JOURNAL OF NUMBER THEORY 37, 242–252 (1991)

Gauss Sums for Function Fields

DINESH S. THAKUR

School of Mathematics, TIFR, Bombay 5, India

Communicated by D. Goss

Received January 2, 1990; revised March 11, 1990

In this paper, we study the behaviour of "Gauss sums" (introduced in [Th1, Th2]) for function fields of one variable over finite fields. We will show (Section 1) that their prime factorization is analogous to the classical case for the rational function field (at least when the infinite place chosen is of degree not more than two) and is quite interesting, though different for higher genus fields. Classically, the factorization of Gauss sums for composite modulus into those for its prime power factors, gives control on their absolute values and is quite important in "the local constants decomposition." In our case, the situation is wildly different (Section 2). All these results should be seen in the light of various analogies established in [Th2].

0. CYCLOTOMIC THEORY FOR FUNCTION FIELDS

Gauss sums arise naturally and play a prominent role in the cyclotomic theory, which is essentially a theory of abelian extensions over $\mathbf{Q}$ by the Kronecker–Weber theorem. For a function field K of one variable over a finite field, in addition to the usual cyclotomic extensions $K(\mu_n)$, which are just constant field extensions, there are, of course, many more abelian extensions of K, like Kummer or Artin–Schreier extensions. Carlitz [Ca], Drinfeld [Dr], and Hayes [Ha1, Ha2, Ha3] provided families of abelian extensions of K analogous to the cyclotomic extensions over $\mathbf{Q}$. We now describe these and summarize their main properties. For details and more general notions, which we will not need, see the papers of Hayes referred to above. (See also [GR, Go]).

DEFINITIONS. Let K be a function field of one variable over its field of constants $\mathbf{F}_q$. Let ∞ be a place of K and let A be ring of elements of K integral outside ∞.

Fix an algebraic closure $\bar{K}$ of K, as our universe. Let $\bar{K}^+$ be its underlying additive group and $\mathrm{End}(\bar{K}^+)$ be its ring of endomorphisms. For subring $L \supset A$ of $\bar{K}$, let $L\{F\}$ denote the noncommutative ring generated

0022-314X/91 $3.00

by elements of L and by a symbol F, satisfying the commutation relation $Fl = l^q F$, for all $l \in L$. Then $L\{F\}$ can be thought of as subring of $\mathrm{End}(\bar{K}^+)$ in an obvious fashion.

By a Drinfeld A-module D over L (in fact, of "rank one" and of "generic characteristic;" but we will drop these words), we will mean an injective homomorphism $D: A \subsetneq L\{F\}$, $(a \in A \mapsto D_a \in L\{F\})$ such that degree of D_a as a polynomial in F is the same as a degree of a and the constant term (i.e., coefficient of F^0) in D_a is a. Two Drinfeld A-modules $D, \tilde{D}$ are considered isomorphic if there is a nonzero $k \in \bar{K}^*$ such that $kD_a = \tilde{D}_a k$ for $a \in A$.

For $a \in A$, put $\Lambda_a =: \{u \in \bar{K}: D_a(u) = 0\}$. This A-module (under D) is nothing but the a-torsion of D.

The analogy with the classical case is

$$K \leftrightarrow \mathbf{Q}, \qquad A \leftrightarrow \mathbf{Z}$$

$$a \in A \mapsto D_a \in \mathrm{End}\ \mathbf{G}_a \leftrightarrow n \in \mathbf{Z} \mapsto T_n =: (x \mapsto x^n) \in \mathrm{End}\ \mathbf{G}_m$$

and $\Lambda_a \leftrightarrow \mu_n$, which is the n-torsion of the usual action T of $\mathbf{Z}$ on the multiplicative group $\mathbf{G}_m$. Note that 0 is always a-torsion, just like 1 is always the nth root of 1. In fact, $\lambda \in \Lambda_a$ is an analogue of both $\zeta \in \mu_n$ and $1 - \zeta$.

Let h denote the class number of K and δ denote the degree of the place ∞, so that $h\delta$ is the class number of A.

EXAMPLES. (a) $A = \mathbf{F}_q[T]$, $h = \delta = 1$. T being a generator of A over $\mathbf{F}_q$, to give D, it is enough to prescribe a nonzero l and to put $D_T = T + lF$. All such D's are isomorphic. In this case, T^2-torsion of D is

$$\{u \in \bar{K}: D_{T^2}(u) = l^{q+1}u^{q^2} + (Tl + lT^q)\,u^q + T^2 u = 0\}.$$

(b) [Ha2, 11.3] $A = \mathbf{F}_2[x, y]/y^2 + y = x^3 + x + 1$. $h = \delta = 1$, $D_x = x + (x^2 + x)\,F + F^2$, $D_y = y + (y^2 + y)\,F + x(y^2 + y)F^2 + F^3$. Since x and y generate A and since $D_x D_y = D_y D_x$, D is well defined by this prescription.

(c) [Ha2, 11.2] $A = \mathbf{F}_3[x, y]/y^2 = x - x^2$. K is again a rational function field, so that $h = 1$, but $\delta = 2$. There is no A-module D over A, but if one considers $B = A[c]/c^2 = -1$ and puts $\eta = 1 + x + cy$, $\bar{\eta} = 1 + x - cy$ ($\eta, \bar{\eta}$ are units in B), then one has D over B given by

$$D_x = x + y\eta F + \bar{\eta}F^2, \qquad D_y = y + (1 + x)\,\eta F + c\bar{\eta}F^2.$$

Function Field Cyclotomic Theory [Ha2, Ha3]

(1) Let H (notation H_A or H_e is also used) denote the maximal abelian unramified extension of K, where ∞ splits completely. This is an analogue of the Hilbert class field (see [Ro] for more on the notion). Its

field of constants has degree δ over $\mathbf{F}_q$ and $[H: K] = h\delta$. The galois group $\mathrm{Gal}(H/K)$ is isomorphic to the class group of A. Let B be the integral closure of A in H. A prime P of A splits completely iff its ideal is principal.

(2) There are $h(A) = h\delta$ isomorphism classes of Drinfeld A-modules over $\bar{K}$. Each isomorphism class has a model over H and models in other isomorphism classes can be obtained as $\mathrm{Gal}(H/K)$ conjugates of such a model. (In fact H can be characterized as minimal or common field of definition.) Further, the model D can be chosen over B with the highest coefficient of D_a, considered as a polynomial in F, a unit in B (i.e., "good reduction everywhere") (see [Ta]). We will call such a model a normalized module.

(3) Let K_∞ (resp. k_∞) be the completion of K (resp. residue field) at ∞ and U_1 be the group of one-units at ∞. A choice of uniformizer t at ∞, gives us a splitting of K_∞^* as $k_\infty^* \times U_1 \times t^{\mathbf{Z}}$. In other words, z in K_∞^* can be written uniquely as $z = \mathrm{sgn}(z) \times \bar{z} \times t^n$, with $\mathrm{sgn}(z) \in k_\infty^*$, $\bar{z} \in U_1$, $n \in \mathbf{Z}$. This gives the homomorphism sgn: $K_\infty^* \to k_\infty^*$. There are $q^\delta - 1$ such sgn functions, depending on the choice of t. For $\sigma \in \mathrm{Gal}(k_\infty/\mathbf{F}_q)$, $\sigma \circ \mathrm{sgn}$ is called a twisted sign function and a Drinfeld module is called sgn-normalized if the highest coefficient of D is a twisting of sign. Any Drinfeld module is isomorphic to a sgn-normalized one, for a given sgn. Given sgn, let H_1 be the field generated by coefficients of a sgn-normalized D. H_1 is abelian of degree $h\delta(q^\delta - 1)/(q-1)$ over K. H_1/K is unramified except at ∞, H_1/H is totally ramified at ∞. In particular, if $\delta = 1$, $H_1 = H$. H_1 is the class field corresponding to $K^* \times t^{\mathbf{Z}} \times U_+$, where t is a uniformizer at ∞ with $\mathrm{sgn}(t) = 1$ and U_+ is the subgroup of the idele group consisting of those ideles with unit components at finite places and with the component at ∞ of sgn 1. In other words, a finite place v of K splits completely in H_1 iff v corresponds to a principal ideal xA with $\mathrm{sgn}(x) \in \mathbf{F}_q^*$. Let B_1 be the integral closure of A in H_1.

(4) Given a Drinfeld A-module D over L and an ideal I of A, define D_I to be the unique monic generator of the principal left ideal in $L\{F\}$ generated by D_i, $i \in I$. The I-torsion Λ_I is defined as

$$\Lambda_I =: \{u \in \bar{K}: D_I(u) = 0\} = \{u \in \bar{K}: D_i(u) = 0, i \in I\}.$$

If I is a principal ideal iA, then $D_I = D_i/l$, where l is the highest coefficient of D_i. Note that D_I need not commute with D_J, so that, e.g., D_I need not take P-torsion to P-torsion. If $a \in A$ is nonconstant, then D_a determines D. It is not known whether D_I, for a nontrivial ideal I determines D. (It does, when, for example, D is known to be sgn-normalized.) Let i be the coefficient of F^0 in D_I for a normalized D over B, then $iB = IB$ (explicit principal ideal theorem), see [Ro].

(5) Let D be a normalized A-module over B. Let P be a prime of A, then the polynomial $D_P(u)/u$ is Eisenstein at P. Moreover $H(\Lambda_P) = K(\Lambda_P)$ is an abelian extension of H with Galois group $(A/P)^*$ and with primes above P totally ramified. If Q is a prime of A distinct from P, then Q splits in $H(\Lambda_P)$ iff $Q = xA$ with $x \equiv 1 \bmod P$ and the highest coefficient of D_x is also congruent to 1 modulo every place $\bar{Q}$ of B above Q.

(6) Let D be a sgn-normalized A-module over H_1. Let P be a prime of A, then the polynomial $D_P(u)/u$ is Eisenstein at P. Moreover $H_1(\Lambda_P) = K(\Lambda_P)$ is an abelian extension over H_1 with Galois group $(A/P)^*$ and with primes above P totally ramified. If Q is a prime of A distinct from P, then Q splits in $H_1(\Lambda_P)$ iff $Q = xA$ with $x \equiv 1 \bmod P$ and $\operatorname{sgn}(x) = 1$. The subgroup of the idele group corresponding to the extension $H_1(\Lambda_P)$ of K is $K^* t^{\mathbf{Z}} U^*(P)$, where t is a positive (i.e., $\operatorname{sgn}(t) = 1$) uniformizer at ∞, $U^*(P)$ consists of those ideles i with $i_P \equiv 1 \bmod P$, i_Q a Q-unit for primes Q distinct from P and $\operatorname{sgn}(i_\infty) = 1$. In particular, $K(\Lambda_P)$ is independent of the choice of a sgn-normalized D. (But it depends on the choice of sgn. $K(\Lambda_P)(\mu_{(q^\delta - 1)^2/(q-1)})$ is independent of the choice of sgn also.)

Splitting criterion shows that, if one selects sgn functions appropriately and if v_1 and v_2 are distinct places of K and if Λ_{ij} $(i, j = 1, 2; i \neq j)$ denotes v_i-torsion for a sgn-normalized D for A with v_j as the infinite place; then

$$K(\Lambda_{ij})(\mu_{q^{\deg v_i} - 1}) = K(\Lambda_{ji})(\mu_{q^{\deg v_j} - 1}).$$

(7) In both (5) and (6), the primes of A other than P are unramified in the respective extensions and ramification index of ∞ is $q - 1$ and $q^\delta - 1$, respectively, with the decomposition and inertia groups the same.

Remarks. (I) Hence, one has a quite unified explicit cyclotomic theory for any K. Appearance of H in (1), (2) illustrates the analogy with the case of an elliptic curve with complex multiplication by an imaginary quadratic field. But note that in the classical case, one need not have a model over the Hilbert class field with good reduction everywhere.

(II) One obtains the maximal abelian extension of K by adjoining a-torsion of a sgn-normalized D for all nonzero a in A, letting ∞ (and with it A) also vary through all places of K.

(III) Iwasawa theory was based on the analogy with the constant field extensions ("cyclotomic") of K. In the cyclotomic theory described above, the Galois groups are much wilder than $\mathbf{Z}_p$. Even for geometric $\mathbf{Z}_p$ extensions, the class number growths are different from their classical counterpart. Also the "Iwasawa theory" for these extensions is different. (See [GK].) On the other hand, let $A = \mathbf{F}_q[T]$, D defined by $D_T = T + F$, P a prime of A of degree d, then by (6), (7) and the Riemann–Hurwitz theorem, the genus g_n of $K(\Lambda_{P^n})$ is asymptotically $d(q^d - 1)\, nq^{d(n-1)}$ as n

tends to infinity (see [Ha1, Thm. 4.1]). Now, by the Riemann-hypothesis for function fields, the class number h_n is $\prod_{i=1}^{2g}(1-\alpha_i)$, $|\alpha_i|=\sqrt{q}$, so that $(\sqrt{q}+1)^{2g_n} \geqslant h_n \geqslant (\sqrt{q}-1)^{2g_n}$, which implies that, if $q>4$ (so that $\sqrt{q}-1>1$), $\log h_n$ is of the order (in the sense that the ratio of the two sides is bounded between two positive constants) $n(\mathbf{N}P)^n$, as n tends to infinity. It is not known whether the same estimate holds in the classical case. For the minus part of the class number such estimate holds in the classical case (see [Wa, Thm. 4.20]) and also in function field case (if $q>4$), by similar considerations. But note that, in function field case, for $q=2$ the minus part of h_n is just 1 and also that there is a difference between the notions of class numbers of fields and those of their "rings of integers." By the well-known analogy (see, e.g., Weil's "Basic number theory") between q^{2g-2} (where g is genus of the function field) and the discriminant, the order of $\log h_n$ described above is analogous to that predicted by the Brauer–Siegel theorem, because the regulator of a field is 1 here.

1. Gauss Sums

Now we recall ([Th1], see also [Th2]) the definition of Gauss sums. Let D be a Drinfeld A-module. (To obtain gauss sums with good properties, one may normalize D as described below. The effect of normalization is also described below). Let P be a prime of A of degree d. Choose an A-module isomorphism $\psi: A/P \to \Lambda_P$ (an analogue of additive character $\psi: \mathbf{Z}/p \to \mu_p$) and let χ_j ($j \bmod d$) be $\mathbf{F}_q$-homomorphisms $A/P \subsetneq L$, where L is a field containing $K(\Lambda_P)$, indexed so that $\chi_j^q = \chi_{j-1}$ ($j \bmod d$) (special multiplicative characters which are q^j-powers of "teichmuller character"). Then one defines Gauss sums

$$g_j =: g(\chi_j) =: -\sum_{z \in (A/P)^*} \chi_j(z^{-1})\,\psi(z) \in K(\Lambda_P)(\mu_{q^d-1}).$$

One has [Th2] "Fourier expansion" $\psi(z) = \sum g_j \chi_j(z)$ of ψ in terms of all characters of $(A/P)^*$.

Let D be a sgn-normalized A-module. Let L be the compositum of the extensions $H_1(\mu_{q^d-1})$ and $H_1(\Lambda_P)$ of H_1, which are linearly disjoint by simple considerations (see (1), (2), (3) of Section 0). Hence the Galois group of L over H_1 is canonically isomorphic to the product of the Galois groups of these extensions. So the powers of q^δth power Frobenius for the extension $H_1(\mu_{q^d-1})$ over H_1 and elements of $(A/P)^* = \mathrm{Gal}(H_1(\Lambda_P)/H_1)$ can be thought of as elements of $\mathrm{Gal}(L/H_1)$. Then just as in [Th2, Thm. I] as ψ is nonzero, g_{j_0} is nonzero for some j_0 and hence using the Galois

action $g_{j_0+k\delta}$ is nonzero for any integer k. In particular, all g_j's are nonzero, when $(d, \delta)=1$ (e.g. when $\delta=1$). In fact, all g_j's are nonzero in general. (See note added in proof.) But just as in [Th2, Prop. I], because of $\mathbf{F}_q$-linearity of ψ, one obtains only zero "gauss sums," unless one restricts the multiplicative character as in the definition given here.

Remark. If one takes D to be just normalized rather than sgn-normalized, the same holds if one replaces H_1 by H. One also sees that, if $h=\delta=1$ then $H=H_1=K$ and the situation is quite similar to the classical case and to the case considered in [Th2].

Hence, the "norm" $G_P=:\prod_{j \bmod d} g_j^{q-1}$ lies in B_1 (resp. B if D is normalized). In [Th2, Thm. II] we saw that $G_P=(-1)^d P$ (analogue of $g(\chi)g(\bar{\chi})=\chi(-1)q$), when $A=\mathbf{F}_q[T]$, P is a monic prime and D is given by $D_T=T+F$. In particular, this implies that all g_j's lie above P in that case. We will see a different scenario in general.

Remark. Change of D to an isomorphic $k^{-1}Dk$ changes G_P to $G_P/k^{(q-1)d}$, so we assume without loss of generality that D is normalized or sgn-normalized. By $\mathrm{Gal}(H/K)$-action one can move to different isomorphism classes.

First note that Eisenstein property ((5), (6) of Section 0) of $D_P(u)/u$ at P implies that P divides G_P.

EXAMPLES. (A) If P is a prime of degree one, then using explicit principal ideal theorem of (4), Section 0, one easily sees that $G_P B=PB$.

(B) Let $q=2$ and $P\in A$ be a prime of degree two. Let $D_P=P+P_1F+P_2F^2$ and $\Lambda_P=\{\lambda_i\}$. Then a direct calculation shows

$$G_P=g_0g_1=\sum\lambda_i^2+\sum_{i\neq j}\lambda_i\lambda_j=0+P_1/P_2=P_1/P_2.$$

Since P_2 is a unit by our assumption, $G_PB=P_1B$. Example (b) in Section 0, with $P=x$, now shows that $G_P=x(x+1)$, so we see that primes other than P can also enter into the factorizations of Gauss sums.

To study this phenomenon in detail, we first focus on the case $h=\delta=1$, when the cyclotomic theory is the simplest and analogous to the classical case and to [Th2].

Apart from infinitely many (one for each q) rational function fields, there are only seven other K's of class number one, as established in [LMQ]. From the list given there, it is easy to check that $h=\delta=1$ forces A to be one of the four cases in the theorem below. (These are Examples 11.3–11.6 of [Ha2]).

THEOREM I. *When $h=\delta=1$, G_P is given by the following recipe.*

(1) ([Ha2, Example 11.3] Example (b), Section 0) $A=\mathbf{F}_2[x, y]/y^2+y=x^3+x+1$. $G_P=PP^\sigma$, *where σ is the order four automorphism of A given by* $\sigma(x)=x+1$, $\sigma(y)=y+x+1$.

(2) ([Ha2, Example 11.4]) $A=\mathbf{F}_4[x, y]/y^2+y=x^3+w$, $w^2+w+1=0$. $G_P=P(P^\sigma)^3$, *where σ is the order two automorphism of A given by* $\sigma(x)=x$, $\sigma(y)=y+1$ *and for a given sign function such that x and y have sign* 1, *representative P of sign* 1 *is chosen.*

(3) ([Ha2, Example 11.5]) $A=\mathbf{F}_3[x, y]/y^2=x^3-x-1$. $G_P=(-1)^d P(P^\sigma)^2$, *where σ is the order three automorphism of A given by* $\sigma(x)=x+1$, $\sigma(y)=y$ *and representative P is chosen as in* (2).

(4) ([Ha2, Example 11.6]) $A=\mathbf{F}_2[x, y]/y^2+y=x^5+x^3+1$. $G_P=P(P^\sigma)^2P^{\sigma^2}$, *where σ is the order four automorphism of A given by* $\sigma(x)=x+1$, $\sigma(y)=y+x^2$.

(*Remark.* (1)–(3) *are of genus* 1, *while* (4) *is of genus* 2).

Proof. When A has degree 2 element (x in our cases), one can obtain a simple expression for g_{j-1}^q/g_j as follows. $D_x=x+x_1F+x_2F^2$ gives, as in [Th2, p. 107], $\chi_j(x)\,g_j=xg_j+x_1\,g_{j-1}^q+x_2\,g_{j-2}^{q^2}$. One uses this relation to successively eliminate higher powers of g_j's from a similar relation obtained from D_y with suitable element y of higher degree (y in our cases).

Write $\chi_0(x)=\theta$ and $\chi_0(y)=\beta$, so that $\chi_j(x)=\theta^{q^j}$ and $\chi_j(y)=\beta^{q^j}$. In our four cases one obtains the following expressions for g_{-1}^q/g_0, respectively:

$$\frac{x(x+\theta)+y+\beta}{x+\theta+1}$$

$$\frac{x^2(x+\theta)+y+\beta}{x+\theta}$$

$$\frac{-y(x-\theta)+y-\beta}{x-\theta+1}$$

$$\frac{(x+\theta)(x^4+x^3+(1+\theta)x^2)+y+\beta}{x^3+\theta x^2+(1+\theta)x+\theta^2+\theta}.$$

Now note that $G_P=\prod(g_{j-1}^q/g_j)$. (The claim about the signs immediately follows from this.) Let the product of numerators of the expression (as written, without reducing) be N and the product of denominators be D. Then we claim the following equalities of ideals in our four cases, respectively:

$$N = P(P^\sigma)^2 P^{\sigma^3}, \qquad D = P^\sigma P^{\sigma^3}$$

$$N = P^2(P^\sigma)^4, \qquad D = PP^\sigma$$

$$N = P(P^\sigma)^3(P^\sigma)^\mu, \qquad D = P^\sigma(P^\sigma)^\mu$$

$$N = (PP^{\sigma^2}P^{\sigma^3})^2(P^\sigma)^4, \qquad D = PP^{\sigma^2}(P^\sigma P^{\sigma^3})^2.$$

(In the third case, μ is the automorphism of A defined by $\mu(y) = -y$ and $\mu(x) = x$.) The theorem immediately follows if we establish this claim. We will give details only for (1), others being similar. Let $P_1, \ldots, P_d$ be the primes above P, in the integral closure of A in $K(\mu_{q^d-1})$, numbered so that $x \equiv \theta$, $y \equiv \beta \bmod P_1$. We want to show (a) $\prod(x + \theta^{2^j} + 1) = P^\sigma P^{\sigma^3}$ and (b) $\prod(x(x + \theta^{2^j}) + y + \beta^{2^j}) = P(P^\sigma)^2 P^{\sigma^3}$.

Case I. $P \neq P^{\sigma^2}$.

Proof of (a). P_1 divides $x + \theta$, hence P divides $\prod(x + \theta^{2^j})$. But this product being invariant by σ^2, P^{σ^2} also divides it. Count of degrees then shows that $\prod(x + \theta^{2^j}) = PP^{\sigma^2}$. Applying σ to both sides we obtain (a).

Proof of (b). (a) and the fact that P divides G_P, imply that $PP^\sigma P^{\sigma^3}$ divides N. It is enough to show that P^2 divides N^{σ^3} or that P_1^2 divides $n_1^{\sigma^3}$, where we have put $n_j =: x(x + \theta^{2^j}) + y + \beta^{2^j}$. Now, since $x^2 \equiv \theta^2$ and $y^2 \equiv \beta^2$ modulo P_1^2, we have modulo P_1^2,

$$n_1^{\sigma^3} \equiv (x+1)(x+1+\theta^2) + y + x + \beta^2 \equiv x^3 + x + 1 + y^2 + y \equiv 0$$

as required.

Case II. $P = P^{\sigma^2}$.

Proof of (a). Write $P = a(x)y + b(x)$, $a(x)$, $b(x) \in \mathbf{F}_2[x]$. Invariance by σ^2 implies that $a(x) = 0$. As degree x is 2, the equation $P(\theta) \equiv 0$ (modulo P_1) is of degree $d/2$ in θ, $\theta = \theta^{2^{d/2}}$, which implies P_1 divides $x + \theta$ and $x + \theta^{2^{d/2}}$ and hence P^2 divides $\prod(x + \theta^{2^j})$. (a) now follows as in Case I.

Proof of (b). In Case I, we saw $(P_1^\sigma)^2$ divides n_1. Similarly, it is easy to see that P_1 and $P_1^{\sigma^3}$ divide n_0. P_1^2 divides $n_1^{\sigma^3} = n_1^\sigma + 1$. Now P_1 does not divide n_1^σ, hence $P_1^{\sigma^3}$ does not divide n_1 and so $P_1^\sigma \neq P_1^{\sigma^3}$; so that we can still conclude $N = P(P^\sigma)^2 P^{\sigma^3}$.

Remark. Results of Section 0, combined with the proof above, give factorizations of g_j's.

Now we will show that the factorization is analogous to the classical case and to [Th2], if one takes K to be the rational function field, but with an infinite place of degree 2 (e.g., Section 0, Example (c)) (Note that the

degree 1 is dealt with in [Th2].) By following the procedure in [Th2], it is enough to show that

THEOREM II. *If K is a rational function field and ∞ is a place of K of degree 2 (i.e., $\delta = 2$), then for a suitable Drinfeld A-module, g^q_{j-1}/g_j has valuation one at one of the primes of the integral closure of A in $K(\mu_{q^d-1})$ above P, valuation zero at all other finite places, and valuation zero (resp. -1) at one (resp. the other) of the infinite places.*

Proof. By Riemann–Roch, one can choose $x \in A$ of degree 2 and $y \in A$ of degree 2 distinct from $\alpha x + \beta$, for all $\alpha, \beta \in \mathbf{F}_q$ and $\alpha \neq 0$. Let D be normalized, wDw^{-1} be sgn-normalized and $c =: \operatorname{sgn}(y)/\operatorname{sgn}(x)$. Now clearly $w(D_y - cD_x)w^{-1}$ and hence $D_y - cD_x$ is of degree less than 2 in F. Expanding $D_x D_y = D_y D_x$ and using the fact that c is not in $\mathbf{F}_q^*$ (by construction), one sees that in fact it is of degree one in F. Hence, $D_y - cD_x = (y - cx) + tF$, with nonzero $t \in B$ (In Example (c) of Section 0, $t = 1$). Then as in [Th2, p. 107], one sees that

$$g^q_{-1}/g_0 = (c(x - \chi_0(x)) - (y - \chi_0(y)))/t.$$

Now t is irrelevant, since it can be changed, as we wish, by choosing suitable isomorphic model for D. The numerator is clearly divisible by a prime above P, so it is sufficient to show that the valuation of the numerator is -1 at one infinite place and is zero at the other infinite place. This is easily seen by expanding x and y with respect to local parameters at ∞. This finishes the proof.

Open problems. It will be very interesting to know (1) whether similar behaviour holds for any infinite place of the rational function field (2) the effect of change of the infinite place on the behaviour of Gauss sums (3) the factorizations of gauss sums for general A. (One should note in this respect that elements with "stickelberger factorization" (for general K) were shown to exist by Tate and Deligne and were constructed explicitly by Hayes [Ha3].) (4) whether they enter into the theory of L-functions developed by Goss.

Remarks. (1) The proof of the analogue of the Hasse–Davenport theorem in [Th2, p. 111], being of formal combinatorial nature, applies in the general case without change. We note here that in $g(\underline{a}, P')$, in the statement of [Th2, Thm. VIII], $\underline{a}$ should be replaced by $\underline{a}'$ obtained from $\underline{a}$ in obvious fashion by making the denominators $q^{rt} - 1$ using digit expansions.

(2) In [Th2, Thm. VI], we have proved an analogue of the Gross–Koblitz theorem, in case $A = \mathbf{F}_q[T]$. It does not generalize in that form, since otherwise by results of [Th1] (see [Th3]) on special values of P-adic gamma functions, the prime factors of G_P would have always been above P.

2. Gauss Sums for Composite Modulus

We restrict to $A = \mathbf{F}_q[T]$ and to D given by $D_T = T + F$ for simplicity. One can define Gauss sums for composite modulus a, just as before by replacing P by a and using isomorphism $\psi: A/a \to \Lambda_a$.

First, let P be a prime of degree d and let $a = P^n$, $n > 1$. Cardinality of $(A/a)^*$ is $q^{d(n-1)}(q^d - 1)$. As q is a power of the characteristic, a multiplicative character χ factors through $(A/P)^*$. (Order of a multiplicative character χ divides $q^d - 1$, so that $\chi^{q^d} = \chi$.) Now, $f = f_{n-1}P^{n-1} + \cdots + f_0$, where f_i run through the polynomials of degree less than d and f_0 is non-zero, are the representatives of reduced residue classes modulo a. We have $\chi(f) = \chi(f^{q^d}) = \chi(f_0)$, since $f^{q^d} \equiv f_0 \bmod P$. Hence, we have

$$g(\chi) = \sum_{f_0 \in (A/P)^*} \chi(f_0)\, \psi\left(\sum_{f_1, \ldots, f_{n-1} \in A/P} f_{n-1}P^{n-1} + \cdots + f_0 \right).$$

Using (a) ψ is $\mathbf{F}_q$-linear and (b) if a term in a sum appears a multiple of p number of times, then it contributes zero; it is easy to see

Proposition I. *When $a = P^n$, $n > 1$, P a prime of degree d, $g(\chi) = 0$ unless $n = 2$, $d = 1$ and $q = 2$ (i.e., unless $P = T$ or $T + 1$ in $\mathbf{F}_2[T]$, when $g(\chi) = \psi(P)$).*

Now classically (see [Na, p. 252–254]), if $n = n_1 \cdots n_r$ is a factorization of composite modulus n into relatively prime factors n_i, then $(\mathbf{Z}/n)^* = \prod(\mathbf{Z}/n_i)^*$ and we have the corresponding decomposition of multiplicative character χ as $\chi = \prod \chi_i$ in an obvious fashion. Put $\chi(m) = 0$, if m and n are not relatively prime and define the Gauss sum

$$g(\chi) = \sum_{x \bmod n} \chi(x) \exp(2\pi i x/n)$$

then (see [Na, p. 253]) one has

$$g(\chi) = \prod_{i=1}^{r} \chi_i(n/n_i)\, g(\chi_i).$$

If one follows the same proof [Na, p. 253], in our case, where we are dealing with additive rather than the multiplicative group, we obtain

Proposition II.

$$g(\chi) = \sum_{i=1}^{r} c_i \chi_i(n/n_i)\, g(\chi_i),$$

where $c_j = \sum_{x_i \bmod n_i,\, i \neq j} \prod \chi_i(x_i)$.

In this wierd additive decomposition, we loose control over the absolute values and even c_i's or $g(\chi_i)$'s can become zero.

ACKNOWLEDGMENTS

I thank David Hayes for various conversations regarding the function field cyclotomic theory and David Goss for his suggestion to look at Gauss sums for composite modulus. I am obliged to the Institute for Advanced Study, Princeton, where the main results of this paper were presented in the Drinfeld module seminar in 1987–1988; and to the Tata Institute of fundamental research, Bombay, for their support.

Note added in proof. Finally, we prove that g_j as defined in Section 1 is never zero: Put $\psi_\mu(z) =: \psi(\mu z)$, $\mu \in A/P$. Since the pairing $A/P \times A/P \to \Lambda_P$ defined by $(x, y) \to \psi(xy)$ is nondegenerate bilinear pairing over $\mathbf{F}_q$, any $\mathbf{F}_q$-linear function from A/P, which is a d-dimensional vector space over $\mathbf{F}_q$, to L is a linear combination of ψ_μ's. Now $\psi_\mu = \sum(\chi_j(\mu)\, g_j)\chi_j$. If g_{j_0} were zero, then ψ_μ's would be in a space generated by less than d of χ_j's, which is a contradiction.

REFERENCES

[Ca] L. CARLITZ, A Class of polynomials, *Trans. Amer. Math. Soc.* **43** (1938), 167–182.

[Dr] V. DRINFELD, Elliptic modules, *Math. USSR-Sb.* **23** (1974), 561–592. [English Translation]

[GR] S. GALOVICH AND M. ROSEN, The class number of cyclotomic fields *J. Number Theory* **13** (1981), 363–375.

[GK] R. GOLD AND H. KISILEVSKY, On geometric $\mathbf{Z}_p$ extensions of function fields, *Manuscripta Math.* **62** (1988), 145–161.

[Go] D. GOSS, The arithmetic of function fields, 2, The cyclotomic theory, *J. Algebra* **81** (1983), 107–149.

[Ha1] D. HAYES, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.

[Ha2] D. HAYES, Explicit class field theory in global function fields, *in* "Studies in Algebra and Number Theory" (G. C. Rota, Ed.), pp. 173–217, Academic Press, New York, 1979.

[Ha3] D. HAYES, Stickelberger elements in function fields, *Compositio Math.* **55** (1985), 209–239.

[LMQ] J. LEITZEL, M. MADAN, AND C. QUEEN, On congruence function fields of class number one, *J. Number Theory* **7** (1975), 11–27.

[Na] W. NARKIEWICZ, "Elementary and Analytic Theory of Algebraic Numbers," PWN (Polish Scientific Publishers), Warsaw, 1974.

[Ro] M. ROSEN, The Hilbert class field in function fields, *Exposition. Math.* **5** (1987), 365–378.

[Ta] T. TAKAHASHI, Good reduction of elliptic modules, *J. Math. Soc. Japan* **34** (1982), 475–487.

[Th1] D. THAKUR, Gamma functions and Gauss sums for function fields and periods of Drinfeld modules, Thesis, Harvard, 1987.

[Th2] D. THAKUR, Gauss sums for $\mathbf{F}_q[T]$, *Invent. Math.* **94** (1988), 105–112.

[Th3] D. THAKUR, Gamma functions for function fields and Drinfeld modules, *Ann. of Math.*, to appear.

[Wa] L. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.

Printed in Belgium