Corps finis

1 Il existe des corps finis ! (mais peu)

Soit $p \in \mathbb{N}^*$. Alors $\mathbb{Z}/p\mathbb{Z}$ est naturellement muni d'une structure d'anneau. Notons $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la projection canonique. Si $k \in \mathbb{Z}$ vérifie que $\pi(k)$ est inversible, alors il existe u tel que $\pi(k)\pi(u) = \pi(1)$ donc il existe v tel que $ku = 1 + pv$, et donc d'après le théorème de Bezout, $k \wedge p = 1$.
Réciproquement, si $k \wedge p = 1$, toujours d'après le théorème de Bezout il existe u, v tels que $ku + pv = 1$, de sorte que $\pi(k)\pi(u) = \pi(1)$, et donc $\pi(k)$ est inversible. On a donc obtenu:

Proposition : Soit $k \in \mathbb{Z}$. $\pi(k)$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $k \wedge p = 1$.

En particulier, lorsque p est premier, $\pi(k)$ est inversible si et seulement si $p \nmid k$, si et seulement si k n'est pas congru à 0 modulo p, i.e. si et seulement si $\pi(k) \neq \pi(0)$. Lorsque p est premier, $\pi(1) \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, ce dernier est donc bien un groupe: $\mathbb{Z}/p\mathbb{Z}$ est donc bien un corps. Réciproquement, si pour tout $k \in \mathbb{Z}, p \nmid k \iff p \wedge k = 1$, alors p est premier. On a donc :

Théorème : $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Un calcul rapide montre que si p est premier, la caractéristique de $\mathbb{Z}/p\mathbb{Z}$ est p (en fait c'est aussi vrai pour p non premier, mais comme on ne parle pas d'anneaux ici on ne va pas parler de la caractéristique d'anneaux qui ne sont pas des corps). En particulier, pour $p = 0$ ou p premier, il existe (au moins) un corps de caractéristique p. Dans la suite, on notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Proposition : Soit K un corps de caractéristique p, p un nombre premier. Alors K admet un unique sous-corps isomorphe à $\mathbb{F}_p$.
Souvent on fera l'abus de dire que $\mathbb{F}_p \subset K$. Cet abus n'est en général pas problématique.
Preuve : Il est clair qu'une intersection de sous-corps de K est encore un sous-corps de K. Soit donc k l'intersection de tous les sous-corps de K, qui est donc un sous-corps de K. $0_K, 1_K \in k$, et donc par récurrence pour tout $n \in \mathbb{Z}, n \cdot 1_K \in k$. De plus, par définition de caractéristique, $n \cdot 1_K = m \cdot 1_K$ si et seulement si $p \mid n - m$, si et seulement $n \equiv m$ modulo p, si et seulement si $\pi(n) = \pi(m)$. Ainsi, $\phi : \mathbb{F}_p \to k$, $\pi(n) \to n \cdot 1_K$ est bien définie et injective.
ϕ est clairement un morphisme de groupes additifs. $\phi(1_{\mathbb{F}_p}) = \phi(\pi(1)) = 1_K$. De plus, par distributivité généralisée, $(n \cdot 1_K)(m \cdot 1_K) = nm \cdot 1_K$, de sorte que $\phi(ab) = \phi(a)\phi(b)$: ϕ est un morphisme de corps. Son image est donc un corps: un sous-corps de k. Donc $k \subset \mathrm{Im}\phi \subset k$: ϕ est bijective, c'est donc un isomorphisme de corps, $k \simeq \mathbb{F}_p$. On a donc l'existence d'un tel sous-corps.
Quant à l'unicité, si L est un autre sous-corps de K isomorphe à $\mathbb{F}_p$, par définition de k, on a $k \subset L$. De plus, k et L sont de cardinal p, donc $k = L$: on a bien l'unicité.

Cette identification nous fera considérer que $n \in K$ pour tout corps K et $n \in \mathbb{Z}$. En particulier on arrêtera de noter $\pi(n)$ pour les éléments de $\mathbb{F}_p$, lorsqu'il n'y aura pas de risque d'ambiguïté. Cette proposition permet de prouver le premier résultat qui contraint la forme des corps finis.

Lemme : Soit K un corps fini de cardinal q, et E un K-espace vectoriel fini. Alors E est de dimension finie, et $|E| = q^{dim(E)}$.
Preuve : E est une famille génératrice finie de E donc par définition, E est de dimension finie; soit n sa dimension. Alors, on a classiquement $E \simeq K^n$. En particulier, $|E| = |K|^n = q^n$.

En particulier, si K est un corps fini de caractéristique p, puisqu'il a un sous-corps isomorphe à $\mathbb{F}_p$, c'est un $\mathbb{F}_p$ espace vectoriel (la multiplication scalaire est $n \cdot x = (n \cdot 1_K)x$, ou encore, avec les abus de notations décrits plus haut, nx). Comme il est fini, $|K| = |\mathbb{F}_p|^n$ pour un certain n, et

donc $|K| = p^n$.
Corollaire : Si K est un corps fini de caractéristique p, alors il existe $n \geq 1$ tel que K est de cardinal p^n.
Corollaire : Il n'existe pas de corps à 6 éléments.
Preuve : On vient de décrire la preuve du premier corollaire. Quant au deuxième, il vient de ce que $6 = 2 \times 3$, et donc d'après le théorème fondamental de l'arithmétique, 6 n'est de la forme p^n pour aucun nombre premier p et entier n.

Mais en fait, notre lemme nous dit bien plus que ça !

Corollaire : Soit K un corps, L un sous-corps de K. On suppose que L, K sont finis, de caractéristique p. Ainsi d'après les corollaires précédents, il existe n, m tels que $|L| = p^n, |K| = p^m$. Alors $n \mid m$.
Preuve : En effet, K est un L-espace vectoriel (avec $\lambda \cdot x = \lambda x$) fini, donc d'après le lemme, il existe d tel que $|K| = |L|^d$, et alors $p^m = p^{nd}$, donc $m = nd, n \mid m$.

En particulier, comme $9 = 3^2, 27 = 3^3$ et $2 \nmid 3$, un corps à 27 éléments n'a pas de sous-corps à 9 éléments.
Dans un corps de caractéristique p, on a $p \cdot 1_K = 0$. Cela donne lieu à des relations intéressantes qui facilitent les calculs.

Proposition : Soit K un corps de caractéristique p. Alors pour tous $a, b \in K, (a+b)^p = a^p + b^p$.
Preuve : Il y a différentes preuves de ce résultat; j'en présente ici deux.

1. On prouve comme dans $\mathbb{C}$ que $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$. Or comme p est premier, pour $i \in [\![1, p-1]\!]$, $p \nmid i!, p \nmid (p-i)!$, et $p \mid p!$ donc $p \mid \frac{p!}{i!(p-i)!} = \binom{n}{i}$ (attention ces relations de divisibilité sont dans $\mathbb{Z}$!), de sorte que dans K, pour $i \in [\![1, p-1]\!]$, on a $\binom{n}{i} = 0$, et donc la formule de Newton donne $(a+b)^p = a^p + b^p$.

2. Considérons le polynôme $(1+X)^p$. Sa dérivée (formelle) est $p(1+X)^{p-1} = 0$ (dans K). Donc si on écrit $(1+X)^p = \sum_{i=0}^{p} a_i X^i$, on obtient que pour tout i, $ia_i = 0$ et donc $i = 0$ ou $a_i = 0$. En particulier, pour $i \in [\![1, p-1]\!]$, $a_i = 0$. Donc $(1+X)^p = a_0 + a_p X^p$. Or il est clair que $a_0 = 1, a_p = 1$, donc $(1+X)^p = 1 + X^p$. Notons Q ce polynôme. On peut clairement supposer $a \neq 0$. Alors $(a+b)^p = a^p(1 + \frac{b}{a})^p = a^p Q(\frac{b}{a}) = a^p(1 + (\frac{b}{a})^p) = a^p + b^p$.

Cette relation, dite "relation du bizut" est très pratique. En particulier, une récurrence immédiate donne :
Corollaire : Soit K un corps de caractéristique p, et $n \in \mathbb{N}$. Alors pour tous $a, b \in K$, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.
Preuve : Par récurrence, c'est évident. En effet, $(a+b)^{p^{n+1}} = ((a+b)^p)^{p^n} = (a^p + b^p)^{p^n}$.

Cela permet de donner quelques résultats de structure de plus:

Proposition : Soit K un corps de caractéristique p. Soit de plus $m \in \mathbb{N}$. Alors l'ensemble des racines de $X^{p^m} - X$ est un sous-corps de K. En particulier, si L est un sous-corps fini de K, L est l'ensemble des racines de $X^{|L|} - X$.
Preuve : a est racine de $X^n - X$ revient à dire que $a^n = a$. Quel que soit n, l'ensemble des racines de $X^n - X$ contient $0, 1$, et est (clairement) stable par multiplication et inverse. Si p est impair, alors $(-1)^{p^m} = -1$,et si $p = 2$, $1 = -1$ dans K, donc si $n = p^m$, cet ensemble contient -1, et est donc stable par multiplication par -1, et donc par opposé. Si $n = p^m$, le corollaire précédent montre alors qu'il est aussi stable par addition. Donc pour $n = p^m$, l'ensemble des racines de $X^n - X$ est un sous-corps de K.
Si L est un sous-corps de K, $X^{|L|} - X$ a au plus $|L|$ racines dans K, donc il suffit de montrer que L est inclus dans l'ensemble des racines pour conclure que L est l'ensemble des racines. Or clairement 0 est racine de ce polynôme, et si $a \in L^*$, alors a est dans le groupe multiplicatif de L

et donc d'après le théorème de Lagrange, $a^{|L|-1} = 1$, $a^{|L|} = a$, et donc a est bien une racine. Donc L est inclus dans l'ensemble des racines de $X^{|L|} - X$, et c'est donc bien l'ensemble des racines de ce polynôme.

Admettons un instant l'existence d'un corps algébriquement clos de caractéristique p. Notons le K. Soit alors $m \geq 1$.Notons $Q = X^{p^m} - X$. Alors $Q' = p^m X^{p^m-1} - 1 = -1$ car $p = 0$ dans K. Donc Q n'a pas de racine double dans K, et comme K est algébriquement clos, Q a p^m racines distinctes dans K. Or l'ensemble de ces racines forme un corps: on a trouvé un corps de cardinal p^m ! Ainsi, s'il existe un corps algébriquement clos de caractéristique p, alors pour tout $m \geq 1$ il existe un corps de cardinal p^m. On le démontrera autrement par la suite.

2 Il existe peu de corps finis... (mais en fait suffisamment !)

Dans cette section nous allons montrer le fameux théorème : pour tout nombre premier p et entier $m \geq 1$, il existe un unique (à isomorphisme près) corps de cardinal p^m. Pour cela nous fixons un nombre premier p qui ne changera pas pour le reste de la section. Seulement, sauf mention explicite, les corps peuvent ne pas être de caractéristique p.

En fait on veut montrer le résultat d'unicité par récurrence sur m (l'existence sera relativement facile). Pour cela on veut pouvoir remonter d'un isomorphisme de $K \to K'$ à un isomorphisme de $K(\alpha) \to K'(\beta)$ lorsque α et β sont des éléments de surcorps de K, K' qui "se ressemblent". Pour cela il nous faut savoir à quoi ressemble $K(\alpha)$. On pourrait faire cela plus systématiquement avec des anneaux et des idéaux, mais comme on est dans ce contexte précis on va simplement montrer que si α et β se ressemblent assez, $K(\alpha) \simeq K(\beta)$.

Lemme : Soit $K \subset L$ deux corps (par là il est entendu que K est un sous-corps de L), et $\alpha \in L$. Nous notons $K(\alpha)$ le sous-corps de L engendré par K et α. Alors de deux choses l'une, ou bien le seul polynôme de $K[X]$ dont α est une racine est 0, auquel cas $K(\alpha) \simeq K(X)$, ou bien il existe $P \in K[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Dans ce second cas, il existe un unique tel polynôme de degré minimal unitaire, noté $\pi_{K,\alpha}$, tel que tout autre annulateur en est un multiple. De plus si $\beta \in L'$ (L' un surcorps de K) et $\pi_{K,\beta} = \pi_{K,\alpha}$, alors $K(\alpha) \simeq K(\beta)$.
Preuve : Dans un premier temps, si $\{P \in K[X] \mid P(\alpha) = 0\} = \{0\}$, alors nous notons que $K(\alpha) = \{\frac{P(\alpha)}{Q(\alpha)} : P, Q \in K[X], Q \neq 0\}$. En effet ce dernier ensemble est bien défini car si $Q \neq 0, Q(\alpha) \neq 0$, c'est de plus clairement un sous-corps de L qui contient K et α, et clairement tout sous-corps de L qui les contient doit le contenir.
Considérons alors $\phi : K(X) \to K(\alpha)$, $F(X) \to F(\alpha)$. ϕ est clairement un morphisme de corps, il est donc injectif, et par ce qui précède il est surjectif: c'est donc un isomorphisme: $K(\alpha) \simeq K(X)$.

Dans un second temps, supposons qu'il existe $P \neq 0$ tel que $P(\alpha) = 0$. Soit alors $n = \min\{\deg(P) : P \in K[X] \setminus \{0\}, P(\alpha) = 0\}$, et P unitaire dans cet ensemble tel que $\deg(P) = n$. Si Q est un autre polynôme unitaire de degré n annulant α, alors en effectuant la division euclidienne de P par Q, on obtient $P = QT + R$ avec $\deg(R) < \deg(Q)$. En particulier, si on évalue en α, $R(\alpha) = 0$ donc par minimalité, $R = 0$, et donc $P = QT$. Or $\deg(P) = \deg(Q)$, donc $T \in K$, et comme les deux sont unitaires, $T = 1$, $P = Q$, d'où l'unicité.
Maintenant, si $Q(\alpha) = 0$, on peut effectuer la division euclidienne de Q par P: $Q = PT + R$, $\deg(R) < n$. En évaluant en α, on a à nouveau $R(\alpha) = 0$, et donc par minimalité, $R = 0$, et donc P divise Q, comme annoncé.

Alors $K(\alpha) = \{P(\alpha) : P \in K[X]\}$. En effet, ce dernier ensemble est clairement un sous-anneau de L contenant K et α. De plus, $\pi_{K,\alpha}$ est irréductible dans $K[X]$ (sinon $\pi_{K,\alpha} = PQ$, P, Q de degrés $< \deg(\pi_{K,\alpha})$, et en évaluant en α, $P(\alpha) = 0$ ou $Q(\alpha) = 0$, ce qui est absurde par minimalité de $\pi_{K,\alpha}$), et donc si $P(\alpha) \neq 0$, $\pi_{K,\alpha} \nmid P$ et donc $\pi_{K,\alpha} \wedge P = 1$, et donc par le théorème de Bezout, il existe $U, V \in K[X]$ tels que $UP + V\pi_{K,\alpha} = 1$ et donc en évaluant en α, $U(\alpha)P(\alpha) = 1$, de sorte que $P(\alpha)$ a un inverse dans cet anneau: cet anneau est donc en réalité un sous-corps de L qui contient K et α, il contient donc $K(\alpha)$. Il est de plus clair que $K(\alpha)$ est contenu dedans, donc on a bien l'égalité annoncée. Alors si $\pi_{K,\alpha} = \pi_{K,\beta} = R$, montrons que $K(\alpha) \simeq K(\beta)$. Soit $\phi : K(\alpha) \to K(\beta)$ définie par $P(\alpha) \mapsto P(\beta)$. Il est clair que si ϕ est bien définie, alors c'est un

morphisme de corps surjectif, et donc un isomorphisme de corps. Il ne reste qu'à montrer qu'elle est bien définie: si $P(\alpha) = Q(\alpha)$, alors $P - Q$ annule α, et est donc divisible par R, de sorte que $P - Q$ annule β, et donc $P(\beta) = Q(\beta)$. Donc ϕ est bien définie: c'est un isomorphisme de corps, et donc $K(\alpha) \simeq K(\beta)$, comme annoncé.

Théorème : Pour tout $m \geq 1$, il existe au plus un corps de cardinal p^m.
Preuve : Soit m l'entier minimal tel que ce soit faux, s'il existe. Soit alors L, L' deux corps non isomorphes de cardinal p^m. Soit $n = \max\{k \leq m : \exists K$ sous-corps de L, K' sous-corps de L' tel que $K \simeq K'$ et $|K| = p^k\}$ (n est bien défini car l'ensemble en question est non vide: il contient 1 d'après la section précédente), et soit K un sous-corps de L, K' de L', de cardinal p^n et $i : K \to K'$ un isomorphisme. Supposons que $K \neq L$: soit $\alpha \in L \setminus K$. D'après le lemme, il existe $P \neq 0$ annulant α: sinon L contiendrait une copie de $K(X)$ qui est infini, une contradiction. Alors on considère $\pi_{K,\alpha} = P$. P divise $X^{|L|} - X$ d'après la section précédente (car $X^{|L|} - X$ annule α et est dans $K[X]$). Si on regarde l'image de P dans $K'[X]$ (que l'on note abusivement P aussi, mais ce n'est pas grave), on a donc aussi $P \mid X^{|L'|} - X$ ($= X^{|L|} - X$ par hypothèse sur L, L'). Ce deuxième polynôme est scindé dans $L'[X]$ car d'après la section précédente il vaut $\prod_{x \in L'} (X - x)$, donc P est aussi scindé dans L': soit β une racine de P. Alors $P = \pi_{K',\beta}$, car il annule β, est unitaire, et irréductible sur K donc sur K'. Alors $K(\alpha) \simeq K'(\beta)$ d'après le lemme précédent (techniquement on n'est pas dans les hypothèses de ce lemme, mais quitte à remplacer K' par K dans L', on peut; tout ceci étant à isomorphisme près. Le.a lecteur.rice que ça gêne pourra refaire la preuve du lemme dans notre situation pour se convaincre qu'il n'y a pas de souci). Or $\alpha \notin K$, donc $K \neq K(\alpha)$, et similairmeent pour K' et β, ce qui contredit donc la maximalité de n: contradiction.
Donc $K = L$, et donc par égalité des cardinaux, $K' = L'$, et donc $L \simeq L'$.

Lorsqu'un corps de cardinal $q = p^m$ existe, il est donc unique à isomorphisme près, et on en note un $\mathbb{F}_q$ ou $\mathbb{F}_{p^m}$, qu'on appellera par abus de langage "le corps à p^m éléments".
En fait en revoyant la preuve précédente, on remarque que si on avait simplement dit L de cardinal p^m, et L' de cardinal p^{md}, tout se serait déroulé de la même manière, sauf à deux détails près: on aurait $X^{|L|} - X \mid X^{|L'|} - X$ au lieu de l'égalité (mais on n'a besoin que de ça dans la preuve) et à la fin on n'aurait pas égalité des cardinaux, seulement $K = L$. Mais on aurait donc L isomorphe à un sous-corps de L'.
Corollaire (de la preuve): Si L est un corps de cardinal p^m et L' de cardinal p^{md}, alors L est isomorphe à un sous-corps de L', i.e. L se plonge dans L'.
Preuve : On reprend mot-à-mot la preuve du théorème, avec les modifications susmentionnées. Il n'y a qu'à justifier que $X^{p^m} - X$ divise $X^{p^{md}} - X$. Il suffit clairement de montrer que $X^{p^m - 1} - 1$ divise $X^{p^{md}-1} - 1$. Or il est clair (cf. formule de sommation des suites géométriques) que $p^m - 1 \mid p^{md} - 1$, il suffit donc de montrer que si a, d sont entiers, $X^a - 1 \mid X^{ad} - 1$, et pour ça il suffit de le montrer dans $\mathbb{Z}[X]$ (car alors la divisibilité passe à $\mathbb{F}_p[X]$, puis à $L'[X]$). Or $X^{ad} - 1 = (X^a - 1) \sum_{i=0}^{d-1} X^{ai}$.

Admettons un instant l'existence d'un corps algébriquement clos de caractéristique p. Alors avec ce qu'on vient de faire et la section précédente, on a un théorème de structure complet sur les corps finis: il existe exactement un corps (à isomorphisme près) de cardinal p^m pour tout $m \geq 1$, et c'est un sous-corps des corps de cardinal p^{md} pour $d \geq 1$, et d'aucun autre corps fini. On va maintenant montrer ce résultat sans hypothèse supplémentaire.

Théorème : Pour tout $m \geq 1$, il existe un corps de cardinal p^m.
Preuve : Soit K un corps fini de caractéristique p et P un polynôme de $K[X] \setminus K$. On veut montrer qu'il existe un surcorps de K, L, dans lequel P est scindé. On procède par récurrence (forte) sur le degré de P, l'hypothèse de récurrence étant "Pour tout corps fini k de caractéristique p et tout polynôme P de $k[X] \setminus k$ de degré $< n$, il existe un surcorps M fini de k dans lequel P est scindé" : si P n'est pas irréductible, il s'écrit QR avec $Q, R \notin K$ de degrés strictement plus petits que $\deg(P)$. On applique alors l'hypothèse de récurrence à K et Q pour obtenir L, puis à L et R pour obtenir L', dans lequel Q et R sont scindés, donc P est scindé dans L', qui est fini. Sinon, P est irréductible. Dans ce cas on considère la matrice de compagnon de P, qu'on notera M, cette

matrice est $\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_0 \\ 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & \ddots & 0 & 0 & a_2 \\ \vdots & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 1 & 0 & a_{d-2} \\ 0 & 0 & \cdots & 0 & 1 & a_{d-1} \end{pmatrix}$ où $P = X^d - \sum_{k=0}^{d-1} a_k X^k$. Alors un calcul rapide montre que $P(M) = 0$. Or P est irréductible, donc $a_0 \neq 0$, de sorte que $M\frac{1}{a_0}(M^{d-1} - \sum_{k=1}^{d-1} a_k M^{k-1}) = I_d$, et donc M est inversible.
En fait plus généralement, on vérifie que $I_d, ..., M^{d-1}$ est une famille libre (calcul facile aussi), et donc P est le polynôme minimal de M. Ainsi, si $Q(M) \neq 0$, $P \nmid Q$, et comme P est irréductible, $P \wedge Q = 1$ et donc par le théorème de Bézout, il existe U, V tels que $PU + QV = 1$. En évaluant en M, on obtient $Q(M)V(M) = I_d$, de sorte que $Q(M)$ est inversible, d'inverse un polynôme en M. Ainsi $K(M) := \{Q(M) : Q \in K[X]\}$ est un sous-anneau de $\mathcal{M}_d(K)$ dans lequel les éléments non nuls sont inversibles, et stable par inverse: c'est donc un corps. De plus $\lambda \to \lambda I_d$ est clairement un morphisme de corps, donc on peut considérer $L = K(M)$ comme un surcorps de K, dans lequel $P(M) = 0$. Alors L est fini (il est de dimension d comme K-espace vectoriel, et K est fini), et donc M est annulé par $X^{|L|} - X$. Par minimalité de P, on a $P \mid X^{|L|} - X$. Ce dernier polynôme étant scindé sur L, P l'est aussi. Cela conclut la récurrence. (en fait on aurait pu la faire sans hypothèse de finitude, mais il y aurait eu un détail en plus à régler: là on n'a rajouté qu'une seule racine de P, et donc sans l'hypothèse de finitude, il faut itérer pour obtenir une extension sur laquelle P est scindée. Ce n'est pas beaucoup plus long, mais j'ai préféré faire comme ça).
On peut maintenant déduire le théorème de ce résultat: soit $K = \mathbb{F}_p$ et $P = X^{p^m} - X$. On applique le résultat pour obtenir un surcorps L de $\mathbb{F}_p$ dans lequel P est scindé. Alors, de la même manière que dans la remarque qui précède la deuxième section, $P' = -1$ et donc P n'a que des racines simples dans L: il en a donc p^m. D'après les résultats qui précède, l'ensemble de ces racines forme un sous-corps L' de L, qui est de cardinal p^m: on a trouvé un corps de cardinal p^m !

On peut prouver ce théorème "plus facilement" avec l'arsenal des anneaux quotients, mais il aurait fallu introduire tout ça et ce n'est pas le cadre de cette présentation.
On a finalement obtenu :

Théorème : Pour tout $m \geq 1$, il existe exactement une classe d'isomorphisme de corps de cardinal p^m. On note $\mathbb{F}_{p^m}$ un de ses représentants. Alors $\mathbb{F}_{p^m}$ se plonge dans F_{p^n} si et seulement si $m \mid n$.

Remarque: D'après la première section, pour $n > 1$, $\mathbb{F}_{p^n} \ncong \mathbb{Z}/p^n\mathbb{Z}$! Le premier est un corps et le second est un anneau qui n'est pas intègre.

Nous allons maintenant décrire des petits corps, à commencer par le plus petit corps qui n'est pas un $\mathbb{F}_p$: $\mathbb{F}_4$. Les éléments de $\mathbb{F}_4$ sont racines de $X^4 - X$, et donc les deux éléments de $\mathbb{F}_4$ qui ne sont pas $0, 1$ sont des racines de $\frac{X^3-1}{X-1} = 1 + X + X^2$. Ce polynôme n'a pas de racine dans $\mathbb{F}_2$ et est de degré 2 donc il est irréductible sur $\mathbb{F}_2$: d'après la construction qui précède, on peut considérer $\mathbb{F}_2(\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix})$. Il s'agit alors d'un corps de caractéristique 2, et c'est un $\mathbb{F}_2$-espace vectoriel de dimension 2: il est isomorphe à $\mathbb{F}_4$. Si on note $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \alpha$, on a $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, et $\alpha(\alpha + 1) = \alpha^2 + \alpha = -1 = 1$, $\alpha + \alpha + 1 = 2\alpha + 1 = 1$. Cela décrit complètement $\mathbb{F}_4$.

Faisons de même pour $\mathbb{F}_9$: c'est l'ensemble des racines de $X^9 - X$. Les éléments $\neq 0, 1, 2$ sont donc racines de $\frac{1+X+...+X^7}{X-2}$. Or dans $\mathbb{F}_3$, $(X - 2)(X^6 + X^4 + X^2 + 1) = X^7 - 2X^6 + X^5 - 2X^4 + X^3 - 2X^2 + X - 2 = X^7 + X^6 + X^5... + 1$ car $-2 = 1$. Si α est racine de ce polynôme, α^2 est racine de $X^3 + X^2 + X^1 + 1$. En particulier, $\alpha^2 = 2$ est cohérent avec ceci: essayons de voir ce qui se passe si on adjoint à $\mathbb{F}_3$ une racine carrée de 2: $K = \mathbb{F}_3(\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix})$ est aussi un corps car $X^2 - 2$ est irréductible sur $\mathbb{F}_3$ (il est de degré 2 et n'a pas de racine, il est donc irréductible). De

plus K est de dimension 2 en tant que $\mathbb{F}_3$-espace vectoriel, c'est donc $\mathbb{F}_9$. Ainsi $\mathbb{F}_9$ est généré par $\mathbb{F}_3$ et une racine carrée de 2. $\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$, et les tables de multiplication/addition se déduisent de $\alpha^2 = 2$, de la caractéristique 3 et des axiomes de corps. Par exemple $\alpha(\alpha+1) = \alpha^2 + \alpha = \alpha + 2$, ou encore $(\alpha+1)(2\alpha+1) = 2\alpha^2 + 3\alpha + 1 = 2 \times 2 + 1 = 2$.

Remarque : Ici on a essentiellement parlé de corps finis, mais attention: il existe des corps infinis de caractéristique finie. Par exemple si K est un corps fini, $K(X)$ est infini et de même caractéristique que K. En fait, admettant l'existence de clôtures algébriques, il est clair qu'une clôture algébrique de $\mathbb{F}_p$ doit être infinie: d'après certaines remarques faites, chaque $\mathbb{F}_q$ se plonge dedans, pour $q = p^n$.

En fait il s'avère que $K = \bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^n}$ est la clôture algébrique de $\mathbb{F}_p$ (il faudrait préciser ce que cette union veut dire: formellement on n'a pas a priori $\mathbb{F}_p \subset \mathbb{F}_{p^2}$ par exemple. Il faut juste faire attention à transformer les plongements en de véritables inclusions, et alors c'est relativement clair que l'union en question est un corps, et qu'il est algébriquement clos. En effet si $P \in K[X]$, alors comme P a un nombre fini de coefficients, $P \in \mathbb{F}_{p^n}[X]$ pour un certain n (et tous ses multiples). Alors par le résultat intermédiaire prouvé dans le théorème, il existe L fini contenant $\mathbb{F}_{p^n}$ dans lequel P est scindé. Par unicité des corps finis, il existe m tel que $L \simeq \mathbb{F}_{p^m}$, et alors P est scindé dans $\mathbb{F}_{p^m}$, et donc dans K: K est algébriquement clos. (il y a des détails à vérifier : par exemple montrer qu'il existe un isomorphisme $L \to \mathbb{F}_{p^m}$ qui est l'identité sur $\mathbb{F}_{p^n}$; mais ce n'est pas très compliqué à montrer et c'est laissé en exercice; inspirez-vous des preuves qui précèdent).