{\infty} \frac{i a_i t^i}{1 - a_i t^i} = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} i(a_i t^i)^j$$

$$= \sum_{n=1}^{\infty} \left(\sum_{i \mid n} i a_i^{n/i} \right) t^n = \sum_{n=1}^{\infty} w_n(a) t^n$$

This concludes the proof of the proposition.

■ (17.2.10) **Remarks** The ring $\Lambda(A)$ has even more structure. It is a so-called λ-ring, which means that there are "exterior product operations" $\lambda^i\colon \Lambda(A) \to \Lambda(A)$ which satisfy certain properties. See (E.2.1) for some notes on λ-rings (and Adams operations and Artin–Hasse exponentials); see (E.2.2) for some notes on universality properties of the functor $A \mapsto \Lambda(A)$.

■ (17.2.11) **Curves in $\hat{\mathbf{G}}_{\mathrm{m}}^{-}(X, Y)$** Let $\hat{\mathbf{G}}_{\mathrm{m}}^{-}(X, Y)$ be the one dimensional formal group law $\hat{\mathbf{G}}_{\mathrm{m}}^{-}(X, Y) = X + Y - XY$. Let $\gamma_1(t)$ and $\gamma_2(t)$ be two curves in $\hat{\mathbf{G}}_{\mathrm{m}}^{-}(X, Y)$; then

$$\gamma_1(t) +_{\hat{\mathbf{G}}_{\mathrm{m}}^{-}} \gamma_2(t) = -(1 - \gamma_1(t))(1 - \gamma_2(t)) + 1$$

so that the map $\gamma(t) \mapsto 1 - \gamma(t)$ defines an isomorphism of groups $\mathscr{C}(\hat{\mathbf{G}}_m^-; A) \simeq \Lambda(A)$ which combined with the isomorphism $\Lambda(A) \simeq W(A)$ identifies the group of curves over A in $\hat{\mathbf{G}}_m^-$ with the underlying group of the ring of generalized Witt vectors with coordinates in A.

■(17.2.12) **p-Typical curves in $\hat{\mathbf{G}}_m^-(X, Y)$** Let p be a prime number and let $\mathscr{C}_p(\hat{\mathbf{G}}_m^-, A)$ be the subgroup of p-typical curves of $\mathscr{C}(\hat{\mathbf{G}}_m^-, A)$, and let $\Lambda_{p^\infty}(A)$ be the subgroup of $\Lambda(A)$ corresponding to $\mathscr{C}_p(\hat{\mathbf{G}}_m^-; A)$ under the isomorphism β: $\gamma(t) \mapsto 1 - \gamma(t)$.

■(17.2.13) **Lemma** $\Lambda_{p^\infty}(A)$ is closed under the multiplication of $\Lambda(A)$.

Proof It suffices to prove this for characteristic zero rings. Let

$$a(t) = 1 + a_1 t + \cdots = \prod_{i=1}^{\infty} (1 - \xi_i t)$$

then $a(t)$ is in $\Lambda_{p^\infty}(A)$ if and only if

$$\log a(t) = \sum_{l=0}^{\infty} c_l t^{p^l}$$

for certain $c_l \in A \otimes \mathbf{Q}$. That is, $a(t)$ is in $\Lambda_{p^\infty}(A)$ iff $s_i(a(t)) = 0$ for all i that are not a power of p. The lemma follows from this.

■(17.2.14) **Lemma** If A is a $\mathbf{Z}_{(p)}$-algebra, then the power series $\Phi(t) = \prod_{(p,n)=1} (1 - t^n)^{\mu(n)/n}$, where $\mu(n)$ is the Möbius function, is in $\Lambda_{p^\infty}(A)$, and

$$a(t) * \prod_{(p,n)=1} (1 - t^n)^{\mu(n)/n} = a(t) \tag{17.2.15}$$

if $a(t)$ in $\Lambda_{p^\infty}(A)$.

Proof We have (if A is of characteristic zero)

$$\log\left(\prod_{(p,n)=1} (1 - t^n)^{\mu(n)/n}\right) = \sum_{(p,n)=1} \frac{\mu(n)}{n} \log(1 - t^n)$$

$$= -\sum_{(p,n)=1} \sum_{k=1}^{\infty} \frac{\mu(n)}{n} \frac{t^{nk}}{k} = -\sum_{r=1}^{\infty} \sum_{\substack{n|r \\ (n,p)=1}} \frac{\mu(n)}{r} t^r$$

$$= -\sum_{l=0}^{\infty} p^{-l} t^{p^l}$$

(because if $r = p^k m$, $(p, m) = 1$, then $\sum_{(n,p)=1, n|r} \mu(n) = \sum_{n|m} \mu(n)$, which is equal to zero if $m > 1$ and equal to 1 if $m = 1$). This shows that

$$s_i\left(\prod_{(p,n)=1} (1 - t^n)^{\mu(n)/n}\right) = \begin{cases} 0 & \text{if } i \text{ is not a power of } p \\ 1 & \text{if } i \text{ is a power of } p \end{cases} \tag{17.2.16}$$

which proves (17.2.15) (for characteristic zero rings A and hence by functoriality for all rings A), once we have shown that $\Phi(t)$ has its coefficients in $\mathbf{Z}_{(p)}$. But $-\sum_{l=0}^{\infty} p^{-l}t^{p^l}$ and $\log(1+t) = \sum_{n=1}^{\infty} n^{-1}(-1)^{n+1}t^n$ both satisfy a functional equation

$$f(t) - p^{-1}f(t) \in \mathbf{Z}_{(p)}[t]$$

so that by the functional equation lemma 2.2, $\Phi(t) = \exp(-\sum_{l=0}^{\infty} p^{-l}t^{p^l})$ has its coefficients in $\mathbf{Z}_{(p)}$. (Cf. also 2.3 where practically the same power series are treated.)

■ (17.2.17) **Corollary** The subgroup $\Lambda_{p^\infty}(A)$ of $\Lambda(A)$ with the multiplication induced by $\Lambda(A)$ is a ring. The unit element is $\prod_{(p,n)=1}(1-t^n)^{\mu(n)/n}$. It is *not* a subring of $\Lambda(A)$ because the unit elements of $\Lambda(A)$ and $\Lambda_{p^\infty}(A)$ do not coincide.

17.3 Frobenius and Verschiebung

We are now going to define Frobenius ring endomorphisms $\mathbf{f}_n$: $W(A) \to W(A)$ for all $n \in \mathbf{N}$ and additive operators $\mathbf{V}_n$: $W(A) \to W(A)$, $n \in \mathbf{N}$, $\langle c \rangle$: $W(A) \to W(A)$, $c \in A$. It is easier to define these (especially Frobenius's) on $\Lambda(A)$. To do this we use the polynomials $Q_{n,i}(X)$ defined in Section (17.2.1). The definition is then

(17.3.1) $$\mathbf{f}_n^{\wedge}(1 + a_1 t + a_2 t^2 + \cdots) = 1 + Q_{n,1}(a)t + Q_{n,2}(a)t^2 + \cdots$$

We recall from (17.2.1) that this means in terms of additional variables ξ_1, $\xi_2, \cdots$

(17.3.2) $$1 + a_1 t + a_2 t^2 + \cdots = \sum_{i=1}^{\infty} (1 - \xi_i t)$$

$$\mathbf{f}_n^{\wedge}(1 + a_1 t + a_2 t^2 + \cdots) = \sum_{i=1}^{\infty} (1 - \xi_i^n t)$$

Let us calculate the $s_m \mathbf{f}_n^{\wedge}$. We have (using (17.3.2))

$$-t\frac{d}{dt}\log(\mathbf{f}_n(1 + a_1 t + a_2 t^2 + \cdots)) = \sum_{i=1}^{\infty} \frac{\xi_i^n t}{1 - \xi_i^n t} = \sum_{i=1}^{\infty} \{(\xi_i^n t) + (\xi_i^n t)^2 + \cdots\}$$

so that

$$s_m(f_n(1 + a_1 t + a_2 t^2 + \cdots)) = \sum_{i=1}^{\infty} \xi_i^{mn} = s_{mn}(1 + a_1 t + a_2 t^2 + \cdots)$$

which proves that

(17.3.3) $$s_m \mathbf{f}_n^{\wedge} = s_{mn}$$

Now the $\mathbf{f}_n^{\wedge}$, being defined by universal polynomials, are compatible with the homomorphisms $\Lambda(\phi)$: $\Lambda(A) \to \Lambda(B)$ induced by homomorphisms ϕ: $A \to B$. It

follows from this (using again the type of argument used in the proof of Theorem (17.1.15)) that the $\mathbf{f}_n^\wedge$ are characterized by property (17.3.3) together with the fact that they are functor endomorphisms $\mathbf{f}_n^\wedge\colon \Lambda \to \Lambda$.

We now define the operators $\mathbf{V}_n^\wedge$, $\langle c\rangle^\wedge$, $c \in A$, by the formulas

$$\mathbf{V}_n^\wedge(1 + a_1 t + a_2 t^2 + \cdots) = 1 + a_1 t^n + a_2 t^{2n} + \cdots \tag{17.3.4}$$

$$\langle c\rangle^\wedge(1 + a_1 t + a_2 t^2 + \cdots) = 1 + a_1 ct + a_2 (ct)^2 + \cdots, \qquad c \in A \tag{17.3.5}$$

In terms of the s_m the $\mathbf{V}_n^\wedge$ and $\langle c\rangle^\wedge$ are characterized by

$$\begin{cases} s_m \mathbf{V}_n^\wedge = 0 & \text{if } n \text{ does not divide } m \\ s_m \mathbf{V}_n^\wedge = n s_{m/n} & \text{if } n \text{ does divide } m \end{cases} \tag{17.3.6}$$

$$s_m \langle c\rangle^\wedge = c^m s_m \tag{17.3.7}$$

This is not difficult to prove. Writing $1 + a_1 t + a_2 t^2 + \cdots = \prod_{i=1}^\infty (1 - \xi_i t)$, we have

$$-t\frac{d}{dt}\log\left(\mathbf{V}_n\left(\prod_{i=1}^\infty (1 - \xi_i t)\right)\right) = -t\frac{d}{dt}\log\left(\prod_{i=1}^\infty (1 - \xi_i t^n\right) = \sum_{i=1}^\infty \frac{n\xi_i t^n}{1 - \xi_i t^n}$$

which proves (17.3.6). (Recall that $s_m(\prod_{i=1}^\infty (1 - \xi_i t)) = \sum_{i=1}^\infty \xi_i^m$.) To prove (17.3.7) we observe

$$-t\frac{d}{dt}\log\langle c\rangle\left(\prod_{i=1}^\infty (1 - \xi_i t)\right) = -t\frac{d}{dt}\log\left(\prod_{i=1}^\infty (1 - c\xi_i t)\right) = \sum_{i=1}^\infty \frac{c\xi_i}{1 - c\xi_i t}$$

Now let $\bar{E}_A\colon W(A) \to \Lambda(A)$ be the isomorphism of Proposition (17.2.9). We define the operators $\mathbf{f}_n$, $\mathbf{V}_n$, $\langle c\rangle\colon W(A) \to W(A)$ by structure transport via $\bar{E}_A$, that is, $\mathbf{f}_n = \bar{E}_A^{-1}\mathbf{f}_n^\wedge \bar{E}_A$, and similarly for $\mathbf{V}_n$ and $\langle c\rangle$. Because $s_n \bar{E}_A = w_n$, the $\mathbf{f}_n$, $\mathbf{V}_n$, $\langle c\rangle$ are characterized by the formulas

$$\begin{aligned} w_m \mathbf{f}_n &= w_{nm} \\ w_m\langle c\rangle &= c^m w_m \\ w_m \mathbf{V}_n &= \begin{cases} 0 & \text{if } n \text{ does not divide } m \\ n w_{m/n} & \text{if } n \text{ does divide } m \end{cases} \end{aligned} \tag{17.3.8}$$

■(17.3.9) **Proposition** Let $\beta\colon \mathscr{C}(\hat{\mathbf{G}}_m^-; A) \to \Lambda(A)$ be the isomorphism $\gamma(t) \mapsto 1 - \gamma(t)$ where $\hat{\mathbf{G}}_m^-(X, Y) = X + Y - XY$. Let $\hat{\mathbf{f}}_n$, $\hat{\mathbf{V}}_m$, $\langle c\rangle$ denote the Frobenius, Verschiebungs, and homothety operators defined in Section 15.1 on the group of curves $\mathscr{C}(\hat{\mathbf{G}}_m^-; A)$. Then we have $\beta\hat{\mathbf{f}}_n = \mathbf{f}_n^\wedge\beta$, $\beta\hat{\mathbf{V}}_n = \mathbf{V}_n^\wedge\beta$, $\beta\langle c\rangle = \langle c\rangle^\wedge\beta$. That is, the isomorphism β preserves the Frobenius, Verschiebungs, and homothety operators.

■(17.3.10) **Corollary** The operators $\mathbf{f}_n^\wedge$, $\mathbf{V}_n^\wedge$, $\langle c\rangle^\wedge$ on $\Lambda(A)$ and the operators $\mathbf{f}_n$, $\mathbf{V}_n$, $\langle c\rangle$ on $W(A)$ satisfy the relations (16.2.1)–(16.2.9).

(This can also be proved directly by using the characterizations (17.3.8).)

■(17.3.11) **Proof of Proposition (17.3.9)** That $\beta\hat{\mathbf{V}}_n = \mathbf{V}_n^\wedge\beta$ and $\beta\langle c\rangle = \langle c\rangle^\wedge\beta$ is obvious from the definitions. To show that $\beta\hat{\mathbf{f}}_n = \mathbf{f}_n^\wedge\beta$ for all rings A it suffices to do this (by the functoriality of $\beta, \hat{\mathbf{f}}_n, \mathbf{f}_n^\wedge$) for characteristic zero rings A (trick of Theorem (17.1.15) again) and hence it suffices to show that $s_m\beta\hat{\mathbf{f}}_n = s_m\mathbf{f}_n^\wedge\beta$. Finally, because s_m, β, $\hat{\mathbf{f}}_n$, $\mathbf{f}_n^\wedge$ are all additive, it suffices to show that

$$s_m\beta\hat{\mathbf{f}}_n(at^r) = s_m\mathbf{f}_n^\wedge\beta(at^r) \tag{17.3.12}$$

We first calculate the right-hand side of (17.3.12). We have

$$\mathbf{f}_n^\wedge\beta(at^r) = \mathbf{f}_n^\wedge(1 - at^r) = \mathbf{f}_n^\wedge\left(\prod_{j=1}^{r}(1 - a^{1/r}\zeta_r^j t)\right)$$

$$= \prod_{j=1}^{r}(1 - a^{n/r}\zeta_r^{nj}t)$$

where ζ_r is a primitive rth root of unity. Applying $-t(d/dt)\log$ to this we find

$$-t\frac{d}{dt}\log\left(\prod_{j=1}^{r}(1 - a^{n/r}\zeta_r^{nj}t)\right) = \sum_{j=1}^{r}\frac{a^{n/r}\zeta_r^{nj}t}{1 - a^{n/r}\zeta_r^{nj}t}$$

$$= \sum_{k=1}^{\infty}\sum_{j=1}^{r}a^{kn/r}\zeta_r^{knj}t^k$$

Now

$$\sum_{j=1}^{r}\zeta_r^{knj} = \begin{cases}0 & \text{if } r \nmid nk\\ r & \text{if } r \mid nk\end{cases}$$

Write $n = dl, r = dm$, with $d = (n, r)$, $(l, m) = 1$. Then $r \mid nk \Leftrightarrow k = sm$ for a certain $s \in \mathbf{N}$. Using this we finally find

$$-t\frac{d}{dt}\log(\mathbf{f}_n^\wedge\beta(at^r)) = \sum_{s=1}^{\infty}ra^{smdl/dm}t^{sm} = \sum_{s=1}^{\infty}ra^{sl}t^{sm} \tag{17.3.13}$$

Now the left-hand side of (17.3.12) is calculated as follows

$$(\beta\hat{\mathbf{f}}_n(at^r)) = \prod_{i=1}^{n}(1 - a\zeta_n^{ir}t^{r/n})$$

so that

$$\log(\beta\hat{\mathbf{f}}_n(at^r)) = -\sum_{i=1}^{n}\sum_{k=1}^{\infty}k^{-1}a^k\zeta_n^{irk}t^{kr/n}$$

But

$$\sum_{i=1}^{n}\zeta_n^{irk} = \begin{cases}0 & \text{if } n \nmid rk\\ n & \text{if } n \mid rk\end{cases}$$

Writing again $n = dl$, $r = dm$, $(l, m) = 1$, we see that $n \mid rk$ is equivalent to $k = lj$ for a certain $j \in \mathbf{N}$. Using this we find

$$\log(\beta\hat{\mathbf{f}}_n(at^r)) = -\sum_{j=1}^{\infty} \frac{dl}{lj} a^{lj} t^{ljdm/dl} = -\sum_{j=1}^{\infty} dj^{-1} a^{lj} t^{mj}$$

and we find

$$-t\frac{d}{dt}\log(\beta\hat{\mathbf{f}}_n(at^r)) = \sum_{j=1}^{\infty} mjdj^{-1}a^{lj}t^{mj} = \sum_{j=1}^{\infty} ra^{jl}t^{jm} \tag{17.3.14}$$

Comparing (17.3.13) and (17.3.14), we see that we have proved the proposition.

■ (17.3.15) **Remarks**

(i) The relations (16.2.1)–(16.2.9) can also be proved by using the characterizations (17.3.3), (17.3.6)–(17.3.8) of $\mathbf{f}_n^\wedge$, $\mathbf{V}_n^\wedge$, $\langle c\rangle^\wedge$ and $\mathbf{f}_n$, $\mathbf{V}_n$, and $\langle c\rangle$.

(ii) We could of course have defined $\mathbf{f}_n$ on $W(A)$ by transport of structure via the isomorphisms β and $\bar{E}_A$. In that case the calculations of (17.3.11) provide one with a different and often useful method for calculating $\mathbf{f}_n$.

Some additional explicit information on how the $\mathbf{V}_n$, $\mathbf{f}_n$, $\langle c\rangle$ act on $W(A)$ is given by the following

■ (17.3.16) **Proposition** Let $\iota_n \in W(A)$ be the element $\iota_n = (0, 0, \ldots, 0, 1, 0, \ldots)$ with the 1 in the nth spot and let $a = (a_1, a_2, \ldots)$ and $b = (b_1, b_2, \ldots)$ be two elements of $W(A)$. One has

$$\mathbf{V}_n(a(\mathbf{f}_n b)) = (\mathbf{V}_n a)b \tag{17.3.17}$$

$$\mathbf{V}_n\mathbf{f}_n a = \iota_n a \tag{17.3.18}$$

$$\mathbf{V}_n a = (\underbrace{0, \ldots, 0}_{n-1}, a_1, \underbrace{0, \ldots, 0}_{n-1}, a_2, 0, \ldots) \tag{17.3.19}$$

$$\langle c\rangle a = (ca_1, c^2a_2, c^3a_3, \ldots) \tag{17.3.20}$$

If A is of characteristic p, where p is a prime number, i.e., $pc = 0$ for all $c \in A$, then we have in addition

$$\mathbf{f}_p a = (a_1^p, a_2^p, a_3^p, \ldots) \tag{17.3.21}$$

$$\mathbf{f}_p\mathbf{V}_p = p = \mathbf{V}_p\mathbf{f}_p = \iota_p \tag{17.3.22}$$

Proof Formulas (17.3.17)–(17.3.20) are proved in the usual way. It suffices to prove them in the case of a characteristic zero ring, and that is done by applying w_k to both sides and checking that the results are equal. One finds in the case of (17.3.17): if n does not divide k, then $w_k(\mathbf{V}_n(a(\mathbf{f}_n b))) = 0$ and $w_k((\mathbf{V}_n a)b) = (w_k\mathbf{V}_n a)w_k(b) = 0 \cdot w_k(b) = 0$; and if n does divide k,

$$w_k(\mathbf{V}_n(a(\mathbf{f}_n b))) = nw_{k/n}(a(\mathbf{f}_n b)) = nw_{k/n}(a)w_{k/n}(\mathbf{f}_n b) = nw_{k/n}(a)w_k(b)$$

and

$$w_k((\mathbf{V}_n a)b)) = w_k(\mathbf{V}_n a)w_k(b) = nw_{k/n}(a)w_k(b)$$

To check (17.3.19) we proceed as follows. Write

$$\bar{a} = (\bar{a}_1, \bar{a}_2, \bar{a}_3, \ldots) = (0, \ldots, 0, a_1, 0, 0, \ldots, 0, a_2, 0, \ldots)$$

Then we have

$$w_k(\bar{a}) = \sum_{d|k} d\bar{a}_d^{k/d} = \sum_{d|k, n|d} d\bar{a}_d^{k/d}$$

So if n does not divide k, $w_k(\bar{a}) = 0$; and if n does divide k, we have

$$\sum_{d|k, n|d} d\bar{a}_d^{k/d} = \sum_{j|(k/n)} nj\bar{a}_{nj}^{k/nj} = \sum_{j|(k/n)} nja_j^{(k/n)/j} = nw_{k/n}(a)$$

To prove (17.3.18) first note that $\imath_1$ is the identity element of $W(A)$ and that hence $\imath_n = \mathbf{V}_n 1 = \mathbf{V}_n \imath_1$. Now apply (17.3.17) with $\imath_1 = 1$ for a and a for b.

The proof of (17.3.20) is left to the reader.

To prove (17.3.21) and (17.3.22) note that $\bar{E}(A)(\imath_p) = (1 - t^p) = (1 - t)^p = \bar{E}(A)(p)$. So that $\imath_p = p$ in $W(A)$ if A is of characteristic p. This proves (17.3.22) in view of (17.3.18) and $\mathbf{f}_p\mathbf{V}_p = p$ which always holds (cf. Corollary (17.3.10)). Finally, if $\bar{E}(A)(a) = 1 + \sum c_i t^i$, then by (17.3.22) $\mathbf{V}_p^\wedge \mathbf{f}_p^\wedge(\bar{E}(A)(a)) = 1 + \sum c_i^p t^{ip}$ which by the definition of $\mathbf{V}_p$ implies that $\mathbf{f}_p^\wedge(\bar{E}(A)(a)) = 1 + \sum c_i^p t^i$. (Note that $\mathbf{V}_n$ is always injective.) But if A is of characteristic p,

$$\bar{E}(A)(a_1^p, a_2^p, a_3^p, \ldots)$$

$$= \prod_{i=1}^{\infty} (1 - a_i^p t^i) = 1 + \sum c_i^p t^i \qquad \text{if} \quad \bar{E}(A)(a_1, a_2, \ldots) = 1 + \sum c_i t^i$$

This proves (17.3.21) because $\bar{E}(A)$ is an isomorphism.

■ (17.3.23) **Remark** The Frobenius operators $\mathbf{f}_n^\wedge$ on $\Lambda(A)$ are the same as the Adams operations Ψ^n on the λ-ring $\Lambda(A)$; cf. (E.2.1).

17.4 Supernatural quotients of $W(A)$

■ (17.4.1) **Definitions** We define a supernatural number $\mathfrak{n}$ as a formal expression

$$\mathfrak{n} = \prod_p p^{\alpha_p}$$

where p runs through all prime numbers and $\alpha_p \in \mathbf{N} \cup \{\infty\} \cup \{0\}$. For $n \in \mathbf{N}$ and p a prime number, let $v_p(n)$ be the p-valuation of n, i.e., the largest integer k such that $p^k \mid n$. Given a supernatural number $\mathfrak{n}$ we define

$$\mathbf{N}(\mathfrak{n}) = \{n \in \mathbf{N} \mid v_p(n) \leq \alpha_p \text{ for all } p\}$$

For example, if p is a fixed prime number and $\mathfrak{n} = p^\infty$, then $\mathbf{N}(\mathfrak{n})$ consists of all the numbers p^r, $r \in \mathbf{N} \cup \{0\}$.

Let $\mathfrak{n}$ be a supernatural number and A a ring, then we define the set $\mathfrak{A}_{\mathfrak{n}}(A) \subset W(A)$ as

$$\mathfrak{A}_{\mathfrak{n}}(A) = \{(a_1, a_2, \ldots) \mid a_d = 0 \text{ for all } d \in \mathbf{N}(\mathfrak{n})\} \tag{17.4.2}$$

■ (17.4.3) **Lemma** $\mathfrak{A}_{\mathfrak{n}}(A)$ is an ideal of $W(A)$ for all supernatural numbers $\mathfrak{n}$.

Proof By definition $w_n(X)$ involves only the X_d with $d \mid n$. It follows readily from this (by induction) that $\Sigma_n(X; Y)$ and $\Pi_n(X; Y)$ involve only those X_d and Y_d for which $d \mid n$. This proves the lemma, because also $\Pi_n(X; Y) \equiv 0 \mod(X_1, \ldots, X_n)$.

■ (17.4.4) **Definitions** For each supernatural number $\mathfrak{n}$ and ring A, we define a ring of Witt vectors $W_{\mathfrak{n}}(A)$ as

$$W_{\mathfrak{n}}(A) = W(A)/\mathfrak{A}_{\mathfrak{n}}(A)$$

It is easy to check that if $\phi\colon A \to B$ is a ring homomorphism, then $W(\phi)\mathfrak{A}_{\mathfrak{n}}(A) \subset \mathfrak{A}_{\mathfrak{n}}(B)$, so that $W(\phi)$ induces a homomorphism

$$W_{\mathfrak{n}}(\phi)\colon W_{\mathfrak{n}}(A) \to W_{\mathfrak{n}}(B)$$

making $W_{\mathfrak{n}}$ into a functor **Ring** $\to$ **Ring**. We shall use $\varepsilon_{\mathfrak{n}}$ or occasionally $\varepsilon_{\mathfrak{n},A}$ to denote the canonical (functorial) projection $W(A) \to W_{\mathfrak{n}}(A)$. The induced projections $W_{\mathfrak{n}}(A) \to W_{\mathfrak{m}}(A)$ if $\mathfrak{m} \mid \mathfrak{n}$ are denoted $\varepsilon_{\mathfrak{n},\mathfrak{m}}$. Both $\varepsilon_{\mathfrak{n}}$ and $\varepsilon_{\mathfrak{n},\mathfrak{m}}$ are functor homomorphisms between ring-valued functors.

Now let $n \in \mathbf{N}(\mathfrak{n})$, then because $w_m \mathbf{f}_n = w_{nm}$, it follows that $\mathbf{f}_n \mathfrak{A}_{\mathfrak{n}} \subset \mathfrak{A}_{\mathfrak{n}}$ for all $n \in \mathbf{N}(\mathfrak{n})$ (this is proved first for characteristic zero rings and then for all rings, as usual). It follows that $\mathbf{f}_n\colon W(A) \to W(A)$ induces a homomorphism of rings $W_{\mathfrak{n}}(A) \to W_{\mathfrak{n}}(A)$ for all $n \in \mathbf{N}(\mathfrak{n})$ which we shall also denote $\mathbf{f}_n$. (If $n \notin \mathbf{N}(\mathfrak{n})$, then $\mathbf{f}_n\colon W_{\mathfrak{n}}(A) \to W_{\mathfrak{n}}(A)$ is not defined.) With respect to the $\mathbf{V}_n$ we have $\mathbf{V}_n \mathfrak{A}_{\mathfrak{n}} \subset \mathfrak{A}_{\mathfrak{n}}$ for all $n \in \mathbf{N}$; and in fact if $n \notin \mathbf{N}(\mathfrak{n})$, then $\mathbf{V}_n W(A) \subset \mathfrak{A}_{\mathfrak{n}}$ so that the $\mathbf{V}_n$ induce additive endomorphisms $\mathbf{V}_n\colon W_{\mathfrak{n}}(A) \to W_{\mathfrak{n}}(A)$ for all $n \in \mathbf{N}$. But the only interesting ones are the $\mathbf{V}_n$ with $n \in \mathbf{N}(\mathfrak{n})$ because $\mathbf{V}_n = 0\colon W_{\mathfrak{n}}(A) \to W_{\mathfrak{n}}(A)$ if $n \notin \mathbf{N}(\mathfrak{n})$.

In particular if $\mathfrak{n} = p^\infty$, then the only Frobenius homomorphisms $W_{p^\infty}(A) \to W_{p^\infty}(A)$ are the powers of $\mathbf{f}_p$ and the only nonzero Verschiebung maps are the powers of $\mathbf{V}_p$.

■ (17.4.5) **Description of** $W_{\mathfrak{n}}(A)$ The functor $W_{\mathfrak{n}}$ enjoys the following properties (cf. also Lemma (17.4.9)):

(i) As a set, $W_{\mathfrak{n}}(A) = \{(a_d)_{d \in \mathbf{N}(\mathfrak{n})} \mid a_d \in A\}$.
(ii) $W_{\mathfrak{n}}(\phi)((a_d)) = (\phi(a_d))$.
(iii) $w_n\colon W_{\mathfrak{n}}(A) \to A$ is a homomorphism of rings for all $n \in \mathbf{N}(\mathfrak{n})$.

(Note that $w_n\colon W_{\mathfrak{n}}(A) \to A$ for $n \in \mathbf{N}(\mathfrak{n})$ is well defined because $w_n(a_1, a_2, \ldots)$ "uses" only the a_d with d a divisor of n.)

And conversely W_n is the unique functor **Ring** $\to$ **Ring** that enjoys these properties.

Taking $n = p^\infty$ for a fixed prime number p, we obtain, for example, that W_{p^∞} is the following ring-valued functor; as a set-valued functor

$$W_{p^\infty}(A) = \{(a_{p^0}, a_{p^1}, a_{p^2}, \ldots) \mid a_{p^i} \in A\}$$

for which it is very tempting to write

$$W_{p^\infty}(A) = \{(b_0, b_1, b_2, \ldots) \mid b_i \in A\}$$

and $W_{p^\infty}(\phi)(b_0, b_1, \ldots) = (\phi(b_0), \phi(b_1), \ldots)$ for $\phi: A \to B$. The w_n for $n \in \mathbf{N}(p^\infty)$ are the w_{p^i} which are equal to

$$w_{p^i}(a_{p^0}, a_{p^1}, a_{p^2}, \ldots) = a_{p^0}^{p^i} + pa_{p^1}^{p^{i-1}} + \cdots + p^i a_{p^i}$$

or in terms of the $b_0, b_1, \ldots$

$$w_{p^i}(b_0, b_1, b_2, \ldots) = b_0^{p^i} + pb_1^{p^{i-1}} + \cdots + p^i b_i$$

which are the "classical" Witt polynomials so that $W_{p^\infty}(A)$ is the (classical) ring of Witt vectors of infinite length associated to the prime p.

■ (17.4.6) **Caveat** If $n \in \mathbf{N}$ is considered as a supernatural number, then $W_n(A)$ is *not* the ring of generalized Witt vectors of length n, i.e., $W_n(A)$ is not $\{(a_1, \ldots, a_n) \mid a_i \in A\}$ with the Witt addition and multiplication. These truncated rings of Witt vectors do not fall under the scheme given above but require separate definition. For each $n \in \mathbf{N}$, let $\mathfrak{A}_{\bar{n}}(A)$

$$\mathfrak{A}_{\bar{n}}(A) = \{(a_1, a_2, \ldots) \in W(A) \mid a_i = 0 \text{ for } i \leq n\}$$

The $\mathfrak{A}_{\bar{n}}(A)$ are clearly ideals in $W(A)$ because $\Sigma_i(X; Y) \equiv 0 \bmod(X_1, \ldots, X_n; Y_1, \ldots, Y_n)$ if $i \leq n$ and $\Pi_i(X; Y) \equiv 0 \bmod(X_1, \ldots, X_n)$ if $i \leq n$. We now define for each $n \in \mathbf{N}$, $W_{\bar{n}}(A) = W(A)/\mathfrak{A}_{\bar{n}}(A)$. These are also functors **Ring** $\to$ **Ring** and admit of a similar description as the functors W_n.

Note that $W_{p^n}(A)$ (no bar!) is the (classical) ring of Witt vectors of length $n + 1$ associated to the prime p. In the literature (e.g., [361]) one often finds the notation $W_{n+1}(A)$ for this ring (p being understood).

■ (17.4.7) **Remarks**

(i) There are natural (surjective) ring homomorphisms $W_{\bar{n}}(A) \to W_{\bar{m}}(A)$ if $n \geq m$ and $W(A) = \varprojlim W_{\bar{n}}(A)$.

(ii) There are also natural surjective ring homomorphisms $W_{p^n}(A) \to W_{p^m}(A)$ if $n \geq m$ and $W_{p^\infty}(A) = \varprojlim W_{p^n}(A)$.

■ (17.4.8) **Teichmüller mapping** For all supernatural numbers n we define a map $\tau: A \to W_n(A)$ as $\tau(a) = (b_d)_{d \in \mathbf{N}(n)}$ with $b_d = 0$ if $d \neq 1$ and $b_1 = a$. This mapping is multiplicative, i.e., $\tau(ab) = \tau(a)\tau(b)$, because $w_n(a, 0, 0, \ldots)w_n(b, 0, 0, \ldots) = a^n b^n = w_n(ab, 0, 0, \ldots)$ for all $n \in \mathbf{N} \cup \{0\}$.

The following lemma is often useful in calculations.

■ (17.4.9) **Lemma** Let $a = (a_d)$, $b = (b_d)$ be two elements of $W_n(A)$ and suppose that for all $d \in \mathbf{N}(n)$, $a_d = 0$ or $b_d = 0$. Then $a + b = (a_d + b_d)$.

Proof It suffices to prove this for characteristic zero rings A. We then have for $n \in \mathbf{N}(n)$

$$w_n((a_d + b_d)) = \sum_{d|n} d(a_d + b_d)^{n/d}$$

$$= \sum_{d|n} (da_d^{n/d} + db_d^{n/d}) = w_n((a_d)) + w_n((b_d))$$

because $(a_d + b_d)^{n/d} = a_d^{n/d} + b_d^{n/d}$ if $a_d = 0$ or $b_d = 0$. This proves the lemma.

■ (17.4.10) **Corollary** Every element $a = (a_d) \in W_n(A)$ can be written (uniquely) as a sum

$$a = \sum_{d \in \mathbf{N}(n)} \mathbf{V}_d(\tau(a_d))$$

■ (17.4.11) **Corollary** Suppose that A is a perfect field of characteristic $p > 0$ and let $b = (b_0, b_1, \ldots) \in W_{p^\infty}(A)$, then

$$b = \sum_{i=0}^{\infty} \tau(b_i^{p^{-i}})p^i$$

and this is the unique way of writing b as a sum $\sum \tau(c_i)p^i$.

Proof This follows from (17.4.10) because $\mathbf{f}_p\mathbf{V}_p = p = \mathbf{V}_p\mathbf{f}_p$ and $\mathbf{f}_p^i(\tau(a_i^{-p^i})) = \tau(a_i^{-p^i})^{p^i} = \tau(a_i)$ if A is of characteristic p; cf. (17.3.21).

■ (17.4.12) **Valuation** Let A be a perfect field of characteristic $p > 0$. For each $b = (b_0, b_1, \ldots) \in W_{p^\infty}$, we define $v(b) =$ largest $k \in \mathbf{N} \cup \{0\} \cup \{\infty\}$ such that $b_i = 0$ for all $i < k$. That is, $v(b) = \infty$ if and only if $b = 0$, and $v(b) = k$ means that $b_0 = b_1 = \cdots = b_{k-1} = 0$ and $b_k \neq 0$. We claim that v: $W_{p^\infty}(A) \to \mathbf{N} \cup \{0, \infty\}$ is a (nonarchimedean exponential) valuation; i.e., that this function satisfies the conditions

(17.4.13) $$v(b) = \infty \iff b = 0, \qquad v(ab) = v(a) + v(b)$$

$$v(a + b) > \min\{v(a), v(b)\}$$

Of these conditions the first holds by definition, and the third is immediate from the definition of v. To prove the second condition we can assume that $a \neq 0$ and $b \neq 0$ let $v(a) = k$, $v(b) = l$. Then by Corollary (17.4.11) we have

$$ab = \tau(a_k^{p^{-k}})\tau(b_l^{p^{-l}})p^{k+l} + p^{k+l+1}c$$

for some element $c \in W_{p^\infty}(A)$. Writing c in the form $c = \sum \tau(c_i^{p^{-i}})p^i$, we see that ab can be written

$$ab = \tau(a_k^{p^{-k}})\tau(b_l^{p^{-l}})p^{k+l} + \sum_{i=0}^{\infty} \tau(c_i^{p^{-i}})p^{k+l+1+i}$$

which by the uniqueness part of Corollary (17.4.11) means that $v(ab) = k + l$.

■ (17.4.14) **Corollary** $W_{p^\infty}(A)$ is an integral domain if A is a perfect field of characteristic $p > 0$.

■ (17.4.15) **Lemma** $W_{p^\infty}(A)$ is complete in the topology induced by the valuation v.

Proof From (17.4.10) and the definition of v we have that $v(b) > k$ is equivalent to the statement that the image of b in $W_{p^{k-1}}(A)$ is zero. The lemma now follows from $\varprojlim W_{p^n}(A) = W_{p^\infty}(A)$.

■ (17.4.16) **Lemma** Let A be a field of characteristic $p > 0$. Then every $b \in W_{p^\infty}(A)$ such that $b_0 \neq 0$ is a unit in $W_{p^\infty}(A)$. That is, b is a unit if $v(b) = 0$.

Proof Write $b = \sum_{i=1}^{\infty} \tau(c_i)p^i$. Because $b_0 \neq 0$ we have (setting $a^{(1)} = \tau(b_0^{-1})$)

$$a^{(1)}b = 1 + \sum_{i=1}^{\infty} \tau(c_i')p^i$$

Assume that $b^{(k)} \in W_{p^\infty}(A)$ is of the form $1 + \sum_{i=k}^{\infty} \tau(c_i)p^i$. Let $a^{(k)} = 1 - p^i\tau(c_i)$, then $a^{(k)}b^{(k)} = 1 + \sum_{i=k+1}^{\infty} \tau(c_i')p^i$. One easily checks (using (17.4.13)) that the sequence $(a^{(k)}a^{(k-1)} \cdots a^{(2)}a^{(1)})_k$ is a fundamental sequence, which by (17.4.15) converges to an element $a \in W_{p^\infty}(A)$. It follows that $ab = 1$.

■ (17.4.17) **Proposition** Let k be perfect field of characteristic $p > 0$, let R be a complete noetherian local ring with residue field k and let $\rho: R \to k$ be the natural projection. Then there is a unique ring homomorphism $\phi: W_{p^\infty}(k) \to R$ such that $\rho\phi = w_1 = w_{p^0}: W_{p^\infty}(k) \to k$. And if R is a discrete valuation ring and $p \neq 0$ in R, then R is a free finite $W_{p^\infty}(k)$-module of rank $[R/pR: k]$. In particular, if $R/pR = k$, then $R = W_{p^\infty}(k)$.

Proof We first prove the uniqueness of ϕ (if it exists at all). To this end recall that for every complete noetherian ring R with residue field k there is a unique Teichmüller mapping $\tau: k \to R$, such that $\tau(x)^p = \tau(x^p)$ for all $x \in k$ (and then one also has $\tau(x)\tau(y) = \tau(xy)$). This mapping τ is constructed as follows: let $x \in k$, let $T(n, x) = \{y \in R \mid \rho(y) = x^{p^{-n}}\}$ and $U(n, x) = \{y^{p^n} \mid y \in T(n, x)\}$. Then $U(n, x) \subset T(0, x)$. Further, if $z, z' \in U(n, x)$, then $z \equiv z' \bmod(\mathfrak{m}_R^{n+1})$ (where $\mathfrak{m}_R$ is the maximal ideal of R) because $z = y^{p^n}$, $z' = y'^{p^n}$ with y, y' both in $T(n, x)$, hence $y \equiv y' \bmod(\mathfrak{m}_R)$. Because R is complete and Hausdorff, there is for every $x \in k$ a unique $\tau(x) \in R$ such that $\tau(x) \in U(n, x)$ for all $n \in \mathbf{N}$. In case $R = W_{p^\infty}(k)$, τ is the Teichmüller mapping of (17.4.8).

Now suppose that there are two ring homomorphisms $\phi, \phi': W_{p^\infty}(k) \to R$ such that $\rho\phi = \rho\phi' = w_1$, then by the uniqueness of the Teichmüller mapping for R we must have $\phi(\tau(x)) = \phi'(\tau(x))$ for all $x \in k$. By Corollary (17.4.11) this implies $\phi = \phi'$.

To prove existence, consider the canonical ring homomorphisms $w_{p^n}: W_{p^n}(R) \to R$. If $r_i \in \mathfrak{m}_R$, the maximal ideal of R, then $w_{p^n}(r_0, \ldots, r_n) \in \mathfrak{m}_R^{n+1}$,

which means that we have a unique well-defined ring homomorphism ψ_n: $W_{p^n}(k) \to R/\mathfrak{m}_R^{n+1}$ such that the following diagram is commutative

$$\begin{array}{ccc} W_{p^n}(R) & \xrightarrow{w_{p^n}} & R \\ \downarrow{\scriptstyle W_{p^n}(\rho)} & & \downarrow \\ W_{p^n}(k) & \xrightarrow{\psi_n} & R/\mathfrak{m}_R^{n+1} \end{array}$$

(where the right-hand vertical arrow is the canonical projection). Let $\chi: k \to k$ be the homomorphism $x \mapsto x^{p^{n-1}}$ and define $\phi_n = \psi_n \circ W_{p^n}(\chi^n)$. Then for all $r_0, \ldots, r_n \in R$

$$\phi_n(\rho(r_0^{p^n}), \ldots, \rho(r_n^{p^n})) = r_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n \quad (\mathrm{mod}(m^{n+1})$$

It follows that $\phi = \varprojlim \phi_n: W_{p^\infty}(k) \to R$ exists and is a ring homomorphism with the required properties. The remainder of the proposition follows by some standard commutative algebra, e.g., [43, Chapter III, Section 2, Corollary 3 of Proposition 12 and Proposition 13]. (NB we have already shown directly that $W_{p^\infty}(\mathbf{F}_p) = \mathbf{Z}_p$ in Section 15.4; a similar technique works for $W_{p^\infty}(\mathbf{F}_q)$ also; cf. Section 25.3.)

■ (17.4.18) **Remark** Let A_n be the ring of integers of the unramified extension of degree n of $\mathbf{Q}_p$. Then by Hensel's lemma all the $p^n - 1$ roots of unity exist in A_n. Let $\tau: \mathbf{F}_{p^n} \to A_n$ be the mapping that takes 0 to 0 and $x \in \mathbf{F}_{p^n}$ to the unique $(p^n - 1)$-th root of unity lying over x. Then τ is the Teichmüller mapping (i.e., the unique map commuting with pth powers) and the unique isomorphism ϕ: $W_{p^\infty}(\mathbf{F}_{p^n}) \to A_n$ which reduces to the identity mod p is

$$\phi(x_0, x_1, x_2, \ldots) = \sum_{i=1}^{\infty} \tau(x_i^{p^{-i}})p^i$$

To conclude this section we discuss the one prime number version of the isomorphism $\bar{E}_A$: $W(A) \to \Lambda(A)$. Choose a prime number p. Let $\hat{\varepsilon}_p$: $\mathscr{C}(\hat{\mathbf{G}}_m^-; A) \to \mathscr{C}_p(\hat{\mathbf{G}}_m^-; A)$ be the canonical projection from the group of curves in $\hat{\mathbf{G}}_m^-$ to the group of p-typical curves in $\hat{\mathbf{G}}_m^-$. Let β be the isomorphism $\mathscr{C}(\hat{\mathbf{G}}_m^-; A) \to \Lambda(A)$, $\gamma(t) \mapsto 1 - \gamma(t)$, and let $\Lambda_{p^\infty}(A) = \beta(\mathscr{C}_p(\hat{\mathbf{G}}_m^-; A))$; i.e., if A is of characteristic zero, the elements of $\Lambda_{p^\infty}(A)$ are the power series $1 + a_1 t + a_2 t^2 + \cdots$ such that $\log(1 + a_1 t + \cdots) = \sum c_i p^i$ for certain $c_i \in A \otimes \mathbf{Q}$, and let $\varepsilon_p^\wedge = \beta_p \hat{\varepsilon}_p \beta^{-1}$ where β_p is the restriction of β to $\mathscr{C}_p(\hat{\mathbf{G}}_m^-, A)$.

Let $\Phi(y)$ be the power series in $\mathbf{Q}[\![y]\!]$

$$\Phi(y) = \prod_{(p,n)=1} (1 - y^n)^{\mu(n)/n} \tag{17.4.19}$$

■ (17.4.20) **Lemma** $\Phi(y)$ has its coefficients in $\mathbf{Z}_{(p)}[\![y]\!]$.

Proof This is part of Lemma (17.2.14).

Remark and second proof

$$1 - \Phi(t) = \hat{\varepsilon}_p(\gamma_0(t)) \tag{17.4.21}$$

where $\gamma_0(t)$ is the curve $\gamma_0(t) = t$.

We now define $\bar{E}_{A,p}\colon W_{p^\infty}(A) \to \Lambda_{p^\infty}(A)$ by the formula

$$\bar{E}_{A,p}(a_0, a_1, a_2, \ldots) = \prod_{i=0}^{\infty} \Phi(a_i t^{p^i}) \tag{17.4.22}$$

■ (17.4.23) **Proposition** $\bar{E}_{A,p}\colon W_{p^\infty}(A) \to \Lambda_{p^\infty}(A)$ is a functorial isomorphism of rings and the diagram

$$\begin{array}{ccccc} W(A) & \xrightarrow{\bar{E}_A} & \Lambda(A) & \xrightarrow{\beta} & \mathscr{C}(\hat{\mathbf{G}}_{\mathrm{m}}^-; A) \\ \downarrow{\scriptstyle \varepsilon_{p^\infty, A}} & & \downarrow{\scriptstyle \varepsilon^{\Lambda}_{p,A}} & & \downarrow{\scriptstyle \hat{\varepsilon}_p} \\ W_{p^\infty}(A) & \xrightarrow{\bar{E}_{A,p}} & \Lambda_{p^\infty}(A) & \xrightarrow{\beta_p} & \mathscr{C}_p(\hat{\mathbf{G}}_{\mathrm{m}}^-; A) \end{array} \tag{17.4.24}$$

is (functorially) commutative. The projection $\varepsilon^{\Lambda}_{p,A}$ is a ring homomorphism.

Proof The right-hand square of (17.4.24) is commutative by the definition of $\varepsilon^{\Lambda}_{p,A}$ and β_p. To see that the left-hand square is commutative remark that

$$1 - \Phi(a_i t^{p^i}) = \hat{\varepsilon}_p(a_i t^{p^i}) \tag{17.4.25}$$

Indeed by the definition of $\hat{\varepsilon}_p$ (cf. (16.3.11))

$$\begin{aligned} \hat{\varepsilon}_p(a_i t^{p^i}) &= \sum_{(p,n)=1}^{\hat{\mathbf{G}}_{\mathrm{m}}^-} \frac{\mu(n)}{n} \mathbf{V}_n \mathbf{f}_n(a_i t^{p^i}) \\ &= \sum_{(p,n)=1}^{\hat{\mathbf{G}}_{\mathrm{m}}^-} \frac{\mu(n)}{n} \mathbf{V}_n \mathbf{f}_n \mathbf{V}_{p^i}(a_i t) \\ &= \sum_{(p,n)=1}^{\hat{\mathbf{G}}_{\mathrm{m}}^-} \frac{\mu(n)}{n} \mathbf{V}_n \mathbf{V}_{p^i} \mathbf{f}_n(a_i t) \\ &= \sum_{(p,n)=1}^{\hat{\mathbf{G}}_{\mathrm{m}}^-} \frac{\mu(n)}{n} \mathbf{V}_n \mathbf{V}_{p^i}(a_i^n t) \\ &= \sum_{(p,n)=1}^{\hat{\mathbf{G}}_{\mathrm{m}}^-} \frac{\mu(n)}{n} a_i^n t^{np^i} \\ &= 1 - \prod_{(p,n)=1} (1 - a_i^n t^{np^i})^{\mu(n)/n} \end{aligned}$$

And

$$\hat{\varepsilon}_p(at^r) = 0 \tag{17.4.26}$$

if r is not a power of p. Indeed (in the characteristic zero case) $\log(at^r) = \sum_{n=1}^{\infty} n^{-1}(-1)^{n+1}t^{rn}$ and setting all coefficients of non-p-powers zero in $\log(at^r)$ hence gives zero if r is not a power of p. By functoriality (17.4.26) is also true is general.

Because $\bar{E}_A$ and $\varepsilon^{\wedge}_{p.A}$ are both additive, (17.4.25) and (17.4.26) together prove the commutativity of the left-hand square of (17.4.24). Now $\hat{\varepsilon}_p$ is surjective (if $\gamma(t)$ is p-typical, then $\hat{\varepsilon}_p(\gamma(t)) = \gamma(t)$) so $\varepsilon^{\wedge}_{p.A}$ is surjective, which proves that $\bar{E}_{A.p}$ is surjective. $\bar{E}_{A.p}$ is additive because $\varepsilon_{p^{\infty}.A}$, $\varepsilon^{\wedge}_{p.A}$, and $\bar{E}_A$ are all additive and $\varepsilon_{p^{\infty}.A}$ is surjective. So to prove that $\bar{E}_{A.p}$ is bijective it suffices to show that $\bar{E}_{A.p}(a_1, a_2, \ldots) \neq 1$ if $(a_0, a_1, a_2, \ldots) \neq 0$. Let a_i be the first coordinate of $(a_0, a_1, a_2, \ldots)$ that is nonzero, then $\bar{E}_{A.p}(a_0, a_1, a_2, \ldots) \equiv (1 - a_i t^{p^i}) \bmod t^{p^{i+1}}$. Further, to check that $\varepsilon^{\wedge}_{p.A}$ preserves multiplication it suffices to check that $s_n(\varepsilon^{\wedge}_{p.A})$ does so for all n (and characteristic zero rings A). But as is easily checked

$$(17.4.27) \qquad s_n(\varepsilon^{\wedge}_{p.A}) = 0 \quad \text{if } n \text{ is not a power of } p$$
$$s_{p^i}(\varepsilon^{\wedge}_{p.A}) = s_{p^i} \quad \text{for } i = 0, 1, 2, \ldots$$

This proves that $\varepsilon^{\wedge}_{p.A}$ is multiplicative; in addition $\varepsilon^{\wedge}_{p.A}(1 - t) = \Phi(t)$ is the unit element of $\Lambda_{p^{\infty}}(A)$ by (17.2.14), so that $\varepsilon^{\wedge}_{p.A}$ is a ring homomorphism. This also proves that $\bar{E}_{A.p}$ is a ring homomorphism because $\varepsilon_{p^{\infty}.A}$, $\bar{E}_A$, and $\varepsilon^{\wedge}_{p.A}$ are ring homomorphisms and $\varepsilon_{p^{\infty}.A}$ is surjective.

17.5 The "classical" Artin–Hasse exponential series

Here we define the "classical" Artin-Hasse exponential series as it is defined in, e.g., Whaples [438]. This mapping is a lift of the isomorphism $\bar{E}_{A.p}$ of (17.4.24). We use again the power series

$$(17.5.1) \qquad \Phi(y) = \prod_{(p,n)=1} (1 - y^n)^{\mu(n)/n}$$

which according to Lemma (17.4.20) has its coefficients in $\mathbf{Z}_{(p)}$.

Now let A be a perfect field of characteristic $p > 0$. Every element of $W_{p^{\infty}}(A)$ can be written uniquely as a sum:

$$(17.5.2) \qquad (b_0, b_1, \ldots) = b = \sum_{i=0}^{\infty} \tau(b_i^{p^{-i}})p^i$$

One now defines the Artin-Hasse exponential mapping $E_{A.p}$: $W_{p^{\infty}}(A) \to \Lambda(W_{p^{\infty}}(A))$ by the formula

$$(17.5.3) \qquad E_{A.p}(b, t) = \prod_{i=0}^{\infty} (\Phi(\tau(b_i^{p^{-i}})t))^{p^i}$$

■(17.5.4) **Proposition** The mapping $E_{A,p}: W_{p^\infty}(A) \to \Lambda(W_{p^\infty}(A))$ is a homomorphism of the abelian groups underlying the rings $W_{p^\infty}(A)$ and $\Lambda(W_{p^\infty}(A))$ and $E_{A,p}$ is also multiplicative (i.e., $E(ab, t) = E(a, t) * E(b, t)$, $E(a + b, t) = E(a, t)E(b, t)$, $E(0, t) = 1$, $E(-a, t) = E(a, t)^{-1}$).

■(17.5.5) **Remark** $E_{A,p}$ is *not* a homomorphism of rings $W_{p^\infty}(A) \to \Lambda(W_{p^\infty}(A))$; it does not preserve unit elements.

Indeed, $E((1, 0, 0, \ldots)) = \prod_{(n,p)=1} (1 - t^n)^{\mu(n)/n}$ and if $p \neq 2$, one easily checks that $\prod_{(n,p)=1} (1 - t^n)^{\mu(n)/n} \equiv 1 - t - \frac{1}{2}t^2 \bmod(t^3)$ in $\mathbf{Z}_{(p)}[\![t]\!]$. But the unit element of $\Lambda(W_{p^\infty}(A))$ is $1 - t$, so that E does not map the unit element of $W_{p^\infty}(A)$ to the unit element of $\Lambda(W_{p^\infty}(A))$. The reason for this is that $E_{A,p}$ is in fact a homomorphism of rings $W_{p^\infty}(A) \to \Lambda_{p^\infty}(W_{p^\infty}(A))$, but as we have seen (cf. Corollary (17.2.17)) the inclusion $\Lambda_{p^\infty}(W_{p^\infty}(A)) \subset \Lambda(W_{p^\infty}(A))$ is not a homomorphism of rings.

■(17.5.6) **Remark** For the moment $E_{A,p}$ is also only defined for perfect characteristic p fields A. We shall later see however (cf. Propositions (17.6.25) and (17.6.26)) that there is a mapping $E_{A,p}: W_{p^\infty}(A) \to \Lambda(W_{p^\infty}(A))$ with the properties listed in (17.5.4) for all $\mathbf{Z}_{(p)}$-algebras A compatible with the homomorphisms $W_{p^\infty}(\phi)$ and $\Lambda(W_{p^\infty}(\phi))$ induced by ring homomorphisms $\phi: A \to B$. Thus we have a morphism of functors $E_p: W_{p^\infty}(-) \to \Lambda(W_{p^\infty}(-))$.

■(17.5.7) **Addendum** (to Proposition (17.5.4)) $E_{A,p}$ maps $W_{p^\infty}(A)$ into $\Lambda_{p^\infty}(A)$ (as is shown by (17.5.9)) and the following diagram is (functorially) commutative

$$\begin{array}{ccccc} W_{p^\infty}(A) & \xrightarrow{E_{A,p}} & \Lambda_{p^\infty}(W_{p^\infty}(A)) & \subset & \Lambda(W_{p^\infty}(A)) \\ & \searrow^{\bar{E}_{A,p}} & \downarrow{\scriptstyle \Lambda_{p^\infty}(w_1)} & & \\ & & \Lambda_{p^\infty}(A) & & \end{array}$$

so that $E_{A,p}$ is so to speak a lift of the isomorphism $\bar{E}_{A,p}$. (All arrows in the diagram above with the exception of the inclusion on the right are ring homomorphisms.)

■(17.5.8) **Proof of Proposition (17.5.4)** $W_{p^\infty}(A)$ is of characteristic zero (Proposition (17.4.17)); so to prove the relations $E(ab, t) = E(a, t) * E(b, t)$, $E(a + b, t) = E(a, t)E(b, t)$, $E(0, t) = 1$, $E(-a, t) = E(a, t)^{-1}$, it suffices to prove that the composed maps

$$W_{p^\infty}(A) \xrightarrow{E} \Lambda(W_{p^\infty}(A)) \xrightarrow{s_n} W_{p^\infty}(A)$$

satisfy the corresponding identities.

We calculate

$$\log(E(b,t)) = \sum_{i=0}^{\infty} p^i \log(\Phi(\tau(b_i^{p^{-i}})t)) \tag{17.5.9}$$

$$= \sum_{i=0}^{\infty} p^i \sum_{(s,p)=1} \frac{\mu(s)}{s} \log(1 - \tau(b_i^{p^{-i}})^s t^s)$$

$$= -\sum_{i=0}^{\infty} p^i \sum_{(s,p)=1} \frac{\mu(s)}{s} \sum_{k=1}^{\infty} \frac{1}{k} \tau(b_i^{p^{-i}})^{sk} t^{sk}$$

$$= -\sum_{i=0}^{\infty} p^i \sum_{r=1}^{\infty} \sum_{\substack{s|r \\ (s,p)=1}} \frac{\mu(s)}{r} \tau(b_i^{p^{-i}})^r t^r$$

$$= -\sum_{i=0}^{\infty} p^i \sum_{l=0}^{\infty} p^{-l} \tau(b_i^{p^{-i}})^{p^l} t^{p^l}$$

where for last equality we have used that

$$\sum_{\substack{(s,p)=1 \\ s|r}} \mu(s) = \begin{cases} 0 & \text{if } r \text{ is not a power of } p \\ 1 & \text{if } r \text{ is a power of } p \end{cases}$$

From (17.5.9) we find that

$$-t\frac{d}{dt}\log(E(b,t)) = \sum_{i=0}^{\infty} \sum_{l=0}^{\infty} p^i \tau(b_i^{p^{-i}})^{p^l} t^{p^l} \tag{17.5.10}$$

Now because $p = \mathbf{V}_p\mathbf{f}_p$ and $\mathbf{f}_p(c_0, c_1, \ldots) = (c_0^p, c_1^p, \ldots)$ and τ is multiplicative,

$$p^i \tau(b_i^{p^{-i}})^{p^l} = (0, 0, \ldots, 0, b_i^{p^l}, 0, \ldots, 0, \ldots)$$

with $b_i^{p^l}$ in the $(i+1)$th spot. Using (17.4.9), we see that

$$\sum_{i=0}^{\infty} p^i \tau(b_i^{p^{-i}})^{p^l} = (b_0^{p^l}, b_1^{p^l}, b_2^{p^l}, \ldots) = \mathbf{f}_p^l(b) \tag{17.5.11}$$

So we see that $s_n \circ E = 0$ if n is not a power of p and $s_{p^l} \circ E = \mathbf{f}_p^l : W_{p^\infty}(A) \to W_{p^\infty}(A)$. The zero map and the ring homomorphisms $\mathbf{f}_p^l$ all satisfy the required properties. This concludes the proof of (17.5.4).

■ (17.5.12) The next things we want to do is to define a ring homomorphism $\Delta_A : W(A) \to W(W(A))$ which generalizes the Artin-Hasse exponential mapping in the sense that the following diagram is commutative

$$\begin{array}{ccccccc}
W(A) & \xrightarrow{\Delta_A} & W(W(A)) & \xrightarrow{\bar{E}_{W(A)}} & \Lambda(W(A)) & \xrightarrow{\beta^{-1}} & \mathscr{C}(\hat{\mathbf{G}}_m^-; W(A)) \\
\downarrow & & & & \downarrow{\scriptstyle \bar{E}_p^A} & & \downarrow{\scriptstyle \bar{\varepsilon}_p} \\
 & & & & \Lambda(W(A)) & \xrightarrow{\beta^{-1}} & \mathscr{C}(\hat{\mathbf{G}}_m^-; W(A)) \\
 & & & & \downarrow & & \downarrow \\
W_{p^\infty}(A) & & \xrightarrow{E_{A,p}} & & \Lambda(W_{p^\infty}(A)) & \xrightarrow{\beta^{-1}} & \mathscr{C}(\hat{\mathbf{G}}_m^-; W_{p^\infty}(A))
\end{array}$$

where all the unlabeled arrows are induced by the natural projectors $W(A) \to W_{p^\infty}(A)$, and where $\bar{\varepsilon}_p: \mathscr{C}(\hat{\mathbf{G}}_m^-; W(A)) \to \mathscr{C}(\hat{\mathbf{G}}_m^-; W(A))$ is the composite of the projection "make curves p-typical" $\varepsilon_p: \mathscr{C}(\hat{\mathbf{G}}_m; W(A)) \to \mathscr{C}_p(\hat{\mathbf{G}}_m^-, W(A))$ and the inclusion $\mathscr{C}_p(\hat{\mathbf{G}}_m^-, W(A)) \to \mathscr{C}(\hat{\mathbf{G}}_m^-, W(A))$, and where $\bar{\varepsilon}_p^\wedge = \beta \bar{\varepsilon}_p \beta^{-1}$ (with β the isomorphism $\gamma(t) \mapsto 1 - \gamma(t)$).

This will be done in 17.6.

17.6 The functor homomorphism $\Delta: W(-) \to W(W(-))$

To define this functor homomorphism of ring functors we use a series of lemmas.

■ (17.6.1) **Lemma** Let A be a characteristic zero ring with endomorphisms $\phi_p: A \to A$ for all prime numbers p such that $\phi_p(a) \equiv a^p \bmod pA$ for all $a \in A$. Let $a_n \in A$ for $n \in \mathbf{N}$ be a series of elements such that for all n and p

$$\phi_p(a_n) \equiv a_{np} \quad \bmod(p^{v_p(n)+1}) \tag{17.6.2}$$

where (as usual) $v_p(n) = k$ if $n = p^k m$ with $m \in \mathbf{N}$, $(m, p) = 1$. Then there exist unique elements $b_1, b_2, \ldots, \in A$ such that $w_n(b) = a_n$ for all $n \in \mathbf{N}$.

Proof Let $\bar{E}: W(A) \to \Lambda(A)$ be the isomorphism of (17.2.7). Then $w_n(b) = a_n$ for all n is the same as $s_n \bar{E}(b) = a_n$ for all n, which, using the isomorphism $\beta: \mathscr{C}_p(\hat{\mathbf{G}}_m^-; A) \simeq \Lambda(A)$, $\gamma(t) \mapsto 1 - \gamma(t)$, is in turn the same thing as

$$f(1 - E(b)) = \sum_{n=1}^{\infty} n^{-1} a_n t^n = g(t) \tag{17.6.3}$$

where

$$f(X) = \log_{\hat{G}_m^-}(X) = X + 2^{-1}X^2 + 3^{-1}X^3 + \cdots \tag{17.6.4}$$

So what we have to prove is that $f^{-1}(g(t))$ has integral coefficients. Now $f(X)$, as a power series over A, satisfies the functional equation

$$f(X) - p^{-1}(\phi_p)_* f(X^p) \in A[\![X]\!] \otimes \mathbf{Z}_{(p)}$$

Let $g(t) = \sum_{n=1}^{\infty} n^{-1} a_n t^n$, then $a_{pn} \equiv \phi_p(a_n) \bmod(p^{v_p(n)+1})$ means precisely that

$$g(t) - p^{-1}(\phi_p)_* g(t^p) \in A[\![t]\!] \otimes \mathbf{Z}_{(p)} \tag{17.6.5}$$

So the functional equation lemma combined with sublemma (17.6.6) below says that $f^{-1}(g(t))$ is indeed integral. (The condition $\phi_p(a) \equiv a \bmod pA$ is of course one of the prerequisites for the functional equation lemma to be applicable. Exercise: give a direct proof using $w_{np}(X) \equiv w_n(X^p) \bmod(p^{v_p(n)+1})$.)

■ (17.6.6) **Sublemma** Let A be a characteristic zero ring. Then if $b \in A \otimes \mathbf{Q}$ is in $A \otimes \mathbf{Z}_{(p)}$ for all primes p, then $b \in A$.

Proof Since b is in $A \otimes \mathbf{Q}$, we can write b as $b = n^{-1}x$ with $x \in A$, $n \in \mathbf{N}$. Write n as a product $pm = n$ with p a prime number. Because $b \in \mathbf{Z}_{(p)} \otimes A$, we

can also write b as $b = l^{-1}y$ with $l \in \mathbf{N}$, $(l, p) = 1$. Because $(l, p) = 1$, there are $r, s \in \mathbf{Z}$ such that $rp + sl = 1$. We have $b = n^{-1}x = l^{-1}y$, hence $lx = ny$ and $slx = sny$ and $x = sny + rpx$, i.e., x is divisible by p, so that we can also write $b = \bar{n}^{-1}\bar{x}$ with $\bar{x} \in A$, $\bar{n} \in \mathbf{N}$, $\bar{n} < n$. Continuing in this way we see that $b \in A$. Q.E.D.

There is also a one prime version of Lemma (17.6.1), which we state without proof. (The proof being virtually identical.)

■ (17.6.7) **Lemma** Let p be a fixed prime number. Let A be a ring without p-torsion with an endomorphism $\phi_p\colon A \to A$ such that $\phi_p(a) \equiv a^p \bmod(pA)$ for all $a \in A$. Let $a_{p0}, a_{p1}, \ldots$ be a series of elements of A such that $\phi_p(a_{pi}) \equiv a_{pi+1} \bmod(p^{i+1}A)$. Then there are unique elements $b_{p0}, b_{p1}, \ldots, \in A$ such that $w_{pn}(b) = a_{pn}$ for all $n \in \mathbf{N} \cup \{0\}$.

■ (17.6.8) **Lemma** Let A be a characteristic zero ring with endomorphisms $\phi_n\colon A \to A$ for all $n \in \mathbf{N}$ such that $\phi_1 = id$ and $\phi_n\phi_m = \phi_{nm}$ and such that $\phi_p(a) \equiv a^p \bmod(pA)$ for all prime numbers p and $a \in A$. Then there exists a unique homomorphism of rings $D_A\colon A \to W(A)$ such that $w_n \circ D_A = \phi_n$ for all $n \in \mathbf{N}$.

Proof Take $a \in A$ and set $a_n = \phi_n(a)$. Then we have $\phi_p(a_n) = a_{np}$ so we can apply Lemma (17.6.1) to find unique $b_1, b_2, \ldots, \in A$ such that $w_n(b) = a_n$. We define $D(a) = (b_1, b_2, \ldots)$, then obviously $w_n D = \phi_n$. Because A is of characteristic zero, to prove that D is a homomorphism of rings it suffices to check that the $w_n D = \phi_n$ are homomorphisms of rings, which they are by hypothesis. Q.E.D.

The one prime version of Lemma (17.6.8) is

■ (17.6.9) **Lemma** Let p be a fixed prime number and let A be a ring without p-torsion and with an endomorphism $\phi_p\colon A \to A$ such that $\phi_p(a) = a^p \bmod(pA)$ for all $a \in A$. Then there is a unique homomorphism of rings: $D_p\colon A \to W_{p^\infty}(A)$ such that $w_{p^n} \circ D = \phi_p^n$ for all $n \in \mathbf{N} \cup \{0\}$.

We now want to apply Lemmas (17.6.8) and (17.6.9) to construct homomorphisms of rings $\Delta_A\colon W(A) \to W(W(A))$ and $\Delta_{A,p}\colon W_{p^\infty}(A) \to W_{p^\infty}(W_{p^\infty}(A))$. The role of the endomorphisms ϕ_n will be played by the Frobenius endomorphisms $\mathbf{f}_n$. So to apply (17.6.8) and (17.6.9) we need to show that $\mathbf{f}_p$ satisfies $\mathbf{f}_p(a) \equiv a^p \bmod pW(A)$ for $a \in W(A)$.

■ (17.6.10) **Lemma** Let A be any ring and p a prime number. Then $\mathbf{f}_p(a_1, a_2, \ldots) \equiv (a_1, a_2, \ldots)^p \bmod(pW(A))$ for all $(a_1, a_2, \ldots) \in W(A)$ and $\mathbf{f}_p(a_0, a_1, a_2, \ldots) \equiv (a_0, a_1, a_2, \ldots)^p \bmod(pW_{p^\infty}(A))$ for all $(a_0, a_1, a_2, \ldots) \in W_{p^\infty}(A)$.

Proof The second statement of the lemma follows from the first because $W(A) \to W_{p^\infty}(A)$ is a surjective ring homomorphism. To prove the first state-

ment we first consider the ring $A = \mathbf{Z}[X_1, X_2, \ldots]$ and the element $X = (X_1, X_2, \ldots) \in W(\mathbf{Z}[X_1, X_2, \ldots])$. We define elements

$$c_n(X) \in \mathbf{Q}[X_1, X_2, \ldots]$$

as

$$c_n(x) = p^{-1}w_n(\mathbf{f}_p(X)) - p^{-1}w_n(X)^p$$

and we are going to prove that

$$\phi_p c_n(X) \equiv c_{pn}(X) \mod(p^{v_p(n)+1}\mathbf{Z}[X_1, X_2, \ldots]) \tag{17.6.11}$$

$$c_m(X) \in \mathbf{Z}[X_1, X_2, \ldots] \quad \text{for all } m \in \mathbf{N}. \tag{17.6.12}$$

where ϕ_p: $\mathbf{Z}[X_1, X_2, \ldots] \to \mathbf{Z}[X_1, X_2, \ldots]$ is the homomorphism $X_i \mapsto X_i^p$, $i = 1, 2, \ldots$. To prove (17.6.12) we write

$$\begin{aligned} c_m(X) &= p^{-1}w_m(\mathbf{f}_p(X)) - p^{-1}w_m(X)^p \\ &= p^{-1}(w_{mp}(X) - w_m(X)^p) \in \mathbf{Z}[X_1, X_2, \ldots] \end{aligned}$$

because $w_{mp}(X) \equiv w_m(X^p) \bmod p$ by (17.1.6) and $w_m(X)^p \equiv w_m(X^p) \bmod p$.

To prove (17.6.11) we use again (17.1.6); that is,

$$w_{np}(X) \equiv w_n(X^p) \mod(p^{v_p(n)+1}\mathbf{Z}[X_1, X_2, \ldots])$$

We find

$$\begin{aligned} c_{np}(X) &= p^{-1}w_{np}(\mathbf{f}_p(X)) - p^{-1}w_{np}(X)^p \\ &= p^{-1}\{w_{np^2}(X) - w_{np}(X)^p\} \\ &\equiv p^{-1}\{w_{np}(X_1^p, X_2^p, \ldots) - w_{np}(X_1, X_2, \ldots)^p\} \\ &\qquad \mod(p^{v_p(n)+1}\mathbf{Z}[X_1, X_2, \ldots]) \end{aligned} \tag{17.6.13}$$

Now

$$w_{np}(X_1, X_2, \ldots) \equiv w_n(X_1^p, X_2^p, \ldots) \mod(p^{v_p(n)+1}\mathbf{Z}[X_1, X_2, \ldots])$$

so that

$$w_{np}(X_1, X_2, \ldots)^p \equiv w_n(X_1^p, X_2^p, \ldots)^p \mod(p^{v_p(n)+2}\mathbf{Z}[X_1, X_2, \ldots]) \tag{17.6.14}$$

Putting (17.6.13) and (17.6.14) together, we find $\mod(p^{v_p(n)+1}\mathbf{Z}[X_1, X_2, \ldots])$

$$\begin{aligned} c_{np}(X) &\equiv p^{-1}\{w_{np}(X_1^p, X_2^p, \ldots) - (w_n(X_1^p, X_2^p, \ldots))^p\} \\ &= c_n(X_1^p, X_2^p, \ldots) = \phi_p c_n(X) \end{aligned}$$

which proves the assertion (17.6.11). We can now apply Lemma (17.6.1) to conclude that there are $b_1(X), b_2(X), \ldots, \in \mathbf{Z}[X_1, X_2, \ldots]$ such that

$$pw_n(b_1(X), \ldots, b_n(X)) = w_n(\mathbf{f}_p(X) - \underbrace{X \cdot X \cdot \cdots \cdot X}_{p\text{-times}})$$

This proves the lemma for $A = \mathbf{Z}[X_1, X_2, \ldots]$ and $X \in W(A)$. The general case follows immediately because for every ring A and every $(a_1, a_2, \ldots) \in W(A)$, there is a (unique) homomorphism $\phi\colon \mathbf{Z}[X_1, X_2, \ldots] \to A$ such that $W(\phi)(X) = (a_1, a_2, \ldots)$, viz the homomorphism defined by $X_i \mapsto a_i$.

(17.6.15) **Definition of the vectors of polynomials** $\Delta(n)(X) \in W(\mathbf{Z}[X_1, X_2, \ldots])$. As before, let $X \in W(\mathbf{Z}[X_1, X_2, \ldots])$ be the element $X = (X_1, X_2, X_3, \ldots)$. We consider the elements $\mathbf{f}_n X$ where $\mathbf{f}_n$ is the Frobenius homomorphism $W(\mathbf{Z}[X_1, X_2, \ldots]) \to W(\mathbf{Z}[X_1, X_2, \ldots])$.

By (17.6.10) and (17.6.1) there are unique elements $\Delta(n)(X) \in W(\mathbf{Z}[X_1, X_2, \ldots])$ such that $w_n(\Delta(1)(X), \ldots, \Delta(n)(X)) = \mathbf{f}_n X$. We now define a map $\Delta_A\colon W(A) \to W(W(A))$ for all rings A by setting

(17.6.16) $\Delta_A(a_1, a_2, \ldots) = (\Delta(1)(a_1, a_2, \ldots), \Delta(2)(a_1, a_2, \ldots), \ldots)$

This defines a morphism of functors $\Delta\colon W(-) \to W(W(-))$ (because the Δ_A are defined in terms of universal polynomials). If A is a characteristic zero ring, then Δ_A satisfies $w_n \Delta_A = \mathbf{f}_n$ so that Δ_A coincides with the ring homomorphism D_A defined by Lemma (17.6.8) with $\phi_n = \mathbf{f}_n$. This proves that Δ_A is a ring homomorphism for characteristic zero rings and hence that Δ_A is a ring homomorphism for all rings A by the usual trick. So we have

■ (17.6.17) **Theorem** There is a unique functormorphism of ring-valued functors $\Delta\colon W(-) \to W(W(-))$ such that $w_n \Delta = \mathbf{f}_n$ for all $n \in \mathbf{N}$.

More generally, if $\mathfrak{m}$ and $\mathfrak{n}$ are a pair of supernatural numbers and all primes $p \in \mathbf{N}(\mathfrak{n})$ that are not in $\mathbf{N}(\mathfrak{m})$ are invertible in A, then we can define a unique multiplication preserving homomorphism of group valued functors

$$\Delta_{\mathfrak{n}, A, \mathfrak{m}}\colon W_{\mathfrak{m}}(A) \to W_{\mathfrak{n}}(W_{\mathfrak{m}}(A))$$

such that

$$w_n \Delta_{\mathfrak{n}, \mathfrak{m}} = \begin{cases} 0 & \text{if } n \in \mathbf{N}(\mathfrak{n}) \backslash \mathbf{N}(\mathfrak{m}) \\ \mathbf{f}_n & \text{if } n \in \mathbf{N}(\mathfrak{n}) \cap \mathbf{N}(\mathfrak{m}) \end{cases}$$

and, as we shall see, $\Delta_{\mathfrak{n}, \mathfrak{m}}$ is a homomorphism of ring-valued functors if and only if $\mathbf{N}(\mathfrak{n}) \subset \mathbf{N}(\mathfrak{m})$ (and in that case there is no condition on A).

Given a set of prime numbers S we define $\mathbf{Z}_{(S)}$ as the ring of all $r \in \mathbf{Q}$ of the form $r = p_1^{-i_1} \cdots p_s^{-i_s} n$ with $p_1, \ldots, p_s \notin S$; $i_1, \ldots, i_s \in \mathbf{N}$ and $n \in \mathbf{Z}$. Note that $\mathbf{Z}_{((p))} = \mathbf{Z}_{(p)}$, the integers localized at p and $\mathbf{Z}_{(\varnothing)} = \mathbf{Z}$ if $\varnothing$ is the empty set. To define the $\Delta_{\mathfrak{n}, A, \mathfrak{m}}$ we need the following "relative" version of Lemma (17.6.1).

■ (17.6.18) **Lemma** Let $\mathfrak{n}$ and $\mathfrak{m}$ be two supernatural numbers and let $S = S(\mathfrak{n}, \mathfrak{m}) = \{p \mid p \text{ is a prime number in } \mathbf{N}(\mathfrak{n}) \backslash \mathbf{N}(\mathfrak{m})\}$. Let A be a $\mathbf{Z}_{(S)}$-algebra of characteristic zero with endomorphisms $\phi_p\colon A \to A$ for all prime numbers $p \in \mathbf{N}(\mathfrak{m})$ such that $\phi_p(a) = a^p \bmod(pA)$ for all $a \in A$. Let a_n for $n \in \mathbf{N}(\mathfrak{n})$ be a set of elements of A such that $a_{np} \equiv a_n \bmod(p^{v_p(n)+1} A)$ for all $n \in \mathbf{N}(\mathfrak{n})$ and

prime numbers $p \in \mathbf{N}(\mathfrak{m})$. Then there exist unique elements $b_n \in A$ for $n \in \mathbf{N}(\mathfrak{n})$ such that $w_n(b) = a_n$ for all $n \in \mathbf{N}(\mathfrak{n})$.

Proof Very similar to the proof of Lemma (17.6.1); exercise. The first application of (17.6.18) is

■ (17.6.19) **Lemma** Let p be a prime number, then p is invertible in $W(\mathbf{Z}[p^{-1}])$.

Proof We need to find $b_1, b_2, \ldots, \in \mathbf{Z}[p^{-1}]$ such that $w_n(b) = p^{-1}$ for all $n \in \mathbf{N}$. We apply Lemma (17.6.18) with

$$\mathfrak{n} = \prod_{q \text{ prime}} q^{\infty} \qquad \text{and} \qquad \mathfrak{m} = \prod_{\substack{q \text{ prime} \\ q \neq p}} q^{\infty}$$

$\phi_q = id$ for all prime numbers $q \in \mathbf{N}(\mathfrak{m})$, and $a_n = p^{-1}$ for all $n \in \mathbf{N}$.

■ (17.6.20) **Lemma** Let $\mathfrak{n}$ and $\mathfrak{m}$ be two supernatural numbers and let $S = S(\mathfrak{n}, \mathfrak{m}) = \{p \mid p \text{ is a prime number and } p \in \mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\mathfrak{m})\}$. Then for every $\mathbf{Z}_{(S)}$-algebra A of characteristic zero, there exists a unique homomorphism of abelian groups

$$\Delta_{\mathfrak{n},A,\mathfrak{m}}\colon W_{\mathfrak{m}}(A) \to W_{\mathfrak{n}}(W_{\mathfrak{m}}(A))$$

such that

$$w_n \Delta_{\mathfrak{n},A,\mathfrak{m}} = \begin{cases} 0 & \text{if } n \in \mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\mathfrak{m}) \\ \mathbf{f}_n & \text{if } n \in \mathbf{N}(\mathfrak{n}) \cap \mathbf{N}(\mathfrak{m}) \end{cases}$$

This homomorphism preserves multiplication.

Proof It follows from Lemma (17.6.19) that $W(A)$ is a $\mathbf{Z}_{(S)}$-algebra if A is a $\mathbf{Z}_{(S)}$-algebra. Choose $a \in W_{\mathfrak{m}}(A)$. Now apply Lemma (17.6.18) with $\phi_p = \mathbf{f}_p$ for all prime numbers $p \in \mathbf{N}(\mathfrak{m})$, $a_n = 0$ if $n \in \mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\mathfrak{m})$ and $a_n = \mathbf{f}_n a$ for $n \in \mathbf{N}(\mathfrak{n}) \cap \mathbf{N}(\mathfrak{m})$, to find $\Delta_{\mathfrak{n},A,\mathfrak{m}}(a)$. The map $\Delta_{\mathfrak{n},A,\mathfrak{m}}$ is a homomorphism of abelian groups and preserves multiplication because the maps $\mathbf{f}_n$, $n \in \mathbf{N}(\mathfrak{n}) \cap \mathbf{N}(\mathfrak{m})$ and 0 have these properties. Q.E.D.

We now define the elements $\Delta_{\mathfrak{n},\mathfrak{m}}(n)(X) \in W_{\mathfrak{m}}(\mathbf{Z}_{(S)}[X_i \mid i \in \mathbf{N}(\mathfrak{m})])$ for $n \in \mathbf{N}(\mathfrak{n})$ by

$$(\Delta_{\mathfrak{n},\mathfrak{m}}(n)(X))_{n \in \mathbf{N}(\mathfrak{n})} = \Delta_{\mathfrak{n},A,\mathfrak{m}}(X)$$

with $A = \mathbf{Z}_{(S)}[X_i \mid i \in \mathbf{N}(\mathfrak{m})]$, $X = (X_i)_{i \in \mathbf{N}(\mathfrak{m})}$. Using these polynomials, one defines a multiplication preserving homomorphism of abelian groups

$$\Delta_{\mathfrak{n},A,\mathfrak{m}}\colon W_{\mathfrak{m}}(A) \to W_{\mathfrak{n}}(W_{\mathfrak{m}}(A))$$

for all $\mathbf{Z}_{(S)}$-algebras by the formula

$$\Delta_{\mathfrak{n},A,\mathfrak{m}}(a) = (\Delta_{\mathfrak{n},\mathfrak{m}}(n)(a))_{n \in \mathbf{N}(\mathfrak{n})}$$

By uniqueness this coincides with the definition of $\Delta_{n,A,m}$ in Lemma (17.6.20) in case A is of characteristic zero.

■ (17.6.21) **Theorem** Let $\mathfrak{n}$ and $\mathfrak{m}$ be two supernatural numbers and $S = S(\mathfrak{n}, \mathfrak{m}) = \{p \mid p \text{ is a prime number and } p \in \mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\mathfrak{m})\}$. Then there exists a unique multiplication preserving functor homomorphism of abelian group $\Delta_{n,m}\colon W_m(-) \to W_n(W_m(-1))$, where both ring-valued functors are restricted to the subcategory $\mathbf{Alg}_{\mathbf{Z}_{(S)}} \subset \mathbf{Ring}$, such that

$$w_n\Delta_{n,m} = \begin{cases} 0 & \text{if } n \in \mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\mathfrak{m}) \\ \mathbf{f}_n & \text{if } n \in \mathbf{N}(\mathfrak{n}) \cap \mathbf{N}(\mathfrak{m}) \end{cases}$$

■ (17.6.22) **Addendum** The following diagram commutes if $\bar{\mathfrak{n}} \mid \mathfrak{n}$

$$\begin{array}{ccc} W_m(A) & \longrightarrow & W_n(W_m(A)) \\ \| & & \downarrow \\ W_m(A) & \longrightarrow & W_{\bar{n}}(W_m(A)) \end{array}$$

■ (17.6.23) **Corollary** There exists a unique homomorphism of ring valued functors $\mathbf{Ring} \to \mathbf{Ring}$, $\Delta_{n,n}\colon W_n(A) \to W_n(W_n(A))$ such that

$$w_n\Delta_{n,n} = \mathbf{f}_n, \qquad n \in \mathbf{N}(\mathfrak{n})$$

■ (17.6.24) **Caveat** If $\bar{\mathfrak{m}} \mid \mathfrak{m}$, then the diagram of functor morphisms

$$\begin{array}{ccc} W_m(-) & \xrightarrow{\Delta_{n,\bar{m}}} & W_n(W_m(-)) \\ \downarrow{\scriptstyle \varepsilon_{n,\bar{m}}} & & \downarrow{\scriptstyle W_n(\varepsilon_{n,\bar{m}})} \\ W_{\bar{m}}(-) & \xrightarrow{\Delta_{n,\bar{m}}} & W_n(W_{\bar{m}}(-)) \end{array}$$

commutes if and only if $\mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\bar{\mathfrak{m}}) = \mathbf{N}(\mathfrak{n})\backslash\mathbf{N}(\mathfrak{m})$. This is in particular the case if $\mathfrak{n} \mid \bar{\mathfrak{m}}$.

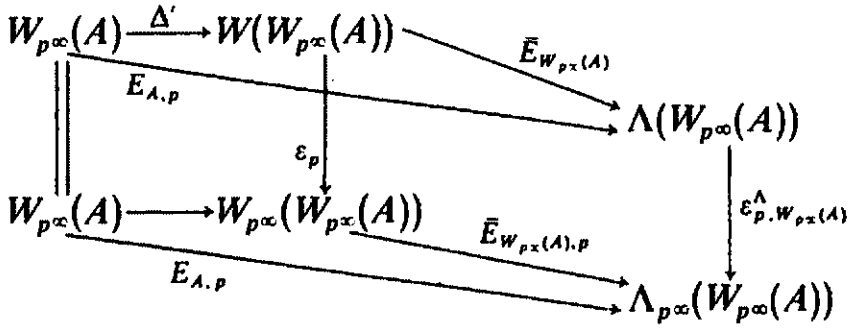
Proofs The proofs of (17.6.21)–(17.6.24) are standard (by now) and are left to the reader.

■ (17.6.25) **Proposition** The following diagram is commutative

$$\begin{array}{ccc} W(-) & \longrightarrow & W(W(-)) \\ \downarrow & & \downarrow \\ W(-) & \longrightarrow & W_{p^\infty}(W(-)) \\ \downarrow & & \downarrow \\ W_{p^\infty}(-) & \longrightarrow & W_{p^\infty}(W_{p^\infty}(-)) \end{array}$$

Proof Immediate from (17.6.22) and (17.6.24).

■(17.6.26) **Proposition** Let p be a prime number and A a perfect field of characteristic $p > 0$. Then the following diagram is commutative



(where we have used that the image of $E_{A,p}$ is in fact in $\Lambda_p(W_{p^\infty}(A))$; cf. Addendum (17.5.7), and where the horizontal arrows are the appropriate Δ homomorphisms).

Proof In view of (17.6.22), (17.5.7), and (17.4.24) it suffices to show that the upper triangle is commutative. To do this we recall that

$$s_n(E_{A,p}) = \begin{cases} 0 & \text{if } n \text{ is not a power of } p \\ \mathfrak{f}_p^l & \text{if } n = p^l, \quad l = 0, 1, 2, \ldots \end{cases}$$

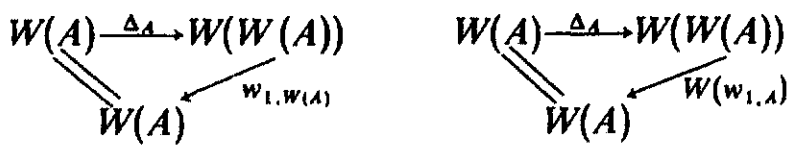
(cf. (17.5.8)). On the other hand $s_n\bar{E}_{W_{p^\infty}(A)} = w_n$ by Proposition (17.2.9) and

$$w_n\Delta' = \begin{cases} 0 & \text{if } n \text{ is not a power of } p \\ \mathfrak{f}_p^l & \text{if } n = p^l, \quad l = 0, 1, 2, \ldots \end{cases}$$

This shows that $s_nE_{A,p} = s_n\bar{E}_{W_{p^\infty}(A)}\Delta'$ for all $n \in \mathbf{N}$ and hence proves the commutativity of the upper triangle of the diagram above.

■(17.6.27) **Remark** Proposition (17.6.26) shows that the Artin–Hasse exponential $E_{A,p}$ of Section 17.5 can indeed be extended to a functor morphism $W_{p^\infty}(-) \to \Lambda(W_{p^\infty}(-))$.

■(17.6.28) **Remark** The following two diagrams are functorially commutative



Proof The first diagram is commutative by the definition of Δ. The commutativity of the second diagram is proved as usual by composing with the $w_{n,A}\colon W(A) \to A$.

■(17.6.29) **Remark** Identifying $\Lambda(A)$ with $W(A)$ and $\Lambda(\Lambda(A))$ with $W(W(A))$, the Artin–Hasse exponential gives us a homomorphism of rings $\Lambda(A) \to \Lambda(\Lambda(A))$. This is the canonical ring homomorphism λ_{-t} defined by the λ-operations on $\Lambda(A)$. See (E.2.1).

E.2 Bibliographical and Other Notes

(E.2.1) **Note on λ-rings, Adams operations, and Artin–Hasse exponentials** A pre-λ-ring (called λ-ring in [15, 152, 154]) is a commutative ring R with identity 1 and a set of maps λ^n: $R \to R$, $n \in \mathbf{N} \cup \{0\}$ such that for all $x, y \in R$, (i) $\lambda^0(x) = 1$, (ii) $\lambda^1(x) = x$, (iii) $\lambda^n(x + y) = \sum_{r=0}^{n} \lambda^r(x)\lambda^{n-r}(y)$.

Examples are, e.g., the rings $K(M)$ (classes of vector bundles over the space M), $K_G(M)$ (G a compact Lie group), $R(G)$, the complex representation ring of a finite group. In all these cases the λ-operations are induced by exterior powers.

Let A be any ring, $\Lambda(A)$ the ring $1 + tA[\![t]\!]$ constructed and studied in Section 17.2. Using symmetric functions as in (17.2.1) we define λ-operations on $\Lambda(A)$ by the formula

$$f(t) = 1 + a_1 t + a_2 t^2 + \cdots = \sum_{i=1}^{\infty} (1 - \xi_i t)$$

$$\lambda^r f(t) = \prod_{i_1 < \cdots < i_r} (1 - \xi_{i_1}\xi_{i_2} \cdots \xi_{i_r} t)$$

One easily checks that $\Lambda(A)$ with these λ-operations is a pre-λ-ring. Let R_1, R_2 be two pre-λ-rings. A ring homomorphism ϕ: $R_1 \to R_2$ is called a homomorphism of pre-λ-rings if $\phi \circ \lambda^i = \lambda^i \circ \phi$ for all $i \in \mathbf{N} \cup \{0\}$. If R is a pre-λ-ring, then λ_{-t}: $R \to \Lambda(R)$, $x \mapsto 1 - \lambda^1(x)t + \lambda^2(x)t^2 - \lambda^3(x)t^3 + \cdots$ is a homomorphism of abelian groups; R is called a *λ-ring* if λ_{-t} is a homomorphism of pre-λ-rings. (These are called special λ-rings in [15, 152, 154].) The examples $K(X)$, $K_G(X)$, $R(G)$ are all λ-rings; and so is $\Lambda(A)$ [154].

Adams operations Let R be a pre-λ-ring. We define operations Ψ^i: $R \to R$ by the formula

$$\sum_{i=1}^{\infty} \Psi^i(x)t^i = -t\frac{d}{dt}\log(\lambda_{-t}(x))$$

Then the Ψ^i: $R \to R$, the Adams operations, satisfy $\Psi^1(x) = x$, $\Psi^n(x + y) = \Psi^n(x) + \Psi^n(y)$ for all $x, y \in R$.

Theorem 1 Let R be a torsion free pre-λ-ring. Define the Ψ^i as above. Suppose that $\Psi^i(1) = 1$, $\Psi^i(xy) = \Psi^i(x)\Psi^i(y)$, $\Psi^i(\Psi^j(x)) = \Psi^{ij}(x)$ for all $x, y \in R$, $i, j \in \mathbf{N}$. Then R is a λ-ring. (Cf. [224, p. 49] for a proof.)

Theorem 2 Let A be a ring, Ψ^n the Adams operations on $\Lambda(A)$ and $\mathbf{f}_n^\wedge$ the Frobenius endomorphisms of $\Lambda(A)$ (cf. 17.3). Then $\Psi^n = \mathbf{f}_n^\wedge$ for all $n \in \mathbf{N}$.

Proof Because Ψ^n and $\mathbf{f}_n^\wedge$ are both additive and continuous and $\Lambda(A)$ is Hausdorff, it suffices to check that $\Psi^n(1 - xt^m) = \mathbf{f}_n^\wedge(1 - xt^m)$ for all $x \in A$, $n, m \in \mathbf{N}$. Let $A' \supset A$ be such that we can write $1 - xt^m = \prod_{i=1}^{m} (1 - y_i t)$ with $y_i \in A'$. Both Ψ^n and $\mathbf{f}_n^\wedge$ being functorial, we see that it suffices to check that $\Psi^n(1 - yt) = \mathbf{f}_n^\wedge(1 - yt)$ for all $y \in A'$ (because $\Lambda(A) \to \Lambda(A')$ is injective if $A \to A'$ is injective). Now $\lambda^i(1 - yt) = 0$ if $i > 1$ and $\lambda^1(1 - yt) = 1 - yt$, where λ^i is the ith λ-operation on $\Lambda(A')$ (cf. the defining formula above). Hence $\Psi^n(1 - yt) = (1 - yt) * \cdots * (1 - yt)$ (n times); i.e., $\Psi^n(1 - yt) = 1 - y^n t = \mathbf{f}_n^\wedge(1 - yt)$. This proves the theorem.

An immediate corollary is that the $\Lambda(A)$ are λ-rings (by Theorem 1). By definition $\Psi^n = s_n \circ \lambda_{-t}$. Hence, recalling that $s_n \circ \bar{E} = w_n$, we find that under the canonical iso-

morphisms $\Lambda(-) \simeq W(-)$ and $\Lambda(\Lambda(-)) \simeq W(W(-))$ the Artin–Hasse exponential Δ_A: $W(A) \to W(W(A))$ (which is characterized by $w_n \circ \Delta_A = \mathbf{f}_n$) corresponds to the canonical homomorphism of λ-rings λ_{-t}: $\Lambda(A) \to \Lambda(\Lambda(A))$.

Remarks

(i) The reader familiar with λ-rings will have noticed that there are a couple minus signs in our formulas above where one is used to plus signs. These are caused by the fact that we defined the ring structure on $\Lambda(A)$ in such a way that $1 - t$ is the unit element (rather than $1 + t$). A transformation $t \mapsto -t$ will put everything right.

(ii) λ-rings were first defined by Grothendieck [152] in an algebraic-geometric setting; they were first used in group theory by Atiyah and Tall [15]. For more material on λ-rings, cf. also [32] (besides the references already mentioned).

(E.2.2) **Universality properties of the functors** $A \mapsto \Lambda(A)$, $A \mapsto W(A)$ The rings and groups $\Lambda(A)$ also have certain universality properties. To state these let Λ_A: $\mathbf{Alg}_A \to \mathbf{Ring}$ be the functor that assigns to every A-algebra B the ring $\Lambda(B)$. We also use Λ_A for the functor $\mathbf{Alg}_A \to \mathbf{Group}$, i.e., the composite of the ring-valued functor Λ_A with the forgetful functor $\mathbf{Ring} \to \mathbf{Group}$. Let D_A: $\mathbf{Alg}_A \to \mathbf{Set}$ be the functor that assigns to every A-algebra B the set B. Finally, let λ_A: $D_A \to \Lambda_A$ be the functor morphism that takes $b \in B$ to $1 - bt \in \Lambda(B)$. One now has

(i) for every receptive group functor G: $\mathbf{Alg}_A \to \mathbf{Group}$ and functor morphism $\mu \in \mathbf{Alg}_A\mathbf{Set}(D_A, G)$ such that $\mu(0) = 1 \in G(A)$, there is a unique functor morphism $\nu \in \mathbf{Alg}_A\mathbf{Group}(\Lambda_A, G)$ such that $\mu = \nu\lambda_A$;

(ii) for every ring functor G: $\mathbf{Alg}_A \to \mathbf{Ring}$ such that the underlying group functor of G is receptive and every functor morphism $\mu \in \mathbf{Alg}_A\mathbf{Set}(D_A, G)$ such that $\mu(0) = 0 \in G(A)$, $\mu(1) = 1 \in G(A)$ and $\mu(ab) = \mu(a)\mu(b)$ for all $a, b \in B \in \mathbf{Alg}_A$, there exists a unique functor morphism ν: $\mathbf{Alg}_A\mathbf{Ring}(\Lambda_A, G)$ such that $\mu = \nu\lambda_A$.

Here receptivity is a certain technical condition and if $\mathbf{C}$ and $\mathbf{D}$ are two categories, then $\mathbf{CD}$ denotes the category with as objects all functors $\mathbf{C} \to \mathbf{D}$ and as morphisms all functor morphisms ϕ: $F \to G$ between functors F, G: $\mathbf{C} \to \mathbf{D}$.

The universality property (i) is very much related to Cartier's first theorem, which we shall discuss later in Chapter V, Section 27.1.

For more details concerning these universality properties and the notion of "receptivity," cf. [95, Chapter V, Section 5, nos. 1 and 2].

In addition to the universality properties (i) and (ii) the functor Λ has the categorically curious property of being right adjoint to the forgetful functor λ-$\mathbf{Ring} \to \mathbf{Ring}$. That is, there is a functorial isomorphism

$$\mathbf{Ring}(S, A) \xrightarrow{\sim} \lambda\text{-}\mathbf{Ring}(S, \Lambda(A))$$

$S \in \lambda$-$\mathbf{Ring}$, $A \in \mathbf{Ring}$. Note that in the formula above Λ appears on the right, while in the universality properties (i) and (ii) Λ appears on the left. For a proof of this right adjointness property of $A \mapsto \Lambda(A)$, cf. [224, p. 20].

(E.2.3) **Notes on Section 16** The notion of curves and p-typical curves in a formal group is due to Cartier [65] and so are the definitions of the operators $\langle a \rangle$, $\mathbf{f}_n$, $\mathbf{V}_n$, the decomposition theorem (16.4.18), and the definition of the projector ε_p. Cartier defined the big Witt vectors $W(A)$ via $\Lambda(A)$, i.e., practically as curves in $\hat{\mathbf{G}}_m^-(X, Y)$; cf.

[64]. Ever since the interpretation of $\mathscr{C}(F; A)$ as a group of Witt-like vectors with associated Witt polynomials $n\bar{w}_n^F$ has been a folklore sort of fact. Lately this has attracted the attention of some topologists ([136; 203, part III]), cf. also B.4.2 below for applications of this observation, which also holds for higher dimensional $F(X, Y)$; cf. [508].

(E.2.4) **Notes on Section 17** For Section 17, I have made use of Cartier's notes [64, 68, and 70], Bergman [29], Serre [361], and Knutson [224]. The definition and characterization of Δ_A: $W(-) \to W(W(-))$ comes from [68], as does the rather crucial lemma (17.6.1). Cartier attributes this lemma to Dwork and Dieudonné. And indeed, as is apparent from the proofs we have given, the three lemmas (2.3.3) (Dieudonné [113]), (2.3.4) (Dwork [137]), and (17.6.1) (Cartier [68]) are very closely related. A proof of Lemma (17.6.1) and a treatment of Δ_A along the lines of [68] can also be found in [256].

The notion of a supernatural number is due to Tate.

The proof of Witt's Theorem (17.4.17) given above is due to Cartier (cf. [94]) which is where I found it.

CHAPTER IV

HOMOMORPHISMS, ENDOMORPHISMS, AND THE CLASSIFICATION OF FORMAL GROUPS BY POWER SERIES METHODS

As in Chapter III all formal group laws in this chapter will be commutative.

18 Definitions and Preliminary Elementary Results. Survey of Chapter IV

18.1 Isomorphisms

Let $F(X, Y)$ and $G(X, Y)$ be formal group laws over a ring A with index sets I and J, respectively. A *homomorphism* $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is a J-tuple of power series in the indeterminates X_i, $i \in I$, such that the "monomials have finite support" condition of Chapter II, Section 9.6 holds, such that $\alpha(X) \equiv 0$ mod(degree 1) and such that

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y)) \tag{18.1.1}$$

The homomorphism $\alpha(X)$ is an *isomorphism* if $J(\alpha)$, the Jacobian matrix of α, is invertible; $\alpha(X)$ is a *strict isomorphism* if $J(\alpha)$ is the identity matrix (of the appropriate size). (Recall that $J(\alpha)$ is defined by $\alpha(X) \equiv J(\alpha)X$ mod(degree 2).)

Of course the homomorphism $\alpha(X)$ is an isomorphism iff there is an inverse homomorphism $\beta(X)$: $G(X, Y) \to F(X, Y)$ such that $\alpha(X) \circ \beta(X) = id$ and $\beta(X) \circ \alpha(X) = id$. We use $\mathbf{FG}_A$ to denote the category of formal group laws over A.

■ (18.1.2) **Universal strict isomorphisms** The first topic we take up in Chapter IV is the construction of some universal strict isomorphisms, notably a strict isomorphism $\alpha_{V,T}(X)$: $F_V(X, Y) \to F_{V,T}(X, Y)$. As in the case of universal formal group laws, the importance of $\alpha_{V,T}(X)$ does not lie in the fact of its existence—a trivial matter—but in the fact that the underlying ring is a free

ring of (commutative) polynomials $\mathbf{Z}[V, T] = \mathbf{Z}[\ldots, V_n(i,j), T_n(i,j), \ldots]$. The precise statement concerning $\alpha_{V,T}(X)$ is

■ (18.1.3) **Theorem** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a strict isomorphism of p-typical r-dimensional formal group laws over a ring A and suppose that A is a $\mathbf{Z}_{(p)}$-algebra or that A is of characteristic zero. Then there is a unique homomorphism ϕ: $\mathbf{Z}[V; T] \to A$ such that

$$\phi_* F_V(X, Y) = F(X, Y), \qquad \phi_* \alpha_{V,T}(X) = \alpha(X), \qquad \phi_* F_{V,T}(X, Y) = G(X, Y)$$

■ (18.1.4) Thus, so to speak, $\alpha_{V,T}(X)$ is the most general strict isomorphism possible. More precisely, since $F_{V,T}(X, Y)$ is a p-typical formal group law over $\mathbf{Z}[V, T]$, there exists a unique homomorphism ψ: $\mathbf{Z}[V] \to \mathbf{Z}[V, T]$ such that $\psi_* F_V(X, Y) = F_{V,T}(X, Y)$ (by the universality of $F_V(X, Y)$ over $\mathbf{Z}[V]$). Let $\bar{V}_n = \psi_*(V_n)$, then the coefficients of the matrices $\bar{V}_n$ are polynomials in the $T_m(i, j)$, $V_m(i, j)$ with $m \leq n$. These polynomials describe the most general possible variation of p-typical formal group laws within a given strict isomorphism class. (And, for applications in algebraic topology, it is interesting and profitable to note that in the one dimensional case $V_i \mapsto \bar{V}_i$ is identifiable with the right unit homomorphism η_R: $BP(pt) \to BP_*(BP)$ of the Hopf algebra $BP_*(BP)$ of Brown–Peterson homology (co)operations.)

In Section 19.3 we discuss some recursion formulas for the $\bar{V}_n$. If these formulas are manageable, then they ought to give some classification results; and in 19.4 we show that they are indeed manageable, at least to the point that they give a new proof of Lazard's theorem that the one dimensional formal group laws over a separably closed field of characteristic $p > 0$ are classified by their heights. (For the notion of height, see (18.3.1)–(18.3.4).)

18.2 Homomorphisms and endomorphisms

Now let $F(X, Y)$ and $G(X, Y)$ be (finite dimensional) formal group laws over a characteristic zero ring A and let $f(X)$ and $g(X)$ be their logarithms. Now every homomorphism of the n-dimensional additive group $\hat{\mathbf{G}}_a^n(X, Y)$ over $A \otimes \mathbf{Q}$ to the m-dimensional additive group $\hat{\mathbf{G}}_a^m(X, Y)$ over $A \otimes \mathbf{Q}$ is of the form $\alpha(X) = aX$ where a is some $m \times n$ matrix with coefficients in $A \otimes \mathbf{Q}$. It follows that every homomorphism $\beta(X)$: $F(X, Y) \to G(X, Y)$ is necessarily of the form

$$\beta(X) = g^{-1}(af(X)), \qquad a \in A^{m \times n} \tag{18.2.1}$$

so that the calculation of $\mathrm{Hom}_A(F(X, Y), G(X, Y))$ boils down to finding out which $m \times n$ matrices a are such that $g^{-1}(af(X))$ has all its coefficients in A. Now suppose that $g(X)$ satisfies some functional equation

$$g(X) - \sum_{i=1}^{\infty} s_{i,p}(\sigma_p^i)_* g(X^{q^i}) \in A \otimes \mathbf{Z}_{(p)}[\![X]\!] \tag{18.2.2}$$

then parts (ii) and (iii) of the functional equation lemma 10.2 say that $g^{-1}(af(X))$ is integral if and only if $af(X)$ satisfies the same type of functional equation. Using this elementary remark, we show in 20.1 that the universal formal group laws $F_V(X, Y)$ have no more endomorphisms than they should have (viz. $\mathbf{Z}$), and we deduce a number of results concerning isomorphisms, homomorphisms, and isomorphisms of (generalized higher dimensional) Lubin–Tate formal group laws. For instance, if $F(X, Y)$ is an n-dimensional generalized Lubin–Tate formal group law over a p-adic integer ring A with logarithm $f(X) = X + \pi^{-1}B\tau_* f(X^{p^r})$ with B invertible, then $F(X, Y)$ is isomorphic over $\hat{A}_{nr}$, the completion of the maximal unramified extension of A, to an n-fold product of the one dimensional twisted Lubin–Tate formal group law with logarithm $f(X) = X + \pi^{-1}\tau_* f(X^{p^r})$.

■ (18.2.3) **Homomorphisms over characteristic $p > 0$ rings** At first sight it would appear that the use of such functional equation techniques as above would be of no use at all in studying homomorphism and endomorphisms over characteristic $p > 0$ rings. This is not the case, and in Section 20.2 we use functional equation tricks to calculate the rings of endomorphisms of one dimensional formal group laws of height $h < \infty$ over a separably closed field of characteristic $p > 0$. The result is that this ring of endomorphisms is the ring of integers of the central division algebra of rank h^2 and invariant h^{-1} over $\mathbf{Q}_p$ (Corollary (20.2.14)). A more systematic treatment of homomorphisms over characteristic $p > 0$ rings via functional equation tricks is the subject matter of Section 20.4.

■ (18.2.4) **Functional equation formal group laws** All this makes it useful to have some idea as to when one can expect a formal group law to be of functional equation type. By Proposition (20.1.3) and Corollary (20.1.5) this is always the case for formal group laws over p-adic integer rings A that are *unramified*.

Assume for the moment that A is a p-adic integer ring with Frobenius endomorphism σ, $\sigma a \equiv a^q \bmod \pi$ where π is a uniformizing element of A, and let $F(X, Y)$, $G(X, Y)$ be one dimensional (for simplicity) formal group laws over A, with logarithms $f(X)$, $g(X)$ that satisfy functional equations

$$(18.2.5)\quad f(X) = X + \sum_{i=1}^{\infty} \pi^{-1}u_i\sigma^i_* f(X^{q^i}), \qquad g(X) = X + \sum_{i=1}^{\infty} \pi^{-1}v_i\sigma^i_* f(X^{q^i})$$

with $u = (u_1, u_2, \ldots)$, $v = (v_1, v_2, \ldots)$ sequences of elements of A. Let $K_\sigma[\![T]\!]$ be the ring of all power series in T with coefficients in K, the quotient field of A, with the multiplication rule $Ta = \sigma(a)T$. We associate to $F(X, Y)$ and $G(X, Y)$ the elements $\eta_u = \pi - u_1 T - u_2 T^2 - \cdots$, $\eta_v = \pi - v_1 T - v_2 T^2 - \cdots$ of $A_\sigma[\![T]\!] \subset K_\sigma[\![T]\!]$. Then there exists a homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ with $J(\alpha) = c$ iff there is an element $\vartheta_c \in A_\sigma[\![T]\!]$ such that $\eta_v c = \vartheta_c \eta_u$ (Proposition (20.3.9)).

This can be applied in particular to a discussion of isomorphisms with as a result the theorem (cf. Theorem (20.3.12)):

■ (18.2.6) **Theorem** Let A be the ring of integers of a complete absolutely unramified discrete valuation field of characteristic zero and perfect residue field of characteristic $p > 0$. Then the strict isomorphism classes of one dimensional formal group laws over A correspond bijectively to elements of $A_\sigma[\![T]\!]$ of the form $p + \sum_{i=1}^{h} b_i T^i$ with $b_i \in pA$ for $i = 1, \ldots, h-1$ and $b_h \in A^*$, the units of A.

18.3 Height of a formal group law and the reduction map

■ (18.3.1) **The one dimensional case** Let k be a field of characteristic $p > 0$. Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of one dimensional formal group laws over k. Suppose $\alpha(X) = a_1 X + a_2 X^2 + \cdots$, then we define $J(\alpha) = a_1$ (the Jacobian "matrix" of $\alpha(X)$). Then if $J(\alpha) = 0$, we either have $\alpha(X) = 0$ or there is a power q of p such that $\alpha(X) = \beta(X^q)$ $\beta(X) \not\equiv 0$ mod(degree 2). Indeed, consider the relation

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$$

Partial differentiation with respect to Y gives us

$$\frac{d\alpha}{dX}(F(X, Y)) \cdot \frac{\partial F}{\partial Y}(X, Y) = \frac{\partial G}{\partial Y}(\alpha(X), \alpha(Y)) \cdot \frac{\partial \alpha}{\partial X}(Y)$$

and substituting 0 for Y in this equality gives us

$$\frac{d\alpha}{dX}(X) \cdot \frac{\partial F}{\partial Y}(X, 0) = \frac{\partial G}{\partial Y}(\alpha(X), 0) \cdot \frac{\partial \alpha}{\partial X}(0)$$

Now $(\partial F/\partial Y)(X, 0) = 1 + X + \cdots$ so is invertible in $k[\![X]\!]$ and $(\partial\alpha/\partial X)(0) = J(\alpha)$. So if $J(\alpha) = 0$ we have $(d\alpha/dX)(X) = 0$ which means that $\alpha(X)$ is of the form $\alpha(X) = \beta(X^p)$ for some power series $\beta(X)$. If we can now show that $\beta(X)$ is a homomorphism of formal group laws (not necessarily between $F(X, Y)$ and $G(X, Y)$), we are through by induction. Let $\sigma_* F(X, Y)$ be the formal group law obtained from $F(X, Y)$ by raising each of its coefficients to the pth power. Then

$$\beta(\sigma_* F(X^p, Y^p)) = \beta(F(X, Y)^p) = \alpha(F(X,Y)) = G(\alpha(X), \alpha(Y)) = G(\beta(X^p), \beta(Y^p))$$

so that $\beta(X)$ is a homomorphism from $\sigma_* F(X, Y)$ to $G(X, Y)$.

■ (18.3.2) **Definition** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be as above in (18.3.1). Then we say that $\mathrm{ht}(\alpha(X)) = \infty$ iff $\alpha(X) = 0$ and $\mathrm{ht}(\alpha(X)) = r$ if $q = p^r$ is the highest power of p such that $\alpha(X) = \beta(X^q)$ for some $\beta(X)$. Note that by (18.3.1) X^{p^r} is the first power of X in $\alpha(X)$ with nonzero coefficient. One checks easily that $\mathrm{ht}(\alpha(X) \circ \beta(X)) = \mathrm{ht}(\alpha(X)) + \mathrm{ht}(\beta(X))$ and that $\mathrm{ht}(\alpha(X) +_G \beta(X)) \geq$

$\min\{\mathrm{ht}(\alpha(X)), \mathrm{ht}(\beta(X))\}$, so the ht function defines a valuation on the ring $\mathrm{End}_k(F(X, Y))$.

■ (18.3.3) **Definition** Let $F(X, Y)$ be a one dimensional formal group law over a characteristic $p > 0$ field k, then we define $\mathrm{ht}(F(X, Y)) = \mathrm{ht}([p]_F(X))$.

■ (18.3.4) **Example** Let $F_V(X, Y)$ over $\mathbf{Z}[V]$ be the one dimensional universal p-typical formal group law of Section 2.3 of Chapter I. Let $v = (v_1, v_2, \ldots)$ be a series of elements of k. Let $h \in \mathbf{N}$ be the smallest natural number such that $v_h \neq 0$. Then $\mathrm{ht}(F(X, Y)) = h$. Indeed

$$F_V(X, Y) \equiv X + Y + V_h C_{p^h}(X, Y) \mod(V_1, V_2, \ldots, V_{h-1}, \text{degree } p^h + 1) \tag{18.3.5}$$

because $f_V(X) \equiv X + p^{-1} V_h X^{p^h} \mod(V_1, \ldots, V_{h-1}, \text{degree } p^{h+1})$; cf., e.g., Chapter I (3.3.8). Now it follows from (18.3.5) that if $v_1 = v_2 = \cdots = v_{h-1} = 0$ and $\mathrm{char}(k) = p > 0$, then

$$[p]_{F_v}(X) \equiv v_h X^{p^h} \mod(\text{degree } p^h + 1) \tag{18.3.6}$$

so that indeed $\mathrm{ht}(F_v(X, Y)) = h$ if $v_h \neq 0$, $v_1 = \cdots = v_{h-1} = 0$.

■ (18.3.7) **Remark** Let $F(X, Y)$, $G(X, Y)$ be one dimensional formal group laws of different heights over a characteristic $p > 0$ field k. Then there are no nonzero homomorphisms $\alpha(X)$: $F(X, Y) \to G(X, Y)$. Indeed, if $\alpha(X)$ is a homomorphism, then we must have

$$\alpha([p]_F(X)) = [p]_G(\alpha(X))$$

and if $\alpha(X) \neq 0$ this is only possible if $\mathrm{ht}([p]_F(X)) = \mathrm{ht}([p]_G(X))$. (NB this is not true for higher dimensional formal group laws.)

■ (18.3.8) **Definition of height (higher dimensional case)** Now let $F(X, Y)$ be an n-dimensional formal group law over k, $\mathrm{char}(k) = p > 0$, as before. Consider the n-tuple of power series $[p]_F(X) = (H_1(X), \ldots, H_n(X))$. We then say that the formal group law $F(X, Y)$ over the perfect field k is of finite height if the ring $k[\![X_1, \ldots, X_n]\!]$ is a finitely generated module over the subring $k[\![H_1(X), \ldots, H_n(X)]\!]$. If this is the case, $k[\![X_1, \ldots, X_n]\!]$ is free of rank p^r, $r \in \mathbf{N}$ over $k[\![H_1(X), \ldots, H_n(X)]\!]$ and we call r the height of $F(X, Y)$. (These statements will be proved in Chapter V, Section 28.2.)

■ (18.3.9) **Remarks** In case $n = 1$ the definition of (18.3.8) of course coincides with the one given in (18.3.2). If $n > 1$, more care must be taken. The arguments of (18.3.1) also work for higher dimensional formal group laws. But, of course, if q is the highest power of X such that $[p]_F(X) = \beta(X^q)$ for some $\beta(X)$ and $n \geq 2$, then $F(X, Y)$ can still very well be of infinite height. (Take, e.g., $F(X, Y) = \hat{\mathbf{G}}_a(X, Y) \times \hat{\mathbf{G}}_m(X, Y)$.)

■ (18.3.10) Now let A be a local ring of characteristic zero with residue field o characteristic $p > 0$, and let $F(X, Y)$ be a formal group law over A. Then w define the height of $F(X, Y)$ as the height of $\bar{F}(X, Y)$, the reduction of $F(X, Y)$ over k.

■ (18.3.11) **Proposition** Let $F(X, Y)$ be a formal group law of finite heigh over a complete local noetherian ring R of characteristic 0 and residue charac teristic $p > 0$. Let $G(X, Y)$ be a second formal group law of over R. Then th reduction map

$$\mathbf{FG}_A(F(X, Y), G(X, Y)) \to \mathbf{FG}_k(\bar{F}(X, Y), \bar{G}(X, Y))$$

is injective.

Proof Because the reduction map is a homomorphism, it suffices to sho that $\bar{\alpha}(X) = 0 \Rightarrow \alpha(X) = 0$. Let $\mathfrak{m}$ be the maximal ideal of R and suppose th the homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is nonzero but that $\bar{\alpha}(X) =$ Let $\mathfrak{m}^r$ be the highest power of $\mathfrak{m}$ such that $\alpha(X) \equiv 0 \bmod \mathfrak{m}^r$. Then $r \geq$ Choose a basis $\{e_j\}$ of the k vector space $\mathfrak{m}^r/\mathfrak{m}^{r+1}$. Then modulo $\mathfrak{m}^{r+1}$ there i unique expression $\alpha_i(X) = \sum_j e_j \beta_{ij}(X)$ where $\alpha_i(X)$ is the ith component $\alpha(X)$ and where $\beta_{ij}(X)$ is a power series with coefficients in k.

Now consider

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$$

modulo $\mathfrak{m}^{r+1}$. Because $G(X, Y) \equiv X + Y \bmod$(degree 2). We obtain

$$\sum_j e_j \beta_{ij}(F(X, Y)) = \sum_j e_j(\beta_{ij}(X) + \beta_{ij}(Y))$$

So if there is a $\beta_{ij}(X) \neq 0$, we find a nonzero homomorphism β_{ij}: $\bar{F}(X, Y$ $\hat{\mathbf{G}}_a(X, Y)$, which is impossible because in the diagram

$$\begin{array}{ccc} \bar{F}(X, Y) & \xrightarrow{\beta_{ij}} & \hat{\mathbf{G}}_a(X, Y) \\ \Big\downarrow{\scriptstyle [p]_F} & & \Big\downarrow{\scriptstyle [p]_{G_a}} \\ \bar{F}(X, Y) & \xrightarrow{\beta_{ij}} & \hat{\mathbf{G}}_a(X, Y) \end{array}$$

the left-hand vertical arrow makes $k[\![X]\!]$ into a finite rank module over while the right-hand vertical arrow is zero.

■ (18.3.12) Now let A be a complete discrete valuation ring of characte zero and let $F(X, Y)$, $G(X, Y)$ be one dimensional formal group laws ov Let $f(X)$, $g(X)$ be the logarithms and let T be an indeterminate.

Consider $g^{-1}(Tf(X)) = \sum_{i=1}^{\infty} \phi_i(T)X^i$. Then the $\phi_i(T)$ are polynomials with coefficients in K, the quotient field of A. Now consider the m $\mathbf{FG}_A(F(X, Y), G(X, Y)) \to A$ which assigns to each $\alpha(X) \in \mathbf{FG}_A(F(X$ $G(X, Y))$ the coefficient of X. First, J is an embedding because every $\alpha(X$ the form $g^{-1}(af(X))$ for some unique $a \in A$ (because A is of characteristic cf. also 18.2).

We claim that the image of J in A is closed. Indeed

$$a \in \mathrm{Im}(J) \quad \Leftrightarrow \quad \phi_i(a) \in A \quad \text{for all} \quad i \quad \Leftrightarrow \quad a \in \bigcap_i \phi_i^{-1}(A)$$

and this is a closed subset of A because $A \subset K$ is closed and because the ϕ_i are polynomials and hence continuous.

Assume that $G(X, Y)$ and $F(X, Y)$ are of finite height. Then there are three filtration topologies that one can consider on $\mathbf{FG}_A(F(X, Y), G(X, Y))$ viz.:

(i) the topology defined by the height filtration on $\mathbf{FG}_k(\bar{F}(X, Y), \bar{G}(X, Y))$ via the injection $\mathbf{FG}_A(F(X, Y), G(X, Y)) \to \mathbf{FG}_k(\bar{F}(X, Y), \bar{G}(X, Y))$;

(ii) the topology defined by the embedding J: $\mathbf{FG}_A(F(X, Y), G(X, Y)) \to A$;

(iii) the topology defined by the subgroups $[p^n]_G\, \mathbf{FG}_A(F(X, Y), G(X, Y))$.

■ (18.3.13) **Proposition** Let A, $F(X, Y)$, $G(X, Y)$ be as in (18.3.12) and assume that $F(X, Y)$ and $G(X, Y)$ are of finite height. Then the three topologies listed above on $\mathbf{FG}_A(F(X, Y), G(X, Y))$ coincide and $\mathbf{FG}_A(F(X, Y), G(X, Y))$ is complete under these topologies (filtrations).

Proof A filtration w on a free $\mathbf{Z}_p$-module E of finite rank is called a *norm* if for some valuation v on $\mathbf{Z}_p$ that is equivalent to the usual one, v_p, one has

$$w(ae) = v(a) + w(e), \qquad a \in \mathbf{Z}_p, \quad e \in E$$

Any two norms on E are then equivalent (that is, they give rise to the same topology). This is seen by the usual argument (cf., e.g., [437, Theorem 2.1.1]). We are now going to view $\mathbf{FG}_A(F(X, Y), G(X, Y))$ as a $\mathbf{Z}_p$-module. To this end consider the commutative diagram

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathrm{End}_A(F(X, Y)) \\ & \searrow & \downarrow J \\ & & A \end{array}$$

where $\mathbf{Z}$ has the p-adic topology, $\mathrm{End}_A(F(X, Y))$ has topology (ii), and A has of course its discrete valuation ring topology. All maps are continuous, and since $\mathrm{End}_A(F(X, Y))$ is complete in topology (ii) by the completeness of A and (18.3.12) we can extend to obtain a commutative diagram

(18.3.14)
$$\begin{array}{ccc} \mathbf{Z}_p & \xrightarrow{i} & \mathrm{End}_A(F(X, Y)) \\ & \searrow & \downarrow \\ & & A \end{array}$$

making $\mathrm{End}_A(F(X, Y))$ and hence also $\mathbf{FG}_A(F(X, Y), G(X, Y))$ a $\mathbf{Z}_p$-module.

Let $w_{(i)}$, $w_{(ii)}$, $w_{(iii)}$ be the three filtrations listed in (18.3.12) and let $\beta(X) \in i(\mathbf{Z}_p)$ (cf. (18.3.14)) and $\alpha(X) \in \mathbf{FG}_A(F(X, Y), G(X, Y))$. Then

(18.3.15)
$$w_{(ii)}(\beta(X) \circ \alpha(X)) = v(J(\beta)) + w_{(ii)}(\alpha(X))$$

showing that $w_{(ii)}$ is a norm filtration.

Now consider $\mathrm{End}_A(F(X, Y))$ and $\mathrm{End}_k(\bar{F}(X, Y))$ with the height filtrations $w_{(i)}$ and $\mathbf{Z}$, $\mathbf{Z}_p$ with the p-adic topology. We find a commutative diagram

$$\begin{array}{ccc} \mathbf{Z}_p & \xrightarrow{i} & \mathrm{End}_A(F(X, Y)) \\ & \searrow \quad \swarrow & \\ & \mathrm{End}_k(\bar{F}(X, Y)) & \end{array} \tag{18.3.16}$$

It follows that the embedding $\mathbf{FG}_A(F(X, Y), G(X, Y)) \to \mathbf{FG}_k(\bar{F}(X, Y), \bar{G}(X, Y))$ is a homomorphism of $\mathbf{Z}_p$-modules. Let k_a be the algebraic closure of k. Then we know from (18.2.3) and Lazard's classification theorems (cf. (18.1.4)) that $\mathbf{FG}_{k_a}(\bar{F}(X, Y), \bar{G}(X, Y)) =$ free $\mathbf{Z}_p$-module of rank h^2, $h = \mathrm{ht}(\bar{F}(X, Y))$, if $\mathrm{ht}(\bar{F}(X, Y)) = \mathrm{ht}(\bar{G}(X, Y))$. And if $\mathrm{ht}(\bar{F}(X, Y)) \neq \mathrm{ht}(\bar{G}(X, Y))$, then $\mathbf{FG}_{k_a}(\bar{F}(X, Y), \bar{G}(X, Y)) = 0$ by the commutativity of the diagram

$$\begin{array}{ccc} \bar{F}(X, Y) & \xrightarrow{\alpha} & \bar{G}(X, Y) \\ \downarrow [p]_F & & \downarrow [p]_{\bar{G}} \\ \bar{F}(X, Y) & \xrightarrow{\alpha} & \bar{G}(X, Y) \end{array}$$

(If $\mathrm{ht}\,\alpha(X) = r$, $\mathrm{ht}(G(X, Y)) = h_2$, $\mathrm{ht}(F(X, Y)) = h_1$, then $\mathrm{ht}([p]_G(X) \circ \alpha(X)) = r + h_2$ and $\mathrm{ht}(\alpha(X) \circ [p]_F(X)) = r + h_1$ (cf. (18.3.2)).

So we see that $\mathbf{FG}_A(F(X, Y), G(X, Y))$ is a sub-$\mathbf{Z}_p$-module of a free $\mathbf{Z}_p$-module of rank h^2 so that

(18.3.17) $\mathbf{FG}_A(F(X, Y), G(X, Y))$ is a free $\mathbf{Z}_p$-module of rank $\leq h^2$

Now note that the restriction to $i(\mathbf{Z}_p)$ in (18.3.16) of the height filtration on $\mathrm{End}_A(F(X, Y))$ is h times the p-adic valuation on $\mathbf{Z}_p$. Hence

$$(18.3.18)\quad w_{(i)}(i(a) \circ \alpha(X)) = w_{(i)}(i(a)) + w_{(i)}(\alpha(X)) = hv_p(a) + w_{(i)}(\alpha(X))$$

showing that $w_{(i)}$ is also a norm filtration. Finally, $w_{(iii)}$ is a norm filtration on $\mathbf{FG}_A(F(X, Y), G(X, Y))$ by its definition. So (18.3.15), (18.3.17), and (18.3.18) prove that all three filtrations are equivalent.

18.4 Rings of endomorphisms

■(18.4.1) **Endomorphisms over $\mathbf{F}_q$ and $\mathbf{F}(p^\infty)$** Let $F(X, Y)$ be a one dimensional formal group law over a finite field $\mathbf{F}_q$ of height h. Then we have already seen that $\mathrm{End}_{\mathbf{F}(p^\infty)}(F(X, Y))$ is the ring of integers of the division algebra of rank h^2 and invariant h^{-1} over $\mathbf{Q}_p$.

Now over $\mathbf{F}_q$ there exists a very special endomorphism of $F(X, Y)$, viz. its Frobenius endomorphism $\xi_F(X) = X^q$ and one easily shows that $\mathrm{End}_{\mathbf{F}_q}(F(X, Y))$ consists of those endomorphisms over $\mathbf{F}(p^\infty)$ that commute with $\xi_F(X)$. So by the general theory of division algebras $\mathrm{End}_{\mathbf{F}_q}(F(X, Y))$ is the ring of integers of a central division algebra of rank h^2/m^2 and invariant m/h over $\mathbf{Q}_p(\xi_F)$ where $m = [\mathbf{Q}_p(\xi_F): \mathbf{Q}_p]$.

■(18.4.2) **Endomorphisms over a p-adic integer ring** Now let A be the ring of integers of a finite extension K of $\mathbf{Q}_p$, and let $F(X, Y)$ be a one dimensional formal group law over A of finite height h. Then first of all $\mathrm{End}_A(F(X, Y)) \to \mathrm{End}_k(\bar{F}(X, Y))$ is injective (Proposition (18.3.7)) so that $\mathrm{End}_A(F(X, Y))$ embeds in D_h the central division algebra of rank h^2 and invariant h^{-1}. It follows that the quotient field of $\mathrm{End}_A(F(X, Y))$ has at most rank h over $\mathbf{Q}_p$ (because $J\colon \mathrm{End}_A(F(X, Y)) \to A$ and because the dimension over $\mathbf{Q}_p$ of every commutative subfield of D_h is a divisor of h).

Even more is true. The injectivity of the reduction map also implies that $\mathrm{End}_A(F(X,Y)) = \mathrm{End}_B(F(X, Y))$ if B/A is totally ramified, so that if A' is the ring of integers of the algebraic closure of K, then $J(\mathrm{End}_{A'}(F(X, Y))) \subset A'$ is an order in some unramified extension L of degree $\leq h$ of K.

■(18.4.3) All the results mentioned so far are contained in Section 23 below, which in addition contains some results on when $\mathrm{End}_{A'}(F(X, Y)) = \mathrm{END}(F(X, Y))$, the absolute endomorphism ring of $F(X, Y)$, is integrally closed and on how to construct (in some cases) formal group laws with pregiven END ring.

18.5 Classification results

Scattered through Chapter IV are a number of classification results, mainly for one dimensional formal group laws. We already mentioned two.

■(18.5.1) **Theorem** Over a separably closed field k of characteristic $p > 0$ the one dimensional formal group laws are classified by their heights.

■(18.5.2) **Theorem** Over the ring of integers A of a complete absolutely unramified discrete valuation field of characteristic zero with perfect residue field k the *strict* isomorphism classes of formal group laws over A correspond bijectively with "Eisenstein" polynomials $p + \sum_{i=1}^{h} b_i T^i \in A_\sigma[\![T]\!]$ with $b_i \in pA$, $i = 1, \ldots, h-1$, $b_h \in U(A)$, the units of A (cf. Theorem (18.2.6)).

■(18.5.3) **Forms** Roughly the "philosophy of forms" is the following. Let L/K be a Galois extension and let Φ be some object defined over K. Then we say that an object Ψ over K is a (twisted) form of Φ, or an L/K-form of Φ, iff Φ and Ψ become isomorphic when one extends the scalars from K to L. For example if $F(X, Y)$ and $G(X, Y)$ are two one dimensional formal group laws of the same height over a characteristic p field k and k_{sc} is the separable closure of k, then Theorem (18.5.1) says that $F(X, Y)$ and $G(X, Y)$ are k_{sc}/k-forms of each other.

Let $E(L/K, \Phi)$ be the set of K-isomorphism classes (isomorphisms defined over K) of L/K-forms of Φ. Then quite often one has a bijective correspondence between $E(L/K, \Phi)$ and the first Galois cohomology group $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_K(\Phi))$ where $\mathrm{Aut}_K(\Phi)$ is the group of K-automorphisms of the object Φ.

The "philosophy of forms" is part of the "philosophy of descent" (or theory of descent) which also examines the question, Given an object Ψ over L, does there exist an object Φ over K that becomes isomorphic to Ψ after extension of scalars? (And, of course, both questions can be, and generally are, studied in a much more general base-change situation than K-L.)

In our case Theorem (18.5.1) combined with form theory gives us a chance to classify one dimensional formal group laws over fields. In case k is finite $H^1(\mathrm{Gal}(k_{sc}/k), \mathrm{Aut}_k(F(X, Y))$ turns out to be manageable, and there follow two classification results for one dimensional formal group laws over finite fields (really two formulations of the same classification result).

Let $F(X, Y)$ be a one dimensional formal group law over $\mathbf{F}(q)$, the field of q elements. Then $\xi_F(X) = X^q$ is an endomorphism of $F(X, Y)$. Now consider the equation that ξ_F satisfies as an element of D_h over the "standard" unramified extension contained in $\mathbf{Q}_p(\xi_F)$. This gives us a polynomial $\Psi_F(x) = x^e + b_1 x^{e-1} + \cdots + b_e$ with coefficients in $W_{p^\infty}(\mathbf{F}_q)$.

■ (18.5.4) **Theorem** One dimensional formal group laws $F(X, Y)$ over $\mathbf{F}_q$, the finite field with q elements, are classified by the characteristic polynomials $\Psi_F(x)$ of their Frobenius endomorphisms $\Psi_F(x) = x^e + b_1 x^{e-1} + \cdots + b_e$. These polynomials $\Psi_F(x)$ have the properties:

(18.5.5) $\Psi_F(x)$ is a polynomial with coefficients in $W_{p^\infty}(\mathbf{F}_q)$ that is irreducible over $K_q = W_{p^\infty}(\mathbf{F}_q) \otimes \mathbf{Q}_p$.

(18.5.6) If ξ is a root of $\Psi_F(x)$, then $\mathbf{Q}_p(\xi)/K_q$ is totally ramified.

(18.5.7) $[\mathbf{Q}_p(b_1, \ldots, b_e): \mathbf{Q}_p]v(b_e)$ divides r where $q = p^r$ and v is the normalized exponential valuation on K_q.

Conversely, every polynomial $\Psi(x)$ with the properties (18.5.5)–(18.5.7) is the characteristic polynomial of some finite height formal group law $F(X, Y)$ over $\mathbf{F}_q$, where the height h is equal to $v(b_e)^{-1}re$.

In the special case $q = p$, the polynomials satisfying (18.5.5)–(18.5.7) are precisely the Eisenstein polynomials over $\mathbf{Z}_p = W_{p^\infty}(\mathbf{F}_p)$.

■ (18.5.8) The second formulation of the classification result for one dimensional formal group laws is obtained as follows. Let $F(X, Y)$ be a one dimensional formal group law over $\mathbf{F}_q$. Choose any isomorphism γ: $\mathrm{End}_{\mathbf{F}(p^\infty)}(F(X, Y)) \xrightarrow{\sim} E_h \subset D_h$ and assign to $F(X, Y)$ the conjugacy class of the element $\gamma \circ \xi_F \circ \gamma^{-1}$ in E_h. This defines a map Ψ: $\mathrm{Iso}(\mathbf{F}_q, h) \to T_r$ where T_r is the set of conjugacy classes of elements of valuation $h^{-1}r$ where $q = p^r$, where $\mathrm{Iso}(\mathbf{F}_q, h)$ is the set of isomorphism classes of formal group laws of dimension one and height h over $\mathbf{F}_q$ and where the valuation on D_h is the unique one extending the normalized exponential valuation on $\mathbf{Z}_p \subset E_h \subset D_h$.

■ (18.5.9) **Theorem** The map Ψ is a bijection.

■ (18.5.10) Now let $F(X, Y)$ be a one dimensional formal group law over $\mathbf{Z}_p$. According to Theorem (18.5.2) $F(X, Y)$ is classified up to strict isomorphism by a certain Eisenstein polynomial of degree $h = \mathrm{ht}(F(X, Y))$ with coefficients in $\mathbf{Z}_p$. Let $\bar{F}(X, Y)$ be the reduction of $F(X, Y)$ over $\mathbf{F}_p$. Then according to Theorem (18.5.4) $\bar{F}(X, Y)$ is classified by a certain Eisenstein polynomial with coefficients in $W_{p^\infty}(\mathbf{F}_p) = \mathbf{Z}_p$ of degree h. These polynomials coincide! More about this will be said in Section 30.4 in connection with Cartier–Dieudonné modules. Meanwhile, the same circle of ideas leads to "lifting of Frobenius" results in Section 24.3.

The link between these two Eisenstein polynomials is provided by the following two results.

■ (18.5.11) **Lemma** Two one dimensional formal group laws over $\mathbf{F}_p$ or $\mathbf{Z}_p$ are isomorphic if and only if they are strictly isomorphic.

■ (18.5.12) **Theorem** Two one dimensional formal group laws $F(X, Y)$, $G(X, Y)$ over $\mathbf{Z}_p$ are isomorphic if and only if their reductions $\bar{F}(X, Y)$ and $\bar{G}(X, Y)$ over $\mathbf{F}_p$ are isomorphic.

■ (18.5.13) Theorem (18.5.12) does not generalize easily (cf., however, (18.6.4)(f). For example, the obvious analogue of (18.5.12) for higher dimensional finite height formal group laws over $\mathbf{Z}_p$ is false and so is the one dimensional analogue of (18.5.12) over unramified extensions of $\mathbf{Z}_p$. This last fact means that in general the link between the Eisenstein polynomial over $W_{p^\infty}(\mathbf{F}_q)$ of Theorem (18.5.2) of a formal group law $F(X, Y)$ and the characteristic polynomial $\Psi_F(x)$ over $W_{p^\infty}(\mathbf{F}_q)$ of Theorem (18.5.4) is a much more tenuous one.

■ (18.5.14) **Formal moduli** One way to tackle classification problems of one dimensional formal groups over a local ring R is via the idea of liftings or deformations. Let k be the residue field of a complete noetherian local ring R with maximal ideal $\mathfrak{m}$. Let $\Gamma(X, Y)$ be a one dimensional formal group law over k. We say that $F(X, Y)$ over R *lifts* $\Gamma(X, Y)$ if $\bar{F}(X, Y) = \Gamma(X, Y)$. Two lifts are $*$-isomorphic if there exists an isomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $\alpha(X) \equiv X \bmod \mathfrak{m}$. The "moduli" problem is now to classify all lifts modulo $*$-isomorphism. (Note that lifts always exist because the underlying ring of the universal one dimensional formal group law is free polynomial.) It turns out that the set of $*$-isomorphisms classes is naturally identifiable with $\mathfrak{m}^{h-1}$ if $h = \mathrm{ht}(\Gamma(X, Y))$; i.e., there are $h - 1$ formal moduli. One can even give an explicit parameterization; cf. Section 22.4 for more details.

18.6 Formal A-modules

Let A be a ring, $B \in \mathbf{Alg}_A$. Roughly speaking, a formal A-module over B is a formal group law that admits A as a ring of endomorphisms. More precisely:

■(18.6.1) **Definitions and example** A formal A-module over B is a formal group law $F(X, Y)$ over B together with a ring homomorphism ρ_F: $A \to \mathrm{End}_B(F(X, Y))$ such that $J \circ \rho_F$: $A \to B$ is the A-algebra structure homomorphism of $B \in \mathbf{Alg}_A$. We shall often write $[a]_F(X)$ for $\rho_F(a)(X)$. A *homomorphism of formal A-modules* is a homomorphism of formal group laws $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $\rho_G(a)(X) \circ \alpha(X) = \alpha(X) \circ \rho_F(a)(X)$ for all $a \in A$.

Examples of one dimensional formal A-modules are the Lubin–Tate formal group laws of Chapter I, Section 8.

■(18.6.2) **A-height** Let A be a discrete valuation ring with uniformizing element π and finite residue field k. Let $F(X, Y)$ over $B \in \mathbf{Alg}_A$ be a formal A-module of dimension 1, where B is a field (of characteristic $p > 0$). Consider $\rho_F(\pi)(X) = [\pi]_F(X)$. The first nonzero term in the power series $\rho_F(\pi)(X)$ is necessarily of the form aX^{q^h} if $\rho_F(\pi)(X) \neq 0$. Then h is defined to be the A-height of $F(X, Y)$. If A is the ring of integers of a finite extension K of $\mathbf{Q}_p$ of degree n, one has A-height $(F(X, Y)) = n^{-1}\,\mathrm{ht}(F(X, Y))$. If A is of characteristic $p > 0$, the underlying formal group law of $F(X, Y)$ is always isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ and there is no relation between A-height and height.

■(18.6.3) **Universal formal A-modules** As in the case of formal group laws, it is an essentially trivial matter to show that there exists a universal formal A-module over some A-algebra L_A for each dimension n (i.e., the functor $\mathbf{Alg}_A \to \mathbf{Set}$, $B \mapsto$ set of all formal A-modules over B, is representable). To determine the structure of L_A is another matter. If A is a discrete valuation ring or a field, then L_A is a free polynomial algebra over A. But in general L_A may have a more complicated structure, for instance, in the case that A is the ring of integers of a global number field K of class number > 1.

■(18.6.4) **The local case** Now suppose that A is a complete discrete valuation ring with finite residue field k of q elements. (For many of the results below completeness is unnecessary.) In this case, by and large, the theory of formal A-modules is completely parallel to the theory of formal group laws over $\mathbf{Z}_{(p)}$-algebras (i.e., formal $\mathbf{Z}_{(p)}$-modules). Here is a short partial list of some of the corresponding results.

(a) L_A is a free polynomial algebra over A. There exists an analogue of the universal p-typical formal group law $F_V(X, Y)$. This formal A-module will be denoted $(F_V^A(X, Y), \rho_V^A)$. Every formal A-module is isomorphic to one obtained from an $(F_V^A(X, Y), \rho_V^A)$ by specialization. These are called A-typical formal A-modules. There is a universal strict isomorphism of A-typical formal A-modules.

(b) One dimensional formal A-modules over a separably closed field are classified by their A-heights.

(c) The ring of A-endomorphisms of a one dimensional formal A-module c

A-height h over a separably closed field is isomorphic to the ring of integers of the central division algebra of rank h^2 and invariant h^{-1} over K, the quotient field of A.

(d) One dimensional formal A-modules over a finite field are classified by the characteristic polynomials of their Frobenius endomorphism.

(e) If R is a local noetherian complete A-algebra with residue field l and $\Gamma(X, Y)$ is a formal A-module of A-height h over l, then the lifts of $\Gamma(X, Y)$ up to $*$-isomorphism are parametrized by $\mathfrak{m}^{h-1}$.

(f) Two one dimensional formal A-modules over A are isomorphic iff their reductions over k are isomorphic.

■ (18.6.5) **q-typification and the Frobenius operator $\mathbf{f}_\pi$** Here are two more instances of the parallelism between formal A-modules and formal group laws over $\mathbf{Z}_{(p)}$-algebras. They concern the p-typification projector ε_p and the Frobenius operator $\mathbf{f}_p$. Recall that the topological group of curves $\mathscr{C}(F; B)$ of a formal group law $F(X, Y)$ over $\mathbf{Z}_{(p)}$-algebra B admits a projector $\varepsilon_p: \mathscr{C}(F; B) \to \mathscr{C}(F; B)$ and a Frobenius operator $\mathbf{f}_p$. They were defined as follows: formally,

$$\mathbf{f}_p\gamma(t) = \gamma(\zeta_p t^{1/p}) +_F \cdots +_F \gamma(\zeta_p^p t^{1/p}) \tag{18.6.6}$$

where ζ_p is a primitive pth root of unity, and given the $\mathbf{f}_n$ and $\mathbf{V}_n$, the operators ε_p can be defined as (cf. Chapter III (16.3.12))

$$\varepsilon_p = \sum_{(n,p)=1} n^{-1}\mu(n)\mathbf{V}_n\mathbf{f}_n \tag{18.6.7}$$

If B is without additive torsion the operators $\mathbf{f}_p$ and ε_p can be described via the logarithm of $F(X, Y)$ as follows

$$f(\gamma(t)) = \sum_{i=1}^{\infty} x_i t^i \quad \Rightarrow \quad f(\mathbf{f}_p\gamma(t)) = \sum_{i=1}^{\infty} p x_{pi} t^i \tag{18.6.8}$$

$$f(\gamma(t)) = \sum_{i=1}^{\infty} x_i t^i \quad \Rightarrow \quad f(\varepsilon_p\gamma(t)) = \sum_{j=0}^{\infty} x_{pj} t^{pj} \tag{18.6.9}$$

The right analogues of ε_p and $\mathbf{f}_p$ for formal A-modules are a projector ε_q (called q-typification) and a Frobenius operator $\mathbf{f}_\pi$ (where π is a uniformizing element of A, and q is the number of elements of the residue field of A). There do not seem to be obvious analogues of Definitions (18.6.6) and (18.6.7), but there are obvious analogues of (18.6.8) and (18.6.9); viz. if $B \in \mathbf{Alg}_A$, B is A-torsion free, and $F(X, Y)$ is an m-dimensional formal A-module over B, then

$$f(\gamma(t)) = \sum_{i=1}^{\infty} x_i t^i \quad \Rightarrow \quad f(\mathbf{f}_\pi\gamma(t)) = \sum_{i=1}^{\infty} \pi x_{qi} t^i \tag{18.6.10}$$

$$f(\gamma(t)) = \sum_{i=1}^{\infty} x_i t^i \quad \Rightarrow \quad f(\varepsilon_q\gamma(t)) = \sum_{j=0}^{\infty} x_{qj} t^{qj} \tag{18.6.11}$$

Taking these as tentative definitions, the first problem is to prove that this defines elements in $\mathscr{C}(F; B)$; i.e., we must show that the m-tuples of power series

$$f^{-1}\left(\sum_{i=1}^{\infty} \pi x_{qi} t^i\right), \qquad f^{-1}\left(\sum_{j=0}^{\infty} x_{qj} t^{qj}\right)$$

have integral coefficients. Here, again, the functional equation lemma does its work. The universal n-dimensional formal A-module $(F_S^A(X, Y), \rho_S^A)$ lives, fortunately, over a free polynomial A-algebra $A[S]$. Let σ: $K[S] \to K[S]$ be the K-endomorphism that takes all the S's into their qth powers; we are then in a functional equation type situation, enabling us to use (18.6.10), (18.6.11) as definitions in case $F(X, Y) = F_S^A(X, Y)$. And then, by specialization, one defines ε_q and $\mathbf{f}_\pi$ for all formal A-modules.

Even more so than in the case of formal group laws, the technique "do everything first in the universal case" seems to be effective in dealing with formal A-modules.

■ (18.6.12) **Other results** If A is a discrete valuation ring with infinite residue field, every one dimensional formal A-module over a $B \in \mathbf{Alg}_A$ is isomorphic to the additive formal A-module.

However, there does exist an obvious twisted analogue of the universal A-typical formal A-module $(F_V^A(X, Y), \rho_V^A)$ which is definitely nontrivial. We call the resulting objects twisted formal A-modules. Examples are the generalized Lubin–Tate formal group laws obtained by Cartier's semilinear trick in Chapter II, Section 13.2.

These objects are less rigid than formal A-modules and possibly not much more difficult to handle.

■ (18.6.13) **Ramified Witt vectors and Artin–Hasse exponentials** Let A be as in (18.6.4). The p-typical version of $\hat{\mathbf{G}}_m^-(X, Y) = X + Y - XY$ over $\mathbf{Z}_p$ is the formal group law with logarithm

$$X + p^{-1}X^p + p^{-2}X^{p^2} + p^{-3}X^{p^3} + \cdots \tag{18.6.14}$$

Its formal A-module analogue appears to be the one dimensional Lubin–Tate formal group law over A with logarithm

$$X + \pi^{-1}X^q + \pi^{-2}X^{q^2} + \cdots \tag{18.6.15}$$

(Of course the isomorphism class of (18.6.15) depends on π, but choosing a different uniformizing element for p in (18.6.14) also changes the isomorphism class involved.) The analogy between the formal group law $F_p(X, Y)$ with logarithm (18.6.14) and the formal A-module $F_\pi(X, Y)$ with logarithm (18.6.15) goes quite deep. For example, we have seen that $\mathscr{C}_p(F_p; -)$ is a ring-valued functor identifiable with $W_{p^\infty}(-)$, the ring functor of Witt vectors associated to the prime number p. Correspondingly, $\mathscr{C}_q(F_\pi; -)$ has a natural structure of

A-algebra-valued functor, giving us a "ramified Witt vector" functor $W^A_{q,\infty}(-)$, which has as its associated polynomials

$$w^A_{q,n}(Z) = Z_0^{q^n} + \pi Z_1^{q^{n-1}} + \cdots + \pi^{n-1} Z_{n-1}^q + \pi^n Z_n$$

instead of the usual Witt polynomials

$$w_{p^n}(Z) = Z_0^{p^n} + pZ_1^{p^{n-1}} + \cdots + p^n Z_n$$

This ramified Witt vector functor has many of the properties one would expect. For example, $W^A_{q,\infty}(k) = A$, where k is the residue field of A and if l/k is an algebraic extension $W^A_{q,\infty}(l)$ is the completion of the ring of integers of the unramified extension of K covering the residue field extension l/k.

Further, there is a functorial A-algebra endomorphism $\mathbf{f}_\pi$ of $W^A_{q,\infty}$ (corresponding to the $\mathbf{f}_\pi$ of (18.6.5)) which on $W^A_{q,\infty}(l)$ corresponds with the Frobenius substitution ($\mathbf{f}_\pi(x) \equiv x^q \bmod \pi$ for all $x \in W^A_{q,\infty}(l)$).

Also there is an Artin–Hasse exponential mapping; in this case a functorial homomorphism of A-algebras Δ^A: $W^A_{q,\infty}(-) \to W^A_{q,\infty}(W^A_{q,\infty}(-))$.

All these things generalize to the case of arbitrary one dimensional formal A-modules over A and even to the case of twisted one dimensional Lubin–Tate formal A-modules over A (and in this case the residue field of A need no longer be finite).

■ (18.6.16) Getting slightly ahead of the story let us also remark that $F_\pi(X, Y)$ plays the same role vis-à-vis the local class field theory of K that $F_p(X, Y)$ (or $\hat{\mathbf{G}}_m(X, Y)$) plays for $\mathbf{Q}_p$ (cf. Section 32 in Chapter VI) and that $W^A_{q,\infty}(-)$ and its associated formal group law take the place of $W_{p^\infty}(-)$ and its formal completion $\hat{W}_{p^\infty}(-)$ when doing Cartier–Dieudonné theory of formal A-modules rather than of formal group laws. (Cf. Sections 26, 29, 30 of Chapter V.)

■ (18.6.17) **Remarks on the global case** In the case of formal group laws $F_p(X, Y)$ for varying p there exists a global formal group law $\hat{\mathbf{G}}_m^-(X, Y)$ over $\mathbf{Z}$ strictly isomorphic to $F_p(X, Y)$ over $\mathbf{Z}_p$ for all p. Now let A be the ring of integers of a global field K. The analogue of $\hat{\mathbf{G}}_m^-(X, Y)$ in this case is a formal A-module $F(X, Y)$ over A such that for every finite place v, $F(X, Y)$ is strictly isomorphic to a Lubin–Tate formal group law over A_v where A_v is the completion of A with respect to v. Such objects exist by the local global results of Section 20.5.

In the case of $\hat{\mathbf{G}}_m^-(X, Y)$ there is a global ring of Witt vectors $W(-) \simeq \mathscr{C}(\hat{\mathbf{G}}_m^-; -)$, but there does not seem to be a natural multiplication on $\mathscr{C}(F; -)$ if $F(X, Y)$ is a global Lubin–Tate formal group law except when K is of class number 1.

Still, one has exactly as in the case of the Witt vectors additive Artin–Hasse exponentials $A_v \to \mathscr{C}(F; A_v)$ for one fixed formal group law $F(X, Y)$ over A. (In the case of the Witt vectors these maps are also multiplicative, but they are not ring homomorphisms even in that case.)

19 Universal Isomorphisms

19.1 The universal isomorphism $\alpha_{U,S}\colon H_U(X, Y) \to H_{U,S}(X, Y)$

Let $H_U(X, Y)$ be the m-dimensional universal commutative formal group law of Chapter II, Section 11.1. It is defined over $\mathbf{Z}[U] = \mathbf{Z}[U(i, \mathbf{n}) \mid \mathbf{n} \in \mathbf{I}, i = 1, \ldots, m, |\mathbf{n}| \geq 2]$. We recall that

$$(19.1.1)\quad a_{\mathbf{n}}(U) = \sum_{(q_1, \ldots, q_t, \mathbf{d})} d(q_1, \ldots, q_t) U_{q_1} U_{q_2}^{(q_1)} \cdots U_{q_t}^{(q_1 \cdots q_{t-1})} U_{\mathbf{d}}^{(q_1 \cdots q_t)}$$

$$(19.1.2)\quad H_U(X, Y) = h_U^{-1}(h_U(X) + h_U(Y)), \qquad h_U(X) = \sum_{|\mathbf{n}| \geq 1} a_{\mathbf{n}} X^{\mathbf{n}}$$

(For the notations used, we refer to Chapter II, Section 11.1 and (11.2.1).)

Let $\phi\colon \mathbf{Z}[U] \to \mathbf{Z}[U]$ be the ring endomorphism defined by $\phi(U(i, \mathbf{n})) = 0$ if $|\mathbf{n}| \geq 2$, $\mathbf{n} \neq p^r \mathbf{e}(j)$ for all $r \in \mathbf{N}$, prime numbers p, and $j \in \{1, \ldots, m\}$ and by $\phi(U(i, p^r \mathbf{e}(j))) = U(i, p^r \mathbf{e}(j))$ for all $i, j \in \{1, \ldots, m\}$, prime numbers p, and $r \in \mathbf{N}$. Write

$$(19.1.3)\quad \bar{a}_{\mathbf{n}}(U) = \phi(a_{\mathbf{n}}(U)), \qquad \bar{h}_U(X) = \sum_{|\mathbf{n}| \geq 1} \bar{a}_{\mathbf{n}}(U) X^{\mathbf{n}}$$

$$\bar{H}_U(X, Y) = \bar{h}_U^{-1}(\bar{h}_U(X) + \bar{h}_U(Y))$$

■ (19.1.4) **Lemma** For every prime number p, $\bar{h}_U(X)$ satisfies a functional equation of the form

$$(19.1.5)\quad \bar{h}_U(X) = \bar{g}_p(X) + \sum_{i=1}^{\infty} p^{-1} U_{p^i} \bar{h}_U^{(p^i)}(X^{p^i}), \quad \bar{g}_p(X) \in \mathbf{Z}_{(p)}[U][\![X]\!]^m$$

Proof This follows by applying ϕ_* to the corresponding functional equation for $h_U(X)$ (cf. Lemma (11.2.4)) because $\phi(U_{p^i}) = U_{p^i}$.

■ (19.1.6) **Remark** Because $\bar{h}_U(X)$ satisfies the functional equations (19.1.5), it follows that $\bar{H}_U(X, Y)$ is an m-dimensional formal group law over $\mathbf{Z}[U]$, which is also obvious from the observation $\bar{H}_U(X, Y) = \phi_* H_U(X, Y)$. Because $\bar{h}_U(X)$ and $h_U(X)$ satisfy the same type of functional equation, it follows that $H_U(X, Y)$ and $\bar{H}_U(X, Y)$ are strictly isomorphic over $\mathbf{Z}[U]$ (cf. Chapter I, Section 2.2 for the notion "same type").

■ (19.1.7) **Remark** The vectors $\bar{a}_{\mathbf{n}}(U)$ are obtained from the $a_{\mathbf{n}}(U)$ by setting all $U(i, \mathbf{d})$ with $\mathbf{d} \neq p^r \mathbf{e}(j)$ equal to zero, or, equivalently $\bar{a}_{\mathbf{n}}(U)$ is given by a sum (19.1.1) where now the sum is over all sequences $(q_1, \ldots, q_t, \mathbf{d})$ with $|\mathbf{d}| = 1$. This means in particular that $\bar{a}_{\mathbf{n}}(U) = 0$ unless $\mathbf{n}$ is of the form $\mathbf{n} = n\mathbf{e}(j)$ for some $n \in \mathbf{N}$ and $j \in \{1, 2, \ldots, m\}$ (so that $\bar{H}_U(X, Y)$ is a curvilinear formal group law). Now for each $n \in \mathbf{N}$ we write $\bar{A}_n(U)$ for the matrix consisting of the columns

$$\bar{a}_{n\mathbf{e}(1)}(U), \qquad \ldots, \qquad \bar{a}_{n\mathbf{e}(m)}(U)$$

Then by the remarks made above and (19.1.1), (19.1.3) we have

$$(19.1.8)\quad \bar{h}_U(X) = \sum_{n=1}^{\infty} \bar{A}_n(U)X^n$$

$$(19.1.9)\quad \bar{A}_n(U) = \sum_{(q_1,\ldots,q_t)} d(q_1, \ldots, q_t)U_{q_1}U_{q_2}^{(q_1)} \cdots U_{q_t}^{(q_1 \cdots q_{t-1})}, \quad \bar{A}_1 = I_m$$

where, as usual, X^n is short for the column vector $(X_1^n, X_2^n, \ldots, X_m^n)$ and where the sum in (19.1.9) is over all sequences of powers of prime numbers $(q_1, \ldots, q_t)$, $q_i = p_i^{r_i}$, $r_i \in \mathbf{N}$, such that $q_1 \cdots q_t = n$.

■ (19.1.10) **Constructions** Now for each $i \in \{1, \ldots, m\}$ and $\mathbf{n} \in \mathbf{I}$, $|\mathbf{n}| \geq 2$ let $S(i, \mathbf{n})$ be another indeterminate and let $S_{\mathbf{n}}$ be short for the column vector $(S(1, \mathbf{n}), \ldots, S(m, \mathbf{n}))$. We also define $S_{\mathbf{e}(j)}$, $j = 1, \ldots, m$ as the column vector $(0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the jth spot. We now define for all $\mathbf{n} \in \mathbf{I}$, a column vector $a_{\mathbf{n}}(U, S)$ by the formula

$$(19.1.11)\quad a_{\mathbf{n}}(U, S) = \sum_{i|\mathbf{n}} \bar{A}_i(U)S_{i^{-1}\mathbf{n}}$$

where $i \in \mathbf{N}$ divides the multi-index $\mathbf{n}$ if $\mathbf{n} = (n_1, \ldots, n_m) = (ir_1, \ldots, ir_m)$ $r_j \in \mathbf{N} \cup \{0\}$, $j = 1, \ldots, m$ and then $i^{-1}\mathbf{n} = (r_1, \ldots, r_m)$. Finally, we set

$$(19.1.12)\quad h_{U,S}(X) = \sum_{|\mathbf{n}| \geq 1} a_{\mathbf{n}}(U, S)X^{\mathbf{n}}$$

$$(19.1.13)\quad H_{U,S}(X) = h_{U,S}^{-1}(h_{U,S}(X) + h_{U,S}(Y))$$

$$(19.1.14)\quad \alpha_{U,S}(X) = h_{U,S}^{-1}(h_U(X))$$

■ (19.1.15) **Lemma** For each prime number p we have

$$(19.1.16)\quad h_{U,S}(X) - \sum_{i=1}^{\infty} p^{-1}U_{p^i}h_{U,S}^{(p^i)}(X^{p^i}) \in \mathbf{Z}_{(p)}[U; S][\![X]\!]$$

Proof Let $\mathbf{n} \in \mathbf{I}$ and let p be a prime number and suppose p^r is the highest power of p that divides $\mathbf{n}$. To prove (19.1.16) we must show that

$$a_{\mathbf{n}}(U, S) - \sum_{i=1}^{r} p^{-1}U_{p^i}a_{p^{-i}\mathbf{n}}(U^{p^i}; S^{p^i}) \in \mathbf{Z}_{(p)}[U, S]$$

This is immediate from (19.1.11) and Lemma (19.1.4) because (19.1.5) combined with (19.1.8) says that if $p^k \mid n$ but $p^{k+1} \nmid n$, then

$$\bar{A}_n - \sum_{i=1}^{k} p^{-1}U_{p^i}\bar{A}_{p^{-i}n} \in \mathbf{Z}_{(p)}[U]$$

■ (19.1.17) **Corollary** The power series $H_{U,S}(X, Y)$ and $\alpha_{U,S}(X)$ have their coefficients in $\mathbf{Z}[U, S]$ so that $H_{U,S}(X, Y)$ is an m-dimensional formal group law over $\mathbf{Z}[U, S]$ that is strictly isomorphic over $\mathbf{Z}[U; S]$ to the formal group law $H_U(X, Y)$ over $\mathbf{Z}[U] \subset \mathbf{Z}[U; S]$. The strict isomorphism is $\alpha_{U,S}(X)$.

■ (19.1.18) **Proposition** $\alpha_{U,S}(X)$: $H_U(X, Y) \to H_{U,S}(X, Y)$ is a universal isomorphism of m-dimensional formal group laws. That is, if $(F(X, Y))$, $\alpha(X)$, $G(X, Y))$ form a triple over a ring A consisting of two m-dimensional formal group laws over A and a strict isomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over A, then there exists a unique homomorphism ϕ: $\mathbf{Z}[U, S] \to A$ such that $F(X, Y) = \phi_*(H_U(X, Y))$, $\alpha(X) = \phi_*(\alpha_{U,S}(X))$, $G(X, Y) = \phi_*(H_{U,S}(X, Y))$.

Proof For each $n \in \mathbf{N}$, $n \geq 2$ let $h_{U,S(n)}(X)$ and $\alpha_{U,S(n)}(X)$ be the m-tuples of power series obtained from $h_{U,S}(X)$ and $\alpha_{U,S}(X)$ by setting $S(i, \mathbf{n}) = 0$ for all $\mathbf{n} \in \mathbf{I}$ with $|\mathbf{n}| \geq n$.

Immediately from the definition of $h_{U,S}(X)$ we then have that

$$h_{U,S}(X) \equiv h_{U,S(n)}(X) + \sum_{|\mathbf{n}|=n} S_{\mathbf{n}} X^{\mathbf{n}} \quad \text{mod(degree } n+1) \tag{19.1.19}$$

$$h_{U,S}(X) \equiv h_{U,S(n)}(X) \quad \text{mod(degree } n)$$

It follows that

$$\alpha_{U,S}(X) \equiv \alpha_{U,S(n)}(X) - \sum_{|\mathbf{n}|=n} S_{\mathbf{n}} X^{\mathbf{n}} \quad \text{mod(degree } n+1) \tag{19.1.20}$$

$$\alpha_{U,S}(X) \equiv \alpha_{U,S(n)}(X) \quad \text{mod(degree } n)$$

Now let $(F(X, Y), \alpha(X), G(X, Y))$ be a triple consisting of two formal group laws and strict isomorphism over A. Because $H_U(X, Y)$ is universal, there is a unique homomorphism $\bar{\phi}$: $\mathbf{Z}[U] \to A$ such that $\bar{\phi}_*(H_U(X, Y)) = F(X, Y)$. This determines ϕ: $\mathbf{Z}[U, S] \to A$ on the U's. Given the $\phi(U(i, \mathbf{n}))$ for all i and $\mathbf{n}$, it follows from (19.1.20) (and $\alpha_{U,S}(X) \equiv \alpha(X) \equiv X$ mod(degree 2)) that there are unique $\phi(S(i, \mathbf{n})) \in A$ such that $\phi_*(\alpha_{U,S}(X)) = \alpha(X)$. It follows that also $\phi_*(H_{U,S}(X, Y)) = G(X, Y)$ because

$$\begin{aligned}
\phi_* H_{U,S}(X, Y) &= \phi_*(\alpha_{U,S}(H_U(\alpha_{U,S}^{-1}(X), \alpha_{U,S}^{-1}(Y)))) \\
&= \phi_*(\alpha_{U,S})(\phi_* H_U(\phi_*(\alpha_{U,S})^{-1}(X), \phi_*(\alpha_{U,S})^{-1}(Y))) \\
&= \alpha(F(\alpha^{-1}(X), \alpha^{-1}(Y))) = G(X, Y)
\end{aligned}$$

■ (19.1.21) **Remark** It is quite easy to find universal strict isomorphisms $\hat{\alpha}(X)$: $H_U(X) \to ?$. For example, if $S_{\mathbf{n}}$ is the column vector consisting of the $S(i, \mathbf{n})$, then $\hat{\alpha}(X) = \sum_{\mathbf{n}} S_{\mathbf{n}} X^{\mathbf{n}}$ is a universal isomorphism $H_U(X, Y) \to \hat{\alpha}(H_U(\hat{\alpha}^{-1}(X), \hat{\alpha}^{-1}(Y)))$. The isomorphism of (19.1.18) is mainly useful because it "p-typifies" in the right way and because the receiving formal group law's logarithm is reasonably easy to express in terms of the logarithm $h_U(X)$; cf. 19.2, and also 34.1.

19.2 The universal isomorphism $\alpha_{V,T}(X)$: $F_V(X, Y) \to F_{V,T}(X, Y)$ between p-typical formal group laws

Fix a prime number p. Let $F_{V,T}(X, Y)$ over $\mathbf{Z}[V, T]$ and $F_V(X, Y)$ over $\mathbf{Z}[V]$ be the m-dimensional formal group laws constructed in Chapter II, 10.3 (the

one dimensional case was also treated in Chapter I, 2.3 and 3.3). We quickly recall a number of formulas and facts:

$$f_V(X) = X + \sum_{i=1}^{\infty} p^{-1} V_i f_V^{(p^i)}(X^{p^i}) \tag{19.2.1}$$

$$F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y))$$

$$f_{V,T}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i} + \sum_{i=1}^{\infty} p^{-1} V_i f_{V,T}^{(p^i)}(X^{p^i}) \tag{19.2.2}$$

$$F_{V,T}(X, Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y))$$

Explicit formulas for the coefficients of $f_V(X)$ and $f_{V,T}(X)$ are

$$f_V(X) = \sum_{i=0}^{\infty} a_i(V) X^{p^i} \tag{19.2.3}$$

$$a_m(V) = \sum_{i_1 + \cdots + i_r = m} p^{-r} V_{i_1} V_{i_2}^{(p^{i_1})} \cdots V_{i_r}^{(p^{i_1 + \cdots + i_{r-1}})}$$

$$f_{V,T}(X) = \sum_{i=0}^{\infty} a_i(V, T) X^{p^i}$$

$$a_0(V) = a_0(V, T) = I_m$$

$$a_m(V, T) = a_m(V) + a_{m-1}(V) T_1^{(p^{m-1})} + \cdots + a_1(V) T_{m-1}^{(p)} + T_m$$

Recall that the V_j and T_j are $m \times m$ matrices of indeterminates and that $T_j^{(p^r)}$ is the matrix obtained from T_j by raising each of its entries to the p^rth power. All these formulas can be found in Chapter II, 10.3 and 10.4.

■ (19.2.4) We now define a homomorphism $\rho\colon \mathbf{Z}[U; S] \to \mathbf{Z}[V; T]$ and a homomorphism $\iota\colon \mathbf{Z}[V; T] \to \mathbf{Z}[U; S]$ as follows:

(i) $\rho(U(i, \mathbf{n})) = 0 = \rho(S(i, \mathbf{n}))$ for all $i \in \{1, 2, \ldots, m\}$ and all $\mathbf{n} \in \mathbf{I}$, $|\mathbf{n}| \geq 2$, that are not of the form $\mathbf{n} = p^r \mathbf{e}(j)$ for some $r \in \mathbf{N}$ and $j \in \{1, 2, \ldots, m\}$. (Here p is the fixed prime number chosen above.)

(ii) $\rho(U(i, p^r \mathbf{e}(j))) = V_r(i, j)$, $\rho(S(i, p^r \mathbf{e}(j))) = T_r(i, j)$, $i, j \in \{1, 2, \ldots, m\}$, $r \in \mathbf{N}$.

(iii) $\iota(V_r(i, j)) = U(i, p^r \mathbf{e}(j))$, $\iota(T_r(i, j)) = S(i, p^r \mathbf{e}(j))$.

■ (19.2.5) **Lemma** If ρ and ι are the homomorphisms defined in (19.2.4), then we have $\rho\iota = id$ and $\rho_* H_{U,S}(X, Y) = F_{V,T}(X, Y)$, $\rho_* H_U(X, Y) = F_V(X, Y)$.

Proof The first statement of the lemma is obvious and the third and second statements follow from the (defining) formulas for $H_U(X, Y)$ (via $h_U(X)$) and $H_{U,S}(X, Y)$ (via $h_{U,S}(X, Y)$) as compared to the corresponding formulas for $F_V(X, Y)$ and $F_{V,T}(X, Y)$; cf. respectively formulas (19.1.1), (19.2.3) and (19.1.8), (19.1.11), (19.2.3). This proves the lemma. Note that $\rho_* H_U(X, Y) = F_V(X, Y)$ has been proved and used before in Chapter III, (16.4.2).

Let $\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X))$. We have proved in Chapter II, Theorem (10.3.5) that $\alpha_{V,T}(X)$ is a strict isomorphism (over $\mathbf{Z}[V, T]$) $F_V(X, Y) \to F_{V,T}(X, Y)$. We also know by Proposition (15.2.4) of Chapter II that $F_V(X, Y)$ and $F_{V,T}(X, Y)$ are p-typical formal group laws.

■ (19.2.6) **Theorem** The triple $(F_V(X, Y), \alpha_{V,T}(X), F_{V,T}(X, Y))$ is universal for triples over $\mathbf{Z}_{(p)}$-algebras or characteristic zero rings $(F(X, Y), \alpha(X), G(X, Y))$ consisting of two p-typical (m-dimensional) formal group laws $F(X, Y)$ and $G(X, Y)$ and a strict isomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$.

That is, if $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over a ring A, which is a characteristic zero ring or a $\mathbf{Z}_{(p)}$-algebra, is a strict isomorphism between p-typical formal group laws, then there is a unique homomorphism ϕ: $\mathbf{Z}[V; T] \to A$ such that $\phi_* F_V(X, Y) = F(X, Y)$, $\phi_* \alpha_{V,T}(X) = \alpha(X)$, $\phi_* F_{V,T}(X, Y) = G(X, Y)$.

Proof By Theorem (19.1.18) there is a unique homomorphism $\tilde{\phi}$: $\mathbf{Z}[U; S] \to A$ such that $\tilde{\phi}_* H_U(X, Y) = F(X, Y)$, $\tilde{\phi}_* \alpha_{U,S}(X) = \alpha(X)$, $\tilde{\phi}_* H_{U,S}(X, Y) = G(X, Y)$. We are going to prove that $\tilde{\phi}(U(i, \mathbf{n})) = 0 = \tilde{\phi}(S(i, \mathbf{n}))$ for all $i \in \{1, 2, \ldots, m\}$ and $\mathbf{n} \in \mathbf{I}$, $|\mathbf{n}| \geq 2$, that are not of the form $p^r \mathbf{e}(j)$, $r \in \mathbf{N}$, $j \in \{1, 2, \ldots, m\}$. That $\tilde{\phi}(U(i, \mathbf{n})) = 0$ for all such $\mathbf{n}$ follows from the p-typical universality of $F_V(X, Y)$ (otherwise there would be two different homomorphisms $\mathbf{Z}[U] \to A$ taking $H_U(X, Y)$ into $F(X, Y)$, namely $\tilde{\phi}$ and ρ composed with the homomorphism $\mathbf{Z}[V] \to A$ taking $F_V(X, Y)$ into $F(X, Y)$, which latter exists because $F(X, Y)$ is p-typical). It therefore remains to prove that $\tilde{\phi}(S(i, \mathbf{n})) = 0$ for all $\mathbf{n}$, $|\mathbf{n}| \geq 2$, not of the form $p^r \mathbf{e}(j)$. We use again the lexicographic ordening on $\mathbf{I}$ (cf. Chapter III, 16.4). Let $\mathbf{d}$ be the smallest multi-index not of the form $p^r \mathbf{e}(j)$ for which there is an $i \in \{1, 2, \ldots, m\}$ such that $\tilde{\phi}(S(i, \mathbf{n})) \neq 0$. We can then find $r_1, \ldots, r_m \in \mathbf{N}$ such that

(19.2.7) $\qquad \hat{d} = d_1 p^{r_1} + \cdots + d_m p^{r_m}$ is not a power of p

(19.2.8) If $\mathbf{d} <_l \mathbf{e}$, then $d_1 p^{r_1} + \cdots + d_m p^{r_m} < e_1 p^{r_1} + \cdots + e_m p^{r_m}$.

(Cf. Chapter III, Section 16.4, where the same trick was used.) As in Section 16.4 we now first do a universal calculation. Let $H_{U,S(\mathbf{d})}(X, Y)$ be the formal group law obtained from $H_{U,S}(X, Y)$ by setting equal to zero all $U(i, \mathbf{n})$ with $|\mathbf{n}| \geq 2$ and $v(\mathbf{n}) \neq p$ and all $S(i, \mathbf{n})$ with $|\mathbf{n}| \geq 2$, $v(\mathbf{n}) \neq p$, $\mathbf{n} <_l \mathbf{d}$. Let q be a prime number $\neq p$ which divides $\hat{d}$ (cf. (19.2.7)). We claim that then in $\mathscr{C}(H_{U,S(\mathbf{d})}, \mathbf{Z}[U, S])$

(19.2.9) $\qquad \mathbf{f}_q \gamma(t) \equiv q S_{\mathbf{d}} t^{\hat{d}/q} \mod(\text{degree } 1 + q^{-1}\hat{d})$

where $\gamma(t)$ is the curve

(19.2.10) $\qquad \gamma(t) = (t^{p^{r_1}}, \ldots, t^{p^{r_m}})$

This follows from the fact that (cf. (19.1.11))

(19.2.11) $\qquad a_{\mathbf{n}}(U, S) \equiv 0 \quad$ if $\quad \mathbf{n} <_l \mathbf{d}$, $v(\mathbf{n}) \neq p$

$\qquad\qquad a_{\mathbf{d}}(U, S) \equiv S_{\mathbf{d}}$

where all the congruences are $\bmod(U(i, \mathbf{k}),\ S(j, \mathbf{l}) \mid v(\mathbf{k}) \neq p,\ v(\mathbf{l}) \neq p,\ |\mathbf{k}|, |\mathbf{l}| \geq 2, \mathbf{l} <_l \mathbf{d})$. Indeed from (19.2.11) it follows that $h_{U,S(\mathbf{n})}(\gamma(t))$ is of the form

$$h_{U,S(\mathbf{d})}(\gamma(t)) \equiv \sum b_i t^{p^i} + S_{\mathbf{d}} t^{\hat{d}} \quad \bmod(\text{degree } \hat{d} + 1)$$

and (19.2.9) is immediate from this.

Now $\tilde{\phi}_* H_{U,S}(X, Y) = G(X, Y)$ is p-typical. Hence $\mathbf{f}_q \gamma(t) = 0$ in $\mathscr{C}(G; A)$. It follows that $q\tilde{\phi}(S(i, \mathbf{d})) = 0$ so that $\tilde{\phi}(S(i, \mathbf{d})) = 0$ because A is a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring. This is a contradiction, proving that indeed $\tilde{\phi}(S(i, \mathbf{n})) = 0$ for all $\mathbf{n}$ with $|\mathbf{n}| \geq 2$, $v(\mathbf{n}) \neq p$. Thus $\tilde{\phi}$ factors through ρ: $\mathbf{Z}[U; S] \to \mathbf{Z}[V, T]$ to give us a homomorphism ϕ: $\mathbf{Z}[V, T] \to A$ such that $\phi_* F_V(X, Y) = F(X, Y)$, $\phi_* \alpha_{V,T}(X, Y) = \alpha(X)$, $\phi_* F_{V,T}(X, Y) = G(X, Y)$ (by Lemma (19.2.5)). Uniqueness of ϕ is easy to prove. Indeed if ϕ': $\mathbf{Z}[V, T] \to A$ were a second homomorphism taking the universal triple to the given triple over A, then $\phi\rho$ and $\phi'\rho$ are two homomorphisms taking the triple $(H_U(X, Y), \alpha_{U,S}(X), H_{U,S}(X, Y))$ into the given triple over A. By Theorem (19.1.18) this means $\phi\rho = \phi'\rho$ and hence $\phi = \phi'$ because ρ is surjective. Q.E.D.

■ (19.2.12) **Remark** The hypothesis "A is a characteristic zero ring or a $\mathbf{Z}_p$-algebra" cannot be omitted from Theorem (19.2.6). Indeed, let q be any prime number different from p. Then $X + X^q$: $\hat{\mathbf{G}}_a(X, Y) \to \hat{\mathbf{G}}_a(X, Y)$ is a strict isomorphism between p-typical formal groups over any ring A of characteristic q; but, as is easily checked (especially if $q < p$), there is no homomorphism ϕ: $\mathbf{Z}[V, T] \to A$ such that $\phi_* F_V(X, Y) = \hat{\mathbf{G}}_a(X, Y)$ and $\phi_* \alpha_{V,T}(X) = X + X^q$. (The counterexample (16.4.16) of Chapter III uses essentially the same idea.)

19.3 On the isomorphism $\alpha_{V,T}(X)$: the $\bar{V}_n$ formulas

$F_{V,T}(X, Y)$ is an m-dimensional p-typical formal group law over $\mathbf{Z}[V; T]$. By the universality of the p-typical formal group law $F_V(X, Y)$ this means that there is a unique homomorphism

(19.3.1) $\qquad \eta_R$: $\mathbf{Z}[V] \to \mathbf{Z}[V; T]$, $\qquad (\eta_R)_* F_V(X, Y) = F_{V,T}(X, Y)$

(The notation η_R comes from algebraic topology where the same homomorphism turns up as the right unit homomorphism η_R: $BP(pt) \to BP_*(BP)$ of the Hopf algebra $BP_*(BP)$ of all Brown–Peterson homology operations; cf. Chapter VI, Section 34.5 for more details.)

We shall write $\bar{V}_n$ for the image $\eta_R(V_n)$; the $\bar{V}_n$ are then polynomials in $V_1, \ldots, V_n; T_1, \ldots, T_n$ with coefficients in $\mathbf{Z}$. The first two are

$$\bar{V}_1 = V_1 + pT_1$$

$$\bar{V}_2 = V_2 + pT_2 + V_1 T_1^p + p^{-1}\{(V_1 + pT_1)(V_1 + pT_1)^p - V_1 V_1^p\}$$

and $\bar{V}_3$ is already almost impossible to write down explicitly (even modulo p).

We recall from Chapter II, 10.4 that

(19.3.2) $\qquad pa_n(V) = a_{n-1}(V)V_1^{(p^{n-1})} + \cdots + a_1(V)V_{n-1}^{(p)} + V_n$

(19.3.3) $\quad a_n(V; T) = a_n(V) + a_{n-1}(V)T_1^{(p^{n-1})} + \cdots + a_1(V)T_{n-1}^{(p)} + T_n$

This means that the $\bar{V}_n$ satisfy (and are characterized by)

$$(19.3.4)\qquad pa_n(V;\,T) = a_{n-1}(V;\,T)\bar{V}_1^{(p^{n-1})} + \cdots + a_1(V;\,T)\bar{V}_{n-1}^{(p)} + \bar{V}_n$$

where $\bar{V}_i^{(p^r)}$ is the matrix obtained from $\bar{V}_i$ by raising each of its entries to the p^rth power; we have chosen a different kind of bracket to denote this so as not to have to use $\bar{V}_i^{(p^r)}$ which could be taken to denote the result of applying the endomorphism

$$\sigma\colon \mathbf{Z}[V,\,T] \to \mathbf{Z}[V,\,T], \qquad V_j \mapsto V_j^p, \qquad T_j \mapsto T_j^p$$

r times to the entries of $\bar{V}_r$.

■ (19.3.5) **Proposition**

$$pa_n(V,\,T) = pT_n + \sum_{i=1}^{n} a_{n-i}(V,\,T)V_i^{(p^{n-i})} + \sum_{k=2}^{n}\sum_{i+j=k} a_{n-k}(V)[V_i^{(p^{n-k})}T_j^{(p^{n-j})} - T_j^{(p^{n-k})}V_i^{(p^{n-i})}]$$

Proof Using formulas (19.3.2)–(19.3.4) we have

$$\begin{aligned} pa_n(V,\,T) &= pa_n(V) + \sum_{i=1}^{n-1} pa_{n-i}(V)T_i^{(p^{n-i})} + pT_n \\ &= pT_n + V_n + \sum_{i=1}^{n-1} a_{n-i}(V)V_i^{(p^{n-i})} \\ &\quad + \sum_{i=1}^{n-1}\sum_{j=1}^{n-i} a_{n-i-j}(V)V_j^{(p^{n-i-j})}T_i^{(p^{n-i})} \\ &= pT_n + V_n + \sum_{i=1}^{n-1} a_{n-i}(V,\,T)V_i^{(p^{n-i})} \\ &\quad - \sum_{i=1}^{n-1}\sum_{j=1}^{n-i} a_{n-i-j}(V)T_j^{(p^{n-i-j})}V_i^{(p^{n-i})} \\ &\quad + \sum_{i=1}^{n-1}\sum_{j=1}^{n-i} a_{n-i-j}(V)V_j^{(p^{n-i-j})}T_i^{(p^{n-i})} \\ &= pT_n + \sum_{i=1}^{n} a_{n-i}(V,\,T)V_i^{(p^{n-i})} \\ &\quad + \sum_{i=1}^{n-1}\sum_{j=1}^{n-i} a_{n-i-j}(V)[V_i^{(p^{n-i-j})}T_j^{(p^{n-j})} - T_j^{(p^{n-i-j})}V_i^{(p^{n-i})}] \end{aligned}$$

which proves the proposition. (To go from the next but last line to the last line in the derivation above, first interchange summation over i and summation

over j in the last double sum in the next but last line and then write i for j and j for i.)

■ (19.3.6) **Corollary**

$$\bar{V}_n - V_n = pT_n + \sum_{i=1}^{n-1} a_{n-i}(V, T)(V_i^{(p^{n-i})} - \bar{V}_i^{(p^{n-i})}) + \sum_{k=2}^{n} \sum_{\substack{i+j=k \\ i,j\geq 1}} a_{n-k}(V)[V_i^{(p^{n-k})}T_j^{(p^{n-j})} - T_j^{(p^{n-k})}V_i^{(p^{n-i})}]$$

Proof This follows immediately from Proposition (19.3.5) by the use of (19.3.4) (and $a_0(V, T) = 1$).

■ (19.3.7) **Theorem**

$$\bar{V}_n = V_n + pT_n + \sum_{\substack{i+j=n \\ i,j\geq 1}} (V_i T_j^{(p^i)} - T_j \bar{V}_i^{(p^i)}) + \sum_{k=1}^{n-1} a_{n-k}(V)(V_k^{(p^{n-k})} - \bar{V}_k^{(p^{n-k})}) + \sum_{k=2}^{n-1} a_{n-k}(V) \left[\sum_{\substack{i+j=k \\ i,j\geq 1}} (V_i^{(p^{n-k})}T_j^{(p^{n-j})} - T_j^{(p^{n-k})}\bar{V}_i^{(p^{n-i})}) \right]$$

Proof Using Proposition (19.3.5) and replacing the $a_{n-i}(V, T)$ in that formula by

$$\sum_{j=1}^{n-i} a_{n-i-j}(V)T_j^{(p^{n-i-j})} + a_{n-i}(V) = a_{n-i}(V, T) \tag{19.3.8}$$

and using (19.3.4), we obtain

(19.3.9)

$$\begin{aligned}\bar{V}_n + \sum_{i=1}^{n-1} a_{n-i}(V, T)\bar{V}_i^{(p^{n-i})} &= pT_n + V_n + \sum_{i=1}^{n-1}\sum_{j=1}^{n-i} a_{n-i-j}(V)T_j^{(p^{n-i-j})}V_i^{(p^{n-i})} \\ &\quad + \sum_{i=1}^{n-1} a_{n-i}(V)V_i^{(p^{n-i})} \\ &\quad + \sum_{k=2}^{n} \sum_{\substack{i+j=k \\ i,j\geq 1}} a_{n-k}(V)[V_i^{(p^{n-k})}T_j^{(p^{n-j})} - T_j^{(p^{n-k})}V_i^{(p^{n-i})}] \\ &= pT_n + V_n + \sum_{i=1}^{n-1} a_{n-i}(V)V_i^{(p^{n-i})} \\ &\quad + \sum_{k=2}^{n} \sum_{\substack{i+j=k \\ i,j\geq 1}} a_{n-k}(V)V_i^{(p^{n-k})}T_j^{(p^{n-j})}\end{aligned}$$

Now use (19.3.8) again to get rid of the $a_{n-i}(V, T)$ in the left-hand side of (19.3.9). The result is the formula of Theorem (19.3.7).

■ (19.3.10) **Remark** Theorem (19.3.7) can be used to give a proof that the $\bar{V}_n$ are in fact polynomials with integral coefficients in $V_1, \ldots, V_n; T_1, \ldots, T_n$; cf. [172].

In spite of its somewhat forbidding appearance we shall find the formula of Theorem (19.3.7) most useful on a number of occasions, notably when discussing formal moduli in 22.4 and or when we are studying BP-cohomology operations in Chapter VI, Section 34.5. (Cf. also 20.2 where Corollary (19.3.6) is used to calculate certain endomorphism rings of formal group laws over finite fields.) As a fairly weak first illustration of the uses of Theorem (19.3.7) we use it in 19.4 to classify one dimensional formal group laws over a separably closed field of characteristic $p > 0$.

19.4 Classification of one dimensional formal group laws over a separably closed field

Let k be a separably closed field and $F(X, Y)$ a one dimensional formal group law over k. If k is of characteristic zero, then k is a $\mathbf{Q}$-algebra and $F(X, Y)$ is strictly isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ so there is nothing left to classify. The situation changes drastically if $\mathrm{char}(k) = p > 0$. In that case we have already constructed a formal group law $\bar{F}_{\Delta_h}(X, Y)$ of height h over $\mathbf{F}_p \subset k$ for each $h \in \mathbf{N}$, and Corollary (3.2.10) of Chapter I says that these formal group laws are definitely pairwise nonisomorphic. The classification theorem now says:

■ (19.4.1) **Theorem** Let k be a separably closed field of characteristic $p > 0$. Then the one dimensional formal group laws over k are classified by their heights.

So, if $F(X, Y)$ is a one dimensional formal group law over k of height h and $h < \infty$, then $F(X, Y)$ is isomorphic to $\bar{F}_{\Delta_h}(X, Y)$ over k and if $h = \infty$, $F(X, Y)$ is isomorphic to $\hat{\mathbf{G}}_a(X, Y)$.

■ (19.4.2) **Start of the proof of Theorem (19.4.1)** If $F(X, Y)$ is of infinite height, then $[p]_F = 0$, and hence Corollary (5.7.6) of Chapter I says that $F(X, Y)$ is (strictly) isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ over k. We have already seen (Chapter I, Corollary (3.2.10)) that the $\bar{F}_{\Delta_h}(X, Y)$ are pairwise nonisomorphic. The same argument shows that $\bar{F}_{\Delta_h}(X, Y)$ is not isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ for all $h \neq \infty$. It therefore remains to show that $F(X, Y)$ is isomorphic to $\bar{F}_{\Delta_h}(X, Y)$ over k if $F(X, Y)$ is of height $h < \infty$. To do this we use two congruence formulas for the $\bar{V}_n$ (in the one dimensional case).

■ (19.4.3) **Lemma** Fix $h \in \mathbf{N}$. Then we have for all $n \in \mathbf{N}$,

$$\bar{V}_n \equiv V_n \mod(V_1, \ldots, V_{n-1}, p) \tag{19.4.4}$$

(19.4.5) $$\bar{V}_{n+h} \equiv V_{n+h} - T_n V_h^{p^n} + V_h T_n^{p^h} \quad \mathrm{mod}(V_1, \ldots, V_{h-1}, V_{h+1}, \ldots, V_{n+h-1}, T_1, \ldots, T_{n-1}, p)$$

■ (19.4.6) **Remark** Once we have identified $V_n \to \bar{V}_n$ with η_R: $BP_*(pt) \to BP_*(BP)$, formula (19.4.5) will give us immediately some results on BP-cohomology operations related to the so-called Budweiser lemma; cf. Chapter VI, 34.5.

Proof To prove the first formula we work in $\mathbf{Q}[V; T]$. First, we have that (cf. (19.2.3))

$$a_i(V) \equiv 0 \quad \mathrm{mod}(V_1, \ldots, V_{n-1}) \quad \text{if} \quad i < n$$
$$a_n(V) \equiv p^{-1} V_n \quad \mathrm{mod}(V_1, \ldots, V_{n-1})$$

Using (19.3.3) this gives that

(19.4.7) $$a_i(V, T) \equiv T_i \quad \mathrm{mod}(V_1, \ldots, V_{n-1}) \quad \text{if} \quad i < n$$
$$a_n(V, T) \equiv T_n + p^{-1} V_n \quad \mathrm{mod}(V_1, \ldots, V_{n-1})$$

Now use (19.3.4) to obtain (19.4.4) from (19.4.7).

To prove (19.4.5) we use Theorem (19.3.7) in the one dimensional case. In that case all upper brackets disappear and we have

(19.4.8) $$\bar{V}_n = V_n + pT_n + \sum_{\substack{i+j=n \\ i,j \geq 1}} (V_i T_j^{p^i} - T_j \bar{V}_i^{p^j}) + \sum_{k=1}^{n-1} a_{n-k}(V)(V_k^{p^{n-k}} - \bar{V}_k^{p^{n-k}}) + \sum_{k=1}^{n-1} a_{n-k}(V) \left[\sum_{\substack{i+j=k \\ i,j \geq 1}} (V_i^{p^{n-k}} T_j^{p^{n-j}} - T_j^{p^{n-k}} \bar{V}_i^{p^{n-i}}) \right]$$

We proceed by induction on n, $n = 0, 1, 2, \ldots$. The induction hypothesis then gives

(19.4.9) if $i < n + h$, $\bar{V}_i \equiv V_i$
$$\mathrm{mod}(V_1, \ldots, V_{h-1}, V_{h+1}, \ldots, V_{n+h-1}, T_1, \ldots, T_{n-1}, p)$$

(Note that this also holds for $n = 1$, because of (19.4.4).) Let $\mathfrak{a}$ be the ideal $(V_1, \ldots, V_{h-1}, V_{h+1}, \ldots, V_{n+h-1}, T_1, \ldots, T_{n-1})$ (in $\mathbf{Z}[V; T]$). We now deal with the various terms of (19.4.8) separately.

(a) The terms $V_i T_j^{p^i}$, $i, j \geq 1$, $i + j = n + h$. These are zero mod $\mathfrak{a}$ unless $i = h$ and (hence) $j = n$, which gives a term $V_h T_n^{p^h}$.

(b) The terms $T_j \bar{V}_i^{p^j}$, $i, j \geq 1$, $i + j = n$. These are zero mod$(\mathfrak{a}, p)$ unless $j = h$ and $i = n$, which gives a term $-T_n V_h^{p^n}$ (use (19.4.9)).

Let $\bar{\mathfrak{a}}$ be the ideal $\mathfrak{a}\mathbf{Q}[V, T] \subset \mathbf{Q}[V, T]$. We shall use the notation $b(V, T) \equiv 0$ mod$(\bar{\mathfrak{a}}, p)$ to mean that $b(V, T) \in \bar{\mathfrak{a}} + p\mathbf{Z}[V, T]$.

(c) The terms $a_{n-k}(V)(V_k^{p^{n-k}} - \bar{V}_k^{p^{n-k}})$, $k = 1, \ldots, n-1$. By the induction hypothesis (19.4.9) we have that $V_k \equiv \bar{V}_k \bmod(\mathfrak{A}, p)$ for these k. Hence $V_k^{p^{n-k}} \equiv \bar{V}_k^{p^{n-k}} \bmod(\mathfrak{A}, p^{n-k+1})$, which implies that these terms are $\equiv 0$ $\bmod(\bar{\mathfrak{A}}, p)$ because $p^{n-k}a_{n-k}(V) \in \mathbf{Z}[V; T]$.

(d) The terms $a_{n-k}(V)V_i^{p^{n-k}}T_j^{p^{n-j}}$, $k = 1, \ldots, n-1$; $i + j = k$; $i, j \geq 1$. These are all zero mod $\bar{\mathfrak{A}}$ because for these i and j either $V_i \in \mathfrak{A}$ or $T_j \in \mathfrak{A}$.

(e) The terms $a_{n-k}(V)T_j^{p^{n-k}}\bar{V}_i^{p^{n-i}}$, $k = 1, \ldots, n-1$; $i + j = k$, $i, j - 1$. For these i and j, we have $T_j \in \mathfrak{A}$ unless $j \geq n$, which means that $i < h$ so that $\bar{V}_i \equiv 0$ $\bmod(\mathfrak{A}, p)$ and $\bar{V}_i^{p^{n-i}} \equiv 0 \bmod(\mathfrak{A}, p^{n-k+1})$ so that all these terms are $\equiv 0$ $\bmod(\bar{\mathfrak{A}}, p)$.

Putting all this together we find

$$\bar{V}_{n+h} \equiv V_{n+h} + V_h T_n^{p^h} - T_n V_h^{p^n} \bmod(\bar{\mathfrak{A}}, p)$$

which by the sublemma (19.4.10) below implies that (19.4.5) holds.

■ (19.4.10) **Sublemma** Let $b(V, T) \in \mathbf{Z}[V; T]$ and suppose that $b(V, T) \in \bar{\mathfrak{A}} + p\mathbf{Z}[V, T]$. Then $b(V, T) \in \mathfrak{A} + p\mathbf{Z}[V; T]$.

Proof Write $b(V, T)$ as a sum of monomials $\sum c_{\mathbf{n},\mathbf{m}} V^{\mathbf{n}} T^{\mathbf{m}}$. Then $b(V, T) \in \bar{\mathfrak{A}} + p\mathbf{Z}[V, T]$ means that for all $\mathbf{n}$, $\mathbf{m}$ at least one of the following holds (i) $c_{\mathbf{n},\mathbf{m}} \equiv 0 \bmod p$, (ii) $V_i \mid V^{\mathbf{n}}$ for some $i \in \{1, \ldots, h-1, h+1, \ldots, h+n-1\}$, (iii) $T_j \mid T^{\mathbf{m}}$ for some $j \in \{1, 2, \ldots, n-1\}$. And this, in turn, implies that $b(V, T) \in \mathfrak{A} + p\mathbf{Z}[V, T]$ because the $c_{\mathbf{n},\mathbf{m}}$ are integral.

■ (19.4.11) **Remark** The sublemma (19.4.10) does not hold for arbitrary ideals $\mathfrak{A} \subset \mathbf{Z}[V, T]$ as the example $T_1 + T_1^p = p^{-1}(V_1 - pT_1) - p^{-1}(V_1 - pT_1^p)$ shows.

■ (19.4.12) **Proof of Theorem (19.4.1)** (conclusion) Let $F(X, Y)$ be a one dimensional formal group law over k of height $h < \infty$. Because k is a $\mathbf{Z}_{(p)}$-algebra, we can assume that $F(X, Y)$ is a p-typical formal group law (Chapter III, Theorem (15.2.9)), i.e., that $F(X, Y) = \phi_* F_V(X, Y)$ for a suitable homomorphism ϕ: $\mathbf{Z}[V] \to k$. Let $v_i = \phi(V_i)$, $i = 1, 2, \ldots$. We shall write $F_v(X, Y)$ for $\phi_* F_V(X, Y)$. Because $F_v(X, Y)$ is of height h (and k is of characteristic $p > 0$), we have that $v_1 = \cdots = v_{h-1} = 0$, $v_h \neq 0$. We are now going to construct sequences $v(n) = (v_1(n), v_2(n), \ldots)$ of elements of k, starting with $v(1) = v$ such that for all $n \in \mathbf{N}$ the following holds

(19.4.13) $v_i(n) = 0$ for $i = 1, \ldots, h-1, h+1, \ldots, h+n-1$

$v_h(n) \neq 0$

and at the same time we shall obtain power series $\psi_n(X)$ such that

(19.4.14) $\psi_n(X) \equiv X \bmod(\text{degree } p^n)$

(19.4.15) $\psi_n(X)$: $F_{v(n)}(X, Y) \to F_{v(n+1)}(X, Y)$

is a strict isomorphism.

We take $v(1) = v$. Suppose we have already found $v_i(n)$, $i = 1, 2, \ldots$, for a certain $n \geq 1$. We now define $t_i(n) = 0$ for $i = 1, \ldots, n-1, n+1, n+2, \ldots$, and we choose $t_n(n)$ such that

$$v_{n+h}(n) - t_n(n)v_h(n)^{p^n} + v_h(n)t_n(n)^{p^h} = 0 \tag{19.4.16}$$

(Such a $t_n(n)$ exists in K because K is separably closed and because $v_h(n) \neq 0$.) Now define

$$v_i(n+1) = \bar{V}_i(v(n), t(n)), \qquad \psi_n(X) = \alpha_{v(n),t(n)}(X)$$

where $\bar{V}_i(v(n), t(n))$ is the element of k obtained by substituting $v_j(n)$ and $t_j(n)$ for V_j and T_j, $j = 1, \ldots, i$ and $\alpha_{v(n),t(n)}(X)$ is obtained from $\alpha_{V,T}(X)$ by the same substitutions. We then have $\psi_n(X) \equiv X \bmod(\text{degree } p^n)$ because

$$\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X)) \equiv X \mod(T_1, \ldots, T_{n-1}, \text{degree } p^n)$$

since $f_{V,T}(X) \equiv f_V(X) \bmod(T_1, \ldots, T_{n-1}, \text{degree } p^n)$ by the definition of $f_{V,T}(X)$; cf. (19.2.3). Further (19.4.13) holds (with n replaced by $n+1$) because $v_i(n) = 0$ for $i = 1, \ldots, h-1, h+1, \ldots, n+h-1$; $t_i(n) = 0$ for $i = 1, 2, \ldots, n-1$ and (19.4.16). This follows from Lemma (19.4.3).

The composed strict isomorphisms

$$F_v(X, Y) \to F_{v(1)}(X, Y) \to \cdots \to F_{v(n)}(X, Y)$$

converge to some strict isomorphism

$$\psi(X)\colon F_v(X, Y) \to G(X, Y)$$

(because of (19.4.14)) and because of (19.4.15) we see that

$$G(X, Y) = F_w(X, Y)$$

with $w_i = 0$ if $i \neq h$, and $w_h \neq 0$. Now let $\phi(X) = a^{-1}X$ where a is a $(p^h - 1)$th root of unity of w_h. Then $\phi(X)$ is an isomorphism $F_w(X, Y) \to \bar{F}_{\Delta_h}(X, Y)$. This concludes the proof of Theorem (19.4.1).

■ (19.4.17) **Remark** We have also shown that over a separably closed field every one dimensional formal group of finite height h is strictly isomorphic to a formal group law of the form $F_w(X, Y)$ with $w_i = 0$ for all $i \neq h$.

20 Existence and Nonexistence of Homomorphisms and Isomorphisms

This section contains (together with Section 19) most of the general results and criteria that we shall develop on the existence (and nonexistence) of homomorphisms and isomorphisms between formal group laws. However, it certainly does not contain all results on the classification of formal groups (by power series methods) that we shall obtain (and have obtained). More classification results occur in Sections 22, 24, and more results on endomorphism rings will be found in 21 and 23.

20.1 Conditions for the existence of homomorphisms for functional equation formal group laws. Calculation of the endomorphism rings of the universal formal group laws $F_V(X, Y)$ and $H_U(X, Y)$ and of the Lubin–Tate formal group laws

■ (20.1.1) Let A be a characteristic zero ring and $F(X, Y)$ a "functional equation formal group law" over A. By this phrase we mean that for every prime number p there exist associated functional equation ingredients K_p, σ_p: $K_p \to K_p$, $\mathfrak{A}_p \subset A_p$, q_p, $s_{1,p}$, $s_{2,p}$, $\ldots \in K_p$, satisfying the usual conditions (cf. Chapter I, 2.1 and Chapter II, 10.1) such that the logarithm $f(X)$ of $F(X, Y)$ satisfies for all prime numbers p a functional equation

$$f(X) - \sum_{i=1}^{\infty} s_{i,p}(\sigma_p^i)_* f(X^{q_p{}^i}) \in A[\![X]\!]$$

Examples of "functional equation formal group laws" are, e.g., the p-typical universal formal group laws $F_V(X, Y)$, the universal formal group laws $H_U(X, Y)$, and the various Lubin–Tate formal group laws constructed in Chapter I, 8 and Chapter II, 13.2. We emphasize that not all formal group laws are functional equation formal group laws in spite of the fact that the $H_U(X, Y)$ are functional equation formal group laws. Part of the reason is of course that the endomorphisms σ_p: $\mathbf{Z}[U] \to \mathbf{Z}[U]$ may not "factor" through a homomorphism ϕ: $\mathbf{Z}[U] \to A$. That is, given a ring A and a homomorphism ϕ: $\mathbf{Z}[U] \to A$, there may not be an endomorphism $\bar{\sigma}_p$: $A \to A$ such that $\bar{\sigma}_p \phi = \phi \sigma_p$.

■ (20.1.2) **Example** Let $[K : \mathbf{Q}_p]$ be a totally ramified Galois extension of degree 3, A the ring of integers of K, and π a uniformizing element of A. Let $F_V(X, Y)$ be the one dimensional p-typical universal formal group law over $\mathbf{Z}[V]$, and let ϕ: $\mathbf{Z}[V] \to A$ be defined by $\phi(V_1) = \pi$, $\phi(V_2) = 1$, $\phi(V_i) = 0$ if $i \geq 3$ and let $F(X, Y) = \phi_* F_V(X, Y)$. Then we claim $F(X, Y)$ is not a functional equation formal group law. This is easy to see because the only endomorphisms σ of A such that $\sigma(a) \equiv a^q \bmod(\pi)$ for some power q of p are the identity and (powers of) the Frobenius endomorphism of A.

On the other hand, we have

■ (20.1.3) **Proposition** Let A be a characteristic zero ring that is also a $\mathbf{Z}_{(p)}$-algebra which admits an endomorphism σ: $K \to K$, $K = A \otimes_{\mathbf{Z}} \mathbf{Q}$, such that $\sigma(a) \equiv a^p \bmod(pA)$ for all $a \in A$. Then every formal group law over A is a functional equation formal group law (with A, K as given, $\sigma_p = \sigma$, $\mathfrak{A}_p = pA$, $q_p = p$, and $\sigma = id$ for all $\hat{p} \neq p$).

Proof Because of part (iii) of the functional equation lemma 10.2, it suffices to show that $F(X, Y)$ is strictly isomorphic to a functional equation formal group law. Further, because A is a $\mathbf{Z}_{(p)}$-algebra we have only one prime number, viz., the prime number p, to worry about. (For all other prime numbers $\hat{p}$, take $\sigma = id$ and $s_{1,\hat{p}} = s_{2,\hat{p}} = \cdots = 0$.) And finally, again because A is a

$\mathbf{Z}_{(p)}$-algebra, we can (modulo isomorphism) assume that $F(X, Y)$ is a p-typical formal group law (Theorem (15.2.9) of Chapter III). We are now going to construct matrices s_i with coefficients in $A \otimes \mathbf{Q}$ such that

$$(20.1.4) \qquad s_i p \in A^{m \times m},\ f(X) = X + \sum_{i=1}^{\infty} s_i(\sigma^i)_* f(X^{p^i})$$

We are going to construct the s_i inductively. First, $F(X, Y) \equiv X + Y$ mod(degree 2); hence by the p-typical comparison lemma (cf. (20.1.7)) there is a unique matrix a such that

$$F(X, Y) \equiv X + Y + a(p^{-1}(X^p + Y^p - (X + Y)^p)) \quad \text{mod(degree } p + 1)$$

Take $s_1 = p^{-1}a$, then $s_1 p \in A^{m \times m}$. Let $F_{(1)}(X, Y)$ be the formal group law over A with logarithm

$$f_{(1)}(X) = X + s_1 \sigma_* f_{(1)}(X^p)$$

then $F_{(1)}(X, Y) \equiv F(X, Y)$ mod(degree $p + 1$). ($F_{(1)}(X, Y)$ is a formal group law *over* A by the functional equation lemma.) Now suppose we have already found $s_1, \ldots, s_n$ such that $F_{(n)}(X, Y) \equiv F(X, Y)$ mod(degree $p^n + 1$), where $F_{(n)}(X, Y)$ has the logarithm

$$f_{(n)}(X) = X + \sum_{i=1}^{n} s_i(\sigma^i)_* f_{(n)}(X^{p^i})$$

Again by the p-typical comparison lemma (20.1.7) there is a unique matrix a such that

$$F(X, Y) \equiv F_{(n)}(X, Y) + a(p^{-1}(X^{p^{n+1}} + Y^{p^{n+1}} - (X + Y)^{p^{n+1}})) \quad \text{mod(degree } p^{n+1} + 1)$$

Now set $s_{n+1} = p^{-1}a$. Then $F_{(n+1)}(X, Y) \equiv F(X, Y)$ mod(degree $p^{n+1} + 1$). Continuing in this way we find all s_i and $F(X, Y) \equiv f^{-1}(f(X) + f(Y))$ mod(degree $p^n + 1$) for all n, hence $F(X, Y) = f^{-1}(f(X) + f(Y))$ where $f(X)$ is the power series (20.1.4). This concludes the proof of (20.1.3).

■ (20.1.5) **Corollary** (of the proof of Proposition (20.1.3)) If A is a characteristic zero ring (but not necessarily a $\mathbf{Z}_{(p)}$-algebra) with an endomorphism $\sigma: A \to A$ such that $\sigma(a) \equiv a^p$ mod(p) for all $a \in A$ and $F(X, Y)$ is a p-typical formal group law over A, then there exist unique matrices $v_1, v_2, \ldots$ with coefficients in A such that the logarithm of $F(X, Y)$ satisfies the functional equation

$$(20.1.6) \qquad f(X) = X + \sum_{i=1}^{\infty} p^{-1} v_i(\sigma^i)_* f(X^{p^i})$$

■ (20.1.7) ***p*-typical comparison lemma** Let $F(X, Y)$, $G(X, Y)$ be two m-dimensional p-typical formal group laws over a ring A, and suppose that

$F(X, Y) \equiv G(X, Y) \bmod(\text{degree } p^r + 1)$ for some $r \in \mathbf{N} \cup \{0\}$. Then there is a unique matrix a with coefficients in A such that

$$F(X, Y) \equiv G(X, Y) + a(p^{-1}(X^{p^{r+1}} + Y^{p^{r+1}} - (X + Y)^{p^{r+1}})) \mod(\text{degree } p^{r+2})$$

Proof Immediate from the p-typical universality of the formal group law $F_V(X, Y)$ and the structure of $F_V(X, Y)$, cf. (18.3.5).

■ (20.1.8) **Conditions for the existence of endomorphisms** After these preliminaries, partly designed to show that many (but not all) formal group laws are of functional equation type, let us turn to the question of necessary (and sufficient) conditions for the existence of endomorphisms. Let $F(X, Y)$ be a formal group law of dimension m over a characteristic zero ring A and suppose that $F(X, Y)$ is of functional equation type. An endomorphism of $F(X, Y)$ over A is necessarily of the form $f^{-1}(af(X))$ where a is an $m \times m$ matrix with coefficients in A, and $f^{-1}(af(X))$ is an endomorphism of $F(X, Y)$ if and only if all coefficients of $f^{-1}(af(X))$ are in A; cf. 18.2. Suppose this is the case. Then we have $af(X) = f(h(X))$ for some m-tuple of power series $h(X)$, which by part (iii) of the functional equation lemma means that we must have

$$af(X) - \sum_{i=1}^{\infty} s_{i,p}(\sigma_p^i(a)(\sigma_p^i)_* f(X^{q_p{}^i}) \in A \otimes \mathbf{Z}_{(p)}[\![X]\!] \tag{20.1.9}$$

for all prime numbers p. (Where the $s_{i,p}$, σ_p, q_p are part of the ingredients entering into the definition of "being of functional equation type"; cf. 20.1.1. Conversely, if (20.1.9) is satisfied for all p, then part (ii) of the functional equation lemma (together with sublemma (17.6.6) of Chapter III) shows that $f^{-1}(af(X)) \in A[\![X]\!]$ so that $f^{-1}(af(X))$ is an endomorphism of $F(X, Y)$. So (20.1.9) is a set of necessary and sufficient conditions for the existence of endomorphisms.

Of course, if A is also a $\mathbf{Z}_{(p)}$-algebra, then the only nontrivial condition (20.1.9) is the one that involves precisely the prime number p.

■ (20.1.10) **Homomorphisms** Now let $F(X, Y)$ and $G(X, Y)$ be two formal group laws over a characteristic zero ring A of dimensions m and n, respectively. Let $f(X)$, $g(X)$ be the logarithms of $F(X, Y)$ and $G(X, Y)$. Any homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is of the form $g^{-1}(af(X))$ where a is an $n \times m$ matrix with coefficients in A. Suppose that $G(X, Y)$ is a formal group law of functional equation type ($F(X, Y)$ may be arbitrary) and let σ_p, q_p, $s_{1,p}$, $s_{2,p}$, ... be the corresponding ingredients, then $g^{-1}(af(X))$ is a homomorphism over A from $F(X, Y)$ to $G(X, Y)$ if and only if the n-tuple of power series in m variables $af(X)$ satisfies a functional equation

$$af(X) - \sum_{i=1}^{\infty} s_{i,p}\sigma_p^i(a)(\sigma_p^i)_* f(X^{q_p{}^i}) \in A[\![X]\!] \tag{20.1.11}$$

Note that in this case the $s_{i,p}$, σ_p, q_p "belong to $G(X, Y)$" rather than to $F(X, Y)$, i.e., they are the functional equation ingredients of the "receiving" group law.

■ (20.1.12) **The endomorphism ring** $\mathrm{End}_{\mathbf{Z}[V]}(F_V(X, Y))$ To see that (20.1.8) actually tells us something useful on occasion we calculate the endomorphism ring of the p-typical universal m-dimensional formal group law $F_V(X, Y)$ over $\mathbf{Z}[V]$. Recall that the logarithm of $F_V(X, Y)$ satisfies

$$f_V(X) = X + \sum_{i=1}^{\infty} p^{-1} V_i f_V^{(p^i)}(X^{p^i})$$

Let a be an $m \times m$ matrix with coefficients in $\mathbf{Z}[V]$. Now $f_V(X)$ only has pth powers as denominators, so, by (20.1.8), $f^{-1}(af(X))$ has coefficients in $\mathbf{Z}[V]$ if and only if

$$af_V(X) - \sum_{i=1}^{\infty} p^{-1} V_i a^{(p^i)} f_V^{(p^i)}(X^{p^i}) \in \mathbf{Z}[V][\![X]\!] \tag{20.1.13}$$

This means in particular that

$$aa_1(V) - p^{-1} V_1 a^{(p)} \in \mathbf{Z}[V] \tag{20.1.14}$$

But $a_1(V) = p^{-1} V_1$, and hence it follows from (20.1.14) that a is of the form

$$a = nI_m + pb \tag{20.1.15}$$

with $n \in \mathbf{Z}$, I_m the $m \times m$ unit matrix, and b a suitable matrix with coefficients in $\mathbf{Z}[V]$.

Now suppose we have shown that $a \equiv nI_m \bmod(p^{l-1})$. Then looking at the coefficients of degree p^l in (20.1.13), we find the condition

$$aa_l(V) - p^{-1} V_1 a^{(p)} a_{l-1}^{(p)}(V) - \cdots - p^{-1} V_{l-1} a^{(p^{l-1})} a_1^{(p^{l-1})}(V) - p^{-1} V_l a^{(p^l)} \in \mathbf{Z}[V] \tag{20.1.16}$$

Using $a \equiv a^{(p^i)} \bmod(p^{l-1})$, $a \equiv nI_m \bmod(p^{l-1})$, and $a_l(V) = p^{-1} V_1 a_{l-1}^{(p)}(V) + \cdots + p^{-1} V_l$, it readily follows from (20.1.16) that we must have

$$p^{-l} a V_1 V_1^{(p)} \cdots V_1^{(p^{l-1})} - p^{-l} V_1 a^{(p)} V_1^{(p)} \cdots V_1^{(p^{l-1})} \in \mathbf{Z}[V]$$

which then in turn implies $a \equiv nI_m \bmod(p^l)$.

We have proved the proposition

■ (20.1.17) **Proposition** $\mathrm{End}_{\mathbf{Z}[V]}(F_V(X, Y)) = \mathbf{Z}$.

In a similar manner one can show that

■ (20.1.18) **Proposition** $\mathrm{End}_{\mathbf{Z}[U]}(H_U(X, Y)) = \mathbf{Z}$ where $H_U(X, Y)$ is the universal m-dimensional formal group law over $\mathbf{Z}[U]$, of Chapter II, Section 11.

(Proposition (20.1.18) can also be obtained as a consequence of the slight variant $\mathrm{End}_{\mathbf{Z}_{(p)}[V]}(F_V(X, Y)) = \mathbf{Z}_{(p)}$ of Proposition (20.1.17) (which is proved in

exactly the same way) via the observation that $F_V(X, Y)$ is strictly isomorphic to $H_U(X, Y)$ over $\mathbf{Z}_{(p)}[U]$ if we identify the matrices V_i and U_{p^i}.)

Of course Propositions (20.1.17) and (20.1.18) say exactly what one expects of a universal type object: they have as few endomorphisms as possible. A corollary of (20.1.17) and (20.1.18) might be stated as: "generically" the ring of endomorphisms of a formal group law is no larger than $\mathbf{Z}$ (or, e.g., $\mathbf{Z}_{(p)}$ if one considers only formal group laws over $\mathbf{Z}_{(p)}$-algebras; or ...).

■ (20.1.19) **Endomorphisms of Lubin–Tate formal group laws** Let K be a discretely valued field with ring of integers A, maximal ideal $\mathfrak{m}$, residue field $k = A/\mathfrak{m}$ of q elements. (K need not be complete.) Let π be an uniformizing element of A and let B be an $m \times m$ matrix with coefficients in A; let $t \in \mathbf{N}$. We set

$$f(X) = X + \pi^{-1}Bf(X^{q^t}), \qquad F(X, Y) = f^{-1}(f(X) + f(Y))$$

then (by the functional equation lemma) $F(X, Y)$ is an m-dimensional formal group law over A; if B is invertible, $F(X, Y)$ is a Lubin–Tate formal group law as discussed in Chapter II, 13.3.

Let K_{nr} be the maximal unramified extension of K and $\hat{K}_{nr}$ its completion and let A_{nr}, $\hat{A}_{nr}$ be the rings of integers of K_{nr} and $\hat{K}_{nr}$. We can also consider $F(X, Y)$ as a functional equation type formal group over $\hat{A}_{nr}$ because $f(X)$ satisfies (over $\hat{K}_{nr}$) the functional equation

$$f(X) = X + \pi^{-1}B\sigma_* f(X^{q^t})$$

where σ: $\hat{K}_{nr} \to \hat{K}_{nr}$ is the unique Frobenius endomorphism that satisfies $\sigma(a) \equiv a^{q^t} \bmod(\pi)$ for all $a \in \hat{A}_{nr}$. We are going to calculate $\mathrm{End}_{\hat{A}_{nr}}(F(X, Y))$. Let C be an $m \times m$ matrix with coefficients in $\hat{A}_{nr}$. Then (by (20.1.8)) C gives rise to an endomorphism $f^{-1}(Cf(X))$ over $\hat{A}_{nr}$ of $F(X, Y)$ if and only if

$$Cf(X) - \pi^{-1}B\sigma(C)f(X^{q^t}) \in \hat{A}_{nr}$$

Writing out these conditions, we find

$$\begin{aligned} \pi^{-1}CB - \pi^{-1}B\sigma(C) &\in \hat{A}_{nr} \\ \pi^{-2}CB^2 - \pi^{-2}B\sigma(C)B &\in \hat{A}_{nr} \\ &\vdots \\ \pi^{-n}CB^n - \pi^{-n}B\sigma(C)B^{n-1} &\in \hat{A}_{nr} \end{aligned} \tag{20.1.20}$$

Now suppose that B is invertible. Then these conditions imply first that $\sigma(C) \equiv B^{-1}CB \bmod(\pi^n)$ for all $n \in \mathbf{N}$, hence $\sigma(C) = B^{-1}CB$. Specializing to various special cases we find the results:

■ (20.1.21) Let $F(X, Y)$ be a one dimensional Lubin–Tate formal group law over A with logarithm $f(X) = X + u\pi^{-1}f(X^{q^t})$ with $u \in U(A)$, the units of A, then we have $\mathrm{End}_A(F(X, Y)) = A$, $\mathrm{END}(F(X, Y)) = A_t$, where A_t is the ring of integers of the unramified extension of degree t of K, and $\mathrm{END}(F(X, Y)) =$

$\mathrm{End}_{\hat{A}_{nr}}(F(X, Y))$ is the absolute endomorphism ring of $F(X, Y)$. Finally, $\mathrm{End}_{A_{nr}}(F(X, Y)) = \mathrm{END}(F(X, Y)) = A_t$.

■ (20.1.22) Let $F(X, Y)$ be an m-dimensional Lubin–Tate formal group law over A with logarithm $f(X) = X + \pi^{-1}Bf(X^{q^t})$, B an invertible $m \times m$ matrix with coefficients in A, then $\mathrm{End}_A(F(X, Y))$ is the ring of all $m \times m$ matrices C over A that commute with B. In particular, if $B = I_m$, then $\mathrm{End}_A(F(X, Y)) = M_m(A)$, the full ring of $m \times m$ matrices over A.

In a similar manner, using (20.1.10) instead of (20.1.8), one obtains:

■ (20.1.23) Let $F(X, Y)$ and $G(X, Y)$ be an m-dimensional and an n-dimensional Lubin–Tate formal group law over A with logarithms $f(X) = X + \pi^{-1}B_f f(X^{q^t})$, $g(X) = X + \pi^{-1}B_g g(X^{q^t})$ with B_f and B_g invertible matrices over A (and the same t in both cases). Then $\mathbf{FG}_A(F(X, Y), G(X, Y))$ is the group of all $n \times m$ matrices C with coefficients in A such that $CB_f = B_gC$. (*Remark:* this holds also if B_g is not necessarily invertible (but B_f must be invertible).)

■ (20.1.24) **Remark** Let K, A, π, and q be as before and let $\tau = \sigma^r$ be a power of the Frobenius endomorphism σ: $K \to K$, $\sigma(a) \equiv a^p \bmod(\pi)$ for all $a \in A$. Let $F(X, Y)$ be the twisted one dimensional Lubin–Tate formal group law with logarithm $f(X) = X + \pi^{-1}u\tau_* f(X^{p^r})$; cf. Chapter II, Section 13.2. Then (using (20.1.8) again) one finds that $\mathrm{End}_A(F(X, Y)) = \{a \in A \mid \tau(a) = a\}$.

■ (20.1.25) Let K, A, π, q, τ be as above. Let $F(X, Y)$ be an m-dimensional twisted Lubin–Tate formal group law over A with logarithm $f(X) = X + \pi^{-1}B\tau_* f(X^{p^r})$ with B invertible, and let $G(X, Y)$ be the m-dimensional Lubin–Tate formal group law with logarithm $g(X) = X + \pi^{-1}\tau_* g(X^{p^r})$. Then $G(X, Y)$ and $F(X, Y)$ are isomorphic over $\hat{A}_{nr}$.

Proof Both $F(X, Y)$ and $G(X, Y)$ can be considered as twisted formal group laws over $\hat{A}_{nr}$. By Lemma (20.1.26) we have that there exists an invertible matrix C over $\hat{A}_{nr}$ such that $C^{-1}\tau_*(C) = B$. Then we have

$$Cf(X) = X + \pi^{-1}CB\tau_* f(X^{p^r}) = X + \pi^{-1}\tau_* Cf(X^{p^r})$$

so that $Cf(X)$ satisfies the same functional equation as $g(X)$, which proves by the functional equation lemma that $g^{-1}(Cf(X))$ has its coefficients in $\hat{A}_{nr}$; i.e., we have an isomorphism.

■ (20.1.26) **Lemma** Let B be an invertible $m \times m$ matrix with coefficients in $\hat{A}_{nr}$. Then there exists an invertible matrix C with coefficients in $\hat{A}_{nr}$ such that $B = C^{-1}\tau_*(C)$.

This will be proved in Section 24.1 (Proposition (24.1.7)).

20.2 Calculation of the endomorphism rings of the formal group laws $\bar{F}_{\Delta_h}(X, Y)$

At first sight it would seem that the use of functional equation type techniques to study endomorphisms and homomorphisms would be limited to formal group laws over characteristic zero rings. To show that this is not the case, we now calculate the endomorphism rings of the formal group laws $\bar{F}_{\Delta_h}(X, Y)$ over $\mathbf{F}_p$, $\mathbf{F}_q$, and $\mathbf{F}(p^\infty)$, where F_q is the field of $q = p^h$ elements, $\mathbf{F}(p^\infty)$ is the algebraic closure of $\mathbf{F}_p$, and $\bar{F}_{\Delta_h}(X, Y)$ is the one dimensional formal group law of height h over $\mathbf{F}_p$ defined in Chapter I, 3.2.

■ (20.2.1) Choose a prime number p. Recall that $F_{\Delta_h}(X, Y)$ over $\mathbf{Z}$ is the formal group law with logarithm

(20.2.2) $$f_{\Delta_h}(X) = X + p^{-1}f_{\Delta_h}(X^{p^h}) = X + p^{-1}X^{p^h} + p^{-2}X^{p^{2h}} + \cdots$$

and $\bar{F}_{\Delta_h}(X, Y)$ is the reduction modulo p of $F_{\Delta_h}(X, Y)$. To simplify notation we shall from now on in this subsection 20.2 write F_h, f_h, and $\bar{F}_h$ for $F_{\Delta_h}, f_{\Delta_h}$, and $\bar{F}_{\Delta_h}$, respectively, and we shall write q for p^h.

Recall that the endomorphism $[p]_{F_h}(X) = X +_{F_h} X +_{F_h} \cdots +_{F_h} X$ (p times) of $F_h(X, Y)$ satisfies

(20.2.3) $$[p]_{F_h}(X) \equiv X^q \mod(p)$$

so that

(20.2.4) $$[p]_{\bar{F}_h}(X) = X^q$$

We shall from now also occasionally write $\xi(X)$ for X^q.

■ (20.2.5) **Lemma** Let $\alpha(X)$ be an endomorphism of $\bar{F}_h(X, Y)$ over any separably closed field k of characteristic p, e.g., $k = \mathbf{F}(p^\infty)$, then all coefficients of $\alpha(X)$ are actually in $\mathbf{F}_q$.

Proof Because $\alpha(X)$ is an endomorphism we must have $\alpha([p]_{\bar{F}_h}(X)) = [p]_{\bar{F}_h}(\alpha(X))$, i.e., $\alpha(X)^q = \alpha(X^q)$ and hence $a^q = a$ for all coefficients of $\alpha(X)$. Q.E.D.

■ (20.2.6) The next step is to find a fairly large number of automorphisms of $\bar{F}_h(X, Y)$. To this end recall that $F_h(X, Y)$ can be obtained from $F_V(X, Y)$, the universal one dimensional p-typical formal group law, by the specification $V_h = 1$, $V_i = 0$ if $i \neq h$. Let $A = W_{p^\infty}(\mathbf{F}_q)$ be the ring of integers of the unramified extension of degree h of $\mathbf{Q}_p$ and let $b_1, \ldots, b_{h-1}$ be a sequence of $h - 1$ elements of A and set $g(X) = X + b_1 X^p + \cdots + b_{h-1} X^{p^{h-1}}$. Let $F_g(X, Y)$ be the formal group obtained from the one dimensional formal group law $F_{V,T}(X, Y)$ by substituting $V_h = 1$, $V_i = 0$ for $i \neq h$, $T_i = b_i$ for $i = 1, \ldots, h - 1$ and $T_i = 0$ for $i \geq h$, and let $\alpha_g(X)$ be the power series obtained from $\alpha_{V,T}(X)$ by the same substitutions. Then $\alpha_g(X)$: $F_h(X, Y) \to F_g(X, Y)$ is a strict isomorphism of

formal group laws over A. The formal group law $F_g(X, Y)$ is p-typical, therefore there exists a sequence of elements $\hat{v} = (\hat{v}_1, \hat{v}_2, \hat{v}_3, \ldots)$, $\hat{v}_i \in A$, such that $F_{\hat{v}}(X, Y) = F_g(X, Y)$.

We now have

■ (20.2.7) **Lemma** $\hat{v}_i \equiv 0 \bmod p$ if $i \neq h$, $\hat{v}_h \equiv 1 \bmod p$.

Proof Writing $v = (v_1, v_2, \ldots)$ for the sequence $(0, 0, \ldots, 0, 1, 0, 0, \ldots)$ with the 1 in the ith spot and $t = (t_1, t_2, \ldots)$ for the sequence $(b_1, \ldots, b_{h-1}, 0, 0, \ldots)$, we have according to Corollary (19.3.6) that

$$\hat{v}_n - v_n = pt_n + \sum_{i=1}^{n-1} \hat{a}_{n-i}(v_i^{p^{n-i}} - \hat{v}_i^{p^{n-i}}) + \sum_{k=2}^{n} \sum_{i+j=k} a_{n-k}(v_i^{p^{n-k}} t_j^{p^{n-j}} - t_j^{p^{n-k}} v_i^{p^{n-i}}) \tag{20.2.8}$$

where $f(X) = \sum a_i X^{p^i}$ and $f_g(X) = \sum \hat{a}_i X^{p^i}$. Now suppose we have already proved that $v_i \equiv \hat{v}_i \bmod p$ for all $i < n$. Then we have, taking the various terms in (20.2.8) in turn,

$$v_i^{p^{n-i}} \equiv \hat{v}_i^{p^{n-i}} \quad \bmod(p^{n-i+1}) \tag{20.2.9}$$

hence

$$\hat{a}_{n-i}(v_i^{p^{n-i}} - \hat{v}_i^{p^{n-1}}) \equiv 0 \quad \bmod(p)$$

As regards the terms of the double sum in (20.2.8), we have $v_i = 0$ unless $i = h$ and $v_h = 1$ so the only possible nonzero contributions of the double sum are of the form

$$a_{n-k}(t_{k-h}^{p^{n-k+h}} - t_{k-h}^{p^{n-k}})$$

and these are congruent zero modulo p because $t_{k-h}^{p^h} \equiv t_{k-h} \bmod(p)$ since $t_{k-h} \in A$ and hence $t_{k-h}^{p^{n-k+h}} - t_{k-h}^{p^{n-k}} \equiv 0 \bmod(p^{n-k+1})$. It now follows from (20.2.8) that also $\hat{v}_n - v_n \equiv 0 \bmod(p)$, which concludes the proof of the lemma.

■ (20.2.10) Lemma (20.2.7) says that by reducing $F_g(X, Y)$ modulo p we get the same thing as by reducing $F_h(X, Y)$ so that the reduction of $\alpha_g(X)$ modulo p provides us with an automorphism:

$$\bar{\alpha}_g^{-1}(X)\colon \bar{F}_h(X, Y) \to \bar{F}_h(X, Y), \qquad \bar{\alpha}_g(X) = \bar{\alpha}_{v,t}(X)$$

which starts off as $\bar{\alpha}_g^{-1}(X) = X + \bar{b}_1 X^p + \cdots + \bar{b}_{n-1} X^{p^{h-1}} + \cdots$ where the $\bar{b}_i$ are the images of the b_i under the natural projection $A \to \mathbf{F}_q$. The last statement follows because $a_i(V, T) \equiv T_i \bmod(V_1, \ldots, V_{h-1})$ if $i < h$ (cf. (19.3.3)) and hence

$$f_{V,T}(X) \equiv X + T_1 X^p + \cdots + T_{h-1} X^{p^{h-1}} \quad \bmod(\text{degree } p^h, V_1, \ldots, V_{h-1})$$

and

$$\alpha_{V,T}^{-1}(X) = f_V^{-1}(f_{V,T}(X)) \equiv X + T_1 X^p + \cdots + T_{h-1} X^{p^{h-1}} \mod(V_1, \ldots, V_{h-1}, \text{degree } p^h))$$

■ (20.2.11) Let M_h be the additive group of all polynomials of the form $a_0 X + a_1 X^p + \cdots + a_{h-1} X^{p^{h-1}}$ with $a_i \in \mathbf{F}_q$ with the usual (coordinatewise) addition. Multiplication on M_h is defined as follows

$$\begin{aligned}(a_0 X + a_1 X^p + \cdots + a_{h-1} X^{p^{h-1}})(b_0 X + b_1 X^p + \cdots + b_{h-1} X^{p^{h-1}}) \\ = a_0 b_0 X + (a_0 b_1 + a_1 b_0^p) X^p + \cdots \\ + (a_0 b_{h-1} + a_1 b_{h-2}^p + \cdots + a_{h-1} b_0^{p^{h-1}}) X^{p^{h-1}} \\ \equiv a_0 (b_0 + h_1 X^p + \cdots + b_{h-2} X^{p^{h-1}}) + \cdots \\ + a_{h-1} (b_0 + b_1 X^p + \cdots + b_{h-1} X^{p^{h-1}})^{p^{h-1}} \mod(\text{degree } p^h)\end{aligned}$$

This turns M_h into an associative (but noncommutative if $h > 1$) ring with unit element. We now define a map ϕ: $\mathrm{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y)) \to M_h$ by assigning to $\alpha(X) \in \mathrm{End}(\bar{F}_h(X, Y))$ the mod(degree p^h) part of $\alpha(X)$. To show that this is well defined, we must of course show that $\alpha(X)$ is of the form $\alpha(X) \equiv a_0 + a_1 X^p + a_2 X^{p^2} + \cdots + a_{h-1} X^{p^{h-1}}$ mod(degree p^h). This follows from the fact that $\bar{F}_h(X, Y) \equiv X + Y$ mod(degree p^h) so that $\alpha(X)$, being an endomorphism, must satisfy $\alpha(X) + \alpha(Y) \equiv \alpha(X + Y)$ mod(degree p^h). The same remark ($\bar{F}_h(X, Y) \equiv X + Y$ mod(degree p^k)) shows that ϕ: $\mathrm{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y)) \to M_h$ is a homomorphism of abelian groups, and, by the definition of the multiplication on M_h, it is then also a homomorphism of rings with identity element.

■ (20.2.12) **Lemma** ϕ: $\mathrm{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y)) \to M_h$ is a surjective homomorphism of associative rings with identity elements. The kernel of ϕ consists of all endomorphisms of height $\geq h$ and $\mathrm{Ker}\ \phi = p\ \mathrm{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y))$.

Proof First, because $F_h(X, Y)$ is a Lubin–Tate formal group law over A, there are endomorphisms $\alpha(X)$ of $F_h(X, Y)$ such that $\alpha(X) \equiv aX$ mod(degree 2) for every $a \in A$; cf. (20.1.21). Reducing these mod p, we find elements of the form $\bar{a}X + a_1 X^p + \cdots + a_{b-1} X^{p^{h-1}} \in \mathrm{Im}\ \phi$ for every $\bar{a} \in \mathbf{F}_q$. In addition to these, we have found in (20.2.10) elements $X + b_1 X^p + \cdots + b_{h-1} X^{p^{h-1}}$ in Im ϕ for all $b_1, \ldots, b_{h-1} \in \mathbf{F}_q$. Together these elements in Im ϕ generate all of M_h additively so that ϕ is indeed surjective.

By the definition of height of an endomorphism (cf. 18.3) $\phi(\alpha(X)) = 0$ iff $\mathrm{ht}(\alpha(X)) \geq h$. Now suppose that height $(\alpha(X)) \geq h$ we want to show that $\alpha(X) \in p\ \mathrm{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y))$ which means (because $[p]_{\bar{F}_h}(X) = X^q$) that we must show $\alpha(X) = \beta(X)^q$ for some endomorphism β. Now $\alpha(X)$, being of height $\geq h$, can be written as $\alpha(X) = \beta(X^q)$ for some power series β over $\mathbf{F}_q$ (cf. (18.3.1)). We have

$$\alpha(\bar{F}_h(X, Y)) = \beta(\bar{F}_h(X, Y)^q) = \beta(\bar{F}_h(X^q, Y^q))$$

and

$$\bar{F}_h(\alpha(X), \alpha(Y)) = \bar{F}_h(\beta(X^q), \alpha(Y^q))$$

Comparing these expressions, we see that $\beta(X)$ is indeed an endomorphism of $\bar{F}_h(X, Y)$.

Finally, if $\alpha(X) \in p \operatorname{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y))$, then $\alpha(X) = \beta(X)^q = \beta(X^q)$ for some endomorphism $\beta(X)$, which shows that $\phi(\alpha(X)) = 0$ in M_h. Q.E.D.

■ (20.2.13) **Theorem** Writing E_h for $\operatorname{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y))$, we have:

(i) E_h is a free module of rank h^2 over $\mathbf{Z}_p$.
(ii) $E_h \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = D_h$ is a division algebra of rank h^2 over $\mathbf{Q}_p$.
(iii) E_h is the maximal order of D_h (over $\mathbf{Z}_p$).
(iv) The center of D_h is $\mathbf{Q}_p$, so that D_h is a central division algebra over $\mathbf{Q}_p$.
(v) The invariant of D_h is $\operatorname{inv}(D_h) = h^{-1}$.
(vi) The map $a \mapsto f_h^{-1}(af_h(X))$ defines a ring homomorphism $A_h \to \operatorname{End}_{A_h}(F_h(X, Y))$ which by composition with the reduction homomorphism $\operatorname{End}_{A_h}(F_h(X, Y)) \to E$ yields an injective ring homomorphism $\psi: A_h \to E$. Further, $\psi(A_h) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a maximal unramified commutative subfield of D_h. Here A_h is the ring of integers of the unramified extension of degree h of $\mathbf{Q}_p$.

Before proving most of this theorem we shall certainly need to know what the various words in its statement mean. To this end we have inserted below (20.2.16) a short intermezzo on (central) division algebras. First, however, we state a corollary and prove part (i) of Theorem (20.2.13).

■ (20.2.14) **Corollary** Let $F(X, Y)$ be a one dimensional formal group law of height $h < \infty$ over a separably closed field k of characteristic $p > 0$. Then the endomorphism ring $\operatorname{End}_k(F(X, Y))$ is isomorphic to the maximal order in the central division algebra D_h of invariant h^{-1} and rank h^2 over $\mathbf{Q}_p$.

(This follows immediately from Theorem (20.2.13) and Lemma (20.2.5) because over a separably closed field of characteristic $p > 0$ the one dimensional formal group laws are classified by their heights (Theorem (19.4.1)).)

■ (20.2.15) **Proof of part (i) of Theorem (20.2.13)** We know that E_h is a complete Hausdorff topological module over $\mathbf{Z}_p$ and that E_h is $\mathbf{Z}_p$-torsion free because E_h has no zero divisors (cf. (18.3.2)). Further, $E_h/pE_h = M_h$, which is a free module of rank h^2 over $\mathbf{F}_p$. It follows that E_h is a free module of rank h^2 over $\mathbf{Z}_p$.

■ (20.2.16) **Intermezzo on division algebras** This little intermezzo contains no proofs. For these, see [361, Chapter XII] or the nice little booklet [36]. Let K be a field. A central division algebra D over K is a finite dimensional associative (but not necessarily commutative) algebra over K in which every element $\neq 0$ is invertible such that the center of D is precisely K. Three of the important theorems concerning central division algebras are (cf. [36; Theorems III-1, III-3, III-4]):

Rank theorem Let D be a central division algebra over K, then $[D:K]$, the dimension of D over K, is a square n^2, $n \in \mathbf{N}$.

Commutant theorem (weak form) Let D be a central division algebra over K and L a commutative subfield of D that contains K. Then the commutant $D_L = \{x \in D \mid xa = ax \text{ for all } a \in L\}$ is a central division algebra over L and $[L:K][D_L:K] = [D:K]$.

Skolem–Noether theorem (weak form) Let D be a central division algebra over K and let L and L' be two subfields of D that contain K. Then every K-isomorphism $\sigma: L \to L'$ can be extended to an internal automorphism of D. (I.e., there exists an element $\gamma \in D$ such that $\sigma(x) = \gamma x \gamma^{-1}$ for all $x \in L$.)

Let us examine the situation of the commutant theorem in more detail. Suppose $[L:K] = m$ and $[D:K] = n^2$. Because L is commutative, we have $L \subset D_L$ so that the situation is $D \supset D_L \supset L \supset K$. Using $m[D_L:K] = n^2$ we see that $[D_L:L] = n^2/m^2$, so D_L is a central division algebra over L of rank n^2/m^2. We also note that evidently a commutative subfield L of D that contains K is of dimension a divisor of n over K if $[D:K] = n^2$.

From now on we suppose that K is a finite extension of $\mathbf{Q}_p$. Let $v: K \to \mathbf{Z} \cup \{\infty\}$ be the normalized (exponential) valuation on K. There is a unique extension of v to a valuation on D. (For example, because K is complete one can extend v uniquely to all the commutative subfields $K(\alpha)$, $\alpha \in D$, and (by uniqueness) these extensions agree to define a unique extension of v on all of D.) Let $A_D = \{x \in D \mid v(x) \geq 0\}$; A_D, the maximal order of D, is an algebra of rank n^2 over $A_K = \{x \in K \mid v(x) \geq 0\}$. Let $\mathfrak{m}_D = \{x \in D \mid v(x) > 0\}$; this is the maximal (two sided) ideal of A_D; let $k_D = A_D/\mathfrak{m}_D$ be the residue field of D. Let e be the ramification index of D/K (i.e., e is such that $v(D/\{0\}) = e^{-1}\mathbf{Z}$) and let $f = [k_D:k]$, where k is the residue field of K. Then $ef = n^2$. Since k is a finite field, $k_D = k(\bar{x})$ for some $x \in A_D$ ($\bar{x}$ denotes the residue class of x) and because (as we have seen above) $[K(x):K] \leq n$, it follows that $f \leq n$. Further, there is an $x \in D$ such that $v(x) = e^{-1}$ (by the definition of e) and again because $[K(x):K] \leq n$ we also have $e \leq n$. Combined with $ef = n^2$, this gives $e = f = n$.

Since $[k_D:k] = n$, there is an $x \in A_D$ such that $k_D = k(\bar{x})$ and $[K(x):K] \geq n$, but always $[K(x):K] \leq n$. It follows that $[K(x):K] = n$ and since also $[k(x):k] = n$, it follows that $K(x)/K$ is unramified of degree n. Thus D contains a maximal unramified (commutative) subfield of degree n.

Finally, we discuss the invariant of D (which is classifying). Every central division algebra D over K is in particular a central simple algebra over K and thus gives rise to an element $\delta \in \mathrm{Br}(K) = H^2(K_{nr}/K)$, the Brauer group K. Now, since K is a local field $H^2(K_{nr}/K) \simeq \mathbf{Q}/\mathbf{Z}$, and the element of $\mathbf{Q}/\mathbf{Z}$ corresponding to δ is the invariant of D. This number can be calculated as follows. Let L be a maximal unramified commutative subfield of D, and let $\sigma: L \to L$ be the Frobenius automorphism of L, then, by the Skolem–Noether theorem

quoted above, there exists an element $\gamma \in D$ such that $\sigma(x) = \gamma x \gamma^{-1}$ for all $x \in L$. Consider $v(\gamma) \in n^{-1}\mathbf{Z}/\mathbf{Z}$; this is the invariant of D. (*Remark:* neither L nor γ (given L) are unique, but $v(\gamma)$ is uniquely determined modulo $\mathbf{Z}$; e.g., one can obviously change γ to γy for any $y \in L$, $y \neq 0$.)

■(20.2.17) **Proof of part (ii) of Theorem (20.2.13)** By part (i) $D_h = E_h \otimes \mathbf{Q}_p$ is an algebra of dimension n^2 over $\mathbf{Q}_p$. Further, E_h has no zero divisors; it follows that D_h is a division algebra of rank n^2 over $\mathbf{Q}_p$. (It is also clear that $\mathbf{Q}_p$ is in the center of D_h (since $\mathbf{Z}_p$ is in the center of E_h); to see that every $x \neq 0$ in D_h is invertible, consider the vector space homomorphisms $y \mapsto xy$, $D_h \to D_h$; since x is not a zero divisor, this map is injective; hence by the finite dimensionality of D_h over $\mathbf{Q}_p$ it is also surjective; so there is an $z \in D_h$ such that $xz = 1$.)

■(20.2.18) **Proof of part (iii) of Theorem (20.2.13)** Let height: $\mathrm{End}_{\mathbf{F}_q}(\bar{F}_h(X, Y)) \to \mathbf{N} \cup \{0\} \cup \{\infty\}$ be the map that assigns to an endomorphism $\alpha(X)$ its height. It is obvious from the definition of height that we have $\mathrm{ht}(\alpha(X)) = \infty \Leftrightarrow \alpha(X) = 0$, $\mathrm{ht}(\alpha(X) +_F \beta(X)) \geq \min(\mathrm{ht}(\alpha(X)), \mathrm{ht}(\beta(X)))$, and $\mathrm{ht}(\alpha(\beta(X)) = \mathrm{ht}(\alpha(X))\,\mathrm{ht}(\beta(X))$; cf. (18.3.2). Further, $\mathrm{ht}([p]_{\bar{F}_h}(X)) = h$ so that $h^{-1}(\mathrm{ht})$ is a valuation on E_h which coincides with the p-adic valuation v: $\mathbf{Z}_p \to \mathbf{N} \cup \{0\} \cup \{\infty\}$. It follows (by the uniqueness of the valuation on D_h extending v) that on E_h the valuation $h^{-1}(\mathrm{ht})$ is this unique extension. Hence clearly $E_h \subset A_{D_h} = \{x \in D_h \mid v(x) \geq 0\}$, where v is the unique extension of v on $\mathbf{Q}_p$ to all of D_h. To prove the opposite inclusion we first note that

$$p^n E_h = \{\alpha(X) \in E_h \mid \mathrm{ht}(\alpha(X)) \geq nh\} \tag{20.2.19}$$

(We already used and proved this for $n = 1$ in Lemma (20.2.12).) Because height is a valuation, we have $\mathrm{ht}[p^n]_{F_h}(\alpha(X)) \geq nh$. Conversely, let $\alpha(X)$ be of height $\geq nh$, then $\alpha(X) = \beta(X^{p^{nh}})$ for some power series $\beta(X)$. We have $\beta(\bar{F}_h(X^{p^{nh}}, Y^{p^{nh}})) = \beta((\bar{F}_h(X, Y)^{p^{nh}}) = \alpha(\bar{F}_h(X, Y)) = \bar{F}_h(\alpha(X), \alpha(Y)) = \bar{F}_h(\beta(X^{p^{nh}}), \beta(Y^{p^{nh}}))$ proving that β is an endomorphism and hence $\alpha(X) \in p^n E_h$.

Now let $\beta(X) \in A_{D_h}$. Because $D_h = E_h \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, there is an $n \in \mathbf{N}$ such that $p^n \beta(X) \in E_h$. Now $v(p^n \beta(X)) \geq n$, hence (because $v = h^{-1}(\mathrm{ht})$ on E_h) $\mathrm{ht}(p^n \beta(X)) \geq nh$, i.e., $p^n \beta(X) \in p^n E_h$ by (20.2.19) and $\beta(X) \in E_h$ because D_h is torsion free. This concludes the proof of part (iii) of Theorem (20.2.13).

■(20.2.20) **Proof of part (iv) of Theorem (20.2.13)** We already know that $\mathbf{Q}_p \subset \mathrm{center}(D_h)$. Let $Z(E_h)$ be the center of E_h. If $\alpha(X) \in E_h$ and $p\alpha(X) \in Z(E_h)$, then also $\alpha(X) \in Z(E_h)$. It follows from this that if $[Z(D_h) : \mathbf{Q}_p] \geq 2$, then, since $E_h = A_{D_h}$, the image of $Z(E_h)$ in k_h, the residue field of D_h (cf. (20.2.16)) would be of dimension ≥ 2 over $\mathbf{F}_p$. (By the way, $[k_h : \mathbf{F}_p] = h$ (cf. (20.2.16)) so that $k_h = \mathbf{F}_q$.) Hence it suffices to prove that the image of $Z(E_h)$ in k_h is of dimension ≤ 1 over $\mathbf{F}_p$; and to do this, in turn, it certainly suffices to prove that the center of the algebra M_h of (20.2.11) is of dimension 1 over $\mathbf{F}_p$ (because $E_h \to M_h$ is surjective).

Let $a(X) = a_0 X + a_1 X^p + \cdots + a_{h-1} X^{p^{h-1}} \in M_h$. First, let $b(X) = b_0 X$, then $a(b(X)) = b(a(X))$ mod(degree p^h) implies that $a_j(b_0 - b_0^{p^j}) = 0$. So for $a(X)$ to be in the center of M_h we must first have $a_j = 0$ for $j = 1, \ldots, h-1$.

So suppose this is the case, i.e., $a(X) = a_0 X$. Now take $b(X) = X + \cdots + X^{p^{h-1}}$. Then we must have $(a_0 - a_0^{p^j}) = 0$ for all j if $a_0 X$ is to be in center of M_h. It follows that $a_0 \in \mathbf{F}_p$. This concludes the proof of part (iv) of Theorem (20.2.13).

■ (20.2.21) **Proof of part (vi) of Theorem (20.2.13)** (Part (v) will be proved below using part (vi).) We already know that

$$A_h \to \mathrm{End}_{A_h}(F_h(X, Y)), \qquad a \mapsto f_h^{-1}(a f_h(X)) = [a]_{F_h}(X)$$

is a ring homomorphism because F_h is a Lubin–Tate formal group law over A_h. In fact by (20.1.21) this is an isomorphism. Further, because $[p]_{F_h}(X) \equiv X^q$ mod(p) and $[u]_{F_h}(X) \equiv uX$ mod(degree 2) if u is a unit of A_h, we have that $[up^n]_{F_h}(X) \equiv uX^{q^n}$ mod(p, degree $q^n + 1$) which proves that the composed map $\psi\colon A_h \to E_h$ is injective. To prove that $\psi(A_h) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is unramified, it suffices to show that $v(\psi(p)) = 1$. But $v = h^{-1}(\mathrm{ht})$ on E_h and $\mathrm{ht}[p]_{F_h}(X) = h$, hence indeed $v(\psi(p)) = 1$. This concludes the proof of part (vi) of Theorem (20.2.13) because $\psi(A_h) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is commutative and of dimension h over $\mathbf{Q}_p$, hence maximal; cf. (20.2.16).

■ (20.2.22) **Proof of part (v) of Theorem (20.2.13)** Let $\sigma\colon A_h \to A_h$ be the Frobenius homomorphism and let $\alpha_a(X) = [a]_{F_h}(X)$ and $\bar{\alpha}_a(X)$ its reduction in $\psi(A_h) \subset E_h$. We have, because $f_h(X)$ has its coefficients in $\mathbf{Q}_p$,

$$\sigma_* [a]_{F_h}(X) = f_h^{-1}(\sigma(a) f_h(X)) = [\sigma(a)]_{F_h}(X)$$

Hence

$$\bar{\alpha}_a(X)^p = \sigma_* \bar{\alpha}_a(X^p) = \bar{\alpha}_{\sigma(a)}(X^p)$$

So the endomorphism $\beta(X) = X^p \in E_h$ is such that $\beta(\alpha_a(X)) = \alpha_{\sigma(a)}(\beta(X))$. That is, the Frobenius automorphism on the maximal unramified subfield $\psi(A_h) \otimes \mathbf{Q}_p$ is induced by conjugation with $\beta(X) = X^p$. By (20.2.16) (last paragraph) this means that the invariant of D_h is equal to $v(\beta(X)) = h^{-1}\,\mathrm{ht}(\beta(X)) = h^{-1}$. This concludes the proof of part (v) of Theorem (20.2.13).

■ (20.2.23) Let us now try to calculate $E_h^0 = \mathrm{End}_{\mathbf{F}_p}(\bar{F}_h(X, Y))$. One element of $\mathrm{End}_{\mathbf{F}_p}(\bar{F}_h(X, Y))$ is the endomorphism $\beta(X) = X^p$ (because $\bar{F}_h(X, Y)$ has all its coefficients in $\mathbf{F}_p$). Write π for $\beta(X)$ as an element of D_h. Then π satisfies in D_h the equation $\pi^h = p$ (because $[p]_{\bar{F}_h}(X) = X^q$). An endomorphism $\alpha(X) \in E_h$ is in E_h^0 if and only if $\alpha(X)^p = \alpha(X)^p$, i.e., if in D_h it commutes with π. But because $[\mathbf{Q}_p[\pi] : \mathbf{Q}_p] = h$, the commutant of $\mathbf{Q}_p[\pi]$ in D_h is $\mathbf{Q}_p[\pi]$ itself (cf. (20.2.16)). It follows that $E_h^0 \otimes \mathbf{Q}_p = \mathbf{Q}_p[\pi]$, and hence, using part (iii) of Theorem (20.2.13), that E_h^0 is $\mathbf{Z}_p[\pi]$. Thus we have

■ (20.2.24) **Proposition** $\mathrm{End}_{\mathbf{F}_p}(\bar{F}_h(X, Y))$ is (isomorphic to) the ring of integers in the totally ramified extension $\mathbf{Q}_p[\pi]/\mathbf{Q}_p$ where π satisfies the equation $\pi^h = p$.

■ (20.2.25) The relation between the unramified subfield $\psi(A_h) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and totally ramified subfield $E_h^0 \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ in D_h is given by $\pi x = \sigma(x)\pi$ where $x \in \psi(A_h) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and σ is the Frobenius automorphism of $\psi(A_h) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. This was used in (20.2.22).

20.3 Honda's noncommutative power series calculating methods

In [189] Honda developed a "not quite commutative" method of calculating with power series which is most useful (if not absolutely necessary) for describing, e.g., some of the results of 20.1.

■ (20.3.1) **The setting** The basic ingredients for this subsection 20.3 are: a characteristic zero ring A; $K = A \otimes_{\mathbf{Z}} \mathbf{Q}$; an element π of A such that $A/\pi A$ is a ring of characteristic $p > 0$, p a prime number; an endomorphism $\sigma\colon K \to K$; a power q of p. These ingredients are supposed to satisfy $\sigma(a) \equiv a^q \bmod(\pi)$ for all $a \in A$ and $\sigma(\pi) = w\pi$ for some unit $w \in A^*$, the group of units of A.

Note that if we take $\mathfrak{A} = \pi A$ we are in the situation of the functional equation lemma. We also note that π is not a zero divisor in A because $p \in \pi A$ and A is of characteristic zero.

For the remainder of this subsection 20.3, A, K, etc. will be as above and satisfy the requirements listed; after a while we shall specify K to be a discrete valuation ring with ring of integers A.

■ (20.3.2) We let $K_\sigma[\![T]\!]$ be the noncommutative power series ring in one indeterminate T with the multiplication rule $Ta = \sigma(a)T$ for all $a \in K$; $A_\sigma[\![T]\!]$ is the subring of all power series in T with coefficients in A. We use $K_\sigma[\![T]\!]^{m \times n}$ to denote $m \times n$ matrices with coefficients in $K_\sigma[\![T]\!]$. Elements of $K_\sigma[\![T]\!]^{m \times n}$ can also be seen as sums $\sum c_i T^i$ with $c_i \in K^{m \times n}$, from which it is easy to see how an element $\eta \in K_\sigma[\![T]\!]^{m \times n}$ and an element $\vartheta \in K_\sigma[\![T]\!]^{n \times l}$ can be multiplied to give an element $\eta\vartheta$ in $K_\sigma[\![T]\!]^{m \times l}$.

Now let $X = (X_1, \ldots, X_n)$ be a sequence of n indeterminates, let $\eta = \sum_{i=0}^{\infty} C_i T^i \in K_\sigma[\![T]\!]^{l \times m}$ and let $f(X)$ be an m-tuple of power series in X such that $f(0) = 0$. Then we define

$$\eta * f(X) = \sum_{i=0}^{\infty} C_i(\sigma_*^i) f(X^{q^i})$$

It is immediately obvious from this definition that

$$(\eta * f(x)) + (\vartheta * f(x)) = (\eta + \vartheta) * f(X) \tag{20.3.3}$$

$$(\eta\vartheta) * f(X) = \eta * (\vartheta * f(X))$$

■(20.3.4) Now let us see what these definitions have to do with the functional equation lemma situation. Choose $m \times m$ matrices $v_1, v_2, \ldots$ with coefficients in A and let $f(X)$ be the m-tuple of power series in m variables defined by the functional equation

$$f(X) = X + \sum_{i=1}^{\infty} \pi^{-1} v_i(\sigma_*^i) f(X^{q^i}) \tag{20.3.5}$$

On the other hand, let η_v be the element $\pi I_m - \sum_{i=1}^{\infty} v_i T^i$ of $A_\sigma[\![T]\!]^{m \times m}$. We calculate that the coefficients matrices B_i of

$$\eta_v^{-1}\pi = \sum_{i=0}^{\infty} B_i T^i$$

satisfy

$$B_0 = I_m, \qquad B_n = \pi^{-1} v_1 \sigma(B_{n-1}) + \cdots + \pi^{-1} v_{n-1} \sigma^{n-1}(B_1) + \pi^{-1} v_n$$

so that

$$(\eta_v^{-1}\pi) * i(X) = f(X), \qquad i(X) = X \tag{20.3.6}$$

(We shall reserve the symbol $i(X)$ for the m-tuple of power series X in this section.)

More generally, let $f_g(X)$ be the functional equation power series

$$f_g(X) = g(X) + \sum_{i=1}^{\infty} \pi^{-1} v_i \sigma_*^i f_g(X^{q^i})$$

then

$$(\eta_v^{-1}\pi) * g(X) = f_g(X)$$

and if $g(X)$ is of the form $g(X) = \sum_{i=0}^{\infty} b_i X^{q^i}$, let $\vartheta_g(T) = \sum_{i=0}^{\infty} b_i T^i$, then

$$g(X) = \vartheta_g * i(X)$$

so that (using (20.3.3)) in this case

$$f_g(X) = (\eta_v^{-1}\pi\vartheta_g) * i(X) \tag{20.3.7}$$

■(20.3.8) **Reinterpretation of the results of (20.1.8) and (20.1.10)** Let $v = (v_1, v_2, \ldots)$ be a sequence of $m \times m$ matrices and $u = (u_1, u_2, \ldots)$ a sequence of $n \times n$ matrices, both with coefficients in A. Let

$$\eta_v = I_m\pi - \sum_{i=1}^{\infty} v_i T^i, \qquad \eta_u = I_n\pi - \sum_{i=1}^{\infty} u_i T^i$$

be the corresponding elements of $A_\sigma[\![T]\!]^{m \times m}$ and $A_\sigma[\![T]\!]^{n \times n}$. Let $f(X) = \eta_u^{-1}\pi * i(X)$, $g(X) = \eta_v^{-1}\pi * i(X)$. Let $F(X, Y)$, $G(X, Y)$ be the formal group laws with logarithms $f(X)$ and $g(X)$. Every homomorphism $\alpha(X)$: $F(X, Y) \to$

$G(X, Y)$ must be of the form $\alpha(X) = g^{-1}(cf(X))$ for a suitable $m \times n$ matrix c with coefficients in A, and by the functional equation lemma $\alpha(X)$ is integral if and only if $cf(X)$ is of the form $g_h(X) = h(X) + \sum \pi^{-1} v_i \sigma_*^i g_h(X^{q^i})$ with $h(X) \in A[\![X]\!]$; cf. (20.1.8) and (20.1.10). The power series $h(X)$ is then necessarily of the form $h(X) = \sum b_i X^{q^i}$, which by (20.3.7) above means that $g_h(X) = (\eta_v^{-1} \pi \vartheta) * i(X)$, where $\vartheta = \sum b_i T^i$. On the other hand, $cf(X) = (c\eta_u^{-1}\pi) * i(X)$. It follows (trivially) that $\eta_v^{-1}\pi\vartheta = c\eta_u^{-1}\pi$. Now because $\sigma(\pi) = w\pi$ for some unit $w \in A^*$, there is a power series $\vartheta_c = \sum_{i=0}^{\infty} a_i T^i$, $a_i \in A$, such that $\pi\vartheta = \vartheta_c \pi$. We find $\eta_v^{-1}\vartheta_c = c\eta_u^{-1}$ and hence $\eta_v c = \vartheta_c \eta_u$. We have proved

■ (20.3.9) **Proposition** Let $u = (u_1, u_2, \ldots)$ be a sequence of elements in $A^{m\times m}$ and $v = (v_1, v_2, \ldots)$ a sequence of elements in $A^{n\times n}$. Let $F(X, Y)$ and $G(X, Y)$ be the formal group laws with logarithms

$$f(X) = X + \sum \pi^{-1} u_i \sigma_*^i f(X^{q^i}), \qquad g(X) = X + \sum \pi^{-1} v_i \sigma_*^i g(X^{q^i})$$

and let $\eta_u = \pi I_m - \sum u_i T^i$, $\eta_v = \pi I_n - \sum v_i T^i$. Then there is a homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over A with $\alpha(X) \equiv cX$ mod(degree 2) if and only if there is an element $\vartheta_c \in A_\sigma[\![T]\!]^{m\times n}$ such that $\eta_v c = \vartheta_c \eta_u$.

Remark Because the formal group law $\hat{F}(X, Y)$ with logarithm $f_h(X) = h(X) + \sum \pi^{-1} u_i \sigma_*^i f_h(X^{q^i}))$ is strictly isomorphic to the formal group law $F(X, Y)$ of (20.3.9), and similarly for $G(X, Y)$, we can extend Proposition (20.3.9) to cover also a description of all homomorphisms $\hat{F}(X, Y) \to \hat{G}(X, Y)$ where $\hat{f}(X)$ and $\hat{g}(X)$ satisfy the same type of functional equation as $f(X)$ and $g(X)$, respectively.

■ (20.3.10) **Corollary** The formal group laws $F(X, Y)$ and $G(X, Y)$ of Proposition (20.3.9) are strictly isomorphic iff ($m = n$ and) there exists an element $\vartheta \in A_\sigma[\![T]\!]^{m\times m}$ such that $\eta_u \vartheta = \eta_v$.

■ (20.3.11) **Corollary** Now suppose that A is the ring of integers of a discrete totally unramified valuation field K (in addition to the hypotheses of (20.3.1)), then the strict isomorphism classes of formal group laws of dimension m over A correspond bijectively to left associate classes of elements $\eta \in A_\sigma[\![T]\!]^{m\times m}$ of the form $\eta \equiv pI_m$ mod(degree 1).

Recall that two elements x, y in a ring R are called left associate if there is a unit $w \in R$ such that $x = wy$. This corollary follows immediately from (20.3.10) because in this case every formal group law over A is strictly isomorphic to a formal group with logarithm of the form $f(X) = X + \sum p^{-1} u_i \sigma_*^i f(X^{q^i})$, by Proposition (20.1.3).

■ (20.3.12) **Theorem** Let A be the ring of integers of a complete absolutely unramified discrete valuation field of characteristic zero and residue characteristic $p > 0$, and suppose there is an endomorphism σ: $K \to K$ such that

$\sigma(a) \equiv a^p \bmod(p)$ for all $a \in A$. Then the strict isomorphism classes of one dimensional formal group laws of height h over A correspond bijectively to elements of $A_\sigma[\![T]\!]$ of the form $p + \sum_{i=1}^{h} b_i T^i$, with $b_1, \ldots, b_{h-1} \in (p)$ and $b_h \in A^*$, the units of A. The (classes of) formal group laws corresponding to $p + \sum_{i=1}^{h} b_h T^i$ and $p + \sum_{i=1}^{h} \hat{b}_h T^i$ are isomorphic if and only if there is a unit $c \in A^*$ such that $b_i = c\hat{b}_i \sigma^i(c^{-1})$ for all $i = 1, \ldots, h$.

The first step in the proof of this theorem is the following twisted formal Weierstrass preparation lemma.

■ (20.3.13) **Lemma** Let A be a complete discrete valuation ring of residue characteristic $p > 0$ such that there exists an endomorphism $\sigma\colon K \to K$ and a power q of p such that $\sigma(a) \equiv a^q \bmod \pi A$ for all $a \in A$ (where K is the quotient field of A and π is a uniformizing element of A). Let $\eta = \pi + \sum_{i=1}^{\infty} b_i T^i$ be an element of $A_\sigma[\![T]\!]$ such that $b_i \in \pi A$ for $i = 1, \ldots, h-1$ and $b_h \in A^* = U(A)$. Then there is a unit $\vartheta \in A_\sigma[\![T]\!]$ such that $\vartheta\eta = \pi + \sum_{i=1}^{h} \hat{b}_i T^i$ with $\hat{b}_h \in A^*$ and $\hat{b}_i \in \pi A$ for $i = 1, \ldots, h-1$.

Proof Inductively we are going to construct elements $c_1(i), \ldots, c_h(i) \in A$ and units $\vartheta_i \in A_\sigma[\![T]\!]$ such that

$$c_j(i) \equiv c_j(i+1) \bmod \pi^i, \qquad c_j(1) \equiv b_j \bmod \pi \tag{20.3.14}$$

$$\vartheta_i \equiv 1 \bmod(\text{degree } 1), \qquad \vartheta_{i+1} \equiv \vartheta_i \bmod(\pi^i) \tag{20.3.15}$$

$$\vartheta_i \eta \equiv \pi + \sum_{j=1}^{h} c_j(i) T^j \bmod \pi^i \tag{20.3.16}$$

The first step is to take $c_1(1) = \cdots = c_{h-1}(1) = 0$ and $c_h(1) = b_h$ and $\vartheta_1 = b_h(\sum_{i=h}^{\infty} b_i T^{i-h})^{-1}$. (Note that $(\sum_{i=h}^{\infty} b_i T^{i-h})^{-1}$ exists in $A_\sigma[\![T]\!]$ because b_h is a unit.) We get $\vartheta_1 \eta \equiv b_h T^h \bmod(\pi)$ so that (20.3.16) for $i = 1$ is indeed satisfied. Now suppose we have found $c_1(n), \ldots, c_h(n)$ and ϑ_n such that (20.3.14)–(20.3.16) hold for $i = n$. To find the $c_j(n+1)$ we set $c_j(n+1) = c_j(n) + \pi^n d_j$, $j = 1, \ldots, h$ and $\vartheta_{n+1} = \vartheta_n + \pi^n \hat{\vartheta}$. These are to satisfy (20.3.16). Let

$$\vartheta_n \eta = \pi + \sum_{j=1}^{h} c_j(n) T^j + \pi^n \hat{\eta}$$

We find

$$\vartheta_{n+1}\eta = \pi + \sum_{j=1}^{h} c_j(n) T^j + \pi^n \hat{\eta} + \pi^n \hat{\vartheta}\eta \tag{20.3.17}$$

$$= \pi + \sum_{j=1}^{h} c_j(n+1) T^j + \pi^n \left(\hat{\eta} + \hat{\vartheta}\eta - \sum_{i=1}^{h} d_j T^j \right)$$

So we must choose d_j, $j = 1, \ldots, h$ and $\hat{\vartheta}$ such that mod(π)

$$\hat{\vartheta}\eta \equiv \sum_{i=1}^{h} d_j T^j - \hat{\eta} \tag{20.3.18}$$

Now $\eta \equiv \sum_{i=h}^{\infty} b_h T^h \bmod(\pi)$, and b_h is a unit, so choosing the d_j such that the right-hand side of (20.3.18) is $\equiv 0$ mod(degree $h+1$), we see that there is a $\hat{\vartheta}$ such that (20.3.18) holds and such that $\hat{\vartheta} \equiv 0$ mod(degree 1).

■(20.3.19) **Proof of Theorem (20.3.12)** Let $F(X, Y)$ be a one dimensional formal group law of height h over A. Because K is absolutely unramified, $F(X, Y)$ is strictly isomorphic to a formal group law with logarithm $f(X)$ of the form $f(X) = X + \sum_{i=1}^{\infty} p^{-1} u_i \sigma_*^i f(X^{p^i})$, i.e., $f(X) = \eta_u^{-1} p * i(X)$ for certain u_1, $u_2, \ldots \in A$. So we can assume that the logarithm of $f(X)$ is of this form. Now suppose that $u_1, u_2, \ldots, u_r \in (p)$. Then one proves easily (with induction using $pa_n = u_1 \sigma(a_{n-1}) + \cdots + u_{n-1}\sigma^{n-1}(a_1) + u_n$ if $f(X) = \sum a_n X^{p^n}$), that

$$f(X) \equiv u_{r+1} p^{-1} X^{p^{r+1}}$$

mod(1, degree $p^{r+1}+1$). It follows that $\mathrm{ht}(F(X, Y)) \geq r+1$ and $\mathrm{ht}\, F(X, Y) = r+1$ if u_{r+1} is unit. Since $F(X, Y)$ is of height h, we conclude that $u_1, \ldots, u_{h-1} \in (p)$ and $u_h \notin (p)$, i.e., u_h is a unit.

Now apply Lemma (20.3.13) and Proposition (20.3.9) to find a formal group law $G(X, Y)$ strictly isomorphic to $F(X, Y)$ whose logarithm $g(X)$ is equal to $g(X) = (\eta_v^{-1} p) * i(X)$ with $v_1, \ldots, v_{h-1} \in (p)$, v_h a unit, and $v_i = 0$ for $i \geq h$.

The next thing we have to prove (in view of (20.3.9)) is that if $\vartheta \in A_\sigma[\![T]\!]$ is such that

$$\vartheta\left(p + \sum_{i=1}^{h} b_i T^i\right) = p + \sum_{i=1}^{h} \hat{b}_i T^i, \qquad b_i, \hat{b}_i \in (p), \qquad b_h \text{ and } \hat{b}_h \text{ units}$$

then $\vartheta = 1$. More generally, let c be an element of A and consider the equation

$$\vartheta\left(p + \sum_{i=1}^{h} b_i T^i\right) = \left(p + \sum_{i=1}^{h} \hat{b}_i T^i\right) c \tag{20.3.20}$$

By Lemma (20.3.21) below, Eq. (20.3.20) implies that $\vartheta = c$, which concludes the proof of the theorem.

■(20.3.21) **Lemma** Let A, K, etc. be as in (20.3.1) and suppose π is not a zero divisor and $\bigcap_n \pi^n A = \{0\}$. Let η_u, η_v be the elements of $A_\sigma[\![T]\!]^{m\times m}$ and $A_\sigma[\![T]\!]^{n\times n}$, respectively, of the form

$$\eta_u = \pi + \sum_{i=1}^{h} u_i T^i, \qquad \eta_v = \pi + \sum_{i=1}^{h} v_i T^i \tag{20.3.22}$$

and suppose that u_h is an invertible matrix and $u_i \equiv 0 \bmod \pi$ for $i = 1, \ldots, h-1$. Let c be an $n \times m$ matrix and suppose that

$$\vartheta_c \eta_u = \eta_v c \tag{20.3.23}$$

for some $\vartheta_c \in A_\sigma[\![T]\!]^{n \times m}$. Then $\vartheta_c = c$.

Proof Write $\vartheta_c = \sum_{i=0}^{\infty} a_i T^i$, $a_i \in A^{n \times m}$. Comparing the coefficients of T^{i+h} for $i > 0$ on both sides of (20.3.23) we find the matrix equation

$$a_{i+h}\sigma^{i+h}(\pi) + a_{i+h-1}\sigma^{i+h-1}(u_1) + \cdots + a_{i+1}\sigma^{i+1}(u_{h-1}) + a_i\sigma^i(u_h) = 0 \tag{20.3.24}$$

Because u_h is an invertible matrix and $u_i \equiv 0 \bmod \pi$ for $i = 1, \ldots, h-1$, we see from (20.3.24) that $a_i \equiv 0 \bmod \pi$ for all $i > 0$. Using that in (20.3.24) we find $a_i \equiv 0 \bmod \pi^2$ for all $i > 0$, and by induction $a_i \equiv 0 \bmod \pi^n$ for all n, $i > 0$. Hence $a_i = 0$ for $i > 0$. Comparing the constant terms of (20.3.23) we also see that $a_0 = c$.

■ (20.3.25) **Corollary** Let $F(X, Y)$, $G(X, Y)$ be formal groups laws over A with logarithms $f(X) = \eta_u^{-1}\pi * i(X)$, $g(X) = \eta_v^{-1}\pi * i(X)$ where η_u and η_v are as in Lemma (20.3.21). Then there is a homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over A such that $\alpha(X) \equiv CX \bmod(\text{degree } 2)$ if and only if $C\eta_u = \eta_v C$.

In particular, this result gives us again the results on endomorphisms and homomorphisms of (higher dimensional) Lubin-Tate formal group laws which we obtained in (20.1.22) and (20.1.23).

■ (20.3.26) **Remarks** Let A be the ring of integers of a (not necessarily unramified) complete discrete valuation field K such that the conditions of (20.3.1) hold. Let $f(X) = \eta_u^{-1}\pi * i(X)$ for some sequence of elements $u_1, u_2, u_3, \ldots, \in A$ and let $F(X, Y)$ be the one dimensional formal group law with logarithm $f(X)$. Then $F(X, Y)$ is of infinite height if all u_i are in πA, and the height of $F(X, Y) = eri$ if $u_1, \ldots, u_{i-1} \in \pi A$ and u_i is a unit of A, where $q = p^r$ and e is the ramification index of K. (Recall that q is the number entering in $\sigma(a) \equiv a^q \bmod(\pi)$ and that q plays a role in the $*$ operation.) Both these facts follow easily from part (iv) of the functional equation lemma; cf. also (20.4.2). Using this we have a classification result for one dimensional formal group laws over A which are of functional equation type.

■ (20.3.27) **Warning** Let $u = (u_1, u_2, \ldots)$ be a series of elements of A and suppose for the moment that $p = \pi = q$ in the setting of (20.3.1). Then we clearly have two ways of associating a one dimensional formal group law to the sequence $u_1, u_2, \ldots$. First, we can use the functional equation lemma directly; i.e., we write

$$f(X) = X + \sum_{i=1}^{\infty} p^{-1}u_i\sigma_*^i f(X^{p^i}) \quad \text{and} \quad F(X, Y) = f^{-1}(f(X) + f(Y))$$

secondly, we can substitute u_i for V_i in the universal p-typical formal group law $F_V(X, Y)$ and its logarithm $f_V(X)$ to obtain a formal group law $F_u(X, Y)$ with logarithm $f_u(X)$. Both methods give, for varying u, up to strict isomorphism, all formal group laws over A. Yet these two methods are far from being the same or even equivalent. For example, if $v = (v_1, v_2, \ldots)$ is a second series of elements of A and $v_i \equiv u_i \bmod p$ for all i, then the reductions mod p of the formal group laws $F_u(X, Y)$ and $F_v(X, Y)$ are the same, $\bar{F}_u(X, Y) = \bar{F}_v(X, Y)$, but this is definitely not necessarily true for the two formal group laws with logarithms

$$f(X) = X + \sum_{i=1}^{\infty} p^{-1} u_i \sigma_*^i f(X^{p^i}) \quad \text{and} \quad \hat{f}(X) = X + \sum_{i=1}^{\infty} p^{-1} v_i \sigma_*^i \hat{f}(X^{p^i})$$

20.4 Homomorphisms and endomorphisms of formal group laws over rings of characteristic $p > 0$

We have already seen in 20.2 that functional equation techniques can be used to study homomorphisms and endomorphisms of formal group laws over characteristic $p > 0$ rings. In this subsection 20.4 we describe a general technique for dealing with these matters of which the "trick" used in 20.2 is a sort of deformed version, which works because the ring $A_\sigma[\![T]\!]$ in that case is commutative.

■ (20.4.1) The setting for this subsection 20.4 is the same as in 20.3. That is, we have a characteristic zero ring A, an element $\pi \in A$, such that $A/\pi A$ is a ring of prime characteristic $p > 0$ and there is an endomorphism $\sigma: K \to K$ such that $\sigma(a) = a^q \bmod \pi$ for all $a \in A$ where q is a certain (fixed) power of p, and $\sigma(\pi) = w\pi$ for a unit $w \in A^*$.

We shall need two lemmas. The first is a special case of part (iv) of the functional equation lemma; cf. Chapter II, 10.2. For the convenience of the reader (and author) we recall it explicitly.

■ (20.4.2) **Lemma** Let $u_1, u_2, \ldots$ be a sequence of elements of $A^{m \times m}$ and $f(X) = X + \sum_{i=1}^{\infty} \pi^{-1} u_i \sigma_*^i f(X^{q^i})$. Let $\alpha(X)$ and $\beta(X)$ be two m-tuples of power series in n variables with coefficients in A and K, respectively. Then we have

$$f(\alpha(X)) \equiv f(\beta(X)) \mod \pi^r \quad \Leftrightarrow \quad \alpha(X) \equiv \beta(X) \mod \pi^r$$

The second lemma that we shall need is of the same general nature.

■ (20.4.3) **Lemma** Let $f(X)$ be as in Lemma (20.4.2) and let $\vartheta \in A_\sigma[\![T]\!]^{n \times m}$ and let $\psi(X)$ be an m-tuple of power series in l variables. Then we have

$$\vartheta * (f \circ \psi)(X) \equiv (\vartheta * f) \circ \psi(X) \mod \pi$$

where the small circle denotes composition.

Proof By the additivity of the $*$ operation (cf. (20.3.3)) it suffices to show this for ϑ of the form $\vartheta = cT^i$. If $i = 0$, we have $\vartheta * (f \circ \psi)(X) = (\vartheta * f) \circ \psi(X)$.

So suppose $i > 0$. Then we have modulo π (writing $f(X) = \sum a_i X^{q^i}$)

$$(\vartheta * f) \circ \psi(X) = c\sigma^i_* f(\psi(X)^{q^i}) = c \sum_{j=1}^{\infty} \sigma^i(a_j)\psi(X)^{q^{i+j}}$$

$$\equiv c \sum_{j=1}^{\infty} \sigma^i(a_j)(\sigma^i_* \psi(X^{q^i}))^{q^j} = c\sigma^i_* f(\psi(X^{q^i})) = \vartheta * (f \circ \psi)(X)$$

because $\psi(X)^{q^i} \equiv \sigma^i{}_*\psi(X^{q^i}) \bmod \pi$ and hence $\psi(X)^{q^{i+j}} \equiv (\sigma^i_* \psi(X^{q^i}))^{q^j} \bmod \pi^{j+1}$ and because $\pi^j a_j \in A$. Q.E.D.

■ (20.4.4) **Theorem** Let A, K, p, q, σ, π be as in (20.4.1). Let $F(X, Y)$ and $G(X, Y)$ be the formal group laws over A with logarithms

$$f(X) = X + \sum_{i=1}^{\infty} \pi^{-1} u_i \sigma^i_* f(X^{q^i}), \qquad g(X) = X + \sum_{i=1}^{\infty} \pi^{-1} v_i \sigma^i_* g(X^{q^i})$$

$u_1, u_2, \ldots, \in A^{m \times m}$, $v_1, v_2, \ldots, \in A^{n \times n}$. Let ϑ be an element of $A_\sigma[\![T]\!]^{n \times m}$ and let $\eta_u = \pi - \sum_{i=1}^{\infty} u_i T^i$, $\eta_v = \pi - \sum_{i=1}^{\infty} v_i T^i$.

(i) Set $\alpha_\vartheta(X) = g^{-1}((\vartheta * f)(X))$, then $\alpha_\vartheta(X) \in A[\![X]\!]^m$ if and only if there is an $\eta_\vartheta \in A_\sigma[\![T]\!]^{n \times m}$ such that $\eta_\vartheta \eta_u = \eta_v \vartheta$.

(ii) If $\alpha_\vartheta(X) \in A[\![X]\!]^m$, then reducing modulo π we find a homomorphism $\bar{\alpha}_\vartheta(X)$: $\bar{F}(X, Y) \to \bar{G}(X, Y)$ (where $\bar{F}(X, Y)$ and $\bar{G}(X, Y)$ are the reductions modulo π of $F(X, Y)$ and $G(X, Y)$).

Let $n = m$ and $F(X, Y) = G(X, Y)$, and let us write $\mathscr{E}_m$ for the ring $A_\sigma[\![T]\!]^{m \times m}$.

(iii) If $\vartheta_1, \vartheta_2 \in \mathscr{E}_m$ and $\alpha_{\vartheta_1}(X), \alpha_{\vartheta_2}(X) \in A[\![X]\!]^m$, then

$$\bar{\alpha}_{\vartheta_1\vartheta_2}(X) = \bar{\alpha}_{\vartheta_1}(\bar{\alpha}_{\vartheta_2}(X))$$

(iv) If $\vartheta \in \mathscr{E}_m$ and $\alpha_\vartheta(X) \in A[\![X]\!]^m$, then $\bar{\alpha}_\vartheta(X) = 0$ iff $\vartheta \in \mathscr{E}_m \eta_u$.

(v) For each $\vartheta \in \mathscr{E}_m$ such that there is an $\eta_\vartheta \in \mathscr{E}_m$ with $\eta_u \vartheta = \eta_\vartheta \eta_u$ let Φ_ϑ: $\mathscr{E}_m \to \mathscr{E}_m$ be the right $\mathscr{E}_m$-module homomorphism $\eta \mapsto \eta_\vartheta \eta$. Then Φ_ϑ induces a homomorphism of right $\mathscr{E}_m$-modules $\mathscr{E}_m/\eta_u\mathscr{E}_m \to \mathscr{E}_m/\eta_u\mathscr{E}_m$, and this identifies the ring of all right $\mathscr{E}_m$-module endomorphisms of $\mathscr{E}_m/\eta_u\mathscr{E}_m$ with the subring of $\mathrm{End}_{A/\pi A}(\bar{F}(X, Y))$ consisting of the $\bar{\alpha}_\vartheta(X)$ with $\vartheta \in \mathscr{E}_m$ and $\alpha_\vartheta(X) \in A[\![X]\!]^m$.

(vi) Suppose that $p = q = \pi$ for the ingredients (20.4.1). Then $\mathrm{End}_{A/\pi A}(\bar{F}(X, Y))$ is isomorphic to the ring of all right $\mathscr{E}_m$-module endomorphisms of $\mathscr{E}_m/\eta_u\mathscr{E}_m$.

■ (20.4.5) **Proof of part (i) of Theorem (20.4.4)** Suppose there is an η_ϑ such that $\eta_\vartheta \eta_u = \eta_v \vartheta$. Then we have $\vartheta * f(X) = \vartheta * (\eta_u^{-1}\pi * i(X)) = (\vartheta\eta_u^{-1}\pi) * i(X) = (\eta_v^{-1}\eta_\vartheta \pi) * i(X) = (\eta_v^{-1}\pi\hat{\eta}_\vartheta) * i(X)$, where we have used (20.3.3). But according to (20.3.7) and the functional equation lemma

$\eta_v^{-1}\pi\hat{\eta}_\vartheta * i(X)$ satisfies the same type of functional equation as $g(X)$. Hence $g^{-1}(\vartheta * f(X))$ is integral. Conversely, if $g^{-1}(\vartheta * f(X))$ is integral, then (by the functional equation lemma and (20.3.7)) there is an $\hat{\eta}_\vartheta$ such that $(\vartheta * f(X)) = \eta_v^{-1}\pi\hat{\eta}_\vartheta * i(X)$. Let η_ϑ be such that $\eta_\vartheta \pi = \pi\hat{\eta}_\vartheta$, then $\eta_\vartheta \eta_u = \eta_v \vartheta$.

■(20.4.6) **Proof of part (ii) of Theorem (20.4.4)** Using Lemma (20.4.3), we have modulo π

$$\begin{aligned} g(\alpha_\vartheta(F(X, Y))) &= (\vartheta * f)(F(X, Y)) \equiv \vartheta * (f(F(X, Y)) = \vartheta * (f(X) + f(Y)) \\ &= (\vartheta * f(X)) + (\vartheta * f(Y)) \\ &= g(\alpha_\vartheta(X)) + g(\alpha_\vartheta(Y)) = g(G(\alpha_\vartheta(X), \alpha_\vartheta(Y))) \end{aligned}$$

and by Lemma (20.4.2) this implies $\alpha_\vartheta F(X, Y) \equiv G(\alpha_\vartheta(X), \alpha_\vartheta(Y))$.

■(20.4.7) **Proof of part (iii) of Theorem (20.4.4)** Using Lemma (20.4.3), we have modulo π

$$\begin{aligned} f(\alpha_{\vartheta_1}(\alpha_{\vartheta_2}(X))) &= (\vartheta_1 * f)(f^{-1}(\vartheta_2 * f(X))) \equiv \vartheta_1 * (\vartheta_2 * f(X)) \\ &= \vartheta_1 \vartheta_2 * f(X) = f(\alpha_{\vartheta_1\vartheta_2}(X)) \end{aligned}$$

By Lemma (20.4.2) it follows that $\bar{\alpha}_{\vartheta_1}(\bar{\alpha}_{\vartheta_2}(X)) = \bar{\alpha}_{\vartheta_1\vartheta_2}(X)$.

■(20.4.8) **Proof of part (iv) of Theorem (20.4.4)** We have, using Lemma (20.4.2),

$$\begin{aligned} \bar{\alpha}_\vartheta(X) = 0 &\Leftrightarrow \vartheta * f(X) \equiv 0 \mod \pi \\ &\Leftrightarrow \vartheta * (\eta_u^{-1}\pi * i(X)) \equiv 0 \mod \pi \\ &\Leftrightarrow \vartheta\eta_u^{-1}\pi * i(X) \equiv 0 \mod \pi \\ &\Leftrightarrow \vartheta\eta_u^{-1}\pi \equiv 0 \mod \pi \\ &\Leftrightarrow \vartheta\eta_u^{-1} \in \mathscr{E}_m \\ &\Leftrightarrow \vartheta \in \mathscr{E}_m\eta_u \end{aligned}$$

■(20.4.9) **Proof of part (v) of Theorem (20.4.4)** We have

$$\eta_\vartheta \eta_u \mathscr{E}_m = \eta_u \vartheta \mathscr{E}_m \subset \eta_u \mathscr{E}_m$$

Conversely, if Φ: $\mathscr{E}_m/\eta_u\mathscr{E}_m \to \mathscr{E}_m/\eta_u\mathscr{E}_m$ is a right $\mathscr{E}_m$-module homomorphism, let $\eta = \Phi(1)$. Then we have $\eta\eta_u \in \eta_u\mathscr{E}_m$ hence $\eta\eta_u = \eta_u \vartheta$ for a certain ϑ proving that $\eta = \eta_\vartheta$ for a certain ϑ. Finally, $\Phi_\vartheta = 0 \Leftrightarrow \eta_\vartheta \in \eta_u\mathscr{E}_m \Leftrightarrow \eta_\vartheta\eta_u \in \eta_u\mathscr{E}_m\eta_u \Leftrightarrow \eta_u\vartheta \in \eta_u\mathscr{E}_m\eta_u \Leftrightarrow \vartheta \in \mathscr{E}_m\eta_u \Leftrightarrow \bar{\alpha}_\vartheta(X) = 0$ (where we have used part (iv)) and that η_u, being a unit in $K_\sigma[\![T]\!]^{m\times m}$, is not a zero divisor in $\mathscr{E}_m$).

■(20.4.10) **Proof of part (vi) of Theorem (20.4.4)** Let $\bar{\alpha}(X)$ be an endomorphism of $F(X, Y)$. Let $\alpha(X)$ be any m-tuple of power series that reduces

mod p to $\alpha(X)$. Then we have $\alpha(F(X, Y)) \equiv F(\alpha(X), \alpha(Y)) \bmod p$ and hence by Lemma (20.4.2)

$$f(\alpha(F(X, Y)) \equiv f(F(\alpha(X), \alpha(Y))) = f(\alpha(X)) + f(\alpha(Y)) \mod p$$

By Lemma (20.4.12) below it follows that

$$f(\alpha(X)) \equiv \vartheta * f(X) \mod p$$

for some $\vartheta \in \mathscr{E}_m$. By Lemma (20.4.2) this implies that $\alpha(X) \equiv f^{-1}(\vartheta * f(X)) \bmod p$ and hence $\bar{\alpha}(X) = \bar{\alpha}_\vartheta(X)$.

We have now proved Theorem (20.4.4) modulo Lemma (20.4.12). To prove this lemma we need a sublemma.

■ (20.4.11) **Sublemma** Let A be a characteristic zero ring and let $\alpha(X)$ be a homogeneous form in m variables of degree r with coefficients in $K = A \otimes_{\mathbf{Z}} \mathbf{Q}$. Then if $\alpha(X) + \alpha(Y) \equiv \alpha(X + Y) \bmod pA$ we have $r = p^h$ for some $h \in \mathbf{N}$ and $\alpha(X) \equiv \sum_{i=1}^m c_i X_i^{p^h} \bmod pA$ for certain $c_i \in A$.

Proof Write $\alpha(X) = \sum_{|\mathbf{n}|=r} d_{\mathbf{n}} X^{\mathbf{n}}$, where $\mathbf{n}$ is a multi-index of length m and $d_{\mathbf{n}} \in K$. Suppose there is an $\mathbf{n} = (n_1, n_2, \ldots, n_m)$ with $d_{\mathbf{n}} \neq 0$ and with $\mathbf{n}$ not of the form $re(j)$ for some $j \in \{1, \ldots, m\}$. Up to a permutation we can assume that $n_1 \neq 0$, $n_2 \neq 0$. Then $\alpha(X + Y)$ contains a term $d_{\mathbf{n}} X_1^{n_1} Y_2^{n_2} \cdots Y_m^{n_m}$ proving that $r_{\mathbf{n}} \equiv 0 \bmod p$ for all $\mathbf{n}$ not of the type $re(j)$. So we have

$$\alpha(X + Y) \equiv \sum_{i=1}^m d_{re(i)}(X_i + Y_i)^r \equiv \sum_{i=1}^m d_{re(i)}(X_i^r + Y_i^r) \mod p$$

The greatest common multiple of $\{\binom{r}{1}, \ldots, \binom{r}{r-1}\}$ is $v(r)$. It follows that $v(r)d_{re(i)} \equiv 0 \bmod pA$. And $v(r)$ is a unit in A/pA unless r is a power of p, and then $v(r) = p$. This proves the sublemma.

■ (20.4.12) **Lemma** Let A, K, π, p, q, σ be as in (20.4.1) and suppose that $\pi = p = q$. Then if $\alpha(X) \in K[\![X]\!]^m$, $\alpha(0) = 0$, and $\alpha(F(X, Y)) \equiv \alpha(X) + \alpha(Y) \bmod pA$ where $F(X, Y)$ is a formal group law over A with logarithm $f(X) = X + \sum p^{-1} u_i \sigma_*^i f(X^{p^i})$, $u_1, u_2, \ldots, \in A^{m \times m}$. Then there is a $\vartheta \in A_\sigma[\![X]\!]^{m \times m} = \mathscr{E}_m$ such that $\alpha(X) \equiv \vartheta * f(X) \bmod pA$.

Proof First notice that if $\vartheta \in A_\sigma[\![X]\!]^{m \times m}$, then by Lemma (20.4.3)

$$(\vartheta * f)(F(X, Y))$$

$$\equiv \vartheta * (f(F(X, Y)) = \vartheta * (f(X) + f(Y)) = (\vartheta * f)(X) + (\vartheta * f)(Y)$$

So if we change $\alpha(X)$ to $\hat{\alpha}(X) = \alpha(X) - \vartheta * f(X)$ for any $\vartheta \in \mathscr{E}_m$, we (again) obtain an $\hat{\alpha}(X)$ that satisfies $\hat{\alpha}(F(X, Y)) \equiv \hat{\alpha}(X) + \hat{\alpha}(Y) \bmod pA$. We now proceed by induction.

Write $\alpha(X) = \sum_{n=1}^\infty \alpha_n(X)$ where $\alpha_n(X)$ is homogeneous of degree n. Let $r \in \mathbf{N}$ be the smallest natural number such that $\alpha_r(X) \not\equiv 0 \bmod pA$. Then because $\alpha(F(X, Y)) \equiv \alpha(X) + \alpha(Y) \bmod pA$ and $F(X, Y) \equiv X + Y$

mod(degree 2) we must have $\alpha_r(X + Y) \equiv \alpha_r(X) + \alpha_r(Y) \bmod pA$. By sublemma (20.4.11) this means that $\alpha_r(X) \equiv \sum_{i=1}^{m} a_i X_i^{p^h} \bmod(pA)$, $r = p^h$ for some $h \in \mathbf{N}$ and $a_i \in A$. Now let $\hat{\alpha}(X) = \alpha(X) - \vartheta * f(X)$ with $\vartheta = cT^h$ where c is the diagonal matrix with entries $a_1, \ldots, a_m$. Then $\hat{\alpha}(X)$ satisfies (as we remarked above) the same condition as $\alpha(X)$ and $\hat{\alpha}(X) \equiv 0 \bmod(pA$, degree $r + 1)$. Continuing with induction we see that there is a ϑ such that $\alpha(X) \equiv \vartheta * f(X) \bmod pA$.

20.5 Local–global results

Essentially this result says that one knows a formal group law over a characteristic zero ring A iff one knows it for every prime number p over $A \otimes \mathbf{Z}_{(p)}$. In the case that A is the ring of integers of a number field K, then there is a refinement where the place of the $A \otimes \mathbf{Z}_{(p)}$ is taken by the rings of integers A_v of the local completions K_v for every nonarchimedean valuation v. The two theorems are:

■ (20.5.1) **Theorem** Let A be a characteristic zero ring.

(i) If $F(X, Y)$ and $G(X, Y)$ are two formal group laws over A, then they are strictly isomorphic over A if and only if they are strictly isomorphic over $A \otimes \mathbf{Z}_{(p)}$ for all prime numbers p.

(ii) Suppose we have given for every prime number p an m-dimensional formal group $F_{(p)}(X, Y)$ over $A \otimes \mathbf{Z}_{(p)}$. Then there exists an m-dimensional formal group law $F(X, Y)$ over A that is strictly isomorphic over $A \otimes \mathbf{Z}_{(p)}$ to $F_{(p)}(X, Y)$ for every prime number p.

■ (20.5.2) **Theorem** Let A be the ring of integers of a number field K. For each nonarchimedean valuation v let A_v be the ring of integers of the local completion K_v of K.

(i) If $F(X, Y)$ and $G(X, Y)$ are two formal group laws over A, then they are strictly isomorphic over A if and only if they are strictly isomorphic over A_v for all nonarchimedean valuations v of K.

(ii) Suppose we have given for every nonarchimedean valuation v an m-dimensional formal group law $F_{(v)}(X, Y)$ over A_v. Then there exists an m-dimensional formal group law $F(X, Y)$ over A that is strictly isomorphic to $F_{(v)}(X, Y)$ over A_v for all nonarchimedean valuations v.

■ (20.5.3) **Proof of Theorem (20.5.1)**

(i) The m-dimensional formal group laws $F(X, Y)$ and $G(X, Y)$ are strictly isomorphic if and only if the power series $g^{-1}(f(X))$ has its coefficients in A, where $f(X)$ and $g(X)$ are the logarithms of $F(X, Y)$, $G(X, Y)$. By sublemma (17.6.6) this is the case if and only if $g^{-1}(f(X)) \in A \otimes \mathbf{Z}_{(p)}[\![X]\!]$ for all prime numbers p.

(ii) Because $A \otimes \mathbf{Z}_{(p)}$ is a $\mathbf{Z}_{(p)}$-algebra we can assume that all the $F_{(p)}(X, Y)$ are p-typical formal group laws. Let $v_p = (v_{1,p}, v_{2,p}, \ldots)$ be a sequence of $m \times m$ matrices such that $F_{(p)}(X, Y) = F_{v_p}(X, Y)$, where $F_{v_p}(X, Y)$ is the formal group law obtained from the universal p-typical formal group law $F_V(X, Y)$ over $\mathbf{Z}[V]$ by substituting $v_{i,p}$ for V_i, $i \in \mathbf{N}$. Up to strict isomorphism we can assume that the matrices $v_{i,p}$ have their coefficients in A and not just in $A \otimes \mathbf{Z}_{(p)}$. Indeed suppose that i is the smallest natural number such that $v_{i,p} \notin A^{m \times m}$. Then there exists a $t_i \in A \otimes \mathbf{Z}_{(p)}^{m \times m}$ and a $\bar{v}_{i,p} \in A^{m \times m}$ such that $\bar{v}_{i,p} = v_{i,p} + pt_i$. (Let $v_{i,p} = n^{-1}(\hat{v}_{i,p})$, $(n, p) = 1$, $\hat{v}_{i,p} \in A^{m \times m}$, take $r, s \in \mathbf{Z}$ such that $ps + rn = 1$; take $\bar{v}_{i,p} = r\hat{v}_{i,p}$, $t_i = -n^{-1}s\hat{v}_{i,p}$.) Applying the isomorphism $\alpha_{v_p, t_p}(X)$ to $F_{v_p}(X, Y)$ with $t_p = (t_{p,1}, t_{p,2}, \ldots)$, $t_{p,j} = 0$ if $i \neq j$, $t_{p,i} = t_i$, we find an isomorphic formal group law $F_{\bar{v}}(X, Y)$ with $\bar{v}_j = v_{p,j}$ for $j < i$, $\bar{v}_i = \bar{v}_{p,i}$.) Now let $H_U(X, Y)$ be the universal m-dimensional formal group law over $\mathbf{Z}[U]$. Substitute $U_{p^i} = v_{p,i}$ for all prime number powers p^i and $U(i, \mathbf{n}) = 0$ for all $\mathbf{n}$ not of the form $p^i\mathbf{e}(j)$. Let $F(X, Y)$ be the formal group law over A thus obtained. Then $F(X, Y)$ is strictly isomorphic to $F_{v_p}(X, Y)$ over $A \otimes \mathbf{Z}_{(p)}$ because for each prime number p, $H_U(X, Y)$ is strictly isomorphic to $F_V(X, Y)$ over $\mathbf{Z}_{(p)}[U]$ if one identifies V_i with U_{p^i}, $i = 1, 2, \ldots$ (cf. Chapter II, (16.4.15) and (16.4.14)).

■ (20.5.4) **Remark** Part (ii) of Theorem (20.5.1) also holds if A is not necessarily of characteristic zero; in fact this hypothesis was not used in the proof of part (ii) given above.

To prove Theorem (20.5.2) we need the strong approximation theorem of algebraic number theory. For the convenience of the reader we state it here explicitly in the form in which we shall use it.

■ (20.5.5) **Strong approximation theorem** Let $\mathfrak{S}$ be a finite set of nonarchimedean valuations on a number field K with ring of integers A and for each $v \in \mathfrak{S}$, let a_v be an element of K_v, the completion of K with respect to v. For each $v \in \mathfrak{S}$, choose an $r_v \in \mathbf{N}$. Then there exists an $a \in K$ such that $v(a - a_v) \geq r_v$ for all $v \in \mathfrak{S}$ and $v(a) \geq 0$ for all $v \notin \mathfrak{S}$. (Note that if $a_v \in A_v$, the ring of integers of K_v, for all $v \in \mathfrak{S}$, then $a \in A$.)

■ (20.5.6) **Proof of Theorem (20.5.2)**

(i) trivial; cf. the proof of part (i) of Theorem (20.5.2).

(ii) As in (20.5.3) we can assume that the $F_{(v)}(X, Y)$ are all p-typical formal group laws. We are going to obtain $F(X, Y)$ by substituting inductively suitable values for the $U(i, \mathbf{n})$ in the universal formal group law $H_U(X, Y)$ over $\mathbf{Z}[U]$. Suppose we have already found elements $a(i, n) \in A$ for $|\mathbf{n}| \leq n$ and power series $\alpha_{(v),n}(X)$ such that

$$(20.5.7) \quad F_{(n)}(X, Y) - \alpha_{(v),n}^{-1}(F_{(v)}(\alpha_{(v),n}(X), \alpha_{(v),n}(Y))) \equiv 0 \mod(\text{degree } n)$$

where $F_{(n)}(X, Y)$ is the formal group law obtained by substituting $a(i, \mathbf{n})$ for $U(i, \mathbf{n})$ for $|\mathbf{n}| < n$ and $U(i, \mathbf{n}) = 0$ for $|\mathbf{n}| \geq n$.

By the comparison lemma (Chapter II, Corollary (11.4.2)) there exist m-tuples of homogeneous forms $\Gamma_{(v)}(X)$ and $m \times m$ matrices $M_{(v)}$ such that the differences (20.5.7) are mod(degree $n+1$) equal to

$$\Gamma_{(v)}(X) + \Gamma_{(v)}(Y) - \Gamma_{(v)}(X+Y) + M_{(v)}(v(n)^{-1}(X^n + Y^n - (X+Y)^n))$$

If n is not a power of a prime number, then $v(n) = 1$, and we take $a(i, \mathbf{n}) = 0$ for all $\mathbf{n}$ with $|\mathbf{n}| = n$ and let $\alpha_{(v),n+1}(X) = \alpha_{(v),n}(X) + \Gamma_{(v)}(X) + M_{(v)}X^n$. Then (20.5.7) holds with $n+1$ instead of n. Now suppose that $n = p^r$ for a prime number p and $r \in \mathbf{N}$. Then $v(n) = p$. Let $\mathfrak{S}$ be the set of all valuations v "dividing" p (i.e., for which $v(p) > 0$). By the strong approximation theorem (20.5.5) there exists a matrix a with coefficients in A such that $a \equiv M_{(v)} \bmod(pA_v)$ for all $v \in \mathfrak{S}$. Let $N_{(v)} = p^{-1}(M_{(v)} - a)$. Now we take

$$a(i, ne(j)) = a_{ij} \qquad \text{for} \quad i = 1, \ldots, m; \quad j = 1, \ldots, m$$

and

$$\alpha_{(v),n+1}(X) = \alpha_{(v),n}(X) + \Gamma_{(v)}(X) + N_{(v)}X^n \qquad \text{for} \quad v \in \mathfrak{S}$$

$$\alpha_{(v),n+1}(X) = \alpha_{(v),n}(X) + \Gamma_{(v)}(X) + p^{-1}M_{(v)}X^n + aX^n \qquad \text{for} \quad v \notin \mathfrak{S}$$

then (20.5.7) holds with $n+1$ instead of n for all v. To see this use, e.g., formulas (11.4.1)–(11.4.3) of Chapter II. By induction this completes the proof.

21 Formal A-Modules

This section studies formal A-modules, that is, roughly speaking, formal group laws over A-algebras B admitting A as a ring of endomorphisms. More precisely, the study of formal A-modules is begun in this section; more results will appear later, notably in Sections 22–25 and in Chapter V, Sections 29, 30.

We give the definition of "formal A-module" for m-dimensional formal group laws, but, immediately after in this section all formal group laws will be of dimension one. This is more a convenience than a necessity for the development of the theory.

21.1 Definitions, examples, and elementary properties of formal A-modules

■ (21.1.1) Let A be a ring. If B is an A-algebra, we let $A \to B^{m \times m}$ be the (structural) ring homomorphism $a \mapsto aI_m$, where I_m is the identity matrix of $B^{m \times m}$. Given an m-dimensional formal group law $F(X, Y)$ over B, then J: $\mathrm{End}_B(F(X, Y)) \to B^{m \times m}$ denotes the Jacobian ring homomorphism that assigns to every $\alpha(X) \in \mathrm{End}_B(F(X, Y))$ the Jacobian matrix of $\alpha(X)$, that is, the matrix $M \in B^{m \times m}$ such that $\alpha(X) \equiv MX$ mod(degree 2).

■ (21.1.2) **Definitions** An m-dimensional formal A-module over an A-algebra B consists of an m-dimensional commutative formal group law over B together with a homomorphism of rings $\rho_F\colon A \to \mathrm{End}_B(F(X, Y))$ such that the following diagram commutes

(21.1.3)
$$\begin{array}{ccc} A & \xrightarrow{\rho_F} & \mathrm{End}_B(F(X, Y)) \\ & \searrow & \downarrow J \\ & & B^{m \times m} \end{array}$$

Note that every m-dimensional formal group law over a ring B carries a unique structure of a formal $\mathbf{Z}$-module.

A homomorphism between two formal A-modules over B is a homomorphism $\alpha(X)\colon F(X, Y) \to G(X, Y)$ of the formal group laws $F(X, Y)$, $G(X, Y)$ over B such that $\alpha(X) \circ \rho_F(a) = \rho_G(a) \circ \alpha(X)$ for all $a \in A$. A (strict) isomorphism of two formal A-modules over B is a (strict) isomorphism of formal group laws over B, $\alpha(X)\colon F(X, Y) \to G(X, Y)$, such that $\alpha(X) \circ \rho_F(a) = \rho_G(a) \circ \alpha(X)$ for all $a \in A$.

■ (21.1.4) **Remarks**

(i) If B is a characteristic zero ring and $F(X, Y)$ is a formal group law over B, then there is—if it exists—only one possible formal A-module structure on $F(X, Y)$, viz., $\rho_F(a) = f^{-1}(aI_m f(X)) = f^{-1}(af(X))$ where $f(X)$ is the logarithm of $F(X, Y)$. But if B is not of characteristic zero, there may exist—at least a priori—more than one formal A-module structure on $F(X, Y)$; i.e., there may be two or more different homomorphisms $\rho_F\colon A \to \mathrm{End}_B(F(X, Y))$ such that diagram (21.1.3) is commutative. And in fact this happens; cf., e.g., Examples (21.1.8) and (21.1.10). See also Theorem (21.6.2), however, and the last paragraph of (21.8.1) in connection with Remark (21.1.14).

(ii) We also note that if B is of characteristic zero and $F(X, Y)$, $G(X, Y)$ are two formal A-modules over B then every homomorphism of the formal group laws $\alpha(X)\colon F(X, Y) \to G(X, Y)$ is automatically a homomorphism of the formal A-modules $F(X, Y)$, $G(X, Y)$. Indeed, if $f(X)$ and $g(X)$ are the logarithms of $F(X, Y)$ and $G(X, Y)$, then $\alpha(X)$ is necessarily of the form $\alpha(X) = g^{-1}(Mf(X))$ for some matrix M. So we have

$$\begin{aligned} \alpha(X) \circ \rho_F(a)(X) &= \alpha(X) \circ f^{-1}(aI_m f(X)) = g^{-1}(Maf(X)) \\ &= g^{-1}(ag(X)) \circ g^{-1}(Mf(X)) = \rho_g(a)(X) \circ \alpha(X). \end{aligned}$$

This is not true in general if B is not of characteristic zero.

■ (21.1.5) From here through the end of Section 21 all formal groups laws and formal A-modules will be one dimensional and commutative.

■ (21.1.6) **Example** Let A be the ring of integers of a finite extension K of $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$. Let π be a uniformizing element of A, $q = \#(A/\pi A)$, the number of elements in the residue field of K. Let $F(X, Y)$ over A be the Lubin–Tate formal

group law with logarithm $f(X) = X + \pi^{-1}f(X^q)$; then as we have seen $f^{-1}(af(X))$ is a power series with coefficients in A for all $a \in A$ so that $a \mapsto f^{-1}(af(X))$ defines a formal A-module structure on $F(X, Y)$ over A. Reducing everything modulo π, we find a formal A-module $F(X, Y)$ over $k = A/\pi A$.

■ (21.1.7) **Example** Let A be any ring. Then $\rho(a) = aX$ defines a formal A-module structure on the additive formal group law over any A-algebra B. We shall call this the additive formal A-module.

(21.1.8) **Example** Let $A = \mathbf{F}_p[t]$ and define ρ: $A \to \mathrm{End}_A(\hat{\mathbf{G}}_a(X, Y))$ by $t \mapsto tX + X^p$, $n \mapsto nX$ for $n \in \mathbf{F}_p$. Then ρ defines a formal A-module structure on $\hat{\mathbf{G}}_a(A, Y)$ not isomorphic to the additive one.

(21.1.9) **Example** Let $A = \mathbf{Z}_p[t]$. We are going to prove that the only formal group law over $\mathbf{Z}_p[t]$ that admits a formal A-module structure is the additive one. The ring A is a characteristic zero $\mathbf{Z}_{(p)}$-algebra that admits an endomorphism σ: $A \to A$ such that $\sigma(a) \equiv a^p \bmod pA$ for all $a \in A$, viz. σ: $t \mapsto t^p$. It follows from Proposition (20.1.3) and Corollary (20.1.5) that every formal group law $F(X, Y)$ over A is strictly isomorphic to one with a logarithm of the type

$$f(X) = X + \sum_{i=1}^{\infty} p^{-1}v_i(\sigma_*^i)f(X^{p^i})$$

for certain $v_i \in A$. By the results of (20.3.9) it follows that there is an endomorphism $\alpha(X)$ of $F(X, Y)$ with $\alpha(X) \equiv tX \bmod(\text{degree } 2)$ if and only if there is an element $\vartheta_t \in A_\sigma[\![T]\!]$ such that

$$(p - v_1 T - v_2 T^2 - \cdots)t = \vartheta_t(p - v_1 T - v_2 T^2 - \cdots)$$

Writing $\vartheta_t = a_0 + a_1 T + a_2 T^2 + \cdots$, we find

$$\begin{aligned} pa_0 &= pt \\ -v_1 t^p &= -a_0 v_1 + pa_1 \\ -v_2 t^{p^2} &= -a_0 v_2 - a_1 \sigma(v_1) + pa_2 \\ -v_3 t^{p^3} &= -a_0 v_3 - a_1 \sigma(v_2) - a_2 \sigma^2(v_1) + pa_3 \\ &\vdots \end{aligned}$$

which gives $a_0 = t$ and then inductively $p \mid v_1$, $p \mid v_2$, ..., which in turn means that $f(X) \in A[\![X]\!]$ so that $F(X, Y)$ is strictly isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ over A.

■ (21.1.10) **Example** The example (21.1.8) is a kind of trivial example of a nontrivial formal A-module structure. It is not at all clear that there exist, e.g., nontrivial formal A-module structures on $\hat{\mathbf{G}}_a(X, Y)$ over A for A an arbitrary field of characteristic p. They do exist though and in abundance as the following example shows. (Later we shall prove that they are all isomorphic.)

Let A be any ring of characteristic $p > 0$, p a prime number. Let $T_1, T_2, \ldots$ be

a set of indeterminates. We now define power series $\rho(a, T)(X)$ for every $a \in A$ by the formulas

$$\rho(a, T)(X) = y_0(a)X + y_1(a)X^p + y_2(a)X^{p^2} + \cdots$$

$$y_0(a) = a$$

$$y_n(a) = T_1(y_{n-1}(a))^p + T_2(y_{n-2}(a))^{p^2} + \cdots + T_n(y_0(a))^{p^n} - T_n a$$

so the first few $y_i(a)$ are respectively

$$y_0(a) = a$$

$$y_1(a) = T_1(a^p - a)$$

$$y_2(a) = T_1 T_1^p(a^{p^2} - a^p) + T_2(a^{p^2} - a)$$

$$y_3(a) = T_1 T_1^p T_1^{p^2}(a^{p^3} - a^{p^2}) + T_1 T_2^p(a^{p^3} - a^p) + T_2 T_1^{p^2}(a^{p^3} - a^{p^2}) + T_3(a^{p^3} - a)$$

(The resemblance to the kind of formula we have seen in dealing with the universal (functional equation) formal groups law $F_V(X, Y)$ is not an accident.)

We claim that

$$\rho(a, T)(X) + \rho(b, T)(X) = \rho(a + b, T)(X) \tag{21.1.11}$$

$$\rho(a, T)(\rho(b, T)(X)) = \rho(ab, T)(X) \tag{21.1.12}$$

so that $\rho(a, T)$: $A \to A[T_1, T_2, \ldots][\![X]\!]$ is a sort of Artin–Hasse exponential map. This particular Artin–Hasse-like exponential map does not, however, seem to fit into the general framework of Artin–Hasse-like exponential maps associated to formal group laws which we shall discuss in Section 25.

We now proceed to prove (21.1.11) and (21.1.12). Formula (21.1.11) is trivial because A is of characteristic p. (Prove via induction that $y_n(a + b) = y_n(a) + y_n(b)$.) Formula (21.1.12) is also proved by induction. The coefficient of X^{p^n} in $\rho_F(a)(\rho_F(b)(X))$ is equal to

$$y_0(a)y_n(b) + y_1(a)(y_{n-1}(b))^p + \cdots + y_{n-1}(a)(y_1(b))^{p^{n-1}} + y_n(a)(y_0(b))^{p^n}$$

$$= ay_n(b) - T_1 a(y_{n-1}(b))^p - \cdots - T_n a(y_0(b))^{p^n} + \sum_{i=1}^{n} (y_i(a) + T_i a)(y_{n-i}(b))^{p^i}$$

$$= -abT_n + \sum_{i=1}^{n} \sum_{k=1}^{i} T_k(y_{i-k}(a))^{p^k}(y_{n-i}(b))^{p^i}$$

$$= -abT_n + \sum_{i=1}^{n} \sum_{k=1}^{i} T_k(y_{i-k}(a)y_{n-i}(b)^{p^{i-k}})^{p^k}$$

$$= -abT_n + \sum_{k=1}^{n} T_k y_{n-k}(ab)^{p^k} = y_n(ab)$$

(The induction hypothesis has been used in getting from the fourth to the fifth expression.) This proves (21.1.12).

One now obtains a host of nontrivial formal A-module structures on $\hat{\mathbf{G}}_a(X, Y)$ by specifying the T_i to be various elements of A. For example, taking $T_i = 0$ for all $i \neq h$ and $T_h = 1$, one finds a formal A-module structure on $F(X, Y) = \hat{\mathbf{G}}_a(X, Y)$ over A for which $\rho_F(a)(X)$ is equal to

$$\rho_F(a)(X) = aX + (a^{p^h} - a)X^{p^h} + (a^{p^{2h}} - a^{p^h})X^{p^{2h}} + \cdots \tag{21.1.13}$$

To conclude this section we remark

■ (21.1.14) **Remark** Let A be a ring of characteristic $p > 0$ and let $F(X, Y)$ be a formal A-module over an A-algebra B. Then, as a formal group law, $F(X, Y)$ is strictly isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ over B.

Indeed, because $p = 0$ in B we must have $0 = \rho_F(p)(X) = \rho_F(1)(X) +_F \cdots +_F \rho_F(1)(X) = X +_F \cdots +_F X = [p]_F(X)$. Hence, as a formal group law, $F(X, Y)$ is strictly isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ over B by Corollary (5.7.6) of Chapter I.

21.2 Universal formal A-modules (existence)

■ (21.2.1) **Definition** Let A be a ring. A universal formal A-module is a formal A-module $F^u(X, Y)$ over a certain A-algebra L_A such that for every formal A-module $F(X, Y)$ over an A-algebra B, there is a unique homomorphism of A-algebras $\phi: L_A \to B$ such that $\phi_* F^u(X, Y) = F(X, Y)$ and $\phi_*(\rho_{F^u}(a)(X)) = \rho_F(a)(X)$ for all $a \in A$.

■ (21.2.2) It is easy to check that universal formal A-modules exist. This is done as follows. Write $F(X, Y) = X + Y + \sum C_{ij} X^i Y^j$ and $\rho_F(a) = aX + D_{2,a}X^2 + D_{3,a}X^3 + \cdots$ where the $C_{i,j}$ and the $D_{i,a}$ are indeterminates for all i, $j \in \mathbf{N}$ and $a \in A$. The requirements that $F(X, Y)$ be associative and commutative, that the $\rho_F(a)$ are endomorphisms, and that $a \mapsto \rho_F(a)$ is a ring homomorphism define certain equations between the $C_{i,j}$ and $D_{i,a}$, viz. those expressing that the following power series identities hold:

$$F(F(X, Y), Z) = F(X, F(Y, Z)), \qquad F(X, Y) = F(Y, X)$$

$$F(\rho_F(a)(X), \rho_F(a)(Y)) = \rho_F(a)(F(X, Y)) \tag{21.2.3}$$

$$\rho_F(a)(\rho_F(b)(X)) = \rho_F(ab)(X), \qquad \rho_F(a + b)(X) = F(\rho_F(a)(X), \rho_F(b)(X))$$

$$F(\rho_F(-a)(X), \rho_F(a)(X)) = 0, \qquad \rho_F(1)(X) = X, \qquad \rho_F(0)(X) = 0$$

Now let $L_A = A[C_{i,j}; D_{i,a}]/I$ where I is the ideal generated by the elements of $A[C_{i,j}; D_{i,a}]$, which must be zero for (21.2.3) to hold. The universal formal A-module is now

$$F^u(X, Y) = X + Y + \sum \phi(C_{ij}) X^i Y^j, \qquad \rho_{F^u}(a)(X) = aX + \phi(D_{2,a})X^2 + \cdots$$

where $\phi: A[C_{ij}; D_{i,a}] \to L_A$ is the natural projection.

Give $C_{i,j}$ degree $i + j - 1$, $D_{i,a}$ degree $i - 1$, and X and Y degree -1. Then all elements of $A[C_{ij}; D_{i,a}][\![X, Y, Z]\!]$ occurring in (21.2.3) are of degree -1. It follows that I is a graded ideal and that L_A is a graded ring.

Recall that for each $n \in \mathbf{N}$ we have defined $C_n(X, Y) = v(n)^{-1}(X^n + Y^n - (X + Y)^n)$ and that $C_n(X, Y)$ is a primitive polynomial; recall also that $v(n) = 1$ if n is not a power of a prime number or $n = 1$ and $v(n) = p$ if $n > 1$ and n is a power of the prime number p. The formal A-module version of the comparison lemma is:

■ (21.2.4) **Formal A-module comparison lemma** Let $(F(X, Y), \rho_F)$ and $(G(X, Y), \rho_G)$ be two formal A-modules over an A-algebra B and suppose that they are congruent mod(degree n) for some $n \geq 2$. (This means that $F(X, Y) \equiv G(X, Y)$ mod(degree n), and $\rho_F(a)(X) \equiv \rho_G(a)(X)$ mod(degree n) for all $a \in A$.) Then there exist a unique element $d \in B$ and unique elements $c_a \in B$, one for each $a \in A$, such that

$$F(X, Y) \equiv G(X, Y) + dC_n(X, Y) \quad \text{mod(degree } n + 1) \tag{21.2.5}$$

$$\rho_F(a)(X) \equiv \rho_G(a)(X) + c_a X^n \quad \text{mod(degree } n + 1)$$

These elements d and c_a are subject to the following relations

$$\begin{aligned} d(a - a^n) &= v(n)c_a && \text{all } a \in A \\ c_{a+b} - c_a - c_b &= dC_n(a, b) && \text{all } a, b \in A \\ ac_b + b^n c_a &= c_{ab} && \text{all } a, b \in A \end{aligned} \tag{21.2.6}$$

Proof The ordinary comparison lemma gives the existence of a $d \in B$ such that $F(X, Y) \equiv G(X, Y) + dC_n(X, Y)$ mod(degree $n + 1$). The existence of $c_a \in B$ such that the second line of (21.2.5) holds is of course a triviality. The relations (21.2.6) arise as follows (all congruences are modulo degree $n + 1$):

$$\begin{aligned} \rho_F(a)(F(X, Y)) &\equiv \rho_F(a)(G(X, Y)) + adC_n(X, Y) \\ &\equiv \rho_G(a)(G(X, Y)) + c_a(X + Y)^n + adC_n(X, Y) \end{aligned}$$

and on the other hand

$$\begin{aligned} \rho_F(a)(F(X, Y)) &= F(\rho_F(a)(X), \rho_F(a)(Y)) \\ &\equiv G(\rho_F(a)(X), \rho_F(a)(Y)) + dC_n(aX, aY) \\ &\equiv G(\rho_G(a)(X), \rho_G(a)(X)) + c_a X^n + c_a Y^n + dC_n(aX, aY) \\ &= \rho_G(a)(G(X, Y)) + c_a X^n + c_a Y^n + a^n dC_n(X, Y) \end{aligned}$$

Comparing these two expressions, we see that $c_a v(n)C_n(X, Y) = (ad - a^n d)C_n(X, Y)$ which proves $d(a - a^n) = c_a v(n)$ because $C_n(X, Y)$ is a primitive polynomial, cf. Section 4.1 of Chapter I.

To obtain the second identity of (21.2.6) we calculate mod(degree $n+1$)

$$\rho_F(a+b)(X) \equiv \rho_G(a+b)(X) + c_{a+b}X^n$$

and

$$\begin{aligned}\rho_F(a+b)(X) &= F(\rho_F(a)(X), \rho_F(b)(X)) \equiv G(\rho_F(a)(X), \rho_F(b)(X)) + dC_n(aX, bX)\\ &\equiv G(\rho_G(a)(X), \rho_G(b)(X)) + c_aX^n + c_bX^n + dC_n(aX, bX)\\ &\equiv \rho_G(a+b)(X) + c_aX^n + c_bX^n + dC_n(a, b)X^n\end{aligned}$$

and comparing these two expressions we see that $c_{a+b} = c_a + c_b + dC_n(a, b)$. Finally, to obtain the third identity of (21.2.6), we observe

$$\begin{aligned}\rho_F(a)(\rho_F(b)(X)) &\equiv \rho_F(a)(\rho_G(b)(X)) + ac_bX^n\\ &\equiv \rho_G(a)(\rho_G(b)(X)) + c_ab^nX^n + ac_bX^n\\ &= \rho_G(ab)(X) + c_ab^nX^n + ac_bX^n\end{aligned}$$

and

$$\rho_F(a)(\rho_F(b)(X)) = \rho_F(ab)(X) \equiv \rho_G(ab)(X) + c_{ab}X^n$$

This concludes the proof of the lemma.

■ (21.2.7) **Remarks**

(i) It follows from the third identity of (21.2.6) that $c_1 = 0$ and $c_0 = 0$ (as they should be).

(ii) If B is of characteristic zero, then the first identity of (21.2.6) implies the other two; as is easily checked.

■ (21.2.8) We have seen that L_A, the A-algebra over which the universal formal A-module is defined, is graded. Let L_A^{n-1} be its degree $n-1$ summand and let $D_A^{n-1} \subset L_A^{n-1}$ be the submodule of "decomposables," i.e., the submodule of L_A^{n-1} generated by all elements of L_A^{n-1} of the form xy with x and y homogeneous of degree $< n-1$.

■ (21.2.9) **Corollary** L_A^{n-1}/D_A^{n-1} is the A-module generated by the symbols d and c_a, $a \in A$, subject to the relations (21.2.6).

Proof This is a special case of (21.2.4). Indeed, let J_{n-1} be the ideal of L_A generated by all homogeneous elements of degree $< n-1$, and let $F^u(X, Y)$ be the universal formal A-module over L_A. Reducing mod J_{n-1}, we obtain a formal A-module $\bar{F}^u(X, Y)$ over L_A/J_{n-1} such that $\bar{F}^u(X, Y) \equiv X + Y$ mod(degree n) and $\rho_{F^u}(a)(X) \equiv aX$ mod(degree n). Now apply Lemma (21.2.4) and observe that all relations (mod J_{n-1}) needed to make $F^u(X, Y)$ commutative and associative mod(degree $n+1$) and ρ_{F^u} a ring homomorphism (mod degree $n+1$) are consequences of (21.2.6). (Cf. also remark (21.2.7)(i).) Q.E.D.

■ (21.2.10) **Proposition** If A is a $\mathbf{Q}$-algebra or an infinite field of characteristic $p > 0$, then $L_A = A[z_2, z_3, \ldots]$ with degree $z_i = i - 1$, and $F_A^u(X, Y)$, the universal formal A-module, is as a formal group strictly isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ over L_A.

Proof First suppose that A is a $\mathbf{Q}$-algebra. Then we can divide by $v(n)$ so that the first relation of (21.2.6) says that L_A^{n-1}/D_A^{n-1} has one generator d. Further, every A-algebra is a $\mathbf{Q}$-algebra, hence of characteristic zero; so the second and third relations of (21.2.6) are implied by the first. This proves that L_A^{n-1}/D_A^{n-1} is free on one generator, so that L_A has one generator in each degree modulo decomposables. This means $L_A = A[z_2, z_3, \ldots]$, degree$(z_i) = i - 1$. Also $F_A^u(X, Y)$ is isomorphic to $\hat{\mathbf{G}}_a(X, Y)$ because L_A is a $\mathbf{Q}$-algebra.

Now let A be an infinite field of characteristic $p > 0$. Then if n is not a power of p, $v(n)$ is invertible in A and L_A, and it follows as before that L_A^{n-1}/D_A^{n-1} is a free A-module of rank 1. Now let n be a power of p, then $v(n) = p$; it follows that $d(a - a^n) = 0$ for all $a \in A$. Because A is an infinite field, there is an $a \in A$ such that $a - a^n \neq 0$, hence $d = 0$ in L_A^{n-1}/D_A^{n-1}. From the third relation of (21.2.6) we obtain $(a - a^n)c_b = (b - b^n)c_a$. Fix one element $a \in A$ such that $(a - a^n) \neq 0$. We claim that we can choose c_a (for this one particular a) arbitrarily and that then the $c_b = (a - a^n)^{-1}(b - b^n)c_a$ satisfy the remaining relations (i.e., the second relation of (21.2.6). Indeed, since $d = 0$ we must show

$$(a - a^n)^{-1}(b_1 + b_2 - (b_1 + b_2)^n)c_a$$
$$= (a - a^n)^{-1}(b_1 - b_1^n)c_a + (a - a^n)^{-1}(b_2 - b_2^n)c_a$$

which is obvious since n is a power of p and A and L_A are of characteristic p. Hence L_A^{n-1}/D_A^{n-1} is also free on one generator if n is a power of p, so that $L_A = A[z_2, z_3, \ldots]$ also in this case. Finally, the last statement has already been proved (Lemma (21.1.8)).

■ (21.2.11) **Remark** The hypothesis "infinite" in the proposition above cannot be removed. Indeed, let $A = \mathbf{F}_q$, the finite field of q elements. We claim that $L_A^{q-1}/D_A^{q-1} = 0$ in this case. To see this we calculate $\mathbf{Mod}_A(L_A^{q-1}/D_A^{q-1}, A)$; that is, we calculate all solutions of the equations (21.2.6) with $d, c_a \in A$. First, the second equation of (21.2.6) gives quite generally $d(1 - p^{n-1}) = c_p - pc_1$. Since $c_p = 0 = pc_1 = p$, it follows that $d = 0$. Further, since $a^q = a$ for all $a \in A = \mathbf{F}_q$ we have $ac_b + bc_a = c_{ab}$ making $C: a \mapsto c_a$ a derivation on $\mathbf{F}_q \to \mathbf{F}_q$. Then $a^q \mapsto qa^{q-1}c_a = 0$ under this derivation but $C(a^q) = C(a) = c_a$. Hence $c_a = 0$ for all a, which proves that $\mathbf{Mod}_A(L_A^{q-1}/D_A^{q-1}, A) = 0$ so that also $L_A^{q-1}/D_A^{q-1} = 0$ since A is a field. ($\mathbf{Mod}_A$ is the category of A-modules.)

It is not difficult to see that $L_A^{n-1}/D_A^{n-1} = A = \mathbf{F}_q$ for all n that are not a power of q. (Then there is an a such that $a^n - a \neq 0$ in $\mathbf{F}_q$ and c_a becomes a generator if n is a power of p, and d is the generator if n is not a power of p.) So we have that $L_{\mathbf{F}_q}$ is a polynomial ring over $\mathbf{F}_q$ with one generator in every degree that is not a power of q.

21.3 On the calculation of L_A for local and global rings of integers

■ (21.3.1) **Proposition** Let A be a (nontrivial) discrete valuation ring. Then L_A^{n-1}/D_A^{n-1} is a free A-module on one generator for all $n \in \mathbf{N}$.

Proof Let π be a uniformizing element of A. Consider the ideal $\mathfrak{A}$ of A generated by the elements $a^n - a$, $a \in A$. There are two possibilities:

Case 1: $\mathfrak{A} = A$ In this case there is an $a \in A$ such that $a^n - a$ is a unit (because A is a local ring). We claim that c_a generates L_A^{n-1}/D_A^{n-1}. Indeed, from $(a^n - a)c_b = (b^n - b)c_a$ for all $a, b \in A$, we see that

$$c_b = (a^n - a)^{-1}(b^n - b)c_a \qquad \text{and} \qquad d = (a - a^n)^{-1}v(n)c_a$$

Further, there is a surjective homomorphism $L_A^{n-1}/D_A^{n-1} \to A$ defined by $c_a \mapsto 1$, $c_b \mapsto (a^n - a)^{-1}(b^n - b)$, $d \mapsto v(n)(a - a^n)^{-1}$. It follows that $A \simeq L_A^{n-1}/D_A^{n-1}$.

Case 2: $\mathfrak{A} \neq A$ Then $\mathfrak{A} = (\pi)$ because $\pi - \pi^n \in \mathfrak{A}$. We claim that c_π generates L_A^{n-1}/D_A^{n-1}. Note that in this case $a - a^n \equiv 0 \bmod \pi$ for all $a \in A$, so that $x = x^n$ holds in k for all $x \in k$, proving that case 2 can happen only if the residue field k is finite and if n is a power of $p = \mathrm{char}(k)$.

Let us write M for the A-module L_A^{n-1}/D_A^{n-1} and $\bar{M} = M/c_\pi A$. Then because $(\pi - \pi^n)c_a = (a - a^n)c_\pi$, we have $(\pi - \pi^n)\bar{c}_a = 0$, hence $\pi\bar{c}_a = \pi^n\bar{c}_a = 0$ because $1 - \pi^{n-1}$ is a unit in A. Further, $(\pi - \pi^n)\bar{d} = v(n)c_\pi$ so that also $\pi\bar{d} = 0$.

It follows that $\bar{M}$ is a k-module; and since $a^n - a \equiv 0 \bmod \pi$, we have $\bar{c}_{ab} = a\bar{c}_b + b\bar{c}_a$ in $\bar{M}$, so that the map $C\colon k \to \bar{M}$ defined by $\bar{a} \mapsto \bar{c}_a$ is well defined and satisfies $C(\bar{a}\bar{b}) = \bar{a}C(\bar{b}) + \bar{b}C(\bar{a})$. In particular, $C(\bar{a}) = C(\bar{a}^n) = n\bar{a}^{n-1}C(\bar{a}) = 0$ because $x^n = x$ in k and n is a power of p. This proves that $\bar{c}_a = 0$ in $\bar{M}$ for all a. The second relation of (21.2.6) now says that $C_n(a, b)\bar{d} = 0$ in $\bar{M}$ for all $a, b \in A$. According to Lemma (21.3.2) there exists an $x \in \mathbf{F}_p$, the field of p elements, such that $C_n(x, 1) \neq 0$ in $\mathbf{F}_p$ (n is still a power of p). This proves that also $\bar{d} = 0$ in $\bar{M}$ so that $\bar{M} = 0$, which proves that c_π generates M. There is also a surjective homomorphism $M \to A$, viz. $c_a \mapsto \pi^{-1}(a - a^n)$ and $d \mapsto \pi^{-1}p$. This proves that $L_A^{n-1}/D_A^{n-1} = M \simeq A$ also in this case.

■ (21.3.2) **Lemma** Let n be a power of the prime number p, then there exists an $x \in \mathbf{F}_p$ such that $C_n(x, 1) \neq 0$.

Proof First note that $(X^{p^{i-1}} + Y^{p^{i-1}}) \equiv (X + Y)^{p^{i-1}} \bmod(p)$ and hence

$$(X^{p^{i-1}} + Y^{p^{i-1}})^p - X^{p^i} - Y^{p^i} \equiv (X + Y)^{p^i} - X^{p^i} - Y^{p^i} \bmod(p^2)$$

so that

$$C_{p^i}(X, Y) \equiv C_p(X^{p^{i-1}}, Y^{p^{i-1}}) \bmod(p)$$

which means that it suffices to prove the lemma in case $n = p$. Let $t(X)$ be the polynomial $C_p(X, 1)$ over $\mathbf{F}_p$. This is a nonzero polynomial of degree $p - 1$; it

looks like $t(X) = X^{p-1} + (\cdots) + X$. So $t(X)$ can have at most $p-1$ different roots in $\mathbf{F}_p$, which means that there is an $x \in \mathbf{F}_p$ such that $t(x) \neq 0$.

■ (21.3.3) **Example A** Let A be the ring of integers of an algebraic number field. Then for n a power of a prime number p we have that $\mathbf{Mod}_A(L_A^{n-1}/D_A^{n-1}, A)$ is isomorphic (as an A-module) to the ideal $p\mathfrak{A}^{-1} \subset A$ where $\mathfrak{A}$ is the ideal generated by all the elements $a - a^n$, $a \in A$. This is seen as follows. We have to find all solutions of (21.2.6) with d, $c_a \in A$. Observe that $d \in p\mathfrak{A}^{-1}$ because $d = pc_a(a - a^n)^{-1}$ for all $a \in A$. So, to every solution of (21.2.6) there corresponds a unique element $d \in p\mathfrak{A}^{-1}$. Conversely, suppose that d is any element in $p\mathfrak{A}^{-1}$, then $c_a = p^{-1}(a - a^n)d$ is in A, and these c_a together with d constitute a solution of (21.2.6). It follows that L_A^{n-1}/D_A^{n-1} need not be isomorphic to A in case A is the ring of integers of an algebraic number field. (Example: let $\mu^2 = 3\sqrt{-2}$ and A the ring of integers of $K = \mathbf{Q}(\mu)$. An integral basis of A over $\mathbf{Z}$ is $\{1, \mu, \sqrt{-2}, \mu\sqrt{-2}\}$, the ideal (2) factors as $\mathfrak{p}_2^4$ with $\mathfrak{p}_2$ the ideal $(\mu, \sqrt{-2})$ and $\mathfrak{p}_2$ is nonprincipal. In this case the ideal of A generated by the $a - a^2$, $a \in A$ is $\mathfrak{p}_2$ (as is easily checked by taking $a = 2$, $a = \mu$, and $a = \sqrt{-2}$). Incidentally, the class number of K is 2. For more details concerning K, cf. [399, p. 56].)

However, if K has class number 1, then we see that $\mathbf{Mod}_A(L_A^{n-1}/D_A^{n-1}) \simeq A$. More generally, if $\mathfrak{S}$ is a set of primes of K and $A_{\mathfrak{S}}$, the ring of $\mathfrak{S}$-integers is principal, then $\mathbf{Mod}_A(L_A^{n-1}/D_A^{n-1}, A) \simeq A$. (This holds for all n; if n is not a prime power, then L_A^{n-1}/D_A^{n-1} is free with generator d.)

■ **Example B** A rather similar result holds for the case that A is the ring of integers of a global function field. In this case d is a free generator for L_A^{n-1}/D_A^{n-1} for all n that are not a power of p. Let n be a power of p. First, observe that then $(a - a^n)d = 0$ for all $a \in A$, so that (since A is an integral domain and $d \in A$) we must have $d = 0$.

Now let $\mathfrak{A}$ be the ideal generated by the elements $a - a^n$, $a \in A$, and suppose that $\mathfrak{A}$ is principal $\mathfrak{A} = (x)$. Write $x = \sum r_a(a - a^n)$ (where almost all r_a are zero). Now let $\{c_a\}$, $c_a \in A$ be a solution of (21.2.6). Then $(a - a^n)c_b = (b - b^n)c_a$ for all $a, b \in A$. Multiplying with r_a and summing over a, we obtain $xc_b = (b - b^n)\sum r_a c_a$. Now $(b - b^n) \in (x)$, let $(b - b^n) = z_b x$. Then $c_b = z_b(\sum r_a c_a)$. So we have found an element $y \in A$, viz., $y = \sum r_a c_a$ in terms of which all the c_b can be expressed. Inversely, given $y \in A$, then $c_b = yz_b$, $d = 0$ is a solution of (21.2.6). So also in this case we have $\mathbf{Mod}_A(L_A^{n-1}/D_A^{n-1}, A) \simeq A$ if A is principal.

■ (21.3.4) We shall now focus on a ring A of one of the following types:

(a) A is a nontrivial discrete valuation ring (not necessarily complete);

(b) A is the ring of integers of an algebraic number field or an algebraic function field in one variable over a finite field of constants;

(c) A is the ring of $\mathfrak{S}$-integers of one of the two types of field K listed under

(b), where $\mathfrak{S}$ is a finite set of valuations including all the infinite ones, i.e., $A = \{x \in K \mid v(x) \geq 0 \text{ for all } v \notin \mathfrak{S}\}$.

In cases (b) and (c) we note that A is finitely generated as an algebra over $\mathbf{Z}$.

(d) A is a field with infinitely many elements.

■ (21.3.5) **Theorem** Let A be one of types of rings listed in (21.3.4) and suppose that A is a principal ideal ring, then $L_A \simeq \mathbf{Z}[z_2, z_3, z_4, \ldots]$ with $\text{degree}(z_i) = i - 1$.

Proof We first show that under the hypotheses stated $L_A^{n-1}/D_A^{n-1} \simeq A$. In case A is of type (a) or (d) this has already been done. In case (b) and (c) write $M = L_A^{n-1}/D_A^{n-1}$. By the very definition of L_A (as the solution of a certain universal problem) we have that $(L_A)_\mathfrak{p} = L_{A_\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$ of A.

It follows that

$$M_\mathfrak{p} = L_{A_\mathfrak{p}}^{n-1}/D_{A_\mathfrak{p}}^{n-1} \simeq A_\mathfrak{p} \tag{21.3.6}$$

(using Proposition (21.3.1)). Let

$$\phi\colon M \to \mathbf{Mod}_A(\mathbf{Mod}_A(M, A), A), \qquad m \mapsto \psi_m, \quad \psi_m(\chi) = \chi(m)$$

be the canonical double duality homomorphism. Because A is finitely generated as a ring, we see from (21.2.6) that M is finitely generated as an A-module, and, A being also noetherian, we have that for all prime ideals $\mathfrak{p}$

$$(\mathbf{Mod}_A(\mathbf{Mod}_A(M, A), A))_\mathfrak{p} = \mathbf{Mod}_{A_\mathfrak{p}}(\mathbf{Mod}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p}), A_\mathfrak{p})$$

(cf. [42, Chapter II, Section 2, Proposition 19]). It follows by (21.3.6) that $\phi_\mathfrak{p}$ is an isomorphism for all prime ideals $\mathfrak{p}$, hence that ϕ is an isomorphism (by [42, Chapter II, Section 3, Theorem 1]). But according to Examples (21.3.3) A and B we have $\mathbf{Mod}_A(M, A) \simeq A$, so that indeed $M \simeq A$.

Now in case A is of type (d) we have already shown that $L_A \simeq A[z_2, z_3, \ldots]$. In the remaining cases there is certainly a surjective homomorphism of A-algebras $\psi\colon A[z_2, z_3, \ldots] \to L_A$, viz. the homomorphism that maps z_i to a generator of L_A^i/D_A^i. Let K be the quotient field of A. Then $\psi \otimes_A K$ is an isomorphism (because $L_A \otimes K \simeq L_K$) and hence ψ is also injective and hence an isomorphism.

■ (21.3.7) We stress once more that this theorem cannot be generalized to cover the case of, say, rings of integers of arbitrary algebraic number fields (Example (21.3.3)).

21.4 Explicit universal formal A-modules

■ (21.4.1) **Construction in case A is a field of characteristic zero** In this case $L_A \simeq A[z_2, z_3, z_4, \ldots]$. Let $f(X) = X + \sum_{i=2}^{\infty} z_i X^i$ and let $F_A^u(X, Y) = f^{-1}(f(X) + f(Y))$, $\rho_F(a)(X) = f^{-1}(af(X))$ for all $a \in A$. It is not difficult to see that this defines a universal formal A-module over L_A.

■ (21.4.2) **The universal formal A-module structure on $\hat{G}_a(X, Y)$ in case A is an infinite field of characteristic $p > 0$, p a prime number** Let $\rho_F(a, T)(X) \in A[T_1, T_2, \ldots][[X]]$ be the power series defined in Example (21.1.10). Then these power series define a formal A-module structure on $\hat{G}_a(X, Y)$ over $A[T_1, T_2, \ldots]$. We claim that this formal A-module structure is universal in the following sense: given an A-algebra B and a formal A-module structure on $\hat{G}_a(X, Y)$ over B, i.e., a map $\rho: A \to \mathrm{End}_B(\hat{G}_a(X, Y))$, then there is a unique homomorphism $\phi: A[T_1, T_2, \ldots] \to B$ such that $\phi_*\rho(a, T)(X) = \rho(a)(X)$ for all $a \in A$.

This is proved as follows. Suppose we have already found $\phi(T_1), \ldots, \phi(T_n)$ such that

$$\phi_*\rho(a, T) \equiv \rho(a)(X) \mod(\text{degree } p^n + 1)$$

Because we are dealing with the additive group law, it follows that

$$\rho(a)(X) \equiv \phi_*\rho(a, T)(X) - c_a X^{p^{n+1}} \mod(\text{degree } p^{n+1} + 1)$$

where the c_a in B satisfy

$$c_{a+b} = c_a + c_b, \qquad ac_b + b^{p^{n+1}}c_a = c_{ab} \tag{21.4.3}$$

Now

$$\rho(a, T)(X) \equiv T_{n+1}(a^{p^{n+1}} - a)X^{p^{n+1}} \mod(T_1, \ldots, T_n, \text{degree } p^{n+1} + 1)$$

so our contention will be proved if we can show that there is a unique element $t \in B$ such that

$$c_a = t(a^{p^{n+1}} - a) \qquad \text{for all} \quad a \in A \tag{21.4.4}$$

This is where we use the hypothesis that A is an infinite field. In that case there is an $a_0 \in A$ such that $a_0^{p^{n+1}} - a_0 \neq 0$ in A and we see that the only possible solution for t is $t = (a_0^{p^{n+1}} - a_0)^{-1}c_{a_0}$ where a_0 is a fixed element such that $a_0^{p^{n+1}} - a_0 \neq 0$, hence is a unit. The relations (21.4.3) imply $(a_0 - a_0^{p^{n+1}})c_b = (b - b^{p^{n+1}})c_{a_0}$ for all $b \in A$. It follows that (21.4.4) holds for all $a \in A$.

■ (21.4.5) **The universal formal A-module structure on $\hat{G}_a(X, Y)$ in case A is a finite field** Now let A be a finite field with $q = p^r$ elements, p a prime number, $\tilde{A}[T] = A[T_i; i \in \mathbf{N}, r \nmid i]$ and let $\tilde{\rho}(a, T)(X)$ for all $a \in A$ be the power series obtained from $\rho(a, T)(X)$ by setting $T_{rj} = 0$ for all $j = 1, 2, \ldots$. Then $a \mapsto \tilde{\rho}(a, T)(X)$ is, we claim, a universal formal A-module structure on $\hat{G}_a(X, Y)$ over $\tilde{A}[T]$. The proof of this is as above in (21.4.2) except in case $n + 1$ is a multiple of r. In that case (21.4.3) says, since $b^{p^{n+1}} = b$ in this case, that $c_{a+b} = c_a + c_b$ and $ac_b + bc_a = c_{ab}$. So that by induction $c_a = c_{a^q} = qa^{q-1}c_a = 0$ for all $a \in A$ (since $a = a^q$). So that if $n + 1$ is a multiple of r $\phi_*\tilde{\rho}(a, T)(X) \equiv \rho(a)(X) \mod(\text{degree } p^n + 1)$ implies $\phi_*\tilde{\rho}(a, T)(X) \equiv \rho(a)(X) \mod(\text{degree } p^{n+1} + 1)$.

■ (21.4.6) **The universal formal A-module in case A is a field of characteristic p** Let

$$f(X) = X + \sum_{i=2}^{\infty} z_i X^i - \sum_{j=1}^{\infty} z_{p^j} X^{p^j} \tag{21.4.7}$$

and let $F(X, Y)$ be the formal group law $f^{-1}(f(X) + f(Y))$. For A an infinite field, we define $\rho\colon A \mapsto \mathrm{End}_{A[z]}(F(X, Y))$ by the formula

$$\rho(a) = f^{-1}(\psi_* \rho(a, T)(f(X)))$$

where $\psi\colon A[T] \to A[z] = L_A$ takes T_i into z_{p^i}. For A a finite field of $q = p^r$ elements, $L_A = A[z_i \mid i \text{ not a power of } q,\ i \geq 2]$ and we define

$$\rho(a) = f^{-1}(\tilde{\psi}_* \tilde{\rho}(a, T)(f(X)))$$

where $\tilde{\psi}\colon \tilde{A}[T] \to L_A$ takes T_i into z_{p^i}, where i runs through all elements of $\mathbf{N}$ that are not divisible by r, $q = p^r$.

It is not difficult (given (21.4.2), (21.4.5) and (21.2.10), (21.2.11)) to show that these definitions do indeed give us (explicit) universal formal A-modules for A a field of characteristic $p > 0$.

■ (21.4.8) **Universal formal A-modules for A a discrete valuation ring with finite residue field** Let A be a nontrivial discrete valuation ring with uniformizing element π, quotient field K, and residue field k of q elements. Let $\sigma\colon K[S_2, S_3, \ldots] \to K[S_2, S_3, \ldots]$ be the K-automorphism $S_i \mapsto S_i^q$. Then $\sigma a \equiv a^q \bmod \pi A[S]$ for all $a \in A[S]$, so that we are in a functional equation type situation. We now define

$$f_S^A(X) = X + \sum_{i=2}^{\infty} S_i X^i - \sum_{j=1}^{\infty} S_{q^j} X^{q^j} + \sum_{j=1}^{\infty} \pi^{-1} S_{q^j} (\sigma_*^j) f_S^A(X^{q^j})$$

$$F_S^A(X, Y) = (f_S^A)^{-1}(f_S^A(X) + f_S^A(Y)) \tag{21.4.9}$$

$$\rho_S^A(a)(X) = (f_S^A)^{-1}(a f_S^A(X))$$

Because of the functional equation lemma (Chapter I, Section 2, Lemma 2.2), we know that the power series $F_S^A(X, Y)$ and $\rho_S^A(a)(X)$ have their coefficients in $A[S]$. It follows that $(F_S^A(X, Y), \rho_S^A)$ is a formal A-module over $A[S]$. We claim that it is a universal formal A-module.

To see this observe that modulo $(S_2, \ldots, S_{n-1}$, degree $n + 1)$

$$f_S^A(X) \equiv \begin{cases} X + S_n X^n & \text{if } n \text{ is not a power of } q \\ X + \pi^{-1} S_n & \text{if } n \text{ is a power of } q \end{cases}$$

Using this we see that modulo $(S_2, \ldots, S_{n-1}$, degree $n + 1)$

$$F_S^A(X, Y) \equiv \begin{cases} X + Y + S_n \nu(n) C_n(X, Y) & \text{if } n \text{ is not a power of } q \\ X + Y + \pi^{-1} S_n \nu(n) C_n(X, Y) & \text{if } n \text{ is a power of } q \end{cases}$$

$$\rho_S^A(a)(X) \equiv \begin{cases} aX + (a - a^n) S_n X^n & \text{if } n \text{ is not a power of } q \\ aX + \pi^{-1}(a - a^n) S_n X^n & \text{if } n \text{ is a power of } q \end{cases}$$

Using (the proof of) Proposition (21.3.1), it is now not difficult to show that $(F_S^A(X, Y), \rho_S^A)$ is indeed a universal formal A-module. For the reader who does not like this exercise, the details of the proof are written out (in painful detail) for the higher dimensional case in 25.4 (proof of Theorem (25.4.16)).

■ (21.4.10) **Universal formal A-modules for A the ring of integers of an algebraic number field of class number 1 or algebraic function field in one variable with finite field of constants of class number 1** Let A be a ring of integers of a field K as indicated in the title of this subsection. For each finite valuation v, let $\mathfrak{p}_v$ be the corresponding prime ideal, and $\pi_v \in A$ an element such that $\mathfrak{p}_v = (\pi_v)$, and q_v the number of elements in $A/\pi_v A$. For each $n \in \mathbf{N}$, let $\mathfrak{S}_n = \{v \mid n \text{ is a power of } q_v\}$ and

$$c_n = \prod_{v \in \mathfrak{S}_n} \pi_v^{-1} \tag{21.4.11}$$

where $c_n = 1$ if $\mathfrak{S}_n = \varnothing$ (which happens in particular if n is not a power of a prime number). We are now going to construct a power series

$$f_U^A(X) \in A[U_2, U_3, U_4, \ldots][\![X]\!]$$

To do this let $Q_A \subset \mathbf{N}$ be the set of all elements $n \in \mathbf{N}$ that are a power of a q_v for some finite valuation v of A. We now define

$$a_n^A(U) = \sum_{(q_1, \ldots, q_t, m)} d^A(q_1, \ldots, q_t, m) U_{q_1} U_{q_2}^{q_1} \cdots U_{q_t}^{q_1 \cdots q_{t-1}} U_d^{q_1 \cdots q_t} \tag{21.4.12}$$

where the sum is over all sequences $(q_1, \ldots, q_t, m)$ with $q_i \in Q_A$, $t \in \mathbf{N} \cup \{0\}$, $m \in \mathbf{N}$ such that $q_1 \cdots q_t m = n$ and where (for convenience) we have introduced $U_1 = 1$. The coefficients $d^A(q_1, \ldots, q_t, m)$ are not arbitrary but are required to satisfy the following conditions: if $t = 0$,

$$d^A(n) = c_n \tag{21.4.13}$$

where c_n is defined in (21.4.8); and if $t \geq 1$, then

(21.4.14)

$$v(d^A(q_1, \ldots, q_t, m) - \pi_v^{-1} d^A(q_2, \ldots, q_t, m)) \geq 0 \quad \text{if } q_1 \text{ is a power of } q_v$$

$$v(d^A(q_1, \ldots, q_t, m) \geq 0 \quad \text{if } q_1 \text{ is not a power of } q_v$$

Note that if n is a power of q_v, then

$$v(c_n - \pi_v^{-1}) \geq 0 \tag{21.4.15}$$

Observe that because of (21.4.14) and (21.4.15) $f_U^A(X)$ satisfies for every finite valuation v a functional equation of the type

$$f_U^A(X) - \sum_{i=1}^{\infty} \pi_v^{-1} U_{q_v^i}(\sigma_v^i)_* f_U(X^{q_v^i}) \in A_{(v)}[U][\![X]\!]$$

where $A_{(v)} = \{x \in K \mid v(x) \geq 0\}$ is the localization of A with respect to v, and where σ_v: $K[U] \to K[U]$ is the K-automorphism $U_j \mapsto U_j^{q_v}$.

Now define

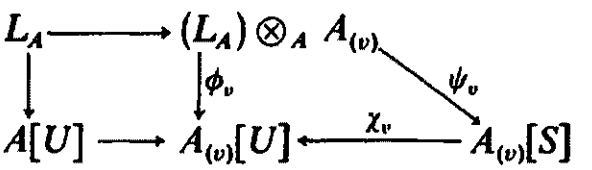
$$F_U^A(X, Y) = (f_U^A)^{-1}(f_U^A(X)) + f_U^A(Y)) \tag{21.4.16}$$

$$\rho_U^A(a)(X) = (f_U^A)^{-1}(af_U^A(X)) \tag{21.4.17}$$

then the functional equation lemma (Chapter I, 2.2) says that $(F_U^A(X, Y), \rho_U^A)$ is a formal A-module over $A[U]$.

We claim that it is in fact a universal formal A-module. To prove this, let $F^u(X, Y)$ and L_A be the objects constructed abstractly in (21.2.2). The formal A-module $(F_U^A(X, Y), \rho_U^A)$ gives rise to a unique homomorphism ϕ: $L_A \to A[U]$ taking $F^u(X, Y)$ (and ρ_{F^u}) into $F_U^A(X, Y)$ (and ρ_U^A).

Let v be a finite valuation and let $(F_S^{A_{(v)}}(X, Y), \rho_S^{A_{(v)}})$ be the universal formal $A_{(v)}$-module constructed above. This formal $A_{(v)}$-module gives rise to a unique homomorphism ψ_v: $L_A \to A_{(v)}[S]$ which takes $F^u(X, Y)$ and ρ_{F^u} into $F_S^{A_{(v)}}(X, Y)$ and $\rho_S^{A_{(v)}}$. Moreover, the localization $\hat{\psi}_v$: $L_{A_{(v)}} = L_A \otimes_A A_{(v)} \to A_{(v)}[S]$ is an isomorphism because both $F^u(X, Y)$ over $L_A \otimes A_{(v)} = L_{A_{(v)}}$ and $F_S^{A_{(v)}}(X, Y)$ over $A_{(v)}[S]$ are universal formal $A_{(v)}$-modules. Finally, consider $F_U^A(X, Y)$ over $A_{(v)}$. By the functional equation lemma we see that ρ_U^A extends to a homomorphism $A_{(v)} \to \mathrm{End}_{A_{(v)}}(F_U^A(X, Y))$ turning $F_U^A(X, Y)$ into a formal $A_{(v)}$-module over $A_{(v)}[U]$. By the universality of $F_S^{A_{(v)}}(X, Y)$ there is a unique homomorphism χ_v $A_{(v)}[S] \to A_{(v)}[U]$ taking $(F_S^{A_{(v)}}(X, Y), \rho_S^{A_{(v)}})$ into $(F_U^A(X, Y), \rho_U^A)$. We have a diagram



which is commutative by the uniqueness of the various homomorphisms involved. (Both $\chi_v\psi_v$ and ϕ_v take $F^u(X, Y)$ into $F_U^A(X, Y)$, so they must be equal.) Comparing the expressions for $f_S^{A_{(v)}}(X)$ and $f_U^A(X)$, we see that χ_v satisfies modulo $(U_2, \ldots, U_{n-1})$

$$\chi_v(S_n) \equiv \begin{cases} \pi_v c_n U_n & \text{if } n \text{ is a power of } q_v \\ c_n U_n & \text{if } n \text{ is not a power of } q_v \end{cases}$$

Hence, because $v(\pi_v c_n) = 0$ if n is a power of q_v and $v(c_n) = 0$ if n is not a power of q_v, it follows that χ_v is an isomorphism. (It is at this point that the hypothesis "class number 1" essentially enters; if the class number is > 1, it is generally not possible to find elements $c_n \in K$, one for every $n \in \mathbf{N}$, with the property $v(c_n) = -1$ if n is a power of q_v and $v(c_n) = 0$ if n is not a power of q_v; everything else can be done also in the class number ≥ 1 case.)

To continue with the proof, we have already seen that ψ_v is an isomorphism so that ϕ_v is also an isomorphism. This holds for every finite v, so using also

that L_A and $A[U]$ are graded and that ϕ is homogeneous of degree 0, it follows that ϕ is an isomorphism, which in turn implies that $F_U^A(X, Y)$ is a universal formal A-module.

■ (21.4.18) **Remark**

(i) The same constructions and proofs apply to rings of $\mathfrak{S}$-integers $A_{\mathfrak{S}}$ that are principal, where $\mathfrak{S}$ is a finite (or infinite) collection of valuations (including the infinite ones).

(ii) This proof that $L_A \simeq A[U_2, U_3, \ldots]$ did not use "A is finitely generated as a ring," as our calculation of L_A in Theorem (21.3.5) did. On the other hand, we used "finite residue field," which is in principle irrelevant for Theorem (21.3.5). More generally, constructions as in (21.4.10) can be carried out for "global fields" of class number 1 with not necessarily finite residue fields, for which there exists for every finite prime v an endomorphism $\sigma_v: A \to A$ and a power q of the residue field $A/\pi_v A$ such that $\sigma_v(a) \equiv a^q \bmod(\pi_v A)$.

■ (21.4.19) **Remark on notation** Taking $A = \mathbf{Z}$, we obtain formal group laws $F_U^{\mathbf{Z}}(X, Y)$, $F_S^{\mathbf{Z}}(X, Y)$; these are (variants of) the universal formal group laws $F_U(X, Y)$ and $F_S(X, Y)$ constructed in Chapter I. Similarly for the $a_n^A(U)$ and $d^A(q_1, \ldots, q_t, m)$.

(21.4.20) **Universal formal A-modules for A a discrete valuation ring with infinite residue field k** Let

$$f(X) = X + \sum_{i=2}^{\infty} z_i X^i \in A[z_1, z_2, \ldots][\![X]\!]$$

and let $F(X, Y) = f^{-1}(f(X) + f(Y))$ and $\rho_F(x) = f^{-1}(af(X))$ for all $a \in A$. We claim that $(F(X, Y), \rho_F)$ is a universal formal A-module over $A[z]$ if k is infinite. The proof is by induction. Suppose $(G(X, Y), \rho_G)$ is a formal A-module over $B \in \mathbf{Alg}_A$ and suppose that we have already found $b_2, b_3, \ldots, b_n \in B$ such that

(21.4.21) $\quad \phi_*(F(X, Y), \rho_F) \equiv (G(X, Y), \rho_G) \quad \bmod(\text{degree } n+1)$

where $\phi: A[z] \to B$ is the homomorphism $\phi(z_i) = b_i$, $i = 2, \ldots, n$, $\phi(z_j) = 0$ for $j > n$. (The induction starts because the case $n = 1$ is trivial.) By the comparison lemma (21.2.4) we know that there are unique elements $d \in B$ and $c_a \in B$ for all $a \in A$ such that

$$\phi_* F(X, Y) \equiv G(X, Y) + dC_{n+1}(X, Y) \quad \bmod(\text{degree } n+2)$$

$$\phi_* \rho_F(a)(X) \equiv \rho_G(a)(X) + c_a X^{n+1} \quad \bmod(\text{degree } n+2)$$

and such that

(21.4.22) $\quad d(a - a^{n+1}) = v(n+1)c_a, \qquad c_{a+b} - c_a - c_b = dC_{n+1}(a, b),$

$$ac_b + b^{n+1}c_a = c_{ab}$$

Now consider the elements $a - a^{n+1}$, $a \in A$. If $a - a^{n+1} \equiv 0 \bmod \mathfrak{m}(A)$ for all $a \in A$, then $x - x^{n+1} = 0$ for all $x \in k = A/\mathfrak{m}(A)$, which would make k a finite field. Hence there is an $a_0 \in A$ such that $a_0 - a_0^{n+1}$ is a unit in A.

Now

$$F(X, Y) \equiv X + Y + v(n+1)z_{n+1}C_{n+1}(X, Y) \mod(z_2, \ldots, z_n, \text{degree } n+2)$$

$$\rho_F(a)(X) \equiv aX + z_{n+1}(a - a^{n+1})X^{n+1} \mod(z_2, \ldots, z_n, \text{degree } n+2)$$

Now define $\hat{\phi}(z_i) = b_i$, $i = 2, \ldots, n$, $\hat{\phi}(z_{n+1}) = (a_0 - a_0^{n+1})^{-1}c_{a_0}$. Then relations (21.4.22) guarantee that $\phi(v(n+1)z_{n+1}) = d$, $\phi(z_{n+1}(a - a^{n+1})) = c_a$ for all $a \in A$. Moreover, $\hat{\phi}$ is clearly uniquely determined on $A[z_2, \ldots, z_{n+1}] \subset A[z]$ by (21.4.21) with n replaced by $n+1$ if ϕ is uniquely determined on $A[z_2, \ldots, z_n]$ by (21.4.21). By induction this concludes the proof that the formal A-module $(F(X, Y), \rho_F)$ constructed above is universal.

■ (21.4.23) **Corollary** Let A be a discrete valuation ring with infinite residue field. Then every formal A-module over an A-algebra B is isomorphic to the additive formal A-module $\hat{\mathbf{G}}_a(X, Y) = X + Y$, $\rho_{\mathbf{G}_a}(a)(X) = aX$.

21.5 A-typical formal A-modules

In this subsection unless explicitly stated otherwise A is always a nontrivial discrete valuation ring with uniformizing parameter π and residue field k of q elements; K is the quotient field of A; K may be either of characteristic zero or of characteristic $p > 0$; σ: $K[V_1, V_2, \ldots] \to K[V_1, V_2, \ldots]$ is the K-automorphism $V_j \mapsto V_j^q$.

■ (21.5.1) **Constructions** Let $f_V^A(X)$ be the power series defined by the functional equation

$$f_V^A(X) = X + \sum_{i=1}^{\infty} \pi^{-1}V_i(\sigma_*^i)f_V^A(X^{q^i}) \tag{21.5.2}$$

and, using $f_V^A(X)$ we define

$$F_V^A(X, Y) = (f_V^A)^{-1}(f_V^A(X) + f_V^A(Y)), \qquad \rho_V^A(a)(X) = (f_V^A)^{-1}(af_V^A(X)) \tag{21.5.3}$$

Then, by the functional equation lemma (Chapter I, 2.2) $(F_V^A(X, Y), \rho_V^A)$ is a formal A-module. We also note that, identifying V_i with S_{q^i}, $f_V^A(X)$ and $f_S^A(X)$ (cf. (21.4.6)) satisfy the same type of functional equation, so that again by the functional equation lemma $(F_V^A(X, Y), \rho_V^A)$ and $(F_S^A(X, Y), \rho_S^A)$ are strictly isomorphic formal A-modules. (The isomorphism $(f_S^A)^{-1}(f_V^A(X))$ is compatible with the given formal A-structures.)

If we take $A = \mathbf{Z}_{(p)}$ and $\pi = p\ (= q)$. Then $f_V^A(X)$ and $F_V^A(X, Y)$ become the $f_V(X)$ and $F_V(X, Y)$ of Chapter I, 2.3 and 3.3, and the following formulas should therefore come as no surprise

$$(21.5.4) \qquad f_V^A(X) = \sum_{n=0}^{\infty} a_n^A(V)X^{q^n}, \qquad a_0^A(V) = 1$$

$$\pi a_n^A(V) = a_{n-1}^A(V)V_1^{q^{n-1}} + \cdots + a_1^A(V)V_{n-1}^q + V_n$$

$$a_n^A(V) = \sum_{i_1+\cdots+i_r=n} \cdot \pi^{-r} V_{i_1} V_{i_2}^{q^{i_1}} \cdots V_{i_r}^{q^{i_1+\cdots+i_{r-1}}}$$

This is proved exactly as in the special case $A = \mathbf{Z}_{(p)}$, $p = \pi = q$ which was treated in Chapter I, Section 3.3.

■ (21.5.5) **Definition** A formal A-module over an A-algebra B is called A-typical if it is of the form $(\phi_* F_V^A(X, Y), \phi_* \rho_V^A)$ for a certain ring homomorphism $\phi\colon A[V] \to B$.

Note that this homomorphism is also necessarily unique, for otherwise there would also be two different homomorphisms $A[S] \to B$ both transforming $(F_S^A(X, Y), \rho_S^A)$ into the same formal A-module over B, contradicting the universality of $(F_S^A(X, Y), \rho_S^A)$ over $A[S]$. We have thus proved

■ (21.5.6) **Theorem**

(i) Every formal A-module over an A-algebra B is strictly isomorphic over B (as a formal A-module) to an A-typical formal A-module.

(ii) The formal A-module $(F_V^A(X, Y), \rho_V^A)$ over $A[V]$ is a universal A-typical formal A-module.

To be able to use this theorem effectively we need something like a workable criterion for being A-typical. To this end we first discuss logarithms for formal A-modules.

■ (21.5.7) **A-logarithms** If B is an A-algebra such that $B \to B \otimes_A K$ is injective (where K is the quotient field of A), then every formal A-module $(F(X, Y), \rho_F)$ over B has a logarithm (with coefficients in $B \otimes_A K$); that is there exists a power series $f(X)$ such that $f^{-1}(f(X) + f(Y)) = F(X, Y)$, $f^{-1}(af(X)) = \rho_F(a)(X)$. This follows immediately from the fact that the universal formal A-module $(F_S^A(X, Y), \rho_S^A)$ has such a logarithm. Such a logarithm is also necessarily unique. Indeed, this is trivial in case $\mathrm{char}(K) = 0$; and if $\mathrm{char}(K) = p$, this is seen as follows. Suppose there are two logarithms, then composing one with the inverse of the other we find a strict formal A-module automorphism $\alpha(X)\colon \hat{\mathbf{G}}_a(X, Y) \to \hat{\mathbf{G}}_a(X, Y)$ (with coefficients in $K \otimes_A B$). As $B \otimes_A K$ is of characteristic p, this means that $\alpha(X)$ is of the form

$$\alpha(X) = X + b_1 X^p + b_2 X^{p^2} + \cdots$$

and being an automorphism of the additive formal A-module $\hat{G}_a(X, Y)$ we must also have $\alpha(aX) = a\alpha(X)$ for all $a \in A$. This gives

$$ab_n = a^{p^n} b_n$$

for all $a \in A$. Since B is without A-torsion and A is infinite, this implies that $b_n = 0$ for all $n \geq 1$.

To avoid confusion with logarithms of formal group laws, we shall (if it exists) use the appellation "A-logarithm" and notation "A-log" for a power series $f(X)$ (with coefficients in $B \otimes_A K$ if necessary) such that $F(X, Y) = f^{-1}(f(X) + f(Y))$, $f(\rho_F(a)(X)) = af(X)$ and $f(X) \equiv X \bmod(\text{degree } 2)$.

We have then proved (the arguments above work in somewhat greater generality)

■ (21.5.8) **Proposition** Let $(F(X, Y), \rho_F)$ be a formal A-module over an A-algebra B and suppose that $B \to B \otimes_A K$ is injective. Then an A-logarithm of $(F(X, Y), \rho_F)$ (if it exists) is unique if A is an infinite integral domain. Moreover, if A is a discrete (nontrivial) valuation ring, then A-logarithms exist for all formal A-modules defined over A-algebras B such that $B \to B \otimes_A K$ is injective.

Now let A again be a discrete valuation ring with K, k, q, π as usual. Then, as in the case of formal group laws there is a formula for the A-logarithm. We have

$$A\text{-}\log_F(X) = \lim_{n \to \infty} \pi^{-n}[\pi^n]_F(X)$$

for every formal A-module $F(X, Y)$ over A-algebras B such that $B \to B \otimes_A K$ is injective and $\bigcap_n \pi^n B = \{0\}$. The proof is essentially the same as in the case of one dimensional formal group laws. Cf. Proposition (5.4.5) of Chapter I, cf. also (25.4.26) below for the more dimensional case.

Still assuming that A is a discrete valuation ring with finite residue field we have the following criterion for A-typicality.

■ (21.5.9) **Criterion for A-typicality** Let B be an A-algebra such that $B \to B \otimes_A K$ is injective. Then a formal A-module over B is A-typical if and only if its A-logarithm is of the form

$$A\text{-}\log_F(X) = X + b_1 X^q + b_2 X^{q^2} + \cdots \tag{21.5.10}$$

with $b_i \in B \otimes_A K$.

Proof This is practically a triviality. If $(F(X, Y), \rho_F)$ is A-typical, then it certainly satisfies the criterion because the universal A-typical formal A-module satisfies the criterion. Conversely, suppose that $(F(X, Y), \rho_F)$ is a formal A-module over B such that $A\text{-}\log_F(X)$ is of the form (21.5.10). Let ψ: $A[S] \to A[V]$ be the canonical projection $S_i \mapsto 0$ if i is not a power of q; $S_{q^i} \mapsto T_i$. Because $(F_S^A(X, Y), \rho_S^A)$ over $A[S]$ is a universal formal A-module, there is a unique homomorphism χ: $A[S] \to B$ taking $(F_S^A(X, Y), \rho_S^A)$ into $(F(X, Y), \rho_F)$.

By the uniqueness of A-logs we must have

$$\chi_* f_S^A(X) = A\text{-}\log_F(X)$$

It follows that $\chi(S_i) = 0$ for all i that are not a power of q. Hence χ factors through ψ to give a homomorphism ϕ: $A[V] \to B$. Then $\phi\psi = \chi$ takes $(F_S^A(X, Y), \rho_S^A)$ to $(F(X, Y), \rho_F)$ and because $(\psi_* F_S^A(X, Y), \psi_* \rho_S^A) = (F_V^A(X, Y), \rho_V^A)$ it follows that $F(X, Y)$ is A-typical.

■ (21.5.11) **Calculation of ρ_V^A in case A is of characteristic $p > 0$** We claim that if A is of characteristic $p > 0$,

$$\text{(21.5.12)} \quad \rho_V^A(a)(X) = x_0(a) + x_1(a)X^q + x_2(a)X^{q^2} + \cdots$$

$$x_n(a) = \pi^{-1} V_1(x_{n-1}(a))^q + \cdots + \pi^{-1} V_n(x_0(a))^{q^n} - \pi^{-1} V_n a$$

To prove this it suffices to check that $f_V^A(\rho_V^A(a)(X)) = a f_V^A(X)$, a calculation that is practically the same as the one we did to prove that $\rho(a, T)(\rho(b, T)(X)) = \rho(ab, T)(X)$ in (21.1.10). (One uses of course that if $f_V^A(X) = \sum_{n=0}^{\infty} a_n^A(V)X^{q^n}$, then $a_0^A(V) = 1$ and

$$\pi a_n^A(V) = a_{n-1}^A(V)V_1^{p^{n-1}} + \cdots + a_1^A(V)V_{n-1}^{p^n} + V_n$$

cf. (21.5.4); the details are left to the reader.)

This, in turn, of course suggests that we should take another look at Example (21.1.10) from the functional equation point of view.

21.6 Universal formal A-modules for A a field of characteristic p. Revisited

■ (21.6.1) For this subsection, let A be a field of characteristic p and, for the moment, suppose that A is infinite. We "apply" functional equation type techniques in a somewhat unusual setting: σ: $A[T] \to A[T]$ is the endomorphism "raising to the power p"; i.e., $a \mapsto a^p$ for $a \in A$ and $T_i \mapsto T_i^p$. Let

$$f(X) = X + \sum_{i=1}^{\infty} T_i(\sigma_*^i) f(X^p)$$

(i.e., we take, so to speak, $\mathfrak{a} = 0$, in functional equation lemma terms). Let $F(X, Y) = f^{-1}(f(X) + f(Y))$, $\rho_F(a) = f^{-1}(af(X))$. Then we have just as above in (21.5.11)

$$\rho(a) = \hat{x}_0(a) + \hat{x}_1(a)X^p + \hat{x}_2(a)X^{p^2} + \cdots$$

$$\hat{x}_n(a) = T_1(\hat{x}_{n-1}(a)^p + \cdots + T_n(\hat{x}_0(a))^{p^n} - T_n a$$

and a quick comparison with (21.1.10) shows that hence

$$\rho_F(a)(X) = \rho(a, T)(X)$$

In particular, this shows that the universal formal A-module structure on $\hat{G}_a(X, Y)$ is isomorphic (as a formal A-module) to the additive one; cf. (21.4.2). This works also for finite fields A. Simply take $T_i = 0$ for i a multiple of r if A has $q = p^r$ elements; cf. (21.4.5).

Further, in (21.4.6) we constructed a universal formal A-module for A a field of characteristic $p > 0$ that as a formal A-module is strictly isomorphic to $\hat{G}_a(X, Y)$ with the A-module structure of (21.4.2) and (21.4.5). (The isomorphism is of course (21.4.7).) So we have proved

■ (21.6.2) **Theorem** Let K be a field of characteristic p (finite or infinite). Then every formal K-module over a K-algebra B is strictly isomorphic (as a formal K-module) to the additive formal K-module $\hat{G}_a(X, Y) = F(X, Y)$, $\rho_F(a) = aX$.

21.7 Universal isomorphisms of formal A-modules

The assumptions of 21.5 hold, i.e., A is a discrete valuation ring with quotient field K, residue field k with $q = p^r$ elements and uniformizing parameter π.

■ (21.7.1) **Construction** Let $V_1, V_2, \ldots; T_1, T_2, \ldots$ be two sequences of indeterminates and σ: $K[V, T] \to K[V, T]$ be the K-endomorphism $V_i \mapsto V_i^q$, $T_j \mapsto T_j^q$. Let $f^A_{V,T}(X)$ be the functional equation power series

$$f^A_{V,T}(X) = X + \sum_{j=1}^{\infty} T_j X^{q^j} + \sum_{i=1}^{\infty} \pi^{-1} V_i(\sigma_*^i) f^A_{V,T}(X^{q^i}) \tag{21.7.2}$$

and using $f^A_{V,T}(X)$ we define (as usual)

$$F^A_{V,T}(X, Y) = (f^A_{V,T})^{-1}(f^A_{V,T}(X) + f^A_{V,T}(Y)) \tag{21.7.3}$$

$$\rho^A_{V,T}(a)(X) = (f^A_{V,T})^{-1}(a f^A_{V,T}(X))$$

$$\alpha^A_{V,T}(X) = (f^A_{V,T})^{-1}(f^A_V(X)) \tag{21.7.4}$$

where $f^A_V(X)$ is the power series of (21.5.2).

Note that if we take $A = \mathbf{Z}_{(p)}$, $\pi = p = q$, then the formulas given above for $f^A_{V,T}(X)$, $F^A_{V,T}(X, Y)$, $\alpha^A_{V,T}(X)$ become the ones we gave in Chapter I, 3.3 and 19.2 for $f_{V,T}(X)$, $F_{V,T}(X, Y)$, $\alpha_{V,T}(X)$. As in the case $A = \mathbf{Z}_{(p)}$ we have a formula

$$f^A_{V,T}(X) = \sum_{n=0}^{\infty} a_n^A(V, T) X^{q^n}, \qquad a_0^A(V) = 1 \tag{21.7.5}$$

$$a_n^A(V, T) = a_{n-1}^A(V) T_1^{q^{n-1}} + \cdots + a_1^A(V) T_{n-1}^q + T_n$$

According to the criterion (21.5.9) for A-typicality, the formal A-module $(F^A_{V,T}(X, Y), \rho^A_{V,T})$ is A-typical. Hence by the universality of $(F^A_V(X, Y), \rho^A_V)$ there exists a unique homomorphism ϕ: $A[V] \to A[V; T]$ taking $F^A_V(X, Y)$, ρ^A_V, and $f^A_V(X)$ into $F^A_{V,T}(X, Y)$, $\rho^A_{V,T}$, and $f^A_{V,T}(X)$. We write $\bar{V}_i$ for $\phi(V_i)$. Then, as in

the special case $A = \mathbf{Z}_{(p)}$, $p = \pi$, $p = q$, we have the formulas

$$(21.7.6)\quad \pi a_n^A(V, T) = \pi T_n + \sum_{i=1}^{n-1} a_{n-i}^A(V, T) V_i^{q^{n-i}} + \sum_{k=2}^{n} \sum_{\substack{i+j=k \\ i,j \geq 1}} a_{n-k}^A(V)(V_i^{q^{n-k}} T_j^{q^{n-j}} - T_j^{q^{n-k}} V_i^{q^{n-i}})$$

$$(21.7.7)\quad \bar{V}_n - V_n = \pi T_n + \sum_{i=1}^{n-1} a_{n-i}^A(V, T)(V_i^{q^{n-i}} - \bar{V}_i^{q^{n-i}}) + \sum_{k=2}^{n} \sum_{\substack{i+j=k \\ i,j \geq 1}} a_{n-k}^A(V)(V_i^{q^{n-k}} T_j^{q^{n-j}} - T_j^{q^{n-k}} V_i^{q^{n-i}})$$

$$(21.7.8)\quad \bar{V}_n = V_n + \pi T_n + \sum_{\substack{i+j=n \\ i,j \geq 1}} (V_i T_j^{q^i} - T_j \bar{V}_i^{q^j}) + \sum_{k=1}^{n-1} a_{n-k}^A(V)(V_k^{q^{n-k}} - \bar{V}_k^{q^{n-k}}) + \sum_{k=2}^{n-1} a_{n-k}^A(V) \sum_{\substack{i+j=k \\ i,j \geq 1}} (V_i^{q^{n-k}} T_j^{q^{n-j}} - T_j^{q^{n-k}} \bar{V}_i^{q^{n-i}})$$

These are proved exactly as in the special case $A = \mathbf{Z}_{(p)}$, $\pi = p = q$ in 19.3. The details are left to the reader.

We have also a theorem analogous to Theorem (19.2.6) which makes these formulas useful, except that we do not have a criterion in terms of curves or similar objects for being A-typical. At first sight it seems that this would imply that we have to restrict ourselves to the case where A-logarithms exist. However, there is a way around that because we have a functorial way of making formal A-modules A-typical; cf. (21.7.17)–(21.7.18).

■ (21.7.9) **Theorem** Let $(F(X, Y), \rho_F)$ and $(G(X, Y), \rho_G)$, be a pair of A-typical formal A-modules over B and let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a strict isomorphism of formal A-modules. Then there exists a unique homomorphism of A-algebras ϕ: $A[V, T] \to B$ such that $\phi_* F_V^A(X, Y) = F(X, Y)$, $\phi_* \rho_V^A = \rho_F$, $\phi_* F_{V.T}^A(X, Y) = G(X, Y)$, $\phi_* \rho_{V.T}^A = \rho_G$, $\phi_* \alpha_{V.T}^A(X) = \alpha(X)$.

In other words, the triple $((F_V^A(X, Y), \rho_V^A), \alpha_{V.T}^A(X), (F_{V.T}^A(X, Y), \rho_{V.T}^A))$ is universal for strict isomorphisms of A-typical formal A-modules.

Proof We shall first prove this theorem under the extra hypothesis that B is A-torsion free, i.e., that $B \to B \otimes_A K$ is injective and then later in (21.7.17), (21.7.18) remove this hypothesis.

There are unique $v_i \in B$ such that if ϕ_0: $A[V, T] \to B$ is the homomorphism $\phi_0(V_i) = v_i$, $\phi_0(T_i) = 0$ then $\phi_{0*} F_V^A(X, Y) = F(X, Y)$, $\phi_{0*} \rho_V^A = \rho_F$ (universality

of $F_V^A(X, Y)$, ρ_V^A). Now suppose we have already found unique $t_1, \ldots, t_{n-1}$ such that if $\phi_{n-1}\colon A[V, T] \to B$ is the homomorphism $V_i \mapsto v_i$, $i = 1, 2, \ldots$; $T_i \mapsto t_i$, $i = 1, \ldots, n-1$; $T_i \mapsto 0$ if $i \geq n$, then

$$(21.7.10) \qquad (\phi_{n-1})_* \alpha_{V,T}^A(X) \equiv \alpha(X) \mod(\text{degree } q^{n-1} + 1)$$

$$(\phi_{n-1})_* F_{V,T}^A(X) \equiv G(X, Y) \mod(\text{degree } q^{n-1} + 1)$$

By uniqueness of A-logarithms (21.7.10) implies

$$(21.7.11) \qquad (\phi_{n-1})_* f_{V,T}^A(X) \equiv A\text{-}\log_G(X) \mod(\text{degree } q^{n-1} + 1)$$

(More precisely we use here that if two formal A-modules with A-logarithms are congruent mod(degree n), then their A-logarithms are also congruent mod(degree n). This is proved in the same way as the uniqueness of A-logarithms; cf. (21.5.7).)

Because $F_{V,T}^A(X, Y)$ and $G(X, Y)$ are both A-typical, (21.7.11) implies that

$$(21.7.12) \qquad (\phi_{n-1})_* f_{V,T}^A(X) \equiv A\text{-}\log_G(X) \mod(\text{degree } q^n)$$

and hence that

$$(\phi_{n-1})_* F_{V,T}^A(X) \equiv G(X, Y) \mod(\text{degree } q^n)$$

which in turn implies that

$$(21.7.13) \qquad (\phi_{n-1})_* \alpha_{V,T}^A(X) \equiv \alpha(X) \mod(\text{degree } q^n)$$

again essentially because A-logarithms are unique (cf. the remark just below (21.7.11)).

Now

$$(21.7.14) \qquad \alpha_{V,T}^A(X) \equiv X - T_n X^{q^n}$$

$$\mod(V_1, V_2, \ldots; T_1, T_2, \ldots, T_{n-1}; \text{degree } q^n + 1)$$

so that, given (21.7.13), we can find a unique $t_n \in B$ such that (21.7.10) holds with $n-1$ replaced by n. By induction we thus find a unique $\phi\colon A[V, T] \to B$ taking $F_V^A(X, Y)$, ρ_V^A, $\alpha_{V,T}^A(X, Y)$ into $F(X, Y)$, ρ_F, $\alpha(X)$, $G(X, Y)$. Because $\alpha(X)$ is a strict isomorphism of formal A-modules and A-logarithms are unique, it follows that also $\phi_* \rho_{V,T}^A = \rho_G$. This concludes the proof.

■ (21.7.15) **Remark** If B is of characteristic zero, then every formal group law (strict) isomorphism over B is automatically a formal A-module (strict) isomorphism. This holds also for (strict) isomorphisms between formal A-modules that admit unique A-logarithms.

■ (21.7.16) **Remark** If in Theorem (21.7.9) $\alpha(X)$ is just a strict isomorphism of formal group laws, then there still exists a unique $\phi\colon A[V, T] \to B$ taking $F_V^A(X, Y)$, ρ_V^A, $\alpha_{V,T}^A(X)$, $F_{V,T}^A(X, Y)$ into $F(X, Y)$, ρ_F, $\alpha(X)$, $G(X, Y)$ and it also satisfies $\phi_* \rho_{V,T}^A = \rho_G$ if and only if $\alpha(X)$ is a formal A-module morphism. This follows immediately from the proof.

■ (21.7.17) We still have to remove the unnecessary hypothesis that $B \to B \otimes_A K$ is injective. To do this we first need to know something more about the universal way of making a formal A-module A-typical, which is provided by the strict isomorphism $\alpha^A_{S,V}\colon F^A_S(X, Y) \to F^A_V(X, Y)$ over $A[S]$, where we have identified V_i with S_{q^i}. Here $F^A_S(X, Y)$ is the universal formal A-module of (21.4.8) and $F^A_V(X, Y)$ is the universal A-typical formal A-module of 21.5, and $\alpha^A_{S,V}(X) = (f^A_V)^{-1}(f^A_S(X))$. First, we notice that (still identifying V_i and S_{q^i})

$$f^A_S(X) \equiv f^A_V(X) \mod(\ldots, S_j, \ldots; j \text{ not a power of } q)$$

and hence

$$\alpha^A_{S,V}(X) \equiv X \mod(\ldots, S_j, \ldots; j \text{ not a power of } q)$$

Now let $F(X, Y)$ be a formal A-module over an A-algebra R and suppose that $R \to B$ is a surjective A-algebra homomorphism with kernel $\mathfrak{m}$ and suppose that the reduction $\bar{F}(X, Y)$ over B of $F(X, Y)$ is A-typical. Let $\phi\colon A[S] \to R$ be the unique homomorphism such that $\phi_* F^A_S(X, Y) = F(X, Y)$; then because $\bar{F}(X, Y)$ is A-typical, we must have $\phi(S_i) \in \mathfrak{m}$ if i is not a power of q (by the uniqueness part of the universality property of $F^A_S(X, Y)$), which in particular means that $\phi_*(\alpha^A_{S,V}(X)) \equiv X \mod \mathfrak{m}$ so the reduction of $\phi_*(\alpha^A_{S,V}(X))$ is the identity; i.e., in words, if $\bar{F}(X, Y)$ is A-typical, then the A-typical version of $F(X, Y)$ also reduces to $\bar{F}(X, Y)$; we have, so to speak, a commutative diagram

$$\begin{array}{ccc} F(X, Y) & \overset{\alpha(X)}{} & \hat{F}(X, Y) \\ \Big| & & \Big| \\ \bar{F}(X, Y) & = & \bar{F}(X, Y) \end{array}$$

where $\alpha(X) = \phi_*(\alpha^A_{S,V}(X))$ and $\hat{F}(X, Y) = \alpha F(\alpha^{-1}(X), \alpha^{-1}(Y))$ is the A-typical version of $F(X, Y)$.

■ (21.7.18) **Removal of the hypothesis $B \to B \otimes_A K$ is injective from the proof of Theorem (21.7.9)** Let $B \in \mathbf{Alg}_A$ and let R be any A-algebra such that there is a surjective A-algebra homomorphism $R \to B$ and such that $R \to R \otimes_A K$ is injective. (Such an R exists; take, e.g., $R = A[\ldots, Z_b, \ldots | b \in B]$, the A-algebra of polynomials in the indeterminates Z_b, one such indeterminate for every $b \in B$.)

Let $\alpha(X)\colon F(X, Y) \to G(X, Y)$ be a strict isomorphism of A-typical formal A-modules. Let $\tilde{F}(X, Y)$ be an A-typical formal A-module over R that lifts $F(X, Y)$. (Note that $\tilde{F}(X, Y)$ exists because the universal A-typical formal A-module is defined over a *free* commutative A-algebra.) Let $\hat{\alpha}(X)$ be any strict power series over R that lifts $\alpha(X)$ and let $\hat{G}(X, Y)$ be the formal A-module $\hat{\alpha}(F(\hat{\alpha}^{-1}(X), \hat{\alpha}^{-1}(Y)))$. Then $\hat{G}(X, Y)$ reduces to $G(X, Y)$. Making $\hat{G}(X, Y)$ A-typical gives us an A-typical formal A-module $\tilde{G}(X, Y)$ that also reduces to $G(X, Y)$ (by (21.7.17)) and a strict isomorphism

$$\tilde{\alpha}(X)\colon F(X, Y) \xrightarrow{\hat{\alpha}} \hat{G}(X, Y) \to \tilde{G}(X, Y)$$

which reduces to $\alpha(X)$ mod $\mathfrak{m}$, where $\mathfrak{m} = \mathrm{Ker}(R \to B)$. By Theorem (21.7.9) (in the torsion free case) $\tilde{\alpha}(X)$ is of the form $\alpha^A_{v,t}(X)$ for suitable sequences $v = (v_1, v_2, \ldots)$, $t = (t_1, t_2, \ldots)$ of elements of R. Hence $\alpha(X) = \alpha^A_{\bar{v},\bar{t}}(X)$ where $\bar{v}_i$, $\bar{t}_i$ are the residue classes mod $\mathfrak{m}$ of v_i, t_i. This proves the existence of a ϕ: $A[V, T] \to B$ that takes the universal triple into the given one. Uniqueness of ϕ is much easier and results from the simple observation that ϕ is in any case unique on $A[V] \subset A[V, T]$ (by the universality of $F^A_V(X, Y)$) and from the congruence $\alpha^A_{V,T}(X) \equiv X - T_n X^{q^n} \bmod(V_1, \ldots, V_n; T_1, \ldots, T_{n-1}; \text{degree } q^n + 1)$, which has already been used (cf. (21.7.14)).

This concludes the proof of Theorem (21.7.9).

21.8 Endomorphisms and isomorphisms of formal A-modules

■(21.8.1) **Formal A-module height** In this section we suppose that A is the ring of integers in some finite extension K of $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$. We write m for the degree of K over $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$ as the case may be. As usual we use π to denote a (fixed) uniformizing element and $q = p^r$ to denote the number of elements of the residue field. Further, in this section B is always the ring of integers in some finite extension L of K and π_L is a uniformizing element of L. The residue field of L is denoted k_L. For much of what follows, these conditions are unnecessarily restrictive, especially the completeness of A and B. Note that in the setting described formal A-modules over B always have A-logarithms.

■(21.8.2) **Definition** Let A be of characteristic zero and let $F(X, Y)$ be a formal A-module over B (where B is as above in (21.8.1)) and suppose that $F(X, Y)$ is of height h (cf. 18.3). We define the formal A-module height of $F(X, Y)$, also called A-height, and denoted h^A or A-ht, as the number h/m where $m = [K : \mathbf{Q}_p]$. We claim that $h^A(F(X, Y))$ is always an integer (or ∞).

This is seen as follows. We can assume that $F(X, Y)$ is of the form $F^A_v(X, Y)$ where $v = (v_1, v_2, \ldots)$ is a sequence of elements of B and where $F^A_v(X, Y)$ is obtained from the universal A-typical formal A-module $F^A_V(X, Y)$ by substituting v_i for V_i. Let t be the largest number in $\mathbf{N} \cup \{\infty\}$ such that $v_i \in \pi_L B$ for all $i < t$. The coefficients of $\rho^A_V(a)(X) = (f^A_V)^{-1}(af^A_V(X))$ for all $a \in A$ are polynomials in the $V_1, V_2, \ldots$ with coefficients in A. Also

$$(21.8.3) \quad f^A_V(X) \equiv X + \pi^{-1} V_i X^{q^i} \quad \bmod(V_1, \ldots, V_{i-1}, \text{degree } q^i + 1)$$

and since $f^A_V(X) \equiv X \bmod(V_1, V_2, V_3, \ldots)$, we have

$$\rho^A_V(a)(X) \equiv aX \quad \bmod(V_1, V_2, V_3, \ldots)$$

It follows that if $t = \infty$, then $\rho^A_v(\pi)(X) \equiv 0 \bmod \pi$, so that $\mathrm{ht}(F) = \infty$; and if $t < \infty$, then (by (21.8.3) and the formula above) $\rho^A_v(\pi)(X) \equiv v_t X^{q^t} \bmod(\pi, \text{degree } q^t + 1)$. Since $p = \pi^e u$ for some unit $u \in A^*$, it follows that

$$[p]_F(X) = \rho^A_v(p)(X) \equiv u v_t v_t^q \cdots v_t^{q^{(e-1)t}} X^{q^{et}} \quad \bmod(\pi, \text{degree } q^{et} + 1)$$

so that $\mathrm{ht}(F(X, Y)) = ret$ and $A\text{-ht}(F(X, Y)) = ret/m = t$, which is in $\mathbf{N} \cup \{\infty\}$.

If $\mathrm{char}(B) = p$, then $\mathrm{ht}(F(X, Y))$ is always ∞, giving us no information at all. However, we can still consider the power series $\rho_F(\pi)(X)$ which may or may not be congruent to zero mod π. Let $\hat{t}$ be the largest element of $\mathbf{N} \cup \{\infty\}$ such that $\rho_F(\pi)(X) \equiv 0 \bmod(\pi, \text{degree } \hat{t})$. Then by the arguments above (since $\hat{t}$ is clearly invariant under isomorphisms) we know that $\hat{t}$ is of the form q^t for some $t \in \mathbf{N} \cup \{\infty\}$. We now define in this case $A\text{-ht}(F(X, Y)) = t$. In the characteristic zero case this agrees with the definition via ordinary height.

It is easy to check that also in this case isomorphic formal A-modules have the same A-height, so there exist many nonisomorphic formal A-modules over, e.g., $\mathbf{F}_p[t]$ or $\mathbf{F}_p[\![t]\!]$.

■ (21.8.4) **Proposition** A formal A-module $F(X, Y)$ over B is of infinite A-height if and only if $\pi^e f(X) \equiv 0 \bmod \pi B$, where $f(X)$ is the A-logarithm of $F(X, Y)$ and e is the ramification index of L/K.

Proof We can assume that $F(X, Y)$ is A-typical (Theorem (21.5.6)). Let $F(X, Y) = F_v(X, Y)$. Then $v_i \in \pi_L B$ for all i iff $A\text{-ht}(F(X, Y)) = \infty$, cf. (21.8.2). Now assume that $v_i \in \pi_L B$ for all $i = 1, 2, \ldots$. Let $f(X) = \sum a_n X^{q^n}$ be the A-logarithm of $F(X, Y)$. The coefficients a_n, $n \geq 1$, are sums of terms of the form

$$\pi^{-r} v_{i_1} v_{i_2}^{q^{i_1}} \cdots v_{i_r}^{q^{i_1 + \cdots + i_{r-1}}}$$

Let v_L be the normalized exponential valuation on L. It follows that $v_L(\pi_L^{e^2 - e} a_n) \geq e^2 - e + 1 + q + \cdots + q^{r-1} - re \geq 2^r - 1 - re + e^2 - e$. For fixed r the minimum of this is assumed for $e = \frac{1}{2}(r + 1)$, and this minimum is equal to $2^r - 1 - \frac{1}{4}(r^2 + 2r + 1)$ which is ≥ 0 for all $r \geq 1$.

Inversely, suppose that $\pi^t f(X) \in \pi B[\![X]\!]$ for some (large) $t \in \mathbf{N}$. Assume that $A\text{-}ht(F(X, Y)) = h < \infty$. Then $f^{-1}(\pi^t f(X)) = [\pi^t]_F(X) \equiv uX^{q^{ht}} \bmod (\pi_L, \text{degree } (q^{ht} + 1))$ for some unit $u \in B^*$. Hence $\pi^t f(X) \equiv uX^{q^{ht}} \bmod (\pi_L, \text{degree } (q^{ht} + 1))$. This is a contradiction proving that $A\text{-}ht(F(X, Y)) = \infty$.

Remark The second half of the proof shows that $\lim_{n \to \infty} v_L(a_n) = -\infty$ if $A\text{-}ht(F(X, Y)) < \infty$.

■ (21.8.5) **Functional equation formal A-modules** We shall call a formal A-module $(F(X, Y), \rho_F)$ over B a functional equation formal A-module if its A-logarithm $f(X)$ satisfies a functional equation

$$f(X) - \sum_{i=1}^{\infty} \pi_L^{-1} v_i(\sigma_*^i) f(X^{q^i}) \in B[\![X]\!]$$

where π_L is a uniformizing element of L and where $\sigma\colon L \to L$ is a lift of the Frobenius automorphism in $\mathrm{Gal}(k_L/k)$, $x \mapsto x^q$.

As an analogue to Proposition (20.1.3) we have in the formal A-module case

■ (21.8.6) **Proposition** If L/K is unramified, then every formal A-module over B is a functional equation formal A-module.

Proof By part (iii) of the functional equation lemma and Theorem (21.5.6) it suffices to consider the case that $(F(X, Y), \rho_F)$ is an A-typical formal A-module. $A\text{-}\log_F(X) = f(X)$ then looks like

$$f(X) \equiv X + \pi^{-1} v_1 X^q \mod(\text{degree } q + 1)$$

for a certain $v_1 \in B$. Now suppose we have already found $v_1, \ldots, v_{n-1}$ such that

$$f(X) \equiv X + \sum_{i=1}^{n-1} \pi^{-1} v_i(\sigma_*^i) f(X^{q^i}) \mod(\text{degree } q^{n-1} + 1) \tag{21.8.7}$$

The formal A-module $F(X, Y)$ and the formal A-module with A-logarithm equal to

$$\hat{f}(X) = X + \sum_{i=1}^{n-1} \pi^{-1} v_i(\sigma_*^i) \hat{f}(X^{q^i})$$

are both A-typical. It follows that the congruence (21.8.7) holds mod(degree q^n), and then via the universality of $F_V^A(X, Y)$ we see that there is a $v_n \in B$ such that

$$\hat{f}(X) \equiv f(X) - \pi^{-1} v_n X^{q^n} \mod(\text{degree } q^n + 1)$$

which implies that

$$f(X) \equiv X + \sum_{i=1}^{n} \pi^{-1} v_i(\sigma_*^i) f(X^{q^i}) \mod(\text{degree } q^n + 1)$$

■ (21.8.8) **Homomorphisms, isomorphisms, and endomorphisms over B** Let $F(X, Y)$ and $G(X, Y)$ be two formal A-modules over B. Since $F(X, Y)$ and $G(X, Y)$ have A-logarithms, every homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ must be of the form $g^{-1}(bf(X))$ for some $b \in B$ (because the only formal A-module endomorphisms of the additive formal A-module $\hat{\mathbf{G}}_a(X, Y)$ over L are of the form bX, $b \in L$; cf. (21.5.7); this holds also if A and B are of characteristic p).

So $g^{-1}(bf(X))$ is a homomorphism of formal A-modules if and only if the power series $g^{-1}(bf(X))$ has its coefficients in B. If the characteristic of B is p, this does not mean that every formal group law homomorphism (resp. (strict) isomorphism) is automatically a formal A-module homomorphism (resp. (strict) isomorphism) because if $\text{char}(B) = p$, there may be homomorphisms (resp. (strict) isomorphisms) of formal group laws that are not of the form $g^{-1}(bf(X))$.

Indeed, we have seen that as a formal group law every formal A-module over B is strictly isomorphic to $\hat{\mathbf{G}}_a(X, Y)$, but (by the uniqueness of A-logarithms) the formal A-module $G(X, Y)$ is strictly isomorphic to the additive formal A-module $\hat{\mathbf{G}}_a(X, Y)$ iff $A\text{-}\log_G(X) = g(X)$ is in $B[\![X]\!]$ (which implies that $A\text{-ht}(G(X, Y)) = \infty$).

If now $F(X, Y)$ and $G(X, Y)$ are functional equation formal A-modules

(which is always the case if L/K is unramified), then we have available all the results of Section 20.3 (Honda's noncommutative power series techniques).

It is perhaps appropriate at this point to remark that the results of 20.3 also hold if A is the ring of integers of a finite extension of $\mathbf{F}_p((t))$ and similarly for B (the role of $B \otimes_{\mathbf{Z}} \mathbf{Q}$ is then played by $B \otimes_A K = L$).

Of the results of 20.3 that thus acquire their formal A-module analogues we single out for special mention the analogue of Theorem (20.3.12).

■(21.8.9) **Theorem** Let A, p, q, π, K be as in (21.8.1), and let L/K be unramified, B the ring of integers of L, and $\sigma \in \mathrm{Gal}(L/K)$, the Frobenius automorphism. Then the strict isomorphism classes of (one dimensional) formal A-modules of height h over B correspond bijectively to elements of $B_\sigma[\![T]\!]$ of the form $\pi + \sum_{i=1}^{h} b_i T^i$ with $b_1, \ldots, b_{h-1} \in \pi B$ and $b_h \in B^*$, the units of B. The (classes of) formal A-modules corresponding to $\pi + \sum_{i=1}^{h} b_i T^i$ and $\pi + \sum_{i=1}^{h} \hat{b}_i T^i$ are isomorphic if and only if there is a unit $c \in B^*$ such that $b_i = c\hat{b}_i \sigma^i(c^{-1})$ for all $i = 1, 2, \ldots, h-1$.

In particular, if $F(X, Y)$ is a formal A-module of A-height 1 over A, then there exists an element $v_1 \in U(A)$ such that the logarithm $f(X)$ of $F(X, Y)$ satisfies $f(X) - \pi^{-1} v_1 f(X^q) \in A[\![X]\!]$ so that $F(X, Y)$ is a Lubin–Tate formal group law over A (with associated uniformizing element $\pi(F) = v_1^{-1}\pi$; cf. Chapter I, (8.3.16)–(8.3.23)).

The proof of this is exactly as the proof of Theorem (20.3.12). Note that completeness of B is essential for this proof.

To complete the picture we note that if $A\text{-ht}(F(X, Y)) = \infty$ (and L/K is unramified), then $F(X, Y)$ is isomorphic to the additive formal A-module (because if $v_i \in \pi B$ for all $i \in \mathbf{N}$, then $f_v^A(X) \in B[\![X]\!]$ as is immediately clear from the definition of $f_v^A(X)$; cf. (21.5.4) and (21.8.2).)

■(21.8.10) **Homomorphisms and endomorphisms of formal A-modules over the residue fields** Now let $F(X, Y)$ be a formal A-module over some extension l of k. Let L/K be the unramified extension of K covering l/k. By the existence of a universal formal A-module $F_A^S(X, Y)$ over $A[S]$ there exists a formal A-module $\tilde{F}(X, Y)$ over B that reduces mod π to $F(X, Y)$ and by Proposition (21.8.4) this formal A-module is of functional equation type, so that, up to strict isomorphism, we can assume that its A-logarithm $\tilde{f}(X)$ satisfies a functional equation

$$\tilde{f}(X) = X + \sum_{i=1}^{\infty} \pi^{-1} v_i(\sigma_*^i) \tilde{f}(X^{q^i})$$

Let $\vartheta \in B_\sigma[\![T]\!]$; as in Theorem (20.4.4) we associate to ϑ a power series $\alpha_\vartheta(X) = \tilde{f}^{-1}(\vartheta * \tilde{f}(X))$. We now have in this situation the following complements to Theorem (20.4.4).

■(21.8.11) **Complements to Theorem (20.4.4):**

(ii)$_A$ If $\alpha_\vartheta(X)$ has integral coefficients, then $\bar{\alpha}_\vartheta(X)$, its reduction mod π, is an endomorphism of the formal A-module $F(X, Y)$.

(vi)$_A$ Every formal A-module endomorphism of $F(X, Y)$ arises as an $\bar{\alpha}_\vartheta(X)$.

(21.8.12) **Proof of (21.8.11), part (ii)$_A$** We already know that $\bar{\alpha}_\vartheta(X)$ is an endomorphism of the formal group law $F(X, Y)$ by Theorem (20.4.4)(ii). Using Lemma (20.4.3) and the fact that $\sigma(a) = a$ for all $a \in A$, we have modulo π (just as in (20.4.6))

$$\begin{aligned}\tilde{f}(\alpha_\vartheta(\rho_F(a)(X))) &= (\vartheta * \tilde{f})(\rho_F(a)(X)) \equiv \vartheta * (\tilde{f}(\rho_F(a)(X)) \\ &= \vartheta * (a\tilde{f}(X)) = \vartheta a * \tilde{f}(X) = a\vartheta * \tilde{f}(X) = a(\vartheta * \tilde{f}(X)) \\ &= a\tilde{f}(\tilde{f}^{-1}(\vartheta * \tilde{f}(X)) = \tilde{f}(\rho_F(a)(\alpha_\vartheta(X))\end{aligned}$$

which by Lemma (20.4.2) (= part (iv) of the functional equation lemma) implies that $\alpha_\vartheta(\rho_F(a)(X)) \equiv \rho_F(a)(\alpha_\vartheta(X))$. (We used $\sigma(a) = a$ in the transition $\vartheta a = a\vartheta$ in $B_\sigma[\![T]\!]$.)

■(21.8.13) **Proof of (28.8.11), part** (vi)$_A$ Let $\bar{\alpha}(X)$ be an endomorphism of $F(X, Y)$ and let $\alpha(X)$ be any lift of $\bar{\alpha}(X)$ with coefficients in B. Then $\alpha(X)$ satisfies for all $a \in A$,

$$\alpha(\rho_F(a))(X) \equiv \rho_F(a)(\alpha(X)) \mod \pi$$

and this in turn implies that (Lemma (20.4.2))

$$\tilde{f}(\alpha(\rho_F(a)(X))) \equiv \tilde{f}\rho_F(a)(\alpha(X)) = a\tilde{f}(\alpha(X)) \mod \pi$$

By Lemma (21.8.14) below this means that there is a $\vartheta \in B_\sigma[\![T]\!]$ such that $\tilde{f}(\alpha(X)) \equiv \vartheta * \tilde{f}(X) \mod \pi$, which proves (vi)$_A$.

■(21.8.14) **Lemma** Let A, K, B, L, $\tilde{f}(X)$ be as above in (21.8.7). Let $\beta(X)$ be a power series with coefficients in L such that $\beta(\rho_F(a)(X)) \equiv a\beta(X) \mod \pi$ for all $a \in A$. Then there is a $\vartheta \in B_\sigma[\![T]\!]$ such that $\beta(X) \equiv \vartheta * \tilde{f}(X) \mod \pi$.

Proof We first observe that if $\hat{\beta}(X) = \vartheta * \tilde{f}(X)$ for any ϑ, then it satisfies $\hat{\beta}(\rho_F(a)(X)) \equiv a\hat{\beta}(X) \mod \pi$. Indeed, as in (21.8.12), using Lemma (20.4.3) and $\sigma(a) = a$, we obtain modulo π

$$\begin{aligned}\vartheta * \tilde{f}(\rho_F(a)(X)) \equiv \vartheta * (\tilde{f}(\rho_F(a)(X))) &= \vartheta * a\tilde{f}(X) \\ &= \vartheta a * \tilde{f}(X) = a\vartheta * \tilde{f}(X) = a(\vartheta * \tilde{f}(X))\end{aligned}$$

Now let $\beta(X)$ be such that $\beta(\rho_F(a)(X)) \equiv a\beta(X) \mod \pi$ for all $a \in A$. Let $\beta(X) = b_1 X + b_2 X^2 + \cdots$ and let b_r be the first coefficient which is not $\equiv 0 \mod \pi$. We then have $b_r a^r X^r \equiv a b_r X^r \mod \pi$ for all $a \in A$, which implies first that $b_r \in B$ and second that r is a power of q, say $r = q^i$. Now consider $\tilde{\beta}(X) =$

$\beta(X) - (b, T^t\tilde{f}(X))$. Then $\tilde{\beta}(X)$ also satisfies the condition $\tilde{\beta}(\rho_F(a)(X)) \equiv a\tilde{\beta}(X)$ and $\tilde{\beta}(X) \equiv 0 \bmod(\pi, \text{degree } r+1)$. By induction this completes the proof.

■ (21.8.15) **Calculation of a formal A-module endomorphism ring over a residue field** Let A be of characteristic zero and $F(X, Y)$ over A be the formal A-module with logarithm

$$f(X) = X + \pi^{-1}f(X^{q^h}) \tag{21.8.16}$$

This formal A-module has A-height h. Let $\bar{F}(X, Y)$ be the reduction of $F(X, Y)$ modulo π. Since A is of characteristic zero, we know that $\bar{F}(X, Y)$ has as a formal group law height hm. So that $\mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$ is the ring of integral elements in a division algebra over $\mathbf{Q}_p$ of rank h^2m^2 and invariant $(hm)^{-1}$. Let us write $A\text{-}\mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$ for the subring of formal A-module endomorphisms of $\bar{F}(X, Y)$. Now $a \mapsto \rho_F(a)(X) \mapsto \rho_F(a)(X)$ defines an embedding of A into $\mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$, and by the definition of the formal A-module structure of $\bar{F}(X, Y)$, the formal A-module endomorphisms of $\bar{F}(X, Y)$ are precisely those that commute with $A \subset \mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$. Using the commutant theorem of (20.2.16), we conclude that $A\text{-}\mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$ is the ring of integers of a central division algebra of rank h^2 over K.

One can calculate that its invariant is h^{-1}. More generally, one can repeat 20.2 in the formal A-module context (using (28.8.11)) to get hold of $A\text{-}\mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$ and to obtain (also in the characteristic p case):

■ (21.8.17) **Proposition** Let $F(X, Y)$ be the formal A-module with A-logarithm (21.8.16) and let $\bar{F}(X, Y)$ be its reduction modulo π. Then $A\text{-}\mathrm{End}_k(\bar{F}(X, Y) = A\text{-}\mathrm{End}_{\bar{\mathbf{F}}(p^\infty)}(\bar{F}(X, Y))$ is the ring of integers of a central division algebra over K of rank h^2 and invariant h^{-1}.

■ (21.8.18) Let $F(X, Y)$ be a formal A-module over B such that $A\text{-ht}(F(X, Y)) < \infty$. If A is of characteristic zero, then $F(X, Y)$ is also of finite height as a formal group law; and if B is a local A-algebra, it follows that the reduction homomorphism $A\text{-}\mathrm{End}_B(F(X, Y)) \to A\text{-}\mathrm{End}_k(\bar{F}(X, Y))$ is injective (cf. (18.3.11)). If A is of characteristic $p > 0$, this argument breaks down. Still we have

■ (21.8.19) **Proposition** Let $F(X, Y)$ be a formal A-module over B of finite A-height. Then $A\text{-}\mathrm{End}_B(F(X, Y)) \to A\text{-}\mathrm{End}_{k_L}(\bar{F}(X, Y))$ is injective.

Proof We can assume that $F(X, Y)$ is A-typical. Let $f(X) = \sum a_n X^{q^n}$ be the A-logarithm of $F(X, Y)$. Let $\alpha(X) \in A\text{-}\mathrm{End}_B(F(X, Y))$ be $\neq 0$ and suppose that $\bar{\alpha}(X) = 0$. Then $\alpha(X) = f^{-1}(bf(X))$ for a certain $0 \neq b \in \pi_L B$. It follows that $\alpha(X) \circ \alpha(X) \circ \cdots \circ \alpha(X) = f^{-1}(b^t f(X)) \in \pi B[\![X]\!]$ for large enough $t \in \mathbb{N}$. Hence $b^t f(X) \in \pi B[\![X]\!]$ because $\pi^n a_n \in B$ for all n. And this would imply that $A\text{-}ht(F(X, Y)) = \infty$ by (21.8.4). Q.E.D.

21.9 Classification of formal A-modules over an algebraically closed field of characteristic $p > 0$

Let A be a discrete valuation ring with finite residue field k of characteristic $p > 0$. Let q be the number of elements of k and let π be a uniformizing element of A. By $\bar{k}$ we denote a separably closed extension of k.

(21.9.1) Theorem

(i) Two formal A-modules over $\bar{k}$ are isomorphic (as formal A-modules) if and only if their A-heights are equal.

(ii) Every formal A-module of A-height $h < \infty$ over k is strictly isomorphic (as a formal A-module) to a unique formal A-module of the form $F_v^A(X, Y)$ with $v = (0, \ldots, 0, x, 0, 0, \ldots)$, $x \neq 0$ in the hth spot, $x \in \bar{k}$.

Proof Since every formal A-module over $\bar{k}$ is strictly isomorphic to an A-typical one, we can assume that the formal A-module $F(X, Y)$ over $\bar{k}$ is of the form $F(X, Y) = F_v^A(X, Y)$ with $v = (v_1, v_2, \ldots)$, $v_i \in \bar{k}$. The formal A-module height of $F(X, Y)$ is then the index of the first $v_i \neq 0$. Thus if A-height$(F(X, Y)) = \infty$, we have $F_v^A(X, Y) = \hat{\mathbf{G}}_a(X, Y)$.

Now suppose that A-height$(F(X, Y)) = h < \infty$. We shall now proceed to construct sequences of elements $v(n) = (v_1(n), v_2(n), \ldots$ and strict A-module isomorphisms

$$\alpha_n(X)\colon F_{v(n)}^A(X, Y) \to F_{v(n+1)}^A(X, Y) \tag{21.9.2}$$

such that

$$\begin{cases} v_i(n) = 0 & \text{for } i = 1, \ldots, h-1, h+1, \ldots, h+n-1 \\ v_h(n) \neq 0 \end{cases} \tag{21.9.3}$$

$$v(1) = v \tag{21.9.4}$$

$$\alpha_n(X) \equiv X \mod(\text{degree } q^n) \tag{21.9.5}$$

To obtain the isomorphisms $\alpha_n(X)$ we specify the universal isomorphism $\alpha_{V,T}^A(X)$ in various ways. Let $\bar{V}_1, \bar{V}_2, \ldots$ be the unique polynomials in V_i, T_i such that $F_{V,T}^A(X, Y) = F_{\bar{V}}^A(X, Y)$. Then one shows exactly as in (19.4.3) that

$$\bar{V}_n \equiv V_n \mod(V_1, \ldots, V_{n-1}, \pi) \tag{21.9.6}$$

$$\bar{V}_{n+h} \equiv V_{n+h} - T_n V_h^{q^n} + V_h T_n^{q^h} \tag{21.9.7}$$

$$\mod(V_1, \ldots, V_{h-1}, V_{h+1}, \ldots, V_{n+h-1}, T_1, \ldots, T_{n-1}, \pi)$$

We now proceed as in (19.4.12). Note that $v(1) = v$ satisfies (21.9.3). Given $v(n)$, take $t_i(n) = 0$ for $i \in \mathbf{N}\backslash\{n\}$ and let $t_n(n)$ be such that

$$v_{h+n}(n) - t_n(n)v_h(n)^{q^n} + v_h(n)t_n(n)^{q^h} = 0$$

and let $v_i(n+1) = \bar{V}_i(v(n), t(n))$, $\alpha_n(X) = \alpha^A_{v(n).t(n)}(X))$. Then (21.9.5) holds because $\alpha^A_{V.T}(X) \equiv X \bmod(T_1, \ldots, T_{n-1}, \text{degree } q^n)$. The composed isomorphisms

$$F^A_{v(1)}(X, Y) \to F^A_{v(2)}(X, Y) \to \cdots \to F^A_{v(n)}(X, Y)$$

converge because of (21.9.5) to a strict isomorphism $\alpha_\infty(X)$: $F^A_{v(1)}(X, Y) \to F^A_{v(\infty)}(X, Y)$ with $v_i(\infty) = 0$ if $i \neq h$ and $v_h(\infty) \neq 0$. A final isomorphism of the form $\beta(X) = u^{-1}X$, $u \neq 0$, gives an isomorphism

$$F^A_{v(\infty)}(X, Y) \to F^A_{\hat{v}(\infty)}(X, Y)$$

with $\hat{v}_i(\infty) = 0$ if $i \neq h$ and $\hat{v}_h(\infty) = u^{q^h-1}v_h(\infty)$, so with a suitable choice of u we can see to it that $\hat{v}_h(\infty) = 1$.

To finish the proof of part (i) of the theorem it now suffices to remark that formal A-modules of different A-heights are nonisomorphic. Suppose that $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is an isomorphism of formal A-modules. Then we must have $\alpha(X) \circ \rho_F(\pi) = \rho_G(\pi) \circ \alpha(X)$, and it follows that A-ht$(F(X, Y)) = A$-ht$(G(X, Y))$; cf. (21.8.2).

To finish the proof of part (ii) of the theorem we must show that two formal A-modules $F^A_{a\Delta_h}(X, Y)$, $F^A_{b\Delta_h}(X, Y)$, $a, b \in \bar{k}$, $\Delta_h = (0, 0, \ldots, 0, 1, 0, \ldots)$ are strictly isomorphic if and only if $a = b$. By Theorem (21.7.9) we know that such a strict isomorphism is necessarily of the form $\alpha^A_{a\Delta_h.t}(X)$ for a certain sequence $t = (t_1, t_2, \ldots)$ of elements of $\bar{k}$. We then have

$$\bar{V}_i(a\Delta_h, t) = \begin{cases} 0 & \text{if } i \neq h \\ b & \text{if } i = h \end{cases}$$

Using (21.9.6) with $n = h$, we see that this implies $a = b$.

22 Lifting and Reducing Formal Group Laws. Formal Moduli

In this section we study formal group laws (and formal A-modules) over a local ring B in connection with their reductions over the residue field k of B. Unless the opposite is explicitly stated, all formal group laws in this section will be one dimensional and commutative.

22.1 Formal group laws over $\mathbf{Z}_p$

Choose a prime number p. Let B be a ring and $v = (v_1, v_2, \ldots)$ a series of elements of B. We write $F_v(X, Y)$ for the formal group law obtained from the universal p-typical formal group law $F_V(X, Y)$ over $\mathbf{Z}[V]$ by substituting v_i for V_i for all $i \in \mathbf{N}$.

■ (22.1.1) **Proposition** Suppose that $a^p \equiv a \bmod pB$ for all $a \in B$, and that B is of characteristic zero; let $v = (v_1, v_2, \ldots)$, $\bar{v} = (\bar{v}_1, \bar{v}_2, \ldots)$ be two sequences of

elements of B. Then the formal group laws $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are strictly isomorphic over B if and only if $v_i \equiv \bar{v}_i \bmod(pB)$ for all $i \in \mathbf{N}$.

Proof First suppose that $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are strictly isomorphic over B. By the universality of the isomorphism $\alpha_{V,T}(X)\colon F_V(X, Y) \to F_{V,T}(X, Y)$ this means that there are $t_1, t_2, \ldots, \in B$ such that $f_{\bar{v}}(X) = f_{v,t}(X)$. By Corollary (19.3.6) we know that

$$\bar{v}_n - v_n = pt_n + \sum_{i=1}^{n-1} a_{n-i}(v, t)(v_i^{p^{n-i}} - \bar{v}_i^{p^{n-i}}) + \sum a_{n-k}(v)(v_i^{p^{n-k}} t_j^{p^{n-j}} - t_j^{p^{n-k}} v_i^{p^{n-i}}) \tag{22.1.2}$$

So in particular we see that $v_1 \equiv \bar{v}_1 \bmod(pB)$. Now suppose we have already shown that $v_i \equiv \bar{v}_i \bmod(pB)$ for all $i < n$. Then

$$v_i^{p^{n-i}} \equiv \bar{v}_i^{p^{n-i}} \bmod(p^{n-i+1}B) \tag{22.1.3}$$

and by the assumption on B, we also have

$$v_i^{p^{n-k}} t_j^{p^{n-j}} \equiv t_j^{p^{n-k}} v_i^{p^{n-i}} \bmod(p^{n-k+1}B) \tag{22.1.4}$$

So that, using $p^{n-i}a_{n-i}(v, t) \in B$, we obtain from (22.1.2)–(22.1.4) that $v_n \equiv \bar{v}_n \bmod(pB)$.

Conversely, suppose that $v_i \equiv \bar{v}_i$ for all $i \in \mathbf{N}$. Calculate t_i from v_i and $\bar{v}_i$ by means of formula (22.1.2). If we can show that $t_i \in B$ for all i, we are through because then (22.1.2) says that $f_{\bar{v}}(X) = f_{v,t}(X)$, so that $F_{\bar{v}}(X, Y)$ and $F_v(X, Y)$ are strictly isomorphic via $\alpha_{v,t}(X)$. We have $t_1 = p^{-1}(\bar{v}_1 - v_1)$ so that $t_1 \in B$. Now suppose that we have already shown that $t_i \in B$ for $i < n$. It then follows from (22.1.3) and (22.1.4) that

$$\bar{v}_n - v_n \equiv pt_n \bmod(pB)$$

and, since $\bar{v}_n \equiv v_n \bmod(pB)$, it follows that $t_n \in B$. This concludes the proof of the proposition.

■ (22.1.5) **Corollary** Under the assumptions of Proposition (22.1.1) the formal group laws $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are isomorphic if and only if $v_i \equiv \bar{v}_i \bmod(pB)$. (The only difference between this corollary and Proposition (22.1.1) is the omission of the word *strict*.)

Proof We only have to show that if $\alpha(X) = uX + u_2X^2 + \cdots$, $u \in B^*$, is an isomorphism $F_v(X, Y) \to F_{\bar{v}}(X, Y)$, then $v_i \equiv \bar{v}_i \bmod pB$ for all i. Now let $\beta(X) = uX$, $G(X, Y) = \beta F_v(\beta^{-1}(X), \beta^{-1}(Y))$. Then we have a commutative diagram of isomorphisms

$$\begin{array}{ccc} F_v(X, Y) & \xrightarrow{\beta(X)} & G(X, Y) \\ & {\scriptstyle\alpha(X)}\searrow \quad \swarrow{\scriptstyle\gamma(X)} & \\ & F_{\bar{v}}(X, Y) & \end{array}$$

with $\gamma(X) = u^{-1}\alpha(X)$ so that $\gamma(X)$ is a strict isomorphism. The logarithm of $G(X, Y)$ is easily seen to be equal to $g(X) = uf_v(u^{-1}X)$ so that $g(X) = f_{\hat{v}}(X)$ with

$$\hat{v}_i = u^{p^i - 1}v_i \tag{22.1.6}$$

(Use, e.g., formula (3.3.9) of Chapter I to see this.) Because $u^{p^i} \equiv u \bmod pB$, this gives us $\hat{v}_i \equiv v_i \bmod(pB)$, and by Proposition (22.1.1) we have that $\hat{v}_i \equiv \bar{v}_i \bmod(pB)$; this proves the corollary.

■ (22.1.7) **Corollary** Two p-typical formal group laws over $\mathbf{F}_p$, the field of p elements, are isomorphic if and only if they are identical.

Proof Let $F(X, Y)$, $G(X, Y)$ be two p-typical formal group laws over $\mathbf{F}_p$, and let $\alpha(X)$ be an isomorphism between these. As in the proof of (22.1.5) we break up $\alpha(X)$ into an isomorphism $\beta(X) = uX$: $F(X, Y) \to H(X, Y)$ and a strict isomorphism $\gamma(X)$: $H(X, Y) \to G(X, Y)$. Note that $H(X, Y)$ is also p-typical (use (22.1.6), e.g.). By the universality of the triple $(F_V(X, Y), \alpha_{V,T}(X), F_{V,T}(X, Y))$ there is over $\mathbf{Z}_{(p)}$ a strict isomorphism of formal group laws $\tilde{\gamma}(X)$: $\tilde{H}(X, Y) \to \tilde{G}(X, Y)$ which reduces to $\gamma(X)$ modulo p. Lifting $\beta(X)$ by an isomorphism $\tilde{\beta}(X) = \tilde{u}X$, $u \in \mathbf{Z}_{(p)}^*$ and setting $\tilde{F}(X, Y) = \tilde{u}^{-1}(\tilde{H}(\tilde{u}X, \tilde{u}Y))$, we find an isomorphism $\tilde{\alpha}(X)$: $\tilde{F}(X, Y) \to \tilde{G}(X, Y)$ between p-typical formal group laws that reduces modulo p to $\alpha(X)$: $F(X, Y) \to G(X, Y)$. Because $\tilde{F}(X, Y)$ and $\tilde{G}(X, Y)$ are p-typical isomorphic formal group laws over $\mathbf{Z}_{(p)}$, there are by Corollary (22.1.5) sequences of elements $v = (v_1, v_2, \ldots)$, $\bar{v} = (\bar{v}_1, \bar{v}_2, \ldots)$ of $\mathbf{Z}_{(p)}$ such that $\tilde{F}(X, Y) = F_v(X, Y)$, $\tilde{G}(X, Y) = F_{\bar{v}}(X, Y)$ and $v_i \equiv \bar{v}_i \bmod p$. It follows that $F(X, Y) = G(X, Y)$ by Lemma (22.1.8) below. This proves the corollary. (NB the isomorphism $\alpha(X)$ need not be the identity isomorphism!)

■ (22.1.8) **Lemma** Let $v = (v_1, v_2, \ldots)$, $\bar{v} = (\bar{v}_1, \bar{v}_2, \ldots)$ be two sequences of elements of a ring B. Then $F_v(X, Y) \equiv F_{\bar{v}}(X, Y) \bmod(pB)$ if and only if $v_i \equiv \bar{v}_i \bmod(pB)$.

Proof The coefficients of $F_v(X, Y)$ over $\mathbf{Z}[V]$ are polynomials in the V_i, say $F_V(X, Y) = \sum a_{ij}(V)X^iY^j$, and we have also

$$F_V(X, Y) \equiv X + Y + V_n C_{p^n}(X, Y) \quad \bmod(V_1, \ldots, V_{n-1}, \text{degree } p^n + 1) \tag{22.1.8a}$$

Now suppose that $v_i \equiv \bar{v}_i \bmod(pB)$ for $i = 1, \ldots, n-1$. Then it follows from (22.1.8a) that

$$F_v(X, Y) \equiv F_{\bar{v}}(X, Y) + (v_n - \bar{v}_n)C_{p^n}(X, Y) \quad \bmod(pB, \text{degree } p^n + 1)$$

which proves the lemma because $C_{p^n}(X, Y)$ is a primitive polynomial with coefficients in $\mathbf{Z}$.

■ (22.1.9) **Remark** There is a reason we have treated the essentially very trivial Lemma (22.1.8) so extensively. The reason is that the analogous result

for formal group laws over, e.g., $B = \mathbf{Z}_p$ constructed *directly* by means of a functional equation does *not* hold. Take for example $p = 2$, $B = \mathbf{Z}_2$, $\sigma =$ the identity endomorphism, $c \in B$, and let $F_c(X, Y)$ be the formal group law with logarithm

$$f_c(X) = X + \frac{c}{2} f_c(X^2)$$

A little bit of explicit calculation then gives that mod(degree 5)

$$F_c(X, Y) \equiv X + Y - cXY + c^2(XY^2 + X^2Y) - \left(\frac{5c^3}{2} + \frac{3c^2}{2}\right) X^2Y^2 - (c^2 + c^3)(XY^3 + X^3Y)$$

(Note that this is always integral because $c^3 \equiv c^2 \bmod 2$ for all $c \in \mathbf{Z}_2$.) Substituting $c = 1$ and $c = -1$, we see that $F_1(X, Y) \not\equiv F_{-1}(X, Y)$ mod(2, degree 5).

■ (22.1.10) **Theorem** Two formal group laws $F(X, Y)$, $G(X, Y)$ over $\mathbf{Z}_{(p)}$ or $\mathbf{Z}_p$ (or any ring between) are isomorphic if and only if their reductions modulo p, $\bar{F}(X, Y)$, $\bar{G}(X, Y)$, over $\mathbf{F}_p$ are isomorphic.

Proof Suppose that $\bar{F}(X, Y)$ and $\bar{G}(X, Y)$ over $\mathbf{F}_p$ are isomorphic. Since every formal group law over $\mathbf{Z}_{(p)}$ or $\mathbf{Z}_p$ is strictly isomorphic to a p-typical formal group, we can assume that $F(X, Y)$ and $G(X, Y)$ are p-typical. Then there are sequences $v = (v_1, v_2, \ldots)$, $\bar{v} = (\bar{v}_1, \bar{v}_2, \ldots)$ with $v_i, \bar{v}_i$ in $\mathbf{Z}_{(p)}$ or $\mathbf{Z}_p$ such that $F_v(X, Y) = F(X, Y)$, $G(X, Y) = F_{\bar{v}}(X, Y)$. Because $\bar{F}(X, Y)$ is isomorphic to $\bar{G}(X, Y)$ over $\mathbf{F}_p$, it follows that $\bar{F}(X, Y) = \bar{G}(X, Y)$ (Corollary (22.1.7)) which implies that $v_i \equiv \bar{v}_i \bmod(p)$ by Lemma (22.1.8) and this result in turn implies that $F(X, Y) = F_v(X, Y)$ and $G(X, Y) = F_{\bar{v}}(X, Y)$ are strictly isomorphic by Proposition (22.1.1).

■ (22.1.11) **Corollary** (of the proof) Two formal group laws over $\mathbf{Z}_{(p)}$ or $\mathbf{Z}_p$ are strictly isomorphic if they are isomorphic.

We conclude this subsection with two counterexamples to imaginable generalizations of Theorem (22.1.10).

■ (22.1.12) **Example** Let $W_{3^2}(\mathbf{F}_9) = \mathbf{Z}_3[i]$, $i^2 = -1$, be the ring of integers of the unramified extension of degree 2 of $\mathbf{Q}_3$. Consider the sequences of elements $v = (0, i, 0, 0, \ldots)$ and $\bar{v} = (3i, i, 0, 0, \ldots)$, and consider the formal group laws $F_v(X, Y)$, $F_{\bar{v}}(X, Y)$ over $\mathbf{Z}_3[i]$. The reductions mod 3 of these formal group laws over $\mathbf{F}_9$ are equal. We show that $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are not isomorphic over $\mathbf{Z}_3[i]$.

Indeed, suppose that $\alpha(X) = uX + u_2X^2 + \cdots$ were an isomorphism. As usual we break up $\alpha(X)$ into a composite

$$F_v(X, Y) \xrightarrow{\beta(X)} G(X, Y) \xrightarrow{\gamma(X)} F_{\bar{v}}(X, Y)$$

where $\beta(X) = uX$ and $\gamma(X)$ is a strict isomorphism. Then $G(X, Y) = uF_v(u^{-1}X, u^{-1}Y)$, so that $\log_G(X) = u \log_F(u^{-1}X)$, which means that $G(X, Y) = F_{\hat{v}}(X, Y)$ with $\hat{v} = (0, u^{-8}i, 0, 0, \ldots)$. Now $\gamma(X)$ is a strict isomorphism between p-typical formal group laws. By the universality of the strict isomorphism $\alpha_{V,T}(X)$ this means that there must be elements $t_1, t_2, \ldots$ in $\mathbf{Z}_3[i]$ such that $f_{\bar{v}}(X) = f_{\hat{v},t}(X)$. According to Proposition (19.3.5) this means that we must have

$$\frac{\bar{v}_1}{3} = \frac{\hat{v}_1}{3} + t_1$$

i.e., $t_1 = i$, and (looking at the coefficients of X^{27})

$$\frac{\bar{v}_3}{3} + \bar{a}_1 \frac{\bar{v}_2^3}{3} + \bar{a}_2 \frac{\bar{v}_1^9}{3} = \frac{\hat{v}_3}{3} + \bar{a}_1 \frac{\hat{v}_2^3}{3} + \bar{a}_2 \frac{\hat{v}_1^9}{3} + \frac{\hat{v}_1}{3}\left(\frac{\hat{v}_1^3 t_1^9 - t_1^3 \hat{v}_1^9}{3}\right) + \frac{\hat{v}_1 t_2^3 - t_2 \hat{v}_1^9}{3} + \frac{\hat{v}_2 t_1^9 - t_1 \hat{v}_2^3}{3} + t_3$$

where $f_{\bar{v}}(X) = \sum_{i=0}^{\infty} \bar{a}_i X^{3^i}$. Substituting the known values of $\bar{v}_1, \bar{v}_2, \bar{v}_3, \ldots, \hat{v}_1, \hat{v}_2, \ldots$, i.e., $\bar{v}_1 = 3i$, $\hat{v}_1 = 0$, $\bar{v}_2 = i$, $\hat{v}_2 = u^{-8}i$, $\bar{v}_3 = \hat{v}_3 = 0$, we find that we must have

$$\bar{a}_1 \frac{\bar{v}_2^3}{3} + \bar{a}_2 \frac{\bar{v}_1^9}{3} = \bar{a}_1 \frac{\hat{v}_2^3}{3} + \frac{\hat{v}_2 t_1^9 - t_1 \hat{v}_2^3}{3} + t_3 \tag{22.1.13}$$

Now $\bar{a}_1 = \frac{1}{3}\bar{v}_1 = i$, and $\hat{v}_2 = u^{-8}i \equiv i = \bar{v}_2 \bmod 3$ so that $\bar{a}_1(\bar{v}_2^3/3) \equiv \bar{a}_1(\hat{v}_2^3/3) \bmod(\mathbf{Z}_3[i])$. Further, $\bar{v}_1^9 = (3i)^9 \equiv 0 \bmod(3^3\mathbf{Z}_3[i])$ so that $3^{-1}\bar{a}_2\bar{v}_1^9 \equiv 0 \bmod(\mathbf{Z}_3[i])$. Hence it follows from (22.1.13) that we must have

$$\hat{v}_2 t_1^9 - t_1 \hat{v}_2^3 \equiv 0 \bmod(3\mathbf{Z}_3[i]) \tag{22.1.14}$$

However $t_1 = i$ and $\hat{v}_2 = u^{-8}i \equiv i \bmod 3$, which contradicts (22.1.14).

■ (22.1.15) **Example** Now let $F_V(X, Y)$ over $\mathbf{Z}[V]$ be the two dimensional universal p-typical formal group of Chapter II, Section 10.3. Consider the two sequences of 2×2 matrices

$$v = \left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \ldots\right)$$

$$\bar{v} = \left(\begin{pmatrix}1 & p\\ p & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \ldots\right)$$

and let $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ be the formal group laws over $\mathbf{Z}$ that are obtained by substituting $v_i(j, k)$ and $\bar{v}_i(j, k)$ for $V_i(j, k)$ in $F_V(X, Y)$, $i = 1, 2, \ldots$, $j, k = 1, 2$. Then $\bar{F}_v(X, Y) = \bar{F}_{\bar{v}}(X, Y)$ over $\mathbf{F}_p$. We show that $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are not isomorphic over $\mathbf{Z}_p$. Note that $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are both of height 3, hence in particular of finite height.

Suppose that $\alpha(X)$: $F_v(X, Y) \to F_{\bar{v}}(X, Y)$ is an isomorphism. As usual we decompose $\alpha(X)$ into an isomorphism $\beta(X) = u^{-1}X$: $F_v(X, Y) \to G(X, Y)$ and a strict isomorphism $\gamma(X)$: $G(X, Y) \to F_{\bar{v}}(X, Y)$. Here u is an invertible (over $\mathbf{Z}_p$) 2×2 matrix. The logarithm of $G(X, Y)$ is equal to

$$\log_G(X) = u^{-1} f_v(uX)$$

As a rule $G(X, Y)$ is not a p-typical formal group law. However, by Chapter III, Theorem (15.2.9), $G(X, Y)$ is strictly isomorphic to a p-typical formal group law whose logarithm is obtained from $\log_G(X)$ by simply striking out all terms in $\log_G(X)$ that should not be there for a p-typical formal group law. This means that $G(X, Y)$ is strictly isomorphic to the p-typical formal group law $\hat{G}(X, Y)$ with logarithm

$$\log_{\hat{G}}(X) = X + u^{-1}a_1(v)u^{(p)}X^p + u^{-1}a_2(v)u^{(p^2)}X^{p^2} + \cdots \tag{22.1.16}$$

where $f_v(X) = \log_{F_v}(X) = \sum_{i=1}^{\infty} a_i(v)X^{p^i}$ and $u^{(p^i)}$ is the matrix obtained from u by raising each of its entries to the power p^i, and where, as usual, X^{p^i} denotes the column vector $(X_1^{p^i}, X_2^{p^i})$.

Composing the strict isomorphism $\hat{G}(X, Y) \to G(X, Y)$ with the strict isomorphism $\gamma(X)$: $G(X, Y) \to F_{\bar{v}}(X, Y)$, we find a strict isomorphism $\delta(X)$: $\hat{G}(X, Y) \to F_{\bar{v}}(X, Y)$. By the universality of the strict isomorphism $\alpha_{V,T}(X)$ (two dimensional case; cf. Section 19.2) this means that these must be 2×2 matrices $t_1, t_2, \ldots$ with coefficients in $\mathbf{Z}_p$ such that

$$f_{\hat{v},t}(X) = f_{\bar{v}}(X) \tag{22.1.17}$$

where $\hat{v} = (\hat{v}_1, \hat{v}_2, \ldots)$ is a sequence of matrices such that $F_{\hat{v}}(X, Y) = \hat{G}(X, Y)$. (Such a sequence of matrices exists because $\hat{G}(X, Y)$ is p-typical.) From (22.1.16) we see that

$$\frac{\hat{v}_1}{p} = u^{-1}a_1(v)u^{(p)} = u^{-1}\frac{v_1}{p}u^{(p)} \tag{22.1.18}$$

$$\frac{\hat{v}_1\hat{v}_1^{(p)}}{p^2} + \frac{\hat{v}_2}{p} = u^{-1}a_2(v)u^{(p^2)}$$

and (22.1.17) gives us that (cf. Proposition (19.3.5))

$$\frac{\hat{v}_1}{p} + t_1 = \frac{\bar{v}_1}{p} \tag{22.1.19}$$

$$a_1(\bar{v})\frac{\bar{v}_1^{(p)}}{p} + \frac{\bar{v}_2}{p} = t_2 + a_1(\bar{v})\frac{\hat{v}_1^{(p)}}{p} + \frac{\hat{v}_2}{p} + \frac{\hat{v}_1 t_1^{(p)} - t_1\hat{v}_1^{(p)}}{p}$$

Suppose that $u = \left(\begin{smallmatrix} b & c \\ d & e \end{smallmatrix}\right)$. Now $u^{(p)} \equiv u \bmod p$ and by (22.1.19) $\hat{v}_1 \equiv \bar{v}_1 \bmod p$. Using this in (22.1.18), we find that u must satisfy

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & c \\ d & e \end{pmatrix} \equiv \begin{pmatrix} b & c \\ d & e \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \mod p$$

This gives us $c \equiv d \equiv 0 \bmod p$ so that u is of the form

$$u = \begin{pmatrix} b & py \\ pz & e \end{pmatrix}$$

Substituting this in (22.1.18) gives that modulo p^2

$$\hat{v}_1 = \det(u)^{-1} \begin{pmatrix} e & -py \\ -pz & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b^p & p^p y^p \\ p^p z^p & e^p \end{pmatrix} \equiv \begin{pmatrix} b^{p-1} & 0 \\ -pze^{-1}b^{p-1} & 0 \end{pmatrix}$$

which by (22.1.18) and using $p^2 a_2(v) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ gives for $p\hat{v}_2$ that mod p^2

$$\begin{aligned} p\hat{v}_2 &\equiv \det(u)^{-1} \begin{pmatrix} e & -py \\ -pz & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} b^{p^2} & p^{p^2} y^{p^2} \\ p^{p^2} z^{p^2} & e^{p^2} \end{pmatrix} - \begin{pmatrix} b^{p^2-1} & 0 \\ -pe^{-1}zb^{p^2-1} & 0 \end{pmatrix} \\ &\equiv (eb)^{-1} \begin{pmatrix} e & -py \\ -pz & b \end{pmatrix} \begin{pmatrix} b^{p^2} & 0 \\ 0 & pe^{p^2} \end{pmatrix} - \begin{pmatrix} b^{p^2-1} & 0 \\ -pe^{-1}zb^{p^2-1} & 0 \end{pmatrix} \\ &\equiv \begin{pmatrix} 0 & 0 \\ 0 & pe^{p^2-1} \end{pmatrix} \end{aligned}$$

so that we find

$$\hat{v}_2 \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \bmod p, \qquad \hat{v}_1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \bmod p$$

This means that

$$\hat{v}_2 \equiv \bar{v}_2 \bmod p, \qquad \hat{v}_1 \equiv \bar{v}_1 \bmod p \tag{22.1.20}$$

and hence

$$\hat{v}_1^{\{p\}} \equiv \bar{v}_1^{\{p\}} \bmod p^2 \tag{22.1.21}$$

Using (22.1.20) and (22.1.21) in the second line of (22.1.19), we must have

$$\hat{v}_1 t_1^{\{p\}} - t_1 \hat{v}_1^{\{p\}} \equiv 0 \bmod p \tag{22.1.22}$$

But

$$t_1 = p^{-1}(\bar{v}_1 - \hat{v}_1) = p^{-1} \begin{pmatrix} 1 & p \\ p & 0 \end{pmatrix} - p^{-1} \begin{pmatrix} 1 + p\hat{y} & 0 \\ p\hat{z} & 0 \end{pmatrix} = \begin{pmatrix} -\hat{y} & 1 \\ 1 - \hat{z} & 0 \end{pmatrix}$$

where $\hat{z}$, $\hat{y} \in \mathbf{Z}_p$ are such that $b^{p-1} = 1 + p\hat{y}$, $-pzc^{-1}b^{p-1} = p\hat{z}$, so that modulo p

$$\hat{v}_1 t_1^{\{p\}} \equiv \hat{v}_1 t_1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} -\hat{y} & 1 \\ 1 - \hat{z} & 0 \end{pmatrix} \equiv \begin{pmatrix} -\hat{y} & 1 \\ 0 & 0 \end{pmatrix} \bmod p$$

$$t_1 \hat{v}_1^{\{p\}} \equiv t_1 \hat{v}_1 \equiv \begin{pmatrix} -\hat{y} & 1 \\ 1 - \hat{z} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} -\hat{y} & 0 \\ 1 - \hat{z} & 0 \end{pmatrix} \bmod p$$

which is a contradiction with (22.1.22). This proves that the two two-dimensional formal group laws $F_v(X, Y)$, $F_{\bar{v}}(X, Y)$ over $\mathbf{Z}_p$ are not isomorphic.

22.2 Formal A-modules over A

There is a nice generalization of Theorem (22.1.10) (in spite of the two counterexamples (22.1.12) and (22.1.15)). It is

■ (22.2.1) **Theorem** Let A be a discrete valuation ring with finite residue field k. Then two formal A-modules over A are (strictly) isomorphic if and only if the reductions of these formal A-modules over the residue field k of A are isomorphic (as formal A-modules over k).

■ (22.2.2) **Remark** A may be either of characteristic zero or characteristic $p > 0$.

■ (22.2.3) **Proof of Theorem (22.2.1)** This proof is almost completely analogous to the proof of Theorem (22.1.10) (which is essentially the case $A = \mathbf{Z}_{(p)}$). We outline the various steps. First, let $F_V^A(X, Y)$ be the one dimensional universal A-typical formal A-module over $A[V]$. Then one proves first the analogue of Proposition (22.1.2), viz:

(22.2.4) Let $v = (v_1, v_2, \ldots)$, $\bar{v} = (\bar{v}_1, \bar{v}_2, \ldots)$ be two sequences of elements of A. Then $F_v^A(X, Y)$ and $F_{\bar{v}}^A(X, Y)$ are strictly isomorphic (as formal A-modules) if and only if $v_1 \equiv \bar{v}_i \bmod(\pi)$ where π is a uniformizing element of A.

This is proved exactly as in the analogous statement (22.1.1) using the results of 21.5 and 21.7 instead of those of 19.3.

(22.2.5) Then as in (22.1.5) the simple fact that $a^q \equiv a \bmod \pi$ where q is the number of elements of k permits the removal of the word *strict* in statement (22.2.4).

(22.2.6) We now use a slightly different argument to finish the proof. Let $F(X, Y)$ and $G(X, Y)$ be two formal A-modules over A such that the reductions $\bar{F}(X, Y)$ and $\bar{G}(X, Y)$ are isomorphic formal A-modules over k. By taking any lift over A of the isomorphism over k (and transporting the formal A-module structure via this lift) we are reduced to the case that $\bar{F}(X, Y) = \bar{G}(X, Y)$.

The isomorphism of formal A-modules (cf. (21.5.1))

$$(f_V^A)^{-1}(f_S^A(X)): F_S^A(X, Y) \to F_V^A(X, Y)$$

of the universal formal A-module $F_S^A(X, Y)$ with the universal A-typical formal A-module $F_V^A(X, Y)$ provides us with a universal way of making the formal A-modules $F(X, Y)$ and $G(X, Y)$ A-typical, which in particular does not destroy the equality $\bar{F}(X, Y) = \bar{G}(X, Y)$. Indeed, if $F(X, Y) = F_s^A(X, Y)$ for $s = (s_1, s_2, \ldots)$, $s_i \in A$, and $G(X, Y) = F_{\bar{s}}^A(X, Y)$, $\bar{s} = (\bar{s}_1, \bar{s}_2, \ldots)$, then $\bar{F}(X, Y) = \bar{G}(X, Y)$ is equivalent to $\bar{s}_i \equiv s_i \bmod \pi$ (cf. Lemma (22.2.9)). Now the

A-typical version of $F(X, Y)$ is $F_v^A(X, Y)$ with $v_i = s_{q^i}$, $i = 1, 2, \ldots$, obtained from $F_V^A(X, Y)$ by substituting v_i for V_i, $i = 1, 2, \ldots$, and similarly the A-typical version of $G(X, Y)$ is $F_{\bar{v}}^A(X, Y)$ with $\bar{v}_i = \bar{s}_{q^i}$, $i = 1, 2, \ldots$. Hence $v_i \equiv \bar{v}_i \bmod \pi$ so that $\bar{F}_v^A(X, Y) = \bar{F}_{\bar{v}}^A(X, Y)$. We are thus reduced to the case that $F(X, Y)$ and $G(X, Y)$ are A-typical formal A-modules, $F(X, Y) = F_v^A(X, Y)$, $G(X, Y) = F_{\bar{v}}^A(X, Y)$ with $v_i \equiv \bar{v}_i \bmod \pi$. By (22.2.4) this means that $F(X, Y)$ and $G(X, Y)$ are strictly isomorphic. This concludes the proof of Theorem (22.2.1).

■ (22.2.7) **Corollaries**

(i) Two formal A-modules over A are isomorphic if and only if they are strictly isomorphic.

(ii) Two A-typical formal A-modules over k are isomorphic if and only if they are identical (as formal A-modules).

Proof

(i) This follows from (22.2.5) if one first makes both formal A-modules A-typical via a strict formal A-module isomorphism.

(ii) We can find A-typical formal A-modules over A lifting the given formal A-modules over k (because $F_V^A(X, Y)$ is universal over $A[V]$ and $A[V]$ is a free commutative algebra over A). These two lifts are strictly isomorphic by Theorem (22.2.1) combined with Corollary (22.2.7)(i), and hence their reductions are identical by (22.2.4). (NB this does not mean that the original isomorphism over k was the identity.)

■ (22.2.8) **Remark** Example (21.1.15) shows that Theorem (22.2.1) does not hold for higher dimensional formal A-modules.

■ (22.2.9) **Lemma** Let $s = (s_1, s_2, \ldots)$, $\bar{s} = (\bar{s}_1, \bar{s}_2, \ldots)$ be two sequences of elements of an A-algebra R and let $\phi: R \to B$ be an A-algebra homomorphism. Then $\phi_* F_s^A(X, Y) = \phi_* F_{\bar{s}}^A(X, Y)$ as formal A-modules if and only if $\phi(s_i) = \phi(\bar{s}_i)$ for all i.

Proof This is an immediate consequence of the uniqueness part of the universality property of $(F_S^A(X, Y), \rho_S^A)$ over $A[S]$. (This, of course, also gives a second proof of Lemma (21.1.8).)

22.3 Intermezzo concerning the universal isomorphism $\alpha_{V,T}^A(X)$ of A-typical formal A-modules

The next topic we want to take up is that of formal moduli; i.e., given a discrete valuation ring A and an A-algebra B that is a complete local ring with residue field k_B and given a formal A-module $F(X, Y)$ over k_B, we want to describe all formal A-modules over B reducing to $F(X, Y)$ modulo all (strict) isomorphisms that reduce to the identity over k_B. To do this we need some more information concerning the universal isomorphism $\alpha_{V,T}^A(X)$.

■ (22.3.1) Let A be a nontrivial discrete valuation ring (not necessarily complete) with residue field k of q elements, $q = p^r$, and uniformizing element π. Let $F^A_{V,T}(X, Y)$ be the A-typical formal A-module over $A[V, T]$ constructed in (21.7.1) with A-logarithm $f^A_{V,T}(X)$. Let $\bar{V}_1, \bar{V}_2, \ldots, \in A[V; T]$ be the unique polynomials such that

$$F^A_{V,T}(X, Y) = F^A_{\bar{V}}(X, Y) \tag{22.3.2}$$

where $F^A_{\bar{V}}(X, Y)$ is obtained from the universal A-typical formal A-module $F^A_V(X, Y)$ by substituting $\bar{V}_i$ for V_i, $i = 1, 2, \ldots$. In 21.7 we proved that

$$\bar{V}_n = V_n + T_n + \sum_{\substack{i+j=n \\ i,j-1}} (V_i T_j^{q^i} - T_j \bar{V}_i^{q^j}) + \sum_{k=1}^{n-1} a^A_{n-k}(V)(V_k^{q^{n-k}} - \bar{V}_k^{q^{n-k}}) \tag{22.3.3}$$
$$+ \sum_{k=2}^{n-1} a^A_{n-k}(V) \sum_{\substack{i+j=k \\ i,j \geq 1}} (V_i^{q^{n-k}} T_j^{q^{n-j}} - T_j^{q^{n-k}} \bar{V}_i^{q^{n-i}})$$

To discuss formal moduli we use a more manageable consequence of this formula, viz.

■ (22.3.4) **Theorem** Let J be the ideal in $A[V, T]$ generated by the elements $T_i T_j$, $i, j \in \mathbf{N}$, then we have modulo J

$$\begin{aligned} \bar{V}_n \equiv V_n &+ \sum (-1)^t (B^A_{s_1} V^{q^{s_1}-1}_{n-s_1})(B^A_{s_2} V^{q^{s_2}-1}_{n-s_1-s_2}) \cdots \\ &\times (B^A_{s_t} V^{q^{s_t}-1}_{n-s_1-\cdots-s_t})(-T_i V_j^{q^i}) \\ &+ \sum (-1)^t (B^A_{s_1} V^{q^{s_1}-1}_{n-s_1})(B^A_{s_2} V^{q^{s_2}-1}_{n-s_1-s_2}) \cdots \\ &\times (B^A_{s_t} V^{q^{s_t}-1}_{n-s_1-\cdots-s_t})(\pi T_i) \end{aligned} \tag{22.3.5}$$

where $B^A_s = q^s a^A_s(V) \in A[V]$ and where the first sum is over all sequences $(s_1, \ldots, s_t, i, j)$ such that $s_t, i, j \in \mathbf{N}$, $t \in \mathbf{N} \cup \{0\}$ and $s_1 + \cdots + s_t + i + j = n$, and the second sum is over all sequences $(s_1, \ldots, s_t, i)$ such that $s_t, i \in \mathbf{N}$, $t \in \mathbf{N} \cup \{0\}$, and $s_1 + \cdots + s_t + i = n$.

■ (22.3.6) **Corollary**

(i) Suppose that A is unramified and k has p elements (i.e., we can take $p = q = \pi$). Let I be the ideal in $A[V, T]$ generated by the elements $pT_1, pT_2, \ldots$ and the ideal J. Then we have modulo I

$$\begin{aligned} \bar{V}_n \equiv V_n - T_1 V^p_{n-1} - \cdots - T_{n-1} V_1^{p^{n-1}} &+ \sum (-1)^t V_1^{(p-1)^{-1}(p^{s_1}+\cdots+p^{s_t})} \\ &\times V^{p^{s_1}-1}_{n-s_1} \cdots V^{p^{s_t}-1}_{n-s_1-\cdots-s_t}(-T_i V_j^{p^i}) \end{aligned} \tag{22.3.7}$$

where the sum is over all sequences $(s_1, s_2, \ldots, s_t, i, j)$ such that $s_t, i, j \in \mathbf{N}$, $t \in \mathbf{N}$, and $s_1 + \cdots + s_t + i + j = n$.

(ii) In all other cases, i.e., if $q > p$ or if A is ramified, we have

$$\bar{V}_n \equiv V_n - T_1 V^q_{n-1} - \cdots - T_{n-1} V_1^{q^{n-1}} \tag{22.3.8}$$

modulo I where I is the ideal generated by the elements $\pi T_1, \pi T_2, \ldots$ and the ideal J.

Proof Both these statements follow immediately from Theorem (22.3.4) because

$$B_s^A = q^s a_s^A(V) \equiv q^s \pi^{-s} V_1 V_1^q \cdots V_1^{q^{s-1}} \mod(\pi A[V])$$

as can be seen directly from formula (21.5.4).

The first step in the proof of Theorem (22.3.4) is the following obvious lemma.

■ (22.3.9) **Lemma** Suppose that $\bar{V}_l \equiv V_l + \sum_i T_i C_i \mod J$ for certain $C_i \in A[V; T]$. Then

$$\bar{V}_l^{p^j} \equiv V_l^{p^j} + p^j V_l^{p^j-1}\left(\sum_i T_i C_i\right) \mod J$$

Proof Obvious.

■ (22.3.10) **Proof of Theorem (22.3.4)** We proceed by induction on n, the case $n = 1$ being trivial ($\bar{V}_1 = V_1 + \pi T_1$). So suppose Theorem (22.3.4) holds for all $l < n$. This means in particular that $\bar{V}_l \equiv V_l \mod(T_1, T_2, \ldots)$ (which is also directly clear), so that the hypothesis of Lemma (22.3.9) is satisfied if $l < n$. We now use formula (22.3.3). First notice that the third sum in (22.3.3) is $\equiv 0$ mod J. The second sum in (22.3.3) gives us contributions of the form

$$a_{n-k}^A(V)(V_k^{q^{n-k}} - \bar{V}_k^{q^{n-k}})$$

Let $\bar{V}_k \equiv V_k + \sum T_i C_i$, then, using Lemma (22.3.9), we find

$$\begin{aligned} a_{n-k}^A(V)(V_k^{q^{n-k}} - \bar{V}_k^{q^{n-k}}) &\equiv -a_{n-k}^A(V) q^{n-k} V_k^{q^{n-k}-1}(\textstyle\sum T_i C_i) \\ &= -B_{n-k}^A V_k^{q^{n-k}-1}(\textstyle\sum T_i C_i) \end{aligned}$$

Theorem (22.3.4) follows immediately from this by induction.

22.4 Formal moduli for formal A-modules

■ (22.4.1) **The setting** In this section A is a nontrivial discrete valuation ring with residue field k of q elements, $q = p^r$, p a prime number. Let π be a uniformizing element of A, K the quotient field of A. Let R be an A-algebra that is a local ring with maximal ideal $\mathfrak{m}_R$ such that $\bigcap_n \mathfrak{m}_R^n = \{0\}$ such that R is complete in the $\mathfrak{m}_R$-adic topology, and such that $A \to R$ maps π into $\mathfrak{m}_R$. We shall use k_R to denote the residue field of R.

■ (22.4.2) **The moduli problem** Now let $\Phi(X, Y)$ be a formal A-module over k_R. The existence of the universal formal A-module $F_A^S(X, Y)$ over $A[S]$ guarantees the existence of lifts over R of $\Phi(X, Y)$; i.e., there are formal A-modules $F(X, Y)$ over R that reduce to $\Phi(X, Y)$ modulo $\mathfrak{m}_R$. We shall call two

such lifts $F(X, Y)$ and $G(X, Y)$ $*$-isomorphic if there exists an isomorphism of formal A-modules $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $\alpha(X) \equiv X \bmod \mathfrak{m}_R$ and the lifts $F(X, Y)$ and $G(X, Y)$ are strictly $*$-isomorphic if there exists a $*$-isomorphism $\alpha(X)$ such that $\alpha(X) \equiv X$ mod(degree 2). We want to describe the set of all lifts modulo (strict) $*$-isomorphisms. The answer is that if $\Phi(X, Y)$ is a formal A-module of height h, then $\{\text{lifts}\}/(*\text{-isomorphism}) = \mathfrak{m}_R^{h-1}$ and $\{\text{lifts}\}/(\text{strict } *\text{-isomorphism}) = \mathfrak{m}_R^h$. A more precise and explicit result is Theorem (22.4.4).

■ (22.4.3) Before we can state Theorem (22.4.4) we need some preliminaries. Let $\Phi(X, Y)$ have formal A-module height h over k_R and suppose that $\Phi(X, Y)$ is A-typical. (This does not restrict the generality of the problem because every formal A-module is strictly isomorphic to an A-typical one; cf. (21.5.6).) Then there are unique elements $v_1, v_2, \ldots, \in k_R$ such that $\Phi(X, Y) = F_v^A(X, Y)$; moreover, because $A\text{-ht}(\Phi(X, Y)) = h$, we know that $v_1 = v_2 = \cdots = v_{h-1} = 0$ and $v_h \neq 0$ (cf. (21.8.2)).

Choose arbitrary elements $\tilde{v}_i \in R$ for $i = h, h+1, \ldots$ such that $\phi(\tilde{v}_i) = v_i$ where ϕ: $R \to k_R$ is the natural projection. For each h-tuple of elements $s = (s_1, \ldots, s_h)$, $s_i \in \mathfrak{m}_R$, let $F_{\tilde{v}(s)}^A(X, Y)$ be the formal A-module obtained from the universal A-typical formal A-module $F_V^A(X, Y)$ by the substitutions

$$V_i \to s_i \qquad \text{for} \quad i = 1, \ldots, h-1$$

$$V_h \to \tilde{v}_h + s_h$$

$$V_i \to \tilde{v}_i \qquad \text{for} \quad i = h+1, h+2, \ldots$$

The formal A-modules $F_{\tilde{v}(s)}^A(X, Y)$ are all lifts of $\Phi(X, Y)$.

■ (22.4.4) **Theorem** Suppose the assumptions of (22.4.3) are fulfilled and let $\Phi(X, Y)$ be an A-typical formal A-module of A-height $h < \infty$. Then we have in terms of the notations of (22.4.3):

(i) For every lift $F(X, Y)$ of $\Phi(X, Y)$, there is a unique $s = (s_1, \ldots, s_h)$ with $s_i \in \mathfrak{m}_B$ such that $F(X, Y)$ is strictly $*$-isomorphic to $F_{\tilde{v}(s)}^A(X, Y)$.

(ii) For every lift $F(X, Y)$ of $\Phi(X, Y)$, there is a unique $s = (s_1, \ldots, s_h)$ with $s_i \in \mathfrak{m}_B$ and $s_h = 0$ such that $F(X, Y)$ is $*$-isomorphic to $F_{\tilde{v}(s)}^A(X, Y)$.

Proof Let $F(X, Y)$ be a formal A-module over R that lifts $\Phi(X, Y)$. We first show that $F(X, Y)$ is strictly $*$-isomorphic to an A-typical formal A-module (which lifts $\Phi(X, Y)$). Indeed, let $\alpha_{V,S}(X) = (f_S^A)^{-1}(f_V^A(X))$: $F_V^A(X, Y)) \to F_S^A(X, Y)$ be the strict isomorphism between the universal A-typical formal A-module and the universal formal A-module. Identifying V_i and S_{q^i}, $i \in \mathbf{N}$, we have that $F_S^A(X, Y) \equiv F_V^A(X, Y) \bmod(\ldots, S_i, \ldots;\ i \neq q^r,\ r \in \mathbf{N})$ and hence $\alpha_{V,S}(X) \equiv X \bmod(\ldots, S_i, \ldots;\ i \text{ not a power of } q)$. Now let ϕ: $A[S] \to R$ be the unique A-algebra homomorphism such that $\phi_* F_S^A(X, Y) = F(X, Y)$. Then $\phi(S_i) \in \mathfrak{m}_R$ if i is not a power of q because $F(X, Y)$ reduces to

$\Phi(X, Y)$ mod $\mathfrak{m}_R$ and $\Phi(X, Y)$ is A-typical. It follows that $\phi_*(\alpha_{V,S}(X))$ is a strict $*$-isomorphism $\phi_*(F_V(X, Y)) \to F(X, Y)$ and $\phi_*(F_V(X, Y))$ is A-typical (we are still identifying V_i with S_{q^i}). (Of course $\phi_*(F_V(X, Y))$ also reduces to $\Phi(X, Y)$ because $\phi_*(\alpha_{V,S}(X)) \equiv X$ mod $\mathfrak{m}_R$.)

We can therefore assume that the lift $F(X, Y)$ is A-typical. Let $w = (w_1, w_2, \ldots)$ be the unique sequence of elements such that $F(X, Y) = F^A_w(X, Y)$. Because $F(X, Y)$ reduces to $\Phi(X, Y)$ mod $\mathfrak{m}_R$, as does $F^A_{\tilde{v}(0)}(X, Y)$, we must have (cf. Lemma (22.2.9))

$$w_1, \ldots, w_{h-1} \in \mathfrak{m}_R, \qquad w_i \equiv \tilde{v}_i \mod \mathfrak{m}_R \qquad \text{for} \quad i \geq h$$

Inductively, we are now going to construct sequences $v(n) = (v_1(n), v_2(n), \ldots)$ and power series $\beta_n(X) \in R[\![X]\!]$ for $n = 1, 2, 3, \ldots$ such that

$$\beta_n(X)\colon F^A_{v(n)}(X, Y) \to F^A_{v(n+1)}(X, Y) \tag{22.4.5}$$

is a strict isomorphism of formal A-modules

$$\beta_n(X) \equiv X \mod(\mathfrak{m}_R^n) \tag{22.4.6}$$

$$v(1) = w, \qquad v_i(n+1) \equiv v_i(n) \mod \mathfrak{m}_R^n \qquad \text{for} \quad i = 1, \ldots, h, \ldots \tag{22.4.7}$$

$$v_i(n) \equiv \tilde{v}_i \mod \mathfrak{m}_R^n \qquad \text{for} \quad i = h+1, h+2, \ldots$$

First assume that $h > 1$ or that A is ramified or that $q > p$. Suppose we have already found $v_i(n)$ (and $\beta_{n-1}(X)$). Define elements $t_i(n)$ with induction with respect to i by means of the formula

$$t_i(n) = v_h(n)^{-q^i}(v_{i+h}(n) - \tilde{v}_{i+h} - t_1(n)v_{i+h-1}(n)^q - \cdots - t_{i-1}(n)v_{h+1}(n)^{q^{i-1}}) \tag{22.4.8}$$

(note that this is well defined because $v_h(n) \equiv \tilde{v}_h$ mod$(\mathfrak{m}_R^n)$ so that $v_h(n)$ is a unit of R because $\tilde{v}_h$ is). Induction with respect to i gives us that

$$t_i(n) \in \mathfrak{m}_R^n, \qquad i = 1, 2, \ldots$$

Now let $t(n) = (t_1(n), t_2(n), \ldots)$ and let

$$\beta_n(X) = \alpha^A_{v(n),t(n)}(X), \qquad v_i(n+1) = \bar{V}_i(v(n), t(n))$$

where the $\bar{V}_i$ are the unique polynomials in $V_1, \ldots, V_i; T_1, \ldots, T_i$, such that $F^A_{\bar{V}}(X, Y) = F^A_{V,T}(X, Y)$. Then $\beta_n(X)\colon F^A_{v(n)}(X, Y) \to F^A_{v(n+1)}(X, Y)$ is a strict isomorphism and because $\alpha^A_{V,T}(X) \equiv X$ mod$(T_1, T_2, \ldots)$, we have that $\beta_n(X) \equiv X$ mod $\mathfrak{m}_R^n$. This takes care of (22.4.5) and (22.4.6).

Now according to (22.3.7) and (22.3.8) we have modulo I (where I is the ideal generated by all elements $T_i T_j$, $i, j \in \mathbf{N}$, πT_i, $i \in \mathbf{N}$) that

$$\bar{V}_{i+h} \equiv V_{i+h} - T_1 V^q_{i+h-1} - \cdots - T_{i+h-1} V_1^{q^{i+h-1}} + V_1(\sum T_i C_i)$$

where $V_1(T_iC_i) \equiv 0 \bmod I$ unless $q = p$ and $pA = \pi A$. Because $v_i(n) \in \mathfrak{m}_R$ for $i = 1, \ldots, h-1$, and $t_i(n) \in \mathfrak{m}_R^n$, $\pi \in \mathfrak{m}_R$ and (22.4.8) this means that

$$v_i(n+1) \equiv \tilde{v}_i \mod(\mathfrak{m}_R^{n+1}) \qquad \text{for} \quad i = h+1, h+2, \ldots$$

In case $h = 1$, $q = p$, A unramified one proceeds similarly except that the formula for $t_i(n)$ now becomes

$$\begin{aligned}(22.4.9)\quad t_i(n) = {} & v_1(n)^{-p^i}(v_{i+1}(n) - \tilde{v}_{i+1} - t_1(n)v_i(n)^p - \cdots \\ & - t_{i-1}(n)v_2(n)^{p^{i-1}}) \\ & + v_1(n)^{-p^i} \sum (-1)^t v_1(n)^{(p-1)^{-1}(p^{s_1}+\cdots+p^{s_t}-t)} v_{i+1-s_1}^{p^{s_1}-1}(n) \cdots \\ & \times v_{i+1-s_1-\cdots-s_t}^{p^{s_t}-1}(n)(-t_j v_i^{p^j}(n))\end{aligned}$$

reflecting the fact that now formula (22.3.7) is appropriate instead of (22.3.8).

Now consider the composed isomorphisms

$$F(X, Y) = F_w^A(X, Y) \to F_{v(2)}^A(X, Y) \to \cdots \to F_{v(n)}^A(X, Y)$$

Because of (22.4.6) and the completeness of R, these converge to an isomorphism

$$F(X, Y) \to F_{v(\infty)}^A(X, Y)$$

and because of (22.4.7) we have that

$$v_i(\infty) \equiv \tilde{v}_i \mod \mathfrak{m}_R^n, \qquad i = h+1, h+2, \ldots$$

for all $n \in \mathbf{N}$ so that we have that $v_i(\infty) = \tilde{v}_i$ because $\bigcap_n \mathfrak{m}_R^n = \{0\}$. This proves that every formal A-module $F(X, Y)$ over R is strictly $*$-isomorphic to a formal A-module of the form $F_{\tilde{v}(s)}^A(X, Y)$ for certain $s = (s_1, \ldots, s_h)$, $s_j \in \mathfrak{m}_R$.

Thus to finish the proof of part (i) of the theorem it remains to prove only that two formal A-modules $F_{\tilde{v}(s)}^A(X, Y)$ and $F_{\tilde{v}(\bar{s})}^A(X, Y)$ are strictly $*$-isomorphic if and only if they are equal. So suppose that $F_{\tilde{v}(s)}^A(X, Y)$ and $F_{\tilde{v}(\bar{s})}^A(X, Y)$ are strictly $*$-isomorphic. By the universality of the isomorphism $\alpha_{V,T}^A(X)$ this means that there are $t_1, t_2, \ldots, \in R$ such that this isomorphism is equal to $\alpha_{\tilde{v}(s),t}^A(X)$.

Now $\alpha_{V,T}^A(X) \equiv X - T_n X^{q^n} \mod(T_1, \ldots, T_{n-1}; \text{degree } q^n + 1)$. So since $\alpha_{\tilde{v}(s),t}^A(X)$ is a $*$-isomorphism, we must have $t_i \in \mathfrak{m}_R$ for all $i \in \mathbf{N}$. Suppose that $\alpha_{\tilde{v}(s),t}^A(X) \neq X$ and let $n, r \in \mathbf{N}$ be such that

$$\begin{aligned}& t_i \in \mathfrak{m}_R^{r+1} \qquad \text{if} \quad i = 1, \ldots, n-1 \\ (22.4.10)\quad & t_n \in \mathfrak{m}_R^r \setminus \mathfrak{m}_R^{r+1}, \qquad t_i \in \mathfrak{m}_R^r \qquad \text{if} \quad i = n+1, n+2, \ldots\end{aligned}$$

We have that $\tilde{v}_{n+h} = \bar{V}_{n+h}(\tilde{v}(s), t)$ for all $n \in \mathbf{N}$. However, formula (22.3.7) or (22.3.8) combined with (22.4.10) gives that

$$\bar{V}_{n+h}(\tilde{v}(s), t) \equiv \tilde{v}_{n+h} - t_n v_h^{q^n} \mod \mathfrak{m}_R^{r+1}$$

which is a contradiction, so that indeed $\alpha^A_{\hat{v}(s),t}(X) = X$. This proves the first part of the theorem.

To prove the second part of the theorem we need to use more general isomorphisms than the strict isomorphisms $\alpha_{v,t}(X)$. The isomorphism $\gamma(X) = (1 + T_0)^{-1}(X)$ applied to $F^A_{V,T}(X, Y) = F^A_{\bar{V}}(X, Y)$ changes $F^A_{\bar{V}}(X, Y)$ to an A-typical formal group law $F^A_{\hat{V}}(X, Y)$ with

$$\hat{V}_n = (1 + T_0)^{q^n - 1}\bar{V}_n \tag{22.4.11}$$

as the logarithm of $(1 + T_0)^{-1}F_{\bar{V}}((1 + T_0)X, (1 + T_0)Y)$ is

$$(1 + T_0)^{-1}f_{\bar{V}}((1 + T_0)X)).$$

Now let J_0 be the ideal generated by all the elements T_iT_j, $i, j = 0, 1, 2, \ldots$, and I_0 the ideal generated by all the πT_i, $i = 0, 1, 2, \ldots$, and the ideal J_0. Then using (22.3.7) and (22.3.8) we find modulo I_0, respectively,

$$\begin{aligned}\hat{V}_n \equiv{}& (1 - T_0)V_n - T_1V_{n-1}^p - \cdots - T_{n-1}V_1^{p^{n-1}} \\ &+ \sum (-1)^t V_1^{(p-1)^{-1}(p^{s_1}+\cdots+p^{s_t}-t)}V_{n-s_1}^{p^{s_1}-1}\cdots \\ &\times V_{n-s_1-\cdots-s_t}^{p^{s_t}-1}(-T_iV_j^{p^i})\end{aligned} \tag{22.4.12}$$

$$\hat{V}_n \equiv (1 - T_0)V_n - T_1V_{n-1}^q - T_2V_{n-2}^{q^2} - \cdots - T_{n-1}V_1^{q^{n-1}} \tag{22.4.13}$$

Of course, for all this to make sense we must be working over a ring with T_0 in it and moreover such that $(1 + T_0)^{-1}$ exists. All the above can, e.g., be considered to be taking place over $A[\![T_0]\!][V; T]$.

The proof of the second part of the theorem now proceeds exactly as the proof of the first part; i.e., we construct sequences of elements $\hat{v}(n) = (\hat{v}_1(n), \hat{v}_2(n), \ldots)$ for all $n \in \mathbf{N}$, $\hat{v}(1) = w$, $\hat{v}_i(n + 1) = \hat{V}_i(\hat{v}(n), \hat{t}(n))$ where now $\hat{t}(n) = (\hat{t}_0(n), \hat{t}_1(n), \ldots)$ and power series $\hat{\beta}(X) = (1 + \hat{t}_n(0))^{-1}\alpha_{\hat{v}(n),\hat{t}'(n)}(X)$ where $\hat{t}'(n) = (\hat{t}_1(n), \hat{t}_2(n), \ldots)$ is such that

(22.4.14)

$\hat{\beta}_n(X)$: $F^A_{\hat{v}(n)}(X, Y) \to F^A_{\hat{v}(n+1)}(X, Y)$ is an isomorphism of formal A-modules

$$\begin{aligned}&\hat{\beta}_n(X) \equiv X \mod(\mathfrak{m}_R^n) \\ &\hat{v}_i(n) \equiv \tilde{v}_i \mod(\mathfrak{m}_R^n) \qquad \text{for} \quad i = h, h + 1, h + 2 \\ &\hat{v}_i(n) \equiv \hat{v}_i(n + 1) \mod(\mathfrak{m}_R^n) \qquad \text{for} \quad i = 1, 2, \ldots\end{aligned}$$

(Note the two changes with respect to (22.4.5)–(22.4.7).) The relevant formulas for the $\hat{t}_i(n)$ are

$$\hat{t}_0(n) = \hat{v}_h(n)^{-1}(\hat{v}_h(n) - \tilde{v}_h(n)) \qquad \text{and} \qquad \hat{t}_i(n) = t_i(n) - \hat{t}_0(n)\hat{v}_h(n)$$

for $i = 1, 2, 3, \ldots$, where $t_i(n)$ is as in (22.4.8) or (22.4.9) (depending on whether $q = p = \pi$ and $h = 1$ or not. The remainder of the proof is as before and the task of filling in the last details is left to the reader (if he wishes to do so).

■ (22.4.15) Now consider the special case $A = \mathbf{Z}_{(p)}$. Every formal group law over a local ring R with residue field of characteristic p has exactly one formal A-module structure. So the theorem applies in particular to this case. Suppose therefore that R is any complete Hausdorff local ring with residue field k_R of characteristic p and let $\Phi(X, Y)$ be a formal group law over k_R of height h. Then $\{\text{lifts}\}/(*\text{-isomorphism}) \simeq \mathfrak{m}_R^{h-1}$ and $\{\text{lifts}\}/(\text{strict } *\text{-isomorphism}) \simeq \mathfrak{m}_R^h$.

More precisely, we have

■ (22.4.16) **Theorem** Let R be a complete Hausdorff local ring with residue field k_R of characteristic $p > 0$. Let $\Phi(X, Y)$ be a p-typical formal group law over k_R and of height h and let $v_1 = \cdots = v_{h-1} = 0$, $v_h \neq 0$, $v_{h+1}, v_{h+2}, \ldots$ be such that $\Phi(X, Y) = F_v(X, Y)$ and let $\tilde{v}_i \in R$, $i = h, h+1, \ldots$, be a lift of v_i. Then we have:

(i) For every lift $F(X, Y)$ over F of $\Phi(X, Y)$, there is a unique h-tuple of elements $(s_1, \ldots, s_h)$, $s_i \in \mathfrak{m}_R$, such that $F(X, Y)$ is strictly $*$-isomorphic to the formal group law $F_{\tilde{v}(s)}(X, Y)$ (which is of course also a lift of $\Phi(X, Y)$) where $\tilde{v}(s) = (s_1, \ldots, s_{h-1}, \tilde{v}_h + s_h, \tilde{v}_{h+1}, \tilde{v}_{h+2}, \ldots)$.

(ii) For every lift $F(X, Y)$ over R of $\Phi(X, Y)$, there is a unique $(h-1)$-tuple of elements $(s_1, \ldots, s_{h-1})$, $s_i \in \mathfrak{m}_R$, such that $F(X, Y)$ is $*$-isomorphic to the formal group law $F_{\tilde{v}_0(s)}(X, Y)$ (which is of course also a lift of $\Phi(X, Y)$) where $\tilde{v}_0(s) = (s_1, \ldots, s_{h-1}, \tilde{v}_h, \tilde{v}_{h+1}, \ldots)$.

23 Rings of Endomorphisms of Formal Group Laws

All formal group laws and formal A modules in this section are one dimensional.

23.1 On the endomorphism rings of one dimensional formal group laws over finite fields

■ (23.1.1) Let k be a field of characteristic $p > 0$ and let k_{sc} be a separable closure of k. Let $G(X, Y)$ be a one dimensional formal group law over k of height h.

We recall that $\mathrm{End}_{k_{sc}}(G(X, Y))$ is isomorphic to the maximal order E_h in the central division algebra D_h of invariant h^{-1} and rank h^2 over $\mathbf{Q}_p$ (cf. Corollary (20.2.14)).

■ (23.1.2) **Lemma** Let k be a finite field of q elements, let $G(X, Y)$ be a formal group law over k and let $\xi_G(X) \equiv X^q$ be the "Frobenius" endomorphism of $G(X, Y)$. Then $\mathrm{End}_k(G(X, Y)$ consists of those elements of $\mathrm{End}_{k_{sc}}(G(X, Y))$ that commute with ξ_G.

Proof If $\alpha(X) \in k_{sc}[\![X]\!]$, then $\alpha(X)^q = \alpha(X^q)$ if and only if all coefficients of $\alpha(X)$ are in $\mathbf{F}_q = k$.

■ (23.1.3) This result can be used to say something about $\mathrm{End}_k(G(X, Y))$. Indeed, according to the intermezzo on division algebras (20.2.16), we know that the set of all elements of D_h commuting with ξ_G is a central division algebra over $\mathbf{Q}_p(\xi_G)$ of rank h^2/m^2 where $m = [\mathbf{Q}_p(\xi_G): \mathbf{Q}_p]$. According to the second intermezzo on division algebras (23.1.4) below, we know in addition that the invariant of $\mathrm{End}_k(G(X, Y)) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is m/h and that $\mathrm{End}_k(G(X, Y))$ is the ring of integers in $\mathrm{End}_k(G(X, Y)) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

■ (23.1.4) **Second intermezzo on division algebras** We use the notations of (20.2.16) where K is a finite extension of $\mathbf{Q}_p$. Let D be a central division algebra over K and let L be a commutative subfield of D and D_L the commutant of L. Let $m = [L: K]$ and let i be the invariant of D over K. Then we have

$$\mathrm{inv}_L(D_L) = mi$$

where, of course, the number mi must be interpreted modulo 1.

There is a unique valuation v_D on D that extends the valuation on k. The restriction of v_D to L gives a valuation on L that is (by uniqueness of extension of valuations for local fields) the valuation of the local field L (up to multiplication by a constant). Hence v_D restricts on D_L to v_{D_L} up to multiplication by a constant. It follows that the integers of D_L are precisely those elements of A_D, the integers of D, that commute with L.

For later purposes we need one more result on central division algebras:

Embedding theorem Let D be central division algebra of rank n^2 over a finite extension K of $\mathbf{Q}_p$. Then every commutative field extension L/K of degree n can be embedded as a (maximal) commutative subfield of D. For a proof, see, e.g., [73, Appendix to Chapter VI]; cf. also (23.1.7) below for a proof in case the invariant of D is n^{-1} (which is the only case that will be used below).

■ (23.1.5) **Notation** Let $F(X, Y)$ be a formal A-module over an A-algebra B. Then for every B-algebra C we shall use $A\text{-}\mathrm{End}_C(F(X, Y))$ to denote the ring of A-module endomorphisms of $F(X, Y)$ over C (more properly of $\phi_* F(X, Y)$ over C where $\phi: B \to C$ is the B-algebra structural homomorphism of C).

■ (23.1.6) **Proposition** Let A be the ring of integers of a finite extension K of $\mathbf{Q}_p$ or $\mathbf{F}_p((x))$ and let K be the residue field of A. Let $F(X, Y)$ be a formal A-module over some finite extension l of k of height $h < \infty$. Let k_{sc} be the algebraic closure of k. Then $A\text{-}\mathrm{End}_{k_{sc}}(F(X, Y))$ is the ring of integers of a central division algebra over K of rank h^2 and invariant h^{-1}.

Proof This follows from Proposition (21.8.17) combined with (21.9.1). In case A is of characteristic zero, one can also argue as follows. Let $m = [K: \mathbf{Q}_p]$, then as a formal group law over k_{sc} we have that $F(X, Y)$ has height mh, so that $\mathrm{End}_{k_{sc}}(F(X, Y))$ is the ring of integers of a central division algebra of rank m^2h^2 and invariant $m^{-1}h^{-1}$ over $\mathbf{Q}_p$. Now $A\text{-}\mathrm{End}_{k_{sc}}(F(X, Y))$

consists of all elements of $\mathrm{End}_{k_{sc}}(F(X, Y))$ that commute with the $\rho_F(a)$. Now $a \mapsto \rho_F(a)$ defines an injection $A \to \mathrm{End}_{k_{sc}}(F(X, Y))$ (cf. (21.8.19)), so that A-$\mathrm{End}_{k_{sc}}(F(X, Y))$ is the ring of integers of the commutant of $A \otimes \mathbf{Q}_p = K$ in $\mathrm{End}_{k_{sc}}(F(X, Y)) \otimes \mathbf{Q}_p$. Now apply (23.1.4).

■ (23.1.7) **Proof of the embedding theorem in a special case** Incidentally, here is a quick and amusing "formal group" proof of the embedding theorem of (23.1.4) in case the invariant of D is n^{-1}. Let $[L: K] = n$. Let π_L be a uniformizing element of L and let $F(X, Y)$ over $A(L)$ be the formal group law with logarithm

$$f(X) = X + \pi_L^{-1} f(X^{q^r})$$

where q^r is the number of elements of the residue field of L. Then $F(X, Y)$ is a formal $A(L)$-module of $A(L)$-height 1, and it can also be considered as a formal $A(K)$-module of $A(K)$-height n. It follows that $A(K)$-$\mathrm{End}_{k_{sc}}(F(X, Y)) \otimes \mathbf{Q}_p$ is the central division algebra $D_n(K)$ of rank n^2 and invariant n^{-1} over K; cf. Proposition (23.1.6). Now $a \mapsto [a]_F(X)$ embeds $A(L)$ into

$$A(K)\text{-}\mathrm{End}_{A(L)}(F(X, Y))$$

so that by (21.8.18) we find an embedding

$$A(L) \to A(K)\text{-}\mathrm{End}_l(\bar{F}(X, Y))$$

Tensoring with $\mathbf{Q}_p$ now gives the desired embedding $L \to D_n(K)$. The same argument works for L and K finite extensions of $\mathbf{F}_p((x))$.

23.2 On the rings of endomorphisms of (one dimensional commutative) formal group laws over a p-adic integer ring

■ (23.2.1) In this subsection R or B is the ring of integers of some finite extension L of $\mathbf{Q}_p$, and $F(X, Y)$ is a formal group law over B. Recall that the reduction homomorphism $\mathrm{End}_B(F(X, Y)) \to \mathrm{End}_l(\bar{F}(X, Y))$ is injective if $F(X, Y)$ is of finite height (here l is the residue field of B and $\bar{F}(X, Y)$ the reduction of $F(X, Y)$). Our first results exploit this injectivity of the reduction map. Later in this subsection $F(X, Y)$ will be a formal A-module where A is the ring of integers of some subextension K, $\mathbf{Q}_p \subset K \subset L$.

We use B_{nr} to denote the ring of integers of the maximal unramified extension L_{nr} of L and $\hat{B}_{nr}$ is the ring of integers of the completion $\hat{L}_{nr}$.

As usual q is the number of elements of the residue field of A and π or π_K is a uniformizing element of K.

■ (23.2.2) **Proposition** Let $F(X, Y)$ be a formal group law of height h over R, let S be the ring of integers of a finite totally ramified extension of L, and let $\alpha(X)$ be an endomorphism of $F(X, Y)$ over S. Then $\alpha(X) \in R[\![X]\!]$, so that $\alpha(X)$ is in fact an endomorphism over R.

Proof Let k be the residue field of S (and of R). Because S is totally ramified, we know that $S \otimes_R S$ is also a local ring with residue field k. Let ϕ_1, $\phi_2 : S \to S \otimes_R S$ be the ring homomorphisms $s \mapsto 1 \otimes s$ and $s \mapsto s \otimes 1$. We claim that

$$\text{(23.2.3)} \quad \mathrm{End}_R(F(X, Y)) = \{\alpha(X) \in \mathrm{End}_S(F(X, Y)) \mid (\phi_1)_*\alpha(X) = (\phi_2)_*\alpha(X)\}$$

To see this first observe that

$$\text{(23.2.4)} \qquad R = \{s \in S \mid \phi_1(s) = \phi_2(s)\}$$

Indeed, since S is free over R with basis, say, $x_1, \ldots, x_n$, $x_1 = 1$, we know that a basis for $S \otimes_R S$ over R is $\{x_i \otimes x_j,\ i, j = 1, \ldots, n\}$, and (23.2.4) follows. Now (23.2.3) is a formal consequence of (23.2.4) because $R \mapsto \mathrm{End}_R(F(X, Y))$ is a representable functor. In more detail: there is an R-algebra E_F such that $\mathbf{R\text{-}Alg}(E_F, B) = \mathrm{End}_B(F(X, Y))$ for all R-algebras B. Indeed, let $\tilde{E}_F$ be the R-algebra $\tilde{E}_F = R[c_1, c_2, \ldots]$, where the c_i are indeterminates. Let $c(X) = c_1 X + c_2 X^2 + \cdots$ and consider

$$F(c(X), c(Y)) - c(F(X, Y)) = \sum_{i,j=1}^{\infty} d_{i,j} X^i Y^j$$

Let I be the ideal of $\tilde{E}_F$ generated by the $d_{i,j}$ and set $E_F = \tilde{E}_F / I$. Under the obvious identification $\mathbf{R\text{-}Alg}(E_F, S) \xrightarrow{\sim} \mathrm{End}_S(F(X, Y))$ and the R-endomorphisms of $F(X, Y)$ correspond to $\mathbf{R\text{-}Alg}(E_F, R)$, which is the subset of $\mathbf{R\text{-}Alg}(E_F, S)$ of homomorphisms $E_F \to S$ whose image is in R. Formula (23.2.3) now follows directly from (23.2.4).

Now both the diagrams

$$\begin{array}{ccc} \mathrm{End}_S(F(X, Y)) & \xrightarrow{(\varphi_i)_*} & \mathrm{End}_{S \otimes_R S}(F(X, Y)) \\ \downarrow & & \downarrow \\ \mathrm{End}_k(\bar{F}(X, Y)) & = & \mathrm{End}_k(\bar{F}(X, Y)) \end{array}$$

$i = 1, 2$, commute. (Here the vertical arrows are reduction homomorphisms.) Moreover, the right vertical arrow is injective by (18.3.11). It follows that $(\phi_1)_*\alpha(X) = (\phi_2)_*\alpha(X)$ for all $\alpha(X) \in \mathrm{End}_S(F(X, Y))$, so by (23.2.3) $\mathrm{End}_R(F(X, Y)) = \mathrm{End}_S(F(X, Y))$.

■ (23.2.5) As before we use J (or J_F) to denote the map that assigns to a homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over B the first coefficient of $\alpha(X)$, i.e., the Jacobian "matrix" of $\alpha(X)$. We recall from (18.3.12) that

$$J : \mathrm{Hom}_B(F(X, Y), G(X, Y)) \to B$$

is an injective continuous map with closed image. We shall usually identify $\mathrm{Hom}_B(F(X, Y), G(X, Y))$ with this image. Also recall that the three natural topologies on $\mathrm{Hom}_B(F(X, Y), G(X, Y))$, viz

(i) the topology induced via the embedding J,

(ii) the topology induced by the height filtration on $\mathrm{Hom}_B(F(X, Y), G(X, Y))$, and

(iii) the topology defined by the (open) subgroups $[p^n]_G \mathrm{Hom}_B(F(X, Y), G(X, Y))$,

all agree if $F(X, Y)$ and $G(X, Y)$ are of finite height and that $\mathrm{Hom}_B(F(X, Y), G(X, Y))$ is complete in these topologies.

■ (23.2.6) **Proposition** Let $F(X, Y)$ be of finite height h, then $\mathrm{End}_B(F(X, Y))$ is a commutative order over $\mathbf{Z}_p$ whose quotient field $\mathrm{End}_B(F(X, Y)) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ has degree a divisor of h over $\mathbf{Q}_p$.

Proof The reduction homomorphism gives us an embedding $\mathrm{End}_B(F(X, Y)) \to \mathrm{End}_{k_{sc}}(\bar{F}(X, Y))$. Tensoring with $\mathbf{Q}_p$ over $\mathbf{Z}_p$ (cf. 18.3), we obtain an embedding $\mathrm{End}_B(F(X, Y)) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \to D_h$ where D_h is the division algebra over $\mathbf{Q}_p$ of rank h^2 and invariant h^{-1} (cf. (20.2.14)). Now $\mathrm{End}_B(F(X, Y))$ is commutative (because J is injective) and the proposition follows since a commutative subfield of D_h has degree a divisor of h (cf. the intermezzo on division algebras (20.2.16)).

■ (23.2.7) **Corollary** (of Proposition (23.2.2) and Proposition (23.2.6)) Let B_h be the ring of integers of the unramified extension of degree h of B and then let C be the ring of integers of any algebraic extension of $B_h \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Then $\mathrm{End}_C(F(X, Y)) = \mathrm{End}_{B_h}(F(X, Y))$.

■ (23.2.8) Let $\mathrm{END}(F(X, Y))$, the absolute endomorphism ring of $F(X, Y)$, be the ring of all endomorphisms $\alpha(X)$ of $F(X, Y)$ with $\alpha(X) \in C[\![X]\!]$ where C is the ring of integers of some algebraic extension of L. (Note that C may vary with $\alpha(X)$ (at least a priori).) Corollary (23.2.7) then says that $\mathrm{END}(F(X, Y)) = \mathrm{END}_{B_h}(F(X, Y))$.

Using Proposition (23.1.6) instead of (20.2.14), we find the formal A-module version of this result:

■ (23.2.9) **Proposition** Let $F(X, Y)$ be a formal A-module over B of formal A-module height h and let B_h be the ring of integers of the unramified extension of degree h of L. Then $\mathrm{End}_{B_h}(F(X, Y)) = \mathrm{END}(F(X, Y))$. (Recall that every endomorphism of $F(X, Y)$ over B (or an extension of B) is automatically a formal A-module endomorphism since B is of characteristic zero.)

■ (23.2.10) We have seen that $\mathrm{END}(F(X, Y))$ is an order in some finite extension of L. The question arises whether this is perhaps, on occasion, the maximal order; i.e., the question is whether $\mathrm{END}(F(X, Y))$ is (sometimes) integrally closed.

■ (23.2.11) **Lemma** Let L be unramified over K and let $F(X, Y)$ be a formal A-module of height h defined over B and let u be an element in a ring of integers

C of some unramified extension of L. Write $[u]_F(X) = f^{-1}(uf(X)) = \sum_{i=1}^{\infty} u_i X^i$ and assume that $[u]_F(X) \notin C[\![X]\!]$. Let $n \in \mathbf{N}$ be the smallest natural number such that $u_n \notin C$. Then $n \geq q^h$ and we have $\pi^{r+1} u_{n+r} \in C$ for all $r \in \mathbf{N} \cup \{0\}$.

Proof We can assume that $F(X, Y)$ is A-typical. Hence $F_v^A(X, Y) = F(X, Y)$ for suitable $v = (v_1, v_2, \ldots)$, $v_i \in B$; and since A-height $(F(X, Y)) = h$, we know that $v_i \in \mathfrak{m}(B)$ for $i = 1, \ldots, h-1$ and $v_h \in B^*$. Because L/K is unramified, it follows that the logarithm $f(X)$ of $F(X, Y)$ satisfies

$$f(X) \in B[\![X]\!] \mod(\text{degree } q^h)$$

(cf. also Lemma (23.2.15) below). This proves that $n \geq q^h$. Now we have

$$[u]_F(X) \circ [\pi]_F(X) = [\pi]_F(X) \circ [u]_F(X) \tag{23.2.12}$$

where $[\pi]_F(X) = \rho_F(\pi) = f^{-1}(\pi f(X))$. Looking at the coefficient of X^n in (23.2.12), we have

$$u_n(\pi X)^n \equiv \pi(u_n X^n) \mod C$$

proving that $\pi u_n \in C$. More generally, assuming that we have proved that $\pi^{j+1} u_{n+j} \in C$ for $j = 0, 1, \ldots, r-1$, consider the coefficient of X^{n+r} in (23.2.12). We have mod($\pi^{-r}C$, degree $n + r + 1$)

$$\begin{aligned}
&[\pi]_F([u]_F(X)) \\
&\quad \equiv \pi u_{n+r} X^{n+r} + [\pi]_F(uX + \cdots + u_{n-1} X^{n-1} + u_n X^n + \cdots + u_{n+r-1} X^{n+r-1}) \\
&\quad \equiv \pi u_{n+r} X^{n+r}
\end{aligned}$$

and on the other hand

$$[u]_F(X) \circ [\pi]_F(X) = u[\pi]_F(X) + u_2([\pi]_F(X))^2 + \cdots \equiv u_{n+r}(\pi X)^{n+r}$$

so that we find

$$\pi u_{n+r} \equiv \pi^{n+r} u_{n+r} \mod(\pi^{-r}C)$$

proving that $\pi^{r+1} u_{n+r} \in C$.

■ (23.2.13) **Proposition** Let L/K be unramified and let $F(X, Y)$ be a formal A-module of finite A-height h over B. Then $\mathrm{END}(F(X, Y))$ is integrally closed in its field of fractions.

Proof We know that $\mathrm{END}(F(X, Y)) = \mathrm{End}_{B_h}(X, Y)$. We identify $\mathrm{END}(F(X, Y))$ with its image $R \subset B_h$ under J. Now R is a local ring with maximal ideal $\pi B_h \cap R$. So to show that R is a discrete valuation ring and hence integrally closed it suffices to show that $\pi B_h \cap R = \pi R$. In other words it suffices to show that if $c \in B_h$, $c \notin R$, then also $\pi c \notin R$.

By Lemma (23.2.15) below we can assume that $F(X, Y) = F_v^A(X, Y)$ with $v_1 = \cdots = v_{h-1} = 0$.

Then

$$f_v(X) \equiv X + \pi^{-1} v_h X^{q^h} \mod(\text{degree } q^h + 1)$$

$$[\pi]_F(X) \equiv \pi X + v_h(1 - \pi^{q^h - 1}) X^{q^h} \mod(\text{degree } q^h + 1)$$

Write

$$[\pi]_F(X) = \pi X + uX^{q^h} + u_2 X^{q^h+1} + \cdots, \qquad u \in B_h^*, \quad u_2, u_3, \ldots, \in B_h$$

Let $[c]_F(X) = \sum c_i X^i$ and let $n \in \mathbf{N}$ be the smallest natural number such that $c_n \notin B_h$. We consider the coefficient of X^{nq^h} in $[c\pi]_F(X) = [c]_F(X) \circ [\pi]_F(X)$.

Now the coefficient of X^{nq^h} in

$$c_{n+r}(\pi X + uX^{q^h} + u_2 X^{q^h+1} + u_3 X^{q^h+2} + \cdots)^{n+r} \tag{23.2.14}$$

is of the form

$$\sum \binom{n+r}{i_0, \ldots, i_k} \pi^{i_0} u^{i_1} u_2^{i_2} u_3^{i_3} \cdots u_k^{i_k}$$

where the $i_0, \ldots, i_k \in \mathbf{N} \cup \{0\}$ must be such that $i_0 + i_1 + \cdots + i_k = n + r$ and $i_0 + q^h i_1 + \cdots + (q^h + k - 1) i_k = nq^h$. This gives $i_0 \geq q^{-h}(q^h r + n + r - i_1)$. Now $i_1 \leq n + r$ and $i_1 = n + r$ is possible only if $r = 0$; using Lemma (23.2.11), it follows that the coefficient of X^{nq^h} in (23.2.14) is integral except in the case that $r = 0$; then we have that the coefficient of X^{nq^h} in (23.2.14) is $c_n u^n \bmod 1$ which is not in B_h because u is a unit and $c_n \notin B_h$. Further, $c_i([\pi]_F(X)^i) \equiv 0 \bmod 1$ for $i = 1, \ldots, n - 1$ because $c_i \in B_h$ for these i. It follows that $[\pi c]_F(X) \notin B_h[\![X]\!]$, which concludes the proof of the proposition.

■ (23.2.15) **Lemma** Let $F(X, Y)$ be a formal A-module of A-height h over B and let L/K be unramified. Then $F(X, Y)$ is strictly isomorphic to a formal A-module of the form $F_v^A(X, Y)$ with $v_1 = \cdots = v_{h-1} = 0$.

Proof $F(X, Y)$ is strictly isomorphic to an A-typical formal A-module $F_v^A(X, Y)$ with $v = (v_1, v_2, \ldots)$, $v_i \in B$. Because A-height $(F_v^A(X, Y)) = h$ and L/K is unramified, we know that $v_i \in \pi B$ for $i = 1, \ldots, h - 1$. If $h > 1$, take $t_1 = -\pi^{-1} v_1 \in B$, $t_i = 0$ for $i \geq 2$. Let $\hat{v}_i = \bar{V}_i(v, t)$, then we have $F_v^A(X, Y)$ strictly isomorphic to $F_{\hat{v}}^A(X, Y)$ and $\hat{v}_1 = 0$, $\hat{v}_i \in \pi B$ for $i = 1, \ldots, h - 1$. Suppose we have $F_w^A(X, Y)$ of A-height h and $w_1 = \cdots = w_i = 0$, $i < h - 1$, $w_{i+1}, \ldots, w_{h-1} \in \pi B$. Take $t_{i+1} = -\pi^{-1} w_{i=1}$, $t_j = 0$ for $j \neq i$, and $\hat{w}_i = \bar{V}_i(w, t)$. Then we find a strictly isomorphic formal A-module $F(X, Y)$ with $\hat{w}_j = 0$ for $j = 1, \ldots, i + 1$ because $V_j \equiv V_j + \pi T_j \mod(V_1, \ldots, V_{j-1})$. By induction this concludes the proof.

■ (23.2.16) **Proposition** Let A be the ring of integers of a finite extension K of $\mathbf{Q}_p$, let L/K be unramified and B be the ring of integers of L. Let $[L : K] = n$. Then for every $r \in \mathbf{N}$, there exists a formal A-module $F(X, Y)$ over A such that A-height $(F(X, Y)) = rn$, $\mathrm{END}(F(X, Y)) = B$.

Proof Let π be a uniformizing element of A. Then π is also a uniformizing element of B. Now consider $F_v^B(X, Y)$, using this particular π for its construction. Take $v_r = 1 = v_{r+1}$, $v_i = 0$ for $i \neq r, r+1$. Then $F_v^B(X, Y)$ is a formal B-module with all its coefficients in A, so it is also a formal A-module over A. Now $\mathrm{END}(F_v^B(X, Y))$ is integrally closed (Proposition (23.2.13)), so it is the ring of integers C in some extension M of L. So $F_v^B(X, Y)$ is also a formal C-module. Let m be the residue field of C. Then if $C \neq B$ (cf. Proposition (23.2.9)) $[m: l] > 1$. Let $\#l = q^s$, $\#m = q^t$, $t > s$. But $f_v^C(X)$ is a sum of terms of the form $c_i X^{q^{ri}}$, which $f_v^B(X)$ is not since it involves both $X^{q^{rs}}$ and $X^{q^{rs+s}}$; a contradiction. Therefore $C = B$.

■ (23.2.17) **Remark** Later in Chapter VI, Section 35.5, we shall also see how to construct formal group laws with pregiven END which is not an integrally closed order in some ring of integers. That construction uses the so-called Tate module of a formal group law.

23.3 On the classification of formal group laws with many endomorphisms

■ (23.3.1) **Proposition** Let A be the ring of integers of a finite extension of $\mathbf{Q}_p$ and let B be an A-algebra that is a characteristic zero complete discrete valuation ring with algebraically closed residue field and such that $A \to B$ takes πA into the maximal ideal of B. Let $F(X, Y)$ and $G(X, Y)$ be two formal A-modules over B such that:

(i) $\bar{F}(X, Y)$ and $\bar{G}(X, Y)$ have the same height (or A-height).

(ii) $J(\mathrm{END}(F(X, Y)) = J(\mathrm{END}(G(X, Y))$, and this ring is integrally closed.

(iii) $J(\mathrm{END}(F(X, Y)) \otimes \mathbf{Q}_p$ is of dimension A-$\mathrm{ht}(F(X, Y))$ over K.

Then $F(X, Y)$ and $G(X, Y)$ are isomorphic over B.

■ (23.3.2) **Remark** Conditions (iii) and (ii) say that $\mathrm{END}(F(X, Y))$ and $\mathrm{END}(G(X, Y))$ are both maximally large; cf. (23.2.6).

■ (23.3.3) **Proof of Proposition (23.3.1)** Let $C = J(\mathrm{END}(F(X, Y)))$. Then C is the ring of integers of some finite extension of K by (23.2.9) and condition (ii). Further, because B has no unramified extensions (the residue field being algebraically closed), we know that $C \subset B$ (by (23.2.2)). Hence B is a C-algebra, and we can regard $F(X, Y)$ and $G(X, Y)$ as formal C-modules over B. Because of (iii) we then have that C-$\mathrm{ht}(F(X, Y)) = C$-$\mathrm{ht}(G(X, Y)) = 1$. This means that there are no formal C-module moduli for $F(X, Y)$ and $G(X, Y)$, so condition (i) says that $F(X, Y)$ and $G(X, Y)$ are isomorphic over B; cf. (22.4.2), (22.4.4), and Theorem (21.9.1).

24 Classification of One Dimensional Formal Group Laws Over Finite Fields

In this section we classify (in various ways) the one dimensional formal group laws over finite fields. Our main tool is the theory of forms, which works over any field. To be able to say something more explicit one needs to know quite a bit about a certain Galois cohomology group. This knowledge is obtainable in case k is finite. All formal group laws in this section are commutative and one dimensional.

24.1 Galois cohomology and forms of formal group laws

■ (24.1.1) **Definitions** Let Γ and A be topological groups. We say that A is a Γ-*group* if there is a continuous map $\Gamma \times A \to A$, $(\sigma, a) \mapsto \sigma a$ such that:

for every σ, $a \mapsto \sigma a$ is an automorphism of A;
for all $\sigma, \tau \in \Gamma$, $(\sigma\tau)(a) = \sigma(\tau a)$ for all $a \in A$;
for the unit element e_Γ of Γ, $e_\Gamma a = a$ for all $a \in A$.

A 1-*cocycle* of Γ with values in the Γ-group A is a continuous map $z\colon \Gamma \to A$ such that $z(\sigma\tau) = z(\sigma) \cdot \sigma z(\tau)$ where the dot denotes the multiplication of A. The special 1-cocycle $\sigma \mapsto e_A$ for all $\sigma \in \Gamma$ is called the *zero cocycle*. Two cocycles z and $\hat{z}$ are called *cohomologous* if there exists an element $a \in A$ such that $\hat{z}(\sigma) = a^{-1} \cdot z(\sigma) \cdot \sigma a$. Note that this is an equivalence relation. The set of equivalence classes—also called 1-cohomology classes—is denoted $H^1(\Gamma, A)$. There is a distinguished element in $H^1(\Gamma, A)$, viz. the class of the zero cocycle. Elements of this class are called *splitting cocycles*. These are of the form $z(\sigma) = a^{-1}\sigma a$ for some $a \in A$.

■ (24.1.2) **Galois groups** In the remainder of this section Γ will always be a Galois group with the Krull topology. More precisely, let k be a field, K an algebraic normal separable extension of k, and $\Gamma = \mathrm{Gal}(K/k)$.

Let $\hat{k}$ be a finite extension of k. The topology of Γ is now given by declaring all subgroups of the form $\mathrm{Gal}(K/\hat{k})$ of $\mathrm{Gal}(K/k)$ to be open.

For A one can now, e.g., take the additive group K^+ underlying K or the group of nonzero elements K^* of K. Both are given the discrete topology.

In case the Γ-group A is commutative we can turn $H^1(\Gamma, A)$ into an abelian group via the addition $(z_1 + z_2)(\sigma) = z_1(\sigma) + z_2(\sigma)$ of 1-cocycles. In this case $H^1(\Gamma, A)$ is then but one of a whole series of cohomology groups $H^i(\Gamma, A)$. In fact we have already briefly encountered one of those cohomology groups, viz. $H^2(\Gamma, K^*)$ which, if K is the algebraic closure of k, is the Brauer group of k; cf. intermezzo (20.2.16).

■ (24.1.3) **Lemma** $H^1(\Gamma, K^+) = 0$.

Proof Let $z\colon \Gamma \to K^+$ be a 1-cocycle. Because Γ is compact and K^+ is discrete, there is an open subgroup $\Gamma_0 \subset \Gamma$ such that z factors through Γ/Γ_0 giving us a 1-cocycle $\hat{z}\colon \Gamma/\Gamma_0 \to K^+$. The image of z (or $\hat{z}$) is finite; so we can assume that $\hat{z}(\Gamma/\Gamma_0) \subset L^+$ where L^+ is a finite Galois extension of k that contains the invariant field of Γ_0. By making Γ_0 smaller if necessary, we can assume that $\Gamma_0 = \mathrm{Gal}(K/L)$. It suffices to show that the 1-cocycle $\hat{z}\colon \Gamma/\Gamma_0 = \mathrm{Gal}(L/k) \to L^+$ is cohomologous to the zero cocycle. Let $\mathrm{Gal}(L/k) = \{\tau_1, \tau_2, \ldots, \tau_n\}$. By the normal basis theorem (cf. [205, Vol. III, Theorem 17, p. 57, and Lemma 2, p. 61]) there is an element $a \in L$ such that $\tau_1 a, \ldots, \tau_n a$ is a basis for L over k. We write for all $\sigma \in \mathrm{Gal}(L/k)$

$$\hat{z}(\sigma) = \sum_{\tau} x_\tau(\sigma)(\tau a)$$

with $x_\tau(\sigma) \in k$. The cocycle relation $\hat{z}(\rho\sigma) = \hat{z}(\rho) + \rho\hat{z}(\sigma)$ then gives

$$x_\tau(\rho\sigma) = x_\tau(\rho) + x_{\rho \cdot 1\tau}(\sigma) \tag{24.1.4}$$

for all $\tau \in \mathrm{Gal}(L/k)$. Now let b be the element

$$b = \sum_{\tau} x_1(\tau^{-1})\tau a$$

where 1 is the identity element of $\mathrm{Gal}(L/k)$. We claim that

$$z(\sigma) = \sigma(b) - b$$

for all $\sigma \in \mathrm{Gal}(L/k)$. Indeed

$$\begin{aligned}\sigma(b) - b &= \sum_{\tau} x_1(\tau^{-1})\sigma\tau a - \sum_{\tau} x_1(\tau^{-1})\tau a \\ &= \sum_{\tau} x_1(\tau^{-1}\sigma)\tau a - \sum_{\tau} x_1(\tau^{-1})\tau a\end{aligned}$$

Hence it suffices to show that

$$x_1(\tau^{-1}\sigma) - x_1(\tau^{-1}) = x_\tau(\sigma)$$

for all $\tau \in \mathrm{Gal}(L/k)$, which follows from (24.1.4) by taking $\tau \mapsto 1$, $\rho \mapsto \tau^{-1}$.

■ (24.1.5) **Lemma** $H^1(\Gamma, K^*) = 0$.

Proof Let $z\colon \Gamma \to K^*$ be a 1-cocycle. Arguing as in the proof of (24.1.3) we observe that z factors as $\Gamma \to \Gamma/\Gamma_0 \xrightarrow{\hat{z}} L^* \subset K^*$ where L is a finite Galois extension of k and $\Gamma_0 = \mathrm{Gal}(K/L)$. And it suffices to prove that the cocycle $\hat{z}\colon \mathrm{Gal}(L/k) \to L$ is cohomologous to the zero cocycle. Let $\mathrm{Gal}(L/k) = \{\tau_1, \ldots, \tau_n\}$. The automorphisms $\tau_1, \ldots, \tau_n$ are algebraically independent (cf. [205, Vol. III, Theorem 16, p. 56]) and hence in particular linearly independent, which means in particular that there is an $a \in L^*$ such that

$$0 \neq b = \sum_{\tau \in \mathrm{Gal}(L/k)} \hat{z}(\tau)\tau(a)$$

We then have

$$\sigma(b) = \sum_{\tau} \sigma(\hat{z}(\tau)\tau(a)) = \sum_{\tau} \hat{z}(\sigma)^{-1}\hat{z}(\sigma\tau)\sigma\tau(a) = \hat{z}(\sigma)^{-1}b$$

because by the cocycle relation $\sigma(\hat{z}(\tau)) = \hat{z}(\sigma)^{-1}\hat{z}(\sigma\tau)$. So $\hat{z}(\sigma) = b\sigma(b)^{-1} = (b^{-1})^{-1}\sigma(b^{-1})$. Q.E.D.

More generally one has

■ (24.1.6) **Lemma** $H^1(\Gamma, \mathrm{GL}_n(K)) = 0$, where $\mathrm{GL}_n(K)$ is the group of invertible $n \times n$ matrices with coefficients in K.

Proof Let $z\colon \tau \mapsto z(\tau)$ be a 1-cocycle. By the compactness of Γ and the continuity of z we can, arguing as in the beginning of the proofs of Lemmas (24.1.3) and (24.1.5), assume that K/k is finite and Galois and $\Gamma = \mathrm{Gal}(K/k)$. For every n-vector $x \in K^n$, form the vector

$$(*) \qquad b(x) = \sum_{\tau \in \Gamma} z(\tau)(\tau(x))$$

We claim that the vectors $b(x)$ generate K^n as a vector space over K. Indeed suppose this is not the case. Then there is a nontrivial linear form $u(X) = u_1X_1 + \cdots + u_nX_n$, $u_i \in K$, such that $u(b(x)) = u_1b(x)_1 + \cdots + u_nb(x)_n = 0$ for all $x \in K^n$, where $b(x)_i$ is the ith component of $b(x)$. Substituting $(*)$ we find for all $a \in K$.

$$0 = u(b(ax)) = \sum_{\tau} u(z(\tau)\tau(ax)) = \sum_{\tau} \tau(a)u(z(\tau)\tau(x))$$

By the linear independence of the τ this can only hold if $u(z(\tau)\tau(x)) = 0$ for all x, which because $z(\tau)$ is invertible means that $u = 0$ identically.

So the $b(x)$ generate K^n over K. Let $x_1, \ldots, x_n \in K^n$ be such that $b(x_1), \ldots, b(x_n)$ is a basis and let (c_{ij}) be the matrix of coefficients of the $x_1, \ldots, x_n$, i.e., $x_i = \sum_j c_{ji}e_j$ for all i where $\{e_1, \ldots, e_n\}$ is the standard basis of K^n. Let B be the matrix

$$B = \sum_{\tau} z(\tau)\tau(c)$$

Then of course $B(e_i) = \sum_\tau z(\tau)\tau(c)(e_i) = \sum_\tau z(\tau)\tau(x_i) = b(x_i)$, so the matrix B is invertible. As in the one dimensional case (Lemma (24.1.5)) we now have

$$\sigma(B) = \sum_{\tau} \sigma(z(\tau))\sigma\tau(c) = \sum_{\tau} z(\sigma)^{-1}z(\sigma\tau)\sigma\tau(c) = z(\sigma)^{-1}B$$

proving that $\sigma \mapsto z(\sigma)$ is a splitting cocycle.

Given Lemmas (24.1.3) and (24.1.6) we can prove a result which has been used before in Chapter I, 8.3 (cf. Remark (8.3.15)(ii)) and in (20.1.25) (cf. Lemma (20.1.26)).

■ (24.1.7) **Proposition** Let A be the ring of integers of a complete discrete valuation field K with finite residue field k and uniformizing element π. Let $\hat{A}_{nr}$

be the ring of integers of the completion $\hat{K}_{nr}$ of the maximal unramified extension K_{nr} of K. Then for every element $B \in \mathrm{GL}_n(\hat{A}_{nr}) = \{n \times n$ matrices with coefficients in $\hat{A}_{nr}$ and determinant a unit of $\hat{A}_{nr}\}$ there is a $C \in \mathrm{GL}_n(\hat{A}_{nr})$ such that $B = C^{-1}\tau_*(C)$ where $\tau \in \mathrm{Gal}(\hat{K}_{nr}/K)$ is the (extension by continuity of the) Frobenius substitution (characterized by $\tau(x) \equiv x^q \bmod \pi$ if $q = \#k$).

Proof We filter $\mathrm{GL}_n(\hat{A}_{nr})$ by the subgroups $U^{(m)} = \{D \in \mathrm{GL}_n(\hat{A}_{nr}) \mid D \equiv I_n \bmod \pi^m\}$. Because $\hat{A}_{nr}$ is complete, we have that $\mathrm{GL}_n(\hat{A}_{nr})$ is complete in the topology defined by the normal subgroups $U^{(m)}$. Let k_{sc} be the residue field of $\hat{A}_{nr}$; k_{sc} is an algebraic closure of k. We have that

$$\mathrm{GL}_n(\hat{A}_{nr})/U^{(1)} \simeq \mathrm{GL}_n(k_{sc})$$

Now let C be an element of $\mathrm{GL}_n(\hat{A}_{nr})$, and let $\bar{C}$ be the image of C in $\mathrm{GL}_n(k_{sc})$. Let $\Gamma = \mathrm{Gal}(k_{sc}/k)$. Since $\Gamma \simeq \hat{\mathbf{Z}}$ is topologically free on one generator τ, the Frobenius substitution, we can define a 1-cocycle $\Gamma \to \mathrm{GL}_n(k_{sc})$ by $\tau \mapsto \bar{C}$. By lemma (24.1.6) there exists a $\bar{B}_1 \in \mathrm{GL}_n(k_{sc})$ such that $\bar{B}_1^{-1}\tau(\bar{B}_1) = \bar{C}$. Let $B_1 \in \mathrm{GL}_n(\hat{A}_{nr})$ be any lift of $\bar{B}_1$, then we have

$$B_1^{-1}\tau(B_1) \equiv C \mod U^{(1)}$$

Consider the element

$$B_1 C\tau(B_1)^{-1} = I_n + \pi D_1 \in U^{(1)}$$

where D_1 is an $n \times n$ matrix with coefficients in $\hat{A}_{nr}$. Because $\tau(x) \equiv x^q \bmod \pi$ and because k_{sc} is algebraically closed (so that $x^q - x = y$ can always be solved), there exists a matrix E_2 such that $E_2 - \tau(E_2) \equiv D_1 \bmod \pi$. Let $B_2 = I_n + \pi E_2$, then $B_2(I_n + \pi D_1)\tau(B_2)^{-1} \equiv I_n \bmod \pi^2$. So

$$B_2 B_1 C\tau(B_2 B_1)^{-1} = I_n + \pi^2 D_2$$

where D_2 is an $n \times n$ matrix with coefficients in A_{nr}. Let E_3 be such that $E_3 - \tau(E_3) \equiv D_2 \bmod \pi$, take $B_3 = I_n + \pi^2 E_3, \ldots$. Continuing in this way we find a series of matrices $B_1, B_2, B_3, \ldots$. Because $B_i \in U^{(i+1)}$ and $\mathrm{GL}_n(\hat{A}_{nr})$ is complete, we know that

$$\lim_{i \to \infty} B_i B_{i-1} \cdots B_1 = B$$

exists in $\mathrm{GL}_n(\hat{A}_{nr})$, and since $\bigcap U^{(m)} = \{I_n\}$, it follows that $BC\tau(B)^{-1} = I_n$.

■ (24.1.8) Now let $\mathscr{M}$ be the group of all power series in one variable of the form $a_1 X + a_2 X^2 + \cdots$ with $a_i \in K, a_1 \neq 0$. The group operation on $\mathscr{M}$ is composition of power series. That is, if $\alpha(X), \beta(X) \in \mathscr{M}$, then $\alpha(X) \cdot \beta(X) = \alpha(\beta(X))$. The topology on $\mathscr{M}$ is the one inherited from $K[\![X]\!]$. (The field K is again an algebraic normal separable extension of k.) We let $\mathscr{M}_n$ denote the subgroup

$\mathcal{M}_n = \{\alpha(X) \in \mathcal{M} \mid \alpha(X) \equiv X \mod(\text{degree } n)\}$ of $\mathcal{M}$. These are normal subgroups of $\mathcal{M}$, and we have exact sequences

$$\{1\} \to \mathcal{M}_1 \to \mathcal{M} \to K^* \to \{1\}$$

$$\{1\} \to \mathcal{M}_{n+1} \to \mathcal{M}_n \to K^+ \to \{0\}, \qquad n \geq 1$$

The group $\mathrm{Gal}(K/k) = \Gamma$ acts on $\mathcal{M}$ by acting on the coefficients of the elements of $\mathcal{M}$, i.e., $\sigma(\alpha(X)) = \sigma_* \alpha(X)$. This is a continuous action.

■ (24.1.9) **Proposition** $H^1(\Gamma, \mathcal{M}) = 0$.

Proof This is proved in a very similar manner as Proposition (24.1.7). Indeed, let $z\colon \Gamma \to \mathcal{M}$ be a 1-cocycle. We must show that there exists an $\alpha(X) \in \mathcal{M}$ such that $z(\sigma) = \alpha^{-1}(X) \cdot \sigma(\alpha(X)) = \alpha^{-1}(\sigma(\alpha(X))$ for all $\sigma \in \Gamma$. Composing z with $\mathcal{M} \to K^*$, $\alpha(X) = a_1 X + a_2 X^2 + \cdots \mapsto a_1$ we find a 1-cocycle $\hat{z}(1)\colon \Gamma \to K^*$. By Lemma (23.1.5) there exists an element $b_1 \in K$ such that $\hat{z}(1)(\sigma) = b_1^{-1}\sigma(b_1)$ for all $\sigma \in \Gamma$. Take $\alpha_1(X) = b_1 X$ and let $z(2)\colon \Gamma \to \mathcal{M}$ be the cocycle

$$z(2)(\sigma) = \alpha_1(X) \circ z(\sigma) \circ \sigma(\alpha_1(X))^{-1}$$

Then we have $z(2)(\sigma) \in \mathcal{M}_2$ for all σ, i.e.,

$$z(2)(\sigma) = X + a_2(2)X^2 + \cdots$$

so that $\hat{z}(2)\colon \sigma \mapsto a_2(2)$ is a 1-cocycle $\Gamma \to K^+$. By Lemma (23.1.3) there exists an element $b_2 \in K^+$ such that $\hat{z}(2)(\sigma) = -b_2 + \sigma(b_2)$. Let $\beta_2(X) = X + b_2 X^2$ and $\alpha_2(X) = \beta_2(X) \circ \alpha_1(X)$. Let $z(3)\colon \Gamma \to \mathcal{M}$ be the cocycle

$$z(3)(\sigma) = \alpha_2(X) \circ z(\sigma) \circ \sigma(\alpha_2(X))^{-1} = \beta_2(X) \circ z(1)(\sigma) \circ \sigma(\beta_2(X))^{-1}$$

with values in $\mathcal{M}_3$. Continuing in this way we obtain a sequence of elements $\alpha_1(X)$, $\alpha_2(X)$, ...; $\alpha_n(X) = \beta_n(X) \circ \alpha_{n-1}(X)$; $\beta_n(X) = X + b_n X^n$, such that $\alpha_n(X) \equiv \alpha_{n-1}(X) \mod \mathcal{M}_n$ so that the sequence $\alpha_1(X), \alpha_2(X), \ldots$ converges to an element $\alpha(X) \in \mathcal{M}$. Then (since $\mathcal{M}$ is Hausdorff) we have $z(\sigma) = \alpha^{-1}(X) \circ \sigma(\alpha(X))$.

■ (24.1.10) Let $F(X, Y)$ be a (one dimensional commutative) formal group law over k and let K be a normal algebraic separable extension of k. We shall use $\mathrm{Iso}_{K/k}(F)$ to denote the set of isomorphism classes of formal group laws over k that become isomorphic to $F(X, Y)$ over K; the elements of $\mathrm{Iso}_{K/k}(F)$ are also called the *K/k-forms* of $F(X, Y)$.

■ (24.1.11) **The map** $\mathrm{Iso}_{K/k}(F) \to H^1(\Gamma, \mathrm{Aut}_K(F(X, Y)))$ Let $G(X, Y)$ be a K/k-form of $F(X, Y)$ and let $\alpha(X)\colon F(X, Y) \to G(X, Y)$ be an isomorphism over K. Because $G(X, Y)$ and $F(X, Y)$ are defined over k, we have for all $\sigma \in \Gamma = \mathrm{Gal}(K/k)$

$$(\sigma_*\alpha)(F(X, Y)) = \sigma_*(\alpha(F(X, Y))) = \sigma_*(G(\alpha(X), \alpha(Y))) = G(\sigma_*\alpha(X), \sigma_*\alpha(Y))$$

so that $\sigma_*\alpha(X)$ is also an isomorphism over K from $F(X, Y)$ to $G(X, Y)$. It follows that $z(\sigma) = \alpha^{-1}(X) \circ \sigma_*\alpha(X)$ is an automorphism of $F(X, Y)$. We claim that

$$z\colon \Gamma \to \mathrm{Aut}_K(F(X, Y)), \qquad \sigma \mapsto \alpha^{-1}(X) \circ \sigma_*\alpha(X) \tag{24.1.12}$$

is a 1-cocycle. Indeed

$$\begin{aligned} z(\sigma\tau) &= \alpha^{-1}(X) \circ \sigma_*\tau_*\alpha(X) \\ &= \alpha^{-1}(X) \circ \sigma_*\alpha(X) \circ \sigma_*\alpha^{-1}(X) \circ \sigma_*\tau_*\alpha(X) = z(\sigma) \circ \sigma z(\tau). \end{aligned}$$

Further, we claim that z is also a continuous map (where the topology on $\mathrm{Aut}_K(F(X, Y))$ is induced from the topology of $\mathcal{M} \subset K[\![X]\!]$). To see this let k_n be the field obtained from k by adjoining all the coefficients of $X, X^2, \ldots, X^n$ in $\alpha(X)$ to k, and let $\Gamma_n \subset \Gamma$ be the open subgroup $\mathrm{Gal}(K/k_n)$, then if $\sigma^{-1}\tau \in \Gamma_n$ we have $\sigma_*\alpha(X) \equiv \tau_*\alpha(X) \bmod(\text{degree } n+1)$ and hence $z(\sigma) \equiv z(\tau) \bmod(\text{degree } n+1)$. This proves that z is continuous.

The map (24.1.12) defined above depends on $\alpha(X)$ (and $G(X, Y)$). We claim that the cohomology class in $H^1(\Gamma, \mathrm{Aut}_K(F(X, Y)))$ depends only on the isomorphism class over k of $G(X, Y)$. To see this first observe that any other isomorphism $\beta(X)\colon F(X, Y) \to G(X, Y)$ is of the form $\beta(X) = \alpha(X) \circ \gamma(X)$ for a certain $\gamma(X) \in \mathrm{Aut}_K(F(X, Y))$. So that

$$\hat{z}(\sigma) = \beta^{-1}(X) \circ \sigma_*\beta(X) = \gamma^{-1}(X) \circ z(\sigma) \circ \sigma_*\gamma(X)$$

which is cohomologous to $z(\sigma)$. Next if $\delta(X)\colon G(X, Y) \to H(X, Y)$ is an isomorphism over k. Then $\delta(X) \circ \alpha(X)\colon F(X, Y) \to H(X, Y)$ is an isomorphism over K and

$$\begin{aligned} (\delta(X) \circ \alpha(X))^{-1} \circ \sigma_*(\delta(X) \circ \alpha(X)) &= \alpha^{-1}(X) \circ \delta^{-1}(X) \circ \sigma_*\delta(X) \circ \sigma\alpha(X) \\ &= \alpha^{-1}(X) \circ \sigma_*\alpha(X) \end{aligned}$$

because $\sigma_*\delta(X) = \delta(X)$. We have therefore a well-defined map

$$\Theta\colon \mathrm{Iso}_{K/k}(F(X, Y)) \to H^1(\Gamma, \mathrm{Aut}_K(F(X, Y))) \tag{24.1.13}$$

■ (24.1.14) **Theorem** The map Θ of (24.1.13) is a bijection.

Proof First we show that Θ is injective. Suppose therefore that $G(X, Y)$, $H(X, Y)$ are formal group laws over k and that there are isomorphisms $\alpha(X)\colon F(X, Y) \to G(X, Y)$, $\beta(X)\colon F(X, Y) \to H(X, Y)$ over K such that the associated 1-cocycles (defined as in (24.1.11) are cohomologous. That is, there exists an element $\gamma(X) \in \mathrm{Aut}_K(F(X, Y))$ such that

$$\alpha^{-1}(X) \circ \sigma_*\alpha(X) = \gamma^{-1}(X) \circ \beta^{-1}(X) \circ \sigma_*\beta(X) \circ \sigma_*(\gamma(X)) \tag{24.1.15}$$

Composing both sides of (23.1.15) with $\beta(X) \circ \gamma(X)$ on the left and $\sigma_*(\alpha^{-1}(X))$ on the right, we obtain

$$\beta(X) \circ \gamma(X) \circ \alpha^{-1}(X) = \sigma_*(\beta(X) \circ \gamma(X) \circ \alpha^{-1}(X))$$

so that

$$\beta(X) \circ \gamma(X) \circ \alpha^{-1}(X)\colon G(X, Y) \to F(X, Y) \to F(X, Y) \to H(X, Y)$$

is an isomorphism over k.

To prove that Θ is surjective consider a cocycle $z\colon \Gamma \to \mathrm{Aut}_K(F(X, Y))$. Now $\mathrm{Aut}_K(F(X, Y))$ is a (topological) subgroup of $\mathcal{M}$, so that by Proposition (23.1.7) there exists a power series $\alpha(X) \in \mathcal{M}$ such that $z(\sigma) = \alpha^{-1}(X) \circ \sigma_*\alpha(X)$ for all $\sigma \in \Gamma$. We now define a formal group law $G(X, Y)$ by

$$G(X, Y) = \alpha(F(\alpha^{-1}(X), \alpha^{-1}(Y)))$$

A priori $G(X, Y)$ is a formal group law over K which is isomorphic over K to $F(X, Y)$ via $\alpha(X)$. However because $\sigma_*(\alpha(X)) = \alpha(X) \circ z(\sigma)$, we have

$$\begin{aligned}
\sigma_* G(X, Y) &= \sigma_*\alpha(F(\sigma_*(\alpha)^{-1}(X), \sigma_*(\alpha)^{-1}(Y)) \\
&= \alpha(X) \circ z(\sigma) F(z(\sigma)^{-1} \circ \alpha^{-1}(X), z(\sigma)^{-1} \circ \alpha^{-1}(Y)) \\
&= \alpha(F(\alpha^{-1}(X), \alpha^{-1}(Y))) \\
&= G(X, Y)
\end{aligned}$$

so that in fact $G(X, Y)$ has all its coefficients in k and hence is a formal group law over k. Q.E.D.

24.2 Classification of one dimensional formal group laws over finite fields: characteristic polynomials

■ (24.2.1) **Some notation and a construction** Choose a prime number p and a number $h \in \mathbf{N}$. Let $F_h(X, Y)$ denote the formal group law over $\mathbf{Z}$ with logarithm $f_h(X) = X + p^{-1}f_h(X^{p^h})$, and let $\bar{F}_h(X, Y)$ denotes its reduction over $\mathbf{Z}/(p) = \mathbf{F}_p$; we shall also consider $\bar{F}_h(X, Y)$ over algebraic extensions of $\mathbf{F}_p$ without changing notation to call attention to this fact.

Let $\mathbf{F}_q$ be some fixed finite extension of $\mathbf{F}_p$, $q = p^r$, and $G(X, Y)$ be a formal group law over $\mathbf{F}_q$ of height h (same h as above; so that $G(X, Y)$ is an $\mathbf{F}(p^\infty)/\mathbf{F}_q$-form of $\bar{F}_h(X, Y)$). We write $\xi_G(X)$ for the Frobenius endomorphism of $G(X, Y)$ *over* $\mathbf{F}_q$; i.e., $\xi_G(X) = X^q$.

We shall write $\mathrm{End}(G(X, Y))$ for the ring of endomorphisms of $G(X, Y)$ over $\mathbf{F}(p^\infty)$. Then $\mathrm{End}(G(X, Y))$ is isomorphic to the ring of integers of D_h, and ξ_G generates a commutative subfield $\mathbf{Q}_p(\xi_G)$ of D_h. Let $\Lambda = \Lambda(G)$ be the ring of integers of the maximal unramified subfield of $\mathbf{Q}_p(\xi_G)$. We use Φ_G to denote the irreducible polynomial over $\Lambda(G) \otimes \mathbf{Q}_p$ of which ξ_G is a root.

We write e for $e(\mathbf{Q}_p(\xi_G)/\mathbf{Q}_p)$, the ramification index of $\mathbf{Q}_p(\xi_G)$ and f for $f(\mathbf{Q}_p(\xi_G)/\mathbf{Q}_p)$, the residue extension degree of $\mathbf{Q}_p(\xi_G)$. By restriction to Λ of J: $\mathrm{End}_{\mathbf{F}_q}(G(X, Y)) \to \mathbf{F}_q$ we find a natural homomorphism $J: \Lambda \to \mathbf{F}_q$ and we let λ: $\Lambda \to W_{p^\infty}(\mathbf{F}_q)$ be the unique isomorphism such that the diagram

$$\begin{array}{ccc} \Lambda & \xrightarrow{\lambda} & W_{p^\infty}(\mathbf{F}_{p^f}) \\ & {\scriptstyle J}\searrow \quad \swarrow{\scriptstyle w_1} & \\ & \mathbf{F}_{p^f} & \end{array}$$

commutes. (Here w_1 is the projection on the first component.) Applying λ to the coefficients of Φ_G, we find a polynomial $\Psi_G(x) = x^e + b_1 x^{e-1} + \cdots + b_e$ with coefficients in $W_{p^\infty}(\mathbf{F}_{p^f})$. This polynomial will be called the *characteristic polynomials* of $G(X, Y)$.

■ (24.2.2) **Remarks** We note that the "normalization" that the introduction of λ accomplishes sees to it that isomorphic formal group laws have the same characteristic polynomial.

(24.2.3) Over $\mathbf{Q}_p(b_1, \ldots, b_e)$ the field $\mathbf{Q}_p(\xi_G)$ (more properly an isomorphic field) is generated by a root of $\Psi_G(x)$. It follows for degree reasons that

$$[\mathbf{Q}_p(b_1, \ldots, b_e) : \mathbf{Q}_p] = f \tag{24.2.4}$$

We also note that since $\mathbf{Q}_p(\xi_G) \subset \mathrm{End}_{\mathbf{F}_q}(G(X, Y))$, we have that Λ is contained in $\mathrm{End}_{\mathbf{F}_q}(G(X, Y))$ so that $J(\Lambda) = \mathbf{F}_{p^f} \subset \mathbf{F}_q$ so that q is a power of p^f, i.e.,

$$f \text{ divides } r \tag{24.2.5}$$

We shall from now on in Section 24 use A_r to denote $W_{p^\infty}(\mathbf{F}_q)$ and K_r to denote the quotient field $A_r \otimes \mathbf{Q}_p$, where $q = p^r$.

■ (24.2.6) **Theorem** The characteristic polynomial $\Psi_G(x)$ of a formal group law $G(X, Y)$ over $\mathbf{F}_q$, $q = p^r$, of height h has the following properties: .

(i) $\Psi_G(x) = x^e + b_1 x^{e-1} + \cdots + b_e$ is an irreducible polynomial over K_r with coefficients in A_r.

(ii) If ξ is a root of $\Psi_G(x)$, then $K_r(\xi)/K_r$ is totally ramified.

(iii) $f = [\mathbf{Q}_p(b_1, \ldots, b_e) : \mathbf{Q}_p]$ and $fe \mid h$.

(iv) $v_p(b_e) = h^{-1} re$ (where $q = p^r$ and v_p is the normalized exponential valuation on A_r).

Proof (iii) According to the construction of $\Psi_G(x)$ we know that $fe = [\mathbf{Q}_p(\xi_G) : \mathbf{Q}_p]$, but $\mathbf{Q}_p(\xi_G)$ is (isomorphic to) a commutative subfield of D_h, the division algebra of rank h^2 and invariant h^{-1}. It follows that $[\mathbf{Q}_p(\xi_G) : \mathbf{Q}_p]$ divides h. (Cf. the intermezzo on division algebras (20.2.16).)

(iv) Let D_h be the field of quotients of $E_h = \mathrm{End}(\bar{F}_h(X, Y))$ and let v_p be the unique extension to D_h of the p-adic valuation on $\mathbf{Q}_p$. We know (cf. (20.2.23)–(20.2.25)) that v_p is discrete on D_h and that $\zeta(X) = X^p$ is a prime

element and that $v_p(\zeta(X)) = h^{-1}$. Now let $\alpha(X)$ be an isomorphism over $\mathbf{F}(p^\infty)$ of $G(X, Y)$ with $\bar{F}_h(X, Y)$. This induces an isomorphism $\mathrm{End}(G(X, Y)) \to \mathrm{End}(\bar{F}_h(X, Y))$, $\beta(X) \mapsto \alpha^{-1}(X) \circ \beta(X) \circ \alpha(X)$. Under this isomorphism $\xi_G(X)$ is taken into $\alpha^{-1}(X) \circ \xi(X) \circ \alpha(X) = \alpha^{-1}(X) \circ \alpha(X)^q = \alpha^{-1}(X) \circ \sigma_* \alpha(X) \circ X^q$ where $\sigma \in \mathrm{Gal}(\mathbf{F}(p^\infty)/\mathbf{F}_q)$ is the Frobenius automorphism. Now $\alpha^{-1}(X) \circ \sigma_* \alpha(X)$ is an automorphism of $\bar{F}_h(X, Y)$ and $v_p(X^q) = r$. So we have

$$v_p(\alpha^{-1}(X) \circ \xi_G(X) \circ \alpha(X)) = h^{-1} r$$

Since $\mathbf{Q}_p(\xi_G)/K_f$ is totally ramified of degree e it follows that $v_p(b_e) = h^{-1} er$ proving (iv).

(i) and (ii) We have already remarked (cf. (24.2.3)) that f is a divisor of r, i.e., $K_r \supset \mathbf{Q}_p(b_1, \ldots, b_e) = W_{p^\infty}(\mathbf{F}_{p^f})$. Let K_f be the quotient field of $W_{p^\infty}(\mathbf{F}_{p^f})$, then $K_f(\xi)/K_f$ is totally ramified and K_r/K_f is unramified. So (i) and (ii) follow. (*Remark*: note that (iii) and (iv) together also imply that f divides r.)

■ (24.2.7) **Remarks** In the course of the proof of part (iv) of Theorem (24.2.4) we saw that $v_p(\xi_G) = h^{-1} r > 0$. It follows that all the coefficients $b_1, \ldots, b_e$ have valuation > 0 (i.e., are divisible by p). We note also that if $q = p$, i.e., $r = 1$, than also $f = 1$ and (iii) and (iv) together give $e = h$ so that then $v_p(b_e) = 1$. That is, in the case of formal group laws $G(X, Y)$ over $\mathbf{F}_p$ we have that $\Psi_G(x)$ is an Eisenstein polynomial.

■ (24.2.8) **Proposition** Let $\Psi(x) = x^e + b_1 x^{e-1} + \cdots + b_e$ be a polynomial over A_r and $h \in \mathbf{N}$ a natural number such that (i)–(iv) of (24.2.6) hold. Then there exists a formal group law $G(X, Y)$ over $\mathbf{F}_q$ of height h such that $\Psi_G(x) = \Psi(x)$.

Proof Let ξ be a root of $\Psi(x)$ in some suitable extension of $\mathbf{Q}_p$. Let K_f be the maximal unramified subextension of $\mathbf{Q}_p(\xi)/\mathbf{Q}_p$. Then because of (i) and (ii), we have that $[\mathbf{Q}_p(\xi) : K_f] = e$ and hence $\mathbf{Q}_p(b_1, \ldots, b_e) = K_f$. Using (iii) this gives us that $[\mathbf{Q}_p(\xi) : \mathbf{Q}] = ef$ is a divisor of h. Now by the second intermezzo on division algebras (23.1.4) we can embed in D_h every field of degree a divisor of h. So there exists an element $\beta \in D_h$ that satisfies over $\mathbf{Q}_p$ (as a subfield of D_h) the same equation as ξ. Write $\beta = \alpha\zeta^t$ where $\zeta \in D_h$ is the endomorphism $\zeta(X) = X^p$ of $\mathrm{End}(\bar{F}_h(X, Y))$ and α is a unit of D_h. We note that we must have $t = r$ because $v(\beta) = v(\xi) = e^{-1} v(b_e)$.

Now

$$\mathrm{Gal}(\mathbf{F}(p^\infty)/\mathbf{F}_q) = \hat{\mathbf{Z}} = \varprojlim_n \mathbf{Z}/(n)$$

with as free topological generator the Frobenius substitution σ: $a \mapsto a^q$, $a \in \mathbf{F}(p^\infty)$. Then $\sigma \mapsto \alpha$ defines a continuous 1-cocycle, and according to Theorem (24.1) there exists a formal group law $G(X, Y)$ of height h over $\mathbf{F}_q$ together with an isomorphism $\gamma(X)$: $\bar{F}_h(X, Y) \to G(X, Y)$ over $\mathbf{F}(p^\infty)$ such that

$\alpha = \gamma^{-1}(X) \circ \sigma_* \gamma(X)$. The isomorphism $\gamma(X)$ gives us an isomorphism $D_h \xrightarrow{\sim} \mathrm{End}(G(X, Y))$, and composing this with the embedding $\mathbf{Q}_p(\xi) \to D_h$ given by $\xi \mapsto \beta$, we thus find an embedding $\mu\colon \mathbf{Q}_p(\xi) \to \mathrm{End}(G(X, Y))$ under which ξ goes to ξ_G because

$$\beta = \alpha\zeta^r = \gamma^{-1}(X) \circ \sigma_* \gamma(X) \circ \zeta^r(X) = \gamma^{-1}(X) \circ \xi_G(X) \circ \gamma(X)$$

The embedding μ identifies the unramified subfield K_f of $\mathbf{Q}_p(\xi)$ with the unramified subfield $\Lambda_G \otimes \mathbf{Q}_p$ of $\mathbf{Q}_p(\xi_G)$ so that

$$\mu = \tau \circ (\lambda^{-1} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$$

for some $\tau \in \mathrm{Gal}(\Lambda_G \otimes \mathbf{Q}_p/\mathbf{Q}_p)$ where λ is as in (24.2.1). Now let $\tilde{G}(X, Y)$ be obtained from $G(X, Y)$ by applying τ^{-1} to the coefficients of $G(X, Y)$. Then $\Psi_{\tilde{G}}(x) = \Psi(x)$.

■ (24.2.9) **Proposition** Let $G(X, Y)$ and $H(X, Y)$ be two formal group laws of height h over $\mathbf{F}_q$ and suppose that $\Psi_G(x) = \Psi_H(x)$. Then $G(X, Y)$ and $H(X, Y)$ are isomorphic over $\mathbf{F}_q$.

Proof Choose isomorphisms over $\mathbf{F}(p^\infty)$

$$\gamma(X)\colon \bar{F}_h(X, Y) \to G(X, Y), \qquad \delta(X)\colon \bar{F}_h(X, Y) \to H(X, Y)$$

According to Theorem (24.1.14) we must show that the automorphisms

$$\alpha_\gamma(X) = \gamma^{-1}(X) \circ \sigma_* \gamma(X), \qquad \alpha_\delta(X) = \delta^{-1}(X) \circ \sigma_* \delta(X)$$

generate cohomologous 1-cocycles $\mathrm{Gal}(\mathbf{F}(p^\infty)/\mathbf{F}_q) = \hat{\mathbf{Z}} \to \mathrm{Aut}_{\mathbf{F}(p^\infty)}(\bar{F}_h(X, Y))$. (The corresponding cocycles are defined by $\sigma \mapsto \alpha_\gamma$ and $\sigma \mapsto \alpha_\delta$, where σ is the Frobenius substitution in $\mathrm{Gal}(\mathbf{F}(p^\infty/\mathbf{F}_q)$.) In other words we must find a $\beta(X) \in \mathrm{Aut}(\bar{F}_h(X, Y))$ such that

$$\alpha_\delta = \beta^{-1}\alpha_\gamma(\sigma_* \beta) \tag{24.2.10}$$

Let $\zeta \in \mathrm{End}(\bar{F}_h(X, Y)) \subset D_h$ be the element $\zeta(X) = X^p$. Then (24.2.10) holds if and only if

$$\alpha_\delta \zeta^r = \beta^{-1}\alpha_\gamma \zeta^r \beta \tag{24.2.11}$$

because D_h is a division ring and $(\sigma_* \beta)\zeta^r = \zeta^r \beta$ because $q = p^r$. Now by hypothesis the subfields $\mathbf{Q}_p(\alpha_\gamma \zeta^r)$ and $\mathbf{Q}_p(\alpha_\delta \zeta^r)$ of D_h are isomorphic (because $\Psi_G(x) = \Psi_H(x)$), so there exists by the Skolem–Noether theorem (cf. the first intermezzo on division algebras (20.2.16)) an element $\varepsilon \in D_h$ such that

$$\alpha_\delta \zeta^r = \varepsilon^{-1}\alpha_\gamma \zeta^r \varepsilon \tag{24.2.12}$$

Let λ_G and λ_H be the isomorphisms $\Lambda(G) \to W_{p^\infty}(\mathbf{F}_{p^f}) = A_f$ and $\Lambda(H) \to A_f$. The elements $\alpha_\gamma \zeta^r$ and $\alpha_\delta \zeta^r$ are roots of polynomials

$$x^e + a_1 x^{e-1} + \cdots + a_e, \qquad x^e + \hat{a}_1 x^{e-1} + \cdots + \hat{a}_e \tag{24.2.13}$$

with $a_i \in \Lambda(G)$ and $\hat{a}_i \in \Lambda(H)$ and the polynomials $\Psi_G(x)$ and $\Psi_H(x)$ are then respectively

$$\Psi_G(x) = x^e + \lambda_G a_1 x^{e-1} + \cdots + \lambda_G a_e \tag{24.2.14}$$

$$\Psi_H(x) = x^e + \lambda_H \hat{a}_1 x^{e-1} + \cdots + \lambda_H \hat{a}_e$$

By (24.2.12) and (24.2.13) we have that

$$\hat{a}_i = \varepsilon^{-1} a_i \varepsilon, \qquad i = 1, \ldots, e$$

and writing $\varepsilon = \zeta^m \beta_1$ where β_1 is a unit of D_h (recall that ζ is a prime element of D_h), we obtain

$$\hat{a}_i = \beta_1^{-1} \zeta^{-m} a_i \zeta^m \beta_1$$

(By interchanging γ and δ if necessary, one can assume that $m \geq 0$.) As usual J: $\mathrm{End}(\bar{F}_h(X, Y)) \to \mathbf{F}(p^r)$ assigns to an endomorphism $\alpha(X)$ the coefficient of X. Write $a_i = \zeta^s b_i, \hat{a}_i = \zeta^s \hat{b}_i$, where b_i and $\hat{b}_i$ are units of D_h. Then $r \mid s$ because a_i and $\hat{a}_i$ are unramified over $\mathbf{Q}_p$. A simple calculation using $\zeta^m \beta_1 \hat{a}_i = a_i \zeta^m \beta_1$ then shows that

$$J(\hat{b}_i)^{p^m} = J(b_i)$$

Now $\Psi_G(x) = \Psi_H(x)$ and $\mathbf{Q}_p(\lambda_G a_1, \ldots, \lambda_G a_e) = K_f = \mathbf{Q}_p(\lambda_H a_1, \ldots, \lambda_H a_e)$. By the definition of λ_G and λ_H, cf. (24.2.1), it follows that raising to the power p^m is the identity on the residue field of K_f, so that f divides m. Set $m = fn$.

Let $K \subset D_h$ be a maximal commutative subfield of D_h that contains $\mathbf{Q}_p(\alpha_\gamma \zeta^r)$ and such that $K/\mathbf{Q}_p(\alpha_\gamma \zeta^r)$ is totally ramified. Such a subfield exists; it has degree h over $\mathbf{Q}_p$; and since $K/\mathbf{Q}_p(\alpha_\gamma \zeta^r)$ is totally ramified and $f(\mathbf{Q}_p(\alpha_\gamma \zeta^r)/\mathbf{Q}_p) = f$, it follows that a prime element of K is of the form $\zeta^f \beta_2^{-1}$ for some unit β_2 of D_h. The nth power of $\zeta^f \beta_2^{-1}$ is of the form $\zeta^m \beta_3^{-1}$ for some unit β_3 of D_h (we use repeatedly that ζ is a uniformizing element of D_h and that the units of D_h are precisely the elements of valuation 0 in D_h). Now since $\alpha_\gamma \zeta^r$ and $\zeta^m \beta_3^{-1}$ are both elements of K, they commute so that we have (since $\varepsilon = \zeta^m \beta_1$)

$$\alpha_\delta \zeta^r = \varepsilon^{-1} \alpha_\gamma \zeta^r \varepsilon = (\beta_1^{-1} \zeta^{-m})(\zeta^m \beta_3^{-1})(\alpha_\gamma \zeta^r)(\zeta^m \beta_3^{-1})^{-1} \zeta^m \beta_1$$

$$= (\beta_3 \beta_1)^{-1} (\alpha_\gamma \zeta^r)(\beta_3 \beta_1)$$

with $\beta_3 \beta_1$ a unit of D_h. This proves the existence of a β such that (24.2.11) holds and hence proves the proposition.

■ (24.2.15) We notice that if $\Psi(x)$ is a polynomial over A_r such that conditions (i)–(iv) of Theorem (24.2.6) hold for a certain $h \in \mathbf{N}$, then h is determined by $\Psi(x)$. Thus putting together Theorem (24.2.6), Proposition (24.2.8) and Proposition (24.2.9) we obtain the classification theorem:

■ (24.2.16) **Theorem** One dimensional commutative formal group laws $G(X, Y)$ over $\mathbf{F}_q$, the finite field of $q = p^r$ elements are classified up to isomor-

phism by polynomials $\Psi(x)$ over $A_r = W_{p^\infty}(\mathbf{F}_q)$ that satisfy:

(i) $\Psi(x) = x^e + a_1 x^{e-1} + \cdots + a_e$ is irreducible over $K_r = A_r \otimes \mathbf{Q}_p$.
(ii) If ξ is a root of $\Psi(x)$, then $K_r(\xi)/K_r$ is totally ramified.
(iii) $[\mathbf{Q}_p(a_1, \ldots, a_e) : \mathbf{Q}_p]v(a_e)$ divides r.

The polynomial associated to $G(X, Y)$ is the characteristic polynomial of the Frobenius endomorphism $\xi_G(X) = X^q$ of $G(X, Y)$ as constructed in (24.2.1) and the height of the formal group law over $\mathbf{F}_q$, $q = p^r$, corresponding to $\Psi(x) = x^e + a_1 x^{e-1} + \cdots + a_e$ is $v(a_e)^{-1}re$.

In the special case $q = p$ we have that the formal group laws over $\mathbf{F}_p$ are classified by Eisenstein polynomials $\Psi(x) = x^e + b_1 x^{e-1} + \cdots + b_e$ over $\mathbf{Z}_p$ and the height of the formal group corresponding to $\Psi(x)$ is then equal to e.

24.3 Lifting Frobenius

■ (24.3.1) Let $G(X, Y)$ over $\mathbf{F}_q$ be a formal group law of height h and let $\xi_G(x) = X^q$ be the Frobenius endomorphism. The problem of this subsection is. Does there exist a characteristic zero discrete valuation ring A and a formal group law $\tilde{G}(X, Y)$ over A with an endomorphism $\tilde{\xi}_G(X)$ over A of $\tilde{G}(X, Y)$ such that $\tilde{G}(X, Y)$ reduces to $G(X, Y)$ mod $\mathfrak{m}(A)$ and such that $\tilde{\xi}_G(X)$ reduces to $\xi_G(X)$ mod $\mathfrak{m}(A)$? That is, we want to lift $G(X, Y)$ together with its Frobenius endomorphism.

■ (24.3.2) If $h = \infty$, then $G(X, Y) \simeq \hat{\mathbf{G}}_a(X, Y) = X + Y$. Now suppose A is a discrete valuation ring and $\tilde{G}(X, Y)$ and $\tilde{\xi}_G(X)$ are lifts of $\hat{\mathbf{G}}_a(X, Y)$ and $\xi_{\mathbf{G}_a}(X)$, respectively. Let $g(X)$ be the logarithm of $\tilde{G}(X, Y)$. Then $\tilde{\xi}_G(X) = g^{-1}(ag(X))$ for some $a \in \mathfrak{m}(A)$. Then $\tilde{\xi}_G(X) \circ \cdots \circ \tilde{\xi}_G(X) = g^{-1}(a^t g(X)) \equiv X^{q^t}$ mod $\mathfrak{m}(A)$ and hence $a^t g(X) \equiv X^{q^t} \not\equiv 0$ mod$(\mathfrak{m}(A), \text{degree}(q^t + 1))$ for all $t \in \mathbf{N}$. But this contradicts (21.8.4) which says that $p^e g(X) \equiv 0$ mod pA because $ht(G(X, Y)) = \infty$. (Here e is the absolute ramification index of A.) We would need, so to speak, infinite ramification to lift $\hat{\mathbf{G}}_a(X, Y)$ together with its Frobenius endomorphism.

■ (24.3.3) Now suppose that $\text{ht}(G(X, Y)) = h < \infty$. In that case we claim that we can lift $G(X, Y)$ together with its Frobenius endomorphism to characteristic zero. Indeed, we have seen in 24.2 that $\mathbf{Q}_p(\xi_G)$ is a totally ramified extension of $W_{p^\infty}(\mathbf{F}_{p^f})$ where $\mathbf{F}_{p^f}$ is a subfield of $\mathbf{F}_q$. Let A be the ring of integers of $\mathbf{Q}_p(\xi_G)$, then $A = \mathbf{Q}_p(\xi_G) \cap \text{End}_{\mathbf{F}(p^\infty)}(G(X, Y))$. Also $\text{End}_{\mathbf{F}(p^\infty)}(G(X, Y))$ is the ring of integers of $\text{End}_{\mathbf{F}(p^\infty)}(G(X, Y)) \otimes \mathbf{Q}_p \simeq D_h$. It follows (because all elements of A commute with ξ_G) that $A \subset \text{End}_{\mathbf{F}_q}(G(X, Y))$; cf. Lemma (23.1.2).

So we can consider $G(X, Y)$ as a formal A-module where A is the ring of integers of $\mathbf{Q}_p(\xi_G)$. By the existence of a universal formal A-module over $A[S]$ (cf. Section 21.4) it follows that there exists lifts of $G(X, Y)$ together with $\xi_G(X)$ over every discrete valuation ring B with residue field $\mathbf{F}_q$ that is also an A-

algebra. One such ring B is the ring of integers of the composite field $\mathbf{Q}_p(\xi_G)K = L$ (because $K_f = W_{p^\infty}(\mathbf{F}_{p^f}) \otimes \mathbf{Q}_p \subset W_{p^\infty}(\mathbf{F}_q)$ and K_f is the unramified subfield of $\mathbf{Q}_p(\xi_G)$. More generally, we can take for B the ring of integers of any ramified extension of L. We have proved

■ (24.3.4) **Theorem** Let $G(X, Y)$ be a formal group law of height $h < \infty$ over $\mathbf{F}_q$ and let A be the ring of integers of $\mathbf{Q}_p(\xi_G)K_r$. Then the residue field of A is $\mathbf{F}_q$ and there exists a formal group law $\tilde{G}(X, Y)$ over A that reduces to $G(X, Y)$ mod $\mathfrak{m}(A)$ and which admits an endomorphism $\tilde{\xi}(X)$ such that $\tilde{\xi}(X) \equiv X^q$ mod $\mathfrak{m}(A)$.

■ (24.3.5) Conversely, suppose that B is a characteristic zero discrete valuation ring with residue field k such that there exist over B a lift $\tilde{G}(X, Y)$ of $G(X, Y)$ and an endomorphism $\tilde{\xi}(X)$ of $\tilde{G}(X, Y)$ that reduces to $\xi_G(X)$ mod $\mathfrak{m}(B)$. Now $\mathrm{End}_B(\tilde{G}(X, Y)) \to \mathrm{End}_k(G(X, Y))$ is injective and J: $\mathrm{End}(\tilde{G}(X, Y)) \to B$ identifies $\mathrm{End}_B(\tilde{G}(X, Y))$ with the subring of those $b \in B$ for which $[b]_{\tilde{G}}(X) = \tilde{g}^{-1}(b\tilde{g}(X))$ happens to be integral (where $\tilde{g}(X)$ is the logarithm of $\tilde{G}(X, Y)$). Let $a = J(\tilde{\xi}(X))$. Then the reduction homomorphism induces an embedding $\mathbf{Q}_p(a) \to \mathbf{Q}_p(\xi_G)$ under which $a \mapsto \xi_G$, i.e., an isomorphism. It follows that there exists an embedding $\mathbf{Q}_p(\xi_G) \to B \otimes \mathbf{Q}_p$ under which ξ_G goes to $a \in B$, and we see that A, the ring of integers of $\mathbf{Q}_p(\xi_G)$ is embeddable in B because B is integrally closed. Moreover, $\mathbf{Q}_p(\xi_G) \to B \otimes \mathbf{Q}_p$ induces the inclusion $\mathbf{F}_{p^f} \to \mathbf{F}_q$ where $\mathbf{F}_{p^f}$ is the residue field of $\mathbf{Q}_p(\xi_G)$, given by J: $A \to \mathbf{F}_q$. So we have

■ (24.3.6) **Theorem** Let $G(X, Y)$ be a formal group law of height $h < \infty$ over $\mathbf{F}_q$; let A be the ring of integers of $\mathbf{Q}_p(\xi_G)$ where $\xi_G(X)$ is the Frobenius endomorphism of $G(X, Y)$. Let B be a discrete valuation ring with residue field $\mathbf{F}_q$. Then there exists a lift $G(X, Y)$ together with an endomorphism $\tilde{\xi}(X)$ of $\tilde{G}(X, Y)$ over B which reduces to ξ_G mod $\mathfrak{m}(B)$ if and only if there is an embedding $A \to B$ that reduces to the embedding $\mathbf{F}_{p^f} \to \mathbf{F}_q$ given by J: $A \to \mathbf{F}_q$.

24.4 Classification of formal group laws over finite fields: conjugacy classes of elements in D_h

■ (24.4.1) Consider again $\bar{F}_h(X, Y)$ over $\mathbf{F}_q$, and identify $\mathrm{End}_{\mathbf{F}(p^\infty)}(\bar{F}_h(X, Y))$ with the ring of integers E_h of D_h. For each element $\alpha \in E_h$ let $\mathrm{cl}(\alpha)$ be the conjugacy class of α (under the automorphisms $\beta \mapsto \gamma^{-1}\beta\gamma$, $\gamma \in U(E_h)$ of E_h). Let ζ be a prime element of E_h, i.e., we can, e.g., take the endomorphism $X \mapsto X^p$ for ζ; cf. (20.2.25). Let v be the unique extension of the valuation $v = v_p$ on $\mathbf{Z}_p \subset E_h$ and let T_r be the set of conjugacy classes of elements of E_h of valuation $h^{-1}r$. Now let $G(X, Y)$ be any other formal group law of height h over $\mathbf{F}_q$. Choose any isomorphism $\gamma(X)$: $\bar{F}_h(X, Y) \to G(X, Y)$ and assign to G the conjugacy class of the element $\gamma^{-1}(X) \circ \xi(X) \circ \gamma(X)$ of E_h. This defines a map

$$\psi\colon \mathrm{Iso}(\mathbf{F}_q, h) \to T_r$$

where $\mathrm{Iso}(\mathbf{F}_q, h)$ is the set of isomorphism classes of formal group laws of height h over $\mathbf{F}_q$.

■ (24.4.2) **Theorem** The map ψ is a bijection.

Proof Because $\Gamma = \mathrm{Gal}(\mathbf{F}(p^\infty)/\mathbf{F}_q)$ is topologically free on one generator σ: $a \mapsto a^q$, $a \in \mathbf{F}(p^\infty)$, we have that the 1-cocycles of Γ with values in $\mathrm{Aut}_{\mathbf{F}(p^\infty)}(\bar{F}_h(X, Y)) = U(E_h) =$ units of E_h can be identified with elements of E_h. Let $Z^1(\Gamma, U(E_h))$ be the set of 1-cocycles, then in view of the remark just made

$$\phi\colon Z^1(\Gamma, U(E_h)) \to \{\alpha \in E_h \mid v(\alpha) = h^{-1}r\}, \qquad z \mapsto z(\sigma)\zeta^r \tag{24.4.3}$$

is a bijection. Let z_1, z_2 be two 1-cocycles and suppose that they are cohomologous. Then there is an element $\beta \in U(E)$ such that $z_2(\sigma) = \beta^{-1} z_1(\sigma)(\sigma_* \beta)$. Now $\zeta^r \beta = (\sigma_* \beta)\zeta^r$, so that $z_2(\sigma)\zeta^r = \beta^{-1} z_1(\sigma)(\sigma_* \beta)\zeta^r = \beta^{-1} z_1(\sigma)\zeta^r \beta$ and we see that ϕ takes cohomologous 1-cocycles into conjugate elements and conversely. So ϕ induces an isomorphism

$$H^1(\Gamma, U(E_h)) \to T_r \tag{24.4.4}$$

The map $\psi\colon \mathrm{Iso}(\mathbf{F}_q, h) \to T_r$ can be seen as the composite (Isomorphism class of $G(X, Y)) \mapsto$ (element of $H^1(\Gamma, U(E_h))) \mapsto$ (element of T_r) defined by

$$\sigma \mapsto \gamma^{-1}(X) \circ \sigma_* \gamma(X)) \mapsto \gamma^{-1}(X) \circ \sigma_* \gamma(X) \circ \zeta^r(X)$$
$$= \gamma^{-1}(X) \circ \zeta^r(X) \circ \gamma(X) = \gamma^{-1}(X) \circ \xi_G(X) \circ \gamma(X))$$

so that ψ decomposes as $\mathrm{Iso}(\mathbf{F}_q, h) \to H^1(\Gamma, U(E_h)) \to T_r$ where the first arrow is the bijection of Theorem (24.1.14) and the second arrow is the bijection (24.4.4). This proves the theorem.

■ (24.4.5) **Remark** The classification theorem (24.4.2) is essentially the same as the classification theorem (24.2.16) by means of the polynomials $\Psi_G(x)$. Indeed, the proof of Proposition (24.2.9) consists a proof that the two elements $\alpha_\gamma \zeta^r$ and $\alpha_\delta \zeta^r$ are conjugate if (and only if) the polynomials $\Psi_G(x)$ and $\Psi_H(x)$ are equal.

■ (24.4.6) **Lemma** With notations as in (24.4.1) let α_γ be the element $\gamma^{-1}(X) \circ \xi_G(X) \circ \gamma(X)$ of E_h. Then $\beta \mapsto \gamma^{-1}\beta\gamma$ is an isomorphism of $\mathrm{End}_{\mathbf{F}_q}(G(X, Y))$ with the subring of E_h of elements commuting with α_γ.

Proof $\mathrm{End}_{\mathbf{F}_q}(G(X, Y)) = \{\delta \in \mathrm{End}_{\mathbf{F}(p^\infty)}(G(X, Y)) \mid \delta\xi_G = \xi_G \delta\}$ by Lemma (23.1.2).

■ (24.4.7) **Corollary** $\mathrm{End}_{\mathbf{F}_q}(G(X, Y))$ is the ring of integers of $\mathrm{End}_{\mathbf{F}_q}(G(X, Y)) \otimes \mathbf{Q}_p$.

Proof $\delta \in \mathrm{End}_{\mathbf{F}_q}(G(X, Y)) \Leftrightarrow \delta \in \mathrm{End}(G(X, Y))$ and $\delta\xi_G = \xi_G \delta$.

■ (24.4.8) **Corollary** There exists a formal group law $G(X, Y)$ over $\mathbf{F}_q$, $q = p^r$ of height h such that $\mathrm{End}_{\mathbf{F}_q}(G(X, Y)) = \mathrm{End}(G(X, Y))$ if and only if h divides r.

Proof If $\mathrm{End}_{\mathbf{F}_q}(G(X, Y)) = \mathrm{End}(G(X, Y))$, then $\gamma^{-1}\xi_G\gamma = \alpha_\gamma$ must be in the center of E_h which is $\mathbf{Z}_p$, hence $v(\xi_G) = v(\alpha_\gamma) \in \mathbf{N}$; and since $v(\zeta) = h^{-1}$, we must have $h \mid r$. Conversely, if $h \mid r$, then $\mathbf{Z}_p$ contains elements of valuation $h^{-1}r$ which by Theorem (24.4.2) (and the constructions of (24.4.1)) give us formal group laws $G(X, Y)$ over $\mathbf{F}_q$ with $\alpha_\gamma \in \mathbf{Z}_p \subset E_h$. (Alternatively, we note that $\bar{F}_h(X, Y)$ over $\mathbf{F}_q$ works if $h \mid r$ because we have seen that all endomorphism of $\bar{F}_h(X, Y)$ are defined over $\mathbf{F}_{p^h}$ in (20.2.5).)

(24.4.9) **Corollary** If $q = p$, i.e., $r = 1$, then $\mathrm{End}_{\mathbf{F}_p}(G(X, Y))$ is commutative and its field of quotients is totally ramified of degree h over $\mathbf{Q}_p$.

Proof The element $\alpha_\gamma = \gamma^{-1}\xi_G\gamma$ has valuation h^{-1} in this case (because $v(\zeta) = h^{-1}$). It follows that $\mathbf{Q}_p(\xi_G)$ has ramification index at least h over $\mathbf{Q}_p$. But $\mathbf{Q}_p(\xi_G)$ is embeddable in D_h and is commutative. Thus $[\mathbf{Q}_p(\xi_G) : \mathbf{Q}_p] \leq h$. Hence $[\mathbf{Q}_p(\xi_G) : \mathbf{Q}_p] = h$, and $\mathbf{Q}_p(\xi_G)/\mathbf{Q}_p$ is totally ramified. The commutant of $\mathbf{Q}_p(\xi_G)$ in D_h is $\mathbf{Q}_p(\xi_G)$ itself (being a division algebra of rank 1 over $\mathbf{Q}_p(\xi_G)$ by the first intermezzo on division algebras (20.2.16)). This also proves the first statement of (24.4.9) because of (24.4.6).

24.5 Classification of formal A-modules over finite fields

■(24.5.1) In this section A is a complete discrete valuation ring of characteristic zero with finite residue field k of q elements and uniformizing element π. Let K be the quotient field of A. We fix a maximal unramified extension K_{nr} of K and let $A_{nr} \subset K_{nr}$ be its ring of integers.

Let k' be any finite extension of k and let A' be the ring of integers of the unique unramified extension $K' \subset K_{nr}$ with residue field k'. It is now possible to give a classification theory for formal A-modules over k' in terms of characteristic polynomials with coefficients in A' which is completely analogous to the theory given in 24.2 for formal group laws (i.e., formal $\mathbf{Z}_p$-modules). Below we quickly give the constructions and results. Details of the proofs will be left to the reader.

■(24.5.2) **Some notation and construction of the characteristic polynomial** The role of $F_h(X, Y)$ in 24.2 is now played by the formal A-module $F_h^A(X, Y)$ of A-height h which has logarithm

$$f_h^A(X) = X + \pi^{-1}X^{q^h} + \pi^{-2}X^{q^{2h}} + \cdots$$

Let $\bar{F}_h^A(X, Y)$ over k be the reduction mod π of $F_h^A(X, Y)$. This formal A-module over k has as endomorphism ring the ring of integers of the central division algebra of rank h^2 and invariant h^{-1} over K. This division algebra will be denoted D_h^A and its ring of integers is E_h^A. A prime element of E_h^A is the element $\zeta^A(X) = X^q$, this element plays the role of $\zeta(X) = X^p$ in 24.2; cf. Proposition (21.3.17).

Let k' be some fixed extension of k with $q' = q^r$ elements and $G(X, Y)$ be a formal A-module over k' of A-height h. Let k_{sc} be the algebraic closure of k, then, according to Theorem (21.8.18), we know that $G(X, Y)$ and $\bar{F}_h^A(X, Y)$ are isomorphic as formal A-modules over k_{sc}. We shall write A-End$(G(X, Y))$ for the ring of formal A-module endomorphisms of $G(X, Y)$ over k_{sc}. Let $\xi_G^A(X) = X^q$ be the Frobenius formal A-module endomorphism of $G(X, Y)$. (Note that this is indeed a formal A-module endomorphism!) Now A-End$(G(X, Y))$ is isomorphic to E_h^A and $\xi_G^A(X)$ generates a commutative subfield $K(\xi_G^A)$ of A-End$(G(X, Y)) \otimes_A K$. Let $\Lambda^A(G)$ be the ring of integers of the maximal unramified subextension of K in $K(\xi_G^A)/K$ and let $\Phi_G^A(x)$ be the irreducible polynomial with coefficients in $\Lambda^A(G) \otimes K$ of which ξ_G^A is a root. Then Φ_G^A has its coefficients in $\Lambda^A(G)$ of course. We note that A-End$_{k'}(G(X, Y))$ consists precisely of the elements of A-End$(G(X, Y))$ which commute with ξ_G^A. Thus $\Lambda^A(G) \subset A$-End$_{k'}(G(X, Y))$. Let $e = e(K(\xi_G^A)/K)$ and $f = f(K(\xi_G^A)/K)$. By restriction to $\Lambda^A(G)$ of J: A-End$_{k'}(G(X, Y)) \to k'$ we obtain a homomorphism J: $\Lambda^A(G) \to k'$. Let A_f be the ring of integers of the unique unramified extension of degree f, $K_f \subset K_{nr}$. Then there is a unique isomorphism λ such that the diagram

$$\begin{array}{ccc} \Lambda^A(G) & \xrightarrow{\lambda} & A_f \\ & \searrow^{J} \quad \swarrow & \\ & k_f \subset k' & \end{array}$$

commutes, where the right arrow is a restriction of the canonical projection $A_{nr} \to k_{sc}$. Applying λ to the coefficients of Φ_G^A we find a polynomial $\Psi_G^A(x) = x^e + b_1 x^{e-1} + \cdots + b_e$ with coefficients in A_f, which will be called the characteristic A-polynomial of the formal A-module $G(X, Y)$.

The formal A-module version of Theorem (24.2.16) is now

■ (24.5.3) **Theorem** One dimensional formal A-modules over finite extensions k' of k, the residue field of A, are classified (up to A-isomorphism) by polynomials $\Psi^A(x)$ over A' satisfying:

(i) $\Psi^A(x) = x^e + a_1 x^{e-1} + \cdots + a_e$ is irreducible over $K' = A' \otimes K$.
(ii) If ξ is a root of $\Psi^A(x)$, then $K'(\xi)/K'$ is totally ramified.
(iii) $[K(a_1, \ldots, a_e) : K] v_K(a_e)$ divides $[k' : k]$.

The polynomial associated to the formal A-module $G(X, Y)$ over k' is the characteristic A-polynomial $\Psi_G^A(x)$ of the Frobenius endomorphism ξ_G^A of $G(X, Y)$ as constructed in (24.5.2), and the A-height of the formal A-module corresponding to a given $\Psi^A(x)$ such that (i)–(iii) hold is equal to $v_K(a_e)^{-1} \times [k' : k]e$. In the special case that $k' = k$ we have that the formal A-modules over A of A-height h are classified by Eisenstein polynomials $\Psi^A(x) = x^h + b_1 x^{h-1} + \cdots + b_e$ over A of degree h.

25 Rings of Curves and Artin–Hasse-like Exponential Mappings

25.1 The Witt-vector-like group functor W^F attached to a one dimensional formal group law $F(X, Y)$

■ (25.1.1) Let A be a characteristic zero ring and let $F(X, Y)$ be a one dimensional formal group law over A. Let $f(X) = X + a_2X^2 + a_3X^3 + \cdots$ be the logarithm of $F(X, Y)$, $a_i \in A \otimes \mathbf{Q}$. We define polynomials $\bar{w}_n^F(Z_1, \ldots, Z_n)$ in the indeterminates $Z_1, Z_2, \ldots$ by the formula

$$\bar{w}_n^F(Z_1, Z_2, \ldots, Z_n) = \sum_{d|n} a_{n/d} Z_d^{n/d} \tag{25.1.2}$$

Let $\Sigma_1^F(X_1, Y_1)$, $\Sigma_2^F(X_1, X_2; Y_1, Y_2)$, $\ldots$, $\Sigma_n^F(X_1, \ldots, X_n; Y_1, \ldots, Y_n)$ be the polynomials defined by the equations

$$\bar{w}_n^F(\Sigma_1^F, \Sigma_2^F, \ldots, \Sigma_n^F) = \bar{w}_n^F(X) + \bar{w}_n^F(Y) \tag{25.1.3}$$

A priori the Σ_n^F have their coefficients in $A \otimes \mathbf{Q}$. But in fact

(25.1.4) **Lemma** The $\Sigma_i^F(X_1, \ldots, X_i; Y_1, \ldots, Y_i)$ are polynomials with their coefficients in A.

■ (25.1.5) To prove this directly is a not completely trivial matter. Instead, we look at the most general situation possible, i.e., take $F(X, Y)$ to be the universal one dimensional formal group law $F_U(X, Y)$ over $\mathbf{Z}[U]$. The logarithm $f_U(X)$ of $F_U(X, Y)$ then satisfies functional equations

$$f_U(X) - \sum_{i=1}^{\infty} p^{-1} U_{p^i} f^{(p^i)}(X^{p^i}) \in \mathbf{Z}_{(p)}[U][\![X]\!] \tag{25.1.6}$$

for all prime numbers p. Now let $\bar{w}(Z_1, Z_2, \ldots)$ be the series of polynomials $\bar{w}_n^F(Z)$ of (25.1.2) for the case $F(X, Y) = F_U(X, Y)$. We claim that $\bar{w}(Z)$ satisfies the functional equations

$$\bar{w}(Z) - \sum_{i=1}^{\infty} p^{-1} U_{p^i} Q_p^i \bar{w}^{(p^i)}(Z^{p^i}) \in \mathbf{Z}_{(p)}[U][Z]^{\mathbf{N}} \tag{25.1.7}$$

Here Q_p is the operator that maps a vector $(b_1, b_2, \ldots)$ to $(c_1, c_2, c_3, \ldots)$ where $c_i = 0$ unless $p \mid i$ and $c_{pj} = b_j$ for all $j \in \mathbf{N}$.

Indeed, let $n \in \mathbf{N}$ and $n = p^r m$ with $(m, p) = 1$. The nth component of the left-hand side of (25.1.7) is then equal to

$$\begin{aligned} \bar{w}_n(Z) - p^{-1} U_p \bar{w}_{n/p}^{(p)}(Z^p) - p^{-1} U_{p^2} \bar{w}_{n/p^2}^{(p^2)}(Z^{p^2}) - \cdots - p^{-1} U_{p^r} \bar{w}_m^{(p^r)}(Z^{p^r}) \\ = \sum_{d|n} a_{n/d}(U) Z_d^{n/d} - p^{-1} U_p \sum_{d_1 | p^{-1}n} a_{p^{-1}n/d_1}(U^p) Z_{d_1}^{n/d_1} - \cdots \\ - p^{-1} U_{p^r} \sum_{d_r | m} a_{m/d_r}(U^{p^r}) Z_{d_r}^{n/d_r} \end{aligned} \tag{25.1.8}$$

Fix some divisor d of n, and let p^j be the highest power of p dividing n/d. The terms of (25.1.8) that involve Z_d are then

(i) if $i = 0$, $\quad a_{n/d} Z_d^{n/d}$

(ii) if $i > 0$, $\quad a_{n/d} Z_d^{n/d} - p^{-1} U_p a_{p^{-1}n/d}(U^p) Z_d^{n/d} - \cdots$

$$- p^{-1} U_{p^j} a_{p^{-j}n/d}(U^{p^j}) Z_d^{n/d}$$

and these expressions are integral by (25.1.6). It follows that the $\mathbf{N}$-tuple of polynomials $\bar{w}(Z)$ satisfies an (infinite dimensional) functional equation, and by the infinite dimensional version of the functional equation lemma it follows that

$$\begin{pmatrix} \Sigma_1^U(X_1, Y_1) \\ \Sigma_2^U(X_1, X_2; Y_1, Y_2) \\ \vdots \\ \Sigma_n^U(X_1, \ldots, X_n; Y_1, \ldots, Y_n) \\ \vdots \end{pmatrix} = \bar{w}^{-1}(\bar{w}(X) + \bar{w}(Y)) \tag{25.1.9}$$

is a vector of polynomials with coefficients in $\mathbf{Z}[U]$. This proves the lemma for the special case $F(X, Y) = F_U(X, Y)$. Now let $F(X, Y)$ be any one dimensional formal group law over a ring A of characteristic zero and let $\phi\colon \mathbf{Z}[U] \to A$ be the unique homomorphism such that $\phi_* F_U(X, Y) = F(X, Y)$. Then, since ϕ is a ring homomorphism, $\phi_* \Sigma_i^U(X; Y) = \Sigma_i^F$ because obviously $\phi_* \bar{w}_n(Z) = \bar{w}_n^F(Z)$. This proves the lemma. (Cf. E.3.9 for a remark pertaining to this proof.)

■ (25.1.10) We have proved more however. Let $F(X, Y)$ be a one dimensional formal group law over any ring A (not necessarily of characteristic zero) and $\phi\colon \mathbf{Z}[U] \to A$ be the unique ring homomorphism taking $F_U(X, Y)$ into $F(X, Y)$. Then we can define $\Sigma_n^F(X_1, \ldots, X_n; Y_1, \ldots, Y_n)$ as $\phi_* \Sigma_n^U(X; Y)$. Let B be any A-algebra, then the polynomials $\Sigma_n^F(X; Y)$ define an addition on $B^{\mathbf{N}} = \{(b_1, b_2, b_3, \ldots) \mid b_i \in B\}$ which gives us a (new) commutative group structure on $B^{\mathbf{N}}$. We shall denote this abelian group by $W^F(B)$. Then $W^F(-)$ is a functor $\mathbf{Alg}_A \to \mathbf{Ab}$; the group homomorphism $W^F(B) \to W^F(C)$ associated to an A-algebra homomorphism $\phi\colon B \to C$ is

$$(b_1, b_2, b_3, \ldots) \mapsto (\phi(b_1), \phi(b_2), \phi(b_3), \ldots).$$

■ (25.1.11) If $F(X, Y)$ is again a one dimensional formal group law over a characteristic zero ring, we define $\hat{w}_n^F(Z) = n\bar{w}_n^F(Z)$. The coefficients of $\hat{w}_n^F(Z)$ are then always in A (because $ia_i \in A$ for all i if $f(X) = \sum a_i X^i$ is the logarithm of $F(X, Y)$). Now $(d/dX)f(X) \cdot (\partial F/\partial X)(0, X) = 1$, so that $\sum_{i=1}^{\infty} i a_i X^{i-1}$ is always defined also if A is not necessarily of characteristic zero; it follows that $\hat{w}_n^F(Z)$ is defined for all formal group laws $F(X, Y)$. Putting everything together we have

■ (25.1.12) **Theorem** For every one dimensional formal group law $F(X, Y)$ over a ring A, there exists a functor $W^F\colon \mathbf{Alg}_A \to \mathbf{Ab}$ such that the following

properties hold:

(i) As a set-valued functor we have

$$W^F(B) = B^{\mathbf{N}} = \{(b_1, b_2, b_3, \ldots) \mid b_i \in B\}$$

and $W^F(\phi)(b_1, b_2, \ldots) = (\phi(b_1), \phi(b_2), \ldots)$ for $\phi: B \to C \in \mathbf{Alg}_A$.

(ii) The $\hat{w}_n^F$: $W^F(B) \to B$ are functorial group homomorphisms for all $n \in \mathbf{N}$.

(iii) If ϕ: $A_1 \to A_2$ is a homomorphism of rings and $F_1(X, Y)$ over A_1, $F_2(X, Y)$ over A_2 are formal group laws such that $\phi_* F_1(X, Y) = F_2(X, Y)$, then

$$W^{F_2} = W^{F_1} \circ \psi$$

where ψ: $\mathbf{Alg}_{A_2} \to \mathbf{Alg}_{A_1}$ is the obvious forgetful functor associated to ϕ: $A_1 \to A_2$.

The functors W^F are uniquely characterized by (i)–(iii); and for a fixed ring A of characteristic zero, the functors W^F, with $F(X, Y)$ a given fixed formal group law over A, are uniquely characterized by (i) and (ii) alone.

■ (25.1.13) **Addendum** The polynomials $\Sigma_i^U(X; Y)$ of (25.1.9) also define an infinite dimensional formal group law in the sense of Chapter II, Section 9.6. Thus we have for every one dimensional formal group law $F(X, Y)$ over a ring A an infinite dimensional formal group law defined by the polynomials $\Sigma_i^F(X; Y)$. This formal group law will be denoted $\hat{W}^F$.

■ (25.1.14) **Remark** If we take $F(X, Y) = \hat{G}_m^-(X, Y) = X + Y - XY$, then $\log_{G_m^-}(X) = \sum_{n=1}^{\infty} n^{-1} X^n$ so that $\hat{w}_n^{G_m^-}(X) = w_n(X)$ where the $w_n(X)$ are the usual (generalized) Witt polynomials defined in Chapter III, Section 17. Thus if $F(X, Y) = \hat{G}_m^-(X, Y)$, we recover the underlying abelian group functor of the ring functor of Witt vectors W.

■ (25.1.15) There is a second functor $\mathbf{Alg}_A \to \mathbf{Ab}$ associated to a one dimensional formal group law $F(X, Y)$ over a ring A, viz. the functor of curves $B \mapsto \mathscr{C}(F; B)$. We show that these functors are isomorphic in a way that is compatible with the base changes $F(X, Y) \to \phi_* F(X, Y)$.

To this end define the universal isomorphism $\bar{E}^U$: $W^U(-) \to \mathscr{C}(F_U; -)$ as follows:

$$\bar{E}_B^U(b_1, b_2, \ldots) = \Sigma^{F_U} b_i t^i, \qquad (b_1, b_2, \ldots) \in W^U(B)$$

this is clearly a bijection. It remains to show that it respects addition, zero elements, and inverses. To see this compose with the logarithm f_U. We have

$$f_U(\Sigma^{F_U} b_i t^i) = \sum_{i=1}^{\infty} f_U(b_i t^i) = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} a_j(U)(b_i t^i)^j$$

$$= \sum_{l=1}^{\infty} \sum_{j|l} a_j(U) b_{l/j}^j t^l = \sum_{l=1}^{\infty} \bar{w}_l(b) t^l$$

Because the addition in $W^U(-)$ is uniquely characterized by the requirement that the $\bar{w}_n$ are group homomorphisms (functorially), it follows that $\bar{E}_B^U$ is indeed a homomorphism of abelian groups. Now for an arbitrary formal group law $F(X, Y)$ over a ring A, let $\bar{E}_B^F(b_1, b_2, \ldots) = \Sigma^F b_i t^i$; then if $\phi : \mathbf{Z}[U] \to A$ is such that $\phi_* F_U(X, Y) = F(X, Y)$, we have for every A-algebra B

$$\mathscr{C}(\phi_* F_U; B) = \mathscr{C}(F; B), \qquad W^U(B) = W^F(B), \qquad \text{and} \qquad \bar{E}_B^U = \bar{E}_B^F$$

so $\bar{E}_B^F$ is a homomorphism of abelian groups.

Note that if $F(X, Y)$ admits a logarithm, we have

$$\bar{E}_B^F(b_1, b_2, \ldots) = f^{-1}\left(\sum_{l=1}^{\infty} \bar{w}_l^F(b) t^l\right)$$

which is Artin–Hasse like; more precisely this map is the analogue of the isomorphism $\bar{E}_B$ of Chapter III (17.2.7).

25.2 q-typical curves and q-typification

■ (25.2.1) Let A be a discrete valuation ring with residue field of q elements and uniformizing element π. Let $F_S^A(X, Y)$ over $A[S]$ be the universal formal A-module (cf. (21.4.8)). Let $C_1, C_2, \ldots$ be another set of indeterminates and consider $F_S^A(X, Y)$ over $A[S; C]$. Let $\gamma(t) = \sum_{i=1}^{\infty} C_i t^i$ and consider

$$g(t) = f_S^A(\gamma(t)) = \sum_{j=1}^{\infty} b_j(S, C) t^j$$

By the functional equation lemma, this power series $g(t)$ over $K[S; C]$ (where K is the quotient field of A) satisfies a functional equation

$$g(t) - \sum \pi^{-1} S_{q^i} g^{(q^i)}(t^{q^i}) \in A[S; C] \tag{25.2.2}$$

Now define $\varepsilon_q g(t)$ as

$$\varepsilon_q g(t) = \sum_{i=0}^{\infty} b_{q^i}(S, C) t^{q^i} = \hat{g}(t)$$

Then, we claim $\hat{g}(t)$ also satisfies a functional equation

$$\hat{g}(t) - \sum \pi^{-1} S_{q^i} \hat{g}^{(q^i)}(t^{q^i}) \in A[S; C] \tag{25.2.3}$$

This follows immediately by writing out what (25.2.2) means in terms of the coefficients of $g(t)$. (The reason that this works is of course that the functional equation (25.2.2) gives "feed forward relations with degrees multiplied by powers of q"); note that, e.g., $\tilde{g}(t) = \sum_{i=0}^{\infty} b_{q^{2i}}(S, C) t^{q^{2i}}$ need not satisfy a functional equation like (25.2.3).)

Now let

$$\varepsilon_q \gamma(t) = (f_S^A)^{-1}(\hat{g}(t))$$

then again by the functional equation lemma we know that $\varepsilon_q \gamma(t)$ has its coefficients in $A[S; C]$. Let

$$\varepsilon_q \gamma(t) = \sum_{i=1}^{\infty} Q_i(S; C) t^i \tag{25.2.4}$$

This defines for us certain universal polynomials $Q_i(S; C)$, $i = 1, 2, \ldots$.

Now let $B \in \mathbf{Alg}_A$ and let $F(X, Y)$ be any formal A-module over B and let $\gamma(t)$ be any curve in $F(X, Y)$ over B. Let ϕ: $A[S; C] \to B$ be the unique A-algebra homomorphism such that $\phi_* F_S^A(X, Y) = F(X, Y)$ (and $\phi_* \rho_S^A = \rho_F$) and such that $\phi_*(\sum_{i=1}^{\infty} C_i t^i) = \gamma(t)$. Let $\phi(S_i) = s_i$ and $\phi(C_i) = c_i$. We now define

$$\varepsilon_q^F \gamma(t) = \sum_{i=1}^{\infty} Q_i(s; c) t^i \tag{25.2.5}$$

and we shall call $\varepsilon_q^F \gamma(t)$ the q-typification of $\gamma(t)$. Note that ε_q^F does depend on F.

■ (25.2.6) **Definition** A curve $\gamma(t) \in \mathscr{C}(F; B)$ is called q-typical if $\varepsilon_q^F \gamma(t) = \gamma(t)$. Let $\mathscr{C}_q(F; B)$ denote the set of q-typical curves in $\mathscr{C}(F; B)$.

■ (25.2.7) **Proposition** $\mathscr{C}_q(F; B)$ is a (complete Hausdorff) filtered subgroup of $\mathscr{C}(F; B)$, ε_q^F: $\mathscr{C}(F, B) \to \mathscr{C}(F, B)$ is a homomorphism of abelian groups with image $\mathscr{C}_q(F, B)$, and $\varepsilon_q^F \varepsilon_q^F = \varepsilon_q^F$ (i.e., ε_q^F is a projector).

Before proving this we first give an alternative description of ε_q^F that works in case $F(X, Y)$ has an A-logarithm.

■ (25.2.8) Suppose that $F(X, Y)$ has an A-logarithm $f(X)$ and let ϕ: $A[S] \to B$ be the unique homomorphism that takes the formal A-module $F_S^A(X, Y)$ into the formal A-module $F(X, Y)$. Then $f(X) = \phi_* f_S^A(X)$. It follows that if $\gamma(t) \in \mathscr{C}(F; B)$, then $\varepsilon_q^F \gamma(t)$ can be obtained as follows: form $f(\gamma(t))$; remove all terms of the form $c_i t^i$ of $f(\gamma(t))$ for which i is not a power of q; let the sum of the remaining terms be $\hat{g}(t)$; then $\varepsilon_q^F \gamma(t) = f^{-1}(\hat{g}(t))$. This obviously works because this is precisely what one does in the universal case described in (25.2.1).

■ (25.2.9) **Proof of Proposition (25.2.7)** A particular formal A-module $F(X, Y)$ which has an A-logarithm is $F_S^A(X, Y)$ over $A[S; C; D]$ where D is yet another set of indeterminates. Let $\tilde{\gamma}(t) = \sum C_i t^i$, $\tilde{\delta}(t) = \sum D_i t^i$. Then using the description of ε_q given in (25.2.8), we see that

$$\varepsilon_q(\tilde{\gamma}(t) +_{F_S^A} \tilde{\delta}(t)) = \varepsilon_q \tilde{\gamma}(t) +_{F_S^A} \varepsilon_q \tilde{\delta}(t) \tag{25.2.10}$$

$$\varepsilon_q(\varepsilon_q(\tilde{\gamma}(t))) = \varepsilon_q(\tilde{\gamma}(t))$$

Now let $F(X, Y)$ be any formal A-module over an A-algebra B and let $\gamma(t)$, $\delta(t) \in \mathscr{C}(F; B)$. Let ϕ: $A[S; C; D] \to B$ be the unique homomorphism such that $\phi_*(F_S^A(X, Y)) = F(X, Y)$ (as formal A-modules), $\phi_*(\tilde{\gamma}(t)) = \gamma(t)$, $\phi_* \tilde{\delta}(t) = \delta(t)$. Then $\varepsilon_q^F \gamma(t) = \varepsilon_q^F \varepsilon_q^F \gamma(t)$ and $\varepsilon_q^F(\gamma(t) +_F \delta(t) = \varepsilon_q^F \gamma(t) +_F \varepsilon_q^F \delta(t)$ follow by applying ϕ_* to (25.2.10).

■ (25.2.11) **Remarks**

(i) If $F(X, Y)$ over B has an A-logarithm $f(X)$ then $\gamma(t) \in \mathscr{C}(F; B)$ is in $\mathscr{C}_q(F; B)$ if and only if $f(\gamma(t))$ involves only qth powers of t. This follows from (25.2.8).

(ii) One can similarly define $\hat{q}$-typification and $\hat{q}$-typical curves for all $\hat{q}$ that divide q, but as a rule $\hat{q}$-typification is not defined for $\hat{q} = q^i$, $i \geq 2$.

(iii) Of course one can quite generally define what a $\hat{q}$-typical curve is for any power $\hat{q}$ of q whatever: if $F(X, Y)$ admits an A-logarithm, these are the curves $\gamma(t)$ such that $f(\gamma(t))$ is a sum of $\hat{q}$-powers of t (with coefficients); and if $F(X, Y)$ does not admit an A-logarithm, these are all curves $\gamma(t)$ for which there exists a covering $\psi: \tilde{B} \to B$, a lift $\tilde{F}(X, Y)$ of $F(X, Y)$, and a $\hat{q}$-typical curve $\tilde{\gamma}(t)$ in $\mathscr{C}(\tilde{F}; \tilde{B})$ that reduces to $\gamma(t)$ under ψ.

■ (25.2.12) **Definition** Let $\bar{E}^F$: $W^F(-) \to \mathscr{C}(F; -)$ be the isomorphism of (25.1.15), then the projector ε_q^F of $\mathscr{C}(F; -)$ yields a projector of $W^F(-)$ which we shall also denote ε_q^F. The image functor $\varepsilon_q^F W^F(-)$ will also be denoted $W_{q.\infty}^F(-)$. Note that with this notation

$$W_{p,\infty}^{\hat{\mathbf{G}}_m}(-) = W_{p^\infty}(-)$$

where $W_{p^\infty}(-)$ is the Witt vector functor discussed at length in Chapter III, Section 17.4.

For later purposes, we shall need a universality result on curves in $\mathscr{C}_q(F; B)$.

■ (25.2.13) **Lemma** Let $\gamma_C(t) \in C_q(F_U; A[S; C])$ be the q-typical curve

$$\gamma_C(t) = \varepsilon_q^{F_U}\left(\sum_{i=0}^{\infty} {}^{F_U}C_i t^{q^i}\right)$$

then for every A-algebra B, every formal A-module $F(X, Y)$ over B, and every curve $\gamma(t) \in \mathscr{C}_q(F; B)$, there exists a unique homomorphism ϕ: $A[S; C] \to B$ such that $\phi_* \gamma_C(t) = \gamma(t)$ and $\phi_* F^U(X, Y) = F(X, Y)$.

Proof First uniqueness; ϕ is in any case unique on $A[S]$. Suppose that there are two extensions ϕ, ψ, both taking $\gamma_C(t)$ into $\gamma(t)$, and suppose $\phi \neq \psi$. Let i be the smallest element of $\mathbf{N}$ such that $\phi(C_i) \neq \psi(C_i)$. Then we have modulo degree$(q^i + 1)$

$$\begin{aligned}\sum_{n=0}^{\infty}{}^F \phi(C_n)t^{q^n} - \sum_{n=0}^{\infty}{}^F \psi(C_n)t^{q^n} &\equiv \sum_{n=0}^{i-1}{}^F \phi(C_n)t^{q^n} - \sum_{n=0}^{i-1}{}^F \psi(C_n)t^{q^n} \\ &\quad + \phi(C_i)t^{q^i} - \psi(C_i)t^{q^i} \\ &= (\phi(C_i) - \psi(C_i))t^{q^i}\end{aligned}$$

which contradicts

$$\varepsilon_q^F \phi_*(\gamma_C(t)) = \phi_*(\varepsilon_q^F \gamma_C(t)) = \gamma(t) = \psi_*(\varepsilon_q^F \gamma_C(t)) = \varepsilon_q^F(\psi_*(\gamma_C(t))$$

because ε_q^F is a group homomorphism and if $\delta(t) \equiv bt^j \bmod(\text{degree } j+1)$ and j is a power of q, then $\varepsilon_q^F(\delta(t)) \equiv bt^j \bmod(\text{degree } j+1)$.

To prove existence it suffices to do this in the case that B is A-torsion free because $\mathscr{C}_q(F;\psi)\colon \mathscr{C}_q(F;B_1) \to \mathscr{C}_q(F;B_2)$ is surjective if $\psi\colon B_1 \to B_2$ is surjective as follows from the commutativity of the diagram

$$\begin{array}{ccc} \mathscr{C}(F;B_1) & \xrightarrow{\varepsilon_q^F} & \mathscr{C}_q(F;B_1) \\ \downarrow{\scriptstyle \mathscr{C}(F;\psi)} & & \downarrow{\scriptstyle \mathscr{C}_q(F;\psi)} \\ \mathscr{C}(F;B_2) & \xrightarrow{\varepsilon_q^F} & \mathscr{C}_q(F;B_2) \end{array}$$

and the surjectivity of ε_q^F, $\mathscr{C}(F,\psi)$ and ε_q^F. So suppose that $\gamma(t) \in \mathscr{C}_q(F;B)$ and that B is A-torsion free. Suppose we have already found $b_0, b_1, b_2, \ldots, b_n \in B$ such that

$$\varepsilon_q^F\left(\sum_{i=0}^{n}{}^F\, b_i t^{q^i}\right) \equiv \gamma(t) \quad \bmod(\text{degree } q^n+1) \tag{25.2.14}$$

Let

$$f\left(\varepsilon_q^F \sum_{i=0}^{n}{}^F\, b_i t^{q^i}\right) = \sum_{i=0}^{\infty} x_i t^{q^i}, \qquad f(\gamma(t)) = \sum_{i=0}^{\infty} y_i t^{q^i} \tag{25.2.15}$$

It then follows from (25.2.14) that $x_i = y_i$ for $i \le n$ in (25.2.15) which then (q-typicality!) implies that

$$\varepsilon_q^F\left(\sum_{i=0}^{n} b_i t^{q^i}\right) \equiv \gamma(t) \quad \bmod(\text{degree } q^{n+1})$$

which in turn implies the existence of a $b_{n+1} \in B$ such that (25.2.14) holds with n replaced by $n+1$.

An immediate corollary is a second, very similar representability result:

■ (25.2.16) **Lemma** Let $F(X, Y)$ be a formal A-module over an A-algebra B. Then for every B-algebra B' and every q-typical curve $\gamma(t) \in \mathscr{C}_q(F;B')$, there is a unique homomorphism $\phi\colon B[C_0, C_1, C_2, \ldots] \to B'$ such that

$$\phi_*(\varepsilon_q^F(\textstyle\sum^F C_i t^{q^i})) = \gamma(t)$$

(I.e., the B-algebra $B[C]$ represents the functor $B' \mapsto \mathscr{C}_q(F;B')$.)

Proof There is a one-one correspondence between homomorphisms $\psi\colon A[S;C] \to B'$ such that $\psi_* F_S^A(X,Y) = F(X,Y)$ and homomorphisms $\phi\colon B[C] \to B'$. This correspondence is given by "$\phi(C_i) = \psi(C_i)$". Now apply Lemma (25.2.13).

■ (25.2.17) **Notation and remark** It follows from (25.2.16) and the definition (25.2.12) that as a set functor

$$W_{q,\infty}^F(B') = \{(b_0, b_1, b_2, \ldots) \mid b_i \in B'\}$$

We shall (as a rule) also use $\bar{E}^F$ to denote the isomorphism $W^F_{q,\infty}(-) \to \mathscr{C}_q(F; -)$ induced by $\bar{E}^F : W^F(-) \to \mathscr{C}(F; -)$. Thus we have for $(b_0, b_1, b_2, \ldots) \in W^F_{q,\infty}(B')$:

$$\bar{E}^F(b_0, b_1, b_2, \ldots) = \varepsilon^F_q\left(\sum_{i=0}^{\infty F} b_i t^{q^i}\right) \tag{25.2.18}$$

and we have a commutative diagram

$$\begin{array}{ccc} W^F(-) & \xrightarrow{\bar{E}^F} & \mathscr{C}(F; -) \\ \downarrow{\scriptstyle \varepsilon^F_q} & & \downarrow{\scriptstyle \varepsilon^F_q} \\ W^F_{q,\infty}(-) & \xrightarrow{\bar{E}^F} & \mathscr{C}_q(F; -) \end{array}$$

25.3 "Ramified Witt vectors" (local case)

■ (25.3.1) In this subsection A is a complete discrete valuation ring with quotient field K and residue field k of q elements. Let $F(X, Y)$ be a formal A-module over A of A-height 1. According to Theorem (24.5.3), Theorem (21.8.9), or Proposition (8.3.22) of Chapter I, there is then a unique uniformizing element $\pi(F)$ of A such that the characteristic polynomial of $F(X, Y)$ is equal to $\Psi^A_F(x) = x - \pi(F)$. The element $\pi(F)$ is also the unique element of A such that the logarithm $f(X)$ of $F(X, Y)$ satisfies $f(X) - \pi(F)^{-1} f(X^q) \in A[\![X]\!]$.

■ (25.3.2) We now define the Witt polynomials $w^F_{q,n}(Z_0, \ldots, Z_n)$ associated to $F(X, Y)$ as

$$w^F_{q,n}(Z) = \pi(F)^n Z_n + \pi(F)^n a_q Z^q_{n-1} + \cdots + \pi(F)^n a_{q^n} Z^{q^n}_0 \tag{25.3.3}$$

where the a_{q^i} are the coefficients of X^{q^i} in $f(X) = \sum_{i=1}^{\infty} a_i X^i$. Note that $f(X) - \pi(F)^{-1} f(X^q) \in A[\![X]\!]$ implies that $v(a_{q^i}) = -i$ where v is the normalized exponential valuation on K, so the coefficients of $w^F_{q,n}(Z)$ are all in A; in fact modulo $\pi(F)$ we have $w^F_{q,n}(Z) \equiv \pi(F)^n a_{q^n} Z^{q^n}_0$.

■ (25.3.4) Let B be an A-algebra that is A-torsion free and let π be a uniformizing element of A. Let $R_q(B \otimes_A K)$ be the abelian group of all power series in t with coefficients in $B \otimes_A K$ of the form $\sum_{i=0}^{\infty} x_i t^{q^i}$ (with the obvious coefficientwise addition). We define a multiplication and an A-module structure on $R_q(B \otimes_A K)$ as follows:

$$\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right) *_\pi \left(\sum_{i=0}^{\infty} y_i t^{q^i}\right) = \sum_{i=0}^{\infty} \pi^i x_i y_i t^{q^i}$$

$$a\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right) = \sum_{i=0}^{\infty} a x_i t^{q^i}$$

One checks trivially that these definitions turn $R_q(B \otimes_A K)$ into an A-algebra with unit element $\sum_{i=0}^{\infty} \pi^{-i} X^{q^i}$. We shall denote this A-algebra by $R_{q,\pi}(B \otimes_A K)$.

■ (25.3.5) **The A-algebra functors $\mathscr{C}_q(F;-)$** Let $F(X, Y)$ be as in (25.3.1). We are going to define an A-algebra structure on $\mathscr{C}_q(F; B)$ for all A-algebras B. Recall that the logarithm $f(X)$ of $F(X, Y)$ satisfies

$$(25.3.6)\quad f(X) = \sum_{i=1}^{\infty} a_i X^i, \qquad a_{qi} - \pi(F)^{-1} a_i \in A \qquad \text{for all} \quad i \in \mathbf{N}$$

$$v(a_i) = -r \qquad \text{if} \quad q^r \mid i \quad \text{but} \quad q^{r+1} \nmid i$$

To define the A-algebra structure on $\mathscr{C}_q(F; B)$ for all A-algebras B we first do a special case, viz. $B = A[C_0, C_1, \ldots; D_0, D_2, \ldots]$ where the C_i and D_i are indeterminates. Let $\sigma\colon B \otimes_A K \to B \otimes_A K$ be the K-endomorphism $C_i \mapsto C_i^q$, $D_i \mapsto D_i^q$. Note that $\sigma(b) \equiv b^q \bmod \pi(F)B$ for all $b \in B$. Now let $\gamma(t)$ and $\delta(t)$ be two elements of $\mathscr{C}_q(F; B)$ and consider

$$f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i}, \qquad f(\delta(t)) = \sum_{i=0}^{\infty} y_i t^{q^i}$$

($f(\gamma(t)), f(\delta(t))$ are of the form indicated because $\gamma(t), \delta(t) \in \mathscr{C}_q(F; B)$.) Here the x_i and y_i are certain polynomials (with coefficients in K) in the C_i and D_i. By the functional equation lemma these coefficients satisfy

$$(25.3.7)\quad x_0, y_0 \in B; \qquad x_i - \pi(F)^{-1}\sigma(x_{i-1}) \in B$$

$$y_i - \pi(F)^{-1}\sigma(y_{i-1}) \in B \qquad \text{for} \quad i \in \mathbf{N}$$

Now consider

$$\varepsilon(t) = f(\gamma(t)) *_{\pi(F)} f(\delta(t)) = \sum_{i=0}^{\infty} \pi(F)^i x_i y_i t^{q^i}$$

We claim that this power series also satisfies a functional equation $\varepsilon(t) - \pi(F)^{-1}\varepsilon(t^q) \in B[\![t]\!]$. Indeed, we have $\pi(F)^0 x_0 y_0 = x_0 y_0 \in B$, and writing $x_i = \pi(F)^{-1}\sigma(x_{i-1}) + b_i(x)$, $y_i = \pi(F)^{-1}\sigma(y_{i-1}) + b_i(y)$, $b_i(x)$, $b_i(y) \in B$, we have

$$\begin{aligned}\pi(F)^i x_i y_i &- \pi(F)^{-1}\sigma(\pi(F)^{i-1} x_{i-1} y_{i-1}) \\ &= \pi(F)^i \pi(F)^{-1}\sigma(x_{i-1}) b_i(y) + \pi(F)^i \pi(F)^{-1}\sigma(y_{i-1}) b_i(x) + \pi(F)^i b_i(x) b_i(y) \\ &\equiv 0 \mod B\end{aligned}$$

because $\pi(F)^i x_i$, $\pi(F)^i y_i \in B$ for all $i \in \mathbf{N} \cup \{0\}$ by (25.3.7). It follows from the functional equation lemma that $f^{-1}(\varepsilon(t))$ has its coefficients in B and hence is an element of $\mathscr{C}_q(F; B)$. The formula

$$(25.3.8)\quad \gamma(t) *_F \delta(t) = f^{-1}(f(\gamma(t)) *_{\pi(F)} f(\delta(t)))$$

therefore defines a multiplication on $\mathscr{C}_q(F; B)$. The element $\sum \pi(F)^{-i}t^{q^i}$ of $R_{q,\pi(F)}(B \otimes_A K)$ also satisfies a functional equation (25.3.7) and hence

$$e_F(t) = f^{-1}\left(\sum_{i=0}^{\infty} \pi(F)^{-i}t^{q^i}\right) \in \mathscr{C}_q(F; A) \tag{25.3.9}$$

is in $\mathscr{C}_q(F; A) \subset \mathscr{C}_q(F; B)$ and is the unit element of $\mathscr{C}_q(F; B)$. Finally,

$$af(\gamma(t)) = \sum_{i=0}^{\infty} ax_i t^{q^i}$$

also satisfies a functional equation (25.3.7), so $f^{-1}(a\gamma(t))$ is in $\mathscr{C}_q(F; B)$, so

$$a\gamma(t) = f^{-1}(af(\gamma(t))) = [a]_F\gamma(t) \tag{25.3.10}$$

where $[a]_F$ is the endomorphism of $\mathscr{C}(F; B)$ induced by the endomorphism $[a]_F = \rho_F(a)$ of $F(X, Y)$, defines an A-module structure on $\mathscr{C}_q(F; B)$. It is now easy to check that (25.3.8)–(25.3.10) do indeed define an A-algebra structure on $\mathscr{C}_q(F; B)$. Note that this A-algebra structure is such that $\gamma(t) \mapsto f(\gamma(t))$ is an A-algebra homomorphism $\mathscr{C}_q(F; B) \to R_{q,\pi(F)}(B \otimes_A K)$.

To define the A-algebra structure on all A-algebras B, especially A-algebras that have A-torsion, we take the universal example of two q-typical curves in $F(X, Y)$. Consider the following two elements of $\mathscr{C}_q(F; A[C; D])$:

$$\gamma_C(t) = \varepsilon_q^F\left(\sum_{i=0}^{\infty F} C_i t^{q^i}\right), \qquad \gamma_D(t) = \varepsilon_q^F\left(\sum_{i=0}^{\infty F} D_i t^{q^i}\right)$$

We claim that they satisfy the following universality property:

(25.3.11) For any A-algebra B and any two elements $\gamma(t)$, $\delta(t) \in \mathscr{C}_q(F; B)$ there is a unique homomorphism ϕ: $A[C; D] \to B$ such that $\phi_*\gamma_C(t) = \gamma(t)$, $\phi_*\gamma_D(t) = \delta(t)$.

This is of course an immediate and trivial corollary of Lemma (25.2.13). Now let $\gamma(t)$, $\delta(t)$ be any two elements in $\mathscr{C}_q(F; B)$, B any A-algebra. Let ϕ be the unique homomorphism $A[C; D] \to B$ such that $\phi_*\gamma_C(t) = \gamma(t)$, $\phi_*\gamma_D(t) = \delta(t)$. We now define

$$\gamma(t) *_F \delta(t) = \phi_*(\gamma_C(t) *_F \gamma_D(t)) \tag{25.3.12}$$

$$a\gamma(t) = \phi_*(a\gamma_G(t)) \tag{25.3.13}$$

It follows immediately from the uniqueness of ϕ that for A-algebras B that are A-torsion free we always have

$$\gamma(t) *_F \delta(t) = f^{-1}(f(\gamma(t)) *_{\pi(F)} f(\delta(t)) \tag{25.3.14}$$

$$a\gamma(t) = f^{-1}(af(\gamma(t))) = [a]_F(\gamma(t))$$

which proves that $\mathscr{C}_q(F; B)$ is an A-algebra if B is A-torsion free (and also shows that this definition agrees with (25.3.8)). The general case follows, because by

construction, $\psi_* = \mathscr{C}_q(F; \psi)$ for $\psi: B_1 \to B_2 \in \mathbf{Alg}_A$, is a multiplication preserving, addition preserving, A-module structure preserving surjective map if $\psi: B_1 \to B_2$ is surjective. The unit element of $\mathscr{C}_q(F; B)$ is $\iota_* e_F(t)$ where $\iota: A \to B$ is the A-algebra structure homomorphism of the A-algebra B. Because $\psi_* = \mathscr{C}_q(F; \psi)$ is (by definition) A-algebra structure preserving, we have defined a functor $\mathscr{C}_q(F; -)$: $\mathbf{Alg}_A \to \mathbf{Alg}_A$ for every formal A-module over A of A-height 1.

■ (25.3.15) **Isomorphisms** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a strict isomorphism of formal A-modules over A. Then $\pi(F) = \pi(G) = \pi$ (Proposition (8.3.22) of Chapter I or Theorem (24.5.3)) and $f(X) = g(\alpha(X))$, so the commutative diagram

$$\begin{array}{ccc} \mathscr{C}_q(F; -) & & \\ \downarrow{\scriptstyle \alpha_*} & \searrow^{f} & \\ & & R_{q,\pi}(- \otimes_A K) \\ \mathscr{C}_q(G; -) & \nearrow_{g} & \end{array}$$

shows that α_* is an isomorphism of A-algebra functors.

If $\alpha(X)$ is an isomorphism but not a strict isomorphism, then also $\pi(F) = \pi(G) = \pi$ and we have a commutative diagram

$$\begin{array}{ccc} C_q(F; -) & \xrightarrow{f} & R_{q,\pi}(- \otimes_A K) \\ \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle u_*} \\ C_q(G; -) & \xrightarrow{g} & R_{q,\pi}(- \otimes_A K) \end{array}$$

where u_* is multiplication with some unit $u \neq 1$ of A; u_* is not an A-algebra homomorphism and so neither is α_*.

However, the algebra functors $\mathscr{C}_q(F; -)$ and $\mathscr{C}_q(G; -)$ are still isomorphic (in this case also because two formal A-modules of A-height 1 over A are isomorphic iff they are strictly isomorphic) essentially because there is a distinct lack of necessity of defining the A-algebra structure as we did and a concomitant plethora of isomorphisms.

Indeed, let $G(X, Y)$ be any other formal A-module over A of A-height 1 with corresponding prime element $\pi(G)$. Then if B is A-torsion free consider the following diagram

$$\begin{array}{ccc} \mathscr{C}_q(F; B) & \xrightarrow{f} & R_{q,\pi(F)}(B \otimes_A K) \\ & & \downarrow{\scriptstyle \vartheta} \\ \mathscr{C}_q(G; B) & \xrightarrow{g} & R_{q,\pi(G)}(B \otimes_A K) \end{array}$$

where ϑ takes $\sum x_i t^{q^i}$ into $\sum \pi(G)^{-i}\pi(F)^i x_i t^{q^i}$. One quickly checks (via the universal example and using functional equation arguments) that ϑ takes $f(\mathscr{C}_q(F; B))$ bijectively onto $g(\mathscr{C}_q(G; B))$ and that ϑ is an A-algebra homomorphism. It follows that ϑ induces a functor isomorphism of the functors

$\mathscr{C}_q(F; -)$, $\mathscr{C}_q(G; -)$: $\mathbf{Alg}_A \to \mathbf{Alg}_A$. (Of course this isomorphism need not be of the form α_* for any homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$.) Even more is true. Let $c = (c_0, c_1, c_2, \ldots)$ be any series of elements of K such that $c_0 \in U(A)$ and $c_i \equiv \pi(F)^{-1} c_{i-1} \mod B$ for $i \in \mathbf{N}$. Define a multiplication $*_c$ on $R_q(B \otimes_A K)$ by

$$\sum x_i t^{q^i} *_c \sum y_i t^{q^i} = \sum c_i^{-1} x_i y_i t^{q^i}$$

then

$$\gamma(t) *_{F,c} \delta(t) = f^{-1}(f(\gamma(t)) *_c f(\delta(t)))$$

defines an A-algebra structure on $\mathscr{C}_q(F; B)$ and the resulting functor is again isomorphic to $\mathscr{C}_q(F; -)$ as defined in (25.3.5). A somewhat tempting choice for the c_i might be the sequence $(a_{q^0}, a_{q^1}, a_{q^2}, \ldots)$ of coefficients of $X, X^q, X^{q^2}, \ldots$ in the logarithm $f(X)$ of $F(X, Y)$. This choice leads to difficulties later when dealing with Frobenius operators; but on the other hand appears to have certain advantages in the global case; cf. Section 25.11 for some more details.

■ (25.3.16) **A special case** Choose a uniformizing element π of A. Then there is one particular formal A-module $G_\pi(X, Y)$ with $\pi(G_\pi) = \pi$ that gives especially pleasing formulas. It is the formal group law $G_\pi(X, Y)$ with logarithm

$$g_\pi(X) = X + \pi^{-1} X^q + \pi^{-2} X^{q^2} + \cdots = X + \pi^{-1} g_\pi(X^q)$$

In this case the unit element $e_{G_\pi}(t)$ of $\mathscr{C}_q(G_\pi; B)$ is the curve $\gamma_0(t) = t$, the curves $(\sum^{G_\pi})_{i=0}^{\infty} b_i t^{q^i}$ are automatically in $\mathscr{C}_q(G_\pi; B)$ (without applying ε_q) and the Witt polynomials associated to $G_\pi(X, Y)$ are

(25.3.17) $$w_{q.n}^{G_\pi}(Z) = \pi^n Z_n + \pi^{n-1} Z_{n-1}^q + \cdots + \pi Z_1^{q^{n-1}} + Z_0^{q^n} = w_{q.n}^A(Z)$$

We shall from now on write $w_{q.n}^A(Z)$ for these polynomials; the dependence on π being understood.

■ (25.3.18) **The A-algebra functor $W_{q.\infty}^F(-)$ associated to the formal A-module $F(X, Y)$** We have seen that the functor $\mathscr{C}_q(F; -)$ is representable by $A[X_0, X_1, X_2, \ldots] = A[X]$ the isomorphism of functors being

(25.3.19) $$\mathbf{Alg}_A(A[Z], B) \xrightarrow{\sim} \mathscr{C}_q(F; B), \qquad \phi \mapsto \varepsilon_q^F\left(\sum_{i=0}^{\infty} \phi(Z_i) t^{q^i}\right)$$

Now $\mathscr{C}_q(F; -)$ has a functorial addition and multiplication and these induce a coaddition and comultiplication on $A[Z]$.

$$c_\Sigma^F: A[Z] \to A[Z] \otimes_A A[Z], \qquad c_\Pi^F: A[Z] \to A[Z] \otimes_A A[Z]$$

Let $\Sigma_i^F(S; T)$ (resp. $\Pi_i^F(S; T)$) be the polynomials in $S_0, S_1, \ldots; T_0, T_1, \ldots$ such that

$$\Sigma_i^F(Z_0 \otimes 1, Z_1 \otimes 1, \ldots; 1 \otimes Z_0, 1 \otimes Z_1, \ldots) = c_\Sigma^F(Z_i)$$

(resp. $\Pi_i^F(Z_0 \otimes 1,\ Z_1 \otimes 1, \ldots;\ 1 \otimes Z_0,\ 1 \otimes Z_1, \ldots) = c_\Pi^F(Z_i)$). According to (25.3.19) these polynomials must satisfy

$$\varepsilon_q^F\left(\sum_{i=0}^{\infty F} \Sigma_i^F(S;\ T)t^{q^i}\right) = \varepsilon_q^F\left(\sum_{i=0}^{\infty F} S_i t^{q^i}\right) +_F \varepsilon_q^F\left(\sum_{i=0}^{\infty F} T_i t^{q^i}\right) \tag{25.3.20}$$

$$\varepsilon_q^F\left(\sum_{i=0}^{\infty F} \Pi_i^F(S;\ T)t^{q^i}\right) = \varepsilon_q^F\left(\sum_{i=0}^{\infty F} S_i t^{q^i}\right) *_F \varepsilon_q^F\left(\sum_{i=0}^{\infty F} T_i t^{q^i}\right)$$

Now, by the definition of ε_q^F we have $f(\varepsilon_q^F(\sum c_i t^i)) = \sum_{i=0}^{\infty} x_{q^i} t^{q^i}$ if $f(\sum c_i t^i) = \sum x_i t^i$ for $\sum x_i t^i \in \mathscr{C}(F;\ B)$, if B is A-torsion free. Hence (25.3.20) gives us

(25.3.21)

$$w_{q,n}^F(\Sigma_0^F, \Sigma_1^F, \ldots, \Sigma_n^F) = w_{q,n}^F(S_0, S_1, \ldots, S_n) + w_{q,n}^F(T_0, T_1, \ldots, T_n)$$

$$w_{q,n}^F(\Pi_0^F, \Pi_1^F, \ldots, \Pi_n^F) = w_{q,n}^F(S_0, S_1, \ldots, S_n) w_{q,n}^F(T_0, T_1, \ldots, T_n)$$

Of course the polynomials Σ_i^F and Π_i^F are uniquely determined by these conditions, and from the way in which they were obtained we know that the coefficients of the Σ_i^F and Π_i^F are in A; a fact that does not immediately follow from (25.3.21).

The polynomials Σ_i^F and Π_i^F describe the ring structure of $\mathscr{C}_q(F;\ -)$. What about the A-module structure? The ring homomorphism $A \to \mathscr{C}_q(F;\ A)$ satisfies, according to (25.3.14),

$$a \mapsto [a]_F(e_F(t)) = f^{-1}\left(\sum_{i=0}^{\infty} a\pi(F)^{-i} t^{q^i}\right) \tag{25.3.22}$$

Write

$$f^{-1}\left(\sum_{i=0}^{\infty} a\pi(F)^{-i} t^{q^i}\right) = \varepsilon_q^F\left(\sum_{i=0}^{\infty} \Omega_i^F(a) t^{q^i}\right), \qquad \Omega_i^F(a) \in A \tag{25.3.23}$$

By applying f to this equality we obtain that

$$w_{q,i}^F(\Omega_0^F(a), \Omega_1^F(a), \ldots) = a \tag{25.3.24}$$

which of course determines the elements $\Omega_i^F(a)$ of A uniquely.

In case $F(X,\ Y) = G_\pi(X,\ Y)$ we shall write Σ_i^A, Π_i^A, and $\Omega_i^A(a)$ instead of $\Sigma_i^{G_\pi}$, $\Pi_i^{G_\pi}$, $\Omega_i^{G_\pi}(a)$ where again the dependence on π is understood. We note that the Σ_i^F, Π_i^F are polynomials with coefficients in A, but that the elements $\Omega_i^F(a)$ are given by polynomials Ω_i^F with coefficients in K which happen to be such that $\Omega_i^F(a) \in A$ for all $a \in A$. For example, the first three $\Omega_i^A(a)$ are

$$\Omega_0^A(a) = a, \qquad \Omega_1^A(a) = \pi^{-1}(a - a^q)$$

$$\Omega_2^A(a) = \pi^{-2}(a^q - a^{q^2}) - \pi^{-1}\{\pi^{-q}(a - a^q)^q - \pi^{-1}(a - a^q)\}$$

All this ((25.3.19)–(25.3.24)) amounts to the following alternative description of $\mathscr{C}_q(F; -)$.

■ (25.3.25) **Theorem** For every formal A-module of A-height 1 over A, there exists a unique functor $W^F_{q,\infty}$: $\mathbf{Alg}_A \to \mathbf{Alg}_A$ with the following properties:

(i) As set-valued functors $W^F_{q,\infty}(B) = \{(b_0, b_1, b_2, \ldots) b_i \in B\}$ and $W^F_{q,\infty}(\phi)(b_0, b_1, b_2, \ldots) = (\phi(b_0), \phi(b_1), \phi(b_2), \ldots)$ for $\phi: B \to C$ in $\mathbf{Alg}_A$.

(ii) The polynomials $w^F_{q,i}(Z)$ of (25.3.3) induce functorial A-algebra homomorphisms $W^F_{q,\infty}(B) \to B$, $b = (b_0, b_1, b_2, \ldots) \mapsto w^F_{q,i}(b)$ for all $i \in \mathbf{N} \cup \{0\}$.

Addition and multiplication in the $W^F_{q,\infty}(B)$ are given by the universal polynomials Σ^F_i and Π^F_i and the A-algebra structure is given by the universal sequences $(\Omega_0(a), \Omega_1(a), \ldots)$ of elements of A.

The functors $W^F_{q,\infty}(-)$, $\mathscr{C}_q(F; -)$: $\mathbf{Alg}_A \to \mathbf{Alg}_A$ are isomorphic under the functor transformation η: $(b_0, b_1, b_2, \ldots) \to \varepsilon^F_q(\Sigma^F b_i t^{q^i})$, and we have a commutative (functorial) diagram

$$\begin{array}{ccc} W^F_{q,\infty}(B) & \xrightarrow{\eta} & \mathscr{C}_q(F; B) \\ & {\scriptstyle w^F_{q,\infty}} \searrow \quad \swarrow {\scriptstyle s^F_{q,i}} & \\ & B & \end{array}$$

where $s^F_{q,i}$ is the A-algebra functor homomorphism $s^F_{q,i}(\gamma(t)) = \pi(F)^i$ times the coefficient of t^{q^i} in $f(\gamma(t))$.

■ (25.3.26) **Remarks**

(i) We shall write $W^A_{q,\infty}(-)$ for $W^{G_\pi}_{q,\infty}(-)$.

(ii) If $F(X, Y) = G_\pi(X, Y)$, then the unit element of $\mathscr{C}_q(F; B)$ is the curve t, and it follows that the unit element of $W^A_{q,\infty}(B)$ is the vector $(1, 0, 0, 0, \ldots)$.

(iii) If $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is a strict isomorphism over A of formal A-modules of A-height 1, then $\alpha(X)$ induces an isomorphism of functors $W^\alpha_{q,\infty}$: $W^F_{q,\infty}(-) \to W^G_{q,\infty}(-)$ such that $w^G_{q,i} W^\alpha_{q,\infty} = w^F_{q,i}$ for all $i \in \mathbf{N} \cup \{0\}$. More generally, if $F(X, Y)$ and $G(X, Y)$ are any two formal A-modules over A of A-height 1, then the isomorphism ϑ of (25.3.15) gives us via η^F and η^G (cf. Theorem (25.3.25)) an isomorphism $W^F_{q,\infty}(-) \to W^G_{q,\infty}(-)$ which changes $w^F_{q,i}$ into $w^G_{q,i}$ for all i.

■ (25.3.27) Remark (25.3.26)(iii) above tells us that the functors $W^F_{q,\infty}$ together with the functor transformations $w^F_{q,i}$ do not yet possess sufficient structure to distinguish between nonisomorphic formal A-modules of A-height 1 over A. The introduction of Frobenius operators in 25.5 will remedy this. But first we want to prove the theorem that justifies to some extent the appellation "ramified Witt vectors" for $W^F_{q,\infty}(-)$ or $\mathscr{C}_q(F; -)$.

■ (25.3.28) **A construction** Let A_n be the ring of integers of the unramified extension K_n of degree n of K and let k_n be the residue field of K_n. We use σ to

denote the Frobenius substitution in $\mathrm{Gal}(K_n/K)$, i.e., $\sigma(x) \equiv x^q \bmod \mathfrak{m}(A_n)$ for all $x \in A_n$. Let $F(X, Y)$ be a formal A-module of A-height 1 over A. For each $y \in A_n$, consider the power series

$$\sum_{i=0}^{\infty} \pi(F)^{-i}\sigma^i(y)t^{q^i}$$

This satisfies a functional equation

$$\pi(F)^{-i}\sigma^i(y) - \pi(F)^{-1}\sigma(\pi(F)^{-i+1}\sigma^{i-1}(y)) \in A_n$$

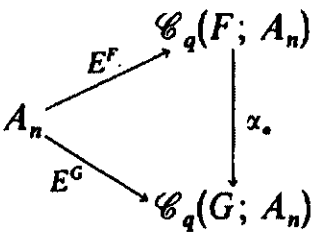
so that by the functional equation lemma

$$E^F(y) = f^{-1}\left(\sum_{i=0}^{\infty} \pi(F)^{-i}\sigma^i(y)t^{q^i}\right) \in \mathscr{C}_q(F; A_n)$$

It is trivial to check that $E^F\colon A_n \to \mathscr{C}_q(F; A_n)$ is in fact an homomorphism of A-algebras (use the characterization (25.3.14)).

Also if $\alpha(X)\colon F(X, Y) \to G(X, Y)$ is a strict isomorphism over A, then we have a commutative diagram

(25.3.29)



(More generally, if $F(X, Y)$ and $G(X, Y)$ are any two A-height 1 formal A-modules over A, then the isomorphism ϑ of (25.3.15) takes E^F into E^G.)

■ (25.3.30) **Theorem** Let $F(X, Y)$ be a formal A-module of A-height 1 over A. Then the composed map $A_n \to \mathscr{C}_q(F; A_n) \to \mathscr{C}_q(F; k_n)$ is an isomorphism of A-algebras.

In particular, $W^F_{q,\infty}(k_n) \simeq A_n$ generalizing a well-known property of the usual Witt vectors $W_{p^\infty}(-)$.

Proof Let $\pi = \pi(F)$. The map $E^F\colon A_n \to \mathscr{C}_q(F; A_n)$ is an A-algebra homomorphism, and multiplication with $a \in A$ in $\mathscr{C}_q(F; A_n)$ is the same thing as applying the endomorphism of $\mathscr{C}_q(F; A_n)$ induced by $[a]_F(X)\colon F(X, Y) \to F(X, Y)$. It follows that for all $a \in A$ and $y \in A_n$,

$$E^F(ay) = [a]_F(E^F(y)) \tag{25.3.31}$$

Now because $F(X, Y)$ is of A-height 1, we have that $[\pi]_F(t) \equiv t^q \bmod(\pi, \text{degree } q+1)$, so that

$$[\pi^i]_F(t) \equiv t^{q^i} \bmod(\pi, \text{degree } q^i + 1) \tag{25.3.32}$$

Now let $y \in A_n$ and write $y = \pi^m u$, with u a unit of A_n. Then (25.3.31) and (25.3.32) together give us

$$E^F(y) \equiv u^{q^m}t^{q^m} \bmod(\pi, \text{degree } q^m + 1) \tag{25.3.33}$$

which proves that $E^F(y) \not\equiv 0 \bmod \pi$, so the composed homomorphism $A_n \to \mathscr{C}_q(F; A_n) \to \mathscr{C}_q(F; k_n)$ is injective.

Let $\mathscr{C}_q^{(m)}(F; B)$ be the subgroup of all elements of $\mathscr{C}_q(F; B)$ of the form $\varepsilon_q^F(\sum_{i=m}^{\infty} b_i t^{q^i})$, $b_i \in B$. These subgroups are functorial and define a complete Hausdorff topology on the $\mathscr{C}_q(F; B)$. This is easily checked. Now we have just proved that

$$\rho E^F(\pi^m A_n) \subset \mathscr{C}_q^{(m)}(F; k_n)$$

where ρ is the reduction map $\mathscr{C}_q(F; A_n) \to \mathscr{C}_q(F; k_n)$, and we have shown that the induced maps

$$\pi^m A_n \to \mathscr{C}_q^{(m)}(F; k_n)/\mathscr{C}_q^{(m+1)}(F; k_n) \simeq k_n$$

are surjective (cf. (25.3.33)). Since A is complete in the topology defined by the $\pi^m A_n$ and $\mathscr{C}_q(F; k_n)$ is Hausdorff, we have that E^F is surjective.

Alternatively, one can prove the surjectivity of E^F as follows. First, because diagram (25.3.29) is commutative, it suffices to prove the theorem for $F(X, Y) = G_\pi(X, Y)$. Let

$$\gamma(t) = \sum_{i=0}^{\infty}{}^{G_\pi} x_i t^{q^i}$$

be any element of $\mathscr{C}_q(G_\pi; k_n)$. (Because $G_\pi(X, Y)$ is A-typical, all elements of $\mathscr{C}_q(G_\pi; k_n)$ are of this form.) Choose elements $y_i \in A_n$ that reduce to $x_i \in k_n$ modulo π. Now define elements z_i by the equations

$$\begin{aligned}
z_0 &= y_0 \\
z_1 &= \sigma^{-1} y_1 + \pi^{-1}(\sigma^{-1}(y_0^q) - y_0) \\
z_2 &= \sigma^{-2} y_2 + \pi^{-1}\sigma^{-1}(\sigma^{-1}(y_1^q) - y_1) \\
&\quad + \pi^{-2}(\sigma^{-2}(y_0^{q^2}) - \sigma^{-1}(y_0^q)) \qquad (25.3.34) \\
z_3 &= \sigma^{-3} y_2 + \pi^{-1}\sigma^{-2}(\sigma^{-1}(y_2^q) - y_2) + \pi^{-2}\sigma^{-1}(\sigma^{-2}(y_1^{q^2}) \\
&\quad - \sigma^{-1}(y_1^q)) + \pi^{-3}(\sigma^{-3}(y_0^{q^3}) - \sigma^{-2}(y_0^{q^2}) \\
&\ \ \vdots
\end{aligned}$$

(Note that the z_i are in A_n because $\sigma^{-i}(y_j^{q^i}) - \sigma^{-i+1}(y_j^{q^{i-1}}) \equiv 0 \bmod \pi^i$.) Then we have for all $i \in \mathbf{N} \cup \{0\}$

$$\sigma^i(z_i + \pi^{-1} z_{i-1} + \cdots + \pi^{-i} z_0) = \pi^{-i} y_0^{q^i} + \pi^{-i+1} y_1^{q^{i-1}} + \cdots + y_i$$

and

$$\begin{aligned}
g_\pi\left(E^{G_\pi}\left(\sum_{i=0}^{\infty} z_i \pi^i\right)\right) &= z_0 t + \pi^{-1}\sigma(z_0)t^q + \pi^{-2}\sigma^2(z_0)t^{q^2} + \cdots \\
&\quad + \pi z_1 t + \sigma(z_1)t^q + \pi^{-1}\sigma^2(z_1)t^{q^2} + \cdots \\
&\quad + \pi^2 z_2 t + \pi\sigma(z_2)t^q + \sigma^2(z_2)t^{q^2} + \cdots \\
&\quad + \cdots
\end{aligned}$$

On the other hand

$$g_\pi\left(\sum_{i=0}^{\infty}{}^{G_\pi}y_i t^{q^i}\right) = y_0 t + (\pi^{-1}y_0^q + y_1)t^q + (\pi^{-2}y_0^{q^2} + \pi^{-1}y_1^q + y_2)t^{q^2} + \cdots$$

so we have

$$g_\pi\left(E^F\left(\sum_{i=0}^{\infty} z_i\pi^i\right)\right) \equiv g_\pi\left(\sum_{i=0}^{\infty}{}^{G_\pi}y_i t^{q^i}\right) \mod(\pi)$$

which by part (iv) of the functional equation lemma implies that

$$E^F\left(\sum_{i=0}^{\infty} z_i\pi^i\right) \equiv \sum_{i=0}^{\infty}{}^{G_\pi}y_i t^{q^i} \mod(\pi)$$

proving the surjectivity of $A_n \to \mathscr{C}_q(G_\pi; A_n) \to \mathscr{C}_q(G_\pi; k_n)$.

■ (25.3.35) **Remarks**

(i) We have encountered formulas like (25.3.34) before; cf., e.g., (21.1.10).

(ii) Identifying $\mathscr{C}_q(F; k_n)$ and A_n, we see that E^F gives us an algebra homomorphism $\mathscr{C}_q(F; k_n) \to \mathscr{C}_q(F; \mathscr{C}_q(F; k_n))$; or in terms of the Witt functors $W^F_{q,\infty}$ we have A-algebra homomorphisms (Artin–Hasse exponentials) $W^F_{q,\infty}(k_n) \to W^F_{q,\infty}(W^F_{q,\infty}(k_n))$ which are clearly reminiscent of the ring homomorphisms $W_{p^\infty}(-) \to W_{p^\infty}(W_{p^\infty}(-))$ which we discussed at length in Chapter III, 17.5 and 17.6.

(iii) We can therefore recover A_n from $\mathscr{C}_q(F; k_n)$, an object which is at first sight completely determined by the reduction of $F(X, Y)$ mod π. This is not quite true because the definition of the multiplication on $\mathscr{C}_q(F; k_n)$ uses $\pi(F) = \pi$! Still it seems worthwhile to figure out which formal group laws over k_n are reductions of formal A-modules over A of A-height 1 where A is a characteristic zero complete discrete valuation ring with residue field k. First suppose that $F(X, Y)$ over k is the reduction of an $\tilde{F}(X, Y)$ over A that is a formal A-module of A-height 1. Let $\pi = \pi(\tilde{F})$ and let $R \subset A$ be the ring of integers of the maximal unramified subextension of $K = A \otimes_{\mathbf{Z}} \mathbf{Q}$. Now the logarithm $\tilde{f}(X)$ of $\tilde{F}(X, Y)$ satisfies $\tilde{f}(X) - \pi^{-1}\tilde{f}(X^q) \in A[\![X]\!]$ and it follows that $[\pi]_{\tilde{F}}(X) \equiv X^q \bmod \pi$. Let

$$\pi^e + b_1\pi^{e-1} + \cdots + b_{e-1}\pi + b_e = 0$$

be the irreducible equation of π over $R \otimes \mathbf{Q}$. Since $\tilde{F}(X, Y)$ is a formal A-module, we deduce a relation

$$[\pi]^e_{\tilde{F}} + [b_1]_{\tilde{F}}[\pi]^{e-1}_{\tilde{F}} + \cdots + [b_{e-1}]_{\tilde{F}}[\pi]_{\tilde{F}} + [b_e]_{\tilde{F}} = 0$$

Now reduction mod π gives us (because $\tilde{F}(X, Y)$ has finite height!) an embedding $A \otimes \mathbf{Q} \to \mathrm{End}_k(F(X, Y))$, and using this we see that the characteristic polynomial $\Psi_F(x)$ of $F(X, Y)$ is

$$\Psi_F(x) = x^e + \lambda(b_1)x^{e-1} + \cdots + \lambda(b_{e-1})x + \lambda(b_e)$$

where λ: $R \to W_{p^\infty}(k)$ is the canonical identification which reduces to the identity mod p. So the characteristic polynomial of a formal group law $F(X, Y)$ that can be lifted to a formal A-module over A of A-height 1 is necessarily an Eisenstein polynomial.

Conversely suppose that $\Psi_F(x)$ is Eisenstein. Let π be any root of $\Psi_F(x)$ considered as a polynomial over $W_{p^\infty}(k)$. Let $\tilde{G}(X, Y)$ be the formal group law over $A = W_{p^\infty}(k)[\pi]$ with logarithm $\tilde{g}(X) = X + \pi^{-1}\tilde{g}(X^q)$. Then $\tilde{G}(X, Y)$ is a formal A-module over A of A-height 1 and by the argument above if $G(X, Y)$ is the reduction of $\tilde{G}(X, Y)$, then $\Psi_G(x) = \Psi_F(x)$. It follows that $G(X, Y)$ and $F(X, Y)$ are isomorphic. Taking any lift of the isomorphism, we find a lift $\tilde{F}(X, Y)$ over A of $F(X, Y)$ which being isomorphic to $\tilde{G}(X, Y)$ is also a formal A-module of A-height 1.

(iv) A corollary of the above is that every formal group law $F(X, Y)$ over $\mathbf{F}_p$ is the reduction of some Lubin–Tate formal group law; cf. Theorem (24.2.16).

25.4 Higher dimensional universal formal A-modules

■ (25.4.1) Let A be a discrete valuation ring with finite residue field k. (Both characteristic zero and characteristic $p > 0$ for A are allowed.) In the next section we shall construct Frobenius operators and Verschiebung operators which are peculiar to formal A-modules. These constructions go—as so often before—via the universal example. In order to be able to discuss also Frobenius and Verschiebung on higher dimensional formal A-modules we take time out to discuss higher dimensional universal formal A-modules in this section. Let us remark in passing that the case "k is infinite" is of little interest. A mixture of the arguments below and the ones used in (21.4.20) shows that in that case also every higher dimensional formal A-module is strictly isomorphic to an additive one.

■ (25.4.2) **Some notation** Choose $m \in \mathbf{N}$. Let π be a uniformizing element of A and let q be the number of elements of k. For each $n \in \mathbf{N}$ let V_n be a matrix of indeterminates $V_n(i, j)$, $i, j \in \{1, 2, \ldots, m\}$. For each multi-index $\mathbf{n} = (n_1, \ldots, n_m)$ of length m with $n_i \in \mathbf{N} \cup \{0\}$ such that $|\mathbf{n}| \geq 2$ and such that $\mathbf{n} \neq i\mathbf{e}(j)$ for all $i \in \mathbf{N}, j \in \{1, \ldots, m\}$, let $S_{\mathbf{n}}$ be a column vector $S_{\mathbf{n}} = (S(\mathbf{n}, 1), \ldots, S(\mathbf{n}, m))$ of indeterminates; for each $n \in \mathbf{N}\backslash\{1\}$, let S_n be the matrix of indeterminates $S_n(i, j)$, $i, j \in \{1, 2, \ldots, n\}$. We write $A[V]$ and $A[S]$ for the rings of polynomials over A in the Vs and Ss. Identifying V_n with S_{q^n} gives us a natural embedding $A[V] \to A[S]$ and there is also a natural projection $A[S] \to A[V]$, viz. $S_{q^n}(i, j) \mapsto V_n(i, j)$, all other Ss $\mapsto 0$. Let K be the quotient field of A and let σ: $K[V] \to K[V]$ and σ: $K[S] \to K[S]$ be the K-algebra endomorphism that raises each indeterminate to its qth power. Then $\sigma(b) \equiv b^q \bmod \pi$ for all $b \in A[V]$ or $A[S]$.

■ (25.4.3) **Construction of some m-dimensional formal A-modules** Now let $f_V^A(X)$ be the m-tuple of power series in $X = (X_1, X_2, \ldots, X_m)$ defined by the equation

$$f_V^A(X) = X + \sum_{i=1}^{\infty} \pi^{-1} V_i(\sigma_*^i f_V^A(X^{q^i})) \tag{25.4.4}$$

and let $F_V^A(X, Y)$ and $\rho_V^A(a)(X)$ for all $a \in A$ be respectively equal to

$$F_V^A(X, Y) = (f_V^A)^{-1}(f_V^A(X) + f_V^A(Y)) \tag{25.4.5}$$

$$\rho_V^A(a)(X) = (f_V^A)^{-1}(a f_V^A(X)) \tag{25.4.6}$$

Further, let $\beta(X)$ be the m-tuple of power series

$$\beta(X) = X + \sum_{\substack{\mathbf{n} \neq |\mathbf{n}|\mathbf{e}(i) \\ |\mathbf{n}| \geq 2}} S_{\mathbf{n}} X^{\mathbf{n}} \tag{25.4.7}$$

where the sum is over all multi-indices $\mathbf{n}$ such that $|\mathbf{n}| \geq 2$ and such that $\mathbf{n} \neq l\mathbf{e}(i)$ for all $l \in \mathbf{N}$ and $i \in \{1, \ldots, m\}$, and where $X^{\mathbf{n}}$, as usual, is equal to $X_1^{n_1} X_2^{n_2} \cdots X_m^{n_m}$.

Let $\hat{f}_S^A(X)$ be the m-tuple of power series defined by

$$\hat{f}_S^A(X) = X + \sum_{n \neq q^r} S_n X^n + \sum_{i=1}^{\infty} \pi^{-1} S_{q^i}(\sigma_*^i \hat{f}_S^A(X^{q^i})) \tag{25.4.8}$$

and we define further

$$f_S^A(X) = \hat{f}_S^A(\beta(X)), \qquad F_S^A(X, Y) = (f_S^A)^{-1}(f_S^A(X) + f_S^A(Y)) \tag{25.4.9}$$

$$\rho_S^A(a)(X) = (f_S^A)^{-1}(a f_S^A(X)) \quad \text{for all} \quad a \in A \tag{25.4.10}$$

■ (25.4.11) **Proposition** The power series $F_V^A(X, Y)$, $\rho_V^A(a)(X)$, $F_S^A(X, Y)$, $\rho_S^A(a)(X)$ all have integral coefficients (i.e., in $A[V]$ or $A[S]$ as the case might be). So that $(F_V^A(X, Y), \rho_V^A)$ is a formal A-module over $A[V]$ and $(F_S^A(X, Y), \rho_S^A)$ is a formal A-module over $A[S]$. Moreover, $(F_V^A(X, Y), \rho_V^A)$ and $(F_S^A(X, Y), \rho_S^A)$ are strictly isomorphic over $A[S] \supset A[V]$.

Proof Straightforward applications of the functional equation lemma.

■ (25.4.12) For each $r \in \mathbf{N}\backslash\{1\}$, let $\Gamma_r(X)$ be the homogeneous part of degree r of $\beta(X)$, and recall that $B_n(X, Y) = X^n + Y^n - (X + Y)^n$. With these notations we have the following congruences:

(25.4.13)

$$F_V^A(X, Y) \equiv X + Y + \pi^{-1} V_n B_n(X, Y) \mod(V_1, \ldots, V_{n-1}, \text{degree } q^n + 1)$$

$$\rho_V^A(a)(X) \equiv aX + \pi^{-1} V_n(a - a^{q^n}) X^{q^n} \mod(V_1, \ldots, V_{n-1}, \text{degree } q^n + 1)$$

If n is not a power of q, we have mod$(S_2, \ldots, S_{n-1}, S_n$ with $|\mathbf{n}| < n$, degree $n+1)$,

$$(25.4.14)\quad F_S^A(X, Y) \equiv X + Y + S_n B_n(X, Y) + \Gamma_n(X) + \Gamma_n(Y) - \Gamma_n(X+Y)$$
$$\rho_S^A(a)(X) \equiv aX + (a - a^n)\Gamma_n(X) + (a - a^n)S_n X^n$$

and if $n = q^r$, $r \in \mathbf{N}$, we have mod$(S_2, \ldots, S_{q^r-1}, S_n$ with $|\mathbf{n}| < q^r$, degree $q^r + 1)$

(25.4.15)

$$F_S^A(X, Y) \equiv X + Y + \pi^{-1} S_{q^r} B_{q^r}(X, Y) + \Gamma_{q^r}(X) + \Gamma_{q^r}(Y) - \Gamma_{q^r}(X+Y)$$
$$\rho_S^A(a)(X) \equiv aX + (a - a^{q^r})\Gamma_{q^r}(X) + (a - a^{q^r})\pi^{-1} S_{q^r} X^{q^r}$$

■ (25.4.16) **Theorem** $F_S^A(X, Y)$ over $A[S]$ is a universal m-dimensional formal A-module.

Proof Let $A[S]_n$ be the sub-A-algebra of $A[S]$ generated by the $S_l(i, j)$ with $l < n$ and the $S(\mathbf{n}, i)$ with $|\mathbf{n}| < n$. Let B be any A-algebra and let $(G(X, Y), \rho_G)$ be a formal A-module over B. Suppose we have shown that there is a homomorphism ϕ_n: $A[S]_n \to B$ such that

$$(25.4.17)\quad \phi_n(F_S^A(X, Y), \rho_S^A) \equiv (G(X, Y), \rho_G) \quad \text{mod(degree } n)$$

and that ϕ_n is uniquely determined on $A[S]_n$ by this condition. This holds obviously for $n = 2$ so that the induction starts.

Now according to the higher dimensional comparison lemma (11.4.12) of Chapter II, (25.4.17) implies that there are unique m-tuples of homogeneous forms $\Gamma(a; X)$, $\Gamma(X)$ not involving $X_1^n, X_2^n, \ldots, X_m^n$ and unique $m \times m$ matrices M, M_a such that modulo(degree $n+1$)

$$(25.4.18)\quad (\phi_n)_* F_S^A(X, Y) \equiv G(X, Y) + \Gamma(X) + \Gamma(Y) - \Gamma(X+Y) + M(v(n)^{-1} B_n(X, Y))$$

$$(25.4.19)\quad (\phi_n)_* \rho_S^A(a)(X) \equiv \rho_G(a)(X) + \Gamma(a, X) + M_a X^n$$

Let $A[S]_{n+}$ be the subring generated by $A[S]_n$ and the $S(\mathbf{n}, i)$ with $|\mathbf{n}| = n$ (and $\mathbf{n} \neq |\mathbf{n}|\mathbf{e}(i)$ for all $i \in \{1, \ldots, m\}$). Then there clearly is a homomorphism ϕ_{n+}: $A[S] \to B$ such that ϕ_{n+} coincides with ϕ_n on $A[S]_n$ and such that $(\phi_{n+})_* \Gamma_n(X) = \Gamma(X)$ and moreover ϕ_{n+} is unique on $A[S]_{n+}$. According to (25.4.18) and (25.4.15) we then have modulo degree $n+1$

$$(25.4.20)\quad (\phi_{n+})_* F_S^A(X, Y) \equiv G(X, Y) + M(v(n)^{-1} B_n(X, Y))$$
$$(\phi_{n+})_* \rho_S^A(a)(X) \equiv \rho_G(a)(X) + \hat{\Gamma}(a, X) + M_a X^n$$

for certain m-tuples of homogeneous polynomials $\hat{\Gamma}(a, X)$ not involving $X_1^n, \ldots, X_m^n$.

As in (21.2.4) one now calculates $(\phi_{n+})_*\rho_S^A(a)((\phi_{n+})_*F_S^A(X, Y))$ in two ways modulo degree $n+1$. The result is

$$aM(v(n)^{-1}B_n(X, Y)) + \hat{\Gamma}(a, X+Y) + M_a(X+Y)^n = M(v(n)^{-1}B_n(aX, aY)) + \hat{\Gamma}(a, X) + \hat{\Gamma}(a, Y) + M_aX^n + M_aY^n \tag{25.4.21}$$

and because $\hat{\Gamma}(a, X)$ does not involve $X_1^n, X_2^n, \ldots, X_m^n$, we must have $\hat{\Gamma}(a, X) = 0$ for all a. Using this and using that $v(n)^{-1}B_n(X, Y)$ is an m-tuple of primitive polynomials, and collecting terms we find from (25.4.21)

$$(a - a^n)M = v(n)M_a \tag{25.4.22}$$

And by considering $(\phi_{n+})\rho_S^A(a+b)$ and $(\phi_{n+})\rho_S^A(ab)$ we obtain as in (21.2.4) that moreover

$$M_{a+b} - M_a - M_b = (v(n)^{-1}B_n(a, b))M \quad \text{for all} \quad a, b \in A \tag{25.4.23}$$

$$aM_b + b^nM_a = M_{ab} \quad \text{for all} \quad a, b \in A \tag{25.4.24}$$

Now if n is not a power of p = characteristic(k), then $v(n)$ is a unit in A and there is a homomorphism $\phi_{n+1}: A[S] \to B$ that agrees with ϕ_{n+} on $A[S]_{n+}$ and which is such that $\phi_{n+1}(S_n)B_n(X, Y) = M(v(n)^{-1}B_n(X, Y))$. Moreover, ϕ_{n+1} is uniquely determined on $A[S]_{n+1}$ by these requirements. Since $v(n)$ is a unit, relation (25.4.22) then sees to it that also $(\phi_{n+1})_*(a - a^n)S_nX^n = (a - a^n)Mv(n)^{-1} = M_a$, so by (25.4.14) and (25.4.20) (recall that $\hat{\Gamma}(a, X) = 0$ for all a) ϕ_{n+1} satisfies (25.4.17) with n replaced by $n+1$ and is uniquely determined on $A[S]_{n+1}$ by this condition.

Now let $n = p^r$ but n is not a power of q, the number of elements of k. Then there is an $x \in k$ such that $x - x^n \neq 0$, so there is an $a_0 \in A$ such that $a_0 - a_0^n$ is a unit of A. Then there is a homomorphism $\phi_{n+1}: A[S] \to B$ that agrees with ϕ_{n+} on $A[S]_{n+}$ and such that $(\phi_{n+1})_*(a_0 - a_0^n)S_n = M_{a_0}$; moreover, ϕ_{n+1} is uniquely determined on $A[S]_{n+1}$ by these requirements. Now (25.4.24) implies that

$$(a_0 - a_0^n)M_b = (b - b^n)M_{a_0}$$

so that, $a_0 - a_0^n$ being a unit we also have $(\phi_{n+1})_*(b - b^n)S_n = M_b$ for all $b \in A$ and again because $a_0 - a_0^n$ is a unit we have

$$(\phi_{n+1})_*(v(n)S_n(v(n)^{-1}B_n(X, Y)) = (a_0 - a_0^n)^{-1}v(n)M_{a_0}(v(n)^{-1}B_n(X, Y)) = M(v(n)^{-1}B_n(X, Y))$$

by (25.4.22). So that by (25.4.14) and (25.4.20), using again that $\hat{\Gamma}(a, X) = 0$ for all a, we have that ϕ_{n+1} satisfies (25.4.17) with n replaced by $n+1$ and is uniquely determined on $A[S]_{n+1}$ by this condition.

Finally, let n be a power of q. In this case there is a homomorphism ϕ_{n+1}: $A[S] \to B$ that agrees with ϕ_{n+} on $A[S]_{n+}$ and such that

$$(\phi_{n+1})_*(1 - \pi^{n-1})S_nX^n = M_\pi X^n \tag{25.4.25}$$

and ϕ_{n+1} is uniquely determined by this condition. Note also that (25.4.25) must hold if (25.4.17) is to hold with n replaced by $n+1$ (because of (25.4.15) and (25.4.20)).

Now consider the A-module generated by symbols $\hat{M}_a(i,j)$, $\hat{M}(i,j)$, $a \in A$, $i,j \in 1,\ldots,m$, subject to the relations $(a-a^n)\hat{M} = \nu(n)\hat{M}_a$, $\hat{M}_{a+b} - \hat{M}_a - \hat{M}_b = (\nu(n)^{-1}B_n(a,b))\hat{M}$, $a\hat{M}_b + b^n\hat{M}_a = \hat{M}_{ab}$. Exactly as in the proof of Proposition (21.3.1) one shows that this module is free on the generators $\hat{M}_\pi(i,j)$. It follows that all the $\hat{M}_a(i,j)$ and $\hat{M}(i,j)$ can uniquely be written as linear combinations of the $\hat{M}_\pi(i,j)$. These expressions then turn out to be

$$\hat{M}_a(i,j) = t_a\hat{M}_\pi(i,j), \qquad \hat{M}(i,j) = t\hat{M}_\pi(i,j)$$

with

$$t_a = \pi^{-1}(a-a^n)(1-\pi^{n-1})^{-1}, \qquad t = \pi^{-1}\nu(n)(1-\pi^{n-1})^{-1}$$

simply because if one takes an arbitrary matrix $\hat{M}_\pi$ and one takes $\hat{M}_a = t_a\hat{M}_\pi$ and $\hat{M} = t\hat{M}_\pi$, then all the relations above are satisfied.

It follows in particular that $M_a = t_a M_\pi$ and $M = tM_\pi$ (where the M_a and M are as in (25.4.20), (25.4.21); cf. (25.4.22)–(25.4.24)). Now we also have

$$\pi^{-1}(a-a^n)S_n = t_a(\pi^{-1}(\pi-\pi^n))S_n, \qquad \nu(n)\pi^{-1}S_n = t(\pi^{-1}(\pi-\pi^n)S_n$$

and it follows that

$$(\phi_{n+1})_*(\pi^{-1}(a-a^n)S_nX^n = M_aX^n, \qquad (\phi_{n+1})_*(\nu(n)\pi^{-1}S_n) = M,$$

so by (24.4.15) and (24.4.20) we have that (25.4.17) holds with n replaced by $n+1$. This completes the induction step and the proof of Theorem (25.4.16).

■ (25.4.26) We note that $(F_S^A(X,Y), \rho_S^A)$ has an A-logarithm (viz. $f_S^A(X)$) over $K[S]$. As a corollary of Theorem (25.4.16) we therefore obtain that a formal A-module over B has a (unique, cf. (21.5.7)) A-logarithm if B is A-torsion free. If moreover $\bigcap_n \pi^n B = \{0\}$ then one has the formula

$$A\text{-}\log_F(X) = \lim_{n\to\infty} \pi^{-n}[\pi^n]_F(X) \tag{25.4.27}$$

which is proved as follows. It suffices to prove this formula for the case $B = A[S]$ and $F(X,Y) = F_S^A(X,Y)$. We have

$$f(X) = f_S^A(X) = \sum a_nX^n, f(X) \equiv X \bmod(\text{degree } 2)$$

with $a_n \in \pi^{-k}A[S]^m$ if q^k is the highest power of q dividing n (and m is the dimension of $F(X,Y)$). Choose $r \in \mathbf{N}$ and let k be the largest integer such that q^k divides one of the numbers $1, 2, \ldots, r$. Then we have that $\pi^n f(X) \equiv 0 \bmod(\text{degree } r+1, \pi^{n-k})$ and hence

$$f(\pi^n f(X)) \equiv \pi^n f(X) \bmod(\text{degree } r+1, \pi^{2n-3k})$$

So, for $2n > 3k$ we have by Part (iv) of the functional equation lemma

$$\pi^n f(X) \equiv f^{-1}(\pi^n f(X)) = [\pi^n]_F(X) \bmod(\pi^{2n-3k}, \text{degree } r+1)$$

and hence $f(X) \equiv \pi^{-n}[\pi^n]_F(X) \bmod(\text{degree } r+1, \pi^{n-3k})$ proving (25.4.27).

■ (25.4.28) Let us call a higher dimensional formal A-module over B A-typical if it is of the form $\phi_*(F_V^A(X, Y), \rho_V^A)$ for some A-algebra homomorphism ϕ: $A[V] \to B$. If B is A-torsion free, then $(G(X, Y), \rho_G)$ is A-typical if and only if $A\text{-log}_G(X)$ is of the form

$$A\text{-log}_G(X) = \sum_{i=0}^{\infty} a_i X^{q^i}$$

for some $m \times m$ matrices a_i with coefficients in $B \otimes_A K$.

One proves as usual that $(F_V^A(X, Y), \rho_V^A)$ is a universal A-typical formal A-module.

■ (25.4.29) **Corollary** (of Proposition (25.4.11)) Every formal A-module over an A-algebra B is strictly isomorphic over B to an A-typical formal A-module.

25.5 Frobenius and Verschiebung for formal A-modules

■ (25.5.1) In this subsection A is a discrete valuation ring with finite residue field k of q elements, and quotient field K; $F(X, Y)$ is always a not necessarily one dimensional formal A-module over an A-algebra B; π is a uniformizing element of A, which for the remainder of this subsection 25.5 is kept fixed, and v denotes the normalized exponential valuation on K, i.e., $v(\pi) = 1$. We note in passing that the restriction "k is finite" is not a serious one. If k is infinite, then a mixture of the arguments in (21.4.20) and Section 25.4 shows that also every higher dimensional formal A-module over B is strictly isomorphic to a higher dimensional additive formal A-module over B.

■ (25.5.2) We can of course consider $F(X, Y)$ as just a formal group law over B. This means that we have on $\mathscr{C}(F; B)$ operators $\mathbf{V}_n$, $\mathbf{f}_n$ for $n \in \mathbf{N}$ and operators $\langle b \rangle$ for $b \in B$. Then if $F(X, Y)$ is a formal A-module, we have in addition that $\mathscr{C}(F; B)$ is a module over A, that is, we have operators $[a]_F$: $\mathscr{C}(F; B) \to \mathscr{C}(F; B)$ for all $a \in A$, induced by the endomorphisms $[a]_F(X) = \rho_F(a)(X)$ of $F(X, Y)$; and these operators $[a]_F$ commute with the $\mathbf{V}_n$, $\mathbf{f}_n$, and $\langle b \rangle$ operators. In case A is a discrete valuation ring this is still not all; there exists in addition a Frobenius type operator $\mathbf{f}_\pi$ that has the property $\mathbf{f}_\pi \mathbf{V}_q = [\pi]_F$. There is in fact such an operator $\mathbf{f}_{\hat{\pi}}$ for every uniformizing element $\hat{\pi}$ of A. Their relations are $\mathbf{f}_{\hat{\pi}} = [u]_F \mathbf{f}_\pi$ if $u\pi = \hat{\pi}$.

■ (25.5.3) **Definition of $\mathbf{f}_\pi$** To define $\mathbf{f}_\pi$ we proceed—as so often before—via the universal example. Let $F(X, Y) = F_S^A(X, Y)$ be the m-dimensional universal

formal A-module over $A[S]$ constructed above in 25.4. Let $C_n(i)$, $n \in \mathbf{N}$; $i \in \{1, \ldots, m\}$ be a second set of indeterminates and let

$$\gamma_C(t) = \sum_{n=1}^{\infty} {}^{F_A^S} C_n t^n \tag{25.5.4}$$

be the universal curve in $\mathscr{C}(F_S^A; A[S; C])$, where C_n is short for the column vector $(C_n(1), \ldots, C_n(m))$. Let $f_S^A(X)$ be the A-logarithm of $F_S^A(X, Y)$ and consider the m-tuple of power series

$$f_S^A(\gamma_C(t)) = \sum_{n=1}^{\infty} x_n t^n \tag{25.5.5}$$

where the x_n are column vectors of length m of polynomials in the Ss and Cs with coefficients in K. Let $\sigma\colon K[S; C] \to K[S; C]$ be the K-endomorphism that takes all the Ss and Cs into their qth powers. Then the functional equation lemma says that the x_n of (25.5.5) satisfy the conditions

$$\text{if } q \nmid n, \quad \text{then } x_n \in A[S; C]^m \tag{25.5.6}$$

$$\text{if } q^r \mid n, \quad \text{but } q^{r+1} \nmid n, \quad \text{then} \tag{25.5.7}$$

$$x_n - \pi^{-1} S_q \sigma(x_{q^{-1}n}) - \pi^{-1} S_{q^2} \sigma^2(x_{q^{-2}n}) - \cdots - \pi^{-1} S_{q^r} \sigma^r(x_{q^{-r}n}) \in A[S; C]^m$$

Now define for all $n \in \mathbf{N}$,

$$y_n = \pi x_{nq} \tag{25.5.8}$$

Then we have: (i) if $q \nmid n$, $y_n = \pi x_{nq} = \pi(x_{nq} - \pi^{-1} S_q \sigma(x_n)) + S_q \sigma(x_n) \in A[S; C]^m$ by (25.5.6) and (25.5.7) and (ii) if $q^r \mid n$ but $q^{r+1} \nmid n$, then

$$y_n - \pi^{-1} S_q \sigma(y_{q^{-1}n}) - \cdots - \pi^{-1} S_{q^r} \sigma^r(y_{q^{-r}n})$$
$$= \pi(x_{nq} - \pi^{-1} S_q \sigma(x_n) - \cdots - \pi^{-1} S_{q^{r+1}} \sigma^{r+1}(x_{q^{-r}n})) + S_{q^{r+1}} \sigma^{r+1}(x_{q^{-r}n})$$

which is in $A[S; C]$ by (25.5.6) and (25.5.7).

The functional equation lemma now says that $(f_S^A)^{-1}(\sum_{n=1}^{\infty} y_n t^n)$ has its coefficients in $A[S; C]^m$, i.e., is a curve in $F_S^A(X, Y)$ over $A[S; C]$. We define

$$\mathbf{f}_\pi(\gamma_C(t)) = (f_S^A)^{-1}\left(\sum_{n=1}^{\infty} y_n t^n\right) = (f_S^A)^{-1}\left(\sum_{q \mid n} \pi x_n t^{n/q}\right) \tag{25.5.9}$$

Now let $F(X, Y)$ be any formal A-module over any A-algebra B and let $\gamma(t)$ be any element of $\mathscr{C}(F; B)$. Then there is a unique A-algebra homomorphism σ: $A[S; C] \to B$ such that

$$\phi_* F_S^A(X, Y) = F(X, Y), \qquad \phi_* \rho_S^A = \rho_F, \qquad \phi_*(\gamma_C(t)) = \gamma(t) \tag{25.5.10}$$

We now define

$$\mathbf{f}_\pi \gamma(t) = \phi_*(\mathbf{f}_\pi(\gamma_C(t)) \tag{25.5.11}$$

Of course $\mathbf{f}_\pi$ depends on $F(X, Y)$ and one should more properly write $\mathbf{f}_\pi^F$ or something similar. So that (25.5.11) should be read as

$$\mathbf{f}_\pi^F \gamma(t) = \phi_*(\mathbf{f}_\pi^{F_S^A}(\gamma_C(t)) \tag{25.5.12}$$

The uniqueness of the ϕ: $A[S; C] \to B$ such that (25.5.10) holds gives us immediately:

■ (25.5.13) **Lemma** Let $F(X, Y)$ be a formal A-module over B, ϕ: $B \to \hat{B}$ an A-algebra homomorphism and $G(X, Y) = \phi_* F(X, Y)$. Then for all $\gamma(t) \in \mathscr{C}(F; B)$

$$\mathbf{f}_\pi^G(\phi_* \gamma(t)) = \phi_*(\mathbf{f}_\pi^F \gamma(t))$$

■ (25.5.14) **Characterization of $\mathbf{f}_\pi$ in terms of A-logarithms** Suppose that $F(X, Y)$ has an A-logarithm $f(X)$ (this happens, e.g., when B is A-torsion free), then the definition of $\mathbf{f}_\pi$ (cf. (25.5.12)) implies that for all $\gamma(t) \in \mathscr{C}(F; B)$

$$f(\gamma(t)) = \sum_{n=1}^{\infty} x_n t^n \quad \Rightarrow \quad f(\mathbf{f}_\pi \gamma(t)) = \sum_{n=1}^{\infty} \pi x_{nq} t^n \tag{25.5.15}$$

(25.5.16) **Proposition** Let $F(X, Y)$ be a formal A-module over B. Then:

(i) $\mathbf{f}_\pi$: $\mathscr{C}(F; B) \to \mathscr{C}(F; B)$ is a homomorphism of A-modules so that in particular $\mathbf{f}_\pi$ commutes with the $[a]_F$ operators, $a \in A$.
(ii) $\mathbf{f}_\pi \mathbf{V}_q = [\pi]_F$.
(iii) $\mathbf{f}_\pi \langle b \rangle = \langle b^q \rangle \mathbf{f}_\pi$.
(iv) $\mathbf{f}_\pi = [u]_F \mathbf{f}_{\hat{\pi}}$ if $\pi = u\hat{\pi}$.
(v) $\mathbf{f}_\pi \mathbf{f}_n = \mathbf{f}_n \mathbf{f}_\pi$ for all $n \in \mathbf{N}$.
(vi) $\mathbf{f}_\pi \mathbf{V}_r = \mathbf{V}_r \mathbf{f}_\pi$ if $(p, r) = 1$.

Proof To prove all these facts it suffices to prove them in the case of A-algebras B that are A-torsion free (by the usual lifting trick) and if B is A-torsion free and $f(X)$ is the A-logarithm of $F(X, Y)$, then it suffices to check that the translations of (i)–(vi) hold in $f(\mathscr{C}(F; B))$. As an example we prove (ii). Let $f(\gamma(t)) = \sum x_n t^n$, then $f([\pi]_F \gamma(t)) = \sum \pi x_n t^n$ and $f(\mathbf{V}_q \gamma(t)) = \sum x_n t^{qn}$, which by (25.5.15) gives $f(\mathbf{f}_\pi \mathbf{V}_q \gamma(t)) = \sum \pi x_n t^n$. All the other statements are proved similarly. (For (v), recall that $f(\mathbf{f}_n \gamma(t)) = \sum n x_{ni} t^i$ if $f(\gamma(t)) = \sum x_i t^i$.)

■ (25.5.17) **q-typical curves and q-typification for the higher dimensional case** Let $\gamma_C(t)$ and $F_S^A(X, Y)$ be the universal curve and the higher dimensional universal formal A-module. Write

$$f_S^A(\gamma_C(t)) = \sum_{n=1}^{\infty} x_n t^n$$

Then the x_n satisfy the functional equation relations (25.5.6), (25.5.7), and it follows that

$$\varepsilon_q^{F_S^A}(\gamma_C(t)) = (f_S^A)^{-1}\left(\sum_{i=0}^{\infty} x_{q^i} t^{q^i}\right) \in \mathscr{C}(F_S^A; A[S; C]) \tag{25.5.18}$$

If $F(X, Y)$ is any formal A-module over any A-algebra B and $\gamma(t) \in \mathscr{C}(F; B)$, there is a unique homomorphism ϕ: $A[S; C]$ such that (25.5.10) holds and we define

$$\varepsilon_q^F(\gamma(t)) = \phi_*(\varepsilon_q^{FS}(\gamma_C(t))) \tag{25.5.19}$$

An element $\gamma(t)$ of $C(F; B)$ is called q-typical if $\varepsilon_q^F\gamma(t) = \gamma(t)$. We have $\varepsilon_q^F\varepsilon_q^F = \varepsilon_q^F$, and ε_q^F is an A-module endomorphism of $\mathscr{C}(F; B)$. Its image is denoted $\mathscr{C}_q(F; B)$, all exactly as in the one dimensional case (cf. 25.2). Also if $F(X, Y)$ has an A-logarithm, then $\gamma(t)$ is q-typical if and only if $f(\gamma(t))$ involves only q powers of t and if $\gamma(t)$ is not necessarily q-typical, then $f(\varepsilon_q^F\gamma(t))$ is obtained from $f(\gamma(t))$ by simply removing all terms involving non-q-powers of t.

■ (25.5.20) **Proposition** $\mathbf{f}_\pi^F\varepsilon_q^F = \varepsilon_q^F\mathbf{f}_\pi^F$ and $\mathbf{f}_\pi^F\mathscr{C}_q(F; B) \subset \mathscr{C}_q(F; B)$.

Proof Again it suffices to prove this in the case that B is A-torsion free. Let $\gamma(t) \in \mathscr{C}(F; B)$ and $f(\gamma(t)) = \sum x_n t^n$, then

$$f(\varepsilon_q^F\gamma(t)) = \sum_{i=0}^{\infty} x_{q^i} t^{q^i} \qquad \text{and} \qquad f(\mathbf{f}_\pi^F\varepsilon_q^F\gamma(t)) = \sum_{i=0}^{\infty} \pi x_{q^{i+1}} t^{q^i}$$

and on the other hand

$$f(\mathbf{f}_\pi^F\gamma(t)) = \sum_{n=1}^{\infty} \pi x_{qn} t^n \qquad \text{and} \qquad f(\varepsilon_q^F\mathbf{f}_\pi^F\gamma(t)) = \sum_{i=0}^{\infty} \pi x_{qq^i} t^{q^i}$$

which proves the first statement. The second statement of the proposition follows from the first one. Q.E.D.

In the case that A is of characteristic zero, $\mathbf{f}_\pi$ is not unrelated to $\mathbf{f}_p$. We have

■ (25.5.21) **Proposition** Let A be a characteristic zero discrete valuation ring and let $p = \pi^e u$, where u is a unit of A. Then we have for all formal A-modules,

$$\mathbf{f}_p = [u]_F\, \mathbf{f}_\pi^e \mathbf{V}_p^{er-1}$$

where r is the degree of the residue extension $[k : \mathbf{F}_p]$, i.e., $q = p^r$.

Proof Again it suffices to prove this in the case that B is A-torsion free. Let $\gamma(t) \in \mathscr{C}(F; B)$ and $f(\gamma(t)) = \sum x_n t^n$. Then we have

$$f(\mathbf{f}_p\gamma(t)) = \sum_{n=1}^{\infty} px_{pn} t^n$$

and on the other hand

$$f(\mathbf{V}_p^{er-1}\gamma(t)) = \sum_{n=1}^{\infty} x_n t^{np^{er-1}}$$

$$f(\mathbf{f}_\pi^e\mathbf{V}_p^{er-1}\gamma(t)) = \sum_{n=1}^{\infty} \pi^e x_{,n} t^n$$

$$f([u]_F\mathbf{f}_\pi^e\mathbf{V}^{er-1}\gamma(t)) = \sum_{n=1}^{\infty} u\pi^e x_{pn} t^n = \sum_{n=1}^{\infty} px_{pn} t^n$$

■(25.5.22) Note that the order of the factors in the formula (25.5.21) matters. The operator $[u]_F$ commutes with $\mathbf{f}_\pi$ and $\mathbf{V}_p$, but $\mathbf{f}_\pi$ and $\mathbf{V}_p$ definitely do not commute with one another; and, e.g., $\mathbf{f}_p \neq [u]_F \mathbf{V}_p^{er-1} \mathbf{f}_\pi^e$ as a rule. (Applying $\mathbf{f}_\pi^e$ "kills off" all coefficients x_n with n not divisible by q^e, while $\mathbf{f}_p$ kills off only the x_n with n prime to p.)

25.6 The Frobenius operator $\mathbf{f}_\pi$ on $\mathscr{C}_q(F; -)$ and $W^F_{q,\infty}(-)$

■(25.6.1) In this section A is a discrete valuation ring with fixed uniformizing element π and residue field k of q elements and $F(X, Y)$ will always be a one dimensional formal A-module over A of A-height 1 such that $\pi(F) = \pi$.

■(25.6.2) **Proposition** Let A, π, $F(X, Y)$ be as above. Then $\mathbf{f}_\pi: \mathscr{C}_q(F; -) \to \mathscr{C}_q(F; -)$ is a functorial A-algebra endomorphism of $\mathscr{C}_q(F; -)$.

Proof As usual it suffices to prove this for $\mathbf{f}_\pi: \mathscr{C}_q(F; B) \to \mathscr{C}_q(F; B)$ with B A-torsion free (in fact it suffices to take $B = A[C_1, C_2, \ldots]$). If B is A-torsion free and $\gamma(t), \delta(t) \in \mathscr{C}_q(F; B)$ and

$$f(\gamma(t)) = \sum x_i t^{q^i}, \qquad f(\delta(t)) = \sum y_i t^{q^i}$$

then we have

$$f(\gamma(t) *_F \delta(t)) = \sum_{i=0}^{\infty} \pi^i x_i y_i t^{q^i}$$

$$f(\mathbf{f}_\pi(\gamma(t) *_F \delta(t))) = \sum_{i=0}^{\infty} \pi(\pi^{i+1} x_{i+1} y_{i+1}) t^{q^i}$$

$$f(\mathbf{f}_\pi \gamma(t)) = \sum_{i=0}^{\infty} \pi x_{i+1} t^{q^i}, \qquad f(\mathbf{f}_\pi \delta(t)) = \sum_{i=0}^{\infty} \pi y_{i+1} t^{q^i}$$

$$f(\mathbf{f}_\pi \gamma(t) *_F \mathbf{f}_\pi \delta(t)) = \sum_{i=0}^{\infty} \pi^i (\pi x_{i+1})(\pi y_{i+1}) t^{q^i}$$

which proves that $\mathbf{f}_\pi$ is multiplicative. Now let $a \in A$. Then we have

$$f([a]_F \mathbf{f}_\pi \gamma(t)) = \sum_{i=0}^{\infty} a(\pi x_{i+1}) t^{q^i}$$

$$f([a]_F \gamma(t)) = \sum_{i=0}^{\infty} a x_i t^{q^i}$$

$$f(\mathbf{f}_\pi [a]_F \gamma(t)) = \sum_{i=0}^{\infty} \pi(a x_{i+1}) t^{q^i}$$

proving that $\mathbf{f}_\pi$ preserves the A-module structure. Finally, $f(e_F(t)) = \sum \pi^{-i} t^{q^i}$ and hence $f(\mathbf{f}_\pi e_F(t)) = f(e_F(t))$, which shows that $\mathbf{f}_\pi$ preserves the unit element of $\mathscr{C}_q(F; B)$. This concludes the proof.

■ (25.6.3) **Remark** If $\hat{\pi} \neq \pi$, then $\mathbf{f}_{\hat{\pi}}: \mathscr{C}_q(F; B) \to \mathscr{C}_q(F; B)$ is not an A-algebra homomorphism; it does not preserve the unit element and is also not multiplication preserving.

■ (25.6.4) **Interpretation of $\mathbf{f}_\pi$, $\mathbf{V}_q$: $W^F_{q,\infty}(-) \to W^F_{q,\infty}(-)$** Via the isomorphism of A-algebra functors $W^F_{q,\infty}(-) \to \mathscr{C}_q(F; -)$, we find a functorial A-algebra endomorphism $\mathbf{f}_\pi$. Now recall that $w^F_{q,i}(b_0, b_1, b_2, \ldots) = \pi^i$ times the coefficient of t^{q^i} in $f((\sum^F)_{i=0}^\infty b_i t^{q^i})$ which, given the definition of $\mathbf{f}_\pi$, means that functorially

$$w^F_{q,i}\mathbf{f}_\pi = w^F_{q,i+1} \qquad \text{for all} \quad i \in \mathbf{N} \cup \{0\} \tag{25.6.5}$$

This of course also determines $\mathbf{f}_\pi$ uniquely (and shows that $\mathbf{f}_\pi$ is an A-algebra homomorphism).

While we are at it, we might just as well describe $\mathbf{V}_q: W^F_{q,\infty}(-) \to W^F_{q,\infty}(-)$ also. Recall that $\mathbf{V}_q\gamma(t) = \gamma(t^q)$ and the isomorphism $\bar{E}: W^F_{q,\infty}(B) \to \mathscr{C}_q(F; B)$ takes $(b_0, b_1, b_2, \ldots)$ into $\varepsilon^F_q\ (\sum^F)_{i=0}^\infty b_i t^{q^i}$ (cf. (25.2.17)) so that

$$\mathbf{V}_q\bar{E}(b_0, b_1, b_2, \ldots) = \varepsilon^F_q \sum^F b_i t^{q^{i+1}} = \bar{E}(0, b_0, b_1, b_2, \ldots)$$

so that on $W^F_{q,\infty}(-)$

$$\mathbf{V}_q(b_0, b_1, b_2, \ldots) = (0, b_0, b_1, b_2, \ldots) \tag{25.6.6}$$

In terms of the $w^F_{q,i}$ we therefore find (cf. (25.3.3))

$$w^F_{q,i}\mathbf{V}_q = \begin{cases} 0 & \text{if} \quad i = 0 \\ \pi w^F_{q,i-1} & \text{if} \quad i \geq 1 \end{cases} \tag{25.6.7}$$

■ (25.6.8) **Proposition** For all $\gamma(t) \in \mathscr{C}_q(F; B)$ we have

$$\mathbf{f}_\pi\gamma(t) \equiv \gamma(t)^q \mod [\pi]\mathscr{C}_q(F; B)$$

Proof It suffices to prove this in the universal case, i.e., in the case that $B = A[C_0, C_1, \ldots]$ and $\gamma(t)$ is the curve

$$\gamma_C(t) = \varepsilon^F_q\left(\sum_{i=0}^\infty{}^F C_i t^{q^i}\right) \in \mathscr{C}_q(F; A[C_0, C_1, \ldots])$$

As usual we put

$$f(\gamma_C(t)) = \sum_{i=0}^\infty x_i t^{q^i}$$

and the x_i are then polynomials in the $C_0, C_1, \ldots$ with coefficients in K satisfying the functional equation conditions

$$x_0 \in A[C], \qquad x_i - \pi^{-1}\sigma x_{i-1} \in A[C]$$

where $\sigma: K[C] \to K[C]$ is the K-algebra endomorphism $C_j \mapsto C_j^q$. Writing $y_i = \pi^i x_i$, we have $y_i \in A[C]$ and

$$y_i \equiv \sigma(y_{i-1}) \mod \pi^i, \qquad i \in \mathbf{N} \tag{25.6.9}$$

We have

$$f(\gamma_C^q(t)) = \sum_{i=0}^{\infty} \pi^{i(q-1)} x_i^q t^{q^i} = \sum_{i=0}^{\infty} \frac{y_i^q}{\pi^i} t^{q^i}$$

and

$$f(\mathbf{f}_\pi \gamma_C(t)) = \sum_{i=0}^{\infty} \pi x_{i+1} t^{q^i} = \sum_{i=0}^{\infty} \frac{y_{i+1}}{\pi^i} t^{q^i}$$

Now to prove that $\mathbf{f}_\pi \gamma(t) - \gamma(t)^q \in [\pi]\mathscr{C}_q(F; B) = f^{-1}(\pi f(\mathscr{C}_q(F; B))$ we must clearly show that

$$f^{-1}\left(\pi^{-1}\left(\sum_{i=0}^{\infty} \pi^{-i} y_i^q t^{q^i} - \sum_{i=0}^{\infty} \pi^{-i} y_{i+1} t^{q^i}\right)\right) \in \mathscr{C}_q(F; B)$$

and by the functional equation lemma this is equivalent to showing that

$$\pi^{-1}(y_0^q - y_1) \in A[C] \tag{25.6.10}$$

$$\pi^{-1}(\pi^{-i} y_i^q - \pi^{-i} y_{i+1}) - \pi^{-2}\sigma(\pi^{-i+1} y_{i-1}^q - \pi^{-i+1} y_i) \in A[C] \tag{25.6.11}$$

for all $i \in \mathbf{N}$

Now by (25.6.9) $y_1 \equiv \sigma(y_0) \bmod \pi$ and also $\sigma(y_0) \equiv y_0^q \bmod \pi$ which proves (25.6.10). Further again by (25.6.9)

$$y_i \equiv \sigma(y_{i-1}) \mod \pi^i, \qquad y_{i+1} \equiv \sigma(y_i) \mod \pi^{i+1} \tag{25.6.12}$$

Hence

$$y_i^q \equiv \sigma(y_{i-1})^q = \sigma(y_{i-1}^q) \mod \pi^{i+1} \tag{25.6.13}$$

and (25.6.12) and (25.6.13) together prove (25.6.11). This concludes the proof.

A closely related result is

■ (25.6.14) **Proposition** Let $(b_0, b_1, \ldots) \in W_{q,\infty}^F(B)$ and $\mathbf{f}_\pi(b_0, b_1, \ldots) = (\hat{b}_0, \hat{b}_1, \hat{b}_2, \ldots)$, then $\hat{b}_i \equiv b_i^q \bmod \pi B$ for all $i \in \mathbf{N} \cup \{0\}$.

Proof It suffices to prove this in the case $B = A[C_0, C_1, C_2, \ldots]$ and $b_i = C_i$ for all $i \in \mathbf{N} \cup \{0\}$. We then have as usual (cf. (25.2.17))

$$f(\bar{E}(C_0, C_1, C_2, \ldots)) = f(\varepsilon_q^F(\textstyle\sum^F C_i t^{q^i})) = \displaystyle\sum_{i=0}^{\infty} \pi^{-i} w_{q,i}^F(C) t^{q^i}$$

which means that

$$f(\bar{E}(\mathbf{f}_\pi(C_0, C_1, C_2, \ldots))) = \sum_{i=0}^{\infty} \pi^{-i} w_{q,i+1}^F(C) t^{q^i}$$

Now let $\mathbf{f}_\pi(C_0, C_1, C_2, \ldots) = (\hat{C}_0, \hat{C}_1, \hat{C}_2, \ldots)$. Then the $\hat{C}_i$ are polynomials in the $C_0, C_1, C_2, \ldots$ and we have

$$f\left(\varepsilon_q^F\left(\sum_{i=0}^{\infty F} \hat{C}_i t^{q^i}\right)\right) = \sum_{i=0}^{\infty} \pi^{-i} w_{q,i}^F(\hat{C}_0, \hat{C}_1, \ldots) t^{q^i}$$

and

$$\pi^{-i}w_{q.i}^F(\hat{C}_0, \hat{C}_1, \ldots) = \pi^{-i}w_{q.i+1}^F(C_0, C_1, C_2, \ldots)$$

On the other hand we have modulo π

$$\begin{aligned}\pi^{-i}w_{q.i}^F(C_0^q, C_1^q, \ldots) &= C_i^q + a_q C_{i-1}^{q^2} + \cdots + a_{q^i} C_0^{q^{i+1}} \\ &\equiv \pi(C_{i+1} + a_q C_i^q + a_{q^2} C_{i-1}^{q^2} + \cdots + a_{q^{i+1}} C_0^{q^{i+1}}) \\ &= \pi^{-i}w_{q.i+1}^F(C_0, C_1, C_2, \ldots)\end{aligned}$$

because $\pi a_q \equiv 1 \bmod \pi$, $\pi a_{q^i} \equiv a_{q^{i-1}} \bmod \pi$ as $f(X) = \sum a_i X^i$, the A-logarithm of A satisfies $f(X) - \pi^{-1}f(X^q) \in A[\![X]\!]$. It follows that

$$\varepsilon_q^F \textstyle\sum^F \hat{C}_i t^{q^i} = \mathbf{f}_\pi \varepsilon_q^F(\sum^F C_i t^{q^i}), \qquad \varepsilon_q^F \sum^F C_i^q t^{q^i}$$

are two power series with integral coefficients such that

$$f(\varepsilon_q^F(\textstyle\sum^F \hat{C}_i t^{q^i})) = f(\varepsilon_q^F(\sum^F C_i^q t^{q^i})) \mod(\pi).$$

Part (iv) of the functional equation lemma now gives

$$\varepsilon_q^F \textstyle\sum^F \hat{C}_i t^{q^i} \equiv \varepsilon_q^F \sum^F C_i^q t^{q^i} \mod \pi$$

from which one obtains by induction that $\hat{C}_i \equiv C_i^q \bmod \pi$ for all i. This proves the proposition.

■ (25.6.15) **Remark on notation** Let $\gamma(t)$ and $\delta(t)$ be two elements of $\mathscr{C}_q(F; B)$ or $\mathscr{C}(F; B)$, then writing out $\gamma(t)$ and $\delta(t)$ as power series in t, $\gamma(t) = \sum a_i t^i$, $\delta(t) = \sum b_i t^i$, $a_i, b_i \in B$, it may happen that $a_i \equiv b_i \bmod \pi$ for all i. This will be written $\gamma(t) \equiv \delta(t) \bmod \pi$. On the other hand, $\mathscr{C}_q(F; B)$ and $\mathscr{C}(F; B)$ are A-modules, so it may happen that there is an $\varepsilon(t) \in \mathscr{C}_q(F; B)$ or $\mathscr{C}(F; B)$ such that $\gamma(t) = \delta(t) + [\pi]_F \varepsilon(t)$. This will be written $\gamma(t) \equiv \delta(t) \bmod [\pi]_F \mathscr{C}(F; B)$ or $\bmod [\pi]\mathscr{C}(F; B)$.

This means of course that $f(\gamma(t)) - f(\delta(t)) \in \pi f\mathscr{C}(F; B)$ which is decidedly a different condition from $f(\gamma(t)) - f(\delta(t)) \in \pi B[\![t]\!]$ which by part (iv) of the functional equation lemma is equivalent to $\gamma(t) \equiv \delta(t) \bmod \pi$ (if $F(X, Y)$ is of functional equation type).

■ (25.6.16) **Remarks**

(i) It follows from (25.6.8) that under the isomorphism $A_n \xrightarrow{\sim} \mathscr{C}_q(F; k_n)$ of (25.3.30) the Frobenius substitution σ of A_n ($\sigma x \equiv x^q \bmod \pi$) corresponds to the endomorphism of $\mathscr{C}_q(F; k_n)$ induced by the $\mathbf{f}_\pi$.

(ii) Under the identification $A_n \xrightarrow{\sim} \mathscr{N}_{q.\infty}^F(k_n)$ the Frobenius substitution σ becomes $(b_0, b_1, \ldots) \mapsto (b_0^q, b_1^q, \ldots)$ by remark (i) above and Proposition (25.6.14).

25.7 Artin–Hasse-like exponential maps

■ (25.7.1) A is again a discrete valuation ring with uniformizing element π and residue field k of q elements and $F(X, Y)$ is a one dimensional formal A-module over A of A-height 1 such that $\pi(F) = \pi$.

■ (25.7.2) **Proposition** Let B be an A-torsion free A-algebra that admits an A-algebra endomorphism $\sigma\colon B \to B$ with the property $\sigma(b) \equiv b^q \bmod \pi B$ for all $b \in B$. Then there exists a unique A-algebra homomorphism $D_B\colon B \to W^F_{q,\infty}(B)$ such that $w^F_{q,i} D_B = \sigma^i$ for all $i \in \mathbf{N} \cup \{0\}$.

Proof For each $b \in B$ let $\vartheta(b)$ be the power series

$$(25.7.3)\quad \vartheta(b)(t) = bt + \pi^{-1}\sigma(b)t^q + \pi^{-2}\sigma^2(b)t^{q^2} + \cdots \in (B \otimes_A K)[\![t]\!]$$

Now because $\sigma(b) \equiv b^q \bmod \pi B$, we are in a functional equation type situation if we take $B \subset B \otimes_A K$, $\mathfrak{A} = \pi B$, σ, p, q as above, and $s_1 = \pi^{-1}$, $s_2 = s_3 = \cdots = 0$. And $\vartheta(b)$ for each $b \in B$ satisfies the functional equation

$$\vartheta(b)(t) - \pi^{-1}\sigma_*(\vartheta(b)(t^q)) \in B[\![t]\!]$$

because $bt \in B[\![t]\!]$ and $\pi^{-i}\sigma^i(b) - \pi^{-1}\sigma(\pi^{-i+1}\sigma^{i-1}(b)) = 0$. It follows that

$$\bar{D}_B(b) = f^{-1}(\vartheta(b)(t)) \in \mathscr{C}_q(F; B)$$

We now define $D_B = \bar{E}\bar{D}_B$. Then $w^F_{q,i}(D_B(b)) = (\pi^i$ times the coefficient of t^{q^i} in $\bar{D}_B(b)) = \sigma^i(b)$, so that indeed $w^F_{q,i} D_B = \sigma^i$, which also proves that D_B is an A-algebra homomorphism. (Alternatively, one checks this directly via (25.7.3).)

■ (25.7.4) **Theorem** There exists a unique functorial A-algebra homomorphism $\Delta^F\colon W^F_{q,\infty}(-) \to W^F_{q,\infty}(W^F_{q,\infty}(-))$ such that $w^F_{q,i}\Delta^F = \mathbf{f}^i_\pi$ for all $i \in \mathbf{N} \cup \{0\}$.

Proof Let $B = A[C_1, C_2, \ldots]$. Then $W^F_{q,\infty}(B)$ is an A-torsion free A-algebra (very easy to check; follows from the fact that $R_{q,\pi}(B \otimes_A K)$ is clearly A-torsion free) with an A-algebra homomorphism $\mathbf{f}_\pi\colon W_{q,\infty}(B) \to W_{q,\infty}(B)$, which satisfies $\mathbf{f}_\pi(b) \equiv b^q \bmod \pi W_{q,\infty}(B)$, by Proposition (25.6.8). According to Proposition (25.7.2) there therefore exists a unique A-algebra homomorphism $D\colon W_{q,\infty}(B) \to W_{q,\infty}(W_{q,\infty}(B))$ such that $w^F_{q,i} D = \mathbf{f}^i_\pi$ for all $i \in \mathbf{N} \cup \{0\}$.

Now let B be any A-algebra and $(b_0, b_1, \ldots) \in B$. There then exists (cf. (25.2.17)) a unique homomorphism $\phi\colon A[C] \to B$ such that $\phi(\bar{E}^{-1}\gamma_C(t)) = (b_0, b_1, \ldots)$ where $\gamma_C(t)$ is the curve $\varepsilon^F_q \sum^F C_i t^{q^i} \in \mathscr{C}_q(F; A[C])$ and we define

$$\Delta^F_B(b_0, b_1, \ldots) = W^F_{q,\infty}(W^F_{q,\infty}(\phi))(\Delta^F_{A[C]}(\bar{E}^{-1}(\gamma_C(t))))$$

That Δ^F is functorial follows from this definition (uniqueness of ϕ!) and that Δ^F is a homomorphism of A-algebras is proved as usual. Q.E.D.

■ (25.7.5) Alternatively, consider $\Delta^F_{A[C]}(\bar{E}^{-1}(\gamma_C(t))) \in W^F_{q,\infty}(W^F_{q,\infty}(-))$. This is a sequence of elements of $W^F_{q,\infty}(A[C])$, i.e., a sequence of sequences of polyno-

mials in the $C_0, C_1, \ldots$ with coefficients in A. These are the universal polynomials that define the functor morphism Δ^F.

■ (25.7.6) By definition Δ^F is such that $w^F_{q,0}\Delta^F = id$. There is however a second functorial A-algebra homomorphism, viz.

$$W^F_{q,\infty}(w^F_{q,0})\colon W^F_{q,\infty}(W^F_{q,\infty}(-)) \to W^F_{q,\infty}(-)$$

In fact there is a whole series of functorial A-algebra homomorphisms, viz. the $W^F_{q,\infty}(w^F_{q,i})$ for all i.

■ (25.7.7) **Addendum to Theorem (25.7.4)** Δ^F also satisfies

$$W^F_{q,\infty}(w^F_{q,i})\Delta^F = \mathbf{f}^i_\pi$$

Proof To prove this recall that if $\phi\colon B \to B'$ is a homomorphism of A-algebras, then we have for all $i \in \mathbf{N} \cup \{0\}$ a commutative diagram

(25.7.8)
$$\begin{array}{ccc} W^F_{q,\infty}(B) & \xrightarrow{W^F_{q,\infty}(\phi)} & W^F_{q,\infty}(B') \\ \downarrow{\scriptstyle w^F_{q,i}(B)} & & \downarrow{\scriptstyle w^F_{q,i}(B')} \\ B & \xrightarrow{\phi} & B' \end{array}$$

Now consider the diagram

(25.7.9)
$$\begin{array}{ccccc} W^F_{q,\infty}(B) & \xrightarrow{\Delta^F} & W^F_{q,\infty}(W^F_{q,\infty}(B)) & \xrightarrow{w^F_{q,i}} & W^F_{q,\infty}(B) \\ & \searrow^{\phi_n} & \downarrow{\scriptstyle W^F_{q,\infty}(w^F_{q,n})} & & \downarrow{\scriptstyle w^F_{q,n}} \\ & & W^F_{q,\infty}(B) & \xrightarrow{w^F_{q,i}} & B \end{array}$$

where we have written ϕ_n for the composed homomorphism $W^F_{q,\infty}(w^F_{q,n}) \circ \Delta^F$. The right-hand square of (25.7.9) is a special case of (25.7.8). Now we have $w^F_{q,i} \circ \Delta^F = \mathbf{f}^i_\pi$ and $w^F_{q,n}\mathbf{f}^i_\pi = w^F_{q,n+i}$. So the unknown homomorphism ϕ_n satisfies

$$w^F_{q,i}\phi_n = w^F_{q,n+i}$$

In case B is A-torsion free, this means that we must have $\phi_n = \mathbf{f}^n_\pi$, and by functoriality we therefore have proved the addendum.

■ (25.7.10) **Corollary** There exists a functorial Artin–Hasse-like exponential mapping $E^F\colon W^F_{q,\infty}(-) \to \mathscr{C}(F; W^F_{q,\infty}(-))$ with the properties:

(i) E^F is a homomorphism of A-modules.
(ii) The composed map

$$W^F_{q,\infty}(-) \to \mathscr{C}(F; W^F_{q,\infty}(-)) \xrightarrow{t^i_q} \mathscr{C}_q(F; W^F_{q,\infty}(-))$$

is a homomorphism of A-algebras.

(iii) There is a commutative diagram

$$\begin{array}{ccccc} W^F_{q,\infty}(-) & \xrightarrow{E^F} & \mathscr{C}(F, W^F_{q,\infty}(-)) & \xrightarrow{\varepsilon^F_q} & \mathscr{C}_q(F; W^F_{q,\infty}(-)) \\ \downarrow{\scriptstyle \bar{E}^F} & & \downarrow & & \downarrow{\scriptstyle \mathscr{C}_q(F; w^F_{q,0})} \\ \mathscr{C}_q(F; -) & \xrightarrow{i} & \mathscr{C}(F; -) & \xrightarrow{\varepsilon^F_q} & \mathscr{C}_q(F; -) \end{array}$$

where i is the natural inclusion. Because $\varepsilon^F_q i = id$, this also means that:

(iv) $\mathscr{C}_q(F; w^F_{q,0}) \circ \varepsilon^F_q \circ E^F = \bar{E}^F$, so that E^F can be considered as a sort of lift of $\bar{E}^F$, which explains (possibly) some of our notation.

(v) The image of E^F is contained in $\mathscr{C}_q(F; W^F_{q,\infty}(-))$.

Proof Define E^F as the composite of $\Delta^F\colon W^F_{q,\infty}(-) \to W^F_{q,\infty}(W^F_{q,\infty}(-))$ with

$$\bar{E}^F(W^F_{q,\infty}(-))\colon W^F_{q,\infty}(W^F_{q,\infty}(-)) \to \mathscr{C}_q(F; W^F_{q,\infty}(-))$$

with the natural embedding of $\mathscr{C}_q(F; W^F_{q,\infty}(-))$ in $\mathscr{C}(F; W^F_{q,\infty}(-))$.

25.8 Global Lubin–Tate formal group laws

■ (25.8.1) In this section A is the ring of integers of a global field K, i.e., K is a finite extension of $\mathbf{Q}$ or a finite extension of $\mathbf{F}_p(X)$ for some prime number p. For every finite valuation v, we use A_v to denote the ring of integers of K_v, the completion of K with respect to v.

Now let $F(X, Y)$ be a formal group law over A (of dimension 1) such that for every finite valuation v, $F(X, Y)$ is a formal A_v-module over A_v of A_v-height 1. We shall call such formal group laws *global Lubin–Tate formal group laws*. It follows of course that $F(X, Y)$ admits A as a ring of endomorphisms, and one readily shows that $F(X, Y)$ is in any case a formal A-module.

■ (25.8.2) **Existence of global Lubin–Tate formal group laws** For every finite valuation v, choose a formal A_v-module $F^v(X, Y)$ over A_v of A_v-height 1. Then if K is of characteristic zero, the results of 20.5 say that there exists (up to isomorphism exactly one) formal group law $F(X, Y)$ over A that is isomorphic to $F^v(X, Y)$ over A_v for all v.

In case K is of characteristic p, the same results holds. The reason is the following: because the $F^v(X, Y)$ over A_v are A_v-modules, they have A_v-logarithms. The same technique of 20.5 of fitting A_v-logarithms together for all the different v's works also in this case (of course one works now over K not over $A \otimes \mathbf{Q}$) and the same theorems hold.

■ (25.8.3) **Artin–Hasse-type maps** Now let $F(X, Y)$ be a global Lubin–Tate formal group law over A. Then by the results of 25.7 we have for all A_v-algebras B_v Artin–Hasse-like exponential maps $W^F_{q,\infty}(B_v) \to \mathscr{C}(F; W^F_{q,\infty}(B_v))$ into the *same* group scheme $\mathscr{C}(F; -)$.

In particular, we can take $B_v = k_v$, the residue field of A_v, or more generally

$B_v = k_{v,n}$, the extension of degree n of k_v. Then using that $W^F_{q,\infty}(k_{v,n}) = A_{v,n}$, the ring of integers of the unramified extension of degree n of K_v, we find A-module homomorphisms

$$A_{v,n} \to \mathscr{C}(F; A_{v,n})$$

for all finite valuations v. These A-module homomorphisms I am inclined to view as the ramified version of the Artin–Hasse exponentials $W_{p^\infty}(k) \to \Lambda(W_{p^\infty}(k))$ for all prime numbers p and finite fields k of characteristic p. In both cases one has one *fixed* group scheme (in the ramified case $\mathscr{C}(F; -)$; in the case of the rational numbers $\Lambda(-)$) into which the various local rings of integers are mapped.

In fact one of the reasons why we developed the theory of the $W^F_{q,\infty}(-)$ for all formal A-modules of A-height 1 over A instead of only for $G_\pi(X, Y)$ was a desire to find homomorphisms $A_{v,n} \to \mathscr{C}(F; A_{v,n})$ for all v with F, or rather $\mathscr{C}(F; -)$, independent of v.

25.9 Rings of curves, Witt vectors, and Artin–Hasse-like exponential morphisms for twisted one dimensional Lubin–Tate formal group laws

■ (25.9.1) **The set up** Much of the theory developed above can be generalized considerably. In particular one can define suitable Witt vectors $W^F_{q,\infty}(-)$ and Artin–Hasse-like morphisms for twisted one dimensional Lubin–Tate formal group laws; cf. Chapter II, Section 13.2. The basic setup consists of the ingredients:

(i) a ring A that is a (unitary) subring of a ring K;
(ii) an element $\omega \in A$ that is a unit in K;
(iii) an endomorphism $\sigma\colon K \to K$;
(iv) a prime number p and a power q of p

that are subject to the following conditions:

(v) $\sigma(a) \equiv a^q \bmod \omega A$ for all $a \in A$;
(vi) $p \in \omega A$.

In particular, it follows that we are in a functional equation type situation if we take A, K, p, q, σ as above, $\mathfrak{A} = \omega A$ and $s_1 = \omega^{-1}$, $s_2 = s_3 = \cdots = 0$.

As examples we have, e.g.:

(a) A the ring of integers of a local field K, σ a power r of the Frobenius substitution, $q = p^r$, p = residue characteristic of K, ω a uniformizing element of A.

(b) $A = W_{p^\infty}(k)$ where k is any perfect field of characteristic p.

(c) $A = \mathbf{Z}[\varepsilon]/(\varepsilon^n)$, $K = \mathbf{Q}[\varepsilon]/(\varepsilon^n)$, $\omega = p = q$, $\sigma(\varepsilon) = \varepsilon^p$.

Now let $f(X)$ be any power series in one variable with coefficients in K such that

(25.9.2) $f(X) \equiv X \mod(\text{degree } 2), \qquad f(X) - \omega^{-1}\sigma_* f(X^q) \in A[\![X]\!]$

The functional equation lemma now says that $F(X, Y) = f^{-1}(f(X) + f(Y))$ is a formal group law over A. In the remainder of this subsection (25.9) $F(X, Y)$ will always be a formal group law over A that admits a logarithm $f(X) \in K[\![X]\!]$ such that (25.9.2) holds. Note that the *one dimensional* twisted Lubin–Tate formal group laws of Chapter II, Section 13.2 are of this type.

■ (25.9.3) Below we shall give a quick sketch of constructions and results which generalize those of 25.1–25.8. The proofs are all virtually identical with those given in 25.1–25.8. We leave to the interested (resp. mildly interested, resp. indifferent) reader the task of filling in the details (resp. looking up the details in [181]; resp. taking the details on faith).

All the constructions and (sketches of) proofs below are first done for the A-algebra $B = A[C_0, C_1, \ldots]$ and are then functorially extended as usual via the universal curve(s) to constructions and proofs for all A-algebras B. All proofs are essentially based on the fact that $\sigma\colon K \to K$ extends to an endomorphism of rings $\sigma\colon K[C] \to K[C]$, $C_i \mapsto C_i^q$ such that $\sigma(b) \equiv b^q \bmod \omega A[C]$ for all $b \in A[C]$. This uses (v) and (vi) of (25.9.1).

■ (25.9.4) **q-typification** A curve $\gamma(t) \in \mathscr{C}(F; A[C])$ is q-typical if its logarithm $f(\gamma(t))$ does not involve non-q powers of t. A curve is made q-typical by taking $f(\gamma(t))$, removing all non-q-power terms, and applying f^{-1} to the result. We thus find a functorial group homomorphism $\varepsilon_q^F\colon \mathscr{C}(F; -) \to \mathscr{C}(F; -)$. Its image is denoted $\mathscr{C}_q(F; -)$ and ε_q^F is the identity on $\mathscr{C}_q(F; -)$.

■ (25.9.5) **Multiplication on $\mathscr{C}_q(F; -)$** For $\gamma(t)$, $\delta(t) \in \mathscr{C}_q(F; A[C])$ the multiplication is given by

(25.9.6) $$f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i}, \qquad f(\delta(t)) = \sum_{i=0}^{\infty} y_i t^{q^i}$$

$$\Rightarrow \quad f(\gamma(t) * \delta(t)) = \sum_{i=0}^{\infty} m_i x_i y_i t^{q^i}$$

with

(25.9.7) $$m_0 = 1, \qquad m_i = \omega\sigma(\omega) \cdots \sigma^{i-1}(\omega) \quad \text{if } i \in \mathbf{N}$$

This turns $\mathscr{C}_q(F; -)$ into a ring functor on $\mathbf{Alg}_A$ with unit element

(25.9.8) $e_F(t)$

$$= f^{-1}(t + \omega^{-1}t^q + \omega^{-1}\sigma(\omega)^{-1}t^{q^2} + \omega^{-1}\sigma(\omega)^{-1}\sigma^2(\omega)^{-1}t^{q^3} + \cdots)$$

■ (25.9.9) **The ring homomorphisms $A \to \mathscr{C}_q(F; -)$** Given $a \in A$ and $\gamma(t) \in \mathscr{C}_q(F; A[C])$ we define a new curve $\{a\}_F\gamma(t) \in \mathscr{C}_q(F; A[C])$ by the formula

$$(25.9.10) \qquad f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i} \quad \Rightarrow \quad f(\{a\}_F\gamma(t)) = \sum_{i=0}^{\infty} x_i \sigma^i(a) t^{q^i}$$

This turns $\mathscr{C}_q(F; -)$ functorially into an A-module, and the map $a \to \{a\}_F e_F(t)$ defines a ring homomorphism $A \to \mathscr{C}_q(F; -)$ making $\mathscr{C}_q(F; -)$ into a functor $\mathbf{Alg}_A \to \mathbf{Alg}_A$.

It is not true, however, that $\{a\}_F$ is induced by the endomorphism $[a]_F(X) = f^{-1}(af(X))$ of $F(X, Y)$, whence the different notation. In fact $f^{-1}(af(X))$ need not have integral coefficients and there may be no endomorphism of $F(X, Y)$ at all inducing the operator $\{a\}_F$.

■ (25.9.11) **The twisted Frobenius operator $\mathbf{f}_\omega^{\mathrm{tw}}$** Let $\gamma(t) \in \mathscr{C}_q(F; A[C])$, then we define $\mathbf{f}_\omega^{\mathrm{tw}}\gamma(t)$ by the formula

$$(25.9.12) \qquad f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i} \quad \Rightarrow \quad f(\mathbf{f}_\omega^{\mathrm{tw}}\gamma(t)) = \sum_{i=0}^{\infty} \sigma^i(\omega) x_{i+1} t^{q^i}$$

We remark that even in the case that A is a discrete valuation ring and $\omega = \pi$ is a uniformizing element of A, it is in general not true that $\mathbf{f}_\omega^{\mathrm{tw}} = \mathbf{f}_\pi$ where $\mathbf{f}_\pi$ is the Frobenius operator discussed in 21.5 and 25.6. In fact $F(X, Y)$ is as a rule not a formal A-module, and hence $\mathbf{f}_\pi$ need not be defined. One should however view $F(X, Y)$ as a twisted formal A-module in the sense of 25.10.

■ (25.9.13) **Proposition** The Frobenius operator $\mathbf{f}_\omega^{\mathrm{tw}}$ on $\mathscr{C}_q(F; -)$ has the properties:

(i) $\mathbf{f}_\omega^{\mathrm{tw}}$ is a ring endomorphism of $\mathscr{C}_q(F; -)$.

(ii) $\mathbf{f}_\omega^{\mathrm{tw}}$ is a *semilinear* A-module endomorphism of $\mathscr{C}_q(F; -)$, which means that $\mathbf{f}_\omega^{\mathrm{tw}}(\{a\}_F\gamma(t)) = \{\sigma(a)\}_F(f_\omega^{\mathrm{tw}}\gamma(t))$ for all $a \in A$. In other words $\mathbf{f}_\omega^{\mathrm{tw}}$ is a ring endomorphism of $\mathscr{C}_q(F; -)$ that extends the ring endomorphism σ of A.

(iii) $\mathbf{f}_\omega^{\mathrm{tw}}\mathbf{V}_q = \{\omega\}_F$.

(iv) $\mathbf{f}_\omega^{\mathrm{tw}}\gamma(t) \equiv \gamma(t)^q \bmod \{\omega\}_F\mathscr{C}_q(F; -)$.

Property (ii) of $\mathbf{f}_\omega^{\mathrm{tw}}$ is extremely fortunate because the generalization which works of Proposition (25.7.2) is

■ (25.9.14) **Proposition** Let B be an A-algebra such that $B \to B \otimes_A K$ is injective and such that there is an endomorphism σ_B: $B \otimes_A K \to B \otimes_A K$ which restricts to σ on K and such that $\sigma_B(b) \equiv b^q \bmod \omega B$ for all $b \in B$. Then there is a unique A-algebra homomorphism D: $B \to \mathscr{C}_q(F; B)$ such that $s_{q,i}^F D = \sigma_B^i$ for all $i \in \mathbf{N} \cup \{0\}$, where $s_{q,i}^F$: $\mathscr{C}_q(F; B) \to B$ is defined as $s_{q,i}^F\gamma(t) = \omega\sigma(\omega) \cdots \sigma^{i-1}(\omega)$ times coefficient of t^{q^i} in $f(\gamma(t))$.

■ (25.9.15) **Remarks**

(i) $s_{q,i}^F$: $\mathscr{C}_q(F; B) \to B$ is a ring homomorphism and also a semilinear A-algebra homomorphism. The twist is $s_{q,i}^F(\{a\}_F\gamma(t)) = \sigma^i(a)(s_{q,i}^F\gamma(t))$.

(ii) Using σ_B instead of σ and B and $B \otimes_A K$ instead of A and K, we can view $F(X, Y)$ (more properly $\iota_* F(X, Y)$ where $\iota: A \to B$ is the A-algebra structure morphism) as a formal group law over B. Applying (25.9.9) or (25.9.14) we see that $\mathscr{C}_q(F; B)$ is also a B-algebra that extends the already given A-algebra structure and that D is a B-algebra homomorphism (in fact the B-algebra structure map of $\mathscr{C}_q(F; B)$). This gives us additional information even in the case of the untwisted formal group laws studied in 25.6 and 25.7.

One particular B that which one can take in Proposition (25.9.14) is $\mathscr{C}_q(F; A[C])$ with $\mathbf{f}_\omega^{\mathrm{tw}}$ as σ_B. (NB $\mathscr{C}_q(F; A[C]) \hookrightarrow \mathscr{C}_q(F; K[C])$ and $\mathbf{f}_\omega^{\mathrm{tw}}$, being functorial, extends.) This yields

■(25.9.16) **Proposition** There exists a unique A-algebra functor homomorphism $\tilde{\Delta}_*^F$: $\mathscr{C}_q(F; -) \to \mathscr{C}_q(F; \mathscr{C}_q(F; -))$ such that $s_{q,i}^F \tilde{\Delta}^F = (\mathbf{f}_\omega^{\mathrm{tw}})^i$ for all $i \in \mathbf{N} \cup \{0\}$.

■(25.9.17) Now let us specialize somewhat to the case that A is a complete discrete valuation ring with perfect residue field k of characteristic $p > 0$, K its quotient field, and $\omega = \pi$ is a uniformizing element of A. (Note that A may be of characteristic $p > 0$ and that k may be infinite.) Let K' be an unramified extension of K, A' the ring of integers of K', and k' the residue field of K'. Then we have A-algebra homomorphisms $A' \to \mathscr{C}_q(F; A') \to \mathscr{C}_q(F; k')$, and the composite $A' \to \mathscr{C}_q(F; k')$ is again an isomorphism, just as in the untwisted case (Theorem (25.3.30)).

■(25.9.18) **The "Witt vectors" $W_{q,\infty}^F(-)$** We can now of course use the fact that $\mathscr{C}_q(F; -)$ is representable by $A[C_0, C_1, C_2, \ldots]$ and restate everything in terms of $W_{q,\infty}^F(-)$. The relevant polynomials $w_{q,i}^F$ are

$$(25.9.19) \qquad w_{q,i}^F(Z_0, \ldots, Z_i) = \omega\sigma(\omega) \cdots \sigma^{i-1}(\omega)(Z_i + a_q Z_{i-1}^q + \cdots + a_{q^i} Z_0^{q^i}), \qquad w_{q,0}^F(Z_0) = Z_0$$

where the a_{q^n} are the coefficients of t^{q^n} in $f(X)$, the logarithm of $F(X, Y)$.

Note that the $w_{q,i}^F$ are polynomials with coefficients in A because $a_{q^n} - \omega^{-1}\sigma(a_{q^{n-1}}) \in A$ for all $n \in \mathbf{N}$. We find the theorem:

■(25.9.20) **Theorem** Let A, K, p, q, σ, ω, and $F(X, Y)$ be as in (25.9.1). Then there exists a unique functor $W_{q,\infty}^F$: $\mathbf{Alg}_A \to \mathbf{Alg}_A$ with the properties:

(i) As a set-valued functor we have $W_{q,\infty}^F(B) = \{(b_0, b_1, b_2, \ldots) \mid b_i \in B\}$ and $W_{q,\infty}^F(\phi)(b_0, b_1, \ldots) = (\phi(b_0), \phi(b_1), \ldots)$ for ϕ: $B \to D$ in $\mathbf{Alg}_A$.

(ii) The $w_{q,i}^F(Z)$ of (25.9.19) define twisted (or semilinear) functorial A-algebra homomorphisms $W_{q,r}^F(B) \to B$ with twist $w_{q,i}^F(\{a\}(b_0, b_1, \ldots)) = \{\sigma^i(a)\}(w_{q,i}^F(b_0, b_1, b_2, \ldots))$ (i.e., the $w_{q,i}^F$ are ring homomorphisms that twist the A-module structure around in the manner indicated).

The functor $W_{q,\infty}^F$ is determined uniquely by (i) and (ii) and satisfies in addition:

(iii) There exists a twisted A-algebra endomorphism $\mathbf{f}_\omega^{tw}$ of $W_{q,\infty}^F(-)$ with twist $\mathbf{f}_\omega^{tw}\{a\} = \{\sigma(a)\}\mathbf{f}_\omega^{tw}$ for all $a \in A$. This endomorphism is uniquely determined by $w_{q,i}^F \mathbf{f}_\omega^{tw} = w_{q,i+1}^F$ for all $i \in \mathbf{N} \cup \{0\}$.

(iv) If $\mathbf{f}_\omega^{tw}(b_0, b_1, \ldots) = (\hat{b}_0, \hat{b}_1, \ldots)$, then $\hat{b}_i \equiv b_i^q \bmod \omega B$.

(v) $\mathbf{f}_\omega^{tw}(b_0, b_1, \ldots) \equiv (b_0, b_1, \ldots)^q \bmod\{\omega\} W_{q,\infty}^F(B)$.

(vi) $\mathbf{V}_q\colon (b_0, b_1, b_2, \ldots) \mapsto (0, b_0, b_1, b_2, \ldots)$ is an additive endomorphism of $W_{q,\infty}^F(-)$ with the reverse twist $\mathbf{V}_q(\{\sigma(a)\}(b_0, b_1, \ldots)) = \{a\}\mathbf{V}_q(b_0, b_1, \ldots)$.

(vii) $\mathbf{f}_\omega^{tw}\mathbf{V}_q = \{\omega\}$.

(viii) There exists a unique functorial A-algebra functor transformation $\Delta^F\colon W_{q,\infty}^F(-) \to W_{q,\infty}^F(W_{q,\infty}^F(-))$ such that $w_{q,i}^F \Delta^F = (\mathbf{f}_\omega^{tw})^i$ for all $i \in \mathbf{N} \cup \{0\}$.

(ix) This functor transformation Δ^F has in addition the property

$$W_{q,\infty}^F(w_{q,n}^F) \circ \Delta^F = (\mathbf{f}_\omega^{tw})^n$$

■ (25.9.21) **Remark** If A is the ring of integers of a global field K, then there exist for exactly the same reasons as in 25.8 sufficient formal group laws $F(X, Y)$ over A such that $F(X, Y)$ is of the type (25.9.1) over A_v for each finite valuation v of K. For these formal group laws, we have, using (25.9.17), results completely analogous to those of 25.8.

25.10 Twisted formal A-modules

■ (25.10.1) In this subsection A is a discrete valuation ring with uniformizing element π, quotient field K, and residue field k of characteristic $p > 0$. In addition we suppose that there is an endomorphism σ of K and a power q of p such that $\sigma(a) \equiv a^q \bmod \pi A$ for all $a \in A$. The residue field k need not be finite or even perfect.

■ (25.10.2) We have seen in Corollary (21.4.3) that if k is infinite, there are no nontrivial formal A-modules. We have also seen in 25.9 above that the twisted Lubin–Tate formal groups laws admit a functorial A-module structure on the curve functor $\mathscr{C}_q(F; -)$, and it would be tempting to call these twisted formal A-modules of A-height 1 over A—also because over $\hat{A}_{nr}$ they become isomorphic to untwisted Lubin–Tate formal group laws over A. Just what the precise formal definition of a twisted formal A-module should be is not completely clear at the moment. Meanwhile here is a plentiful supply.

■ (25.10.3) **A construction** Let B be any A-algebra that is A-torsion free and which is such that there is an endomorphism $\sigma_B\colon B \otimes_A K \to B \otimes_A K$ such that $\sigma_B | K = \sigma$ and $\sigma_B(b) \equiv b^q \bmod \pi B$ for all $b \in B$. Choose $m \times m$ matrices b_1, b_2, b_3, ... with coefficients in B and let $f(X)$ be any m-tuple of power series in $X = (X_1, X_2, \ldots, X_m)$ such that the following functional equation holds:

$$f(X) - \sum_{i=1}^{\infty} \pi^{-1} b_i (\sigma_B^i)_* f(X^{q^i}) \in B[\![X]\!]^m \tag{25.10.4}$$

and such that $f(X) \equiv X \bmod$ (degree 2).

We now define

$$F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{25.10.5}$$

Then the functional equation lemma says that $F(X, Y)$ is a formal group law over B. Now consider the ring $B[C] = B[C_1, C_2, \ldots]$ and the curve

$$\gamma_C(t) = \sum_{i=1}^{\infty} C_i t^i \quad \text{in} \quad \mathscr{C}(F; B[C]) \tag{25.10.6}$$

Let

$$f(\gamma_C(t)) = \sum_{i=1}^{\infty} x_i t^i, \qquad x_i \in B \otimes_A K[C]$$

For each $b \in B$, we now define

$$\{b\}_F \gamma_C(t) = f^{-1}\left(\sum_{i=1}^{\infty} \sigma_B^{v_q(i)}(b) x_i t^i\right)$$

where $v_q(i) = r$ if $q^r \mid i$ but $q^{r+1} \nmid i$. (One proves in the usual manner that this is indeed a curve in $\mathscr{C}(F; B[C])$.) Now if $\gamma(t) \in \mathscr{C}(F; B')$ where B' is any B-algebra, there is a unique homomorphism $\phi\colon B[C] \to B'$ such that $\phi_*(\gamma_C(t)) = \gamma(t)$ and we define

$$\{b\}_F \gamma(t) = \phi_*(\{b\}_F \gamma_C(t))$$

One now proves easily that this makes $\mathscr{C}(F; -)$ into a functor $\mathbf{Alg}_B \to \mathbf{Mod}_B$ and hence in particular into a functor $\mathbf{Alg}_B \to \mathbf{Mod}_A$, i.e., the $\{a\}_F$ define a functorial A-module structure on $\mathscr{C}(F; -)$.

■ (25.10.7) **Provisional definition of twisted formal A-module** The twisted formal A-modules over B are now:

(i) formal group laws $F(X, Y)$ over B of the type constructed in (25.10.3) together with the functorial A-module structure given by the operators $\{a\}_F$ constructed in (25.10.3);

(ii) the formal group laws $\phi_* F(X, Y)$ together with the induced functorial A-module structure on $\mathscr{C}(\phi_* F; -)$ obtained from a twisted formal A-module of type (i) by means of a base change $\phi\colon B \to B'$ in $\mathbf{Alg}_A$.

So a twisted formal A-module over B is in any case a formal group law over B with a functorial A-module structure on $\mathscr{C}(F; -)$ given by the additive operators $\{a\}_F$ that satisfy

$$\{1\}_F = id, \{a\}_F + \{b\}_F = \{a + b\}_F, \{a\}_F\{b\}_F = \{ab\}_F. \tag{25.10.8}$$

(25.10.9) $\{a\}_F$ preserves the filtration by the $\mathscr{C}^n(F; -)$ of $\mathscr{C}(F; -)$.

(25.10.10) The induced A-module endomorphisms of

$$\mathscr{C}^n(F; B)/\mathscr{C}^{n+1}(F; B) \simeq B^m$$

are given by multiplication with $\sigma^{v_q(n)}(a)$.

(25.10.11) $\mathbf{V}_q\{\sigma a\}_F = \{a\}_F\mathbf{V}_q$, $\mathbf{V}_j\{a\}_F = \{a\}_F\mathbf{V}_j$ if $(j, p) = 1$.

(25.10.12) $\{\sigma a\}_F\mathbf{f}_q = \mathbf{f}_q\{a\}_F$, $\mathbf{f}_j\{a\}_F = \{a\}_F\mathbf{f}_j$ if $(j, p) = 1$.

(25.10.13) $\{a\}_F\langle b\rangle = \langle b\rangle\{a\}_F$ for all $a \in A$, $b \in B$.

■ (25.10.14) **A special case** One particular B that we can take in the constructions of (25.10.3) is the ring $A[S]$ in the indeterminates $S(\mathbf{n}, i)$ and $S_\pi(i, j)$ of (25.4.2). Let $\hat{\sigma}$: $K[S] \to K[S]$ be the unique endomorphism that is σ on K and which takes all the S's to their qth powers. Now let $F_S^{A,\mathrm{tw}}(X, Y)$ be the formal group law over $A[S]$ defined by the formulas (25.4.8), (25.4.9) with σ replaced by $\hat{\sigma}$, and let the operator $\{a\}$ be defined as in (25.10.3).

The author is inclined to conjecture that $F_S^{A,\mathrm{tw}}(X, Y)$ is universal m-dimensional for twisted formal A-modules. In any case all twisted formal A-modules of type (i) with B a ring such that σ_B is an automorphism and such that B is complete in the π-adic topology are obtainable from $F_S^{A,\mathrm{tw}}(X, Y)$ by specialization.

We also note that specialization of the S's gives us a large supply of nonisomorphic twisted formal A-modules over, e.g., A or k.

■ (25.10.15) **q-typification** Let B, σ_B, $F(X, Y)$, $f(X)$ be as in (25.10.3), then

$$\varepsilon_q^F\gamma_C(t) = f^{-1}\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right)$$

is again a curve in $\mathscr{C}(F; B[C])$ and via ϕ_* this defines as usual a projector ε_q^F with image $\mathscr{C}_q(F; -)$. This subfunctor of q-typical curves is stable under the $\{a\}_F$ and we have of course the relations (25.10.11) and (25.10.12) concerning $\mathbf{f}_q$ and $\mathbf{V}_q$.

■ (25.10.16) **The operator $\mathbf{f}_\pi^{\mathrm{tw}}$** There is also again defined an operator $\mathbf{f}_\pi^{\mathrm{tw}}$. For $\gamma_C(t)$ the formula is

$$\mathbf{f}_\pi^{\mathrm{tw}}\gamma_C(t) = f^{-1}\left(\sum_{i=1}^{\infty} \sigma^{v_q(i)}(\pi)x_{qi}\, t^i\right)$$

We have $\mathbf{f}_\pi^{\mathrm{tw}}\mathbf{V}_q = \{\pi\}_F$ and the subfunctor $\mathscr{C}_q(F; -)$ is stable under $\mathbf{f}_\pi^{\mathrm{tw}}$.

25.11 A global ring of ramified Witt vectors: a curiosity

■ (25.11.1) In this section A is the ring of integers of a global field K *of class number* 1. For each finite valuation v of A let $\mathfrak{p}_v$ be the corresponding prime ideal and π_v a generator of $\mathfrak{p}_v$. We write q_v for the number of elements of $A/\mathfrak{p}_v = A/(\pi_v)$ and r_v: $\mathbf{N} \to \mathbf{N} \cup \{0\}$ is defined as $r_v(n) = r$ if $q_v^r \mid n$ but $q_v^{r+1} \nmid n$.

■ (25.11.2) Given the choices made above, we now define a formal group law $F(X, Y)$ as follows. Let

(25.11.3) $$f(X) = X + \sum_{n=1}^{\infty} a_n X^n, \qquad a_n = \prod_v (\pi_v^{-1})^{r_v(n)}$$

where the product is over all finite valuations v. Let $F(X, Y) = f^{-1}(f(X) + f(Y))$. Then $F(X, Y)$ is isomorphic to the formal group law with logarithm $f_v(X) = X + \pi_v^{-1} f(X^{q_v})$ over A_v for all finite valuations v so that $F(X, Y)$ is a global Lubin–Tate formal group law over A.

■(25.11.4) **Ring structure on $\mathscr{C}(F; -)$** Let $F(X, Y)$ be as in (25.11.2) above and let $\gamma_C(t)$, $\gamma_D(t)$ be the two universal curves

$$\gamma_C(t) = \sum^F C_i t^i, \qquad \gamma_D(t) = \sum^F D_i t^i$$

over $A[C; D]$. Consider

$$f(\gamma_C(t)) = \sum x_i t^i, \qquad f(\gamma_D(t)) = \sum y_i t^i$$

and define

$$\gamma_C(t) *_F \gamma_D(t) = f^{-1}\left(\sum_{i=1}^{\infty} a_i^{-1} x_i y_i t^i\right) \tag{25.11.5}$$

then one proves as usual that (25.11.5) is in fact an element of $\mathscr{C}(F; A[C; D])$. Using (25.11.5) as the universal example, one thus defines a ring structure on $\mathscr{C}(F; -)$ with unit element $e_F(t) = f^{-1}(\sum_{i=1}^{\infty} a_n t^n) = t$. Let

$$[a]_F \gamma_C(t) = f^{-1}\left(\sum_{i=1}^{\infty} a x_i t^i\right) = f^{-1}(af(\gamma(t)))$$

then $a \mapsto [a]_F e_F(t) = [a]_F(t)$ defines a ring endomorphism $A \to \mathscr{C}(F; -)$ turning $\mathscr{C}(F; -)$ into an A-algebra functor.

■(25.11.6) We remark that to prove that (25.11.5) is in fact an element of $\mathscr{C}(F; A[C; D])$ it is necessary that $v(a_i^{-1}) \geq r_v(i)$ for all $i \in \mathbf{N}$. This coupled with the fact that $f(X)$ is the logarithm of a global Lubin–Tate formal group law and the desire to have a unit element in $\mathscr{C}(F; A)$ seems to make the hypothesis "class number one" necessary.

■(25.11.7) There seem to be no Frobenius operators on $\mathscr{C}(F; -)$ beyond the usual ones.

■(25.11.8) Let B be an A_v-algebra. Then we have the natural projection $\varepsilon_{q_v}^F$: $\mathscr{C}(F; B) \to \mathscr{C}_{q_v}(F; B)$. Give $\mathscr{C}(F; B)$ the A-algebra structure defined above and $\mathscr{C}_q(F; B)$ the A-algebra structure obtained by restricting the A_v-algebra structure on $\mathscr{C}_q(F; -)$ of Section 25.3. Then $\varepsilon_{q_v}^F$ is not an A-algebra homomorphism but only an A-module homomorphism.

It is possible to remedy this by redefining the A_v-algebra structure on $\mathscr{C}_q(F; -)$ by taking the multiplication $*_{F,c}$ briefly discussed in (25.3.15) with $c = (a_0, a_q, a_{q^2}, \ldots)$. The resulting A-algebra functor $\mathscr{C}_{q,c}(F; -)$ is isomorphic to $\mathscr{C}_q(F; -)$ as an A-algebra functor. But the operator $\mathbf{f}_\pi$ is no longer an A-algebra endomorphism of $\mathscr{C}_{q,c}(F; -)$. This again can be remedied, but then $\mathbf{f}_\pi \mathbf{V}_q = [\pi]_F$ breaks down, unless $\mathbf{V}_q$ is changed also.

These defects together with (25.11.7) and the restriction "class number 1" make the author think that—for the moment at least—the global A-algebra functor $\mathscr{C}(F; -)$ should be seen as a curiosity.

E.3 Bibliographical and Other Notes

(E.3.1) **Notes on Section 18** Theorem (18.3.11) is due to Waterhouse [433] who proves it more generally also for p-divisible groups. The one dimensional case is due to Lubin [263]. The proof of Proposition (18.3.13) follows Fröhlich [144].

Some references for forms and descent are Grothendieck [153], Serre [362, Chapter III] and Knus, Ojanguren [223, Chapter II].

(E.3.2) **Notes on Section 19** The universal p-typical isomorphism theorem (19.2.6) can be found in [170, 173]; cf. also [172, 179]. The classification theorem of one dimensional formal group laws over a separably closed field is Lazard's [251]. The proof given here comes from [174].

(E.3.3) **Notes on Section 20** Corollary (20.2.14) is due to Dieudonné [108], who showed that this endomorphism ring is some order in D_h, and Lubin [263], who showed that it is in fact the maximal order. The proof of this result (via Theorem (20.2.13)) follows Fröhlich [144] quite closely, except for the use of functional equation techniques to obtain a particularly pleasant formal group to work with and to obtain a sufficient supply of endomorphisms.

The results of Sections 20.3 and 20.4 are Honda's [189] and so, mostly, are the proofs. The calculations of [189] (and 20.3, 20.4) bear an extraordinary resemblance to the calculations of [108]. Not an accident of course since the problems studied are the same. Still it might bear taking a closer look at for the starting points (power series versus hyperalgebras) are after all quite different.

The local-global results of Section 20.5 appeared in [176].

Some results much related to those of Honda and also connected to the ideas and results to be discussed in Chapter V below are contained in [141–143].

(E.3.4) **Notes on Section 21** The concept "formal A-module" goes back to Lubin and Tate [264]. Lemma (21.2.4), Proposition (21.2.10), and Proposition (21.3.1) come from Drinfel'd [134]. The explicit universality results of 21.4 have not appeared before, except (21.4.8) in [177].

The techniques of Honda [189] were applied to the study of formal A-modules by Cox [91]. Results (21.8.4), (21.8.6), and (21.8.9) come from this paper.

Theorem (21.8.17) for A of characteristic zero is in Lubin [269]. I know of no explicit reference for the classification theorem (21.9.1). But for A of characteristic zero, it was known, e.g., to Lubin; cf. the introduction of [270].

(E.3.5) **Notes on Section 22** The theorem that two one dimensional formal group laws over $\mathbf{Z}_p$ (or $\mathbf{Z}_{(p)}$, or any ring between) are isomorphic if and only if their reductions over $\mathbf{F}_p$ are isomorphic is due to Honda [188] and Hill [186]. The proof we used comes from [176], as do Examples (22.1.12) and (22.1.15). The corresponding theorem for formal A-modules over A is due to Lubin [269] (for the case that A is of characteristic zero). The proof above is from [177]. The moduli theorem (22.4.16) for

formal group laws is due to Lubin and Tate [265]. The proof in [265] uses a special second cohomology group for formal group laws and as such is closer to the more general theory which we shall discuss in Chapter V, Section 30 than the explicit parameterization given above. This explicit construction is from [174].

(E.3.6) **Notes on Section 23** Proposition (23.2.2) is due to Waterhouse [433] and is valid much more generally for higher dimensional finite height formal groups and also for p-divisible groups. Absolute endomorphism rings were first studied and defined by Lubin [263]. Lemma (23.2.11) was taken from Cox [91]. Proposition (23.2.13) is due to Lubin [271] and Cox [91]. In a way, Proposition (23.2.16) goes back all the way to Lubin and Tate [264] (the construction of formal group laws with large endomorphism rings). The present form was taken from Cox [91]; cf., however, also Lubin [263, 266, 271] and also [176]. Proposition (23.3.1) is due to Lubin and Waterhouse [432, 433], which latter paper also contains more general results.

(E.3.7) **Notes on Section 24** For the treatment of forms and first galois cohomology groups in Section 24.1 I have heavily relied on [144], especially for (24.1.9) and (24.1.11)–(24.1.14). Lemma (24.1.6) follows the proof in Serre [361], which in turn rests on a procedure of Cartier. For some bibliographical references concerning forms and descent, cf. (E.3.1).

Theorem (24.2.16) is due to Koch [225], and our proofs follow that paper closely. The special case of formal laws over the prime field $\mathbf{F}_p$ (classification by Eisenstein polynomials) is due to Hill [186]. Theorem (24.4.2) is due to Serre [364]; our treatment follows Fröhlich [144].

The special case of formal A-modules over k, the residue field of A, of Theorem (24.5.3) (classification by Eisenstein polynomials) can be deduced from the classification theorem (21.8.9). In this way this special case of (24.5.3) is deduced in Cox [91]; cf. also Section 30.4 of Chapter V.

(E.3.8) **Notes on Section 25** Some of the results of Section 25 have been announced in [181]; cf. also [183]. The ring $W^A(-)$ determined by the Witt-type polynomials $Z_0^{q^n} + \pi Z_1^{q^{n-1}} + \cdots + \pi^n Z_n$ has also been described by Ditters [124] (using a line a reasoning very similar to that in Witt's original paper [443]) and by Drinfel'd [135].

(E.3.9) **Note on an "infinite dimensional functional equation lemma"** In Section 25.1 we made use of an infinite dimensional version of the functional equation lemma to prove integrality of the addition polynomials Σ_n^F. This was really unnecessary because by considering only $\Sigma_1^F, \ldots, \Sigma_n^F$ in $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ the situation becomes finite dimensional again.

Still an infinite dimensional version of the functional equation lemma does exist (in fact more than one; the most general one deals with power series over topological rings). One version says that provided all the power series occurring in its formulation satisfy the "monomials have finite support" condition (cf. (9.6.3), Chapter II), then all four statements are also true in the infinite dimensional case.

CHAPTER V

CARTIER–DIEUDONNÉ MODULES

All formal group laws in this chapter will be commutative.

26 Basic Definitions and Reminders. Survey of the Results of Chapter V

26.1 The Cartier–Dieudonné module of a formal group law

Let $F(X, Y)$ be a commutative formal group law over a ring A of dimension n, say. Let $\mathscr{C}(F; A)$ be the abelian group of curves of $F(X, Y)$ with coefficients in A. Recall that the elements of $\mathscr{C}(F; A)$ are n-tuples of power series $\gamma(t)$ in one variable t with coefficients in A such that $\gamma(0) = 0$, that the addition is defined by $\gamma(t) +_F \delta(t) = F(\gamma(t), \delta(t))$, and that $\mathscr{C}(F; A)$ is a complete Hausdorff topological group with the topology defined by the subgroups $\mathscr{C}^n(F; A)$ consisting of all curves $\gamma(t)$ such that $\gamma(t) \equiv 0 \bmod t^n$, $n \in \mathbf{N}$. We also defined a number of operators on $\mathscr{C}(F; A)$, viz. operators $\mathbf{f}_n$ and $\mathbf{V}_n$ for all $n \in \mathbf{N}$, and operators $\langle a \rangle$ for all $a \in A$. The defining relations were

$$\langle a \rangle \gamma(t) = \gamma(at), \qquad \mathbf{V}_n \gamma(t) = \gamma(t^n)$$

$$\mathbf{f}_n \gamma(t) = \gamma(\zeta_n t^{1/n}) +_F \cdots +_F \gamma(\zeta_n^n t^{1/n})$$

where ζ_n is a primitive nth root of unity, and where the last formula must be interpreted with some care in case A is not a torsion free ring. There are a number of relations between these operators; these were listed and derived in Section 16.2 of Chapter III (cf. also (27.2.11) below).

One now defines the *Carter–Dieudonné module* of the formal group law $F(X, Y)$ over A as the topological abelian group $\mathscr{C}(F; A)$ with the continuous operators $\mathbf{f}_n$, $\langle a \rangle$, $\mathbf{V}_n$. This defines a functor $\mathscr{C}(-; A)$ on $\mathbf{FG}_A$, the category of formal group laws over A, to a certain category of abelian groups. These groups $\mathscr{C}(F; A)$ have the properties:

(26.1.1) $\mathscr{C}(F; A)$ is filtered by subgroups $\mathscr{C}(F; A) = \mathscr{C}^1(F; A) \supset \cdots \supset$

$\mathscr{C}^n(F; A) \supset \cdots$ and $\mathscr{C}(F; A)$ is complete and Hausdorff in the topology defined by the $\mathscr{C}^n(F; A)$.

(26.1.2) There are continuous additive operators $\mathbf{V}_n$, $\mathbf{f}_n$, and $\langle a\rangle$ on $\mathscr{C}(F; A)$ for all $n \in \mathbf{N}$, $a \in A$ that satisfy the relations (16.2.1)–(16.2.9).

(26.1.3) The operators $\mathbf{V}_m$ are injective, they map $\mathscr{C}^n(F; A)$ into $\mathscr{C}^{nm}(F; A)$ and induce isomorphisms

$$\mathscr{C}^n(F; A)/\mathscr{C}^{n+1}(F; A) \simeq \mathscr{C}^{nm}(F; A)/\mathscr{C}^{nm+1}(F; A)$$

(26.1.4) $\mathscr{C}^1(F; A)/\mathscr{C}^2(F; A)$ is a free A-module (the A-module structure being induced by the operators $\langle a\rangle$).

Cartier's second and third theorems together now say:

■ (26.1.5) **Theorem** The functor $F(X, Y) \mapsto \mathscr{C}(F; A)$ is an equivalence of categories from the category of formal group laws over A onto the category of abelian groups with the properties (26.1.1)–(26.1.4).

One can collect the operators $\mathbf{V}_n$, $\mathbf{f}_n$, $\langle a\rangle$ in one ring $\mathrm{Cart}(A)$ whose elements are all formal sums of the form

$$\sum_{m,n} \mathbf{V}_m \langle a_{mn}\rangle \mathbf{f}_n \tag{26.1.6}$$

with for every $m \in \mathbf{N}$ only finitely many n such that $a_{m,n} \neq 0$. With (16.2.1)–(16.2.9) as calculation rules $\mathrm{Cart}(A)$ is now completely described. In passing we note that $a = (a_1, a_2, \ldots) \mapsto \sum_n \mathbf{V}_n \langle a\rangle \mathbf{f}_n$ defines a ring embedding of the ring of Witt vectors $W(A)$ into $\mathrm{Cart}(A)$.

The abelian groups $\mathscr{C}(F; A)$ can now be considered as $\mathrm{Cart}(A)$-modules and even as topological $\mathrm{Cart}(A)$-modules where we give $\mathrm{Cart}(A)$ the topology defined by the right ideals $\mathfrak{A}_l$ consisting of those elements (26.1.6) for which $a_{m,n} = 0$ for $m \leq l$.

One can now restate Theorem (26.1.5) in more fanciful language as an equivalence of categories between $\mathbf{FG}_A$ and a certain kind of topological $\mathrm{Cart}(A)$-modules, so called *reduced* $\mathrm{Cart}(A)$-modules. These are defined as follows:

■ (26.1.7) **Definition** A topological $\mathrm{Cart}(A)$-module $\mathscr{C}$ is called reduced if the following four conditions hold:

(i) If $(x_i)_{i \in J}$ is a set of elements in $\mathrm{Cart}(A)$ converging to zero (for the filter of complements of finite sets) and $(\gamma_i)_{i \in J}$ is any set of elements of $\mathscr{C}$, then $\sum_{i \in J} x_i \gamma_i$ converges in $\mathscr{C}$.

(ii) For each $n \in \mathbf{N}$, let $\mathscr{C}^n$ be the closure of the sum of all the subgroups $\mathbf{V}_i\mathscr{C}$ of $\mathscr{C}$ for $i \geq n$. Then the topology of $\mathscr{C}$ is the same as the topology defined by the $\mathscr{C}^n$.

(iii) $\mathbf{V}_m: \mathscr{C}^1 = \mathscr{C} \to \mathscr{C}^m$ induces a bijection $\mathscr{C}/\mathscr{C}^2 \xrightarrow{\sim} \mathscr{C}^m/\mathscr{C}^{m+1}$.

(iv) $\mathscr{C}/\mathscr{C}^2$ is a free A-module.

With this terminology Theorem (26.1.5) can be restated as

■ (26.1.8) **Theorem** The functor $F \mapsto \mathscr{C}(F; A)$ is an equivalence of categories between $\mathbf{FG}_A$ and the category of reduced Cart(A)-modules (with continuous Cart(A)-module morphisms as morphisms).

To prove Theorem (26.1.5) one makes essential use of the formal group law $\hat{W}(X, Y)$ of Witt vectors as follows. Let $\gamma_w(t)$ be the curve $(t, 0, 0, \ldots)$ in $\hat{W}(X, Y)$ over A. (NB do not confuse $\gamma_w(t)$ with the element $(t, 0, 0, \ldots) \in W(A[\![t]\!])$.) Then one has

■ (26.1.9) **Theorem** For every curve $\gamma(t) \in \mathscr{C}(F; A)$, where $F(X, Y)$ is a commutative formal group law over A, there exists a unique homomorphism of formal group laws $\alpha_\gamma(X)$: $\hat{W}(X, Y) \to F(X, Y)$ such that $(\alpha_\gamma)_* \gamma_w(t) = \gamma(t)$.

In other words $\hat{W}(X, Y)$ represents the functor $F \mapsto \mathscr{C}(F; A)$.

Thus, in order to prove Theorem (26.1.5), even for finite dimensional formal group laws only, one unavoidably meets infinite dimensional formal group laws, albeit only very nice ones like $\hat{W}(X, Y)$. As a matter of fact, the proof of Theorem (26.1.5) given below is complete only for the finite dimensional case; to do the existence proof given below also for infinite dimensional formal group laws one needs the generalities that we already briefly discussed in Section 9.6 of Chapter II.

26.2 Cartier–Dieudonné theory over $\mathbf{Z}_{(p)}$-algebras

■ (26.2.1) Now suppose that we are studying formal group laws over a ring A that is a $\mathbf{Z}_{(p)}$-algebra, i.e., a ring A in which all prime numbers except possibly p are invertible. In this case the theory outlined in 26.1 simplifies a good deal. This is due to the following facts:

(i) The topological groups of curves $\mathscr{C}(F; A)$ splits as a direct sum $\mathscr{C}(F; A) \simeq \oplus_{I(p)} \mathscr{C}_p(F; A)$, where $I(p) = \{n \in \mathbf{N} \mid (p, n) = 1\}$ and where $\mathscr{C}_p(F; A)$ is the topological group of p-typical curves (Proposition (16.4.18)).

(ii) The ring Cart(A) "is" an $I(p) \times I(p)$ matrix ring with entries in a much smaller quotient ring $\mathrm{Cart}_p(A)$ of Cart(A), whose elements are all formal expressions of the form $\sum_{n,m} \mathbf{V}_p^n \langle a_{n,m} \rangle \mathbf{f}_p^m$. Moreover, this decomposition and the one mentioned just above in (i) are compatible.

(iii) $\mathrm{Cart}_p(A)$ is a much nicer ring than Cart(A).

The calculation rules for $\mathrm{Cart}_p(A)$ are obtained from those of Cart(A) by setting all $\mathbf{V}_n$, $\mathbf{f}_n$ zero for $(n, p) = 1$. A reduced $\mathrm{Cart}_p(A)$ module is now:

■ (26.2.2) **Definition** A reduced $\mathrm{Cart}_p(A)$-module is a module $\mathscr{C}$ over $\mathrm{Cart}_p(A)$ such that:

(i) $\mathscr{C}$ is complete and Hausdorff in the topology defined by the subgroups $\mathbf{V}_p^n \mathscr{C} = \mathscr{C}^{(n)}$, i.e., $\mathscr{C} = \varprojlim \mathscr{C}/\mathscr{C}^{(n)}$;

(ii) $\mathbf{V}_p$ is injective;
(iii) $\mathscr{C}/\mathbf{V}_p\mathscr{C}$ is a free A-module.

The one prime number version of the equivalence of categories Theorem (26.1.5) is now

■ (26.2.3) **Theorem** Let A be a $\mathbf{Z}_{(p)}$-algebra. Then $F \mapsto \mathscr{C}_p(F; A)$ is an equivalence of categories between $\mathbf{FG}_A$ and the category of reduced $\mathrm{Cart}_p(A)$-modules.

There is also a one prime version of the representation theorem (26.1.9). It says that the functor $F \mapsto \mathscr{C}_p(-; A)$ is representable by $\hat{W}_{p^\infty}(X, Y)$.

One way to prove Theorem (26.2.3) is to use the decomposition results (i) and (ii) of (26.2.1) to deduce Theorem (26.2.3) from Theorem (26.1.5). And in fact this is precisely what we do to prove that the functor $\mathscr{C}_p(-; A)$ is fully faithful. The existence part, on the other hand, which in the global case is by far the hardest to prove, is almost a triviality in this one prime number case. It is immediate from Definition (26.2.2) that every element γ in $\mathscr{C}$ can be written as a unique sum

$$\gamma = \sum_{n=0}^{\infty} \sum_{i=1}^{m} \mathbf{V}_p^n \langle a_{n,i} \rangle \delta_i$$

where $m = \dim_A(\mathscr{C}/\mathbf{V}_p\mathscr{C})$ and where $\delta_1 \ldots, \delta_m$ in $\mathscr{C}$ are such that their classes mod $\mathbf{V}_p\mathscr{C}$ are a basis for $\mathscr{C}/\mathbf{V}_p\mathscr{C}$. In particular we have expressions

$$\mathbf{f}_p \delta_i = \sum_{n=0}^{\infty} \sum_{j=1}^{m} \mathbf{V}_p^n \langle c(n, j, i) \rangle \delta_j$$

Now let $F_V(X, Y)$ over $\mathbf{Z}[V]$ be the universal p-typical m-dimensional formal group law of Section 10.3, Chapter II. Substitute $c(n, i, j)$ for $V_{n+1}(i, j)$; an elementary calculation shows that the module of p-typical curves of the resulting formal group law is precisely $\mathscr{C}$.

26.3 Cartier–Dieudonné theory for formal A-modules

■ (26.3.1) Now let A be a discrete valuation ring with finite residue field k of q-elements. The ring A may be either of characteristic zero or of characteristic $p = \mathrm{char}(k) > 0$. In this case there is a theory of Cartier–Dieudonné modules for formal A-modules that is completely parallel to the one discussed above for formal group laws over $\mathbf{Z}_{(p)}$-algebras, i.e., formal $\mathbf{Z}_{(p)}$-modules. We choose a fixed uniformizing element π of A.

The role of $\hat{W}_{p^\infty}$ is now played by $\hat{W}^A_{q,\infty}$ and instead of $\mathrm{Cart}_p(A)$ we have $\mathrm{Cart}_A(B)$, where B is in $\mathbf{Alg}_A$, which consists of all expressions

$$\sum_{n,m=0}^{\infty} \mathbf{V}_q^n \langle b_{n,m} \rangle \mathbf{f}_\pi^m$$

with, for all n, $b_{n,m} = 0$ for all but finitely many m. Here $\mathbf{f}_\pi$ is the Frobenius operator introduced and studied in Section 25.5, Chapter IV. The calculation rules for $\mathrm{Cart}_A(B)$ are similar to the ones of $\mathrm{Cart}_p(B)$.

The role of $\mathscr{C}_p(-; B)$ is now taken over by the group of q-typical curves (cf. 25.2). We recall that if B is A-torsion free, a curve $\gamma(t)$ in $\mathscr{C}(F; B)$ is q-typical iff

$$f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i}, \qquad x_i \in (B \otimes_A K)^m$$

where K is the quotient field of A.

The definition of a reduced $\mathrm{Cart}_A(B)$-module is obtained from (26.2.2) by replacing $\mathrm{Cart}_p(A)$ by $\mathrm{Cart}_A(B)$, $\mathbf{V}_p$ by $\mathbf{V}_q$ and A by B everywhere.

Thus in this case we find an equivalence of categories $\mathbf{FG}_B^A \simeq$ (category of reduced $\mathrm{Cart}_A(B)$-modules) and $F \mapsto \mathscr{C}_q(F; B)$ is representable by $\hat{W}_{q,\infty}^A(X, Y)$.

■ (26.3.2) **The A-module structure** Let $F(X, Y) \in \mathbf{FG}_B^A$ be a formal A-module over B. Then by what was said above $\mathscr{C}_q(F; B)$ is classifying, and the natural operators on $\mathscr{C}_q(F; B)$ are $\mathbf{V}_q$, $\mathbf{f}_\pi$, and the operators $\langle b \rangle$ for $b \in B$. One may wonder how the A-module structure on $\mathscr{C}_q(F; B)$ that is induced by the $\rho_F(a)$ is hidden in here.

To this end we first recall that $W_{q,\infty}^A(B)$ is an A-algebra with structural homomorphism given by

$$A \to W_{q,\infty}^A(B), \qquad a \mapsto (\Omega_0(a), \Omega_1(a), \Omega_2(a), \ldots)$$

$$w_{q,n}^A(\Omega(a)) = a \qquad \text{for all} \quad n \in \mathbf{N} \cup \{0\}$$

Second, $(b_0, b_1, b_2, \ldots) \mapsto \sum_{n=0}^{\infty} \mathbf{V}_q^n \langle b_n \rangle \mathbf{f}_\pi^n$ is an injective ring homomorphism $W_{q,\infty}^A(B) \to \mathrm{Cart}_A(B)$. The composite of these two homomorphism gives the action of A on $\mathscr{C}_q(F; B)$.

26.4 Classification up to isogeny over an algebraically closed field

Now let $F(X, Y)$ be a formal group law, or a formal A-module, where A is as in 26.3, over an algebraically closed field l of characteristic $p > 0$. We shall describe the results below only for formal A-modules; the corresponding results for formal group laws follow by taking $A = \mathbf{Z}_{(p)}$ because l is a $\mathbf{Z}_{(p)}$-algebra.

■ (26.4.1) **A-Height** Consider $\mathscr{C} = \mathscr{C}_q(F; B)$. Then $\mathscr{C}/[\pi]\mathscr{C} = \mathscr{C}/\mathbf{f}_\pi \mathbf{V}_q \mathscr{C}$ is a vector space over l, with the vector space structure induced by the operators $\langle b \rangle$, $b \in l$. We define the A-height of $F(X, Y)$ as $\dim_l(\mathscr{C}/[\pi]\mathscr{C})$. It turns out that this agrees with the definitions we have given before in the one dimensional cases (cf. Section 18.3 and (21.8.2) of Chapter IV).

Since $\dim F = \dim_l(\mathscr{C}/\mathbf{V}_q\mathscr{C})$, one also has that always $A\text{-ht}(F(X, Y)) \geq \dim(F(X, Y))$, so that formal A-modules of A-height 1 are necessarily of dimension 1.

■ (26.4.2) **The Dieudonné ring $\mathbf{D}^A(l)$** We define $\mathbf{D}^A(l)$ as the over algebra of $W^A_{q.\infty}(l)$ generated by two symbols $\mathbf{f}_\pi$ and $\mathbf{V}_q$ subject to the relations $\mathbf{f}_\pi \mathbf{V}_q = \mathbf{V}_q \mathbf{f}_\pi = [\pi]$, $x\mathbf{V}_q = \mathbf{V}_q \tau^A(x)$, $\mathbf{f}_\pi y = \tau^A(y)\mathbf{f}$ where τ^A is the Frobenius automorphism of $W^A_{q.\infty}(l)$. This ring is naturally a dense subring of $\mathrm{Cart}_A(l)$; and since $\mathscr{C}_q(F; L)$ is complete, the study of reduced $\mathrm{Cart}_A(l)$-modules is equivalent to the study of reduced $\mathbf{D}^A(l)$ modules.

■ (26.4.3) **Classification up to isogeny** Now let $F(X, Y) \in \mathbf{FG}^A_l$ be a formal A-module of finite height. Then $\mathscr{C}_q(F; l)$ is a free $W^A_{q.\infty}(l)$-module of finite rank $h = A\text{-ht}(F(X, Y))$.

"Localize" $\mathbf{D}^A(l)$ with respect to $\mathbf{V}_q$ to obtain a ring of twisted Laurent series in $\mathbf{V}$ with coefficients in the ramified Witt vector ring $W^A_{q.\infty}(l)$. $\mathscr{C}_q(F; l)$ is a torsion module over this ring $\mathbf{D}^A_{\mathbf{V}}(l)$ if $A\text{-ht}(F(X, Y)) < \infty$ and it turns out that one can classify all finitely generated torsion modules over $\mathbf{D}^A_{\mathbf{V}}(l)$ by means of a standard technique which goes back all the way to Dieudonné's paper [108].

It turns out that "$\mathscr{C}_q(F; l)$ and $\mathscr{C}_q(G; l)$ become isomorphic over $\mathbf{D}^A_{\mathbf{V}}(l)$" is the same thing as "$F(X, Y)$ and $G(X, Y)$ are isogenous as formal A-modules over l." Here *isogenous* is the weakest equivalence relation that identifies two formal A-modules over l that are of the same dimension and between which there exists a formal A-module homomorphism with finite kernel. The resulting classification theorem is:

■ (26.4.4) **Theorem** Let l be an algebraically closed extension field of k. Then every finite dimensional formal A-module over l is isogenous to a direct sum of certain formal A-modules $G^A_{n.m}(X, Y)$, $1 \le n \le \infty$, $0 \le m \le \infty$, $(n, m) = 1$. This decomposition is unique up to isogeny.

Here $G^A_{1.0}(X, Y)$ is the (unique) formal A-module of A-height 1 over l, the $G^A_{n.\infty}(X, Y)$ are the obvious n-dimensional quotients of $\hat{W}^A_{q.\infty}(X, Y)$ and the $G^A_{n.m}(X, Y)$ for $n, m \in \mathbf{N}$, $(n, m) = 1$ are certain simple formal A-modules of dimension n and A-height $n + m$.

26.5 "Le tapis de Cartier"

In Section 30 we shall take up again the question of reducing and lifting formal A-modules and formal group laws. In Section 30 we treat only the case of formal A-modules explicitly, the case of formal group laws being obtained by considering them as formal $\mathbf{Z}_{(p)}$-modules. By way of contrast we shall here describe the results for formal group laws only.

■ (26.5.1) **The setting** Let k be a perfect field and $A = W_{p^\infty}(k)$ the ring of Witt vectors for the prime p over k. Let σ be the Frobenius automorphism of A, let K be the quotient field of A. We take p as a uniformizing element of K. Let M be a free module of finite rank h over A together with a semilinear endomorphism η: $M \to M$ (i.e., $\eta(am) = \sigma(a)\eta(m)$ and η is additive) and a

σ^{-1}-semilinear endomorphism ζ: $M \to M$ such that $\eta\zeta = \zeta\eta = p$ and $\zeta^r M \subset pM$ for r sufficiently large. Finally, let N be a free finite rank submodule of M such that $N + pM = \zeta M$ and such that M/N is also free.

■ (26.5.2) **The constructions** Given (M, η) as in (26.5.1), one constructs generalized Lubin–Tate formal group laws $G(M, \eta)(X, Y)$ as in Section 13.2 of Chapter II. We recall that $G(M, \eta)(X, Y)$ is the formal group law over A with logarithm

$$g(M, \eta)(X) = X + p^{-1}D(\eta)\sigma_* g(M, \eta)(X^p)$$

When $D(\eta)$ is the matrix of η with respect to some chosen basis of M over A. (The isomorphism class of $G(M, \eta)(X, Y)$ does not depend on this choice, but the formal group *law* itself does depend on it.) Identifying M with A^h via the same basis and thus identifying M with the Lie algebra of $G(M, \eta)(X, Y)$, one finds the following description of $\mathscr{C}_p(G(M, \eta); A)$ or rather of $g(M, \eta)$ $(\mathscr{C}_p(G(M, \eta); A))$. This is the subgroup of the additive group $t(K \otimes_A M)[\![t]\!]$ consisting of all power series

$$\sum_{i=0}^{\infty} x_i t^{p^i}, \qquad x_i \in M \otimes_A K$$

such that $x_0 \in M$ and $x_i \equiv p^{-1}\eta(x_{i-1}) \bmod M$ for all $i \in \mathbf{N}$.

There is a canonical map β_0: $M \to \mathscr{C}_p(G(M, \eta); A)$ defined as follows

$$g(M, \eta)(\beta_0(x)) = \sum_{i=0}^{\infty} p^{-i}\eta^i(x)t^{p^i} \tag{26.5.3}$$

This map has the following properties:

$$\beta_0(\eta x) = \mathbf{f}_p \beta_0(x); \tag{26.5.4}$$

(26.5.5) β_0 is A-linear, where $\mathscr{C}_p(G(M, \eta); A)$ is seen as an A-module via the Artin–Hasse exponential

$$\Delta_A: A \to W_{p^\infty}(A) \subset \mathrm{Cart}_p(A)$$

Now let N be a submodule of M as in (26.5.1). Then $N \subset \zeta M$. For each $x \in N$, let $y \in M$ be such that $\zeta y = x$ (NB ζ is injective). Then $g(M, \eta)^{-1}(xt) = \beta_0(x) - \mathbf{V}_p\beta_0(y)$ (subtraction in the group $\mathscr{C}_p(G(M, \eta); A)$), and it follows that the additive formal group law $N^+(X, Y)$ with Lie algebra N is canonically (via β_0) a subformal group law of $G(M, \eta)(X, Y)$. The quotient exists as a formal group law, and we find an exact sequence with additive Kernel

$$0 \to N^+(X, Y) \to G(M, \eta)(X, Y) \to G(X, Y) \to 0 \tag{26.5.6}$$

One now has the following universality properties:

■ (26.5.7) **Theorem** There is a one-one functorial correspondence between

homomorphisms $G(M, \eta)(X, Y) \to H(X, Y)$ and maps $\beta\colon M \to \mathscr{C}_p(H; A)$ such that (the analogues of) (26.5.4) and (26.5.5) hold. (The correspondence is given by the map β_0.)

■ (26.5.8) **Theorem** (26.5.6) is the universal extension with additive kernel of $G(X, Y)$. That is, for every exact sequence of formal group laws

$$0 \to R^+(X, Y) \to H(X, Y) \to M_1(X, Y) \to 0$$

there is a unique homomorphism $N^+(X, Y) \to R^+(X, Y)$ such that this sequence is obtained from (26.5.6) by pushout.

■ (26.5.9) **Theorem** The composed map

$$M \to \mathscr{C}_p(G(M, \eta); A) \to \mathscr{C}_p(G; A) \to \mathscr{C}_p(\bar{G}; k)$$

where the last map is reducing mod pA, is an isomorphism which takes η to $\mathbf{f}_p$ and ζ to $\mathbf{V}_p$.

(We have encountered similar isomorphisms before; cf. Theorem (15.4.11) of Chapter III and Theorem (25.3.30) of Chapter IV.)

■ (26.5.10) We now turn our attention to the lifting of formal group laws. Let $\Gamma(X, Y)$ be a formal group law of finite height h over k. Then $\mathscr{C}_p(\Gamma; k)$ is a free module of rank h over $W_{p^\infty}(k) = A$ with a σ-semilinear endomorphism $\mathbf{f}_p$ and a σ^{-1}-semilinear endomorphism $\mathbf{V}_p$. We now take $M = \mathscr{C}_p(\Gamma; k), \eta = \mathbf{f}_p, \zeta = \mathbf{V}_p$. Then all the hypotheses of (26.5.1) concerning (M, η, ζ) are satisfied. Take any free submodule N of M such that $N + pM = \zeta M$ and such that M/N is free. Now carry out the constructions of (26.5.2). Theorem (26.5.9) says that the $G(X, Y)$ thus obtained is a lift of $\Gamma(X, Y)$.

Conversely, given a lift $G(X, Y)$ of $\Gamma(X, Y)$, one proves that there is a unique map $\beta\colon M \to \mathscr{C}_p(G; A)$ that is A-linear (via $A \to W_{p^\infty}(A) \subset \mathrm{Cart}_p(A)$ again) and such that $\beta \circ \eta = \mathbf{f}_p \circ \beta$. Let $\beta(X)\colon G(M, \eta)(X, Y) \to G(X, Y)$ be the corresponding homomorphism of formal group laws over A. Then $\mathrm{Ker}(\beta(X))$ turns out to be an additive formal group law with Lie algebra $N = \mathrm{Ker}(\mathrm{Lie}(\beta))$, a submodule of M, such that $N + pM = \zeta M$ (and M/N free).

Thus one obtains the following picture:

(a) The middle formal group law $\tilde{G}(X, Y)$ of the universal extension with additive kernel of a lift $G(X, Y)$ over $W_{p^\infty}(k)$ of $\Gamma(X, Y)$ over k depends only on $\Gamma(X, Y)$ and not on the particular lift $G(X, Y)$.

(b) The Lie algebra of $\tilde{G}(X, Y)$ is the Cartier–Dieudonné module $\mathscr{C}_p(\Gamma; k)$.

(c) The various lifts of $\Gamma(X, Y)$ to a formal group law $G(X, Y)$ over $W_{p^\infty}(k)$ correspond to the various ways of lifting the exact sequence

$$0 \to M/\mathbf{f}_p M \xrightarrow{\mathbf{V}_p} M/[p]M \to M/\mathbf{V}_p M \to 0$$

where $M = \mathscr{C}_p(\Gamma; k)$, to an exact sequence (26.5.6).

This is a picture, which, to quote Cartier quoting Grothendieck (cf. [66, p. 223]) "is only a small subpart of Grothendieck's conjectures concerning cristalline cohomology."

■ (26.5.11) **The case of formal A-modules** There is a completely parallel picture in the case of formal A-modules where A is a discrete valuation ring (of characteristic p or of characteristic zero) with finite residue field of q elements. Basically the results are obtained by the transcribing rules:

$$\mathscr{C}_p(-;-) \mapsto \mathscr{C}_q(-;-), \qquad \mathbf{f}_p \mapsto \mathbf{f}_\pi, \qquad \mathbf{V}_p \mapsto \mathbf{V}_q$$

$$N + pM \mapsto N + \pi M, \qquad \zeta\eta = \eta\zeta = p \mapsto \zeta\eta = \eta\zeta = \pi$$

27 Cartier–Dieudonné Modules for Formal Group Laws

In this section all formal group laws will be over one fixed ring A and all curves and power series in one or more variables will have coefficients in A, unless otherwise specified.

In principle, formal group laws may be infinite dimensional in this section. But we shall give complete proofs of the main theorems only in the finite dimensional case.

27.1 Cartier's first theorem

■ (27.1.1) **Morphisms** Let I and J be two index sets. A homomorphism between an (infinite dimensional) formal group law with index set I (cf. Chapter II, Section 9.6) and an (infinite dimensional) formal group law with index set J is of course some set $\alpha(X) = (\alpha_j(X))_{j \in J}$, indexed by J, of power series in the X_i, $i \in I$. That is,

(27.1.2) $$\alpha_j(X) = \sum_{\mathbf{n}} c_{j,\mathbf{n}} X^{\mathbf{n}}$$

where $\mathbf{n}$ runs over all functions $\mathbf{n}\colon I \to \mathbf{N} \cup \{0\}$ with finite support, i.e., $\{i \in I \mid \mathbf{n}(i) \neq 0\}$ is a finite set, and where $X^{\mathbf{n}}$ is short for the product $\prod_i X^{\mathbf{n}(i)}$ where i runs over all $i \in I$ for which $\mathbf{n}(i) \neq 0$. Functions $\mathbf{n}\colon I \to \mathbf{N} \cup \{0\}$ with finite support will (still) be called multi-indices. Now we have already seen in Section 9.6 of Chapter II that in general if $\alpha(X)$ is a J-tuple of power series in the $(X_i)_{i \in I}$ and $\beta(Y)$ is a J-tuple of power series in the variables Y_k, $k \in K$, and I, J, and K are possibly infinite, then $\alpha(\beta(Y))$ need not be defined. We have also seen how to avoid this. In complete analogy with the restriction introduced there we define:

■ (27.1.3) **Definitions** Let I, J be two possibly infinite index sets. Then we define $\mathrm{Mor}(I, J)$ as the set of J-tuples of power series $\alpha(X) = (\alpha_j(X))_{j \in J}$ such that for every multi-index $\mathbf{n}\colon I \to \mathbf{N} \cup \{0\}$ there are only finitely many j such

that $c_{j,\mathbf{n}} \neq 0$. We shall refer to this condition as the "monomials have compact support" condition. If J is finite, this is no restriction at all.

We shall write $\mathrm{Mor}(n, m)$ for $\mathrm{Mor}(I, J)$ if $I = \{1, 2, \ldots, n\}$, $J = \{1, 2, \ldots, m\}$.

Now let $F(X, Y)$ be a formal group law with index set I and $G(X, Y)$ a formal group law with index set J. A homomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is now an element $\alpha(X) \in \mathrm{Mor}(I, J)$ such that $\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$, and we note that this last condition makes sense precisely because of the "monomials have compact support" condition on $\alpha(X)$, $F(X, Y)$, and $G(X, Y)$.

■ (27.1.4) **Topology on** $\mathrm{Mor}(I, J)$ We give the set $\mathrm{Mor}(I, J)$ a kind of compact open topology. Let $\alpha(X) \in \mathrm{Mor}(I, J)$, then the open neighborhoods of $\alpha(X)$ are defined by pairs (n, κ) where $n \in \mathbf{N}$ and κ is a finite subset of I, and these are defined as

$$U(\alpha(X); n, \kappa) = \{\beta(X) \in \mathrm{Mor}(I, J) \mid \beta(X) \equiv \alpha(X) \mod(X_i, i \notin \kappa; \text{degree } n)\}$$

So if I is finite, of size m say, the topology is defined by the open neighborhoods

$$\{\beta(X) \in \mathrm{Mor}(m, J) \mid \beta(X) \equiv \alpha(X) \mod \text{degree } n\}$$

and if I is infinite, then $\beta_n(X)$, $n \in \mathbf{N}$, converges to $\alpha(X)$ if and only if $\beta_n(X)$ converges to $\alpha(X)$ for all finite (i.e., compact) subsets of I.

■ (27.1.5) **Group structures on** $\mathrm{Mor}(I, J)$ Let $F(X, Y)$ be a (possibly infinite dimensional) formal group law with index set J. And let $\alpha(X), \beta(X) \in \mathrm{Mor}(I, J)$, then $F(\alpha(X), \beta(X))$ makes sense and defines a new element of $\mathrm{Mor}(I, J)$, turning $\mathrm{Mor}(I, J)$ into an abelian topological group.

■ (27.1.6) **An example** Consider the formal group law $\hat{W}(X, Y)$ defined by the Witt addition polynomials $\Sigma_1, \Sigma_2, \ldots$ of Chapter III, Section (17.1.18). We have already seen (Chapter III, Lemma (17.4.9) that if $a = (a_1, a_2, a_3, \ldots)$, $b = (b_1, b_2, \ldots)$ are two sequences of elements of a ring R and for all $i \in \mathbf{N}$, $a_i = 0$ or $b_i = 0$, then $\Sigma_i(a, b) = a_i + b_i$ for all $i \in \mathbf{N}$. Now let $\delta_i(t) \in \mathrm{Mor}(1, \mathbf{N})$ be the $\mathbf{N}$-tuple of power series $(\delta_i)_j(t) = 0$ if $j \neq i$, $(\delta_i)_i(t) = t$. We can consider $\delta_i(X_i)$ as an element of $\mathrm{Mor}(\mathbf{N}, \mathbf{N})$; in the topological group structure defined by $\hat{W}(X, Y)$ we then have

$$(X_1, X_2, X_3, \ldots) = \sum_{i=1}^{\infty}{}^{\hat{W}} \delta_i(X_i) \tag{27.1.7}$$

where the sum on the right converges in the (compact open) topology of $\mathrm{Mor}(\mathbf{N}, \mathbf{N})$. (Note that the element of $\mathrm{Mor}(\mathbf{N}, \mathbf{N})$ on the left is the identity endomorphism of $\hat{W}(X, Y)$.)

■ (27.1.8) **Curves** Let again $F(X, Y)$ be a (possibly infinite dimensional) formal group law with index set I. Then the set of curves $\mathscr{C}(F; A)$ is simply $\mathrm{Mor}(1, I)$ which we give the topology defined in (27.1.4) and the group struc-

ture discussed in (27.1.5). The set of all curves that are $\equiv 0$ mod degree n is then an open subgroup $\mathscr{C}^n(F; A)$ of $\mathscr{C}(F; A)$ and the topology of $\mathscr{C}(F; A)$ is the topology defined by these subgroups. Moreover, $\mathscr{C}(F; A)$ is complete in this topology. All this is exactly as in the finite dimensional case.

The operators $\langle a\rangle$, $a \in A$, $\mathbf{V}_m$ and $\mathbf{f}_m$, $m \in \mathbf{N}$, on $\mathscr{C}(F; A)$ are defined exactly as in the finite dimensional case. (The only thing to check is that one stays in Mor(1, I), which is a triviality.) The operators $\langle a\rangle$, $\mathbf{V}_m$, and $\mathbf{f}_m$ are all continuous, and $\mathbf{V}_m$ maps $\mathscr{C}^n(F; A)$ into $\mathscr{C}^{mn}(F; A)$; the induced homomorphisms

$$\mathbf{V}_m\colon \mathscr{C}^n(F; A)/\mathscr{C}^{n+1}(F; A) \to \mathscr{C}^{mn}(F; A)/\mathscr{C}^{mn+1}(F; A)$$

are isomorphisms.

■ (27.1.9) **Lemma** Let $\alpha(X) \in \mathrm{Mor}(I, J)$. Then $\alpha_*\colon \beta(X) \mapsto \alpha(\beta(X))$ from $\mathrm{Mor}(K, I)$ to $\mathrm{Mor}(K, J)$ is a continuous map. In particular, if $\alpha(X)$ is a homomorphism of formal group laws $F(X, Y) \to G(X, Y)$, then $\alpha(X)$ induces a continuous homomorphism $\alpha_*\colon \mathscr{C}(F; A) \to \mathscr{C}(G; A)$. Moreover, α_* commutes with the operators $\mathbf{V}_m$ and $\langle a\rangle$ for all $m \in \mathbf{N}$, $a \in A$ (in any case) and also with the operators $\mathbf{f}_m$ if $\alpha(X)$ is a homomorphism.

Proof Easy exercise.

■ (27.1.10) Let $F(X, Y)$ be a formal group law (possibly infinite dimensional) with index set I and let for each $i \in I$, $\delta_i(t)$ be the curve with components $(\delta_i)_j(t) = 0$ if $j \neq i$ and $(\delta_i)_i(t) = t$. This notation will be standard from now on. We shall refer to $\{\delta_i(t), i \in I\}$ as the standard $\mathbf{V}$-basis for $\mathscr{C}(F; A)$.

■ (27.1.11) **Lemma** Every curve $\gamma(t) \in \mathscr{C}(F; A)$ can be uniquely written as a convergent sum

$$\gamma(t) = \sum_{\substack{i \in I \\ m \in \mathbf{N}}}{}^{F} \mathbf{V}_m\langle a_{m,i}\rangle \delta_i(t) \tag{27.1.12}$$

where for every $m \in \mathbf{N}$ there are only finitely many $a_{m,i}$ that are $\neq 0$.

Proof Let $\mathscr{C}^n(F; A)$ be the subgroup of $\mathscr{C}(F; A)$ of all curves that are $\equiv 0$ mod(degree n). Now because $F(X, Y) \equiv X + Y$ mod(degree 2) and because of the "monomials have compact support" condition on the elements of $\mathscr{C}(F; A) = \mathrm{Mor}(1, I)$ (cf. (27.1.3)), we have that

$$\mathscr{C}^n(F; A)/\mathscr{C}^{n+1}(F; A) \simeq \oplus_{m \in I} A,$$

the direct sum of I copies of the abelian group A. The lemma is now proved by successive approximation; to take the limit on the right of (27.1.12) and to prove the identity (27.1.12), one uses the facts that $\mathscr{C}(F; A)$ is complete and Hausdorff and that the topology on $\mathscr{C}(F; A)$ is defined by the subgroups $\mathscr{C}^n(F; A)$.

■ (27.1.13) Let $\mathbf{FG}_A$ be the category of all (possibly infinite dimensional) formal

group laws over A with as morphisms homomorphisms between formal group laws as defined in (27.1.3). The assignment $F(X, Y) \mapsto \mathscr{C}(F; A), \alpha \mapsto \alpha_*$ defines a functor $\mathbf{FG}_A \to \mathbf{Set}$ (if we forget about the topological group structure of $\mathscr{C}(F; A)$). Cartier's first theorem says that this functor is representable by $\hat{W}(X, Y)$.

Let $\gamma_w(t) \in \mathscr{C}(\hat{W}; A) = \mathrm{Mor}(1, \mathbf{N})$ be the curve $\delta_1(t)$ of Example (27.1.6), i.e., $\gamma_w(t)$ is the N-tuple of power series with components $(\gamma_w)_1(t) = t$, $(\gamma_w)_i(t) = 0$ for $i \geq 2$. The theorem now says

■ (27.1.14) **Theorem** (representability of $\mathscr{C}(-; A)$) Let $F(X, Y)$ be a formal group law over A and let $\gamma(t) \in \mathscr{C}(F; A)$ be a curve. Then there exists precisely one homomorphism of formal group laws $\alpha_\gamma(X)$: $\hat{W}(X, Y) \to F(X, Y)$ over A such that $\alpha_\gamma(\gamma_w(t)) = \gamma(t)$. This correspondence $\mathscr{C}(F; A) \simeq \mathbf{FG}_A(\hat{W}(X; Y), F(X, Y))$ is an isomorphism of topological groups.

■ (27.1.15) To prove this theorem we need to know something about the action of the Frobenius operators $\mathbf{f}_n$ on $\mathscr{C}(\hat{W}; A)$. Let $\delta_n(t)$ be the curve defined in the example (27.1.6) which consists of the components zero for all $i \neq n$ and which has the power series t in component n. Then we have

$$\mathbf{f}_n \gamma_w(t) = \delta_n(t) \tag{27.1.16}$$

We prove this for $\hat{W}(X, Y)$ considered as a formal law over $\mathbf{Z}$. It then follows over all rings A because $\phi_*: \mathscr{C}(\hat{W}; \mathbf{Z}) \to \mathscr{C}(\hat{W}; A)$ commutes with $\mathbf{f}_n$ if $\phi: \mathbf{Z} \to A$ is a ring homomorphism. Now (27.1.16) is equivalent with

$$w_i(\mathbf{f}_n \gamma_w(t)) = w_i(\delta_n(t)) \qquad \text{all} \quad i \in \mathbf{N} \tag{27.1.17}$$

where the w_i are the Witt polynomials; and since roots of unity make sense over $\mathbf{Z}$, we have

$$\mathbf{f}_n(\gamma_w(t)) = \gamma_w(\xi_n t^{1/n}) +_{\hat{w}} \cdots +_{\hat{w}} \gamma_w(\xi_n^n t^{1/n})$$

where ξ_n is a primitive nth root of unity, so

$$\begin{aligned} w_i(\mathbf{f}_n \gamma_w(t)) &= w_i(\gamma_w(\xi_n t^{1/n})) + \cdots + w_i(\gamma_w(\xi_n^n t^{1/n})) \\ &= (\xi_n^i + \cdots + \xi_n^{ni}) t^{i/n} \\ &= \begin{cases} 0 & \text{if } n \text{ does not divide } i \\ n t^{i/n} & \text{if } n \text{ divides } i \end{cases} \\ &= w_i(\delta_n(t)) \end{aligned}$$

which proves (27.1.17).

■ (27.1.18) **Caveat** It is very tempting to write $\gamma_w(t) = (t, 0, 0, 0, \ldots)$, and this in turn can be viewed as an element of the group $W(A[\![t]\!])$ (rather than as an

element of $\mathscr{C}(\hat{W}; A)$). The group functor W has a Frobenius endomorphism which is (naturally) denoted $\mathbf{f}_n$. But then

$$\mathbf{f}_n(t, 0, 0, \ldots) = (t^n, 0, 0, \ldots)$$

and

$$\mathbf{V}_n(t, 0, 0, \ldots) = (0, 0, \ldots, 0, t, 0, 0, \ldots)$$

with the t in the nth spot. The reason for this is that the algebraic group scheme W and the formal group scheme $\hat{W}$ are dual to each other and the duality interchanges **f**'s and **V**'s!

We shall be careful to distinguish between the various **f**'s, which is one reason to write $\gamma_w(t)$ rather than $(t, 0, 0, \ldots)$.

■ (27.1.19) Proof of Theorem (27.1.14)

(i) *Uniqueness of* α_γ Suppose there is a homomorphism $\alpha_\gamma(X)$ such that $\alpha_\gamma(\gamma_w(t)) = \gamma(t)$. Because α_γ is a formal group homomorphism we have that $(\alpha_{\gamma *})\mathbf{f}_n = \mathbf{f}_n(\alpha_{\gamma *})$ so that by (27.1.16)

$$(\alpha_{\gamma *})\delta_n(t) = \mathbf{f}_n\gamma(t)$$

Composing $\alpha_\gamma(X)$ with the identity morphism, using the continuity of $\alpha_{\gamma *}$ and formula (27.1.7) now gives us

$$\alpha_\gamma(X) = \sum_{n=1}^{\infty F} \mathbf{f}_n\gamma(X_n) \tag{27.1.20}$$

which determines $\alpha_\gamma(X)$ completely in terms of the curve $\gamma(t)$, and which also shows that $\gamma(t) \mapsto \alpha_\gamma(X)$ is a homomorphism of the group $\mathscr{C}(F; A)$ to the group $\mathbf{FG}_A(\hat{W}(X, Y), F(X, Y))$ once we have shown that $\alpha_\gamma(X)$ is indeed a homomorphism.

(ii) *Existence of* α_γ *in case* $F(X, Y)$ *is finite dimensional* First suppose that $F(X, Y)$ is the universal m-dimensional formal group law over $\mathbf{Z}[U]$. Let $f(X) = \sum a_n X^n$ be the logarithm of $F(X, Y)$. The logarithm $f_w(X)$ of $\hat{W}(X, Y)$ is equal to

$$f_w(X) = \begin{pmatrix} X_1 \\ X_2 + 2^{-1}X_1^2 \\ X_3 + 3^{-1}X_1^3 \\ X_4 + 2^{-1}X_2^2 + 4^{-1}X_1^4 \\ \vdots \end{pmatrix}$$

Now let

$$\gamma_C(t) = \sum_{i=1}^{\infty F} C_i t^i$$

be the universal curve in $F(X, Y)$ with coefficients in $\mathbf{Z}[U; C]$ and consider

$$f(\gamma_C(t)) = \sum_{i=1}^{\infty} x_i t^i$$

The x_i are column vectors of length m in the U's and C's and satisfy of course a functional equation relation

$$x_i - p^{-1}U_p x_{p^{-1}i}^{(p)} - \cdots - p^{-1}U_{p^r} x_{p^{-r}i}^{(p^r)} \in \mathbf{Z}_{(p)}[U; C]^m \tag{27.1.21}$$

if $p^r \mid i$ but $p^{r+1} \nmid i$. Now let B be the $n \times \infty$ matrix consisting of the column vectors $b_i = ix_i$

$$B = (x_1, 2x_2, 3x_3, 4x_4, \ldots) \tag{27.1.22}$$

and let

$$\alpha_\gamma(X) = f^{-1}(Bf_w(X)) \tag{27.1.23}$$

then because

$$f_w(\gamma_w(t)) = \begin{pmatrix} t \\ 2^{-1}t^2 \\ 3^{-1}t^3 \\ \vdots \end{pmatrix}$$

we have $f(\alpha_\gamma(\gamma_w(t))) = f(\gamma_C(t))$ and hence $\alpha_\gamma(\gamma_w(t)) = \gamma_C(t)$. (This by the way also proves uniqueness of α_γ in this case; the matrix B is uniquely determined by the condition $Bf_w(\gamma_w(t)) = f(\gamma(t))$ in the torsion free case.)

It remains to prove that $\alpha_\gamma(X)$ has integral coefficients because this $\alpha_\gamma(X)$ is certainly additive. This follows from part (i) because $\alpha_\gamma(X)$ is also unique over $\mathbf{Q}[U; C]$. Alternatively, we can prove this by showing that $Bf_w(X)$ satisfies the same type of functional equation as $f(X)$. A small calculation shows that

$$\begin{aligned} Bf_w(X) = {} & x_1 X_1 + x_2 X_1^2 + x_3 X_1^3 + \cdots \\ & + 2x_2 X_2 + 2x_4 X_2^2 + 2x_6 X_2^3 + \cdots \\ & + \cdots \\ & + nx_n X_n + nx_{2n} X_n^2 + nx_{3n} X_n^3 + \cdots \end{aligned}$$

So to prove that $Bf_w(X)$ satisfies the same functional equation as $f(X)$ we must show that for each $n \in \mathbf{N}$ and $i \in \mathbf{N}$,

$$nx_{in} \in \mathbf{Z}_{(p)}[U; C]^m \qquad \text{if} \quad p \nmid i$$

$$nx_{in} - p^{-1}U_p nx_{p^{-1}in}^{(p)} - \cdots - p^{-1}U_{p^r} nx_{p^{-r}in}^{(p^r)} \in \mathbf{Z}_{(p)}[U; C]^m$$

if $p^r \mid i$ but $p^{r+1} \nmid i$. (Note that the powers of X behave just right.) This follows

from (27.1.21) because $p^s x_n \in \mathbf{Z}_p[U; C]^m$ if $p^{s+1} \nmid n$ and if $n = p^s t$, $(t, p) = 1$, then

$$n(x_{in} - p^{-1}U_p x^{(p)}_{p^{-1}in} - \cdots - p^{-1}U_{p^{r+s}} x^{(p^{r+s})}_{p^{-r-s}in}) \in \mathbf{Z}_{(p)}[U; C]^m$$

and

$$tp^s(p^{-1}U_{p^{r+1}} x^{(p^{r+1})}_{p^{-r-1}in} + \cdots + p^{-1}U_{p^{r+s}} x^{(p^{r+s})}_{p^{-r-s}in}) \in \mathbf{Z}_{(p)}[U; C]^m$$

because the highest power of p dividing $p^{-r-j}in$ is p^{s-j}.

To conclude the proof of existence of $\alpha_\gamma(X)$, let $F(X, Y)$ be any m-dimensional formal group law and $\gamma(t)$ any curve in $\mathscr{C}(F; A)$. Let ϕ be the unique homomorphism $\mathbf{Z}[U; C] \to A$ such that $\phi_* F_U(X, Y) = F(X, Y)$ and $\phi_* \gamma_C(t) = \gamma(t)$. Let $\hat{\alpha}(X)$ be the $\alpha_\gamma(X)$ constructed above (cf. (27.1.23)) for $F_U(X, Y)$ and $\gamma_C(t)$. Then $\alpha_\gamma(X) = \phi_* \hat{\alpha}(X)$ is a homomorphism $\hat{W}(X, Y) \to F(X, Y)$, and $\alpha_\gamma(\gamma_w(t)) = \gamma(t)$.

(iii) Formula (27.1.20) shows that $\alpha_\gamma(X)$ depends continuously on $\gamma(t)$ and $\gamma_\alpha(t) = \alpha(\gamma_w(t))$ depends of course continuously on $\alpha(X)$.

(iv) *Remarks on the proof of Theorem* (27.1.14) *for infinite dimensional formal group laws* An examination of the first proof of existence given above shows that this works for every formal group law over a characteristic zero ring A (i.e., ring A such that $A \to A \otimes \mathbf{Q}$ is injective). So to prove the theorem also for infinite dimensional formal group laws it suffices to show that every formal group law can be lifted to one over a characteristic zero ring; this is true: a proof can be found, e.g., in [256].

(v) During the second proof of the integrality of $\alpha_\gamma(X)$ we used the functional equation lemma in the case of an infinity of variables X. This makes no difference, neither in statement nor in proof. But the reader unhappy about this may observe that setting $X_{n+1} = X_{n+2} = \cdots = 0$ converts the situation to a case with finitely many X's to which the functional equation lemma applies and this shows that $\alpha_\gamma(X)$ is integral mod$(X_{n+1}, X_{n+2}, \ldots)$ for all n, hence integral.

27.2 The ring of operators Cart(A)

■ (27.2.1) **Composition operators** Let $\chi(t) \in \mathrm{Mor}(1, 1)$. Then $\chi(t)$ defines an additive continuous operator on $\mathscr{C}(F; A)$ for all formal group laws $F(X, Y)$ by the rule

$$\mathrm{comp}(\chi)\gamma(t) = \gamma(\chi(t)) \tag{27.2.2}$$

These operators are called *composition operators*. Of course $\mathbf{V}_m$ and $\langle a \rangle$ for $m \in \mathbf{N}$ and $a \in A$ are special composition operators with their χ's respectively equal to t^m and at.

■ (27.2.3) **Operators in general** In general we now define an operator on $\mathscr{C}(-; A)$ as a functor endomorphism of the (set-valued) functor $\mathscr{C}(-; A)$. This

means that if Q is an operator and $\alpha(X)\colon F(X, Y) \to G(X, Y)$ a homomorphism of formal group laws, then we must have a commutative diagram of maps

(27.2.4)
$$\begin{array}{ccc} \mathscr{C}(F; A) & \xrightarrow{Q} & \mathscr{C}(F; A) \\ \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \alpha_*} \\ \mathscr{C}(G; A) & \xrightarrow{Q} & \mathscr{C}(G; A) \end{array}$$

As happens so often (e.g., in the case of cohomology operations), the functoriality of an operator (together with the representability of $\mathscr{C}(-; A)$) forces the operator to have more properties, such as additivity and continuity.

■ (27.2.5) **Proposition** Let Q_1, Q_2 be two operators on $\mathscr{C}(-; A)$, then we have:

(i) $Q_1 \gamma_w(t) = Q_2 \gamma_w(t) \Rightarrow Q_1 = Q_2$.
(ii) Q_1 and Q_2 are additive and continuous.
(iii) Conversely, let $\gamma(t) \in \mathscr{C}(\hat{W}; A)$ be any curve, then there is a unique operator Q_γ such that $Q_\gamma(\gamma_w(t)) = \gamma(t)$.

Proof (i) Let $\gamma(t) \in \mathscr{C}(F; A)$ be any curve and let $\alpha_\gamma(X)$ be the unique homomorphism $\hat{W}(X, Y) \to F(X, Y)$ such that $\alpha_\gamma(\gamma_w(t)) = \gamma(t)$. By the commutativity of (27.2.4) (with α_γ for α, $\hat{W}$ for F, and F for G) we have

(27.2.6)
$$Q_1 \gamma(t) = \alpha_{\gamma *}(Q_1 \gamma_w(t))$$

and similarly for Q_2. This proves (i).

(ii) To prove the continuity and additivity of Q_1 and Q_2 it suffices to remark that in formula (27.2.6) $\alpha_\gamma(X)$ depends continuously and additively on $\gamma(t)$ by Theorem (27.1.14).

(iii) For any curve $\delta(t) \in \mathscr{C}(F; A)$, define $Q_\gamma(\delta(t)) = \alpha_\delta(\gamma(t))$. By uniqueness of α_δ this defines an operator.

■ (27.2.7) **Corollary** There is a one–one onto correspondence between operators on $\mathscr{C}(-; A)$ and curves in $\mathscr{C}(\hat{W}; A)$.

■ (27.2.8) Now according to Lemma (27.1.11) every curve in $\mathscr{C}(\hat{W}; A)$ can be written uniquely as a sum

$$\sum_{m=1}^{\infty} \sum_{i=1}^{\infty} {}^{\hat{W}}\mathbf{V}_m\langle a_{m,i}\rangle \delta_i(t)$$

with for every $m \in \mathbf{N}$ only finitely many $i \in \mathbf{N}$ for which $a_{m,i} \neq 0$. But by (27.1.16) we know that $\mathbf{f}_n \gamma_w(t) = \delta_n(t)$, so every curve $\gamma(t) \in \mathscr{C}(\hat{W}; A)$ can be uniquely written in the form

$$\sum_{m,i \in \mathbf{N}} \mathbf{V}_m\langle a_{m,i}\rangle \mathbf{f}_i \gamma_w(t)$$

and combining this with Proposition (27.2.5) we find

■ (27.2.9) **Proposition** Every operator Q on $\mathscr{C}(-; A)$ can be uniquely written in the form

$$\sum_{m,i \in \mathbf{N}} \mathbf{V}_m \langle a_{m,i} \rangle \mathbf{f}_i \tag{27.2.10}$$

with for every $m \in \mathbf{N}$ only finitely many $i \in \mathbf{N}$ such that $a_{m,i} \neq 0$.

■ (27.2.11) **The ring** $\mathrm{Cart}(A)$ We shall denote the ring of all operators by $\mathrm{Cart}(A)$. This is therefore the ring of all expressions (27.2.10). The calculation rules are those that we derived in Section 16 of Chapter III. We repeat them for completeness sake:

$$\langle a \rangle \langle b \rangle = \langle ab \rangle, \qquad \langle 1 \rangle = \mathbf{f}_1 = \mathbf{V}_1 = \text{identity operator}$$

$$\mathbf{V}_m \mathbf{V}_n = \mathbf{V}_{mn}, \qquad \mathbf{f}_m \mathbf{f}_n = \mathbf{f}_{mn}$$

$$\langle a \rangle \mathbf{V}_m = \mathbf{V}_m \langle a^m \rangle, \qquad \mathbf{f}_m \langle a \rangle = \langle a^m \rangle \mathbf{f}_m$$

$$\text{if} \quad (n, m) = 1, \qquad \text{then} \quad \mathbf{V}_m \mathbf{f}_n = \mathbf{f}_n \mathbf{V}_m$$

$$\mathbf{f}_n \mathbf{V}_n = [n] = 1 + \cdots + 1 \quad (n \text{ times})$$

$$\langle a + b \rangle = \sum_{n=1}^{\infty} \mathbf{V}_n \langle r_n(a, b) \rangle \mathbf{f}_n$$

where the $r_n(Z_1, Z_2)$ are the polynomials with coefficients in $\mathbf{Z}$ defined by

$$Z_1^n + Z_2^n = \sum_{d|n} d r_d(Z_1, Z_2)^{n/d}$$

The reader can easily convince himself that the calculation rules given above suffice to calculate any sum and product of expressions like (27.2.10).

■ (27.2.12) $\mathrm{End}_A(\hat{W}(X, Y))$ By Proposition (27.2.5) there is a one–one correspondence between curves in $\mathscr{C}(\hat{W}; A)$ and operators Q. By Theorem (27.1.14) there is a one–one correspondence between curves in $\hat{W}(X, Y)$ and endomorphisms of $\hat{W}(X, Y)$. This permits us to identify $\mathrm{Cart}(A)$ with $\mathrm{End}_A(\hat{W}(X, Y))$. Now the formal group law $\hat{W}(X, Y)$ has endomorphisms $\mathbf{f}_n$ and $\mathbf{V}_n$ defined by the same formulas as the endomorphisms $\mathbf{f}_n$ and $\mathbf{V}_n$ of the group-valued functor $W(-)$. Under the identification just described, the endomorphism $\mathbf{f}_n$ of $\hat{W}(X, Y)$ corresponds to the operator $\mathbf{V}_n$ and the endomorphism $\mathbf{V}_n$ of $\hat{W}(X, Y)$ corresponds to the operator $\mathbf{f}_n$.

■ (27.2.13) $\mathrm{Cart}(A)$ **as a topological ring** We give $\mathrm{Cart}(A)$ the topology inherited from $\mathscr{C}(\hat{W}; A)$. The $\mathscr{C}^n(\hat{W}; A)$ correspond to right ideals

$\mathfrak{A}_n \subset \mathrm{Cart}(A)$. Since $\mathscr{C}^n(\hat{W}; A)$ consists of all curves $\equiv 0 \bmod(\text{degree } n)$, we have

$$\mathfrak{A}_n = \left\{ \sum_{m,i} \mathbf{V}_m \langle a_{m,i} \rangle \mathbf{f}_i \,|\, a_{m,i} = 0 \quad \text{for all} \quad i \quad \text{if} \quad m < n \right\}$$

(One has to check that the $\mathfrak{A}_n$ are indeed right ideals!) This makes $\mathrm{Cart}(A)$ a complete topological ring with its topology defined by the (open and closed) right ideals $\mathfrak{A}_n$.

27.3 Cartier's second theorem

■ (27.3.1) **Curve lemma** (Faithfulness of the set-valued functor "curves") Let $\alpha(X), \beta(X) \in \mathrm{Mor}(I, J)$ where I and J are two possibly infinite index sets. If for every $\gamma(t) \in \mathrm{Mor}(1, I)$ we have $\alpha(\gamma(t)) = \beta(\gamma(t))$, then $\alpha(X) = \beta(X)$.

Proof It suffices to prove this for every component $\alpha_j(X), \beta_j(X)$ of $\alpha(X)$ and $\beta(X)$. So we can assume that J has one element. Then it also suffices to prove that $\alpha(\gamma(t)) = \beta(\gamma(t))$ implies $\alpha(X) \equiv \beta(X) \bmod(X_i, i \notin \kappa)$ for all finite subsets κ of I. So we can assume that I is finite and we are reduced to the case of an $\alpha(X), \beta(X) \in \mathrm{Mor}(m, 1)$. Write

$$\alpha(X) = \sum_{\mathbf{n}} a_{\mathbf{n}} X^{\mathbf{n}}, \qquad \beta(X) = \sum_{\mathbf{n}} b_{\mathbf{n}} X^{\mathbf{n}}$$

where $\mathbf{n}$ runs through all multi-indices $\mathbf{n} = (n_1, \ldots, n_m)$, $n_i \in \mathbf{N} \cup \{0\}$ of length m and with $|\mathbf{n}| = n_1 + \cdots + n_m \geq 1$. Order these indices lexicographically and let $\mathbf{k}$ be the lexicographically smallest index such that $a_{\mathbf{k}} \neq b_{\mathbf{k}}$. Let $\mathbf{k} = (k_1, \ldots, k_m)$. Then there exist integers $d_1, \ldots, d_m$ such that

$$(27.3.2) \quad \mathbf{k} <_l \mathbf{n} \quad \Rightarrow \quad k_1 d_1 + k_2 d_2 + \cdots + k_m d_m < n_1 d_1 + \cdots + n_m d_m$$

where $<_l$ denotes lexicographic order. Indeed one can take $d_m = 1$, $d_{m-1} = k_m d_m + 1, \ldots, d_1 = k_2 d_2 + \cdots + k_m d_m + 1$. Now let $\gamma(t)$ be the curve

$$\gamma(t) = (t^{d_1}, t^{d_2}, \ldots, t^{d_m})$$

then because by hypothesis $a_{\mathbf{n}} = b_{\mathbf{n}}$ for $\mathbf{n} <_l \mathbf{k}$, we have using (27.3.2)

$$\alpha(\gamma(t)) \equiv \beta(\gamma(t)) + (a_{\mathbf{k}} - b_{\mathbf{k}}) t^d \bmod(\text{degree } d + 1)$$

where $d = k_1 d_1 + \cdots + k_m d_m$. This concludes the proof.

■ (27.3.3) **Remark** We have used this trick several times before in Chapter II when proving various universality statements.

■ (27.3.4) **Proposition** Let $F(X, Y), G(X, Y)$ be two formal group laws over A, and let $\beta: \mathscr{C}(F; A) \to \mathscr{C}(G; A)$ be a map. Then there is a homomorphism of formal group laws $\alpha(X): F(X, Y) \to G(X, Y)$ such that $\beta = \alpha_* = \mathscr{C}(\alpha; A)$ if (and

only if) β is continuous additive and commutes with all composition operators comp(χ).

■ (27.3.5) **Corollary** (Cartier's second theorem) Let $F(X, Y)$, $G(X, Y)$ be two formal group laws over A and let $\beta: \mathscr{C}(F; A) \to \mathscr{C}(G; A)$ be a map. Then there is a homomorphism of formal group laws $\alpha(X): F(X, Y) \to G(X, Y)$ such that $\beta = \alpha_*$ if and only if β is continuous, additive, and commutes with the operators $\mathbf{V}_m$, $\langle a \rangle$, $\mathbf{f}_n$ for all $m, n \in \mathbf{N}$ and $a \in A$.

This follows from Proposition (27.3.4) by Proposition (27.2.9), which says that every operator can be written in terms of the $\mathbf{V}_m$, $\langle a \rangle$, and $\mathbf{f}_n$.

■ (27.3.6) **Proof of Proposition (27.3.4)** Let $F(X, Y)$ have dimension m and let $\delta_1(t), \ldots, \delta_m(t)$ be the standard $\mathbf{V}$-basis for $F(X, Y)$. Because isomorphisms $F(X, Y) \to \hat{F}(X, Y)$ induce continuous additive isomorphisms $\mathscr{C}(F; A) \to \mathscr{C}(\hat{F}; A)$ that commute with composition operators (cf. Lemma (27.1.9)) it suffices to prove Proposition (27.3.4) with $F(X, Y)$ possibly replaced by an isomorphic formal group law. By Chapter II, Theorem (12.3.6) we can therefore assume that $F(X, Y)$ is curvilinear, which means in particular that if

$$(x_1, \ldots, x_m), \qquad (y_1, \ldots, y_m)$$

are two sets of power series and for all $i \in \{1, \ldots, m\}$ we have $x_i = 0$ or $y_i = 0$, then

$$(x_1, \ldots, x_m) +_F (y_1, \ldots, y_m) = (x_1 + y_1, \ldots, x_m + y_m)$$

(This follows immediately from the definition of curvilinear; cf. Chapter II, Section (12.1).) Now let $\gamma(Z)$ be any m-tuple of power series in the indeterminates $Z_1, Z_2, \ldots$. Then

$$\gamma(Z) = \sum_{i=1}^{m}{}^{F} \delta_i(\gamma_i(Z)) = \sum_{i=1}^{m}{}^{F} \delta_i(t) \circ \gamma_i(Z)$$

Let $\beta(\delta_i(t)) = \hat{\delta}_i(t) \in \mathscr{C}(G; A)$. We now define for every $\gamma(Z)$ a J-tuple of power series $\tilde{\beta}(\gamma(Z))$ as

$$\tilde{\beta}(\gamma(Z)) = \sum_{i=1}^{m}{}^{G} \hat{\delta}_i(\gamma_i(Z)) = \sum_{i=1}^{m}{}^{G} \hat{\delta}_i(t) \circ \gamma_i(Z) \tag{27.3.7}$$

$$= \sum_{i=1}^{m}{}^{G} \beta(\delta_i(t)) \circ \gamma_i(Z)$$

where J is the index set of the formal group law $G(X, Y)$. We claim that this map $\tilde{\beta}$: Mor$(K, m) \to$ Mor(K, J), thus defined for all index sets K, satisfies the property

$$\tilde{\beta}(\gamma(Z)) \circ \delta(t) = \beta(\gamma(Z) \circ \delta(t)) \tag{27.3.8}$$

for all curves $\delta(t) \in \mathrm{Mor}(1, K)$. (By the curve lemma (27.3.1) $\tilde{\beta}$ is also uniquely determined by (27.3.8).) To prove (27.3.8) observe that

$$\begin{aligned}
\tilde{\beta}(\gamma(Z)) \circ \delta(t) &= \sum_{i=1}^{m}{}^{G} \hat{\delta}_i(t) \circ \gamma_i(Z) \circ \delta(t) \\
&= \sum_{i=1}^{m}{}^{G} \beta(\delta_i(t)) \circ \gamma_i(\delta(t)) \\
&= \sum_{i=1}^{m}{}^{G} \mathrm{comp}(\gamma_i(\delta(t)))\beta(\delta_i(t)) \\
&= \sum_{i=1}^{m}{}^{G} \beta(\mathrm{comp}(\gamma_i(\delta(t)))\delta_i(t)) \\
&= \sum_{i=1}^{m}{}^{G} \beta(\delta_i(\gamma_i(\delta(t)))) \\
&= \beta\left(\sum_{i=1}^{m}{}^{F} \delta_i(\gamma_i(\delta(t)))\right) \\
&= \beta(\gamma(Z) \circ \delta(t))
\end{aligned}$$

where we have used the fact that β commutes with composition operators to go from line 3 to line 4 and the additivity of β was used to go from line 5 to line 6.

We claim that $\tilde{\beta}$ is also additive. That is, we claim that

$$\tilde{\beta}(\gamma(Z) +_F \hat{\gamma}(Z)) = \tilde{\beta}(\gamma(Z)) +_G \tilde{\beta}(\hat{\gamma}(Z)) \tag{27.3.9}$$

for all $\gamma(Z), \hat{\gamma}(Z) \in \mathrm{Mor}(K, m)$.

To prove (27.3.9) observe that by (27.3.8) and the additivity of β

$$\begin{aligned}
\tilde{\beta}(\gamma(Z) +_F \hat{\gamma}(Z)) \circ \delta(t) &= \beta((\gamma(Z) +_F \hat{\gamma}(Z)) \circ \delta(t)) \\
&= \beta((\gamma(Z) \circ \delta(t)) +_F (\hat{\gamma}(Z) \circ \delta(t))) \\
&= \beta(\gamma(Z) \circ \delta(t)) +_G \beta(\hat{\gamma}(Z) \circ \delta(t)) \\
&= \tilde{\beta}(\gamma(Z)) \circ \delta(t) +_G \tilde{\beta}(\hat{\gamma}(Z)) \circ \delta(t) \\
&= (\tilde{\beta}(\gamma(Z)) +_G \tilde{\beta}(\hat{\gamma}(Z))) \circ \delta(t)
\end{aligned}$$

which proves (27.3.9) by the curve lemma (27.3.1). Now take

$$Z = (X_1, X_2, \ldots, X_m, Y_1, \ldots, Y_m)$$

and

$$\gamma(Z) = (X_1, \ldots, X_m),\ \hat{\gamma}(Z) = (Y_1, \ldots, Y_m)$$

then (27.3.9) says that

$$\begin{aligned}\tilde{\beta}(F(X, Y)) &= \tilde{\beta}((X_1, \ldots, X_m) +_F (Y_1, \ldots, Y_m)) \\ &= \tilde{\beta}(X_1, \ldots, X_m) +_G \tilde{\beta}(Y_1, \ldots, Y_m) = G(\tilde{\beta}(X), \tilde{\beta}(Y))\end{aligned}$$

so that $\alpha(X) = \tilde{\beta}(\gamma(X))$ with $\gamma(X) = (X_1, \ldots, X_m)$ is the desired homomorphism ($\alpha(X)$ does indeed induce β because by (27.3.7), taking $\gamma(Z) = (X_1, \ldots, X_m)$, we find $\alpha(X) \circ \delta(t) = \beta(X_1, \ldots, X_m) \circ \delta(t)) = \beta(\delta(t)))$.

■ (27.3.10) **Remark** For future use, we note that the formula for $\alpha(X)$ is

$$\alpha(X) = \sum_i^G \beta(\delta_i(X_i))$$

where $\delta_1(t), \ldots, \delta_m(t)$ is the standard **V**-basis for $\mathscr{C}(F; A)$.

27.4 Entwined pairs of functions

This section contains some material related to the proof of Cartier's third theorem (which describes all Cart(A)-modules that can arise as a $\mathscr{C}(F; A)$). In fact if A is of characteristic zero, Cartier's third theorem over A can be proved by means of these ideas; cf. (27.5.11) and (27.6.13).

■ (27.4.1) **The "structure coefficients"** $c(p, r, j, i)$ Let $F(X, Y)$ be an m-dimensional formal group law over A. Let $\delta_i(t)$ be the standard **V**-basis for $\mathscr{C}(F; A)$. The Frobenius operators $\mathbf{f}_p$, p a prime number, act on $\mathscr{C}(F; A)$; by Lemma 27.1.11 we have unique expressions

$$\mathbf{f}_p\delta_i(t) = \sum_{r,j}^F \mathbf{V}_r\langle c(p, r, j, i)\rangle\delta_j(t) \tag{27.4.2}$$

for the curves $\mathbf{f}_p\delta_i(t)$. (Conversely, if we know the $\mathbf{f}_p\delta_i(t)$ for all $i \in \{1, \ldots, m\}$ and all prime numbers p, then we know the Cart(A) structure of $\mathscr{C}(F; A)$.)

The "structure coefficients" $c(p, r, j, i)$ for varying p are not independent, and we proceed to derive certain relations.

■ (27.4.3) **Relations between the** $c(p, r, j, i)$ To this end suppose for the moment that A is of characteristic zero and that $F(X, Y)$ is a curvilinear formal group law. The logarithm $f(X)$ of $F(X, Y)$ then has the form

$$f(X) = \sum_{i=1}^{\infty} a_i X^i \tag{27.4.4}$$

where the a_i are $m \times m$ matrices with coefficients in $A \otimes \mathbf{Q}$ and X^i is short for $(X_1^i, X_2^i, \ldots, X_m^i)$; cf. Chapter II, Section 12.1.

Let a_n be the matrix $a_n(j, k), j, k \in \{1, \ldots, m\}$ and let $a_n(i)$ be the ith column of a_n. Then we have

$$f(\delta_i(t)) = \sum_{n=1}^{\infty} a_n(i)t^n$$

and hence by Chapter III, (15.1.9)

$$f(\mathbf{f}_p\delta_i(t)) = \sum_{n=1}^{\infty} pa_{pn}(i)t^n \tag{27.4.5}$$

On the other hand, from (27.4.2) we find

$$\begin{aligned} f(\mathbf{f}_p\delta_i(t)) &= f\left(\sum\nolimits_{r,j}^{F} \mathbf{V}_r\langle c(p, r, j, i)\rangle\delta_j(t))\right) \\ &= \sum_{r,j} f(\delta_j(c(p, r, j, i)t^r)) \\ &= \sum_{r,j}\sum_{n} a_n(j)c(p, r, j, i)^n t^{rn} \\ &= \sum_{n=1}^{\infty}\left(\sum_{d|n}\sum_{j=1}^{m} a_{n/d}(j)c(p, d, j, i)^{n/d}\right)t^n \end{aligned} \tag{27.4.6}$$

Writing $c(p, d)$ for the matrix with as (i, j)th entry the element $c(p, d, i, j)$ and using the notation $c^{\{k\}}$ to denote the matrix obtained from a matrix c by raising each of its entries to the kth power, we obtain from the comparison of (27.4.5) and (27.4.6) that

$$pa_{pn} = \sum_{d|n} a_{n/d}\, c(p, d)^{\{n/d\}} \tag{27.4.7}$$

Now let $b(n) = na_n$, then (27.4.7) yields in terms of the matrices b_n

$$b(pn) = \sum_{d|n} db(n/d)c(p, d)^{\{n/d\}}, \qquad b_1 = I_m \tag{27.4.8}$$

Now the matrices $b(n)$ and $c(p, d)$ all have their coefficients in A. And because every (curvilinear) formal group law over a ring A can be lifted to a (curvilinear) formal group law over a characteristic zero ring, it follows that for any (curvilinear) formal group $F(X, Y)$ over any ring A there exists a function b: $\mathbf{N} \to A^{m\times m}$ such that (27.4.8) holds, where the $c(p, d)$ are the matrices given by (27.4.2).

■ (27.4.9) **Definition** An m-dimensional pair of entwined functions over A is a pair of matrix valued functions b: $\mathbf{N} \to A^{m\times m}$, c: $\mathbf{P} \times \mathbf{N} \to A^{m\times m}$, where $\mathbf{P}$ is the set of prime numbers such that (27.4.8) holds.

■ (27.4.10) **Remark** If $F(X, Y)$ is any formal group law, not necessarily curvilinear, then it gives rise to the same pair of entwined functions as its curvilinear version, which in the characteristic zero case is obtained by removing from $f(X)$ all terms that are not pure powers of one of the $X_1, \ldots, X_m$. To see this simply observe that $f(\delta_i(t))$ does not change if the terms that involve several different X's are removed.

■ (27.4.11) We have seen that an m-dimensional formal group law $F(X, Y)$ over A gives rise to a pair of entwined functions b: $\mathbf{N} \to A^{m\times m}$, c: $\mathbf{P} \times \mathbf{N} \to A^{m\times m}$.

Conversely, as we shall show, every pair of entwined functions b, c comes from a (unique) curvilinear formal group law over A provided A is of characteristic zero. The precise version of this statement is Theorem (27.4.15) below.

■ (27.4.12) Let $C(p, n)_{i,j}$ for $p \in \mathbf{P}$, $n \in \mathbf{N}$, $i, j \in \{1, \ldots, m\}$, and $B(r)_{i,j}$ for $r \in \mathbf{N}$, $i, j \in \{1, 2, \ldots, m\}$, be indeterminates and let $\tilde{L}$ be the ring of polynomials $\tilde{L} = \mathbf{Z}[\ldots, C(p, n)_{i,j}, \ldots; \ldots, B(r)_{i,j}, \ldots]$ and let $\mathfrak{a}$ be the ideal of $\tilde{L}$ generated by the relations

$$B(pn) = \sum_{d|n} dB(n/d)C(p, d)^{(n/d)}, \qquad B_1 = I_m$$

and let L be the quotient ring

$$L = \tilde{L}/\mathfrak{a}$$

Then there is an obvious one–one correspondence between m-dimensional pairs of entwined functions b: $\mathbf{N} \to A^{m \times m}$ and c: $\mathbf{P} \times \mathbf{N} \to A^{m \times m}$ and ring homomorphisms $L \to A$.

■ (27.4.13) Now let $F_R(X, Y)$ over $\mathbf{Z}[R] = \mathbf{Z}[\ldots, R_n(i, j), \ldots]$ be the universal m-dimensional curvilinear formal group law of Chapter II, Section 12.2. According to (27.4.3) and (27.4.12) $F_R(X, Y)$ defines a homomorphism

(27.4.14) $$\vartheta: L \to \mathbf{Z}[R]$$

■ (27.4.15) **Theorem** (entwined function theorem) Every pair of m-dimensional entwined functions with values in a characteristic zero ring A comes from an m-dimensional formal group law over A. More precisely, the homomorphism $\vartheta: L \to \mathbf{Z}[R]$ of (27.4.14) induces an isomorphism $\hat{\vartheta}$: $L/\text{torsion}(L) \to \mathbf{Z}[R]$ and if $\phi: L \to A$ defines a pair of entwined functions, then $(\hat{\phi}\hat{\vartheta}^{-1})_* F_R(X, Y)$ is a formal group law over A that gives rise to the pair of entwined functions defined by ϕ. (Here $\hat{\phi}$: $L/\text{torsion}(L) \to A$ is the homomorphism induced by ϕ, which exists because A is of characteristic zero.)

■ (27.4.16) **Corollary** Pairs of entwined functions over characteristic zero rings correspond biuniquely to curvilinear formal group laws (via ϑ of course).

■ (27.4.17) **Example** We show that L has nontrivial torsion. If we give the $B(n)_{ij}$ degree $n - 1$ and the $C(p, r)_{i,j}$ degree $pr - 1$ then $\tilde{L}$ is a graded ring and $\mathfrak{a}$ is a homogeneous ideal in $\tilde{L}$ so that L is a graded ring. It turns out that the first bit of nontrivial torsion of L occurs in degree 11. We show the existence of a 2-torsion element. Let $m = 1$ and write x_2, x_3, x_4, x_6 respectively for the classes in L of the elements $C(2, 1)$, $C(3, 1)$, $C(2, 2)$, $2C(2, 3) - C(3, 2)$ of $\tilde{L}$. We further use $b(i)$ and $c(p, r)$ to denote the classes mod $\mathfrak{a}$ of $B(i)$ and $C(p, r)$ in $\tilde{L}$. Consider the element $z \in L$

$$z = 3x_2^6 x_6 + 2x_2^9 x_3 + x_3 x_4^3 + 6x_6^2 x_2 - 6x_2^2 x_3^2 x_6 - 3x_2^5 x_3^3 + x_2^3 x_3^4$$
$$+ 6x_2^4 x_3 x_6 + 3c(2, 6) - x_3^4 x_4 - x_2 c(3, 2)^2 - 2c(3, 4)$$

Now define a homogeneous ring homomorphism $\tilde{\phi}$: $\tilde{L} \to \mathbf{Z}/(2)[y]/(y^{12})$, by $\tilde{\phi}(B(i)) = 0$ all $i > 1$, $\tilde{\phi}(B(1)) = 1$, $\tilde{\phi}(C(p, r)) = 0$ if $pr \neq 12$, $\tilde{\phi}(C(2, 6)) = y^{11}$, $\tilde{\phi}(C(3, 4)) = 0$. One now easily checks that

$$\tilde{\phi}(B(pn) - \sum_{d|n} dB(n/d)C(p, d)^{n/d}) = 0$$

for all $(p, n) \in \mathbf{P} \times \mathbf{N}$. (The only nontrivial pair to check is $(p, n) = (2, 6)$.) It follows that $\tilde{\phi}$ induces a ring homomorphism ϕ: $L \to \mathbf{Z}/(2)[y]/(y^{12})$ and we see that $\phi(z) = y^{11} \neq 0$ proving that $z \neq 0$ in L.

We now show that $2z = 0$ in L. This requires some calculations. First

$$b(2) = c(2, 1) = x_2, \qquad b(3) = c(3, 1) = x_3$$

$$b(4) = b(2.2) = b(2)c(2, 1)^2 + 2b(1)c(2, 2) = x_2^3 + 2x_4$$

$$b(6) = b(2.3) = b(3)c(2, 1)^3 + 3b(1)c(2, 3) = x_3x_2^3 + 3c(2, 3)$$

$$b(6) = b(3.2) = b(2)c(3, 1)^2 + 2b(1)c(3, 2) = x_2x_3^2 + 2c(3, 2)$$

From this, setting $x_6 = 2c(2, 3) - c(3, 2)$ (which is a free generator for L in degree 5) we obtain the expressions

$$c(2, 3) = 2x_6 - x_2x_3^2 + x_3x_2^3, \; c(3, 2) = 3x_6 - 2x_2x_3^2 + 2x_3x_2^3$$

$$b(6) = 6x_6 - 3x_2x_2^3 + 4x_3x_2^3$$

There are two prime numbers dividing 12. We find respectively

$$\begin{aligned} b(12) &= b(6)c(2, 1)^6 + 2b(3)c(2, 2)^3 + 3b(2)c(2, 3)^2 + 6c(2, 6) \\ &= 6x_2^6x_6 - 3x_2^7x_3^2 + 4x_2^9x_3 + 2x_3x_4^3 + 3x_2(2x_6 - x_2x_3^2 + x_3x_2^3)^2 \\ &\quad + 6c(2, 6) \\ &= 6x_2^6x_6 + 4x_2^9x_3 + 2x_3x_4^3 + 12x_2x_6^2 + 3x_2^3x_3^4 - 12x_2^2x_3^2x_6 \\ &\quad + 12x_2^4x_3x_6 - 6x_2^5x_3^3 + 6c(2, 6) \end{aligned}$$

$$\begin{aligned} b(12) &= b(4)c(3, 1)^4 + 2b(2)c(3, 2)^2 + 4b(1)c(3, 4) \\ &= x_2^3x_3^4 + 2x_3^4x_4 + 2x_2c(3, 2)^2 + 4c(3, 4) \end{aligned}$$

Subtracting these two expressions for $b(12)$ from each other we find $2z$, so that indeed $2z = 0$ in L.

■ (27.4.18) **Example** It may be thought that the occurrence of torsion in L is due to the fact that there is a certain lack of symmetry in considering only the structure coefficients $c(p, r, i, j)$ with p a prime number. Suppose we are again in the setting of (27.4.1). For each $n \in \mathbf{N}$ let

$$\mathbf{f}_n\delta_i(t) = \sum_{r,j} \mathbf{V}_r\langle c(n, r, j, i)\rangle\delta_j(t) \tag{27.4.19}$$

Then, arguing exactly as in (27.4.3) one finds that for all $n, s \in \mathbf{N}$

$$b(sn) = \sum_{d|n} db(n/d)c(s, d)^{\{n/d\}} \tag{27.4.20}$$

$$b(1) = I_m = c(1, 1), \quad c(1, i) = 0 \qquad \text{for} \quad i > 1$$

Now let L' be the ring generated by the indeterminates $C(s, n)_{i,j}$, $s, n \in \mathbf{N}$, $i, j \in \{1, \ldots, m\}$, $B(n)_{i,j}$, $n \in \mathbf{N}$, $i, j \in \{1, \ldots, m\}$ subject to the relations (27.4.20). If we give $C(s, n)_{i,j}$ and $B(n)_{i,j}$ respectively degree $sn - 1$ and $n - 1$ all the relations (27.4.20) are homogeneous so that L' becomes a graded ring. This ring L' has even more torsion than L. The first torsion elements now occur in degree 7. Take again $m = 1$ and consider the element

$$z = 2c(2, 4) - c(2, 1)c(2, 2)^2 - c(2, 1)^4c(2, 2) - c(4, 2)$$

in L'. We claim that $z \neq 0$ in L'. To see this we define $\tilde{\phi}$: $\tilde{L}' \to \mathbf{Z}/(2)[y]/(y^8)$, where $\tilde{L}' = \mathbf{Z}[C(s, n);\ B(n) \mid n \in \mathbf{N}\backslash\{1\},\ s \in \mathbf{N}]$, by $\tilde{\phi}(B(n)) = 0$ for all $n \geq 2$, $\tilde{\phi}(C(s, n)) = 0$ if $(s, n) \neq (4, 2)$ and $\tilde{\phi}(C(4, 2)) = y^7$. One easily checks that

$$\tilde{\phi}(B(sn) - \sum_{d|n} dB(n/d)C(s, d)^{n/d}) = 0$$

for all (s, n) (where of course $B(1) = 1 = C(1, 1)$, $C(1, i) = 0$ if $i > 1$), so that $\tilde{\phi}$ induces a homomorphism ϕ: $L' \to \mathbf{Z}/(2)[y]/(y^8)$. One finds $\phi(z) = y^7 \neq 0$ so that $z \neq 0$ in L'. We claim that $2z = 0$ in L'. To see this first observe that (27.4.20) with $n = 1$ gives us $b(s) = c(s, 1)$ for all $s \in \mathbf{N}$. Further

$$\begin{aligned}
b(4) &= b(2)c(2, 1)^2 + 2b(1)c(2, 2) = c(2, 1)^3 + 2c(2, 2) \\
b(8) &= b(2.4) = b(4)c(2, 1)^4 + 2b(2)c(2, 2)^2 + 4c(2, 4) \\
&= c(2, 1)^7 + 2c(2, 1)^4c(2, 2) + 2c(2, 1)c(2, 2)^2 + 4c(2, 4) \\
b(8) &= b(4.2) = b(2)c(4, 1)^2 + 2c(4, 2) \\
&= c(2, 1)^7 + 4c(2, 1)^4c(2, 2) + 4c(2, 1)c(2, 2)^2 + 2c(4, 2)
\end{aligned}$$

Subtracting these two expressions for $b(8)$ from one another we find $2z$, so that indeed $2z = 0$ in L'.

27.5 Cartier's third theorem

■ (27.5.1) Let $F(X, Y)$ be an m-dimensional formal group over A and let $\mathscr{C} = \mathscr{C}(F; A)$ be its group of curves. Then $\mathscr{C}$ has the following properties:

(27.5.2) $\mathscr{C}$ is a commutative topological group with its topology defined by open subgroups $\mathscr{C}^n$, $n \in \mathbf{N}$, $\mathscr{C} = \mathscr{C}^1$, and $\mathscr{C}$ is complete and Hausdorff in this topology.

(27.5.3) $\mathscr{C}$ admits continuous and additive operators $\langle a \rangle$, $\mathbf{f}_n$, $\mathbf{V}_n$ such that the relations listed in (27.2.11) hold.

(27.5.4) The operators $\mathbf{V}_n$ map $\mathscr{C}^r$ into $\mathscr{C}^{rm}$ and induce isomorphisms $\mathscr{C}^r/\mathscr{C}^{r+1} \to \mathscr{C}^{rm}/\mathscr{C}^{rm+1}$.

(27.5.5) The operators $\langle a\rangle$ map $\mathscr{C}^r$ into $\mathscr{C}^r$ for all r and $a \mapsto \langle a\rangle$ gives $\mathscr{C}^1/\mathscr{C}^2$ the structure of a free finite rank A-module.

Properties (27.5.4) and (27.5.5) can, using some of the relations of (27.2.11), be restated as:

(27.5.6) There exists a finite set $\delta_1, \ldots, \delta_m$ of elements of $\mathscr{C}$ such that every element $\gamma \in \mathscr{C}$ can be written uniquely as a convergent sum

$$\gamma = \sum_{r,j} \mathbf{V}_r\langle a_{r,j}\rangle\delta_j$$

and $\gamma \in \mathscr{C}^n$ is equivalent to $a_{r,j} = 0$ for all $r < n$.

Note also that all of (27.5.5) except the freeness of $\mathscr{C}^1/\mathscr{C}^2$ follows from (27.5.3) together with (27.5.4).

■ (27.5.7) **Theorem** (Cartier's third theorem) Let $\mathscr{C}$ be a group such that (27.5.2)–(27.5.5) (and hence (27.5.6)) hold. Then there is a formal group law $F(X, Y)$ over A of dimension $\operatorname{rank}_A(\mathscr{C}^1/\mathscr{C}^2)$ such that $\mathscr{C} = \mathscr{C}(F; A)$ (as topological groups with operators $\langle a\rangle$, $\mathbf{V}_n$, $\mathbf{f}_n$).

For A of characteristic zero this theorem follows from the entwined function theorem (27.4.15). First a lemma:

■ (27.5.8) **Lemma** Let $\mathscr{C}$ be as in (27.5.7). Then

(27.5.9) $\mathbf{f}_m\mathbf{V}_r\gamma \equiv 0 \mod \mathscr{C}^2$ if r does not divide m

(27.5.10) $\mathbf{f}_m\mathbf{V}_r\gamma \equiv \langle r\rangle\mathbf{f}_{m/r}\gamma \mod \mathscr{C}^2$ if r divides m

Proof We use of course the relations (27.2.11). Let $d = (r, m)$ and suppose that $d < r$. Then we have

$$\mathbf{f}_m\mathbf{V}_r\gamma = \mathbf{f}_{m/d}\mathbf{f}_d\mathbf{V}_d\mathbf{V}_{r/d}\gamma = d(\mathbf{f}_{m/d}\mathbf{V}_{r/d}\gamma) = d(\mathbf{V}_{r/d}\mathbf{f}_{m/d})\gamma \equiv 0 \mod \mathscr{C}^2$$

because $r/d > 1$. To prove (27.5.10) note that the $\langle a + b\rangle$ relation of (27.2.11) implies that $\langle r\rangle\gamma \equiv r\gamma \mod \mathscr{C}^2$ for all γ and $r \in \mathbf{N}$.

Now let $r \mid m$, then we have

$$\mathbf{f}_m\mathbf{V}_r\gamma = \mathbf{f}_{m/r}\mathbf{f}_r\mathbf{V}_r\gamma = r\mathbf{f}_{m/r}\gamma \equiv \langle r\rangle\mathbf{f}_{m/r}\gamma \mod \mathscr{C}^2$$

■ (27.5.11) **Proof of Cartier's third theorem over characteristic zero rings** Let $\delta_1, \ldots, \delta_m \in \mathscr{C}$ be such that (27.5.6) holds. For each $n \in \mathbf{N}$, we then have a unique expression

(27.5.12) $$\mathbf{f}_n\delta_i = \sum_{r=1}^{\infty}\sum_{j=1}^{m} \mathbf{V}_r\langle c(n, r, j, i)\rangle\delta_j$$

We now define

$$(27.5.13)\quad c(p, r)_{i,j} = c(p, r, i, j), \qquad p \in \mathbf{P},\quad r \in \mathbf{N},\quad i, j \in \{1, \ldots, m\}$$

$$(27.5.14)\quad b(n)_{i,j} = c(n, 1, i, j), \qquad n \in \mathbf{N},\quad i, j \in \{1, \ldots, m\}$$

We claim that the matrices $c(p, r)$, $b(n)$ defined by (27.5.12)–(27.5.14) constitute an entwined pair of functions.

It follows from (27.5.6) that the classes mod $\mathscr{C}^2$ of the elements $\delta_1, \ldots, \delta_m$ are a basis for $\mathscr{C}^1/\mathscr{C}^2$; and by (27.5.12), (27.5.14) the matrices $b(n)$ are determined by the $\mathbf{f}_n\delta_i$ mod $\mathscr{C}^2$. We have

$$(27.5.15)\quad \mathbf{f}_n\mathbf{f}_p\delta_i = \mathbf{f}_{np}\delta_i \equiv \sum_{k=1}^{m} b(pn)_{k,i}\delta_k \mod \mathscr{C}^2$$

On the other hand, using Lemma (27.5.8), we have mod $\mathscr{C}^2$,

$$\begin{aligned}
\mathbf{f}_n\mathbf{f}_p\delta_i &= \mathbf{f}_n\left(\sum_{r=1}^{\infty}\sum_{j=1}^{m} \mathbf{V}_r\langle c(p, r, j, i)\rangle\delta_j\right)\\
&= \sum_{r=1}^{\infty}\sum_{j=1}^{m} \mathbf{f}_n\mathbf{V}_r\langle c(p, r, j, i)\rangle\delta_j\\
&\equiv \sum_{r|n}\sum_{j=1}^{m} \langle r\rangle\mathbf{f}_{n/r}\langle c(p, r, j, i)\rangle\delta_j\\
&= \sum_{r|n}\sum_{j=1}^{m} \langle rc(p, r, j, i)^{n/r}\rangle\mathbf{f}_{n/r}\delta_j\\
&\equiv \sum_{r|n}\sum_{j=1}^{m} \langle rc(p, r, j, i)^{n/r}\rangle \sum_{k=1}^{m} b(n/r)_{k,j}\delta_k\\
&\equiv \sum_{k=1}^{m}\left(\sum_{r|n}\sum_{j=1}^{m} \langle rc(p, r, j, i)^{n/r}b(n/r)_{k,j}\rangle\right)\delta_k
\end{aligned}$$

where we have used $\langle a + b\rangle \equiv \langle a\rangle + \langle b\rangle$ mod $\mathscr{C}^2$, Lemma (27.5.8), the additivity and continuity of the $\mathbf{f}_n$, the relations $\mathbf{f}_n\langle a\rangle = \langle a^n\rangle\mathbf{f}_n$, $\langle a\rangle\langle b\rangle = \langle ab\rangle$, and $\langle a\rangle\mathscr{C}^2 \subset \mathscr{C}^2$.

Comparing the result of this calculation with (27.5.15) gives that the b and c defined by (27.5.12)–(27.5.14) are indeed an entwined pair of functions. Let $F(X, Y)$ over A be the corresponding formal group law according to the entwined functions theorem (27.4.15). Then the calculations of (27.4.3) show that $\mathscr{C}(F; A)$ identifies with $\mathscr{C}$, with the standard $\mathbf{V}$-basis $\delta_1(t), \ldots, \delta_m(t)$ going to $\delta_1, \ldots, \delta_m$.

The remainder of this section concerns a proof of theorem (27.5.7) (= Cartier's third theorem), which works over *all* rings A. The first step consists of the construction of a "universal Cart(L_C)-module," where L_C is a certain, yet to be determined, universal ring.

■ (27.5.16) **Construction of a universal curve module** Choose $m \in \mathbf{N}$ and choose a set of elements $\delta_1, \ldots, \delta_m$. Let $\tilde{L}_C$ be the ring $\tilde{L}_C = \mathbf{Z}[C(n, r)_{i,j} | r \in \mathbf{N}, n \in \mathbf{N}\backslash\{1\}, i, j \in \{1, \ldots, m\}]$ of polynomials in the indeterminates $C(n, r)_{i,j}$. For convenience we also introduce $C(1, 1)_{i,j} = 0$ if $i \neq j$, $C(1, 1)_{i,i} = 1$, $C(1, r)_{i,j} = 0$ for all $r \in \mathbf{N}\backslash\{1\}$, $i, j \in \{1, \ldots, m\}$.

Now consider the set $\mathscr{C}$ of all formal expressions

$$\sum_{s=1}^{\infty} \sum_{j=1}^{m} \mathbf{V}_s \langle a_{s,j} \rangle \delta_j, \qquad a_{s,j} \in \tilde{L}_C \tag{27.5.17}$$

We now introduce the defining relations

$$\mathbf{f}_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^{m} \mathbf{V}_s \langle C(n, s)_{j,i} \rangle \delta_j \tag{27.5.18}$$

for all $n \in \mathbf{N}$. One can now use the calculation rules (16.2.1)–(16.2.3), (16.2.5)–(16.2.9) and the defining relations (27.5.18) to add expressions of the form (27.5.17) and to define $\mathbf{f}_r$ of such an expression, $r \in \mathbf{N}$.

To do this we start by showing how to rewrite any sum of the form

$$\sum_{s=1}^{\infty} \sum_{j=1}^{m} \sum_{t} \mathbf{V}_s \langle a_{s,j,t} \rangle \delta_j, \qquad a_{s,j,t} \in \tilde{L}_C \tag{27.5.19}$$

in the form (25.5.17). Here for each $s \in \mathbf{N}$, $j \in \{1, \ldots, m\}$, the index t runs over some finite index set which may depend on s and j.

For each $n \in \mathbf{N}$, let $\lambda(n)$ be the number of prime factors of n, i.e., $\lambda(1) = 0$ and if $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$, p_i a prime number, $r_i \in \mathbf{N}$, then $\lambda(n) = r_1 + \cdots + r_t$. One now proceeds as follows:

$$\begin{aligned} \sum_{s,j,t} \mathbf{V}_s \langle a_{s,j,t} \rangle \delta_j &= \sum_{j,t} \langle a_{1,j,t} \rangle \delta_j + \sum_{s \geq 2} \sum_{j,t} \mathbf{V}_s \langle a_{s,j,t} \rangle \delta_j \\ &= \sum_{j} \sum_{i=1}^{\infty} \mathbf{V}_i \langle b_{i,j} \rangle \mathbf{f}_i \delta_j + \sum_{s \geq 2} \sum_{j,t} \mathbf{V}_s \langle a_{s,j,t} \rangle \delta_j \end{aligned}$$

where $b_{i,j} = r_i(a_{1,j,1}, a_{1,j,2}, \ldots)$ with $r_1, r_2, \ldots$ the polynomials in k variables defined by

$$Z_1^n + \cdots + Z_k^n = \sum_{d|n} d r_d (Z_1, \ldots, Z_k)^{n/d}, \qquad n = 1, 2, \ldots \tag{27.5.20}$$

(cf. Section 16.2; of course k may depend on j). Now use (27.5.18) to rewrite (27.5.19) further as

$$\begin{aligned} &\sum_{j} \langle b_{1,j} \rangle \delta_j + \sum_{j} \sum_{i \geq 2} \mathbf{V}_i \langle b_{i,j} \rangle \sum_{l,k} \mathbf{V}_l \langle C(i, l)_{k,j} \rangle \delta_k + \sum_{s \geq 2} \sum_{j,t} \mathbf{V}_s \langle a_{s,j,t} \rangle \delta_j \\ &\quad = \sum_{j} \langle b_{1,j} \rangle \delta_j + \sum_{j,k} \sum_{i \geq 2} \sum_{l} \mathbf{V}_{il} \langle b'_{i,j} C(i, l)_{k,j} \rangle \delta_k + \sum_{s \geq 2} \sum_{j,t} \mathbf{V}_s \langle a_{s,j,t} \rangle \delta_j \\ &\quad = \sum_{j} \langle b_{1,j} \rangle \delta_j + \sum_{\lambda(s) \geq 1} \sum_{j} \sum_{t} \mathbf{V}_s \langle b'_{s,j,t} \rangle \delta_j \end{aligned}$$

for certain well determined $b'_{s,j,t} \in \tilde{L}_C$. And of course the summation set for t for a given s, j will now in general be different than the one in (27.5.19). For each $s \in \mathbf{N}$ with $\lambda(s) \geq 1$ (i.e., $s \geq 2$) write $s = p_s s'$, where p_s is the first prime number dividing s. We find an expression

$$\sum_j \langle b_{1,j}\rangle \delta_j + \sum_{\lambda(r)=1} \mathbf{V}_r \left(\sum_{s,j,t} \mathbf{V}_s \langle a'_{r,s,j,t}\rangle \delta_j \right) \tag{27.5.21}$$

where now the summation set for t may also depend on r. Now repeat the procedure given above for each of the interior sums

$$\sum_{s,j,t} \mathbf{V}_s \langle a'_{r,s,j,t}\rangle \delta_j$$

to obtain an expression

$$\sum_j \langle b_{1,j}\rangle \delta_j + \sum_{\lambda(r)=1} \mathbf{V}_r \sum_j \langle b_{r,1,j}\rangle \delta_j + \sum_{\lambda(r)=2} \mathbf{V}_r \left(\sum_{s,j,t} \mathbf{V}_s \langle a''_{r,s,j,t}\rangle \delta_j \right)$$

Now apply the same procedure to the interior sums in the third summand, ..., etc., ... After k steps we know the coefficients $x_{s,j}$ in

$$\sum_{s,j,t} \mathbf{V}_s \langle a_{s,j,t}\rangle \delta_j = \sum_{s,j} \mathbf{V}_s \langle x_{s,j}\rangle \delta_j \tag{27.5.22}$$

for all s with $\lambda(s) \leq k - 1$.

We now proceed to define $\mathbf{f}_n$ of an expression (27.5.17). Write

$$\begin{aligned} \mathbf{f}_n \left(\sum_{s,j} \mathbf{V}_s \langle a_{s,j}\rangle \delta_j \right) &= \sum_{s,j} d \mathbf{V}_{s/d} \mathbf{f}_{n/d} \langle a_{s,j}\rangle \delta_j \\ &= \sum_{s,j} \mathbf{V}_{s/d} d \langle a_{s,j}^{n/d}\rangle \mathbf{f}_{n/d} \delta_j \\ &= \sum_{s,j,r,k} d \mathbf{V}_{s/d} \langle a_{s,j}^{n/d}\rangle \mathbf{V}_r \langle C(n/d, r)_{k,j}\rangle \delta_k \\ &= \sum_{s,j,r,k} d \mathbf{V}_{rs/d} \langle a_{s/j}^{rn/d} C(n/d, r)_{k,j}\rangle \delta_k \end{aligned} \tag{27.5.23}$$

where $d = (s, n)$. This is a sum of the type (27.5.19), which then is put into the form (27.5.17) by the procedure outlined above.

To complete the picture we also define

$$\mathbf{V}_r \left(\sum_{s,j} \mathbf{V}_s \langle a_{s,j}\rangle \delta_j \right) = \sum_{s,j} \mathbf{V}_{rs} \langle a_{s,j}\rangle \delta_j$$

$$\langle a \rangle \left(\sum_{s,j} \mathbf{V}_s \langle a_{s,j}\rangle \delta_j \right) = \sum_{s,j} \mathbf{V}_s \langle a^s a_{s,j}\rangle \delta_j$$

We have now defined a topological abelian group $\mathscr{C}$ with operators $\langle a \rangle$, $\mathbf{V}_n$, $\mathbf{f}_n$ for all $a \in L_C$, $n \in \mathbf{N}$. (The topology is the obvious one.) Note that $\mathscr{C}$ is definitely not a Cart($\tilde{L}_C$) module. For one thing it is not at all clear that $\mathbf{f}_n$ is

additive and obviously $\mathbf{f}_n\mathbf{f}_m = \mathbf{f}_{nm}$ does not hold in general. Before discussing the relations one must introduce to make a variant of $\mathscr{C}$ a Cart(L_C) module over some quotient ring L_C of $\tilde{L}_C$ we note a homogeneity property. First make $\tilde{L}_C$ into a graded ring by giving $C(n, r)_{i,j}$ degree $nr - 1$ for all $n, r \in \mathbf{N}$, $i, j \in \{1, \ldots, m\}$. We then have

(27.5.24) **Lemma** Suppose that in the sum (27.5.19) each $a_{s,j,t}$ is homogeneous of degree $ks - 1$ for some $k \in \mathbf{N}$ independent of s, j, t. Then the $x_{s,j}$ in (27.5.22) are homogeneous of degree $ks - 1$.

Proof To prove this by induction it suffices to show that, under the hypothesis stated, the $b_{1,j}$ and $a'_{r,s,j,t}$ of (27.5.21) are of degree $k - 1$ and $krs - 1$ respectively. Now $b_{1,j} = a_{1,j,1} + a_{1,j,2} + \cdots$ which is homogeneous of degree $k - 1$. As to the $a'_{r,s,j,t}$, they are of two types, viz. 1°) $a'_{r,s,j,t} = a_{rs,j,t}$ which by hypothesis is homogeneous of degree $krs - 1$, and 2°) $a'_{r,s,j,t} = b^l_{i,j'}C(i, l)_{k,j'}$ with $il = rs$. Now from (27.5.20) we see that $r_i(Z_1, \ldots, Z_k)$ is homogeneous of degree i (if each Z_i is given degree 1) so that $b_{i,j'} = r_i(a_{1,j,1}, a_{1,j,2}, \ldots)$ is homogeneous of degree $i(k - 1)$. It follows that $a'_{r,s,j,t} = b^l_{i,j'}C(i, l)_{k,j'}$ is homogeneous of degree $li(k - 1) + il - 1 = krs - 1$. This proves the lemma.

■ (27.5.25) **Corollary** Let $\mathbf{f}_n\mathbf{f}_l\delta_i = \mathbf{f}_n(\sum_{s,j}\mathbf{V}_s\langle C(l, s)_{j,i}\rangle\delta_j) = \sum_{s,j}\mathbf{V}_s\langle y_{n,l,s,j,i}\rangle\delta_j$ where the $y_{n,l,s,j,i}$ are calculated as in (27.5.16). Then $y_{n,l,s,j,i}$ is homogeneous of degree $nls - 1$.

Proof In this particular case of (27.5.23) we have $a_{s,j} = C(l, s)_{j,i}$. Thus $a^{rn/d}_{s,j}C(n/d, r)$ is homogeneous of degree $d^{-1}rn(ls - 1) + d^{-1}nr - 1 = d^{-1}rnls - 1 = (d^{-1}rs)nl - 1$ and the corollary follows by lemma (27.5.24).

■ (27.5.26) **Lemma** If $l > 1$ then $y_{n,l,t,i,j} \equiv nC(l, nt)_{i,j}$ mod(decomposables). (Here (decomposables) stands for the ideal of $\tilde{L}_C$ generated by all products of the form $C(n, r)_{i,j}C(s, t)_{k,l}$ with $n, s \in \mathbf{N}\backslash\{1\}$, $r, t \in \mathbf{N}$. $i, j, k, l \in \{1, \ldots, m\}$).

Proof From (27.5.23) we have

$$\sum_{t,j}\mathbf{V}_t\langle y_{n,l,t,j,i}\rangle\delta_j = \sum_{s,r,j,k}\mathbf{V}_{rs/d}d\langle C(l, s)^{nr/d}_{j,i}C(n/d, r)_{k,j}\rangle\delta_k$$

where $d = (s, n)$ in the sum on the right. Choose a fixed $t \in \mathbf{N}$. By the rewriting procedure of (27.5.16) a summand in the sum on the right can contribute to $y_{n,l,t,j,i}$ iff $d^{-1}rs \leq t$. Moreover, if this contribution is to be nonzero modulo decomposables, we must in addition have $d = nr$, $d^{-1}n = 1$, $r = 1$, $k = j$ (because $l > 1$). It follows that s is a multiple of n and $s \leq tn$ so that the only contributions to $y_{n,l,t,j,i}$ which are possibly nonzero modulo decomposables come from

$$\sum_{a=1}^{t}\mathbf{V}_a n\langle C(l, an)_{j,i}\rangle\delta_j$$

However $n\langle C(l, an)_{j,i}\rangle\delta_j = \langle nC(l, an)_{j,i}\rangle\delta_j +$ (terms which are zero modulo decomposables). The lemma follows.

(27.5.27) **Remark** By definition one has $y_{1,n,s,j,i} = y_{n,1,s,j,i} = C(n, s)_{j,i}$ so that lemma (27.5.26) does not hold for $l = 1$.

(27.5.28) **The universal ring** L_C Let $\mathfrak{A}$ be the homogeneous ideal in $\tilde{L}_C$ generated by the polynomials

$$C(nl, t)_{ji} - y_{n,l,t,j,i}, \qquad n, l, t \in \mathbf{N}, \quad i, j \in \{1, \ldots, m\}$$

and define $L_C = \tilde{L}_C/\mathfrak{A}$.

■ (27.5.29) **Theorem** $L_C \simeq \mathbf{Z}[T(n)_{i,j} \mid n = 2, 3, \ldots; i, j \in \{1, \ldots, m\}]$ as a graded ring with degree$(T(n)_{i,j}) = n - 1$.

Proof The ring L_C is graded because the relations (27.5.28) are homogeneous by Corollary (27.5.25). Let $L_C^{(t)}$ be its homogeneous summand of degree $t - 1$ and let $M^{(t)}$ be the submodule of $L_C^{(t)}$ generated by the decomposables. Then $L_C^{(t)}/M^{(t)}$ is generated (as an abelian group) by the $C(s, r)$ with $sr = t$. Now by lemma (27.5.26) and the defining relations (27.5.28) we see that modulo decomposables

$$C(rs, t)_{i,j} \equiv rC(s, rt)_{i,j}$$

for all $i, j \in \{1, \ldots, m\}$, $s \in \mathbf{N}\backslash\{1\}$, $r \in \mathbf{N}$. It follows that if s is not a prime number, $s \neq 1$, and p is a prime number dividing s, then

(27.5.30) $$C(s, r)_{i,j} \equiv p^{-1}sC(p, p^{-1}sr)_{i,j}$$

It readily follows that $L_C^{(t)}/M^{(t)}$ is the abelian group generated by the $C(p, p^{-1}t)_{i,j}$, where p runs through all prime divisors of t, subject to the relations

(27.5.31) $$qC(p, p^{-1}t)_{i,j} \equiv pC(q, q^{-1}t)_{i,j}$$

for all prime number divisors p and q of t. If t is a power of a prime number p, $t = p^r$, this means that $L_C^{(t)}/M^{(t)}$ is a free abelian group of rank m^2 generated by the classes of the $T(t)_{i,j} = C(p, p^{-1}t)_{i,j}$. If t is not a power of a prime number, let $P(t)$ be the set of prime numbers dividing t. Choose $\kappa(p) \in \mathbf{Z}$ such that

(27.5.32) $$\sum_{p \in P(t)} p\kappa(p) = 1$$

Let

$$T(t)_{i,j} = \sum_{p \in P(t)} \kappa(p)C(p, p^{-1}t)_{i,j}$$

it then follows from (27.5.31) and (27.5.32) that $L_C^{(t)}/M^{(t)}$ is the free abelian group of rank m^2 generated by the classes of $T(t)_{i,j}$. This proves the theorem.

■ (27.5.33) **Remark** [Construction of a "universal Cart(L_C)-module" (continued).] Let $\mathscr{C}_C$ be the set of all expressions $\sum_{s,j} \mathbf{V}_s\langle a_{s,j}\rangle\delta_j$ with $a_{s,j} \in L_C$.

Now calculate sums and $\mathbf{f}_r\gamma$, $\langle a\rangle\gamma$, $\mathbf{V}_r\gamma$ for $\gamma \in \mathscr{C}_C$ as in (27.5.16). Then $\mathscr{C}_C$ is in fact a Cart(L_C) module. One has of course $\mathbf{f}_n\mathbf{f}_l\delta_i = \mathbf{f}_{nl}\delta_i$ by the relations defining L_C. And, using this, one can now prove directly that the $\langle a\rangle$, $\mathbf{f}_n$, $\mathbf{V}_n$ are additive and that all the relations (16.2.1)–(16.2.9) hold. This also follows from the isomorphism result below, cf. Remark (27.5.38).

■ (27.5.34) **The homomorphism** η_C Let $F(X, Y)$ be any m-dimensional formal group law over a ring A. Let $\delta_1(t), \ldots, \delta_m(t)$ be the standard $\mathbf{V}$-basis for $\mathscr{C}(F; A)$. Then we have unique expressions

$$\mathbf{f}_n\delta_i(t) = \sum_{s=1}^{\infty}\sum_{j=1}^{m} \mathbf{V}_s\langle c(n, s)_{j,i}\rangle\delta_j(t)$$

Now define $\tilde{\eta}\colon \tilde{L}_C \to A$ by $\tilde{\eta}(C(n, s)_{i,j}) = c(n, s)_{i,j}$. Because $\mathbf{f}_n\mathbf{f}_l\delta_i(t) = \mathbf{f}_{nl}\delta_i(t)$ in $\mathscr{C}(F; A)$ for all n, l, i it follows that

$$\tilde{\eta}(y_{n,l,s,j,i}) = c(nl, s)_{j,i}$$

for all $s, l, n \in \mathbf{N}, i, j \in \{1, \ldots, m\}$. Therefore $\tilde{\eta}$ induces a homomorphism of rings $\eta_F\colon L_C \to A$. We can in particular apply this to the case $F(X, Y) = F_R(X, Y)$, the universal curvilinear m-dimensional formal group law over $\mathbf{Z}[\mathrm{R}] = \mathbf{Z}[R_n(i, j) \mid n \in \mathbf{N}\backslash\{1\}, i, j \in \{1, \ldots, m\}]$. This gives us a homomorphism

$$\eta_C\colon L_C \to \mathbf{Z}[R]$$

■ (27.5.35) **Theorem** The homomorphism η_C of (27.5.34) is an isomorphism of graded rings.

Proof Let $f_R(X)$, the logarithm of $F_R(X, Y)$, be equal to $f_R(X) = \sum_{n=1}^{\infty} b_n(R)X^n$. A formula for $b_n(R)$ is (12.2.1). Let $R_n(i, j)$ have degree $n - 1$. Then $b_n(R)$ is homogeneous of degree $n - 1$. Let $\delta_1(t), \ldots, \delta_m(t)$ be the standard $\mathbf{V}$-basis for $\mathscr{C}(F_R; \mathbf{Z}[R])$, and let

$$\mathbf{f}_p\delta_i(t) = \sum_{s,j} \mathbf{V}_s\langle c(p, s)_{j,i}\rangle\delta_j(t)$$

Then we have (cf. (27.4.7))

$$pb_{pn}(R) = \sum_{d\mid n} b_{n/d}(R)c(p, d)^{n/d} \tag{27.5.36}$$

It follows by induction that $c(p, s) \in \mathbf{Z}[R]$ is homogeneous of degree $ps - 1$. Now $b_{pn}(R) \equiv p^{-1}R_{pn}$ modulo decomposables if n is a power of p and $b_{pn}(R) \equiv R_{pn}$ modulo decomposables if n is not a power of p, (cf. (12.2.1)). It follows that η_C satisfies

$$\eta_C(C(p, p^{r-1})_{i,j}) \equiv R_{p^r}(i, j) \qquad \text{mod(decomposables)}$$

and

$$\eta_C(C(p, s)_{i,j}) \equiv pR_{ps}(i, j) \qquad \text{mod(decomposables)}$$

if s is not a power of p. Hence $\eta_C(T_{p^r}(i,j)) \equiv R_{p^r}(i,j)$ mod(decomposables) and if s is not a power of a prime number

$$\eta_C(T_s(i,j)) = \eta_C\left(\sum_{p \in P(s)} \kappa(p)C(p, p^{-1}s)\right) \equiv \sum_{p \in P(s)} \kappa(p)pR_s(i,j) = R_s(i,j)$$

modulo(decomposables). Here $P(s)$ and the $\kappa(p)$ are as in (27.5.29). It follows that η_C is indeed an isomorphism (homogeneous of degree zero).

■ (27.5.37) **Proof of Cartier's third theorem** Let $\mathscr{C}$ be such that (27.5.2)–(27.5.6) hold. Let $\delta_1, \ldots, \delta_m$ be a V-basis for $\mathscr{C}$. Then every $\mathbf{f}_n\delta_i$ can be uniquely written as a convergent sum (cf. (27.5.6))

$$\mathbf{f}_n\delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^{m} \mathbf{V}_s\langle c(n,s)_{j,i}\rangle\delta_j, \qquad c(n,s)_{j,i} \in A$$

Now define $\tilde{\eta}$: $\tilde{L}_C \to A$ by $\tilde{\eta}(C(n,s)_{j,i}) = c(n,s)_{j,i}$. Because $\mathbf{f}_n\mathbf{f}_l = \mathbf{f}_{nl}$ in $\mathscr{C}$ we have that

$$\tilde{\eta}(C(nl,s)_{j,i} - y_{n,l,s,j,i}) = 0$$

for all n, l, s, j, i so that $\tilde{\eta}$ factorizes through L_C to define a homomorphism η: $L_C \to A$. Now let ϕ: $\mathbf{Z}[R] \to A$ be equal to $\phi = \eta\eta_C^{-1}$, where η_C is the isomorphism of (27.5.34) and (27.5.35). Then $F(X, Y) = \phi_* F_R(X, Y)$ is a formal group law over A such that $\mathscr{C}(F; A)$ as a topological group with operators. The isomorphism is given by $\delta_i(t) \mapsto \delta_i$, where $\delta_1(t), \ldots, \delta_m(t)$ is the standard V-basis of $\mathscr{C}(F; A)$.

■ (27.5.38) **Remark** The module $\mathscr{C}_C$ of (27.5.33) above is the module of curves of the formal group law $(\eta_C^{-1})_* F_R(X, Y)$ over L_C.

27.6 Proof of the entwined functions theorem

First we show how the concept of a pair of entwined functions relates to functional equation type considerations. Essentially the relations (27.4.8) enable us to write $a(n) = n^{-1}b(n)$ in such a way that the series $\sum a(n)X^n$ is seen to satisfy a higher dimensional functional equation.

■ (27.6.1) Let A be a characteristic zero ring and let ϕ: $L \to A$ be a homomorphism and $b(n)$, $c(p, r)$ the associated pair of entwined functions, i.e., $b(n)_{i,j} = \phi(B(n)_{i,j})$, $c(p, r)_{i,j} = \phi(C(p, r)_{i,j})$.

Choose a prime number p and choose an ordering of the prime numbers p_1, p_2, p_3, ... such that $p = p_1$; choose $n \in \mathbf{N}$ and write n as a product

$$n = p_1^{r_1}p_2^{r_2} \cdots p_t^{r_t}, \quad r_i \in \mathbf{N} \cup \{0\} \quad \text{for } i = 1, \ldots, t-1, \quad r_t \in \mathbf{N}$$

Then we have

(27.6.2)
$$a(n) = n^{-1}b(n)$$
$$= \sum \prod_{i=1}^{t} p_i^{-s_i} c(p_i, d_{i,1})^{(e_{i,1})} \cdots c(p_i, d_{i,s_i})^{(e_{i,s_i})}$$

where the sum is over all sequences of elements of $\mathbf{P} \times \mathbf{N}$ of the form

$(p_1, d_{1.1}), \ldots, (p_1, d_{1.s_1}); \quad (p_2, d_{2.1}), \ldots, (p_2, d_{2.s_2}); \ldots; \quad (p_t, d_{t.1}), \ldots, (p_t, d_{t.s_t})$

such that

(27.6.3) $\quad (p_1 d_{1.1}) \cdots (p_1 d_{1.s_1})(p_2 d_{2.1}) \cdots (p_t d_{t.1}) \cdots (p_t d_{t.s_t}) = n$

(27.6.4) $\qquad\qquad s_1, \ldots, s_{t-1} \in \mathbf{N} \cup \{0\}, \qquad s_t \in \mathbf{N}$

(27.6.5) $d_{i.j}$ is divisible by no other prime numbers than $p_1, \ldots, p_i$; and the exponents $e_{i.j}$ in (27.6.2) are given by the formula

(27.6.6) $\quad e_{i.j} = (p_1 d_{1.1}) \cdots (p_1 d_{1.s_1}) \cdots (p_i d_{i.1}) \cdots (p_i d_{i.j-1})$

Here the products

$$c(p_i, d_{i.1})^{(e_{i.1})} \cdots c(p_i, d_{i.s_i})^{(e_{i.s_i})}$$

and the products

$$(p_k d_{k.1}) \cdots (p_k d_{k.l})$$

occurring in (27.6.2) and (27.6.6) are to be interpreted as 1 if s_i resp. l is equal to zero. Also $e_{1.1} = 1$.

For example, we have

$$\begin{aligned}(27.6.7)\quad a(p_1 p_2^2) = {} & p_1^{-1} p_2^{-2} c(p_1, 1) c(p_2, 1)^{(p_1)} c(p_2, 1)^{(p_1 p_2)} \\ & + p_2^{-2} c(p_2, p_1) c(p_2, 1)^{(p_1 p_2)} \\ & + p_1^{-1} p_2^{-1} c(p_1, 1) c(p_2, p_2)^{(p_1)} \\ & + p_2^{-2} c(p_2, 1) c(p_2, p_1)^{(p_2)} + p_2^{-1} c(p_2, p_2 p_1)\end{aligned}$$

where the various sequences and exponents are respectively

$(p_1, 1), \quad (p_2, 1), \quad (p_2, 1)$	$1, p_1, p_1 p_2$
$(p_1, 1), \quad (p_2, p_2)$	$1, p_1$
$(p_2, 1), \quad (p_2, p_1)$	$1, p_2$
$(p_2, p_1), \quad (p_2, 1)$	$1, p_1 p_2$
$(p_2, p_1 p_2)$	1

Formula (27.6.2) is much more difficult to write down than to prove. One simply writes $a(n) = a(rp_t)$ with $r = p_t^{-1} m$. (Note that one "takes out" the *last* prime number (in the chosen ordering) that divides n.) Then we have

$$a(n) = n^{-1} b(n) = n^{-1} \sum_{d|r} d b(r/d) c(p_t, d)^{(r/d)}$$

$$= \sum_{d|r} a(r/d) \frac{c(p_t, d)^{(r/d)}}{p_t}$$

and now use induction on the $a(r/d)$.

■ (27.6.8) **One prime number versions of L** We now construct rings $L(p<)$ which for a given prime number p do the same job for us over $\mathbf{Z}_{(p)}$ as the universal entwined functions ring L does over $\mathbf{Z}$. The notation $L(p<)$ is meant to suggest: "that L corresponding to an ordering of $\mathbf{P}$ for which p is smallest."

Choose a prime number p and choose an ordering $p_1, p_2, \ldots$ of the set of prime numbers such that $p = p_1$. For each pair (p_i, d) such that d is not divisible by any prime number p_j with $j > i$, take n^2 indeterminates $C(p_i, d)_{k,l}$, $k, l \in \{1, \ldots, m\}$ and let $L(p<)$ be the ring of polynomials in the $C(p_i, d)_{k,l}$ over $\mathbf{Z}$. There is of course a natural inclusion $L(p<) \to \tilde{L}$ (cf. (27.4.12) for $\tilde{L}$) and hence a natural homomorphism

$$L(p<) \to \tilde{L} \to \tilde{L}/\mathfrak{a} = L \tag{27.6.9}$$

For each $n \in \mathbf{N}$, $n \geq 2$, let $A(n)$ be the matrix with coefficients in $L(p<) \otimes \mathbf{Q}$ given by formula (27.6.2) with all the small $c(p_i, d_{i,j})$ replaced by the matrices of indeterminates $C(p_i, d_{i,j})$. Let $Q(n)$ be the sum of those terms in $A(n)$ for which $s_1 = 0$ (i.e., for which the denominator is prime to p_1). For example (cf. (27.6.7)), we have

$$Q(p_1 p_2^2) = p_2^{-2} C(p_2, p_1) C(p_2, 1)^{(p_1 p_2)} + p_2^{-2} C(p_2, 1) C(p_2, p_1)^{(p_2)} + p_2^{-1} C(p_2, p_2 p_1)$$

Let $A(1) = Q(1) = I_m$ and

$$q(X) = \sum_{n=1}^{\infty} Q(n) X^n \tag{27.6.10}$$

$$g_{p<}(X) = \sum_{n=1}^{\infty} A(n) X^n \tag{27.6.11}$$

where as usual X^n is short for the column vector $(X_1^n, \ldots, X_m^n)$. Then $g_{p<}(X)$ satisfies the functional equation

$$g_{p<}(X) = q(X) + \sum_{i=1}^{\infty} p^{-1} C(p, p^{i-1}) g_{p<}^{(p^i)}(X^{p^i}) \tag{27.6.12}$$

This follows immediately from (27.6.2) (with lowercase a's and c's replaced by capitals).

Now let $G_{p<}(X, Y)$ be the formal group law with logarithm $g_{p<}(X)$. The functional equation lemma says that $G_{p<}(X, Y)$ is a formal group law over $L(p<) \otimes \mathbf{Z}_{(p)}$.

■ (27.6.13) **Proof of Theorem (27.4.15) in the characteristic zero case** Let A be a characteristic zero ring and $b(n)$, $c(p, d)$ a pair of entwined functions with values in $A^{m \times m}$. We define

$$f(X) = \sum_{n=1}^{\infty} n^{-1} b(n) X^n, \qquad F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{27.6.14}$$

Then by (27.6.2) and (27.6.8) we know that $F(X, Y)$ can be obtained from $G_{p^<}(X, Y)$ by specializing the $C(p_i, d)_{k,l}$ to $c(p_i, d)_{k,l}$. It follows that $F(X, Y)$ has its coefficients in $A \otimes \mathbf{Z}_{(p)}$. But this holds for every prime number p; hence $F(X, Y)$ has its coefficients in A (cf. Chapter III, sublemma (17.6.6)). Note also that $F(X, Y)$ is curvilinear. Because A is of characteristic zero, the $b(n)$ determine (inductively) the $c(p, d)$ (cf. (27.4.8)), and hence the calculations of (27.4.3) show that the pair of entwined functions associated to $F(X, Y)$ is precisely the pair $b(n)$, $c(p, d)$ we started out with.

■ (27.6.15) **Proof of Theorem (27.4.15)** Let $\delta_1(t), \ldots, \delta_m(t)$ be the standard $\mathbf{V}$-basis for $\mathscr{C}(F_R; \mathbf{Z}[R])$. Write

$$\mathbf{f}_p \delta_i(t) = \sum_{s=1}^{\infty} \sum_{j=1}^{m} \mathbf{V}_s \langle c(p, s)_{j,i} \rangle \delta_j(t)$$

Then we have already seen (cf. (27.5.35)) that $c(p, s) \equiv p v_p(s)^{-1} R_{ps}$ mod(decomposables), where $v_p(s) = p$ if s is a power of p and $v_p(s) = 1$ otherwise. Hence

$$\vartheta(C(p, s)_{i,j}) \equiv p v_p(s)^{-1} R_{ps}(i, j) \qquad \text{mod(decomposables)}$$

and it follows that ϑ is surjective. Note also (cf. (27.5.35) again) that ϑ is homogeneous of degree zero. Let $f_R(X)$, the logarithm of $F_R(X, Y)$, be equal to

$$f_R(X) = \sum_{n=1}^{\infty} b_n(R) X^n$$

Then, cf. (12.2.1), $n b_n(R) \equiv n v(n)^{-1} R_n$ mod(decomposables) and it follows that

$$\vartheta(B(n)_{i,j}) \equiv n v(n)^{-1} R(n)_{i,j} \qquad \text{mod(decomposables)}$$

Now the relations of (27.4.12) show that $L \otimes \mathbf{Q}$ is generated by the $B(n)_{i,j}$ and in fact they show that $L \otimes \mathbf{Q}$ is the free polynomial ring over $\mathbf{Q}$ generated by the $B(n)_{i,j}$, $n \in \mathbf{N} \backslash \{1\}$, $i, j \in \{1, \ldots, m\}$; cf. also (27.6.13). It follows that $\vartheta \otimes \mathbf{Q}$: $L \otimes \mathbf{Q} \to \mathbf{Q}[R]$ is injective. Q.E.D.

27.7 Cartier–Dieudonné modules in the one prime number case

Choose a prime p and let A be a $\mathbf{Z}_{(p)}$-algebra. Then the theory of Cartier–Dieudonné modules of Sections 27.1–27.6 can be simplified considerably by considering $\mathscr{C}_p(F; A)$, the subgroup of p-typical curves instead of $\mathscr{C}(F; A)$. We start with some generalities concerning $\mathscr{C}_p(F; A)$.

■ (27.7.1) ***p*-typical curves** Recall that $\gamma(t) \in \mathscr{C}_p(F; A)$ if and only if $\mathbf{f}_l \gamma(t) = 0$ for all prime numbers $l \neq p$. This defines a subfunctor $F(X, Y) \mapsto \mathscr{C}_p(F; A)$ of the functor $\mathscr{C}(-; A)$. The group $\mathscr{C}_p(F; A)$ is a closed subgroup of $\mathscr{C}(F; A)$ with its topology defined by the subgroups $\mathscr{C}_p^{(i)}(F; A) = \mathscr{C}_p(F; A) \cap \mathscr{C}^{p^i}(F; A)$. It is of course complete in this topology. The subfunctor $\mathscr{C}_p(-; A)$ of

$\mathscr{C}(-; A)$ is stable under the operators $\mathbf{f}_p$, $\mathbf{V}_p$, and $\langle a\rangle$ for all $a \in A$. (It is not stable under the $\mathbf{V}_n$ with n not a power of p.)

The operator $\mathbf{V}_p$ maps $\mathscr{C}_p^{(i)}(F; A)$ to $\mathscr{C}_p^{(i+1)}(F; A)$ and induces isomorphisms

$$\mathscr{C}_p^{(i)}(F; A)/\mathscr{C}_p^{(i+1)}(F; A) \xrightarrow{\sim} \mathscr{C}_p^{(i+1)}(F; A)/\mathscr{C}_p^{(i+2)}(F; A)$$

■ (27.7.2) Now suppose in addition that $F(X, Y)$ is p-typical. Then the standard basis curves $\delta_1(t)$, $\delta_2(t)$, ... are p-typical, and every p-typical curve can be written as a convergent sum

$$\gamma(t) = \sum_{i \in I} \sum_{n=0}^{\infty} \mathbf{V}_p^n \langle a_{n,i}\rangle \delta_i(t) \tag{27.7.3}$$

All this is either contained in Chapter III, Section 16.3 or is proved in exactly the same way as the corresponding facts for $\mathscr{C}(-; A)$ in 27.1.

■ (27.7.4) **The formal group law** $\hat{W}_{p^\infty}(X; Y)$ Let $\hat{W}_{p^\infty}(X; Y)$ be the formal group law defined by the Witt addition polynomials $\Sigma_1(X; Y)$, $\Sigma_p(X; Y)$, ... that involve only $X_1, X_p, X_{p^2}, \ldots; Y_1, Y_p, Y_{p^2}, \ldots$. That is, with this numbering of the indeterminates the index set of $\hat{W}_{p^\infty}(X; Y)$ is $\{1, p, p^2, \ldots\}$.

Let $\gamma_{w.p}(t)$ be the curve with components $(\gamma_{w.p})_1(t) = t$ and $(\gamma_{w.p})_{p^n}(t) = 0$ for all $n \in \mathbf{N}$.

There is a natural (quotient) homomorphism of formal group laws over $\mathbf{Z}$:

$$\imath(X)\colon \hat{W}(X; Y) \to \hat{W}_{p^\infty}(X, Y)$$

defined by the $\{1, p, p^2, \ldots\}$-tuple of power series in $X_1, X_2, X_3, \ldots$

$$\imath_1(X) = X_1, \qquad \imath_p(X) = X_p, \qquad \imath_{p^2}(X) = X_{p^2}, \qquad \ldots$$

(This is a homomorphism precisely because $\Sigma_{p^r}(X; Y)$ involves only $X_1, X_p, \ldots, X_{p^r}; Y_1, Y_p, \ldots, Y_{p^r}$.)

We obviously have

$$\imath(\gamma_w(t)) = \gamma_{w.p}(t)$$

There is also a (subformal group law) homomorphism $\varepsilon_p(X)\colon \hat{W}_{p^\infty}(X, Y) \to \hat{W}(X, Y)$ over $\mathbf{Z}_{(p)}$ defined by the $\mathbf{N}$-tuple of power series in $X_1, X_p, X_{p^2}, \ldots$

$$\varepsilon_p(X) = f_w^{-1}\begin{pmatrix} X_1 \\ 0 \\ \vdots \\ 0 \\ X_p + pX_1 \\ 0 \\ \vdots \\ 0 \\ X_{p^2} + pX_p^p + p^2X_1^{p^2} \\ \vdots \end{pmatrix}$$

where $f_w(X)$, the logarithm of $\hat{W}(X, Y)$ is as in (27.1.19). Note that this homomorphism $\varepsilon_p(X)$ is *not* defined over $\mathbf{Z}$ but only over $\mathbf{Z}_{(p)}$.

The one prime number version of the representation theorem (= Cartier's first theorem) is now

■ (27.7.5) **Theorem** Let $F(X, Y)$ be a formal group law over a ring A (which does not need to be a $\mathbf{Z}_{(p)}$-algebra) and let $\gamma(t) \in \mathscr{C}_p(F; A)$. Then there exists a unique homomorphism $\alpha_\gamma(X)$: $\hat{W}_{p^\infty}(X, Y) \to F(X, Y)$ such that $\alpha_\gamma(\gamma_{w,p}(t)) = \gamma(t)$. This sets up an isomorphism of topological groups $\mathbf{FG}_A(W_{p^\infty}(X, Y), F(X, Y)) \simeq \mathscr{C}_p(F; A)$.

Proof Let $\tilde{\alpha}_\gamma(X)$ be the unique homomorphism $\hat{W}(X, Y) \to F(X, Y)$ such that $\tilde{\alpha}_\gamma(\gamma_w(t)) = \gamma(t)$. The defining formula for $\tilde{\alpha}_\gamma(X)$ (cf. (27.1.20))

$$\tilde{\alpha}_\gamma(X) = \sum_{n=1}^{\infty} {}^{\hat{w}}\mathbf{f}_n \gamma(X_n)$$

shows that $\tilde{\alpha}_\gamma(X)$ depends only on $X_1, X_p, X_{p^2}, \ldots$ because $\mathbf{f}_n\gamma(t) = 0$ for all n that are not powers of p since $\gamma(t)$ is p-typical. This means that $\tilde{\alpha}_\gamma(X)$ factors through $\iota(X)$ (i.e., $\tilde{\alpha}_\gamma(X) = \alpha_\gamma(\iota(X))$ for some $\alpha_\gamma(X)$); and because $\iota(X)$ takes $\gamma_w(t)$ to $\gamma_{w.p}(t)$, we have $\alpha_\gamma(\gamma_{w.p}(t)) = \gamma(t)$; cf. (27.7.4). The homomorphism $\alpha_\gamma(X)$ is also unique because if $\alpha_\gamma(X)$ and $\alpha(X)$ are different, then so are $\alpha_\gamma(\iota(X))$ and $\alpha(\iota(X))$.

■ (27.7.6) **Remarks** The homomorphism $\iota(X)$: $\hat{W}(X, Y) \to \hat{W}_{p^\infty}(X, Y)$ corresponds to the inclusions $\mathscr{C}_p(F; A) \to \mathscr{C}(F; A)$ and the homomorphism $\varepsilon_p(X)$: $\hat{W}_{p^\infty}(X, Y) \to \hat{W}(X, Y)$ (over $\mathbf{Z}_p$) corresponds to p-typification. All this in the sense that the following diagrams are commutative:

$$\begin{array}{ccc} \mathbf{FG}_A(\hat{W}_{p^\infty}(X, Y), F(X, Y)) & \xrightarrow{\sim} & \mathscr{C}_p(F; A) \\ \Big\downarrow{\scriptstyle \mathbf{FG}_A(\iota(X), F(X, Y))} & & \Big\downarrow \\ \mathbf{FG}_A(\hat{W}(X, Y), F(X, Y)) & \xrightarrow{\sim} & \mathscr{C}(F; A) \end{array}$$

$$\begin{array}{ccc} \mathbf{FG}_A(\hat{W}(X, Y), F(X, Y)) & \xrightarrow{\sim} & \mathscr{C}(F; A) \\ \Big\downarrow{\scriptstyle \mathbf{FG}_A(\varepsilon_p(X), F(X, Y))} & & \Big\downarrow{\scriptstyle \varepsilon_p^F} \\ \mathbf{FG}_A(\hat{W}_{p^\infty}(X, Y), F(X, Y)) & \xrightarrow{\sim} & \mathscr{C}_p(F; A) \end{array}$$

where the horizontal isomorphisms are those of Theorems (27.7.5) and (27.1.14) (and where the vertical arrows in the second diagram are only defined if A is a $\mathbf{Z}_{(p)}$-algebra).

■ (27.7.7) **Operators** An operator of the functor $\mathscr{C}_p(-; A)$ is of course a functorial endomorphism of $\mathscr{C}_p(-; A)$, and using Theorem (27.7.5) one has the obvious analogue of Proposition (27.2.5) giving us in this case a one-one correspondence between operators of $\mathscr{C}_p(-; A)$ and p-typical curves in

$\hat{W}_{p^\infty}(X, Y)$, i.e., elements of $\mathscr{C}_p(\hat{W}_{p^\infty}; A)$. The standard **V**-basis for $\hat{W}_{p^\infty}$ is $\delta_1(t)$, $\delta_p(t)$, ... These are all p-typical curves, and (27.7.3) together with (27.1.16) now gives us that every element in $\mathscr{C}_p(\hat{W}_{p^\infty}; A)$ can be uniquely written as a sum

$$\gamma(t) = \sum_{n=0}^{\infty} \sum_{i=0}^{\infty} \mathbf{V}_p^n \langle a_{n,i} \rangle \mathbf{f}_p^i \gamma_{w.p}(t)$$

giving us a unique expression for every operator of $\mathscr{C}_p(-; A)$ in terms of $\mathbf{V}_p$, $\mathbf{f}_p$, and $\langle a \rangle$'s:

$$\sum_{n,i=0}^{\infty} \mathbf{V}_p^n \langle a_{n,i} \rangle \mathbf{f}_p^i \tag{27.7.8}$$

with for every $n \in \mathbf{N}$ only finitely many $a_{n,i} \neq 0$.

■ (27.7.9) **The ring** $\mathrm{Cart}_p(A)$ Let $\mathrm{Cart}_p(A)$ be the ring of operators of $\mathscr{C}_p(-; A)$. Then $\mathrm{Cart}_p(A)$ consist of expressions like (27.7.8); the multiplication and addition are given by the calculation rules

$$\langle a \rangle \mathbf{V}_p = \mathbf{V}_p \langle a^p \rangle, \qquad \mathbf{f}_p \langle a \rangle = \langle a^p \rangle \mathbf{f}_p$$

$$\mathbf{f}_p \mathbf{V}_p = p$$

$$\langle a + b \rangle = \sum_{n=0}^{\infty} \mathbf{V}_p^n \langle r_{p^n}(a, b) \rangle \mathbf{f}_p^n$$

where the $r_{p^n}(a, b)$ are as in (27.2.11).

■ (27.7.10) **Theorem** (Cartier's second theorem in the case of one prime number) Let $F(X, Y)$ and $G(X, Y)$ be two formal group laws over a $\mathbf{Z}_{(p)}$-algebra A and let $\beta: \mathscr{C}_p(F; A) \to \mathscr{C}_p(G; A)$ be a continuous additive homomorphism that commutes with the operators $\langle a \rangle$, $\mathbf{f}_p$, and $\mathbf{V}_p$. Then there is a unique homomorphism $\alpha(X): F(X, Y) \to G(X, Y)$ such that $\mathscr{C}_p(\alpha; A) = \beta$.

Proof It suffices to prove this for $F(X, Y)$ and $G(X, Y)$ p-typical formal group laws because every formal group law over A is isomorphic to a p-typical one (Chapter III, Theorem (15.2.9)). Now every curve $\gamma(t) \in \mathscr{C}(F; A)$ can be written uniquely as a sum

$$\gamma(t) = \sum_{(p.n)=1} \mathbf{V}_n \gamma_n(t), \qquad \gamma_n(t) \in \mathscr{C}_p(F; A) \tag{27.7.11}$$

(cf. Chapter III, Lemma (16.3.8)). We now use this to extend $\beta: \mathscr{C}_p(F; A) \to \mathscr{C}_p(G; A)$ to an additive continuous homomorphism $\hat{\beta}: \mathscr{C}(F; A) \to \mathscr{C}(G; A)$ that commutes with $\mathbf{f}_r$, $\mathbf{V}_r$, and $\langle a \rangle$ for all $r \in \mathbf{N}$, $a \in A$. We take (of course)

$$\hat{\beta}\gamma(t) = \sum_{(p.n)=1} \mathbf{V}_n \beta(\gamma_n(t)) \tag{27.7.12}$$

Note that this is the only possibility if we want $\hat{\beta}$ to be additive and continuous and such that $\hat{\beta}$ commutes with the $\mathbf{V}_r$. The map $\hat{\beta}$ defined by (27.7.12) is

certainly additive and continuous. We prove that $\hat{\beta}$ commutes with all $\mathbf{V}_l$, $\mathbf{f}_l$ for l a prime number and with $\langle a\rangle$ for all $a \in A$. (This suffices because $\mathbf{V}_r\mathbf{V}_s = \mathbf{V}_{rs}$, $\mathbf{f}_r\mathbf{f}_s = \mathbf{f}_{rs}$.) Let $\gamma(t)$ be as in (27.7.11), then the corresponding unique expressions for $\langle a\rangle\gamma(t)$, $\mathbf{V}_p\gamma(t)$, $\mathbf{f}_p\gamma(t)$, $\mathbf{V}_l\gamma(t)$, $\mathbf{f}_l\gamma(t)$ where l is a prime number $\neq p$ are respectively

$$\langle a\rangle\gamma(t) = \sum_{(p,n)=1} \mathbf{V}_n(\langle a^n\rangle\gamma_n(t))$$

$$\mathbf{V}_p\gamma(t) = \sum_{(p,n)=1} \mathbf{V}_n(\mathbf{V}_p\gamma_n(t))$$

$$\mathbf{f}_p\gamma(t) = \sum_{(p,n)=1} \mathbf{f}_p\mathbf{V}_n\gamma_n(t) = \sum_{(n,p)=1} \mathbf{V}_n(\mathbf{f}_p\gamma_n(t))$$

$$\mathbf{V}_l\gamma(t) = \sum_{(p,n)=1} \mathbf{V}_{nl}\gamma_n(t)$$

$$\mathbf{f}_l\gamma(t) = \sum_{\substack{(p,n)=1\\(n,l)=1}} \mathbf{V}_n\mathbf{f}_l\gamma_n(t) + \sum_{\substack{(p,n)=1\\l\mid n}} l\mathbf{V}_{n/l}\gamma_n(t)$$

$$= \sum_{\substack{(p,n)=1\\l\mid n}} \mathbf{V}_{n/l}(l\gamma_n(t))$$

(where one uses of course that $\mathbf{f}_l\gamma_n(t) = 0$ because $\gamma_n(t) \in \mathscr{C}_p(F; A)$). It follows that

$$\hat{\beta}(\langle a\rangle\gamma(t)) = \sum_{(p,n)=1} \mathbf{V}_n\beta(\langle a^n\rangle\gamma_n(t))$$

$$= \sum_{(p,n)=1} \mathbf{V}_n\langle a^n\rangle\beta(\gamma_n(t)) = \langle a\rangle\hat{\beta}(\gamma(t))$$

$$\hat{\beta}(\mathbf{V}_p\gamma(t)) = \sum_{(p,n)=1} \mathbf{V}_n\beta(\mathbf{V}_p\gamma_n(t))$$

$$= \sum_{(p,n)=1} \mathbf{V}_n\mathbf{V}_p\beta(\gamma_n(t)) = \mathbf{V}_p\hat{\beta}(\gamma(t))$$

$$\hat{\beta}(\mathbf{f}_p\gamma(t)) = \sum_{(n,p)=1} \mathbf{V}_n\beta(\mathbf{f}_p\gamma_n(t)) = \sum_{(p,n)=1} \mathbf{V}_n\mathbf{f}_p\beta(\gamma_n(t))$$

$$= \sum_{(n,p)=1} \mathbf{f}_p\mathbf{V}_n\beta(\gamma_n(t)) = \mathbf{f}_p\hat{\beta}(\gamma(t))$$

$$\hat{\beta}(\mathbf{V}_l\gamma(t)) = \sum_{(p,n)=1} \mathbf{V}_{nl}\beta(\gamma_n(t)) = \mathbf{V}_l\hat{\beta}(\gamma(t))$$

$$\hat{\beta}(\mathbf{f}_l\gamma(t)) = \sum_{\substack{(p,n)=1\\l\mid n}} \mathbf{V}_{n/l}\beta(l\gamma_n(t)) = \sum_{\substack{(p,n)=1\\l\mid n}} \mathbf{V}_{n/l}l\beta(\gamma_n(t))$$

$$= \sum_{\substack{(p,n)=1\\l\mid n}} \mathbf{f}_l\mathbf{V}_l\mathbf{V}_{n/l}\beta(\gamma_n(t)) + \sum_{\substack{(p,n)=1\\(l,n)=1}} \mathbf{f}_l\mathbf{V}_n\beta(\gamma_n(t))$$

$$= \sum_{(p,n)=1} \mathbf{f}_l\mathbf{V}_n\beta(\gamma_n(t)) = \mathbf{f}_l\hat{\beta}(\gamma(t))$$

(where, again, one uses that $\mathbf{f}_l \mathscr{C}_p(G; A) = 0$). By Corollary (27.3.5) there is a unique $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $\mathscr{C}(\alpha; A) = \hat{\beta}$. Then $\mathscr{C}_p(\alpha; A) = \beta$, and $\alpha(X)$ is unique because $\hat{\beta}$ is uniquely determined by β (cf. just below (27.7.12)).

■ (27.7.13) We have now proved the one prime analogues of Cartier's first and second theorems. It is the third theorem, however, that is really substantially easier to prove in the one prime number case.

■ (27.7.14) **Theorem** Let $\mathscr{C}$ be a complete Hausdorff topological group with additive continuous operators $\mathbf{V}$ and $\mathbf{f}$ and $\langle a \rangle$ for all $a \in A$ such that the relations (27.7.9) hold. Suppose that $\mathscr{C} = \varprojlim \mathscr{C}/\mathbf{V}^n\mathscr{C}$ (i.e., the topology of $\mathscr{C}$ is defined by the subgroups $\mathbf{V}^n\mathscr{C}$), that $\mathbf{V}$ is injective, and that $\mathscr{C}/\mathbf{V}\mathscr{C}$ is free of finite rank over A. (This quotient is an A-module via the operators $\langle a \rangle$.) Then there exists a formal group law $F(X, Y)$ over A of dimension $\operatorname{rank}_A(\mathscr{C}/\mathbf{V}\mathscr{C})$ such that $\mathscr{C}(F, A) \xrightarrow{\sim} \mathscr{C}$ and such that under this isomorphism $\mathscr{C}_p^{(n)}(F; A)$ corresponds to $\mathbf{V}^n\mathscr{C}$, $\mathbf{V}_p$ to $\mathbf{V}$, $\mathbf{f}_p$ to $\mathbf{f}$, and $\langle a \rangle$ to $\langle a \rangle$.

Proof Let $\delta_1, \ldots, \delta_m$ be a set of elements of $\mathscr{C}$ such that their classes mod $\mathbf{V}\mathscr{C}$ are a basis for $\mathscr{C}/\mathbf{V}\mathscr{C}$. Then one shows as usual that the $\delta_1, \ldots, \delta_m$ are a $\mathbf{V}$-basis for $\mathscr{C}$, i.e., that every element $\gamma \in \mathscr{C}$ can be written uniquely as a convergent sum

$$\gamma = \sum_{n=0}^{\infty} \sum_{j=1}^{m} \mathbf{V}^n \langle a_{n,j} \rangle \delta_j$$

($\mathbf{V}$ injective and "$\mathscr{C}^{(n)} = \mathbf{V}^n\mathscr{C}$" together see to it that $\mathbf{V}$ induces isomorphisms $\mathscr{C}^{(n)}/\mathscr{C}^{(n+1)} \to \mathscr{C}^{(n+1)}/\mathscr{C}^{(n+2)}$ and $\langle a \rangle \mathscr{C}^{(n)} \subset \mathscr{C}^{(n)}$ follows from $\langle a \rangle \mathbf{V}^m = \mathbf{V}^m \langle a^{p^m} \rangle$.)

In particular, we have that the $\mathbf{f}\delta_i$ can be written as a unique convergent sum

$$\mathbf{f}\delta_i = \sum_{n=0}^{\infty} \sum_{j=1}^{m} \mathbf{V}^n \langle c(n, j, i) \rangle \delta_j$$

Let $F_V(X; Y)$ be the m-dimensional universal p-typical formal group law constructed in Chapter II, Section 10.3, with logarithm

$$f_V(X) = \sum_{n=1}^{\infty} a_n(V) X^{p^n}$$

Let $\delta_1(t), \ldots, \delta_m(t)$ be the standard $\mathbf{V}$-basis of $\mathscr{C}_p(F_V; \mathbf{Z}[V])$. Then we claim

$$\mathbf{f}_p \delta_i(t) = \sum_{n=0}^{\infty} \sum_{j=1}^{m} {}^{F_V}(\mathbf{V}_p^n \langle V_{n+1}(j, i) \rangle \delta_j(t)) \tag{27.7.15}$$

Admitting this for the moment, it follows that if ϕ: $\mathbf{Z}[V] \to A$ is the homomorphism ϕ: $V_n(i, j) \to c(n-1, i, j)$, then $\mathscr{C}_p(\phi * F_V(X, Y); A) = \mathscr{C}$ where moreover the standard basis $\delta_1(t), \ldots, \delta_m(t)$ goes into $\delta_1, \ldots, \delta_m$.

It remains to prove (27.7.15). We recall that over characteristic zero rings $\mathbf{f}_p$ is characterized by

$$(27.7.16) \qquad f(\gamma(t)) = \sum_{i=1}^{\infty} x_i t^i \quad \Rightarrow \quad f(\mathbf{f}_p \gamma(t)) = \sum_{i=1}^{\infty} p x_{pi} t^i$$

cf. Chapter III, (15.1.9) or (27.4.5). Let $a_n(V)(i)$ be the ith column of the matrix $a_n(V)$, then

$$f_V(\delta_i(t)) = \sum_{n=1}^{\infty} a_n(V)(i) t^{p^n}$$

so that by (27.7.16)

$$(27.7.17) \qquad f_V(\mathbf{f}_p \delta_i(t)) = \sum_{n=0}^{\infty} p a_{n+1}(V)(i) t^{p^n}$$

On the other hand, we have, writing $V_{n+1}(i)$ for the ith column of V_{n+1},

$$(27.7.18) \quad f_V\left(\sum_{n,j} F^r \mathbf{V}_p^n \langle V_{n+1}(j, i) \rangle \delta_j(t) \right) = \sum_{n=0}^{\infty} \sum_{j=1}^{m} f_V(V_{n+1}(j, i) \delta_j(t^{p^n}))$$

$$= \sum_{n=0}^{\infty} f_V(V_{n+1}(i) t^{p^n})$$

$$= \sum_{n=0}^{\infty} \sum_{r=0}^{\infty} a_r(V)(V_{n+1}(i) t^{p^n})^{p^r}$$

$$= \sum_{l=0}^{\infty} \left(\sum_{d=0}^{l} a_d(V) V_{l+1-d}(i)^{p^d} \right) t^{p^l}$$

$$= \sum_{l=0}^{\infty} p a_{l+1}(V)(i) t^{p^l}$$

where we have used that

$$a_{l+1}(V) = p^{-1} a_l(V) V_1^{(p^l)} + \cdots + p^{-1} a_1(V) V_l^{(p)} + p^{-1} V_{l+1}$$

(cf. Chapter II, (10.4.3)), and where (as usual) $V_r(i)^{p^d}$ is short for the column vector $(V_r(1, i)^{p^d}, \ldots, V_r(m, i)^{p^d})$.

Comparing (27.7.17) and (27.7.18) we see that we have proved (27.7.15) and hence the theorem.

■ (27.7.19) **Remarks**

(i) We have not used that A is a $\mathbf{Z}_{(p)}$-algebra.

(ii) Formula (27.7.15) gives us of course the structure of the Cartier–Dieudonné module $\mathcal{C}_p(F; A)$ for any formal group law of the form $\phi_* F_V(X, Y)$ in terms of the $\phi(V_n(i, j)) \in A$.

(iii) There are no relations that the structure constants $c(n, j, i)$ must satisfy, a completely different situation compared to the case where two or

more prime numbers are noninvertible. In fact the proof above gives us a one-one correspondence between p-typical formal group laws and modules $\mathscr{C}$ over $\mathrm{Cart}_p(A)$ of the type described together with a particular $\mathbf{V}$-basis of $\mathscr{C}$.

■ (27.7.20) **Definition** We shall (following Lazard) call modules $\mathscr{C}$ over $\mathrm{Cart}_p(A)$ *reduced* if $\mathscr{C} = \varprojlim \mathscr{C}/\mathbf{V}^i\mathscr{C}$ (also topologically with $\mathscr{C}/\mathbf{V}^i\mathscr{C}$ discrete), $\mathbf{V}: \mathscr{C} \to \mathscr{C}$ is injective and $\mathscr{C}/\mathbf{V}\mathscr{C}$ is a free A-module. Then the $\mathrm{Cart}_p(A)$ modules that come from a (finite dimensional) formal group law over A are precisely the reduced $\mathrm{Cart}_p(A)$ modules (of finite $\mathbf{V}$-dimension), where finite $\mathbf{V}$-dimension means that there is a finite $\mathbf{V}$-basis.

28 On the Classification of Commutative Formal Group Laws over an Algebraically Closed Field of Characteristic $p > 0$

All formal group laws in this Section 28 will be finite dimensional.

28.1 On the rings $\mathrm{Cart}(A)$ and $\mathrm{Cart}_p(A)$

We want to give a more pleasant description of especially the ring $\mathrm{Cart}_p(A)$ in case A is a perfect field of characteristic p. To this end, first a lemma:

■ (28.1.1) **Lemma** Let $d = (n, i)$. Then we have in $\mathrm{Cart}(A)$

$$(\mathbf{V}_m\langle a\rangle\mathbf{f}_n)(\mathbf{V}_i\langle b\rangle\mathbf{f}_j) = d\mathbf{V}_{mi/d}\langle a^{i/d}b^{n/d}\rangle\mathbf{f}_{nj/d}$$

Proof Use $\mathbf{f}_n\mathbf{V}_i = \mathbf{f}_{n/d}\mathbf{f}_d\mathbf{V}_d\mathbf{V}_{i/d} = d\mathbf{f}_{n/d}\mathbf{V}_{i/d} = d\mathbf{V}_{i/d}\mathbf{f}_{n/d}$.

■ (28.1.2) Now let for the moment A be a torsion free ring without nilpotents. Let $\mathfrak{A}_2 \subset \mathrm{Cart}(A)$ be the right ideal of all elements $\sum \mathbf{V}_m\langle a_{m,n}\rangle\mathbf{f}_n$ such that $a_{1,n} = 0$ for all n. Note that $\mathrm{Cart}(A)/\mathfrak{A}_2$ is a free A-module with the classes of the $\mathbf{f}_l$ mod $\mathfrak{A}_2$ as basis. For each $l \in \mathbf{N}$ we calculate $\mathbf{f}_l x$ mod $\mathfrak{A}_2$ for $x \in \mathrm{Cart}(A)$. We find using (28.1.1)

$$\mathbf{f}_l(\sum \mathbf{V}_m\langle a_{m,n}\rangle\mathbf{f}_n) \equiv \sum_{d|l} d a_{d,n}^{l/d}\mathbf{f}_{nl/d} \mod \mathfrak{A}_2$$

Note that if A is torsion free and without nilpotents, then the congruences above for each l determine $\sum \mathbf{V}_m\langle a_{m,n}\rangle\mathbf{f}_n$ completely. We also note that $x \in \mathrm{Cart}(A)$ is of the form

$$(*) \qquad x = \sum_{n=1}^{\infty} \mathbf{V}_n\langle a_{n,n}\rangle\mathbf{f}_n$$

if and only if we have for all $l \in \mathbf{N}$

$$\mathbf{f}_l x \equiv \lambda\mathbf{f}_l$$

for some $\lambda \in A$. This is a property which is preserved under sums and products, and it follows that the set of all elements of $\mathrm{Cart}(A)$ of the form $(*)$ is a subring

of $\mathrm{Cart}(A)$, at least if A is torsion free, and without nilpotent elements. But then this holds in general because a surjective ringhomomorphism $\phi: B \to A$ induces a surjective ring homomorphism $\mathrm{Cart}(B) \to \mathrm{Cart}(A)$, $\sum \mathbf{V}_m\langle b_{m,n}\rangle \mathbf{f}_n \mapsto \sum \mathbf{V}_m\langle \phi(b_{m,n})\rangle \mathbf{f}_n$.

■ (28.1.3) We are now going to identify the subring $R(A) = \{\sum \mathbf{V}_n\langle a_n\rangle \mathbf{f}_n\}$ of $\mathrm{Cart}(A)$. This is obviously a functorial subring (cf. (28.1.2)) and we define functor morphisms w_n by the formula

$$w_n\left(\sum_{r=1}^{\infty} \mathbf{V}_r\langle a_r\rangle \mathbf{f}_r\right) = \sum_{d|n} d a_d^{n/d}$$

If we can show that the w_n define functorial ring homomorphisms $R(A) \to A$, we shall have identified the ring functor $R(-)$ with the ring functor $W(-)$ of generalized Witt vectors (cf. Chapter III, Theorem (15.3.9)). To this end, first observe that obviously

$$w_n\left(\sum_{r=1}^{\infty} \mathbf{V}_r\langle a_r\rangle \mathbf{f}_r\right) = \sum_{r=1}^{\infty} w_n(\mathbf{V}_r\langle a_r\rangle \mathbf{f}_r) \tag{28.1.4}$$

It therefore suffices to show that

$$w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m + \mathbf{V}_m\langle b\rangle \mathbf{f}_m) = w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m) + w_n(\mathbf{V}_m\langle b\rangle \mathbf{f}_m) \tag{28.1.5}$$

and

$$w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m \mathbf{V}_s\langle b\rangle \mathbf{f}_s) = w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m) w_n(\mathbf{V}_s\langle b\rangle \mathbf{f}_s) \tag{28.1.6}$$

Now using the formula for $\langle a + b\rangle$ (cf., e.g., (27.2.11)) we find

$$\begin{aligned} w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m + \mathbf{V}_m\langle b\rangle \mathbf{f}_m) &= w_n(\mathbf{V}_m(\langle a\rangle + \langle b\rangle)\mathbf{f}_m) \\ &= w_n\left(\mathbf{V}_m\left(\sum_{i=1}^{\infty} \mathbf{V}_i\langle r_i(a, b)\rangle \mathbf{f}_i\right)\mathbf{f}_m\right) \\ &= w_n\left(\sum_{i=1}^{\infty} \mathbf{V}_{mi}\langle r_i(a, b)\rangle \mathbf{f}_{mi}\right) \\ &= \sum_{md|n} md\, r_d(a, b)^{n/md} \\ &= m\left(\sum_{d|(n/m)} d\, r_d(a, b)^{n/md}\right) \end{aligned}$$

where of course we (must) interpret the sum as 0 if m does not divide n. By the definition of the $r_d(a, b)$ this last sum is equal to

$$ma^{n/m} + mb^{n/m} = w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m) + w_n(\mathbf{V}_m\langle b\rangle \mathbf{f}_m)$$

if m divides n. This proves (28.1.5). Formula (28.1.6) is easier. Let $d = (m, s)$, then by Lemma (28.1.1)

$$w_n(\mathbf{V}_m\langle a\rangle \mathbf{f}_m \mathbf{V}_s\langle b\rangle \mathbf{f}_s) = w_n(d\mathbf{V}_{ms/d}\langle a^{s/d} b^{m/d}\rangle \mathbf{f}_{ms/d})$$

which is equal to 0 if $d^{-1}ms$ does not divide n and equal to $ms\, a^{n/m} b^{n/s}$ if $d^{-1}ms$

does divide n. The same holds for the product $w_n(\mathbf{V}_m\langle a\rangle\mathbf{f}_m)w_n(\mathbf{V}_s\langle b\rangle\mathbf{f}_s)$ because m and s both divide n if and only if msd^{-1} divides n.

■ (28.1.7) In exactly the same manner, using the same calculations, one shows that $R_p(A) = \{\sum \mathbf{V}_p^n\langle a_n\rangle\mathbf{f}_p^n\}$ is a subring of $\mathrm{Cart}_p(A)$ which identifies with $W_{p^\infty}(A)$.

We sum up the results obtained in a proposition:

■ (28.1.8) **Proposition**

(i) The map $(a_1, a_2, \ldots)\mapsto\sum_{n=1}^{\infty}\mathbf{V}_n\langle a_n\rangle\mathbf{f}_n$ defines an injective functorial ring homomorphism $W(A)\to\mathrm{Cart}(A)$.

(ii) The map $(a_0, a_1, a_2, \ldots)\to\sum_{n=0}^{\infty}\mathbf{V}_p^n\langle a_n\rangle\mathbf{f}_p^n$ defines an injective functorial ring homomorphism $W_{p^\infty}(A)\to\mathrm{Cart}_p(A)$.

■ (28.1.9) We now identify $W(A)$ and $W_{p^\infty}(A)$ with their images in $\mathrm{Cart}(A)$ and $\mathrm{Cart}_p(A)$ and shall try to describe $\mathrm{Cart}_p(A)$ as a certain overring of $W_{p^\infty}(A)$. To do this without unreasonable possibilities of confusion we make a change of notation. We have defined in Chapter III a Frobenius functorial ring endomorphism $\mathbf{f}_p$ of the functor $W_{p^\infty}(-)$. To avoid confusion with the symbol (or element) $\mathbf{f}_p$ occurring in $\mathrm{Cart}_p(A)$ we shall from now on in this chapter use σ to denote the Frobenius endomorphism of the ring functor $W_{p^\infty}(-)$.

■ (28.1.10) We first note that every element of $\mathrm{Cart}_p(A)$ can be written as a sum

$$\sum_{n,m}\mathbf{V}_p^m\langle a_{m,n}\rangle\mathbf{f}_p^n = x_0 + \sum_{i=1}^{\infty}x_i\mathbf{f}_p^i + \sum_{j=1}^{\infty}\mathbf{V}_p^j y_j \tag{28.1.11}$$

with $x_i, y_j\in W_{p^\infty}(A)$. Next let $x = \sum_{n=0}^{\infty}\mathbf{V}_p^n\langle a_n\rangle\mathbf{f}_p^n\in W_{p^\infty}(A)$ and let us calculate $\mathbf{f}_p x$. We find

$$\begin{aligned}\mathbf{f}_p x = \mathbf{f}_p\left(\sum_{n=0}^{\infty}\mathbf{V}_p^n\langle a_n\rangle\mathbf{f}_p^n\right) &= \langle a_0^p\rangle\mathbf{f}_p + \sum_{n=1}^{\infty}\mathbf{f}_p\mathbf{V}_p^n\langle a_n\rangle\mathbf{f}_p^n\\ &= \langle a_0^p\rangle\mathbf{f}_p + \left(\sum_{n=1}^{\infty}p\mathbf{V}_p^{n-1}\langle a_n\rangle\mathbf{f}_p^{n-1}\right)\mathbf{f}_p\\ &= y\mathbf{f}_p\end{aligned}$$

for a certain element y of $W_{p^\infty}(A)$, viz.

$$y = \langle a_0^p\rangle + p\sum_{m=0}^{\infty}\mathbf{V}_p^m\langle a_{m+1}\rangle\mathbf{f}_p^m$$

To identify y, we calculate $w_{p^n}(y)$ for all $n\in\mathbf{N}\cup\{0\}$. We find

$$\begin{aligned}w_{p^n}(y) &= (a_0^p)^{p^n} + pw_{p^n}(a_1, a_2, \ldots)\\ &= a_0^{p^{n+1}} + p(a_1^{p^n} + pa_2^{p^{n-1}} + \cdots + p^n a_{n+1})\\ &= w_{p^{n+1}}(a_0, a_1, a_2, \ldots)\\ &= w_{p^{n+1}}(x)\end{aligned}$$

and this, everything being functorial, identifies y as $\sigma(x)$ where σ is the Frobenius endomorphism of $W_{p^\infty}(-)$. We have found the following calculation rule in $\mathrm{Cart}_p(A)$ as an overring of $W_{p^\infty}(A)$:

$$\mathbf{f}_p x = \sigma(x)\mathbf{f}_p \tag{28.1.12}$$

Similarly one finds

$$x\mathbf{V}_p = \mathbf{V}_p\sigma(x) \tag{28.1.13}$$

And of course we still have that

$$\mathbf{f}_p\mathbf{V}_p = p \in W_{p^\infty}(A) \tag{28.1.14}$$

Also recall that $\mathbf{V}_p\mathbf{f}_p \in \mathrm{Cart}_p(A)$ is an element of $W_{p^\infty}(A)$, viz.

$$\mathbf{V}_p\mathbf{f}_p = (0, 1, 0, 0, \ldots) \in W_{p^\infty}(A) \tag{28.1.15}$$

We have obtained a description of $\mathrm{Cart}_p(A)$ as the ring of all expressions (28.1.11) in the symbols $\mathbf{f}_p$ and $\mathbf{V}_p$ with coefficients in $W_{p^\infty}(A)$ and the calculation rules (28.1.12)–(28.1.15). This description is not yet quite complete because we have neglected to take along the "convergence condition" for elements $\sum \mathbf{V}_p^m\langle a_{m,n}\rangle\mathbf{f}_p^n$ of $\mathrm{Cart}_p(A)$, which says that for every $m \in \mathbf{N}$ there are only finitely many $n \in \mathbf{N}$ such that $a_{m,n} \neq 0$. This translates into the condition that in (28.1.11) we must have $\lim_{i\to\infty} x_i = 0$ in $W_{p^\infty}(A)$. That is, if a_{i,n_i} is the first coefficient of $x_i = \sum \mathbf{V}_p^n\langle a_{i,n}\rangle\mathbf{f}_p^n$ that is nonzero, then n_i must go to infinity as i goes to infinity.

(Note that the topology on $W_{p^\infty}(A)$ defined by the ideals $\{(0, \ldots, 0, a_{n+1}, a_{n+2}, \ldots)\}$ and the topology of $W_{p^\infty}(A)$ as a subring of the topological ring $\mathrm{Cart}_p(A)$ coincide.)

Now suppose that A is of characteristic $p > 0$, then (cf. Proposition (17.3.16) of Chapter III)

$$p = \mathbf{f}_p\mathbf{V}_p(1, 0, 0, \ldots) = \mathbf{f}_p(0, 1, 0, 0, \ldots) = (0, 1, 0, 0, \ldots)$$

so in this case we have $\mathbf{f}_p\mathbf{V}_p = \mathbf{V}_p\mathbf{f}_p = p$ in $\mathrm{Cart}_p(A)$.

Finally, suppose that A is a perfect field of characteristic $p > 0$, then $W_{p^\infty}(A)$ is the unique unramified complete discrete valuation ring of characteristic zero with residue field A and σ is an automorphism of A (cf. Chapter III, Proposition (17.4.17)). This means that we can also write $\mathbf{V}_p x$ as $\mathbf{V}_p x = \sigma^{-1}(x)\mathbf{V}_p$ and that we can move $\mathbf{f}_p$ and $\mathbf{V}_p$ left or right at will. We now have the following description of $\mathrm{Cart}_p(k)$ if k is a perfect field of characteristic $p > 0$.

■ (28.1.16) **Proposition** Let k be a perfect field of characteristic $p > 0$ and $W_{p^\infty}(k)$ its ring of Witt vectors. Then $\mathrm{Cart}_p(k)$ is the ring of all expressions

$$x_0 + \sum_{i=1}^{\infty} x_i\mathbf{V}^i + \sum_{i=1}^{\infty} y_i\mathbf{f}^i$$

in two symbols **f** and **V** with coefficients in $W_{p^\infty}(k)$ with the extra condition that $\lim_{i\to\infty} y_i = 0$. The calculation rules are

$$\mathbf{f}x = \sigma(x)\mathbf{f}, \qquad \mathbf{V}x = \sigma^{-1}(x)\mathbf{V}, \qquad \mathbf{fV} = \mathbf{Vf} = p$$

28.2 The property "finite height" of formal group laws

In this section (28.2) k is a perfect field of characteristic $p > 0$ and $F(X, Y)$ is a formal group law of finite dimension over k.

■ (28.2.1) In Chapter IV, Section 18 we defined $F(X, Y)$ to be of finite height if $k[\![X_1, X_2, \ldots, X_m]\!]$ was of finite rank over the subring $k[\![H_1, \ldots, H_m]\!]$ where H_i is the ith component of the m-tuple of power series $[p]_F(X)$, and we claimed (without proof except in the case $m = 1$) that then this rank is of the form p^h and we defined h as the height of $F(X, Y)$.

Consider $\mathscr{C}_p(F; k)/[p]_F\mathscr{C}_p(F; k)$. We claim that this is a k-vector space (with the vector space structure given by the operators $\langle a\rangle$ for $a \in k$). To prove this we (must) show that $\langle a + b\rangle - \langle a\rangle - \langle b\rangle$ maps $\mathscr{C}_p(F; k)$ into $[p]_F\mathscr{C}_p(F; k)$. Now $\langle a + b\rangle - \langle a\rangle - \langle b\rangle$ is of the form

$$\langle a + b\rangle - \langle a\rangle - \langle b\rangle = \sum_{n=1}^{\infty} \mathbf{V}^n\langle a_n\rangle\mathbf{f}^n$$

Now $\mathbf{Vf} = \mathbf{fV} = p$, so if $n \geq 1$,

$$\mathbf{V}^n\langle a\rangle\mathbf{f}^n\gamma(t) = \mathbf{V}^n\mathbf{f}^n\langle\sigma^{-n}(a)\rangle\gamma(t) \in [p^n]_F\mathscr{C}(F; k)$$

(where we have also used σ for the (compatible) automorphism $a \mapsto a^p$ of k). So $\mathscr{C}_p(F; k)/[p]_F\mathscr{C}_p(F; k)$ is a k-vector space. In this section we show that this is a finite dimensional vector space iff $F(X, Y)$ is of finite height and that $h = \dim_k(\mathscr{C}_p(F; k)/[p]_F\mathscr{C}_p(F, k))$.

To do this we use a result on closed submodules of $\mathrm{Cart}_p(k)$-modules $\mathscr{C}$ which are of the type $\mathscr{C}_p(F; k)$.

■ (28.2.2) **Proposition** Let $\mathscr{C}$ be a complete Hausdorff $\mathrm{Cart}_p(k)$-module such that $\mathscr{C} = \varprojlim \mathscr{C}/\mathbf{V}^n\mathscr{C}$, such that $\dim_k(\mathscr{C}/\mathbf{V}\mathscr{C}) < \infty$ and such that **V** is injective. Let $\mathscr{D}$ be a closed submodule of $\mathscr{C}$. Then there exists a **V**-basis $\gamma_1, \ldots, \gamma_m$ of $\mathscr{C}$ and a disjoint partition $I_\infty \cup I_0 \cup I_1 \cup I_2 \cup \cdots$ of $\{1, \ldots, m\}$ (almost all of the I_j are empty) such that the following holds: if

$$\gamma = \sum_{n=0}^{\infty}\sum_{i=1}^{m} \mathbf{V}^n\langle a_{n,i}\rangle\gamma_i$$

is the unique expression of γ in terms of the **V**-basis $\{\gamma_1, \ldots, \gamma_m\}$, then $\gamma \in \mathscr{D}$ if and only if $a_{n,i} = 0$ if $i \in I_l$ and $n < l$. (In particular we have $a_{n,i} = 0$ for all n if $i \in I_\infty$ for all $\gamma \in \mathscr{D}$.)

Proof Consider the subgroups $\mathscr{D} \cap \mathbf{V}^n\mathscr{C}$ of $\mathscr{D}$ and let $\mathrm{gr}_n(\mathscr{D}) = \mathscr{D} \cap \mathbf{V}^n\mathscr{C}/\mathscr{D} \cap \mathbf{V}^{n+1}\mathscr{C}$, $\mathrm{gr}_n(\mathscr{C}) = \mathbf{V}^n\mathscr{C}/\mathbf{V}^{n+1}\mathscr{C}$. Then $\mathrm{gr}_n(\mathscr{D})$ is a subvector space of $\mathrm{gr}_n(\mathscr{C})$. (The vector space structure in $\mathrm{gr}_n(\mathscr{C})$ is induced by the operators $\langle a\rangle\colon \mathbf{V}^n\mathscr{C} \to \mathbf{V}^n\mathscr{C}$.) Applying $\mathbf{V}$ gives us *semilinear* k-vector space embeddings

$$\mathbf{V}\colon \mathrm{gr}_n(\mathscr{C}) \to \mathrm{gr}_{n+1}(\mathscr{C}), \qquad \mathbf{V}\colon \mathrm{gr}_n(\mathscr{D}) \to \mathrm{gr}_{n+1}(\mathscr{D}) \tag{28.2.3}$$

which, because k is perfect, gives us subvector spaces $\mathbf{V}\mathrm{gr}_n(\mathscr{C})$ and $\mathbf{V}\mathrm{gr}_n(\mathscr{D})$ of $\mathrm{gr}_{n+1}(\mathscr{C})$ and $\mathrm{gr}_{n+1}(\mathscr{D})$, respectively. For each $n \in \mathbf{N} \cup \{0\}$, let Γ_n be a subvector space of $\mathrm{gr}_n(\mathscr{D})$ such that

$$\mathrm{gr}_n(\mathscr{D}) = \Gamma_n \oplus \mathbf{V}\mathrm{gr}_{n-1}(\mathscr{D}), \qquad \mathrm{gr}_0(\mathscr{D}) = \Gamma_0 \tag{28.2.4}$$

and for each n choose elements $\tilde{\gamma}_{i.n} \in \mathscr{D} \cap \mathbf{V}^n\mathscr{C}$ such that their classes in $\mathrm{gr}_n(\mathscr{D})$ are a basis for Γ_n and let $\gamma_{i.n} \in \mathscr{C}$ be such that $\mathbf{V}^n\gamma_i = \tilde{\gamma}_i$. If $\Gamma_n = 0$, then there are no $\tilde{\gamma}_{i.n}$ and $\gamma_{i.n}$. We claim that the γ_i thus found are part of a $\mathbf{V}$-basis of $\mathscr{C}$. To prove this it suffices to show that all these γ_i are linearly independent mod $\mathbf{V}\mathscr{C}$. Let $\gamma_{i_1.n_1}, \ldots, \gamma_{i_r.n_r}$ be a finite set of these γ's. Let n be the maximum of the n_i. Now by (28.2.3) and (28.2.4) we know that

$$\mathrm{gr}_n(\mathscr{C}) \supset \mathrm{gr}_n(\mathscr{D}) = \mathbf{V}^n\Gamma_0 \oplus \mathbf{V}^{n-1}\Gamma_1 \oplus \cdots \oplus \mathbf{V}\Gamma_{n-1} \oplus \Gamma_n$$

so that the $\mathbf{V}^n\gamma_{i_1.n_1}, \ldots, \mathbf{V}^n\gamma_{i_r.n_2}$ are linearly independent in $\mathrm{gr}_n(\mathscr{C})$ which proves our contention because $\mathbf{V}^n$ induces a semilinear isomorphism $\mathrm{gr}_0(\mathscr{C}) \to \mathrm{gr}_n(\mathscr{C})$. (This also shows that $\Gamma_n = 0$ for n sufficiently large.) Let $\{\delta_1, \ldots, \delta_s\}$ be the union of all the $\gamma_{i_1.n_1}$ thus found and complete this to a $\mathbf{V}$-basis $\{\delta_1, \ldots, \delta_m\}$ of $\mathscr{C}$. Then $\{\delta_1, \ldots, \delta_m\}$ falls into disjoint subsets

$$\{\delta_1, \ldots, \delta_{i_0}\} \cup \{\delta_{i_0+1}, \ldots, \delta_{i_0+i_1}\} \cup \cdots \cup \{\delta_{s+1}, \ldots, \delta_m\}$$

many of which are empty, such that

$$\mathbf{V}^n\delta_1, \ldots, \mathbf{V}^n\delta_{i_0+\cdots+i_n}$$

is a basis for $\mathscr{D} \cap \mathbf{V}^n\mathscr{C}$ for all $n \in \mathbf{N} \cup \{0\}$. We set $I_n = \{i_0 + \cdots + i_{n-1} + 1, \ldots, i_0 + \cdots + i_n\}$, $I_\gamma = \{s+1, \ldots, m\}$.

Now let $\gamma \in \mathscr{D}$ and write

$$\gamma = \sum_{n=0}^{\infty} \sum_{i=1}^{m} \mathbf{V}^n\langle a_{n.i}\rangle\delta_i \tag{28.2.5}$$

the class of γ mod $\mathbf{V}\mathscr{C}$ is in $\mathrm{gr}_0(\mathscr{D}) \subset \mathrm{gr}_0(\mathscr{C})$ and it follows that $a_{0.i} = 0$ for $i \notin I_0$. Subtracting $\sum_{i \in I_0} \langle a_{0.i}\rangle\delta_i$, which is in $\mathscr{D}$, we find an element

$$\gamma_1 = \sum_{n=1}^{\infty} \sum_{i=1}^{m} \mathbf{V}^n\langle a_{n.i}\rangle\delta_i$$

which is in $\mathscr{D} \cap \mathbf{V}\mathscr{C}$; the class of γ_1 mod $\mathbf{V}^2\mathscr{C}$ is in $\mathrm{gr}_1(\mathscr{D}) \subset \mathrm{gr}_1(\mathscr{C})$; it follows that $a_{1.i} = 0$ if $i \notin I_0 \cup I_1$. Now subtract $\sum_{i \in I_0 \cup I_1} \mathbf{V}\langle a_{1.i}\rangle\delta_i$ from γ_1 to find an element $\gamma_2 \in \mathscr{D} \cap \mathbf{V}^2\mathscr{C}$, etc.

Conversely, suppose that the $a_{n.i}$ of the element γ of (28.2.5) satisfy the

condition of the proposition. Then $\mathbf{V}^n\langle a_{n,i}\rangle\delta_i \in \mathscr{D}$ for all n, i and because $\mathscr{D}$ is closed in $\mathscr{C}$, it follows that $\gamma \in \mathscr{D}$. Q.E.D.

We now use the proposition to put every homomorphism between formal group laws into a particularly pleasant form.

■ (28.2.6) **Proposition** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of formal group laws over k. Then there are isomorphisms of formal group laws $\beta(X)$: $F(X, Y) \to \hat{F}(X, Y)$, $\gamma(X)$: $G(X, Y) \to \hat{G}(X, Y)$ where $\hat{F}(X, Y)$ and $\hat{G}(X, Y)$ are curvilinear such that $\hat{\alpha}(X)$: $\hat{F}(X, Y) \to \hat{G}(X, Y)$, $\hat{\alpha}(X) = \gamma(X) \circ \alpha(X) \circ \beta^{-1}(X)$ is of the following form: there exist elements $n_1 \le n_2 \le \cdots \le n_r$ in $\mathbf{N}$ such that

$$(28.2.7) \qquad \hat{\alpha}_1(X) = X_1^{p^{n_1}}, \quad \ldots, \quad \hat{\alpha}_r(X) = X_r^{p^{n_r}}, \quad \hat{\alpha}_s(X) = 0 \text{ for } s > r$$

Proof Consider the homomorphism of $\mathrm{Cart}_p(k)$-modules α_* induced by $\alpha(X)$ and let $\mathscr{D}_1 \subset \mathscr{C}(F; k)$ be the kernel of α_* and $\mathscr{D}_2 \subset \mathscr{C}(G; k)$ the image of α_*. We then have

$$\mathscr{D}_1 \subset \mathscr{C}(F; k) \longrightarrow \mathscr{D}_2 \subset \mathscr{C}(G; k)$$

Now $\mathscr{D}_1$ is clearly a closed submodule of $\mathscr{C}(F; k)$, and it also has the property

$$\gamma \in \mathscr{D}_1 \cap \mathbf{V}^n\mathscr{C}(F; k) \quad \Rightarrow \quad \gamma \in \mathbf{V}^n\mathscr{D}_1$$

Indeed, let $\mathbf{V}^n\tilde{\gamma} = \gamma \in \mathscr{D}_1$, then $0 = \alpha_*(\mathbf{V}^n\tilde{\gamma}) = \mathbf{V}^n\alpha_*(\gamma) \Rightarrow \alpha_*(\tilde{\gamma}) = 0$ because $\mathbf{V}^n$ is injective on $\mathscr{C}(G; k)$. This means that all the $\Gamma_i \subset \mathrm{gr}_i(\mathscr{D}_1)$ of the proof of Proposition (28.2.2) are zero for $i > 0$, so that by the proof of Proposition (28.2.2) there exists a $\mathbf{V}$-basis $\{\delta_1, \ldots, \delta_{n_i}\}$ for $\mathscr{C}(F; k)$ such that $\{\delta_{s+1}, \ldots, \delta_{n_i}\}$ is a $\mathbf{V}$-basis for $\mathscr{D}_1$. The $\mathrm{Cart}_p(k)$-homomorphism α_* is then injective on the closed submodule of $\mathscr{C}(F; k)$ generated by the $\delta_1, \ldots, \delta_s$, and it follows that $\alpha_*(\delta_1), \ldots, \alpha_*(\delta_s)$ form a $\mathbf{V}$-basis for $\mathscr{D}_2$ so that in particular $\mathscr{D}_2$ is closed in $\mathscr{C}(G; k)$. (Another way to prove that $\mathscr{D}_2$ is closed is to remark that $\mathscr{C}(F; k)$ and $\mathscr{C}(G; k)$ are linearly topologized $W_{p^\infty}(k)[\![\mathbf{V}]\!]$-modules and that—having a finite $\mathbf{V}$-basis—they are linearly compact; since α_* is continuous, its image is linearly compact hence closed in $\mathscr{C}(G; k)$; cf. [43, Chapitre III, Section 2, Exercises 14–16].)

Now apply Proposition (28.2.2) to $\mathscr{D}_2 \subset \mathscr{C}(G; k)$. Let the resulting basis be $\hat{\delta}_1, \ldots, \hat{\delta}_n$ and for each $i \in \{1, \ldots, n\}$ let n_i be such that $i \in I_{n_i}$ and let r be such that $t \in I_\infty \Leftrightarrow t > r$. Then, of course, $s = r$.

Now let $\hat{F}(X, Y)$ be the p-typical formal group law over k corresponding to the $\mathrm{Cart}_p(k)$-module $\mathscr{C}(F; k)$ with $\mathbf{V}$-basis $\{\delta_1, \ldots, \delta_r, \delta_{r+1}, \ldots, \delta_m\}$ and let $\hat{G}(X, Y)$ be the p-typical formal group law over k corresponding to the $\mathrm{Cart}_p(k)$-module $\mathscr{C}(G; k)$ with $\mathbf{V}$-basis $\{\hat{\delta}_1, \ldots, \hat{\delta}_n\}$ (cf. Remark (27.7.19)(iii)). On these bases α_* looks like

$$(28.2.8) \qquad \alpha_*(\delta_1) = \mathbf{V}^{n_1}\hat{\delta}_1, \quad \ldots, \quad \alpha_*(\delta_r) = \mathbf{V}^{n_r}\hat{\delta}_r$$

$$\alpha_*(\delta_{r+1}) = \cdots = \alpha_*(\delta_m) = 0$$

Now let $\hat{\alpha}(X)$ be the homomorphism of formal group laws $\hat{F}(X, Y) \to \hat{G}(X, Y)$ determined by α_* on these bases for $\mathscr{C}(F; k)$ and $\mathscr{C}(G, k)$. The formula for $\hat{\alpha}(X)$ is (cf. Remark (27.3.10))

$$\hat{\alpha}(X) = \sum\nolimits^{\hat{G}} \alpha_*(\delta_i(X_i))$$

and because $\hat{G}$ is p-typical, hence curvilinear, this means that $\hat{\alpha}(X)$ has the desired form.

■ (28.2.9) **Corollary** Let $F(X, Y)$ be a formal group law over k of finite height h (in the sense of Chapter IV, Section (18.3.8); or cf. (28.2.1)). Then

$$h = \dim_k(\mathscr{C}_p(F; k)/[p]_F\mathscr{C}_p(F; k))$$

and, conversely, if this dimension is finite, then $F(X, Y)$ is of finite height.

Proof Apply Proposition (28.2.6) to the homomorphism $[p]_F$: $F(X, Y) \to F(X, Y)$. Then if $F(X, Y)$ is of finite height, we must have $r = m = \dim(F(X, Y))$ and hence $h = n_1 + \cdots + n_r$. On the other hand, $\dim_k(\mathscr{C}_p(F; k)/\alpha_*\mathscr{C}_p(F; k))$ is clearly h if one uses the description (28.2.8) of α_*. (Here α_* is the homomorphism induced by $[p]_F$, i.e., multiplication by p in $\mathscr{C}_p(F; k)$.)

Conversely, if $\dim_k(\mathscr{C}_p(F; k)/\alpha_*\mathscr{C}_p(F; k))$ is finite then $r = m$ in (28.2.8), hence (28.2.7) says that $F(X, Y)$ has finite height.

■ (28.2.10) **Corollary**

(i) Every closed $\mathrm{Cart}_p(k)$-submodule of a reduced $\mathrm{Cart}_p(k)$-module is also reduced.

(ii) If $\mathscr{C}$ is a reduced $\mathrm{Cart}_p(k)$-module and $\delta_1, \ldots, \delta_r$ a finite set of elements of $\mathscr{C}$, then the submodule of $\mathscr{C}$ generated by the $\delta_1, \ldots, \delta_r$ is closed and hence reduced.

Proof (i) is immediate from Proposition (28.2.2). As to (ii), there is an obvious $\mathrm{Cart}_p(k)$-module map $\mathscr{C}^m \to \mathrm{Cart}_p(k)\delta_1 + \cdots + \mathrm{Cart}_p(k)\delta_r \subset \mathscr{C}$, and the first part of the proof of (28.2.6) shows that the image of this morphism is closed.

28.3 Isogenies; unipotent and finite height formal group laws

In this section all formal group laws are over a perfect field k of characteristic $p > 0$ and they are finite dimensional.

■ (28.3.1) **Definition** We shall say that a formal group law $F(X, Y)$ over k is *unipotent* if the endomorphism $\mathbf{f}$ of $\mathscr{C}_p(F; k)$ is nilpotent (i.e., $\mathbf{f}^n = 0$ for some $n \in \mathbf{N}$). We have already defined when a formal group law is of finite height.

■ (28.3.2) **Decomposition of a formal group law in a unipotent and finite height part** Let $F(X, Y)$ be a formal group law over k. Consider the kernels of the homomorphisms $\mathbf{f}^n$: $\mathscr{C}_p(F; k) \to \mathscr{C}_p(F; k)$. Let

$$\mathscr{D}_n = \mathrm{Ker}(\mathbf{f}^n: \mathscr{C}_p(F; k) \to \mathscr{C}_p(F; k))$$

Then $\mathscr{D}_n \supset \mathscr{D}_{n-1}$. Consider $\mathscr{D}_n/\mathscr{D}_n \cap \mathbf{V}\mathscr{C}$ where $\mathscr{C}$ is short for $\mathscr{C}_p(F; k)$. This is a finite dimensional vector space over k and hence there is an $n_0 \in \mathbf{N}$ such that for all $n \geq n_0$, $\mathscr{D}_n/\mathscr{D}_n \cap \mathbf{V}\mathscr{C} = \mathscr{D}_{n+1}/\mathscr{D}_{n+1} \cap \mathbf{V}\mathscr{C}$. We claim that it follows that $\mathscr{D}_n = \mathscr{D}_{n+1}$ for $n \geq n_0$. Indeed, the submodule $\mathscr{D}_n$ being a kernel has the property $\gamma \in \mathscr{D}_n \cap \mathbf{V}\mathscr{C} \Rightarrow \gamma \in \mathbf{V}\mathscr{D}_n$ (cf. beginning of the proof of Proposition (28.2.6)) and hence $\mathscr{D}_n$ has a V-basis that is part of a V-basis of all of $\mathscr{C}$. We can now apply Proposition (28.2.6) to $\mathscr{D}_{n+1} \supset \mathscr{D}_n$, observe that also $\gamma \in \mathscr{D}_n \cap \mathbf{V}\mathscr{D}_{n+1} \Rightarrow \gamma \in \mathbf{V}\mathscr{D}_n$ and conclude that $\mathscr{D}_n$ has a V-basis that is part of a V-basis of D_{n+1}, which since

$$\mathscr{D}_{n+1}/\mathbf{V}\mathscr{D}_{n+1} = \mathscr{D}_{n+1}/\mathscr{D}_{n+1} \cap \mathbf{V}\mathscr{C} = \mathscr{D}_n/\mathscr{D}_n \cap \mathbf{V}\mathscr{C} = \mathscr{D}_n/\mathbf{V}\mathscr{D}_n$$

implies that $\mathscr{D}_n = \mathscr{D}_{n+1}$.

We have already observed that $\mathscr{D}_n$ has a V-basis that is part of a V-basis $\{\delta_1, \ldots, \delta_n\}$ of all of $\mathscr{C}$. Let $\hat{\mathscr{C}}$ be the sub-$\mathrm{Cart}_p(k)$-module generated by the elements of the V-basis $\{\delta_1, \ldots, \delta_n\}$ that are not in $\mathscr{D}_n$. Then by the usual Weyr-Fitting argument $\mathbf{f}$ is injective on $\hat{\mathscr{C}}$. It follows that we have an exact sequence

$$0 \to \mathscr{D}_n \to \mathscr{C}_p(F; k) \to \hat{\mathscr{C}} \to 0$$

where both $\mathscr{D}_n$ and $\hat{\mathscr{C}}$ are reduced $\mathrm{Cart}_{(p)}(k)$-modules (i.e., they are of the type that have formal group laws attached to them), so that we have a decomposition of $F(X, Y)$

$$0 \to G(X, Y) \to F(X, Y) \to H(X, Y) \to 0$$

with $G(X, Y)$ unipotent and $H(X, Y)$ such that $\mathbf{f}$ is injective on $\mathscr{C}_p(H; k)$.

Because $\mathbf{V}$ is always injective, it follows that $[p]_H = \mathbf{Vf}$ is injective; so applying Proposition (28.2.6) to $[p]_H$ we see that H is of finite height. The injectivity of $\mathbf{f}$ also implies that $\dim_k(\mathbf{V}\hat{\mathscr{C}}/\mathbf{fV}\hat{\mathscr{C}}) = \dim_k(\hat{\mathscr{C}}/\mathbf{f}\hat{\mathscr{C}})$ so that

$$h = \dim_k(\hat{\mathscr{C}}/\mathbf{V}\hat{\mathscr{C}}) + \dim_k(\hat{\mathscr{C}}/\mathbf{f}\hat{\mathscr{C}}) = m + m'$$

which holds (therefore) generally for all formal group laws of finite height.

■ (28.3.3) **Remark** It is not true as in the Weyr-Fitting lemma of finite dimensional linear algebra that $\mathbf{f}$ is necessarily an automorphism of $\hat{\mathscr{C}}$. Take, e.g., a one dimensional formal group law of height 2 over k.

■ (28.3.4) **isogenies** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of formal group laws. We shall say that $\alpha(X)$ is an isogeny if $F(X, Y)$ and $G(X, Y)$ are of equal dimension m and the r (the *rank* of $\alpha(X)$) of Proposition (28.2.6) is also equal to m.

Before interpreting what this means in terms of the curve modules of $F(X, Y)$ and $G(X, Y)$ we replace $\mathrm{Cart}_p(k)$ by a very similar ring.

■ (28.3.5) **The Dieudonné ring $\mathbf{D}(k)$** We define $\mathbf{D}(k)$ as the subring of $\mathrm{Cart}_p(K)$ consisting of all expressions

$$x_0 + \sum_{i=1}^{\infty} x_i \mathbf{V}^i + \sum^{<\infty} y_i \mathbf{f}^i$$

with coefficients in $W_{p^\infty}(k)$. That is, instead of allowing arbitrary power series $\sum_{i=1}^{\infty} y_i \mathbf{f}^i$ with $\lim_{i\to\infty} y_i = 0$ in $W_{p^\infty}(k)$, we allow only polynomials in $\mathbf{f}$. Let $\mathscr{C}$ be a reduced $\mathrm{Cart}_p(k)$-module (cf. (27.7.20)), then $\mathscr{C}$ is also a $\mathbf{D}(k)$-module; and, conversely, if $\mathscr{C}$ is a reduced $\mathbf{D}(k)$-module (meaning $\mathscr{C} = \varprojlim \mathscr{C}/\mathbf{V}^i\mathscr{C}$; $\mathbf{V}$ injective), then the action of $\mathbf{D}(k)$ on $\mathscr{C}$ extends uniquely to an action of $\mathrm{Cart}_p(k)$, precisely because, $\mathscr{C}$ being Hausdorff and complete, a limit $\sum y_i \mathbf{f}^i \gamma$ for $\gamma \in \mathscr{C}$ exists uniquely in $\mathscr{C}$ if $\lim_{i\to\infty} y_i = 0$ in $W_{p^\infty}(k)$ (use also $\mathbf{V}\mathbf{f} = p$).

So reduced $\mathrm{Cart}_p(k)$-modules are the same thing as reduced $\mathbf{D}(k)$-modules and from now on in this Section 28.3 we shall view the $\mathscr{C}(F; k)$ as $\mathbf{D}(k)$-modules.

■ (28.3.6) **The "localized" Dieudonné ring $\mathbf{D}_{\mathbf{V}}(k)$** We define $\mathbf{D}_{\mathbf{V}}(k)$ as the ring

$$\mathbf{D}_{\mathbf{V}}(k) = \left\{ \sum_{i=n}^{\infty} \mathbf{V}^i x_i \,\middle|\, x_i \in W_{p^\infty}(k), n \in \mathbf{Z} \right\}$$

of all formal Laurent series over $W_{p^\infty}(k)$ with multiplication rule $x\mathbf{V} = \mathbf{V}\sigma(x)$ for all $x \in W_{p^\infty}(k)$ where σ is the Frobenius automorphism of $W_{p^\infty}(k)$. The ring $\mathbf{D}_V(k)$ is the "localized version" of $\mathbf{D}(k)$ obtained by making $\mathbf{V}$ invertible.

There is a natural homomorphism $\mathbf{D}(k) \to \mathbf{D}_{\mathbf{V}}(k)$ defined by $\mathbf{f} \to \mathbf{V}^{-1}p$ making $\mathbf{D}_{\mathbf{V}}(k)$ a right $\mathbf{D}(k)$-module and

$$\mathscr{C} \mapsto \mathbf{D}_{\mathbf{V}}(k) \otimes_{\mathbf{D}(k)} \mathscr{C} = \mathscr{C}_{\mathbf{V}}$$

is a functor taking $\mathbf{D}(k)$-modules into $\mathbf{D}_{\mathbf{V}}(k)$-modules.

■ (28.3.7) **The equivalence relation "isogenous"** We shall call two formal group laws $F(X, Y)$, $G(X, Y)$ isogenous over k if there is an isogeny over k from $F(X, Y)$ to $G(X, Y)$ and also if there is an isogeny over k from $G(X, Y)$ to $F(X, Y)$. More generally, $F(X, Y)$ is isogenous to $G(X, Y)$ if there exists a finite sequence of formal group laws $H_0(X, Y), \ldots, H_n(X, Y)$ such that $H_i(X, Y)$ is isogenous over k to $H_{i+1}(X, Y)$, $i = 0, 1, \ldots, n-1$ and $F(X, Y) = H_0(X, Y)$, $H_n(X, Y) = G(X, Y)$.

■ (28.3.8) **Proposition** Two formal group laws $F(X, Y)$, $G(X, Y)$ over k are isogenous over k if and only if their $\mathbf{D}_{\mathbf{V}}(k)$-modules $\mathbf{D}_{\mathbf{V}}(k) \otimes_{\mathbf{D}(k)} \mathscr{C}(F; k)$ and $\mathbf{D}_{\mathbf{V}}(k) \otimes_{\mathbf{D}(k)} \mathscr{C}(G; k)$ are isomorphic.

Proof Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be an isogeny. Then, clearly, putting $\alpha(X)$ in the form of Proposition (28.2.6), we see that the $\mathbf{D}_{\mathbf{V}}(k)$-modules of $F(X, Y)$ and $G(X, Y)$ are isomorphic. Conversely, suppose that $\mathscr{C}(F; k)$ and $\mathscr{C}(G; k)$ become isomorphic over $\mathbf{D}_{\mathbf{V}}(k)$. Identifying $\mathscr{C}(F; k)_{\mathbf{V}}$ and $\mathscr{C}(G; k)_{\mathbf{V}}$, we can view $\mathscr{C}(F; k)$ and $\mathscr{C}(G; k)$ as submodules of $\mathscr{C}(F, k)_{\mathbf{V}}$. Both $\mathscr{C}(F; k)$ and $\mathscr{C}(G; k)$ have a finite $\mathbf{V}$-basis, so there are $r, s \in \mathbf{N}$ such that $\mathbf{V}^r\mathscr{C}(F; k) \subset \mathscr{C}(G; k)$, $\mathbf{V}^s\mathscr{C}(G; k) \subset \mathscr{C}(F; k)$. It follows immediately that $\dim(F(X, Y)) = \dim(G(X, Y))$, and given this the inclusions

$$\mathscr{C}(F; k) \supset \mathbf{V}^r\mathscr{C}(F; k) \subset \mathscr{C}(G; k)$$

define the desired chain of isogenies.

■ (28.3.9) **Proposition** Let $\mathscr{C}$ be a reduced $\mathbf{D}(k)$-module of finite $\mathbf{V}$-dimension. Then $\mathscr{C}_{\mathbf{V}}$ is a torsion $\mathbf{D}_{\mathbf{V}}(k)$-module (i.e., there is an $\vartheta \in \mathbf{D}_{\mathbf{V}}(k)$ such that $\vartheta\mathscr{C}_{\mathbf{V}} = 0$).

Proof Since $\mathscr{C}$ has a finite $\mathbf{V}$-basis, it suffices to show that for each $\delta \in \mathscr{C}$ there is a $\vartheta \in \mathbf{D}_{\mathbf{V}}(k)$ such that $\vartheta\delta = 0$. So we can assume that δ generates $\mathscr{C}$ (since the submodule of $\mathscr{C}$ generated by δ is also reduced; cf. Corollary (28.2.10)(ii)).

Let $\mathbf{D}_{\mathbf{V}}^+(k)$ be the subring of $\mathbf{D}_{\mathbf{V}}(k)$ of all power series in $\mathbf{V}$; i.e., no negative powers of $\mathbf{V}$ occur in elements of $\mathbf{D}_{\mathbf{V}}^+(k)$. Now assume that the annihilator of δ is zero and consider

$$\mathfrak{A} = \{\eta \in \mathbf{D}_{\mathbf{V}}(k) \mid \eta\delta \in \mathscr{C}\}$$

Then $\mathfrak{A} \to \mathscr{C}$, $\eta \mapsto \eta\delta$ is an isomorphism of $\mathbf{D}_{\mathbf{V}}^+(k)$-modules. (Injectivity follows from the vanishing of the annihilator of δ; surjectivity follows from the fact that δ generates $\mathscr{C}$ as a $\mathbf{D}(k)$-module and $p\mathbf{V}^{-1} = \mathbf{f}$ and $p\mathbf{V}^{-1} \subset \mathfrak{A}$.) Now $\mathscr{C}$, being reduced, is a finitely generated $\mathbf{D}_{\mathbf{V}}^+(k)$-module and hence so is $\mathfrak{A}$. Now $p\mathbf{V}^{-1} \in \mathfrak{A}$ and hence for some $n \geq 1$ we must have

$$(p\mathbf{V}^{-1})^n = \sum_{i=0}^{n-1} a_i(p\mathbf{V}^{-1})^i, \qquad a_i \in \mathbf{D}_{\mathbf{V}}^+(k)$$

and so $p^n \in \mathbf{V}\mathbf{D}_{\mathbf{V}}^+(k)$, which is impossible.

■ (28.3.10) **Remark** If $F(X, Y)$ is of finite height, then as we have seen $\dim_k(\mathscr{C}(F; k)/[p]_F\mathscr{C}(F; k)) = h < \infty$, and it follows that $\mathscr{C}(F; k)$ as a module over $W_{p^s}(k)$ is free of rank h. (Cf. [43, Chapter III, Section 2, Proposition 13], or [42, Chapter II, Section 3, Proposition 5].)

■ (28.3.11) **Remark** If $F(X, Y)$ is of finite height, then $\mathbf{f}$: $\mathscr{C}(F; k) \to \mathscr{C}(F; k)$ is not necessarily an automorphism, but $\mathbf{f}$ becomes an automorphism of the extended module $\mathscr{C}(F; k)_{\mathbf{V}}$. Indeed, $\mathbf{V}\mathbf{f} = [p]_F$ is an isogeny if $F(X, Y)$ is of finite height and $\mathbf{V}$ is invertible in $\mathbf{D}_{\mathbf{V}}(k)$. Now use Proposition (28.3.8).

28.4 Classification of finitely generated torsion modules over $\mathbf{D}_{\mathbf{V}}(k)$

In this section (28.4) we classify all finitely generated torsion modules over $\mathbf{D}_{\mathbf{V}}(k)$. In fact we shall do this over a somewhat more general ring which will turn up later when dealing with formal A-modules.

■ (28.4.1) **The setting** Let A be a complete discrete valuation ring with algebraically closed residue field k of characteristic $p > 0$, uniformizing element π, and quotient field K. Moreover, suppose that there is an automorphism σ of K and a power q of p such that $\sigma(a) \equiv a^q \bmod \pi$ for all $a \in A$ and such that $\sigma(\pi) = \pi$.

Let $\mathscr{E}$ be the ring of all Laurent series $\{\sum_{i=n}^{\infty} T^i x_i \mid x_i \in A,\ n \in \mathbf{Z}\}$ with the multiplication rule $xT = T\sigma(x)$ (and hence $xT^{-1} = T^{-1}\sigma^{-1}(x)$).

The two examples that are important for us are: (1) $A = W_{p^\infty}(k)$ where k is an algebraically closed field of characteristic $p > 0$ and where σ is the Frobenius automorphism and $\pi = p$; and (2) $A = \hat{B}_{nr}$, the completion of the maximal unramified extension B_{nr} of a complete discrete valuation ring B with uniformizing element π and residue field of q elements with σ the continuous extension of the Frobenius generator of $\mathrm{Gal}(L_{nr}/L)$ where L is the quotient field of B. In this second example A may be of characteristic $p = \text{characteristic}(k) > 0$. Note that always $\sigma(\pi) = \pi$.

From now on in 28.4 the notations $\mathscr{E}$, A, π, k, K, σ, q, p, T have the meaning given them above. Moreover, $v\colon K \to \mathbf{Z} \cup \{\infty\}$ denotes the normalized exponential valuation on K, and $d\colon \mathscr{E} \to \mathbf{Z}$ assigns to each $\eta = \sum T^i x_i$ the smallest $n \in \mathbf{Z}$ for which $x_n \neq 0$.

■ (28.4.2) **Valuation and "euclidean algorithm" on $\mathscr{E}$** For each $\eta \in \mathscr{E}$, $\eta = \sum a_i T^i$ let $n \in \mathbf{Z}$ be the smallest integer for which $a_n \neq 0$. We define a function $s\colon \mathscr{E} \to \mathbf{N} \cup \{0\} \cup \{\infty\}$ by $s(\eta) = v(a_n)$ if $\eta \neq 0$ and $s(0) = \infty$. This function has the properties

$$s(\eta\vartheta) = s(\eta)s(\vartheta)$$

(28.4.3)
$$s(\eta) = 0 \iff \eta \text{ is invertible in } \mathscr{E}$$

$$s(\eta) = \infty \iff \eta = 0$$

We show that s can be used to define a left euclidean algorithm on $\mathscr{E}$ in the sense that for every pair of elements $\eta_1, \eta_2 \in \mathscr{E}$, there exist ϑ and ζ in $\mathscr{E}$ such that

$$\eta_1 = \vartheta\eta_2 + \zeta, \qquad s(\zeta) < s(\eta_2) \quad \text{or} \quad \zeta = 0$$

Indeed, we can assume $s(\eta_1) \geq s(\eta_2)$ (otherwise take $\vartheta = 0$, $\zeta = \eta_1$). Assume that $\eta_1 \notin A\eta_2$. Let $d(\eta_1) = n$ be the smallest integer for which the coefficient a_n is nonzero in the Laurent series η_1. Then there exists an element ϑ_1 such that $d(\eta_1 - \vartheta_1\eta_2) \geq n + 1$. (This uses $s(\eta_1) \geq s(\eta_2)$.) Now if $s(\eta_1 - \vartheta_1\eta_2) \geq s(\eta_2)$

we can repeat the process (with η_1 replaced $\eta_1 - \vartheta_1\eta_2$) to find a ϑ_2 such that $d(\eta_1 - \vartheta_1\eta_2 - \vartheta_2\eta_2) \geq n+2$. Because $d(\vartheta_2) \geq d(\vartheta_1) + 1$ this process cannot be continued indefinitely because then the series $\sum \vartheta_i$ converges in $\mathscr{E}$ and we would have $(\sum_{i=1}^{\infty} \vartheta_i)\eta_2 = \eta_1$, which was excluded.

■ (28.4.4) **Corollary** Every left ideal of $\mathscr{E}$ is principal.

In the same way one proves that there is a right euclidean algorithm and that every right ideal is principal.

■ (28.4.5) **Corollary** The ring $\mathscr{E}$ is noetherian. (Cf. [204, Chapter 3,2].)

■ (28.4.6) **Corollary** Every finitely generated torsion $\mathscr{E}$-module is isomorphic to a direct sum of cyclic $\mathscr{E}$-modules $\mathscr{E}/\mathscr{E}\eta$ where η is of the form

$$\eta = \pi^i, \quad i \geq 1 \qquad \text{or} \qquad \eta = \sum_{i=0}^{h-1} T^i a_i + T^h\zeta$$

with $\zeta \in \mathscr{E}$, $s(\zeta) = 0$, $d(\zeta) = 0$, $a_i \in \pi A$.

Proof Every torsion module over a principal ideal ring is a direct sum of cyclic modules $\mathscr{E}/\mathscr{E}\eta$. It therefore remains to show only that η can be chosen to have one of the two forms indicated above. If $d(\eta) \neq 0$, then $\eta = \vartheta T^{d(\eta)}$; and since T is a unit in $\mathscr{E}$, we have $\mathscr{E}/\mathscr{E}\eta \simeq \mathscr{E}/\mathscr{E}\vartheta$. We can therefore assume that $d(\eta) = 0$. Set $\eta = \pi^m\vartheta$ with m maximal. We can then write

$$\vartheta = \sum_{i=0}^{h-1} T^i a_i + \zeta T^h$$

with h the first index such that a_h in $\vartheta = \sum_{i=0}^{\infty} T^i a_i$ is not divisible by π. If $h = 0$, then ϑ is a unit and $\mathscr{E}/\mathscr{E}\eta \simeq \mathscr{E}/\mathscr{E}\pi^m$; and if $h \neq 0$, we have to show that

$$\mathscr{E}/\mathscr{E}\pi^m\vartheta \simeq \mathscr{E}/\mathscr{E}\pi^m \oplus \mathscr{E}/\mathscr{E}\vartheta$$

which as usual follows from the Weyr–Fitting lemma, applied to the endomorphism "multiplication with π." (Cf. [204, Chapter 1,5]; this is in fact the same decomposition (V being injective) as we obtained in (28.3.2) if $\mathscr{E}/\mathscr{E}\pi^m\vartheta$ comes from a $\mathrm{Cart}_p(k)$-module.)

■ (28.4.7) **Remarks**

(i) The function $s: \mathscr{E} \to \mathbf{N} \cup \{0\} \cup \{\infty\}$ is not a valuation on $\mathscr{E}$. There is no relation whatever between $s(\eta + \vartheta)$ and $s(\eta)$, $s(\vartheta)$. Correspondingly, there is no uniqueness (within units) statement concerning the ϑ and ζ in the left euclidean "algorithm" $\eta_1 = \vartheta\eta_2 + \zeta$.

(ii) The ring $\mathscr{E}$ has no zero divisors (follows from (28.4.3)).

■ (28.4.8) **Lemma** The modules $\mathscr{E}/\mathscr{E}\pi^i$ are indecomposable and every submodule of $\mathscr{E}/\mathscr{E}\pi^i$ is of the form $\mathscr{E}\pi^j/\mathscr{E}\pi^i$.

Proof This follows from the fact that (up to unit factors) every divisor of π^i in $\mathscr{E}$ is of the form π^j, $0 \le j \le i$ (cf. also Lemma (28.4.19)).

■ (28.4.9) **Lemma** Let $\eta = \sum_{i=0}^{h-1} T^i a_i + T^h\zeta$ with $\zeta \in \mathscr{E}$, $s(\zeta) = 0$, $d(\zeta) = 0$, $a_i \in \pi A$. Then there is a unit $\vartheta \in \mathscr{E}$ such that

$$\vartheta\eta = \sum_{i=0}^{h-1} T^i b_i + T^h, \qquad b_i \in \pi A \tag{28.4.10}$$

Proof This is Lemma (20.3.13) of Chapter IV.

■ (28.4.11) An element of the form (28.4.10) (with $h \ge 1$) will be called *distinguished*. Up to now we have not yet used that k is algebraically closed. This will now come into play to decompose cyclic $\mathscr{E}$-modules $\mathscr{E}/\mathscr{E}\eta$ with distinguished η.

■ (28.4.12) **Lemma** Let $\eta \in \mathscr{E}$ be distinguished. Then there exists a natural number $m \in \mathbf{N}$ such that over $\mathscr{E}[\pi^{1/m}] = A[\pi^{1/m}]((T))$, $T\pi^{1/m} = \pi^{1/m}T$, we can decompose η as

$$\eta = \prod_{i=1}^{h} (T - \pi^{n_i/m}u_i) = a_0 + Ta_1 + \cdots + T^{h-1}a_{h-1} + T^h$$

where the $u_i \in A[\pi^{1/m}]$ are invertible.

Proof It suffices to show that a distinguished η has a linear factor over some $A[\pi^{1/m}]$. A trivial induction then finishes the proof. Now

$$\eta = (T - a)\eta_1 \tag{28.4.13}$$

is equivalent to the condition

(28.4.14)

$$a_0 + aa_1 + a\sigma(a)a_2 + \cdots + a\sigma(a)\cdots\sigma^{h-2}(a)a_{h-1} + a\sigma(a)\cdots\sigma^{h-1}(a) = 0$$

(To see this just equate coefficients in (28.4.13).) Now consider

$$\frac{r}{s} = \underset{i=0,1,\ldots,h-1}{\text{minimum}} ((h-i)^{-1}v(a_i)), \qquad r, s \in \mathbf{N}, \quad (r, s) = 1 \tag{28.4.15}$$

where v is the valuation on A. Suppose that $s^{-1}r$ is an integer, i.e., $s = 1$, then we claim a linear factor $T - a$ of η can already be found over A itself. Indeed, if $s = 1$ in (28.4.15), then $a_i = \pi^{r(h-i)}b_i$ with $b_i \in A$ and putting $a = \pi^r x$ we see that to solve (28.4.14) it suffices to solve

$$b_0 + xb_1 + x\sigma(x)b_2 + \cdots + x\sigma(x)\cdots\sigma^{h-1}(x) = 0 \tag{28.4.16}$$

where at least two of the coefficients are units, i.e., not in πA. Because $\sigma(x) \equiv x^q \bmod \pi$ and k is algebraically closed, it follows that this equation has a nonzero solution mod π.

Now suppose that we have found an $x_n \in A^*$ such that x_n solves (28.4.16) mod π^n. Put $x_{n+1} = x_n + \pi^n y$. Then mod π^{n+1}

$$x_{n+1}\sigma(x_{n+1}) \cdots \sigma^i(x_{n+1}) \equiv x_n\sigma(x_n) \cdots \sigma^i(x_n) + \pi^n \sum_{j=0}^{i} \sigma^j(x_n)^{-1} x_n \sigma(x_n) \cdots \sigma^i(x_n)\sigma^j(y)$$

Let

$$b_0 + x_n b_1 + \cdots + x_n\sigma(x_n) \cdots \sigma^{h-1}(x_n) \equiv c\pi^n \mod \pi^{n+1}$$

Then for x_{n+1} to solve (28.4.16) mod π^{n+1} we must choose y such that

$$\sum_{i=0}^{h} b_i \sum_{j=0}^{i} \sigma^j(x_n)^{-1}\sigma^j(y)x_n\sigma(x_n) \cdots \sigma^i(x_n) \equiv c \mod \pi$$

which can be done because $\sigma^j(y) \equiv y^{q^j} \bmod \pi$, because x_n is a unit, because at least two of the b_i are units ($b_h = 1$), and because k is algebraically closed.

This proves our claim. To prove the lemma it then suffices to take $m = s$, then the minimum (28.4.15) becomes an integer if we replace v by the normalized exponential valuation of $A[\pi^{1/m}]$.

■ (28.4.17) **Lemma** Let $\mathscr{C} = \mathscr{E}/\mathscr{E}\eta$ where η is distinguished. Then there exists a K-vector space structure on $\mathscr{C}$ that is compatible with the A-module structure. This K-vector space structure is unique and $\dim_K(\mathscr{C}) = h$.

Proof Write $-\eta = (\pi\vartheta - 1)T^h$ for some $\vartheta \in \mathscr{E}$. (This can be done of course because η is distinguished.) Now define $\pi^{-1}\gamma = \vartheta\gamma$ for all $\gamma \in \mathscr{C}$. Since $\pi\vartheta \equiv 1 \bmod \mathscr{E}\eta$, it follows that $\pi(\pi^{-1}\gamma) = \gamma$; it is not hard to check that $\mathscr{C}$ does indeed become a K-vector space, nor that this is the only possible definition (precisely because we must have $\pi(\pi^{-1}\gamma) = \gamma$). A basis for $\mathscr{C}$ over K is $1, T, T^2, \ldots, T^{h-1}$.

■ (28.4.18) This lemma should not have come as a surprise to the reader. If $\mathscr{C}$ comes from a "finite height" $\mathrm{Cart}_p(k)$-module, i.e., $\mathscr{C} = \mathscr{C}'_{\mathbf{V}}$ for some "finite height" reduced $\mathbf{D}(k)$-module, then we have already seen that $\mathbf{f}$ acts as an automorphism on $\mathscr{C}$ (Remark (28.3.11)) and $\mathbf{V}$ being invertible in $\mathbf{D}_{\mathbf{V}}(k)$ also acts as an automorphism. Therefore $p^{-1} = \mathbf{f}^{-1}\mathbf{V}^{-1}$ is uniquely determined and takes $\mathscr{C}$ into $\mathscr{C}$.

■ (28.4.19) **Lemma** Let $\mathscr{C} = \mathscr{E}/\mathscr{E}\eta\vartheta$ and let $\mathscr{D}$ be the submodule $\mathscr{E}\vartheta/\mathscr{E}\eta\vartheta$. Then $\mathscr{D}$ is a direct summand of $\mathscr{C}$ if and only if the equation $x\eta + \vartheta y = 1$ is solvable in $\mathscr{E}$, and in that case $\hat{\mathscr{D}} = \mathscr{E}(1 - y\vartheta)/\mathscr{E}\eta\vartheta$ is a complementary direct summand.

Proof We first show that $\mathscr{D} \simeq \mathscr{E}/\mathscr{E}\eta$. Let $\gamma \in \mathscr{C}$ be the image of $1 \in \mathscr{E}$ under the natural map $\mathscr{E} \to \mathscr{E}/\mathscr{E}\eta\vartheta$. Then $\mathscr{E}\eta\vartheta$ is the annihilator of γ and $\mathscr{C} = \mathscr{E}\gamma$, $\mathscr{D} = \mathscr{E}\vartheta\gamma$. Because $\mathscr{E}$ is principal, the annihilator of $\vartheta\gamma$ is $\mathscr{E}\eta$, so $\mathscr{D} \simeq \mathscr{E}/\mathscr{E}\eta$.

Second, suppose that $\mathscr{D} \oplus \hat{\mathscr{D}} = \mathscr{C}$. We show that $\hat{\mathscr{D}} \simeq \mathscr{E}/\mathscr{E}\vartheta$. Let $\gamma = \delta_{\mathscr{D}} + \delta_{\hat{\mathscr{D}}}$ be the decomposition of γ. Let $\delta_{\hat{\mathscr{D}}} = \zeta\gamma$ with $\zeta \in \mathscr{E}$. Then $\xi\delta_{\hat{\mathscr{D}}} = 0 \Leftrightarrow \xi\gamma \in \mathscr{D} \Leftrightarrow \xi\gamma = \hat{\xi}\vartheta\gamma \Leftrightarrow \xi \in \mathscr{E}\vartheta$, so the annihilator of $\delta_{\hat{\mathscr{D}}}$ is $\mathscr{E}\vartheta$ and hence $\hat{\mathscr{D}} \simeq \mathscr{E}/\mathscr{E}\vartheta$.

Now let $\delta_{\mathscr{D}} = y\vartheta\gamma$. We had $\delta_{\hat{\mathscr{D}}} = \zeta\gamma$ so $1 - y\vartheta - \zeta \in \mathscr{E}\eta\vartheta$ because $\delta_{\mathscr{D}} + \delta_{\hat{\mathscr{D}}} = \gamma$. Now ζ is arbitrary mod $\mathscr{E}\eta\vartheta$ so we can assume that $\zeta = 1 - y\vartheta$. Now $\vartheta(1 - y\vartheta)\gamma = \vartheta\zeta\gamma = 0$ because ϑ annihilates $\zeta\gamma = \delta_{\mathscr{D}}$. Hence $\vartheta(1 - y\vartheta) = x\eta\vartheta$ for some x, which, because $\mathscr{E}$ has no zero divisors, means that $1 - \vartheta y = x\eta$.

Conversely, $\mathscr{D} + \mathscr{E}(1 - y\vartheta)\gamma = \mathscr{C}$ because $\mathscr{D}$ contains $\vartheta\gamma$ and if $\xi\vartheta\gamma = \hat{\xi}(1 - y\vartheta)\gamma \in \mathscr{D} \cap \mathscr{E}(1 - y\vartheta)\gamma$, then $\xi\vartheta - \hat{\xi}(1 - y\vartheta) \in \mathscr{E}\eta\vartheta$, so that $\hat{\xi} = z\vartheta$ for some $z \in \mathscr{E}$. Hence $\hat{\xi}(1 - y\vartheta)z\vartheta(1 - y\vartheta) = z(\vartheta - \vartheta y\vartheta) = z(1 - \vartheta y)\vartheta = zx\eta\vartheta \in \eta\vartheta$, so $\hat{\xi}(1 - y\vartheta)\gamma = 0$.

■ (28.4.20) **Lemma** The modules $\mathscr{E}/\mathscr{E}(T - a)$, $a \in A$, are simple and any extension between two such modules is trivial. If $v(a) = r$, then $\mathscr{E}/\mathscr{E}(T - a) \simeq \mathscr{E}/\mathscr{E}(T - \pi^r)$.

Proof If $v(a) = 0$, then $T - a$ is a unit in $\mathscr{E}$ so $\mathscr{E}/\mathscr{E}(T - a) \simeq 0 \simeq \mathscr{E}/\mathscr{E}(T - 1)$ because $T - 1$ also a unit.

Suppose that $v(a) \neq 0$, and define an $\mathscr{E}$-module structure on K, the quotient field of A, by the rule $Tx = \sigma^{-1}(x)a$. (Check that this does indeed define an $\mathscr{E}$-module structure on K; i.e., that $b(Tx) = (bT)x = (T\sigma(b))x = T(\sigma(b)x)$.) The map $\mathscr{E}/\mathscr{E}(T - a) \to K$ induced by $\mathscr{E} \ni 1 \mapsto 1 \in K$ is then an $\mathscr{E}$-module isomorphism. Now $\mathscr{E}/\mathscr{E}(T - b)$ and K are isomorphic $\mathscr{E}$-modules if and only if there is a $y \in K$ such that $Ty = by$, i.e., $\sigma^{-1}(y)a = by$, which shows that this happens if and only if $v(a) = v(b)$ (because the equation $\sigma^{-1}(y)/y = u$ is solvable in A for any unit $u \in A$ by the usual successive approximation method; cf. Chapter I, Remark (8.3.15)(ii)).

Now let $0 \to \mathscr{C}_1 \to \mathscr{C} \to \mathscr{C}_2 \to 0$ be an exact sequence with $\mathscr{C}_1 = \mathscr{E}/\mathscr{E}(T - a)$, $\mathscr{C}_2 = \mathscr{E}/\mathscr{E}(T - b)$. Let $\gamma_1 \in \mathscr{C}_1$ be the image of $1 \in \mathscr{E}$, $\gamma_2 \in \mathscr{C}_2$ the image of 1 in $\mathscr{C}_2$ and $\gamma \in \mathscr{C}$ a lift of γ_2. Then obviously $\{\gamma_1, \gamma\}$ is a K-basis for the K-vector space $\mathscr{C}$ (cf. Lemma (28.4.17)). It is now sufficient to find a $\delta_2 \in \mathscr{C}$, $\delta_2 \equiv \gamma$ mod $\mathscr{C}_1$ such that $T\delta_2 = b\delta_2$. To this end write $\delta_2 = \gamma + z\gamma_1$ for some yet to be determined $z \in K$. We have

$$T\delta_2 = T\gamma + \sigma^{-1}(z)a\gamma_1 = b\gamma + c\gamma_1 + \sigma^{-1}(z)a\gamma_1$$

for a certain $c \in K$ (because $T\gamma \equiv b\gamma$ mod $\mathscr{C}_1$). So the condition $T\delta_2 = b\delta_2$ translates to

$$b\gamma + c\gamma_1 + \sigma^{-1}(z)a\gamma_1 = b\gamma + bz\gamma_1$$

and it suffices to solve

$$\hat{c} + \hat{a}z = \hat{b}\sigma(z)$$

where $\hat{a}, \hat{b}, \hat{c}$ are certain elements of K. This can always be done by successive approximation as usual. (NB if $\hat{a}, \hat{b}, \hat{c} \in A$, a solution $z \in A$ may not exist; e.g., if $\hat{a}, \hat{b} \in \pi A$, $\hat{c} \notin \pi A$. This is easily taken care of by writing $z = \pi^{-r}\hat{z}$ for a suitable r.)

■ (28.4.21) **Corollary** If $\eta = \prod_{i=1}^{h} (T - \pi^{r_i}u_i)$, then

$$\mathscr{E}/\mathscr{E}\eta \simeq \bigoplus_{i=1}^{h} \mathscr{E}/\mathscr{E}(T - \pi^{r_i})$$

■ (28.4.22) **Corollary** Every cyclic module $\mathscr{E}/\mathscr{E}\eta$ with η distinguished is semisimple.

Proof Let $\mathscr{C}_1 \subset \mathscr{E}/\mathscr{E}\eta$ be a cyclic submodule of $\mathscr{E}/\mathscr{E}\eta$. Say $\mathscr{C}_1 = \mathscr{E}\zeta/\mathscr{E}\eta$, then $\eta = \vartheta\zeta$ for some ϑ (look at annihilators and use the principal ideal property). Now $\mathscr{C}_1$ is a direct summand of $\mathscr{E}/\mathscr{E}\vartheta\zeta$ over $\mathscr{E}[\pi^{1/m}]$ for a suitable m by (28.4.21) and (28.4.20). It follows that $x\vartheta + \zeta y = 1$ is solvable with x, $y \in \mathscr{E}[\pi^{1/m}]$ by Lemma (28.4.19). Write

$$x = \sum_{i=0}^{m-1} x_i\pi^{i/m}, \qquad y = \sum_{i=0}^{m-1} y_i\pi^{i/m}, \qquad x_i, y_i \in E$$

Then also $x_0\vartheta + \zeta y_0 = 1$, so that, again by Lemma (28.4.19), $\mathscr{C}_1$ is also a direct summand of $\mathscr{E}/\mathscr{E}\eta$ over $\mathscr{E}$ itself.

■ (28.4.23) **Lemma** Let $\mathscr{C} = \mathscr{E}/\mathscr{E}\eta$ with η distinguished. Then

$$\mathscr{C} \simeq \bigoplus_{i} \mathscr{E}/\mathscr{E}(T^{s_i} - \pi^{r_i})$$

with $(s_i, r_i) = 1$, $s_i, r_i \in \mathbf{N}$. The modules $\mathscr{E}/\mathscr{E}(T^s - \pi^r)$ are simple if $(s, r) = 1$ and pairwise nonisomorphic for different pairs s, r and $\bar{s}, \bar{r}$ with $(s, r) = (\bar{s}, \bar{r}) = 1$.

Proof Put $\mathscr{E}_s = \mathscr{E}[\pi^{1/s}]$. For a suitable s, the $\mathscr{E}_s$-module $\mathscr{C}_s = \mathscr{E}_s \otimes_{\mathscr{E}} \mathscr{C}$ is isomorphic to a direct sum

$$\mathscr{C}_s \simeq \bigoplus_{i} \mathscr{E}_s/\mathscr{E}_s(T - \pi^{r_i/s})$$

Let $x \in \mathscr{C}_s$ be an element such that $(T - \pi^{r/s})x = 0$ (where $r = r_i$ for some i). Dividing s and r by (s, r) if necessary, we can assume that $(s, r) = 1$. Write $x = \sum_{i=0}^{s-1} \pi^{i/s}x_i$ with $x_i \in \mathscr{C}$. Then $(T^s - \pi^r)x = 0$; hence $(T^s - \pi^r)x_i = 0$, so $\mathscr{E}x_i \subset \mathscr{C}$ is a quotient of $\mathscr{E}/\mathscr{E}(T^s - \pi^r)$. So if we can show that $\mathscr{E}/\mathscr{E}(T^s - \pi^r)$ is simple, then $\mathscr{E}x_i \simeq \mathscr{E}/\mathscr{E}(T^s - \pi^r)$ (if $x_i \neq 0$), which will prove the lemma by Corollary (28.4.22) and Lemma (28.4.19).

Suppose that $\mathscr{E}/\mathscr{E}(T^s - \pi^r)$ is not simple (and $(s, r) = 1$). Then there is a simple submodule $\mathscr{C}' \subset \mathscr{E}/\mathscr{E}(T^s - \pi^r)$ with $\mathscr{C}' = \mathscr{E}/\mathscr{E}\eta$ with a distinguished η. The degree of η must be less than s because degree $\eta = \dim_K(\mathscr{C}') < \dim_K(\mathscr{C}) = s$ (cf. Lemma (28.4.17)). Over some extension $\mathscr{E}[\pi^{1/t}]$ the module $\mathscr{C}'$ must contain

a direct summand of the form $\mathscr{E}_t/\mathscr{E}_t(T-\pi^{r'/s'})$ with $s' \leq$ degree $\eta < s$. And this is impossible because $\mathscr{E}/\mathscr{E}(T^s-\pi^r)$ decomposes as s copies of $\mathscr{E}_s/\mathscr{E}_s(T-\pi^{r/s})$ over $\mathscr{E}_s$ by the addendum to Lemma (28.4.12) and Lemma (28.4.20) and because the modules $\mathscr{E}_s/\mathscr{E}_s(T-\pi^{r/s})$ remain simple over all $\mathscr{E}_t$.

■ (28.4.24) **Addendum to Lemma (28.4.12)** Let η and r/s be as in Lemma (28.4.12) and (28.4.15); suppose that r/s is an integer and that l is the smallest j for which the minimum is assumed. Then $h-l$ linear factors of the form $T-\pi^r u$, u a unit of A can be split off. That is,

$$\eta = (T-\pi^r u_1)\cdots(T-\pi^r u_{h-l})\hat{\eta} \tag{28.4.25}$$

To prove this it suffices to show that if $l < h-1$ and $\eta = (T-\pi^r u)\eta_1$, then the minimum (28.4.15) for η_1 instead of η is still r. This is seen as follows. Writing

$$\eta = \sum_{i=0}^{h} T^i a_i = (T-\pi^r u)\sum_{i=0}^{h-1} T^i b_i \tag{28.4.26}$$

we find that

$$a_0 = -\pi^r u b_0, \qquad a_i = -\pi^r \sigma^i(u) b_i + b_{i-1}, \qquad i \geq 1 \quad (b_h = 0) \tag{28.4.27}$$

Now we have $v(a_l) = r(h-l)$, $v(a_i) \geq r(h-i)$ for all i and $v(a_i) > r(h-i)$ for $i < l$. It follows easily from (28.4.27) that $v(b_i) > r(h-1-i)$ for $i < l$, $v(b_l) = r(h-1-l)$ and $v(b_i) \geq r(h-1-i)$ for all i, which proves our assertion and the addendum.

We group the results obtained together in one final theorem.

■ (28.4.28) **Theorem** Let A, k, p, q, π, $\mathscr{E}$, σ, T be as in (28.4.1). Then every finitely generated torsion left $\mathscr{E}$-module is isomorphic to a direct sum of modules of the forms

$$\mathscr{E}/\mathscr{E}\pi^i, \qquad \mathscr{E}/\mathscr{E}(T^r-\pi^s)$$

with $(r, s) = 1$. The modules $\mathscr{E}/\mathscr{E}\pi^i$ are indecomposable and the modules $\mathscr{E}/\mathscr{E}(T^r-\pi^s)$ are simple and pairwise nonisomorphic for different pairs r, s with $(r, s) = 1$.

28.5 Classification up to isogeny of finite dimensional formal group laws over an algebraically closed field k of characteristic $p > 0$

In this section k is an algebraically closed field of characteristic $p > 0$. All formal group laws are over k and finite dimensional.

■ (28.5.1) **Which $\mathbf{D}_V(k)$-modules come from $\mathbf{D}(k)$ modules?** Every $\mathbf{D}_V(k)$-module is isomorphic to a direct sum

$$\mathscr{C}' = \bigoplus_i \mathbf{D}_V(k)/\mathbf{D}_V(k)(V^{r_i}-p^{s_i}) \oplus \bigoplus_i \mathbf{D}_V(k)/\mathbf{D}_V(k)p^i \tag{28.5.2}$$

$$(r_i, s_i) = 1$$

by Theorem (28.4.28). We claim that the module (28.5.2) is of the form $\mathscr{C}_{\mathbf{V}}$ for some finitely generated reduced $\mathbf{D}(k)$-module $\mathscr{C}$ if and only if $r_i > s_i$ for all i, for which r_i or s_i is > 1; so $r = s = 1$ is the only pair that is allowed with $s \geq r$. Sufficiency of this condition is readily verified because if $r \geq s$, we have

$$\mathbf{D}_{\mathbf{V}}(k)/\mathbf{D}_{\mathbf{V}}(k)(\mathbf{V}^r - p^s) \simeq \mathbf{D}_{\mathbf{V}}(k) \otimes_{\mathbf{D}(k)} \mathbf{D}(k)/\mathbf{D}(k)(\mathbf{f}^s - \mathbf{V}^{r-s})$$

$$\mathbf{D}_{\mathbf{V}}(k)/\mathbf{D}_{\mathbf{V}}(k)p^i \simeq \mathbf{D}_{\mathbf{V}}(k) \otimes_{\mathbf{D}(k)} \mathbf{D}(k)/\mathbf{D}(k)\mathbf{f}^i$$

(The formal group laws corresponding to the $\mathbf{D}(k)/\mathbf{D}(k)(\mathbf{f}^s - \mathbf{V}^{r-s})$, $\mathbf{D}(k)/\mathbf{D}(k)\mathbf{f}^i$ will be constructed below in (28.5.3), proving that these modules are reduced, which can also be seen directly.) The condition is also necessary. Assume that the module $\mathscr{C}'$ of (28.5.2) is of the form $\mathscr{C}' = \mathscr{C}_{\mathbf{V}}$. Then $\mathscr{C} \subset \mathscr{C}'$. Suppose that $r_1 < s_1$ and let $\mathbf{V}^{-h}\gamma$, $\gamma \in \mathscr{C}$ be the image of $1 \in \mathbf{D}_{\mathbf{V}}(k)$ in the first direct summand of $\mathscr{C}'$ (under the natural map $\mathbf{D}_{\mathbf{V}}(k) \to \mathbf{D}_{\mathbf{V}}(k)/\mathbf{D}_{\mathbf{V}}(k)(\mathbf{V}^{r_1} - p^{s_1}) \subset \mathscr{C}'$). Let

$$\vartheta = 1 - \mathbf{V}^{(s_1 - r_1)}\mathbf{f}^{s_1} \in \mathbf{D}(k)$$

Then one finds $\vartheta\gamma = 0$, which is impossible because $\gamma \neq 0$ and ϑ is a unit of $\mathbf{D}(k)$ because $r_1 < s_1$.

■ (28.5.3) **Construction of some formal group laws** Let $F_V(X, Y)$ over $\mathbf{Z}[V]$ be the universal n-dimensional p-typical formal group law constructed in Chapter II, Section 10.3. Now substitute

$$V_1 = \begin{pmatrix} 0 & \cdots & & 0 \\ 1 & \ddots & & \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & & \\ 0 & \cdots & 0\ 1 & 0 \end{pmatrix}, \qquad V_2 = V_3 = \cdots = 0$$

(If $n = 1$, then also $V_1 = 0$.) The resulting formal group law has logarithm $f(X) = f(X_0, \ldots, X_{n-1})$ with components

$$f_0(X) = X_0$$

$$f_1(X) = X_1 + p^{-1}X_0^p, \ldots,$$

$$f_{n-1}(X) = X_{n-1} + p^{-1}X_{n-2}^p + \cdots + p^{-n+1}X_0^{p^{n-1}}$$

i.e., it is the Witt vector formal group law $\hat{W}_{p^{n-1}}(X; Y)$ of dimension n defined by the Witt addition polynomials $\Sigma_1, \Sigma_p, \ldots, \Sigma_{p^{n-1}}$. According to (27.7.15), we have that

$$\mathbf{f}_p\delta_i = \sum_{n=0}^{\infty} \mathbf{V}_p^n\langle V_{n+1}(i, i)\rangle\delta_j \tag{28.5.4}$$

where $\delta_1, \ldots, \delta_n$ is the standard basis. So that using (28.5.3), (28.5.4) we find for $\hat{W}_{p^n}(X; Y)$

$$\mathbf{f}\delta_1 = \delta_2, \qquad \mathbf{f}\delta_2 = \delta_3, \qquad \ldots, \qquad \mathbf{f}\delta_{n-1} = \delta_n, \qquad \mathbf{f}\delta_n = 0$$

so that the $\mathbf{D}(k)$-module of $\hat{W}_{p^n}(X; Y)$ (over k) is

$$\mathscr{C}_p(\hat{W}_{p^n}(X; Y); k) = \mathbf{D}(k)/\mathbf{D}(k)\mathbf{f}^n \tag{28.5.5}$$

Now assuming $n \geq 1$ and $m \geq 1$, let us substitute

$$V_1 = \begin{pmatrix} 0 & \cdots & & & 0 \\ 1 & \ddots & & & \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & & & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \qquad V_2 = \cdots = V_m = 0$$

$$V_{m+1} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}, \qquad V_{m+2} = V_{m+3} = \cdots = 0$$

(and again $V_1 = 0$ if $n = 1$).

Let $(n, m) = 1$ and let $G_{n,m}(X, Y)$ be the formal group law over $\mathbf{Z}$ thus obtained. Then using (28.5.4) we find for $G_{n,m}(X, Y)$

$$\mathbf{f}\delta_1 = \delta_2, \quad \mathbf{f}\delta_2 = \delta_3, \quad \ldots, \quad \mathbf{f}\delta_{n-1} = \delta_n, \quad \mathbf{f}\delta_n = \mathbf{V}^m\delta_1 \tag{28.5.6}$$

so that the $\mathbf{D}(k)$-module of $G_{n,m}(X; Y)$ as a formal group law over k is

$$\mathscr{C}_p(G_{n,m}, k) \simeq \mathbf{D}(k)/\mathbf{D}(k)(\mathbf{f}^n - \mathbf{V}^m) \tag{28.5.7}$$

Finally, taking $n = 1$, $m = 0$ and $V_1 = 1$, $V_2 = V_3 = \cdots = 0$, we find a (p-typical version of) the multiplicative formal group law $\hat{\mathbf{G}}_m(X, Y)$ with $\mathbf{D}(k)$-module

$$\mathscr{C}_p(\hat{\mathbf{G}}_m; k) \simeq \mathbf{D}(k)/\mathbf{D}(k)(\mathbf{f} - 1) \quad (= W_{p^\infty}(k)) \tag{28.5.8}$$

So combining this with the results of (28.5.1) and (28.4.28), we find the classification up to isogeny theorem.

■ (28.5.9) **Theorem** Every finite dimensional formal group law $F(X, Y)$ over an algebraically closed field k of characteristic $p > 0$ is isogenous to a direct sum of formal group laws

$$\hat{\mathbf{G}}_m(X, Y); \qquad G_{n,m}(X, Y) \quad \text{with} \quad (n, m) = 1, \ n, m \in \mathbf{N}$$
$$\hat{W}_{p^n}(X, Y), \quad n \in \mathbf{N} \cup \{0\}$$

This decomposition is unique up to isogeny. The formal group laws $G_{n,m}(X, Y)$, $n, m \in \mathbf{N}$, $(n, m) = 1$, are simple and the $\hat{W}_{p^n}(X; Y)$ are indecomposable.

■ (28.5.10) **Remark** Manin introduced the notation $G_{n,m}(X, Y)$ with $1 \leq n < \infty$, $0 \leq m \leq \infty$, $(n, m) = 1$ (with the convention $(n, \infty) = 1$ for all n) as a unifying notation for all the formal group laws occurring in (28.5.9). One sets

$G_{1,0}(X, Y) = \hat{G}_m(X, Y)$. $G_{n,\infty}(X, Y) = \hat{W}_{p^n-1}(X, Y)$. Then the $G_{n,m}(X, Y)$ are determined up to isogeny by:

(i) $\dim G_{n,m}(X, Y) = n$;
(ii) $G_{n,m}(X, Y)$ is indecomposable up to isogeny;
(iii) $G_{n,m}(X; Y)$ is of height $n + m$.

29 Cartier–Dieudonné Theory for Formal A-Modules

In this section A is a discrete valuation ring with quotient field K, uniformizing element π, residue field k of characteristic p and with q elements, $q = p^r$. The uniformizing element π will be kept fixed throughout this section. A may be of characteristic $p > 0$ also.

In principle formal A-modules may be infinite dimensional in this section, but the main theorems are stated and proved only for finite dimensional formal A-modules.

29.1 Generalities concerning infinite dimensional formal A-modules

■ (29.1.1) **Infinite dimensional formal A-modules** Let I be an index set. A possibly infinite dimensional formal A-module over an A-algebra B with index set I is a formal group law $F(X, Y)$ over B with index set I together with a ring homomorphism $\rho_F: A \to \mathrm{End}_B(F(X, Y))$ such that the ith component of $\rho_F(a)(X)$ is congruent to aX_i mod(degree 2) for all $i \in I$. We shall also write $[a]_F(X)$ for the I-tuple of power series $\rho_F(a)(X)$ in (X_i), $i \in I$.

Of course, the $[a]_F(X)$ must satisfy the "monomials have compact support" condition of (27.1.3).

■ (29.1.2) **The formal A-module $\hat{W}_{q,\infty}(X, Y)$** Let $G_\pi(X, Y)$ over A be the Lubin–Tate formal group law with logarithm

$$G_\pi(X) = X + \pi^{-1}X^q + \pi^{-2}X^{q^2} + \cdots$$

and let Σ_0^A, Σ_1^A, Σ_2^A, ... be the addition polynomials for the functor $W_{q,\infty}^A(-)$ associated to $G_\pi(X, Y)$; cf. Chapter IV, Section (25.3.18). These polynomials $\Sigma_n^A(X; Y)$ in $X_0, \ldots, X_n; Y_0, \ldots, Y_n$ define a formal group law with index set $\{0, 1, 2, 3, \ldots\}$ over A with logarithm

$$\bar{w}_q^A(X) = \begin{pmatrix} X_0 \\ X_1 + \pi^{-1}X_0^q \\ X_2 + \pi^{-1}X_1^q + \pi^{-2}X_0^{q^2} \\ \vdots \end{pmatrix} \tag{29.1.3}$$

Now define for all $a \in A$,

$$[a]_{W^A_{q,\infty}}(X) = (\bar{w}^A_q)^{-1}(a\bar{w}^A_q(X)) \tag{29.1.4}$$

The usual functional equation arguments now show that this defines $(\mathbf{N} \cup \{0\})$-tuples of power series with coefficients in A. (For those unhappy about the infinity of indeterminates, cf. (27.1.19)(v) above; cf. also (E.3.9).

More generally, one has infinite dimensional formal A-modules $\hat{W}^F_{q,\infty}(X, Y)$, $\hat{W}^F(X, Y)$ associated to every one dimensional formal A-module $F(X, Y)$; cf. Chapter IV, Sections 25.1, 25.2, where the associated group functors are treated of which $\hat{W}^F_{q,\infty}$ and $\hat{W}^F$ are the "formal completions."

■ (29.1.5) **Curves** The group of curves $\mathscr{C}(F; B)$ of a possibly infinite dimensional formal A-module over the A-algebra B becomes an A-module via $(a, \gamma(t)) \mapsto [a]_F(\gamma(t))$. We have of course the usual operators $\mathbf{f}_n$, $\mathbf{V}_n$, $\langle b \rangle$; and since $[a]_F(X)$ is an endomorphism of $F(X, Y)$, we have that $[a]_F$ commutes with all of $\mathbf{f}_n$, $\mathbf{V}_n$, $\langle b \rangle$.

As a rule we shall simply write $[a]$ instead of $[a]_F$. Thus of the four kinds of operators $\mathbf{f}_n$, $\mathbf{V}_n$, $[a]$, $\langle b \rangle$ on $\mathscr{C}(F; B)$ the first and third kind depend on $F(X, Y)$ and the others do not depend on $F(X, Y)$.

■ (29.1.6) **q-Typification and q-typical curves in the infinite dimensional case** In Chapter IV, Section (25.5.17) we defined functor endomorphisms $\varepsilon^F_q: \mathscr{C}(F; -) \to \mathscr{C}(F; -)$ called "q-typifications" for finite dimensional formal A-modules $F(X, Y)$ and we defined a subfunctor $\mathscr{C}_q(F; -)$ of $\mathscr{C}(F; -)$, the image of ε^F_q, called "q-typical curve functor." The constructions relied in a fairly essential way on the universal m-dimensional formal A-modules $F^A_S(X, Y)$ and the universal curves $\gamma_C(t)$. Neither object exists in the infinite dimensional case, nor can they exist because of the "monomials have finite support" conditions; cf. (27.1.3).

There does exist a substitute universal object, a sort of inductive limit of finite dimensional universal formal A-modules (or formal group laws) which can be made to perform the same services as the universal formal A-modules and group laws in the finite dimensional case. We shall not expose these constructions here (cf. [184]) but shall rely instead on a direct functional equation argument that works for $\hat{W}^A_{q,\infty}$ and which works more generally for all "infinite dimensional functional equation" formal A-modules (but not for all (infinite dimensional) formal A-modules). For the Cartier–Dieudonné theory for finite dimensional formal A-modules which is to be developed below, only $\hat{W}^A_{q,\infty}$ is important.

The functional equation type character of $\hat{W}^A_{q,\infty}(X, Y)$ lies in the facts that $\hat{W}^A_{q,\infty}(X, Y)$ has an A-logarithm (cf. (29.1.3) and (29.1.4)) and that this A-logarithm satisfies a functional equation

$$\bar{w}^A_q(X) - \pi^{-1}Q\bar{w}^A_q(X^q) = X \in A[\![X]\!]^{\mathbf{N} \cup \{0\}} \tag{29.1.7}$$

where Q is the operator that maps the column vector $(b_0, b_1, b_2, \ldots)$ to the column vector $(0, b_0, b_1, b_2, \ldots)$.

In general of course the functional equation may involve infinitely many terms and a "twisting" endomorphism σ. All one dimensional formal A-modules $F(X, Y)$ have infinite dimensional functional equation type formal A-modules $\hat{W}^F(X, Y)$ associated to them; cf. Chapter IV, Sections 25.1, 25.2.

We shall present the general q-typification method for functional equation type infinite dimensional formal A-modules by just treating the case $\hat{W}_{q,\infty}(X; Y)$ (this saves a number of $\sum$ signs).

■ (29.1.8) **q-typification for $\hat{W}^A_{q,\infty}(X, Y)$** Let $I = \{0, 1, 2, \ldots\}$ be the index set of $\hat{W}^A_{q,\infty}(X, Y)$ and let $A[C]$ be short for $A[C_{i,n}; i \in I, n \in \mathbf{N}]$. For each finite subset κ of I, let $\gamma_\kappa(t)$ be the curve

$$\gamma_\kappa(t) = \sum_{i \in \kappa, n \in \mathbf{N}}^{W^A_{q,\infty}} C_{i,n}\delta_i(t^n) \tag{29.1.9}$$

where $\delta_i(t)$, $i \in I$, is the standard V-basis for $\mathscr{C}(\hat{W}^A_{q,\infty}; -)$. Note that $\gamma_\kappa(t)$ is a curve, i.e., satisfies the "monomials have compact support" condition. Consider

$$\bar{w}^A_q(\gamma_\kappa(t)) = \sum_{n=1}^{\infty} x_{n,\kappa} t^n \tag{29.1.10}$$

where the $x_{n,\kappa}$ are I-tuples of polynomials in the $C_{i,n}$ with coefficients in K. Let σ: $K[C] \to K[C]$ be the K-endomorphism $C_{i,n} \to C^q_{i,n}$. Then by the functional equation lemma the $x_{n,\kappa}$ satisfy the conditions:

$$x_{n,\kappa} \in A[C]^I \quad \text{if } q \text{ does not divide } n$$

$$x_{n,\kappa} - \pi^{-1}Q\sigma_* x_{q^{-1}n,\kappa} \in A[C]^I \quad \text{if } q \text{ does divide } n \tag{29.1.11}$$

It follows (by the functional equation lemma) that

$$\varepsilon_q \gamma_\kappa(t) = (\bar{w}^A_q)^{-1}\left(\sum_{n=0}^{\infty} x_{q^n,\kappa} t^{q^n}\right) \tag{29.1.12}$$

has its coefficients in $A[C]$ and hence is an element of $\mathscr{C}(\hat{W}^A_{q,\infty}; A[C])$.

This defines the ε_q for the particular curves $\gamma_\kappa(t)$.

Now let $\gamma(t) \in \mathscr{C}(\hat{W}^A_{q,\infty}; B)$ be any curve with coefficients in any A-algebra B Choose a number $s \in \mathbf{N}$. Because of the "monomials have finite support" condition there is a finite subset $\kappa(s) \subset I$ and a homomorphism ϕ_s: $A[C] \to B$ such that

$$(\phi_s)_* \gamma_{\kappa(s)}(t) = \gamma(t) \mod(\text{degree } s) \tag{29.1.13}$$

$$\phi_s(C_{i,n}) = 0 \quad \text{for} \quad i \notin \kappa \quad \text{or} \quad n \geq s$$

Moreover ϕ_s is uniquely determined by the conditions (29.1.13), simply because $\hat{W}^A_{q,\infty}(X, Y) \equiv X + Y \mod(\text{degree } 2)$.

We now define

$$\varepsilon_q\gamma(t) = \lim_{s\to\infty} (\phi_s)_* \varepsilon_q \gamma_{\kappa(s)}(t) \tag{29.1.14}$$

(where the limit is of course with respect to the topology of $\mathscr{C}(\hat{W}^A_{q,\infty}; B)$ defined by the subgroups $\mathscr{C}^n(W^A_{q,\infty}; B)$). Because of the uniqueness of the ϕ_s satisfying (29.1.13), we have that

$$\varepsilon_q\psi_*\gamma(t) = \psi_*\varepsilon_q\gamma(t) \tag{29.1.15}$$

for any $\psi: B \to B'$ in $\mathbf{Alg}_A$.

Now suppose that B is A-torsion free. Then (29.1.10), (29.1.12), and (29.1.14) show that we have

$$\bar{w}_q(\gamma(t)) = \sum_{n=1}^{\infty} x_n t^n \quad\Rightarrow\quad \bar{w}_q(\varepsilon_q\gamma(t)) = \sum_{n=0}^{\infty} x_{q^n} t^{q^n} \tag{29.1.16}$$

and this of course determines ε_q uniquely if B is A-torsion free. This characterization plus (29.1.15) plus the simple remark that any curve can be lifted back to a curve over an A-torsion free A-algebra then shows as usual that

■ (29.1.17) **Lemma** Formula (29.1.14) defines a functor endomorphism of the A-module-valued functor $\mathscr{C}(\hat{W}^A_{q,\infty}; -)$ and $\varepsilon_q\varepsilon_q = \varepsilon_q$. Moreover, ε_q commutes with the operators $[a]$, $a \in A$, $\langle b\rangle$, and $\mathbf{V}_q$.

■ (29.1.18) More generally, the method given above works for any functional equation formal A-module and for any formal A-module of the form $\phi_* F(X, Y)$ with $\phi \in \mathbf{Alg}_A$ and $F(X, Y)$ of functional equation type. We also note that (29.1.14) agrees with the definitions given in (25.5.17) in the finite dimensional case. This, and (29.1.16), (29.1.12) means that ε_q commutes with the A-module homomorphisms induced by formal A-module homomorphisms $\alpha(X)$. That is, the diagram

$$\begin{array}{ccc} \mathscr{C}(F; B) & \xrightarrow{\varepsilon_q} & \mathscr{C}(F; B) \\ \downarrow{\scriptstyle \alpha_*} & & \downarrow{\scriptstyle \alpha_*} \\ \mathscr{C}(G; B) & \xrightarrow{\varepsilon_q} & \mathscr{C}(G; B) \end{array}$$

commutes for every homomorphism of formal A-modules $\alpha(X)$: $F(X, Y) \to G(X, Y)$.

■ (29.1.19) **Definition** $\mathbf{FG}^A_B$ denotes the category of formal A-modules over the A-algebra B.

■ (29.1.20) **Definition** By the remarks made in (29.1.18), (29.1.17), and (29.1.6) we have defined a functor endomorphism ε_q of the functor $\mathscr{C}(-; B)$: $\mathbf{FG}^A_B \to \mathbf{Mod}_A$. We shall denote the image functor by $\mathscr{C}_q(-; B)$. The elements of $\mathscr{C}_q(-; B)$ are called q-typical curves.

Strictly speaking of course, we have defined ε_q only for the full subcategory of $\mathbf{FG}_B^A$ consisting of the finite dimensional formal A-modules and $\hat{W}_{q,\infty}^A$. This is in fact enough for our purposes below.

■ (29.1.21) **Definition** A formal A-module $F(X, Y)$ with index set I in $\mathbf{FG}_B^A$ will be called A-typical if it is of the form $F(X, Y) = \phi_* G(X, Y)$, where $G(X, Y) \in \mathbf{FG}_{B'}^A$ is a formal A-module with a logarithm $g(X)$ of the form

$$g(X) = X + \sum_{i=0}^{\infty} b_i X^{q^i} \tag{29.1.22}$$

where the b_i are I-tuples of elements of $B' \otimes_A K$, B' is A-torsion free, and ϕ: $B' \to B$ is an A-algebra homomorphism. Note that this agrees with our previous definition in the finite dimensional case (cf. Chapter IV, Section (25.4.27)). Note also that $\hat{W}_{q,\infty}^A(X; Y)$ is A-typical.

If $F(X, Y)$ is A-typical, then its standard $\mathbf{V}$-basis $\delta_i(t)$, $i \in I$, consists of q-typical curves and we have

■ (29.1.23) **Lemma** Let $F(X, Y)$ be an A-typical formal A-module over B. Then every element $\gamma(t) \in \mathscr{C}_q(F; B)$ can be written uniquely as a convergent sum

$$\sum_{n=0}^{\infty} {}^F \sum_{i \in I} {}^F \mathbf{V}_q^n \langle b_{n,i} \rangle \delta_i(t)$$

with for every n only finitely many i such that $b_{n,i} \neq 0$, and every element $\gamma(t) \in \mathscr{C}(F; B)$ can be written uniquely as a convergent sum

$$\sum_{q \nmid m} \mathbf{V}_m \gamma_m(t), \qquad \gamma_m(t) \in \mathscr{C}_q(F; B)$$

Proof Standard; do the case "B is A-torsion free" first.

■ (29.1.24) $\mathscr{C}_q(F; B)$ is a closed sub-A-module of $\mathscr{C}(F; B)$; its (inherited) topology is defined by the sub-A-modules $\mathscr{C}_q^{(n)}(F; B) = \mathscr{C}_q(F; B) \cap \mathscr{C}^{q^n}(F; B)$; $\mathscr{C}_q(F; B)$ is stable under $\mathbf{V}_q$, $[a]$, $\mathbf{f}_q$, and $\langle b \rangle$. Cf. Lemma (29.1.17). It is not stable under $\mathbf{V}_m$ if m is not a power of q nor under $\mathbf{f}_p$ (unless $q = p$).

The topological A-module $\mathscr{C}_q(F; B)$ is Hausdorff and complete.

■ (29.1.25) **The Frobenius operator $\mathbf{f}_\pi$ in the infinite dimensional case** With respect to the Frobenius operator $\mathbf{f}_\pi$ on $\mathscr{C}(F; B)$ for infinite dimensional formal A-modules, the situation is exactly the same as for q-typification.

The relevant formulas for the case of $\hat{W}_{q,\infty}^A(X, Y)$ are

$$\mathbf{f}_\pi \gamma_\kappa(t) = (\bar{w}_q^A)^{-1} \left(\sum_{n=1}^{\infty} \pi x_{qn,\kappa} t^n \right) \tag{29.1.26}$$

$$\mathbf{f}_\pi \gamma(t) = \lim_{s \to \infty} (\phi_s)_* \mathbf{f}_\pi \gamma_{\kappa(s)}(t) \tag{29.1.27}$$

where γ_κ, x_κ, $\gamma_{\kappa(s)}$, and ϕ_s are as in (29.1.9), (29.1.10), (29.1.13). The integrality of $\mathbf{f}_\pi \gamma_\kappa(t)$ is proved as usual (cf. Chapter IV, Section (25.5.3)). If B is torsion free, then $\mathbf{f}_\pi$ is characterized by

$$(29.1.28) \qquad \bar{w}_q^A(\gamma(t)) = \sum_{i=1}^{\infty} y_i t^i \quad \Rightarrow \quad \bar{w}_q^A(\mathbf{f}_\pi \gamma(t)) = \sum_{i=1}^{\infty} \pi y_{iq} t^i$$

and using this one proves in the usual way that

■ (29.1.29) **Lemma** $\mathbf{f}_\pi$ is a continuous, additive, functor endomorphism of the functor $\mathscr{C}(-; B)$: $\mathbf{FG}_B^A \to \mathbf{Mod}_A$. Moreover, $\mathbf{f}_\pi \phi_* = \phi_* \mathbf{f}_\pi$ for $\phi \in \mathbf{Alg}_A$ and $\mathbf{f}_\pi$ commutes with ε_q, so $\mathbf{f}_\pi$ induces a functor endomorphism of $\mathscr{C}_q(-; B)$. The commutation rules of $\mathbf{f}_\pi$ with the various other operators on $\mathscr{C}(-; B)$ are

$$(29.1.30) \qquad \mathbf{f}_\pi \mathbf{f}_n = \mathbf{f}_n \mathbf{f}_\pi \qquad \text{for all} \quad n \in \mathbf{N}$$

$$(29.1.31) \qquad \mathbf{f}_\pi [a] = [a] \mathbf{f}_\pi \qquad \text{for all} \quad a \in A$$

$$(29.1.32) \qquad \mathbf{f}_\pi \langle b \rangle = \langle b^q \rangle \mathbf{f}_\pi \qquad \text{for all} \quad b \in B$$

$$(29.1.33) \qquad \mathbf{f}_\pi \mathbf{V}_q = [\pi]$$

$$(29.1.34) \qquad [u] \mathbf{f}_\pi^e \mathbf{V}_p^{r-1} = \mathbf{f}_p \qquad \text{if} \quad u\pi^e = p$$

(in the characteristic zero case)

■ (29.1.35) **Example** Let $\delta_0(t)$, $\delta_1(t)$, $\delta_2(t)$, ... be the standard $\mathbf{V}$-basis for $\hat{W}_{q,\infty}^A(X; Y)$ over some A-algebra B. Then we have

$$(29.1.36) \qquad \mathbf{f}_\pi^n \delta_0(t) = \delta_n(t)$$

It suffices (because $\mathbf{f}_\pi^n$ commutes with ϕ_*'s) to prove this for A-torsion free A-algebras B. We then have (cf. (29.1.3))

$$\bar{w}_q^A(\delta_0(t)) = \begin{pmatrix} t \\ \pi^{-1} t^q \\ \pi^{-2} t^{q^2} \\ \pi^{-3} t^{q^3} \\ \vdots \end{pmatrix}, \qquad \bar{w}_q^A(\delta_n(t)) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ t \\ \pi^{-1} t^q \\ \pi^{-2} t^{q^2} \\ \vdots \end{pmatrix} \text{nth row}$$

and the result follows from (29.1.28). Now $\hat{W}_{q,\infty}^A(X, Y)$ is an A-typical formal A-module, so that the $\delta_0(t)$, $\delta_1(t)$, ... are all in $\mathscr{C}_q(\hat{W}_{q,\infty}^A; B)$. So that writing $\gamma_\pi(t)$ for $\delta_0(t)$ we have by (29.1.36), Lemma (29.1.23) and (29.1.24) a unique convergent sum expression for all $\gamma(t) \in \mathscr{C}_q(\hat{W}_{q,\infty}^A; B)$:

$$(29.1.37) \qquad \gamma(t) = \sum_{i,n}^{W_{q,\infty}^A} \mathbf{V}_q^n \langle b_{n,i} \rangle \mathbf{f}_\pi^i \gamma_\pi(t)$$

Further, $\hat{W}^A_{q,\infty}$ is curvilinear so that

$$\sum_{i=0}^{\infty}{}^{W^A_{q,\infty}} \delta_i(X_i) = (X_0, X_1, X_2, \ldots)$$

so that we also have

$$(X_0, X_1, X_2, \ldots) = \sum_{i=0}^{\infty}{}^{W^A_{q,\infty}} \mathbf{f}^i_\pi \gamma_\pi(X_i) \tag{29.1.38}$$

These formulas are of course the analogues for $\hat{W}^A_{q,\infty}(X, Y)$ of (27.1.7) and the formulas of (27.1.8) for $\hat{W}(X, Y)$.

29.2 The representation theorem (= analogue of first theorem)

In this case the representation theorem says that for a fixed A-algebra B the functor $\mathbf{FG}^A_B \to \mathbf{Mod}_A$, $F(X, Y) \mapsto \mathscr{C}_q(F; B)$ is representable by $\hat{W}^A_{q,\infty}(X, Y)$ as a formal A-module over B. More precisely,

■ (29.2.1) **Theorem** (representation theorem) Let B be an A-algebra, let $F(X, Y) \in \mathbf{FG}^A_B$, and let $\gamma(t) \in \mathscr{C}_q(F; B)$ be a curve. Then there exists precisely one homomorphism of formal A-modules $\alpha_\gamma(X)$: $\hat{W}^A_{q,\infty}(X, Y) \to F(X, Y)$ such that $\alpha_\gamma(\gamma_\pi(t)) = \gamma(t)$. The correspondence $\mathscr{C}_q(F; B) \xrightarrow{\sim} \mathbf{FG}^A_B(\hat{W}^A_{q,\infty}(X, Y), F(X, Y))$ is an isomorphism of topological A-modules.

Proof Suppose that $\alpha_\gamma(X)$ is a homomorphism of formal A-modules such that $\alpha_\gamma(\gamma_\pi(t)) = \gamma(t)$. Now $\alpha_{\gamma\bullet}$ commutes with $\mathbf{f}_\pi$ and is additive and continuous, so applying $\alpha_{\gamma\bullet}$ to (29.1.38) we find that we must have

$$\alpha_\gamma(X) = \sum_{i=0}^{\infty}{}^{F} \mathbf{f}^i_\pi(X_i) \tag{29.2.2}$$

This takes care of the uniqueness of $\alpha_\gamma(X)$ and it remains to prove only that this $\alpha_\gamma(X)$ is indeed a homomorphism of formal A-modules. The proof of this is completely parallel to the proof of the analogous fact concerning $\hat{W}(X, Y)$; cf. (27.1.19). Here are the details. (The reader who fears this may become tedious is invited to skip this bit.) First note that if we have proved the theorem for a formal group A-module $\hat{F}(X, Y)$ that is A-isomorphic to $F(X, Y)$ over B, then we have also proved it for $F(X, Y)$. We can therefore suppose that $F(X, Y)$ is A-typical. Now suppose first that $B = A[V; C]$, that $F(X, Y)$ is the universal m-dimensional A-typical formal A-module over $A[V] \subset A[V; C]$, and that

$$\gamma_C(t) = \sum^F C_i t^{q^i}$$

(where C_i is short for the column vector $(C_{i,1}, \ldots, C_{i,m})$) is the universal q-typical curve in $\mathscr{C}_q(F; B)$. Consider

$$f(\gamma_C(t)) = \sum_{n=0}^{\infty} x_n t^{q^n}$$

The x_i are column vectors of polynomials in the V's and C's with coefficients in K; by the functional equation lemma they satisfy relations

$$(29.2.3)\quad x_i - \pi^{-1}V_1 x_{i-1}^{(q)} - \cdots - \pi^{-1}V_{i-1}x_1^{(q^{i-1})} - \pi^{-1}V_i x_0^{(q^i)} \in A[V, C]^m$$

Now let M be the $m \times (\mathbf{N} \cup \{0\})$ matrix consisting of the column vectors x_0, πx_1, $\pi^2 x_2$, $\pi^3 x_3$, ... (note that all entries of M are integral, i.e., elements of $A[V; C]$). Now define

$$(29.2.4)\qquad \alpha_\gamma(X) = f^{-1}(M\bar{w}_q^A(X))$$

We have already seen (cf. (29.1.33)) that $\bar{w}_q^A(\gamma_\pi(t))$ is the column vector $(t, \pi^{-1}t^q, \pi^{-2}t^{q^2}, \ldots)$. So we have

$$(29.2.5)\qquad f(\alpha_\gamma(\gamma_\pi(t))) = f(\gamma(t))$$

and hence $\alpha_\gamma(\gamma_\pi(t)) = \gamma(t)$ because $A[V; C]$ is A-torsion free, so (29.2.4) is the right formula (in the torsion free case). It remains to prove that $\alpha_\gamma(X)$ as defined by (29.2.4) is integral because this $\alpha_\gamma(X)$ is certainly a formal A-module homomorphism over $K[V; C]$. The integrality follows from (29.2.2) (which is certainly integral) and the fact that $\alpha_\gamma(X)$ is also unique over $K[V; C]$ (also by (29.2.2)). This proves the theorem in the case $F_V^A(X, Y)$, $\gamma_C(t)$ over $A[V; C]$. (Alternatively, one can easily show that $M\bar{w}_q^A(X)$ satisfies the same type of functional equation as $f(X) = f_V^A(X)$, by using (29.2.3), exactly as we did for $\hat{W}(X, Y)$ in (27.1.19).) Now let $F(X, Y)$ over B be any formal A-module over any A-algebra B and $\gamma(t)$ any element of $\mathscr{C}_q(F; B)$. Then there is a unique homomorphism ϕ_*: $A[V; C] \to B$ such that $\phi_* F_V^A(X, Y) = F(X, Y)$, $\phi_* \gamma_C(t) = \gamma(t)$. Applying ϕ_* to the $\alpha_\gamma(X)$ of (29.2.4) then gives a homomorphism $\hat{W}_{q,\infty}^A(X, Y) \to F(X, Y)$ that takes $\gamma_\pi(t)$ to $\gamma(t)$, which is the unique homomorphism doing this by (29.2.2). This takes care of existence of $\alpha_\gamma(X)$ for finite dimensional formal A-modules.

(To take care of the infinite dimensional formal A-modules one uses a corollary of the universal constructions alluded to in (29.1.6), viz that every formal A-module over B is of the form $\phi_* F(X, Y)$ where $F(X, Y)$ is a functional equation formal A-module over an A-algebra of the form $A[C]$; cf. [184] for details.)

Finally, we observe that, given the fact that $\alpha_\gamma(X)$ as defined by (29.2.2) is a formal A-module homomorphism, formula (29.2.2) says that $\gamma(t) \mapsto \alpha_\gamma(X)$ is additive, continuous, and commutes with the A-module structures on $\mathscr{C}_q(F; B)$ and $\mathbf{FG}_B^A(\hat{W}_{q,\infty}^A(X, Y), F(X, Y))$; i.e., we have $[a]\gamma(t) \mapsto [a](\alpha_\gamma(X)) = [a]_F(X) \circ \alpha_\gamma(X)$.

29.3 The ring of operators $\mathrm{Cart}_A(B)$

■ (29.3.1) **Operators of $\mathscr{C}_q(-; B)$** Let B be a fixed A-algebra. An operator Q on $\mathscr{C}_q(-; B)$ is a functor endomorphism of the set-valued functor $\mathscr{C}_q(-; B)$ on $\mathbf{FG}_B^A$. As usual, this forces other properties of Q.

■ (29.3.2) **Lemma** Let Q_1, Q_2 be two operators on $\mathscr{C}_q(-; A)$. Then we have:

(i) $Q_1\gamma_\pi(t) = Q_2\gamma_\pi(t) \Rightarrow Q_1 = Q_2$.

(ii) Q_1 is additive and continuous and induces A-module endomorphisms.

(iii) Let $\gamma(t) \in \mathscr{C}_q(\hat{W}^A_{q,\infty}; B)$, then there is a unique operator Q_γ such that $Q_\gamma(\gamma_\pi(t)) = \gamma(t)$.

Proof (i) Let $\gamma(t) \in \mathscr{C}_q(F; B)$, $F(X, Y) \in \mathbf{FG}^A_B$. Then by Theorem (29.2.1) there is a unique homomorphism $\alpha_\gamma(X)$: $\hat{W}^A_{q,\infty}(X, Y) \to F(X, Y)$ such that $\alpha_\gamma(\gamma_\pi(t)) = \gamma(t)$. The functoriality of Q_1 and Q_2 now gives us

$$Q_1\gamma(t) = Q_1\alpha_\gamma(\gamma_\pi(t)) = \alpha_\gamma(Q_1\gamma_\pi(t)) = \alpha_\gamma(Q_2\gamma_\pi(t)) = Q_2\alpha_\gamma(\gamma_\pi(t)) = Q_2\gamma(t)$$

(ii) To prove that Q_1 is additive, continuous, and commutes with the $[a]$ operators simply observe that the formula

$$Q_1\gamma(t) = \alpha_\gamma(Q_1\gamma_\pi(t))$$

implies all this because $\gamma(t) \mapsto \alpha_\gamma(X)$ is a continuous A-module homomorphism (cf. Theorem (29.2.1)).

(iii) The defining formula for Q_γ is $Q_\gamma(\delta(t)) = \alpha_\delta(\gamma(t))$. This is functorial by the uniqueness of the $\alpha_\delta(X)$ such that $\alpha_\delta(\gamma_\pi(t)) = \delta(t)$.

■ (29.3.3) **Corollary** There is a one–one correspondence between operators Q and elements $\gamma(t) \in \mathscr{C}_q(\hat{W}^A_{q,\infty}; B)$.

■ (29.3.4) **Corollary** Every operator of $\mathscr{C}_q(-; B)$ can be uniquely written as a sum

$$\sum_{m,n=0}^{\infty} \mathbf{V}_q^m\langle b_{m,n}\rangle\mathbf{f}_\pi^n, \qquad b_{m,n} \in B \tag{29.3.5}$$

with for every m only finitely many n such that $b_{m,n} \neq 0$. This follows from Corollary (29.3.3), together with formula (29.1.37).

■ (29.3.6) Let $b, c \in B$. Then one particular operator on $\mathscr{C}_q(-; B)$ is $\langle b\rangle + \langle c\rangle$, and according to Corollary (29.3.4) we must be able to write this operator in the form (29.3.5). We claim that

$$\langle b\rangle + \langle c\rangle = \sum_{n=0}^{\infty} \mathbf{V}_q^m\langle r_m^A(b, c)\rangle\mathbf{f}_\pi^m \tag{29.3.7}$$

where the $r_m^A(Z_1, Z_2)$ are certain polynomials with coefficients in A, defined by the conditions

$$(Z_1^{q^n} + Z_2^{q^n}) = \sum_{i=0}^{n} \pi^i r_i^A(Z_1, Z_2)^{q^{n-i}} \tag{29.3.8}$$

(To prove that these polynomials do indeed have their coefficients in A, use induction on n and the fact that for any polynomial $r(Z_1, Z_2)$ with coefficients in A we have $r(Z_1^q, Z_2^q)^{q^i} \equiv r(Z_1, Z_2)^{q^{i+1}} \bmod \pi^{i+1}$.)

■ (29.3.9) **Proof of formula (29.3.7)** Because every $F(X, Y) \in \mathbf{FG}_B^A$ comes (via a ϕ_*) from a formal A-module with an A-logarithm and because both sides of (29.3.7) commute with ϕ_*'s and α_*'s, it suffices to prove (29.3.7) for the case of an additive formal A-module. (Cf. Chapter III, Sections (16.2.11) and (16.2.12) for a similar argument in detail.)

So suppose that $F(X, Y)$ is an additive formal A-module. Then $\mathscr{C}_q(F; B)$ is the abelian group of power series $\gamma(t) = \sum_{n=0}^{\infty} x_n t^{q^n}$ with ordinary addition and $\mathbf{f}_\pi(\sum_{n=0}^{\infty} x_n t^{q^n}) = \sum_{n=0}^{\infty} \pi x_{n+1} t^{q^n}$; cf. (29.1.28) So the right-hand side of (29.3.7) applied to $\gamma(t)$ yields

$$\begin{aligned}\left(\sum_{m=0}^{\infty} \mathbf{V}_q^m \langle r_m^\pi(b, c)\rangle \mathbf{f}_\pi^m\right)\left(\sum_{n=0}^{\infty} x_n t^{q^n}\right) &= \sum_{m=0}^{\infty} \mathbf{V}_q^m \langle r_m(b, c)\rangle \sum_{n=0}^{\infty} x_{n+m} \pi^m t^{q^n} \\ &= \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \pi^m r_m(b, c)^{q^n} x_{n+m} t^{q^{n+m}} \\ &= \sum_{s=0}^{\infty} \left(\sum_{n=0}^{s} \pi^{n-s} r_{n-s}(b, c)^{q^n}\right) x_s t^{q^s} \\ &= \sum_{s=0}^{\infty} (b^{q^s} + c^{q^s}) x_s t^{q^s} \\ &= \langle b\rangle \gamma(t) + \langle c\rangle \gamma(t))\end{aligned}$$

which proves our assertion.

■ (29.3.10) **Remark** Formula (29.3.7) for $\langle b\rangle + \langle c\rangle$ holds for $\langle b\rangle + \langle c\rangle$ considered as an operator on $\mathscr{C}_q(-; B)$. It does not hold for $\langle b\rangle + \langle c\rangle$ considered as an operator on $\mathscr{C}_p(-; B)$ and also of course not for $\langle b\rangle + \langle c\rangle$ as an operator on $\mathscr{C}(-; B)$.

■ (29.3.11) **The operators** $[a]$ Because we are dealing with formal A-modules, we also have the operators $[a]$ of $\mathscr{C}_q(-; B)$; these are, according to (29.3.4), also writable as expressions of the form (29.3.5). We claim that

$$[a] = \sum_{n=0}^{\infty} \mathbf{V}_q^n \langle b_n\rangle \mathbf{f}_\pi^n \tag{29.3.12}$$

where the b_n are such that

$$w_{q,n}^A(b_0, \ldots, b_n) = a \qquad \text{for all} \quad n \in \mathbf{N} \cup \{0\} \tag{29.3.13}$$

i.e., we have that $b_i = \Omega_i^A(a)$; cf. Chapter IV, Section (25.3.18). Here the Ω_i^A are polynomials with coefficients in K such that $\Omega_i(a) \in A$ for all $a \in A$. The first two Ω_i^A are $\Omega_0^A = Z$, $\Omega_1^A = \pi^{-1}(Z - Z^q)$. That the $\Omega_i^A(a)$ are in A for all $a \in A$ follows of course from Corollary (29.3.4) (once we have shown that (29.3.12) holds); it also follows from Section (25.3.18) of Chapter IV. Here is an indepen-

dent (really the same) proof. If $b_0, \ldots, b_n \in A$, then $w^A_{q,n}(b_0^q, \ldots, b_n^q) \equiv w^A_{q,n+1}(b_0, \ldots, b_{n+1}) \bmod \pi^{n+1}$, hence

$$b_{n+1} = \pi^{-(n+1)}(w_{q,n+1}(b_0, \ldots, b_{n+1}) - w_{q,n}(b_0^q, \ldots, b_n^q)) \equiv 0 \mod A$$

■ (29.3.14) **Proof of formula (29.3.12)** As usual it suffices to prove this for the additive formal A-module. We find

$$\begin{aligned}\left(\sum_{n=0}^{\infty} \mathbf{V}_q^n\langle b_n\rangle \mathbf{f}_\pi^n\right)\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right) &= \sum_{n=0}^{\infty}\sum_{i=0}^{\infty} \pi^n b_n^{q^i} x_{i+n} t^{q^{i+n}} \\ &= \sum_{n=0}^{\infty} w_{q,n}(b_0, \ldots, b_n) x_n t^{q^n} \\ &= [a]\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right)\end{aligned}$$

We can now describe the A-algebra $\mathrm{Cart}_A(B)$ as follows:

■ (29.3.15) **Proposition** Let B be an A-algebra. Then $\mathrm{Cart}_A(B)$ is the A-algebra consisting of all expressions

$$\sum_{n,m=0}^{\infty} \mathbf{V}_q^m\langle b_{m,n}\rangle \mathbf{f}_\pi^n, \qquad b_{m,n} \in B \tag{29.3.16}$$

in the symbols $\mathbf{V}_q$ and $\mathbf{f}_\pi$ with for every m only finitely many $b_{m,n} \neq 0$. The A-algebra structure is given by

$$[a] = \sum_{m=0}^{\infty} \mathbf{V}_q^m\langle \Omega_m^A(a)\rangle \mathbf{f}_\pi^m \tag{29.3.17}$$

where the $\Omega_m^A(Z)$ are the polynomials with coefficients in K determined by

$$w^A_{q,n}(\Omega_0^A, \Omega_1^A, \ldots, \Omega_n^A) = Z \qquad \text{for all} \quad n \in \mathbf{N} \cup \{0\} \tag{29.3.18}$$

The calculation rules in $\mathrm{Cart}_A(B)$ are

$$\langle b\rangle \mathbf{V}_q = \mathbf{V}_q\langle b^q\rangle, \qquad \mathbf{f}_\pi\langle b\rangle = \langle b^q\rangle \mathbf{f}_\pi \tag{29.3.19}$$

$$\mathbf{f}_\pi \mathbf{V}_q = [\pi] = \sum_{n=0}^{\infty} \mathbf{V}_q^m\langle \Omega_m^A(\pi)\rangle \mathbf{f}_\pi^m \tag{29.3.20}$$

$$\langle b + c\rangle = \sum_{m=0}^{\infty} \mathbf{V}_q^m\langle r_m^A(b, c)\rangle \mathbf{f}_\pi^m \tag{29.3.21}$$

where the $r_m^A(Z_1, Z_2)$ are the polynomials with coefficients in A given by

$$Z_1^{q^n} + Z_2^{q^n} = \sum_{s=0}^{n} \pi^s r_s^A(Z_1, Z_2)^{q^{n-s}} \tag{29.3.22}$$

29.4 The faithfulness theorem (= analogue of second theorem)

■ (29.4.1) **Theorem** Let $F(X, Y)$, $G(X, Y) \in \mathbf{FG}_B^A$ and let β: $\mathscr{C}_q(F; B) \to \mathscr{C}_q(G; B)$ be an additive continuous homomorphism that commutes with the operators $\mathbf{V}_q$, $\mathbf{f}_\pi$, and $\langle b\rangle$ for all $b \in B$. Then there is a unique homomorphism of formal A-modules $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $\alpha_* = \beta$.

Proof It suffices to prove this for A-typical formal A-modules $F(X, Y)$ and $G(X, Y)$. These are also p-typical, and by Lemma (29.1.23) we can write every p-typical curve in $\mathscr{C}_p(F; B)$ as a finite sum

$$\gamma(t) = \sum_{i=0}^{r-1}{}^{F} \mathbf{V}_p^i \gamma_i(t), \qquad \gamma_i(t) \in \mathscr{C}_q(F; B) \tag{29.4.2}$$

where $q = p^r$. We now define an extension $\tilde{\beta}$: $\mathscr{C}_p(F; B) \to \mathscr{C}_p(G; B)$ by the formula

$$\tilde{\beta}(\gamma(t)) = \sum_{i=0}^{r-1}{}^{G} \mathbf{V}_p^i \beta(\gamma_i(t)) \tag{29.4.3}$$

Note that this is the only possible extension of β if we want $\tilde{\beta}$ to be additive. Clearly $\tilde{\beta}$ is an additive continuous map $\mathscr{C}_p(F; B) \to \mathscr{C}_p(G; B)$. We claim that $\tilde{\beta}$ also commutes with the operators $\mathbf{f}_\pi$, $\langle b\rangle$, $\mathbf{V}_p$, $\mathbf{f}_p$, and $[a]$.

To see this note that the unique expressions of $[a]$, $\langle b\rangle$, $\mathbf{V}_p$, $\mathbf{f}_\pi$, applied to $\gamma(t)$ as sums of elements in $\mathscr{C}_q(F; B)$ are respectively

$$[a]\gamma(t) = \sum_{i=0}^{r-1}{}^{F} \mathbf{V}_p^i([a]\gamma_i(t))$$

$$\langle b\rangle\gamma(t) = \sum_{i=0}^{r-1}{}^{F} \mathbf{V}_p^i(\langle b^{p^i}\rangle\gamma_i(t))$$

$$\mathbf{V}_p\gamma(t) = \sum_{i=0}^{r-2}{}^{F} \mathbf{V}_p^{i+1}(\gamma_i(t) +_F (\mathbf{V}_q\gamma_{r-1}(t))$$

$$\mathbf{f}_\pi\gamma(t) = \sum_{i=0}^{r-1}{}^{F} \mathbf{V}_p^i(\mathbf{f}_\pi\gamma_i(t))$$

The first three of these formulas are obvious ($[a]$ operators commute with $\mathbf{V}_p$ and $\langle b\rangle\mathbf{V}_p = \mathbf{V}_p\langle b^p\rangle$ and $\mathbf{V}_p\mathbf{V}_p^{r-1} = \mathbf{V}_q$). The fourth formula is less obvious because in general $\mathbf{V}_m$ and $\mathbf{f}_\pi$ certainly do not commute.

However, we have

(29.4.4) if $q \nmid m$ and $\gamma(t) \in \mathscr{C}_q(F; B)$, then $\mathbf{V}_m\mathbf{f}_\pi\gamma(t) = \mathbf{f}_\pi\mathbf{V}_m\gamma(t)$.

To prove this it suffices to prove this for the additive formal A-modules, and then we have

$$\mathbf{V}_m\mathbf{f}_\pi\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right) = \mathbf{V}_m\left(\sum_{i=0}^{\infty} \pi x_{i+1} t^{q^i}\right) = \sum_{i=0}^{\infty} \pi x_{i+1} t^{q^i m}$$

and on the other hand

$$\mathbf{f}_\pi\mathbf{V}_m\left(\sum_{i=0}^{\infty} x_i t^{q^i}\right) = \mathbf{f}_\pi\left(\sum_{i=0}^{\infty} x_i t^{q^i m}\right) = \sum_{q|q^i m} \pi x_i t^{q^{i-1}m}$$

and these sums are equal because q divides $q^i m$ if and only if $i \geq 1$ because q does not divide m.

Applying (29.4.3), we now find respectively

$$\tilde{\beta}([a]\gamma(t)) = \sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i \beta([a]\gamma_i(t)) = \sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i [a]\beta(\gamma_i(t))$$
$$= [a]\sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i \beta(\gamma_i(t)) = [a]\tilde{\beta}(\gamma(t))$$

because β commutes with $[a]$ operators since every $[a]$ operator can be written in terms of $\mathbf{V}_q$, $\langle b\rangle$'s and $\mathbf{f}_\pi$ (cf. (29.3.11));

$$\tilde{\beta}(\langle b\rangle\gamma(t)) = \sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i(\beta\langle b^{p^i}\rangle\gamma_i(t)) = \sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i\langle b^{p^i}\rangle\beta(\gamma_i(t))$$
$$= \sum_{i=0}^{r-1}{}^G \langle b\rangle \mathbf{V}_p^i \beta(\gamma_i(t)) = \langle b\rangle\tilde{\beta}(\gamma(t))$$

because β commutes with $\langle c\rangle$ operators;

$$\tilde{\beta}(\mathbf{V}_p\gamma(t)) = \sum_{i=0}^{r-2}{}^G \mathbf{V}_p^{i+1}\beta(\gamma_i(t)) +_G \beta(\mathbf{V}_q\gamma_{r-1}(t))$$
$$= \mathbf{V}_p\left(\sum_{i=0}^{r-2}{}^G \mathbf{V}_p^i\beta(\gamma_i(t))\right) +_G \mathbf{V}_q\beta(\gamma_{r-1}(t))$$
$$= \mathbf{V}_p\left(\sum_{i=0}^{r-2}{}^G \mathbf{V}_p^i\beta(\gamma_i(t)) +_G \mathbf{V}_p^{r-1}\beta(\gamma_{r-1}(t))\right) = \mathbf{V}_p\tilde{\beta}(\gamma(t))$$

because β commutes with $\mathbf{V}_q$;

$$\tilde{\beta}(\mathbf{f}_\pi\gamma(t)) = \sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i\beta(\mathbf{f}_\pi\gamma_i(t)) = \sum_{i=0}^{r-1}{}^G \mathbf{V}_p^i\mathbf{f}_\pi\beta(\gamma_i(t))$$
$$= \sum_{i=0}^{r-1}{}^G \mathbf{f}_\pi\mathbf{V}_p^i\beta(\gamma_i(t)) = \mathbf{f}_\pi\tilde{\beta}(\gamma(t))$$

because β commutes with $\mathbf{f}_\pi$ and because of (29.4.4).

Now if A is of characteristic zero, we have

$$\mathbf{f}_p = [u]\mathbf{f}_\pi^e \mathbf{V}_p^{r-1}$$

if $p = u\pi^e$, u a unit of A. So $\tilde{\beta}$ also commutes with $\mathbf{f}_p$. And if A is of characteristic p, we have that $\mathbf{f}_p = 0$ by Remark (29.4.6) below.

It follows that $\tilde{\beta}: \mathscr{C}_p(F; B) \to \mathscr{C}_p(G; B)$ is an additive continuous homomorphism that commutes with $\mathbf{f}_p$, $\mathbf{V}_p$, and $\langle b \rangle$ operators. By Theorem (27.7.10) it follows that there is a homomorphism of formal group laws $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $\tilde{\beta} = \mathscr{C}_p(\alpha(X); B)$. This homomorphism $\alpha(X)$ has the additional property that

$$\alpha([a]\gamma(t)) = [a](\alpha(\gamma(t)))$$

for every p-typical curve $\gamma(t)$ (because $\tilde{\beta}$ commutes with the $[a]$ operators). A slightly modified version of the curve lemma (27.1.9) (we must now take $d_1, \ldots, d_m$ to be powers of p to prove this modified version of (27.1.9); this can be done of course) then shows that

$$\alpha([a]_F(X)) = [a]_G(\alpha(X))$$

so that $\alpha(X)$ is in fact an A-homomorphism.

■ (29.4.5) **Corollary** Let $F(X, Y)$, $G(X, Y) \in \mathbf{FG}_B^A$ and let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of the formal group laws $F(X, Y)$, $G(X, Y)$. Then $\alpha(X)$ is a homomorphism of formal A-modules if and only if α_* commutes with $\mathbf{f}_\pi$.

■ (29.4.6) **Remark** Let $F(X, Y)$ be a formal A-module over $B \in \mathbf{Alg}_A$ and suppose that A is of characteristic $p > 0$. Then $[p]_F(X) = 0$ so that $F(X, Y)$ is isomorphic to the additive formal group law (cf. Chapter I, Corollary (5.6.7) and Chapter IV, Remark (21.1.14)). Now $\mathbf{f}_p^F$ depends only on the formal group structure of $F(X, Y)$ not on the formal A-module structure and $\mathbf{f}_p^F$ is zero if $F(X, Y)$ is an additive formal group law. Hence $\mathbf{f}_p^F = 0$ if $F(X, Y)$ is a formal A-module with A of characteristic $p > 0$.

29.5 The existence theorem (= analogue of third theorem)

As in the one prime case, the existence theorem is the easiest to prove.

■ (29.5.1) **Theorem** Let $\mathscr{C}$ be a complete Hausdorff topological group with continuous additive operators $\mathbf{V}_q$, $\mathbf{f}_\pi$, and $\langle b \rangle$ such that the relations (29.3.19)–(29.3.21) hold. Suppose that $\mathscr{C} = \varprojlim \mathbf{V}_q^n \mathscr{C}$, that $\mathbf{V}_q$ is injective, and that $\mathscr{C}/\mathbf{V}_q\mathscr{C}$ is a free B-module of finite rank. Then there exists a formal A-module $F(X, Y)$ over B of dimension $\operatorname{rank}_B(\mathscr{C}/\mathbf{V}_q\mathscr{C})$ such that $\mathscr{C} \simeq \mathscr{C}_q(F; B)$ and such that under this isomorphism the various operators correspond.

Proof Let $\delta_1, \ldots, \delta_m$ be a set of elements of $\mathscr{C}$ such that their classes

mod $\mathbf{V}_q\mathscr{C}$ are a basis for $\mathscr{C}/\mathbf{V}_q\mathscr{C}$ as a B-module. Then one proves as usual that $\delta_1, \ldots, \delta_m$ is a V-basis for $\mathscr{C}$, i.e., that every element of $\mathscr{C}$ can be written uniquely as a convergent sum

$$\gamma = \sum_{j=1}^{m} \sum_{n=0}^{\infty} \mathbf{V}_q^n\langle b_{n,j}\rangle\delta_j$$

In particular, we can write

$$\mathbf{f}_\pi\delta_i = \sum_{n=0}^{\infty} \sum_{j=1}^{m} \mathbf{V}_q^n\langle c(n, j, i)\rangle\delta_j \tag{29.5.2}$$

Let $F_V^A(X, Y)$ over $A[V]$ be the m-dimensional universal A-typical formal A-module. Let $\delta_1(t), \ldots, \delta_m(t)$ be the standard V-basis of $\mathscr{C}_q(F_V^A; A[V])$. Then we claim

$$\mathbf{f}_\pi\delta_i(t) = \sum_{n,j}^{F_V^A} \mathbf{V}_q^n\langle V_{n+1}(j, i)\rangle\delta_j(t) \tag{29.5.3}$$

This is proved exactly as in the corresponding formula for $\mathbf{f}_p$ in the proof of Theorem (27.7.14). The calculations are identical and so are the formulas except that some p's must be changed into π's and other p's must be changed into q's.

Let $\phi\colon A[V] \to B$ be the A-algebra homomorphism defined by $\phi(V_{n+1}(j, i)) = c(n, j, i)$ for $n \in \mathbf{N} \cup \{0\}$. Then formulas (29.5.2) and (29.5.3) show that $\mathscr{C}_q(\phi_* F_V^A; B) \cong \mathscr{C}$ where the isomorphism takes the standard basis $\delta_1(t), \ldots, \delta_m(t)$ into the chosen basis $\delta_1, \ldots, \delta_m$. Q.E.D.

■ (29.5.4) **Remark** A $\mathrm{Cart}_A(B)$-module $\mathscr{C}$ will be called *reduced* if it satisfies the conditions of (29.5.1) (i.e., if it comes from a formal A-module over B). Then we have also proved a one–one correspondence between A-typical formal A-modules and reduced $\mathrm{Cart}_A(B)$-modules with a particular V-basis.

■ (29.5.5) **Remark** In the hypothesis of Theorem (29.5.1) it is not necessary to require that all relations (29.3.19) hold exactly. For example, concerning the relation $\langle b\rangle + \langle c\rangle$, it suffices to require that $(\langle b\rangle + \langle c\rangle)\gamma \equiv \langle b + c\rangle\gamma$ mod $\mathbf{V}_q\mathscr{C}$. A similar remark applies to Theorem (27.7.14).

29.6 Description of the ring $\mathrm{Cart}_A(B)$

In this section we give a description of $\mathrm{Cart}_A(B)$ which is analogous to the description of $\mathrm{Cart}_p(A)$ given in 28.1.

■ (29.6.1) Recall that $W_{q,\infty}^A(-)$ is the unique functor $\mathbf{Alg}_A \to \mathbf{Alg}_A$ that as a set functor looks like $W_{q,\infty}^A(B) = \{(b_0, b_1, b_2, \ldots) \mid b_i \in B\}$, $W_{q,\infty}^A(\phi)(b_0, b_1, b_2, \ldots) = (\phi(b_0), \phi(b_1), \ldots)$ and which is such that the polynomials

$$w_{q,n}^A(Z_0, \ldots, Z_n) = Z_0^{q^n} + \pi Z_1^{q^{n-1}} + \cdots + \pi^n Z_n \tag{29.6.2}$$

induce functorial A-algebra homomorphisms $w_{q,n}^A\colon W_{q,\infty}^A(B) \to B$. Recall also that $W_{q,\infty}^A(-)$ admits two operators $\mathbf{V}_q$ and $\mathbf{f}_\pi$ which are defined by

$\mathbf{V}_q(b_0, b_1, \ldots) = (0, b_0, b_1, \ldots)$ and $w^A_{q,n}\mathbf{f}_\pi = w^A_{q,n+1}$ for all $n \in \mathbf{N} \cup \{0\}$. Finally, recall that $\mathbf{f}_\pi$ is an A-algebra endomorphism of $W^A_{q,\infty}(B)$. To avoid confusion with the symbol $\mathbf{f}_\pi$ occurring in $\mathrm{Cart}_A(B)$ we shall from now on use τ^A in Section 29 to denote the functorial A-algebra endomorphism $\mathbf{f}_\pi$ of $W^A_{q,\infty}(-)$.

■ (29.6.3) **Proposition** The map $(b_0, b_1, b_2, \ldots) \mapsto \sum_{n=0}^{\infty} \mathbf{V}_q^n\langle b_n\rangle \mathbf{f}_\pi^n$ is a functorial A-algebra homomorphism that identifies $W^A_{q,\infty}(-)$ with a subfunctor of $\mathrm{Cart}_A(-)$.

Proof It suffices to prove this for A-torsion free A-algebras B (by the functorial character of $W^A_{q,\infty}(-)$ and $\mathrm{Cart}_A(-)$). Let $\mathfrak{A}_2 \subset \mathrm{Cart}_A(B)$ be the right ideal of all elements $\sum \mathbf{V}_q^m\langle b_{m,n}\rangle \mathbf{f}_\pi^n$ such that $b_{0,n} = 0$ for all n. Note that $\mathrm{Cart}_A(B)/\mathfrak{A}_2$ is a free B-module with as a basis the classes of the $\mathbf{f}_\pi^n$ mod $\mathfrak{A}_2$, $n = 0, 1, 2, \ldots$. Now calculate $\mathbf{f}_\pi^n x$ mod $\mathfrak{A}_2$ for all $x \in \mathrm{Cart}_A(B)$. We find mod $\mathfrak{A}_2$

$$\begin{aligned}\mathbf{f}_\pi^n x &= \mathbf{f}_\pi^n \left(\sum_{i,j} \mathbf{V}_q^i\langle b_{i,j}\rangle \mathbf{f}_\pi^j\right)\\ &\equiv \sum_{i=0}^{n}\sum_{j=0}^{\infty} \pi^i \mathbf{f}_\pi^{n-i}\langle b_{i,j}\rangle \mathbf{f}_\pi^j\\ &\equiv \sum_{j=0}^{\infty}\sum_{i=0}^{n} \pi^i b_{i,j}^{q^{n-i}} \mathbf{f}_\pi^{n-i+j}\end{aligned}$$

We note that if B is A-torsion free and without nilpotents, then knowledge of $\mathbf{f}_\pi^n x$ mod $\mathfrak{A}_2$ for all n determines x completely, and we also note that x has $b_{m,n} = 0$ for all $m \neq n$ if and only if $\mathbf{f}_\pi^n x = \lambda_n \mathbf{f}_\pi^n$ for all $n \in \mathbf{N} \cup \{0\}$. It follows that

$$\left\{\sum_{n=0}^{\infty} \mathbf{V}_q^n\langle b_n\rangle \mathbf{f}_\pi^n\right\} \tag{29.6.4}$$

is a subring of $\mathrm{Cart}_A(B)$ at least in the case that B is A-torsion free. But then as (29.6.4) clearly defines a subfunctor of $\mathrm{Cart}_A(-)$ we have that this holds for all A-algebras B.

We are now going to identify the functorial subring $R(B) = \sum_{n=0}^{\infty} \mathbf{V}_q^n\langle b_n\rangle \mathbf{f}_\pi^n$ with $W^A_{q,\infty}(B)$. To this end define

$$w^A_{q,n}\left(\sum_{r=0}^{\infty} \mathbf{V}_q^r\langle b_r\rangle \mathbf{f}_\pi^r\right) = \sum_{r=0}^{n} \pi^r b_r^{q^{n-r}}$$

We shall now prove that

$$\begin{aligned} w^A_{q,n}(\mathbf{V}_q^r\langle b\rangle \mathbf{f}_\pi^r + \mathbf{V}_q^r\langle c\rangle \mathbf{f}_\pi^r) &= w^A_{q,n}(\mathbf{V}_q^r\langle b\rangle \mathbf{f}_\pi^r) + w^A_{q,n}(\mathbf{V}_q^r\langle c\rangle \mathbf{f}_\pi^r)\\ w^A_{q,n}([a]\mathbf{V}_q^r\langle b\rangle \mathbf{f}_\pi^r) &= a w^A_{q,n}(\mathbf{V}_q^r\langle b\rangle \mathbf{f}_\pi^r)\\ w^A_{q,n}((\mathbf{V}_q^r\langle b\rangle \mathbf{f}_\pi^r)(\mathbf{V}_\pi^m\langle c\rangle \mathbf{f}_\pi^m)) &= w^A_{q,n}(\mathbf{V}_q^r\langle b\rangle \mathbf{f}_\pi^r) w^A_{q,n}(\mathbf{V}_q^m\langle c\rangle \mathbf{f}_\pi^m)\end{aligned} \tag{29.6.5}$$

for all $n, m, r \in \mathbf{N} \cup \{0\}$. This will then prove the proposition. To prove relations (29.6.5) first observe that for all $x \in R(B)$,

$$w^A_{q,n}(\mathbf{V}^r_q x \mathbf{f}^r_\pi) = \begin{cases} 0 & \text{if } n < r \\ \pi^r w_{q,n-r}(x) & \text{if } r \le n \end{cases} \tag{29.6.6}$$

Thus for the first formula of (29.6.5) we can take $r = 0$. Then we have

$$\begin{aligned} w^A_{q,n}(\langle b\rangle + \langle c\rangle) &= w^A_{q,n}\left(\sum_{i=0}^{\infty} \mathbf{V}^i_q \langle r^A_i(b, c)\rangle \mathbf{f}^i_\pi\right) \\ &= \sum_{i=0}^{n} \pi^i (r^A_i(b, c))^{q^{n-i}} = b^{q^n} + c^{q^n} \\ &= w^A_{q,n}(\langle b\rangle) + w^A_{q,n}(\langle c\rangle) \end{aligned}$$

By the definition of the polynomials $r^A_i(Z_1, Z_2)$; cf. (29.3.8). Because $[a]$ commutes with $\mathbf{V}^r_q$, we can also take $r = 0$ in the second formula of (29.6.5). Then we have

$$\begin{aligned} w^A_{q,n}([a]\langle b\rangle) &= w^A_{q,n} \sum_{i=0}^{\infty} \mathbf{V}^i_q \langle \Omega^A_i(a)\rangle \mathbf{f}^i_\pi \langle b\rangle \\ &= w^A_{q,n}\left(\sum_{i=0}^{\infty} \mathbf{V}^i_q \langle \Omega^A_i(a) b^{q^i}\rangle \mathbf{f}^i_\pi\right) = \sum_{i=0}^{n} \pi^i (\Omega^A_i(a) b^{q^i})^{q^{n-i}} \\ &= \left(\sum_{i=0}^{n} \pi^i (\Omega_i(a)^{q^{n-i}}) b^{q^n}\right) = a b^{q^n} = a w^A_{q,n}(\langle b\rangle) \end{aligned}$$

by (29.3.18). Finally, re the third formula of (29.6.5) we have if $r \le m$,

$$(\mathbf{V}^r_q \langle b\rangle \mathbf{f}^r_\pi)(\mathbf{V}^m_q \langle c\rangle \mathbf{f}^m_\pi) = [\pi]^r \mathbf{V}^r_q \langle b\rangle \mathbf{V}^{m-r}_q \langle c\rangle \mathbf{f}^m_\pi = [\pi]^r \mathbf{V}^m_q \langle b^{q^{m-r}} c\rangle \mathbf{f}^m_\pi$$

so using (29.6.6) again, we find, using the second formula of (29.6.5),

$$\begin{aligned} w^A_{q,n}(\mathbf{V}^r_q \langle b\rangle \mathbf{f}^r_\pi \mathbf{V}^m_q \langle c\rangle \mathbf{f}^m_\pi) &= w^A_{q,n}([\pi]^r \mathbf{V}^m_q \langle b^{q^{m-r}} c\rangle \mathbf{f}^m_\pi) \\ &= \pi^r w^A_{q,n}(\mathbf{V}^m_q \langle b^{q^{m-r}} c\rangle \mathbf{f}^m_\pi) \\ &= \begin{cases} 0 & \text{if } n < m \\ \pi^{r+m} b^{q^{n-r}} c^{q^{n-m}} & \text{if } n \ge m \end{cases} \end{aligned}$$

and on the other hand (still assuming $r \le m$)

$$w^A_{q,n}(\mathbf{V}^r_q \langle b\rangle \mathbf{f}^r_\pi) w^A_{q,n}(\mathbf{V}^m_q \langle c\rangle \mathbf{f}^m_\pi) = \begin{cases} 0 & \text{if } n < m \\ (\pi^r b^{q^{n-r}})(\pi^m c^{q^{n-m}}) & \text{if } n \ge m \end{cases}$$

The case $m \le r$ is treated similarly. This proves (29.6.5) and hence the proposition.

■ (29.6.7) Now let us see what $\mathbf{f}_\pi$ and $\mathbf{V}_q$ do to elements of $W^A_{q,\infty}(B) \subset \mathrm{Cart}_A(B)$. We have

$$\mathbf{f}_\pi\left(\sum_{i=0}^{\infty} \mathbf{V}_q^i\langle b_i\rangle \mathbf{f}_\pi^i\right) = \langle b_0^q\rangle \mathbf{f}_\pi + [\pi]\sum_{i=1}^{\infty} \mathbf{V}_q^{i-1}\langle b_i\rangle \mathbf{f}_\pi^i$$

$$= \left(\langle b_0^q\rangle + [\pi]\sum_{i=1}^{\infty} \mathbf{V}_q^{i-1}\langle b_i\rangle \mathbf{f}_\pi^{i-1}\right)\mathbf{f}_\pi$$

$$= y\mathbf{f}_\pi$$

for some $y \in W^A_{q,\infty}(B)$. We claim that $y = \tau^A(x)$. To prove this we calculate

$$w^A_{q,n}(y) = w^A_{q,n}\left(\langle b_0^q\rangle + [\pi]\sum_{i=1}^{\infty} \mathbf{V}_q^{i-1}\langle b_i\rangle \mathbf{f}_\pi^{i-1}\right)$$

$$= b_0^{q^{n+1}} + \pi w^A_{q,n}(b_1, b_2, b_3, \ldots)$$

$$= b_0^{q^{n+1}} + \pi b_1^{q^n} + \cdots + \pi\pi^n b_{n+1}$$

$$= w^A_{q,n+1}\left(\sum_{i=0}^{\infty} \mathbf{V}_q^i\langle b_i\rangle \mathbf{f}_\pi^i\right) = w^A_{q,n+1}(x)$$

which proves that $x\mathbf{f}_\pi = \mathbf{f}_\pi\tau^A(x)$ for all $x \in W^A_{q,\infty}(B) \subset \mathrm{Cart}_A(B)$ for A-torsion free A-algebras B and hence by functoriality for all $B \in \mathbf{Alg}_A$.

Similarly, one finds that $\mathbf{V}_q x = \tau^A(x)\mathbf{V}_q$. Putting all this together we find the following description of $\mathrm{Cart}_A(B)$ as an overring of $W^A_{q,\infty}(B)$.

■ (29.6.8) **Proposition** $\mathrm{Cart}_A(B)$ is the A-algebra of all expressions

$$x_0 + \sum_{i=1}^{\infty} \mathbf{V}_q^i x_i + \sum_{i=1}^{\infty} y_i \mathbf{f}_\pi^i$$

with coefficients in the A-algebra $W^A_{q,\infty}(B)$ with the condition that $\lim_{i\to\infty} y_i = 0$. The calculation rules are

$$x\mathbf{V}_q = \mathbf{V}_q\tau^A(x), \qquad \mathbf{f}_\pi x = \tau^A(x)\mathbf{f}_\pi,$$

$$\mathbf{f}_\pi\mathbf{V}_q = [\pi] \in W^A_{q,\infty}(B), \qquad \mathbf{V}_q\mathbf{f}_\pi = (0, 1, 0, \ldots) \in W^A_{q,\infty}(B)$$

■ (29.6.9) Now suppose that k' is a perfect algebraic extension of k, the residue field of A and let A' be the (completed if necessary) unramified extension of A with residue field k'. Then we know that $W^A_{q,\infty}(k') = A'$, and that under this isomorphism τ^A goes to the Frobenius substitution in $\mathrm{Gal}(K'/K)$ (Theorem (25.3.30) and Remark (25.6.16)). Moreover, in this case we have that $(0, 1, 0, 0, \ldots)$ corresponds to $\pi \in A'$ (and $[a]$ corresponds to a). Also τ^A is an automorphism, so we can write $\mathbf{f}_\pi$ and $\mathbf{V}_q$ on the left or on the right as we please.

More generally, if k' is a perfect (algebraic or not) field extension of k, then

we have that $W^A_{q,\infty}(k')$ is a discrete valuation ring with uniformizing element π and, since k' is of characteristic p, we have

$$\pi = \mathbf{f}_\pi \mathbf{V}_q(1, 0, 0, 0, \ldots) = \mathbf{f}_\pi(0, 1, 0, 0, \ldots) = (0, 1, 0, 0, \ldots) = \mathbf{V}_q \mathbf{f}_\pi(1, 0, 0, \ldots)$$

(cf. Proposition (25.6.14)).

■ (29.6.10) **The Dieudonné algebras $\mathbf{D}^A(k')$ and $\mathbf{D}^A_{\mathbf{V}}(k')$** For any perfect extension k' of k we now define the Dieudonné algebra $\mathbf{D}^A(k')$ as the sub-A-algebra of $\mathrm{Cart}_A(k')$ consisting of all expressions

$$x_0 + \sum_{i=0}^{\infty} \mathbf{V}_q^i x_i + \sum^{<\infty} y_i \mathbf{f}_\pi^i$$

with x_i, $y_i \in W^A_{q,\infty}(k')$. The calculation rules are $\mathbf{f}_\pi x = \tau^A(x)\mathbf{f}_\pi$ ($\tau^A(x) \equiv x^q \bmod \pi$) and $x\mathbf{V}_q = \mathbf{V}_q \tau^A(x)$ and $\mathbf{f}_\pi \mathbf{V}_q = \pi = \mathbf{V}_q \mathbf{f}_\pi$. The only difference between $\mathrm{Cart}_A(k')$ and $\mathbf{D}^A(k')$ is that in the latter we allow only finite sums $\sum y_i \mathbf{f}_\pi^i$ instead of infinite sums $\sum y_i \mathbf{f}_\pi^i$ with $\lim_{i\to\infty} y_i = 0$. Because $\mathscr{C}_q(F; k')$ is complete for formal A-modules $F(X, Y)$, there is a one–one correspondence between reduced $\mathbf{D}^A(k')$ modules and reduced $\mathrm{Cart}_A(k')$ modules.

We define the localized Dieudonné algebras $\mathbf{D}^A_{\mathbf{V}}(k')$ as the A-algebras of all expressions $\sum_{i=n}^{\infty} \mathbf{V}_q^i x_i$, $x_i \in W^A_{q,\infty}(k')$, $n \in \mathbf{Z}$, with the calculation rule $x\mathbf{V}_q = \mathbf{V}_q \tau^A(x)$.

Note that if k' is algebraically closed, then $\mathbf{D}^A_{\mathbf{V}}(k')$ is a ring $\mathscr{E}$ of the type discussed in (28.4.1) for which we can classify all finitely generated torsion modules.

29.7 A-Height of formal A-modules

■ (29.7.1) **Definition** Let k' be a perfect extension field of k and $F(X, Y)$ a finite dimensional formal A-module over k'. Then we define the A-height of $F(X, Y)$ as the dimension of $\mathscr{C}_q(F; k')/[\pi]\mathscr{C}_q(F; k')$ over k'. (Note that the operators $\langle b\rangle$, $b \in k'$, turn $\mathscr{C}_q(F; k')/[\pi]\mathscr{C}_q(F; k')$ into a vector space over k'.) If k' is not perfect, consider $F(X, Y)$ as a formal A-module over some perfect extension field l of k'; we define the A-height of $F(X, Y)$ as the height of $F(X, Y)$ over l.

■ (29.7.2) **Comparison with the definition of Chapter IV** In case A is the ring of integers of some finite extension K of $\mathbf{Q}_p$ of degree n we have also defined the height of a formal A-module over k' as

$$A\text{-ht}(F(X, Y)) = n^{-1} \operatorname{ht}(F(X, Y)) \tag{29.7.3}$$

The two definitions agree in this case. Indeed, we know that

$$\operatorname{ht}(F(X, Y)) = \dim_{k'}(\mathscr{C}_p(F; k')/[p]\mathscr{C}_p(F; k'))$$

Now every element $\gamma(t)$ of $\mathscr{C}_p(F; k')$ can be written uniquely as a sum $\gamma(t) =$

$\sum_{i=0}^{r-1} V_p^i \gamma_i(t)$ with $\gamma_i(t) \in \mathscr{C}_q(F; k')$, i.e., $\mathscr{C}_q(F; k')$ has index r in $\mathscr{C}_p(F; k')$ where r is such that $q = p^r$.

Because $p = u\pi^e$ for some unit $u \in A$, we have that $[p]$ is injective if and only if $[\pi]$ is injective.

Using this we see that

$$\begin{aligned}\dim_{k'}(\mathscr{C}_p(F; k')/[p]\mathscr{C}_p(F; k')) &= r \dim_{k'}(\mathscr{C}_q(F; k')/[p]\mathscr{C}_q(F; k')) \\ &= re \dim_{k'}(\mathscr{C}_q(F; k')/[\pi]\mathscr{C}_q(F; k'))\end{aligned}$$

so that indeed height $= n \times (A\text{-height})$.

Of course if A is of characteristic p, then $[p] = 0$ and only Definition (29.7.1) makes sense.

(29.7.4) **A-height and dimension** Suppose that $F(X, Y)$ is of finite A-height h. Then $\mathbf{f}_\pi$ is injective and we find

$$\begin{aligned}h = A\text{-ht}(F(X, Y)) &= \dim_{k'}(\mathscr{C}_q(F; k')/[\pi]\mathscr{C}_q(F; k')) \\ &= \dim_{k'}(\mathscr{C}_q(F; k')/\mathbf{V}_q\mathscr{C}_q(F; k')) + \dim_{k'}(\mathbf{V}_q\mathscr{C}_q(F; k')/[\pi]\mathscr{C}_q(F; k')) \\ &= m + \dim_{k'}(\mathscr{C}_q(F; k')/\mathbf{f}_\pi\mathscr{C}_q(F; k')) = m + m'\end{aligned}$$

where $m = \dim(F(X, Y))$. In particular, we see that always

$$A\text{-ht}(F(X, Y)) \geq \dim(F(X, Y))$$

so that the only formal A-modules of A-height 1 are one dimensional.

■ (29.7.5) Let $F(X, Y)$ be a formal A-module of finite A-height over a perfect field k'. Then $\mathscr{C}_q(F; k')$ is a module over the discrete valuation ring $W_{q,\infty}^A(k')$ and $\mathscr{C}_q(F; k')/[\pi]\mathscr{C}_q(F; k')$ is free of finite rank over $k' = W_{q,\infty}^A(k')/\pi W_{q,\infty}^A(k')$. Thus we see that $\mathscr{C}_q(F; k')$ is a free $W_{q,\infty}^A(k')$-module of finite rank $h = A\text{-ht}(F(X, Y))$ (just as in the case of formal group laws in (28.3.10)).

29.8 Classification up to isogeny of formal A-modules over an algebraically closed field of characteristic $p > 0$

■ (29.8.1) **Isogenies** An isogeny between formal A-modules is a formal A-module homomorphism that as a homomorphism of formal group laws is an isogeny. Two formal A-modules are said to be isogenous if they can be connected to each other by a chain of isogenies (going in either direction). One shows as in Proposition (28.3.8) that two formal A-modules are isogenous if and only if their $\mathbf{D}_{\mathbf{V}}^A(k')$-modules

$$\mathbf{D}_{\mathbf{V}}^A(k') \otimes_{\mathbf{D}^A(k')} \mathscr{C}_q(F; k'), \qquad \mathbf{D}_{\mathbf{V}}^A(k') \otimes_{\mathbf{D}^A(k')} \mathscr{C}_q(G; k')$$

are isomorphic.

■ (29.8.2) **Construction of some formal A-modules** Let $F_V^A(X, Y)$ be the universal A-typical formal A-module of dimension $n \geq 1$. Substituting

$$V_1 = \begin{pmatrix} 0 & \cdots & & & 0 \\ 1 & \ddots & & & \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & & & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \qquad V_2 = \cdots = V_m = 0$$

$$V_{m+1} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & & 0 & 0 \\ & & & \vdots \\ 0 & \cdots & & 0 \end{pmatrix}, \qquad V_{m+2} = V_{m+3} = \cdots = 0$$

with $m \geq 1$, and $(n, m) = 1$ (and $V_1 = 0$ if $n = 1$) we obtain a formal A-module over A, which when considered as a formal A-module over k' has $\mathbf{D}^A(k')$-module isomorphic to

$$\mathbf{D}^A(k')/\mathbf{D}^A(k')(\mathbf{f}_\pi^n - \mathbf{V}_q^m)$$

We shall denote this formal A-module with $G_{n.m}^A(X, Y)$. This formal A-module is of dimension n and A-height $m + n$.

Now let $n = 1$ and substitute $V_1 = 1$, $V_2 = V_3 = \cdots = 0$; the result is the one dimensional formal A-module $G_\pi(X, Y)$ of A-height 1 that as a formal A-module over k' has $\mathbf{D}^A(k')$-module

$$\mathbf{D}^A(k')/\mathbf{D}^A(k')(\mathbf{f}_\pi - 1)$$

We shall now also use $G_{1,0}^A(X, Y)$ to denote this formal A-module.

Finally, let $n \geq 1$ and substitute

$$V_1 = \begin{pmatrix} 0 & \cdots & & & 0 \\ 1 & \ddots & & & \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & & & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

$$V_2 = V_3 = \cdots = 0 \quad (\text{if } n = 1, \text{ then also } V_1 = 0)$$

The result is a formal A-module of dimension n and infinite A-height; it is in fact the quotient $\hat{W}_{q,n}^A(X, Y)$ of $\hat{W}_{q,\infty}^A(X, Y)$ obtained by considering only the first n addition polynomials $\Sigma_0^A, \ldots, \Sigma_{n-1}^A$. Its $\mathbf{D}^A(k')$-module is

$$\mathbf{D}^A(k')/\mathbf{D}^A(k')\mathbf{f}_\pi^n$$

We shall also use $G_{n,\infty}^A(X; Y)$ as a notation for this formal A-module. If $n = 1$, we obtain the one dimensional additive formal A-module.

All this is proved exactly as the corresponding facts for $\mathbf{Z}_p$-modules in (28.5.3); cf. also (29.5.3).

One now reasons exactly as in Section 28.5 to obtain the following classification theorem for formal A-modules.

■ (29.8.3) **Theorem** Let k' be an algebraically closed extension field of k the (finite) residue field of the discrete valuation ring A. Then every finite dimensional formal A-module over k' is isogenous to a direct sum of the formal A-modules

$$G^A_{n,m}(X, Y), \qquad 1 \leq n < \infty, \quad 0 \leq m \leq \infty, \quad (n, m) = 1$$

This decomposition is unique up to isogeny (of formal A-modules). The formal A-modules $G^A_{n,m}(X, Y)$ with $n, m \in \mathbf{N}$ and $(n, m) = 1$ are simple (as formal A-modules), and the $G^A_{n,\infty}(X, Y)$ are indecomposable.

■ (29.8.4) **Remarks**

(i) Theorem (29.8.3) holds also for A of characteristic $p > 0$; in that case the underlying formal group laws are all additive.

(ii) If $(n, m) = 1$, $n, m \in \mathbf{N}$, then $G^A_{n,m}(X, Y)$ is simple as a formal A-module; but even when A is of characteristic zero, it may be decomposable as a formal group law. For instance, if $n = 2$ and $[K : \mathbf{Q}_p] = 2$, then as a formal group law $G^A_{2,1}(X, Y)$ decomposes up to isogeny into two copies of $G_{1,2}(X; Y)$.

30 "Le Tapis de Cartier" for Formal A-Modules, or Lifting Formal Group Laws and Formal A-Modules Revisited

Let A be a discrete valuation ring with uniformizing element π and finite residue field k of q elements. The quotient field of A is denoted K. In this section we discuss a generalization for formal A-modules of what has become known as the "tapis de Cartier," the subject of Cartier's 1972 IHES seminar. One obtains the case of formal group laws by taking $A = \mathbf{Z}_{(p)}$ and $p = \pi = q$ everywhere below.

30.1 Generalized Lubin–Tate formal A-modules associated to a semilinear endomorphism

■ (30.1.1) **The formal A-module homomorphisms $\mathscr{F}$ and $\mathscr{V}$** Let $\Gamma(X, Y)$ be a formal A-module over a field l (i.e., l is an extension field of k). Let σ be the Frobenius k-endomorphism of l, i.e., $\sigma(x) = x^q$ for all $x \in l$. Applying σ to the coefficients of the power series $\Gamma(X, Y)$ and the power series $[a]_\Gamma(X) \in l[\![X]\!]$, $a \in A$, gives us a formal A-module which we shall denote $\sigma_*\Gamma(X, Y)$. (Note that indeed $J(\sigma_*[a]_\Gamma(X)) =$ (image of a in l) because $a^q \equiv a \bmod \pi$; note also that applying $\tau: x \mapsto x^p$ to $\Gamma(X, Y)$ and the $[a]_\Gamma(X)$ does as a rule not define a formal A-module, but only a twisted formal A-module in the sense of Chapter IV, Section 25.10.)

The power series X^q now defines a homomorphism of formal A-modules

$$\mathscr{F}(X)\colon \Gamma(X, Y) \to \sigma_*\Gamma(X, Y) \tag{30.1.2}$$

because $\Gamma(X, Y)^q = \sigma_*\Gamma(X^q, Y^q)$ and $([a](X))^q = \sigma_*[a](X^q)$ for all $a \in A$. The endomorphism $[\pi]_\Gamma(X)$ of $\Gamma(X, Y)$ is necessarily a power series in X^q (cf. the definition of A-height in Chapter IV, Section 21.8 for the one dimensional case; for the higher dimensional case, cf. Lemma (30.1.31) below).

Let $\mathscr{V}(X)$ be the power series such that

$$\mathscr{V}(X^q) = [\pi]_\Gamma(X) \tag{30.1.3}$$

Then we claim $\mathscr{V}(X)$ is a homomorphism of formal A-modules:

$$\mathscr{V}(X)\colon \sigma_*\Gamma(X, Y) \to \Gamma(X, Y) \tag{30.1.4}$$

Indeed, we have

$$\begin{aligned}\mathscr{V}(\sigma_*\Gamma(X^q, Y^q)) &= \mathscr{V}((\Gamma(X, Y))^q) = \mathscr{V}\mathscr{F}(\Gamma(X, Y))\\ &= [\pi]_\Gamma(\Gamma(X, Y)) = \Gamma([\pi]_\Gamma(X), [\pi]_\Gamma(Y))\\ &= \Gamma(\mathscr{V}(X^q), \mathscr{V}(Y^q))\end{aligned}$$

so that indeed $\mathscr{V}(\sigma_*\Gamma(X, Y)) = \Gamma(\mathscr{V}(X), \mathscr{V}(Y))$. Similarly, one shows that $\mathscr{V}(\sigma_*[a]_\Gamma(X)) = [a]_\Gamma(\mathscr{V}(X))$. This also proves that

$$[\Gamma(X, Y) \xrightarrow{\mathscr{F}} \sigma_*\Gamma(X, Y) \xrightarrow{\mathscr{V}} \Gamma(X, Y)] = \Gamma(X, Y) \xrightarrow{[\pi]_\Gamma} \Gamma(X, Y) \tag{30.1.5}$$

and similarly one has

$$[\sigma_*\Gamma(X, Y) \xrightarrow{\mathscr{V}} \Gamma(X, Y) \xrightarrow{\mathscr{F}} \sigma_*\Gamma(X, Y)] = \sigma_*\Gamma(X, Y) \xrightarrow{[\pi]_{\sigma_*\Gamma}} \sigma_*\Gamma(X, Y) \tag{30.1.6}$$

because $\mathscr{F}(\mathscr{V}(X^q)) = \mathscr{F}([\pi]_\Gamma(X)) = ([\pi]_\Gamma(X))^q = \sigma_*[\pi]_\Gamma(X^q) = [\pi]_{\sigma_*\Gamma}(X^q)$.

More properly, we should write $\mathscr{F}_\Gamma$ and $\mathscr{V}_\Gamma$ (especially $\mathscr{V}_\Gamma$) instead of $\mathscr{F}$ and $\mathscr{V}$; in case of possible confusion, we shall do so. Slightly more generally, one has of course Frobenius homomorphisms $\mathscr{F}(X)\colon \sigma_*^n\Gamma(X, Y) \to \sigma_*^{n+1}\Gamma(X, Y)$ and Verschiebung homomorphisms $\mathscr{V}(X)\colon \sigma_*^{n+1}\Gamma(X, Y) \to \sigma_*^n\Gamma(X, Y)$ for all $n \in \mathbf{N} \cup \{0\}$.

■ (30.1.7) **Construction of certain generalized Lubin–Tate formal A-modules; the setting** Let B be an A-torsion free local A-algebra with maximal ideal πB that admits an A-algebra endomorphism $\sigma\colon B \to B$ such that $\sigma(b) \equiv b^q \bmod \pi B$ for all $b \in B$. Let M be a free B-module of finite rank together with a σ-semilinear endomorphism $\eta\colon M \to M$; i.e., η is additive and $\eta(bm) = \sigma(b)\eta(m)$ for all $b \in B$ and $m \in M$. Note that η is an A-module homomorphism.

The most important example for us will be $B = W_{q,\infty}^A(l)$ where l is a perfect field extension of k; σ the Frobenius endomorphism of B induced by $\mathbf{f}_\pi$:

$W^A_{q,\infty}(-) \to W^A_{q,\infty}(-)$; and M the Cartier–Dieudonné module of q-typical curves $\mathscr{C}_q(\Gamma; l)$ of some formal A-module $\Gamma(X, Y)$ over l, which is of finite A-height. The assumptions made above all hold by Chapter IV, Propositions (25.6.8), (25.6.14); cf. also (28.3.10), (29.6.10), and (29.7.5).

■ (30.1.8) **Construction of certain generalized Lubin–Tate formal A-modules** Let B, σ, M, η be as in (30.1.7). Choose a basis $e_1, \ldots, e_h$ of M over B and let $D = D(\eta)$ be the matrix of η with respect to the basis $e_1, \ldots, e_h$, i.e.,

$$\eta e_i = \sum_{j=1}^{h} d_{ji} e_j, \qquad i = 1, \ldots, h \tag{30.1.9}$$

Let $g(M, \eta)(X)$ be the h-tuple of power series in $X = (X_1, \ldots, X_h)$ defined by the functional equation

$$g(M, \eta)(X) = X + \pi^{-1} D(\eta) \sigma_* g(M, \eta)(X^q) \tag{30.1.10}$$

and define $G(M, \eta)(X, Y)$ and $[a](X)$ for all $a \in A$ by

$$G(M, \eta)(X, Y) = g(M, \eta)^{-1}(g(M, \eta)(X) + g(M, \eta)(Y)) \tag{30.1.11}$$

$$\begin{aligned} \rho(M, \eta)(a)(X) &= [a](X) \\ &= g(M, \eta)^{-1}(a g(M, \eta)(X)) \quad \text{for all } a \in A \end{aligned} \tag{30.1.12}$$

By the functional equation lemma (30.1.10)–(30.1.12) define a formal A-module $(G(M, \eta)(X, Y), \rho(M, \eta))$ with A-logarithm $g(M, \eta)(X)$. (We shall generally use G and g to denote formal A-modules and their A-logarithms in all of Section 30 so as to not overwork the letter F.)

■ (30.1.13) **Functorial properties of the construction** Let B, σ, M, η be as in (30.1.7). Let $\hat{M}$, $\hat{\eta}$ be a second free B-module of finite rank h' with a σ-semilinear endomorphism $\hat{\eta}: \hat{M} \to \hat{M}$ and let $\mu: M \to \hat{M}$ be a homomorphism of B-modules such that $\mu\eta = \hat{\eta}\mu$. Choose a basis $\hat{e}_1, \ldots, \hat{e}_{h'}$ of $\hat{M}$ and let E be the matrix of μ with respect to the bases $e_1, \ldots, e_h$ of M and $\hat{e}_1, \ldots, \hat{e}_{h'}$ of $\hat{M}$. Define

$$\alpha_\mu(X) = g(\hat{M}, \hat{\eta})^{-1}(E g(M, \eta)(X)) \tag{30.1.14}$$

then, again by the functional equation lemma, $\alpha_\mu(X)$ has its coefficients in B and hence is a formal A-module homomorphism $G(M, \eta)(X, Y) \to G(\hat{M}, \hat{\eta})(X, Y)$.

In particular, it follows that $G(M, \eta)(X, Y)$ does not depend (up to isomorphism) on the choice of the basis $e_1, \ldots, e_h$, thus justifying (to some extent) the notation $G(M, \eta)(X, Y)$. We should of course write something like $G(M, \eta, e_1, \ldots, e_h)(X, Y)$ instead because the *power series* $G(M, \eta)(X, Y)$ and $\rho(M, \eta)(\alpha)(X)$ *do* depend on the choice of $\{e_1, \ldots, e_h\}$.

■ (30.1.15) **The q-typical curves in $G(M, \eta)(X, Y)$** Let B, σ, η, M be as in (30.1.7). Let $\gamma(t) \in \mathscr{C}_q(G(M, \eta); B)$; let

$$g(M, \eta)(\gamma(t)) = \sum_{i=0}^{\infty} y_i t^{q^i}, \qquad y_i \in (B \otimes_A K)^n \tag{30.1.16a}$$

Then by the functional equation lemma the y_i satisfy $y_i \equiv \pi^{-1} D(\eta)\sigma_*(y_{i-1})$ mod B^n for all $i = 1, 2, \ldots$; $y_0 \in B^n$. And conversely, if the y_i satisfy these congruences, then $g(M, \eta)^{-1}(\sum y_i t^{q^i})$ has integral coefficients and hence is in $\mathscr{C}(G(M, \eta); B)$.

Identifying M with B^n via the basis $e_1, \ldots, e_h$ and $M \otimes_A K$ with $(B \otimes_A K)^n$ via the same basis, we find that

$$\gamma(t) \in \mathscr{C}_q(G(M, \eta); B) \quad \Leftrightarrow \quad g(M, \eta)(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i}$$

with $x_i \in M \otimes_A K$ such that

$$x_i \equiv \pi^{-1}\eta(x_{i-1}) \mod M \qquad \text{for all} \quad i \in \mathbf{N} \tag{30.1.16b}$$
$$x_0 \in M$$

This description is independent of the choice of the basis $\{e_1, \ldots, e_h\}$ of M.

■ (30.1.17) **A canonical map $\beta_0 : M \to \mathscr{C}_q(G(M, \eta); B)$** Let B, σ, M, η be as in (30.1.7). For each $x \in M$, we define a curve $\beta_0(x) = \gamma_x(t)$ by the formula

$$g(M, \eta)(\beta_0(x)) = g(M, \eta)(\gamma_x(t)) = \sum_{i=0}^{\infty} \pi^{-i}\eta^i(x)t^{q^i} \tag{30.1.18}$$

This does indeed define a curve in $\mathscr{C}_q(G(M, \eta); B)$ by (30.1.16b). We note that β_0 is additive and A-linear. Further, since $\mathbf{f}_\pi$ is characterized by

$$g(M, \eta)(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i} \quad \Rightarrow \quad g(M, \eta)(\mathbf{f}_\pi \gamma(t)) = \sum_{i=0}^{\infty} \pi x_{i+1} t^{q^i}$$

we see that

$$\mathbf{f}_\pi \gamma_x(t) = \gamma_{\eta(x)}(t) \tag{30.1.19}$$

i.e., β_0 takes η into the Frobenius operator on $\mathscr{C}_q(G(M, \eta); B)$.

An immediate corollary of (30.1.16b) is now

■ (30.1.20) **Corollary** Every $\gamma(t) \in \mathscr{C}_q(G(M, \eta); B)$ can be uniquely written as a convergent sum

$$\gamma(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \gamma_{x_i}(t), \qquad x_i \in M \tag{30.1.21}$$

■ (30.1.22) **"Recovering" (M, η)** Let B, σ, η, M be as in (30.1.7) and suppose in addition that σ is an automorphism of B. (This will be the case in the important example that we briefly discussed in (30.1.7).) Let M^σ be the free B-module of rank h over B obtained from M by modifying the B-module

structure by setting $b * m = \sigma^{-1}(b)m$. Then $\eta = \eta^\sigma$: $M^\sigma \to M^\sigma$ is still a σ-semilinear map and η: $M^\sigma \to M$ is a B-linear map. Choose the same basis $e_1, \ldots, e_h$ for M^σ as for M and let $D^\sigma = D(\eta^\sigma)$ be the matrix of $\eta = \eta^\sigma$: $M^\sigma \to M^\sigma$, then we claim $D^\sigma = \sigma_* D(\eta)$. Indeed, if $D^\sigma = (d_{ij}^\sigma)$, then

$$\eta e_i = \sum_{j=1}^{\infty} (d_{ij}^\sigma) * e_j = \sum_{j=1}^{n} \sigma^{-1}(d_{ji}^\sigma) e_j$$

But $\eta e_i = \sum d_{ji} e_j$, so that indeed $d_{ij}^\sigma = \sigma(d_{ij})$. It follows that

$$G(M^\sigma, \eta)(X, Y) = \sigma_* G(M, \eta)(X, Y) \tag{30.1.23}$$

We have just seen that η: $M^\sigma \to M$ is a B-module homomorphism. Moreover, we have of course $M^\sigma \xrightarrow{\eta} M \xrightarrow{\eta} M = M^\sigma \xrightarrow{\eta} M^\sigma \xrightarrow{\eta} M$, so that by (30.1.13) we have an induced homomorphism of formal A-modules

$$\mathfrak{v}(M, \eta)(X)\colon \sigma_* G(M, \eta)(X, Y) \to G(M, \eta)(X, Y) \tag{30.1.24}$$

Identifying $Lie(G(M, \eta))$ with $M = \mathscr{C}_q(G(M, \eta); B)/\mathscr{C}_q^{(1)}(G(M, \eta); B)$ (cf. (30.1.15)), we note that

$$Lie(\mathfrak{v}(M, \eta)) = \eta\colon M^\sigma \to M \tag{30.1.25}$$

(30.1.26) **Lemma** Let B, σ, η, M be as in (30.1.22). Then the reduction mod πB of $\mathfrak{v}(M, \eta)(X)$ is the Verschiebung homomorphism $\mathscr{V}(X)$: $\bar{G}(M^\sigma, \eta)(X, Y) \to \bar{G}(M, \eta)(X, Y)$.

Proof First note that $\bar{G}(M^\sigma, \eta) = \overline{\sigma_* G(M, \eta)} = \sigma_* \bar{G}(M, \eta)$ where we have used σ both to denote the given automorphism of B and the automorphism $x \mapsto x^q$ of $l = B/\pi B$ induced by σ.

Let $\Gamma(X, Y)$ be a formal A-module over l. Then applying σ_* to the coefficients of a $\gamma(t) \in \mathscr{C}_q(\Gamma(X, Y), l)$ induces a $\mathrm{Cart}_A(l)$-homomorphism $\mathscr{C}_q(\Gamma(X, Y), l) \to \mathscr{C}_q(\sigma_* \Gamma(X, Y), l)$, $\gamma(t) \mapsto \sigma_* \gamma(t)$; and since $\gamma(t)^q = \sigma_* \gamma(t^q)$, we find the following relation between σ_*, $\mathscr{F}_*$, and $\mathbf{V}_q$ (where $\mathscr{F}_*$: $\mathscr{C}_q(\Gamma(X, Y), l) \to \mathscr{C}_q(\sigma_* \Gamma(X, Y), l)$ is the curve morphism induced by the homomorphism $\mathscr{F}(X)$):

$$\mathscr{F}_* = \mathbf{V}_q^{\sigma_* \Gamma} \sigma_* = \sigma_* \mathbf{V}_q^{\Gamma}\colon \mathscr{C}_q(\Gamma; l) \to \mathscr{C}_q(\sigma_* \Gamma; l) \tag{30.1.27}$$

We claim that similarly

$$\mathscr{V}_* = \mathbf{f}_\pi^\Gamma \sigma_*^{-1} = \sigma_*^{-1} \mathbf{f}_\pi^{\sigma_* \Gamma}\colon \mathscr{C}_q(\sigma_* \Gamma; l) \to \mathscr{C}_q(\Gamma; l) \tag{30.1.28}$$

To prove (30.1.28) note that

$$\mathscr{F}_* \mathscr{V}_* = [\pi]_{\sigma_* \Gamma} = \mathbf{V}_q^{\sigma_* \Gamma} \mathbf{f}_\pi^{\sigma_* \Gamma} = \mathbf{V}_q^{\sigma_* \Gamma} \sigma_* \sigma_*^{-1} \mathbf{f}_\pi^{\sigma_* \Gamma} = \mathscr{F}_* \sigma_*^{-1} \mathbf{f}_\pi^{\sigma_* \Gamma}$$

and (30.1.28) follows because $\mathscr{F}_*$ is injective.

Now let $x \in M$ and let $\gamma_x(t) \in \mathscr{C}_q(G(M, \eta), B)$ be the curve $\beta_0(x)$. The A-algebra homomorphism σ: $B \to B$ induces a $\mathrm{Cart}_A(B)$-homomorphism

$$\sigma_*\colon \mathscr{C}_q(G(M, \eta); B) \to \mathscr{C}_q(\sigma_* G(M, \eta); B) = \mathscr{C}_q(G(M^\sigma, \eta); B)$$

and $\sigma_* \gamma_x(t) = \gamma_x^\sigma(t)$ where the upper σ on $\gamma_x^\sigma(t)$ means that we now view x as an element of M^σ, i.e., $\gamma_x^\sigma(t) \in \mathscr{C}_q(G(M^\sigma, \eta); B)$ is the curve with

$$g(M^\sigma, \eta)(\gamma_x^\sigma(t)) = \sum \pi^{-i}\eta^i(x)t^{q^i}, \qquad \pi^{-i}\eta^i(x) \in M^\sigma \otimes_A K$$

(Here we have identified $(B \otimes_A K)^n$ with M on the left-hand side by means of a basis $e_1, \ldots, e_h$ and $(B \otimes_A K)^n$ with M^σ on the right-hand side by means of the same basis $e_1, \ldots, e_h$.) The curves homomorphism $\mathbf{v}_\bullet$ induced by $\mathrm{v}(M, \eta)(X)$ takes the curve $\gamma(t)$ with $g(M^\sigma, \eta)(\gamma(t)) = \sum x_i t^{q^i}$, $x_i \in M^\sigma \otimes_A K$ into the curve $\mathbf{v}_\bullet \gamma(t)$ with $g(M, \eta)(\mathbf{v}_\bullet \gamma(t)) = \sum \eta(x_i)t^{q^i}$, $\eta(x_i) \in M \otimes_A K$. It follows that if $x \in M$, then

$$\mathbf{v}_\bullet \sigma_* \gamma_x(t) = \gamma_{\eta(x)}(t), \qquad x \in M \tag{30.1.29}$$

Reducing mod πB and using (30.1.19) and (30.1.28) we find for all $y \in M^\sigma$

$$\begin{aligned}\mathbf{v}_\bullet \bar{\gamma}_y^\sigma(t) &= \mathbf{v}_\bullet \sigma_* \sigma_*^{-1} \bar{\gamma}_y^\sigma(t) = \mathbf{v}_\bullet \sigma_* \bar{\gamma}_y(t) = \bar{\gamma}_{\eta(y)}(t) \\ &= \mathbf{f}_\pi \bar{\gamma}_y(t) = \mathbf{f}_\pi \sigma_*^{-1} \sigma_* \bar{\gamma}_y(t) = \mathbf{f}_\pi \sigma_*^{-1} \bar{\gamma}_y^\sigma(t) = \mathscr{V}_\bullet \bar{\gamma}_y^\sigma(t)\end{aligned}$$

where bars over symbols denote reductions mod πB. Therefore $\mathbf{v}_\bullet$ and $\mathscr{V}_\bullet$ coincide on all curves of the form $\bar{\gamma}_y^\sigma(t)$. But both $\mathbf{v}_\bullet$ and $\mathscr{V}_\bullet$ are $\mathrm{Cart}(l)$-homomorphisms and hence commute with $\mathbf{V}_q$, so $\mathbf{v}_\bullet = \mathscr{V}_\bullet$ by Corollary (30.1.20), which in turn implies $\mathrm{v}(X) = \mathscr{V}(X)$ by the faithfulness theorem (29.4.1).

■ (30.1.30) **Summing up** Let B, σ, M, η as in (30.1.22) (i.e., σ is an automorphism). We have associated in a functorial way to (M, η) a formal A-module $G(M, \eta)(X, Y)$ together with a homomorphism of formal A-modules $\mathrm{v}(M, \eta)(X)$: $\sigma_* G(M, \eta)(X, Y) \to G(M, \eta)(X, Y)$ which modulo πB reduces to the Verschiebung homomorphism $\mathscr{V}(X)$: $\sigma_* G(M, \eta)(X, Y) \to G(M, \eta)(X, Y)$. The pair (M, η) is recoverable from $(G(M, \eta)(X, Y), \mathrm{v}(M, \eta)(X))$ as $M = Lie(G(M, \eta)(X, Y))$, $\eta = Lie(\mathrm{v}(M, \eta)(X))$.

We still have to prove that $[\pi]_\Gamma(X)$ is a power series in X^q also in the higher dimensional case. This follows from

■ (30.1.31) **Lemma** Let $F(X, Y)$ be an m-dimensional formal A-module over $B \in \mathbf{Alg}_A$. Then there is an m-tuple of power series $\beta(X)$ over B such that $[\pi]_F(X) \equiv \beta(X^q) \bmod \pi B$.

Proof It suffices to prove this in the case that $B = A[V]$ and $F(X, Y) = F_V^A(X, Y)$, the universal A-typical m-dimensional formal A-module. Suppose we have already found a power series $\beta(X)$ such that

$$\beta(X^q) \equiv [\pi](X) \mod(\pi A[V], \text{degree } n)$$

Write

$$\beta(X^q) \equiv [\pi](X) + \sum_{|\mathbf{n}| = n} a_{\mathbf{n}} X^{\mathbf{n}} \mod(\pi A[V], \text{degree } n+1)$$

where the $a_{\mathbf{n}}$ are certain m-vectors with coordinates in $A[V]$. By part (iv) of the functional equation lemma it follows that

$$f_V^A(\beta(X^q)) \equiv \pi f_V^A(X) + \sum_{|\mathbf{n}|=n} a_{\mathbf{n}} X^{\mathbf{n}} \mod(\pi A[V], \text{degree } n+1)$$

(where we have also used that $f_V^A(X) \equiv X$ mod(degree 2). Now both $f_V^A(\beta(X^q))$ and $\pi f_V^A(X)$ are power series in $X_1^q, \ldots, X_m^q$ modulo $\pi A[V]$. It follows that $a_{\mathbf{n}} \equiv 0 \bmod \pi A[V]$ for all $\mathbf{n}$ not of the form $\mathbf{n} = q\mathbf{d}$. With induction this completes the proof.

■ (30.1.32) **Remark** Note that this is virtually the same argument as we used in Remark (5.4.8) of Chapter I to establish formula (5.4.9). More generally one shows in this manner that $[\pi^n]_F(X)$ is of the form

$$(30.1.33)\quad [\pi^n]_F(X) = \pi^n \beta_0(X) + \pi^{n-1}\beta_1(X^q) + \cdots + \pi\beta_{n-1}(X^{q^{n-1}}) + \beta_n(X^{q^n})$$

with $\beta_i(X) \in B[[X]]$, $i = 0, \ldots, n$, and $\beta_0(X) = X$ mod(degree 2).

■ (30.1.34) **Remark** The same argument (essentially) shows that if $F(X, Y) = F_v(X, Y)$, $v_i \in B^{m\times m}$, is an A-typical formal A-module and r is the largest number in $\mathbf{N}$ such that $v_i \equiv 0 \bmod \pi B^{m\times m}$ for all $i < r$, then $[\pi]_F(X)$ is an m-tuple of power series in $X_1^{q^r}, \ldots, X_m^{q^r} \bmod \pi B$. Cf. also Section 21.8 in the one dimensional case.

30.2 Universality (adjointness) properties of Lubin–Tate formal A-modules

■ (30.2.1) **The equivalence of categories** Let B, σ be as in (30.1.22). Let $\mathbf{Mod}_\sigma(B)$ be the category of pairs (M, η) where M is a free B-module of finite rank and η: $M \to M$ is a σ-semilinear endomorphism of M (i.e., $\eta(bm) = \sigma(b)\eta(m)$ for all $b \in B$, $m \in M$). The morphisms of $\mathbf{Mod}_\sigma(B)$ are B-module homomorphisms μ: $M \to \hat{M}$ such that $\hat{\eta}\mu = \mu\eta$.

Let $\mathbf{FG}_{B,\sigma}^A$ be the category of pairs $(G(X, Y), \mathrm{v}(X))$ where $G(X, Y)$ is a finite dimensional formal A-module over B and $\mathrm{v}(X)$ is a homomorphism of formal A-modules $\mathrm{v}(X)$: $\sigma_* G(X, Y) \to G(X, Y)$ that reduces mod πB to the Verschiebung homomorphism $\mathcal{V}(X)$: $\sigma_* \bar{G}(X, Y) \to \bar{G}(X, Y)$ over l. The morphisms of $\mathbf{FG}_{B,\sigma}^A$ are formal A-module homomorphisms $\alpha(X)$: $G(X, Y) \to \hat{G}(X, Y)$ such that $\hat{\mathrm{v}}(X) \circ \alpha(X) = \alpha(X) \circ \mathrm{v}(X)$.

In Section 30.1 we have constructed a functor LT: $\mathbf{Mod}_\sigma(B) \to \mathbf{FG}_{B,\sigma}^A$, $(M, \eta) \mapsto (G(M, \eta)(X, Y), \mathrm{v}(M, \eta)(X))$, and we have also a functor in the inverse direction, Lie: $\mathbf{FG}_{B,\sigma}^A \to \mathbf{Mod}_\sigma(B)$. We have already seen that $Lie \circ LT = id$.

■ (30.2.2) **Theorem** The functors LT and Lie are (inverse) equivalences of categories.

Proof Since $Lie \circ LT = id$, we only have to show that if $(G(X, Y), \mathbf{v}(X)) \in \mathbf{FG}^A_{B,\sigma}$, then there exists a pair $(M, \eta) \in \mathbf{Mod}_\sigma(B)$ such that $(G(M, \eta)(X, Y), \mathbf{v}(M, \eta)(X))$ is isomorphic to the given pair $(G(X, Y), \mathbf{v}(X))$. Let $g(X)$ be the A-logarithm of $G(X, Y)$. Then the A-logarithm of $\sigma_* G(X, Y)$ is $\sigma_* g(X)$; and since B is A-torsion free, the formal A-module homomorphism $\mathbf{v}(X)$ is necessarily of the form

$$\mathbf{v}(X) = g^{-1}(D\sigma_* g(X)) \tag{30.2.3}$$

for some matrix D. Now we also know that $\mathbf{v}(X)$ reduces to $\mathscr{V}(X)$ mod πB. Now $\mathscr{V}(X^q) = \mathscr{V}(X) \circ \mathscr{F}(X) = [\pi]_G(X)$, which means that

$$\mathbf{v}(X^q) = g^{-1}(D\sigma_* g(X^q)) \equiv [\pi]_G(X) \mod \pi B \tag{30.2.4}$$

Now B admits an A-algebra endomorphism σ such that $\sigma(b) \equiv b^q$ mod πB, so by Proposition (21.8.6) of Chapter IV we can assume (up to isomorphism) that $G(X, Y)$ is a functional equation formal A-module. (The proof given there is for the one dimensional case; the higher dimensional case is proved in exactly the same way; cf. also Corollary (20.1.5).) By part (iv) of the functional equation lemma 10.2 we then have

$$D\sigma_* g(X^q) \equiv \pi g(X) \mod \pi B \tag{30.2.5}$$

and hence

$$g(X) - \pi^{-1} D\sigma_* g(X^q) \in B[\![X]\!] \tag{30.2.6}$$

which by the functional equation lemma means that $G(X, Y)$ is strictly isomorphic to the formal A-module with logarithm

$$\hat{g}(X) = X + \pi^{-1} D\sigma_* \hat{g}(X^q) \tag{30.2.7}$$

which is the logarithm associated to the B-module B^n with σ-semilinear endomorphism given by the matrix D; cf. (30.1.10) above. Transferring $\mathbf{v}(X)$ via this strict isomorphism gives us the homomorphism $\hat{\mathbf{v}}(X) = \hat{g}^{-1}(D\sigma_* \hat{g}(X))$, which is precisely the homomorphism induced by η: $(B^n)^\sigma \to B^n$. This proves the theorem.

■ (30.2.8) **Adjointness (universality) properties of the Lubin–Tate formal A-module construction** Let $H(X, Y)$ be a formal A-module over B and let $(M, \eta) \in \mathbf{Mod}_\sigma(B)$ and $\alpha(X)$: $G(M, \eta)(X, Y) \to H(X, Y)$ a homomorphism of formal A-modules. This induces a homomorphism of $\mathrm{Cart}_A(B)$-modules α_*: $\mathscr{C}_q(G(M, \eta); B) \to \mathscr{C}_q(H; B)$. In particular, α_* commutes with $\mathbf{f}_\pi$. Composiing α_* with β_0: $M \to \mathscr{C}_q(G(M, \eta); B)$, we therefore find a homomorphism $r(\alpha)$: $M \to \mathscr{C}_q(H(X, Y); B)$. Let Δ_B: $B \to W^A_{q,\infty}(B)$ be the unique A-algebra homomorphism such that $w_{q,n} \circ \Delta_B = \sigma^n$ for all $n \in \mathbf{N} \cup \{0\}$; cf. Chapter IV, Proposition (25.7.2). Via Δ_B we can view $\mathscr{C}_q(H(X, Y); B)$ as a B-module.

■(30.2.9) **Theorem** Let B, σ, M, η be as in (30.1.7). Then:

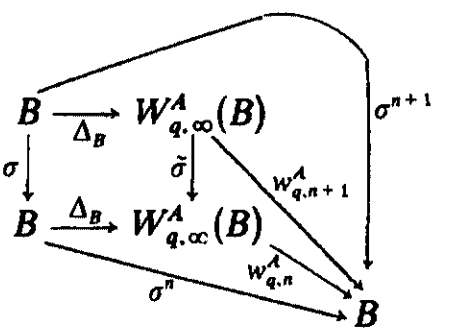
(i) $r(\alpha)$: $M \to \mathscr{C}_q(H(X, Y); B)$ is a homomorphism of B-modules.
(ii) $r(\alpha) \circ \eta = \mathbf{f}_\pi \circ r(\alpha)$.
(iii) $\alpha(X) \mapsto r(\alpha)$ is a bijection between the set of formal A-module homomorphisms $G(M, \eta)(X, Y) \to H(X, Y)$ and B-linear homomorphisms β: $M \to \mathscr{C}_q(H(X, Y); B)$ such that $\beta \circ \eta = \mathbf{f}_\pi \circ \beta$.

■(30.2.10) **Remarks**

(i) Let $\tilde{\sigma}$: $W^A_{q,\infty}(B) \to W^A_{q,\infty}(B)$ be the Frobenius endomorphism (cf. Chapter IV, Section 25.6 where we used $\mathbf{f}_\pi$ to denote $\tilde{\sigma}$). Then we claim

$$\tilde{\sigma} \circ \Delta_B = \Delta_B \circ \sigma$$

This is seen as follows. As a pictorial aid consider the diagram



We have (cf. (25.6.5) and (25.7.2) of Chapter IV)

$$w^A_{q,n} \circ \tilde{\sigma} \circ \Delta_B = w^A_{q,n+1} \circ \Delta_B = \sigma^{n+1}$$

and on the other hand

$$w^A_{q,n} \circ \Delta_B \circ \sigma = \sigma^n \circ \sigma = \sigma^{n+1}$$

so that $w^A_{q,n} \circ (\Delta_B \circ \sigma) = w^A_{q,n} \circ (\tilde{\sigma} \circ \Delta_B)$ for all $n \in \mathbf{N} \cup \{0\}$, which, since B is A-torsion free, implies that $\Delta_B \circ \sigma = \tilde{\sigma} \circ \Delta_B$.

(ii) We know that $\mathbf{f}_\pi$ is a $\tilde{\sigma}$-semilinear endomorphism of the $W^A_{q,\infty}(B)$-module $\mathscr{C}_q(H; B)$, so by (i) above we can (via Δ_B) consider $\mathscr{C}_q(H; B)$ as a B-module with a σ-semilinear endomorphism $\mathbf{f}_\pi$. Enlarging $\mathbf{Mod}_\sigma(B)$ a bit to include also these pairs $(\mathscr{C}_q(H; B), \mathbf{f}_\pi)$, part (iii) of Theorem (30.2.9) becomes an adjoint functor theorem

$$\mathbf{Mod}_\sigma(B)((M, \eta), \mathscr{T}\mathscr{C}_q(H; B)) \simeq \mathbf{FG}^A_B(G(M, \eta)(X, Y), H(X, Y))$$

where $\mathscr{T}$ is the forgetful functor "forget about $\mathbf{V}_q$."

■(30.2.11) **Proof of Theorem (30.2.9)** Part (ii) is an immediate consequence of (30.1.19) because $\mathbf{f}_\pi$ commutes with α_*. To prove part (i) it suffices to show that

(30.2.12) $$\gamma_{bx}(t) = \Delta_B(b)\gamma_x(t)$$

because α_* is a $W^A_{q,\infty}(B)$-homomorphism. The proof of (30.2.12) is again one of the standard ghost component calculations. Let $g(X) = g(M, \eta)(X)$, $G(X, Y) = G(M, \eta)(X, Y)$. Then we have on the one hand

$$g(\gamma_{bx}(t)) = \sum_{i=0}^{\infty} \pi^{-i}\eta^i(bx)t^{q^i} = \sum_{i=0}^{\infty} \pi^{-i}\sigma^i(b)\eta^i(x)t^{q^i} \tag{30.2.13}$$

And on the other hand we have $\Delta_B(b) = (b_0, b_1, b_2, \ldots)$ where the b_i are such that $w^A_{q,n}(b_0, \ldots, b_n) = \sigma^n(b)$, so that

$$\begin{aligned} g(\Delta_B(b)\gamma_x(t)) &= g\left(\sum_{i=0}^{\infty} \mathbf{V}_q^i\langle b_i\rangle \mathbf{f}_\pi^i \gamma_x(t)\right) \\ &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} \eta^{j+i}(x)\pi^{-j}t^{q^{i+j}}b_i^{q^j} \\ &= \sum_{l=0}^{\infty} \pi^{-l}t^{q^l}\eta^l(x)\sum_{s=0}^{l} \pi^s b_s^{q^{l-s}} \\ &= \sum_{l=0}^{\infty} w^A_{q,l}(b_0, \ldots, b_l)\pi^{-l}\eta^l(x)t^{q^l} \\ &= \sum_{l=0}^{\infty} \sigma^l(b)\pi^{-l}\eta^l(x)t^{q^l} \end{aligned}$$

which is the same as (30.2.13) so that we have proved (30.2.12).

To prove part (iii) of Theorem (30.2.9) we first associate to every β: $M \to \mathscr{C}_q(H; B)$ that is B-linear and takes η into $\mathbf{f}_\pi$, a $\mathrm{Cart}_A(B)$-homomorphism $\tilde{\beta}$: $\mathscr{C}_q(G(M, \eta); B) \to \mathscr{C}_q(H; B)$. Recall that every curve in $\mathscr{C}_q(G(M, \eta); B)$ can be uniquely written as a convergent sum

$$\gamma(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \gamma_{x_i}(t) \tag{30.2.14}$$

Write $\beta_x(t)$ for the curve in $\mathscr{C}_q(H; B)$ that β associates to $x \in M$. We define

$$\tilde{\beta}(\gamma(t)) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \beta_{x_i}(t) \tag{30.2.15}$$

where $\gamma(t)$ is as in (30.2.14). We claim that then

$$\tilde{\beta}(\mathbf{V}_q\gamma(t)) = \mathbf{V}_q\tilde{\beta}(\gamma(t)) \tag{30.2.16}$$

$$\tilde{\beta}(\Delta_B(b)\gamma(t)) = \Delta_B(b)\tilde{\beta}(\gamma(t)) \qquad \text{for all} \quad b \in B \tag{30.2.17}$$

$$\tilde{\beta}(\mathbf{f}_\pi\gamma(t)) = \mathbf{f}_\pi\tilde{\beta}(\gamma(t)) \tag{30.2.18}$$

Of these (30.2.16) is a triviality. To prove (30.2.17) we first have to write $\Delta_B(b)\gamma(t)$ in the form (30.2.14). To this end recall that if $\tilde{\sigma}$ is the Frobenius

endomorphism of $W^A_{q,\infty}(B)$, then $\mathbf{V}_q z = \tilde{\sigma}(z)\mathbf{V}_q$ for all $z \in W^A_{q,\infty}(B)$ and recall that $\Delta_B(\sigma b) = \tilde{\sigma}\Delta_B(b)$ by remark (30.2.10)(i). Using this, we have

$$\Delta_B(b)\gamma(t) = \sum_{i=0}^{\infty} \Delta_B(b)\mathbf{V}_q^i \gamma_{x_i}(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \tilde{\sigma}^i \Delta_B(b)\gamma_{x_i}(t)$$

$$= \sum_{i=0}^{\infty} \mathbf{V}_q^i \Delta_B(\sigma^i(b))\gamma_{x_i}(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \gamma_{\sigma^i(b)x_i}(t)$$

where we have also used the B-linearity of $x \mapsto \gamma_x(t)$. It follows that

$$\tilde{\beta}(\Delta_B(b)\gamma(t)) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \beta_{\sigma^i(b)x_i}(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \Delta_B(\sigma^i(b))\beta_{x_i}(t)$$

$$= \sum_{i=0}^{\infty} \Delta_B(b)\mathbf{V}_q^i \beta_{x_i}(t) = \Delta_B(b)\tilde{\beta}(\gamma(t))$$

where we have now used the B-linearity of $x \mapsto \beta_x(t)$. This proves (30.2.17).

To prove (30.2.18) recall that $[\pi] = \Delta_B(\pi)$ as an element of $\mathrm{Cart}_A(B)$; cf. (29.3.11). We have

$$\mathbf{f}_\pi \gamma(t) = \sum_{i=0}^{\infty} \mathbf{f}_\pi \mathbf{V}_q^i \gamma_{x_i}(t) = \mathbf{f}_\pi \gamma_{x_0}(t) + \sum_{i=1}^{\infty} [\pi]\mathbf{V}_q^{i-1}\gamma_{x_i}(t)$$

$$= \gamma_{\eta(x_0)}(t) + \sum_{i=1}^{\infty} \mathbf{V}_q^{i-1}\Delta_B(\pi)\gamma_{x_i}(t)$$

$$= \gamma_{\eta(x_0)+\pi x_1}(t) + \sum_{i=2}^{\infty} \mathbf{V}_q^{i-1}\gamma_{\pi x_i}(t)$$

so that

$$\tilde{\beta}(\mathbf{f}_\pi \gamma(t)) = \beta_{\eta(x_0)+\pi x_1}(t) + \sum_{i=2}^{\infty} \mathbf{V}_q^{i-1}\beta_{\pi x_i}(t)$$

$$= \beta_{\eta(x_0)}(t) + [\pi]\beta_{x_1}(t) + \sum_{i=2}^{\infty} \mathbf{V}_q^{i-1}[\pi]\beta_{x_i}(t)$$

$$= \mathbf{f}_\pi \beta_{x_0}(t) + [\pi] \sum_{i=1}^{\infty} \mathbf{V}_q^{i-1}\beta_{x_i}(t)$$

$$= \mathbf{f}_\pi \beta_{x_0}(t) + \mathbf{f}_\pi \sum_{i=1}^{\infty} \mathbf{V}_q^i \beta_{x_i}(t) = \mathbf{f}_\pi \tilde{\beta}(\gamma(t))$$

Note also that $\tilde{\beta}$ is additive and continuous. It follows that $\tilde{\beta}$ also commutes with the operators $\langle b \rangle$ because (as is very easily checked) each $\langle b \rangle$ can be written as a convergent sum $\sum_{i=0}^{\infty} \mathbf{V}_q^i \Delta_B(c_i)\mathbf{f}_\pi^i$. Hence $\tilde{\beta}$ is a $\mathrm{Cart}_A(B)$-homomorphism and hence comes from some homomorphism of formal A-modules $\tilde{\beta}(X)$: $G(M, \eta)(X, Y) \to H(X, Y)$. This assigns a homomorphism of formal A-

modules $\tilde{\beta}(X)$ to every B-linear map $\beta: M \to \mathscr{C}_q(H; B)$ which takes η into $\mathbf{f}_\pi$. It is obvious that $r(\tilde{\beta}(X)) = \beta$ proving the injectivity of $\beta \mapsto \tilde{\beta}(X)$. On the other hand, because every curve in $\mathscr{C}_q(G(M, \eta); B)$ can be written in the form (30.2.14), the induced homomorphism α_* of a formal A-module homomorphism is completely determined by the $\alpha_* \gamma_x(t)$ proving that $\widetilde{r(\alpha)}(X) = \alpha(X)$. This concludes the proof of Theorem (30.2.9).

■ (30.2.19) The next thing we want to discuss is the remarkable lifting property (which underlies the universal extension theorem (26.5.8)) which the Lubin-Tate formal A-modules associated to a semilinear map enjoy. To this end we need the following technical lemma (30.2.20). The basic setup is as follows: B, σ, M, η are as in (30.1.7); in addition we suppose that B is complete (in the πB-adic topology), that σ is an automorphism, and that there is a σ^{-1}-semilinear endomorphism $\zeta: M \to M$ (i.e., $\zeta(bx) = \sigma^{-1}(b)\zeta(m)$) such that $\zeta\eta = \eta\zeta = \pi$. Finally, we assume that there is an $r \in \mathbf{N}$ such that $\zeta^r M \subset \pi M$.

■ (30.2.20) **Lemma** Let B, σ, M, ζ, η be as in (30.2.19). Let $\mathfrak{h}$ be a A-torsion free B-module that is complete and Hausdorff in the πB-adic topology and let $R \subset \mathfrak{h}$ be a submodule. Suppose that we have for all $j \in \mathbf{N} \cup \{0\}$ a B-linear map $\tau_j: M \to \mathfrak{h}/\pi^j R$ such that

$$\tau_j \zeta \equiv \pi \tau_{j-1} \mod \pi^j R, \qquad j \in \mathbf{N} \tag{30.2.21}$$

Then there exists a unique B-linear map $\tau: M \to \mathfrak{h}$ such that

$$\tau\eta^j \equiv \tau_j \mod \pi^j R, \qquad j \in \mathbf{N} \cup \{0\} \tag{30.2.22}$$

Proof We first prove that τ is (if it exists at all) unique— Suppose that $\hat{\tau}$ is a second B-linear map $M \to \mathfrak{h}$ such that (30.2.22) holds. Then if $\bar{\tau} = \tau - \hat{\tau}$, we have $\bar{\tau}\eta^j x \equiv 0 \mod \pi^j R$ for all $j \in \mathbf{N} \cup \{0\}$. Take $j = ks$ where k is such that $\zeta^k M \subset \pi M$. Then

$$\bar{\tau}\eta^{ks}\zeta^{ks}x \in \bar{\tau}\eta^{ks}\pi^s M \subset \pi^{s+ks}R \subset \pi^{s+ks}\mathfrak{h}$$

and because $\mathfrak{h}$ is A-torsion free it follows that $\bar{\tau}x \in \pi^s\mathfrak{h}$ for all s hence $\bar{\tau}x = 0$ because $\mathfrak{h}$ is Hausdorff in the πB-adic topology.

To prove existence we proceed (of course) by successive approximation. First, because M is a free B-module, there exist B-linear maps $\hat{\tau}_j: M \to \mathfrak{h}$ that lift the τ_j so that (30.2.21) holds with $\hat{\tau}_j$ instead of τ_j. Now take $\rho_0 = \hat{\tau}_0$, then (30.2.22) holds for $j = 0$ with $\tau = \rho_0$. Suppose with induction that we have found $\rho_n: M \to \mathfrak{h}$ such that (30.2.22) holds with $\tau = \rho_n$ for all $j \leq n$. Let

$$\hat{\tau}_{n+1}\zeta \equiv \pi\hat{\tau}_n + \pi^{n+1}\nu \mod(\pi^{n+2}R)$$

$$\rho_n\eta^n \equiv \hat{\tau}_n + \pi^n\mu \mod(\pi^{n+1}R)$$

where ν, $\mu: M \to \mathfrak{h}$ are B-linear maps. (Such ν, μ exist by (30.2.21) (with $\hat{\tau}$'s instead of τ's) and (30.2.22) (with ρ_n for τ).) Define

$$\rho_{n+1} = \rho_n + (\nu - \mu)\zeta^n$$

Then we have modulo$(\pi^{n+2}R)$

$$\rho_{n+1}\eta^{n+1}\zeta = \rho_n\eta^n(\eta\zeta) + (\nu - \mu)(\zeta^n\eta^n)\eta\zeta$$
$$\equiv \hat{\tau}_n\pi + \pi^{n+1}\mu + \hat{\tau}_{n+1}\zeta - \pi\hat{\tau}_n - \pi^{n+1}\mu \equiv \hat{\tau}_{n+1}\zeta$$

so, in particular, we have $\rho_{n+1}\eta^{n+1}\zeta(\eta x) \equiv \hat{\tau}_{n+1}\zeta(\eta x) \bmod(\pi^{n+2}R)$, i.e., $\rho_{n+1}\eta^{n+1}(\pi x) \equiv \hat{\tau}_{n+1}(\pi x)$ for all $x \in M$, so that $\rho_{n+1}\eta^{n+1} \equiv \hat{\tau}_{n+1} \bmod(\pi^{n+1}R)$ because $\mathfrak{h}$ is A-torsion free. So (30.2.22) holds with $j = n+1$ if we take $\tau = \rho_{n+1}$; it follows (using (30.2.21)) that (30.2.22) also holds for all $j \leq n+1$ with $\tau = \rho_{n+1}$. Because $\zeta^k M \subset \pi M$ for a certain k and $\mathfrak{h}$ is complete in the πB-adic topology, we have that the sequence $\{\rho_n\}_n$ converges for $n \to \infty$ to a certain $\tau\colon M \to \mathfrak{h}$. This τ then satisfies (30.2.22) for all $j \in \mathbf{N} \cup \{0\}$.

■ (30.2.23) Let B, σ, M, η, ζ be as in (30.2.19). Let $\tilde{G}(X, Y)$ over B be the formal A-module associated to (M, η) and let $\tilde{g}(X)$ be its A-logarithm. Then for each $x \in M$ we claim that $\tilde{g}^{-1}(\zeta x t) \in \mathscr{C}_q(\tilde{G}; B)$. This is seen as follows: recall that $\sum_{i=0}^{\infty} x_i t^{q^i} \in M \otimes_A K[\![T]\!]$ is of the form $\tilde{g}(\gamma(t))$ with $\gamma(t) \in \mathscr{C}_q(\tilde{G}; B)$ iff $x_i \equiv \pi^{-1}\eta(x_{i-1}) \bmod M$ for all $j \in \mathbf{N}$ and $x_0 \in M$. So the only thing we have to show is that $\pi^{-1}\eta(\zeta x) \in M$ which is the case because $\eta\zeta = \pi$. We shall write

$$\delta_{\zeta x}(t) = \tilde{g}^{-1}(\zeta x t) \in \mathscr{C}_q(\tilde{G}; B) \tag{30.2.24}$$

We have seen in (30.1.20) that every curve $\gamma(t) \in \mathscr{C}_q(\tilde{G}; B)$ can be written uniquely as a convergent sum $\sum \mathbf{V}_q^i \gamma_{x_i}(t)$. In the case of the curves $\delta_{\zeta x}(t)$ the sum in question is

$$\delta_{\zeta x}(t) = \gamma_{\zeta x}(t) + \mathbf{V}_q\gamma_{-x}(t) \tag{30.2.25}$$

Indeed, by definition

$$\tilde{g}(\gamma_{\zeta x}(t)) = \sum_{i=0}^{\infty} \eta^i(\zeta x)\pi^{-i}t^{q^i}, \qquad \tilde{g}(\mathbf{V}_q\zeta_{-x}(t)) = \sum_{i=0}^{\infty} \eta^i(-x)\pi^{-i}t^{q^{i+1}}$$

so that $\tilde{g}(\gamma_{\zeta x}(t)) + \tilde{g}(\mathbf{V}_q\gamma_{-x}(t)) = \zeta x t$.

■ (30.2.26) **Theorem** Let B, σ, M, η, ζ be as in (30.2.19). Let $\tilde{G}(X, Y)$ be the formal A-module associated to (M, η) and suppose we have the following diagram of (A-typical) formal A-modules over B

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^+(X, Y) & \longrightarrow & H(X, Y) & \xrightarrow{\alpha(X)} & H_1(X, Y) & \longrightarrow & 0 \\ & & & & & \nwarrow^{\beta(X)} & & \nearrow_{\beta(X)} & \\ & & & & & & \tilde{G}(X, Y) & & \end{array}$$

where R^+ is the additive formal A-module with Lie algebra R and where the upper line is exact (i.e., the associated sequence of curve modules $0 \to \mathscr{C}_q(R^+; B) \to \mathscr{C}_q(H; B) \to \mathscr{C}_q(H_1; B) \to 0$ is exact). Suppose moreover that for each $x \in M$ there is an $a(x) \in \mathfrak{h}$, the Lie algebra of H, such that $\delta_{a(x)}(t) =$

$h^{-1}(a(x)t) \in \mathscr{C}_q(H; B)$ and $\alpha_*(\delta_{a(x)}(t)) = \beta(\delta_{\zeta x}(t))$. (Here $h(X)$ is the A-logarithm of $H(X, Y)$.) Then there exists a unique homomorphism $\tilde{\beta}(X)$: $\tilde{G}(X, Y) \to H(X, Y)$ of formal A-modules over B such that $\alpha(X) \circ \tilde{\beta}(X) = \beta(X)$.

■ (30.2.27) **Remarks**

(i) Let $G(X, Y)$ be an A-typical formal A-module over B with A-logarithm $g(X)$. Then $g^{-1}(at)$, $a \in \mathfrak{g} = Lie(G)$ is in $\mathscr{C}_q(G; B)$ iff $g^{-1}(aX)$: $\hat{G}_a(X, Y) \to G(X, Y)$ is a homomorphism of formal A-modules over B. (In both cases the condition is $g^{-1}(aX)$ (or $g^{-1}(at)$) has its coefficients in B rather than $B \otimes_A K$.) So the technical lifting condition in the hypothesis of Theorem (30.2.26) can also be stated as: for every one parameter additive subgroup $\beta(\delta_{\zeta x}(X))$ in $H_1(X, Y)$, there is a one parameter additive subgroup $\delta_{a(x)}(X)$ in $H(X, Y)$ that lifts $\beta(\delta_{\zeta x}(X))$.

(ii) Since every formal A-module over B is strictly isomorphic to an A-typical one, the restriction to A-typical formal A-modules in (30.2.26) is harmless.

■ (30.2.28) **Start of the proof of Theorem (30.2.26)** Taking q-typical curves, we have the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{C}_q(R^+; B) & \longrightarrow & \mathscr{C}_q(H; B) & \xrightarrow{\alpha_*} & \mathscr{C}_q(H_1; B) & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle \beta_*} & & \\ & & & & M & \xrightarrow{\beta_0} & \mathscr{C}_q(\tilde{G}; B) & & \end{array}$$

where β_0: $M \to \mathscr{C}_q(\tilde{G}; B)$, $x \mapsto \gamma_x(t)$ is the canonical map of (30.1.17). Let $\mathfrak{h}$ be the Lie algebra of $H(X, Y)$. Then $h(\mathscr{C}_q(H; B))$ is a certain subgroup of the additive group of all power series $\sum_{i=0}^{\infty} y_i t^{q^i} \pi^{-i}$ with $y_i \in \mathfrak{h}$ and $h(\mathscr{C}_q(R^+; B))$ is the subgroup of all power series $\sum_{i=0}^{\infty} z_i t^{q^i} \pi^{-i}$ with $z_i \in \pi^i R \subset \mathfrak{h}$ because R^+ is an additive subgroup of $H(X, Y)$.

Now let $x \in M$ and consider the curve $\beta_* \beta_0(x) = \beta_* \gamma_x(t) = \beta(\gamma_x(t)) \in \mathscr{C}_q(H_1; B)$. Let $\tilde{\gamma}(x; t)$ be any lift of $\beta(\gamma_x(t))$ and write

$$h(\tilde{\gamma}(x; t)) = \sum_{j=0}^{\infty} \tau_j(x) \pi^{-j} t^{q^j} \tag{30.2.29}$$

Then by the remarks just made the $\tau_j(x)$ are well determined modulo $\pi^j R$. So associated to $\beta(X)$ there is a unique collection of B-linear maps

$$\tau_j \colon M \to \mathfrak{h}/\pi^j R$$

■ (30.2.30) **Lemma** The B-linear maps τ_j determined by (30.2.29) satisfy $\tau_j \zeta \equiv \tau_{j-1} \pi \bmod \pi^j R$ for all $j \in \mathbf{N}$.

Proof Let $x \in M$ and let $\delta_{a(x)}(t) = h^{-1}(a(x)t) \in \mathscr{C}_q(H; B)$ be a lift of $\beta(\delta_{\zeta x}(t)) = \beta(\tilde{g}^{-1}(\zeta x t))$. Now by (30.2.25)

$$\beta(\delta_{\zeta x}(t)) = \beta(\gamma_{\zeta x}(t)) +_{H_1} \beta(\mathbf{V}_q \gamma_{-x}(t))$$

So, taking the lift $\mathbf{V}_q \tilde{\gamma}(-x; t)$ of $\mathbf{V}_q \beta(\gamma_{-x}(t))$, we find modulo $h(\mathscr{C}_q(R^+; B))$ in $h(\mathscr{C}_q(H; B))$

$$a(x)t \equiv \sum_{j=0}^{\infty} \tau_j(\zeta x)\pi^{-j} t^{q^j} + \sum_{j=0}^{\infty} \tau_j(-x)\pi^{-j} t^{q^{j+1}}$$

and comparing coefficients we see that

$$\tau_j(\zeta(x)) \equiv \pi \tau_{j-1}(x) \mod \pi^j R$$

proving the lemma.

■ (30.2.31) **On formal A-module homomorphisms $G(M, \eta)(X, Y) \to H(X, Y)$** Let B, σ, M, η, be as in (30.1.7). Suppose that $\beta(X)$: $G(M, \eta)(X, Y) \to H(X, Y)$ is a formal A-module homomorphism. According to Theorem (30.2.9), $\beta(X)$ determines a unique map

$$\beta: M \to \mathscr{C}_q(H; B)$$

which is B-linear and which is such that $\beta\eta = \mathbf{f}_\pi \beta$. Let $h(X)$ be the logarithm of $H(X, Y)$ and let $\mathfrak{h}$ be the Lie algebra of $H(X, Y)$. Then, we claim, β is necessarily of the form

$$h(\beta(x)) = \sum_{i=0}^{\infty} \tau \eta^i(x)\pi^{-i} t^{q^i} \tag{30.2.32}$$

where $\tau: M \to \mathfrak{h}$ is a B-linear homomorphism. To prove this write

$$h(\beta(x)) = \sum_{n=0}^{\infty} \tau_n(x)\pi^{-n} t^{q^n}, \qquad \tau_n: M \to \mathfrak{h}$$

Then using $\beta\eta = \mathbf{f}_\pi \beta$,

$$h(\beta(\eta x)) = h(\mathbf{f}_\pi \beta(x)) = \sum_{n=0}^{\infty} \tau_{n+1}(x)\pi^{-n} t^{q^n}$$

we see that $\tau_n(\eta x) = \tau_{n+1}(x)$ for all x, so that we must have $\tau_n = \tau_0 \eta^n$. So that indeed $\beta(x)$ is of the form (30.2.32) for some map $\tau = \tau_0: M \to \mathfrak{h}$. It remains to show that τ is a morphism of B-modules. The additivity of τ follows from the additivity of β. Now we also know that $\beta(bx) = \Delta_B(b)\beta(x)$. Let $\Delta_B(b) = (b_0, b_1, b_2, \ldots)$. Then $w^A_{q,n}(b_0, \ldots, b_n) = \sigma^n(b)$. And we find

$$h(\beta(bx)) = \sum_{i=0}^{\infty} \tau \eta^i(bx)\pi^{-i} t^{q^i} = \sum_{i=0}^{\infty} \tau(\sigma^i(b)\eta^i(x))\pi^{-i} t^{q^i}$$

while on the other hand

$$h(\Delta_b(b)\beta(x)) = h\left(\sum_{n=0}^{\infty} \mathbf{V}_q^n\langle b_n\rangle \mathbf{f}_\pi^n \beta(x)\right)$$

$$= \sum_{n=0}^{\infty}\sum_{i=0}^{\infty} \tau\eta^{i+n}(x) b_n^{q^i}\pi^{-i}t^{q^{i+n}}$$

$$= \sum_{r=0}^{\infty}\left(\sum_{s=0}^{r} b_s^{q^r-s}\pi^s\right)\tau\eta^r(x)t^{q^r}$$

$$= \sum_{r=0}^{\infty} \sigma^r(b)\tau\eta^r(x)t^{q^r}$$

Comparing these two expressions, we see (by looking at the coefficient of t) that $\tau(bx) = b\tau(x)$ for all b and x; and, conversely, if $\tau(bx) = b\tau(x)$ for all $b \in B$, then $h(\beta(bx)) = h(\Delta_B(b)\beta(x))$. So we have shown

■ (30.2.33) **Lemma** A B-linear morphism β: $M \to \mathscr{C}_q(H; B)$ such that $\beta\eta = \mathbf{f}_\pi \beta$ is necessarily of the form (30.2.32) with τ: $M \to \mathfrak{h}$ a homomorphism of B-modules; and, conversely, if τ: $M \to \mathfrak{h}$ is a homomorphism of B-modules, then (30.2.32) defines a B-linear morphism β: $M \to \mathscr{C}_q(H; B)$ such that $\beta = \mathbf{f}_\pi\beta$ provided that $\beta(x) \in B[\![t]\!]$ for all $x \in M$.

Another, rather easier, way of obtaining this triviality is as follows. Every formal A-module homomorphism $\beta(X)$: $G(M, \eta)(X, Y) \to H(X, Y)$ is of the form $h^{-1}(ag(x))$ where $h(X)$ is the A-logarithm of $H(X, Y)$ and $g(X)$ that of $G(M, \eta)(X, Y)$. It follows that the induced map β_*: $\mathscr{C}_q(G(M, \eta); B) \to \mathscr{C}_q(H; B)$ has the property $h(\beta_*\gamma(t)) = \tau g(\gamma(t))$ where τ is a B-module morphism $M \to \mathfrak{h}$. Substituting $\gamma_x(t) = \beta_0(x)$ and recalling that $g(\gamma_x(t)) = \sum \eta^i(x)\pi^{-i}t^{q^i}$, we find

$$h(\beta(x)) = h(\beta_*\gamma_x(t)) = \sum_{i=0}^{\infty} \tau\eta^i(x)\pi^{-i}t^{q^i}$$

■ (30.2.34) **Proof of Theorem (30.2.26) (conclusion)** Let τ_j: $M \to \mathfrak{h}/\pi^j R$ be as in (30.2.28). By Lemma (30.2.30) we can apply Lemma (30.2.20) to find a map

$$\tau\colon M \to \mathfrak{h}, \qquad \tau\eta^n \equiv \tau_n \mod \pi^n R$$

Now define $\tilde{\beta}$: $M \to \mathscr{C}_q(H; B \otimes_A K)$ by the formula

$$\tilde{\beta}(x) = h^{-1}\left(\sum_{n=0}^{\infty} \tau\eta^n(x)\pi^{-n}t^{q^n}\right) \tag{30.2.35}$$

Then because $\tau\eta^n \equiv \tau_n \mod \pi^n R$, we have that $\alpha_*\tilde{\beta}(x) = \beta_*\beta_0(x)$. We claim that $\tilde{\beta}(x) \in \mathscr{C}_q(H; B) \subset \mathscr{C}_q(H; B \otimes_A K)$. This is seen as follows. As before let $\tilde{\gamma}(x; t) \in \mathscr{C}_q(H; B)$ be any curve such that $\alpha_*(\tilde{\gamma}(x; t)) = \beta_*\beta_0(x)$. We have

$$h(\tilde{\beta}(x)) = \sum_{n=0}^{\infty} \tau\eta^n(x)\pi^{-n}t^{q^n}, \qquad h(\tilde{\gamma}(x; t)) = \sum_{n=0}^{\infty} \tau_n(x)\pi^{-n}t^{q^n}$$

and $\tau\eta^n(x) - \tau_n(x) = \pi^n r_n(x) \in \pi^n R$ because $\tau\eta^n \equiv \tau_n \bmod \pi^n R$. Because R^+ is an additive subgroup of $H(X, Y)$, we have $h^{-1}\left(\sum_{i=0}^{\infty} r_i t^{q^i}\right) \in \mathscr{C}_q(H; B)$ for all sequences $(r_0, r_1, r_2, \ldots)$ of elements of R. Hence

$$\tilde{\beta}(x) = h^{-1}\left(\left(\sum_{n=0}^{\infty} \tau_n(x)\pi^{-n} t^{q^n}\right) + \left(\sum_{n=0}^{\infty} r_n(x) t^{q^n}\right)\right)$$

$$= \tilde{\gamma}(x, t) +_H h^{-1}\left(\sum_{n=0}^{\infty} r_n(x) t^{q^n}\right) \in \mathscr{C}_q(H; B)$$

By Lemma (30.2.33) and Theorem (30.2.9) it follows that there is a unique homomorphism of formal A-modules $\tilde{\beta}(X)$ such that $\tilde{\beta}_* \beta_0 = \tilde{\beta}$ which again by part (iii) of Theorem (30.2.9) means that $\alpha(X) \circ \tilde{\beta}(X) = \beta(X)$.

It remains to show that $\tilde{\beta}(X)$ is unique. Using Theorem (30.2.9), it suffices to show that if $\hat{\beta}\colon M \to \mathscr{C}_q(H; B)$ is such that $\alpha_* \hat{\beta} = \alpha_* \tilde{\beta} = \beta$, then $\hat{\beta} = \tilde{\beta}$. By Lemma (30.2.33) $\hat{\beta}$ is of the form

$$h\hat{\beta}(x) = \sum_{i=0}^{\infty} \hat{\tau}\eta^i(x)\pi^{-i} t^{q^i}$$

for some B-module homomorphism $\hat{\tau}\colon M \to \mathfrak{h}$. Then from $\alpha_* \hat{\beta} = \alpha_* \tilde{\beta} = \beta$ we see that $\hat{\tau}\eta^i \equiv \tau_i \bmod \pi^i R$ and the uniqueness part of Lemma (30.2.20) then says that $\hat{\tau} = \tau$, so that $\hat{\beta} = \tilde{\beta}$. This concludes the proof of the theorem.

30.3 The universal extension with additive kernel

■ (30.3.1) Let $B, \sigma, M, \eta, \zeta$ be as before in (30.2.19). In addition we now suppose that we have given a free submodule $N \subset M$ such that M/N is also free and such that $N + \pi M = \zeta M$. (The hypothesis that M/N is free is equivalent to $N \cap \pi M = \pi N$.)

■ (30.3.2) **Quotients of Lubin–Tate formal A-modules by additive kernels** Let $B, \sigma, M, \eta, \zeta, N$ be as in (30.3.1). Let $\tilde{G}(X, Y) = LT(M, \eta)$ be the Lubin–Tate formal A-module associated to (M, η). By hypothesis $N \subset \zeta M$ so for every $y \in N$ there is a (unique) $x \in M$ (ζ is injective because M, being free, is A-torsion free) such that $y = \zeta x$. We have seen that if $\tilde{g}(X)$ is the A-logarithm of $\tilde{G}(X, Y)$, then $\tilde{g}^{-1}(\zeta x t) \in \mathscr{C}_q(\tilde{G}; B)$ and in fact $\tilde{g}^{-1}(\zeta x t) = \delta_{\zeta x}(t) = \gamma_{\zeta x}(t) + \mathbf{V}_q \gamma_{-x}(t)$ (cf. (30.2.23)). This gives us an embedding $\mathscr{C}_q(N^+; B) \to \mathscr{C}_q(\tilde{G}; B)$ where $N^+(X, Y)$ is the additive formal A-module with Lie algebra N. We form the exact sequence

$$0 \to \mathscr{C}_q(N^+; B) \to \mathscr{C}_q(\tilde{G}; B) \to R \to 0 \tag{30.3.3}$$

■ (30.3.4) **Proposition** The $\mathrm{Cart}_A(B)$-module R is a reduced $\mathrm{Cart}_A(B)$-module. So $R = \mathscr{C}_q(G; B)$ for some formal A-module $G(X, Y)$. Further, $G(X, Y)$ is of finite A-height (and (30.3.3) is the exact sequence of q-typical curves of the extension with additive kernel $0 \to N^+(X, Y) \to \tilde{G}(X, Y) \to G(X, Y) \to 0$).

Proof We show first that $\gamma(t) \in \mathscr{C}_q(\tilde{G}; B)$, $\mathbf{V}_q\gamma(t) \in \mathscr{C}_q(N^+; B) \Rightarrow \gamma(t) \in \mathscr{C}_q(N^+; B)$. We can write $\gamma(t)$ as a unique sum

$$\gamma(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \gamma_{x_i}(t)$$

Now $\mathscr{C}_q(N^+; B) = \{\sum_{i=0}^{\infty} \mathbf{V}_q^i \delta_{\zeta y_i}(t)\}$, where

$$\delta_{\zeta y_i}(t) = \tilde{g}^{-1}(\zeta y_i t) = \gamma_{\zeta y_i}(t) +_{\tilde{G}} \gamma_{-y_i}(t^q)$$

with $\zeta y_i \in N$. So if $\mathbf{V}_q\gamma(t) \in \mathscr{C}_q(N^+; B)$, we must have

$$\sum_{i=0}^{\infty} \mathbf{V}_q^{i+1}\gamma_{x_i}(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \gamma_{\zeta y_i}(t) + \sum_{i=0}^{\infty} \mathbf{V}_q^{i+1}\gamma_{-y_i}(t)$$

$$= \gamma_{\zeta y_0}(t) + \sum_{i=1}^{\infty} V_q^i \gamma_{\zeta y_i - y_{i-1}}(t)$$

which gives us

$$\zeta y_0 = 0, \qquad x_0 = \zeta y_1 - y_0, \qquad x_1 = \zeta y_2 - y_1, \qquad \cdots$$

so that $y_0 = 0$ and

$$\gamma(t) = \sum_{i=0}^{\infty} \mathbf{V}_q^i \gamma_{x_i}(t) = \gamma_{\zeta y_1}(t) +_{\tilde{G}} (\mathbf{V}_q \gamma_{\zeta y_2} +_{\tilde{G}} \mathbf{V}_q \gamma_{-y_1}) +_{\tilde{G}} \cdots$$

$$= \delta_{\zeta y_1}(t) +_{\tilde{G}} \mathbf{V}_q \delta_{\zeta y_2}(t) + \cdots \in \mathscr{C}_q(N^+; B)$$

By Proposition (28.2.2) and the argument used in (28.3.2) it follows that there is a **V**-basis $\{\gamma_1(t), \ldots, \gamma_h(t)\}$ for $\mathscr{C}_q(\tilde{G}; B)$ such that $\{\gamma_1(t), \ldots, \gamma_r(t)\}$ is a **V**-basis for $\mathscr{C}_q(N^+; B)$. It follows immediately that the classes of $\{\gamma_{r+1}(t), \ldots, \gamma_h(t)\}$ are a **V**-basis for R.

Hence R is a reduced $\mathrm{Cart}_A(B)$-module, and so there exists a formal A-module $G(X, Y)$ such that $\mathscr{C}_q(G; B) = R$. It remains to prove that $G(X, Y)$ is of finite A-height.

■ (30.3.5) **Proof that $G(X, Y)$ is of finite A-height** To prove that $G(X, Y)$ is of finite A-height we must show that $\bar{G}(X, Y)$, the reduction of $G(X, Y)$ mod πB, is of finite A-height and by definition this means that we must show that $\mathbf{f}_\pi$ is injective on $\mathscr{C}_q(\bar{G}; l)$. Let $\gamma(t) \in \mathscr{C}_q(\tilde{G}; B)$. Then $\mathbf{f}_\pi$ is injective on $\mathscr{C}_q(\bar{G}; l)$ iff for all $\gamma(t) \in \mathscr{C}_q(\tilde{G}; B)$

$$\mathbf{f}_\pi\gamma(t) \in \mathscr{C}_q(N^+; B) + \pi\mathscr{C}_q(\tilde{G}; B) \tag{30.3.6}$$

implies that

$$\gamma(t) \in \mathscr{C}_q(N^+; B) + \pi\mathscr{C}_q(\tilde{G}; B) \tag{30.3.7}$$

(Recall that $\pi\mathscr{C}_q(\tilde{G}; B) = \{\sum x_i t^i \mid \sum x_i t^i$ is q-typical and $x_i \in \pi B$ for all $i\}$; do

not confuse $\pi\mathscr{C}_q(\tilde{G}; B)$ with $[\pi]\mathscr{C}_q(\tilde{G}; B)$, the image of $\mathscr{C}_q(\tilde{G}; B)$ under the endomorphism $[\pi]$ of $\mathscr{C}_q(\tilde{G}; B)$.)

Write

$$\gamma(t) = \sum_{n \geq n_0} \mathbf{V}_q^n \gamma_{x_n}(t) \tag{30.3.8}$$

We claim that it now suffices to prove that if $\gamma(t)$ satisfies condition (30.3.6), then $x_{n_0} \in N + \pi M$. Indeed, suppose that $x_{n_0} \in N + \pi M$, then $\tilde{g}^{-1}(x_{n_0} t^{q^{n_0}}) \in \mathscr{C}_q(N^+; B) + \pi\mathscr{C}_q(\tilde{G}; B)$ (by part (iv) of the functional equation lemma 10.2) and subtracting $\tilde{g}^{-1}(x_{n_0} t^{q^{n_0}})$ from $\gamma(t)$ we find a $\gamma_1(t)$

$$\gamma_1(t) = \sum_{n \geq n_0 + 1} \mathbf{V}_q^n \gamma_{y_n}(t)$$

(with $y_{n_0+1} = x_{n_0+1} + \zeta^{-1} x_{n_0}$, $y_i = x_i$, $i \geq n_0 + 2$) which also satisfies (30.3.6) (because $\mathbf{f}_\pi \mathscr{C}_q(N^+; B) \subset \mathscr{C}_q(N^+; B)$ and $\mathbf{f}_\pi(\pi\mathscr{C}_q(\tilde{G}; B)) \subset \pi\mathscr{C}_q(\tilde{G}; B)$; this last fact is seen as follows; using part (iv) of the functional equation lemma

$$\begin{aligned}
\gamma(t) \in \pi\mathscr{C}_q(\tilde{G}; B) \quad &\Leftrightarrow \quad f(\gamma(t)) = \sum_{i=0}^{\infty} b_i t^{q^i} \qquad \text{with} \quad b_i \in \pi B \\
&\Rightarrow \quad f(\mathbf{f}_\pi \gamma(t)) = \sum_{i=0}^{\infty} \pi b_{i+1} t^{q^i} \qquad \text{with} \quad b_{i+1} \in \pi B \\
&\Rightarrow \quad \mathbf{f}_\pi \gamma(t) \in \pi^2 \mathscr{C}_q(\tilde{G}; B) \subset \pi\mathscr{C}_q(\tilde{G}; B))
\end{aligned}$$

This proves the claim. So suppose that the $\gamma(t)$ of (30.3.8) satisfies (30.3.6). We have

$$\mathbf{f}_\pi \gamma(t) = \mathbf{f}_\pi \sum_{n \geq n_0} \mathbf{V}_q^n \gamma_{x_n}(t) = \mathbf{f}_\pi \mathbf{V}_q^{n_0} \gamma_{x_{n_0}} + \sum_{n > n_0} \mathbf{V}_q^{n-1} [\pi] \gamma_{x_n}(t)$$

Using part (iv) of the functional equation lemma again and applying $\tilde{g}$, we see that we must have

$$\begin{aligned}
\eta(x_{n_0}) &\equiv y_{n_0} \mod \pi M, & y_{n_0} \in N \\
\pi^{-1}\eta^2(x_{n_0}) + \eta x_{n_0+1} &\equiv y_{n_0+1} \mod \pi M, & y_{n_1} \in N \\
&\vdots \\
\pi^{-r}\eta^{r+1}(x_{n_0}) + \pi^{-r+1}\eta^r(x_{n_0+1}) + \cdots + \eta(x_{n_0+r}) & \\
&\equiv y_{n_0+r} \mod \pi M, & y_{n_0+r} \in N \\
&\vdots
\end{aligned}$$

Applying ζ^r to the rth equation, we obtain (using that M is B-torsion free)

$$\begin{aligned}
&\eta(x_{n_0}) + \pi^{-r+1}\eta^r\zeta^r x_{n_0+1} + \pi^{-r+2}\eta^{r-1}\zeta^r x_{n_0+2} + \cdots + \zeta^r \eta(x_{n_0+r}) \\
&\quad \equiv \zeta^r y_{n_0+r} \mod \pi M
\end{aligned}$$

and hence (since $\eta\zeta = \pi$) we see that

$$\eta(x_{n_0}) \in \zeta^r N + \pi M$$

for all $r \in \mathbf{N}$. There is an r such that $\zeta^r M \subset \pi M$, hence we find that $\eta(x_{n_0}) \in \pi M$ or (since M is torsion free so that η is injective) $x_{n_0} \in \zeta M = N + \pi M$ and we are through.

■ (30.3.9) **Theorem** The sequence

$$0 \to N^+(X, Y) \to \tilde{G}(X, Y) \xrightarrow{\alpha(X)} G(X, Y) \to 0$$

is the universal extension of $G(X, Y)$ with additive kernel.

That is, for every exact sequence of formal group laws with additive kernel

$$0 \to P^+(X, Y) \to H(X, Y) \xrightarrow{\beta(X)} G(X, Y) \to 0$$

there is a unique homomorphism $\tilde{\alpha}(X)$: $\tilde{G}(X, Y) \to H(X, Y)$ such that $\beta(X) \circ \tilde{\alpha}(X) = \alpha(X)$, or in other words there is a unique homomorphism $N^+ \to P^+$ such that $0 \to P^+ \to H \to G \to 0$ is the pushout of $0 \to N^+ \to \tilde{G} \to G \to 0$ along $N^+ \to P^+$.

■ (30.3.10) **Corollary** $\operatorname{Ext}^1(G, P^+) \simeq \mathbf{FG}_B^A(N^+, P^+) = \mathbf{Mod}_B(N, P)$;

$$\operatorname{Ext}^1(G, \hat{\mathbf{G}}_a) = N^*,$$

the linear dual of the Lie algebra N of N^+.

■ (30.3.11) **Proof of the theorem** Consider the diagram

$$\begin{array}{ccccccc} 0 \to & N^+ & \to & \tilde{G}(X, Y) & \xrightarrow{\alpha(X)} & G(X, Y) & \to 0 \\ & & & \downarrow & & \| & \\ 0 \to & P^+ & \to & H(X, Y) & \xrightarrow{\beta(X)} & G(X, Y) & \to 0 \end{array}$$

According to Theorem (30.2.26) there exist a unique $\tilde{\alpha}(X)$ such that $\beta(X) \circ \tilde{\alpha}(X) = \alpha(X)$ if every curve of the form $\alpha_*(\tilde{g}^{-1}(\zeta x t))$ in $G(X, Y)$, $x \in M$, can be lifted to a curve in $H(X, Y)$ of the form $h^{-1}(at)$, $a \in \mathfrak{h}$ the Lie algebra of $H(X, Y)$. Now $\zeta M = N + \pi M$ and $N^+ \subset \operatorname{Ker} \alpha(X)$ so that $\alpha_*(g^{-1}(\zeta x t)$ is of the form $g^{-1}(\pi b t)$, $b \in \mathfrak{g}$, the Lie algebra of G. Since β_* is surjective, there is an $a \in \mathfrak{h}$ such that $Lie(\beta)(a) = b$, and then $h^{-1}(\pi a t) \in \mathscr{C}_q(H; B)$ (part (iv) of the functional equation lemma again), and

$$\beta_*(h^{-1}(\pi a t)) = g^{-1}(\pi b t) = \alpha_*(g^{-1}(\zeta x t)). \quad \text{Q.E.D.}$$

■ (30.3.12) **Theorem** Let B, σ, M, η, ζ, N be as in (30.3.1) and let $0 \to N^+(X, Y) \to \tilde{G}(X, Y) \xrightarrow{\alpha(X)} G(X, Y) \to 0$ be the exact sequence associated to these data. Let $\bar{G}(X, Y)$ over l be the reduction of $G(X, Y)$ mod πB. Then $M \simeq \mathscr{C}_q(\bar{G}; l)$. More precisely, the composed map

$$(30.3.13) \qquad M \xrightarrow{\beta_0} \mathscr{C}_q(\tilde{G}; B) \xrightarrow{\alpha_*} \mathscr{C}_q(G; B) \longrightarrow \mathscr{C}_q(\bar{G}; l)$$

is an isomorphism and under this isomorphism η goes to $\mathbf{f}_\pi$ and ζ to $\mathbf{V}_q$.

Proof Let $\chi: M \to \mathscr{C}_q(G; l)$ be the composed map (30.3.13) and let us write $r: \mathscr{C}_q(G; B) \to \mathscr{C}_q(\bar{G}; l)$ for the reduction map. Then because β_0, α_*, and r are all B-linear (via $B \xrightarrow{\Delta_B} W^A_{q,\infty}(B)$) we see that χ is B-linear. Further, r and α_* commute with $\mathbf{f}_\pi$ and $\beta_0(\eta x) = \mathbf{f}_\pi \beta_0(x)$, so χ takes η into $\mathbf{f}_\pi$. Now consider what χ does to ζ. We can write $\zeta x = y + \pi z$, $y \in N$, $z \in M$. We have

$$\gamma_{\zeta x}(t) = \tilde{g}^{-1}(\zeta x t) +_{\tilde{G}} \mathbf{V}_q \gamma_x(t) = \tilde{g}^{-1}(yt) +_{\tilde{G}} \tilde{g}^{-1}(\pi z t) +_{\tilde{G}} \mathbf{V}_q \gamma_x(t)$$

But $\tilde{g}^{-1}(yt) \in \mathscr{C}_q(N^+; B)$ and $\tilde{g}^{-1}(\pi z t) \in \pi \mathscr{C}_q(\tilde{G}; B)$. It follows that

$$\chi(\zeta x) = r\alpha_*(\mathbf{V}_q \gamma_x(t)) = \mathbf{V}_q(\chi(x))$$

Now filter M by the submodules $\zeta^r M$ (this is a filtration because $\zeta^k M \subset \pi M$ for k large enough) and $\mathscr{C}_q(\bar{G}; l)$ by the submodules $\mathbf{V}_q^r \mathscr{C}_q(\bar{G}; l)$. Then $\chi(\zeta^r M) \subset \mathbf{V}_q^r \mathscr{C}_q(G; l)$ and we have induced maps

$$\zeta^r M/\zeta^{r+1} M \to \mathbf{V}_q^r \mathscr{C}_q(G; l)/\mathbf{V}_q^{r+1} \mathscr{C}_q(G; l) \tag{30.3.14}$$

We want to show that these maps are bijective. Because ζ and $\mathbf{V}_q$ are both injective, it suffices to prove this for the case $r = 0$. Surjectivity is easiest. By the definition of β_0, $M \to \mathscr{C}_q(\tilde{G}; B) \to \mathscr{C}_q(\tilde{G}; B)/\mathbf{V}_q \mathscr{C}_q(\tilde{G}; B)$ is surjective since $\beta_0(x) = \gamma_x(t) \equiv xt \bmod \mathbf{V}_q \mathscr{C}_q(\tilde{G}; B)$. Since $\mathrm{Lie}(\alpha)$ and $\mathrm{Lie}(r)$ (by abuse of notation) are also surjective, it follows that $\chi: M \to \mathscr{C}_q(G; l)/\mathbf{V}_q \mathscr{C}_q(G; l)$ is surjective. To see injectivity, suppose that $r\alpha_*(\gamma_x(t)) \in \mathbf{V}_q \mathscr{C}_q(G; l)$. This means that the coefficient of t in $\gamma_x(t)$ is in $N + \pi M$. But the coefficient of t in $\gamma_x(t)$ is x and $N + \pi M = \zeta M$. Hence $x \in \zeta M$. This concludes the proof of the theorem.

■ (30.3.15) **Lifting formal A-modules** We now turn our attention to the lifting of formal A-modules. Let l be a perfect extension field of k and $\Gamma(X, Y)$ be a formal A-module over l that is of finite A-height. We take $M = \mathscr{C}_q(\Gamma; l)$, $B = W^A_{q,\infty}(l)$, σ is the Frobenius endomorphism of $W^A_{q,\infty}(l)$, and $\eta = \mathbf{f}_\pi$, $\zeta = \mathbf{V}_q$ (as endomorphisms of M). We claim that all the hypotheses of (30.2.19) are satisfied in this case. First, because $\Gamma(X, Y)$ is of finite A-height, we have that $M = \mathscr{C}_q(\Gamma; l)$ is a free $B = W^A_{q,\infty}(l)$-module of finite rank (cf. (29.7.5)). Also $\mathbf{f}_\pi \mathbf{V}_q = \mathbf{V}_q \mathbf{f}_\pi = [\pi]$, which is the image of $\pi \in A$ under the A-algebra structure map $A \to W^A_{q,\infty}(l) = B$. Further, $\eta = \mathbf{f}_\pi$ is σ-semilinear and $\zeta = \mathbf{V}_q$ is σ^{-1}-semilinear (cf. (29.6.7)). It remains to show that $\zeta^r M \subset \pi M$ for r large enough. This is also a consequence of the finite height property of $\Gamma(X, Y)$. Indeed, by Proposition (28.2.2) (or rather its analogue for $\mathrm{Cart}_A(l)$-modules) there exists a $\mathbf{V}$-basis $\{\gamma_1, \ldots, \gamma_n\}$ of $\mathscr{C}_q(\Gamma; l)$ and a partition of $\{1, 2, \ldots, n\} = I_\infty \cup I_0 \cup I_2 \cup \cdots$ such that

$$\gamma = \sum_{s=0}^{\infty} \sum_{i=1}^{n} \mathbf{V}_q^s \langle a_{s,i} \rangle \gamma_i \in [\pi] \mathscr{C}_q(\Gamma; l)$$

iff $a_{s,i} = 0$ if $i \in I_l$ and $n < l$. Because $\Gamma(X, Y)$ is of finite height, we have that $\mathscr{C}_q(\Gamma; l)/[\pi]\mathscr{C}_q(\Gamma; l)$ is a finite dimensional l-module, which means that $I_\infty = \varnothing$

so that $\mathbf{V}_q^r \mathscr{C}_q(\Gamma; l) \subset [\pi]\mathscr{C}_q(\Gamma; l)$ if r is the maximum of the indices i for which $I_i \neq \varnothing$. (There are only finitely many i for which $I_i \neq \varnothing$ because $\Gamma(X, Y)$ is finite dimensional, i.e., $n < \infty$.)

We are now in a position to apply the constructions of (30.3.2) to obtain formal A-modules $G(X, Y)$ over $B = W_{q,\infty}^A(l)$. According to Theorem (30.3.12) we then have that $\mathscr{C}_q(\bar{G}; l) \simeq M = \mathscr{C}_q(\Gamma; l)$ as a $\mathrm{Cart}_A(l)$-module, so that $\bar{G}(X, Y)$ and $\Gamma(X, Y)$ are isomorphic. That is, the formal A-modules thus obtained are lifts of $\Gamma(X, Y)$. The question of course arises whether all lifts are obtained in this way. This is in fact the case, and this is what we are going to prove next. So let $G(X, Y)$ over $B = W_{q,\infty}^A(l)$ be any formal A-module that lifts $\Gamma(X, Y)$. The first thing to do is to construct a homomorphism of formal A-modules $\tilde{G}(X, Y) \to G(X, Y)$ where $\tilde{G}(X, Y) = G(M, \eta)(X, Y)$. The picture is

(30.3.16)

$$\begin{array}{ccc} & & 0 \\ & & \downarrow \\ & & S \\ & & \downarrow \\ \mathscr{C}_q(\tilde{G}; B) & \xrightarrow{\beta_\bullet} & \mathscr{C}_q(G; B) \\ \uparrow{\scriptstyle \beta_0} & \nearrow{\scriptstyle \beta} & \downarrow{\scriptstyle r} \\ M & = & \mathscr{C}_q(\Gamma; l) \\ & & \downarrow \\ & & 0 \end{array}$$

where r is the reduction map, and $S = \mathrm{Ker}\, r$. The existence of $\beta_\bullet$ is (by Theorem (30.2.9)) equivalent to the existence of a B-linear map $\beta: M \to \mathscr{C}_q(G; B)$ such that $\beta(\eta x) = \mathbf{f}_\pi \beta(x)$; or in other words what we have to construct is a section of r that commutes with $\mathbf{f}_\pi$ (but not (necessarily) with $\mathbf{V}_q$).

■ (30.3.17) **Construction of β** Let $\mathfrak{g}$ be the Lie algebra of $G(X, Y)$. For each $x \in M = \mathscr{C}_q(\Gamma; l)$, let $\tilde{\gamma}(x, t)$ be any curve in $\mathscr{C}_q(G; B)$ that lifts $x \in \mathscr{C}_q(\Gamma; l)$. Write

$$g(\tilde{\gamma}(x, t)) = \sum_{i=0}^{\infty} \tau_i(x) \pi^{-i} t^{q^i}$$

Now $S = \pi\mathscr{C}_q(G; B)$, and by part (iv) of the functional equation lemma this means that for all $\delta(t) \in S$, $g(\delta(t)) = \sum_{i=0}^{\infty} \pi b_i t^{q^i}$ with $b_i \in \mathfrak{g}$ for all $i \in \mathbf{N} \cup \{0\}$; cf. also (21.8.6). So the $\tau_i(x)$ are well defined mod $\pi^{i+1}\mathfrak{g}$.

Now consider $\zeta x = \mathbf{V}_a x$ in $\mathscr{C}_q(\Gamma; l)$. Then we have of course

$$g(\tilde{\gamma}(\zeta x, t)) = \sum_{i=0}^{\infty} \tau_i(\zeta x) \pi^{-i} t^{q^i} \mod g(S)$$

On the other hand, $\mathbf{V}_q\tilde{\gamma}(x, t)$ is also a lift of $\zeta x = \mathbf{V}_q x$, and

$$g(\mathbf{V}_q\tilde{\gamma}(x, t)) = \sum_{i=0}^{\infty} \tau_i(x)\pi^{-i}t^{q^{i+1}} \mod g(S)$$

Comparing coefficients, we see that $\tau_i\zeta \equiv \tau_{i-1}\pi \mod \pi^{i+1}\mathfrak{g}$. Take $R = \pi\mathfrak{g}$. Then we see that we can apply Lemma (30.2.20) to obtain a unique map τ: $M \to \mathfrak{g}$ such that

$$\tau\eta^i(x) \equiv \tau_i(x) \mod \pi^{i+1}\mathfrak{g}$$

for all $i \in \mathbf{N} \cup \{0\}$. Now define β: $M \to \mathscr{C}_q(G; B)$ by

$$\beta(x) = g^{-1}\left(\sum_{i=0}^{\infty} \tau\eta^i(x)\pi^{-i}t^{q^i}\right)$$

This map takes η into $\mathbf{f}_\pi$ and is B-linear, so (by Lemma (30.2.33)) the only thing we still have to check is that $\beta(x) \in \mathscr{C}_q(G; B)$ rather than $\mathscr{C}_q(G; B \otimes_A K)$. But modulo $\pi\mathscr{C}_q(G; B)$, we have

$$\sum_{i=0}^{\infty} \tau\eta^i(x)\pi^{-i}t^{q^i} \equiv \sum_{i=0}^{\infty} \tau_i(x)\pi^{-i}t^{q^i} = g(\tilde{\gamma}(x, t))$$

so that by another application of part (iv) of the functional equation lemma we have that indeed $\beta(x) \in \mathscr{C}_q(G; B)$ and even that

$$\beta(x) \equiv \tilde{\gamma}(x, t) \mod \pi\mathscr{C}_q(G; B) \tag{30.3.18}$$

showing that β is in fact a section of r.

■ (30.3.19) **Remark** Note that if we identify (as usual) M with the Lie algebra $\tilde{\mathfrak{g}}$ of $\tilde{G}(X, Y)$, then $Lie(\beta(X)) = \tau$ where $\beta(X)$ is the homomorphism of formal A-modules $\tilde{G}(X, Y) \to G(X, Y)$ corresponding to β.

■ (30.3.20) **Lemma** $\beta_\bullet$ is surjective.

Proof This is practically a triviality. Since β is a section of r, we first have that $M \to \mathfrak{g}/\pi\mathfrak{g}$ is surjective (where we identify $\mathfrak{g}$ with $\mathscr{C}_q(G; B)/\mathbf{V}_q\mathscr{C}_q(G; B)$. Next β is B-linear and $Lie([\pi])$: $\mathfrak{g} \to \mathfrak{g}$ is multiplication with π. Hence $\beta(\pi^r M) \subset \pi^r\mathfrak{g}$ (mod $\mathbf{V}_q\mathscr{C}_q(G; B)$) and the induced maps $\pi^r M/\pi^{r+1}M \to \pi^r\mathfrak{g}/\pi^{r+1}\mathfrak{g}$ are all surjective. It follows that $M \to \mathscr{C}_q(G; B)/\mathbf{V}_q\mathscr{C}_q(G; B)$ is surjective. Since $\beta_\bullet$ commutes with $\mathbf{V}_q$, it follows that $\beta_\bullet$ is surjective.

■ (30.3.21) **Corollary** Let $N = \mathrm{Ker}(Lie(\beta(X)) = \mathrm{Ker}\ \tau$. Then M/N is free.

Proof By the surjectivity of $Lie(\beta(X))$: $\tilde{\mathfrak{g}} \to \mathfrak{g}$ we have $M/N \simeq \mathfrak{g}$.

■ (30.3.22) **Lemma** $N \subset \zeta M$.

Proof Let $x \in N \subset M$. Then $Lie(\beta(X))(x) = 0$, which means that $\beta(x) \in \mathbf{V}_q\mathscr{C}_q(G; B)$. By (30.3.18) this means that

$$x = r\beta(x) \in \mathbf{V}_q\mathscr{C}_q(\Gamma; l) = \zeta M$$

■ (30.3.23) **Lemma** $\mathscr{C}_q(N^+; B) = \operatorname{Ker} \beta_\bullet$.

Proof Let $x \in N \subset \zeta M \subset M$. Then $\tilde{g}^{-1}(xt) = \gamma_x(t) + \gamma_{-y}(t^q)$, where $y \in M$ is such that $x = \zeta y$. Then

$$g(\beta_\bullet(\tilde{g}^{-1}(xt))) = \sum_{i=0}^{\infty} \tau\eta^i(x)\pi^{-i}t^{q^i} - \sum_{i=0}^{\infty} \tau\eta^i(y)\pi^{-i}t^{q^{i+1}} = \tau x t$$

So if $x \in N$, $(\tilde{g}^{-1}(xt)) \in \operatorname{Ker} \beta_\bullet$. Since every element in $\mathscr{C}_q(N^+; B)$ is a convergent sum of expressions of the form $\mathbf{V}_q^i\tilde{g}^{-1}(x_i t)$, $x_i \in N$, and $\beta_\bullet$ commutes with $\mathbf{V}_q$, it follows that $\mathscr{C}_q(N^+; B) \subset \operatorname{Ker} \beta_\bullet$. Now let $\gamma(t) \in \operatorname{Ker} \beta_\bullet$ and write

$$\gamma(t) = \sum_{n \geq s} \mathbf{V}_q^n \gamma_{x_n}(t) \tag{30.3.24}$$

If we can show that $\gamma(t) \in \operatorname{Ker} \beta_\bullet$ then implies that $x_s \in N$, we are through. Indeed, writing $x_s = \zeta y_s$, $y_s \in M$, we have

$$\gamma(t) - \tilde{g}^{-1}(x_s t) = \sum_{n \geq s+1} \mathbf{V}_q^n \gamma_{z_n}(t)$$

with $z_{s+1} = x_{s+1} + y_s$, $z_i = x_i$ for $i \geq s + 2$. Using induction and the fact that $\mathscr{C}_q(N^+; B)$ is complete and that $\mathscr{C}_q(\tilde{G}; B)$ is Hausdorff, it follows that $\gamma(t) \in \mathscr{C}_q(N^+; B)$. So it remains to show that if $\gamma(t)$ is of the form (30.3.24) and $\gamma(t) \in \operatorname{Ker} \beta_\bullet$, then $x_s \in N$. Consider

$$\hat{\gamma}(t) = \sum_{j=0}^{\infty} \mathbf{V}_q^j \gamma_{x_{j+s}}(t)$$

then $0 = \beta_\bullet(\gamma(t)) = \beta_\bullet(\mathbf{V}_q^s\hat{\gamma}(t)) = \mathbf{V}_q^s\beta_\bullet(\hat{\gamma}(t))$; and since $\mathbf{V}_q$ is injective, it follows that $\beta_\bullet(\hat{\gamma}(t)) = 0$. But then $Lie(\beta(X))(x_{0+s}) = \tau(x_s) = 0$ and hence $x_s \in N$. This proves Lemma (30.3.23).

■ (30.3.25) **Lemma** $\zeta M = N + \pi M$.

Proof We have already seen that $N \subset \zeta M$, hence $N + \pi M \subset \zeta M$ since $\pi M = \zeta(\eta M) \subset \zeta M$. Conversely, let $x \in \zeta M \subset M$. We have

$$\beta_0(x) \equiv xt \mod \mathbf{V}_q\mathscr{C}_q(\tilde{G}; B)$$

and hence

$$\beta(x) \equiv \tau(x)t \mod \mathbf{V}_q\mathscr{C}_q(G; B)$$

On the other hand

$$\beta(x) \equiv \tilde{\gamma}(x, t) \mod \pi\mathscr{C}_q(G; B)$$

and $\tilde{\gamma}(x, t)$ is a lift of $x \in \zeta M = \mathbf{V}_q \mathscr{C}_q(\Gamma; l)$, which means that the coefficient of t in $\tilde{\gamma}(x, t)$ is divisible by π, so that $\tau x = \pi y$ for some $y \in \mathfrak{g}$. But $\tau: M \to \mathfrak{g}$ is surjective, so there is a $z \in M$ such that $y = \tau z$, then $\tau x = \tau \pi z$ or $x - \pi z \in N$, proving the lemma.

■ (30.3.26) Putting everything together we obtain the following. Let $\Gamma(X, Y)$ be a finite A-height formal A-module over l. Then if $G(X, Y)$ is a lift of $\Gamma(X, Y)$ over $B = W^A_{q,\infty}(l)$, there is an exact sequence

$$0 \to N^+(X, Y) \to \tilde{G}(X, Y) \to G(X, Y) \to 0$$

with $\tilde{G}(X, Y) = LT(\mathscr{C}_q(\Gamma; l), \mathbf{f}_\pi)(X, Y)$. This sequence is the universal extension of $G(X, Y)$ by an additive kernel by Theorem (30.3.9). So in particular we see that: (i) a universal extension with additive kernel of a finite height formal A-module $G(X, Y)$ over B always exists; and (ii) the middle term of this universal extension depends only on $\Gamma(X, Y)$, the reduction mod πB of $G(X, Y)$.

Now let $G(X, Y)$ and $\hat{G}(X, Y)$ be isomorphic formal A-modules over B. Then taking universal extensions we obtain a diagram

$$\begin{array}{ccccccc} 0 \to & N^+(X, Y) & \to & \tilde{G}(X, Y) & \to & G(X, Y) & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & \hat{N}^+(X, Y) & \to & \tilde{\hat{g}}(X, Y) & \to & \hat{G}(X, Y) & \to 0 \end{array}$$

where the dashed arrows exist by the universal extension property. This gives us an isomorphism $M \simeq \hat{M}$ where $M = \mathscr{C}_q(\bar{G}; l)$, $\hat{M} = \mathscr{C}_q(\bar{\hat{G}}; l)$ which takes N onto $\hat{N}$. Conversely, given an isomorphism of $\mathrm{Cart}_A(l)$-modules $M \xrightarrow{\sim} \hat{M}$ which takes N onto $\hat{N}$, we obtain an isomorphism $LT(M, \mathbf{f}_\pi)(X, Y) \xrightarrow{\sim} LT(\hat{M}, \mathbf{f}_\pi)(X, Y)$ taking $N^+(X, Y)$ onto $\hat{N}^+(X, Y)$ and hence an isomorphism $G(X, Y) \to \hat{G}(X, Y)$. We have

■ (30.3.27) **Corollary** (classification theorem for formal A-modules over $B = W^A_{q,\infty}(l)$) Finite height formal A-modules over $B = W^A_{q,\infty}(l)$ where l is a perfect field extension of k, the residue field of A, are classified by quadruples (M, η, ζ, N) where M is a free B-module of finite rank, N is a free submodule of M of finite rank such that M/N is free, and where η is a σ-semilinear endomorphism of M, ζ is a σ^{-1}-semilinear endomorphism of M such that $\eta\zeta = \zeta\eta = \pi$, $N + \pi M = \zeta M$, $\zeta^r M \subset \pi M$ for r sufficiently large. (It is not really necessary to mention η; assuming $\zeta M \supset \pi M$ and ζ injective, one can define $\eta(x) = \zeta^{-1}(\pi x)$.)

■ (30.3.28) **Artin–Hasse exponentials** (for the third and last time) Let l be a perfect field extension of k and $G(X, Y)$ a Lubin–Tate formal A-module of dimension 1 over $W^A_{q,\infty}(l) = B$. In Chapter IV, Section 25 we have discussed the associated Artin–Hasse exponential, a functorial A-algebra homomorphism $\mathscr{C}_q(G; -) \to \mathscr{C}_q(G; \mathscr{C}_q(G; -))$. Putting in l and using the fact that $\mathscr{C}_q(\Gamma; l) \simeq B$ where $\Gamma(X, Y)$ is the reduction mod πB of $G(X, Y)$, we find a ring homomorphism $\Delta: \mathscr{C}_q(\Gamma; l) \to \mathscr{C}_q(G; B)$. We claim that this is in fact the unique B-linear

section of the reduction map $\mathscr{C}_q(G; B) \to \mathscr{C}_q(\Gamma; l)$ that commutes with $\mathbf{f}_\pi$ which was constructed in (30.3.17).

Now by definition Δ satisfies $w^G_{q,n} \circ \Delta = \mathbf{f}^n_\pi$ (using that under $B \simeq C_q(\Gamma, l)$, σ goes into $\mathbf{f}_\pi$; cf. Chapter IV, Remark (25.6.16)). Hence $w^G_{q,n} \circ (\Delta \circ \mathbf{f}_\pi) = \mathbf{f}^{n+1}_\pi$ (and on the other hand, $w^G_{q,n} \circ \mathbf{f}_\pi \circ \Delta = w^G_{q,n+1} \circ \Delta = \mathbf{f}^{n+1}_\pi$, proving that $\Delta \circ \mathbf{f}_\pi = \mathbf{f}_\pi \circ \Delta$ because $B = \mathscr{C}_q(\Gamma; l)$ is A-torsion free. On the other hand, Δ is a ring homomorphism giving us the B-linearity; and finally by Addendum (25.7.7) of Chapter IV (take $i = 0$), we see that Δ is a section of the reduction map. This proves our claim.

We can therefore view the sections β of (30.3.17) as (a kind of) Artin–Hasse exponential maps.

30.4 Cartier–Dieudonné modules and Eisenstein equations

Let A be a complete discrete valuation ring with residue field k of q elements and uniformizing element π. Let $G(X, Y)$ be a one dimensional formal A-module over A. We then have three ways to classify $G(X, Y)$:

(i) By Theorem (21.8.9) there is a unique polynomial $\vartheta(t) = \pi + v_1 t + \cdots + v_h t^h$ with $v_i \in \pi A$ for $i = 1, \ldots, h-1$, $v_h \in A^* = U(A)$ such that $G(X, Y)$ is strictly isomorphic to a formal A-module over A with logarithm equal to $f(X) = X + \sum_{i=1}^h v_i \pi^{-1} f(X^{q^i})$.

(ii) By Theorem (22.2.1) $G(X, Y)$ is classified by its reduction $\Gamma(X, Y)$ over k, and we can classify $\Gamma(X, Y)$ by the characteristic polynomial of its Frobenius endomorphism $\xi(X) = X^q$ (cf. Section 24.5 of Chapter IV).

(iii) By (30.3.27) $G(X, Y)$ is classified by $\mathscr{C}_q(\Gamma; l) = M$ together with a free submodule N of rank $h-1$ such that M/N is free (of rank 1) and such that $\zeta M = pM + N$.

We now describe the relations between these results. First, notice that the endomorphism $\xi(X) = X^q$ induces of course an endomorphism $\xi_\bullet : \mathscr{C}_q(\Gamma; k) \to \mathscr{C}_q(\Gamma; k)$; we have in fact $\xi_\bullet = \mathbf{V}_q$. Now define a map

$$\text{(30.4.1)} \qquad \mathrm{End}_k(\Gamma(X, Y)) \to \mathscr{C}_q(\Gamma; k), \qquad \alpha(X) \to \alpha_\bullet \gamma_0(t)$$

where $\gamma_0(t) = t$ is the canonical basis curve of $\mathscr{C}_q(\Gamma; k)$. Because $\alpha_\bullet$ is uniquely determined by what it does to $\gamma_0(t)$, this map is injective. It is also surjective. This is seen as follows. The map (30.4.1) is A-linear. And since $\Gamma(X, Y)$ is of finite height, an A-basis for $\mathscr{C}_q(\Gamma; k)$ is $\gamma_0(t)$, $\mathbf{V}_q \gamma_0(t)$, $\ldots$, $\mathbf{V}_q^{h-1} \gamma_0(t)$. Let $\gamma(t) = \sum_{i=0}^{h-1} a_i \mathbf{V}_q^i \gamma_0(t)$ be any curve in $\mathscr{C}_q(\Gamma, k)$, then the endomorphism $a_0 + a_1 \xi + \cdots + a_{h-1} \xi^{h-1}$ maps to $\gamma(t)$ under (30.4.1).

Because $\gamma_0(t), \ldots, \mathbf{V}_q^{h-1} \gamma_0(t)$ is a basis for $\mathscr{C}_q(\Gamma; k)$, we must have a relation

$$\mathbf{V}_q^h \gamma_0(t) + a_{h-1} \mathbf{V}_q^{h-1} \gamma_0(t) + \cdots + a_1 \mathbf{V}_q \gamma_0(t) + a_0 \gamma_0(t) = 0$$

This gives us a polynomial

$$t^h + a_{h-1}t^{h-1} + \cdots + a_1 t + a_0 \tag{30.4.2}$$

which because the isomorphism (30.4.1) takes $\xi(X)$ into $\mathbf{V}_q\gamma_0(t)$ is the characteristic polynomial of $\xi(X)$ and hence an Eisenstein polynomial. We can identify M with $\mathbf{Z}_p[t]/(t^h + a_{h-1}t^{h-1} + \cdots + a_0)$ where "$t = \zeta$."

Another way to see that $t^h + a_{h-1}t^{h-1} + \cdots + a_1 t + a_0 = 0$ is an Eisenstein polynomial is as follows. Let $\eta\colon M \to M$ be given by $1 \mapsto b_{h-1}t^{h-1} + \cdots + b_1 t + b_0$. Then we must have

$$\begin{aligned}\pi &= t(b_{h-1}t^{h-1} + \cdots + b_1 t + b_0)\\ &= b_{h-2}t^{h-1} + \cdots + b_0 t - b_{h-1}(a_{h-1}t^{h-1} + \cdots + a_1 t + a_0)\end{aligned}$$

which gives us

$$\pi = b_{h-1}a_0, \qquad b_0 - a_1 b_{h-1} = 0, \qquad \ldots, \qquad b_{h-2} - b_{h-1}a_{h-1} = 0$$

Suppose that $\pi \mid b_{h-1}$, then also $\pi \mid b_0, \ldots, \pi \mid b_{h-2}$, so that

$$\eta 1 = \pi(c_{h-1}t^{h-1} + \cdots + c_1 t + c_0)\pi$$

$$t\eta = \pi t(c_{h-1}t^{h-1} + \cdots + c_1 t + c_0)$$

or

$$t(c_{h-1}t^{h-1} + \cdots + c_1 t + c_0) = 1$$

making t a unit which contradicts $t^r M \subset \pi M$ for r large. Therefore $\pi \mid a_0$ and in fact $v(a_0) = 1$. Suppose that r is the smallest index such that $\pi \mid a_r$ and suppose that $r < h$. Then we have

$$(t^h + a_{h-1}t^{h-1} + \cdots + a_1 t + a_0) \equiv (t^{h-r} + \cdots + a_r)(t^r) \mod \pi$$

and by Hensel's lemma we have a factor $t^r + d_{r-1}t^{r-1} + \cdots + d_1 t + d_0$ of $t^h + a_{h-1}t^{h-1} + \cdots + a_1 t + a_0$ with $\pi \mid d_i$, $i = 0, \ldots, r-1$. It follows that there is a curve $\gamma(t) \neq 0$ in $\mathscr{C}_q(\Gamma; k)$ such that

$$(\mathbf{V}_q^r + d_{r-1}\mathbf{V}_q^{r-1} + \cdots + d_0)\gamma(t) = 0$$

Let $\gamma(t) \equiv ut^{q^n}$, $u \neq 0$. Then because A-ht$(\Gamma(X, Y)) = h$, we have $d_i\mathbf{V}_q^i\gamma(t) \equiv 0$ mod(degree q^{n+h}) and $\mathbf{V}_q^r\gamma(t) \not\equiv 0$ mod(degree q^{n+r}), which is a contradiction because $r < h$. It follows that $\pi \mid a_i$ for all $i = 0, \ldots, h-1$, i.e., that the polynomial (30.4.2) is Eisenstein.

(Incidentally we know by Theorem (22.2.1) that $G(X, Y)$ is classified by $\mathscr{C}_q(\Gamma; k)$, i.e., by M alone; in other words N is irrelevant (up to isomorphism) in the case of dimension 1 formal A-modules over A; this can also be shown directly.)

To find the connection between classification methods (i) and (ii), we use

$$\pi f(X) \equiv v_1 f(X^q) + \cdots + v_{h-1} f(X^{q^h}) \mod \pi$$

By part (iv) of the functional equation lemma it follows that

$$f^{-1}(\pi f(X)) \equiv f^{-1}(v_1 f(X^q)) +_F \cdots +_F f^{-1}(v_h f(X^{q^h})) \mod \pi$$

i.e., in $\mathscr{C}_q(\Gamma; k)$ we have

$$[\pi]\gamma_0 = [v_1]\xi_0\gamma_0 + \cdots + [v_h]\xi_0^h\gamma_0$$

which gives us that the polynomial $\vartheta(t)$ of classification method (i) and the characteristic polynomial of $\xi(X)$ (classification method (ii)) are related by the formula

$$v_h^{-1}\vartheta(t) = t^h + a_{h-1}t^{h-1} + \cdots + a_1 t + a_0$$

(This of course fits in with the fact that one dimensional formal A-modules over A are isomorphic iff they are strictly isomorphic.)

If $G(X, Y)$ is a one dimensional formal A-module over some unramified (finite) extension B of A, we still have the three classification possibilities (i)–(iii). The relations between them are then much more difficult to trace. In this case N does play a nontrivial role because two lifts $G(X, Y)$, $\hat{G}(X, Y)$ of $\Gamma(X, Y)$ are not necessarily isomorphic if $B \neq A$. (Nor is it true that isomorphic formal A-modules are also necessarily strictly isomorphic in this case.)

E.4 Bibliographical and Other Notes

■ (E.4.1) **On Dieudonné modules** The functor $F(X, Y) \mapsto \mathscr{C}(F; A)$, which assigns to a formal group law over A the module of curves over A is a covariant functor. Now in [277], for instance, one associates Dieudonné modules to formal groups in a contravariant manner. In this subsection we briefly describe this contravariant Dieudonné module functor. For proofs cf. [95]; cf. also [94, 277]. The first topic we take up is:

(a) *Finite commutative group ..nemes* Let k be a perfect field of characteristic $p > 0$. A finite scheme over k is a functor N: $\mathbf{Alg}_k \to$ Set which is representable by an algebra $A(N)$ that as a module over k is finite dimensional. A commutative finite group scheme over k is a commutative group object in the category of finite schemes over k. (See Section 36.1 for the notion of a group object in a category.) Let $A(N)$ represent the commutative finite group scheme N. Then $A(N)$ is a k-module with five structure maps, viz. m: $A(N) \otimes A(N) \to A(N)$, e: $k \to A(N)$, μ: $A(N) \to A(N) \otimes A(N)$, ε: $A(N) \to k$, ι: $A(N) \to A(N)$. Of these, m and e define the k-algebra structure of $A(N)$ and μ, ε, ι are the structure maps of $A(N)$ as a cogroup object in $\mathbf{Alg}_k^f$. (There are of course a number of compatibility conditions that have to be satisfied.) Now let $A(N)^* = \mathrm{Mod}_k(A(N), k)$. Then $A(N)^*$ inherits five structure maps $m^*, e^*, \mu^*, \varepsilon^*, \iota^*$ of which μ^*, ε^* make $A(N)^*$ an object of $\mathbf{Alg}_k^f$ and m^*, e^*, ι^* make $A(N)^*$ a cogroup object in $\mathbf{Alg}_k^f$. Let $D(N)$ be the finite commutative group scheme represented by $A(N)^*$. Then we have just defined a duality functor D: $\mathbf{N}_k \to \mathbf{N}_k$, where $\mathbf{N}_k$ is the category of finite commutative group schemes over k. (As yet the hypothesis that k is perfect has not played a role.) This duality is called Cartier duality, a topic that will be treated in considerable detail and in greater generality in Sections 37.1 and 37.2 of Chapter VII.

Let $N \in \mathbf{N}_k$ and let $A(N) \in \mathbf{Alg}_k^f$ be its algebra. Let $\mathfrak{n}$ be the ideal of nilpotent elements in $A(N)$. Then $A(N)/\mathfrak{n} \in \mathbf{Alg}_k^f$ inherits a cogroup structure from $A(N)$, and we find a subgroup scheme $N_{\text{red}} \subset N$ which is represented by $A(N)/\mathfrak{n}$. Moreover, the quotient $N/N_{\text{red}} = N_{\text{loc}}$ exists. (Its algebra is the local k-algebra which is obtained as follows: $A(N)$ as an artinian k-algebra is a product of local k-algebras and $A(N_{\text{loc}})$ is the local quotient of $A(N)$ through which $\varepsilon\colon A \to k$ factors; the algebra $A(N_{\text{red}})$ is better described as the maximal étale subalgebra of $A(N)$.) We find a direct sum decomposition $N = N_{\text{red}} \times N_{\text{loc}}$. Now consider $D(N_{\text{red}})$ and $D(N_{\text{loc}})$. These can also be decomposed. So that (applying D again and using $DD = id$) we find a decomposition $N = N_{ll} \times N_{lr} \times N_{rl} \times N_{rr}$ and a corresponding decomposition of $\mathbf{N}_k$ into a direct sum of four subcategories $\mathbf{N}_{ll}$, $\mathbf{N}_{lr}$, $\mathbf{N}_{rl}$, $\mathbf{N}_{rr}$. Examples of objects in each of these four categories are:

$\alpha_p \in \mathbf{N}_{ll}$; $\quad \alpha_p = \operatorname{Spec}(k[X]/X^p)$, $\quad \mu(X) = 1 \otimes X + X \otimes 1$,

$$\iota(X) = -X, \qquad \varepsilon(X) = 0, \qquad D(\alpha_p) = \alpha_p$$

$\mu_p \in \mathbf{N}_{lr}$; $\quad \mu_p = \operatorname{Spec}(k[X]/X^p - 1)$, $\quad \mu(X) = X \otimes X$,

$$\iota(X) = X^{p-1}, \qquad \varepsilon(X) = 1$$

$\nu_p \in \mathbf{N}_{rl}$; $\quad \nu_p = \operatorname{Spec}(k[X]/X^p - X)$, $\quad \mu(X) = 1 \otimes X + X \otimes 1$,

$$\iota(X) = -X, \qquad \varepsilon(X) = 0, \qquad D(\nu_p) = \mu_p$$

$\mu_n \in \mathbf{N}_{rr}$ if $(n, p) = 1$; $\quad \mu_n = \operatorname{Spec}(k[X]/X^n - 1)$,

$$\mu(X) = X \otimes X, \qquad \iota(X) = X^{n-1}, \qquad \varepsilon(X) = 1$$

(b) *Dieudonné modules of objects of* $\mathbf{N}_{ll}$, $\mathbf{N}_{rl}$ Let W_{p^n} over k be the group scheme of Witt vectors of length $n+1$ associated to the prime number p. That is, $W_{p^n}(B) = \{(b_0, b_1, \ldots, b_n) \mid b_i \in B\}$ and addition is by means of the Witt addition polynomials Σ_0, $\Sigma_1, \ldots, \Sigma_n$. Let $T\colon W_{p^n} \to W_{p^{n+1}}$ be the homomorphism defined by $T_B(b_0, \ldots, b_n) = (0, b_0, \ldots, b_n)$. Now let $N \in \mathbf{N}_{ll}$ or $N \in \mathbf{N}_{rl}$, then one defines

$$M(N) = \varinjlim \mathbf{GA}_k(N, W_{p^n})$$

where the transition maps are induced by the T's and where $\mathbf{GA}_k$ is the category of affine group schemes over k. Let $\mathbf{D}$, the Dieudonné ring over k, be the ring generated by two symbols $\mathbf{f}$ and $\mathbf{V}$ over $W_{p^\infty}(k)$, subject to the relations $\mathbf{fV} = \mathbf{Vf} = p \in W_{p^\infty}(k)$, $\mathbf{f}a = \sigma(a)\mathbf{f}$, $a\mathbf{V} = \mathbf{V}\sigma(a)$ for all $a \in W_{p^\infty}(k)$, where $\sigma\colon W_{p^\infty}(k) \to W_{p^\infty}(k)$ is the Frobenius endomorphism of $W_{p^\infty}(k)$. Now let $\mathbf{f}$, $\mathbf{V}$, and $a \in W_{p^\infty}(k)$ act on the W_{p^n} as follows: $\mathbf{f}$ acts on $W_{p^n}(B)$ as $\mathbf{f}_p$, i.e., $\mathbf{f}(b_0, \ldots, b_n) = (b_0^p, \ldots, b_n^p)$; $\mathbf{V}$ acts on $W_{p^n}(B)$ as $\mathbf{V}_p$, i.e., $\mathbf{V}(b_0, \ldots, b_n) = (0, b_0, \ldots, b_{n-1})$; and $a \in W_{p^\infty}(k)$ acts on $W_{p^n}(B)$ as multiplication with $\sigma^{-n}(a)$; i.e., if $a = (a_0, a_1, \ldots)$, then $a * (b_0, \ldots, b_n) = (a_0^{p^{-n}}, \ldots, a_n^{p^{-n}}) \cdot (b_0, \ldots, b_n)$ where the dot denotes the multiplication in the ring $W_{p^n}(B)$. These operations are compatible with the T: $W_{p^n} \to W_{p^{n+1}}$. (This is obvious for the $\mathbf{V}$ and $\mathbf{f}$ operators and it holds for the $a \in W_{p^\infty}(k)$ operators because in $W_{p^\infty}(B)$ one has $a \cdot \mathbf{V}_p b = \mathbf{V}_p(\mathbf{f}_p a \cdot b)$ (cf. (17.3.17) in Chapter III). As a result, $M(N)$ becomes a $\mathbf{D}$-module. The $M(N)$ for N in $\mathbf{N}_{ll}$ or $\mathbf{N}_{rl}$ are $W_{p^\infty}(k)$-modules of finite length which are killed by a power of $\mathbf{V}$. If $N \in \mathbf{N}_{ll}$, then $M(N)$ is also killed by a power of $\mathbf{f}$; and if $N \in \mathbf{N}_{rl}$, then $\mathbf{f}$ acts bijectively.

(c) *Dieudonné modules of objects of* $\mathbf{N}_{lr}$ Now let M be any module over $\mathbf{D}$. We define a dual module M^* as follows. As a $W_{p^\infty}(k)$-module $M^* = \mathbf{Mod}_A(M, K/A)$, where

$A = W_{p^r}(k)$ and K is the quotient field of A. We let $\mathbf{f}$ and $\mathbf{V}$ act on M^* as follows: $(\mathbf{f}x)(m) = \sigma(x(\mathbf{V}m))$, $(\mathbf{V}x)(m) = \sigma^{-1}(x(\mathbf{f}m))$ for $x \in M^*$, and $m \in M$. Then $M \mapsto M^*$ defines a duality of $\mathbf{D}$-modules which are of finite length as $W_{p^r}(k)$ modules. One now defines for $N \in \mathbf{N}_{lr}$ the Dieudonné module as $M(N) = M(D(N))^*$ which is well-defined because $D(N) \in \mathbf{N}_{rl}$.

In this connection it is good to know that if $N \in \mathbf{N}_{ll}$, then $M(N) = M(D(N))^*$.

(d) *Dieudonné modules of formal group laws* Now let $F(X, Y)$ be a finite dimensional group law over k. Then $F(X, Y)$ defines a comultiplication map μ: $k[\![X_1, \ldots, X_n]\!] \to k[\![X_1, \ldots, X_n]\!] \otimes k[\![X_1, \ldots, X_n]\!]$, $X_i \mapsto F(i)(X \otimes 1, 1 \otimes X)$ (cf. (36.1.4) below). Let $\mathfrak{m}^{(p^n)}$ be the closed ideal in $k[\![X]\!]$ generated by the p^nth powers of the X_i, $i = 1, \ldots, n$. Then, we claim, $\mu(\mathfrak{m}^{(p^n)}) \subset \mathfrak{m}^{(p^n)} \otimes k[\![X]\!] + k[\![X]\!] \otimes \mathfrak{m}^{(p^n)}$. (This follows directly from $F(X, 0) = X$ and $F(0, Y) = Y$.) It follows that μ induces a comultiplication $k[\![X]\!]/\mathfrak{m}^{(p^n)} \to k[\![X]\!]/\mathfrak{m}^{(p^n)} \otimes k[\![X]\!]/\mathfrak{m}^{(p^n)}$, so we obtain a finite commutative group scheme N_n over k (which is in $\mathbf{N}_{ll} \times \mathbf{N}_{lr}$). One now defines the Dieudonné module of $F(X, Y)$ as $M(F) = \varinjlim M(N_n)$.

(e) The theory briefly indicated above is the Cartier–Gabriel generalization and conceptualization of Dieudonné's original method of attaching a Dieudonné module to a formal group law. The bonuses thus obtained are considerable (for instance, the Dieudonné modules defined in (b) classify all unipotent algebraic groups over k). Note however that in Dieudonné's original version he attached modules in a covariant manner and that he also did not need to suppose the base field to be perfect, a hypothesis that does seem to be required in the Cartier–Gabriel version. For a generalization over nonperfect fields cf. [355] and [506]. Furthermore, recently, Berthelot and Messing [467] established the full-faithfulness of a (generalized cf. [285, 155]) contravariant Dieudonné module functor for p-divisible groups over a not necessarily perfect field (of characteristic $p > 0$).

(f) One can now also proceed in the opposite way. Take a finite local group scheme over a complete local ring. Write N as the kernel of an epimorphic homomorphism of smooth formal groups $0 \to N \to F_0 \to F_1 \to 0$, and define $\mathscr{C}_p(N) = \mathrm{Coker}(\mathscr{C}_p(F_0) \to \mathscr{C}_p(F_1))$ (where $\mathscr{C}_p$ is the p-typical curve functor) to obtain a covariant Dieudonné theory for finite local group schemes over complete local rings; cf. Oort [321].

(g) There is something inelegant about the asymmetric treatment of the three subcategories $\mathbf{N}_{ll}$, $\mathbf{N}_{rl}$, $\mathbf{N}_{lr}$ for which (contravariant) Dieudonné modules can be defined. This can be remedied by using Barsotti's covectors; cf. [21, 22] and also [143].

■ (E.4.2) $\hat{W}(X, Y)$ **as a generator** Let $F(X, Y)$ over A be a formal group law. Then for every curve $\gamma(t) \in \mathscr{C}(F; A)$, there is a homomorphism of formal group laws $\alpha_\gamma(X)$: $\hat{W}(X, Y) \to F(X, Y)$ taking $\gamma_w(t)$ into $\gamma(t)$. So if we let $\gamma(t)$ run through a $\mathbf{V}$-basis of $\mathscr{C}(F; A)$, then we can find in this way an epimorphism $W(X, Y)^I \to F(X, Y)$ showing that every formal group law is the quotient of a (possibly infinite) number of copies of $\hat{W}(X, Y)$.

■ (E.4.3) **Notes on Section 27** The three theorems of Cartier are the subject of his *Comptes Rendus* note [65]. Cartier never published his proofs. By this time, however, a number of proofs have appeared. In [254, 256] Lazard gave proofs of the first and second theorem and two proofs of the third theorem. He also discusses an intermediate case (between $\mathrm{Cart}(A)$ and $\mathrm{Cart}_p(A)$) where a certain number of primes are supposed to be

invertible. These proofs are very much from the power series point of view. In [123] Ditters has given a set of proofs from the bialgebra point of view. Here entwined function pairs play a central role. Unfortunately, as we have seen, the ring L, which classifies entwined pairs of functions, is not torsion free (Examples (27.4.17) and (27.4.18)). As a result the proof of Cartier's third theorem in [123], cf. also [124], appears to be correct only for A of characteristic zero. For some more (classification) uses of entwined function pairs, cf. also [125]. Related results have been written down by Kirillov [222].

The proofs of the first and second theorem which I have given above more or less follow Lazard [256]. The proof of the third theorem, however, comes from [175], which paper also gives the connection between the functional equation lemma and the notion of an entwined pair of functions, the subject matter of Section 27.6.

■ (E.4.4) **Notes on Section 28** The technical proposition (28.2.2) and its proof come from Lazard's notes [256]. Propositions (28.3.8) and (23.3.9) follow Manin [277], and in Section 28.4 we follow Manin [277] very closely (in spite of the fact that we are in a somewhat more general situation).

Euclidean algorithms (proper stathms) for noncommutative rings were first studied by Wedderburn [435] and Ore [323]; cf. also Jacobson [204].

■ (E.4.5) **Notes on Section 29** These results were announced in [180]. Completely independently, Drinfel'd in [135] has also obtained a classification theorem for formal A-modules in terms of $\mathrm{Cart}_A(B)$ modules for A of characteristic zero. He uses a clever two-step reduction method: first go from $\mathbf{Z}_p$ to the ring of integers of a finite unramified extension of $\mathbf{Q}_p$ and then deal with the case of a completely ramified extension. In this way one does not obtain the explicit description of the q-typical curve functor $\mathscr{C}_q(-; B)$, nor of the operator $\mathbf{f}_\pi$, and one also does not obtain the analogue of the first theorem (as far as I can see). And, of course, this method does not work if A is of characteristic $p > 0$.

■ (E.4.6) **Notes on Section 30** These results were announced in [182]. The whole structure of the theory and practically all the proofs are entirely straightforward generalizations of the theorems and proofs sketched by Cartier in his 1972 IHES seminar [68] (once one has available the formal A-module Cartier–Dieudonné theory of Section 29). For (30.1.26), I have also made use of [72].

For very much related material (universial extensions, etc.) in the context of Barsotti–Tate groups, and to see how one can apply these and similar results to, e.g., the theory of abelian varieties, see Messing's book [286]; cf. also [285].

Another treatment of (some of) the results of Cartier's IHES seminar can be found in Lazard's book [256].

The results of Section 30 generalize the more explicit results of Section 22 on moduli for one dimensional formal group laws. More explicit results on moduli for higher dimensional formal group laws are in Umemura [423]; these are useful for explicit calculations of local moduli of abelian varieties; cf. Norman [312].

More, related results on formal groups over $W_{p^\infty}(k)$, k a perfect field, can be found in Fontaine's two notes [141, 142], which moreover also contain results on finite group schemes over $W_{p^\infty}(k)$.

■ (E.4.7) **Note on formal groups up to isomorphism and algebroid formal groups** Manin's big paper [277] contains much more than we have mentioned so far.

It also contains classification results of formal groups up to isomorphism over an algebraically closed field of characteristic $p > 0$ in terms of certain finite dimensional (not connected) algebraic varieties of parameters. It further proves that if $\hat{A}$ is the formal group of an abelian variety over k and if $G_{n,m}$ occurs in the decomposition up to isogeny of $\hat{A}$, then so does $G_{m,n}$ (the symmetry theorem; the opposite theorem has been proved by Serre).

A formal group law F is algebroid if it is the formal completion of some algebraic group scheme. More results pertaining to algebroid formal groups and related questions like algebraic hulls of formal groups can be found in [107, 367, 413, 414].

CHAPTER VI

APPLICATIONS OF FORMAL GROUPS IN ALGEBRAIC TOPOLOGY, NUMBER THEORY, AND ALGEBRAIC GEOMETRY

31 Basic Definitions and Survey of the Results of Chapter VI

This section gives a short survey of some applications of the theory of formal group laws; we discuss these in more detail in Sections 32–35. The interested reader will find brief notes on further applications in Appendix B.

31.1 Formal groups in algebraic topology

All formal group laws in this subsection will be commutative and one dimensional.

■ (31.1.1) **Complex oriented cohomology theories** Let h^* be a multiplicative cohomology theory defined, e.g., on the category of finite CW-complexes (with commutative (in the graded sense) multiplication). The theory h^* is said to be *complex oriented* if one has Euler classes $e^h(L) \in h^2(S)$ for every complex line bundle L over a CW-complex S such that (i) e^h is natural for bundle maps and (ii) $h^*(\mathbf{CP}^n) \simeq h^*(pt)[u]/u^{n+1}$ where $u = e^h(\xi_n)$, where ξ_n is the canonical line bundle over $\mathbf{CP}^n$ (whose fiber in $x \in \mathbf{CP}^n$ "is" the line represented by x). Here $\mathbf{CP}^n$ is complex projective space of complex dimension n.

If one can work with $\mathbf{CP}^\infty$ as well, it is the same to specify an element $u^h \in h^2(\mathbf{CP}^\infty)$ such that $\tilde{h}^*(S^2)$ is free on one generator i^*u^h over $h(pt)$ where i: $S^2 = \mathbf{CP}^1 \to \mathbf{CP}^\infty$ is the canonical inclusion map. (Cf. [2, Part II, Section 2]; there u^h need not be in $h^2(\mathbf{CP}^\infty)$.)

Given a complex oriented cohomology theory (h^*, e^h), one can define Chern classes $(c_1 = e^h)$ and multiplicative Thom classes in h (cf. [133]).

■ (31.1.2) **The formal group law $F_h(X, Y)$ of a complex oriented cohomology theory** Let (h^*, e^h) be a complex oriented cohomology theory.

Let L_1, L_2 be complex line bundles. Then we have (because $\mathbf{CP}^\infty$ is classifying for line bundles)

$$e^h(L_1 \otimes L_2) = \sum a_{ij} e^h(L_1)^i e^h(L_2)^j, \qquad a_{ij} \in h(pt)$$

and by the naturality of Chern classes the coefficients a_{ij} do not depend on L_1 and L_2, so that we find a well-determined power series in two variables X, Y

$$F_h(X, Y) = \sum a_{ij} X^i Y^i$$

which has the properties: (i) $F_h(X, 0) = X$ because $L_1 \otimes 1 \simeq L_1$, (ii) $F_h(X, Y) = F_h(Y, X)$ because $L_1 \otimes L_2 \simeq L_2 \otimes L_1$, (iii) $F_h(X, F_h(Y, Z)) = F_h(F_h(X, Y), Z)$ because $(L_1 \otimes L_2) \otimes L_3 \simeq L_1 \otimes (L_2 \otimes L_3)$. That is, $F_h(X, Y)$ is a formal group law over $h(pt)$, called the formal group law of the complex oriented cohomology theory (h^*, e^h).

■ (31.1.3) **Examples**

(i) Take $h^* = H^*$, ordinary cohomology, and let $u^H \in H^2(\mathbf{CP}^\infty)$ be the usual generator. The associated formal group law is then $F_H(X, Y) = X + Y$.

(ii) Take $h^* = K^*$, complex K-theory, with its usual Euler class. The associated formal group law is then $F_K(X, Y) = X + Y - wXY$, where w is the Bott periodicity element.

■ (31.1.4) **Complex cobordism** Let MU^* be complex cohordism cohomology. This is canonically oriented (cf. 34.1 for details). Let $m_n = (n+1)^{-1}[\mathbf{CP}^n]$ where $[\mathbf{CP}^n]$ denotes the class in $MU(pt)$ of the complex manifold $\mathbf{CP}^n$.

■ (31.1.5) **Theorem** The pair (MU^*, e^{MU}) is universal for complex oriented cohomology theories. That is, for every complex oriented cohomology theory (h^*, e^h), there is a unique (linear, degree preserving, multiplicative, and unit preserving) transformation of cohomology theories ϑ such that $\vartheta e^{MU} = e^h$.

■ (31.1.6) **Theorem** $F_{MU}(X, Y)$ over $MU(pt)$ is a universal one dimensional commutative formal group law.

■ (31.1.7) **Theorem** The logarithm $\log_{MU}(X)$ of $F_{MU}(X, Y)$ is equal to

$$\log_{MU}(X) = \sum_{n=0}^{\infty} m_n X^{n+1} = \sum_{n=0}^{\infty} \frac{[\mathbf{CP}^n]}{n+1} X^{n+1}$$

■ (31.1.8) **Cohomology operations in MU^*** One now uses theorem (31.1.5) to construct lots of cohomology operations as follows. Afflicting MU^* with coefficients, we define a cohomology theory $MU^*[t]$ by $MU^*[t](S, A) = MU^*(S, A)[t]$ where t is short for $t = (t_1, t_2, \ldots)$. Now let $\alpha(X)$ be the power series defined by

$$\alpha^{-1}(X) = \sum_{i=1}^{\infty} t_{i-1} X^i, \qquad t_0 = 1$$

Define a new Euler class for $MU^*[t]$ by $e^{MU[t]}(L) = \alpha(e^{MU}(L))$ (take degree $t_i = -2i$). Then Theorem (31.1.5) says that there is a cohomology transformation (the big Landweber–Novikov operation)

$$s_t: MU^* \to MU^*[t]$$

taking e^{MU} into $e^{MU[t]}$. Let $\mathbf{n}$ run through all multi-indices with finite support $\mathbf{n}: \mathbf{N} \to \mathbf{N} \cup \{0\}$. Let $x \in MU^*(S)$. Write

$$s_t(x) = \sum_{\mathbf{n}} s_{\mathbf{n}}(x) t^{\mathbf{n}}$$

to obtain the Landweber–Novikov operations $s_{\mathbf{n}}$.

■ (31.1.9) ***BP* cohomology** Choose a prime number p. Now let $\alpha(X)$ be the power series over $MU(pt) \otimes \mathbf{Z}_{(p)} = MU_{(p)}(pt)$ such that

$$\alpha(\log_{MU}^{-1}(X)) = (\textstyle\sum m_{p^n - 1} X^{p^n})^{-1}$$

(i.e., $\alpha(X)$ is the canonical isomorphism making $F_{MU}(X, Y)$ p-typical). Let $MU^*_{(p)}(M, A) = MU^*(M, A) \otimes \mathbf{Z}_{(p)}$ and complex orient $MU^*_{(p)}$ by $e^{MU_{(p)}}(L) = \alpha(e^{MU}(L))$. Then by Theorem (31.1.5) we find (after localization) a cohomology transformation

$$\vartheta_p: MU^*_{(p)} \to MU^*_{(p)}$$

which turns out to be idempotent (essentially because the canonical way of making a p-typical group law p-typical is doing nothing). The image of ϑ_p is a new complex oriented cohomology theory BP^* (Brown–Peterson cohomology) whose associated formal group law is p-typical and universal for p-typical formal group laws. Moreover, (BP, e^{BP}) is universal for complex oriented cohomology theories whose associated formal group law is p-typical.

■ (31.1.10) **Generators for $MU(pt)$ and $BP(pt)$** In Chapter I, Sections 3, 5, we constructed a universal formal group law $F_U(X, Y)$ over $\mathbf{Z}[U_2, U_3, \ldots]$ and a p-typically universal formal group law $F_V(X, Y)$ over $\mathbf{Z}[V_1, V_2, \ldots]$. Because $F_{MU}(X, Y)$ is universal and $F_{BP}(X, Y)$ is p-typically universal, there exist isomorphisms $\phi: \mathbf{Z}[U] \xrightarrow{\sim} MU(pt)$, $\psi: \mathbf{Z}_{(p)}[V] \to BP(pt)$ that take $F_U(X, Y)$ into $F_{MU}(X, Y)$ and $F_V(X, Y)$ into $F_{BP}(X, Y)$. Let $u_i = \phi(U_{i+1})$, $v_i = \psi(V_i)$. Then this gives us polynomial generators $u_1, u_2, \ldots$ for $MU(pt)$ and $v_1, v_2, \ldots$ for $BP(pt)$. Moreover, because we have reasonable formulas for the logarithms $f_U(X)$ and $f_V(X)$ and because we know the logarithms $\log_{MU}(X)$ and $\log_{BP}(X)$, one finds formulas for the $u_1, u_2, \ldots$ and $v_1, v_2, \ldots$ in terms of the complex projective spaces. In the case of BP these are

$$(31.1.11) \qquad p\dot{m}_{p^n - 1} = v_n + m_{p-1} v_{n-1}^p + \cdots + m_{p^n - 1 - 1} v_1^{p^n - 1}$$

which is also a description of the Hurewicz map

$$BP(pt) = \pi_*(BP) \to H_*(BP) = Z_{(p)}[m_{p-1}, m_{p^2-1}, \ldots]$$

■ (31.1.12) **Cohomology operations for BP^*** Let $\alpha_{v,t}(X)$: $F_v(X, Y) \to F_{v,t}(X, Y)$ be the universal isomorphism of p-typical formal group laws discussed in Section 19.2 of Chapter IV. Define Euler classes for $BP^*[t]$ by $e^{BP[t]}(L) = \alpha_{v,t}(e^{BP}(L))$. This makes $BP^*[t]$ complex oriented, and the associated formal group law is $F_{v,t}$, which is p-typical. By the universality of (BP^*, e^{BP}) (cf. (31.1.9)), there is a cohomology transformation

$$r_t: BP^* \to BP^*[t]$$

taking e^{BP} into $e^{BP[t]}$. One writes again $r_t = \sum_E r_E t^E$, where E runs through all multi-indices with finite support E: $\mathbf{N} \to \mathbf{N} \cup \{0\}$, to obtain the Quillen–Landweber–Novikov operations r_E for BP-cohomology.

Now because r_t takes e^{BP} into $e^{BP[t]}$, we must have $r_t(pt)_* F_v(X, Y) = F_{v,t}(X, Y)$, which means that (under the identification $V_i \mapsto v_i$, $T_i \mapsto t_i$), $r_t(pt)$ becomes the localized in p version of the homomorphism η_R: $\mathbf{Z}[V] \to \mathbf{Z}[V; T]$, $V_n \mapsto \bar{V}_n$ which we studied in some detail in Sections 19.3 and 22 of Chapter IV. As an immediate result one obtains, e.g.,

$$r_{\Delta_i}(v_n) = -v_{n-i}^{p^i} \mod(p, v_1) \tag{31.1.13}$$

where $\Delta_i = (0, \ldots, 0, 1, 0, \ldots)$ with the 1 in the ith spot.

■ (31.1.14) What has been briefly sketched above by no means exhausts the fun one can have in playing with formal group laws in algebraic topology; cf. Appendix B.4 for some more brief remarks.

31.2 Tate modules

■ (31.2.1) **The group $F(K_{sc})$** Let A be a complete discrete valuation ring without zero divisors with maximal ideal $\mathfrak{m}$ and quotient field K. Let K_{sc} be a separable closure of K and $\mathfrak{m}(K_{sc})$ the maximal ideal of its ring of integers $A(K_{sc})$. Let $F(X, Y)$ be an n-dimensional formal group law over A and let x, $y \in \mathfrak{m}(K_{sc})^n$ be two n-tuples of elements of $\mathfrak{m}(K_{sc})$. Then $F(x, y)$ converges to an element $z = x +_F y$ in $\mathfrak{m}(K_{sc})^n$. We shall denote the resulting abelian group by $F(K_{sc})$. Similarly one has of course the abelian groups $F(L)$ for intermediate extensions $K \subset L \subset K_{sc}$.

■ (31.2.2) **Theorem** Let $N \subset F(K_{sc})$ be a finite subgroup, where $F(X, Y)$ is a one dimensional formal group law over A. Let L/K be a finite extension such that $N \subset F(L)$. Then there exists a formal group law $G(X, Y)$ over $A(L)$ which is the quotient of $F(X, Y)$ by N. (For a more precise and also stronger statement, cf. Theorem (35.2.1).)

■ (31.2.3) **The Tate module** Let $\Lambda(F) \subset F(K_{sc})$ be the torsion subgroup of $F(K_{sc})$. One defines

$$T(F) = \mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \Lambda(F)) \tag{31.2.4}$$

$$V(F) = \mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p, \Lambda(F)) \tag{31.2.5}$$

The natural quotient map $\mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p$ induces an inclusion $T(F) \subset V(F)$. If $F(X, Y)$ is of finite height h, then $V(F)$ is a vector space of dimension h over $\mathbf{Q}_p$ and $T(F)$ is a lattice in $V(F)$.

The following is a (weak) consequence of a theorem of Tate.

■ (31.2.6) **Proposition** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism between finite height, one dimensional formal group laws over A. Then $\alpha(X)$ is an isomorphism iff $T(\alpha)$ is an isomorphism.

■ (31.2.7) **Isogenies** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a nonzero homomorphism of one dimensional, finite height formal group laws over A (i.e., $\alpha(X)$ is an isogeny). Then $\alpha(X)$ induces homomorphisms $T(\alpha)$: $T(F) \to T(G)$ and an isomorphism $V(\alpha)$: $V(F) \to V(G)$. Taking $V(\alpha)^{-1}T(G) \supset V(F)$, one finds a lattice in $V(F)$ that contains $T(F)$ and one shows that there is a 1–1 correspondence between such superlattices L of $T(F)$ in $V(F)$ and isogenies with source $F(X, Y)$. Conversely, there is also a one–one correspondence between sublattices of $T(F)$ in $V(F)$ and isogenies with target $F(X, Y)$; cf. Theorem (35.4.2) for a more precise statement.

■ (31.2.8) **Formal group laws with pregiven END ring** The isogeny theorem sketched above gives one a very strong hold on endomorphisms and homomorphisms of one dimensional formal group laws over (finite extensions of) A. Among other things one shows (with the Lubin–Tate formal group laws as an intermediate construction) that every order $\mathcal{O}$ over $\mathbf{Z}_p$ (contained in $A(K_{sc})$) arises as the absolute endomorphism ring of some one dimensional formal group law over a finite extension $A(L)$ of A (Theorem (35.5.9)).

31.3 Local class field theory

Let A be the ring of integers of a complete discrete valuation field K, with finite residue field k of q elements. Let π be a uniformizing element of K. Let $F_e(X, Y)$ be any Lubin–Tate formal A-module over A with $\pi(F_e) = \pi$. (The simplest such formal group law has logarithm $X + \pi^{-1}X^q + \pi^{-2}X^{q^2} + \cdots$). Let $\Lambda = \Lambda(F_e)$ be the torsion subgroup of $F_e(K_{sc})$, and let $L_\pi = K_\pi(\Lambda)$. Then one has

■ (31.3.1) **Theorem**

(i) $\Lambda \simeq K/A$ as an A-module.

(ii) L_π is a maximal totally ramified abelian extension of K.

(iii) For each $\tau \in \mathrm{Gal}(L_\pi/K)$, there is a unique $u_\tau \in U(K)$ such that $\tau\lambda = [u_\tau](\lambda)$ for all $\lambda \in \Lambda$. (Here $[u](X)$ is, as usual, the unique endomorphism over A of the formal A-module $F_e(X, Y)$ such that $[u](X) \equiv uX$ mod degree 2.)

(iv) $\tau \mapsto u_\tau$ is an isomorphism $\mathrm{Gal}(L_\pi/K) \to U(K)$.

■ (31.3.2) Now let K_{nr} be the maximal unramified extension of K contained in

K_{sc}. One now defines a homomorphism r: $K^* \to \mathrm{Gal}(K_{nr} \cdot L_\pi/K)$ where $K^* = K\backslash\{0\}$ and where the dot denotes "compositum," as follows

$$\pi \mapsto \sigma \in \mathrm{Gal}(L_\pi \cdot K_{nr}/L_\pi) \subset \mathrm{Gal}(K_{nr} \cdot L_\pi/K)$$

$$U(K) \ni u \mapsto \tau(u^{-1}) \in \mathrm{Gal}(L_\pi \cdot K_{nr}/K_{nr}) \in \mathrm{Gal}(K_{nr} \cdot L_\pi/K)$$

where $\tau(u^{-1})$ is the unique element of $\mathrm{Gal}(L_\pi/K)$ corresponding to u^{-1} via (iii) and (iv) of Theorem (31.3.1), and where σ is the Frobenius substitution; i.e., $\sigma(x) \equiv x^q \bmod \mathfrak{m}(L_\pi)$ for all $x \in A(L_\pi)$.

■ (31.3.3) **Theorem**

(i) $L_\pi \cdot K_{nr}$ is the maximal abelian extension of K (in K_{sc}).
(ii) r: $K^* \to \mathrm{Gal}(K^{ab}/K)$ is the reciprocity homomorphism.

31.4 The formal minimal model of an elliptic curve

■ (31.4.1) **Dirichlet series with Euler products** Let $L(s)$ be a Dirichlet series over $\mathbf{Z}$ admitting an Euler factorization

$$\sum_{n=1}^{\infty} a(n)n^{-s} = L(s) = \prod_p (1 - a_p p^{-s} + b_p p^{1-2s})^{-1}, \qquad a(n), a_p, b_p \in \mathbf{Z}$$

Let $f_L(X)$ be the power series

$$f_L(X) = \sum_{n=1}^{\infty} n^{-1} a(n) X^n$$

Then the functional equation lemma says that $f_L(X)$ is the logarithm of a one dimensional formal group law $F_L(X, Y)$ over $\mathbf{Z}$.

■ (31.4.2) **Formal minimal model** Let E be an elliptic curve over $\mathbf{Q}$. Take a minimal (affine) model (F): $Y^2 + c_1 XY + c_3 Y = X^3 + c_2 X^2 + c_4 X + c_6$ of E over $\mathbf{Z}$. Take $t = X/Y$ as a local parameter at the zero element of the group law of E. Expanding the group law E as a power series in t_1, t_2, one obtains a power series $G_E(t_1, t_2)$ which is a formal group law over $\mathbf{Z}$ (the formal minimal model of E). If $g_E(X)$ is the logarithm of $G_E(X, Y)$, then

$$\frac{dg_E}{dX}(z) = \sum_{n=1}^{\infty} \beta(n) z^{n-1}$$

where $\sum_{n=1}^{\infty} \beta(n) z^{n-1}\, dz$ is the power series development in $z = X/Y$ of the invariant differential $\omega = dX(2Y + c_1 X + c_3)^{-1}$.

■ (31.4.3) **Theorem** The formal group laws $G_E(X, Y)$ and $F_L(X, Y)$ are strictly isomorphic over $\mathbf{Z}$ where $L(s)$ is the global L-series of E defined by

$$L(s) = \prod_p (1 - a_p p^{-s} + b_p p^{1-2s})^{-1}$$

where for the primes where E has good reduction $1 - a_p p^{-s} + b_p p^{1-2s}$ is the denominator of the zeta function of the reduction of E over $\mathbf{F}_p$.

Given this theorem of Honda, an easy application of the functional equation lemma gives Atkin–Swinnerton–Dyer congruences

$$\beta(np) - a_p\beta(n) + pb_p\beta(n//p) \equiv 0 \mod p^s \tag{31.4.4}$$

if $n \equiv 0 \mod p^{s-1}$, $s \in \mathbf{N}$. (Here $n//p = p^{-1}n$ if $p \mid n$ and $n//p = 0$ if $p \nmid n$.)

32 Local Class Field Theory

In this section K is a discretely valued complete field with finite residue field k. We are going to give an explicit description of the maximal abelian extension of K and of the reciprocity homomorphism r: $K^* \to \mathrm{Gal}(K_{\mathrm{ab}}/K)$. The field K may be of characteristic zero or of characteristic $p > 0$.

32.1 Construction of the extension L_π

■ (32.1.1) **Some notation** A or $A(K)$ is the ring of integers of K; $\mathfrak{m}(K)$ is the maximal ideal of $A(K)$, and $k = A(K)/\mathfrak{m}(K)$ is the residue field of K. Further, p is the characteristic of K and q the number of elements of k, $q = p^r$. We use $U(K)$ to denote the units of K, i.e., $U(K) = A(K)^*$, the invertible elements of $A(K)$ and $U^n(K) = \{x \in U(K) \mid x \equiv 1 \mod \mathfrak{m}(K)^n\}$. The symbol π or π_K denotes a uniformizing element of K, i.e., $\mathfrak{m}(K) = \pi A(K)$ and v_K: $K \to \mathbf{Z} \cup \{\infty\}$ is the normalized exponential valuation on K, i.e., $v_K(\pi) = 1$.

Let Ω be some fixed algebraically closed extension of K. Then if L/K is an algebraic extension, $\Gamma(K, L \to \Omega)$ denotes the various K embeddings of L in Ω. The symbols $A(L)$, $\mathfrak{m}(L)$, $U(L)$ have the obvious meanings; and if L/K has finite ramification $U^n(L)$, v_L, π_L also make sense. If L/K is Galois, $\mathrm{Gal}(L/K)$ denotes the Galois group.

■ (32.1.2) Fix a uniformizing element $\pi \in A(K)$ and let $\mathscr{E}_\pi$ be the set of all power series $e(X)$ such that $e(X) \equiv X^q \mod \pi$ and $e(X) \equiv \pi X \mod(\text{degree } 2)$. The simplest element of $\mathscr{E}_\pi$ is $X^q + \pi X$. We recall that for every $e(X) \in \mathscr{E}_\pi$, there is a unique formal A-module $F_e(X, Y)$ over A such that $[\pi]_e(X) = e(X)$ (cf. Chapter I, Section 8.1) and that these formal A-modules are strictly isomorphic for varying $e(X) \in \mathscr{E}_\pi$.

The A-height of $F_e(X, Y)$ is 1 because $[\pi]_e(X) = e(X)$; cf. Chapter I, Theorem (8.1.5).

■ (32.1.3) **The modules $M_e(K_{\mathrm{sc}})$, T_e, Λ_e** Let K_{sc} be a separable closure of K, and $\mathfrak{m}(K_{\mathrm{sc}})$ be the maximal ideal of $A(K_{\mathrm{sc}})$. The formal group law $F_e(X, Y)$ defines via $x +_e y = F_e(x, y)$ a new abelian group structure on $\mathfrak{m}(K_{\mathrm{sc}})$ and $ax = [a]_e(x)$ defines an A-module structure on this group. This A-module is

denoted $M_e(K_{sc})$. With $\Lambda_{e,m}$ we denote the submodule consisting of all elements λ such that $[\pi^m]_e(\lambda) = 0$, and $\Lambda_e = \bigcup_m \Lambda_{e,m}$; i.e., Λ_e is the A-torsion submodule of $M_e(K_{sc})$. The map $[\pi]_e$ takes $\Lambda_{e,m}$ into $\Lambda_{e,m-1}$ giving us a projective system of A-modules and we define

$$T_e = \varprojlim \Lambda_{e,m} \tag{32.1.4}$$

■ (32.1.5) **The extension L_π** Let $L_{\pi,e,m}$ be the extension field of K generated by the elements of $\Lambda_{e,m}$. Because $F_e(X, Y)$ and $F_{\bar{e}}(X, Y)$ are strictly isomorphic formal A-modules over A (cf. Chapter I, Theorem (8.1.5)), we have that $L_{\pi,e,m} = L_{\pi,\bar{e},m}$, so we can simply write $L_{\pi,m}$. By definition $L_{\pi,m}$ is Galois over K. Let $L_\pi = \bigcup_m L_{\pi,m}$.

■ (32.1.6) **Theorem** Let π be a uniformizing element of K and let $e \in \mathscr{E}_\pi$. Then:

(i) The A-module $M_e(K_{sc})$ is divisible (i.e., if $x \in M_e(K_{sc})$, then there exists a $y \in M_e(K_{sc})$ such that $[\pi]_e y = x$.

(ii) For each $m \in \mathbf{N}$, the A-module $\Lambda_{e,m}$ is isomorphic to $A/\pi^m A$ and T_e is isomorphic to A.

(iii) Λ_e is isomorphic to K/A as an A-module.

(iv) For each $\tau \in \mathrm{Gal}(L_\pi/K)$, there is a unique $u \in U(K)$ such that $\tau\lambda = [u]_e\lambda$ for all $\lambda \in \Lambda_e$.

(v) The map $\tau \mapsto u$ of (iv) above is an isomorphism of $\mathrm{Gal}(L_\pi/K)$ onto $U(K)$ and the kernel of the composed map $\mathrm{Gal}(L_\pi/K) \to U(K) \to U(K)/U^m(K)$ is $\mathrm{Gal}(L_\pi/L_{\pi,m})$.

(vi) The element π is a norm from $L_{\pi,n}$ for all $m \in \mathbf{N}$.

Proof In view of the formal A-module isomorphisms $F_e(X, Y) \simeq F_{\bar{e}}(X, Y)$ for all $e, \bar{e} \in \mathscr{E}_\pi$, we can assume that $e(X) = X^q + \pi X$. Recall that $[\pi]_e(X) = e(X)$. Let $x \in M_e(K_{sc})$. The polynomial $X^q + \pi X - x$ has all its roots in the maximal ideal of the algebraic closure of K. Also the roots are simple because $qX^{q-1} + \pi$ has no roots in the maximal ideal of the algebraic closure of K. It follows that all roots are in $\mathfrak{m}(K_{sc})$ proving that $M_e(K_{sc})$ is divisible. (Recall that K may be of characteristic $p > 0$.)

The A-module $\Lambda_{e,1}$ consists of the roots of $X^q + \pi X = 0$ and is therefore a k-vector space of dimension 1. Further, Λ_e as the A-torsion submodule of $M_e(K_{sc})$ is also divisible, statements (ii) and (iii) of the theorem now follow, where for the statement concerning T_e the completeness of A is essential. (NB there is nothing canonical about the isomorphisms of A-modules $T_e \simeq A$ and $\Lambda_e \simeq K/A$.)

Now let $\tau \in \mathrm{Gal}(L_\pi/K)$. Then τ induces an automorphism of the A-module T_e (because $\tau_*([\pi]_e(X)) = [\pi]_e(X)$) and the only A-module automorphisms of $T_e \simeq A$ are of the form $z \mapsto uz$ for some unit $u \in U(K)$. This proves (iv). The assignment $\tau \mapsto u$ of (iv) is injective because L_π is generated over K by Λ_e.

Moreover, if $\tau \mapsto u \in U^m(K)$, then multiplication with u is the identity on $\Lambda_{e,m} \simeq A/\pi^m A$ so that $\tau \mapsto u \in U^m(K)$ is equivalent to $\tau \in \mathrm{Gal}(L_\pi/L_{\pi,m})$ because inversely if $\tau \in \mathrm{Gal}(L_\pi/L_{\pi,m})$, then τ is the identity on $\Lambda_{e,m} \subset L_{\pi,m}$. Thus $\tau \mapsto u$ induces an injection

$$\mathrm{Gal}(L_{\pi,m}/K) \to U(K)/U^{(m)}(K) \tag{32.1.7}$$

Now consider $e^{(m)}(X) = e(e(\cdots(e(X)\cdots)))$ (mth iterate of $e(X)$) which is divisible by $e^{(m-1)}(X)$ since $e(X)$ is divisible by X. The quotient $e^{(m)}(X)/e^{(m-1)}(X)$ is of the form

$$X^{(q-1)q^{m-1}} + \pi(\cdots) + \pi \tag{32.1.8}$$

which is an Eisenstein polynomial and hence irreducible. Now $L_{\pi,m}$ contains $\Lambda_{e,m}$ which is the set of all roots of $e^{(m)}(X)$. It follows that $[L_{\pi,m}: K] \geq (q-1)q^{m-1}$ which is the number of elements of $U(K)/U^{(m)}(K)$. So, (32.1.7) being injective, it is also surjective and hence an isomorphism, which, since both $U(K)$ and $\mathrm{Gal}(L_\pi/K)$ are compact, also proves (v). Finally, (vi) follows because if λ_m is a root of (32.1.8), then $N_{L_{m/\pi}/K}(-\lambda_m) = \pi$ (where $N_{L/K}$ denotes the norm mapping $L \to K$).

32.2 The reciprocity law of local class field theory

■ (32.2.1) We recall that the reciprocity law of local class field theory is a homomorphism r: $K^* \to \mathrm{Gal}(K_{\mathrm{ab}}/K)$ such that for every abelian extension L/K, r induces an isomorphism $K^*/N_{L/K}L^* \simeq \mathrm{Gal}(L/K)$.

■ (32.2.2) Let K_{nr} be the maximal unramified extension of K (within Ω) and let $\sigma \in \mathrm{Gal}(K_{nr}/K)$ be the Frobenius substitution (i.e., $\sigma a \equiv a^q \bmod \pi$ for all $a \in A(K_{nr})$). The abelian extension L_π/K of Section 32.1 is totally ramified, so L_π/K and K_{nr}/K are linearly disjoint. We now define a homomorphism $K^* \to \mathrm{Gal}(L_\pi \cdot K_{nr}/K)$ as follows (where $L_\pi \cdot K_{nr}$ is the compositum of L_π and K_{nr}):

$$s_\pi: K \to \mathrm{Gal}(L_\pi \cdot K_{nr}/K)$$

$$U(K) \ni u \mapsto s_\pi(u) \in \mathrm{Gal}(L_\pi \cdot K_{nr}/K_{nr}) \subset \mathrm{Gal}(L_\pi \cdot K_{nr}/K)$$

$$s_\pi(u)(\lambda) = [u^{-1}]_e(\lambda) \quad \text{for all} \quad \lambda \in \Lambda_e \tag{32.2.3}$$

$$\pi \mapsto \sigma \in \mathrm{Gal}(L_\pi \cdot K_{nr}/L_\pi) \subset \mathrm{Gal}(L_\pi \cdot K_{nr}/K)$$

■ (32.2.4) **Theorem** The field $L_\pi \cdot K_{nr}$ and the homomorphism s_π do not depend on the choice of π.

Proof The field $L_{\hat{\pi}}$ is defined in terms of a formal group law $F_{\hat{e}}$ defined by an $\hat{e}(X) \in \mathscr{E}_{\hat{\pi}}$. So we need to compare Lubin–Tate formal group laws belonging to different uniformizing elements. In fact what we need is Proposition (8.3.9) of Chapter I, which says that if $e(X) \in \mathscr{E}_\pi$, $\hat{e}(X) \in \mathscr{E}_{\hat{\pi}}$, then the formal

A-modules $F_e(X, Y)$ and $F_{\hat{e}}(X, Y)$ are isomorphic over $A(\hat{K}_{nr})$, the ring of integers of the completion of the maximal unramified extension of K. More precisely, Proposition (8.3.8) of Chapter I asserts the existence of a power series $\alpha(X) \in A(\hat{K}_{nr})[\![X]\!]$ such that

$$\sigma_* \alpha(X) = \alpha([u]_e(X)), \qquad \text{where} \quad \hat{\pi} = u\pi, \quad u \in U(K)$$

$$\alpha(F_e(X, Y)) = F_{\hat{e}}(\alpha X, \alpha Y), \qquad \alpha([a]_e(X)) = [a]_{\hat{e}}(\alpha(X)) \tag{32.2.5}$$

$$\alpha(X) \equiv \varepsilon X \mod(\text{degree } 2), \qquad \text{where} \quad \varepsilon \in U(\hat{K}_{nr}) \text{ is such that } \sigma\varepsilon/\varepsilon = u$$

We can take $e(X) = X^q + \pi X$, $\hat{e}(X) = X^q + \hat{\pi}X$. Let $\lambda \in \Lambda_{e,m}$, then by (32.2.5) we have that $[\hat{\pi}^m]_{\hat{e}}(\alpha(\lambda)) = 0$, and $\alpha(\lambda) \in \hat{K}_{nr} \cdot L_\pi$. Now $[\hat{\pi}^m]_{\hat{e}}(X) = \hat{e}^{(m)}(X)$ so that $\alpha(\lambda)$ is algebraic over K, and it follows that $\alpha(\lambda) \in K_{nr} \cdot L_\pi$ by Lemma (32.2.6) below. Since $\alpha(X)$ is an isomorphism, this gives that $\lambda \mapsto \alpha(\lambda)$ is a bijection $\Lambda_e \to \Lambda_{\hat{e}}$ so that $\Lambda_{\hat{e}} \subset K_{nr} \cdot L_\pi$. This proves that $L_{\hat{\pi}} \subset K_{nr} \cdot L_\pi$, which by symmetry proves the first part of the theorem.

We now show that $s_\pi(\hat{\pi}) = s_{\hat{\pi}}(\hat{\pi})$ (for all $\hat{\pi}$). This suffices to prove the second part of the theorem because the uniformizing elements generate K^* as an abelian group. Now on the subfield $K_{nr} \subset K_{nr} \cdot L_\pi$ both $s_{\hat{\pi}}(\hat{\pi})$ and $s_\pi(\hat{\pi})$ induce the Frobenius substitution σ. So it remains to show only that $s_\pi(\hat{\pi})(\hat{\lambda}) = s_{\hat{\pi}}(\hat{\pi})(\hat{\lambda})$ for all $\hat{\lambda} \in \Lambda_{\hat{e}}$. Let $\hat{\pi} = u\pi$, then

$$s_\pi(\hat{\pi}) = s_\pi(u) s_\pi(\pi)$$

Let $\lambda \in \Lambda_e$ be such that $\alpha(\lambda) = \hat{\lambda}$. Then we have

$$\begin{aligned} s_\pi(\hat{\pi})(\hat{\lambda}) &= s_\pi(u)(\sigma(\alpha(\lambda))) = s_\pi(u)(\alpha[u]_e(\lambda)) \\ &= \alpha([u]_e(s_\pi(u)(\lambda))) = \alpha([u]_e([u^{-1}]_e(\lambda))) \\ &= \alpha(\lambda) = \hat{\lambda} \end{aligned}$$

where we have used that $s_\pi(\pi) = \sigma \in \mathrm{Gal}(L_\pi \cdot K_{nr}/K_{nr})$. Thus $s_\pi(\hat{\pi})$ is the identity on $L_{\hat{\pi}}$. Now $s_{\hat{\pi}}(\hat{\pi}) = id$ on $L_{\hat{\pi}}$ by definition, and we have proved the second part of theorem modulo Lemma (32.2.6).

■ (32.2.6) **Lemma** Let E be an algebraic extension of K and let $x \in \hat{E}$, the completion of E. If x is separable algebraic over K, then $x \in E$.

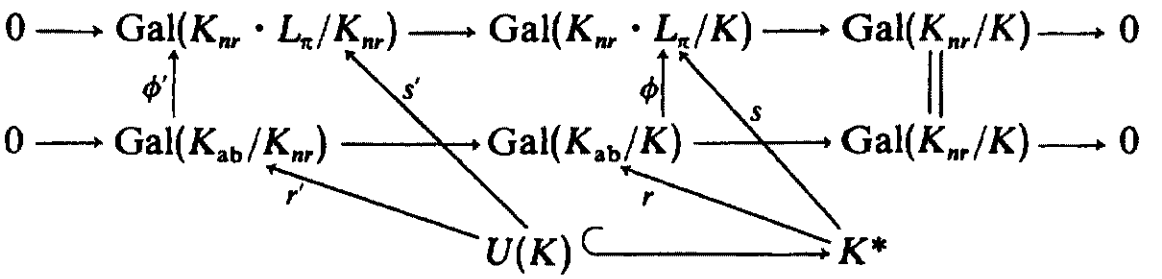
Proof Let E_{sc} be the separable closure of E and $\bar{E}$ the closure of E in E_{sc}. Then $x \in \bar{E}$. Now let $\tau \in \mathrm{Gal}(E_{sc}/E)$, then τ is continuous, so τ is also the identity on $\bar{E}$; hence $\mathrm{Gal}(E_{sc}/E) = \mathrm{Gal}(E_{sc}/\bar{E})$ which by Galois theory says that $E = \bar{E}$; so that $x \in E$.

■ (32.2.7) **Remark** Another way to prove the existence of an $\alpha(X)$ such that (32.2.5) holds is as follows. Both $F_e(X, Y)$ and $F_{\hat{e}}(X, Y)$ are formal A-modulo of A-height 1 over $A(\hat{K}_{nr})$, so their reductions are isomorphic over the residue

field of $A(\hat{K}_{nr})$ (they are of equal height (cf. Chapter IV); but their A-height is 1, so there are no formal moduli and it follows that $F_e(X, Y)$ and $F_{\hat{e}}(X, Y)$ are isomorphic over $A(\hat{K}_{nr})$). Let $\alpha(X)$ be the isomorphism. Because $F_e(X, Y)$ and $F_{\hat{e}}(X, Y)$ are invariant under σ_*, it follows that $\alpha^{-1}(X) \cdot \sigma_*(\alpha(X))$ is an automorphism of $F_e(X, Y)$ over $A(\hat{K}_{nr})$ which by Chapter IV, (20.1.21) means that $\alpha^{-1}(X) \cdot \sigma_*(\alpha(X)) = [u]_e(X)$ for some $u \in U(K)$.

■ (32.2.8) **Theorem** $K_{nr} \cdot L_\pi$ is the maximal abelian extension of K and $s = s_\pi$ is the reciprocity law homomorphism r.

Proof $K_{nr} \cdot L$ is an abelian extension, hence a subextension of K_{ab}. The maximal unramified subextension of both is K_{nr}, so we have a diagram of Galois groups



Now let us show first that $\phi r = s$. Let $\pi \in K$ be a uniformizing element, then $r(\pi)$ is σ on K_{nr}/K and $r(\pi) = id$ on L_π because π is a norm from every $L_{\pi,m}$ (cf. (32.2.1)). On the other hand, by definition $s = s_\pi$, so that $s_\pi(\pi)$ is σ on K_{nr} and identity on L_π. That is, $r(\pi) = s(\pi)$ on $L_\pi \cdot K_{nr}$. This holds for all π hence $\phi r = s$. Now s' and r' are both isomorphisms (cf. Theorem (32.1.6)(v)), so ϕ' is an isomorphism and hence ϕ also, which proves by Galois theory that $K_{ab} = K_{nr} \cdot L_\pi$.

32.3 The case $K = \mathbf{Q}_p$

Let $K = \mathbf{Q}_p$. Then we can take $\pi = p$ and for $e(X) \in \mathscr{E}_p$ we can take $e(X) = (X + 1)^p - 1$. Then

$$e^{(m)}(X) = (X + 1)^{p^m} - 1$$

so that L_p is the extension field of $K = \mathbf{Q}_p$ generated by the p^mth roots of unity $m = 1, 2, 3, \ldots$. The Lubin–Tate formal group law of this $e(X)$ is

$$F_e(X, Y) = X + Y + XY$$

because $e(F_e(X, Y)) = (1 + F_e(X, Y))^p - 1 = (X + 1)^p(Y + 1)^p - 1 = e(X) + e(Y) + e(X)e(Y)$. Also the endomorphisms $[a]_e$ for $a \in \mathbf{Z}_p$ are easy to calculate. One has

$$[a]_e(X) = (1 + X)^a - 1 = \sum_{i=1}^{\infty} \binom{a}{i} X^i$$

(which makes sense in $\mathbf{Z}_p[\![X]\!]$). As a result one obtains the following description of the reciprocity homomorphism for the case of $\mathbf{Q}_p$:

Let $a = p^t u \in \mathbf{Q}_p^*$, $u \in U(\mathbf{Q}_p)$. Then $r(a)$ acts as σ^t on the maximal unramified extension of $\mathbf{Q}_p$ and on the totally ramified extension generated by the p^mth roots of unity $r(a)$ acts as $\zeta_{p^n} \mapsto \zeta_{p^n}^{u^{-1}}$. (Note that this makes sense because if $u^{-1} \equiv v \bmod p^n$, then $\zeta_{p^n}^{u^{-1}} = \zeta_{p^n}^{v}$ so that we only need a finite chunk of the p-adic development of u^{-1} to calculate $\zeta_{p^n}^{u^{-1}}$.)

32.4 On the Šafarevič mapping

■ (32.4.1) Let K be as in (32.1.1). Let L/K be a finite Galois extension and let L_{ab}/L be the maximal abelian extension of L. Then L_{ab}/K is a Galois extension (if $\tau \in \Gamma(K, L_{ab} \to \Omega)$; then because $\tau(L) = L$, we have an abelian extension $\tau(L_{ab})/L$ that is contained in L_{ab}/L because L_{ab} is maximal). Let $\Gamma = \mathrm{Gal}(L_{ab}/K)$ and $G = \mathrm{Gal}(L/K)$. We have an exact sequence

$$0 \to \mathrm{Gal}(L_{ab}/L) \to \Gamma \to G \to 0 \tag{32.4.2}$$

Restricting the elements of Γ to K_{nr}, we obtain a surjection: $\Gamma \to \hat{\mathbf{Z}} = \mathrm{Gal}(K_{nr}/K)$. Let Γ' be the inverse image of $\mathbf{Z} \subset \hat{\mathbf{Z}}$ under this mapping.

Let r_L: $L^* \to \mathrm{Gal}(L_{ab}/L)$ be the reciprocity homomorphism for L. This homomorphism induces a map $H^2(G, L^*) \to H^2(G, \mathrm{Gal}(L_{ab}/L))$, and under this map the fundamental class of L in $H^2(G, L^*)$ goes into the class of the extension (32.4.2) ([348]; cf. (E.5.1)). Also Šafarevič gave an embedding of Γ' into a division algebra with center K and invariant n^{-1}, called a Šafarevič mapping, which on $\Gamma' \cap G(L_{ab}/L)$ is inverse to r_L (the field L is also embeddable in this division algebra; cf. Chapter IV, second intermezzo on division algebras (23.1.4)). Below we shall use Lubin–Tate formal group laws to construct such a Šafarevič mapping.

■ (32.4.3) **Proposition** Let $e(X) \in \mathscr{E}_{\pi_L}$, $\hat{e}(X) \in \mathscr{E}_{\pi_L}$, and let $F_e(X, Y)$ $F_{\hat{e}}(X, Y)$ be the corresponding Lubin–Tate formal A-modules and let T_e, $T_{\hat{e}}$ be the Tate modules of $F_e(X, Y)$, $F_{\hat{e}}(X, Y)$ (cf. (32.1.4)). Then for every $A(L)$-linear homomorphism ϕ: $T_e \to T_{\hat{e}}$, there is a unique homomorphism of formal A-modules over $A(\hat{L}_{nr})$ $\alpha(X)$: $F_e(X, Y) \to F_{\hat{e}}(X, Y)$ such that $\alpha(X)$ induces ϕ.

Proof We know that $T_e \simeq T_{\hat{e}} \simeq A(L)$ as $A(L)$ modules. We also know that $F_e(X, Y)$ and $F_{\hat{e}}(X, Y)$ are isomorphic as formal A-modules over $A(\hat{L}_{nr})$ (Theorem (8.3.8) of Chapter I). The result now follows from the fact that the ring of $A(L)$-linear endomorphisms of $A(L)$ is of course $A(L)$ and that

$$A(L)\text{-}\mathrm{End}_{A(L_{nr})}(F_e(X, Y)) = A(L) = A(L)\text{-}\mathrm{End}_{A(L_{nr})}(F_{\hat{e}}(X, Y))$$

This last fact is proved by (20.1.21) in Chapter IV if $A(L)$ is of characteristic

zero and is proved in exactly the same way if $A(L)$ is of characteristic $p > 0$. (In the latter case one uses that the formal $A(L)$-module endomorphisms of $\hat{G}_a(X, Y)$ over $\hat{L}_{nr}$ are necessarily of the form aX, $a \in A(\hat{L}_{nr})$, and then reasons as in (20.1.19); of course it is absolutely essential in the characteristic $p > 0$ case that we consider only formal $A(L)$ – module endomorphisms of $F_e(X, Y)$ and not all formal group law endomorphisms.)

■ (32.4.4) Fix some $e(X) \in \mathscr{E}_{\pi_L}$ and let $F_e(X, Y)$ and T_e be the corresponding formal $A(L)$-module and Tate module. Fix some arbitrary $A(L)$-module isomorphism $T_e \xrightarrow{\sim} A(L)$. Transporting the $G = \mathrm{Gal}(L/K)$ module structure of $A(L)$ to T_e via this isomorphism, we obtain an $A(L)$-semilinear action of G on T_e, i.e., a homomorphism $\varepsilon\colon G \to \mathrm{Aut}_{\mathbf{Z}_p}(T_e)$ such that $\varepsilon(\tau)(ax) = \tau(a)\varepsilon(\tau)(x)$ for all $a \in A(L)$ and $x \in T_e$.

For each element $\gamma \in \Gamma$, consider the formal $A(L)$-module $\gamma_* F_e(X, Y)$ over $A(L)$ (this is the Lubin–Tate formal A-module associated to $\gamma_* e(X)$). We shall write $F_\gamma(X, Y)$ for $\gamma_* F_e(X, Y)$ and T_γ for its Tate module. Then γ induces of course an isomorphism $T_e \to T_\gamma$ which is $A(L)$-semilinear with the twist given by the image of γ under $\Gamma \to G$. Let ε_γ be the image of γ under $\Gamma \to G \to \mathrm{Aut}_{\mathbf{Z}_p}(T_e)$. Then $\varepsilon_\gamma \cdot \gamma^{-1}\colon T_\gamma \to T_e \to T_e$ is an $A(L)$-linear map, which by Proposition (32.4.3) comes from a unique homomorphism of formal A-modules $\alpha_\gamma(X)$: $F_\gamma(X, Y) \to F_e(X, Y)$.

■ (32.4.5) **Remark** Let $u \in U(L)$ and let $\tau = r(x) \in \mathrm{Gal}(L_{\mathrm{ab}}/L) \subset \Gamma$, then $\varepsilon_\tau = id$, so that $\alpha_\tau(X)$ is induced by τ^{-1}. By (21.1.6)(v) and the definition of the reciprocity homomorphism (32.2.3) we have $\tau\lambda = [u^{-1}]_e(\lambda)$ for all $\lambda \in \Lambda_e$, and it follows that $[u]_e(X)$ induces the $A(L)$-linear map $\tau^{-1}\colon \Lambda_e \to \Lambda_e$; i.e., in this case we have $\alpha_\tau(X) = [u]_e(X)$.

■ (32.4.6) **Lemma** $\alpha_{\gamma\delta}(X) = \alpha_\gamma(X) \circ \gamma_*(\alpha_\delta(X))$.

Proof We have on the Tate-module level

$$\varepsilon_{\gamma\delta} \circ (\gamma\delta)^{-1} = (\varepsilon_\gamma \circ \gamma^{-1}) \circ \gamma \circ (\varepsilon_\delta \circ \delta^{-1}) \circ \gamma^{-1}$$

and the lemma follows because of the uniqueness of the correspondence of Proposition (32.4.3) and because the map of Tate modules induced by $\gamma_*(\alpha(X))$ is of course $\gamma \circ \phi \circ \gamma^{-1}$ if ϕ is induced by the formal A-module homomorphism $\alpha(X)$. One has, so to speak, a "commutative diagram"

$$\begin{array}{ccc} \gamma_* F(X, Y) & \xrightarrow{\gamma_*\alpha(X)} & \gamma_* G(X, Y) \\ \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \gamma} \\ F(X, Y) & \xrightarrow{\alpha(X)} & G(X, Y) \end{array}$$

■ (32.4.7) **Construction of the Šafarevič mapping** s Let $\bar{\alpha}_\gamma(X)$ denote the power series over k_{sc}, the residue field of $\hat{L}_{nr}$, obtained by reducing all

coefficients of $\alpha_\gamma(X)$ mod $\mathfrak{m}(\hat{L}_{nr})$. Let $\gamma \in \Gamma'$ and let $v(\gamma) \in \mathbf{Z} \subset \mathrm{Gal}(K_{nr}/K)$ be its image. Then $X^{q^{v(\gamma)}}$ is a homomorphism of formal $A(K)$-modules $\bar{F}_e(X, Y) \to \bar{F}_\gamma(X, Y)$ over k_{sc} where $\bar{F}_e(X, Y)$ and $\bar{F}_\gamma(X, Y)$ are the reductions modulo $\mathfrak{m}(\hat{L}_{nr})$ of $F_e(X, Y)$ and $F_\gamma(X, Y)$. The composed map $\bar{\alpha}_\gamma(X) \circ X^{q^{v(\gamma)}}$ is then a formal $A(K)$-module endomorphism of $\bar{F}_e(X, Y)$ over k_{sc}. This latter ring is the ring of integers of the division algebra of rank n^2 and invariant n^{-1} over K, where $n = A(K)\text{-height}(F_e(X, Y)) = [L : K]$; cf. (23.1.6). Let $D_n(K)$ be this division algebra. Then we have constructed a map $s: \Gamma' \to D_n(K)$.

■ (32.4.8) **Lemma** The map s in a homomorphism.

Proof Using Lemma (32.4.6) we have

$$\begin{aligned} s(\gamma\delta) &= \bar{\alpha}_{\gamma\delta}(X^{q^{v(\gamma)+v(\delta)}}) \\ &= \bar{\alpha}_\gamma(X) \circ \overline{\gamma_*(\alpha_\delta(X))} \circ X^{q^{v(\gamma)+v(\delta)}} \\ &= \bar{\alpha}_\gamma(X) \circ X^{q^{v(\gamma)}} \circ \bar{\alpha}_\delta(X) \circ X^{q^{v(\delta)}} \end{aligned}$$

because $\overline{\gamma_* \alpha_\delta}(X) \circ X^{q^{v(\gamma)}}$ is equal to $X^{q^{v(\gamma)}} \circ \bar{\alpha}_\delta(X)$, as is easily checked (cf. also Chapter IV, Section 24.2, where this occurs repeatedly).

■ (32.4.9) **Embedding L in $D_n(K)$** This is done in the obvious way. Let $a \in A(L)$, then we have a formal $A(L)$-module endomorphism $[a](X) = [a]_{F_e}(X)$ of $F_e(X, Y)$ over $A(L)$. The reduction map $A(K)\text{-End}(F_e(X, Y)) \to A(K)\text{-End}(\bar{F}_e(X, Y))$ is injective; cf. Chapter IV, (21.8.19). So we find an injective $A(K)$-algebra homomorphism i: $A(L) \to A(K)\text{-End}(\bar{F}_e(X, Y)) \subset D_n(K)$, and tensoring with K gives us an embedding $i: L \to D_n(K)$.

■ (32.4.10) Let $a \in L^*$, then $r(a) \in \Gamma' \cap \mathrm{Gal}(L_{ab}/L)$. We claim that then $sr(a) = i(a)$. First, take $a = \pi$ (same π as in $\mathfrak{o}_\pi$). Then $i(a) = \bar{e}(X) = X^{q'}$ where q' is the number of elements of the residue field of L. On the other hand, $r(\pi)$ is the identity on L_π and the Frobenius substitution on L_{nr}/L so that $v(r(\pi)) = t$. Because $r(\pi)$ is the identity on L_π, we have $\bar{\alpha}_\gamma(X) = X$, so that $s(r(\pi)) = X^{q'}$. Next let $u \in U(L)$, then $v(r(u)) = 0$. Because $r(u)$ is the identity on L_{nr} and by Remark (32.4.5), we have $\alpha_{r(u)}(X) = [u]_e(X)$ so that $s(r(u)) = [u]_e(X) = i(u)$. This proves our assertion because s, r, i all are homomorphisms.

■ (32.4.11) **Lemma** The Šafarevič mapping s is injective.

Proof $\alpha_\gamma(X)$ corresponds to an isomorphism $T_\gamma \to T_e$, hence is an isomorphism of formal A-modules. Then $\bar{\alpha}_\gamma(X) \neq 0$ and hence also $\bar{\alpha}_\gamma(X^{q^{v(\gamma)}}) \neq 0$.

■ (32.4.12) Putting all this together, we have an embedding $s: \Gamma' \to D_n(K)$ which is an inverse to r on $\Gamma' \cap \mathrm{Gal}(L_{ab}/L)$ if one views L as a subfield of $D_n(K)$ via i; i.e., s is a Šafarevič mapping.

33 Zeta Functions of Elliptic Curves over Q and Atkin–Swinnerton–Dyer Conjectures

33.1 Honda's theorem on the relation between the formal minimal model of an elliptic curve E over Q and the zeta function of E

■ (33.1.1) **The formal group law associated to a Dirichlet series** Consider a Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$$

and suppose that $L(s)$ admits an Euler factor for the prime p. More precisely, suppose that over $\mathbf{Z}_p$ we have a factorization

$$L(s) = (1 - b_1 p^{-s} - b_2 p^{-2s} - \cdots)^{-1} \sum_{n=1}^{\infty} c_n n^{-s} \tag{33.1.2}$$

such that

$$v_p(c_n) \geq v_p(n) \tag{33.1.3}$$

where v_p: $\mathbf{Q}_p \to \mathbf{Z} \cup \{\infty\}$ is the normalized exponential valuation.

Consider the power series associated to $L(s)$

$$f_L(X) = \sum_{n=1}^{\infty} n^{-1}a(n)X^n \tag{33.1.4}$$

Then if $L(s)$ admits a factorization (33.1.2) such that (33.1.3) holds, the power series $f_L(X)$ satisfies a functional equation

$$f_L(X) - \sum_{n=1}^{\infty} p^{-n}b_n f_L(X^{p^n}) \in \mathbf{Z}_p[\![X]\!] \tag{33.1.5}$$

and vice versa. The proof of this is easy. A necessary and sufficient condition for (33.1.5) to hold is that if $n = p^r m$, $(p, m) = 1$, then

$$n^{-1}a_n - p^{-1}b_1(p^{-1}n)^{-1}a_{p^{-1}n} - \cdots - p^{-r}b_r(p^{-r}n)^{-1}a_{p^{-r}n} \in \mathbf{Z}_p$$

which (multiplying with n) is equivalent to

$$a_n - b_1 a_{p^{-1}n} - \cdots - b_r a_{p^{-r}n} \in p^r\mathbf{Z}_p \tag{33.1.6}$$

And, on the other hand, if (33.1.2) holds, we have

$$a_n - b_1 a_{p^{-1}n} - \cdots - b_r a_{p^{-r}n} = c_n \tag{33.1.7}$$

which proves our contention in view of (33.1.3).

■ (33.1.8) **Proposition** Let $L(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ be a Dirichlet series with $a(n) \in \mathbf{Z}$, $a(1) = 1$, and suppose that for every prime number p there is over $\mathbf{Z}_p$ a factorization (33.1.2) such that (33.1.3) holds. Suppose moreover that $v_p(b_i) \geq i - 1$. Let $f_L(X) = \sum_{n=1}^{\infty} n^{-1}a(n)X^n$ be the power series associated to $L(s)$. Then $f_L(X)$ is the logarithm of a one dimensional formal group law over $\mathbf{Z}$.

Proof The extra hypothesis on the b_i means that $p(p^{-n}b_n) \in \mathbf{Z}_p$, so that by the functional equation lemma $f_L^{-1}(f_L(X) + f_L(Y)) \in \mathbf{Z}_p[\![X, Y]\!]$ for all prime numbers p. This proves the proposition.

■ **Remark** Conversely, if $f_L(X)$ is the logarithm of a formal group law over $\mathbf{Z}$, then $L(s)$ has for every p an Euler factor (33.1.2) such that (33.1.3) holds and $v_p(b_i) \geq i - 1$. (Use Sections (20.1.3) and 20.5 of Chapter IV.)

■ (33.1.9) **Zeta function of an elliptic curve over Q** Let E be an elliptic curve over $\mathbf{Q}$ (abelian variety of dimension 1). According to Neron [311], there is an essentially unique (affine) minimal model for E over $\mathbf{Z}$ of the form

$$Y^2 + c_1XY + c_3Y = X^3 + c_2X^2 + c_4X + c_6 \tag{33.1.10}$$

where $c_1, c_2, c_3, c_4, c_6 \in \mathbf{Z}$ and where the discriminant of this equation is as small as possible. For this model, the reductions E_p of E modulo p are irreducible curves for all prime numbers p. One now defines the local L-series of E by the recipe:

(33.1.11) If E_p is nonsingular, then $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$, where $1 - a_p x + px^2$ is the numerator of the zeta function of E_p.

(33.1.12) If E_p has an ordinary double point, then we set $L_p(s) = (1 - \varepsilon_p p^{-s})^{-1}$ where $\varepsilon_p = +1$ or -1, depending on whether the tangents to the double point are rational over $\mathbf{F}_p$ or not.

(33.1.13) If E_p has a cusp, one sets $L_p(s) = 1$.

(This exhausts all possibilities; in case (33.1.11) E is said to have good reduction at p, in case (33.1.12) multiplicative reduction, and in case (33.1.13) additive reduction.)

The global L-series of E over $\mathbf{Q}$ is now defined as

$$L(s) = \prod_p L_p(s)$$

For future use we recall that in case (33.1.11) $x^2 - a_p x + p$ is the characteristic polynomial of the Frobenius endomorphism of E_p.

■ (33.1.14) **Formal minimal model of E** Let $t = X/Y$ be a local parameter at the zero element on the global minimal model of E. Expanding the group law on E as a power series in t_1, t_2, we get a power series $G_E(t_1, t_2) \in \mathbf{Z}[\![t_1, t_2]\!]$ which is a formal group law over $\mathbf{Z}$ (because the addition on E is commutative

and associative). One calls $G_E(t_1, t_2)$ the formal minimal model of E over $\mathbf{Z}$, and one often writes $\hat{E}(t_1, t_2)$.

Another way (essentially the same) to obtain E is as follows. Let again $z = X/Y$ be a local parameter at 0. Let $\omega = dX/2Y + c_1 X + c_3$ be the invariant differential on the global minimal model of E. Developing ω locally in terms of z we find an expression

$$\sum_{n=1}^{\infty} \beta(n) z^{n-1}\, dz, \qquad \beta(1) = 1 \tag{33.1.15}$$

The formal minimal model of E is now $G_E(X, Y) = f_E^{-1}(f_E(X) + f_E(Y))$ where $f_E(X) = \sum_{n=1}^{\infty} n^{-1}\beta(n)X^n$. That is, (33.1.15) is the right invariant differential form on $G_E(X, Y)$; cf. Chapter I, Section 5.8.

■ (33.1.16) **Theorem** Let $G_E(X, Y)$ be the formal minimal model over $\mathbf{Z}$ of an elliptic curve E over $\mathbf{Q}$ and let $F_L(X, Y)$ be the formal group law over $\mathbf{Z}$ associated to the global L-series of E. Then $G_E(X, Y)$ and $F_L(X, Y)$ are strictly isomorphic over $\mathbf{Z}$.

(Note that $F_L(X, Y)$ is a formal group law over $\mathbf{Z}$ as a corollary of Proposition (33.1.8).)

■ (33.1.17) **Reduction of the proof** By the local global results of Chapter IV, Section 20.5, it suffices to prove that $F_L(X, Y)$ and $G_E(X, Y)$ are strictly isomorphic over $\mathbf{Z}_p$ (for all p). By the results of Chapter IV, 22.1, it suffices to prove that the reductions of $F_L(X, Y)$ and $G_E(X, Y)$ over $\mathbf{F}_p$ are isomorphic for all primes p.

■ (33.1.18) **The case of good primes** p Suppose we are in case (33.1.11). Then $p - a_p x + x^2$ is the characteristic polynomial of the Frobenius endomorphism ξ of the elliptic curve E_p over $\mathbf{F}_p$. It follows that the Frobenius automorphism of $\bar{G}_E(X, Y)$ over $\mathbf{F}_p$, the reduction of the formal minimal model of E, also satisfies $p - a_p x + x^2$. The characteristic polynomial of $\bar{G}_E(X, Y)$ is the minimal polynomial of $\xi(X) = X^p$, and this is an Eisenstein polynomial. It follows that the characteristic polynomial $\Psi_G(X)$ of $\bar{G}_E(X, Y)$ over $\mathbf{F}_p$ is the unique Eisenstein factor of $x^2 - a_p x + p$, i.e.,

$$\Psi_G(x) = x^2 - a_p x + p \qquad \text{if} \quad p \mid a_p$$
$$\Psi_G(x) = x - pu^{-1} \qquad \text{if} \quad p \nmid a_p$$

where u is the unique p-adic unit such that $u^2 - a_p u + p = 0$ (i.e., $u \equiv a_p \bmod p$).

On the other hand, the logarithm $f_L(X)$ of $F_L(X, Y)$ satisfies a functional equation (cf. (33.1.5))

$$f_L(X) - p^{-1} a_p f_L(X^p) + p^{-1} f_L(X^{p^2}) \in \mathbf{Z}_p[\![X]\!]$$

It follows that

$$pf_L(X) - a_p f_L(X^p) + f_L(X^{p^2}) \equiv 0 \mod p$$

and hence by applying f_L^{-1} and using part (iv) of the functional equation lemma 2.2

$$[p](X) - [a_p](X^p) + X^{p^2} \equiv 0 \mod p$$

Or in other words the Frobenius endomorphism $\xi(X) = X^p$ of $\bar{F}_L(X, Y)$ satisfies an equation $p - a_p\xi + \xi^2 = 0$, and we see as above that the characteristic polynomial of $\bar{F}_L(X, Y)$ over $\mathbf{F}_p$ is $x^2 - a_p x + p$ or $x - pu^{-1}$ depending on whether or not $p \mid a_p$. This takes care of the good primes p.

(33.1.19) **The primes p where E has additive reduction** Now suppose that p is such that (33.1.12) applies. According to Neron [311, Chapter III, Proposition 3], the reduction of the group law of E is the additive group in this case. Hence $\bar{G}_E(X, Y) \simeq \hat{\mathbf{G}}_a(X, Y)$ over $\mathbf{F}_p$ for these primes. On the other hand, $L_p(s) = 1$ for the primes under consideration. Hence $f_L(X) \in \mathbf{Z}_p[\![X]\!]$ for these primes p and $F_L(X, Y) \simeq \hat{\mathbf{G}}_a(X, Y)$ over $\mathbf{Z}_p$.

(33.1.20) **The primes p where E has multiplicative reduction**

Case A: $\varepsilon_p = 1$ Now suppose that p is such that E_p has an ordinary double point whose tangents are rational over $\mathbf{F}_p$. According to Neron [311, Chapter III, Proposition 3], the reduction of the group law of E mod p is the multiplicative group law in this case. Hence $\bar{G}_E \simeq \hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{F}_p$ for these primes. On the other hand, $L_p(s) = (1 - p^{-s})^{-1}$ for these p so that $f_L(X)$ in this case satisfies a functional equation $f_L(X) - p^{-1}f_L(X^p) \in \mathbf{Z}_p[\![X]\!]$. By the functional equation lemma this means that over $\mathbf{Z}_p$, $F_L(X, Y)$ is strictly isomorphic to the formal group law with logarithm $f(X) = X + p^{-1}f(X^p)$ which is the p-typical version of the multiplicative group law $\hat{\mathbf{G}}_m(X, Y) = X + Y - XY$. Hence $F_L(X, Y)$ is isomorphic to $\hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{Z}_p$ for these primes.

(33.1.21) **The primes p where E has multiplicative reduction**

Case B: $\varepsilon_p = -1$ Now suppose that p is such that E_p has an ordinary double point whose tangents are not rational over $\mathbf{F}_p$. Then according to Neron [311, Chapter III, Proposition 3], the group law of E mod p is the unique $\mathbf{F}_{p^2}/\mathbf{F}_p$-form of $\mathbf{G}_m$ that is not isomorphic to $\mathbf{G}_m$ over $\mathbf{F}_p$. It follows that $\bar{G}_E(X, Y)$ is the unique nontrivial $\mathbf{F}_{p^2}/\mathbf{F}_p$-form over $\mathbf{F}_p$ of $\hat{\mathbf{G}}_m(X, Y)$. (Below in (33.1.22) we show that there is precisely one nontrivial $\mathbf{F}_{p^2}/\mathbf{F}_p$ form of $\hat{\mathbf{G}}_m(X, Y)$ and we calculate its logarithm.) It follows that $\bar{G}_E(X, Y)$ over $\mathbf{F}_p$ is isomorphic to the reduction mod p of the formal group law over $\mathbf{Z}_p$ with logarithm $f(X) = X - p^{-1}f(X^p)$. On the other hand, $L_p(s) = (1 + p^{-s})^{-1}$ for the primes under consideration so that $f_L(X)$ satisfies a functional equation $f_L(X) + p^{-1}f_L(X^p) \in \mathbf{Z}_p[\![X]\!]$, which by the functional equation lemma means

that $F_L(X, Y)$ is strictly isomorphic over $\mathbf{Z}_p$ to the formal group law with logarithm $f(X) = X - p^{-1}f(X^p)$. Hence $\bar{F}_L(X, Y) \simeq \bar{G}_E(X, Y)$ also for these primes. This concludes the proof of Theorem (33.1.16) (modulo the calculation of all $\mathbf{F}_{p^2}/\mathbf{F}_p$-forms of $\hat{\mathbf{G}}_m(X, Y)$ below in (33.1.22).)

■ (33.1.22) **The $\mathbf{F}_{p^2}/\mathbf{F}_p$-forms of $\hat{\mathbf{G}}_m(X, Y)$** The p-typical version of $\hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{Z}_p$ has functional equation $f(X) = X + p^{-1}f(X^p)$. Hence $pf(X) \equiv f(X^p) \bmod p$ and (by part (iv) of the functional equation lemma) $[p](X) \equiv X^p \bmod p$. So if $\xi(X) = X^p$, $\xi(X) = [p](X)$, so that the characteristic polynomial of $\hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{F}_p$ is $x - p$. When we consider $\hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{F}_{p^2}$ we must consider $\xi_2(X) = X^{p^2}$. We have $\xi_2(X) = [p^2](X)$, so that the characteristic polynomial of $\hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{F}_{p^2}$ is $x - p^2$:

$$\Psi_{\hat{G}_m/\mathbf{F}_{p^2}}(x) = x - p^2 \tag{33.1.23}$$

Now let $F(X, Y)$ be an $\mathbf{F}_{p^2}/\mathbf{F}_p$-form of $\hat{\mathbf{G}}_m(X, Y)$. The characteristic polynomial of $F(X, Y)$ over $\mathbf{F}_p$ is an Eisenstein polynomial of degree 1 (because $\mathrm{ht}(F(X, Y)) = 1 = \mathrm{ht}(\hat{\mathbf{G}}_m(X, Y))$). Hence

$$\Psi_{F/\mathbf{F}_p}(x) = x - \pi$$

for some $\pi \in \mathbf{Z}_p$, $v_p(\pi) = 1$. It follows as above that

$$\Psi_{F/\mathbf{F}_{p^2}}(x) = x - \pi^2$$

and comparing this with (33.1.23) we see that if $F(X, Y)$ is an $\mathbf{F}_{p^2}/\mathbf{F}_p$-form of $\hat{\mathbf{G}}_m(X, Y)$, then we must have $\pi = \pm p$. In case $\pi = p$, $\Psi_{F/\mathbf{F}_p}(x) = \Psi_{\hat{G}_m/\mathbf{F}_p}(x)$ so $F(X, Y) \simeq \hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{F}_p$; and in case $\pi = -p$, $F(X, Y)$ is not isomorphic to $\hat{\mathbf{G}}_m(X, Y)$ over $\mathbf{F}_p$ (the characteristic polynomials are different). Let $G(X, Y)$ over $\mathbf{Z}_p$ be the formal group law with logarithm $g(X) = X - p^{-1}(X^p)$. Then (as usual) $[-p]_G(X) \equiv X^p \bmod p$ so that the characteristic polynomial of $\bar{G}(X, Y)$ over $\mathbf{F}_p$ is $x + p$.

33.2 Atkin–Swinnerton–Dyer conjectures

■ (33.2.1) Let E be as in 33.1 and let $(1 - a_p p^{-s} + b_p p^{1-2s})^{-1} = L_p(s)$ for all prime numbers p. Let $\omega = \sum_{n=1}^{\infty} \beta(n) z^{n-1}\, dz$ be the local expression around zero of the invariant differential ω in terms of the local uniformizing parameter $z = X/Y$. We define for all $n \in \mathbf{N}$ and $r \in \mathbf{N}$ and prime numbers p,

$$\beta(n//p^r) = \begin{cases} 0 & \text{if } p^r \nmid n \\ \beta(p^{-r}n) & \text{if } p^r \mid n \end{cases} \tag{33.2.2}$$

■ (33.2.3) **Theorem** (Atkin–Swinnerton–Dyer conjectures) With notations as in (33.2.1) we have for all $n \in \mathbf{N}$,

$$\beta(np) - a_p\beta(n) + pb_p\beta(n//p) \equiv 0 \mod p^s \tag{33.2.4}$$

if $n \equiv 0 \bmod p^{s-1}$, $s \in \mathbf{N}$.

Proof We know by Theorem (33.1.16) that the formal group law $G_E(X, Y)$ with logarithm $\sum_{n=1}^{\infty} \beta(n)n^{-1}X^n$ (cf. (33.1.4)) is strictly isomorphic over $\mathbf{Z}$ to the formal group law $F_L(X, Y)$ with logarithm $f_L(X) = \sum_{n=1}^{\infty} n^{-1}a(n)X^n$ with $L(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$, $L(s) = \prod_p L_p(s)$. By (33.1.1), $f_L(X)$ satisfies a functional equation

$$f_L(X) - p^{-1}a_p f_L(X^p) + p^{-1}b_p f_L(X^{p^2}) \in \mathbf{Z}_p[\![X]\!]$$

Because $G_E(X, Y)$ and $F_L(X, Y)$ are strictly isomorphic over $\mathbf{Z}_p$, it follows (by the functional equation lemma) that $g(X)$, the logarithm of $G_E(X, Y)$, satisfies the same type of functional equation; i.e., we have

$$g(X) = \sum_{n=1}^{\infty} \frac{\beta(n)}{n} X^n \tag{33.2.5}$$

$$g(X) - p^{-1}a_p g(X^p) + p^{-1}b_p g(X^{p^2}) \in \mathbf{Z}_p[\![X]\!]$$

Now let $n \in \mathbf{N}$. Taking a look at the coefficients of X^{pn} in (33.2.5), we find

$$\frac{\beta(np)}{pn} - p^{-1}a_p \frac{\beta(n)}{n} + p^{-1}b_p \frac{\beta(n/p)}{n/p} \in \mathbf{Z}_p \qquad \text{if} \quad p \mid n$$

$$\frac{\beta(np)}{pn} - p^{-1}a_p \frac{\beta(n)}{n} \in \mathbf{Z}_p \qquad \text{if} \quad p \nmid n$$

Multiplying these relations with pn we find (33.2.4). Q.E.D.

34 On Complex Cobordism and Brown–Peterson Cohomology

34.1 Universality properties of MU^* and cohomology operations

■ (34.1.1) Given a topological space S, let $MU_*(S)$ and $MU^*(S)$ be the complex bordism and complex cobordism, respectively, of S; i.e., $S \mapsto MU_*(S)$, $S \to MU^*(S)$ are the generalized homology and cohomology theories defined by the Thom spectrum MU. It will be useful to interpret elements of $MU_*(S)$ also as bordism classes of maps $f\colon M \to S$ where M is a closed weakly complex manifold, and to interpret elements of $MU^q(S)$ as cobordism classes of proper complex-oriented maps $f\colon Z \to S$ of dimension $-q$, when S is a C^∞ manifold; cf. [332, Section 1]. For example, the elements of $MU^*(\mathbf{CP}^{n+r})$ and $MU_*(\mathbf{CP}^{n+r})$ defined by the natural embeddings $\mathbf{CP}^n \to \mathbf{CP}^{n+r}$ will be most useful. (Here $\mathbf{CP}^m$ is complex projective space of complex dimension m; e.g., $\mathbf{CP}^1 = S^2$, the Riemann sphere.)

■ (34.1.2) **Complex orientation of MU^*** Let $E \to S$ be a complex n-vector bundle over the manifold X. Then the zero section $i\colon S \to E$ defines a class $\in$

$MU^{2n}(E)$, the Thom class of E; its pullback under i^* is the Euler class of E, $e^{MU}(E) \in MU^{2n}(S)$. If 1_S denotes the class of the identity map $S \to S$, then $e(E) = i^* i_* 1$, where f_*: $MU^*(S) \to MU^*(T)$ for f: $S \to T$ proper and complex oriented, is the forward (Gysin) homomorphism defined by

$$(g\colon Z \to S) \mapsto (fg\colon Z \to T)$$

■ (34.1.3) **Theorem** Let h^* be a complex oriented cohomology theory with Euler classes e^h. Then there is a unique transformation of cohomology theories ϑ: $MU^* \to h^*$ (linear, degree preserving, and multiplicative) such that $\vartheta e^{MU}(L) = e^h(L)$ for all complex line bundles L.

For a proof, see [133, 332, or 203].

■ (34.1.4) **Cohomology operations in MU** Define the cohomology theory $MU^*[t] = MU^*[t_1, t_2, \ldots]$ by $MU^*[t](X, A) \otimes \mathbf{Z}[t_1, t_2, \ldots]$. Let $F_{MU}(X, Y)$ be the formal group law of complex cobordism theory, i.e.,

$$\begin{aligned} e^{MU}(L_1 \otimes L_2) &= F_{MU}(e^{MU}(L_1), e^{MU}(L_2)) \\ &= \sum_{i,j} a_{ij} e^{MU}(L_1)^i e^{MU}(L_2)^j, \qquad a_{ij} \in MU(pt) \end{aligned}$$

(cf. (31.1.2)). Define

$$\alpha_t^{-1}(X) = \sum_{n=1}^{\infty} {}^{F_{MU}} t_{n-1} X^n, \qquad t_0 = 1. \tag{34.1.5}$$

Now define Euler classes for $MU^*[t]$ by the formula

$$e^{MU[t]}(L) = \alpha_t(e^{MU}(L)) \tag{34.1.6}$$

This defines (because $\alpha_t(X) \equiv X$ mod(degree 2)) a complex orientation for $MU[\![t]\!]$. Applying Theorem (34.1.3) one finds a cohomology transformation

$$r_t\colon MU^* \to MU^*[t], \qquad r_t e^{MU[t]} = e^{MU} \tag{34.1.7}$$

which takes the formal group law $F_{MU}(X, Y)$ of complex cobordism theory into the formal group law $F_{MU[t]}(X, Y)$ of $MU^*[t]$ with $e^{MU[t]}$. We identify this last formal group law as follows. First, $MU[t]$ with e^{MU} as Euler class has of course $F_{MU}(X, Y)$ as formal group law, now considered over $MU(pt)[t] \supset MU(pt)$. Now $\alpha_t(X)$ defines, by (34.1.6), the definition of $e^{MU[t]}$, an isomorphism of formal group laws

$$\alpha_t(X)\colon F_{MU}(X, Y) \xrightarrow{\sim} F_{MU[t]}(X, Y)$$

So we have

$$F_{MU[t]}(X, Y) = \alpha_t(F_{MU}(\alpha_t^{-1}(X), \alpha_t^{-1}(Y)) \tag{34.1.8}$$

For each $x \in MU^*(S)$ write

$$r_t(x) = \sum_{\mathbf{n}} r_{\mathbf{n}}(x) t^{\mathbf{n}} \tag{34.1.9}$$

where $\mathbf{n}$ runs through all multi-indices $\mathbf{N} \to \mathbf{N} \cup \{0\}$ with compact support. Then the $r_{\mathbf{n}}$ all are (linear, stable) cohomology operations $MU^* \to MU^*$ (of degree $2|\mathbf{n}|$).

■ (34.1.10) **Theorem**

(i) $r_0 = id$.
(ii) $r_{\mathbf{n}}(x\,y) = \sum_{\mathbf{k}+\mathbf{l}} r_{\mathbf{k}}(x) r_{\mathbf{l}}(y)$.
(iii) Every stable cohomology operation $MU^* \to MU^*$ can be written as a sum $\sum_{\mathbf{n}} a_{\mathbf{n}} r_{\mathbf{n}}$ with $a_{\mathbf{n}} \in MU^*(pt)$.

Of these, (i) and (ii) are immediate from the definition (since r_t is multiplicative); for (iii) see, e.g., [2, part I], combined with the comments (34.1.11).

■ (34.1.11) **Comments** Later we shall identify $F_{MU}(X, Y)$ with $F_U(X, Y)$ over $\mathbf{Z}[U_2, U_3, \ldots]$, the universal one dimensional formal group law over $\mathbf{Z}[U]$, constructed in Section 5 of Chapter I. Let $f_U(X)$ be the logarithm of $F_U(X, Y)$. Now define

$$f_{U,T}(X) = \sum_{i=1}^{\infty} f_U(T_i X^i), \qquad F_{U,T}(X, Y) = f_{U,T}^{-1}(f_{U,T}(X) + f_{U,T}(Y))$$

where $T_1 = 1$. One checks—this is practically a triviality—that $F_{U,T}$ satisfies (over $\mathbf{Z}[U; T]$) the same type of functional equation as $f_U(X)$, and it follows by the functional equation lemma that

$$\alpha_{U,T}(X) = f_{U,T}^{-1}(f_U(X)) \in \mathbf{Z}[T; U][\![X]\!]$$

Because $\alpha_{U,T}(X) \equiv X - T_n X^n \bmod(T_1, \ldots, T_{n-1}, \text{degree } n+1)$, it follows as in Proposition (19.1.18) of Chapter IV that $\alpha_{U,T}(X)$: $F_U(X, Y) \to F_{U,T}(X, Y)$ is a universal strict isomorphism of formal group laws. Now

$$\alpha_{U,T}^{-1}(X) = f_U^{-1}(f_{U,T}(X))$$

$$= f_U^{-1}(f_U(T_1 X) + f_U(T_2 X^{p^2}) + \cdots = \sum_{i=1}^{\infty}{}^{F_U} T_i X^i$$

So if we identify T_i with t_{i-1} and $F_U(X, Y)$ with $F_{MU}(X, Y)$, then $\alpha_{U,T}(X)$ becomes $\alpha_t(X)$, $F_{U,T}(X, Y)$ becomes $F_{MU[t]}(X, Y)$, and $r_t(pt)$: $MU^*(pt) \to MU^*(pt)[t]$ describes the most general change of coordinates $u = (u_1, u_2, \ldots) \mapsto u' = (u'_1, u'_2, u'_3, \ldots)$ for changing a formal group law $F_U(X, Y)$ to a strictly isomorphic formal group law $F_{U'}(X, Y)$ (cf. also Section 19.1 of Chapter IV, especially Remark (19.1.21)).

There are many more universal isomorphisms $\alpha(X)$: $F_U(X, Y) \to F(X, Y)$. For instance, one can take $\tilde{\alpha}(X) = (X + T_2 X^2 + T_3 X^3 + \cdots)^{-1}$, taking the corresponding $\tilde{\alpha}_t^{-1}(X) = X + t_1 X^2 + \cdots$, one finds as above a cohomology transformation s_t: $MU^* \to MU^*[t]$. This is the usual Landweber–Novikov–Boardman operation, giving us the usual operations $s_{\mathbf{n}}$ as defined, e.g., in [332].

Taking different universal isomorphisms $\alpha(X)$; $\tilde{\alpha}(X)$; ... corresponds to taking different polynomial bases $t_1, t_2, \ldots$; $\tilde{t}_1, \tilde{t}_2, \ldots$; ..., $\dim(t_i) = \dim(\tilde{t}_i) = 2i$, for $MU_*(MU)$ as a left $MU(pt)$-algebra, and these different bases are related by formulas $\tilde{t}_i = \tilde{t}_i(t_i, \ldots, t_i)$, $\tilde{t}_i \equiv t_i \bmod(t_1, \ldots, t_{i-1})$ because the coefficients in $\alpha(X)$, $\tilde{\alpha}(X)$ are thus related.

A reason I like to use r_t rather than s_t is that by setting enough things equal to zero r_t specializes to the "right" right unit homomorphism $BP_*(pt) \to BP_*(P)[t_1', t_2', \ldots]$ (where "$t_i' = t_{p^i-1}$") for Brown–Peterson cohomology. It seems that in order to do explicit calculations in terms of a chosen set of generators (of $MU(pt)$ or $BP(pt)$) it is useful to see to it that the logarithm of the receiving formal group law of a universal isomorphism $\alpha(X)$: $F_{MU}(X, Y) \to F(X, Y)$ is reasonably easy to describe in terms of the logarithm of $F_{MU}(X, Y)$ (and similarly for $F_{BP}(X, Y)$ of course). In [2] this logarithm of the receiving formal group law is called the modified logarithm and denoted "mog."

34.2 Universality of the formal group law of complex cobordism

■ (34.2.1) **Some preliminary calculations** Let ξ over $\mathbf{CP}^N$ be the universal complex line bundle and let $u = e^{MU}(\xi) = c_1(\xi) \in MU^2(\mathbf{CP}^N)$. Then

$$MU^*(\mathbf{CP}^N) = MU(pt)[u]/(u^{N+1}), \qquad MU_*(\mathbf{CP}^N) = \bigoplus_{i=0}^{N} MU(pt)\beta_i$$

where the β_i are determined by $\langle \beta_j, u^i \rangle = \delta_{ij}$, where $\langle\ ,\ \rangle$ denotes the Kronecker product. Now let $cp(n) \in U_{2n}(\mathbf{CP}^N)$ be the bordism class of the natural embedding $\mathbf{CP}^n \to \mathbf{CP}^N$. Then of course

$$cp(n) \cap u^i = cp(n-i), \qquad \langle cp(n), u^i \rangle = [\mathbf{CP}^{n-i}] \tag{34.2.2}$$

and as a result

$$cp(n) = \sum_{i=0}^{n} [\mathbf{CP}^i]\beta_{n-i} \tag{34.2.3}$$

as is seen by taking Kronecker products with the u^i. It follows that the $cp(n)$, $n = 0, \ldots, N$ are a basis for the free $MU(pt)$-module $MU_*(\mathbf{CP}^N)$. We now define a new basis for the free $MU(pt)$-module $MU^*(\mathbf{CP}^N)$ by

$$\langle u_j, cp(i) \rangle = \delta_{ij}, \qquad i, j = 0, \ldots, N \tag{34.2.4}$$

Now let D: $MU^*(\mathbf{CP}^N) \to MU_*(\mathbf{CP}^N)$ be Poincaré–Atiyah duality (which is defined by $x \mapsto cp(N) \cap x$). Then

$$Du_j = \beta_{N-j} \tag{34.2.5}$$

Indeed

$$\langle Du_j, u^i \rangle = \langle cp(N) \cap u_j, u^i \rangle = \langle cp(N), u_j \cup u^i \rangle = \langle cp(N) \cap u^i, u_j \rangle$$
$$= \langle cp(N-i), u_j \rangle = \delta_{N-i,j} = \delta_{N-j,i} = \langle \beta_{N-j}, u^i \rangle$$

Finally, we have

(34.2.6) $$u_j = u_0 u^j$$

since

$$\langle u_0 u^j, cp(i)\rangle = \langle u_0, u^j \cap cp(i)\rangle = \langle u_0, cp(i-j)\rangle = \delta_{0,i-j}$$
$$= \delta_{j,i} = \langle u_j, cp(i)\rangle$$

■ (34.2.7) **Milnor hypersurfaces** Let $\xi_r \otimes \xi_s$ over $\mathbf{CP}^r \times \mathbf{CP}^s$ be the tensor product of $\xi = \xi_r$ over $\mathbf{CP}^r$ with $\xi_s = \xi$ over $\mathbf{CP}^s$. Let $h(r, s) \in MU_{2(r+s)-2}(\mathbf{CP}^r \times \mathbf{CP}^s)$ be the Atiyah–Poincaré dual of $e^{MU}(\xi_r \otimes \xi_s) = c_1(\xi_r \otimes \xi_s) \in MU^2(\mathbf{CP}^r \times \mathbf{CP}^s)$. Then $h(r, s)$ is represented by the embedding of a type (1, 1) hypersurface $H_{r,s} \to \mathbf{CP}^r \times \mathbf{CP}^s$, which realizes the cycle represented by $\mathbf{CP}^{r-1} \times \mathbf{CP}^s + \mathbf{CP}^r \times \mathbf{CP}^{s-1}$ in $H_{2(r+s)-2}(\mathbf{CP}^r \times \mathbf{CP}^s)$. So we have by definition

(34.2.8) $$[H_{r,s}] = \varepsilon_* D(e^{MU}(\xi_r \otimes \xi_s)), \qquad \xi_r \otimes \xi_s \to \mathbf{CP}^r \times \mathbf{CP}^s$$

where $\varepsilon\colon \mathbf{CP}^r \times \mathbf{CP}^s \to pt$ is the canonical map. For the proof of the universality of the formal group law of complex cobordism theory, we shall now need the following facts.

■ (34.2.9) **Theorem**

(i) $MU(pt)$ is torsion free and $MU(pt) \otimes \mathbf{Q} = \mathbf{Q}[[\mathbf{CP}^1], [\mathbf{CP}^2], \ldots]$.

(ii) The $[H_{r,s}]$ are a set of multiplicative generators for $MU_*(pt)$; i.e., every element of $MU(pt)$ can be written as a sum with coefficients in $\mathbf{Z}$ of monomials in the $[H_{r,s}]$.

(iii) $[H_{r,0}] = [\mathbf{CP}_{r-1}]$, $[H_{r,1}] = [\mathbf{CP}^1][\mathbf{CP}^{r-1}] = [H_{1,r}]$.

For a proof of (i) and (ii), cf., e.g., [294, 314, or 398] (especially pp. 130, 131 of [398] for (ii). The formulas of (iii) are clear. (Or use Chern numbers.)

■ (34.2.10) **Theorem** Let $CP(Z) = \sum_{n=0}^{\infty} [\mathbf{CP}^n] Z^n \in MU(pt)[\![Z]\!]$. Then the formal group law of complex cobordism theory is equal to

$$F_{MU}(X, Y) = \frac{X + Y + \sum_{r,s=1}^{\infty} [H_{r,s}] X^r Y^s}{CP(X) CP(Y)}$$

Proof Consider $e^{MU}(\xi_r \otimes \xi_s) \in MU^2(\mathbf{CP}^r \times \mathbf{CP}^s)$. We claim that

(34.2.11) $$\langle e^{MU}(\xi_r \otimes \xi_s), cp(i) \otimes cp(j)\rangle = [H_{i,j}]$$

for all $i \le r$, $j \le s$. To see this let $l\colon \mathbf{CP}^i \times \mathbf{CP}^j \to \mathbf{CP}^r \times \mathbf{CP}^s$ be the canonical embedding. (The elements $cp(i) \otimes cp(j) \in MU_{2(i+j)}(\mathbf{CP}^i \times \mathbf{CP}^j)$ and $cp(i) \otimes cp(j) \in MU_{2(i+j)}(\mathbf{CP}^r \times \mathbf{CP}^s)$ are identified via l_*; cf. (34.2.1)). We can write

$$h(i, j) = \sum a_{k,l} \beta_k \otimes \beta_l \in MU_*(\mathbf{CP}^i \times \mathbf{CP}^j), \qquad a_{k,l} \in MU(pt)$$

Then, since $\varepsilon_* h(i,j) = [H_{i,j}]$, we have $a_{0,0} = [H_{i,j}]$. Now using (34.2.5), (34.2.4)

$$\begin{aligned}\langle e^{MU}(\xi_r \otimes \xi_s),\ cp(i) \otimes cp(j)\rangle &= \langle e^{MU}(\xi_r \otimes \xi_s),\ l_*(cp(i) \otimes cp(j)\rangle \\ &= \langle l^* e^{MU}(\xi_r \otimes \xi_s),\ cp(i) \otimes cp(j)\rangle \\ &= \langle e^{MU}(\xi_i \otimes \xi_j),\ cp(i) \otimes cp(j)\rangle \\ &= \langle D^{-1}h(i,j),\ cp(i) \otimes cp(j)\rangle \\ &= \langle \textstyle\sum a_{kl} u_{i-k} \otimes u_{j-l},\ cp(i) \otimes cp(j)\rangle \\ &= a_{0,0} = [H_{i,j}]\end{aligned}$$

proving (34.2.11). Since $[H_{0,1}] = [H_{1,0}] = 1$, it follows that (by taking Kronecker products with the $cp(i) \otimes cp(j)$)

$$(34.2.12)\quad e^{MU}(\xi_r \otimes \xi_s) = u_1 \otimes u_0 + u_0 \otimes u_1 + \sum_{i+j>1} [H_{i,j}] u_i \otimes u_j$$

Now we also have

$$(34.2.13)\qquad u_0 = 1/CP(u)$$

Indeed $u = e^{MU}(\xi \otimes 1) = u_1 + \sum_{i=2}^{\infty} [H_{i,0}] u_i = u_0(u + \sum_{i=2}^{\infty} [\mathbf{CP}^{i-1}] u^i)$, where we have used (34.2.6), and the result follows.

Now combine (34.2.12), (34.2.13), and (34.2.6) and let $r, s \to \infty$ to obtain Theorem (34.2.10).

■ (34.2.14) **Theorem** The logarithm $\log_{MU}(X)$ of $F_{MU}(X, Y)$ is equal to

$$\log_{MU}(X) = \sum_{n=0}^{\infty} \frac{[\mathbf{CP}^n]}{n+1} X^{n+1}$$

Proof Let $F(X, Y)$ be any formal group law over a characteristic zero ring A, and let $f(X)$ be its logarithm. Taking the derivative with respect to Y in $f(F(X, Y)) = f(X) + f(Y)$ and then substituting $Y = 0$, one finds

$$(34.2.15)\qquad \frac{df}{dX}(X) \cdot \frac{\partial F}{\partial Y}(X, 0) = 1$$

Applying this to $F_{MU}(X, Y)$ and using part (iii) of Theorem (34.2.9) one obtains Theorem (34.2.14).

■ (34.2.16) **Theorem** The formal group law $F_{MU}(X, Y)$ over $MU(pt)$ is a universal one dimensional formal group law.

Proof Let $F(X, Y)$ over A be a one dimensional formal group law over a characteristic zero ring A. Let $f(X)$ be the logarithm of $F(X, Y)$. Consider the ring homomorphism ϕ: $MU(pt) \otimes \mathbf{Q} \to A \otimes \mathbf{Q}$ defined by

$$\phi([\mathbf{CP}^n]) = (n+1)a_{n+1}, \quad n \in \mathbf{N} \cup \{0\}, \qquad \text{where } f(X) = \sum_{n=1}^{\infty} a_n X^n, \quad a_1 = 1$$

Then $\phi_* F_{MU}(X, Y) = F(X, Y)$ by Theorem (34.2.14). Hence $\phi(e_{i,j}) \in A$ for all coefficients $e_{i,j}$ of

$$F_{MU}(X, Y) = X + Y + \sum e_{i,j} X^i Y^i$$

Now by Theorem (34.2.9)(ii) and Theorem (34.2.10) the $e_{i,j}$ and $[\mathbf{CP}^n]$ generate $MU(pt)$. It follows (using that $na_n \in A$, which follows, e.g., from (34.2.15)) that $\phi(MU(pt)) \subset A$, so that there is a homomorphism $\phi\colon MU(pt) \to A$ taking $F_{MU}(X, Y)$ into $F(X, Y)$. The homomorphism is also clearly unique since it must take $\log_{MU}(X)$ into $f(X)$.

This proves that $F_{MU}(X, Y)$ is universal for formal group laws over characteristic zero rings. Since $F_U(X, Y)$ over $\mathbf{Z}[U]$, the universal formal group law over $\mathbf{Z}[U]$, is defined over a characteristic zero ring, it follows that there are mutually inverse ring homomorphisms $MU(pt) \to \mathbf{Z}[U]$, $\mathbf{Z}[U] \to MU(pt)$ taking $F_{MU}(X, Y)$ into $F_U(X, Y)$ and vice versa. It follows that $F_{MU}(X, Y)$ over $MU(pt)$ is universal.

34.3 p-Typification in topology

■ (34.3.1) We shall from now on usually identify $MU(pt)$ with $\mathbf{Z}[U]$ and $F_{MU}(X, Y)$ with $F_U(X, Y)$. Just what this means for a set of free polynomial generators for $MU(pt)$ will be discussed later in Section 34.4. For the moment, this is immaterial. We write

$$F_U(X, Y) = F_{MU}(X, Y) = f_U^{-1}(f_U(X) + f_U(Y))$$

$$f_U(X) = \sum_{n=1}^{\infty} m_{n-1} X^n = \sum_{n=1}^{\infty} l_n(U) X^n$$

so that $m_n = (n+1)^{-1}[\mathbf{CP}^n] \in MU(pt) \otimes \mathbf{Q}$, $l_n(U) \in \mathbf{Q}[U]$; cf. Section 5, Chapter I. (We have written $l_n(U)$ instead of $m_n(U)$ to avoid confusion.)

■ (34.3.2) **Generalities and recollections concerning p-typification** Choose a prime number p. Identifying U_{p^i} and V_i, we have that the universal p-typical formal group law $F_V(X, Y)$ and the universal formal group law $F_U(X, Y)$ are strictly isomorphic over $\mathbf{Z}_{(p)}[U]$. (Their logarithms satisfy the same type of functional equation; compare formulas (5.3.3) and (2.3.6) of Chapter I.) Let

$$\alpha_{U,V}(X) = f_V^{-1}(f_U(X))$$

be the (unique) strict isomorphism $F_U(X, Y) \to F_V(X, Y)$. Now $F_V(X, Y)$ is a formal group law over $Z[U]$ (we are still identifying V_i with U_{p^i}), so there exists a unique homomorphism of rings $\Psi_p\colon Z[U] \to Z[U]$ such that $(\Psi_p)_* F_U(X, Y) = F_V(X, Y)$. The homomorphism Ψ_p tells us what we must do to the coefficients of $F_U(X, Y)$ in order to change $F_U(X, Y)$ into $F_V(X, Y)$. It follows of course that $(\Psi_p)_* f_U(X) = f_V(X)$.

Now, since $a_n(V) = l_{p^n}(U)$ (compare formulas (5.2.7) and (3.3.8) of Chapter I), there is a perfectly obvious homomorphism $\mathbf{Z}[U] \to \mathbf{Z}[U]$ that takes $F_U(X, Y)$ into $F_V(X, Y)$; it is $U_i \mapsto 0$ if $(p, i) = 1$ and $U_{p^n} \mapsto U_{p^n}$ for all $n \in \mathbf{N}$. By uniqueness we therefore have

$$\Psi_p(U_i) = \begin{cases} 0 & \text{if } (n, p) = 1 \\ U_i & \text{if } n \text{ is a power of } p \end{cases} \tag{34.3.3}$$

We shall need the following trivial technical lemma.

■ (34.3.4) **Lemma** Let

$$\alpha_{U.V}^{-1}(X) = \sum_{i=0}^{\infty} {}^{FU} y_i X^{i+1}$$

Then $\Psi_p(y_i) = 0$ for all $i \in \mathbf{N}$.

Proof We have

$$\alpha_{U.V}^{-1}(X) = f_U^{-1}(f_V(X))$$

so that $(\Psi_p)_*(\alpha_{U.V}^{-1}(X)) = ((\Psi_p)_* f_U)^{-1}((\Psi_p)_* f_V(X)) = f_V^{-1}(f_V(X)) = X$ since $(\Psi_p)_*$ takes $f_U(X)$ to $f_V(X)$ and Ψ_p is idempotent.

■ (34.3.5) **An idempotent cohomology operation on $MU^*_{(p)}$** Let $MU^*_{(p)}$ be the cohomology theory defined by $MU^*_{(p)}(S, A) = MU^*(S, A) \otimes \mathbf{Z}_{(p)}$. We give $MU^*_{(p)}$ Euler classes as follows:

$$e^{MU_{(p)}}(L) = \alpha_{U.V}(e^{MU}(L)) \tag{34.3.6}$$

for all complex line bundles L. This gives $MU^*_{(p)}$ a complex orientation. Applying Theorem (34.1.3) we find a unique transformation of cohomology theories

$$\vartheta_p : MU^* \to MU^*_{(p)}, \qquad \vartheta_p e^{MU} = e^{MU_{(p)}}$$

As in (34.1.4) one has

$$\begin{aligned} F_{MU_{(p)}}(e^{MU_{(p)}}(L_1), e^{MU_{(p)}}(L_2)) &= e^{MU_{(p)}}(L_1 \otimes L_2) = \alpha_{U.V}(e^{MU}(L_1 \otimes L_2)) \\ &= \alpha_{U.V}(F_{MU}(e^{MU}(L_1), e^{MU}(L_2))) \\ &= \alpha_{U.V}(F_{MU}(\alpha_{U.V}^{-1}(e^{MU_{(p)}}(L_1), \alpha_{U.V}^{-1}(e^{MU_{(p)}}(L_2))))) \end{aligned}$$

so that $F_{MU_{(p)}}(X, Y) = \alpha_{U.V}(F_{MU}(\alpha_{U.V}^{-1}(X), \alpha_{U.V}^{-1}(Y))) = F_V(X, Y)$, the universal p-typical formal group law.

Now ϑ_p takes $F_{MU}(X, Y)$ into $F_{MU_{(p)}}(X, Y)$ and it follows that

$$\vartheta_p(pt) = \Psi_p \tag{34.3.7}$$

where Ψ_p is as in (34.3.2). In particular, writing also ϑ_p for the induced cohomology operation $MU^*_{(p)} \to MU^*_{(p)}$, it follows that $\vartheta_p(pt)$ is idempotent. Quite

generally this implies that $\vartheta_{(p)}$: $MU^*_{(p)} \to MU^*_{(p)}$ is itself idempotent (cf. [2, Lemma 9.3 of Part II]). In this case this can also be seen as follows.

Let ρ_p: $MU^*[t] \to MU^*_{(p)}$ be the multiplicative cohomology operation defined by

$$\rho_p(t_i) = y_i$$

where the y_i are as in Lemma (34.3.4). Then by definition of ρ_p we have that $\rho_p \circ r_t = \vartheta_p$ (cf. (34.1.4)). And

$$\vartheta_p\, \vartheta_p(x) = \vartheta_p \rho_p \left(\sum_n r_n(x) t^n \right) = \vartheta_p \left(\sum_n r_n(x) y^n \right) = \vartheta_p(r_0(x)) = \vartheta_p(x)$$

because $\vartheta_p(y_i) = 0$ for all $i > 0$ by Lemma (34.3.4).

■ (34.3.8) **Definition of Brown–Peterson cohomology** We now define Brown–Peterson cohomology BP^* by

$$BP^*(S, A) = \mathrm{Im}(\vartheta_p\colon MU^*_{(p)}(S, A) \to MU^*_{(p)}(S, A))$$

Since $\vartheta_p(pt) = \Psi_p$, we have immediately from (34.3.3) that

$$BP(pt) \simeq \mathbf{Z}_{(p)}[V_1, V_2, \ldots] \tag{34.3.9}$$

Brown–Peterson cohomology is multiplicative, complex oriented, and its formal group law is the universal p-typical formal group law $F_V(X, Y)$—all of which properties are immediate from the definition above.

■ (34.3.10) **Quillen decomposition** Let h^* be the cohomology theory $h^*(S, A) = BP^*(S, A) \otimes \mathbf{Z}_{(p)}[U_i \mid i \text{ not a power of } p,\ i \geq 2]$. Let η_p: $BP^* \to MU^*_{(p)}$ be the canonical injection defined by the idempotent ϑ_p and define Θ_p: $h^* \to MU^*_{(p)}$ by

$$\Theta_p(U^\alpha \otimes x) = U^\alpha \eta_p(x)$$

Then Θ_p is a linear multiplicative cohomology transformation and $\Theta_p(pt)$ is an isomorphism, so Θ_p is an isomorphism of cohomology theories, showing that $MU^*_{(p)}$ decomposes as a wedge sum of dimension shifted copies of BP^*.

■ (34.3.11) **Proposition** Let h^* be a complex oriented cohomology theory whose associated formal group law is p-typical, and such that $h^*(pt)$ is a $\mathbf{Z}_{(p)}$-algebra. Then there exists a unique (linear, multiplicative) cohomology transformation ϑ: $BP^* \to h^*$ such that $\vartheta e^{BP} = e^h$.

Proof There exists by Theorem (34.1.3) a unique cohomology transformation $\tilde{\vartheta}$: $MU^* \to h^*$ taking e^{MU} to e^h and therefore

$$\tilde{\vartheta}(pt)_* F_{MU}(X, Y) = F_h(X, Y)$$

Let π_p: $MU^* \to BP^*$ be the projection induced by ϑ_p onto the image of ϑ_p: $MU^*_{(p)} \to MU^*_{(p)}$. By hypothesis $F_h(X, Y)$ is p-typical, hence it follows that $\tilde{\vartheta}(pt)$

factors through $\pi_p(pt)$: $MU(pt) \to BP(pt)$, $U_i \mapsto 0$ if i is not a power of p and $U_i \mapsto V_j$ if $i = p^j$:

$$\begin{array}{ccc} MU^*_{(p)} & \xrightarrow{\vartheta} & h^* \\ & \searrow^{\pi_p} & \uparrow \\ & & BP^* \end{array}$$

We claim that it follows that ϑ factors through π_p. To see this it suffices to show that if $x \in MU^*_{(p)}(S, A)$ and $\vartheta_p(x) = 0$, then $\vartheta(x) = 0$ (because $MU^*_{(p)} \simeq \operatorname{Im} \vartheta_p \oplus \operatorname{Ker} \vartheta_p$).

Now

$$\vartheta_p(x) = \sum_n r_n(x) y^n$$

so, if $\vartheta_p(x) = 0$, we have

$$x = -\sum_{n \neq 0} r_n(x) y^n$$

and since $\vartheta_p(pt)(y_i) = 0$ for all i, we have $\vartheta(pt)(y_i) = 0$ all i because $\vartheta(pt)$ factors through $\pi_p(pt)$, and hence $\vartheta(x) = 0$. This proves the proposition.

34.4 Generators for $MU(pt)$ and $BP(pt)$

■ (34.4.1) **Generators for $MU(pt)$** We have seen that $F_{MU}(X, Y)$ is a universal formal group law (Theorem (34.2.16)) so there are mutually inverse isomorphisms

$$\phi: MU(pt) \to \mathbf{Z}[U], \qquad \psi: \mathbf{Z}[U] \to MU(pt)$$

such that $\phi_* F_{MU}(X, Y) = F_U(X, Y)$, $\psi_* F_U(X, Y) = F_{MU}(X, Y)$. Let $f_U(X)$ be the logarithm of $F_U(X, Y)$, where we choose the coefficients of $n(i_1, \ldots, i_s)$ as in Section 5.6 of Chapter I. Then writing $f_U(X) = \sum l_n(U) X^n$, we have according to Theorem (5.6.16)

$$v(n) l_n(U) = U_n + \sum_{\substack{d \mid n \\ d \neq 1, n}} \frac{\mu(n, d) v(n)}{v(d)} l_{n/d}(U) U_d^{n/d} \tag{34.4.2}$$

where $v(i) = p$ if i is a power of the prime p, and $v(i) = 1$ if i is not a power of a prime number or $i = 1$, and where the $\mu(n, d)$ are certain integers

$$\mu(n, d) = \prod_{p \mid n} c(p, d)$$

where the $c(p, d) \in \mathbf{Z}$ have been chosen such that $c(p, d) = 1$ if $v(d) = 1$, p and $c(p, d) \equiv 1 \bmod p$, $c(p, d) \equiv 0 \bmod p'$ if $v(d) = p' \neq p$. (Here p and p' are always prime numbers.)

Now apply ψ to (34.4.2) and recall that $\log_{MU}(X) = \sum_{n=0}^{\infty} m_n X^{n+1}$, $m_n = (n+1)^{-1}[\mathbf{CP}^n]$. Let $u_{n-1} = \psi(U_n)$, $n = 2, 3, \ldots$. Then we find a set of free

polynomial generators $u_1, u_2, \ldots$ for $MU(pt)$ which are related to the $m_n \in MU(pt) \otimes \mathbf{Q}$ by the formula

$$(34.4.3) \qquad \nu(n) m_{n-1} = u_{n-1} + \sum_{\substack{d \mid n \\ d \neq 1, n}} \frac{\mu(n, d)\nu(n)}{\nu(d)} m_{(n/d)-1} u_{d-1}^{n/d}$$

(Note that $\nu(d)^{-1}\mu(n, d)\nu(n)$ is always an integer.) It follows that $\dim u_i = 2i$.

Since $H_*(MU) = \mathbf{Z}[m_1, m_2, \ldots]$, one can also view (34.4.3) as a description of the Hurewicz homomorphism $MU(pt) = \pi_*(MU) \to H_*(MU)$ in terms of the generators $u_1, u_2, u_3, \ldots$.

■ (34.4.4) **Generators for $BP(pt)$** By construction $BP(pt)$ is the image of $\Psi_p: MU(pt) \to BP(pt)$, $u_i \mapsto 0$ if $i+1$ is not a power of p, and $u_i \mapsto u_i$ if $i+1$ is a power of p. Let $v_i = \Psi_p(u_{p^i-1})$, $i = 1, 2, \ldots$. Then the v_i are a free polynomial basis for $BP(pt)$, and by applying $\Psi_p = \vartheta_p(pt)$ to (34.4.3) we see that they are related to the $m_{p^i-1} \in BP(pt) \otimes \mathbf{Q}$ by the formula

$$(34.4.5) \qquad p m_{p^n-1} = v_n + m_{p-1} v_{n-1}^p + m_{p^2-1} v_{n-2}^{p^2} + \cdots + m_{p^{n-1}-1} v_1^{p^{n-1}}$$

which again can be seen as a description of $BP(pt) = \pi_*(BP) \to H_*(BP) = \mathbf{Z}_{(p)}[m_{p^i-1} \mid i = 1, 2, \ldots]$. Since Ψ_p is an endomorphism of $MU(pt)$ (and not just an endomorphism of $MU_{(p)}(pt)$), it follows that the v_i are integral, i.e., they live in $MU(pt)$ and not just in $MU_{(p)}(pt)$; cf. also [6].

■ (34.4.6) **Remark** If BP is constructed in another way than by splitting off a factor of $MU_{(p)}$ and one has proved that BP is complex oriented and has a p-typically universal formal group law with logarithm $\sum m_{p^i-1} X^{p^i}$, then arguing as in (34.4.1) one also finds generators v_i satisfying (34.4.5) (where one uses formula (3.3.9) of Chapter I instead of Theorem (5.6.16)). In this connection it is worth noticing that the original BP spectrum is defined over $\mathbf{Z}$ rather than $\mathbf{Z}_{(p)}$; cf. [47] and also [33, Appendix D, Section 7] for the uncountably many different BP spectra, which, when localized at p, give the version over $\mathbf{Z}_{(p)}$ described above in Section 34.3.

34.5 Brown–Peterson cohomology operations

■ (34.5.1) We shall identify $BP(pt)$ with $\mathbf{Z}_{(p)}[V]$, via $v_i \mapsto V_i$; $F_{BP}(X, Y)$ then becomes the universal p-typical formal group law $F_V(X, Y)$ over $\mathbf{Z}_{(p)}[V]$.

■ (34.5.2) Let $\alpha_{V,T}(X): F_V(X, Y) \to F_{V,T}(X, Y)$ be the universal isomorphism of one dimensional p-typical formal group laws of Theorem (19.2.6) of Chapter IV; cf. also Theorem (2.3.10) of Chapter I where we showed that $\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X))$ is an isomorphism.

Let $BP^*[t]$ be the cohomology theory $BP^*[t](M, A) = BP^*(M, A)[t]$ where t is short for $t = (t_1, t_2, \ldots)$. We give $BP^*[t]$ Euler classes by setting

$$e^{BP[t]}(L) = \alpha_{V,t}(e^{BP}(L))$$

Then $BP^*[t]$ is complex oriented. Moreover, its formal group law is (cf. (34.3.5) for a similar calculation)

$$F_{BP[t]}(X, Y) = \alpha_{V,t}(F_{BP}(\alpha_{V,t}^{-1}(X), \alpha_{V,t}^{-1}(Y))) = \alpha_{V,t}(F_V(\alpha_{V,t}^{-1}(X), \alpha_{V,t}^{-1}(Y))) = F_{V,t}(X, Y)$$

which is p-typical. Hence by Proposition (34.3.11) there exists a unique transformation of cohomology theories

$$r_t: BP^* \to BP^*[t]$$

such that $(r_t)_* F_V(X, Y) = F_{V,t}(X, Y)$. In particular, it follows that

$$r_t(pt)_* f_V(X) = f_{V,t}(X)$$

Now $f_V(X) = \sum_{i=0}^{\infty} m_{p^i-1} X^{p^i}$, and, according to formula (3.3.10) of Chapter I,

$$f_{V,t}(X) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} m_{p^j-1} t_i^{p^j-j} \right) X^{p^i}$$

so that $r_t(pt)$ is given by

$$r_t(pt)(m_{p^n-1}) = \sum_{i=0}^{n} m_{p^i-1} t_{n-i}^{p^i}$$

on $BP(pt) \otimes \mathbf{Q}$. So we see that r_t is precisely the right unit homomorphism η_R: $BP(pt) = \pi_*(BP) \to BP_*(BP)$ as described by Adams in [2, Part II, Theorem 16.1].

The r_t^{BP} we have just defined fits in very well with the r_t^{MU} we have defined above in 34.1 in the sense that the following diagram is commutative:

$$\begin{array}{ccc} MU^* & \xrightarrow{r_{t'}^{MU}} & MU^*[t'] \\ \downarrow{\scriptstyle \pi_p} & & \downarrow{\scriptstyle \tilde{\pi}_p} \\ BP^* & \xrightarrow{r_t^{BP}} & BP^*[t] \end{array}$$

where $\tilde{\pi}_p$ is π_p on MU^* and $\tilde{\pi}_p(t_i') = 0$ if i is not of the form $p^j - 1$ and $\tilde{\pi}_p(t_{p^j-1}') = t_j$.

■ (34.5.3) **The cohomology operations r_E** An exponent sequence $E = (e_1, e_2, \ldots)$ is simply a multi-index $\mathbf{N} \to \mathbf{N} \cup \{0\}$ with finite support. Writing as usual $t^E = \prod_{i \in \operatorname{supp}(E)} t_i^{e_i}$, the big cohomology operation r_t can be written

$$r_t(x) = \sum_E r_E(x) t^E, \qquad r_E(x) \in BP^*(S, A)$$

giving us (stable) BP-cohomology operations r_E for every exponent sequence E.

Every stable BP-cohomology operation r can be written as a sum $r = \sum a_E r_E$ with $a_E \in BP(pt)$. This follows, e.g., from the corresponding fact for MU together with the Quillen splitting (cf. (34.3.10)).

Among the r_E the r_{Δ_i}, $\Delta_i = (0, 0, \ldots, 0, 1, 1, 0, \ldots)$ with the 1 in the ith spot, are especially interesting because every r can be written as a sum with coefficients in $BP(pt)$ of composites of the r_{Δ_i}.

■ (34.5.4) **Relation with the homomorphism η_R of Section 19.3, Chapter IV** $F_{V,T}(X, Y)$ over $\mathbf{Z}[V; T]$ is a p-typical formal group law, so by the universality of $F_V(X, Y)$ over $\mathbf{Z}[V]$ there exists a unique homomorphism η_R: $\mathbf{Z}[V] \to \mathbf{Z}[V; T]$, $V_i \mapsto \bar{V}_i$ such that $(\eta_R)_* F_V(X, Y) = F_{V,T}(X, Y)$; a homomorphism that we studied to some extent in Section 19.3 of Chapter IV and which was most useful in Section 22 of Chapter IV when we were studying liftings and moduli and isomorphism classes of (one dimensional) formal group laws.

Now identify $\mathbf{Z}_{(p)}[V]$ with $BP(pt)$ by $V_i \mapsto v_i$ and $\mathbf{Z}_{(p)}[V; T]$ with $BP(pt)[t] = BP_*(BP)$ by $V_i \mapsto v_i$, $T_i \mapsto t_i$. Then $F_V(X, Y)$ becomes $F_{BP}(X, Y)$ and $F_{V,T}(X, Y)$ becomes $F_{BP[t]}(X, Y)$, so that $r_t(pt)$: $BP(pt) \to BP_*(BP)$ corresponds to the localized in p version of η_R: $V_n \mapsto \bar{V}_n$. Let $\bar{v}_n = r_t(pt)(v_n)$. Then we have

$$r_t(v_{n+h}) \equiv v_{n+h} - t_n v_h^{p^n} + v_h t_n^{p^h} \mod(v_1, \ldots, v_{h-1}, v_{h+1}, \ldots, v_{n+h-1}, t_1, \ldots, t_{n-1}, p) \tag{34.5.5}$$

for all $n, h \in \mathbf{N}$ (formula (19.4.5) of Chapter IV). We also have, applying Theorem (22.3.4) of Chapter IV with $A = \mathbf{Z}_p$ (i.e., $\pi = p = q$),

$$\begin{aligned} r_t(v_n) \equiv\ & v_n + \sum (-1)^m([\mathbf{CP}^{p^{s_1}-1}]v_{n-s_1}^{p^{s_1}-1}) \times \cdots \\ & \times ([\mathbf{CP}^{p^{s_m}-1}]v_{n-s_1-\cdots-s_m}^{p^{s_m}-1})(-t_i v_j^{p^i}) \\ & + \sum (-1)^m([\mathbf{CP}^{p^{s_1}-1}])v_{n-s_1}^{p^{s_1}-1} \times \cdots \\ & \times ([\mathbf{CP}^{p^{s_m}-1}])v_{n-s_1-\cdots-s_m}^{p^{s_m}-1})(pt_i) \end{aligned} \tag{34.5.6}$$

where the congruence is modulo the ideal $(t_i t_j \mid i, j \in \mathbf{N})$, and where the first sum is over all sequences $(s_1, \ldots, s_m, i, j)$ such that $s_l, i, j \in \mathbf{N}$, $m \in \mathbf{N} \cup \{0\}$, and $s_1 + \cdots + s_m + i + j = n$ and the second sum is over all sequences $(s_1, \ldots, s_m, i)$ such that $s_l, i \in \mathbf{N}$, $m \in \mathbf{N} \cup \{0\}$, and $s_1 + \cdots + s_m + i = n$.

From (34.5.5) and (34.5.6) one can simply read off a number of explicit formula and congruences for the cohomology operations r_E: $BP(pt) \to BP(pt)$.

First, we note that if we give V_i and T_i weight $2(p^i - 1)$, then $\bar{V}_n$, V_n, $a_n(V, T)$, $a_n(V)$ are all homogeneous of weight $2(p^n - 1)$. So if we attach weight

$$\|E\| = 2(p-1)e_1 + 2(p^2-1)e_2 + \cdots$$

to an exponent sequence, we have

$$r_t(v_n) = \sum_E r_E(v_n) t^E$$

with $r_E(v_n)$ of dimension $2(p^n - 1) - \|E\|$. A corollary of (34.5.5) is now:

■ (34.5.7) **Lemma** Let $E = (e_1, e_2, \ldots)$ be an exponent sequence such that $e_1 = e_2 = \cdots = e_{n-1} = 0$ and $\|E\| > 2(p^{n+h} - p^{h+1})$. Then $r_E(v_{n+h}) \equiv 0 \bmod(p, v_1, \ldots, v_{h-1})$ unless $E = p^h\Delta_n$; then $r_E(v_{n+h}) \equiv v_h \bmod(p, v_1, \ldots, v_{h-1})$.

A related result is the following generalization of Lemma 1.7 of [210] (sometimes known as the Budweiser lemma).

■ (34.5.8) **Lemma**

(i) For $n \geq 3$ and $2 \leq l \leq n-1$, we have:
  (a) $r_E(v_n) \equiv 0 \bmod(p^{p+1}, v_1, \ldots, v_{l-1})$ if $2(p^n - p^{l-1}) > \|E\| \geq 2(p^n - p^l)$ and E not equal to $p^l\Delta_{n-l}$ or
$$\Delta_1 + (p-1)\Delta_{n-1} + p^l\Delta_{n-l-1};$$
  (b) $r_E(v_n) \equiv v_l \bmod(p^{p+1}, v_1, \ldots, v_{l-1})$ if $E = p^l\Delta_{n-l}$;
  (c) $r_E(v_n) \equiv -p^p v_l \bmod(p^{p+1}, v_1, \ldots, v_{l-1})$ if
$$E = \Delta_1 + (p-1)\Delta_{n-1} + p^l\Delta_{n-l-1}.$$

(ii) For $n \geq 3$ (and $l = 0$), we have:
  (a) $r_E(v_n) \equiv 0 \bmod(p^{p+2})$ if $\|E\| \geq 2(p^n - 1)$ and E not equal to Δ_n or $\Delta_1 + p\Delta_{n-1}$;
  (b) $r_E(v_n) = p$ if $E = \Delta_n$;
  (c) $r_E(v_n) \equiv -p^p \bmod(p^{p+2})$ if $E = p\Delta_{n-1} + \Delta_1$.

(iii) For $n \geq 3$ (and $l = 1$), we have:
  (a) $r_E(v_n) \equiv 0 \bmod(p^{p+1})$ if $2(p^n - 1) > \|E\| \geq 2(p^n - p)$ and E not equal to $p\Delta_{n-1}$ or $\Delta_1 + (p-1)\Delta_{n-1} + p\Delta_{n-2}$;
  (b) $r_E(v_n) \equiv v_1(1 - p^{p-1}) \bmod(p^{p+1})$ if $E = p\Delta_{n-1}$;
  (c) $r_E(v_n) \equiv -p^p v_1 \bmod(p^{p+1})$ if $E = \Delta_1 + (p-1)\Delta_{n-1} + p\Delta_{n-2}$.

(iv) For $n = 1$, we have $r_{\Delta_1}(v_1) = p$.

(v) For $n = 2$, we have:
  (a) $r_E(v_2) = 0$ if $\|E\| \geq 2(p^2 - p)$ and E not equal to Δ_2, $p\Delta_1$, $(p+1)\Delta_1$;
  (b) $r_E(v_2) = p$ if $E = \Delta_2$;
  (c) $r_E(v_2) = -p^p$ if $E = (p+1)\Delta_1$;
  (d) $r_E(v_2) = (1 - p^{p-1} - p^p)v_1$ if $E = p\Delta_1$.

Here $\Delta_0 = (0, 0, \ldots)$. This is proved starting from Theorem (19.3.7) of Chapter IV (a precursor of (34.5.5) and (34.5.6)). For details cf. [172]. The Budweiser lemma results from (34.5.8) by considering congruences $\bmod(p, v_1, \ldots, v_{l-1})$ rather than $\bmod(p^{p+1}, v_1, v_2, \ldots, v_{l-1})$.

The congruence (34.5.6) is modulo the ideal generated by all products $t_i t_j$, $i, j \in \mathbf{N}$. So the coefficient of t_i in the expression on the right of (34.5.6) is equal to $r_{\Delta_i}(v_n)$. We shall not write out the explicit formula; it is obtained from (34.5.6) by setting $t_j = 0$ for all $j \neq i$.

We have according to formula (3.3.8) of Chapter I

$$m_{p^n-1} = p^{-n}[\mathbf{CP}^{p^n-1}] = \sum_{i_1+\cdots+i_r=n} p^{-r} v_{i_1} v_{i_1}^{p^{i_1}} \cdots v_{i_r}^{p^{i_1+\cdots+i_{r-1}}}$$

It follows that $[\mathbf{CP}^{p^n-1}] \equiv v_1 v_1^p \cdots v_1^{p^{n-1}} = v_1^{(p-1)^{-1}(p^n-1)} \bmod p$. Using (34.5.6), it follows that modulo p

$$r_{\Delta_i}(v_n) \equiv -v_{n-i}^{p^i} + \sum (-1)^{m+1} v_1^{(p-1)^{-1}(p^{s_1}+\cdots+p^{s_m}-m)} \times v_{n-s_1}^{p^{s_1}-1} v_{n-s_1-s_2}^{p^{s_2}-1} \cdots v_{n-s_1-\cdots-s_m}^{p^{s_m}-1} v_j^{p^i}$$

where the sum is over all sequences $(s_1, \ldots, s_m, j)$ such that $s_l, j \in \mathbf{N}$, $s_1 + \cdots + s_m + j = n - i$.

■ (34.5.9) **Corollary** For $0 < i < n$, $r_{\Delta_i}(v_n) \equiv -v_{n-i}^{p^i} \bmod (p, v_1)$ and

$$r_{\Delta_i}(v_n) \equiv -v_{n-i}^{p^i} + v_1 v_{n-1}^{p-1} v_{n-i-1}^{p^i} - v_1^2 v_{n-1}^{p-1} v_{n-2}^{p-1} v_{n-i-2}^{p^i} + \cdots + (-1)^{m+1} v_1^m v_{n-1}^{p-1} \cdots v_{n-m}^{p-1} v_{n-i-m}^{p^i}$$

modulo(p, v_1^{p+1}), where $m = \min(n - i - 1, p)$.

35 Tate Modules (for One Dimensional Formal Group Laws)

In this section A is a complete discrete valuation ring of characteristic zero with residue field k of characteristic $p > 0$. We denote the quotient field of A by K, the algebraic closure of K with K_{sc}. If $K \subset L \subset K_{sc}$, then $A(L)$ is the ring of integers of L; $\mathfrak{m}(L)$ is the maximal ideal of L; $U(L) = A(L^*)$, the group of units of $A(L)$; v denotes the normalized exponential valuation on K, and we also use v to denote its extension to a valuation on K_{sc}.

All formal groups in this section (35) will be *commutative, one dimensional, and of finite height* (unless something else is explicitly mentioned). Under this assumption $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is of finite height iff $\alpha(X) \neq 0$. So isogenies are simply nonzero homomorphisms in this case.

35.1 Points of finite order: $\Lambda(F)$ and $F(K_{sc})$

■ (35.1.1) **Points of a formal group law** Let $F(X, Y)$ be a formal group law over A. We write $F(K_{sc})$ for the group of points of $F(X, Y)$ with values in K_{sc}; cf. Chapter I, Section 1.3. That is, as a set, $F(K_{sc})$ is the set of topologically nilpotent elements of K_{sc}, i.e., $\mathfrak{m}(K_{sc})$; and the addition of $F(K_{sc})$ is given by the formula $x +_F y = F(x, y)$. We define $\Lambda(F)$ as the torsion subgroup of $F(K_{sc})$.

■ (35.1.2) **Lemma** $F \mapsto F(K_{sc})$ and $F \mapsto \Lambda(F)$ are functors $\mathbf{FG}_A \to \mathbf{Mod}_\Gamma$, where $\Gamma = \mathrm{Gal}(K_{sc}/K)$ is the Galois group and $\mathbf{Mod}_\Gamma$ is the category of Γ-modules (discrete topology on $F(K_{sc})$ and $\Lambda(F)$, Krull topology on Γ; cf. (24.1.1)–(24.1.2) in Chapter IV).

Proof If $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is a homomorphism of formal group laws over A, then $x \mapsto \alpha(x)$ defines a group homomorphism $F(K_{sc}) \to G(K_{sc})$ which takes $\Lambda(F)$ into $\Lambda(G)$. If $\alpha \in F(K_{sc})$, then $\alpha \in F(L)$ for some finite extension L/K, so $\{\sigma \in \Gamma \mid \sigma(\alpha) = \alpha\}$ is an open subgroup of Γ.

■ (35.1.3) **Examples**

(i) If $F(X, Y) = \hat{\mathbf{G}}_a(X, Y)$ over A, then $\hat{\mathbf{G}}_a(K_{sc}) = \mathfrak{m}(K_{sc})$ with its original addition.

(ii) If $F(X, Y) = \hat{\mathbf{G}}_M(X, Y)$ over A, then, using $(1 + X)(1 + Y) = 1 + X + Y + XY$, we can identify $\hat{\mathbf{G}}_m(K_{sc}) = U^1(K_{sc}) = 1 + \mathfrak{m}(K_{sc})$, the subgroup of $U(K_{sc})$ consisting of elements $\equiv 1 \bmod \mathfrak{m}(K_{sc})$; in this case $\Lambda(\hat{\mathbf{G}}_m)$ is the subgroup of all p^rth roots of unity in K_{sc}, $r = 1, 2, 3, \ldots$.

(iii) We have already encountered $F(K_{sc})$ and $\Lambda(F)$ before in Section 32.1 for the case of a Lubin–Tate formal group law $F_e(X, Y)$ over A. (There we wrote $M_e(K_{sc})$ for $F(K_{sc})$ and Λ_e for $\Lambda(F)$.)

■ (35.1.4) **Filtration of $F(K_{sc})$** For each $\rho \in \mathbf{R}$ let $F^\rho(K_{sc})$ be the subgroup of all elements $x \in F(K_{sc})$ such that $v(x) \geq \rho$ and $F^{\rho+}(K_{sc}) = \{x \in F(K_{sc}) \mid v(x) > \rho\}$. These are subgroups of $F(K_{sc})$; and because $F(X, Y) \equiv X + Y \bmod$ degree 2, we have that $x +_F y \equiv x + y \bmod F^{\rho+}(K_{sc})$ if $x, y \in F^\rho(K_{sc})$ (if $\rho > 0$).

■ (35.1.5) **Proposition** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be an isogeny of height h over A (i.e., $\alpha(X) \equiv uX^{p^h} \bmod(\mathfrak{m}(K)$, degree $p^h + 1)$, $u \in U(A)$; cf. Section 18.3 of Chapter IV and Section 28.2 of Chapter V). Then we have:

(i) $\alpha(K_{sc})$: $F(K_{sc}) \to G(K_{sc})$ is surjective.
(ii) The kernel of $\alpha(K_{sc})$ is a finite group of order p^h.

Proof Let $y \in G(K_{sc})$. Consider the polynomial $\alpha(X) - y$. The Weierstrass degree of $\alpha(X)$ is p^h (cf. Appendix A.3). Hence we can factor $\alpha(X) - y = g(X)u(X)$ where $g(X)$ is a distinguished polynomial over $A(L)$ (where L/K is a finite field extension such that $y \in L$) and where $u(X)$ is a unit in $A(L)[\![X]\!]$. Since $g(X) \equiv X^{p^h} \bmod \mathfrak{m}(L)$, there are roots of $g(X)$ in $\mathfrak{m}(K_{sc})$. This proves (i). Now take $y = 0$. If x is a root of $\alpha(X)$, $x \in \mathfrak{m}(K_{sc})$, then $u(x)$ converges and is $\neq 0$, hence $g(x) = 0$. So the roots of $\alpha(X)$ are precisely those of $g(X)$, and there will be precisely p^h of them if $\alpha(x) = 0 \Rightarrow (d\alpha/dX)(x) \neq 0$. To see this we differentiate the equation $\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$ with respect to Y to obtain

$$\frac{d\alpha}{dX}(F(X, Y)) \cdot \frac{\partial F}{\partial Y}(X, Y) = \frac{\partial G}{\partial Y}(\alpha(X), \alpha(Y)) \cdot \frac{d\alpha}{dX}(Y)$$

Substituting $X = x$, $Y = 0$ where $\alpha(x) = 0$, we obtain

$$\frac{d\alpha}{dX}(x) \cdot \frac{\partial F}{\partial Y}(x, 0) = \frac{\partial G}{\partial Y}(0, 0) \cdot \frac{d\alpha}{dX}(0)$$

Now $(d\alpha/dX)(0) \neq 0$ because (since A is of characteristic zero) $\alpha(X)$ is of the form $\alpha(X) = g^{-1}(af(X))$ for some $a \in A$ and hence $0 \neq a = (d\alpha/dX)(0)$ if $\alpha(X) \neq 0$; also $(\partial G/\partial Y)(0, 0) = 1$. Hence $(d\alpha/dX)(x) \neq 0$ if $\alpha(x) = 0$. Q.E.D.

■ (35.1.6) **Corollary** Let $F(X, Y)$ be a formal group law over A. Then:

(i) $F(K_{sc})$ is a divisible group and so is $\Lambda(F)$.

(ii) If $m \in \mathbf{N}$, $(m, p) = 1$, then every element of $F(K_{sc})$ is uniquely divisible by m.

(iii) $\Lambda(F) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^h$ where $h = ht(F(X, Y))$.

Proof To prove (i) apply for all $m \in \mathbf{N}$ (35.1.5)(i) to the isogeny $[m]_F(X)$: $F(X, Y) \to F(X, Y)$ which is of height p^{rh} if $p^r \mid m$ but $p^{r+1} \nmid m$. For (ii), note that m is a unit if $(m, p) = 1$, so that $[m]_F(X)$ is an isomorphism for these m. As to (iii), $\Lambda(F)$ as the torsion subgroup of a divisible group is divisible; also all elements of $\Lambda(F)$ are of order a power of p (by (ii)). Therefore $\Lambda(F) = (\mathbf{Q}_p/\mathbf{Z}_p)^c$ for some c where $c = \dim_{\mathbf{F}_p}(\mathrm{Ker}[p]_F)$. But $\dim(\mathrm{Ker}[p]_F) = h$ by part (ii) of Proposition (35.1.5). Q.E.D.

(35.1.7) Let $f(X)$ be the logarithm of $F(X, Y)$. Recall that if $f(X) = \sum_{n=1}^{\infty} n^{-1} c_n X^n$, then $c_n \in A$. We now have:

■ (35.1.8) **Proposition**

(i) $f(x)$ converges for all $x \in \mathfrak{m}(K_{sc})$ and $f^{-1}(x)$ converges if $v(x) > (p-1)^{-1}$.

(ii) $x \mapsto f(x)$ is a homomorphism of Γ-modules $F(K_{sc}) \to K_{sc}(+)$ where $K_{sc}(+)$ is the additive group underlying K_{sc}.

(iii) The sequence $0 \to \Lambda(F) \to F(K_{sc}) \to K_{sc}(+) \to 0$ is exact.

(iv) $f(X)$ and $f^{-1}(X)$ define a filtration preserving inverse isomorphism $F^{r+}(K_{sc}) \xrightarrow{\sim} \hat{\mathbf{G}}_a^{r+}(K_{sc})$ where $r = (p-1)^{-1}$.

To prove this theorem we need a lemma:

■ (35.1.9) **Lemma** Let $s \in \mathbf{R}$, $s > 0$. Then there exists an $n \in \mathbf{N}$ (depending on s) such that $v([p^n](x)) > (p-1)^{-1}$ for all x with $v(x) > s$.

Proof We have $[p](X) \equiv pX \bmod(\text{degree } 2)$. Hence $v([p](x)) \geq \min(s+1, 2s)$ if $v(x) \geq s$. By induction this gives $v([p^n](x)) \geq \min(1+s, 2^n s)$. So it suffices to take n such that $2^n s > (p-1)^{-1}$.

■ (35.1.10) **Proof of Proposition (35.1.8)** We can assume that $F(X, Y)$ is a p-typical formal group law. Write $f(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$. Then $v(a_n) \geq -n$. Let $y \in \mathfrak{m}(K_{sc})$; then

$$v(a_n y^{p^n}) \geq p^n v(y) - n \tag{35.1.11}$$

It follows from (35.1.11) that $v(a_n y^{p^n}) \to \infty$ as $n \to \infty$ if $v(y) > 0$. Moreover, one easily checks that

$$v(a_n y^{p^n}) \geq v(y) \quad \text{if} \quad v(y) \geq (p-1)^{-1} \tag{35.1.12}$$

Now let z be an element of $\mathfrak{m}(K_{sc})$ of valuation precisely $(p-1)^{-1}$. Then by (35.1.12) $g(X) = z^{-1}f(zX) \in A[\![X]\!]$; moreover, $g(X) \equiv X$ mod(degree 2) and hence $g^{-1}(X) \in A[\![X]\!]$. But $g^{-1}(X) = z^{-1}f^{-1}(zX)$, so $f^{-1}(zX) \in A[\![X]\!]$ for all z of valuation $(p-1)^{-1}$. This means that $f^{-1}(x)$ converges if $v(x) > (p-1)^{-1}$ and also shows that $f^{-1}(X)$ maps $\hat{\mathbf{G}}_a^{r+}(K_{sc})$ into $F^{r+}(K_{sc})$ with $r = (p-1)^{-1}$. This proves (i) and (iv). Part (ii) of the proposition is a triviality. As to (iii), clearly $\Lambda(F) \subset \mathrm{Ker}(f)$ because $\Lambda(F) = \bigcup \mathrm{Ker}[p^n](X)$ and $f([p^n](X)) = p^n f(X)$ and p^n: $K_{sc}(+) \to K_{sc}(+)$ is injective.

Conversely, suppose that $x \in \mathrm{Ker}(f)$. There is an n such that $v([p^n](x)) > (p-1)^{-1}$ (Lemma (35.1.9)). Then $f([p^n](x)) = p^n f(x) = 0$, so by part (iv) of the proposition (which has already been proved) $[p^n](x) = 0$, i.e., $x \in \Lambda(F)$. It remains to prove the surjectivity of f. Let $x \in K_{sc}(+)$. There is an n such that $v(p^n x) > (p-1)^{-1}$. Let $y = f^{-1}(p^n x)$, then $f(y) = p^n x$ (using parts (i) or (iv) again). By Corollary (35.1.6) there is a $z \in F(K_{sc})$ such that $[p^n](z) = y$, then $p^n(x) = f(y) = f([p^n](z)) = p^n f(z)$, hence $f(z) = x$.

35.2 Isogenies and finite subgroups of $F(K_{sc})$

We have seen that if $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is an isogeny, then the kernel of $\alpha(K_{sc})$: $F(K_{sc}) \to G(K_{sc})$ is a finite subgroup. The converse is also true: every finite subgroup is the kernel of an isogeny.

(35.2.1) **Theorem** Let $N \subset I(K_{sc})$ be a finite subgroup. Let $\Gamma_0 = \{\tau \in \Gamma \mid \tau y \in N \text{ for all } y \in N\}$ be the stabilizer subgroup of N. Let L_0 be the field of invariants of Γ_0 (so L_0/K is a finite field extension). Then there exists a formal group law $G(X, Y)$ over $A(L_0)$ and an isogeny $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over $A(L_0)$ such that the following two properties hold:

(i) $\mathrm{Ker}(\alpha(K_{sc})) = N$.

(ii) If $\beta(X)$: $F(X, Y) \to H(X, Y)$ is an isogeny over $A(L')$, L' a finite field extension of L_0, such that $\mathrm{Ker}(\beta(K_{sc})) \supset N$, then there exists a unique isogeny $\hat{\beta}(X)$: $G(X, Y) \to H(X, Y)$ such that $\beta(X) = \hat{\beta}(X) \circ \alpha(X)$.

(In a sense that can be made precise, this theorem says that quotients of one dimensional commutative finite height formal groups by finite subgroups exist and are one dimensional commutative finite height formal groups.)

Before proving the theorem we state a number of corollaries.

■ (35.2.2) **Corollary**

(i) Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be an isogeny over $A(L)$ where L/K is finite, then there also exists an isogeny $\beta(X)$: $G(X, Y) \to F(X, Y)$ over $A(L)$.

(ii) Suppose that $\mathbf{FG}_A(F(X, Y), G(X, Y)) \neq \{0\}$. Then the quotient fields of $J(\mathrm{End}_A(F(X, Y)))$ and $J(\mathrm{End}_A(G(X, Y)))$ (as subfields of K_{sc}) are equal.

Proof Let $N = \mathrm{Ker}(\alpha(K_{sc}))$, then $L_0 \subset L$. Because N is finite there is an $r \in \mathbf{N}$ such that $N \subset \mathrm{Ker}[p^r]_F(X)$. By part (ii) of Theorem (35.2.1) this means

that there exists a $\beta(X)$: $G(X, Y) \to F(X, Y)$ such that $\beta(X) \circ \alpha(X) = [p^r]_F(X)$ and $\beta(X) \neq 0$ because $[p^r]_F(X) \neq 0$. This proves (i).

As to (ii), first note that if $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is $\neq 0$ (i.e., an isogeny), then $\beta(X) \mapsto \alpha(X) \circ \beta(X)$ is an injective (left) $\mathrm{End}_A(G(X, Y))$-module homomorphism $\mathbf{FG}_A(G(X, Y), F(X, Y)) \to \mathrm{End}_A(G(X, Y))$. Let

$$A_F = J(\mathrm{End}_A(F(X, Y))),$$

L_F the quotient field of A_F. Let $B_{GF} = J(\mathbf{FG}_A(G(X, Y), F(X, Y)))$ and $T_F = \mathrm{End}_{A_F}(B_{GF})$. Similarly, one defines A_G, L_G, T_G. Since B_{GF} is isomorphic to an ideal of A_G, we have that $T_G \subset L_G$ and $T_G \supset A_G$. Now also $A_F \subset T_G$ since A_F acts (on the right) on B_{GF}. Hence $L_F \subset$ quotient field $(T_G) = L_G$. Similarly, using part (i) of the corollary, one shows that $L_G \subset L_F$. Q.E.D.

■ (35.2.3) To prove Theorem (35.2.1) we need some preliminaries. Let R be any complete Hausdorff local ring with maximal ideal $\mathfrak{m}_R$. Consider $R[\![X]\!]$, the ring of power series in one variable over R. This is also a complete Hausdorff local ring, the maximal ideal being $XR[\![X]\!] + \mathfrak{m}_R[\![X]\!]$. Let w be the associated filtration function (cf. Appendix A.2). Let $t \in R[\![X]\!]$ and suppose that $t \notin R$ and $t \in XR[\![X]\!] + \mathfrak{m}_R[\![X]\!]$. Then $T \mapsto t$ defines a continuous injective (local) homomorphism of local rings $R[\![T]\!] \to R[\![X]\!]$, permitting us (by identifying t and T) to view $R[\![T]\!]$ as a closed local subring of $R[\![X]\!]$.

(35.2.4) **Lemma** Let $X \in R[\![X]\!] \supset R[\![T]\!]$ be a root of a (distinguished) polynomial $g(Z) = Z^n - t_{n-1}Z^{n-1} - \cdots - t_1 Z - t_0$ with coefficients in $R[\![T]\!]$ such that $w(t_i) \geq n - i$ for $i = 0, 1, \ldots, n-1$. Then $R[\![X]\!]$ is (finitely) generated as an $R[\![T]\!]$-module by the n elements $1, X, \ldots, X^{n-1}$.

Proof Let $r_{m,i} \in R[\![T]\!]$ for $m \in \mathbf{N} \cup \{0\}$, $i \in \{0, 1, \ldots, n-1\}$ be the unique elements of $R[\![T]\!]$ such that

$$Z^m \equiv \sum_{i=0}^{n-1} r_{m,i} Z^i \mod(g(Z))$$

Multiplying with Z we find the following recursion relations among the $r_{m,i}$:

$$r_{m+1,i} = r_{m,i-1} + r_{m,n-1} t_i \quad \text{if} \quad i \geq 1 \tag{35.2.5}$$

$$r_{m+1,0} = r_{m,n-1} t_0$$

Now $r_{m,i} = 0$ if $m < n$ and $m \neq i$, and $r_{m,m} = 1$ if $m < n$. Also $r_{n,i} = t_i$, $i = 0, 1, \ldots, n-1$. Hence $w(r_{m,i}) \geq m - i$ for $m \leq n$, and using induction and (35.2.5), it easily follows that $w(r_{m,i}) \geq m - i$ for all $m \in \mathbf{N} \cup \{0\}$. It follows that if $\sum a_m X^m$ is any element of $R[\![X]\!]$, then $\sum a_m r_{m,i}$ converges for all i (in $A[\![T]\!]$). Hence

$$\sum_{m=0}^{\infty} a_m X^m = \sum_{i=0}^{n-1} \left(\sum_{m=0}^{\infty} a_m r_{m,i} \right) X^i$$

which proves the lemma.

■ (35.2.6) Now let $F(X, Y)$ be a formal group law over R and let $y \in \mathfrak{m}_R$. Then $X \mapsto F(X, y)$ defines a continuous homomorphism ϕ_y: $R[\![X]\!] \to R[\![X]\!]$ (cf. Appendix A.4). Let $z \in \mathfrak{m}_R$. Then

$$\text{(35.2.7)} \qquad \phi_z(\phi_y(X)) = \phi_z(F(X, y)) = F(F(X, z), y)$$
$$= F(X, F(y, z)) = F(X, y +_F z) = \phi_{z +_F y}(X)$$

Taking z such that $y +_F z = 0$, we see that ϕ_y is in fact a continuous automorphism. And also by (35.2.7) if N is a finite subgroup of $F(R)$ ($= \mathfrak{m}_R$ as a set; addition: $(x, y) \mapsto F(x, y) = x +_F y$), then $y \mapsto \phi_y$ is an injective homomorphism of groups $N \to \mathrm{Aut}_R(R[\![X]\!])$ (injective because y is recoverable from ϕ_y as the constant term in $\phi_y(X)$).

■ (35.2.8) **Lemma** Using the notations of (35.2.6) let $T = \prod_{y \in N} F(X, y)$. Then the invariants of $R[\![X]\!]$ under the action of N above are precisely the elements of $R[\![T]\!]$ (i.e., $\{\alpha(X) \mid \phi_y(\alpha(X)) = \alpha(X) \text{ for all } y \in N\} = R[\![T]\!]$).

Proof Let us write $\mathrm{Inv}_N(R[\![X]\!]) = \{\alpha(X) \in R[\![X]\!] \mid \phi_y(\alpha(X)) = \alpha(X), \forall y \in N\}$. Because N is a subgroup of $F(R)$ and (35.2.7), we have that $T \in \mathrm{Inv}_N(R[\![X]\!])$; also of course $R \subset \mathrm{Inv}_N(R[\![X]\!])$, so (by continuity of the ϕ_y) we have that $R[\![T]\!] \subset \mathrm{Inv}_N(R[\![X]\!])$.

Now consider $F(Z, y)$ as a power series in Z over $R[\![T]\!]$. Its Weierstrass degree (cf. Appendix A.3) is clearly 1. It follows that

$$W\text{-degree}\left(\prod_{y \in N} F(Z, y) - T\right) = n = \#N$$

According to the formal Weierstrass preparation theorem (cf. Appendix A.3) there is a unique factorization

$$g(Z)u(Z) = -T + \prod_{y \in N} F(Z, y)$$

where $g(Z)$ is a distinguished polynomial of degree n over $R[\![T]\!]$ and $u(Z)$ is an invertible power series over $R[\![T]\!]$. Now by definition

$$T = \prod_{y \in N} F(X, y)$$

so that the $F(X, y)$, $y \in N$, are all roots of $g(Z)u(Z)$ (use (35.2.7)) and hence of $g(Z)$. There are n different $F(X, y)$, and degree$(g(Z)) = n$. Hence

$$g(Z) = \prod_{y \in N} (Z - F(X, y))$$

Now $F(X, y) \in XR[\![X]\!] + \mathfrak{m}_R[\![X]\!]$ and hence $g(Z)$ satisfies the condition of Lemma (35.2.4); it follows that $R[\![X]\!]$ as a module over $R[\![T]\!]$ is generated by $1, X, \ldots, X^{n-1}$.

Now let Φ_T be the quotient field of $R[\![T]\!]$ and Φ_X be the quotient field of $R[\![X]\!]$. Then, by what we have just proved,

$$[\Phi_X : \Phi_T] \leq n$$

Let $\Phi = \mathrm{Inv}_N(\Phi_X)$. Then $[\Phi_X : \Phi] = n$ by Galois theory (cf., e.g., [205, Vol. III, Chapter I, Section 4, Theorem 5]). Also $\Phi_T \subset \Phi$ because $A[\![T]\!] \subset \mathrm{Inv}_N(R[\![X]\!])$. Hence $\Phi_T = \Phi = \mathrm{Inv}_N(\Phi_X)$. It follows that $g(Z)$ is irreducible and hence that the $R[\![T]\!]$-module $R[\![X]\!]$ is free with basis $1, X, \ldots, X^{n-1}$.

Now let $\alpha(X) \in \mathrm{Inv}_N(R[\![X]\!])$. Write $\alpha(X)$ as a unique sum $\alpha(X) = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1}$, $r_i \in R[\![T]\!]$. Since $\mathrm{Inv}_N(\Phi_X) = \Phi_T$ and $1, X, \ldots, X^{n-1}$ is also a basis for Φ_X over Φ_T, it follows that $\alpha(X) = r_0$ in $R[\![T]\!]$. Q.E.D.

■ (35.2.9) **Proof of Theorem (35.2.1)** Let L/K be a finite field extension such that $N \subset F(L) \subset F(K_{sc})$ (then of course $L_0 \subset L$). Take

$$\alpha(X) = \prod_{y \in N} F(X, y) \in A[L][\![X]\!]$$

Then $\alpha(0) = 0$ (because $0 \in N$) and we have

$$\alpha(F(X, Y)) = \prod_{y \in N} F(F(X, Y), y) = \prod_{y \in N} F(X, F(Y, y)) \tag{35.2.10}$$

Now take $R = A(L)[\![X]\!]$ and consider $\alpha(F(X, Y))$ as an element of $R[\![Y]\!]$ and $F(X, Y)$ as a formal group law over R. Applying Lemma (35.2.7), we see that (since $\alpha(F(X, Y))$ is invariant under N also in this setting)

$$\alpha(F(X, Y)) \in R[\![T]\!], \qquad T = \prod_{y \in N} F(Y, y) = \alpha(Y) \tag{35.2.11}$$

Now take $R' = A(L)[\![\alpha(Y)]\!]$. By (35.2.11) we can consider $\alpha(F(X, Y))$ as an element of $R'[\![X]\!] = A(L)[\![\alpha(Y)]\!][\![X]\!] = A(L)[\![X]\!][\![\alpha(Y)]\!]$. Then $\alpha(F(X, Y))$ is again invariant under N in this new setting (cf. (35.2.10)); and applying Lemma (35.2.7) again, we find $\alpha(F(X, Y)) \in A(L)[\![\alpha(X), \alpha(Y)]\!]$, so we can write

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y)) \tag{35.2.12}$$

for some power series $G(X, Y) \in A(L)[\![X, Y]\!]$. We have already seen that $\alpha(0) = 0$. As to the coefficient of X in $\alpha(X)$, observe that since $\alpha(X) = \prod F(X, y)$

$$\frac{d\alpha}{dX}(0) = \sum_y \frac{\partial F}{\partial X}(X, y) \prod_{z \neq y} F(X, z)$$

Substituting $X = 0$ and using that $0 \in N$, we see that

$$\frac{d\alpha}{dX}(0) = \frac{\partial F}{\partial X}(0, 0) \prod_{z \neq 0} F(0, z) \neq 0$$

because $(\partial F/\partial X)(0, 0) = 1$ and $F(0, z) = z$. It follows that $\alpha^{-1}(X)$ exists at least as a power series over L, so that by (35.2.12)

$$G(X, Y) = \alpha(F(\alpha^{-1}(X), \alpha^{-1}(Y))) \tag{35.2.13}$$

proving that $G(X, Y)$ is associative, commutative, and that $G(X, 0) = X$. Hence $G(X, Y)$ is a formal group law over $A(L)$ and by (35.2.12) $\alpha(X)$ is a homomorphism of formal group laws over $A(L)$.

Clearly, $y \in \mathrm{Ker}(\alpha(K_{sc}))$ for $y \in N$ because $F(y, z) = y +_F z \in N$ for all y, $z \in N$. So $N \subset \mathrm{Ker}(\alpha(K_{sc}))$. But the Weierstrass degree of $\alpha(X)$ is n so $N = \mathrm{Ker}(\alpha(K_{sc}))$. Finally, we note that $\alpha(X)$ is invariant under Γ_0 (acting on coefficients) so that in fact $\alpha(X) \in L_0[\![X]\!] \subset L[\![X]\!]$ and hence being integral $\alpha(X) \in A(L_0)[\![X]\!]$. By (35.2.13) it follows that then also $G(X, Y) \in A(L_0)[\![X]\!]$. This proves part (i) of the theorem.

Now let $\beta(X)$: $F(X, Y) \to H(X, Y)$ be an isogeny over $A(L') \supset A(L_0)$. Let L/K be finite such that $L' \subset L$, $N \subset F(L)$. Then for all $y \in N$, we have

$$\phi_y(\beta(X)) = \beta(F(X, y)) = H(\beta(X), \beta(y)) = H(\beta(X), 0)) = \beta(X)$$

Take $R = A(L)$ this time, then a third application of Lemma (35.2.7) gives us that $\beta(X) \in A(L)[\![\alpha(X)]\!]$, i.e., $\beta(X) = \hat{\beta}(\alpha(X))$. Using $\alpha^{-1}(X)$ again, we see that $\hat{\beta}(X) = \beta(\alpha^{-1}(X)) \in L'[\![X]\!]$ since $L' \supset L_0$ and hence $\hat{\beta}(X) \in A(L')[\![X]\!]$. Further, $\hat{\beta}(G(X, Y)) = \beta(\alpha^{-1}(G(X, Y))) = \beta(F(\alpha^{-1}(X), \alpha^{-1}(Y)) = H(\beta(\alpha^{-1}(X)), \beta(\alpha^{-1}(Y))) = H(\hat{\beta}(X), \hat{\beta}(Y))$ and $\hat{\beta}(X) = \beta(\alpha^{-1}(X)) \neq 0$. This concludes the proof of the theorem.

35.3 Tate module of a formal group law

■ (35.3.1) **Definition of the functor** $T(F)$ Let $F(X, Y)$ be a formal group law over A. The abelian group $F(K_{sc})$ is a $\mathbf{Z}_p$-module via the action $ax = [a]_F(x)$, $a \in \mathbf{Z}_p$, $x \in F(K_{sc})$ and $\Lambda(F)$ is a $\mathbf{Z}_p$-submodule. One now defines

$$T(F) = \mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, F(K_{sc})) = \mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \Lambda(F)) \tag{35.3.2}$$

Since $F(X, Y) \mapsto F(K_{sc})$ and $\Lambda(F)$ are functors, we immediately observe that $F(X, Y) \mapsto T(F)$, $\alpha(X) \mapsto \mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \alpha(K_{sc}))$ is a functor.

We have seen that $\Lambda(F) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^h$ where $h = \mathrm{ht}(F(X, Y))$. Using $\mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p/\mathbf{Z}_p, \mathbf{Q}_p/\mathbf{Z}_p) = \mathbf{Z}_p$, we note that as a $\mathbf{Z}_p$-module we have

$$T(F) \simeq \mathbf{Z}_p^h \tag{35.3.3}$$

■ (35.3.4) **Description of** $T(F)$ Let M be any abelian group. A homomorphism α: $\mathbf{Q}_p/\mathbf{Z}_p \to M$ is uniquely determined by giving $\alpha(p^{-i})$, $i = 1, 2, \ldots$. And conversely, given a sequence $(m_1, m_2, \ldots)$ of elements of M, then there is a homomorphism α: $\mathbf{Q}_p/\mathbf{Z}_p \to M$ such that $\alpha(p^{-i}) = m_i$ if and only if $pm_{i+1} = m_i$ for $i \in \mathbf{N}$ and $pm_1 = 0$.

Applying this to $M = \Lambda(F)$, we see that

$$T(F) = \{(x_1, x_2, \ldots) \mid x_i \in \Lambda(F),\ [p_F](x_{i+1}) = x_i,\ i \in \mathbf{N},\ [p_F](x_1) = 0\} \tag{35.3.5}$$

with coordinatewise addition

$$(x_1, x_2, \ldots) + (y_1, y_2, \ldots) = (x_1 +_F y_1, x_2 +_F y_2, \ldots),$$

or in other words

$$T(F) = \varprojlim \mathrm{Ker}([p^n]_F(K_{sc}))$$

where the projective limit is taken with respect to the maps

$$[p]_F(K_{sc})\colon \mathrm{Ker}([p^{n+1}]_F) \to \mathrm{Ker}([p^n]_F)$$

Let $x_1(1), \ldots, x_1(h)$ be a basis for the $\mathbf{F}_p$-module $\mathrm{Ker}([p]_F(K_{sc}))$. Then one can find sequences $(x_1(i), x_2(i), \ldots)$ such that $[p]_F(x_{n+1}(i)) = x_n(i)$ for all $n \in \mathbf{N}$. It is now not difficult to check that $\{(x_1(1), x_2(1), \ldots), \ldots, (x_1(h), x_2(h), \ldots)\}$ is a basis for $T(F)$ as a $\mathbf{Z}_p$-module.

■ (35.3.6) **The functor $V(F)$** One also defines

(35.3.7) $$V(F) = \mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p, \Lambda(F))$$

and, arguing as above in (35.3.4), we see that

(35.3.8) $$V(F) = \{(x_0, x_1, \ldots) \mid x_i \in \Lambda(F),\ [p]_F(x_{i+1}) = x_i, \text{ all } i \in \mathbf{N} \cup \{0\}\}$$

with componentwise addition, or, in other words

$$V(F) = \varprojlim \Lambda(F)$$

under the maps $[p]_F(K_{sc})\colon \Lambda(F) \to \Lambda(F)$. Since $\Lambda(F) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^h$ and $\mathbf{Mod}_{\mathbf{Z}_p}(\mathbf{Q}_p, \mathbf{Q}_p/\mathbf{Z}_p) = Q_p$ we see that

$$V(F) \simeq \mathbf{Q}_p^h$$

as a $\mathbf{Z}_p$-module.

(35.3.9) **Proposition** There is an exact sequence

$$0 \to T(F) \to V(F) \to \Lambda(F) \to 0$$

where the first map is the natural inclusion $T(F) \subset V(F)$, $(x_1, x_2, \ldots) \mapsto (0, x_1, x_2, \ldots)$ (cf. (35.3.5), (35.3.8)) and where the second map is $(x_0, x_1, \ldots) \mapsto x_0$.

Proof If $(x_0, x_1, \ldots) \in V(F)$ and $x_0 = 0$, then $(x_1, x_2, \ldots) \in T(F)$, and the surjectivity of $V(F) \to \Lambda(F)$ is immediate by (35.1.6) and (35.3.8).

■ (35.3.10) **Remark** One has an exact sequence $0 \to \mathbf{Z}_p \to \mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to 0$ and (35.3.9) can be seen as the result of applying $\mathbf{Mod}_{\mathbf{Z}_p}(-, \Lambda(F))$ to this exact sequence.

■ (35.3.11) Let v be the extension to K_{sc} of the normalized exponential valuation v on $\mathbf{Q}_p$. It is often useful to know something about the valuations of the x_i in an element $\mathbf{x} = (x_0, x_1, \ldots) \in V(F)$ or $T(F)$.

■ (35.3.12) **Lemma** Let $F(X, Y)$ be a formal group law of height h over A and

let $\varepsilon = v(\pi) = e(K/\mathbf{Q}_p)^{-1}$. Let $x, y \in \Lambda(F)$ and suppose that $[p]_F(y) = x$. Then we have:

(i) $x = 0,\ y \neq 0 \Rightarrow v(y) \leq 1$
(ii) $2 < v(x) < \infty \Rightarrow v(y) \leq v(x) - 1$
(iii) $1 < v(x) \leq 2 \Rightarrow v(y) \leq 1$
(iv) $\varepsilon < v(x) \leq 1 \Rightarrow v(y) \leq p^{-1}v(x)$
(v) $v(x) \leq \varepsilon \Rightarrow v(y) = p^{-h}v(x)$

Proof We can assume that $F(X, Y)$ is p-typical, so that in particular $F(X, Y) \equiv X + Y$ mod(degree p). Now write out $x = [p]_F(y)$ to obtain

$$x = py + \pi y^p(\cdots) + uy^{p^h} + y^{p^h+1}(\cdots), \qquad u \in U(A) \tag{35.3.13}$$

The proof of (35.3.13) is now a simple matter using $v(a + b) \geq \min(v(a), v(b))$ and $v(a + b) = \min\{v(a), v(b)\}$ if $v(a) \neq v(b)$. Here are the details: if $v(y) > 1$, then $v(py) = 1 + v(y)$ and $v(\pi y^p) > 1 + v(y)$, $v(y^{p^h}) > 1 + v(y)$. So in this case $v(x) = 1 + v(y)$. This proves (i), (ii), and (iii). Now assume $\varepsilon < v(x) \leq 1$ and $v(y) > p^{-1}v(x)$. Then $v(py) > 1 + p^{-1}v(x) > 1 \geq v(x)$, $v(\pi y^p) > \varepsilon + v(x) > v(x)$ and $v(y^{p^h}) > p^h \cdot p^{-1}v(x) > v(x)$, a contradiction with (35.3.13). Finally, assume that $v(x) \leq \varepsilon$. Then $v(py) > 1 \geq v(x)$, $v(\pi y^p) > \varepsilon > v(x)$, $v(y^{p^h+1}) > v(y^{p^h})$, so for (35.3.13) to hold we must have $p^h v(y) = v(x)$. Q.E.D.

■ (35.3.14) **Corollary** If $\mathbf{x} \in V(F)$, $\mathbf{x} \neq 0$, then $\lim_{n\to\infty}(v(x_n)) = 0$.

■ (35.3.15) **Proposition** $\alpha(X) \mapsto T(\alpha) \in \mathbf{Mod}_{\mathbf{Z}_p}(T(F), T(G))$ is an injective homomorphism from $\mathbf{FG}_A(F(X, Y), G(X, Y))$ to $\mathbf{Mod}_{\mathbf{Z}_p}(T(F), T(G))$.

Proof That $\alpha(X) \mapsto T(\alpha)$ is a homomorphism is obvious (it is a homomorphism of $\mathbf{Z}_p$-modules). Suppose that $T(\alpha) = 0$. Then let $\mathbf{x} \in T(F)$, $\mathbf{x} \neq 0$, $\mathbf{x} = (x_1, x_2, \ldots)$. Then $T(\alpha)(\mathbf{x}) = 0$, hence

$$0 = T(\alpha)(\mathbf{x}) = (\alpha(x_1), \alpha(x_2), \ldots)$$

and it follows that $\alpha(x_1) = \alpha(x_2) = \cdots = 0$. Now, if $\alpha(X) \neq 0$, then $\alpha(X)$ has finite Weierstrass degree (because $[p]_F(X)$ has finite Weierstrass degree; use e.g. (the proof of) Corollary (35.2.2)(i)) and hence only finitely many roots (use the formal Weierstrass preparation theorem). So it suffices to show that if $0 \neq \mathbf{x} \in T(F)$, then there are infinitely many different values among the x_i. This follows from Lemma (35.3.12) (or Corollary (35.3.14)).

■ (35.3.16) The Tate module functor $F \mapsto T(F)$ is a very useful tool in the study of formal group laws. Here are three applications of what we have done so far (the first two are reproofs of results that we have obtained before).

(35.3.17) The reduction map $\mathrm{Hom}_A(F(X, Y), G(X, Y)) \to \mathrm{Hom}_k(\bar{F}(X, Y), \bar{G}(X, Y))$ is injective (cf. Section 18.3 of Chapter IV).

Proof Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism and suppose that $\bar{\alpha}(X) = 0$. Then for all $\mathbf{x} \in T(F)$, $\mathbf{x} = (x_1, x_2, \ldots)$ we have $T(\alpha)(\mathbf{x}) = (y_1, y_2, \ldots)$ with $y_i = \alpha(x_i) \equiv 0 \bmod \pi$. Hence $y_i = 0$ for all i by Corollary (35.3.14); hence $T(\alpha) = 0$; hence $\alpha(X) = 0$ by Proposition (35.3.15).

(35.3.18) $\mathrm{End}_A(F(X, Y))$ is a free $\mathbf{Z}_p$-module of rank r a divisor of $\mathrm{ht}(F(X, Y))$.

Proof By Proposition (35.3.15) we have an injection $\mathrm{End}_A(F(X, Y) \to \mathrm{End}_{\mathbf{Z}_p}(T(F)) = M_{h\times h}(\mathbf{Z}_p)$, the ring of $h \times h$ matrices with coefficients in $\mathbf{Z}_p$. Tensoring with $\mathbf{Q}_p$ gives us an injection (as $\mathrm{End}_A(F(X, Y))$ is $\mathbf{Z}_p$-torsion free)

$$\mathrm{End}_A(F(X, Y)) \otimes \mathbf{Q}_p \mapsto M_{h\times h}(\mathbf{Q}_p)$$

Now $\mathrm{End}_A(F(X, Y)) \otimes \mathbf{Q}_p$ is commutative and hence, as a commutative subfield of $M_{h\times h}(\mathbf{Q}_p)$, its dimension r is a divisor of h. Q.E.D.

■ (35.3.19) **Proposition** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of formal group laws over A. Then $\alpha(X)$ is an isomorphism if and only if $T(\alpha)$ is an isomorphism.

Proof The "only if" part of the statement is trivial since $T(-)$ is a functor. Suppose that $T(\alpha)$ is an isomorphism. We have for all $n \in \mathbf{N}$ a commutative diagram

$$\begin{array}{ccc} T(F) & \xrightarrow{T(\alpha)} & T(G) \\ \downarrow & & \downarrow \\ \mathrm{Ker}[p^n]_F & \xrightarrow{\alpha(K_s)} & \mathrm{Ker}[p^n]_G \end{array}$$

where both vertical arrows are surjective. (By Corollary (35.1.6); the homomorphism $T(F) \to \mathrm{Ker}[p^n]_F$ is of course $(x_1, x_2, \ldots) \to x_n$.) Then the bottom arrow is surjective if $T(\alpha)$ is surjective. We can suppose that $\alpha(X) \neq 0$. Then $\mathrm{ht}(F(X, Y)) = \mathrm{ht}(G(X, Y)) = h$ (say). Then $\#\mathrm{Ker}[p^n]_F = p^{n+h} = \#\mathrm{Ker}[p^n]_G$; and, since $\alpha(K_{sc})$ is surjective, it follows that $\alpha(K_{sc})$ is injective. But $\mathrm{Ker}(\alpha(K_{sc})) \subset \mathrm{Ker}[p^n]_F$ for n large enough. So $\mathrm{Ker}\ \alpha(K_{sc}) = 0$, which means that W-degree $(\alpha(X)) = 1$, i.e., that $\alpha(X)$ is an isomorphism.

35.4 Isogenies and lattices in $V(F)$

■ (35.4.1) Let $F(X, Y)$ be a formal group law of height h over A. The Tate module $T(F)$ is a free $\mathbf{Z}_p$-submodule of the $\mathbf{Q}_p$-vector space $V(F) \simeq \mathbf{Q}_p^h$, i.e., a lattice, where a lattice is defined as a free $\mathbf{Z}_p$-submodule of $V(F)$ of rank $h = \dim_{\mathbf{Q}_p}(V(F))$, which generates $V(F)$ as a $\mathbf{Q}_p$-vector space.

The Galois group $\Gamma = \mathrm{Gal}(K_{sc}/K)$ acts on $\Lambda(F)$ and hence also on $T(F)$ and $V(F)$ as follows: $\tau(x_0, x_1, \ldots) = (\tau x_0, \tau x_1, \ldots)$ for all $\tau \in \Gamma$ and $\mathbf{x} = (x_0, x_1, \ldots) \in V(F)$. This action is continuous if Γ is given the Krull topology and $V(F)$ the topology defined by the subgroups $\{(0, \ldots, 0, x_{n+1}, x_{n+2}, \ldots)\} \subset V(F)$,

and this latter topology makes $V(F) \simeq \mathbf{Q}_p^h$ an isomorphism of topological vector spaces over $\mathbf{Q}_p$ where $\mathbf{Q}_p$ has its usual p-adic topology.

■ (35.4.2) **Theorem**

(i) Let R be a sublattice of $T(F)$ in $V(F)$. Then there exists an isogeny (over some $A(L)$, L/K finite) $\alpha(X)$: $H(X, Y) \to F(X, Y)$ such that $R = \mathrm{Im}(T(\alpha))$. If R is stable under Γ, $\alpha(X)$ and $H(X, Y)$ can be chosen to be defined over A. If $\hat{\alpha}(X)$: $\hat{H}(X, Y) \to F(X, Y)$ is an isogeny such that $\mathrm{Im}(T(\hat{\alpha})) \subset \mathrm{Im}(T(\alpha))$, then there exists an isogeny $\beta(X)$: $\hat{H}(X, Y) \to H(X, Y)$ such that $\hat{\alpha}(X) = \alpha(X) \circ \beta(X)$. In particular the lattice $\mathrm{Im}(T(\alpha))$ determines $H(X, Y)$ and $\alpha(X)$ to within isomorphism.

(ii) Let R be a lattice in $V(F)$ that contains $T(F)$ (a superlattice). Then there exists an isogeny $\beta(X)$: $F(X, Y) \to G(X, Y)$ such that $V(\beta)^{-1}(T(G)) = R$. If R is stable under Γ, $\beta(X)$ and $G(X, Y)$ can be chosen to be defined over A. If $\hat{\beta}(X)$: $F(X, Y) \to \hat{G}(X, Y)$ is an isogeny such that $V(\beta)^{-1}(T(G)) \subset V(\hat{\beta})^{-1}(T(\hat{G}))$, then there exists an isogeny $\alpha(X)$: $G(X, Y) \to \hat{G}(X, Y)$ such that $\alpha(X) \circ \beta(X) = \hat{\beta}(X)$. In particular, R determines $G(X, Y)$ and $\beta(X)$ up to isomorphism.

To prove this theorem, in fact even to state it, we need to know that if $\alpha(X)$: $F(X, Y) \to G(X, Y)$ is an isogeny, then $V(\alpha)T(F)$ is a lattice in $V(G)$.

■ (35.4.3) **Lemma** Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be an isogeny. Then we have an exact diagram (i.e., all columns and rows are exact and the diagram is commutative)

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & T(F) & \longrightarrow & V(F) & \longrightarrow & \Lambda(F) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle T(\alpha)} & & \downarrow{\scriptstyle V(\alpha)} & & \downarrow{\scriptstyle \Lambda(\alpha)} & & \\
0 & \longrightarrow & T(G) & \longrightarrow & V(G) & \longrightarrow & \Lambda(G) & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

and $\mathrm{CoKer}(T(\alpha)) \simeq \mathrm{Ker}\ \Lambda(\alpha)$. Further, $T(\alpha)(T(F))$ is a sublattice of $T(G)$.

Proof We have already seen that the rows of the diagram above are exact (Proposition (35.3.9)). There is an isogeny $\beta(X)$: $G(X, Y) \to F(X, Y)$ such that $\beta(X) \circ \alpha(X) = [p^n]_F(X)$ for n large enough (Corollary (35.2.2)(i)). Hence $\Lambda(\alpha)$ is surjective by Corollary 35.1.6(i). Let $\mathbf{x} \in V(F)$, then $V(\alpha)(\mathbf{x}) = 0 \Rightarrow \alpha(x_i) = 0$ for all $i \in \mathbf{N}$ and by Lemma (35.3.12) or Corollary (35.3.14) this would give infinitely many different roots of $\alpha(X)$ if $\mathbf{x}$ were $\neq 0$. But $\alpha(X)$ is an isogeny and hence $\mathrm{Ker}(\alpha(K_{sc}))$ is finite. Therefore $\mathbf{x} = 0$ if $V(\alpha)(\mathbf{x}) = 0$ (cf. also the proof of Proposition (35.3.15) where the same argument was used). Hence $V(\alpha)$ and $T(\alpha)$ are injective. Since $V(\alpha)$ is a map of $\mathbf{Q}_p$-vector spaces of equal dimension and

$V(\alpha)$ is injective, it follows that $V(\alpha)$ is also surjective. The isomorphism Ker $\Lambda(\alpha) = \text{CoKer } T(\alpha)$ now follows from the snake lemma (cf. [42, Chapter I, Section 1, no. 4]) and $T(\alpha)(T(F))$ is a lattice in $V(G)$ because $T(G)$ is a lattice in $V(G)$ and $T(G)/T(\alpha)T(F)$ is finite since Ker $\Lambda(\alpha)$ is finite (Proposition (35.1.5)).

■ (35.4.4) **Proof of Theorem (35.4.2)** The proof of Theorem (35.4.2) is now a perfectly straightforward application of Theorem (35.2.1). First, let R be a superlattice of $T(F)$ in $V(F)$. Then $R/T(F)$ is a finite subgroup of $\Lambda(F) = V(F)/T(F)$, and the assignment $R \mapsto R/T(F)$ sets up a bijective correspondence between finite subgroups of $\Lambda(F)$ and superlattices of $T(F)$ in $V(F)$. Further, $R/T(F)$ is stable under Γ iff R is stable under Γ. Finally, if $\hat{\beta}(X)$: $\hat{F}(X, Y) \to \hat{G}(X, Y)$ is an isogeny, then by the exact diagram of (35.4.3) $V(\hat{\beta})^{-1}(T(\hat{G}))/T(F) = \text{Ker}(\hat{\beta}(K_{sc}))$. Now apply Theorem (35.2.1) to obtain part (ii) of Theorem (35.4.2).

To prove part (i), pick any $n \in \mathbf{N}$ such that $[p^n]_F(T(F)) \subset R$, where R is the given sublattice of $T(F)$. Then $[p^n]_F^{-1}(R) \supset T(F)$, hence there exists (by part (ii) of Theorem (35.4.2)) an isogeny $\beta(X)$: $F(X, Y) \to H(X, Y)$ such that $V(\beta)^{-1}(T(H)) = [p^n]_F^{-1}(R)$. Now

$$\text{Ker}(\beta(K_{sc})) = V(\beta)^{-1}(T(H))/T(F) = [p^n]_F^{-1}R/T(F)$$

and hence $[p^n]_F \text{ Ker}(\beta(K_{sc})) = 0$ since $R \subset T(F)$. So $\text{Ker}(\beta(K_{sc})) \subset \text{Ker}[p^n]_F$ and we can apply Theorem (35.2.1) to find a unique isogeny $\alpha(X)$: $H(X, Y) \to F(X, Y)$ such that $\alpha(X) \circ \beta(X) = [p^n]_F(X)$. But then Im $T(\alpha) = V(\alpha)(T(H)) = V(\alpha)(V(\beta)([p^n]_F^{-1}(R))) = R$, as required. If R is stable under Γ, then so is $[p^n]_F^{-1}(R)$, so by part (ii) of Theorem (35.4.2) we can assume that $\beta(X)$ and $H(X, Y)$ are defined over A and hence so is $\alpha(X)$ by Theorem (35.2.1).

Now let $m \in \mathbf{N}$, $m \geq n$, then, taking $\tilde{\beta}(X) = \beta(X) \circ [p^{m-n}]_F(X)$, we find $V(\tilde{\beta})^{-1}(T(H)) = [p^m]^{-1}(R)$; and if $\tilde{\alpha}(X)$ is such that $\tilde{\alpha}(X) \circ \tilde{\beta}(X) = [p^m]_F(X)$, then

$$\tilde{\alpha}(X) \circ \beta(X) \circ [p^{m-n}]_F(X) = [p^n]_F(X) \circ [p^{m-n}]_F(X)$$

so that we find the same $\tilde{\alpha}(X) = \alpha(X)$. That is, the choice of n is essentially immaterial.

Now let $\hat{\alpha}(X)$: $\hat{H}(X, Y) \to F(X, Y)$ be an isogeny such that Im $T(\hat{\alpha}) \subset$ Im $T(\alpha)$. By the remark just made we can assume that $\text{Im}(T(\hat{\alpha})) \supset [p^n]_F(T(F))$, where $\alpha(X)$ and $\beta(X)$ are as constructed above (using this particular n). Now

$$\text{Ker } \Lambda(\hat{\alpha}) \simeq V(T(F)/V(\hat{\alpha})T(\hat{H})$$

and since $V(\hat{\alpha})T(\hat{H}) = \text{Im } T(\hat{\alpha}) \supset [p^n]_F(T(F))$, it follows that

$$[p^n]_{\hat{H}} \text{ Ker } \Lambda(\hat{\alpha}) = 0$$

So by Theorem (35.2.1) there exists an isogeny $\hat{\beta}(X)$: $F(X, Y) \to \hat{H}(X, Y)$ such that $\hat{\beta}(X) \circ \hat{\alpha}(X) = [p^n]_{\hat{H}}(X)$. But then

$$\hat{\beta}(X) \circ \hat{\alpha}(X) \circ \hat{\beta}(X) = [p^n]_{\hat{H}}(X) \circ \hat{\beta}(X) = \hat{\beta}(X) \circ [p^n]_F(X)$$

so that

$$\hat{\alpha}(X) \circ \hat{\beta}(X) = [p^n]_F(X) = \alpha(X) \circ \beta(X)$$

Then

$$\begin{aligned} \operatorname{Ker}(\hat{\beta}(K_{sc})) &= V(\hat{\beta})^{-1} T(\hat{H})/T(F) = V([p^n]_F)^{-1} V(\hat{\alpha}) T(\hat{H})/T(F) \\ &\subset V([p^n]_F)^{-1} V(\alpha) T(H)/T(F) \\ &= V(\beta)^{-1} T(H)/T(F) = \operatorname{Ker}(\beta(K_{sc})) \end{aligned}$$

Hence, by Theorem (35.2.1) there exists a unique isogeny $\gamma(X)$: $\hat{H}(X, Y) \to H(X, Y)$ such that $\gamma(X) \circ \hat{\beta}(X) = \beta(X)$. Then

$$\alpha(X) \circ \gamma(X) \circ \hat{\beta}(X) = \alpha(X) \circ \beta(X) = \hat{\alpha}(X) \circ \hat{\beta}(X)$$

and hence $\alpha(X) \circ \gamma(X) = \hat{\alpha}(X)$, as required. This completes the proof of the theorem.

35.5 Formal group laws with pregiven END-ring

■ (35.5.1) Let $F(X, Y)$, $G(X, Y)$ be formal group laws over A. We shall write $\operatorname{HOM}(F(X, Y), G(X, Y))$ for $\mathbf{FG}_{A(K_{sc})}(F(X, Y), G(X, Y))$ and as before (cf. Chapter IV, Section 23.2.) $\operatorname{END}(F(X, Y)) = \operatorname{HOM}(F(X, Y), F(X, Y))$. We have seen that the map V: $\operatorname{HOM}(F(X, Y), G(X, Y)) \to \operatorname{Hom}(V(F), V(G))$ is injective (more precisely we have seen this for T (cf. Proposition (35.3.9)), but then the result also follows for V; cf. Proposition (35.3.9); cf. also Lemma (35.4.3)).

Tensoring with $\mathbf{Q}_p$ gives us an injection (both modules being $\mathbf{Z}_p$-torsion free)

(35.5.2) $\quad V$: $\mathbf{Q}_p \otimes \operatorname{HOM}(F(X, Y), G(X, Y)) \to \operatorname{Mod}_{\mathbf{Q}_p}(V(F), V(G))$

(where the latter "Mod" is one of $\mathbf{Q}_p$-vector spaces). Also we can view $\operatorname{HOM}(F(X, Y), G(X, Y))$ as a $\mathbf{Z}_p$-submodule of $\mathbf{Q}_p \otimes \operatorname{HOM}(F(X, Y), G(X, Y))$.

■ (35.5.3) **Proposition** Using the notations of (35.5.1), let $\alpha(X) \in \mathbf{Q}_p \otimes \operatorname{HOM}(F(X, Y), G(X, Y))$. Then $\alpha(X) \in \operatorname{HOM}(F(X, Y), G(X, Y))$ if and only if $V(\alpha)$ maps $T(F)$ into $T(G)$ (cf. (35.5.2)).

Proof The "only if" part is trivial. As to the "if" part, there is an $n \in \mathbf{N}$ such that $p^n \alpha(X) \in \operatorname{HOM}(F(X, Y), G(X, Y))$. Let $\beta(X) = p^n \alpha(X) = [p^n]_G(X) \circ \alpha(X)$ (cf. (35.5.1)). Then because of $V(\alpha)T(F) \subset T(G)$, we have $V(\beta)T(F) \subset [p^n]_G T(G)$; hence by Theorem (35.4.2) there is a $\hat{\beta}(X) \in \operatorname{HOM}(F(X, Y), G(X, Y))$ such that $\beta(X) = [p^n]_G(X) \circ \hat{\beta}(X)$. Then $\alpha(X) = \hat{\beta}(X)$.

■ (35.5.4) Let L_F be the quotient field of $J(\mathrm{END}(F(X, Y))$. Then of course J induces an isomorphism $\mathbf{Q}_p \otimes \mathrm{END}(F(X, Y)) \simeq L_F$. Now $T(F)$ is an $\mathrm{END}(F(X, Y))$-module (T being a functor) and so via J we can view $V(F)$ as an L_F-module, i.e., as a vector space over L_F. In these terms Proposition (35.5.3) for endomorphisms becomes:

■ (35.5.5) **Corollary** $J(\mathrm{END}(F(X, Y))) = \{a \in L_F \mid aT(F) \subset T(F)\}$.

■ (35.5.6) Let $\alpha(X)$: $G(X, Y) \to F(X, Y)$ be an isogeny. Then $L_F = L_G$ by Corollary (35.2.2)(ii) and $V(\alpha)$: $V(G) \to V(F)$ becomes an isomorphism of L_F-modules. Thus Proposition (35.5.3) for homomorphisms becomes

■ (35.5.7) **Corollary** $J(\mathrm{HOM}(F(X, Y), G(X, Y))) = \{a \in L_F \mid aT(F) \subset T(G)\}$.

And we have also (in the setting of (35.5.6)):

■ (35.5.8) **Corollary** $J(\mathrm{END}(G(X, Y))) = \{a \in L_F \mid a \operatorname{Im}(T(\alpha)) \subset \operatorname{Im} T(\alpha)\}$.

Indeed, $a \in J(\mathrm{END}(G(X, Y))) \Leftrightarrow aT(G) \subset T(G) \Leftrightarrow J(\alpha)aT(G) \subset J(\alpha)T(G) \Leftrightarrow a \operatorname{Im}(T(\alpha)) \subset \operatorname{Im}(T(\alpha))$ since $J(\alpha)T(G) = \operatorname{Im}(T(\alpha))$.

We can now prove a theorem promised long ago (cf. Chapter IV, Section 23.2).

■ (35.5.9) **Theorem** Let $\mathcal{O}$ be an order over $\mathbf{Z}_p$ (which is contained in $A(K_{sc})$). Then there is a formal group law $F(X, Y)$ (over some $A(L)$) of height $[\mathcal{O} : \mathbf{Z}_p]$ such that $J(\mathrm{END}(F(X, Y))) = \mathcal{O}$.

Proof Let L be the quotient field of $\mathcal{O}$ and $A(L)$ its ring of integers, and $\pi(L)$ a uniformizing element. Let $G(X, Y)$ be the one dimensional Lubin–Tate formal $A(L)$-module over $A(L)$ with logarithm $g(X) = X + \pi(L)^{-1}g(X^{q(L)})$ where $q(L)$ is the number of elements in the residue field of L. Then $J(\mathrm{END}(G(X, Y))) = A(L)$ and $L_G = L$.

Now let R be a sublattice of $T(G) \subset V(G)$ such that $\mathcal{O} = \{a \in L_G \mid aR \subset R\}$. (Such sublattices exist: take, e.g., $R = \mathcal{O}x$ where x is any nonzero element of $T(G)$; for the detailed theory of orders in algebras, see, e.g., [97].) Then there is an isogeny $\alpha(X)$: $F(X, Y) \to G(X, Y)$ such that $R = \operatorname{Im} T(\alpha)$. Now apply Corollary (35.5.8) to obtain $J(\mathrm{END}(F(X, Y))) = \mathcal{O}$.

■ (35.5.10) **Corollary** (of the proof) Let $F(X, Y)$ be a formal group law and $\mathcal{O}$ be an order with quotient field L_F, then there exists an isogenous formal group law $G(X, Y)$ with $J(\mathrm{END}(G(X, Y))) = \mathcal{O}$.

35.6 The Tate module $T(F)$ as a Galois module

■ (35.6.1) Let $F(X, Y)$ be a formal group law over A of height h. Let $\Gamma = \mathrm{Gal}(K_{sc}/K)$. Then Γ acts on $T(F)$ and $V(F)$ as $\tau(x_0, x_1, x_2, \ldots) = (\tau x_0, \tau x_2, \ldots)$ and this is a continuous action, i.e., τ acts continuously on $V(F)$ (with its topology as a $\mathbf{Q}_p$-vector space) and the homomorphism $\Gamma \to \mathbf{GL}(V(F))$ is continuous. The kernel of this homomorphism is of course $\Gamma_1 =$

$\mathrm{Gal}(K_{sc}/K(\Lambda(F)))$, where $K(\Lambda(F))$ is the field obtained from K by adjoining all elements of $\Lambda(F) \subset (K_{sc})$.

■ (35.6.2) **Theorem** $V(F)$ is an irreducible Γ-module over $\mathbf{Q}_p$ (i.e., $\Gamma \to \mathbf{GL}(V(F))$ is an irreducible h-dimensional p-adic representation of Γ).

Proof Let $\mathbf{x} \in V(F)$, then we have to show that $\Gamma\mathbf{x} = \{\tau\mathbf{x} \mid \tau \in \Gamma\}$ generates all of $V(F)$ as a $\mathbf{Q}_p$-vector space if $\mathbf{x} \neq 0$. It suffices to prove this for $\mathbf{x} \in T(F) \setminus [p]T(F)$. Let $W \subset T(F)$ be the sub-$\mathbf{Z}_p$-module of $T(F)$ generated by $\Gamma\mathbf{x}$. Then W is free of rank $s \leq h$, and what we have to show is $s \geq h$.

Let ϕ_n: $T(F) \to \mathrm{Ker}[p^n]_F(K_{sc})$ be the homomorphism of Γ-modules $(x_1, x_2, \ldots, x_n, \ldots) \mapsto x_n$. Since W is of rank $s \leq h$, $\phi_n(W)$ is a direct sum of at most s cyclic subgroups all of rank $\leq n$ (because $[p^n](\mathrm{Ker}[p^n]_F(K_{sc})) = 0$). So the number of elements in $\phi_n(W) - [p]\phi_n(W)$ is at most $p^{ns} - p^{(n-1)s}$. Each element of Γx_n is in $\phi_n(W) - [p]\phi_n(W)$.

Hence

$$\#\Gamma x_n \leq p^{(n-1)s}(p^s - 1)$$

Now $\#\Gamma x_n$ is the number of conjugates of x_n over K so $\#\Gamma x_n \geq [K(x_n) : K]$, so that

$$[K(x_n) : K] \leq p^{(n-1)s}(p^s - 1) \tag{35.6.3}$$

We now use the valuation estimates on $v(x_n)$ of Lemma (35.3.12) (for $\mathbf{x} \in T(F)$) to obtain a lower bound as follows. Let e_n be the ramification index of $K(x_n)/K$. Now $\lim_{i \to \infty} v(x_i) = 0$ by Corollary (35.3.14). Hence there is an $m \in \mathbf{N}$ such that $v(x_i) < \varepsilon = v(\pi)$ for $i \geq m$ where π is a uniformizing element of K. Then by Lemma (35.3.12)(v) we have for all $n \geq m$

$$v(x_n) \leq p^{-(n-m)h} v(\pi)$$

and hence

$$[K(x_n) : K] \geq e_n \geq p^{(n-m)h} \tag{35.6.4}$$

for all $n \geq m$. Combining this with (35.6.3) we find

$$p^{(n-1)s}(p^s - 1) \geq p^{(n-m)h}$$

for all $n \in \mathbf{N}$ (for a certain fixed $m \in \mathbf{N}$). Letting $n \to \infty$ it follows that $s \geq h$. Q.E.D.

E.5 Bibliographical and Other Notes

■ (E.5.1) **Notes on Section 32** The material in 32.1–32.2 comes straight from Lubin and Tate's beautiful paper [264]. Some additional remarks on the Lubin–Tate constructions can be found in [384–386] and [350]. In [264] Lubin and Tate have to use the existence and (certain) properties of the classical reciprocity homomorphism to prove that $L_\pi \cdot K_{nr}$ is indeed maximal abelian. For a different treatment of local class field

theory, avoiding this as well as formal groups and Galois cohomology, cf. [169]. The explicit description of the reciprocity homomorphism for $K = \mathbf{Q}_p$ in Section 32.3 is due to Dwork [137].

The material of Section 32.4 on the Šafarevič mapping comes from [74]. For results on the image of the fundamental class in $H^2(G, L^*)$ under the mapping $H^2(G, L^*) \to H^2(G, \mathrm{Gal}(L_{ab}/L))$ induced by the reciprocity homomorphism (Šafarevič–Weil theorem) in a class formation setting, cf., e.g., [12, Theorem 6, Chapter XV, p. 246] and/or [249, Chapitre IX, Théorème 7, p. 242].

The explicit reciprocity laws of Iwasawa [480] can also be generalized to the Lubin–Tate setting; cf. [509], cf. also (13.3.3) and [470].

■ (E.5.2) **Notes on Section 33** The theorem on the relation between the formal minimal model of an elliptic curve E over $\mathbf{Q}$ and its global L-series is due to Honda [188], who, however, had to stay away from the primes 2 and 3 in [188]. This defect was removed by Hill [186].

Proofs of the Atkin–Swinnerton-Dyer conjectures were announced by Cartier in [67]. Unfortunately in their statement in [67] an inaccuracy slipped in and they were stated as congruences concerning $\beta(np) - \beta(p)\beta(n) + p\beta(n/p)$ rather than $\beta(np) - a_p\beta(n) + pb_p\beta(n/p)$. Now if one takes the standard model and the standard uniformizing element, it may of course happen that $a_p = \beta(p)$. But also not as examples 11B, 14C, 46A (for the prime number 5) of [35] show. In examples 26B, 58A one does have $a_5 = \beta(5)$.) In his 1972 IHES seminar Cartier sketches a proof ([68]) and there the result is stated correctly.

Another proof has been given by Ditters, who also obtained a number of related and more dimensional results; cf. [126–129].

■ (E.5.3) **Notes on Section 34** The important Theorem (34.2.16) (universality of the formal group law of complex cobordism) is due to Quillen, [330, 332]. Theorem (34.2.14) (calculation of the logarithm of $F_{MU}(X, Y)$) is due to Miščenko (cf. [315, appendix 1]).

The proof of the universality of the formal group law of complex cobordism given above is a mixture of part III of [203] and [57]. With a little more trouble one can extend this to give a direct proof of the universality of $F_{MU}(X, Y)$, which does not use Lazard's theorem; cf. [58]. The formula of Theorem (34.2.10) for $F_{MU}(X, Y)$ comes from Buhštaber [48]. According to [2, p. 85] it was also obtained by Boardman. (Most of the formulas of 34.2 above also occur in [2, Part II, Section 10].)

The treatment of MU cohomology operations and the Quillen splitting follows more or less Araki's lecture notes [8].

The results on generators and operations in 34.4 and 34.5 were "announced" in [178, 179] and proved in [172]. Subsequently Kozma in [231, 232], using Cartier's first theorem, also wrote down generators for $BP(pt)$ and $MU(pt)$. His MU generators were different from mine and translating back gave a nicer one dimensional universal formal group law. (This is in fact the universal formal group law $F_U(X, Y)$ of Chapter I, Section 5; the original generators correspond to $H_U(X, Y)$; cf. [178]; cf. also the introduction of [171] for some more remarks.) Still more generators can be found in [8]. The first to write down a formula similar to (34.4.5) was Liulevicius [259], and he also proved that in the case $p = 2$ these (somewhat different) formulas gave generators.

Complex K-theory splits in a similar manner as MU into a wedge sum of dimension shifted copies of a theory with p-typical formal group law; cf. Araki [7, 8] for a treatment of this Adams splitting from the point of view of formal group laws.

Calculations in Brown–Peterson cohomology are often easier than in MU-theory. A number of papers dealing with BP are [213, 395, 440–442, 456].

■ (E.5.4) **Notes on Section 35** For Section 35, I have mainly made use of Fröhlich [144] and Lubin [268]. Proposition (35.1.5) and Corollary (35.1.6) are due to Lubin and Serre, and Proposition (35.1.8) is due to Serre; cf. [364]. Theorem (35.2.1) is due to Lubin [266]; the proof given above follows Fröhlich [144], which in turn is Lubin's original proof with a number of nontrivial details filled in.

Proposition (35.3.18) is a (weak) consequence of a theorem of Tate ([404, Theorem 4, Corollary 2]) which, on the other hand, is proved with the higher dimensional version of (35.3.18) as the main tool. Proposition (32.4.3) is another corollary of this theorem of Tate. Theorem (35.4.2) is, again, due to Lubin [266]; the proof given, again, follows Fröhlich [144]. Theorem (35.5.9) is also due to Lubin [266]. Finally, Theorem (35.6.2) is due to Serre [367] and is presented as in [144]. A related result is: let $F(X, Y)$ be a one dimensional formal group law over A such that $\mathrm{END}(F(X, Y)) = \mathbf{Z}_p$, then the image of $\mathrm{Gal}(K_{ab}/K)$ in $\mathrm{Aut}_{\mathbf{Z}_p}(T(F)) = GL_h(Z_p)$ is an open subgroup; cf. [367, 267]. This can be thought of as a kind of nonabelian reciprocity. Related matters are contained in Sen [358, 359] and Fontaine [140].

CHAPTER VII

FORMAL GROUPS AND BIALGEBRAS

36 Basic Definitions and Survey of the Results of Chapter VII

36.1 The basic categories. Formal group laws, formal groups and their co- and contravariant bialgebras (hyperalgebras)

We shall presently see that a formal group law $F(X, Y)$ defines a cogroup object in a certain category. For the convenience of the reader, we now first discuss briefly group and cogroup objects in a category.

■ (36.1.1) **Intermezzo on cogroup and group objects in category** Let **C** be a category with products ($\times$) and final object E. A *group object* G in **C** is an object of **C** together with morphisms $m: G \times G \to G$, $i: G \to G$, $e: E \to G$ such the first three of the following diagrams are commutative:

$$\begin{array}{ccc} G & \xleftarrow{m} & G \times G \\ \uparrow{\scriptstyle m} & & \uparrow{\scriptstyle m \times 1} \\ G \times G & \xleftarrow{1 \times m} & G \times G \times G \end{array} \qquad \begin{array}{ccc} & & G \times G \\ & \nearrow & \downarrow{\scriptstyle m} \\ E \times G & \simeq & G \end{array}$$

(36.1.2)

$$\begin{array}{ccc} G & \xrightarrow{d} & G \times G \\ & \searrow & \downarrow{\scriptstyle i \times 1} \\ E & & \\ & \searrow^{e} & \\ & & G \end{array} \qquad \begin{array}{ccc} G \times G & \xrightarrow{t} & G \times G \\ & \searrow^{m} \quad \swarrow_{m} & \\ & G & \end{array}$$

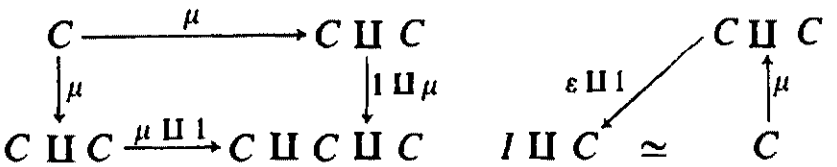
where $G \to E$ is the unique morphism into the final object E, where $d: G \to G \times G$ is the diagonal map (id, id) and $E \times G \simeq G$ is the canonical identification. If the fourth diagram is also commutative (where t is the switch morphism interchanging the two factors), the group object is said to be commutative. (The four diagrams express respectively associativity, left unit

element, left inverses, commutativity; as in the case of ordinary groups, it follows easily that there are two more commutative diagrams expressing right unit element, right inverses.)

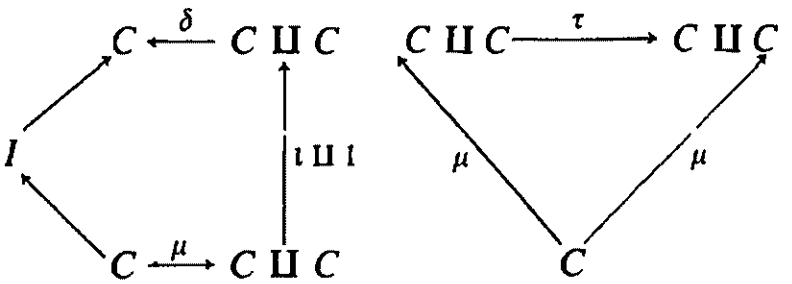
Another way to say that G is a group object in $\mathbf{C}$ is to say that the contravariant functor $\mathbf{C}(-, G)$: $\mathbf{C}^0 \to \mathbf{Set}$ factors through V: **Group** $\to$ **Set** where V is the forgetful functor.

If $\mathbf{C} = \mathbf{Set}$, a group object in $\mathbf{C}$ is simply an ordinary group with its multiplication given by m.

Dually, let $\mathbf{C}$ be a category with finite sums ($\amalg$) and initial object I. A *cogroup object* in $\mathbf{C}$ is an object C of $\mathbf{C}$ together with morphisms μ: $C \to C \amalg C$, ι: $C \to C$, ε: $C \to I$ such that the first three of the following diagrams are commutative (these diagrams are of course obtained from those given above by reversing all arrows):



(36.1.3)



(Here δ is the sum morphism, τ the switch morphism, $I \amalg C \simeq C$ the canonical isomorphism, and $I \to C$ the unique morphism of the initial object I into C.) C is said to be cocommutative if the fourth diagram above is also commutative.

A morphism α: $G_1 \to G_2$ between two groupobjects of $\mathbf{C}$ is a *morphism of group objects* if it is compatible with m, e, and i; i.e., we must have $m_2(\alpha \times \alpha) = \alpha m_1$, $i_2 \alpha = \alpha i_1$, $e_2 = \alpha e_1$.

A morphism α: $C_1 \to C_2$ between two cogroup objects of $\mathbf{C}$ is a *morphism of cogroup objects* if it is compatible with μ, ε, and ι; i.e., we must have $(\alpha \amalg \alpha)\mu_1 = \mu_2 \alpha$, $\iota_2 \alpha = \alpha \iota_1$, $\varepsilon_2 \alpha = \varepsilon_1$.

The category of group objects of $\mathbf{C}$ will be denoted $G\mathbf{C}$ and the category of cogroup objects in a category $\mathbf{C}$ will be denoted $C\mathbf{C}$.

■ (36.1.4) **The contravariant bialgebra of a formal group law** Now let $F(X, Y)$ be a formal group law of dimension n over a ring A. The n-tuple of power series $F(X, Y)$ defines (according to Appendix (A.4.2)) a unique continuous homomorphism $\bar{\mu}$: $R \to R \hat{\otimes}_A R$, $R = A[\![X_1, \ldots, X_n]\!]$, $\bar{\mu}(X_i) = F_i(X_1 \otimes 1, \ldots, X_n \otimes 1; 1 \otimes X_1, \ldots, 1 \otimes X_n)$. Further, $\bar{\iota}(X) = [-1]_F(X)$ defines

a continuous homomorphism $\bar{\imath}$: $R \to R$; and finally there is the natural augmentation homomorphism $\bar{\varepsilon}$: $R \to A$, $X_i \mapsto 0$. We claim that $\bar{\mu}$, $\bar{\imath}$, $\bar{\varepsilon}$ make R a cogroup object (in the category of power series rings over A with continuous A-algebra homomorphisms). Indeed, commutativity of the first diagram of (36.1.3) is the same thing as $F(X, F(Y, Z)) = F(F(X, Y), Z)$; commutativity of the second diagram equals $F(0, Y) = Y$; and commutativity of the third diagram equals $F(\bar{\imath}(X), X) = 0$. Commutativity of the fourth diagram corresponds to $F(X, Y) = F(Y, X)$, so that the formal group law is commutative iff R is cocommutative.

We shall use $R(F)$ to denote this cogroup object associated to a formal group law $F(X, Y)$ and call it the *contravariant bialgebra* of $F(X, Y)$.

Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of formal group laws over A. Let $G(X, Y)$ be m-dimensional. Then $\alpha(X)$ is an m-tuple of power series in n variables and thus defines a unique homomorphism $R(\alpha)$: $R(G) \to R(F)$, $X_i \mapsto \alpha_i(X)$. We claim that $R(\alpha)$ is a homomorphism of cogroup objects. Indeed, $(R(\alpha) \hat{\otimes} R(\alpha)) \circ \bar{\mu}_F = \bar{\mu}_G \circ R(\alpha)$ corresponds to $\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$, $\alpha(X) \equiv 0 \bmod(\text{degree } 1)$ is the same as $\bar{\varepsilon}_2 \circ R(\alpha) = \bar{\varepsilon}_1$ and $\alpha(\bar{\imath}_F(X)) = \bar{\imath}_G(\alpha(X))$ corresponds to $\bar{\imath}_G \circ R(\alpha) = R(\alpha) \circ \bar{\imath}_F$.

Thus R is a contravariant functor from the category of formal group laws into the category of cogroup objects in the category of power series rings over A. (In particular it follows that $R(F)$ depends (up to isomorphism of cogroup objects) only on the isomorphism class of $F(X, Y)$.)

Conversely, if C is a cogroup object in the category of power series rings over A, then it defines an isomorphism class of formal group laws over A. Indeed, let $A[\![X_1, \ldots, X_n]\!]$ be the power series ring underlying C, then $\bar{\mu}$: $C \to C \hat{\otimes} C$ defines a formal group law $F_\mu(X, Y)$ by $F_\mu(i)(X, Y) = \bar{\mu}(X_i)$ (where we write Y_j for $1 \otimes X_j$). Thus the functor $F \mapsto R(F)$ is an equivalence of categories.

■ (36.1.5) **The covariant bialgebra of a formal group law** Let $F(X, Y)$ be again an n-dimensional formal group law over A. Let $R(F)$ be its contravariant bialgebra. Forgetting a lot of structure, $R(F)$ is in any case a linearly topologized A-module (and complete and Hausdorff in that topology). Let M be this module. Then the A-algebra structure on M is given by continuous A-module morphisms

$$M \hat{\otimes} M \xrightarrow{\cdot \bar{m}} M, \qquad A \xrightarrow{\bar{e}} M \tag{36.1.6}$$

and the cocommutative cogroup object structure on M gives us (in any case) continuous A-module morphisms

$$M \xrightarrow{\bar{\imath}} M, \qquad M \xrightarrow{\bar{\mu}} M \hat{\otimes} M, \qquad M \xrightarrow{\bar{\varepsilon}} A \tag{36.1.7}$$

(Of course, there are various compatibilities between all these A-module morphisms, caused, e.g., by the fact that $\bar{\imath}$, $\bar{\varepsilon}$, $\bar{\mu}$ are A-algebra homomorphisms so that, e.g., we must have $\bar{\mu} \circ \bar{m} = (\bar{m} \hat{\otimes} \bar{m}) \circ (1 \hat{\otimes} \bar{\tau} \otimes 1) \circ (\bar{\mu} \hat{\otimes} \bar{\mu})$ where

$1 \hat{\otimes} \bar{\tau} \hat{\otimes} 1$ is the isomorphism that interchanges the middle two factors in $M \hat{\otimes} M \hat{\otimes} M \hat{\otimes} M$.)

There is a pleasing symmetry about the array of morphisms that one obtains by combining (36.1.6) and (36.1.7) (and also a pleasing symmetry about the various compatibility conditions) suggesting that if we dualize everything we should get more or less the same kind of object.

Let $\mathbf{Mod}T_A$ be the category consisting of A-modules of the form $M \simeq \prod_{i \in I} A_i$, $A_i = A$ for all $i \in I$ with the product topology (discrete topology on the factors). The morphisms of $\mathbf{Mod}T_A$ are defined to be the continuous A-module morphisms. Then $R(F) \in \mathbf{Mod}T_A$ (if we forget about its various structure morphisms). Now let

$$U(F) = \mathbf{Mod}T_A(R(F), A)$$

Then as an A-module $U(F)$ is free and the various structure morphisms $\bar{m}$, $\bar{e}$, $\bar{\iota}$, $\bar{\mu}$, $\bar{\varepsilon}$ define A-module morphisms

$$\mu\colon U(F) \to U(F) \otimes U(F), \qquad \varepsilon\colon U(F) \to A$$

(36.1.8)
$$\iota\colon U(F) \to U(F)$$

$$m\colon U(F) \otimes U(F) \to U(F), \qquad e\colon A \to U(F)$$

We now claim that m and e make $U(F)$ an A-algebra with unit element; $U(F)$ is commutative if and only if $R(F)$ is cocommutative, i.e., if and only if $F(X, Y)$ is commutative. Further, we claim that μ, ε, ι almost make $U(F)$ into a commutative cogroup object in the category of associative algebras over A. More precisely, μ and ε are algebra homomorphisms; the diagrams of (36.1.2) are all commutative, but ι is not an A-algebra homomorphism as a rule; it satisfies instead $\iota(xy) = \iota(y)\iota(x)$, $\iota(1) = 1$. Whence the word *almost*. If $F(X, Y)$ is commutative, $U(F)$ *is* a cogroup object in $\mathbf{Alg}_A$. A better way to look at $U(F)$ is as a group object in the category of commutative coalgebras.

$U(F)$ is called the *covariant bialgebra* of $F(X, Y)$; it has also been called the *hyperalgebra* of $F(X, Y)$. Note that $R(F) = \mathbf{Mod}_A(U(F), A)$ and that by dualizing all the A-module homomorphisms in (36.1.8) we get back the continuous A-module homomorphisms (36.1.6) and (36.1.7).

■ (36.1.9) **Summary** Summarizing we see that we have associated to a formal group law $F(X, Y)$ two objects:

(i) its contravariant bialgebra $R(F)$, which is a cogroup object in the category of power series algebras over A; $R(F)$ is cocommutative iff $F(X, Y)$ is commutative;

(ii) its covariant bialgebra $U(F)$, which is almost a commutative cogroup object in the category of associative algebras over A (with unit); $U(F)$ is commutative if and only if $F(X, Y)$ is commutative (and then $U(F)$ is a cogroup object).

Moreover, the objects $R(F)$ and $U(F)$ are dual to each other, where one gets from $R(F)$ to $U(F)$ by taking *continuous linear* duals and from $U(F)$ to $R(F)$ by taking *linear* duals.

Further, this duality extends to the categories formed by the $U(F)$'s and $R(F)$'s. A morphism of power series algebras $R(F) \to R(G)$ is a morphism of cogroup objects iff its continuous linear dual is an algebra homomorphism and a morphism of "cogroup objects." And vice versa. (This duality is known as Cartier duality.)

■ (36.1.10) **Remark** In Section 37.2 we shall discuss more general formal groups than those that we have encountered so far (which are those whose associated contravariant bialgebra is a power series algebra) and discuss Cartier duality in this more general context.

■ (36.1.11) **Theorem** Let $\hat{W}(X, Y)$ be the (infinite dimensional) formal group law of Witt vectors over $\mathbf{Z}$. Then $U(\hat{W}) = \mathbf{Z}[Z_1, Z_2, \ldots]$ as a $\mathbf{Z}$-algebra and the comultiplication is given by $Z_n \mapsto \sum_{i=0}^{n} Z_i \otimes Z_{n-i}$ where we take $Z_0 = 1$.

36.2 Formal Lie theory (revisited)

Let $F(X, Y)$ be a finite dimensional formal group law over A. In Chapter II we associated to $F(X, Y)$ a Lie algebra $L(F)$ as follows. As an A-module, $L(F) = A^n$ where $n = \dim(F)$, and letting e_i be the canonical ith basis vector of A^n the Lie algebra structure is defined by

$$[e_j, e_k] = \sum_{i=1}^{n} (\gamma_{jk}^i - \gamma_{kj}^i) e_i \tag{36.2.1}$$

where the γ_{jk}^i are determined by $F(i)(X, Y) \doteq X_i + Y_i + \sum_{j,k} \gamma_{j,k}^i X_j Y_k$ mod(degree 3).

This defined a functor *Lie*: $\mathbf{FG}_A \to \mathbf{LA}_A$ and we asserted that *Lie* was an equivalence of categories in the case that A is a $\mathbf{Q}$-algebra. Of this we proved that for every $L \in \mathbf{LA}_A$ there is an $F(X, Y) \in \mathbf{FG}_A$ such that $L(F) \simeq L$ but we left till later the proof that *Lie* induces a bijection

$$\mathbf{FG}_A(F(X, Y), G(X, Y)) \xrightarrow{\sim} \mathbf{LA}_A(L(F), L(G)) \tag{36.2.2}$$

Let $U(F)$ be the covariant bialgebra of $F(X, Y)$. We define a map ψ: $L(F) \to U(F)$ as follows: $e_i \mapsto \Delta_i$ where Δ_i is the continuous homomorphism $R(F) \to A$ defined by $\Delta_i(a(X)) =$ coefficient of X_i in $a(X)$.

■ (36.2.3) **Lemma** ψ is a Lie homomorphism. That is, $\psi[x, y] = \psi(x)\psi(y) - \psi(y)\psi(x)$.

Proof By the definition of the multiplication in $U(F)$ we have $\psi(e_j)\psi(e_k)(a(X)) =$ coefficient of $X_j Y_k$ in $a(F(X, Y))$, so if

$$a(X) = a_0 + \sum_{i=1}^{n} a_i X_i + \sum_{r,s} b_{rs} X_r X_s \quad \text{mod(degree 3)}$$

we have that

$$\psi(e_j)\psi(e_k)(a(X)) = \sum_{i=1}^{n} a_i \gamma_{jk}^i + b_{jk} + b_{kj}$$

so that

$$(\psi(e_j)\psi(e_k) - \psi(e_k)\psi(e_j))(a(X)) = \sum_{i=1}^{n} a_i(\gamma_{jk}^i - \gamma_{kj}^i) = \psi([e_j, e_k])(a(X))$$

proving the lemma.

■ (36.2.4) Now let $UL(F)$ be the universal enveloping algebra of $L(F)$. Then by the universality property we find by (36.2.3) a unique homomorphism of associative algebras

(36.2.5) $$\phi\colon UL(F) \to U(F)$$

■ (36.2.6) **Theorem** If A is a $\mathbf{Q}$-algebra, the homomorphism of associative algebras (36.2.5) is an isomorphism.

■ (36.2.7) Using (36.2.6) and Cartier duality (cf. (36.1.9)), it is now not difficult to prove the remainder of formal Lie theory, roughly as follows: $\mathbf{FG}_A(F(X, Y), G(X, Y)) \to \mathbf{LA}_A(L(F), L(G))$ is always injective if A is of characteristic zero (cf. (37.4.9)). Now let $\chi\colon L(F) \to L(G)$ be a homomorphism of Lie algebras. Then there is an induced homomorphism of the universal enveloping algebras $U(\chi)\colon UL(F) \to UL(G)$, hence by Theorem (36.2.6) we have a (bialgebra) homomorphism $U(F) \to U(G)$ which by Cartier duality gives us a (bialgebra) homomorphism $R(G) \to R(F)$ and this in turn gives us a homomorphism of formal group laws $F(X, Y) \to G(X, Y)$; cf. (36.1.4).

■ (36.2.8) **Remark** Theorem (36.2.6) can also be used to prove the formal version of Lie's third theorem (which we proved via the Campbell–Hausdorff formula in Section 14.5 of Chapter II). The argument is of course as follows. Let L be a Lie algebra and UL its universal enveloping algebra, which is a bialgebra. Take $R = \mathbf{Mod}_A(UL, A)$. If we can prove that R is a power series algebra over A, we are through. This is a consequence of the Poincaré–Birkhoff–Witt theorem together with the fact that the comultiplication on UL is given by $x \mapsto x \otimes 1 + 1 \otimes x$ for $x \in L$; cf. (37.4.11) below for the details.

36.3 Curves in noncommutative formal group laws

■ (36.3.1) **Curves** Let $F(X, Y)$ be a not necessarily commutative formal group law over a ring A. A curve in $F(X, Y)$ is an n-tuple of formal power series $\gamma(t)$ such that $\gamma(0) = 0$ (where $n = \dim(F(X, Y))$. By Appendix (A.4.2) $\gamma(t)$ defines a unique continuous homomorphism $\phi(t)\colon R(F) \to A[\![t]\!]$ such that $\phi(t)(X_i) = \gamma(i)(t)$ where $\gamma(i)(t)$ is the ith component of $\gamma(t)$. We write ϕ_i for the coefficient of t^i in $\phi(t)$, so that

(36.3.2) $$\phi(t) = \sum_{i=0}^{\infty} \phi_i t^i, \qquad \phi_i \in U(F)$$

where the ϕ_i are A-linear continuous maps $R(F) \to A$, i.e., elements of $U(F)$. The fact that $\gamma(0) = 0$ means that $\phi_0 = \varepsilon$: $R(F) \to A$, which is the unit element of the associative algebra $U(F)$, and the fact that $\phi(t)$ is an algebra homomorphism translates into

$$\mu\phi_n = \sum_{i+j=n} \phi_i \otimes \phi_j \tag{36.3.3}$$

So $\phi(t)$ is a special sort of element of $1 + tU(F)[\![t]\!]$. Now, using the ring structure of $U(F)$, $1 + tU(F)[\![t]\!]$ is a group. It turns out that the correspondence $\gamma(t) \mapsto \phi(t)$ set up above defines an isomorphism of groups from $\mathscr{C}(F; A)$ onto the subgroup of $1 + tU(F)[\![t]\!]$ consisting of all $1 + \phi_1 t + \phi_2 t^2 + \cdots$ such that (36.3.3) holds.

Moreover, it turns out that in the case of a commutative formal group law $F(X, Y)$ over a characteristic zero ring A, the role of the logarithm $f(X)$ of $F(X, Y)$ is taken over by the ordinary logarithm series $\log(1 + Z) = \sum (-1)^n n^{-1} Z^n$ which takes the group $1 + tU(F)[\![t]\!]$ into the additive group $tU(F)[\![t]\!]$ (coefficientwise addition).

■ (36.3.4) **Divided power sequences** Let $u \in U(F)$, then u defines an A-linear endomorphism $x \mapsto xu$; dualizing this, one find an endomorphism ∂: $R(F) \to R(F)$. Now let $1, \phi_1, \phi_2, \ldots$ be a sequence of elements of $U(F)$ such that (36.3.3) holds. This gives a sequence of A-linear endomorphisms $\partial_1, \partial_2, \partial_3, \ldots$ of $R(F)$ such that

$$\partial_n(xy) = \sum_{i+j=n} \partial_i(x)\partial_j(y), \qquad \partial_0 = id \tag{36.3.5}$$

More generally, if B is any A-algebra, then a sequence of A-module endomorphism $\partial_0, \partial_1, \partial_2$ such that (36.3.5) holds is called a divided power sequence. We write formally $\partial(t) = \sum \partial_i t^i$. Then the set of all divided power sequences becomes a group $H_A(B)$ under the multiplication

$$\partial(t)\hat{\partial}(t) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \partial_i \hat{\partial}_{n-i} \right) t^n \tag{36.3.6}$$

Now suppose that A is a $\mathbf{Q}$-algebra. Let $\partial_1 \in \mathrm{Der}_A(B)$, i.e., ∂_1 is an A-module endomorphism of B satisfying $\partial_1(xy) = (\partial_1 x)y + x(\partial_1 y)$. Then $\exp(\partial_1 t) = id + \partial_1 t + (2!)^{-1}\partial_1^2 t^2 + (3!)^{-1}\partial_1^3 t^3 + \cdots$ is an element of $H_A(B)$, and one proves that every element of $H_A(B)$ can be uniquely written in the form

$$\exp\left(\sum_{i=1}^{\infty} \partial_i t^i \right), \qquad \partial_i \in \mathrm{Der}_A(B) \tag{36.3.7}$$

If $B = K(F)$ where $F(X, Y)$ is a formal group law over A, then every curve in $\mathscr{C}(F; A) = \mathscr{C}(U(F); A)$ gives rise to an element of $H(R(F))$; but of course not all elements $H(R(F))$ arise in this way. The ones that do arise in this way are easily characterized as those $\sum \partial_i t^i \in H(R(F))$, $\partial_i \in \mathbf{Mod}_A T(R(F), A)$, such that all ∂_i

are left invariant in the sense that $\mu \circ \partial_i = (1 \hat{\otimes} \partial_i) \circ \mu$. Using this and (36.3.7) then enables one to reprove the Campbell–Hausdorff theorem (14.4.14) of Chapter II (cf. (38.2.12)).

■ (36.3.8) **The bialgebra U** In the case of a commutative formal group law $F(X, Y)$ we have the representation theorem which says that for every curve $\gamma(t) \in \mathscr{C}(F; A)$, there is a unique homomorphism of formal group laws $\alpha_\gamma(X)$: $\hat{W}(X, Y) \to F(X, Y)$ such that $\alpha_\gamma(\gamma_w(t)) = \gamma(t)$, where $\gamma_w(t)$ is a certain standard curve in $\hat{W}(X, Y)$. Taking covariant bialgebras, we see that $U(\hat{W}) = \mathbf{U}^c$ represents the functor $U(F) \mapsto \mathscr{C}(U(F); A)$, for commutative formal group laws $F(X, Y)$.

Now by (36.1.11) $\mathbf{U}^c = \mathbf{Z}[Z_1, Z_2, \ldots]$ as an algebra, and the comultiplication is given by $Z_n \mapsto \sum_{i+j=n} Z_i \otimes Z_j$. There is an obvious noncommutative analogue of $\mathbf{U}^c$, viz. the Hopf algebra

$$\mathbf{U} = \mathbf{Z}\langle Z_1, Z_2, \ldots \rangle, \qquad Z_n \mapsto \sum_{i=0}^{n} Z_i \otimes Z_{n-i}, \qquad Z_0 = 1$$

of noncommutative polynomials in $Z_1, Z_2, \ldots$ over $\mathbf{Z}$.

One almost trivially has that $\mathbf{U}$ represents (in the covariant bialgebra sense) the functor "curves." Thus $\mathbf{U}$ can be seen as the noncommutative analogue of the covariant bialgebra of the Witt vectors and one can ask whether $\mathbf{U}$ comes from an (infinite dimensional noncommutative) formal group law. It does (Theorem (38.1.10); we shall give no proof).

■ (36.3.9) **Decomposition** If A is a $\mathbf{Z}_{(p)}$-algebra and $F(X, Y)$ a formal group law over A, then, almost trivially, one has the fact that every curve in $F(X, Y)$ can be written as a unique sum of shifted p-typical curves. Something similar is (definitely nontrivially) true in the noncommutative case, and the final subsection (38.4) is devoted to a description of this result (no proofs).

37 Formal Groups and Bialgebras

37.1 Coalgebras, bialgebras, and Hopf algebras

In this subsection A is a fixed base ring (commutative with 1, as always). Unlabeled tensor products will be tensor products over A.

■ (37.1.1) **Coalgebras** A coalgebra over a ring A is an A-module C together with two A-module homomorphisms

$$\mu\colon C \to C \otimes C, \qquad \varepsilon\colon C \to A$$

such that $(1 \otimes \mu) \circ \mu = (\mu \otimes 1) \circ \mu$, $(\varepsilon \otimes 1) \circ \mu = (1 \otimes \varepsilon) \circ \mu = id$ (where we have identified $A \otimes C \simeq C \simeq C \otimes A$). In categorical terms (cf. diagrams 1 and 2 of (36.1.3)) a coalgebra over A is a comonoid object in $\mathbf{Mod}_A$ with two-sided counit.

The coalgebra C is said to be cocommutative if $\tau \circ \mu = \mu$ where $\tau: C \otimes C \to C \otimes C$ is the switching morphism which interchanges the two factors.

An A-module morphism $\phi: C_1 \to C_2$, where C_1 and C_2 are coalgebras over A, is said to be a morphism of coalgebras iff $(\phi \otimes \phi) \circ \mu_1 = \mu_2 \circ \phi$ and $\varepsilon_2 \phi = \varepsilon_1$.

If C_1 and C_2 are two coalgebras over A, then $C_1 \otimes C_2$ is given a coalgebra structure as follows:

$$C_1 \otimes C_2 \xrightarrow{\mu_1 \otimes \mu_2} (C_1 \otimes C_1) \otimes (C_2 \otimes C_2) \xrightarrow{1 \otimes \tau \otimes 1} (C_1 \otimes C_2) \otimes (C_1 \otimes C_2)$$

$$C_1 \otimes C_2 \xrightarrow{\varepsilon_1 \otimes \varepsilon_2} A \otimes A \simeq A$$

$C_1 \otimes C_2$ is the categorical product in the category of coalgebras. The category also has a final object, viz. A, with the obvious trivial coalgebra structure and the unique morphism of coalgebras $C \to A$ into the final object is $\varepsilon: C \to A$.

■ (37.1.2) **Bialgebras** A bialgebra over a ring A is an A-module B together with four A-module homomorphisms

$$\mu: B \to B \otimes B, \qquad \varepsilon: B \to A$$

$$m: B \otimes B \to B, \qquad e: A \to B$$

such that the following conditions hold:

(i) (B, μ, ε) is a coalgebra over A;
(ii) (B, m, e) is an associative algebra over A;
(iii) μ and ε are A-algebra morphisms;
(iv) m and e are A-coalgebra morphisms.

There is some redundancy in these requirements. In fact, conditions (iii) and (iv) are equivalent. In fact, μ is multiplication preserving iff $\mu \circ m = (m \otimes m) \circ (1 \otimes \tau \otimes 1) \circ (\mu \otimes \mu)$ and this holds iff m is comultiplication preserving. Similarly, ε is unit preserving iff $\varepsilon \circ e = id$, and this is the case iff e is counit preserving. Further, m is counit preserving iff $\varepsilon \circ m = \varepsilon \otimes \varepsilon$ (identifying $A \simeq A \otimes A$) which is the case iff ε is multiplication preserving; and finally μ is unit preserving iff $e \otimes e = \mu \circ e$ (again identifying $A \simeq A \otimes A$ canonically) which is the case iff e is comultiplication preserving.

Let B_1 and B_2 be bialgebras over A. Then an A-module homomorphism $\phi: B_1 \to B_2$ is a morphism of bialgebras iff ϕ is a homomorphism of coalgebras and a homomorphism of algebras, i.e., if

$$(\phi \otimes \phi) \circ \mu_1 = \mu_2 \circ \phi, \quad \varepsilon_2 \phi = \varepsilon_1, \quad \phi e_1 = e_2, \quad \phi \circ m_1 = m_2 \circ (\phi \otimes \phi)$$

The bialgebra A over A is both final and initial object in the category of bialgebras: the unique morphisms being $e: A \to B$, $\varepsilon: B \to A$. If B_1 and B_2 are bialgebras, then $B_1 \otimes_A B_2$ with the obvious bialgebra structure is both sum and product in the category of bialgebras over A. The bialgebra B is called cocommutative if the underlying coalgebra is cocommutative, and commutative if the underlying algebra is commutative.

■ (37.1.3) **The convolution product** Let C be a coalgebra over A and D an algebra over A. Then $\mathbf{Mod}_A(C, D)$ can be given an A-algebra structure as follows. Let $\alpha, \beta \in \mathbf{Mod}_A(C, D)$, then $\alpha * \beta$, the convolution product of α and β, is the composite A-module morphism

$$C \xrightarrow{\mu_C} C \otimes C \xrightarrow{\alpha \otimes \beta} D \otimes D \xrightarrow{m_D} D$$

One checks easily that this defines an associative A-linear multiplication on $\mathbf{Mod}_A(C, D)$ for which $e_D\varepsilon_C\colon C \to A \to D$ is the (two-sided) unit element. We shall usually write $1_{C,D}$ for this element.

Let $\gamma\colon D_1 \to D_2$ be a morphism of algebras. Then γ induces a convolution multiplication and convolution unit preserving A-linear map $\mathbf{Mod}_A(C, D_1) \to \mathbf{Mod}_A(C, D_2)$. Dually, if $\delta\colon C_1 \to C_2$ is a morphism of coalgebras, then δ induces a convolution multiplication and convolution unit preserving A-linear map $\mathbf{Mod}_A(C_2, D) \to \mathbf{Mod}_A(C_1, D)$. In formulas one has

$$\begin{aligned} &\gamma(\alpha * \beta) = (\gamma\alpha) * (\gamma\beta), \qquad \gamma 1_{C,D_1} = 1_{C,D_2} \\ &(\alpha * \beta)\delta = (\alpha\delta) * (\beta\delta), \qquad 1_{C_2,D}\delta = 1_{C_1,D} \end{aligned} \tag{37.1.4}$$

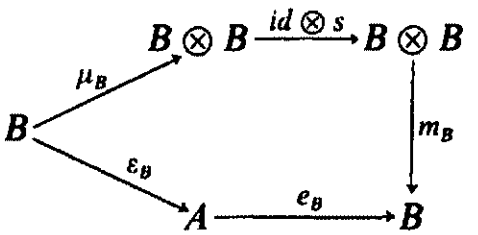
■ (37.1.5) $\sum$ **notation** Let C be a coalgebra and $x \in C$. We shall write

$$\mu_C(x) = \sum_{(x)} x_{(1)} \otimes x_{(2)}$$

This convenient and useful notation is due to Heynemann and Sweedler (cf. [401, Section 1.2]). Let D be an algebra. Using this notation, the convolution product $\alpha * \beta$ of two A-module morphisms is given by

$$(\alpha * \beta)(x) = \sum_{(x)} \alpha(x_{(1)})\beta(x_{(2)})$$

■ (37.1.6) **Antipodes** Let B be a bialgebra over A. An *antipode* for B is a morphism of A-modules $s\colon B \to B$ such that s is a two-sided inverse for $id_B \in \mathbf{Mod}_A(B, B)$ under the convolution product defined in (37.1.3), i.e., $id * s = e_B\varepsilon_B = s * id$. Equivalently, s is an A-module morphism such that the following diagram:



and the corresponding diagram with $s \otimes id$ instead of $id \otimes s$ both commute. Comparing this with diagrams 3 of (36.1.2) and (36.1.3), we see that the bialgebra B with antipode s is a cogroup object in the category of algebras if s happens to be an algebra homomorphism and that (B, s) is a group object in the category of coalgebras if s happens to be a coalgebra morphism. These things happen rather often as Proposition (37.1.8) below shows.

■ (37.1.7) **Definition** A *Hopf algebra* over A is a pair consisting of a bialgebra B with an antipode s.

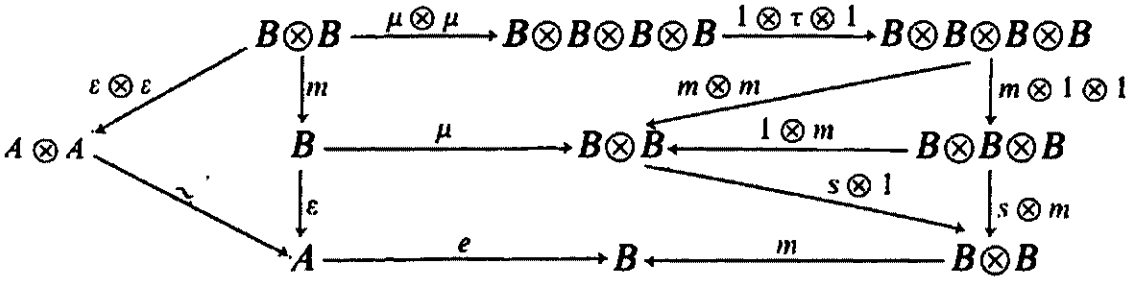
(37.1.8) **Proposition** Let (B, s) be a bialgebra with antipode s over A (i.e., a Hopf algebra). Then s has the properties:

(i) $s(xy) = s(y)s(x)$ for all $x, y \in B$.
(ii) $s(1) = 1$ (where 1 is the unit element of the algebra B).
(iii) $\varepsilon_B \circ s = \varepsilon_B$.
(iv) $\tau \circ (s \otimes s) \circ \mu_B = \mu_B \circ s$.
(v) If B is commutative or cocommutative, then $s \circ s = id$.

Proof (i) Let α, β, γ: $B \otimes B \to B$ be respectively the A-module morphisms $\alpha(x \otimes y) = xy$, $\beta(x \otimes y) = s(y)s(x)$, $\gamma(x \otimes y) = s(xy)$. We now first show that

$$\gamma * \alpha = 1 = \alpha * \beta, \qquad \text{where} \quad 1 = e_B \circ \varepsilon_{B \otimes B} \tag{37.1.9}$$

That $\gamma * \alpha = 1$ is proved by the commutative diagram



Here $\gamma * \alpha$ is, by definition, the composite morphism $B \otimes B \to B$ obtained by starting in $B \otimes B$ at the upper left and going right–down–left along the outer edge. The two triangles on the right are obviously commutative; the triangle on the left is commutative because ε is an A-algebra homomorphism; the upper pentagon is commutative because μ is an A-algebra morphism; and the lower pentagon is commutative because s is an antipode.

To prove that $\alpha * \beta = 1$ we use the $\sum$ notation of (37.1.5). We have

$$\begin{aligned}(\alpha * \beta)(x \otimes y) &= \sum_{(x),(y)} \alpha(x_{(1)} \otimes y_{(1)})\beta(x_{(2)} \otimes y_{(2)}) \\ &= \sum_{(x),(y)} x_{(1)}y_{(1)}s(y_{(2)})s(x_{(2)})\end{aligned}$$

Now because s is an antipode $\sum_{(y)} y_{(1)}s(y_{(2)}) = e_B\varepsilon_B(y)$, and since all morphisms are A-linear and $\varepsilon_B(y) \in A$, we have

$$(\alpha * \beta)(x \otimes y) = e_B\varepsilon_B(y) \sum_{(x)} x_{(1)}s(x_{(2)}) = e_B\varepsilon_B(y)e_B\varepsilon_B(x)$$

so that indeed $\alpha * \beta = 1$. Using the associativity of the convolution multiplication, we now have from (37.1.9)

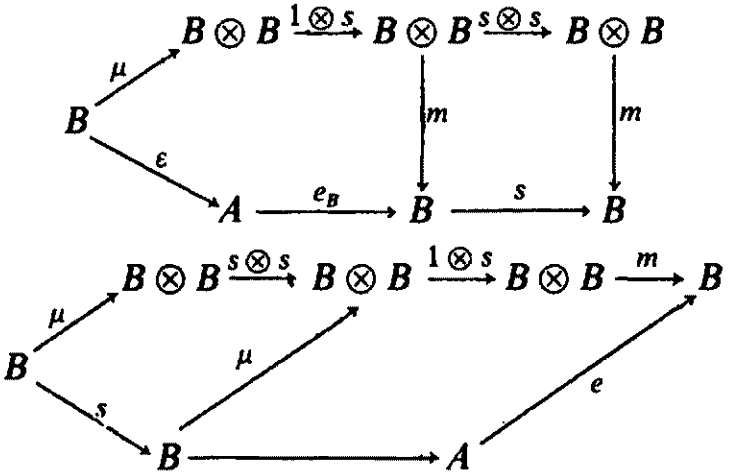
$$\gamma = \gamma * (\alpha * \beta) = (\gamma * \alpha) * \beta = \beta$$

which proves (i). (Of course one can also prove $\alpha * \beta = 1$ by a (rather large) diagram and, conversely, $\gamma * \alpha = 1$ by use of the $\sum$ notation.)

(ii) Because s is an antipode and $\mu(1) = 1 \otimes 1$, we have $e_B\varepsilon_B(1) = 1s(1) = s(1)$. On the other hand, $\varepsilon_B(1) = 1$ and $e_B(1) = 1$ because ε_B is an A-algebra homomorphism and because (by definition) the unit element of the algebra B is $e_B(1)$, $1 \in A$.

(iii) and (iv) These are the dual statements of (ii) and (i), respectively, and are proved similarly. (For (iv) one considers $\alpha', \beta', \gamma' : B \to B \otimes B$ with $\alpha' = \mu_B$, $\beta' = \tau \circ (s \otimes s) \circ \mu_B$, $\gamma' = \mu_B \circ s$.)

(v) Consider the two diagrams



If B is commutative, the first diagram is commutative by (i); and if B is cocommutative, the second diagram is commutative by (iv). Using also (ii) and (iii), we see that in both cases $s * s \circ s = e_B\varepsilon_B = 1_{B,B}$. On the other hand, $id * s = e_B\varepsilon_B = 1_{B,B}$ and by the associativity of the convolution multiplication we find $s \circ s = id$ as in the proof of (i). Q.E.D.

■ (37.1.10) **Proposition** Let B_1 and B_2 be two Hopf algebras over A and let $\alpha : B_1 \to B_2$ be a morphism of the underlying bialgebras. Then α is also a morphism of Hopf algebras (i.e., $\alpha s_1 = s_2\alpha$). (In particular a given bialgebra can have at most one antipode.)

Proof α is a morphism of algebras; so if 1 denotes the unit element of the convolution algebra $\mathbf{Mod}_A(H_1, H_2)$, we have by (37.1.4)

$$1 = \alpha_*(id * s_1) = \alpha * \alpha s_1$$

On the other hand, using that α is a morphism of coalgebras, we have also by (37.1.4)

$$1 = \alpha^*(s_2 * id) = s_2\alpha * \alpha$$

And therefore

$$s_2\alpha = s_2\alpha * 1 = s_2\alpha * (\alpha * \alpha s_1) = (s_2\alpha * \alpha) * \alpha s_1 = 1 * \alpha s_1 = \alpha s_1. \quad \text{Q.E.D.}$$

37.2 The basic categories and Cartier duality

■ (37.2.1) **The category $\mathbf{Mod}T_A$** An object of $\mathbf{Mod}T_A$ is a topological A-module isomorphic to a direct product of free A-modules of rank 1, where the factors have the discrete topology. That is, if $M \in \mathbf{Mod}T_A$, then

$$M \simeq \prod_{i \in I} Am_i \tag{37.2.2}$$

for a certain index set I and a basis of the open subsets in M is given by the inverse images of elements of $\prod_{i \in \kappa} Am_i$ under the natural projection $M \to \prod_{i \in \kappa} Am_i$ where κ runs through all finite subsets of I. Morphisms in $\mathbf{Mod}T_A$ are continuous A-module morphisms. A set of elements $\{m_i \mid i \in I\} \subset M$ such that $M = \prod_{i \in I} Am_i$ is called a *pseudobasis* of M.

■ (37.2.3) **Definition** Let I be a set. A collection $\mathcal{S}$ of subsets of I is called *directed* (sometimes *filtered*) if for every $\kappa_1, \kappa_2 \in S$ there is a $\kappa \in \mathcal{S}$ such that $\kappa_1 \cup \kappa_2 \subset \kappa$.

■ (37.2.4) **The category $\mathbf{AlT}_A$** An object of $\mathbf{AlT}_A$ is a topological A-algebra R (commutative, with 1) that as a topological A-module is an object of $\mathbf{Mod}T_A$ and such that there exists a pseudobasis $\{r_i \mid i \in I\} \subset R$ and a directed set $\mathcal{S}$ of finite subsets of I such that:

(i) $I_\kappa = \{\prod_{i \in I} a_i r_i \mid a_i = 0 \text{ for all } i \in \kappa\}$ is an ideal of R for all $\kappa \in \mathcal{S}$.
(ii) The ideals I_κ, $\kappa \in \mathcal{S}$ define the topology of R.

A morphism of $\mathbf{AlT}_A$ is simply a continuous A-algebra homomorphism.

Let $\mathbf{AlT}_A^f$ be the full subcategory of $\mathbf{AlT}_A$ consisting of those R that as A-modules are free of finite rank (with discrete topology). Then an object $R \in \mathbf{AlT}_A$ is in particular a strict directed projective limit of objects in $\mathbf{AlT}_A^f$, and a morphism in $\mathbf{AlT}_A$ is always induced by a morphism between strict directed projective systems in $\mathbf{AlT}_A^f$.

If A is a field, $\mathbf{Mod}T_A$ is simply the category of linearly compact A-vector spaces and $\mathbf{AlT}_A$ is the category of A-algebras whose underlying vector space is linearly compact.

The T's in $\mathbf{Mod}T$ and $\mathbf{AlT}$ serve as a mnemonic for "topological."

The category $\mathbf{AlT}_A$ has finite sums and as initial object A itself. The sum of R_1, R_2 in $\mathbf{AlT}_R$ is the completed tensorproduct $R_1 \hat{\otimes} R_2$.

■ (37.2.5) **The category $\mathbf{Clg}_A$** An object of $\mathbf{Clg}_A$ is a cocommutative coalgebra U over A whose underlying A-module is free such that there exists a basis $\{u_i \mid i \in I\}$ and a directed set $\mathcal{S}$ of finite subsets of I such that the submodules $\sum_{i \in \kappa} Au_i \subset U$ are subcoalgebras of U for all $\kappa \in \mathcal{S}$. (This is a strictly dual situation to that of (37.2.4): the condition (ii) of (37.2.4) corresponds to the "directedness" of $\mathcal{S}$, a condition that is implied by (ii) in the situation of (37.2.4).)

A morphism of $\mathbf{Clg}_A$ is simply a coalgebra morphism. The category $\mathbf{Clg}_A$ has finite products and a final object. If A is a field, $\mathbf{Clg}_A$ is simply the category of all coalgebras over A since in that case every finite dimensional subspace is contained in some finite dimensional subcoalgebra; cf. [368].

■ (37.2.6) **Cartier duality** (first installment) Let $R \in \mathbf{AlT}_A$. Considering R for the moment as an object of $\mathbf{Mod}T_A$, the algebra structure of R is given by a bilinear map $m\colon R \times R \to R$ and a morphism $A \to R$. Since m is bilinear, it induces a morphism $R \otimes R \to R$; and since m is continuous and R complete, this morphism extends to a morphism $m\colon R \hat{\otimes} R \to R$ in $\mathbf{Mod}T_A$.

Now let $D^T\colon \mathbf{Mod}T_A \to \mathbf{Mod}F_A$, where $\mathbf{Mod}F_A$ is the category of free A-modules, be the functor "linear topological dual." That is,

$$D^T(M) = \mathbf{Mod}T_A(M, A)$$

Applying D^T to $m\colon R \hat{\otimes} R \to R$ we obtain an A-module morphism $\mu\colon D^T(R) \to D^T(R) \otimes D^T(R)$; and applying D^T to $A \to R$, we obtain an A-module morphism $\varepsilon\colon D^T(R) \to A$.

We now claim that $(D^T(R), \mu, \varepsilon)$ is an object of $\mathbf{Clg}_A$. This is easily checked. First, $(D^T(R), \mu, \varepsilon)$ is certainly a cocommutative coalgebra. Second, let $\{r_i \mid i \in I\}$ be a pseudobasis for R and $\mathscr{S}$ a set of finite subsets of I such that (i) and (ii) of (37.2.4) hold. For each $i \in I$, define u_i by $u_i(r_j) = 0$ if $j \neq i$ and $u_i(r_i) = 1$. Then $\{u_i \mid i \in I\}$ is a basis for $D^T(R)$; and if $\kappa \in \mathscr{S}$, we have that $\sum_{i \in \kappa} Au_i$ is a subcoalgebra of $D^T(R)$ precisely because $\{\prod_{i \in I} a_i r_i \mid a_i = 0$ for $i \in \kappa\}$ is an ideal of R.

Conversely, let $U \in \mathbf{Clg}_A$. We now define

$$D(U) = \mathbf{Mod}_A(U, A)$$

and we give $D(U)$ the obvious A-algebra structure. The topology on $D(U)$ is defined as follows. Take any basis $\{u_i \mid i \in J\}$ of U; for each finite subset $\lambda \subset J$, let $M_\lambda = \{f \in D(U) \mid \phi(u_i) = 0$, all $i \in \lambda\}$. Then the subgroups M_λ for all finite λ define the topology of $D(U)$. In particular, we can take a basis $\{u_i \mid i \in I\}$ such that there is a directed set of $\mathscr{S}$ of finite subsets such that the condition of (37.2.5) holds. Let $r_i \in D(U)$ be defined by $r_i(u_j) = 0$ if $j \neq i$, $r_i(u_i) = 0$, then $\{r_i \mid i \in I\}$ is a pseudobasis for $D(U)$; and if $\kappa \in \mathscr{S}$, then

$$\{\prod a_i r_i \mid a_i = 0 \text{ for } i \in \kappa\} = \{\phi \in D(U) \mid \phi(u_i) = 0 \text{ for all } i \in \kappa\}$$

is an open ideal in $D(U)$, and these ideals define the topology of $D(U)$ because $\mathscr{S}$ is directed.

It is clear that $D^T D(U) \simeq U$, $DD^T(R) = R$, so that we have

■ (37.2.7) **Proposition** The functors $D^T\colon \mathbf{AlT}_A \to \mathbf{Clg}_A$, $D\colon \mathbf{Clg}_A \to \mathbf{AlT}_A$ define a duality between the categories $\mathbf{AlT}_A$ and $\mathbf{Clg}_A$.

■ (37.2.8) **Definitions and notations** We let $G\mathbf{Clg}_A$ be the category of group objects in $\mathbf{Clg}_A$ and $G^c\mathbf{Clg}_A$ the category of commutative group objects in

$\mathbf{Clg}_A$. Dually, $C\mathbf{AlT}_A$ is the category of cogroup objects in $\mathbf{AlT}_A$ and $C^c\mathbf{AlT}_A$ the category of cocommutative cogroup objects.

■ (37.2.9) **Proposition** (Cartier duality; second installment) The functors D^T and D of Proposition (37.2.7) define a duality between the categories $C\mathbf{AlT}_A$ and $G\mathbf{Clg}_A$, and a duality between $C^c\mathbf{AlT}_A$ and $G^c\mathbf{Clg}_A$.

Proof Let $R \in C\mathbf{AlT}_A$. Then R is a topological Hopf algebra over A whose underlying topological A-algebra is in $\mathbf{AlT}_A$. Let

$$\bar{m}_R\colon R \hat{\otimes} R \to R, \qquad \bar{e}_R\colon A \to R$$

$$\bar{\imath}_R\colon R \to R$$

$$\bar{\mu}_R\colon R \to R \hat{\otimes} R, \qquad \bar{\varepsilon}_R\colon R \to A$$

be the five structure maps of R. Applying D^T and writing U for $D^T(R)$, we obtain five structure maps

$$\mu_U\colon U \to U \otimes U, \qquad \varepsilon_U\colon U \to A$$

$$i_U\colon U \to U$$

$$m_U\colon U \otimes U \to U, \qquad e_U\colon A \to U$$

Of these μ_U and ε_U make U an object of $\mathbf{Clg}_A$. Further, m_U and e_U are coalgebra morphisms because μ_R and ε_R are algebra morphisms. Thus U is a bialgebra (cf. (37.1.2)). Further, as is easily checked, i_U is an antipode for the bialgebra U (because $\bar{\imath}_R$ is an antipode for R). Because U is cocommutative, it follows i_U is a coalgebra morphism. Hence U is in $G\mathbf{Clg}_A$. Similarly, one proves that $D(U) \in C\mathbf{AlT}_A$ if $U \in G\mathbf{Clg}_A$; and it is obvious that D^T (resp. D) takes cocommutative (resp. commutative) objects into commutative (resp. cocommutative) objects. Q.E.D.

37.3 Formal groups, affine group schemes, and more Cartier duality

■ (37.3.1) **The category of formal groups over** A Let $\mathbf{AlT}^f_A$ be the category of A-algebras that as modules over A are free and finitely generated. A formal group (scheme) over A is now defined as a covariant functor $F\colon \mathbf{AlT}^f_A \to \mathbf{Group}$ which is representable by an object in $C\mathbf{AlT}_A$, where by the last phrase we mean that there is an $R \in C\mathbf{AlT}_A$ such that

(37.3.2) $$F(S) \simeq \mathbf{AlT}_A(R, S)$$

functorially for all $S \in \mathbf{AlT}^f_A$, while the group structure on $F(S)$ is induced by the cogroup object structure of $R \in C\mathbf{AlT}_A$. Practically by definition therefore the category of formal group (schemes) over A is equivalent to the category $C\mathbf{AlT}_A$. The only thing to check is that the functors F_1, F_2 associated to nonisomorphic R_1, R_2 permit us to see that R_1 and R_2 are nonisomorphic, and

this is precisely the case because R_1 and R_2 are strict projective limits of objects in $\mathbf{AlT}_A^f$.

Let $\mathbf{Gf}_A$ denote the category of formal group (schemes) over A. Then there is a natural fully faithful embedding of the category of formal group laws $\mathbf{FG}_A$ in $\mathbf{Gf}_A$, obtained by associating to $F(X, Y)$ its contravariant bialgebra $R(F) \in C\mathbf{AlT}_A$ (cf. (36.1.4) above; cf. also Sections 1.3 of Chapter I and 9.3 of Chapter II).

We now have four categories:

$\mathbf{FG}_A$: formal group laws over A of any dimension, not necessarily commutative;

$\mathbf{Gf}_A$: formal group (schemes) over A. We shall call an object $F \in \mathbf{Gf}_A$ *smooth* if it can be represented by a power series algebra over A. Thus $\mathbf{FG}_A$ is equivalent to the full subcategory of $\mathbf{Gf}_A$ of smooth formal groups. But $\mathbf{Gf}_A$ is definitely larger containing, e.g., also finite group schemes over A, whose underlying A-module is free and of finite rank over A;

$C\mathbf{AlT}_A$: cogroup objects in $\mathbf{AlT}_A$; this category is antiequivalent to $\mathbf{Gf}_A$ and the objects corresponding to smooth formal groups, i.e., objects "in" $\mathbf{FG}_A$ are those whose underlying topological A-algebra is of the form $A[\![X_i \mid i \in I]\!]$;

$G\mathbf{Clg}_A$: group objects in $\mathbf{Clg}_A$, the category of commutative coalgebras over A. This category is antiequivalent to $C\mathbf{AlT}_A$ (and therefore equivalent to $\mathbf{Gf}_A$) by Cartier duality.

■(37.3.3) **The category of (commutative) affine group schemes over A** An affine group scheme over A is (by definition) a functor $G: \mathbf{Alg}_A \to \mathbf{Group}$ which is representable by an object $C \in \mathbf{Alg}_A$, i.e., $G(B) = \mathbf{Alg}_A(C, B)$ for all $B \in \mathbf{Alg}_A$. The object C is then necessarily a cogroup object in $\mathbf{Alg}_A$, i.e., $C \in C\mathbf{Alg}_A$. We now define $\mathbf{GA}_A$ as the subcategory of those functors $\mathbf{Alg}_A \to \mathbf{Group}$ that are representable by A-algebras $C \in C\mathbf{Alg}_A$ such that $C \in \mathbf{Clg}_A$ as a coalgebra. If k is a field, $\mathbf{GA}_A$ is simply the category of affine group schemes over A.

Let $\mathbf{GA}_A^c$ be the full subcategory of commutative group schemes in $\mathbf{GA}_A$. Then $G \in \mathbf{GA}_A^c$ is representable by an object in $C^c\mathbf{Alg}_A$ which can also be considered as an object of $G^c\mathbf{Clg}_A$. (In the noncommutative case this is not quite true.)

■(37.3.4) We are now going to interpret Cartier duality in the commutative case as a sort of Pontryagin duality. Cartier duality will be a pair of duality functors $D^T: \mathbf{Gf}_A^c \to \mathbf{GA}_A^c$ defined essentially by taking all homomorphism of a given formal group into the multiplicative formal group $\hat{\mathbf{G}}_m$; and D: $\mathbf{GA}_A^c \to \mathbf{Gf}_A^c$, defined by taking all homomorphisms of the given affine group scheme G into the algebraic multiplicative group $\mathbf{G}_m$.

■ (37.3.5) **Base change** Let $U \in G\mathbf{Clg}_A$ and $B \in \mathbf{Alg}_A$, then $U \otimes B = U_B$ is canonically an object in $G\mathbf{Clg}_B$ as follows: If μ, ε, m, e, i are the five structure maps of U, then the five structure maps of U_B are

$$\mu_B\colon U \otimes B \xrightarrow{\mu \otimes 1} U \otimes U \otimes B \simeq (U \otimes B) \otimes_B (U \otimes B)$$

$$\varepsilon_B\colon U \otimes B \xrightarrow{\varepsilon \otimes 1} A \otimes B \simeq B$$

$$m_B\colon (U \otimes B) \otimes_B (U \otimes B) \simeq U \otimes U \otimes B \xrightarrow{m \otimes 1} U \otimes B$$

$$i_B\colon U \otimes B \xrightarrow{i \otimes 1} U \otimes B$$

$$e_B\colon B = A \otimes B \xrightarrow{e \otimes 1} U \otimes B$$

where $\otimes$ stands for $\otimes_A$. It is trivial to check that U_B satisfies the conditions that make it an object of $G\mathbf{Clg}_B$.

■ (37.3.6) **Proposition** $G\mathbf{Clg}_B(B[T, T^{-1}], U_B) \xrightarrow{\sim} \mathbf{AlT}_A(D(U), B)$ functorially for all $B \in \mathbf{AlT}_A^f$.

Here $B[T, T^{-1}]$ has the obvious B-algebra structure (giving us m and e), and the coalgebra structure is given by $\mu\colon T \mapsto T \otimes T$, $\varepsilon\colon T \mapsto 1$, while the inverse morphism is given by $i\colon T \mapsto T^{-1}$. (This determines the coalgebra structure of $B[T, T^{-1}]$ completely because by (37.1.2) μ, ε, and i must be B-algebra morphisms.)

■ (37.3.7) **Start of the proof of Proposition (37.3.6)** A $G\mathbf{Clg}_B$-morphism $B[T, T^{-1}] \to U_B$ is, among other things, a B-algebra homomorphism and as such uniquely determined by the image $x \in U_B$ of $T \in B[T, T^{-1}]$. The conditions that $T \mapsto x$ defines actually a $G\mathbf{Clg}_B$-morphism are then

$$\mu_B(x) = x \otimes x \quad \text{(compatibility with comultiplication)}$$

$$\varepsilon_B(x) = 1 \quad \text{(compatibility with counit)}$$

(37.3.8) x is invertible in the algebra B_U (because T is invertible in $B[T, T^{-1}]$)

$$i_B(x) = x^{-1} \quad \text{(compatibility with inverses)}$$

Of these four conditions the first two imply the others. Indeed, since the diagonal morphism of U_B as an object of $\mathbf{Clg}_B$ is μ_B and the unique morphism into the final object is $\varepsilon_B\colon U_B \to B$, we see from the third diagram of (36.1.2) that $m_B \circ (i_B \otimes 1) \circ \mu = e_B \circ \varepsilon_B$. Applying this to x and using $e_B(1) = 1$ and the first two properties of (37.3.8), we find $i_B(x)x = 1$.

Thus $G\mathbf{Clg}_B(B[T, T^{-1}], U_B)$ is canonically a certain subset of $U_B = U \otimes B$. The next step is to identify $U \otimes B$ with $\mathbf{Mod}\, T_A(D(U), B)$.

■ (37.3.9) **Lemma** $\psi: U \otimes B \xrightarrow{\sim} \mathbf{Mod}\, T_A(D(U), B)$, $u \otimes b \mapsto \phi_{u.b}$, $\phi_{u.b}(t) = t(u)b$ is an isomorphism of B-modules.

Proof Let $\phi \in \mathbf{Mod}\, T_A(D(U), B)$ and let $\{t_i \mid i \in I\}$ be the pseudobasis corresponding to a basis $\{e_i \mid i \in I\}$ of U. Then $\phi(t_i) = 0$ for all $i \in I \backslash \kappa$ for some finite subset κ and the morphism inverse to the one defined in the statement of the lemma assigns $\sum_{i \in \kappa} e_i \otimes \phi(t_i) \in U \otimes B$ to ϕ. (*Remark*: Lemma (37.3.9) is really just $D_B^T(D_B(U_B)) = U_B$, D_B^T: $\mathbf{AlT}_B \to \mathbf{Clg}_B$, D_B: $\mathbf{Clg}_B \to \mathbf{AlT}_B$.)

■ (37.3.10) **Conclusion of the proof of Proposition (37.3.6)** Let $x \in U \otimes B$, then we claim $\psi(x)$ is in $\mathbf{AlT}_A(D(U), B)$ if and only if $\mu_B(x) = x \otimes x$ and $\varepsilon_B(x) = 1$. Indeed, by the definition of the algebra structure on $D(U)$ if $t_1, t_2 \in D(U)$, then $t_1 t_2$: $U \to A$ is the composite

$$U \xrightarrow{\mu} U \otimes U \xrightarrow{t_1 \otimes t_2} A \otimes A \to A$$

Hence $\psi(x)(t_1 t_2) = \psi(x)(t_1)\psi(x)(t_2)$ is equivalent to $\mu_B(x) = x \otimes x$, and similarly $\psi(x)(1) = 1$ is equivalent to $\varepsilon_B(x) = 1$. Q.E.D.

■ (37.3.11) **Proposition** $C^c\mathbf{AlT}_B(B[\![T]\!], R_B) \xrightarrow{\sim} \mathbf{Alg}_A(D^T(R), B)$ for all $R \in C^c\mathbf{AlT}_A$ and $B \in \mathbf{Alg}_A$.

Here $R_B = R \hat{\otimes}_A B$ (discrete topology on B) with its inherited $C^c\mathbf{AlT}_B$-structure; $D^T(R) \in G^c\mathbf{Clg}_A$ is viewed as an object in $C^c\mathbf{Alg}_A$ (cf. (37.2.9)); and $B[\![T]\!]$ has the cogroup structure defined by $\varepsilon(T) = 0$, $\mu(T) = 1 \otimes T + T \otimes 1 + T \otimes T$; $\iota(T)$ is such that $T + \iota(T) + T\iota(T) = 0$. This is the other half of the Pontryagin-duality-like interpretation of Cartier duality which we are discussing and of which (37.3.6) is the first half. There is a slight asymmetry about (37.3.11) compared to (37.3.6) caused by the fact that we want to view $D^T(R)$ as an object representing a functor $\mathbf{Alg}_A \to \mathbf{Group}$ rather than as a functor $\mathbf{Clg}_A \to \mathbf{Group}$. The proof of Proposition (37.3.11) is practically identical with that of (37.3.6) and is omitted. (One starts of course with an isomorphism $R \hat{\otimes} B \simeq \mathbf{Mod}_A(D^T(R), B)$.)

Restricting (37.2.9) to the commutative case, and writing things in terms of formal group schemes and affine group schemes rather than in terms of algebras, we have shown

■ (37.3.12) **Theorem** (Cartier duality) There is a duality D^T: $\mathbf{Gf}_A^c \to \mathbf{GA}_A^c$, D: $\mathbf{GA}_A^c \to \mathbf{Gf}_A^c$ between commutative formal groups and commutative affine group schemes ($DD^T \simeq id$, $D^T D \simeq id$) defined by the functors

$$D^T(F)(B) = \mathbf{Gf}_B(F, \hat{\mathbf{G}}_{m,B}), \qquad B \in \mathbf{Alg}_A$$
$$D(G)(B) = \mathbf{GA}_B(G, \mathbf{G}_{m,B}), \qquad B \in \mathbf{AlT}_A^f$$

■ (37.3.13) In particular if $A = k$, a field, then $\mathbf{GA}_k^c$ is the category of all commutative affine group schemes over k (cf. (37.2.5)) and we find a duality between the category of all formal groups over k and the category of all affine group schemes over k.

37.4 Universal enveloping algebras and covariant bialgebras (over Q)

■ (37.4.1) Let $G(X, Y)$ be a finite dimensional formal group law over A. Let $\mathfrak{g}$ be the Lie algebra of $G(X, Y)$ and let $U\mathfrak{g}$ be the universal enveloping algebra of $\mathfrak{g}$. Let $\{x_1, \ldots, x_n\}$ be a basis for $\mathfrak{g}$ over A. Then we recall (cf. Section (14.3.6) of Chapter II) that $U\mathfrak{g}$ as an A-module is free with basis $\{x^{\mathbf{k}}\}$ where $\mathbf{k}$ runs through all multi-indices $\mathbf{k} = (k_1, \ldots, k_n)$, $k_i \in \mathbf{N} \cup \{0\}$. We also recall that the diagonal map Δ of $U\mathfrak{g}$ is given by

$$\Delta(x^{\mathbf{k}}) = \sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} \binom{\mathbf{k}}{\mathbf{i}} x^{\mathbf{i}} \otimes x^{\mathbf{k}} \tag{37.4.2}$$

and that the multiplication on $U\mathfrak{g}$ satisfies

$$x^{\mathbf{k}}x^{\mathbf{l}} = x^{\mathbf{k}+\mathbf{l}} + \sum_{\mathbf{j}<\mathbf{k}+\mathbf{l}} a_{\mathbf{j}} x^{\mathbf{j}}, \qquad a_{\mathbf{j}} \in A \tag{37.4.3}$$

Now let $U(G)$ be the covariant bialgebra of $G(X, Y)$. As a module over A, $U(G)$ is free with as basis the set of elements $z_{\mathbf{k}}\colon A[\![X_1, \ldots, X_n]\!] \to A$ defined by $z_{\mathbf{k}}(a(X)) =$ coefficient of $X^{\mathbf{k}}$ in $a(X)$ where $\mathbf{k}$ runs through all multi-indices $(k_1, \ldots, k_n)$, $k_i \in \mathbf{N} \cup \{0\}$. Let $\mathbf{e}(i)$ be the multi-index $(0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the ith spot. Then

$$\psi\colon \mathfrak{g} \to U(G), \qquad x_i \mapsto z_{\mathbf{e}(i)} \tag{37.4.4}$$

is a Lie homomorphism according to Lemma (36.2.3). Hence ψ induces a homomorphism of associative algebras

$$\phi\colon U\mathfrak{g} \to U(G) \tag{37.4.5}$$

It is our aim to prove that ϕ is an isomorphism of bialgebras in the case that A is a $\mathbf{Q}$-algebra. (More precisely, we shall show that ϕ is an isomorphism of associative algebras which respects comultiplication and counit; no inverse element morphism has been defined on $U\mathfrak{g}$.)

Let $U^m(G)$ be the submodule of $U(G)$ spanned by the $z_{\mathbf{k}}$ with $|\mathbf{k}| = k_1 + \cdots + k_m \leq m$.

■ (37.4.6) **Lemma** $z_{\mathbf{k}} \cdot z_{\mathbf{l}} \equiv z_{\mathbf{k}+\mathbf{l}} \binom{\mathbf{k}+\mathbf{l}}{\mathbf{k}} \bmod U^{m-1}(G)$ if $m = |\mathbf{k} + \mathbf{l}|$.

Proof By the definition of the multiplication in $U(G)$ we have for $a(X) \in A[\![X_1, \ldots, X_n]\!]$

$$(z_{\mathbf{k}}z_{\mathbf{l}})(a(X)) = \text{coefficient of } X^{\mathbf{k}}Y^{\mathbf{l}} \text{ in } a(G(1)(X, Y), \ldots, G(n)(X, Y))$$

and because $G(i)(X, Y) \equiv X_i + Y_i \bmod(\text{degree } 2)$ for all $i = 1, \ldots, n$ we have

$$\text{coefficient of } X^{\mathbf{k}}Y^{\mathbf{l}} \text{ in } a(G(X, Y)) = \binom{\mathbf{k}+\mathbf{l}}{\mathbf{k}} a_{\mathbf{k}+\mathbf{l}} + P(a_{\mathbf{s}})$$

where $P(a_{\mathbf{s}})$ is a polynomial in coefficients $a_{\mathbf{s}}$ of $a(X)$ with $|\mathbf{s}| < |\mathbf{k} + \mathbf{l}|$. This proves the lemma.

■ (37.4.7) **Theorem** Suppose that A is a $\mathbf{Q}$-algebra. The associative algebra homomorphism of (37.4.5) is then an isomorphism, and ϕ respects the comultiplication and counits of $U\mathfrak{g}$ and $U(G)$.

Proof Let $U^m\mathfrak{g}$ be the submodule of $U\mathfrak{g}$ generated by the $x^{\mathbf{k}}$ with $|\mathbf{k}| \leq m$. We claim that

$$\phi(x^{\mathbf{k}}) \equiv \mathbf{k}!\, z_{\mathbf{k}} \mod U^{m-1}(G) \qquad \text{if} \quad m = |\mathbf{k}| \tag{37.4.8}$$

This is proved by induction, being obviously true for $|\mathbf{k}| \leq 1$ (cf. (37.4.4)). If $|\mathbf{k}| \geq 2$, let $\mathbf{k} = \mathbf{j} + \mathbf{l}$ with $|\mathbf{j}|, |\mathbf{l}| \geq 1$. Then because ϕ is an algebra homomorphism and using induction, we find

$$\phi(x^{\mathbf{l}}) \equiv \mathbf{l}!\, z_{\mathbf{l}} \mod U^{l-1}(G), \qquad l = |\mathbf{l}|$$

$$\phi(x^{\mathbf{j}}) \equiv \mathbf{j}!\, z_{\mathbf{j}} \mod U^{j-1}(G), \qquad j = |\mathbf{j}|$$

$$\phi(x^{\mathbf{l}}x^{\mathbf{j}}) = \phi(x^{\mathbf{l}})\phi(x^{\mathbf{j}})$$

Now $U^s(G)U^t(G) \subset U^{s+t}(G)$ (this follows from Lemma (37.4.6) by induction) and from (37.4.8) for $t < |\mathbf{k}|$ we also see that $\phi(U^t\mathfrak{g}) \subset U^t(G)$. Combining all this with (37.4.3) and Lemma (37.4.6) we find mod $U^{m-1}(G)$

$$\phi(x^{\mathbf{k}}) \equiv \phi(x^{\mathbf{l}}x^{\mathbf{j}}) = \phi(x^{\mathbf{l}})\phi(x^{\mathbf{j}}) \equiv (\mathbf{l}!\, z_{\mathbf{l}})(\mathbf{j}!\, z_{\mathbf{j}}) \equiv \mathbf{l}!\, \mathbf{j}! \binom{\mathbf{l}+\mathbf{j}}{\mathbf{l}} z_{\mathbf{l}+\mathbf{j}}$$

which proves (37.4.8). It follows that ϕ induces isomorphisms $U^m\mathfrak{g}/U^{m-1}\mathfrak{g} \to U^m(G)/U^{m-1}(G)$ for all $m \in \mathbf{N}$ and hence that ϕ is an isomorphism $U\mathfrak{g} \to U(G)$.

It remains to show that ϕ respects comultiplication and counit. To prove this it suffices to prove this on a set of algebra generators of $U\mathfrak{g}$ because the structure morphisms $U\mathfrak{g} \to U\mathfrak{g} \otimes U\mathfrak{g}$, $U\mathfrak{g} \to A$, $U(G) \to U(G) \otimes U(G)$, $U(G) \to A$ are all A-algebra homomorphisms. A set of algebra generators for $U\mathfrak{g}$ is $\{1, x_1, \ldots, x_n\}$ and the result follows. Q.E.D.

■ (37.4.9) **Proposition** *Lie*: $\mathbf{FG}_A(F(X, Y), G(X, Y)) \xrightarrow{\sim} \mathbf{LA}_A(L(F), L(G))$ is a bijection if A is a $\mathbf{Q}$-algebra.

Proof Let $\alpha(X)$: $F(X, Y) \to G(X, Y)$ be a homomorphism of formal group laws. Suppose that $\alpha(X) \neq 0$. We claim that then $J(\alpha) \neq 0$ if A is of characteristic zero. Indeed, we have if $\alpha(X) = (\alpha(1)(X), \ldots, \alpha(m)(X))$,

$$\alpha(i)(F(X, Y)) = G(i)(\alpha(X), \alpha(Y))$$

Differentiating this with respect to Y_k we find

$$\sum_{j=1}^{n} \frac{\partial \alpha(i)}{\partial X_j}(F(X, Y)) \cdot \frac{\partial F(j)}{\partial Y_k}(X, Y) = \sum_{s=1}^{m} \frac{\partial G(i)}{\partial Y_s}(\alpha(X), \alpha(Y)) \cdot \frac{\partial \alpha(s)}{\partial Y_k}(Y) \tag{37.4.10}$$

Let $(d\alpha/dX)(X)$ be the $m \times n$ matrix $((\partial\alpha(i)/\partial X_j)(X))_{i,j}$, and $(\partial F/\partial Y)(X, Y)$ the $n \times n$ matrix $((\partial F(i)/\partial Y_j)(X, Y))_{i,j}$, and $(\partial G/\partial Y)(X, Y)$ the $m \times m$ matrix $((\partial G(i)/\partial Y_j)(X, Y)_{i,j}$. Then the equations (37.4.10) for all i simultaneously can be written as a matrix equation

$$\frac{d\alpha}{dX}(F(X, Y)) \cdot \frac{\partial F}{\partial Y}(X, Y) = \frac{\partial G}{\partial Y}(\alpha(X), \alpha(Y)) \cdot \frac{d\alpha}{dX}(Y)$$

Substituting $Y = 0$ and using $F(X, 0) = X$, $(d\alpha/dX)(0) = J(\alpha)$, $\alpha(0) = 0$, we find

$$\frac{d\alpha}{dX}(X) \cdot \frac{\partial F}{\partial Y}(X, 0) = \frac{\partial G}{\partial Y}(\alpha(X), 0) \cdot J(\alpha)$$

Now $F(i)(X, Y) = X_i + Y_i + \sum a_{\mathbf{k},\mathbf{l}} X^{\mathbf{k}} Y^{\mathbf{l}}$ where the sum is over all $\mathbf{k}$, $\mathbf{l}$ with $|\mathbf{k}| \geq 1$, $|\mathbf{l}| \geq 1$ (because $F(i)(X, 0) = X_i$ and $F(i)(0, Y) = Y_i$). It follows that $(\partial F/\partial Y)(0, 0) = I_n$ the $n \times n$ unit matrix. It follows that $(\partial F/\partial Y)(X, 0)$ is an invertible matrix. So if $J(\alpha) = 0$, then $(d\alpha/dX)(X) = 0$; and since $\alpha(0) = 0$ and A is of characteristic zero, this can happen only if $\alpha(X) = 0$.

This proves the injectivity of Lie. (*Remark:* the one dimensional version of the argument above has been used before in Section 18.3 of Chapter IV.) As to the surjectivity of Lie, let ϕ: $L(F) \to L(G)$ be a homomorphism of Lie algebras. Then ϕ induces a homomorphism of associative algebras with comultiplication and counit $U\phi$: $UL(F) \to UL(G)$. Using the isomorphisms $UL(F) \xrightarrow{\sim} U(F)$, $UL(G) \xrightarrow{\sim} U(G)$, we find a comultiplication and counit preserving homomorphism of associative algebras $\tilde{U}\phi$: $U(F) \to U(G)$. Applying D, this gives a comultiplication and counit preserving $D(\tilde{U}\phi)$: $R(G) \to R(F)$. Let $\alpha(i)(X) = D(\tilde{U}\phi)(X_i)$, then $\alpha(X)$ is a homomorphism of formal group laws $F(X, Y) \to G(X, Y)$ and tracing all the steps one easily checks that $L(\alpha) = \phi$.

■ (37.4.11) **Second proof of the formal version of Lie's third theorem** To conclude this section let us show how to use Theorem (37.4.7) to obtain a proof of the formal version of Lie's third theorem (which we also proved via the Campbell–Hausdorff formula in Section 14.5 of Chapter II). Let $\mathfrak{g} \in \mathbf{LA}_A$ and let $U\mathfrak{g}$ be the universal enveloping algebra of $\mathfrak{g}$. Then $U\mathfrak{g}$ is an associative algebra with a cocommutative comultiplication and a counit (or augmentation). Define $R\mathfrak{g} = \mathbf{Mod}_A(U\mathfrak{g}, A)$. Then $R\mathfrak{g}$ is a commutative algebra over A with a (not necessarily commutative) comultiplication and counit. We claim that $R\mathfrak{g}$ as an algebra over A is isomorphic to $A[\![X_1, \ldots, X_n]\!]$ where $n = \dim \mathfrak{g}$ if A is a $\mathbf{Q}$-algebra.

This is proved as follows. Define (using the Poincaré–Birkhoff–Witt theorem)

$$\psi\colon A[\![X_1, \ldots, X_n]\!] \to R\mathfrak{g} = \mathbf{Mod}_A(U\mathfrak{g}, A)$$

$$X^{\mathbf{k}} \mapsto y_{\mathbf{k}} k!, \quad \text{where} \quad y_{\mathbf{k}}(\textstyle\sum a_{\mathbf{l}} x^{\mathbf{l}}) = a_{\mathbf{k}}$$

Now the comultiplication on Ug is given by (cf. (37.3.2))

$$x^{\mathbf{k}} \mapsto \sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} \binom{\mathbf{k}}{\mathbf{i}} x^{\mathbf{i}} \otimes x^{\mathbf{j}}$$

and it follows that the multiplication on Rg is $\mathbf{y}_{\mathbf{i}}\mathbf{y}_{\mathbf{j}} = \binom{\mathbf{i}+\mathbf{j}}{\mathbf{i}} y_{\mathbf{i}+\mathbf{j}}$. Hence ψ is an A-algebra isomorphism. The comultiplication on Rg now defines a comultiplication on $A[\![X]\!]$, and this gives us the desired formal group law with Lie algebra g.

37.5 The covariant bialgebra of the Witt vectors

■ (37.5.1) Let $\hat{W}(X, Y)$ be the formal group law of the Witt vectors over $\mathbf{Z}$. That is, $\hat{W}(i)(X, Y) = \Sigma_i(X_1, \ldots, X_i; Y_1, \ldots, Y_i)$ where Σ_i is the ith Witt vector addition polynomial. The first thing we want to do is to calculate the dual (in the sense of Cartier duality) of the formal group $\hat{W}$. Now according to Section 37.2

$$D^T(\hat{W})(B) = \mathbf{Gf}_B(\hat{W}_B, \hat{\mathbf{G}}_{m,B})$$

But according to the representation theorem (Chapter V, Theorem (27.1.14)) we know that $\mathbf{Gf}_B(\hat{W}, \hat{\mathbf{G}}_m) \simeq \mathbf{FG}_B(\hat{W}(X, Y), \hat{\mathbf{G}}_m(X, Y)) = \mathscr{C}(\hat{\mathbf{G}}_m; B)$. And according to Chapter III, (17.2.11) we know that $\mathscr{C}(\hat{\mathbf{G}}_m; B) \simeq W^+(B)$, the underlying additive group of the ring of Witt vectors with coordinates in B. All these isomorphisms being functorial, we conclude that the commutative affine group scheme dual to $\hat{W}$ is $W^+ = D^T(\hat{W})$, and then of course the duality theorem (37.3.12) says that $D(W^+) = \hat{W}$. This can also be seen fairly directly.

■ (37.5.2) Let $\hat{W}(-)$: **Ring** $\to$ **Ab** be the abelian-group-valued subfunctor of W^+: **Ring** $\to$ **Ab** defined by

$$\hat{W}(B) = \{(b_1, b_2, \ldots) \in W(B) \mid b_i \text{ nilpotent for all } i \text{ and } b_i = 0 \text{ for almost all } i\}$$

Let $\Lambda(B)$ be the abelian group of power series in $1 + tB[\![t]\!]$ and let $\bar{E}$: $W(-) \to \Lambda(-)$ be the functorial isomorphism of Chapter III, (17.2.7) and (17.2.9) $(b_1, b_2, \ldots) \mapsto \prod_{i=1}^{\infty} (1 - b_i t^i)$. Let $\hat{\Lambda}(-)$ be the subfunctor of $\Lambda(-)$ corresponding to $\hat{W}(-)$ under $\bar{E}$. That is, $\hat{\Lambda}(B)$ consists of all polynomials of the form $1 + a_1 t + \cdots + a_n t^n$ with all the a_i nilpotent elements of B.

We now define a pairing

$$\langle\ ,\ \rangle\colon \hat{W}(B) \times W^+(B) \to \hat{\mathbf{G}}_m(B) \tag{37.5.3}$$

for all $B \in$ **Ring** as follows. Let $a = (a_1, a_2, \ldots) \in \hat{W}(B)$ and $b = (b_1, b_2, \ldots) \in W^+(B)$. Then $a \cdot b$, where the dot denotes multiplication in the ring of Witt vectors $W(B)$, is in $\hat{W}(B)$. It follows that $\bar{E}(a, b)$ is in $\hat{\Lambda}(B)$, so that upon substituting $t = 1$ we obtain a well-defined element of $\mathbf{G}_m(B)$ of the form $1 + z$ where z is nilpotent in B. So, writing $\bar{E}(a; t)$ instead of $\bar{E}(a)$ for notational convenience, the formula for the pairing $\langle\ ,\ \rangle$ is

$$\langle a, b \rangle = \bar{E}(a \cdot b; 1) \tag{37.5.4}$$

One obviously has the relations

$$\langle a + a', b\rangle = \langle a, b\rangle\langle a', b\rangle, \qquad \langle a, b + b'\rangle = \langle a, b\rangle\langle a, b'\rangle$$
$$\langle a, 0\rangle = 1, \qquad \langle 0, b\rangle = 1$$

so that the pairing $\langle\ ,\ \rangle$ is bilinear. Now let $a \in \hat{W}(B)$, then a defines a homomorphism of functors ϕ_a: $W_B^+ \to \mathbf{G}_{m,B}$ by the formula $\phi_a(c) = \langle a, c\rangle$ for all $c \in W_B^+(C) = W^+(C)$, $C \in \mathbf{Alg}_B$.

■ (37.5.5) **Theorem** ϕ: $\hat{W}(B) \to \mathbf{Alg}_B\mathbf{Ab}(W_B^+, \mathbf{G}_{m,B})$, $\phi_a(c) = \langle a, c\rangle$ is a functorial isomorphism of abelian groups. Here $\mathbf{Alg}_B\mathbf{Ab}$ is the category of functors $\mathbf{Alg}_B \to \mathbf{Ab}$.

■ (37.5.6) **Proof of Theorem (37.5.5)** Using the functorial isomorphism $\bar{E}$ between W_B^+ and Λ_B and $\hat{W}$ and $\hat{\Lambda}$, we can replace W by Λ everywhere in the statement of the theorem. The inverse ψ of the map ϕ in the theorem is now obtained as follows.

Let u: $\Lambda_B \to \mathbf{G}_{m,B}$ be a functor morphism. Consider the algebra $B[s]$ and the element $1 - st \in \Lambda_B(B[s])$. Applying u, we find an element in $\mathbf{G}_m(B[s])$, i.e., we find a polynomial $h(s) = b_0 + b_1 s + \cdots + b_m s^m$ which is invertible in $B[s]$. It follows that b_0 is a unit of B and that the b_i for $i = 1, \ldots, m$ are nilpotent in B. Now u is a functor morphism; so in particular if ε: $B[s] \to B$ is the B-algebra homomorphism $s \mapsto 0$, we must have $u_B \circ \Lambda(\varepsilon) = \mathbf{G}_m(\varepsilon) \circ u_{B[s]}$; and since $u_B(1) = 1$ (u_B being a group homomorphism), we see that $b_0 = 1$. Thus $h(t) = 1 + b_1 t + \cdots + b_m t^m$ is an element of $\hat{\Lambda}(B)$. This defines an inverse map ψ: $\mathbf{Alg}_B\mathbf{Ab}(\Lambda_B, \mathbf{G}_{m,B}) \to \hat{\Lambda}(B)$.

Let us check that $\psi \circ \phi = id$. So, let $a(t) \in \hat{\Lambda}(B)$; then we must show that the result of substituting $t = 1$ in the product $(1 - st) \cdot a(t)$ is $a(s)$ (where now the dot denotes multiplication in $\Lambda(B)$).

Now quite generally we have in $W(C)$ for any ring C

$$(s, 0, 0, \ldots)(b_1, b_2, \ldots) = (b_1 s, b_2 s^2, \ldots)$$

simply because $w_n(b_1 s, b_2 s^2, b_3 s^3, \ldots) = s^n w_n(b_1, b_2, b_3, \ldots)$. For $\Lambda(C)$, this translates as $(1 - st)a(t) = a(st)$.

So, since substituting $t = 1$ in $a(st) \in \hat{\Lambda}(B[s])$ makes sense and gives of course $a(s)$, we have shown that $\psi \circ \phi = id$.

Now let us prove that the element $h(s)$ associated to u above determines u uniquely.

Let $C = B[x_1, x_2, \ldots]$ and let $x(t)$ be the element $1 + x_1 t + x_2 t^2 + \cdots$ of $\Lambda(C)$. Suppose that $u_C(x(t)) = \Phi(x_1, x_2, \ldots) \in \mathbf{G}_m(C) = B[x_1, x_2, \ldots]^*$. Then the polynomial $\Phi(x_1, x_2, \ldots)$ determines u completely (Yoneda lemma; or: let D be any algebra, $1 + y_1 t + y_2 t^2 + \cdots$ any element of $\Lambda(D)$; define r: $C \to D$ by $r(x_i) = y_i$; then because by functoriality $u_D \circ \Lambda(r) = \mathbf{G}_m(r) \circ u_C$ we find that $u_D(y(t)) = \Phi(y_1, y_2, \ldots)$).

The polynomial $\Phi(x_1, x_2, \ldots)$, being a polynomial, involves only finitely many of the x_i, say, $x_1, \ldots, x_m$.

Now let $C' \supset C$ be a B-algebra over which we can write

$$1 + x_1 t + x_2 t^2 + \cdots + x_m t^m = \prod_{i=1}^{m} (1 - z_i t)$$

By functoriality of u we must have $u_{C'}(1 - z_i t) = h(z_i)$ and because $u_{C'}$ is a group homomorphism, we find $u_{C'}(1 + x_1 t + \cdots + x_m t^m) = \prod h(z_i)$; and $\mathbf{G}_m(C) \to \mathbf{G}_m(C')$ being injective, it follows that h determines u uniquely. This proves that ψ is injective. Since $\psi \circ \phi = id$, ψ is also surjective and hence a bijection. It is easy to check that ϕ is a homomorphism of abelian groups and that ϕ is functorial. This proves the theorem.

■ (37.5.7) We can also use the pairing $\langle\ ,\ \rangle$ to define a χ: $W^+(B) \to \mathbf{Alg}_B\mathbf{Ab}(W_B, \mathbf{G}_{m,B})$ by the formula $\chi_b(c) = \langle c, b \rangle$, and arguing almost exactly as in (37.4.6) one finds that

■ (37.5.8) **Theorem** χ: $W^+(B) \to \mathbf{Alg}_B\mathbf{Ab}(\hat{W}_B, \mathbf{G}_{m,B})$ is a functorial isomorphism of abelian groups.

■ (37.5.9) **Endomorphisms of W^+** The Cartier duality between $\hat{W}$ and W^+ permits us to calculate the ring of endomorphisms of the group-valued functor W^+ over A because we know the ring of endomorphisms of $\hat{W}$ over A. This is the ring $\mathrm{Cart}(A)$ by (27.2.12).

First, we have the endomorphisms $\langle a \rangle$ of $W^+(-)$ defined on $\Lambda(-)$ by $\gamma(t) \to \gamma(at)$ and then transported via $\bar{E}$. We also have the Frobenius endomorphisms $\mathbf{f}_n$ and Verschiebungmorphisms $\mathbf{V}_n$ for all $n \in \mathbf{N}$; cf. Section 17.3 of Chapter III. Using the duality $\hat{W} \to W^+$, one now readily finds that every endomorphism of the group-valued functor W^+ can be uniquely written in the form

$$\sum_{m,n} \mathbf{V}_m \langle a_{m,n} \rangle \mathbf{f}_n$$

where for every m there are only finitely many n such that $a_{m,n} \neq 0$. To see this one uses $\mathbf{V}_n(a \cdot \mathbf{f}_n b) = (\mathbf{V}_n a)b$ and $\bar{E}(\mathbf{V}_n a)(1) = \bar{E}(a)(1)$ for all $a \in \hat{W}(-)$ to establish

$$\langle \mathbf{V}_n, b \rangle = \langle a, \mathbf{f}_n b \rangle, \quad \langle \mathbf{f}_n a, b \rangle = \langle a, \mathbf{V}_n b \rangle$$

where on both sides of the pairing $\mathbf{V}_n$ and $\mathbf{f}_n$ denote endomorphisms of $W(-)$, which, as it happens, also induce endomorphisms of the subfunctor $\hat{W}(-)$. Now combine this with the remark that the endomorphism $\hat{W}(-)$ obtained by restriction of $\mathbf{f}_n$: $W(-) \to W(-)$ is precisely the endomorphism $\mathbf{V}_n$ of $\hat{W}(X, Y)$ induced by the operator $\mathbf{V}_n$ on curves and vice versa; cf. (27.2.12) of Chapter V.

■ (37.5.10) **Proposition** $\mathbf{Alg}_B\mathbf{Ab}(W_B^+, \mathbf{G}_{a,B})$ is the B-module of all polynomials in one variable T over B with zero constant term.

Before proving this result let us notice that it is something quite reasonable to expect. Indeed, we know that $\mathbf{Gf}_B(\hat{W}_B, \hat{\mathbf{G}}_a) \simeq \mathscr{C}(\hat{\mathbf{G}}_a; B)$ (by the representation theorem (Chapter V, Theorem (27.1.14)) and $\mathscr{C}(\hat{\mathbf{G}}_a; B)$ is the additive B-module of power series in one variable without constant term.

■ (37.5.11) **Proof of Proposition (37.5.10)** Using $\bar{E}$: $W_B^+ \simeq \Lambda_B$ again it is equivalent to prove that $\mathbf{Alg}_B\mathbf{Ab}(\Lambda_B, \mathbf{G}_{a.B}) \simeq tB[t]$ as a B-module. Now we already have a largish number of elements of $\mathbf{Alg}_B\mathbf{Ab}(\Lambda_B, \mathbf{G}_{a.B})$, viz. the functorial homomorphisms s_n: $\Lambda(C) \to C$ which correspond to the w_n: $W(C) \to C$ under $\bar{E}$ (cf. Chapter III, (17.2.6)). Recall that

$$\sum_{n=1}^{\infty} s_n(a(t))t^n = -t\frac{a'(t)}{a(t)} = -t\frac{d}{dt}\log(a(t)) \tag{37.5.12}$$

Now let u: $\Lambda_B \to \mathbf{G}_{a.B}$ be a functor morphism. Take again $1 - st \in \Lambda(B[s])$ and let

$$\vartheta(s) = u_{B[s]}(1 - st) \in B[s]$$

Let ε: $B[s] \to B$, $s \mapsto 0$. Because u_B is a group homomorphism, we must have $u_B(1) = 0$ and $\mathbf{G}_a(\varepsilon) \circ u_{B[s]} = u_B \circ \Lambda(\varepsilon)$ then gives that $\vartheta(0) = 0$. So let

$$\vartheta(s) = b_1 s + \cdots + b_n s^n$$

We claim that then $u = b_1 s_1 + \cdots + b_n s_n$ where the s_i are the functor morphisms defined by (37.5.12). The argument is exceedingly similar to that of (37.5.6). Let C, C', $x_1, x_2, \ldots, z_1, \ldots, z_m$ be as in (37.5.6). Again u is given by some polynomial $\Psi(x_1, \ldots, x_m)$, involving only finitely many x_i. This time the functoriality and additivity of u then give that

$$u_C(1 + x_1 t + x_2 t^2 + \cdots + x_m t^m) = \sum_{i=1}^{m} \vartheta(z_i)$$

where

$$(1 + x_1 t + \cdots + x_m t^m) = \prod_{i=1}^{m} (1 - z_i t)$$

showing that $\vartheta(s)$ determines u uniquely. On the other hand, we have

$$-t\frac{d}{dt}\log\left(\prod_{i=1}^{m}(1 - z_i t)\right) = \sum_{i=1}^{m}\sum_{r=1}^{\infty} z_i^r t^r$$

so that $s_r(1 + x_1 t + \cdots + x_m t^m) = \sum_{i=1}^{m} z_i^r$. This proves that $u = b_1 s_1 + \cdots + b_n s_n$, and hence proves the proposition.

■ (37.5.13) **Lie algebra of $F(X, Y)$ and primitive elements of $U(F)$** Let $F(X, Y)$ be a formal group law over A. Let $R(F)$ be its contravariant bialgebra. Now define the Lie algebra of $F(X, Y)$ as all A-linear morphisms $\mathfrak{m}(F)/\mathfrak{m}^2(F) \to A$ where $\mathfrak{m}(F)$ is the maximal ideal of $R(F)$. Then since $R(F) \simeq A[\![X_i \mid i \in I]\!]$, we see that as an A-module $L(F)$ is free of rank $\#I$ (where $\#I$

denotes the cardinality of I). Now $R(F) \simeq A \oplus \mathfrak{m}(F)$ as an A-module. So if $g \in L(F)$, we can see g as an A-linear map $R(F) \to A$, which because $g(\mathfrak{m}^2(F)) = 0$, is also continuous; i.e., g is an element of $U(F)$.

The Lie algebra structure of $L(F)$ is now given by $[g_1, g_2] = g_1 g_2 - g_2 g_1$ (where one uses the multiplication of $U(F)$ induced by the comultiplication of $R(F)$).

To check that this makes sense first the following. We claim that g: $R(F) = A \oplus \mathfrak{m}(F) \to A$ is zero on $\mathfrak{m}^2(F)$ and A if and only if g is a primitive element of $U(F)$, i.e., iff $\mu(g) = 1 \otimes g + g \otimes 1$. This is quite easy to check. Let $a(X \otimes 1, 1 \otimes X) \in R(F) \hat{\otimes} R(F)$,

$$\begin{aligned} a &= a(X \otimes 1; 1 \otimes X) \\ &= a_0 + \sum b_i(X_i \otimes 1) + \sum c_i(1 \otimes X_i) \\ &\quad + \sum_{|k|,|l| \geq 1} a_{k,l}(X \otimes 1)^k (1 \otimes X)^l \end{aligned}$$

Then

$$\mu(g)(a) = g(a_0) + g(\sum (b_i + c_i)X_i) + g\left(\sum_{|n| \geq 2} \sum_{l+k=n} a_{k,l} X^n\right)$$

and

$$(1 \otimes g + g \otimes 1)(a) = 2g(a_0) + g(\sum b_i X_i) + g(\sum c_i X_i)$$

and the claim follows.

Now let $g_1, g_2 \in L(F) \subset U(F)$. Then $\mu([g_1, g_2]) = \mu(g_1 g_2 - g_2 g_1) = \mu(g_1)\mu(g_2) - \mu(g_2)\mu(g_1) = (g_1 g_2 - g_2 g_1) \otimes 1 + 1 \otimes (g_1 g_2 - g_2 g_1)$. So that also $[g_1, g_2] \in L(F)$. It is now quite easy to check that the Lie algebra structure defined in Section 14.1 of Chapter II agrees with the Lie algebra structure just defined. (Identify the ith basis vector e_i of $L(F)$ in Section 14.1 with the linear map g_i: $\mathfrak{m}(F)/\mathfrak{m}^2(F) \to A$ given by $g_i(X_i) = 1$, $g_i(X_j) = 0$ if $i \neq j$.)

■ (37.5.14) The structure of the covariant bialgebra $\mathrm{U}^c = U(\hat{W})$ of the Witt vectors is very closely related to the duality results we have been discussing above. (The reason for the superscript c in U^c will become clearer in the next section; it stands for "commutative.")

■ (37.5.15) **Theorem** Let $\mathrm{U}^c = U(\hat{W})$ be the covariant bialgebra of the formal group $\hat{W}$. Then U^c is a polynomial algebra $\mathrm{U}^c = \mathbf{Z}[Z_1, Z_2, \ldots]$ in countably many indeterminates $Z_1, Z_2, \ldots$. The coalgebra structure of U^c is given by $Z_n \mapsto \sum_{i=0}^n Z_i \otimes Z_{n-i}$, where $Z_0 = 1$. The Lie algebra of $\hat{W}$ as a submodule of U^c has as a basis the elements $r_1, r_2, \ldots$ defined as follows: $r_n(Z) = R_n(Z_1, \ldots, Z_n)$ where R_n is defined by

$$R_n(\sigma_1, \ldots, \sigma_n) = X_1^n + \cdots + X_n^n$$

$$1 + \sigma_1(X)t + \cdots + \sigma_n(X)t^n = \prod_{j=1}^n (1 + X_j t)$$

(That is, the R_n are the polynomials in Z that express the power sums $\sum X_i^n$ as a polynomial in the elementary symmetric functions.)

Proof According to 37.2 $\mathbf{U}^c$ represents the affine commutative group scheme $D^T(\hat{W}) \simeq W^+ \simeq \Lambda$ (by (37.5.5)). Now $\Lambda(B) = \{1 + b_1 t + b_2 t^2 + \cdots \mid b_i \in B\}$, which is clearly represented by $\mathbf{Z}[Z_1, Z_2, \ldots]$ (with $\phi \in \mathbf{Ring}(\mathbf{Z}[Z], B)$ corresponding to $1 + \phi(Z_1)t + \phi(Z_2)t^2 + \cdots \in \Lambda(B)$). The addition in $\Lambda(B)$ is multiplication of power series, so that the corresponding comultiplication in $\mathbf{Z}[Z]$ is given by $Z_n \mapsto \sum_{i=0}^{n} Z_i \otimes Z_{n-i}$.

The Lie algebra of $\hat{W}$ is the Lie algebra of primitive elements of $\mathbf{U}^c$ and these, we claim, correspond precisely to the functor homomorphisms $\Lambda \to \mathbf{G}_a$. Indeed, such a functor homomorphism is given by an algebra homomorphism between the representing rings; this map respects the cogroup structures on these rings. The rings with comultiplication in question are $\mathbf{Z}[Z_1, Z_2, \ldots]$, $Z_n \mapsto \sum Z_i \otimes Z_{n-i}$; $\mathbf{Z}[X]$, $X \mapsto X \otimes 1 + 1 \otimes X$. A comultiplication preserving ring homomorphism $\mathbf{Z}[X] \to \mathbf{Z}[Z_1, Z_2, \ldots]$ thus is uniquely determined by the image of X, which must be a primitive element of $\mathbf{U}^c$. But, according to Proposition (37.5.10) (or rather the proof (37.5.11)) $\mathbf{Alg}_{\mathbf{Z}}\mathbf{Ab}(\Lambda, \mathbf{G}_a)$ is the free $\mathbf{Z}$-module spanned by the elements s_n defined by (37.5.12). Let $z(t) = 1 + Z_1 t + Z_2 t^2 + \cdots = \prod_{i=1}^{\infty} (1 + \xi_i t)$. Then

$$\sum_{n=1}^{\infty} (s_n z(t)) t^n = -t \frac{z'(t)}{z(t)} = \sum_{n=1}^{\infty} \sum_{i=1}^{\infty} (\xi_i^n t^n (-1)^{n-1})$$

$$= \sum_{n=1}^{\infty} (-1)^{n-1} r_n(Z) t^n$$

and the element of $\mathbf{U}^c$ corresponding to s_n: $\Lambda \to \mathbf{G}_a$ is therefore $(-1)^{n-1} r_n(Z)$ (where the $r_n(Z)$ are as described in the statement of the theorem). Q.E.D.

38 Curves in Noncommutative Formal Groups

38.1 Curves and the noncommutative analogue of the representation theorem

■ (38.1.1) **Some notational conventions** Let F: $\mathbf{AlT}_A^f \to \mathbf{Group}$ be a formal group over a ring A. Let $R(F)$ be the contravariant bialgebra and $U(F)$ the covariant bialgebra of F. We shall use barred symbols to denote the structure morphisms of $R(F)$, i.e., $\bar{m}_F$, $\bar{e}_F$, $\bar{\imath}_F$, $\bar{\mu}_F$, $\bar{\varepsilon}_F$ denote multiplication, unit, coinverse, comultiplication, and counit, respectively; and we shall use unbarred symbols m_F, e_F, i_F, ε_F, μ_F to denote the structure maps of $U(F)$. Often we shall omit the index F.

■ (38.1.2) **Definitions and generalities on the theme: curves** Let F be a not necessarily commutative formal group over a ring A. Let $R(F)$ be the

contravariant bialgebra of F and let $U(F)$ be the covariant bialgebra of F. A curve in F over A is now defined as a continuous homomorphism of algebras ϕ: $R(F) \to A[\![t]\!]$ (i.e., a morphism in $\mathbf{AlT}_A$) such that $\varepsilon_0 \phi = \bar{\varepsilon}_F$ where ε_0: $A[\![t]\!] \to A$ is the A-algebra morphism defined by $t \mapsto 0$ and $\bar{\varepsilon}_F$: $R(F) \to A$ is the counit of $R(F)$.

The cogroup structure on $R(F)$ turns the set of curves into a group, which we shall denote $\mathscr{C}(F; A)$ as usual.

We shall write

$$\phi = \sum_{i=1}^{\infty} \phi_i t^i, \qquad \phi_i \in \mathbf{Mod}T_A(R(F), A) = U(F) \tag{38.1.3}$$

Then the fact that ϕ: $R(F) \to A[\![t]\!]$ is an algebra homomorphism translates into the statement that the elements $\phi_1, \phi_2, \ldots \in U(F)$ must satisfy the condition

$$\mu_F(\phi_n) = \sum_{i=0}^{n} \phi_i \otimes \phi_{n-i}, \qquad \phi_0 = 1 \tag{38.1.4}$$

One way to see this is as follows. Dualizing ϕ one obtains a morphism in $\mathbf{Clg}_A$ $D^T(\phi)$: $\bigoplus_{i=0}^{\infty} At_i \to U(F)$ where $\bigoplus At_i$ has the coalgebra structure $t_n \mapsto \sum t_i \otimes t_{n-i}$, $t_0 = 1$. Then $\phi_i = D^T(\phi)(t_i)$, and (38.1.4) follows.

If F is a smooth formal group, then $R(F) \simeq A[\![X_i \mid i \in I]\!]$ as an object in $\mathbf{AlT}_A$ and a morphism ϕ: $R(F) \to A[\![t]\!]$ in $\mathbf{AlT}_A$ is uniquely determined by giving the I-tuple of power series $\phi(X_i) \in A[\![t]\!]$, $i \in I$; so for the case of formal group laws, we recover the original definition of curve.

Let $\phi(t) = \sum_{i=0}^{\infty} \phi_i t^i$ and $\psi(t) = \sum_{i=0}^{\infty} \psi_i t^i$ be two curves in $\mathscr{C}(F; A)$. Then, using the algebra structure of $U(F)$, we define the product of $\phi(t)$ and $\psi(t)$ as

$$\phi(t)\psi(t) = \sum_{n=0}^{\infty} \left(\sum_{r=0}^{n} \phi_r \psi_{n-r} \right) t^n$$

We claim that if F is the formal group of a formal group law $F(X, Y)$, then this agrees with the original addition of curves. Suppose that $R(F) = A[\![X_i \mid i \in I]\!]$. Let us write $\phi(t)(X)$ for the I-tuple of power series $(\sum \phi_n(X_i)t^n)_{i \in I}$. Then we must show that

$$\phi(t)\psi(t)(X) = F(\phi(t)(X), \psi(t)(X))$$

and this is an immediate consequence of the fact that the multiplication in $U(F)$ is defined by the comultiplication $R(F) \to R(F) \hat{\otimes} R(F)$, $X_i \mapsto F(i)(X \otimes 1, 1 \otimes X)$.

■ (38.1.5) **Curves of order n** Let F be a formal group law over A, then a *curve of order n* over A is defined as an $\mathbf{AlT}_A$-morphism $\phi_{(n)}$: $R(F) \to A[\![t]\!]/(t^{n+1})$ such that $\varepsilon_0 \phi_{(n)} = \bar{\varepsilon}_F$.

If F is smooth, then since $R(F)$ is a power series algebra in that case, every curve of order n can be extended to a curve of order ∞. In general, e.g., when F

is a finite group scheme, this is of course not the case. For example, if $R(F) = k[X]/(X^p)$, $X \mapsto 1 \otimes X + X \otimes 1$, where k is a field of characteristic $p > 0$, then there are curves of order n for all $n < \infty$, but $\mathscr{C}(F; k) = \{0\}$.

We shall use $\mathrm{Lie}_n(F; A)$ to denote the group of curves of order n of F over A. Taking $n = \infty$, we thus have so to speak $\mathrm{Lie}_\infty(F; A) = \mathscr{C}(F; A)$, and at the other extreme $\mathrm{Lie}_1(F; A)$ is the underlying additive group of the Lie algebra of F (cf. (37.5.13)).

■ (38.1.6) **The bialgebras U and U(n)** Let $\mathbf{U} = \mathbf{Z}\langle Z_1, Z_2, Z_3, \ldots\rangle$ be the ring of noncommuting polynomials in determinates $Z_1, Z_2, \ldots$ with coefficients in $\mathbf{Z}$. That is, $\mathbf{U}$ is the free associative algebra over $\mathbf{Z}$ on the set $\{Z_1, Z_2, \ldots\}$ (cf. Chapter II, Section (14.4.5)). We give $\mathbf{U}$ a comultiplication by defining $Z_n \mapsto \sum_{i=0}^{n} Z_i \otimes Z_{n-i}$ (where $Z_0 = 1$), a counit $Z_i \mapsto 0$. It is not difficult to check that there is then a unique inverse $i: \mathbf{U} \to \mathbf{U}$ making $\mathbf{U}$ into an object of $G\mathbf{Clg}_A$ because the inverse is necessarily a coalgebra morphism by (37.1.8).

Similarly, we define $\mathbf{U}(n) = \mathbf{Z}\langle Z_1, Z_2, \ldots, Z_n\rangle$, a subobject (in $G\mathbf{Clg}_A$) of $\mathbf{U}$.

■ (38.1.7) **Proposition** $\mathbf{U}$ represents the functor $\mathscr{C}(-; A)$, and $\mathbf{U}(n)$ represents the functor $\mathrm{Lie}_n(-; A)$.

By this we mean the following $\mathscr{C}(F; A) \simeq G\mathbf{Clg}_A(\mathbf{U}, U(F))$ functorially for all $F \in \mathbf{Gf}_A$, and $\mathrm{Lie}_n(F; A) \simeq G\mathbf{Clg}_A(U(n), U(F))$ functorially.

■ (38.1.8) **Proof of (38.1.7)** Let $\phi(t) = \sum \phi_i t^i$ be a curve. Then since $\mathbf{U}$ is the free associative algebra on $Z_1, Z_2, \ldots$, there is a unique algebra homomorphism $\alpha: \mathbf{U} \to U(F)$ such that $\alpha(Z_i) = \phi_i$, and α respects the comultiplication and counit because of (38.1.4). Conversely, if $\alpha: \mathbf{U} \to U(F)$ is a $G\mathbf{Clg}_A$-morphism, then $\phi_\alpha(t) = \sum \phi(Z_i)t^i$ is a curve in F. The argument for $\mathbf{U}(n)$ is analogous.

■ (38.1.9) If F is commutative, then so is $U(F)$, and we have

$$G\mathbf{Clg}_A(\mathbf{U}, U(F)) = G^c\mathbf{Clg}_A(\mathbf{U}^c, U(F))$$
$$= C^c\mathbf{AlT}_A(R(F), R(\hat{W}) = \mathbf{Gf}_A(\hat{W}, F)$$

So, in a way, Proposition (38.1.7) is the analogue of the representation theorem (Cartier's first theorem) which says that curves in a formal group law $F(X, Y)$ correspond biuniquely to formal group law homomorphisms $\hat{W}(X, Y) \to F(X, Y)$. Now, as we have seen, (38.1.7) is a triviality, while the representation theorem definitely was not. The reason for the difference is of course that $U(\hat{W}) = \mathbf{U}^c$ represents a nontrivial calculation. Here the problem is the opposite: what is the dual bialgebra $D(\mathbf{U})$? A first result in this direction is

■ (38.1.10) **Theorem** $D(\mathbf{U})$ is a power series ring over $\mathbf{Z}$; i.e., $D(\mathbf{U})$ represents a smooth formal group.

We shall not proof this theorem here. The proof is long and combinatorially intricate; cf. [374].

38.2 Divided power sequences and the Campbell–Hausdorff theorem

■ (38.2.1) **Divided power sequences in coalgebras** Let C be a coalgebra over A. A divided power sequence over $\phi_0 \in C$ is a sequence $\phi_0, \phi_1, \phi_2, \ldots$ of elements of C such that

$$\mu(\phi_n) = \sum_{i=0}^{n} \phi_i \otimes \phi_{n-i}$$

The element ϕ_0 is called the grouplike element of the sequence.

If $C = U(F)$, the covariant bialgebra of a formal group F and $\phi(t) = \sum \phi_i t^i$ is a curve in F, then by Section 38.1 $\phi_0 = 1, \phi_1, \phi_2, \ldots$ is a divided power sequence over 1. In this case ϕ_1 is primitive, and one often speaks of a divided power sequence $\phi_1, \phi_2, \ldots$ over the primitive ϕ_1.

If U is any bialgebra over A, then the set of divided power sequences over 1 is a group under the multiplication

$$(1, \phi_1, \phi_2, \ldots)(1, \psi_1, \psi_2, \ldots) = (1, \chi_1, \chi_2, \ldots)$$

where $\chi_n = \sum_{i=0}^{n} \phi_i \psi_{n-i}$ with $\phi_0 = \psi_0 = 1$. We shall write $\mathscr{C}(U; A)$ for this group. (The A refers to the fact that the ϕ_i must be A-linear.) Thus if $U = U(F)$, we have $\mathscr{C}(F; A) = \mathscr{C}(U; A)$ by (38.1.2).

■ (38.2.2) **Warning** There is a second, different, notion in algebra that also goes by the name "divided powers." An ideal I in a ring B is said to admit a divided power structure if there exists a sequence of maps $\gamma_n: I \to A$, $n \in \mathbf{N} \cup \{0\}$ such that $\gamma_0(x) = 1$ for all $x \in I$, $\gamma_1(x) = x$ for all $x \in I$, and

$$\gamma_n(x + y) = \sum \gamma_i(x)\gamma_{n-i}(y)$$

$$\gamma_n(ax) = a^n \gamma_n(x)$$

$$\gamma_n(x)\gamma_m(x) = \binom{n+m}{n} \gamma_{n+m}(x)$$

$$\gamma_n(\gamma_m(x)) = (nm)!(n!)(m!)^n \gamma_{nm}(x)$$

If A is a $\mathbf{Q}$-algebra, then one shows that necessarily $\gamma_n(x) = (n!)^{-1}x^n$. This notion of divided powers plays a big role in crystalline cohomology (cf., e.g., [34]). Both this notion and the one defined in (38.2.1) are in a way generalizations of $(n!)^{-1}x^n$, whence the name divided powers; cf. (38.2.10).

■ (38.2.3) **Divided power sequences in bialgebras** Now let U be the covariant bialgebra of a formal group F over A, and let $R(F)$ be the contravariant bialgebra of F. Let $1 = \phi_0, \phi_1, \phi_2, \ldots$ be a divided power sequence over $1 \in U(F)$. The elements ϕ_i define A-linear endomorphisms $\bar{\phi}_i$ of $U(F)$ by

$\bar{\phi}_i(u) = u\phi_i$ and by duality these give continuous A-linear maps ∂_i: $R(F) \to R(F)$. Claim:

$$(38.2.4) \quad \partial_n(xy) = \sum_{i=0}^{n} \partial_i(x)\partial_{n-i}(y) \qquad \text{for all} \quad x, y \in R(F), \quad n \in \mathbf{N} \cup \{0\}$$

This follows (via duality) immediately from (38.2.1). Another way to obtain ∂_i from ϕ_i is as follows: ∂_i is the composed map

$$(38.2.5) \qquad R(F) \xrightarrow{\bar{\mu}} R(F) \hat{\otimes} R(F) \xrightarrow{1 \otimes \phi_i} R(F) \hat{\otimes} A \xrightarrow{\sim} R(F)$$

Then if $u \in U(F) = \mathbf{Mod}T_A(R(F), A)$, we have indeed $D^T(\partial_i)u = u \circ \partial_i = u\phi_i = \bar{\phi}_i(u)$ by the definition of multiplication in $U(F)$.

Just what A-linear endomorphisms of $R(F)$ arise via (38.2.5)? The answer is easy and is given by the following definition and lemma:

■ (38.2.6) **Definition** A continuous A-module endomorphism ∂: $R(F) \to R(F)$ is called left invariant if the following diagram is commutative:

$$\begin{array}{ccc} R(F) & \xrightarrow{\bar{\mu}} & R(F) \hat{\otimes} R(F) \\ \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle 1 \hat{\otimes} \partial} \\ R(F) & \xrightarrow{\bar{\mu}} & R(F) \hat{\otimes} R(F) \end{array}$$

■ (38.2.7) **Lemma** Define ρ: $U(F) = \mathbf{Mod}T_A(R(F), A) \to \mathbf{Mod}T_A(R(F), R(F))$ by $\rho(u) = (1 \otimes u) \circ \bar{\mu}$ (identifying $R(F) \hat{\otimes} A \simeq R(F)$; cf. (38.2.5)) and σ: $\mathbf{Mod}T_A(R(F), R(F) \to \mathbf{Mod}T_A(R(F), A) = U(F)$ by $\sigma(\partial) = \varepsilon_F \circ \partial$. Then $\sigma \circ \rho = id$, ρ is an injective homomorphism of A-algebras (where $\mathbf{Mod}T_A(R(F), R(F))$ is an algebra under composition and $U(F)$ is an A-algebra via m and e), and the image of ρ consists precisely of the left invariant endomorphisms of $R(F)$.

Proof Exercise (easy).

■ (38.2.8) **The group of divided power sequences of an algebra** Let R be any algebra over A. Then we define a divided power sequence over A as a series of A-module endomorphisms $\partial_0 = id, \partial_1, \partial_2, \ldots$ such that (38.2.4) holds. We write formally $\partial(t) = \sum \partial_i t^i$; sequences of divided powers can then be multiplied by the rule

$$\gamma(t)\partial(t) = \sum_{i=0}^{\infty} \left(\sum_{n=0}^{i} \gamma_i \partial_{n-i} \right) t^n$$

Exercise: check that $\gamma(t)\partial(t)$ is again a divided power sequence.

We use $H_A(R)$ to denote the group of divided power sequences of the algebra R.

Now suppose that R is the contravariant bialgebra of a formal group over A.

Then the map ρ of Lemma (38.2.7) gives as an injective homomorphism

$$\rho: \mathscr{C}(F; A) \to H(R(F)) \tag{38.2.9}$$

Note that if $\phi(t) = \sum_{i=0}^{\infty} \phi_i t^i$, $\psi(t) = \sum_{i=0}^{\infty} \psi_i t^i$, $\phi_i, \psi_i \in U(F)$, then the product of $\phi(t)$ and $\psi(t)$ is

$$\phi(t)\psi(t) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \phi_i \psi_{n-i} \right) t^n$$

and in case F is the formal group of a formal group law $F(X, Y)$ this of course coincides with the original "addition" of curves; cf. (38.1.2).

■ (38.2.10) **Example** Let R be a $\mathbf{Q}$-algebra and let ∂ be a derivation over $\mathbf{Q}$ of R (i.e., $\partial(xy) = \partial x \otimes 1 + 1 \otimes \partial y$). Then $\sum_{n=0}^{\infty} (n!)^{-1} \partial^n t^n = \exp(\partial t)$ is a divided power sequence of R. (This explains the name "divided power sequence.") We use $\mathrm{Der}_{\mathbf{Q}}(R)$ to denote the module of derivations of R over $\mathbf{Q}$.

■ (38.2.11) **Proposition** Let R be an A-algebra where A is a $\mathbf{Q}$-algebra and let $\phi_0 = id, \phi_1, \phi_2, \ldots$ be a series of A-module endomorphisms of R. Then the following are equivalent:

(i) $\phi(t) = \sum_{n=0}^{\infty} \phi_n t^n$ is in $H_A(R)$, i.e., a divided power sequence.
(ii) $\phi(t) = \prod_{n=0}^{\infty} \exp(\partial_i t^i)$ (ordered product) with $\partial_i \in \mathrm{Der}_A(R)$.
(iii) $\phi(t) = \exp(\sum_{n=0}^{\infty} \partial_i t^i)$ with $\partial_i \in \mathrm{Der}_A(R)$.

(Of course (ii) and (iii) are different iff the Lie algebra $\mathrm{Der}_A(R)$ is nonabelian.)

Proof The proof of Proposition (38.2.11) is not difficult. The essential observations being first that sequences of the form (ii) and (iii) certainly define elements of $H_A(R)$ and secondly that if $\phi(t) = \sum \phi_n t^n$ and $\psi(t) = \sum \psi_n t^n$ are both in $H_A(R)$ and $\phi_i = \psi_i$ for $i < m$ ($m \in \mathbf{N}$), then $\phi_m - \psi_m \in \mathrm{Der}_A(R)$.

■ (38.2.12) **On the Campbell–Hausdorff theorem** Let R be a $\mathbf{Q}$-algebra and let $\partial_1, \partial_2 \in \mathrm{Der}_{\mathbf{Q}}(R)$. Then $\exp(\partial_1 t), \exp(\partial_2 t) \in H(R)$; since $H(R)$ is a group, we see from Proposition (38.2.11) that there are elements $\gamma_1, \gamma_2, \ldots \in \mathrm{Der}_{\mathbf{Q}}(R)$ such that

$$\exp(\partial_1 t) \exp(\partial_2 t) = \exp\left(\sum_{n=1}^{\infty} \gamma_n t^n \right) \tag{38.2.13}$$

Now let $\mathfrak{g}$ be a Lie algebra over A that is free as an A-module where A is a $\mathbf{Q}$-algebra. Let $U\mathfrak{g}$ be the enveloping algebra of $\mathfrak{g}$ and $R\mathfrak{g}$ the dual algebra of $U\mathfrak{g}$. Then the left invariant derivations of R over A correspond (cf. Lemma (38.2.7)) precisely to the primitive element of $U\mathfrak{g}$; because A is of characteristic zero, these are in turn precisely the elements of $\mathfrak{g} \subset U\mathfrak{g}$. Since (with a slight abuse of notation) $\mathscr{C}(U\mathfrak{g}; A)$ is a subgroup of $H(R\mathfrak{g})$, we know that if ∂_1, ∂_2 are both left invariant then so are the γ_n; hence (38.2.13) gives us precisely the Campbell–Hausdorff theorem (14.4.14) of Chapter II.

■ (38.2.14) **Semiderivations** Let k be a field of characteristic p, and let $R = k[\![X_1, \ldots, X_n]\!]$ be a power series algebra over k. Let $\partial_0 = id, \partial_1, \partial_2, \ldots$ be a divided power sequence of continuous k-module endomorphisms of R. Then we claim for all $x \in R$, $n \in \mathbf{N}$,

$$\partial_n(x^p) = \begin{cases} 0 & \text{if } (p, n) = 1 \\ \partial_{n/p}(x)^p & \text{if } p \mid n \end{cases} \tag{38.2.15}$$

To see this write

$$\partial_n(x^p) = \sum_{i_1 + \cdots + i_p = n} \partial_{i_1}(x) \cdots \partial_{i_p}(x) \tag{38.2.16}$$

where the sum is over all sequences $(i_1, \ldots, i_p)$ such that $i_1 + \cdots + i_p = n$, $i_j \in \mathbf{N} \cup \{0\}$. Now because p is prime, we have that the p-sequences $(i_1, \ldots, i_p)$, $(i_2, \ldots, i_p, i_1), \ldots, (i_p, i_1, i_2, \ldots, i_{p-1})$ are all different unless $i_1 = \cdots = i_p = n/p$. Using (38.2.16), (38.2.15) now follows immediately. It also follows that $\partial_i(a) = 0$ for all $i \in \mathbf{N}$, $a \in k$.

Now let $n = p^r$, and suppose that $x \in k[\![X_i^{p^r} | i \in I]\!]$ and $y \in R$. Then by (38.2.5), linearity, and continuity we have for all $r \in \mathbf{N} \cup \{0\}$

$$\partial_{p^r}(xy) = \partial_{p^r}(x)y + x\partial_{p^r}(y)$$

so that the ∂_{p^r} are semiderivations in the sense of Dieudonné [99].

38.3 Verschiebung, Homothety, and Frobenius operators

■ (38.3.1) **$\mathbf{V}_n$ and $\langle a \rangle$ operators** Let F be a formal group over A. Let $\phi(t) = \sum_{i=0}^{\infty} \phi_i t^i$, $\phi_i \in U(F)$ be a curve in F over A. One then defines for all $n \in \mathbf{N}$ and $a \in A$

(38.3.2)

$$\mathbf{V}_n\phi(t) = \sum_{i=0}^{\infty} \phi_i t^{ni} = \phi(t^n) \qquad \text{and} \qquad \langle a \rangle \phi(t) = \sum_{i=0}^{\infty} \phi_i a^i t^i = \phi(at)$$

It is easy to check that $\mathbf{V}_n\phi(t)$ and $\langle a \rangle \phi(t)$ are again curves. One has of course $\mathbf{V}_n\langle a \rangle = \langle a^n \rangle \mathbf{V}_n$ for all $a \in A$, $n \in \mathbf{N}$.

■ (38.3.3) **Logarithms and logarithms** Let $F(X, Y)$ be a commutative formal group law over A characteristic zero ring A. In this type of situation we have in previous chapters often made use of the additive subgroup $f\mathscr{C}(F; A)$ of the additive group of power series $\{\sum_{n=1}^{\infty} a_n t^n \mid a_n \in A \otimes \mathbf{Q}\}$ where the a_n are I-vectors if $F(X, Y)$ is a formal group law with index set I. What replaces this trick if one views curves as elements of $U(F)[\![t]\!]$ rather than as I-tuples of power series in t? The answer is given by the diagram below (NB $F(X, Y)$ is a *commutative* formal group law):

(38.3.4)

$$\begin{array}{ccc} \mathscr{C}(F; A) & \longrightarrow & \mathscr{C}(U(F); A) \\ \downarrow f & & \downarrow \log \\ t(A \otimes \mathbf{Q}[\![t]\!])^I & \longrightarrow & t(U(F) \otimes \mathbf{Q}[\![t]\!]) \end{array}$$

Here the upper horizontal arrow assigns to the I-tuple of power series $\gamma(t) = (\gamma(i)(t))_{i \in I}$ the algebra homomorphism $R(F) \to A[\![t]\!]$, $X_i \mapsto \gamma(i)(t)$; log is the map that takes $\phi(t) = 1 + \phi_1 t + \phi_2 t^2 + \cdots$ into

$$\log(\phi(t)) = \sum_{n=1}^{\infty} (-1)^{n-1}(\phi_1 t + \phi_2 t^2 + \cdots)^n n^{-1}$$

$tA \otimes \mathbf{Q}[\![t]\!]^I$ is the additive group of I-tuples of power series in t with zero constant terms, $tU(F) \otimes \mathbf{Q}[\![t]\!]$ is the additive group of power series in t with coefficients in $U(F) \otimes \mathbf{Q}$ and zero constant term; $f(X)$ is the logarithm of $F(X, Y)$ and the lower horizontal arrow takes the I-tuple $(a(i)(t))_{i \in I}$ into ψ: $R(F) \otimes \mathbf{Q} \to A \otimes \mathbf{Q}[\![t]\!]$ defined by $\phi(X_i) = a(i)(t)$.

■ (38.3.5) **Lemma** Let $F(X, Y)$ be a commutative formal group law over a characteristic zero ring A. The diagram (38.3.4) is commutative, the two horizontal arrows are isomorphisms of topological groups, and f and log are injective.

Proof Check the definitions and cf. also (38.1.2).

■ (38.3.6) **Remark** Let $F(X, Y)$ be as above in Lemma (38.3.5) and let $\phi(t) \in \mathscr{C}(U(F); A)$. Let $\log(\phi(t)) = \sum_{i=1}^{\infty} \psi_i t^i$. Then $\psi_i \in P(U(F) \otimes \mathbf{Q})$, the Lie algebra of primitive elements of the coalgebra $U(F) \otimes \mathbf{Q}$ over $A \otimes \mathbf{Q}$. And in fact if $\phi(t) \in 1 + tU(F)[\![t]\!]$ then $\phi(t) \in \mathscr{C}(U(F); A)$ iff $\log(\phi(t)) = \sum_{i=1}^{\infty} \psi_i t^i$ with $\psi_i \in P(U(F) \otimes \mathbf{Q})$. Indeed, if we define $\phi(t)(x)$ as $\sum_{i=0}^{\infty} \phi_i(x) t^i$ for all $x \in R(F)$, then $\phi(t) \in \mathscr{C}(U(F); A)$ iff $\phi(t)(xy) = \phi(t)(x)\phi(t)(y)$ for all $x \in R(F)$. So $\phi(t) \in \mathscr{C}(U(F); A)$ iff $\log \phi(t)(x) + \log \phi(t)(y) = \log \phi(t)(xy)$, which is the case iff $\psi_i(xy) = \psi_i(x) + \psi_i(y)$ for all $x, y \in R(F)$, which in turn means that $\psi_i \in P(U(F) \otimes \mathbf{Q})$.

■ (38.3.7) **The Frobenius operators $\mathbf{f}_n$** Now let F be any commutative formal group and $U(F)$ its covariant bialgebra. Let $\phi(t) \in \mathscr{C}(U(F); A)$. We write

$$\phi(t) = 1 + \phi_1 t + \phi_2 t^2 + \cdots = \prod_{i=1}^{\infty} (1 + u_i t^i), \qquad u_i \in U(F)$$

Applying log we see that

$$\log \phi(t) = \sum_{i=1}^{\infty} \sum_{n=1}^{\infty} (-1)^n n^{-1} (u_i t^i)^n = \sum_{n=1}^{\infty} n^{-1} \lambda_n t^n$$

where the λ_n are certain polynomials with coefficients from $\mathbf{Z}$ in the u_i; so $\lambda_n \in U(F)$ and hence $\lambda_n \in P(U(F))$ by Remark (38.3.6) above. One now defines the Frobenius operators $\mathbf{f}_m$ for all $m \in \mathbf{N}$ by the formula

$$\mathbf{f}_m \phi(t) = \exp\left(\sum_{n=1}^{\infty} n^{-1} \lambda_{mn} t^n \right)$$

■ (38.3.8) **Lemma** If $\phi(t) \in \mathscr{C}(U(F); A)$, then $\mathbf{f}_m \phi(t)$ is in $\mathscr{C}(U(F); A)$ (and not just in $\mathscr{C}(U(F) \otimes \mathbf{Q}; A \otimes \mathbf{Q})$).

Proof Diagram (38.3.4) and Lemma (38.3.5) show that the definition of $\mathbf{f}_m$ given in (38.3.7) agrees with the one we used before for curves in formal group laws. Hence $\mathbf{f}_m \phi(t) \in \mathscr{C}(U(F); A)$ if $\phi(t) \in \mathscr{C}(U(F); A)$ and F comes from a formal group law $F(X, Y)$ over A. This implies in particular that $\mathbf{f}_m \xi(t) \in \mathscr{C}(U(\hat{W}); A)$ where $\xi(t)$ is the "canonical curve" $\xi(t) = 1 + Z_1 t + Z_2 t^2 + \cdots \in 1 + tU(\hat{W})[\![t]\!]$. Now the definition of $\mathbf{f}_m$ is obviously functorial, and every curve $\phi(t) \in \mathscr{C}(U(F); A)$ can be obtained via a suitable Hopf algebra map $U(\hat{W}) \to U(F)$ which takes Z_i into ϕ_i (Proposition (38.1.7)). This proves the lemma.

■ (38.3.9) One has of course the usual relations between the $\mathbf{V}_n$, $\langle a \rangle$, $\mathbf{f}_n$ operators, e.g., $\langle a \rangle \mathbf{f}_n = \mathbf{f}_n \langle a^n \rangle$ and $\mathbf{f}_n \mathbf{V}_n = n$, simply because these relations hold for the universal example $\mathscr{C}(U(\hat{W}); A)$ since $U(\hat{W})$ is the bialgebra of a commutative formal group *law*.

38.4 V-basis and decomposition

In this final subsection we briefly discuss two more results that generalize to the case of noncommutative formal groups. They are the existence of a V-basis and the decomposition of an arbitrary curve into a sum of shifted p-typical ones when we are working our $\mathbf{Z}_{(p)}$-algebra. (Both almost trivial in the commutative case.)

■ (38.4.1) **Lemma** Let F be a smooth formal group over A with covariant bialgebra $U(F)$. Suppose that $P(U(F))$ is a free A-module and let $(u_i)_{i \in I}$ be a basis for $P(U(F))$. Choose a total order on I. For each $i \in I$, choose a curve $\psi_{(i)}(t) \in \mathscr{C}(U(F); A)$ such that $\psi_{(i)}(t) \in 1 + u_i t \bmod(\text{degree } 2)$ (such curves exist because F is supposed to be smooth). Then every curve $\phi(t) \in \mathscr{C}(F; A) = \mathscr{C}(U(F); A)$ can be written uniquely as an ordered product

$$\phi(t) = \prod_{n=1}^{\infty} \prod_{i \in I} \mathbf{V}_n \langle a_{n,i} \rangle \psi_{(i)}(t)$$

where for every $n \in \mathbf{N}$ there are only finitely many $i \in I$ such that $a_{n,i} \neq 0$.

Proof Successive approximation.

■ (38.4.2) Let $\mathbf{U}_{(p)} = \mathbf{U} \otimes \mathbf{Z}_{(p)}$ with the obvious Hopf algebra structure. Let $\xi(t) = 1 + Z_1 t + Z_2 t^2 + Z_3 t^2 + \cdots$ be the standard curve of $\mathbf{U}_{(p)}$. Now let $\eta(t)$ be any curve in $\mathbf{U}_{(p)}$. Then the representation theorem (38.1.7) says that there is a unique homomorphism $\alpha_\eta \colon \mathbf{U}_{(p)} \to \mathbf{U}_{(p)}$ which takes $\xi(t)$ to $\eta(t)$. We now define

$$\operatorname{Im} \eta(t) = \operatorname{Im} \alpha_\eta$$

(This is a sub-Hopf algebra of $\mathbf{U}_{(p)}$.)

The operators $\mathbf{V}_n$, $\langle a \rangle$ applied to $\xi(t)$ define curves in $\mathbf{U}_{(p)}$, which in turn,

define morphisms of Hopf algebras $\mathbf{U}_{(p)} \to \mathbf{U}_{(p)}$ which we shall denote $\mathbf{v}_n$ and λ_a. Of course these generalities also hold for $\mathbf{U}$ itself.

■ (38.4.3) **Pure curves and E-pure sequences** A curve $E(t) \in \mathscr{C}(\mathbf{U}_{(p)}; \mathbf{Z}_{(p)})$ is said to be p-pure if the following hold:

(i) $E(t)$ is isobaric; i.e., if $E(t) = 1 + E_1 t + E_2 t^2 + \cdots$, then $E_i \in \mathbf{U}_{(p)} = \mathbf{Z}_{(p)}\langle Z_1, Z_2, \ldots\rangle$ is homogeneous of weight i (where Z_n has weight n).

(ii) The image of $E(t)$ is the subalgebra of $\mathbf{U}_{(p)}$ generated by the E_1, E_p, E_{p^2}, ...

(iii) $E_1 = Z_1$.

Let us write $Y_i = E_{p^i}$, $i = 0, 1, 2, \ldots$. Then condition (ii) says that $E(t)$ can be written as

$$E(t) = 1 + \sum_{n=1}^{\infty} E_n(Y)t^n$$

where the $E_n(Y)$ are certain polynomials in the Y_i.

Now let F be any formal group over a $\mathbf{Z}_{(p)}$-algebra A. A sequence $u = (u_0, u_1, u_2, \ldots)$ of elements of $U(F)$ is called an E-pure sequence if

$$E_u(t) = 1 + \sum_{n=1}^{\infty} E_n(u)t^n$$

is a curve in $U(F)$.

■ (38.4.4) **Remarks** The curves that thus arise are the noncommutative analogues of the p-typical curves in the commutative case. In that case the analogue of E is the curve in $\mathbf{U}^c_{(p)} = U(\hat{W})_{(p)}$ corresponding to $\varepsilon_p \gamma_w(t) \in \mathscr{C}_p(\hat{W}; \mathbf{Z}_{(p)})$, the p-typified version of the universal curve $\gamma_w(t) = (t, 0, 0, \ldots)$. A main difference between the noncommutative case and the commutative case is that E is far less canonical than $\varepsilon_p \gamma_w(t)$ (cf., however, (38.4.5)).

Let $\mathbf{U}_E = \operatorname{Im} E(t) = \mathbf{Z}_{(p)}\langle Y_0, Y_1, \ldots\rangle$ with $\mu Y_n = \sum_{i+j=p^n} E_i(Y) \otimes E_j(Y)$ (cf. (38.4.3)). Then $G\mathbf{Clg}_A(\mathbf{U}_E, U(F))$ corresponds bijectively to the set of E-typical sequences in $U(F)$. Thus $\mathbf{U}_E$ could be a noncommutative analogue of $\hat{W}_{p^\infty}$ (or more precisely $U(\hat{W}_{p^\infty}) \otimes \mathbf{Z}_{(p)}$).

■ (38.4.5) **Decomposition theorem**

(a) There exists a p-pure curve $E(t) \in \mathscr{C}(\mathbf{U}_{(p)}; \mathbf{Z}_{(p)})$. The image of $E(t)$ is unique up to isomorphism (but $E(t)$ itself not).

(b) Given $E(t)$, there exist for every (n, m), $n \in \mathbf{N} \cup \{0\}$, $(m, p) = 1$, unique homogeneous elements $Y_{n,m} \in \mathbf{U}_{(p)}$ of weight $p^n m$ such that the following conditions hold:

(i) $Y_{n,m} \equiv Z_{p^n m} \bmod(Z_1, \ldots, Z_{p^n m - 1})$;

(ii) for each $m \in \mathbf{N}$, $(m, p) = 1$, the sequence $y(m) = (Y_{0,m}, Y_{1,m}, \ldots)$ is E-pure;

(iii) $\xi(t) = \prod_{(m,p)=1} \mathbf{V}_m E_{y(m)}(t)$ (ordered product);

(iv) $\mathbf{v}_p^i Y_{n,m} = Y_{n-i,m}$ for all $i \le n$ (and $= 0$ if $i > n$).

For a proof, see [123, Théorème 6.4].

■ (38.4.6) Let $F \in \mathbf{Gf}_A$ where A is a $\mathbf{Z}_{(p)}$-algebra. Let $\eta(t) = (\eta_0(t), \eta_1(t), \ldots)$ be a sequence of elements of $tU(F)[\![t]\!]$ such that $\lim_{i\to\infty} \eta_i(t) = 0$ in the t-adic topology on $U(F)[\![t]\!]$. Let $E(t) \in \mathscr{C}(\mathbf{U}_{(p)}; \mathbf{Z}_{(p)})$ be a pure curve. Then

$$E_\eta(t) = 1 + \sum_{n=1}^{\infty} E_n(\eta(t))$$

(substitute $\eta_i(t)$ for Y_i in $E_n(Y)$ and sum over all n) is well defined and is an element of $1 + tU(F)[\![t]\!]$. One now has

■ (38.4.7) **Theorem** Let $\xi(t)$ be a pure curve in $\mathscr{C}(U_{(p)}; \mathbf{Z}_{(p)})$, then there exists a unique sequence $\eta(t) = (\eta_0(t), \eta_1(t), \ldots)$ of elements of $t\mathbf{U}_{(p)}[\![t]\!]$ such that $\lim_{i\to\infty} \eta_i(t) = 0$ such that

$$\xi(t) = E_\eta(t)$$

For a proof, see [123, Théorème 6.9]. This result is of Campbell–Hausdorff type (cf. also (38.2.12)) and thus gives something like a Campbell–Hausdorff formula over $\mathbf{Z}_{(p)}$-algebras. See also [106, Sections 18–21].

E.6 Bibliographical and Other Notes

■ (E.6.1) **General remarks and apology** In Chapter VII we tried to give something like an introduction to the theory of formal groups (formal group laws) from the bialgebra point of view as a sort of antithesis and supplement to the six earlier chapters. There is, in my opinion, no question about it that both the power series approach and the bialgebra approach contribute essentially to our understanding of formal group laws, and it would be a mistake, I think, to neglect either one. Since this book is mainly about the formal power series side of things and as we have already seen how formal group laws occur in nature, let us now mention that, e.g., the bialgebra of the Witt vectors $\mathbf{U}^c$ occurs in nature as $H^*(BU; \mathbf{Z})$ (cf. [194, 195, 296]; cf. also (E.6.3) for some more remarks on $\mathbf{U}^c$).

Of course in this fairly short chapter we could not really do justice to the bialgebra side of things. For more we refer the reader first to Dieudonné's long and impressive series of papers [102–109] and the closely related papers [100, 101, 110, 111, 113]. For background and the role of "semiderivatives" in this, cf. [99]. A most useful exposé of the foundations of the theory is [357]. In Dieudonné's book [114] many, but not nearly all, of these results are expounded in a systematic way.

For the foundations of the general theory of formal group schemes, cf. Gabriel [145].

As to that theory *in statu nascendi*: the use of curves in bialgebras the reader is referred to Ditters' treatment [123] of which [124] is a sort of resumé version; cf. also [118, 307]. For the use of curves in the bialgebras that naturally occur in algebraic topology, cf., e.g., [369–373].

■ (E.6.2) **Notes on Section 37** The terminology re bialgebras and Hopf algebras is not totally fixed; different authors use the same words for (slightly) different concepts.

We have followed Sweedler [401], which shows in Proposition (37.1.8) and its proof which are proposition (4.0.1) (and proof) of [401]. A lot of material on Hopf algebras (especially on the kinds that occur in topology) can be found in the fundamental paper of Milnor and Moore [295]; cf. also [196, 356, 354].

Cartier duality is (of course) due to Cartier. The first statement of Theorem (37.3.12) (over fields) can be found in [63]. The fact that the formal group $\hat{W}$ is dual to the algebraic group W^+ is also due to Cartier [64] and so is the calculation of the covariant bialgebra $U(\hat{W}) = \mathbf{U}^c$ [64]. For the case of $\hat{W}_{p^\infty}$, $U(\hat{W}_{p^\infty})$ (over a field) was determined by Dieudonné; cf. [110]. The proofs of Theorems (37.5.5), (37.5.8) given above follow some lecture notes of Cartier [70] as does the proof of the "additive duality" result (37.5.9).

For an exposé of global (not necessarily affine) Cartier duality in the algebra-coalgebra version, cf. [145].

■ (E.6.3) **Notes on the Hopf algebras $\mathbf{U}^c$, $\mathbf{U}$** The module $\oplus\, \mathbf{Z}Z_i$ with the comultiplication $Z_n \mapsto \sum_{i+j=n} Z_i \otimes Z_j$, $Z_0 = 1$, is a coalgebra and $\mathbf{U}$ (resp. $\mathbf{U}^c$) can be seen as the universal enveloping Hopf algebra (resp. universal commutative enveloping Hopf algebra) of this coalgebra. This type of construction was first done by Moore [299]; cf. also [195]. As a result, $\mathbf{U}$ and $\mathbf{U}^c$ enjoy a number of universality properties (cf. [299]) also for dual statements since the graded dual of $\oplus\, \mathbf{Z}Z_i$ is the polynomial algebra in one variable $Z[t]$.

The dual of $\mathbf{U}^c$ is the contravariant bialgebra $R(\hat{W})$ of the formal group of the Witt vectors. Now $\mathbf{U}^c$ carries a natural grading, and one finds that the graded dual of $\mathbf{U}^c$ is $\mathbf{U}^c$ itself. This duality occurs naturally in topology as the duality $H^*(BU; \mathbf{Z}) \simeq H_*(BU; \mathbf{Z})$.

The universality properties of $\mathbf{U}^c$ are not exhausted by what has been said above. For example, $\mathbf{U}^c$ also has a natural λ-ring structure (induced, from the topological point of view, by exterior products of vector bundles), and it is in fact the universal λ-ring on one generator (cf. [224]). As such, it is isomorphic to the representation ring $R(S_\infty) = \oplus\, R(S_n)$ (with outer product), where $R(S_n)$ is the representation ring of complex representations of S_n, the symmetric group on n letters. See [14] and [224], and for a Hopf algebraic proof [491], which also contains a new proof of the "autoduality" of $\mathbf{U}^c$.

For a freeness property of $\hat{W}$ resulting from the representation theorem, cf. (E.4.2).

■ (E.6.4) **Note on divided power algebras, free coalgebras, and additive formal groups** Let M be a module over a ring A. The algebra of divided powers $\Gamma(M)$ (in the sense of (38.1.2)!) over M is now constructed as follows. It is generated by elements $m^{(r)}$, $m \in M$, $r \in \mathbf{N} \cup \{0\}$, subject to the relations $(m_1 + m_2)^{(r)} = \sum_{i+j=r} m_1^{(i)} m_2^{(j)}$, $(am)^{(r)} = a^r m(r)$, $m^{(0)} = 1$, $m^{(r)} m^{(s)} = \binom{r+s}{s} m^{(r+s)}$. Now let $T^n M = M \otimes M \otimes \cdots \otimes M$ (n factors), and let the symmetric group on n letters act on $T^n M$ by permutation of the factors. Let $\bar{S}^n M$ be the module of invariants. The isomorphism $T^{n+m} M \simeq T^n M \otimes T^m M$ induces an injection $\bar{S}^{n+m} M \hookrightarrow \bar{S}^n M \otimes \bar{S}^m M$. Taking direct sums, we find the so-called free commutative coalgebra on M (cf. [195]). There is also a natural product on $\bar{S}M$ which is defined as follows. Let $x \in \bar{S}^n M$, $y \in \bar{S}^m M$, then $x \cdot y = \sum \sigma(x \otimes y)$ where σ runs through a set of representatives in S_{n+m} of the quotient set $S_{n+m}/S_n \times S_m$. It now turns out that the algebras $\Gamma(M)$ and $\bar{S}M$ are naturally isomorphic if M is free as an A-module. Thus $\Gamma(M)$ and $\bar{S}M$ are (covariant) bialgebras. The corresponding formal group over A is the additive formal group over A with Lie algebra M (cf. [357], exposé

3). If M is free of rank 1 over $\mathbf{Z}$, then the free (commutative) coalgebra over M is $\oplus\ \mathbf{Z}Z_i$ (cf. (E.6.3)). The multiplication defined above is $Z_i Z_j = Z_{i+j}\binom{i+j}{j}$. The dual of this is indeed $Z[\![X]\!]$ with the comultiplication $X \mapsto 1 \otimes X + X \otimes 1$.

The algebra $\Gamma(M)$ has a natural divided power structure (in the sense of (38.1.2)) on its augmentation ideal and the functor $M \mapsto \Gamma(M)$ has certain obvious functorial and universality properties; cf. [344].

■ (E.6.5) **Notes on Section 38** Theorems (38.4.5), (38.4.7), and Proposition (38.2.11) are due to Ditters; cf. [118] and [123]. A proof of theorem (38.1.11) (smoothness of $D(\mathbf{U})$) can be found in [374]; for the case where one works over a field, cf. also [106, Théorème 1]. The proof of (38.1.11) in [118] is probably not (quite) complete; cf. [123, p. 29]. For a Campbell–Hausdorff formula over $\mathbf{F}_p$, cf. also [106].

APPENDIX A

ON POWER SERIES RINGS

A.1 Power Series Rings

■ (A.1.1) **Multi-indices** Let κ be an index set, finite or infinite. A *multi-index* indexed by κ is a function $\mathbf{n}: \kappa \to \mathbf{N} \cup \{0\}$ such that $\mathbf{n}(i) \neq 0$ for only finitely many $i \in \kappa$ (i.e., $\mathbf{n}$ has finite support). Given multi-indices $\mathbf{n}, \mathbf{k}$, we define

$$|\mathbf{n}| = \sum_{i \in \kappa} \mathbf{n}(i) \tag{A.1.2}$$

$$\mathbf{n} \leq \mathbf{k} \quad \Leftrightarrow \quad \mathbf{n}(i) \leq \mathbf{k}(i) \qquad \text{for all} \quad i \in \kappa \tag{A.1.3}$$

$$\mathbf{n} + \mathbf{k} = \mathbf{l} \quad \Leftrightarrow \quad \mathbf{l}(i) = \mathbf{n}(i) + \mathbf{k}(i) \qquad \text{for all} \quad i \in \kappa \tag{A.1.4}$$

$$\mathbf{n} < \mathbf{k} \quad \Leftrightarrow \quad \mathbf{n} \leq \mathbf{k} \text{ and } |\mathbf{n}| < |\mathbf{k}| \tag{A.1.5}$$

We write $\mathbf{0}$ for the multi-index $\mathbf{0}(i) = 0$ for all $i \in \kappa$. Then $\mathbf{n} > \mathbf{k}$ iff $\mathbf{n} = \mathbf{k} + \mathbf{l}$ for some multi-index $\mathbf{l} \neq \mathbf{0}$.

We write $\mathbf{I}_\kappa$ for the set of all multi-indices indexed by κ; and if $\kappa = \{1, \ldots, m\}$, we simply write $\mathbf{I}_m$ or even $\mathbf{I}$ for the set of multi-indices indexed by $\{1, \ldots, m\}$, i.e., $\mathbf{I}_m = \{(n_1, n_2, \ldots, n_m) \mid n_i \in \mathbf{N} \cup \{0\}\}$.

■ (A.1.6) **Power series rings** For each $i \in \kappa$, let X_i be an indeterminate. For each $\mathbf{n} \in \mathbf{I}_\kappa$, we define $X^{\mathbf{n}}$ as

$$X^{\mathbf{n}} = \prod_{i \in \kappa, \mathbf{n}(i) \neq 0} X_i^{\mathbf{n}(i)}$$

Let A be a ring (commutative, $1 \in A$). Then the power series ring $A[\![X_i \mid i \in \kappa]\!]$ is defined as the set of all formal sums

$$f(X) = \sum_{\mathbf{n} \in \mathbf{I}_\kappa} a_{\mathbf{n}} X^{\mathbf{n}}, \qquad a_{\mathbf{n}} \in A$$

with addition and multiplication defined by

$$\sum a_{\mathbf{n}} X^{\mathbf{n}} + \sum b_{\mathbf{n}} X^{\mathbf{n}} = \sum (a_{\mathbf{n}} + b_{\mathbf{n}}) X^{\mathbf{n}} \tag{A.1.7}$$

$$\left(\sum a_{\mathbf{n}} X^{\mathbf{n}}\right)\left(\sum b_{\mathbf{n}} X^{\mathbf{n}}\right) = \sum c_{\mathbf{n}} X^{\mathbf{n}}, \qquad c_{\mathbf{n}} = \sum_{\mathbf{k}+\mathbf{l}=\mathbf{n}} a_{\mathbf{k}} b_{\mathbf{l}} \tag{A.1.8}$$

There are two obvious ring homomorphisms

$$\iota\colon A \to A[\![X_i \mid i \in \kappa]\!], \qquad \varepsilon\colon A[\![X_i \mid i \in \kappa]\!] \to A \tag{A.1.9}$$

defined by $\iota(a) = \sum a_{\mathbf{n}} X^{\mathbf{n}}$ with $a_{\mathbf{n}} = 0$ if $|\mathbf{n}| \geq 1$, $a_{\mathbf{0}} = a$, and $\varepsilon(\sum a_{\mathbf{n}} X^{\mathbf{n}}) = a_{\mathbf{0}}$. Of course $\varepsilon \circ \iota = id_A$.

Note that (A.1.7), (A.1.8) make $A[\![X_i \mid i \in \kappa]\!]$ a commutative ring with unit element $\iota(1)$. We shall usually identify $a \in A$ with its image $\iota(a)$ and thus view A as a subring of $A[\![X_i \mid i \in \kappa]\!]$.

■ (A.1.10) **Lemma** An element $f(X) \in A[\![X_i \mid i \in \kappa]\!]$ is invertible iff $\varepsilon(f(X)) \in A$ is invertible in A.

Proof Since ε is a ring homomorphism, the "only if" part is trivial. So suppose that $\varepsilon(f(X)) = a_{\mathbf{0}} \in U(A)$, the group of invertible elements of A, where $f(X) = \sum a_{\mathbf{n}} X^{\mathbf{n}}$. Let $g(X) = \sum b_{\mathbf{n}} X^{\mathbf{n}}$ with $b_{\mathbf{n}} \in A$ yet to be determined. $f(X)g(X) = 1$ gives us the equations

$$a_{\mathbf{0}} b_{\mathbf{0}} = 1 \tag{A.1.11}$$

$$0 = \sum_{\mathbf{k}+\mathbf{l}=\mathbf{n}} a_{\mathbf{n}} b_{\mathbf{n}} = a_{\mathbf{0}} b_{\mathbf{n}} + \sum_{\substack{\mathbf{k}+\mathbf{l}=\mathbf{n} \\ \mathbf{l}<\mathbf{n}}} a_{\mathbf{k}} b_{\mathbf{l}} \tag{A.1.12}$$

Since $a_{\mathbf{0}}$ is invertible, we can solve (A.1.11) with $b_{\mathbf{0}} \in A$; and given $b_{\mathbf{l}} \in A$ with $\mathbf{l} < \mathbf{n}$, we can solve (A.1.12) with $b_{\mathbf{n}} \in A$ again because $a_{\mathbf{0}} \in U(A)$. Q.E.D.

■ (A.1.13) **Notation and convention** If $\kappa = \{1, \ldots, m\}$, we shall write $A[\![X_1, \ldots, X_m]\!]$ for $A[\![X_i \mid i \in \{1, \ldots, m\}]\!]$ and even $A[\![X]\!]$ if m is clear from the context. *From now on* in this appendix $A[\![X]\!]$ *will always be a power series ring in a finite number of variables.*

■ (A.1.14) **Exercise**

$$A[\![X_1, \ldots, X_n]\!][\![X_{n+1}]\!] = A[\![X_1, \ldots, X_{n+1}]\!]$$

A.2 Filtration and Topology

Let R be a ring. A *ring filtration* on R is a function.

$$v\colon R \to \mathbf{N} \cup \{\infty\} \cup \{0\}$$

such that

$$v(0) = \infty, \qquad \mathrm{Im}(v) \neq \{\infty\} \tag{A.2.1}$$

$$v(a - b) \geq \min\{v(a), v(b)\} \tag{A.2.2}$$

$$v(ab) \geq v(a) + v(b) \tag{A.2.3}$$

For each $m \in \mathbf{N} \cup \{\infty\}$, we define $I_m = \{a \in R \mid v(a) \geq m\}$. Then I_m is an ideal of R and we have $I_m I_k \subset I_{m+k}$. The ideals I_m define a topology on A as follows:

the sequence $\{a_n\}$ converges to $a \in A$ iff $\lim_{n\to\infty} v(a_n - a) = 0$. This topology turns R into a topological ring (i.e., addition, subtraction, and multiplication are continuous). The topology is Hausdorff iff $I_\infty = \{0\}$.

■ (A.2.4) **Example** Let A be any ring, $R = A[\![X]\!]$. Define $v: R \to \mathbf{N} \cup \{0\}$ by

$$(A.2.5) \qquad \left(\sum a_{\mathbf{n}} X^{\mathbf{n}}\right) \geq s \quad \Leftrightarrow \quad a_{\mathbf{n}} = 0 \qquad \text{for all } \mathbf{n} \text{ with } |\mathbf{n}| < s$$

One easily checks that this is a ring filtration. Moreover, the induced topology on R is Hausdorff and complete (exercise).

■ (A.2.6) **Exercise** Suppose that A has no zero divisors. Show that then $v(f(X)g(X)) = v(f(X))v(g(X))$ and conclude that $A[\![X]\!]$ has no zero divisors. (*Hint:* use induction and (A.1.14).)

■ (A.2.7) **Exercise** Let R be as in (A.2.4). Let M_s be the subgroup of R of all $f(X) \in R$ such that $a_{\mathbf{n}} = 0$ for $|\mathbf{n}| \geq s$. Then $R = M_s \oplus I_s$ as an abelian group.

■ (A.2.8) **Example** Let A be a local ring with maximal ideal $\mathfrak{m}$. Define v: $A \to \mathbf{N} \cup \{\infty\}$ by $v(x) \geq m \Leftrightarrow x \in \mathfrak{m}^m$. This is a ring filtration on A.

■ (A.2.9) **Theorem** Let R and A be as in (A.2.4). If A is noetherian, so is R.

For a proof, see e.g., [511, Volume II, Chapter VII, Theorem 4, p. 138].

A.3 Formal Weierstrass Preparation Theorem

Let now A be a complete Hausdorff local ring with maximal ideal $\mathfrak{m}$ (cf. example (A.2.8)), and let $R = A[\![X]\!] = A[\![X_1]\!]$; i.e., the index set has one element in this section.

■ (A.3.1) **Definitions** An element $f(X) \in A[\![X]\!]$ is called a *distinguished polynomial* if it is of the form $f(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$ with $a_0, \ldots, a_{n-1} \in \mathfrak{m}$. An element $f(X) \in A[\![X]\!]$ is said to have *Weierstrass degree* n if $f(X) = \sum_{i=0}^{\infty} a_i X^i$ with $a_i \in \mathfrak{m}$ for $i < n$ and $a_n \in U(A) = A \backslash \mathfrak{m}$. We write W-degree$(f(X)) = n$. If $f(X) \in \mathfrak{m}[\![X]\!]$, we have W-degree$(f(X)) = \infty$ (and inversely).

■ (A.3.2) **Weierstrass preparation theorem** Let $f(X) \in A[\![X]\!]$ and suppose that W-degree $f(X) = n < \infty$. Then there exist a unique invertible power series $u(X) \in A[\![X]\!]$ and a unique distinguished polynomial $g(X)$ of degree n such that $f(X) = u(X)g(X)$.

Proof We shall construct power series $u^{(m)}(X)$ and distinguished polynomials $g^{(m)}(X)$ such that

$$(A.3.3) \qquad f(X) = u^{(m)}(X)g^{(m)}(X) \mod(\mathfrak{m}^m[\![X]\!])$$

and we shall show that these $u^{(m)}(X)$ and $g^{(m)}(X)$ are unique mod $\mathfrak{m}^m[\![X]\!]$.

First take $m = 1$. Take $g^{(1)}(X) = X^n$, $u^{(1)}(X) = \sum_{i=n}^{\infty} a_i X^{i-n}$. Then clearly (A.3.3) holds for $m = 1$, and one easily checks that $u^{(1)}(X)$ and $g^{(1)}(X)$ are unique mod $\mathfrak{m}[\![X]\!]$. Indeed, $g^{(1)}(X)$ being distinguished must be of the form X^s mod $\mathfrak{m}[\![X]\!]$.

Now suppose we have found $u^{(m)}(X)$, $g^{(m)}(X)$, $m \geq 1$. Write

$$g^{(m+1)}(X) = g^{(m)}(X) + b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}, \qquad b_i \in \mathfrak{m}^m$$

$$u^{(m+1)}(X) = u^{(m)}(X) + h(X), \qquad h(X) \in \mathfrak{m}^m[\![X]\!]$$

Suppose that $-g^{(m)}(X)u^{(m)}(X) + f(X) \equiv l(X) \in \mathfrak{m}^m[\![X]\!]$ mod $\mathfrak{m}^{m+1}[\![X]\!]$. Then we see that $b_0, b_1, \ldots, b_{n-1}, h(X)$ must satisfy

$$\text{(A.3.4)} \quad l(X) \equiv X^n h(X) + b_0 u^{(m)}(X) + b_1 X u^{(m)}(X) + \cdots + b_{n-1} X^{n-1} u^{(m)}(X)$$

mod $\mathfrak{m}^{m+1}[\![X]\!]$ because $g^{(m)}(X)h(X) \equiv X^n h(X)$ mod $\mathfrak{m}^{m+1}[\![X]\!]$ since $g^{(m)}(X)$ is distinguished of degree n and $h(X) \in \mathfrak{m}^m[\![X]\!]$ and $b_i h(X) \in \mathfrak{m}^{m+1}[\![X]\!]$ for all $i = 1, \ldots, n-1$. Because $u^{(m)}(X)$ is a unit there exist $b_0, \ldots, b_{n-1} \in \mathfrak{m}^m$ and $h(X) \in \mathfrak{m}^m[\![X]\!]$ such that (A.3.4) holds (if $l(X) \in \mathfrak{m}^m[\![X]\!]$), moreover such b_i and $h(X)$ are unique modulo $\mathfrak{m}^{m+1}$.

Now let $u(X), g(X)$ be the unique elements of $A[\![X]\!]$ such that $u(X) \equiv u^{(m)}(X)$, $g(X) \equiv g^{(m)}(X)$ mod $\mathfrak{m}^m[\![X]\!]$ for all $m \in \mathbf{N}$. Q.E.D.

A.4 Homomorphisms and Isomorphisms. Formal Inverse Function and Implicit Function Theorems

■ (A.4.1) **Continuous homomorphisms** Let R_1 and R_2 be two rings with ring filtrations v_1, v_2. Then a ring homomorphism $\vartheta: R_1 \to R_2$ is continuous (with respect to the topologies defined by v_1 and v_2 iff $v_1(a_n) \to \infty$ as $n \to \infty$ implies $v_2(\vartheta(a_n)) \to \infty$ as $n \to \infty$.

■ (A.4.2) **Proposition** Let $R = A[\![X_1, \ldots, X_m]\!]$ as in Example (A.2.4). Let R' be an A-algebra with a ring filtration v such that R' is complete and Hausdorff in the topology defined by v. Let $a_1, \ldots, a_m \in R'$ be n elements such that $v(a_i) \geq 1$, $i = 1, \ldots, m$. Then there exists a unique continuous A-algebra homomorphism $\vartheta: R \to R'$ such that $\vartheta(X_i) = a_i$.

Proof Define $\vartheta: R \to R'$ by the formula

$$\text{(A.4.3)} \qquad \vartheta\left(\sum a_{\mathbf{n}} X^{\mathbf{n}}\right) = \sum_{\mathbf{n}} a_{\mathbf{n}} a_1^{n_1} \cdots a_m^{n_m}$$

where we note that the sum on the right converges to a unique element of R' because R' is complete and Hausdorff.

Now because ϑ must be an A-algebra homomorphism, ϑ is necessarily unique on the sub-A-algebra $A[X_1, \ldots, X_m] \subset A[\![X_1, \ldots, X_m]\!]$ and given by (A.4.3) in this case (the sum is then finite). Also ϑ is an A-algebra homo-

morphism on $A[X]$. By continuity of ϑ it follows that (A.4.3) is the only possibility for ϑ because every element of $A[\![X]\!]$ is a limit of elements of $A[X]$. This approximation argument also shows that ϑ as defined by (A.4.3) is an A-algebra homomorphism since ϑ is an A-algebra homomorphism on $A[X]$.

■ (A.4.4) **Jacobian matrix** Let $X = (X_1, \ldots, X_m)$, $Y = (Y_1, \ldots, Y_n)$ be two sets of indeterminates, and let ϑ: $A[\![X]\!] \to A[\![Y]\!]$ be a continuous homomorphism of A-algebras. By Proposition (A.4.2) ϑ is uniquely determined by giving the m power series $\vartheta(X_1), \ldots, \vartheta(X_m) \in A[\![Y]\!]$; i.e., ϑ corresponds to an m-tuple $\alpha_\vartheta(Y)$ of power series in $Y_1, \ldots, Y_n$. Let $J(\vartheta)$ be the unique $m \times n$ matrix with coefficients in A such that

$$J(\vartheta)\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} \equiv \alpha_\vartheta(Y) \quad \text{mod(degree 2)}$$

in $A[\![Y]\!]^m$. The matrix $J(\vartheta)$ is called the Jacobian matrix of ϑ and also the Jacobian matrix of the m-tuple of power series $\alpha_\vartheta(Y)$.

■ (A.4.5) **Proposition** (formal inverse function theorem) A continuous A-algebra homomorphism ϑ: $A[\![X]\!] \to A[\![Y]\!]$ is an isomorphism iff $J(\vartheta)$ is an invertible matrix.

Proof If ϑ is an isomorphism, there is an inverse isomorphism ϕ, $A[\![Y]\!] \to A[\![X]\!]$; let M be the unique matrix such that

$$\begin{pmatrix} \phi(Y_1) \\ \vdots \\ \phi(Y_n) \end{pmatrix} \equiv M \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} \quad \text{mod(degree 2)}$$

then because $\vartheta \circ \phi = id$, $\phi \circ \vartheta = id$, we must have $J(\vartheta)M = I_m$, $MJ(\vartheta) = I_n$ so that $J(\vartheta)$ is invertible.

Conversely, suppose that $J(\vartheta)$ is invertible. Then $n = m$ and identifying $A[\![X]\!]$ with $A[\![Y]\!]$ by means of $X_i \mapsto Y_i$ we find the following reformulation of (A.4.5).

(A.4.6) Let $\alpha(X)$ be an n-tuple of elements of $A[\![X_1, \ldots, X_n]\!]$ such that $\alpha(X) \equiv JX$ mod(degree 2) where J is an invertible $n \times n$ matrix in $A^{n \times n}$ and where X is short for the column vector $(X_1, \ldots, X_n)$. Then there exists a unique n-tuple of elements $\beta(X)$ such that $\beta(\alpha(X)) = X = \alpha(\beta(X))$.

Proof Take $\beta^{(1)}(X) = J^{-1}X$. Then $\beta^{(1)}(\alpha(X)) \equiv X$ mod(degree 2) and $\beta^{(1)}(X)$ is uniquely determined mod(degree 2) by this condition. Suppose we have found $\beta^{(m)}(X)$ such that $\beta^{(m)}(\alpha(X)) \equiv X$ mod(degree $m+1$) and suppose that $\beta^{(m)}(X)$ is uniquely determined mod(degree $m+1$) by this condition. Let $\beta^{(m)}(\alpha(X)) - X \equiv N(X)$ mod(degree $m+2$) where $N(X)$ is an n-tuple of homogeneous polynomials of degree $m+1$. Now take $\beta^{(m+1)}(X) = \beta^{(m)}(X) - R(X)$

where $R(X)$ is such that $R(JX) = N(X)$, i.e., $R(X) = N(J^{-1}X)$. Then $\beta^{(m+1)}(\alpha(X)) \equiv X$ mod(degree $m+2$) and $\beta^{(m+1)}(X)$ is unique modulo(degree $m+2$) with this property. Let $\beta(X)$ be the unique power series such that $\beta(X) \equiv \beta^{(m)}(X)$ mod(degree $m+1$) for all m. ($\beta(X)$ exists and is unique because $A[\![X]\!]$ is complete and Hausdorff.) Then $\beta(\alpha(X)) = X$. Similarly, one shows the existence of a $\hat{\beta}(X)$ such that $\alpha(\hat{\beta}(X)) = X$, and then $\beta(X) = \beta(\alpha(\hat{\beta}(X))) = (\beta \circ \alpha)(\hat{\beta}(X)) = \hat{\beta}(X)$. Q.E.D.

■ (A.4.7) **Formal implicit function theorem** Let

$$F(X; Y) \in A[\![X_1, \ldots, X_m; Y_1, \ldots, Y_n]\!]$$

be an n-tuple of power series in $X_1, \ldots, X_m$ and $Y_1, \ldots, Y_n$ such that $F(0; 0) = 0$ and such that the unique (partial Jacobian) matrix J such that $F(X, Y) \equiv JY$ mod($X_1, \ldots, X_m$; degree 2) is invertible (in particular there are as many variables Y_i as there are power series). Then there exists a unique n-tuple of power series $\alpha(X) \in A[\![X_1, \ldots, X_m]\!]^n$ such that $F(X; \alpha(X)) = 0$.

Proof We can write

$$F(X; Y) \equiv MX + JY + G(X; Y) \tag{A.4.8}$$

where every monomial occurring in $G(X; Y)$ is at least of degree 2 and where M is some $n \times m$ matrix with coefficients in A.

Now take $\alpha^{(1)}(X) = -J^{-1}MX$. Then $F(X, \alpha^{(1)}(X)) \equiv 0$ mod(degree 2) and $\alpha^{(1)}(X)$ is uniquely determined mod(degree 2) by this condition. Suppose we have found an $\alpha^{(r)}(X)$, unique mod(degree $r+1$), such that $F(X, \alpha^{(r)}(X)) \equiv 0$ mod(degree $r+1$). Suppose $F(X, \alpha^{(r)}(X)) \equiv N(X)$ mod(degree $r+2$) with $N(X)$ an n-tuple of homogeneous polynomials of degree $r+1$. Now take $\alpha^{(r+1)}(X) = \alpha^{(r)}(X) - J^{-1}N(X)$, then $F(X, \alpha^{(r+1)}(X)) \equiv 0$ mod(degree $r+1$) (cf. (A.4.8)) and $\alpha^{(r+1)}(X)$ is uniquely determined mod(degree $r+2$) by this condition because $\alpha^{(r)}(X)$ is unique mod(degree $r+1$). Let $\alpha(X)$ be the unique element of $A[\![X]\!]^n$ such that $\alpha(X) \equiv \alpha^{(r)}(X)$ mod(degree $r+1$) for all $r \in \mathbf{N}$. Q.E.D.

APPENDIX B

BRIEF NOTES ON FURTHER APPLICATIONS OF FORMAL GROUP (LAW) THEORY

This Appendix B is more or less a supplement to E.5. It contains a number of mainly bibliographical notes on other applications of formal group laws in number theory, geometry, and topology. I have made no real attempt to mention *all* references which use or treat formal groups in the E.1–E.6 sections and/or Appendix B.

B.1 More on Formal Groups in Number Theory

■ (B.1.1) **Global class field theory over function fields** In [134] Drinfel'd uses formal A-modules to study class field theory of global function fields. He obtains analogues of (i) the Kronecker–Weber theorem concerning the maximal abelian extension of $\mathbf{Q}$ or an imaginary quadratic extension of $\mathbf{Q}$, (ii) the Eichler–Shimura theorem on ζ-functions of modular curves (cf. also [328]).

The main tool is an *elliptic module*, which Drinfel'd defines as follows. Let A be the ring of integers of the global function field k of characteristic $p > 0$. Let K be any field over A. Then an elliptic module over K is a nontrivial embedding $A \to K_\sigma[T]$, where $K_\sigma[T]$ is the ring of twisted polynomials in T with coefficients in K with the multiplication $Tx = x^p T$. Of course, $K_\sigma[T]$ is the ring of endomorphisms of the additive algebraic group $\mathbf{G}_a$ over K, and this provides a link with formal A-modules and also Lubin–Tate local class field theory in the case of local fields of characteristic p. Indeed, if A_v is a completion of A at a finite place v, and $F(X, Y)$ a formal A_v-module of A_v-height 1 over A_v, then $F(X, Y)$ is isomorphic as a formal group law to $\hat{\mathbf{G}}_a(X, Y)$ so that $a \mapsto [a]_F(X)$ gives us a (nontrivial) embedding $A_v \to (A_v)_\sigma[\![T]\!]$.

Some of Drinfel'd results are obtained (and generalized) by Hayes [164] without using formal group laws.

■ (B.1.2) **Kummer theory; quadratic reciprocity** In [144, Chapter IV, Section 3] Fröhlich obtains a number of interesting results for one dimensional

formal group laws $F(X, Y)$ over the ring of integers of a finite extension of $\mathbf{Q}_p$, which, for the case $F(X, Y) = \hat{\mathbf{G}}_m(X, Y)$, the multiplicative formal group law, relate to Kummer theory.

Honda [192] uses the formal group law $X + Y + SXY$ where S is a gaussian sum with quadratic character to obtain a new interpretation and proof of the quadratic reciprocity law.

B.2 More on Formal Groups in Algebraic Geometry

■ (B.2.1) **p-divisible groups (or Barsotti–Tate groups)** p-divisible groups are a generalization (due to Barsotti and Tate) of finite height formal groups. Here is the definition. Let R be a commutative ring and $h \in \mathbf{N}$. A p-divisible group of height h over R is a system of commutative finite group schemes $G = (G_n, i_n)$, $n \in \mathbf{N}$, over R such that (i) the R-algebra $A(G_n)$ of G_n is locally free of rank p^{nh} over R; (ii) $i_n\colon G_n \to G_{n+1}$ is a homomorphism of group schemes; and (iii) the sequence

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}$$

is exact. (Here p^n is the homomorphism "adding an element to itself p^n times.") An example is the constant group $\mathbf{Q}_p/\mathbf{Z}_p$ as union of the $p^{-n}\mathbf{Z}_p/\mathbf{Z}_p$. A most important example is the p-divisible group $A(p)$ associated to an abelian scheme A over R, which consists of the kernels $A(p)_n = \mathrm{Ker}(A \xrightarrow{p^n} A)$.

As to the connection between formal groups and p-divisible groups, we have the following. Let R be a complete local noetherian ring of residue characteristic $p > 0$. Then if N is a finite group scheme over R we have a short exact sequence $0 \to N^\circ \to N \to N^{\mathrm{et}} \to 0$ with N° connected (i.e., its algebra $A^\circ = A(N^\circ)$ is local) and N^{et} étale over R. Now if $G = (G_n, i_n)$ is a p-divisible group, one finds an induced decomposition $0 \to G^\circ \to G \to G^{\mathrm{et}} \to 0$ corresponding to $0 \to G_n^\circ \to G_n \to G_n^{\mathrm{et}} \to 0$ for each n. Now G° "is" a formal group over R in the following sense. Let $F(X, Y)$ be a formal group law of dimension m over R. Consider the m-tuple of power series $[p^n]_F(X)$. Suppose that $F(X, Y)$ is of finite height h. Let J_n be the ideal of $R[\![X]\!]$ generated by the m power series $[p^n]_F(X)$. Then $R[\![X]\!]/J_n$ is free of rank p^{nh} over R (cf. 28.2, especially the proof of (28.2.9)) and the comultiplication $\mu_F\colon R[\![X]\!] \to R[\![X]\!] \otimes_R R[\![X]\!]$ defined by $F(X, Y)$ (cf. (36.1.4)) induces a comultiplication $R[\![X]\!]/J_n \to R[\![X]\!]/J_n \otimes_R R[\![X]\!]/J_n$ making $F(p)_n = \mathrm{Spec}(R[\![X]\!]/J_n)$ into a finite commutative group scheme over R. These $F(p)_n$ combine to define a p-divisible group $F(p)$ over R. Moreover, one has the theorem (Tate [404]): the functor $F(X, Y) \mapsto F(p)$, taking finite height formal group laws over R into connected p-divisible groups, is an equivalence of categories (if R is complete local noetherian). This equivalence of categories does not hold in general over Hensel rings (cf. Koch [226]).

So, over complete local noetherian rings, p-divisible groups are extensions of divisible étale groups by formal groups. Many theorems of formal group theory carry over to the case of p-divisible groups. For the theory of p-divisible groups,

cf. [365, 404, 433, 94]. In [464] Abraškin settles an old question of Tate, [404], by showing that there do exist nontrivial 2-divisible groups over **Z**.

■ (B.2.2) **Lifting abelian varieties** One reason for the high interest among algebraic geometers in p-divisible groups is their connection with the theory of (lifting) abelian varieties as embodied in the following theorem of Serre and Tate.

Theorem Let R be a local artinian ring of residue field k of characteristic $p > 0$ and let A_0 be an abelian variety over k and $A_0(p)$ the corresponding p-divisible group. Then liftings of A_0 to an abelian scheme over R correspond bijectively (up to isomorphism) to liftings of the p-divisible group $A_0(p)$.

For a proof, cf. Messing [286, Chapter V, Theorem 2.3]. In [135] there is a proof that avoids the use of crystals.

This theorem gives rather immediately liftings to characteristic zero of ordinary abelian varieties; the so-called canonical liftings; cf. [365]. Nonordinary abelian varieties are then handled via deformation techniques. Biextensions of formal groups are an important tool. Some references (besides those already mentioned) concerning liftings and biextensions are [156, 309, 313].

■ (B.2.3) **Crystalline cohomology** A second reason for the high interest in p-divisible groups (also called Barsotti–Tate groups) is their relation with crystals and crystalline cohomology, which was already hinted at in the last few lines of Section 26. Here space–time considerations and the state of this author's knowledge of these matters definitely forbid him to do anything but give a list of references [33, 34, 37, 38, 155, 157, 198, 199, 221, 282, 283, 318, 477, 285–287], where he cannot refrain from pointing to the connection of formal group laws to algebraic K-theory via (a reinterpretation of) p-typical curves; cf. [33, 37]. In this connection see also [283, 96, 261, 489]. In [489], for instance, a natural completion of $\mathrm{Ker}(K_2(k[\![t]\!] \to K_2(k))$, where k is a field, is seen as a $\mathrm{Cart}(k)$-module. (Here the Frobenius operators correspond to the transfer homomorphisms induced by $t \mapsto t^n$; cf. [495].) Added in proof. Cf. in addition also [13] for some connections between the crystalline cohomology of varieties and certain invariants of formal groups arising (sometimes) from these varieties.

B.3 More on Formal Groups in Arithmetical Algebraic Geometry

■ (B.3.1) **Formal structure of algebraic varieties and formal groups attached to differential equations** With [188, 189] Honda started a systematic program of investigating the formal structure of (Jacobians of) algebraic varieties and (via the interpretation of the differential of the logarithm of a formal group law as a left invariant differential) a search for formal group laws attached to differential equations. His paper [190] contains an outline of this program. The differential equations in question are expected to be of

fuchsian type in view of results of Katz [220]. However, formal groups also turn up in nonfuchsian situations; cf. Dwork [475] and Sperber [503–505]. Results concerning this program are contained in [191, 193, 197]. The congruences which (according to the functional equation lemma) the coefficients of the logarithms of the formal group laws associated to hypergeometric functions must satisfy are basically the congruences on binomial type numbers in Lemma 1 of Dwork [138]. In [192] Honda uses formal groups to verify the Weil conjecture for some elliptic curves. (This result is not new, but the method is.)

■ (B.3.2) **Norm maps, class field type theories, and Iwasawa–Mazur theory** Let L/K be a Galois extension of the local field K, and let $F(X, Y)$ be a formal group law over $A(K)$. For each $x \in \mathfrak{m}(L) = F(L)$, consider $\tau_1 x +_F \tau_2 x +_F \cdots +_F \tau_n x$ where $\{\tau_1, \ldots, \tau_n\} = \mathrm{Gal}(L/K)$. This element is invariant under $\mathrm{Gal}(L/K)$ (because the τ_i act continuously and $F(X, Y)$ has its coefficients in $A(K)$). So we have defined a norm map

$$F\text{-Norm}_{L/K}\colon F(L) \to F(K)$$

In case $F(X, Y) = \hat{\mathbf{G}}_m(X, Y)$, the corresponding norm map is the ordinary norm map $N_{L/K}\colon U^1(L) \to U^1(K)$. Now the description of the image or cokernel of $N_{L/K}\colon L^* \to K^*$ is what local class field theory is about (to a great extent in any case). By far the hardest part of this is the analysis of $N_{L/K}\colon U^1(L) \to U^1(K)$.

The general goal is now to develop class field type theories for other algebraic (and formal) groups than $\mathbf{G}_m$. For the case of abelian varieties over number fields, the local norm maps $\hat{A}(L) \to \hat{A}(K)$ play a not unimportant role in Mazur's work on $\mathbf{Z}_p$-extensions, rational points of abelian varieties, and the Šafarevič–Tate group Ш; cf. [281], especially Section 4; cf. also [278]. Particularly important in this case are the norm maps $F(K_n) \to F(K)$ where K_n is a finite level in a $\mathbf{Z}_p$-extension (also called Γ-extension) K_∞/K; i.e., $\mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p$, K_n the invariant field of $p^n\mathbf{Z}_p$.

In case $F(X, Y)$ is of height 1, the cokernel of F-Norm is up to a twist described by local class field theory (essentially because $F(X, Y)$ becomes isomorphic to $\hat{\mathbf{G}}_m(X, Y)$ over $\hat{K}_{nr}$ (if K is a local field). In [281] Mazur treats the case that $\hat{A}$ is a $\hat{K}_{nr}/K$ form of $\hat{\mathbf{G}}_m^d(X, Y)$.

In the case that $F(X, Y)$ is one dimensional and of height ≥ 2 there are a number of rather precise results on the image of F-Norm: $F(K_n) \to F(K)$ in [165–168]. As a corollary one obtains a universal norm theorem saying that the intersection of all subgroups F-Norm$(F(L))$ for L/K Galois is zero. This last result generalizes fairly easily. For these and related matters, cf. also [26, 228, 229, 427, 149, 412, 485, 486].

Some detailed specific calculations on $E(K_n)$ and Ш(K_n) as K_n runs through the finite levels of a $\mathbf{Z}_p$-extension are in [30, 27, 28, 25, 31, 238, 239, 228, 200].

Of course the results of Fröhlich mentioned in (B.1.2) above also fit in the general framework of other types of class field theories as do (in a different way)

results of Serre *et al.* which we already mentioned in the last paragraph of (E.5.4). In this connection (of other type class field theories) let me also mention a number of papers of Vvedenskii [428–430, 426].

■ (B.3.3) ***L*-functions of elliptic curves** In [470] Coates and Wiles use formal group techniques to obtain results concerning the Birch–Swinnerton-Dyer conjecture on the behavior of the Hasse–Weil zeta function $L_E(s)$ near $s = 1$. Very much related are certain explicit formulas for the reciprocity symbol in terms of Lubin–Tate formal group law endomorphisms $[u]_F$; cf. [509], and also [144], Chapter IV, Section 3. These explicit formulas generalize those of Iwasawa [480] for the cyclotomic case.

■ (B.3.4) **Other results** Let K be a p-adic field. In [135] Drinfel'd uses formal A-modules (especially moduli) to construct étale coverings of Ω^d over K, the domain in $\mathbf{P}^d$ of all points which are not on any hyperplane in $\mathbf{P}^d$ which is defined over K. These constructions use that $\hat{\Omega}^d$ can be interpreted as a (sort of) moduli space for a certain kind of formal A-module; according to [135] these constructions specialize to Lubin–Tate class field theory in the case of $d = 1$.

B.4 More on Formal Groups in Algebraic Topology

■ (B.4.1) **Realizing formal group laws, extraordinary *K*-theories** If h^* is a complex oriented cohomology theory, then as we have seen one has a formal group law $F_h(X, Y)$ over $h(pt)$ attached to it. The questions naturally arise: Can all formal group laws be realized this way? and: Are cohomology theories with the same formal group law necessarily isomorphic? Positive results in this direction are first Morava's extraordinary K-theories, which realize the height h formal group laws $\bar{F}_{\Delta_h}(X, Y)$ and, e.g., his "ordinary" K-theories attached to various "genera" like the Ramanujam τ-function and the quadratic residue symbol. More precisely, taking the τ-function case as an example: there exists a complex oriented cohomology theory h^* such that if ϑ: $MU^* \to h^*$ is the associated transformation of cohomology theories (cf. Theorem (34.1.3)), then $\vartheta([\mathbf{CP}^{n-1}]) = \tau_n$ where τ is the Ramanujam τ-function defined by $\sum \tau_n q^n = q \prod (1 - q^n)^{24}$. For these and related matters, cf. [303–306, 210]. More positive results have been obtained by Würgler [449] and Rudjak [346], using the Baas–Sullivan technique of cobordism with singularities; cf. [400, 16–18]. (Landweber's exact functor theorem is also important here [248, 452].)

All this is relevant for the general problem formulated by Cartier [71] of defining cohomology theories "with coefficients in any given algebraic or formal group." Personally, I think that among the most interesting formal group laws to try to realize are the height 1 formal A-modules (Lubin–Tate formal A-modules) for A not necessarily unramified. Also in connection with Golo's note [151], where he finds a link between the norm residue symbol of local class field theory and Adams operations.

As far as I know there is at the moment no counterexample; i.e., there is as yet no formal group law of which it has been proved that it cannot be the formal group law of a complex oriented cohomology theory.

■ (B.4.2) **Stable (multiplicative) operations** Let h^* be a complex oriented cohomology theory. Let $w_i \in h^{-2i}(pt)$, $w_1 = 1$ be a series of elements. When does there exist a (multiplicative) transformation ϑ: $MU^* \to h^*$ taking $[\mathbf{CP}^i]$ into w_{i+1}. (This relates of course to the "genera" question touched upon above.) The answer is quite easy to obtain. This happens iff there is a new Euler class $\tilde{e}(L)$ defined by $\tilde{e}(L) = \sum_{i=1}^{\infty} a_i e^h(L)^i$, $a_1 = 1$ for h^* which takes $\log_h(X)$ into the "logarithm belonging to the w_i," i.e., we must have

$$\log_h(a(X)) = \sum_{n=0}^{\infty} (n+1)^{-1} w_n X^{n+1}$$

which in terms of the Witt-like polynomials $nw_n^h(X)$ of the formal group law $F_h(X, Y)$ (cf. Section 25.1) means that we must have,

$$nw_n^h(b_1, \ldots, b_n) = w_n, \qquad \text{where} \quad \sum_{i=1}^{\infty} a_i X^i = \sum_{i=1}^{\infty F_h} b_i X^i,$$

cf. [203]. Of course in case $F_h(X, Y)$ is a functional equation formal group law (as, e.g., in case $h^* = k^*$, K^*, MU^*, BP^*, H^*) this means that necessary and sufficient conditions for the existence of such a ϑ are given by functional equation lemma type conditions.

Applying this to BP and taking only p-typical sequences $(w_1, w_p, w_{p^2}, \ldots)$ one obtains information on the multiplicative operations in $BP^*(BP)$; cf. [334, 172].

See also [300], especially Chapter I, Section 7 and [77] where formal group laws are used to describe $K_*(K)$.

■ (B.4.3) **Algebraic theory of $MU_*(MU)$-comodules** Let S be a topological space. Then $MU_*(S)$ is not only an $MU_*(pt)$-module but also a $MU_*(MU)$-comodule, and this structure carries a lot of extra information. A number of papers deal systematically with properties and restrictions arising from the presence of $MU_*(MU)$- and $BP_*(BP)$-comodule structures on $MU_*(S)$ and $BP_*(S)$. See, e.g., [242–248, 301, 302, 161, 213].

■ (B.4.4) **Calculations, homotopy groups of spheres, Adams–Novikov spectral sequence** BP cohomology, its operations, and the generators $v_1, v_2, \ldots$ have proved to be useful on a number of occasions for calculations (often via the Adams–Novikov spectral sequence); for example, to prove that certain stable homotopy elements of the spheres are nonzero or to prove that certain $MU^*(pt)$-modules cannot be realized as an $MU^*(S)$; cf., e.g., [212, 290, 319, 395, 406, 407, 454, 461–463].

In this connection a number of papers analyze in detail the E_2-terms $\mathrm{Ext}^*_{BP_*BP}(BP_*, BP_*(X))$ and $\mathrm{Ext}^*_{MU_*MU}(MU_*, MU_*(X))$ of the Adams–

Novikov spectral sequence, obtaining, e.g., simplifications under certain hypotheses on $BP_*(X)$; cf., e.g., [288, 289, 291–293, 301, 302, 335, 336, 338, 498].

■ (B.4.5) **On $BP_*(BP)$ and $MU_*(MU)$** Let $\mathscr{I}$: $\mathrm{Alg}_{\mathbf{Z}_{(p)}} \to \mathbf{Set}$ be the functor that assigns to a $\mathbf{Z}_{(p)}$-algebra A the set of triples $(F(X, Y), \alpha(X), G(X, Y))$ consisting of two p-typical formal group laws $F(X, Y)$, $G(X, Y)$ over A and a strict isomorphism $\alpha(X)$: $F(X, Y) \to G(X, Y)$ over A. Let Φ: $\mathbf{Alg}_{\mathbf{Z}_{(p)}} \to \mathbf{Set}$ be the functor that assigns to A the set of p-typical formal group laws over A. Then Φ is representable by $\mathbf{Z}_{(p)}[V] = BP_*(pt)$ by the universality of $F_V(X, Y)$ and $\mathscr{I}$ is representable by $\mathbf{Z}_{(p)}[V; T] = BP_*(BP)$. There are a number of obvious functor morphisms between $\mathscr{I}$ and Φ, viz.

$$\mathscr{I} \to \Phi, \quad (F(X, Y), \alpha(X), G(X, Y)) \mapsto F(X, Y)$$

$$\mathscr{I} \to \Phi, \quad (F(X, Y), \alpha(X), G(X, Y)) \mapsto G(X, Y)$$

$$\mathscr{I} \to \mathscr{I}, \quad (F(X, Y), \alpha(X), G(X, Y)) \mapsto (G(X, Y), \alpha^{-1}(X), F(X, Y))$$

$$\mathscr{I} \times_{\Phi} \mathscr{I} \to \mathscr{I}, \quad ((F(X, Y), \alpha(X), G(X, Y)), (G(X, Y), \beta(X), H(X, Y)) \mapsto (F(X, Y), \beta(X) \circ \alpha(X), H(X, Y))$$

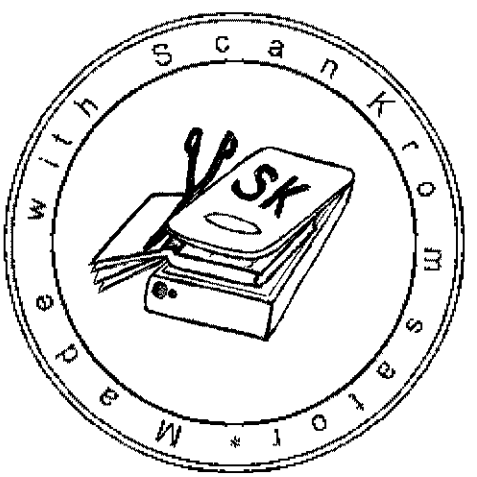
By the representability of $\mathscr{I}$ and Φ there result $\mathbf{Z}_{(p)}$-algebra homomorphisms η_L: $BP(pt) \to BP_*(BP)$, η_R: $BP(pt) \to BP_*(BP)$, ι: $BP_*(BP) \to BP_*(BP)$, and μ: $BP_*(BP) \to BP_*(BP) \otimes_{BP(pt)} BP_*(BP)$, which are the structure maps of the Hopf algebra $BP_*(BP)$. (NB this is a more general notion of Hopf algebra than occurs in (37.1.7) since the left and right $BP_*(pt)$-algebra structure of $BP_*(BP)$ are different.) Similar results hold for $MU_*(MU)$. This was remarked by Landweber [246]; cf. also [172; 300, Chapter 1, Section 7].

■ (B.4.6) **Hopf rings** The ring functor W: **Ring** $\to$ **Ring** of Witt vectors is representable by $\mathbf{Z}[X_1, X_2, \ldots]$. It follows that the addition and multiplication polynomials Σ_i, Π_i define on $\mathbf{Z}[X_1, X_2, \ldots]$ the structure of a coring object. Its dual $\mathbf{U}^c$ (cf. 37.5) is therefore a ring object in the category of coalgebras. We have already remarked that $\mathbf{U}^c = H^*(BU; \mathbf{Z})$. This is by no means the only such object in topology. Ravenel and Wilson named these objects *Hopf rings* and devoted a big (and to my mind fascinating) paper to them [341]; cf. also [340].

(B.4.7) **Other topics** A number of topics in algebraic topology where formal groups have been used have not yet been mentioned, e.g., fixed points of periodic mappings, two-valued formal groups, power systems, the formal group law of unoriented cobordism theory and a $\mathbf{Z}/(p)$-analogue, equivariant cobordism. A selection of references is [57, 58, 60, 4, 139, 214–217, 236, 237, 298, 352, 354, 376, 379, 381].

Much information on formal group laws in algebraic topology can be found in the fairly recent survey [54]; the intersection between [54] and (B.4.1)–(B.4.6) and Section 34 above is practically empty.

This page intentionally left blank



BIBLIOGRAPHY

1. J. F. Adams, Lectures on generalized cohomology, *in* "Category Theory, Homology Theory and Their Applications III" (P. J. Hilton, ed.), pp. 1–138. Lect. Notes Math., Vol. 99, Springer-Verlag, Berlin and New York, 1969.
2. J. F. Adams, "Stable Homotopy and Generalized Homology." Univ. of Chicago Press, Chicago, Illinois, 1974. (34.1.11, 34.1.10, 34.5.2, 31.1.1, 34.3.5, E.5.3)
3. J. F. Adams, Algebraic topology in the last decade, *Proc. Symp. Pure Math., 22nd, Algebraic Topology*, pp. 1–22. *Amer. Math. Soc.*, 1971.
4. J. F. Adams and A. Liulevicius, The Hurewicz homomorphism for MU and BP, *J. London Math. Soc.* **5** (1972), 539–545.
5. J. F. Adams and A. Liulevicius, Buhštaber's work on two-valued formal groups, *Topology* **14** (1975), 291–296. (B.4.7)
6. J. C. Alexander, On Liulevicius' and Hazewinkel's generators for $\pi_*(BP)$, preprint. Univ. of Maryland, 1972. (34.4.4)
7. S. Araki, A typical formal group in K-theory, *Proc. Japan Acad.* **49** (1973), 477–482. (E.5.3)
8. S. Araki, Typical formal groups in complex cobordism and K-theory, *Lect. Math. Kyoto Univ.* **6**, Kinokuniya Book Store, 1973. (E.5.3)
9. S. Araki, p-typical formal groups and the homomorphism $\Omega^U_* \to \Omega^{SO}_*$, *Osaka J. Math.* **11** (1974), 347–352.
10. S. Araki, Multiplicative operations in BP cohomology, *Osaka J. Math.* **12** (1975), 343–356.
11. E. Artin and H. Hasse, Die beide Ergänzungssätze zum Reciprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswürzeln, *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 146–162. (15.3.12)
12. E. Artin and J. Tate, Class field theory, Lecture notes, Princeton Univ. 1951–1952 seminar. (E.5.1)
13. M. Artin and B. Mazur, Formal groups arising from algebraic varieties, *Ann. École Norm. Sup.* (4) **10** (1977), 87–131. (B.2.3)
14. M. F. Atiyah, Power operations in K-theory, *Quart. J. Math.* **17** (1966), 165–193. (E.5.3)
15. M. F. Atiyah and D. O. Tall, Group representations, λ-rings and the J-homomorphism, *Topology* **8** (1969), 253–297. (E.2.1, E.5.3)
16. N. A. Baas, On formal groups and singularities in complex cobordism theory, *Math. Scand.* **33** (1973), 303–313. (B.4.1)
17. N. A. Baas, On bordism theory of manifolds with singularities, *Math. Scand.* **33** (1973), 279–302. (B.4.1)
18. N. A. Baas, On bordism theories with singularities, *Proc. Advances Study Inst. Algebraic Topology, Aarhus* **I**, 1–16, Various Publ. Ser. 13, Mat. Inst., Aarhus Univ., 1970. (B.4.1)
19. N. A. Baas and I. Madsen, On the realization of certain modules over Steenrods algebra, *Math. Scand.* **31** (1972), 220–224.

20. I. Barsotti, On Witt vectors and periodic group varieties, *Illinois J. Math.* **2** (1958), 99–110; Corrections, *ibid.* 608–610.
21. I. Barsotti, Moduli canonici i gruppi analitici commutativi, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **13** (1959), 303–372. (E.4.1)
22. I. Barsotti, Analytical methods for abelian varieties in positive characteristic, Coll. sur la theorie des groupes algebriques, *CBRM* (1962), 77–86. (E.4.1)
23. I. Barsotti, Metodi analitici per varieta abeliane in caratteristica positiva, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **18** (1964), 1–25; **19** (1965), 277–330; **19** (1965), 481–512; **20** (1966), 101–137; **20** (1966), 331–365.
24. I. Barsotti, Sviluppi e applicazione della teoria dei gruppi analitici commutativi, *Atti dell' Congr. dell' Unione Mat. Italiana, 8th, Trieste* (1967).
25. M. I. Bačmakov and N. Z. Al'Nader, Behaviour of the curve $x^3 + y^3 = 1$ in a cyclotomic Γ-extension, *Mat. Sb.* **90** (1973), 117–130. (B.3.2)
26. M. I. Bačmakov and A. N. Kirillov, The Lutz filtration of a formal group (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **39** (1975), 1227–1239. (B.3.2)
27. M. I. Bačmakov and A. S. Kuročkin, Rational points on a certain modular curve with values in the cyclotomic 2-extension, *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* **57** (1976), 5–7. (B.3.2)
28. M. I. Bačmakov and A. S. Kuročkin, Selmer groups of the elliptic curve $X_0(32)$. *In* "Sbornik Contemporary Algebra," Vol. IV (1975), 3–12. (B.3.2)
29. G. M. Bergman, Ring schemes, Lecture 26 in D. Mumford, "Lectures on Curves on an Algebraic Surface," Princeton Univ. Press, Princeton, New Jersey, 1966. (E.2.4, 15.3)
30. V. G. Berkovič, Division by isogeny of the points of an elliptic curve (Russian), *Mat. Sb.* **93** (1974), 467–486. (B.3.2)
31. V. G. Berkovič, Mazur module for elliptic curves (Russian), *Mat. Zametki* **17** (1975), 319–328 (*English Transl.: Math. Notes* **17** (1975), 183–188). (B.3.2)
32. P. Berthelot, Généralités sur les λ-anneaux, *Sem. Géomét. Algébrique du Bois Marie* **6** (1966/1967), Exposé V, *LNM* **225** (1971), 297–365. (E.2.1, E.5.3)
33. P. Berthelot, Slopes of Frobenius in cristalline cohomology, *in* R. Hartshore (ed.), Algebraic geometry, *Proc. Symp. Pure Math.* **29** (1975), 315–328. (B.2.3)
34. P. Berthelot, Cohomology cristalline des schémes de caracteristique $p > 0$, *LNM* **407** (1974). (B.2.3, 38.2.2)
35. B. J. Birch a.o., Numerical tables on elliptic curves, *in* "Modular Functions of One Variable IV." Lect. Notes Math. Vol. 476. Springer-Verlag, Berlin and New York, 1975. (E.5.2)
36. A. Blanchard, Les corps non commutatifs, Pr. Univ. de France, 1972. (20.2.16)
37. S. Bloch, Algebraic K-theory and cristalline cohomology, *Publ. Math. IHES.* (B.2.3) (to appear).
38. S. Bloch, Dieudonné crystals associated to p-divisible groups, preprint. (B.2.3)
39. J. M. Boardman, Stable homotopy theory: appendix C-localization theory; appendix D-localization and splittings of MU, preprints, Johns Hopkins Univ., 1976. (34.4.6)
40. S. Bochner, Formal Lie groups, *Ann. of Math.* **47** (1946), 192–201. (9.7, E.1.1)
41. A. Borel, "Linear Algebraic Groups." Benjamin, New York, 1969.
42. N. Bourbaki, "Algèbre commutative," Chapter 1, Modules plats, Chapter 2, Localisation. Hermann, Paris, 1961. (35.4.3, 28.3.10, 21.3.5)
43. N. Bourbaki, "Algèbre Commutative," Chapter 3, Graduations, filtrations et topologies, Chapter 4, Idéaux premiers associés et décomposition primaire. Hermann, Paris, 1961. (17.4.17, 28.3.10, 28.2.6)
44. N. Bourbaki, "Groupes et algèbres de Lie," Chapter 2, Algèbres de Lie libres, Chapter 3, Groupes de Lie. Hermann, Paris, 1972. (E.1.9)
45. G. E. Bredon, Equivariant cohomology theories, Lect. Notes Math. Vol. 34. Springer-Verlag, Berlin and New York, 1967.

46. Th. Brôcker and T. tom Dieck, Kobordismentheorie, Lect. Notes Math. Vol. 178. Springer-Verlag, Berlin and New York, 1970.
47. E. H. Brown, Jr., and F. P. Peterson, A spectrum whose $\mathbf{Z}_p$-cohomology is the algebra of reduced pth powers, *Topology* **5** (1966), 149–154. (34.4.6)
48. V. M. Buhštaber, The Chern-Dold character in cobordism theory I, *Mat. Sb.* **83** (1970), 575–595 (*English transl.: Math. USSR Sb.* **12** (1970), 573–593. (E.5.3)
49. V. M. Buhštaber, Two-valued formal groups. Some applications to cobordism, *Usp. Mat. Nauk* **26** (1971), 195–196.
50. V. M. Buhštaber, Classification of two-valued formal groups, *Uspehi Mat. Nauk* **28** (1974), 173–174.
51. V. M. Buhštaber, New Methods in cobordism theory (Russian), Appendix in the Russian translation of R. E. Stong: "Notes on Cobordism Theory," Mir, 1973.
52. V. M. Buhštaber, Two valued formal groups. Algebraic theory and applications to cobordism I (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **39** (1975), 1044–1064.
53. V. M. Buhštaber, Two valued formal groups. Algebraic theory and applications to cobordism II (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **40** (1976), 289–325.
54. V. M. Buhštaber, Cobordism in algebraic topology. Survey 1965–1975, *in* "Algebra, Topology and Geometry" (Russian) (R. V. Gamhrelidze, ed.), Vol. 13. Itogi Nauki i Tech., 1975. (B.4.7)
55. V. M. Buhštaber and A. S. Miščenko, K-theory on the category of infinite cell complexes, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), 560–604 (*English transl.: Math. USSR Izv.* **2** (1968), 515–556).
56. V. M. Buhštaber and A. S. Miščenko, Remark on the paper "K-theory on the category of infinite cell complexes," *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 239 (*English transl.: Math. USSR Izv.* **3** (1969), 227–228).
57. V. M. Buhštaber, A. S. Miščenko, and S. P. Novikov, Formal groups and their role in the apparatus of algebraic topology, *Usp. Mat. Nauk* **26** (1971), 131–154. (E.5.3, B.4.7)
58. V. M. Buhštaber and S. P. Novikov, Formal groups, power systems and Adams operations, *Mat. Sb.* **84** (1971), 81–118. (E.5.3, B.4.7, E.1.3)
59. S. Bullett, A $\mathbf{Z}/(p)$ Analogue for Unoriented Bordism, Ph.D. Thesis, Univ. of Warwick, 1973.
60. S. Bullett, $\mathbf{Z}/p$ bordism, *Math. Z.* **141** (1975), 9–24. (B.4.7)
61. P. Cartier, Calcul différentiel sur les variétés algébriques en caractéristique non nulle, *C.R. Acad. Sci. Paris* **235** (1957), 1109–1111.
62. P. Cartier, Théorie différentielle des groupes algébriques, *C.R. Acad. Sci. Paris* **244** (1957), 540–542.
63. P. Cartier, Groupes algébriques et groupes formels. Dualité, Coll. sur la théorie des groupes algébriques, Bruxelles, 1962, CBRM, 87–112. (E.5.2)
64. P. Cartier, Groupes formels associés aux anneaux de Witt généralisés, *C.R. Acad. Sci. Paris* **265** (1967), A50–52. (E.2.4, 15.3, E.5.2)
65. P. Cartier, Modules associés à un groupe formel commutatif. Courbes typiques, *C.R. Acad. Sci. Paris* **265** (1967), A129–132. (E.4.3, E.2.3)
66. P. Cartier, Relèvement des groupes formels commutatifs, Sém. Bourbaki, 1968/1969, Exp. 359. *Lect. Notes Math.* **179** (1971). (26.5.10)
67. P. Cartier, Groupes formels, fonctions automorphes et fonctions zéta des courbes elliptiques, *Actes Congr. Int. Math. Nice, 1970*, Vol. 2, pp. 291–299, Gauthiers-Villars, 1971. (E.5.2)
68. P. Cartier, Seminaire sur les groupes formels, IHES 1972 (Unpublished Notes). (E.1.8, E.1.2, E.2.4, E.4.6)
69. P. Cartier, Groupes formels, Lecture notes, Strassbourg. (E.1.5)
70. P. Cartier, Anneaux de Witt, preprint of chapter I of .... (E.2.4, E.6.2)
71. P. Cartier, Problems and directions in mathematics, Preprint, 1975. (B.4.1)
72. P. Cartier, Groupes de Lubin–Tate généralisés, *Inv. Math.* **35** (1976), 273–284. (E.4.6, E.1.8, E.1.2)

73. J. W. S. Cassels and A. Fröhlich (eds.), "Algebraic Number Theory." Academic Press, New York, 1967. (23.1.4)
74. I. V. Čerednik, On a problem concerning the Šafarevič map, *Mat. Sb.* **90** (1973), 231–234. (E.5.1)
75. C. Chevalley, "Théorie des Groupes de Lie," Tome II, Groupes algébriques. Hermann, Paris, 1971. (E.1.1)
76. C. Chevalley, Classification des groupes de Lie algébriques, Sém. C. Chevalley 1956–1958. Secr. Math., Paris, 1958.
77. F. Clarke, On the determination of $K_*(K)$ using the Conner–Floyd isomorphism, preprint. (B.4.2)
78. J. M. Cohen, The Hurewicz homomorphism on MU, *Inv. Math.* **10** (1970), 177–186.
79. I. G. Connell, Abelian formal groups, *Proc. Amer. Math. Soc.* **17** (1966), 958–959. (E.1.5, E.1.1)
80. P. E. Conner, Lectures on the action of a finite group, *Lect. Notes Math.* **34** (1967).
81. P. E. Conner and E. E. Floyd, Periodic maps which preserve a complex structure, *Bull. Amer. Math. Soc.* **70** (1964), 574–579.
82. P. E. Conner and E. E. Floyd, "Differentiable Periodic Maps." Springer-Verlag, Berlin and New York, 1964.
83. P. E. Conner and E. E. Floyd, The relation of cobordism to K-theories, Lect. Notes Math. Vol. 28. Springer-Verlag, Berlin and New York, 1966.
84. P. E. Conner and E. E. Floyd, Maps of odd period, *Ann. Math.* **84** (1966), 132–156.
85. P. E. Conner and L. Smith, On the complex bordism of finite complexes, *Publ. Math. IHES* **37** (1969), 117–221.
86. P. E. Conner and L. Smith, Homological dimension of complex bordism modules, "Topological Manifolds," pp. 472–482. Markham, 1970.
87. P. E. Conner and L. Smith, On generators for complex bordism modules, *Inv. Math.* **10** (1970), 199–204.
88. P. E. Conner and L. Smith, On the complex bordism of complexes with few cells, *J. Math. Kyoto Univ.* **11** (1971), 315–356.
89. P. E. Conner and L. Smith, On the complex bordism of finite complexes II, *J. Differential Geometry* **6** (1971), 135–174.
90. L. Cox, Formal A-modules, *Bull. Amer. Math. Soc.* **79** (1973), 690–694.
91. L. Cox, Formal A-modules over p-adic integer rings, *Compositio Math.* **29** (1974), 287–308. (E.3.7, E.3.6, E.3.4)
92. J. Damon, The Gysin homomorphism for flag bundles, *Amer. J. Math.* **95** (1973), 643–659.
93. J. Damon, The Gysin homomorphism for flag bundles, applications, *Amer. J. Math.* **96** (1974), 248–260.
94. M. Demazure, p-divisible groupes, Lect. Notes Math. Vol. 302. Springer-Verlag, Berlin and New York, 1972. (E.4.1, B.2.1)
95. M. Demazure and P. Gabriel, "Groupes Algébriques," Vol. I. North-Holland Publ., Amsterdam, 1971. (E.4.1, E.2.2)
96. P. K. Dennis and M. R. Stein, K_2 of discrete valuation rings, *Advances in Math.* **18** (1975), 182–238. (B.2.3)
97. M. Deuring, "Algebren." Springer-Verlag, Berlin and New York, 1935. (35.5.9)
98. M. Deuring, Die typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg* **14** (1941), 197–272.
99. J. Dieudonné, Le calcul différentiel dans les corps de caractéristique $p > 0$, *Proc. Int. Congr. Math., Amsterdam*, Vol. 1, 240–252. (E.1.1, E.6.1, 38.2.14)
100. J. Dieudonné, Sur quelques groupes de Lie abéliens sur un corps de caractéristique $p > 0$, *Arch. Math. (Basel)* **5** (1954), 274–281. Corrections, *Ibid.* **6** (1955), 88. (E.1.1, E.6.1)
101. J. Dieudonné, Sur les groupes de Lie algébriques sur un corps de caractéristique $p > 0$, *Rend. Circ. Mat. Palermo* **1** (1952), 380–402. (E.1.1, E.6.1)

102. J. Dieudonné, Groupes de Lie et hyperalgèbres sur un corps de caractéristique $p > 0$ (I), *Comm. Math. Helv.* **28** (1954), 87–117. (E.1.1, E.6.1)
103. J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (II), *Amer. J. Math.* **77** (1955), 218–244. (E.1.1, E.6.1)
104. J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (III), *Math. Z.* **63** (1955), 53–75. (E.1.1, E.6.1)
105. J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (IV), *Amer. J. Math.* (1955), 429–452. (E.1.1, E.6.1)
106. J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (V), *Bull. Soc. Math. France* **84** (1956), 207–239. (E.1.1, E.5.5, E.6.1, 38.4.7)
107. J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VI), *Amer. J. Math.* **79** (1957), 331–388. (E.4.7, E.1.1, E.6.1)
108. J. Dieudonné, Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$ (VII), *Math. Ann.* **134** (1957), 114–133. (26.4.3, E.3.3, E.1.1, E.6.1)
109. J. Dieudonné, Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VIII), *Amer. J. Math.* **80** (1958), 740–772. (E.1.1, E.6.1)
110. J. Dieudonné, Witt groups and hyperexponential groups, *Matematica* **2** (1955), 21–31. (E.1.1, E.6.2, E.6.1)
111. J. Dieudonné, Sur les groupes formels abéliens unipotents, *Rend. Circ. Mat. Palermo* **5** (1956), 170–180. (E.1.1, E.6.1)
112. J. Dieudonné, On a theorem of Lazard, *Amer. J. Math.* **78** (1956), 675–676. (E.1.5, E.1.1)
113. J. Dieudonné, On the Artin-Hasse exponential series, *Proc. Amer. Math. Soc.* **8** (1957), 210–214. (E.1.2, E.1.1, 2.3.3, E.2.4, E.6.1)
114. J. Dieudonné, "Introduction to the Theory of Formal Groups." Dekker, New York, 1973. (E.1.1, E.5.1)
115. E. J. Ditters, Curves and Exponential Series in the Theory of Noncommutative Formal Groups, Thesis, Univ. of Nijmegen, 1969.
116. E. J. Ditters, Sur une série exponentielle noncommutative définie sur les corps de caractéristique p, *C.R. Acad. Sci. Paris* **268** (1969), 580–582.
117. E. J. Ditters, On the structure of $P(\mathbf{Z}(\mathbf{Z}))$, Mimeographed notes, Nijmegen (1971).
118. E. J. Ditters, Curves and formal (co)groups, *Inv. Math.* **17** (1972), 1–20. (E.5.5, E.5.1)
119. E. J. Ditters, Groupes formels à un paramètre sur $\mathbf{Z}$ et $\mathbf{Z}_p$, *C.R. Acad. Sci. Paris* **275** (1972), A251–254.
120. E. J. Ditters, Fonctions lexoides et produits Euleriens, *C.R. Acad. Sci. Paris* **276** (1973), 531–534.
121. E. J. Ditters, Sur la théorie des composantes fantômes, Application aux schémas de Greenberg, *C.R. Acad. Sci. Paris Ser. A* **279** (1974), 403–406.
122. E. J. Ditters, Decomposition du groupe des puissances divisées sur un anneau de base arbitraire. Théorème de base pour le group universel de Lazard, *C.R. Acad. Sci. Paris Ser. A* **279** (1974), 443–446.
123. E. J. Ditters, Groupes formels, Cours 3^e cycle 73/74, *Univ. Paris, 11th, Orsay*, pp. 149–75.42 (1975). (E.5.5, E.5.1, 38.4.7, E.4.3, 38.4.5)
124. E. J. Ditters, Formale Gruppen, die Vermutungen von Atkin-Swinnerton Dyer und verzweigte Witt Vektoren, Lect. Notes, Göttingen, 1975. (E.3.8, E.6.1)
125. E. J. Ditters, On the Classification of n-dimensional Commutative Formal Groups over Integrity Domains of Characteristic Zero, preprint, Univ. of Nijmegen, 1976. (E.4.3)
126. E. J. Ditters, Sur le developement p-adique de la trace de Frobenius d'une courbe elliptique en fonction de son module de Legendre, *C.R. Acad. Sci. Paris Ser. A* **282** (1976), 849–851. (E.5.2)
127. E. J. Ditters, Sur les congruences d'Atkin et de Swinnerton-Dyer, *C.R. Acad. Sci. Paris Ser. A* **282** (1976), 1131–1134. (E.5.2)
128. E. J. Ditters, On the Congruences of Atkin and Swinnerton-Dyer, Univ. of Nijmegen, Preprint, 1976. (E.5.2)

129. E. J. Ditters, Formal Group Laws and Abelian Varieties, preprint, Univ. of Nijmegen, 1976. (E.5.2)
130. E. J. Ditters, On the Characteristic Polynomial of One Parameter Formal Group Laws over Finite Fields, preprint, Univ. of Nijmegen, 1976.
131. A. Dold, Structure de l'anneau de cobordisme, *Sém. Bourbaki* (1959/1960).
132. A. Dold, Relations between ordinary and extraordinary cohomology, Coll. Algebraic Topology, Aarhus Univ., pp. 2–9 (1962).
133. A. Dold, Chern classes in general cohomology, *Symp. Mat. INDAM* **5**, 385–410. Academic Press, New York. (34.1.3, 31.1.1)
134. V. G. Drinfel'd, Elliptic modules, *Mat. Sb.* **94** (1974), 594–624 (*English transl.: Math. USSR Sb.* **23** (1974), 561–592). (E.4.5, B.1.1, E.3.4)
135. V. G. Drinfel'd, Coverings of p-adic symmetric domains (Russian), *Funk. Anal. i ego Priloz.* **10** (1976), 29–40. (B.3.4, B.2.2, E.3.8)
136. B. A. Dubrovin, Generalized Witt groups, *Mat. Zametki* **13** (1973), 419–426. (E.2.3)
137. B. Dwork, Norm residue symbol in local number fields, *Abh. Math. Sem. Univ. Hamburg* **22** (1958), 180–190. (E.5.1, E.1.2, E.2.4, 2.3.4)
138. B. Dwork, p-adic cycles, *Publ. Math. IHES* **37** (1970), 327–415. (B.3.1)
139. B. T. Flynn, The complex bordism of the cyclic groups, *Osaka J. Math.* **11** (1974), 503–516. (B.4.7)
140. J. M. Fontaine, Points d'ordre fini d'un groupe formel sur une extension non-ramifié de $\mathbf{Z}_p$, Journées Arithmétiques Grenoble, *Bull. Soc. Math. France memoire* 37 (1973), 75–79. (E.5.4)
141. J. M. Fontaine, Groupes finis commutatifs sur les vecteurs de Witt, *C.R. Acad. Sci. Paris Ser. A* **280** (1975), 1423–1425. (E.3.3, E.4.6)
142. J. M. Fontaine, Groupes p-divisibles sur les vecteurs de Witt, *C.R. Acad. Sci. Paris Ser. A* **280** (1975), 1353–1356. (E.3.3, E.4.6)
143. J. M. Fontaine, Sur la construction du module de Dieudonné d'un groupe formel, *C.R. Acad. Sci. Paris Ser. A* **280** (1975), 1273–1276. (E.3.3, E.4.6)
144. A. Fröhlich, Formal groups. Lecture Notes Math. Vol. 74. Springer-Verlag, Berlin and New York, 1968. (E.3.3, E.3.1, E.1.9, E.1.3, E.5.4, B.1.2, E.3.7, B.3.3)
145. P. Gabriel, Etude infinitésimale des schémas en groupe et groupes formels; Groupes formels. Exposés VII A, B dans A. Grothendieck, M. Demazure (eds.), Schémas en groupes I: Propriétés générales des schémas en groupes. Lect. Notes Math. Vol. 151. Springer-Verlag, Berlin and New York, 1970. (E.6.2, E.6.1)
146. H. Gaudier, Schémas en anneaux affines, *C.R. Acad. Sci. Paris Ser. A* **273** (1971), 768–771.
147. H. Gaudier, Sur les W_k-bimodules et les k-anneaux connexes, *C.R. Acad. Sci. Paris Ser. A* **275** (1972), 61–64.
148. G. Gemignani, Iperalgebra e gruppi analitici commutativi, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **20** (1966), 453–497.
149. M. M. Glazunov, The norm subgroups of one dimensional formal groups that are defined over the ring of integers of a local field (Ukrainian), *Dopovidi Akad. Nauk Ukrain. RSR Ser. A* (1973), 965–968. (B.3.2)
150. N. M. Glazunov, On n-dimensional commutative formal groups over the ring of integers of a field of p-adic numbers, *Ukrain. Mat. Ž.* **25** (1973), 352–355.
151. V. L. Golo, Adams operations and the norm residue symbol, *Mat. Zametki* **12** (1972), 433–441. (B.4.1)
152. A. Grothendieck, La théorie des classes de Chern, *Bull. Soc. Math. France* **86** (1958), 137–154. (E.2.1)
153. A. Grothendieck, Catégories fibrés et descente, *Sem. Géomet. Algéb.* **1** (1960/1961), exposé VI. (E.3.1)
154. A. Grothendieck, Classes de faisceaux et théorème de Riemann–Roch, Appendix 0, *Sem. Géom. Alg. du Bois Marie 6*, Lect. Notes Math. Vol. 225. Springer-Verlag, Berlin and New York, 1972. (E.2.1)

155. A. Grothendieck, Groupes de Barsotti-Tate et cristaux. *Actes du Congr. Int. Math., Nice, 1970*, 1, 431–436. Gauthier-Villars, Paris, 1971. (B.2.3)
156. A. Grothendieck, Biextensions de faisceaux de groupes; Complements sur les biextensions; Modèles de Néron et monodromie, Exposés 7-9, *Sém. Géomet. Algéb. Bois-Marie* 7, Lect. Notes Math. Vol. 288, pp. 133–523. Springer-Verlag, Berlin and New York, 1972. (B.2.2)
157. A. Grothendieck, "Groupes de Barsotti-Tate et Cristaux de Dieudonné." Presses de l'Univ., Montreál, 1974. (B.2.3)
158. S. M. Gusein-Zade, I. M. Kričever, On formulas for fixed points under $\mathbf{Z}_p$ actions, *Uspehi Mat. Nauk* **28** (1973), 237–238.
159. I. Hansen and D. C. Johnson, The primitive elements in $MU_* K(\mathbf{Z}/p, 1)$, *Math. Z.* **148** (1976), 169–175.
160. I. Hansen and L. Smith, Cohomology operations, the Todd Polynomial and the Wu Class, Mat. Inst. Aarhus, Preprint, 1973.
161. I. Hansen and L. Smith, Invariant ideals in BP_* and Hattori-Stong Theorems, preprint. (B.4.3)
162. H. Hasse, Die Gruppe der p^n-primären Zahlen für ein Primteiler von p, *J. Reine Angew. Math.* **176** (1936), 174–183. (2.3.1, 15.3.12)
163. A. Hattori, Integral characteristic numbers for weakly almost complex manifolds, *Topology* **5** (1966), 259–280.
164. D. R. Hayes, Explicit Class Field Theory in Global Function Fields, Preprint, Univ. of Mass., Amherst, 1975. (B.1.1)
165. M. Hazewinkel, Norm maps for formal groups I: the cyclotomic Γ-extension, *J. Algebra* **32** (1974), 89–108. (B.3.2)
166. M. Hazewinkel, Norm maps for formal groups II: Γ-extensions of local fields with algebraically closed residue field, *J. Reine Angew. Math.* **268/269** (1974), 222–250. (B.3.2)
167. M. Hazewinkel, Norm maps for formal groups III, *Duke Math. J.* **44** (1977), 305–314. (B.3.2)
168. M. Hazewinkel, Norm maps for formal groups IV (to appear *Michigan Math. J.*; preliminary version: Report 7506, Econometric Inst., Erasmus Univ. of Rotterdam, 1975). (B.3.2)
169. M. Hazewinkel, Local class field theory is easy, *Advances in Math.* **18** (1975), 148–181. (E.5.1)
170. M. Hazewinkel, Constructing Formal groups I: the local one dimensional case, *J. Pure Appl. Algebra* **9**, 2 (1977), 131–150. (E.3.2, E.1.2, E.1.3)
171. M. Hazewinkel, Constructing formal groups II: the global one dimensional case, *J. Pure Appl. Algebra* **9**, 2 (1977), 151–162. (E.5.3, E.1.2, E.1.3)
172. M. Hazewinkel, Constructing formal groups III: applications to complex cobordism and Brown–Peterson cohomology, *J. Pure Appl. Algebra* **10**, 1 (1977), 1–18.
173. M. Hazewinkel, Constructing formal groups IV: more dimensional formal groups (to appear *Advances in Math.* Preliminary version: Rep. 7505, Econometric Inst., Erasmus Univ., Rotterdam, 1975). (E.3.2, E.1.7, E.1.3, E.1.2)
174. M. Hazewinkel, Constructing formal groups V: the Lubin–Tate formal moduli theorem and Lazard's classification theorem for one dimensional formal groups over an algebraically closed field (Preliminary version: Rep. 7514, Econometric Inst., Erasmus Univ., Rotterdam; *Adv. Math.*, to appear). (E.3.5, E.3.2)
175. M. Hazewinkel, Constructing formal groups VI: Cartier's third theorem and intertwined pairs of functions (Preliminary version: Rep. 7519, Econometric Inst., Erasmus Univ., Rotterdam, 1975; *Adv. Math.*, to appear).
176. M. Hazewinkel, Constructing formal groups VII: examples and complements (Preliminary version: Rep. 7201, 7207, 7322, Econometric Inst., Erasmus Univ., Rotterdam, 1972, 1973; *Adv. Math.*, to appear). (E.4.3, E.3.6, E.3.3)
177. M. Hazewinkel, Constructing formal groups VIII: formal A-modules (Preliminary version: Rep. 7507, Econometric Inst., Erasmus Univ., Rotterdam, 1975). (E.3.6, E.3.5, E.3.4)
178. M. Hazewinkel, A universal formal group and complex cobordism, *Bull. Amer. Math. Soc.* **81** (1975), 930–933. (E.5.3, E.1.3)

179. M. Hazewinkel, Isomorphisms of p-typical formal groups and operations in Brown–Peterson cohomology, *Indag. Math.* **38** (1976), 195–199. (E.5.3, E.3.2)
180. M. Hazewinkel, Une theorie de Cartier–Dieudonné pour les A-modules formels, *C.R. Acad. Sci. Paris* **284** (1977), 655–657. (E.4.5)
181. M. Hazewinkel, Twisted Lubin–Tate formal group laws, ramified Witt vectors and Artin–Hasse exponential mappings, *Trans. Amer. Math. Soc.* (submitted). (E.3.8)
182. M. Hazewinkel, "Tapis de Cartier" pour les A-modules formels, *C.R. Acad. Sci. Paris* **284** (1977), 739–740. (E.4.6)
183. M. Hazewinkel, Three research announcements on formal A-modules, Rep. 7624/M, Econometric Inst., Erasmus Univ., Rotterdam, 1976. (E.3.8)
184. M. Hazewinkel, On Infinite Dimensional Formal A-modules and Formal Group Laws, Preprint 1977. (29.2.1, 29.1.6)
185. M. Hazewinkel, Twisted Formal A-modules, Preprint 1977. (25.9.2)
186. W. Hill, Formal groups and zeta-functions of elliptic curves. *Inv. Math.* **12** (1971), 321–336. (E.5.2, E.3.7, E.3.5)
187. Y. Hirashima, On the BP_*-Hopf invariant, *Osaka J. Math.* **12** (1975), 187–196.
188. T. Honda, Formal groups and zeta functions, *Osaka J. Math.* **5** (1968), 199–213. (B.3.1, E.3.5, E.1.5, E.1.2, E.5.2)
189. T. Honda, On the theory of commutative formal groups, *J. Math. Soc. Japan* **22** (1970), 213–246. (E.3.4, E.3.3, 20.3, E.1.8, E.1.5, E.1.2, B.3.1)
190. T. Honda, Differential equations and formal groups, *U.S.–Japan Seminar Mod. Methods Number Theory, Tokyo, 1971.* (B.3.1)
191. T. Honda, Formal groups obtained from generalized hypergeometric functions, *Osaka J. Math.* **9** (1972), 447–462. (B.3.1)
192. T. Honda, Invariant differentials and L-functions. Reciprocity law for quadratic fields and elliptic curves over **Q**, *Rend. Sem. Math. Univ. Padova* **49** (1973), 323–335. (B.3.1, B.1.2)
193. T. Honda, On the formal structure of the Jacobian variety of the Fermat curve over a p-adic integer ring, *Symp. Math. INDAM* **11** (1973), 271–284. Academic Press, New York, 1974. (B.3.1)
194. D. Husemoller, "Fibre Bundles." McGraw-Hill, New York, 1966. (E.6.1)
195. D. Husemoller, The structure of the Hopf algebra $H_*(BU)$ over a $\mathbf{Z}_{(p)}$-algebra, *Amer. J. Math.* **93** (1971), 329–349. (E.6.4, E.6.3, E.6.1)
196. D. Husemoller and J. C. Moore, Algebras coalgebras and Hopf algebras, *J. Pure Appl. Algebra* (to appear). (E.6.2)
197. T. Ibukiyami, Formal groups and L-functions, *J. Fac. Sci. Univ. Tokyo Sect. 1A Math.* **21** (1974), 249–262. (B.3.1)
198. L. Illusie, Report on Cristalline cohomology, *in* "Algebraic Geometry" (R. Hartsbone, ed.) Proc. Symp. Pure Math., Vol. 29. Amer. Math. Soc., New York, 1975. (B.2.3)
199. L. Illusie, Complexes de Rham–Witt et cohomologie cristalline, Notes d'un cours à Orsay, printemps, 1976. (B.2.3)
200. H. Imai, A remark on the rational points of abelian varieties with values in cyclotomic $\mathbf{Z}_p$-extensions, *Proc. Japan Acad.* **51** (1975), 12–16. (B.3.2)
201. K. Iwasawa, On Γ-extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.
202. K. Iwasawa, On $\mathbf{Z}_p$-extensions of algebraic number fields, *Ann. Math.* **98** (1973), 246–326.
203. S. Jackowski, R. Rubinsztein, and A. Jankowski, *Proc. Algebraic Topology Summer School, 6th, Gdansk* (1973). (34.1.3, E.5.3, B.4.2, E.2.3)
204. N. Jacobson, The theory of rings, *Math. Surveys* **2** (1943). (35.5.9, E.4.4, 28.4.5)
205. N. Jacobson, "Lectures in Abstract Algebra," 3 vols. van Nostrand-Reinhold, Princeton, New Jersey, 1951, 1953, 1964. (35.2.8, 24.1.3)
206. A. Jankowski, Algebras of the cohomology operations in some cohomology theories, *Dissertationes Math.* **110**, PWN (1974).

207. D. C. Johnson, A Stong-Hattori spectral sequence, *Trans. Amer. Math. Soc.* **179** (1973), 211-225.
208. D. C. Johnson, Skeleta of complexes with low MU_* projective dimension, *Proc. Amer. Math. Soc.* **32** (1973), 599-604.
209. D. C. Johnson, On the reduction of complex bordism to unoriented bordism, *Proc. Amer. Math. Soc.* **39** (1973), 417-420.
210. D. C. Johnson and W. S. Wilson, *BP*-operations and Morava's extraordinary *K*-theories, *Math. Z.* **144** (1975), 55-57. (34.5.7, B.4.1)
211. D. C. Johnson, An infinite complex and the spectral sequences for complex cobordism and *K*-theory, *Proc. Amer. Math. Soc.* **44** (1974), 231-234.
212. D. C. Johnson, H. R. Miller, W. S. Wilson, and R. S. Zahler, Boundary homomorphisms in the generalized Adams spectral sequence and the non-triviality of infinitely many γ_t in stable homotopy, *in* "Reunion Sobre Teoria de Homotopia" (D. Davis, ed.). Northwestern Univ., 1974; *Soc. Mat. Mexicana* (1975), 47-59. (B.4.4)
213. D. C. Johnson and W. S. Wilson, Projective dimension and Brown-Peterson homology, *Topology* **12** (1973), 327-353. (E.5.3, B.4.3)
214. M. Kamata, On the ring structure of $U_*(BU(1))$, *Osaka J. Math.* **7** (1970), 417-422. (B.4.7)
215. M. Kamata, The structure of the bordism group $U_*(BZ/p)$, *Osaka J. Math.* **7** (1970), 409-416. (B.4.7)
216. M. Kamata, Notes on the cobordism groups $U(L(m))$, *Osaka J. Math.* **9** (1972), 287-292. (B.4.7)
217. M. Kamata and M. Minami, Bordism groups of dihedral groups, *J. Math. Soc. Japan* **25** (1973), 334-341. (B.4.7)
218. M. Karoubi, Cobordism et groupes formels, Sém. Bourbaki 1971/72, Exposé 408, Lecture Notes Math. Vol. 317. Springer-Verlag, Berlin and New York, 1973.
219 G. G. Kasparov, Invariants of the classical lens spaces in cobordism theory (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 735-747 (*English transl.: Math. USSR-Izv.* **3** (1969), 695-705).
220. N. Katz, Nilpotent connections and the monodromy theorem: applications of a result of Turrittin, *Publ. Math. IHES* **39** (1970), 175-232. (B.3.1)
221. N. Katz, Travaux de Dwork, Sem. Bourbaki, 1971/1972 exposé 409, Lectures Notes Math. Vol. 417. Springer-Verlag, Berlin and New York, 1973. (B.2.3)
222. A. N. Kirillov, Commutative formal groups (Russian), *Zap. Naucn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* **57** (1976), 117-124. (E.4.3)
223. M. A. Knus and M. Ojanguren, Théorie de la descente et algèbres d'Azumaya, Lecture Notes Math. Vol. 389. Springer-Verlag, Berlin and New York, 1974. (E.3.1)
224. D. Knutson, λ-rings and the representation theory of the symmetric group, Lecture Notes Math. Vol. 308. Springer-Verlag, Berlin and New York, 1973. (E.2.2, E.2.1, 17.2.10, E.5.3)
225. H. Koch, Klassifikation der eindimensionalen formalen Gruppen über endlichen Körpern, *Math. Nachr.* **54** (1972), 278-283. (E.3.7)
226. H. Koch, Verallgemeinerung einer Konstruktion von Lubin-Tate in der theorie der Barsotti-Tate Gruppen, *Symp. Math. INDAM* **15**, 487-498. Academic Press, New York, 1973. (B.2.1, E.1.8)
227. S. O. Kochman, Homology of the classical groups over the Dyer-Lashof algebra, *Trans. Amer. Math. Soc.* **85** (1973), 83-136.
228. G. T. Konovalov, On a more dimensional Šafarevič-Serre theorem (Russian), *Mat. Zametki* **13** (1973), 573-576 (*English transl.: Math. Notes USSR* **13** (1973), 346-348). (B.2.3)
229. G. T. Konovalov, On universal norms of formal groups, *Ukrain. Mat. Z.* **27** (1975), 97-100. (B.2.3)
230. G. T. Konovalov, Triviality of universal norms for formal groups over local fields, *Mat. Zametki* **18** (1975), 711-717. (B.2.3)
231. I. Kozma, Witt vectors and complex cobordism, *Topology* **13** (1974), 389-394. (E.5.3)

232. I. Kozma, Generators for $\pi_*(MU)$, *Math. Proc. Cambridge Philos. Soc.* **78** (1975), 321-322. (E.5.3)
233. D. Kraines, Approximations to self dual Hopf algebras, *Amer. J. Math.* **94** (1972), 963-973.
234. D. Kraines, The $\mathfrak{A}(p)$ cohomology of some k-stage Postnikov systems, *Comm. Math. Helv.* **48** (1973), 56-71.
235. D. Kraines, Twisted multiplications on generalized Eilenberg-MacLane spaces, *Math. Scand.* **32** (1973), 273-285.
236. I. M. Kričever, Formal groups and the Atiyah-Hirzebruch formula, *Izv. Akad. Nauk SSSR Ser. Mat.* **38** (1974), 1289-1304. (B.4.7)
237. I. M. Kričever, Equivariant Hirzebruch genus. The Atiyah-Hirzebruch formula, *Uspehi Mat. Nauk* **30** (1975), 1, 243-244. (B.4.7)
238. P. F. Kurčanov, Elliptic curves of infinite rank over Γ-extensions, *Mat. Sb.* **90** (1973), 320-324 (Russian). (B.3.2)
239. P. F. Kurčanov, The rank of elliptic curves over Γ-extensions (Russian), *Mat. Sb.* **93** (1974), 460-466. (B.3.2)
240. P. S. Landweber, Cobordism operations and Hopf algebras, *Trans. Amer. Math. Soc.* **129** (1967), 94-110.
241. P. S. Landweber, Cobordism and classifying spaces, *Proc. Symp. Pure Math.* **22** (1971), 125-129.
242. P. S. Landweber, Associated prime ideals and Hopf algebras, *J. Pure Appl. Algebra* **3** (1973), 43-58. (B.4.3)
243. P. S. Landweber, Annihilator ideals and primitive elements in complex bordism. *Illinois J. Math.* **17** (1973), 273-284. (B.4.3)
244. P. S. Landweber, Unique factorization in graded power series rings, *Proc. Amer. Math. Soc.* **42** (1974), 73-76. (B.4.3)
245. P. S. Landweber, On Panov's theorem, *Proc. Amer. Math. Soc.* **43** (1974), 209-213. (B.4.3)
246. P. S. Landweber, $BP_*(BP)$ and typical formal groups, *Osaka J. Math.* **12** (1975), 357-363. (B.4.3, B.4.5)
247. P. S. Landweber, Invariant ideals in Brown-Peterson homology, *Duke Math. J.* **42** (1975), 499-506. (B.4.3)
248. P. S. Landweber, Homological properties of comodules over $MU_*(MU)$ and $BP_*(BP)$, *Amer. J. Math.* **98**, 3 (1976), 591-610. (B.4.3, B.4.1)
249. S. Lang, "Rapport sur la Cohomologie des Groupes." Benjamin, New York, 1966.
250. M. Lazard, La non-existence des groupes de Lie formels non abéliens à un paramètre, *C.R. Acad. Sci. Paris* **239** (1954), 942-945. (E.1.5, E.1.1)
251. M. Lazard, Sur les groupes de Lie formels à un paramètre, *Bull. Soc. Math. France* **83** (1955), 251-274. (E.3.2, E.1.1, E.1.10)
252. M. Lazard, Lois de groupes et analyseurs, *Ann. Ecole Norm. Sup.* **72** (1955), 299-400. (E.1.3, E.1.1)
253. M. Lazard, Groupes analytiques p-adiques, *Publ. Math. IHES* **26** (1965).
254. M. Lazard, Sur les théorèmes fondamentaux des groupes formels commutatifs, *Indag. Math.* **35** (1973), 281-300, Errata et addenda, *Ibid.* **36** (1974), 122-124. (E.4.3, E.1.7, E.1.3)
255. M. Lazard, Analyseurs, *Bull. Unione Mat. Ital. Suppl. 2* **9** (1974), 49-59. (E.1.3)
256. M. Lazard, Commutative formal groups. Lecture Notes Math. Vol. 443. Springer-Verlag, Berlin and New York, 1975. (E.4.3, 27.1.19, E.1.3, E.2.4, E.4.6, E.4.4)
257. J. Y. Lefebvre, Sur les Lois de Groupes Formelles, Thèse, Univ. de Montpellier (1970). (E.1.4)
258. H. W. Lenstra, Jr. and F. Oort, Simple abelian varieties having a prescribed formal isogeny type, *J. Pure Appl. Algebra* **4** (1974), 47-53.
259. A. Liulevicius, On the algebra $BP_*(BP)$, *Symp. Algeb. Topology*, pp. 47-53, Lecture Notes Math. Vol. 249. Springer-Verlag, Berlin and New York, 1972. (E.5.3)

260. J. L. Loday, Structures multiplicatives on K-théorie, *C.R. Acad. Sci. Paris Ser. A* **274** (1972), 884–887.
261. J. L. Loday, K-théorie algébrique et représentation de groupes, *Ann. Ecole Norm. Sup.* **9** (1976), 309–377. (B.2.3)
262. J. Lubin, J. P. Serre, and J. Tate, Elliptic curves and formal groups, Woods Hole Summer Inst. (Mimeographed notes) (1964).
263. J. Lubin, One parameter formal Lie groups over p-adic integer rings, *Ann. Math.* **80** (1964), 464–484; Correction, *Ibid.* **84** (1966), 372. (E.3.6, E.3.1, E.3.1)
264. J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. of Math.* **81** (1965), 380–387. (E.5.1, E.3.6, E.3.4, E.1.6)
265. J. Lubin and J. Tate, Formal moduli for one parameter formal Lie groups, *Bull. Soc. Math. France* **94** (1966), 49–60. (E.3.5)
266. J. Lubin, Finite subgroups and isogenies of one parameter formal Lie groups, *Ann. of Math.* **85** (1967), 296–302. (E.5.4, E.3.6)
267. J. Lubin, A survey of formal groups, Advanced Sci. Sem. Bowdoin College (1967). (E.5.4)
268. J. Lubin, Introduction à la théorie des groupes formels. Cours à l'Inst. Henri Poincaré 1968/1969, Secr. Math. de l'Ecole Norm. Sup. Paris (1970). (E.5.4)
269. J. Lubin, Formal A-modules defined over A, *Symp. Math. INDAM 1968/1969* Vol. 3, pp. 241–245. Academic Press, New York, 1970. (E.3.5, E.3.4)
270. J. Lubin, Determinants for one Dimensional Formal Modules, preprint, Brown Univ. (1972). (E.3.4)
271. J. Lubin, Entireness of the endomorphism rings of one dimensional formal groups, *Proc. Amer. Math. Soc.* **52** (1975), 8–10. (E.3.6)
272. S. Lubkin, Generalization of p-adic cohomology, bounded Witt vectors (Unpublished).
273. E. Lutz, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques, *J. Reine Angew. Math.* **177** (1937), 237–247.
274. Yu. I. Manin, Two dimensional abelian formal groups, *Dokl. Akad. Nauk SSSR* **143** (1962), 35–37 (*English transl.: Sov. Math. Dokl.* **3**, 335–337).
275. Yu. I. Manin, On the classification of abelian formal groups (Russian), *Dokl. Akad. Nauk SSSR* **144** (1962), 490–492 (*English transl.: Sov. Math. Dokl.* **3**, 757–759).
276. Yu. I. Manin, Commutative formal groups and abelian varieties, *Dokl. Akad. Nauk* **145** (1962), 280–283 (*English transl.: Sov. Math. Dokl.* **3**, 992–994).
277. Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Uspehi Mat. Nauk* **18** (1963); *Russ. Math. Surveys* **18** (1963), 1–84. (E.4.7, E.4.1, E.4.4, E.1.1)
278. Yu. I. Manin, Cyclotomic fields and modular curves (Russian), *Uspehi Mat. Nauk* **26** (1971), 7–71 (*English transl.: Russ. Math. Surveys* **26** (1971), 7–78). (B.3.2)
279. K. Masayoshi and T. Sugawara, A note on Landweber–Novikov operations on the complex cobordism ring U^*, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **29** (1975), 51–58.
280. B. Mazur, Arithmétique des Courbes Elliptiques sur les Corps Cyclotomiques, Mimeographed notes of a course given in Orsay (1970).
281. B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Inv. Math.* **18** (1972), 183–266. (B.3.2)
282. B. Mazur, Frobenius and the Hodge filtration, *Bull. Amer. Math. Soc.* **78** (1972), 653–667. (B.2.3)
283. B. Mazur, Frobenius and the Hodge filtration (estimates), *Ann. of Math.* **98** (1973), 58–95. (B.2.3)
284. B. Mazur, p-adic analytic number theory of elliptic curves and abelian varieties, *Proc. Int. Congr. Math., Vancouver* (1974), 369–378.
285. B. Mazur and W. Messing, Universal extensions and one dimensional crystalline cohomology, Lectures Notes Math. Vol. 370. Springer-Verlag, Berlin and New York, 1974. (B.2.3, E.4.1)
286. W. Messing, The crystals associated to Barsotti–Tate groups with applications to abelian

schemes, Lecture Notes Math. Vol. 264. Springer-Verlag, Berlin and New York, 1972. (E.4.6, B.2.2, B.2.3)
287. W. Messing, The universal extension of an abelian variety by a vector group, *Symp. Math. INDAM*, Vol. XI, 359–372. Academic Press, New York, 1973.
288. H. R. Miller, Some Algebraic Aspects of the Adams-Novikov Spectral Sequence, Thesis, Princeton Univ. (1974). (B.4.4)
289. H. R. Miller and D. C. Ravenel, Morava Stabilizer Algebras and Localization of Novikov's E_2-term, *Duke Math. J.* **44** (1977), 433–448. (B.4.4)
290. H. R. Miller, D. C. Ravenel, and W. S. Wilson, Novikov's Ext^2 and nontriviality of the gamma family, *Bull. Amer. Math. Soc.* **81** (1975), 1073–1076. (B.4.4)
291. H. R. Miller, D. C. Ravenel, and W. S. Wilson, Periodic Phenomena in the Adams-Novikov Spectral Sequence, to appear *Ann. of Math.* (B.4.4)
292. H. R. Miller and W. S. Wilson, On Novikov's Ext^1 modulo an invariant prime ideal, *Topology* **15** (1976), 131–143. (B.4.4)
293. H. R. Miller and W. S. Wilson, On Novikov's Ext^1 modulo an invariant prime ideal, *in* Reunion Sobre Teoria de Homotopia (D. Davis, ed.), Northwestern Univ., 1974; *Soc. Mat. Mexicana* (1975), 159–166. (B.4.4)
294. J. Milnor, On the cobordism ring Ω^* and a complex analogue, *Amer. J. Math.* **82** (1960), 505–521. (34.2.9)
295. J. W. Milnor and J. C. Moore, On the structure of Hopf algebras, *Ann. of Math.* **81** (1965), 211–264. (E.5.2)
296. J. W. Milnor and J. D. Stasheff, "Characteristic Classes." Princeton Univ. Press, Princeton, New Jersey, 1974. (E.5.1)
297. O. K. Mironov, Existence of multiplicative structures in cobordism theories with singularities, *Izv. Akad. Nauk SSSR Ser. Mat.* **39** (1975), 1065–1092.
298. A. S. Miščenko, Extraordinary homology theories: bordism and K-theory, *Actes Congr. Int. Math. Nice, 1970* Vol. 2, pp. 113–119. Gauthier-Villars, Paris, 1971. (B.4.7)
299. J. C. Moore, Algèbres de Hopf universelles, *Sém Cartan, 12e année* (1959/1960), exp. 10. (E.6.3)
300. J. Morava, Cobordism and K-theory, chapters I, III of a projected book. (B.4.2, B.4.1)
301. J. Morava, Structure Theorems for Cobordism Comodules, preprint. (B.4.3)
302. J. Morava, The algebra $\mathrm{Ext}^*_C(U, U)$ of Novikov, preprint. (B.4.3)
303. J. Morava, Extraordinary K-theories: Summary, preprint, Inst. for Advanced Study, Princeton, New Jersey, $\pm$1971. (B.4.1)
304. J. Morava, Unitary cobordism and extraordinary K-theories, Columbia Univ. preprint (1971). (B.4.1)
305. J. Morava, Extraordinary K-theories, preprint (1970). (B.4.1)
306. J. Morava, Forms of K-theory, preprint. (B.4.1)
307. R. A. Morris and B. Pareigis, Formal groups and Hopf algebras over discrete rings, *Trans. Amer. Math. Soc.* **197**, 113–130. (E.5.1)
308. D. Mumford, "Lectures on curves on an Algebraic Surface." Princeton Univ. Press, Princeton, New Jersey, 1966. (E.2.4, 15.3)
309. D. Mumford, Bi-extensions of formal groups, *in* "Algebraic Geometry" (*Bombay Coll., 1968*), pp. 307–322, Oxford Univ. Press, London and New York, 1969. (B.2.2)
310. D. Mumford and F. Oort, Deformations and liftings of finite commutative group schemes, *Inv. Math.* **5** (1968), 317–334.
311. A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, *Publ. Math. IHES* **21** (1964). (31.1.20, 33.1.9)
312. P. Norman, An algorithm for computing local moduli of abelian varieties, *Ann. of Math.* **101** (1975), 499–509. (E.4.6)
313. P. Norman and F. Oort, Moduli of abelian varieties, preprint. (B.2.2)

314. S. P. Novikov, Homotopy properties of Thom complexes (Russian), *Mat. Sb.* **57** (1962), 407–442. (34.2.9)
315. S. P. Novikov, The methods of algebraic topology from the viewpoint of cobordism theory, *Izv. Akad. Nauk SSSR Ser. Mat.* **31** (1967), 855–951. (E.5.3)
316. S. P. Novikov, Adams operations and fixed points, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), 1245–1263.
317. U. Oberst, Untergruppen formeller Gruppen von endlichen Index, *J. Algebra* **31** (1974), 10–44.
318. T. Oda, The first de Rham cohomology group and Dieudonné modules, *Ann. Ecole Norm. Sup.* **2** (1969), 63–125. (B.2.3)
319. S. Oka and H. Toda, Nontriviality of an element in the stable homotopy groups of spheres, *Hiroshima Math. J.* **5** (1975), 115–125. (B.4.4)
320. F. Oort, Commutative group schemes, Lecture Notes Math. Vol. 15, Springer-Verlag, Berlin and New York, 1966.
321. F. Oort, Dieudonné modules of finite local group schemes, *Indag. Math.* **36** (1974), 284–292. (E.4.1)
322. F. Oort, Isogenies of formal groups, *Indag. Math.* **37** (1975), 391–400.
323. O. Ore, Theory of noncommutative polynomials, *Ann. of Math.* **34** (1933), 480–508. (E.4.4)
324. H. Oshima and Z. J. Yosimura, Projective dimension of complex bordism modules of CW-spectra II, *Osaka J. Math.* **10** (1973), 565–570.
325. N. V. Panov, Characteristic numbers in U-theory, *Izv. Akad. Nauk SSSR Ser. Math.* **35** (1971), 1356–1376 (*English transl.: Math. USSR Izv.* **5** (1971), 1365–1385).
326. B. Pareigis, Endliche Hopf-algebren, Lect. Notes Math. Inst., Univ. München (1973).
327. A. A. Peresetskii, *SU* cobordism and formal groups, *Mat. Sb.* **88** (1972), 536–545 (*English transl.: Math. USSR Sb.* **17** (1972), 529–538).
328. I. I. Piatetskii-Šapiro, Zetafunctions of modular curves, *in* "Modular Functions of One Variable II." Lecture Notes Math. Vol. 349. Springer-Verlag, Berlin and New York, 1973. (B.1.1)
329. M. Poletti, Iperalgebre su schieri valutanti, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **23** (1969), 746–770.
330. D. Quillen, On the formal group laws of unoriented and complex cobordism theory, *Bull. Amer. Math. Soc.* **75** (1969), 1293–1298. (E.5.3)
331. D. Quillen, The Adams conjecture, *Topology* **10** (1971), 1–10.
332. D. Quillen, Elementary proofs of some results of cobordism theory using Steenrod operations, *Advances in Math.* **7** (1971), 29–56. (34.1.3, 34.1.1, 34.1.11, E.5.3)
333. D. G. Quillen, The spectrum of an equivariant cohomology ring I, II, *Ann. of Math.* **94** (1971), 549–572, 573–602.
334. D. C. Ravenel, Multiplicative operations in BP^*BP, *Pacific J. Math.* **57** (1975), 539–543. (B.4.2)
335. D. C. Ravenel, The structure of the Morava Stabilizer algebras, *Inv. Math.* **37** (1976), 109–120. (B.4.4)
336. D. C. Ravenel, The structure of BP_*BP modulo an invariant prime ideal, *Topology* **15** (1976), 149–153. (B.4.4)
337. D. C. Ravenel, Dieudonné modules for abelian Hopf algebras, *in* Reunion Sobre Teoria de Homotopia (D. Davis, ed.), Northwestern Univ. (1974); *Soc. Mat. Mexicana* (1975), 177–184.
338. D. C. Ravenel, A May spectral sequence converging to the Adams–Novikov E_2-term, preprint (1976).
339. D. Ravenel and W. S. Wilson, Bipolynomial Hopf algebras, *J. Pure Appl. Algebra* **4** (1974), 45–55.
340. D. C. Ravenel and W. S. Wilson, The Hopf ring for complex cobordism, *Bull. Amer. Math. Soc.* **80**, 1185–1189 (1974). (B.4.6)

341. D. C. Ravenel and W. S. Wilson, The Hopf Ring for Complex Cobordism, *J. Pure Appl. Algebra* **9** (1977), 241–280.
342. N. Roby, Sur les lois formelles, *C.R. Acad. Sci. Paris* **255** (1962).
343. N. Roby, Lois polynomes et lois formelles en théorie des modules, *Ann. Ecole Norm. Sup.* **80** (1963), 213–348.
344. N. Roby, Les algèbres à puissances divisées, *Bull. Soc. Math. France* **89** (1965), 75–91. (E.6.5)
345. N. Roby, Sur les lois completes et les algèbres de puissances divisées, *Bull. Soc. Math. Sao Paulo* **18** (1966), 59–80.
346. Yu. B. Rudjak, Formal groups and bordism with singularities (Russian), *Mat. Sb.* **96** (1975), 523–542. (B.4.1)
347. Yu. B. Rudjak, Stable k-theory and bordism of manifolds with singularities, *Dokl. Akad. Nauk SSSR* **216** (1974), 1222–1225.
348. I. R. Šafarevič, On Galois groups of p-adic fields (Russian), *Dokl. Akad. Nauk SSSR* **53** (1946), 15–16. (32.4.1)
349. J. P. Sanders, The category of H-modules over a spectrum, Memoir 141, Amer. Math. Soc. (1974).
350. W. Schäfer, Bemerkungen zur Theorie der p-adische Lie-Gruppen von Lubin–Tate insbesondere zur Konstruktion des Logarithmus Analogon, Thesis, Karlsruhe (1971). (E.5.1)
351. H. J. Schneider, Bemerkung zu einer Arbeit von Tate–Oort, *Manuscripta Math.* **8** (1973), 319–322.
352. C. Schochet, Cobordism from an algebraic point of view, Lecture Notes *Ser.* Vol. 29. Mat. Inst., Aarhus, 1973. (B.4.7)
353. C. Schochet, On the bordism ring of complex projective space, *Proc. Amer. Math. Soc.* **37** (1973), 267–270.
354. C. Schochet, On the structure of graded formal groups of finite characteristic, *Proc. Cambridge Philos. Soc.* **73** (1973), 215–221. (E.6.2, B.4.7)
355. C. Schoeller, Groupes affines commutatifs unipotents sur un corps nonparfait, *Bull. Soc. Math. France* **100** (1972), 241–300. (E.4.1)
356. Séminaire H. Cartan, 12^e année (1959/1960). Periodicité des groupes d'homotopie stables des groupes classiques, d'après Bott, Secretariat Math. (1961). (E.5.2)
357. Séminaire "Sophus Lie," 2^e année 1955/1956, Fac. des Sciences de Paris (1957). (E.6.1, E.6.4)
358. S. Sen, Ramification in p-adic Lie extensions, *Inv. Math.* **17** (1972), 44–50. (E.5.4)
359. S. Sen, Lie algebras of Galois groups arising from Hodge–Tate modules, *Ann. of Math.* **97** (1973), 160–170. (E.5.4)
360. J. P. Serre, "Groupes Algèbriques et Corps de Classes." Hermann, Paris, 1959.
361. J. P. Serre, "Corps Locaux." Hermann, Paris, 1962. (20.2.16, E.2.4, 17.4.6, E.3.7)
362. J. P. Serre, Cohomologie galoisienne, Lecture Notes Math. Vol. 5. Springer-Verlag, Berlin and New York, 1964. (E.3.1)
363. J. P. Serre, Lie algebras and Lie groups, "Harvard Lectures 1964." Benjamin, New York, 1965. (14.1, E.1.9)
364. J. P. Serre, Courbes elliptiques et groupes formels, Annuaire Collège de France (1966). (E.5.4, E.3.7)
365. J. P. Serre, Groupes p-divisibles, Sém. Bourbaki 1966/67. Exposé 318. (B.2.2, B.2.1)
366. J. P. Serre, Commutativité des groupes formels de dimension 1, *Bull. Sci. Math.* **91** (1967), 113–115. (E.1.5)
367. J. P. Serre, Sur les groupes de Galois attachés aux groupes p-divisibles, *Proc. Conf. Local Fields* (T. A. Springer, ed.), pp. 118–131. Springer-Verlag, Berlin and New York, 1967. (E.5.4, E.4.7)
368. P. K. Sharma, Structure theory of commutative affine groups, Sém. Heidelberg–Strassbourg 1965/1966: Groupes algébriques, exposé 11. (37.2.5)
369. P. B. Shay, Mod p Wu Formulas for the Steenrod and Dyer–Lashof Algebras, Preprint, CUNY. (E.6.1)

370. P. B. Shay, Representatives for p-typical Curves, *J. of Algebra* **45** (1977), 94–101. (E.6.1)
371. P. Brian Shay, The Cohomology and Homology of *BU* Over the Steenrod and Dyer–Lashof algebras, preprint, CUNY. (E.6.1)
372. P. B. Shay, Adams' Operations as Witt Vectors, preprint. (E.6.1)
373. P. B. Shay, Bipolynomial Hopf algebras, $H^*(BSU, \mathbf{Z})$ *et al.*, *J. Pure Appl. Algebra* **9**, 2 (1977), 163–165.
374. P. B. Shay, An Obstruction Theory for Smooth Formal Group Structure, Preprint, Hunter College, CUNY. (E.6.1, 38.1.10)
375. K. Shibata, On Boardman's generating sets of the unoriented bordism ring, *Osaka J. Math.* **8** (1971), 219–232.
376. K. Shibata, A note on the formal group law of unoriented cobordism theory, *Osaka J. Math.* **10** (1973), 33–42. (B.4.7)
377. K. Shibata, Oriented and weakly complex bordism algebra of free periodic maps, *Trans. Amer. Math. Soc.* **177** (1973), 199–200.
378. K. Shibata, Oriented and weakly complex bordism of free metacyclic actions, *Osaka J. Math.* **11** (1974), 171–180.
379. K. Shibata, Sur les images des générateurs canoniques de $\pi_*(MO)$ par l'homomorphisme de Hurewicz, *C.R. Acad. Sci. Paris Ser. A* **278** (1974), 327–329. (B.4.7)
380. N. Shimada and C. M. Wu, Bordism algebras of periodic transformations, *Osaka J. Math.* **10** (1973), 25–32.
381. N. Shimada and N. Yagita, Multiplications in the complex cobordism theory with singularities. *Publ. Math. Res. Inst. Math. Sci.* **12** (1976), 259–294. (B.4.7)
382. G. Shimura, "Arithmetic Theory of Automorphic Functions." Princeton Univ. Press, Princeton, New Jersey, 1971.
383. G. Shimura and Y. Taniyama, Complex Multiplication of Abelian Varieties and its Applications to Number Theory. Math. Soc. of Japan (1961).
384. K. Shiratani, On certain formal Lie groups over p-adic integer rings, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **22** (1968), 31–42. (E.5.1)
385. K. Shiratani, On the Lubin–Tate reciprocity law, *J. Number Theory* **1** (1969), 494–499. (E.5.1)
386. K. Shiratani, Notes on isogenies of one-parameter formal Lie groups over local integer rings, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **23** (1969), 156–158. (E.5.1)
387. L. Smith, On realizing complex bordism modules, *Amer. J. Math.* **92** (1970), 793–856.
388. L. Smith, On realizing complex bordism modules II, *Amer. J. Math.* **93** (1971), 226–263.
389. L. Smith, On realizing complex bordism modules III, *Amer. J. Math.* **94** (1972), 875–890.
390. L. Smith, An application of complex cobordism to the stable homotopy groups of spheres, *Bull. Amer. Math. Soc.* **76** (1970), 601–604.
391. L. Smith, On ideals in Ω^*_U, *Pacific J. Math.* **37** (1971), 527–537.
392. L. Smith, Annihilator ideals of complex bordism classes and Toda's-sequence in the stable homotopy of spheres, *Indiana Univ. Math. J.* **20** (1971), 1119–1123.
392. L. Smith, A note on annihilator ideals of complex cobordism classes, *Pacific J. Math.* **38** (1971), 551–558.
393. L. Smith, A note on the Stong–Hattori theorem, *Illinois J. Math.* **17** (1973), 285–289.
394. L. Smith, The Todd character and the integrality theorem for the Chern character, *Illinois J. Math.* **17** (1973), 301–310.
395. L. Smith and R. Zahler, Detecting stable homotopy classes by primary *BP* cohomology operations, *Math. Z.* **129** (1972), 137–156. (B.4.4)
396. R. E. Stong, Relations among characteristic numbers I, *Topology* **4** (1965), 267–281.
397. R. E. Stong, Relations among characteristic numbers II, *Topology* **5** (1966), 133–148.
398. R. E. Stong, "Notes on Cobordism Theory." Princeton Univ. Press, Princeton, New Jersey, 1968. (34.2.9)

399. R. J. Stroeker, Elliptic Curves Defined over Imaginary Quadratic Number Fields, Thesis, Amsterdam, 1975. (21.3.3)
400. D. Sullivan, Genetics of homotopy theory and the Adams conjecture, *Ann. of Math.* **100** (1974), 1-79. (B.4.1)
401. M. E. Sweedler, "Hopf Algebras." Benjamin, New York, 1969. (37.1.5, E.5.2)
402. R. M. Switzer, "Algebraic Topology-Homotopy and Homology." Springer-Verlag, Berlin and New York, 1975.
403. J. Tate, Endomorphisms of abelian varieties over finite fields, *Inv. Math.* **2** (1966), 134-144.
404. J. Tate, p-divisible groups, *in Proc. Conf. Local Fields* (T. A. Springer, ed.), pp. 158-183. Springer-Verlag, Berlin and New York, 1967. (E.5.4, B.2.1, E.1.10)
405. R. Thom, Quelques propriétés globales des variétés différentiables, *Comment. Math. Helv.* **28** (1954), 17-86.
406. E. Thomas and R. S. Zahler, Nontriviality of the stable homotopy element γ_1, *J. Pure Appl. Algebra* **4** (1974), 189-203. (B.4.4)
407. E. Thomas and R. Zahler, Generalized higher order cohomology operations and stable homotopy groups of spheres, *Adv. Math.* (to appear). (B.4.4)
408. H. Toda, On unstable homotopy of spheres and the classical groups, *Proc. Nat. Acad. Sci. U.S.* **46** (1960), 1102-1105.
409. H. Toda, On spectra realizing exterior parts of the Steenrod algebra, *Topology* **10** (1971), 53-65.
410. H. Toda, On spectra $V(n)$, *Proc. Symp. Pure Math.* **22** (1971), 273-278.
411. H. Toda, Algebra of stable homotopy of $\mathbf{Z}_p$-spaces and applications, *J. Math. Kyoto Univ.* **11** (1971), 197-251.
412. G. H. Todorova, Formal group laws of elliptic curves over a local field (Russian), *Dokl. Akad. Nauk SSSR* **216** (1974), 1229-1232.
413. S. Togo, Note on formal Lie groups, *Amer. J. Math.* **81** (1959), 632-638. (E.4.7)
414. S. Togo, Note on formal Lie groups II, *J. Sci. Hiroshima Univ. Ser. A-I* **25** (1961), 353-356. (E.4.7)
415. T. tom Dieck, Steenrod-Operationen in Kobordism Theorien, *Math. Z.* **107** (1968), 380-401.
416. T. tom Dieck, Bordism of G-manifolds and integrality theorems, *Topology* **9** (1970), 345-358.
417. T. tom Dieck, Characteristic numbers of G-manifolds I, *Inv. Math.* **13** (1971), 213-224; II, *J. Pure Appl. Algebra* **4** (1974), 31-39.
418. T. tom Dieck, Bemerkungen über äquivariante Euler-klassen, *in Proc. Conf. Transformat. Groups 2nd*, Part I, pp. 152-162. Lecture Notes Math. Vol. 298. Springer-Verlag, Berlin and New York, 1972.
419. T. tom Dieck, Kobordismentheorie klassifizierender Räume und Transformations gruppen, *Math. Z.* **126** (1972), 31-39.
420. T. tom Dieck, Periodische Abbildungen unitärer Mannigfaltigkeiten, *Math. Z.* **126** (1972), 275-295.
421. C. Traverso, Sulla classificazione dei gruppi analitici commutativi di caratteristica positiva. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **23** (1969), 481-507.
422. C. Traverso, p-divisible groups over fields, *Symp. Math. INDAM*, Vol. XI, pp. 45-46. Academic Press, New York, 1973.
423. H. Umemura, Formal moduli for p-divisible groups, *Nagoya Math. J.* **42** (1971), 1-7. (E.4.6)
424. Yu. R. Vainberg, On the reduction of formal groups modulo a prime number (Russian), *Sibirsk. Mat. J.* **4** (1963), 1263-1270.
425. R. Vogt, Boardman's stable homotopy category, Lecture Notes Ser. 21, Mat. Inst., Aarhus, 1970.
426. O. N. Vvedenskii, Duality in elliptic curves over local fields I, II, *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 1091-1112; **30** (1966), 891-922. (B.3.2)
427. O. N. Vvedenskii, The universal norms of formal groups defined over the ring of integers of a local field, *Izv. Akad. Nauk SSSR Ser. Mat.* **37** (1973), 737-751. (B.3.2)

428. O. N. Vvedenskii, On "local class field theory" for elliptic curves, *Izv. Akad. Nauk SSSR Ser. Mat.* **37** (1973), 20–88. (B.3.2)
429. O. N. Vvedenskii, Duality in elliptic curves over a quasi local field (Russian), *Dokl. Akad. Nauk SSSR* **219** (1974), 1291–1293. (B.3.2)
430. O. N. Vvedenskii, The quasi local "class fields" of elliptic curves of type II and of certain curves of type (c) (Ukrainian), *Dopovidi Akad. Nauk Ukraïn. RSR Ser. A* (1975), 291–299. (B.3.2)
431. C. T. C. Wall, Determination of the cobordism ring, *Ann. of Math.* **72** (1960), 292–311.
432. W. C. Waterhouse, A classification of almost full formal groups, *Proc. Amer. Math. Soc.* **20** (1969), 426–428. (E.3.6)
433. W. C. Waterhouse, On p-divisible groups over complete valuation rings, *Ann. of Math.* **95** (1972), 55–65. (B.2.1, E.3.6, E.3.1)
434. W. C. Waterhouse, The heights of formal A-modules, *Proc. Amer. Math. Soc.* **46** (1974), 332–334.
435. J. H. M. Wedderburn, Noncommutative domains of integrity, *J. Reine Angew. Math.* **167** (1932), 129–141. (E.4.4)
436. A. Weil, Ueber die Bestimmung Dirichletscher Reihe durch Funktionalgleichungen, *Math. Amer.* **168** (1967), 149–156.
437. E. Weiss, "Algebraic Number Theory." McGraw-Hill, New York, 1963. (18.3.9)
438. G. Whaples, Generalized local class field theory III: Second form of the existence theorem. Structure of analytic groups, *Duke Math. J.* **21** (1954), 575–581. (17.5.1, 15.3.12)
439. G. W. Whitehead, Generalized homology theories, *Trans. Amer. Math. Soc.* **102** (1962), 227–283.
440. W. S. Wilson, The Ω-spectrum for Brown–Peterson cohomology, Part I, *Comment. Math. Helv.* **48** (1973), 45–55. (E.5.3)
441. W. S. Wilson, The Ω-spectrum for Brown–Peterson cohomology, Part II, *Amer. J. Math.* **97** (1975), 101–123. (E.5.3)
442. W. S. Wilson, The Ω-spectrum for Brown–Peterson Cohomology, Part III, preprint (1974). (E.5.3)
443. E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, *J. Reine Angew. Math.* **176** (1937), 126–140. (E.3.8)
444. U. Würgler, Riemann–Roch transformationen und Kobordismen, *Comment. Math. Helv.* **46** (1971), 414–424.
445. U. Würgler, Eine Bemerkung über R-orientierte Kohomologietheorien, *Arch. Math.* **24** (1973), 422–426.
446. U. Würgler, Ueber Kohomologietheorien mit formaler Gruppe der Charakteristik p, *Comment. Math. Helv.* **48** (1973), 531–536.
447. U. Würgler, Cohomologie et groupes formels, *C.R. Acad. Sci. Paris* **278** (1974), 981–983.
448. U. Würgler, Realisierung formaler Gruppen durch Kohomologiefunktoren, *Manuscripta Math.* **14** (1974), 65–87.
449. U. Würgler, Cobordism theories of unitary manifolds with singularities and formal group laws, *Math. Z.* **150** (1976), 239–260. (B.4.1)
450. U. Würgler, Structures multiplicatives dans certaines theories de cobordisme à variétés avec singularities, *C.R. Acad. Sci. Paris Ser. A* **282** (1976), 1417–1420.
451. U. Würgler, On Products in a Family of Cohomology Theories Associated to the Invariant Prime Ideals of $\pi_*(BP)$, preprint (1976).
452. N. Yagita, The exact functor theorem for BP_*/I_n-theory, *Proc. Japan. Acad.* **52** (1976), 1–3. (B.4.1)
453. Y. Yamasaki, On the endomorphism rings of Honda groups $H_{n,m}$ over p-adic integer rings, *Osaka J. Math.* **12** (1975), 457–472.
454. H. Yasumasa, On the BP_* Hopf invariant, *Osaka J. Math.* **12** (1975), 187–196. (B.4.4)

455. Z. I. Yosimura, Projective dimension of complex bordism modules of CW-spectra I, *Osaka J. Math.* **10** (1973), 545–564.
456. Z. Yosimura, Projective dimension of Brown-Peterson cohomology with modulo $(p_1 v_1, \ldots, v_{n-1})$ coefficients, *Osaka J. Math.* **13** (1976), 289–310. (E.5.3)
457. N. Yui, Formal Groups and p-adic Properties of Elliptic Curves, preprint (1975).
458. N. Yui, Elliptic Curves over **Q** and the Associated Formal Groups, preprint (1975).
459. N. Yui, Elliptic Curves and Formal Groups, Thesis, Rutgers, Univ. (1974).
460. R. S. Zahler, The Adams-Novikov spectral sequence for the spheres, *Ann. of Math.* **96** (1972), 480–504.
461. R. Zahler, Existence of the stable homotopy family $\{\gamma_t\}$, *Bull. Amer. Math. Soc.* **79** (1973), 787–789. (B.4.4)
462. R. Zahler, Detecting stable homotopy with secondary cobordism operations I, *Quart. J. Math.* **25** (1974), 213–226. (B.4.4)
463. R. S. Zahler, Nonrealizability of some cyclic complex cobordism modules, *Proc. Amer. Math. Soc.* **47** (1975), 218–222. (B.4.4)

ADDITIONAL BIBLIOGRAPHICAL ITEMS

The list below contains additional bibliographical items which (for various reasons) came to my attention after the manuscript of the book was essentially completed.

464. V. A. Abraškin, 2-divisible groups over **Z** (Russian), *Mat. Zametki* **19** (1976), 5, 717–726. (B.2.1)
465. M. Artin and J. S. Milne, Duality in the flat cohomology of curves, *Inv. Math.* **35** (1976), 111–129.
466. S. A. Basarab, Commutative formal Moufang loops (Roumanian), *Stud. Arcn. Mat.* **28** (1976), 3, 259–265.
467. P. Berthelot, L. Breen, and W. Messing (in preparation). (E.4.1)
468. N. Bourbaki, Hyperalgèbres et Groupes Formels (papiers secrets).
469. V. M. Buhštaber and A. S. Miščenko, Lectures on Extraordinary Cohomology and Formal groups (Russian), *Sb. 10-ya Skola Kiev* (1974), 190–259.
470. J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Inv. Math.* **39** (1977), 223–251. (B.3.3, E.5.1)
471. B. Dwork, On p-adic differential equations I: The Frobenius structure of differential equations. Table ronde anal. non-archim (Paris), *Bull. Soc. Math. France, Memoire* **39/40** (1972), 27–37.
472. B. Dwork, On p-adic differential equations II, *Ann. of Math.* **98** (1973), 366–376.
473. B. Dwork, On p-adic differential equations III: On p-adically bounded solutions of ordinary linear differential equations with rational function coefficients, *Inv. Math.* **20** (1973), 35–45.
474. B. Dwork, On p-adic differential equations IV, *Ann. Sci. Ecole Norm. Suppl.* (4^e) **6** (1973), 3, 295–316.
475. B. Dwork, Bessel functions as p-adic functions of the argument, *Duke Math. J.* **41** (1974), 711–738. (B.3.1)
476. B. Dwork, On p-adic analysis, Belfer Grad. School, Yeshiva Univ., *Proc. Ann. Sci. Conf.* **2** (1969), 129–154.
477. A. Grothendieck, Crystals and the De Rham cohomology of schemes, *in* " Dix Exposés sur la Cohomologie des Schémas." North-Holland Publ., Amsterdam, 1968. (B.2.3)
478. K. Y. Hsu, On decomposition of certain formal groups, *Tamkang J. Math.* **6** (1975), 69–78.
479. K. Y. Hsu, On L series of a formal group, *Tamkang J. Math.* **6** (1975), 1–4.
480. K. Iwasawa, On explicit formulas for the norm residue symbol, *J. Math. Soc. Japan* **20** (1968), 151–164. (B.3.3, E.5.1)

481. M. Kamata and T. Sugawara, A note on Landweber-Novikov operations on the complex cobordism ring U, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **29** (1975), 51–58.
482. N. Katz, p-adic properties of modular schemes and modular forms, Modular functions of one variable II, Lecture Notes Math. Vol. 350. Springer-Verlag, Berlin and New York, 1973, 69–190.
483. N. Katz, The Eisenstein measure and p-adic interpolation, *Amer. J. Math.* **99** (1977), 238–311.
484. N. M. Katz, Formal Groups and p-adic Interpolation, preprint, January, 1977.
485. G. T. Konovalov, Norm subgroups of formal groups over a local field (Russian), *Ukrain Mat. Ž.* **28** (1976), 4, 528–532. (B.3.2)
486. G. T. Konovalov, The universal Γ-norms of formal groups over a local field (Russian), *Ukrain. Mat. Ž.* **28** (1976), 3, 399–401. (B.3.2)
487. M. Kouider, Groupes formels isogènes à un groupe donné, *C.R. Acad. Sci. Paris Ser. A* **283** (1977), 201–202.
488. T. Kubota and H. W. Leopoldt, Eine p-adische Theorie der Zetawerte I, *J. Reine Angew. Math.* **214/215** (1964), 328–339.
489. J. Labute and P. Russell, On K_2 of truncated polynomial rings, *J. Pure Appl. Algebra* **6** (1975), 239–252. (B.2.3)
490. H. W. Leopoldt, Eine p-adische Theorie de Zetawerte II: Die p-adische Γ-transformation, *J. Reine Angew. Math.* **274/275** (1975), 224–239.
491. A. Liulevicius, Representation rings of the symmetric groups, A Hopf algebra approach, Mat. Inst., Århus Univ., preprint series, **29** (June, 1976). (E.6.3)
492. J. Lubin and M. Rosen, Letter to Barry Mazur, September 24, 1976.
493. F. Meden, Algébricité de morphismes entre les formalisés de groupes algébriques sur un corps, *C.R. Acad. Sci. Paris* **283** (1977), 37–40.
494. J. S. Milne and W. C. Waterhouse, Abelian varieties over finite fields, Inst. on Number Theory, *Proc. Symp. Pure Math.* **20** (1971), 53–64.
495. J. Milnor, "Introduction to Algebraic K-theory." Princeton Univ. Press, Princeton, New Jersey, 1971. (B.2.3)
496. T. Oda and F. Oort, Supersingular abelian varieties, preprint, 1976.
497. D. C. Ravenel, The nonexistence of odd primary Arf invariant elements in stable homotopy, *Proc. Cambridge Philos. Soc.* (to appear). (B.4.4)
498. D. C. Ravenel, The cohomology of Morava stabilizer algebras, *Math. Z.* **152** (1977), 287–297. (B.4.4)
499. M. Raynaud, Schémas en groupe de type $(p, p, \ldots, p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.
500. J. P. Serre, Sur la topologie des variétés algébriques en caractéristique p *Symp. Internat. Topology Algebra (Mexico)* (1958), 24–53.
501. J. P. Serre, Quelques propriétés des variétés abéliennes en caractéristique p, *Amer. J. Math.* **80** (1958), 715–739.
502. K. Shimakawa, Remarks on the coefficient ring of quaternionic oriented cohomology theories, *Publ. Res. Inst. Math. Soc.* **12** (1976), 1, 241–254.
503. S. Sperber, P-adic Hypergeometric Functions and Their Cohomology, Thesis, Univ. of Pennsylvania, 1975. (B.3.1)
504. S. Sperber, P-adic hypergeometric functions and their cohomology I, *Duke Math. J.* (to appear). (B.3.1)
505. S. Sperber, P-adic hypergeometric functions and their cohomology II (Congruence properties of the Hyper-Kloosterman sum), preprint, 1976. (B.3.1)
506. M. Takeuchi, On the structure of commutative affine group schemes over a non perfect field, *Manuscripta Math.* **16** (1975), 2, 101–136. (E.4.1)
507. J. Tate, Classes d'Isogénie des variétés abéliennes sur un corps fini (d'après Honda), Sém. Bourbaki 1968–1969, Exp. 352.

508. A. Tyc, Witt groups of commutative formal groups, *Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys.* **23** (1975), 12, 1233–1240. (E.2.3)
509. A. Wiles, Higher explicit reciprocity laws, preprint, Cambridge, England, 1976. (B.3.3, E.5.1)
510. N. Yui, A note on formal groups and zeta functions, preprint, Mat. Inst., København Univ. **10** (April, 1977).
511. O. Zariski and P. Samuel, "Commutative Algebra." Vols. I and II, van Nostrand–Reinhold, Princeton, New Jersey, 1958, 1960. (A.2.9)

NOTATION

■ (I.1.1) **General notational conventions concerning categories** If $\mathbf{C}$ is a category and C_1, C_2 are objects of $\mathbf{C}$, then $\mathbf{C}(C_1, C_2)$ is the set of morphisms from C_1 to C_2. If $\mathbf{C}$ and $\mathbf{D}$ are two categories, then $\mathbf{CD}$ is the category of functors $\mathbf{C} \to \mathbf{D}$. The symbol $\mathbf{C}^\circ$ denotes the dual category of $\mathbf{C}$.

The category of group objects of a category $\mathbf{C}$ is denoted $G\mathbf{C}$, the category of cogroup objects $C\mathbf{C}$; the categories $C^c\mathbf{C}$ and $G^c\mathbf{C}$ are the categories of cocommutative cogroup objects and commutative group objects in $\mathbf{C}$.

The symbol $\times$ is used to denote direct products, $\amalg$ denotes direct sums. A final object is denoted E, an initial object I, multiplication morphisms are generically denoted m, comultiplication morphisms μ, counit morphisms ε, unit morphisms e, coinverse morphisms ι, and inverse morphisms i. Finally $t: C_1 \times C_2 \to C_2 \times C_1$ and $\tau: C_1 \amalg C_2 \to C_2 \amalg C_1$ are the canonical switch morphisms. (Cf. also Section 36.1.)

■ (I.1.2) **Standard notations concerning rings and algebras** If A is a ring and X a set of indeterminates, then $A[X]$ is the ring of polynomials in X over A, and $A[\![X]\!]$ the ring of power series in $X_1, \ldots, X_m$ over A. If T is one indeterminate and σ an endomorphism of A, then $A_\sigma[\![T]\!]$ is the ring of twisted power series in T over A with multiplication rule $Ta = \sigma(a)T$. If A is a ring and $n, m \in \mathbf{N}$, then A^n is the direct product of n copies of A. $A^{n \times m}$ is the group of $n \times m$ matrices over A, sometimes also denoted $M_{n \times m}(A)$; further $U(A) = A^*$ is the group of invertible elements of A; and if A is an integral domain, $Q(A)$ is the quotient field.

■ (I.1.3) **Standard notations concerning discrete valuation fields** If K is a discrete valuation field, then $A = A(K)$ is its ring of integers, $\mathfrak{m}(K)$ the maximal ideal of $A(K)$, π a uniformizing element of K, k, or k_K the residue field, v_K the normalized exponential valuation, $U(K) = A(K)^*$, $U^n(K) = \{x \in A(K) \mid x \equiv 1 \bmod \pi_K^n\}$. If L/K is a finite extension, then $e(L/K)$ is the ramification index and $l = k_L$, $\mathfrak{m}(L)$, $A(L)$, π_L, v_L have the obvious meanings.

■ (I.1.4) Some special notations

$[a]_F(X)$, $[a](X)$, $[b]_F(X)$, $[b](X)$, ...: endomorphism of the formal group law $F(X, Y)$ starting with $aX + \cdots$; also the operator on $\mathscr{C}(F; -)$ induced by these endomorphisms

$\langle b\rangle$, $\langle a\rangle$, ...: homothety operators on $\mathscr{C}(F; B)$, defined by $\langle a\rangle\gamma(t) = \gamma(at)$

$\langle\ ,\ \rangle$: various duality pairings

(q^n), (p^n) as exponent, e.g., $f^{(p^n)}(X)$: result of applying an endomorphism of type $T_i \mapsto T_i^{p^n}$ to the coefficients of the (vector of) power series $f(X)$

$\sigma_* f(X)$: result of applying σ to the coefficients of $f(X)$

$\{n\}$ as exponent of a matrix, e.g., $\bar{V}^{\{n\}}$: result of raising each of the entries of $\bar{V}$ to the power n.

The ith component of a vector of power series $F(X, Y)$, $\alpha(X)$ is generally denoted $F(i)(X, Y)$ and $\alpha(i)(X)$.

■ (I.1.5) Notations using the Latin alphabet

■ A, a Standard notations

A-height	formal A-module height
Ab	category of abelian groups
$\mathbf{Alg}_A$	category of commutative A-algebras with 1
$\mathbf{AlT}_A$	category of certain projective limits of objects of $\mathbf{AlT}_A^{\mathrm{f}}$, 37.2
$\mathbf{AlT}_A^{\mathrm{f}}$	category of A-algebras which are free of finite rank as A-modules
Al_X	free algebra on the set X, (14.4.3)
$\mathbf{Ass}_A$	category of associative algebras over A (with 1)
A-End$(\cdots)$	ring of formal A-module endomorphisms of $\cdots$
$a_i(V)$	coefficient of X^{p^i} in $f_V(X)$ the logarithm of the p-typical universal formal group law $F_V(X, Y)$
$a_i(V, T)$	coefficient of X^{p^i} in $f_{V,T}(X)$ the logarithm of $F_{V,T}(X, Y)$
$a_i^A(V)$	coefficient of X^{q^i} in $f_V^A(X)$
$a_i^A(V, T)$	coefficient of X^{q^i} in $f_{V,T}^A(X)$
Aut..$(\cdots)$	group of automorphisms of $\cdots$ over $\cdot\cdot$
Ass_X	free associative algebra over X

Generic notations A: ring or algebra; a, a_i: vector, matrix; $a(X)$: power series; $A(-)$: ring of integers of $-$; A-$\log_F(X)$: A-logarithm of formal A-module $F(X, Y)$

Incidental notations $A_{(v)}$: localization of A with respect to valuation v; A_v: completion of A with respect to valuation v; $A_{\mathfrak{p}}$: completion of A with respect to prime ideal $\mathfrak{p}$; A_n, A_t: ring of integers of unramified extension of degree n, t; A_F: $= J(\mathrm{End}_A(F(X, Y))$ (35.2.2); $A(\cdot\cdot)$: ring or algebra of the scheme $\cdot\cdot$

■ B, b Standard notations

$B_n(X, Y) = X^n + Y^n - (X + Y)^n$

$\mathrm{Br}(K)$ Brauer group of the field K
$\mathbf{BP}$ Brown–Peterson cohomology

Generic notations B: ring or A-algebra, bialgebra; b: element, vector, or matrix of elements of B

Incidental notations $b(i_1, \ldots, i_s)$ certain special coefficients, (5.6.1)

■ *C, c* **Standard notations**

$C_n(X, Y)$ $= v(n)^{-1}(X^n + Y^n - (X + Y)^n)$
$\mathscr{C}(F; A)$ module of curves of the formal group (law) F with coefficients in A
$\mathscr{C}(F)$ *idem*
$\mathscr{C}^n(F; A)$ $= \{\gamma(t) \in \mathscr{C}(F; A) \mid \gamma(t) \equiv 0 \bmod t^n\}$
$\mathscr{C}_p(F; A)$ p-typical curves in $\mathscr{C}(F; A)$
$\mathscr{C}_q(F; B)$ q-typical curves in $\mathscr{C}(F; B)$, $F(X, Y)$ a formal A-module
$\mathscr{C}_p^{(i)}(F; A)$ $= \mathscr{C}_p(F; A) \cap \mathscr{C}^{p^i}(F; A)$
$\mathscr{C}_q^{(i)}(F; B)$ $= \mathscr{C}_q(F; B) \cap \mathscr{C}^{q^i}(F; B)$
$\mathrm{Cart}(A)$ ring of operators on $\mathscr{C}(-; A)$, (27.2.11)
$\mathrm{Cart}_p(A)$ ring of operators on $\mathscr{C}_p(-; A)$, (27.7.9)
$\mathrm{Cart}_A(B)$ ring of operators on $\mathscr{C}_q(-; B)$, (29.3)
$\mathrm{comp}(\chi)$ composition operator associated to power series $\chi(t)$
$\mathbf{CP}^n$ complex projective space of complex dimension n
$[\mathbf{CP}^n]$ cobordism class of $\mathbf{CP}^n$
$\mathbf{Clg}_A$ certain category of coalgebras over A, (37.2.5)
$\mathscr{C}(U; A)$ group of curves of covariant bialgebra U over A
$\mathrm{char}(\cdots)$ characteristic of the field $\cdots$

Generic notations $\mathbf{C}$: category; C: ring or algebra, indeterminate, set of indeterminates, coalgebra; c: element, vector or matrix; $\mathscr{C}$: topological group or module; $\mathscr{C}_{\mathbf{V}}$: localization of $\mathscr{C}$

Incidental notations $c(p, q)$: certain integers, (5.6.1); $c(p, n, i, j)$: structure constants, (27.4.1); $c(r, i, j)$: structure constants, (27.7.14)

■ *D, d* **Standard notations**

D_h central division algebra over $\mathbf{Q}_p$ of rank h^2 and invariant h^{-1}
$D_h(K)$ central division algebra over K of rank h^2 and invariant h^{-1}
D_h^A $= D_h(K)$ if $K = Q(A)$
D, D^T various duality functors, (37.2, 37.3)
$\mathbf{D}(k)$ Dieudonné ring of k, (28.3.5)
$\mathbf{D}_{\mathbf{V}}(k)$ Dieudonné ring of k localized with respect to $\mathbf{V}$, (28.3.6)
$\mathbf{D}_{\mathbf{V}}^+(k)$ $= W_{p^\infty}(k)_\sigma[\![\mathbf{V}]\!]$
$\mathrm{Der}_A(B)$ derivations of the A-algebra B
$\dfrac{\mathrm{d}\cdots}{\mathrm{d}\cdots}$ differentiation

Generic notations $\mathscr{D}$: submodule of $\mathscr{C}$; D: ring or algebra, set of indeterminates, indeterminate; d: element of $\mathbf{N}$, diagonal morphism in category with products; d, $d(X)$: elements of $\mathscr{E}_\pi$

Incidental notations $D(\eta)$: matrix of semilinear mapping η; D_L: commutant of L in division algebra D; d: $E \to K$ degreelike mapping, (28.4.1); $d(i_1, \ldots, i_s)$ certain special coefficients occurring in the definition of $F_U(X, Y)$, (5.3.2); $D(X, Y)$: power series

■ E, e **Standard notations**

e^h	Euler classes for the cohomology theory h^*, e.g., e^{MU}, e^{BP}
End..$(\cdots)$	endomorphism ring of $\cdots$ over $\cdot\cdot$
END$(\cdots)$	absolute endomorphism ring of $\cdots$
$\bar{E}$	Artin–Hasse exponential isomorphism $W(-) \xrightarrow{\sim} \Lambda(-)$, (17.2.7), (17.2.9)
$\mathbf{e}(i)$	multi-index $(0, \ldots, 0, 1, 0, \ldots)$ with 1 in ith spot
$\bar{E}^F$	Artin–Hasse exponential isomorphism $W^F(-) \xrightarrow{\sim} \mathscr{C}(F; -)$
E_p, $E_{A.p}$	Artin–Hasse exponential $W_{p^\infty}(-) \to \Lambda(W_{p^\infty}(-))$, 17.5, 17.6
E_h	ring of integers of D_h
E_h^A, $E_h(K)$	ring of integers of D_h^A, $D_h(K)$
E^U	$= E^F$ for $F = F_U(X, Y)$, the universal one dimensional formal group law
E^F	Artin–Hasse exponential $A \to C_q(F; A)$, (25.3.28)
exp(?)	$= 1 + ? + (2!)^{-1}?^2 + (3!)^{-1}?^3 + \cdots$

Generic notations e: unit morphism of group object in a category; e_i: ith basis element; E: final object in a category; e, $e(L/K)$, e_L: ramification index of L/K

Incidental notations $\mathscr{E}$: abbreviation for $\mathbf{D}_V(k)$ and similar rings, (28.4.1); $E(X)$: exponential series; $\mathscr{E}_m$: $= A_\sigma[\![T]\!]^{m \times m}$; $E(t)$: pure curve in $\mathbf{U}_{(p)}$, (38.4.2); $\mathscr{E}_\pi$, $\mathscr{E}_{\pi,t}$: certain sets of power series, 8.1; e, $e(X)$: elements of $\mathscr{E}_\pi$, $\mathscr{E}_{\pi,t}$

■ F, f **Standard notations**

$\mathbf{F}_p$, $\mathbf{F}_q$	finite fields with p, q elements
$\mathbf{F}(p^\infty)$	algebraic closure of $\mathbf{F}_p$
$\mathbf{FG}_A$	category of formal group laws over A
$\mathscr{F}$	Frobenius homomorphism $\Gamma(X, Y) \to \sigma_*\Gamma(X, Y)$, (30.1.1)
$\mathbf{FG}_B^A$	category of formal A-modules over B
$\mathbf{f}$, $\mathbf{f}_p$, $\mathbf{f}_\pi$	Frobenius operator in Cart(A). Cart$_p(A)$
$\mathbf{f}_p$	Frobenius endomorphism of $W(-)$, $W_{p^\infty}(-)$
$F(\cdot\cdot)$, $F(K_{sc})$	points of $F(X, Y)$ in $\cdot\cdot$, K_{sc}, (35.1.1)
$\mathbf{f}_\pi$	Frobenius operator in Cart$_A(B)$

$\mathbf{f}_\pi$	Frobenius endomorphism of $W^A(-)$
$F_V(X, Y)$	one or higher dimensional p-typical universal formal group law over $\mathbf{Z}[V]$, 3, 10.3
$f_V(X)$	logarithm of $F_V(X, Y)$
$F_V^A(X, Y)$	one or more dimensional A-typical universal formal A-module over $A[V]$
$f_V^A(X)$	logarithm of $F_V^A(X, Y)$
$F_{V.T}(X, Y)$	most general p-typical formal group law strictly isomorphic to $F_V(X, Y)$, 3, 10, 19.2
$f_{V.T}(X)$	logarithm of $F_{V.T}(X, Y)$
$F_{V.T}^A(X, Y)$	most general A-typical formal A-module strictly isomorphic to $F_V^A(X, Y)$
$f_{V.T}^A(X)$	logarithm of $F_{V.T}^A(X, Y)$
$F_{\Delta_n}(X, Y)$	certain one-dimensional formal group law over $\mathbf{Z}$ of height n, 3.2
$\bar{F}_{\Delta_n}(X, Y)$	reduction mod p of $F_{\Delta_n}(X, Y)$
$f_{\Delta_n}(X)$	logarithm of $F_{\Delta_n}(X, Y)$
$F_R(X, Y)$	universal curvilinear formal group law
$f_R(X, Y)$	logarithm of $F_R(X, Y)$
$F_{MU}(X, Y)$	formal group law of complex cobordism
$F_{BP}(X, Y)$	formal group law of Brown–Peterson cohomology
$F_U(X, Y)$	universal one dimensional formal group law over $\mathbf{Z}[U]$, (5.6.11)
$f_U(X)$	logarithm of $F_U(X, Y)$, (5.6.11)
$F_S(X, Y)$	universal formal group law for formal group laws over $\mathbf{Z}_{(p)}$-algebras
$f_S(X, Y)$	logarithm of $F_S(X, Y)$
$F_S^A(X, Y)$	universal formal A-module
$f_S^A(X, Y)$	logarithm of $F_S^A(X, Y)$
$\mathbf{FG}_{B.\sigma}^A$	category of pairs $(G(X, Y), \mathrm{v}(X))$ consisting of a formal A-module $G(X, Y)$ and a Verschiebung lift $\mathrm{v}(X)$: $\sigma_* G(X, Y) \to G(X, Y)$
$F_p(X, Y)$, $F_\pi(X, Y)$	Lubin–Tate formal group laws associated to uniformizing elements p, π; cf. Section 8
$f_w(X)$	logarithm of $\hat{W}(X, Y)$

Generic notations $F(X, Y)$: formal group law; F: formal group; $f(X)$: logarithm of $F(X, Y)$; $f_g(X)$: logarithm of $F_g(X, Y)$; $F_g(X, Y)$: formal group law attached to power series $g(X)$, 2.1; $F(i)(X, Y)$: ith component of $F(X, Y)$

Incidental notations $F_m(X, Y)$ group law chunk of order m, (5.7.1); $F_h(X, Y) = F_{\Delta_h}(X, Y)$; $f_h(X) = f_{\Delta_h}(X)$; $F_{(m)}(X, Y)$: group law chunk of order m defined by $F(X, Y)$

■ G, g Standard notations

Group	category of groups
$\mathbf{GA}_A$	certain category of affine group schemes over A, (37.3.3)
$\mathbf{Gf}_A$	category of formal groups over A, (37.3.1)
$\hat{\mathbf{G}}_m$	multiplicative formal group law $X + Y + XY$
$\hat{\mathbf{G}}_m^-$	multiplicative formal group law $X + Y - XY$
$\hat{\mathbf{G}}_a$	additive formal group law $X + Y$
$\mathbf{G}_m$	multiplicative group scheme, $\mathbf{G}_m(A) = A^* = U(A)$
$\mathbf{G}_a$	additive group scheme $\mathbf{G}_a(A) = A^+$, the underlying additive group of A
$\mathrm{Gal}(L/K)$	Galois group of L/K
$G(M, \eta)(X, Y)$	generalized Lubin–Tate formal A-module associated to a module M with semilinear endomorphism η, (30.1.8)
$g(M, \eta)(X)$	logarithm of $G(M, \eta)(X, Y)$

Generic notations $G(X, Y)$: formal group law; $g(X)$: logarithm of $G(X, Y)$; G: formal group, group, Galois group, group object in a category; $g(X)$: any power series

Incidental notations $G_{p<}(X, Y)$: certain universal formal group law, (27.6.12): $g_{p<}(X)$: logarithm of $G_{p<}(X, Y)$; $\mathrm{gr}_n(\mathscr{D})$, $\mathrm{gr}_n(\mathscr{C})$: nth direct summand of the associated graded group of a filtered group $\mathscr{C}$, $\mathscr{D}$

■ H, h Standard notations

$\mathrm{ht}(-)$	height of $-$
$H_A(B)$	group of divided power sequences of the A-algebra B
$H_U(X, Y)$	universal formal group law (especially higher dimensional)
$h_U(X)$	logarithm of $H_U(X, Y)$
$H_R(X, Y)$	universal curvilinear formal group law, 12
$h_R(X)$	logarithm of $H_R(X, Y)$
$H^i(\mathrm{Gal}(L/K), l)$ $H^1(\Gamma; -)$, $H^2(K_{nr}/K)$	Galois cohomology groups, (18.5.3), (20.2.16), 24.1
H^*	ordinary cohomology (on CW complexes)
$H_{r,s}$	Milnor hypersurface, (34.2.7)

Generic notations $H(X, Y)$: formal group law; $h(X)$: logarithm of $H(X, Y)$, power series; h: element of $\mathbf{N}$ (especially height of a formal group law)

■ I, i Standard notations

$I(p)$	$= \{n \in \mathbf{N} \mid (n, p) = 1\}$
I_n	$n \times n$ unit matrix
$\mathrm{Iso}(\mathbf{F}_q, h)$	set of isomorphism classes of one dimensional formal group laws of height h over $\mathbf{F}_q$

Generic notations I: index set, initial object in a category; $\mathbf{I}$, $\mathbf{I}_m$: set of

all multi-indices $\{1, \ldots, m\} \to \mathbf{N} \cup \{0\}$, $I \to \mathbf{N} \cup \{0\}$; i: inverse morphism of a group object, element of I or $\mathbf{N}$; $\mathbf{i}$: multi-index

■ J, j **Standard notations**

$J(\alpha)$ Jacobian of $\alpha(X)$

Generic notations $\mathbf{j}$: multi-index; j index, element of $\mathbf{N}$ or I

■ K, k **Standard notations**

k_a, K_a	algebraic closure of the fields k, K
k_{sc}, K_{sc}	separable closure of the fields k, K
k_B, K_L, k_R	residue fields of B, L, R
K^*	complex K-theory, (31.1.3) (group of nonzero elements of field K)
K_{nr}	maximal unramified extension of local field K

Generic notations k, K: fields (especially $\mathrm{char}(k) = p > 0$); k: element of $\mathbf{N}$ or index set; $\mathbf{k}$: multi-index; K: index set

Incidental notations K_n: unramified extension of degree n of K

■ L, l **Standard notations**

Lie(–), L(–)	Lie algebra of –
Lie_n(–)	curves of order n in –
$\mathbf{LA}_A$	category of Lie algebras over A that are free as A-modules
L_X	free Lie algebra over the set X
$\log(1 + X)$	$= X - 2^{-1}X^2 + 3^{-1}X^3 - 4^{-1}X^4 + \cdots$
LT	Lubin–Tate formal A-module functor $\mathbf{Mod}_a(B) \to \mathbf{FG}^A_{B,a}$
$\log_{MU}(X)$	logarithm of $F_{MU}(X, Y)$
$\log_{BP}(X)$	logarithm of $F_{BP}(X, Y)$

Generic notations L, L_1, L_2, L_A: extension field of K, Lie algebra, line bundle, ring or algebra over which a universal formal group is defined; $\log_F(X)$: logarithm of formal group law $F(X, Y)$; l: element of $\mathbf{N}$, extension field of k, residue field of L; $\mathbf{l}$: multi-index

Incidental notations $L(p)$: certain Lazard type ring, (27.6.8); L_π: maximal totally ramified abelian extension of K; L_F: quotient field of $A_F = J(\mathrm{End}_A(F(X, Y)))$

■ M, m **Standard notations**

$\mathbf{Mod}_A$	category of modules over A
$\mathbf{Mod}T_A$	certain category of topological modules over A, (37.2.1)
$\mathbf{Mod}F_A$	category of free A-modules
$m_n(U)$	coefficient of X^n in $f_U(X)$, (5.2.7), (5.6.11)
M_X	free magma on X
Mor(I, J), Mor(1, K), Mor(m, n)	sets of morphisms in the category of formal schemes, (27.1.1)

$\mathbf{Mod}_\Gamma$	category of Γ-modules, (35.1.2), (24.1.1)
$\mathbf{Mod}_\sigma(B)$	category of pairs (M, η), M a free B-module of finite rank and η a semilinear endomorphism
MU^*	complex cobordism cohomology
m_n	$= (n+1)^{-1}[\mathbf{CP}^n]$, (31.1.4)

Generic notations M: manifold, matrix, module; m, m_1, m_2: multiplication morphisms of a group object, element of $\mathbf{N}$; $\mathbf{m}$: multi-index

Incidental notations M_h: certain ring, (20.2.11)

■ N, n **Standard notations**

$\mathbf{N}$	set of natural numbers $\{1, 2, 3, \ldots\}$
$[n]_F(X)$	$= X +_F X +_F \cdots +_F X$, (1.4.2)
$\mathbf{N}(\mathfrak{n})$	$= \{n \in \mathbf{N} \mid n \mid \mathfrak{n}\}$
$N_{L/K}$	norm map $L \to K$, L/K field extension

Generic notations $\mathbf{n}$: multi-index; n: element of $\mathbf{N}$, index; N: module; matrix, element of $\mathbf{N}$

Incidental notations $n(i_1, \ldots, i_s)$: certain coefficient occurring in the definition of $F_U(X, Y)$, (5.2.1), (5.6.1)

■ O, o **Incidental notations**

$\mathcal{O}$	order in a discrete valuation ring

■ P, p **Standard notations**

$\mathbf{P}$	set of all prime numbers
$P(U)$	set of primitive elements of a bialgebra U, (37.5.13)
$[p]_F(X)$	$X +_F \cdots +_F X$ (p times)

Generic notations p: prime number

Incidental notations $[p]_n(X) = [p]_{F_{\Delta_n}}(X)$; P_1, P_2, ... certain universal polynomials

■ Q, q **Standard notations**

$\mathbf{Q}$	rational numbers
$Q(-)$	quotient field of the integral domain $-$
$\mathbf{Q}_p$	p-adic numbers

Generic notations q: power of a prime number, prime number $\neq p$, number of elements in a residue field; Q, Q_1, Q_2 operators on $\mathscr{C}(-; A)$; $q(X)$ power series

Incidental notations Q_p: shift operator, (25.1.1); $Q_{n,1}$, $Q_{n,2}$: certain universal polynomials 17.2; $Q_i(S, C)$ more universal polynomials

■ R, r **Standard notations**

$\mathbf{R}$	real numbers

$r_n(Z_1, Z_2)$ polynomial over $\mathbf{Z}$ defined by $Z_1^n + Z_2^n = \sum_{d|n} d r_d(Z_1, Z_2)^{n/d}$
Ring category of rings
$R(F)$ contravariant bialgebra of formal group (law) F
$r_n^A(Z_1, Z_2)$ polynomials over A, a discrete valuation ring with finite residue field, defined by
$Z_1^{q^n} + Z_2^{q^n} = \sum \pi^s r_s^A(Z_1, Z_2)^{q^{n-s}}$, (29.3.8)
r_E BP-cohomology operation associated to exponent sequence E
$R(\alpha)$ morphism of bialgebras induced by $\alpha(X)$

Generic notations R_i, R: ring or algebra (especially local), bialgebra, B-module, polynomial, indeterminate or set of indeterminates; r: element of $\mathbf{N}$, element of R

Incidental notations $R(A)$, $R_p(A)$: subrings of $\mathrm{Cart}(A)$, $\mathrm{Cart}_p(A)$ isomorphic to $W(A)$ and $W_{p^\infty}(A)$; $R_{q,\pi}(B)$, $R_q(B')$: certain rings of power series, (25.8.4); $r(-)$: certain morphism, (30.2.9); r_n: primitives in $U(\hat{W})$; r, r_L: reciprocity homomorphisms; r_t: big cohomology operation, (31.1.12)

■ S, s **Standard notations**
Set category of sets
s_n certain functorial ring homomorphisms $\Lambda(A) \to A$, (17.2.6)
$s_{q,i}^F$ certain functorial ring homomorphisms $C_q(F; B) \to B$, (23.3.25)
S^2 Riemann sphere
s_i big Landweber–Novikov operation (for $\mathbf{MU}^*$)

Generic notations s: antipode in a bialgebra or Hopfalgebra, element of $\mathbf{N}$; S, S_i: indeterminate, set of indeterminates, set, topological space; $\mathbf{s}$: multi-index; $\mathscr{S}$: set of subsets

Incidental notations s_π, s: reciprocity homomorphism; s: Šafarevič mapping

■ T, t **Standard notations**
$T\mathfrak{g}$ tensor algebra of the module $\mathfrak{g}$
$T_n\mathfrak{g}$ nth direct summand of $T\mathfrak{g}$

Generic notations t: twist or switching morphism $G \times G \to G \times G$ in a category, element of $\mathbf{N}$, element of a pseudobasis of R, indeterminate (especially when dealing with curves); T, T_i: indeterminate or set of indeterminates

Incidental notations $\mathscr{T}$: forgetful functor, (30.2.10); T_r: set of conjugacy classes in D_h, (18.5.9)

■ U, u **Standard notations**
$\mathbf{U}^c$ covariant bialgebra of the Witt vectors, (36.1.11), (36.3.8), (37.5.13)
$\mathbf{U}$ certain noncommutative analogue of $\mathbf{U}^c$, (36.3.8)
$U\mathfrak{g}$ universal enveloping algebra of the Lie algebra $\mathfrak{g}$

$U(F)$, $U(G)$ covariant bialgebra of the formal group F, G
$U(-)$, $U(K)$ ring of units of the ring $-$, the local field K
$U^n(K)$ $= \{x \in U(K) \mid x \equiv 1 \bmod \pi_K^n\}$

Generic notations U: coalgebra, bialgebra, indeterminate or set of indeterminates; u: element of U, $U(F)$, $U(K)$

Incidental notations u: Euler class of ξ in $MU^2(\mathbf{CP}^N)$; u_j: certain elements of $MU(\mathbf{CP}^N)$; $\mathbf{U}(n)$: subbialgebra of $\mathbf{U}$, $\mathbf{U}_{(p)}$: localization of $\mathbf{U}$, (38.4.2), $\mathbf{U}_E$ subbialgebra of $\mathbf{U}_{(p)}$, (38.4.4)

■ V, v **Standard notations**

$\mathscr{V}$ Verschiebungs homomorphism $\sigma_* \Gamma(X, Y) \to \Gamma(X, Y)$
$\mathbf{V}$, $\mathbf{V}_n$ Verschiebungs operator on $\mathscr{C}(F; A)$ or $W(-)$
$\bar{V}_n$ polynomials in $V_1, \ldots, V_n$; $T_1, \ldots, T_n$ describing the most general coordinate change in a formal group law, 18.1
$v_p(n)$ p-valuation of n
v_K normalized exponential valuation on the local field K

Generic notations V, V_i: indeterminate, set of indeterminates; v: element of $U(K)$, valuation

Incidental notations $\mathbf{v}$: Verschiebungslift $\sigma_* G(X, Y) \to G(X, Y)$, (30.2.1); $\mathbf{v}(M, \eta)$: Verschiebungslift $\sigma_* G(M, \eta)(X, Y) \to G(M, \eta)(X, Y)$; $\mathscr{V}$: forgetful functor, (36.1.1)

■ W, w **Standard notations**

$W(-)$ ring of Witt vectors for all primes simultaneously, 17.1
$W^+(-)$ underlying additive group of $W(-)$
$\hat{W}(-)$ formal group of Witt vectors
W group scheme representing $W(-)$
$W^F(-)$ group of Witt-like vectors associated to a formal group law
$W_{p^\infty}(-)$ Witt vectors associated to the prime number p, 15.3, 17.4
w_n functorial ring homomorphisms $W(A) \to A$, Witt polynomials
$\hat{W}(X, Y)$ formal group law of the Witt vectors, 17.1
$\hat{W}^F(X, Y)$ formal group law of Witt vectors associated to formal group $F(X, Y)$
$\bar{w}_n^F$ Witt-like polynomial associated to formal group law $F(X, Y)$, (25.1.1)
$\hat{w}_n^F$ $= n\bar{w}_n^F$
$\hat{W}_{p^\alpha}(X, Y)$ formal group of Witt vectors associated to the prime number p
$w_n^A(Z)$ Witt polynomials of the ramified Witt vector functor $W_{q,\infty}^A$, 25.3
$W_{q,\infty}^A(-)$ functor of ramified Witt vectors, (25.3.26)
$\hat{W}_{q,\infty}^A(X, Y)$ formal A-module of the ramified Witt vectors
$\bar{w}_q^A(X)$ logarithm of $\hat{W}_{q,\infty}^A(X, Y)$
$\bar{w}^F$ logarithm of $\hat{W}^F(X, Y)$

Generic notations w: filtration function

Incidental notations w: Bott periodicity element

■ X, x **Generic notations** X: indeterminate, set or vector of indeterminates; $X^{\mathbf{n}} = X_1^{n_1} \cdots X_m^{n_m}$; $X^n = (X_1^n, \ldots, X_m^n)$; x: element of a set, algebra, coalgebra, or bialgebra

■ Y, y **Generic notations** Y, Y_i: indeterminate, set or vector of indeterminates; y: element of an algebra, set, coalgebra, or bialgebra

Incidental notations Y_i, $Y_{n,m}$: certain elements $\mathbf{U}_{(p)}$, (38.4.3), (38.4.5); $y(i, \mathbf{d})$: certain (basis) elements of $\mathbf{Z}[U]$, 11.4

■ Z, z **Standard notations**

$\mathbf{Z}$	integers
$\mathbf{Z}_p$	p-adic integers
$\hat{\mathbf{Z}}$	$\varprojlim \mathbf{Z}/(n)$, completion of $\mathbf{Z}$ with respect to the topology of subgroups of finite index
$\mathbf{Z}_{(S)}$	all rational numbers with denominators prime to all primes in the set S
$\mathbf{Z}_{(p)}$	$= \mathbf{Z}_{(\{p\})}$
$Z^1(\Gamma; -)$	1-cocycles of Γ with values in $-$ (Galois cohomology)

Generic notations z: element of $Z^1(\Gamma; -)$, element of $U(G)$ and other algebras, bialgebras; Z, Z_i: indeterminate or set or vector of indeterminates

■ (I.1.6) **Notations using the gothic alphabet**

$\mathfrak{A}$, $\mathfrak{a}$ **Generic notations** $\mathfrak{A}$: ideal

Incidental notations $\mathfrak{A}_n$, $\mathfrak{A}_2$: right ideals in $\mathrm{Cart}(A)$, (27.2.13), (28.1.2); $\mathfrak{A}_n(A)$: ideal of $W(A)$ associated to supernatural number $\mathfrak{n}$, (17.4.1)

$\mathfrak{g}$ **Generic notations** $\mathfrak{g}$: Lie algebra

$\mathfrak{h}$ **Generic notations** $\mathfrak{h}$: Lie algebra

$\mathfrak{m}$ **Standard notations**

$\mathfrak{m}(F)$	maximal ideal of the contravariant bialgebra $R(F)$
$\mathfrak{m}(K)$, $\mathfrak{m}(L)$	maximal ideal of ring of integers of K, L, ...

Generic notations $\mathfrak{m}$: maximal ideal, augmentation ideal, supernatural number

$\mathfrak{n}$ **Standard notations**

$\mathfrak{n}(B)$ ideal of nilpotents of the ring B

Generic notations $\mathfrak{n}$: supernatural number, (17.4.1)

$\mathfrak{p}$ **Generic notations** $\mathfrak{p}$: prime ideal

Incidental notations $\mathfrak{S}$: finite set of primes of a global field

■ (I.1.7) Notations using the Greek alphabet

■ α Standard notations

$\alpha_{V,T}(X)$ strict isomorphism $F_V(X, Y) \to F_{V,T}(X, Y)$
$\alpha^A_{V,T}(X)$ strict isomorphism $F^A_V(X, Y) \to F^A_{V,T}(X, Y)$
$\alpha_{V,S}(X)$ strict isomorphism $F_V(X, Y) \to F_S(X, Y)$
$\alpha^A_{V,S}(X)$ strict isomorphism $F^A_V(X, Y) \to F^A_S(X, Y)$

Generic notations α: morphism in a category; $\alpha(X)$: power series homomorphism between formal group laws; α_*: $\mathscr{C}_p(F; A) \to \mathscr{C}(G; A)$ morphism induced by $\alpha(X)$: $F(X, Y) \to G(X, Y)$

■ β Standard notations

β_0: $M \to C_q(G(M, \eta); B)$, certain canonical map, (30.1.17)

Generic notations β: morphism in a category, power series; $\beta(X)$: homomorphism of formal group laws; β_*: induced morphism of curve modules

Incidental notations β_i: certain elements of $MU_*(\mathbf{CP}^N)$; β: isomorphism $\mathscr{C}(\hat{\mathbf{G}}_m^-; A) \simeq \Lambda(A)$

■ Γ, γ Standard notations

$\Gamma(K, L \to \Omega)$ set of K-embeddings of L in Ω
$\gamma_x(t)$ canonical curve in $\mathscr{C}_q(G(M, \eta); B)$ associated to $x \in M$, $\gamma_x(t) = \beta_0(x)$, (30.1.7)
$\gamma_C(t)$ universal curve $\sum^F C_i t^i$, $\varepsilon_q(\sum^F c_i t^{q^i})$, $\varepsilon_p(\sum^F C_i t^{p^i})$

Generic notations $\gamma(t)$: curve in a formal group law; $\Gamma(X, Y)$: formal group law (usually over characteristic p field); Γ: topological group, Galois group; γ: algebra or module morphism

Incidental notations γ^i_{jk}: structure constants, 36.2; Γ_i: subvector spaces of $\mathrm{gr}_n(D)$, (28.2.2); $\Gamma(X)$: homogeneous polynomial

■ Δ, ∂, δ Standard notations

δ_{ij} Kronecker index, $\delta_{ij} = 0$ if $i \neq j$, $\delta_{ii} = 1$
Δ_i $= (0, \ldots, 0, 1, 0, \ldots)$ with 1 in the ith spot; $\Delta_0 = (0, 0, \ldots)$
Δ_A, Δ $W(A) \to W(W(A))$, (functorial) Artin–Hasse exponential, (15.3.9), (15.3.10)
$\Delta_{p^\infty, p^\infty}$, $\Delta_{p^\infty, A, p^\infty}$ $W_{p^\infty}(A) \to W_{p^\infty}(W_{p^\infty}(A))$ Artin–Hasse exponentials, (15.3.10)
Δ^A $W^A_{q,\infty}(-) \to W^A_{q,\infty}(W^A_{q,\infty}(-))$, ramified Witt vector Artin–Hasse exponential, 25.7
Δ^F $W^F_{q,\infty}(-) \to W^F_{q,\infty}(W^F_{q,\infty}(-))$, Artin–Hasse exponential
$\delta_y(t)$ $= \tilde{g}^{-1}(yt) \in \mathscr{C}_q(\tilde{G}; B)$, $\tilde{G} = G(\pi, \eta)$, $y \in \zeta M$, (30.2.23)
$\dfrac{\partial \cdots}{\partial \cdots}$ partial differentiation

Generic notations ∂: derivation, element of a divided power sequence; δ: sum morphism $C \amalg C \to C$; $\delta(t)$ curve, especially element of a V-basis; δ: coalgebra morphism

Incidental notations Δ_t: certain homomorphism $R(F) \to A$, 36.2; Δ: diagonal map of $U\mathfrak{g}$ (37.4.1), 14

■ ε **Standard notations**

ε_p, ε_p^F, ε_q^F canonical projectors $\mathscr{C}(F; -) \to \mathscr{C}_p(F; -)$, $\mathscr{C}(F; -) \to \mathscr{C}_q(F; -)$, also canonical projector $W(-) \to W_{p^\infty}(-)$ and $\Lambda(-) \to \Lambda_{p^\infty}(-)(\varepsilon_p^\wedge)$

Generic notations ε: counit morphism of a coalgebra or cogroup object; $\varepsilon(t)$: curve

Incidental notations ε_n, $\varepsilon_{n,m}$: projectors $W(-) \to W_n(-)$ and $W_n(-) \to W_{n,m}(-)$

■ η **Standard notations**

η_u, η_v element of $K_\sigma[\![T]\!]$ associated to the sequences $u = (u_1, u_2, \ldots)$, $v = (v_1, v_2, \ldots)$, 20.3

η, η_F isomorphism $W^F(-) \xrightarrow{\sim} \mathscr{C}_q(F; -)$

Generic notations η: semilinear endomorphism of a module, 13.2, 30.1; η: indeterminate, element of $K_\sigma[\![T]\!]^{m \times n}$, element of $\mathbf{D}_\nabla(k)$ and similar rings; $\eta(t)$ curve

Incidental notations $\eta(t)$: sequence of elements in $tU(F)[\![t]\!]$

■ ζ **Standard notations**

ζ_m primitive mth root of unity

ζ, $\zeta(X)$ endomorphism $\zeta(X) = X^p$ of formal group law defined over $\mathbf{F}_p$

ζ^A, $\zeta^A(X)$ prime element of D_h^A

Generic notations ζ: σ^{-1}-semilinear endomorphism of a module, element of E (28.4), $K_\sigma[\![T]\!]$, and similar rings

■ Θ, ϑ **Generic notations** ϑ, ϑ_c: element of $\mathbf{D}_\nabla(k)$, $K_\sigma[\![T]\!]^{m \times n}$ and similar rings

Incidental notations Θ: various important isomorphisms, e.g., $L \simeq \mathbf{Z}[R]$, (21.1.14), $\vartheta(s)$ polynomial, (37.5.11)

■ ι **Standard notations**

ι_n element $(0, 0, \ldots, 0, 1, 0, \ldots) \in W(A)$

$\iota_F(X)$, $\iota(X)$ vector of power series such that $F(X, \iota(X)) = 0$

Generic notations ι: coinverse morphism of a cogroup object

Incidental notations ι_1, ι_2, ... Witt vector additive inverse polynomials, 17.1

■ κ **Generic notations** κ: index set, usually finite subset of a larger index set, various canonical embeddings of a ring in another, e.g., $\mathbf{Z}[V] \to \mathbf{Z}[U]$, $V_i \mapsto U_{p^i}$

■ Λ, λ **Standard notations**

$\Lambda(A)$ $= 1 + tA[\![t]\!]$, ring-valued functor
λ^i ith "exterior power operation" in a λ-ring
$\hat{\Lambda}(A)$ formal completion of the abelian group functor $\Lambda(A)$
$\Lambda(F)$ points of finite order of a formal group F; i.e., torsion subgroup of $F(K_{sc})$

Incidental notations λ: finite subset of an index set; $\lambda_i^{(n)}$: integers such that $\sum \lambda_i^{(n)} \binom{n}{i} = \nu(n)$; Λ, $\Lambda(G)$: ring of integers of $\mathbf{Q}_p(\varepsilon_G)$; $\Lambda^A(G)$: ring of integers of $K(\xi_G^A)$; λ_a: endomorphism of $\mathbf{U}$; λ_n element of $U(F)$

■ μ **Standard notations**

$\mu(n)$ Möbius function, (16.3.11)
$\mu(n, d)$ certain integer valued function, 5.7

Generic notations μ, μ_F: comultiplication morphisms of coalgebra, bialgebra, cogroup objects; μ: homomorphism in $\mathbf{Mod}_\sigma(B)$, $\mathbf{Mod}(B)$

■ ν **Standard notations**

$\nu(n)$ $= 1$ if $n \in \mathbf{N}$ is not a power of a prime number or if $n = 1$,
$= p$ if $n = p^r$, $r \in \mathbf{N}$, (1.6.4), (4.4.1)
$\nu_p(n)$ $= 1$ if n is not a power of the specific prime number p,
$= p$ if $n = p^r$, $r \in \mathbf{N}$, (3.1.7)

Generic notations ν: morphism in $\mathbf{Mod}_B$

■ ξ **Standard notations**

$\xi_F(X)$, $\xi(X)$, $\xi_G(X)$, $\xi^A(X)$ Frobenius endomorphism X^q of formal group law or formal A-module over $\mathbf{F}_q$
ξ, ξ_n canonical (very ample) line bundle over $\mathbf{CP}^n$
$\xi(t)$ $= 1 + Z_1 t + Z_2 t^2 + \cdots$ standard curve in $\mathbf{U}$ or $\mathbf{U}^c$

Generic notations ξ_i, ξ: indeterminates, 17.2

Incidental notations ξ_n: primitive nth root of unity

■ Π, π **Standard notations**

$\pi(F)$ uniformizing element attached to a one-dimensional formal A-module over A, 8.3
π, π_L, π_K uniformizing element of the discrete valuation ring K, L
$\Pi_i(X; Y)$ ith Witt vector multiplication polynomial, 17.1

■ ρ **Standard notations**

ρ_F $A \to \mathrm{End}_B(F(X, Y))$ structure morphism of a formal A-module

ρ_S^A structure morphism of $F_S^A(X, Y)$
ρ_V^A structure morphism of $F_V^A(X, Y)$
$\rho_{V.T}^A$ structure morphism of $F_{V.T}^A(X, Y)$

Incidental notations ρ: reduction homomorphism $\mathscr{C}_p(F; \mathbf{Z}_p) \to \mathscr{C}_p(\bar{F}; \mathbf{F}_p)$, certain ring homomorphism $\mathbf{Z}[U] \to \mathbf{Z}[V]$ (16.4.2), morphism in $\mathbf{Mod}_B$, element of R, certain map $U(F) \to \mathbf{Mod}T_A(R(F), R(F))$, (38.2.7)

■ Σ, σ **Standard notations**

σ_i ith elementary symmetric polynomial
Σ_n^F nth Witt-like addition polynomial associated to the formal group law $F(X, Y)$, 15.3, (25.1.1)
Σ_i ith Witt vector addition polynomial
Σ_n^U $= \Sigma_n^F$ with $F(X, Y) = F_U(X, Y)$

Generic notations σ: Frobenius (like) endomorphism of various rings, e.g., $W_{p^\infty}(A)$, (28.1.9)

Incidental notations σ: certain map $\mathbf{Mod}T_A(R(F), R(F)) \to U(F)$, (38.2.7)

■ τ **Standard notations**

τ Teichmüller mapping $k \to R$ of the perfect residue field of a complete noetherian local valuation ring into that ring

Generic notations τ: switch morphism $C_1 \amalg C_2 \to C_2 \amalg C_1$ in a category; τ^A: Frobenius endomorphism of $W_{q.\infty}^A(-)$; τ, τ_i: elements of a Galois group; τ morphism in $\mathbf{Mod}_B$

■ Φ, ϕ **Standard notations**

$\Phi(t)$ unit element of the ring $\Lambda_{p^\infty}(A)$, (17.2.14)
$\Phi_G(x)$ minimum polynomial of ξ_G in $\mathbf{Q}_p(\xi_G)$

Generic notations ϕ: morphism of algebras, rings, coalgebras, bialgebras, or modules; $\phi(t)$: curve in a formal group or bialgebra; ϕ_i: element of $U(F)$; ϕ_*: homomorphism $\mathscr{C}(F; A) \to \mathscr{C}(\phi_* F; B)$ induced by $\phi: A \to B$; $\Phi(X, Y)$: formal A-module (over characteristic p field)

Incidental notations Φ: object; Φ_χ, Φ_Γ, Φ: certain fields, (35.2.8); ϕ_y, ϕ_z: certain homomorphisms, (35.2.6); $\phi_n(X, Y)$: certain polynomials, 17.1

■ χ **Generic notations** χ: homomorphism of algebras, rings, or Lie algebra

■ Ψ, ψ **Standard notations**

$\Psi_F(x)$ characteristic polynomial of a one dimensional formal group law over a finite field, (18.5.3), (18.5.4)
Ψ^n Adams operations (in a λ-ring), (E.2.1)
$\Psi_F^A(x)$ characteristic polynomial of a one dimensional formal A-module over a finite field, (24.5.2)

Generic notations ψ: Lie morphism, homomorphism of rings or algebras

Incidental notations Ψ: object, isomorphism $\mathrm{Iso}(\mathbf{F}_q, h) \to \mathrm{Tr}$, polynomial; Ψ: forgetful functor

■ Ω, ω **Standard notations**

Ω very large algebraically closed field

$\Omega_i^F(a)$ certain elements of $W_{q,\infty}^F(B)$, determining its A-module structure

$\Omega_i^A(a)$ *idem* for $F(X, Y) = F_\pi$

Generic notations ω: (invariant) differential

Incidental notations ω: element of K, (25.9.1)

INDEX

A

Abelian variety, lifting of, B.2.2
Adams–Novikov spectral sequence, B.4.4
Adams operations (in λ-rings), E.2.1
  connection with Frobenius operators, E.2.1
A-height, *see* Height
A-logarithm of a formal A-module, 21.5.7
Algebroid, formal group law, E.4.7
Antipode
  in a bialgebra or Hopf algebra, 37.1.6, uniqueness and preserving of, T37.1.10
Approximation theorem, strong, of algebraic number theory, 20.5.5
Artin–Hasse exponentials
  classical, 17.5, T17.5.4
  related example, E1.6, E21.1.10
  "twisted," 25.9.15
  Δ_A: $W(-) \to W(W(-))$, 15.3, T15.3.9, T15.3.10, T17.6.17
  in connection with the "tapis de Cartier," 30.3.28
  in λ-rings, E.2.1
  generalization for ramified Witt vectors, 25.3.28, 25.3.35, T25.7.4, T25.7.10
  "Global," 25.8.3
  "quotients" of Δ_A, T17.6.21
  reduced, as isomorphism $\bar{E}^F$: $W^F(A) \to \mathcal{G}(F; A)$, 15.3, T15.3.12
Atkin–Swinnerton Dyer congruences, 33.2

B

Barsotti–Tate group, B.2.1
Bialgebra, D37.1.2
  contravariant
    of a formal group law, 36.1.4
    of a formal group scheme, 37.3.1
  covariant
    of a formal group law, 36.1.5
    of a formal group scheme, 37.3.1
    of the Witt vector, T36.1.11, T37.5.14
  $(\mathbf{U}, \mathbf{U}(n), \mathbf{U}^c)$, E37.5.13, E37.5.14, E38.1.6
Binomial coefficients lemma, 4.2
  connection with comparison lemma, 4.3
Brown–Peterson cohomology, 31.1.19, D34.3.8
  cohomology operations, 34.5.2, T34.5.7–34.5.9
  generators for, 31.1.10, 34.4.4
  universality of, T34.3.11

C

Campbell–Hausdorff
  formula, 14.4.10, 38.2.12
  formula over $\mathbf{Z}_{(p)}$-algebras, T38.4.7
  theorem, 14.4.14, 38.2.12
Cartier duality, 36.1.9, 36.1.10, 36.2.9, 37.2.6
  for Witt vectors, T37.3.12
Cartier's theorems
  first theorem
    for formal A molecules, T29.2.1
    general, T27.1.14
    over $\mathbf{Z}_{(p)}$-algebras, T27.7.5
  second theorem
    for formal A-modules, T29.4.1
    general T27.3.5
    over $\mathbf{Z}_{(p)}$-algebras, T27.7.10
  third theorem
    for formal A-modules T29.5.1
    general, T27.5.7
    over $\mathbf{Z}_{(p)}$-algebras, T27.7.14

Cartier-Dieudonné modules, D26.1, Chapter V
Characteristic polynomial
of a formal A-module over a finite field, D24.5.1, T24.5.3
of a formal group law over a finite field, D24.2.1, T24.2.6
Characteristic zero, ring of (= additive torsion free ring), 1.6
Chern classes, 31.1.1
Class field theory
global, over function fields, B.1.1
local, 32
other, B.3.2
Coalgebra, 37.1.1
Cobordism, *see* Complex cobordism
Cocommutative
coalgebra, 37.1.1
cogroup object, 36.1.1
bialgebra, 37.1.2
Cocycle
cohomologous, 24.1.1
lemma, E.1.2, *see also* Binomial coefficients lemma, Multinomial coefficient lemma
1-(Galois cohomology), 24.1.1
splitting, 24.1.1
Cogroup object in a category, 36.1.1
Cohomology operations
in BP, 31.1.12, 34.5.2, T34.5.7–34.5.9
in MU, 31.1.8, 34.1.4, 34.1.11, T34.1.10
Commutative group object, 36.1.1
bialgebra, 37.1.2
Comparison lemma
connection with binomial coefficient lemma, 4.3
for higher dimensional formal group laws, 11.4.12
for one dimensional formal A-modules, 21.2.4
for one dimensional formal group laws, 1.6.6, 5.7.5
for p-typical formal group laws, 20.1.7
Complex cobordism, *see also* Formal group law of complex cobordism
cohomology, T31.1.5, T34.1.3
generators for, 31.1.10, T34.2.9, 34.4.1
Complex orientation of MU, 34.1.2
Complex oriented
cohomology theory, 31.1.1
formal group law of, 31.1.2
map, 34.1.1
Convolution product, 37.1.3
Crystalline cohomology, B.2.3, 26.5.10
Curve lemma (= faithfulness of $\mathcal{C}(-; A)$ on the category of smooth formal schemes, 27.3.1)
Curves
in a formal group law, 1.2, 9.3, 15.1
in a formal group or a covariant bialgebra, 36.3.1, 38.1.2
isobaric, D38.4.2
of order n, 38.1.5
pure, D38.4.2, T38.4.5
p-typical, 16.3, T16.3.1
decomposition of, T16.4.18, T38.4.4
q-typical, 25.2.6
representability of the curve functor, T38.1.7, 38.1.10, *see also* Cartier's first theorem
Curvilinear, *see* Formal group law

D

Decomposition of a curve into a sum of p-typical ones
commutative case, T16.3.8, T16.4.18
noncommutative analogue, 36.3.9, 38.4.5
Deformation (of a formal group law), 18.5.14
Derivation, 38.2.10
semi-, 38.2.14
Dieudonné module, E.1.1, E.4.1, 26.1
Dieudonné ring, $\mathbf{D}(k)$, $\mathbf{D}_{\mathbf{v}}(k)$, 28.3.5
Dieudonné algebras $\mathbf{D}^{\Delta}(k')$, $\mathbf{D}^{\Delta}_{\mathbf{v}}(k')$, 29.6.1
Directed (ordered) index set, 37.2.3
Dirichlet series, formal group associated to, 33.1.1
Distinguished element of $\mathcal{E}$, 28.4.11
Distinguished polynomial, A.3.1
Divided power
sequence
in a coalgebra, 38.2.1
of module endomorphisms of an algebra, 38.2.8, T28.2.11
structure on an ideal, 38.2.2, E.6.4
Division algebra, central, 20.2.16, 23.1.4
Dual module
linear 37.2.6
topological linear, 37.2.6
Duality
additive, of the Witt vectors, T37.5.9
Cartier, 26.2.9, 36.1.9, 36.1.10, 37.2.6, T37.3.12
Pontryagin, 37.3.4, 37.3.11
of the Witt vectors, T37.5.5, T37.5.8
Dwork integrality lemma, 2.3.4

E

Eisenstein polynomial, 18.5.4, 18.5.10
  as characteristic polynomial of a formal group law, 24.2.7, 30.4
Elliptic curves, 33
Elliptic module, B.1.1
Embedding theorem (division algebras), 23.1.4
Endomorphism ring
  absolute-, 18.4.3, 23.2.6
  over characteristic p rings, T20.4.4
  of $F_h(X, Y)$, T20.2.13
  of formal A-module of A-height h over characteristic p field, T21.8.17
  formal group with pregiven absolute endomorphism ring, T35.5.9
  of $F_V(X, Y)$, T20.1.12
  of generalized, Lubin-Tate formal group laws, T13.2, T20.1.21, T20.1.22, T20.1.24
  injectivity of the reduction map, 23.2.2, T23.2.6
  of one dimensional formal A-module over finite field, 23.1.6
  of one dimensional formal group law
    over finite field, 23.1.3
    over separably closed field, T18.2.3, T20.2.14
  of W(-), T37.5.9
  of $\hat{W}(X, Y)$, T27.2.12
Endomorphisms, conditions for existence, 20.1.8
Entwined pair of functions, D27.4.9, T27.4.15
Enveloping algebra, *see* Universal enveloping algebra
E-pure sequence D38.4.3, T38.4.5
Equivariant bordism, B.4.7
Euler classes, 31.1.1, 34
Euler factor (of a Dirichlet series), 33.1.1
Existence theorem (= Cartier's third theorem), 27.5.7, 27.7.14, 29.5.1
Exponent sequence, 34.5.3
Extension, universal, with additive kernel, 30.3

F

Faithfulness theorem (= Cartier's second theorem), 27.3.5, 27.7.10, 29.4.1
Filtered ordered set, 37.2.3
Filtration
  on a power series ring, A.2
  on a $\mathbf{Z}_p$-module, 18.3.9
Final object in a category (= object E such that $\#\, C(C, E) = 1$ for all $C \in \mathbf{C}$),
Form (K/k-form) of a formal group law, D24.1.1, T24.1.14
  philosophy of, 18.5.3
Formal A-module, D18.6.1, D21.1.2, E21.1.6-21.1.10, T21.6.2
  A-typical, D21.5.5, T21.5.6, T21.5.9, D25.4.28, T25.4.29
  A-typification of, 21.7.17
  characterization of infinite height, T21.8.4
  comparison lemma, 21.2.4
  functional equation, D21.8.5
  height, 21.8.1
  higher dimensional universal, C25.4.3 T25.4.11, T25.4.16
  infinite dimensional, 29.1
  structure of the underlying algebra of a universal formal A-module, T21.3.5
  twisted, 25.10
  universal A-typical, C25.4.3, T21.5.9, T21.5.6
  universal one dimensional, D21.2.1, T,C21.4
Formal A-module, classification results
  over A theorem T22.2.1
  classification up to isogeny over algebraically closed field T29.8.3
  over a finite field, T24.5.3
  via the module of q-typical curves, T29.4.1, T29.5.1
  moduli for, T22.4.4
  one dimensional
    over separably closed field, T21.9.1
    over unramified extension, T21.8.9
  via the "tapis de Cartier," T30.3.27
Formal group, D37.3.1
  associated to a formal group law, 1.3, 9.3, 37.3
  ($D(U)$ is smooth), T38.1.10
  historical note, E.1.1
  smooth, 37.3.1
Formal group law
  additive, 1.1.5
  algebroid, E.4.7
  attached to a differential equation, B.3.1
  of Brown-Peterson cohomology, T34.3.11
  curvilinear, D12.2.1, T12.3.6, T27.4.15
  of complex cobordism, T31.1.6, T34.2.10, T34.2.16
  of a complex oriented cohomology theory, 31.1.2
  of a Dirichlet series, T,D31.1
  curvilinear universal, C12.2, T12.3.2
  functional equation, 18.2.4, D20.1.1, T20.1.3

Formal group law (*contd.*)
higher dimensional D9.1
universal D9.5, C11.1, T11.1.5, universal *p*-typical, C10.3, E10.5
infinite dimensional, D9.6.1
universal, 9.6.8
Lubin–Tate, 8.2, 13.2, 30.2
multiplicative, 1.1.5
one dimensional, D1.1
universal, D1.5, C5.2, T5.3, T5.5 *p*-typical, C2.3
p-typical, D15.2.1, T15.2.3
Formal group law, classification results
up to isogeny over algebraically closed fields, T28.5.9
up to isomorphism over algebraically closed field, E4.7
via the module of curves, T27.3.5, T27.5.7, T27.7.10, T27.7.14
one dimensional
over an algebraically closed field, T18.5.1, T19.4.1
over a finite field, T18.5.4, T18.5.9, T24.2.16, T24.4.2
moduli for, T22.4.16
over *p*-adic integer ring with large END ring, T23.3.1
over $\mathbf{Z}_p$, $\mathbf{Z}_{(p)}$, T22.1.10, E22.1.12, E22.1.15
via the "tapis de Cartier," 26.5
Formal group law chunk, D5.7.1, T5.7.3, T5.7.4
Formal minimal model of an elliptic curve, 31.4.2
Formal structure of an algebraic variety, B.3.1
Free algebra, 14.4.3
Free associative algebra, 14.4.5, T14.4.9
Free Lie algebra, 14.4.7, T14.4.9
Free magma, 14.4.1
Frobenius endomorphism
of a formal A-module, D24.5.2, T24.5.3
of a formal group law, T24.3.4, T24.3.6
lifting, 24.2.1
of the Witt vector functor, 15.3.9, 15.3.10, D,C,T17.3
Frobenius homomorphism $F(X, Y) \to \sigma_* F(X, Y)$, 30.1.1
Frobenius operator
as Adams operators, E.2.1
associated to π on $\mathscr{C}_q(F; B)$ for formal A-modules, D25.5.3, T25.5.16, T25.6
on $\mathscr{C}(F; A)$, D15.1, T15.1.9, T16.2, D38.3.7
"twisted," 25.9
Functional equation
formal group law, 18.2.4
historical note on lemma, E.1.2
infinite dimensional, lemma E.3.9
lemma, 2.2, 10.2
type of, 2.2

G

Γ-extension, B.3.2
Γ-group, 24.1.1
Galois cohomology, 24.1
Group, *see* Formal group, Formal group law, Cogroup
finite, scheme, E.4.1
object in a category, 36.1.1
scheme, affine, 37.3.3

H

Height
filtration on $\mathbf{FG}_A(F(X, Y), G(X, Y))$, 18.3.2, T18.3.13
of a formal A-module, A-height, 18.6.2, 21.8.1, 29.7
of a formal group law, 18.3.1–18.3.8, in terms of curve modules, 28.2.1, T28.2.9
Homomorphisms of formal A-modules, D21.1.2, over characteristic p fields, T21.8.11
Homomorphisms of formal group laws, D1.4, D9.4, D18.1
conditions for existence, 20.1.10, 20.3.9
injectivity of the reduction map, T18.3.7
Homomorphisms of Lubin–Tate formal group laws and formal A-modules, T20.1.23, 30.2
Homothety operators, D15.1, T16.2, D38.3.1
Homotopy groups of the spheres, B.4.4
Hopf-algebra, 37.1.7, B.4.5
Hopf-ring, B.4.6
Hurewicz map, 31.1.10
Hyperalgebra (of a formal group law), 36.1.5

I

Implicit function theorem, formal, A.4.7
Initial object in a category (object I such that $\# \mathbf{C}(I, C) = 1$ for all objects $C \in \mathbf{C}$),
Invariant, left
A-module homomorphism of a bialgebra, 36.3.4, 38.2.6
differential form on a formal group law, 5.8

Inverse function theorem, formal, A.4.5
Isogeny, D28.3.4, T28.3.8
  connection with lattices and Tate modules, 35.4.2
Isomorphism of formal A-modules, D21.1.2
  universal, A-typical, C21.7.1, T21.7.9
Isomorphism of formal group laws, D1.4, D9.1, D18.1
  strict, D1.4, D9.1, D18.1
  universal strict, C19.1.10, T19.1.18
  universal strict p-typical, 18.1.2, T19.2.6, T19.3

J

Jacobian matrix of a morphism D9.4, D18.1

K

K-theory, algebraic, B.2.3
K-theory, topological, (extra) ordinary, B.4.1
Kummer theory (for formal group laws), B.1.2

L

λ-ring, E.2.1, 17.2
  universal, on one generator, E.6.3
Landweber-Novikov operators, 31.1.8
Lie algebra
  of a formal group (law) D9.7, D14.1, D37.5.13, T14.2.3
  free, D14.4.7, T14.4.9
Lie morphism, 14.3
Lie theory, formal, 14.2.3, 37.4
Lie's third theorem, formal version, 14.5, 37.4.11
Lifting (a formal group law), 18.5.14
Local-global theorems (for formal group laws), 20.5
Logarithm
  A, of a formal A module, 21.5.7, 25.4.6
  of a formal group law, 5.4
  of the formal group law of complex cobordism, T31.1.7, T34.2.14
  relation with $\log(1+z)$, 36.3.1, 38.3.3
Lubin-Tate formal group law (formal A-module)
  adjointness theorem, T30.2.9, T30.2.10
  as functional equation formal group laws, 8.3.6, 13.4
    generalized, E9.7, D13.2.1, D30.1.8
    more dimensional, 13.3
  isomorphism theorems for, T8.3.9, T8.3.22, T8.3.23, T20.1.25
  lifting theorem, T30.2.26
  one dimensional, D8.1.2, T8.1.5, T8.3
  recovering $(\mathbf{M}, \eta)$, T30.1.30
  relation with Artin-Hasse exponentials, ramified Witt vectors, T25.9.19, T30.3.28
  "twisted," 13.2.4, T25.9.19
  universal extension theorem, T30.3.9
Lubin-Tate lemma, 8.1.2, 13.3.4

M

Magma, free 14.4.1
Milnor hypersurface, 34.2.7
Moduli, formal, 18.5.14, 22.3
Multi-index, 9.6, 11.12
Multinomial coefficient, 11.3.2
  lemma, 11.3.4

N

Norm map for formal groups, B.3.2

O

Operations, cohomology
  stable multiplicative, B.4.2
    in BP-theory, 34.5
    in MU-theory, 34.1
Operators on $\mathscr{C}(F; A)$, $\mathscr{C}_p(F; A)$, D15.1, T16.2, D27.2.3, T27.2.9
  composition, 27.2.1
  ring of, 27.2.11
    description as an overring of Witt vectors, T28.1.16
Operators on $\mathscr{C}_q(F; B)$ (for formal A-modules) D29.3.1
  algebra of, T29.3.15
    description as an overring of $W^A_{q,\infty}(-)$, T29.6.8
Order (in a local field), T35.5.9
Oriented, *see* Complex oriented

P

p-divisible group, E.1.8, E.1.4, B.2.1
Poincaré-Birkhoff-Witt theorem, 14.3.6, 36.2.8
Pontryagin duality, 37.3.4, 37.3.11
Primitive element of a bialgebra, 37.5.13

Primitive polynomial, a polynomial (over **Z**) such that the greatest common divisor of its coefficients is 1
Pseudobasis, 37.2.1
p-typical curve, D15.2.2
  criterion, T15.2.4, T38.4.4
p-typical formal group law, D15.2.1
  criterion, T15.2.3, T15.2.6
p-typical formal group law, universal, 10.3, 15.2.8
p-typification in topology, 34.3

Q

q-typification (for curves in formal A-modules), 25.2, 25.5.17, 29.1.8
Quillen splitting (decomposition) of $MU^*_{(p)}$, 34.3.10
Quillen-Landweber-Novikov operations, 31.1.12

R

Rank of a homomorphism of formal group laws, 28.3.4
Reciprocity
  homomorphism, 32.2
  quadratic, B.1.2
Reduced Cart(A)-module, 26.1.7
Reduced Cart$_A(B)$-module, 29.5.4
Reduced Cart$_p(A)$-module, 26.2.2, 27.7.20
Reduction map, injectivity of, T18.3.7, T21.8.19
Representation ring of the symmetric groups, E.6.3
Representation theorem (= Cartier's first theorem), T27.1.14, T27.7.5, T29.2.1, T37.5.1
Ring filtration, A.2

S

Šafarevič mapping, 32.4
Šafarevič-Weil theorem, E.5.1
Šafarevič-Tate group, B.3.2
Semiderivation, 38.2.14
Semilinear endomorphisms, Cartier's trick, 13.2, 30.1
$\sum$-notation, 37.1.5
Skolem-Noether theorem, 20.2.16
Structure coefficients $c(p, r, i, j)$, 27.4.1, 27.7.14
Supernatural number, 17.4.1
Support
  of a multiindex, 9.6
  conditions, monomials have finite, 9.6.3, 27.1.3
Switch morphism, (morphism which interchanges the two factors of a direct sum or product)
Symmetric groups on n letters, representation ring of, E6.3

T

Tate module of a formal group law, D35.3.1, T35.3.19, TE.5.4,
  connection with isogenies, T35.4.2
  as a Galois-module, T35.6.2
Teichmüller mapping, 17.4.8
Thom classes, 31.1.1
Torsion free, A-torsion free ($= B \to B \otimes_{\mathbf{Z}} \mathbf{Q} \to B \otimes_A K$ injective)
Type of a functional equation, 2.2

U

Universal *see also* Formal A-module, Formal group law, Isomorphism
Universal enveloping algebra of a Lie algebra, D14.3.1, C14.3.3, T14.3.6
  as covariant bialgebra, T36.2.6
Universal λ-ring on one generator, E6.1

V

Valuation on $W_{p^s}(A)$, 17.4.12
V-basis, D16.1.10, D27.1, T38.4.1, T16.1.10
Verschiebung
  endomorphism of the Witt vectors, 17.3
  homomorphism $\gamma: \sigma_*\Gamma(X, Y) \to \Gamma(X, Y)$, 30.1.1
  operator, 15.1, 38.3.1, T16.2

W

Weierstrass preparation theorem
  formal, A.3
  twisted formal, 20.3.13
Witt vectors
  associated to the prime p, 17.4.1
  duality of, T37.5.5, T37.5.8, T37.5.12, E.5.3

formal group law associated to a formal group, 25.1
formal group law of, associated to the prime p, 27.7.4
formal group (law) of big, 17.1.18
the functor of big, 17.1, T17.2
group scheme of, 17.2.11
like group functor associated to a formal group, 15.3, 25.1, T15.3.9, T15.3.10
operators on, 17.3
ramified, 18.6.13, T25.3.25, T25.3.26
ring of endomorphisms of the formal group of big, T27.2.12
ring of endomorphisms of the functor of big, T37.5.9
supernatural quotients of the big, 17.4.1

Z

Zeta function of an elliptic curve, 33.1
$\mathbf{Z}_p$-extension, B.3.2