Les corps finis

Par Pierre, Lucas, Louis, de la promotion 2016 de l'ENS Ulm.

Introduction : Dans cet exposé portant sur les corps finis, nous verrons d'abord, à partir de l'étude du sous-corps premier, quel peut être le cardinal d'un corps fini. Puis, nous verrons les outils nécessaires à la démonstration d'une réciproque, qui dit que tout cardinal accessible à un corps fini est atteint de manière unique à isomorphisme près. Théorème que nous démontrerons à la fin.

1 Définitions et premières propriétés

1.1 Définition d'un anneau, d'un corps, des morphismes

1.1.1 Anneaux

Définition Soit $(A, +, \times)$ un ensemble muni de deux opérations $+$ et $\times$. On dit que A est un anneau ssi :
- $(A, +)$ est un groupe abélien.
- $\times$ est associative.
- Pour tout $(x, y, z) \in A^3$, $x \times (y + z) = x \times y + x \times z$ et $(x + y) \times z = x \times z + y \times z$.

De plus :
- On dit que A est un anneau unitaire, si il existe $1_A \in A$, avec $1_A \neq 0_A$ tel que pour tout $x \in A$, $1_A \times x = x \times 1_A = x$. (autrement dit, 1_A est le neutre pour la multiplication) **Dans la suite, tous les anneaux seront supposés unitaires.**
- On dit que A est un anneau commutatif, si et seulement si, $\times$ est commutative.
- On note $A^\times$ l'ensemble des éléments inversibles de A pour la multiplication, i.e. $A^\times = \{x \in A | \exists y \in A, xy = yx = 1_K\}$

1.1.2 Corps

Définition : Un corps K est un ensemble muni des opérations $(+, \times)$ telles que :
- $(K, +, \times)$ est un anneau commutatif unitaire.
- $(K \backslash \{0_K\}, \times)$ est un groupe.

On dit que le corps K est fini si son cardinal est fini.

1.1.3 Morphisme d'anneaux, de corps

Définition : Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux. Soit $f : A \to B$. f est un morphisme d'anneaux ssi :
- $\forall (a, b) \in A^2$, $f(a + b) = f(a) \oplus f(b)$
- $\forall (a, b) \in A^2$, $f(a \times b) = f(a) \otimes f(b)$
- $f(1_A) = 1_B$

Définition : Une application entre deux corps est un morphisme de corps si il est un morphisme d'anneau pour les anneaux sous-jacents aux corps.

1.2 Caractéristique

Définition Soit $(K, +, \times)$ un corps. On note $\omega_+(1_K)$ l'ordre de 1_K (neutre pour la multiplication de K) pour la loi additive $+$ du corps. Si $\omega_+(1_K) < +\infty$ on dit que le corps K est de caractéristique finie et on note $\text{car}(K) = \omega_+(1_K)$, et si $\omega_+(1_K) = +\infty$, alors on dit que le corps est de caractéristique nulle et on note $\text{car}(K) = 0$.
Si $\text{car}(K) > 0$, on a, par définition de l'ordre d'un élément :

$$\text{car}(K) = \min\{n \in \mathbb{N}^* | n \cdot 1_K = 0_K\} = |\{n \cdot 1_K | n \in \mathbb{Z}\}|$$

Et ce minimum est à la fois valable pour la relation d'ordre usuelle et pour la relation d'ordre qu'est la relation de divisibilité sur $\mathbb{N}$.

Proposition : Soit K un corps fini, alors K est de caractéristique non-nulle, et $\text{car}(K)$ est un nombre premier.

Preuve :

- La suite $(n \cdot 1_K)_{n\in\mathbb{N}}$ ne peut être injective car K est fini, donc il existe $(n, n') \in \mathbb{N}^2$, avec $n \neq n'$, tel que $n \cdot 1_K = n' \cdot 1_K$. Et en supposant $n > n'$, on a $(n - n') \cdot 1_K = 0_K$, donc $\omega_+(1_K) < +\infty$. Donc $\text{car}(K) \neq 0$.
- Supposons par l'absurde $\text{car}(K) = ab$ où a, b sont des entiers ≥ 2. Alors $(ab) \cdot 1_K = 0$ donc $(a \cdot 1_K) \times (b \cdot 1_K) = 0$, donc par intégrité de K, on a $a \cdot 1_K = 0$ ou $b \cdot 1_K = 0$, ce qui contredit la minimalité de $\text{car}(K)$.

Proposition : Soit K un corps fini, $\text{car}(K)$ divise $|K|$.

Preuve : K est un corps fini, donc K est de caractéristique non-nulle. Et alors, $\text{car}(K)$ est l'ordre de 1_K dans le groupe $(K, +)$, donc $\text{car}(K)||K|$.

1.3 Le corps $\mathbb{F}_p$

On ne revient pas sur la construction du corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (pour p premier). Ce corps est fini de cardinal p et de caractéristique p également.
Proposition : Si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. De plus, c'est l'unique corps de cardinal p, à isomorphisme de corps près.

Preuve de l'unicité : Soit K un corps de cardinal p, alors $(K, +)$ est un groupe de cardinal p donc est cyclique. Notons 1_K le neutre multiplicatif, qui engendre donc $(K, +)$. Si $a, b \in K$, notons $a = a' \cdot 1_K = (1_K + ... + 1_K)$ (a' fois) et $b = b' \cdot 1_K$. Alors $ab = (a' \cdot 1_K) \times (b' \cdot 1_K) = (a'b') \cdot 1$ (par distributivité). La loi multiplicative est donc uniquement déterminée.

Proposition : Pour tout corps fini K, il existe p premier tel que $\mathbb{F}_p$ s'injecte dans K via un morphisme de corps.

Preuve : Il suffit de considérer le sous corps engendré par le neutre multiplicatif, et d'utiliser la primalité de la caractéristique.

1.4 Cardinal d'un corps fini

Théorème : Soit $(K, +, x)$ un corps fini, alors il existe p un nombre premier et $\alpha \in \mathbb{N}^*$ tels que $|K| = p^\alpha$.

Preuve : Soit $p = \text{car}(K)$ qui est un nombre premier, alors K contient $\mathbb{F}_p$ (toujours à morphisme de corps injectif près).
On munit K d'une structure d'espace vectoriel sur son sous-corps premier (cf 2.2.2).
De plus, K est de dimension finie, notée $\alpha \in \mathbb{N}^*$ (la dimension ne peut pas être nulle, car K est un anneau unitaire, donc possède ses neutres multiplicatif et additif supposés distincts), sur $\mathbb{F}_p$, car il est fini. Et on a donc $|K| = p^\alpha$.

2 Préliminaires

D'après la section précédente, nous savons que tout corps fini est de cardinal p^α avec p premier et $n > 0$. Nous voudrons nous intéresser à l'existence et à l'unicité de corps finis d'un cardinal donné (à isomorphisme près). Pour cela nous avons besoin de quelques outils que nous allons voir dans cette partie.

2.1 Un peu de théorie des anneaux

2.1.1 Définition d'un idéal

Définition Soit $(A, +, \times)$ un anneau commutatif, soit $I \subset A$. On dit que I est un idéal de A ssi :

- $(I, +)$ est un sous-groupe de $(A, +)$
- Pour tout $(a, i) \in A \times I$, $a \times i \in I$ (autrement dit, I "absorbe" les éléments de A)

La structure de l'idéal est faite pour qu'on puisse quotienter l'anneau par l'idéal, et retrouver une structure d'anneau.

Proposition Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux. Soit $f : A \to B$ un morphisme d'anneaux. Alors $\text{Ker}(f)$ est un idéal.

Preuve Grâce à la définition d'un idéal.

Proposition Soit $(A, +, \times)$ un anneau commutatif. L'anneau A est un corps ssi ses seuls idéaux sont A et $\{0\}$.

Preuve : (La preuve utilise la notion d'idéal engendré : notion définie plus bas)

- Supposons que les seuls idéaux de A sont A et $\{0\}$. Soit $x \in A$, avec $x \neq 0$. Alors $(x) \neq \{0\}$. Donc $(x) = xA = A$ par hypothèse. Donc il existe $y \in A$ tel que $yx = 1_A$.
- Supposons que A est un corps. Soit I un idéal non-réduit à $\{0\}$ de A. Soit $x \in I$ non-nul. Alors il existe $y \in A$ tel que $xy = 1_A$. Donc $xy \in I$ par définition d'un idéal, donc $1_A \in I$, donc $A = I$. (car alors, pour tout $a \in A$, $a \times 1_A \in I$ (car $1_A \in I$ et par définition d'un idéal) donc $a \in I$)

2.1.2 Anneau quotient

Théorème Soit $(A, +, \times)$ un anneau commutatif. Soit $\sim$ une relation d'équivalence sur A, et soit π la surjection canonique associée. Alors on peut munir $A/\sim$ d'une structure d'anneaux telle que π soit un morphisme d'anneau ssi il existe I un idéal de A telle que, pour tout $(x, y) \in A^2$, $x \sim y \Leftrightarrow x - y \in I$, et on note alors $A/\sim = A/I$. Et on a $I = \text{Ker}(\pi)$. (Le noyau de π est le noyau pour le morphisme de groupe additif sous-jacent)

Preuve : Si la relation d'équivalence est de la forme voulue, on utilise la définition d'un idéal pour montrer que cette relation d'équivalence est compatible avec les opérations d'un anneau. Dans l'autre sens, on pose $I = \{x - y | (x, y) \in A^2 \text{ avec } x \sim y\}$, et on montre qu'il s'agit d'un idéal. (En fait, la définition d'un idéal est faite pour que ce théorème marche)

2.1.3 Idéal maximal

Définition : Soit $(A, +, x)$ un anneau commutatif. Soit I un idéal de A. On dit qu'il est maximal ssi il est maximal au sens de l'inclusion sur l'ensemble des idéaux de A, i.e. pour tout J idéal de A, si $I \subset J$, alors $J \in \{A, I\}$.

Théorème : Soit $(A, +, \times)$ un anneau commutatif, soit I un idéal de A. L'anneau quotient A/I est un corps ssi I est un idéal maximal.

Preuve :

- Supposons que A/I est un corps. Soit J un idéal tel que $I \subset J$ et $I \neq J$. Alors il existe $x \in J \backslash I$, alors $x \neq 0$ (car $0_A \in I$) Alors il existe $y \in A$ tel que $\pi(x)\pi(y) = \pi(1_A)$. Donc $\pi(xy) = \pi(1_A)$, donc $xy - 1_A \in I$. Or, comme $x \in J$, on a $x \in I$, donc, $xy \in I$. Ainsi, $1_A \in I$. Donc, $A = (1_A) \subset J$. Donc $J = A$.
- Supposons que I soit un idéal maximal. On note $B = A/I$. B est un anneau commutatif. Soit $J \subset B$ un idéal. (on va montrer que J est soit $\{0\}$ soit B). On pose $H = \pi^{-1}[J]$. On montre sans problème que H est un idéal. Montrons que $I \subset H$. Soit $x \in I$. Alors $\pi(x) = I = \pi(0_K)$. Or, J est un idéal donc contient l'élément neutre pour $+$ de B, qui est $\pi(0_K)$. Donc, $\pi(0_K) \in J$, donc $\pi(x) \in J$, donc $x \in H$. Ainsi, $I \subset H$. Alors, ou bien $J = I$, et donc $J = \{0\}$, ou bien $I = A$, et donc $J = B$. Ainsi, les seuls idéaux de B sont $\{0\}$ et B. Donc B est un corps.

2.1.4 Idéal engendré, élément premier (ou irréductible)

Propriété Soient I_1 et I_2 deux idéaux d'un anneau commutatif A. Alors $I_1 \cap I_2$ est un idéal. Plus généralement, une intersection quelconque d'idéaux est un idéal.

Définition Soit $x \in A$. L'idéal engendré par x noté (x) est l'intersection de tous les idéaux de A contenant x.

Définition Soit $x \in A$. On dit que x est irréductible ssi $x \notin A^\times$ et si l'idéal engendré (x) est un idéal maximal.

Définition (HS) Soit $x \in A$. On dit que x est premier ssi $x \notin A^\times$ et si pour tout $(a, b) \in A^2$, si $p|ab$ alors $p|a$ ou $p|b$.

Proposition Soit $x \in A$, alors $(x) = xA = \{x \times a | a \in A\}$
Preuve : Il suffit de montrer que xA est un idéal et qu'il est contenu dans tout idéal contenant x.

2.1.5 Lien avec la première définition de la primalité : anneau principal

Définition Soit $(A, +, \times)$ un anneau. On dit qu'il est intègre ssi il est commutatif et si pour tout $(a, b) \in A^2$, si $ab = 0_A$ alors $a = 0_A$ ou $b = 0_A$.

Définition On dit qu'un anneau $(A, +, \times)$ est principal ssi A est intègre, et pour tout idéal I de A, il existe $\alpha \in I$ tel que $I = (\alpha) = \alpha A$.

Proposition $(\mathbb{Z}, +, \times)$ est un anneau principal. Si K est un corps, l'anneau des polynômes $K[X]$ est un anneau principal.

Preuve On prend un idéal quelconque I, non réduit à $\{0\}$, de $\mathbb{Z}$ (resp. de $K[X]$). On prend k l'élément non-nul de I qui rend minimal la valeur absolue (resp. le degré) sur I, et on montre grâce à la division euclidienne que I s'écrit $k\mathbb{Z}$ (resp. $kK[X]$)

Définition Soit $(A, +, \times)$. Soit $(a, b) \in A^2$. On dit que $a|b$ (a divise b) ssi il existe $u \in A$ tel que $b = ua$.

Proposition Soit $(A, +, \times)$ un anneau principal, soit $(a, b) \in A^2$. On a $a|b$ ssi $bA \subset aA$.

Proposition Soit $(A, +, \times)$ un anneau principal. Soit $p \in A$. L'élément p est irréductible ssi pour tout $a \in A$, si $a|p$ alors ou bien $a \in A^\times$ ou bien il existe $u \in A^\times$ tel que $a = up$.

Preuve Il faut juste remarquer que pour tout $u \in A^\times$, $(u) = uA = A$ (et que ce sont les seuls tels que $(x) = A$), et que $aA = bA$ ssi il existe $u \in A^\times$ tel que $a = ub$.

Remarque Ces propositions nous montrent d'une part, que les anneaux qu'on utilise habituellement vérifient de bonnes propriétés de structures (être principal) et que cette bonne structure permet de faire coïncider les notions arithmétiques basées sur les idéaux sont les mêmes que celles qu'on a depuis la primaire.

Remarque (HS) Dans un anneau principal, les notions d'élément premier et d'élément irréductible, car tout anneau principal est factoriel (i.e. tout élémént admet une unique décomposition en facteurs irréductibles à l'ordre près des termes)

2.2 Un peu de théorie des corps

2.2.1 Surcorps

Définition Soit $(L, +_L, \times_L)$ un corps, soit $(K, +_K, \times_K)$ un autre corps. On dit que $(L, +_L, \times_L)$ est un surcorps de $(K, +_K, \times_K)$ ssi $K \subset L$ et si les restrictions des opérations de L à K coïncident avec les opérations de K. (En d'autres mots, K est un sous-corps de L). On notera pareil leurs lois dans la suite, sauf notations contraires.

2.2.2 Structure d'espace vectoriel d'un surcorps

Proposition Avec les mêmes notations, L est alors un K-espace vectoriel.

Preuve : On munit L de la loi $\cdot$ de composition externe sur $K \times L$: pour tout $(\lambda, x) \in K \times L$, $\lambda \cdot x = \lambda \times_L x$. Et $(L, +_L, \cdot)$ vérifie alors les axiomes d'un espace vectoriel.

Définition et notation On note $[L : K] = \dim_K(L)$, et on dit que L est une extension finie de K ssi $[L : K] < +\infty$.

Proposition Si H est une extension finie de L, qui est une extension finie de K, on a alors que H est une extension finie de K et que $[H : K] = [H : L][L : K]$.

Preuve Se démontre en prenant une L-base de H et une K-base de L, avec un peu de persévérance.

2.2.3 Corps engendré par un élément, extension simple

Définition et proposition Soit $(K, +, \times)$ un corps, et $(L, +_L, \times_L)$ un surcorps de K. Soit $a \in K$. On définit, $\begin{array}{rccc} \varphi_a & : & K[X] & \to & L \\ & & P & \mapsto & P(a) \end{array}$. Alors, φ_a est un morphisme d'anneau, et un morphisme de K-espace vectoriel. (HS : en clair, un morphisme de K-algèbre). Si φ_a n'est pas injective, $\mathrm{Ker}(\varphi_a)$ est un idéal de $K[X]$ non-réduit à $\{0\}$, et il existe un unique polynôme non-nul unitaire Π_a tel que $\mathrm{Ker}(\varphi_a) = \Pi_a K[X]$. De plus Π_a est irréductible sur $K[X]$.

Preuve Le fait que φ_a soit un morphisme d'anneau est facile à montrer, on la suppose non-injective. Et donc $\mathrm{Ker}(\varphi_a)$ ($\neq \{0\}$) est un idéal (cf. 2.1.2), l'existence et l'unicité de Π_a provienne du fait que $K[X]$ est un anneau principal car K est un corps. Montrons que Π_a est irréductible : supposons qu'il existe $(P, Q) \in K[X]^2$ tel que $\deg(P) \geq 1$ et $\deg(Q) \geq 1$. On a alors $\Pi_a(a) = 0_L = P(a) \times_L Q(a)$. Donc, par intégrité de L, $P(a) = 0_L$ ou $Q(a) = 0_L$. Or, par construction, Π_a est le polynôme unitaire non-nul de plus petit degré de $\mathrm{Ker}(\varphi_a)$, absurde. Donc Π_a est irréductible.

Définition et proposition Avec les mêmes notations, on sait aussi que $\mathrm{Im}(\varphi_a)$ est un corps, et il s'agit du plus petit sous-corps de L contenant a. De plus, $\mathrm{Im}(\varphi_a)$ est un K-espace vectoriel et si φ_a n'est pas injective, alors $\dim_K(\mathrm{Im}(\varphi_a)) = \deg(\Pi_a)$, et, avec $n = \deg(\Pi_a)$, $(a^k)_{k \in [\![0, n-1]\!]}$ est une K-base de $\mathrm{Im}(\varphi_a)$.

Preuve On a ensuite de manière évidente que $\mathrm{Im}(\varphi_a) = \mathrm{Vect}_K\left((a^k)_{k \in \mathbb{N}}\right)$ et est un anneau. Reste à montrer que celui-ci est également un corps. Soit $b \in \mathrm{Im}(\varphi_a)$ non-nul, alors il existe $Q \in K[X]$ tel que $b = Q(a)$. Or, $Q(a) = b \neq 0_L$, donc Π_a ne divise pas Q dans $K[X]$, donc Π_a et Q sont premiers entre eux. Donc, il existe $(U, V) \in K[X]^2$ tel que $1 = QU + \Pi_a V$, en appliquant φ_a, on a : $1_L = Q(a)U(a) + \Pi_a(a)V(a) = b \times_L U(a)$. Donc, b est inversible, donc $\mathrm{Im}(\varphi_a)$ est un corps.
Le fait que tout corps contenant a contienne $\mathrm{Im}(\varphi_a)$ est évident par stabilité d'un corps par ses propres opérations.
En tant que surcorps de K, $\mathrm{Im}(\varphi_a)$ est un K-espace vectoriel. Si φ_a n'est pas injective, alors Π_a existe. Soit $(\lambda_0, ..., \lambda_{n-1}) \in K^{n-1}$ tel que $\lambda_0 \cdot 1_K + \lambda_1 a + ... + \lambda_{n-1} a^{n-1} = 0_L$. Alors, le polynôme $P = \sum_{i=0}^{n-1} \lambda_i X^i$ annule a et est de degré strictement plus petit que a, donc P est le polynôme nul, donc tous les λ_i sont nuls, donc la famille $(a^k)_{k \in [\![0, n-1]\!]}$ est K-libre. Et elle est génératrice : soit $b \in \mathrm{Im}(\varphi_a)$, alors il existe $P \in K[X]$ tel que $b = P(a)$. Par division euclidienne, il existe Q et R deux polynômes tels que $P = Q\Pi_a + R$ avec $\deg(R) < \deg(\Pi_a)$. Donc $b = R(a)$, et b s'exprime en fonction des $(a^k)_{k \in [\![0, n-1]\!]}$.

Notation On note $K(a) = \mathrm{Im}(\varphi_a)$, et on l'appelle le corps engendré par a.

Définition Soit K un corps, soit L un surcorps de K. On dit que L est une extension simple de K ssi il existe $a \in L$ tel que $L = K(a)$.

2.2.4 Corps de rupture

Définition Soit K un corps, soit L un surcorps de K. Soit P un polynôme irréductible sur $K[X]$. On dit que L est un corps de rupture de P sur K ssi
- Il existe $a \in L$ tel que $P(a) = 0_L$
- $L = K(a)$

Théorème : Soit $(K, +, \times)$ un corps, soit P un polynôme irréductible de $K[X]$. Alors il existe un corps de rupture de P sur K.

Preuve : Le polynôme P est irréductible, donc l'idéal (P) est un idéal maximal, donc $K_1 = K[X]/(P)$ est un corps dans lequel s'injecte K. Et on a, avec $\pi : K[X] \to K[X]/(P)$ la surjection canonique, $P(\pi(X)) = \pi(P(X)) = \pi(P) = \pi(0) = 0_L$, car $\mathrm{Ker}(\pi) = (P)$. Donc $\pi(X)$ est une racine de P dans $K[X]/(P)$. On a donc trouvé un surcorps de K contenant une racine de P. On considère ensuite $L = K_1(\pi(X))$ le sous-corps de L engendré par $\pi(X)$. L est bien un corps de rupture de P sur K.
De plus, π est injective sur K, donc K et $\pi(K)$ sont deux corps isomorphes, donc on peut bel et bien voir $K[X]/(P)$ comme un surcorps de K.

Corollaire 1 Soit $(K, +, \times)$ un corps, soit P un polynôme. Alors il existe un surcorps de K dans lequel P est scindé (i.e. P est produit de polynômes de degré 1)

Preuve P se décompose en produit de facteurs irréductibles. (ici, $K[X]^\times = K \backslash \{0_K\}$), et on raisonne par récurrence sur le degré de P, en décomposant le polynôme P sur un corps de rupture, qui existe d'après le théorème précédent. Alors, dans $L[X]$, $P = Q(X - a)$ et Q est de degré plus petit, et on applique l'hypothèse de récurrence.

Corollaire 2 Soit $(K, +, \times)$ un corps, soit Q un polynôme irréductible. Alors tout corps de rupture de Q sur K est isomorphe à $K[X]/(Q)$.

Preuve Soit L un corps de rupture de Q sur K. Alors il existe $\beta \in L$ tel que $L = K(\beta)$ et $P(\beta) = 0$. Alors, on définit la fonction f de L dans $K[X]/(Q)$ qui envoie β sur $\pi(X)$ (avec $\pi : K[X] \to K[X]/(Q)$ la surjection canonique). Cette fonction est bien définie car $L = K(\beta)$. Et cette application est un isomorphisme de corps. (se montre facilement)

2.2.5 Corps de décomposition

Définition Soit $(K, +, \times)$ un corps, soit P un polynôme non-nul de $K[X]$. Soit L un surcorps de K. On dit que L est un corps de décomposition de P sur K ssi
- P est constant ou scindé sur L
- L est le corps engendré par les racines de P, i.e. tout sous-corps de L contenant les racines de P vaut L tout entier.

Théorème Soit $(K, +, \times)$ un corps, soit P un polynôme non-nul de $K[X]$. Alors il existe un corps L de décomposition de P sur K, unique à isomorphisme de corps près. Alors L est une extension finie de K et il s'injecte dans tout surcorps de K sur lequel P est scindé.

Preuve

- Existence : On reprend la démonstration du théorème précédent en ajoutant à l'hypothèse de récurrence que le corps ainsi construit est une extension finie (car le φ_a associé est non-injectif car on a déjà un polynôme annulateur dans $K[X]$). On prend ensuite L le sous-corps de K_1 engendré par les racines de P (ou bien on le construit à l'aide de polynômes à n variables (ou n est le degré de P) de manière analogue à la construction de $K(a)$ ou bien on considère que c'est l'intersection de tous les corps contenant les racines de P). Le corps demandé par le théorème est alors construit.
- Montrons que L s'injecte dans tout surcorps de K sur lequel P est scindé. Pour ce faire nous allons généraliser l'énoncé à démontrer. Enonçons un petit lemme :

  Lemme Soient $(K, +, \times)$ et $(K, \oplus, \otimes)$ deux corps isomorphes par φ. Soit $P \in K[X]$. On note $\varphi(P)$ le polynôme de $K'[X]$ image de P par φ. Soit L' un surcorps de K' sur lequel $\varphi(P')$ est scindé. Alors φ se prolonge sur L en un morphisme de corps injectif de L sur L'.

  Preuve du lemme : Nous allons procéder par récurrence sur $[L : K]$ (qui est fini !).
  - Si $[L : K] = 1$, alors on a L et K isomorphe, donc φ convient ...
  - Si $[L : K] = n + 1$. Cela signifie donc que P admet un facteur irréductible Q, de degré supérieur ou égal à 2, qui possède une racine $\alpha \in L$. Par hypothèse, $\varphi(P)$ est sincdé dans L', donc il existe $\beta \in L'$ tel que $\varphi(P)(\beta) = 0_{L'}$. Alors $K(\alpha)$ est un corps de rupture de P sur K et $K'(\varphi(\alpha))$ est un corps de rupture de $\varphi(P)$ sur K'. Alors, en définissant ψ l'isomorphisme de corps qui à un élément $x \in K$ associe $\varphi(x)$ et à α associe β (ceci est bien défini), les deux corps $K(\alpha)$ et $K'(\beta)$ sont isomorphes. Alors : $[L : K(\alpha)] < [L : K]$. En effet : $[K(\alpha) : K] = \deg(Q)$ et $[L : K] = [L : K(\alpha)][K(\alpha) : K]$. Donc, par hypothèse de récurrence, ψ se prolonge en un morphisme de corps injectif de L dans L', donc ϕ également.

  Fin de la démonstration du lemme.

  Soit L' un surcorps de K sur lequel P est scindé. On note φ l'injection canonique de K dans L'. Alors, d'après le lemme, φ se prolonge en un morphisme injectif de L sur L'. Donc, L s'injecte dans L'.
- Montrons que L est unique à isomorphisme de corps près. Soit L' un autre corps de décomposition. D'après le point précédent, comme P est scindé sur L' par définition d'un corps de décomposition, L s'injecte dans L' par Θ (qui est donc un morphisme de corps injectif). Comme P est scindé sur L', pour toute racine $\beta \in L$ de P, $P(\Theta(\beta)) = \Theta(P(\beta)) = 0$. Donc, toute racine de P dans L s'envoie sur une racine de P dans L', qui est engendré par ces racines. Donc $\Theta(L) = L'$, et Θ est un isomorphisme de corps.

"Corollaire" Soit $(K, +, \times)$ un corps. Soit P un polynôme non-nul de $K[X]$. Soit L un surcorps de K. Si P est scindé sur L' et si L s'injecte dans tout surcorps de K sur lequel P est scindé, alors L est le corps de décomposition de P sur K.

Preuve : Soit $\mathcal{L}$ le corps de décomposition sur K de P. Alors L s'injecte plus particulièrement dans $\mathcal{L}$, donc L contient toutes les racines de P car L est scindé sur L, donc $L = \mathcal{L}$ par définition d'un corps de décomposition.

Remarque Ce dernier corollaire n'est pas à proprement parler une conséquence du théorème d'unicité d'un corps de décomposition. En effet, on a eu besoin uniquement de la définition d'un corps de décomposition pour montrer ce dernier corollaire. Cependant, la définition n'a pas de sens sans ce théorème, et donc toute démonstration qui utilise la démonstration utilise implicitement le théorème.

3 Corps finis d'un cardinal donné

Soit, dans toute cette section, $n \in \mathbb{N}^*$ et $p \geq 2$ un nombre premier. On veut montrer le théorème suivant :

Théorème Il existe un corps fini K, unique à isomorphisme de corps près, tel que $|K| = p^n$, et il s'agit du corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

Notation Pour tout K corps, pour tout $P \in K[X]$, on note $Rac_K(P)$ l'ensemble des racines de P sur K.

3.1 Existence

Lemme 1 Soit $P = X^{p^n} - X$, polynôme de $\mathbb{F}_p$. Soit K un corps de caractéristique p. Alors, $K' = \mathrm{Rac}_K(P)$ est un sous-corps de K.

Preuve : D'abord, K est de caractéristique p donc K est un surcorps de $\mathbb{F}_p$, ce qui justifie la notation $\mathrm{Rac}_K(P)$.
Soit $(x, x') \in (K')^2$, on a (sachant qu'on est en caractéristique p) :

$$(x + x')^{p^n} = x^{p^n} + x'^{p^n} = x + x'$$

donc si $x' \neq -x$, on a $(x + x')^{p^n - 1} = 1$. Sinon, $x + x' = 0_K \in K'$. Et de plus :

$$(xx')^{p^n - 1} = x^{p^n - 1} x'^{p^n - 1} = 1$$

De plus, pour tout $x \in K'$, $x^{p^n} - x = 0_K$ entraîne $(-x)^{p^n} + x = (-1) \times \left(x^{p^n - 1} - 1\right) = 0_K$, donc $-x \in K'$. Et pour tout $x \neq 0_K$, $(x^{-1})^{p^n} - x^{-1} = x^{-p^n} - x^{-1} = -x^{-p^n - 1}\left(x + x^{p^n}\right) = 0_K$, donc $x^{-1} \in K'$.
Donc K' est sous-corps de K.

Théorème : Il existe un corps fini de cardinal p^n.

Preuve : Considérons le polynôme de $\mathbb{F}_p$, $P = X^{p^n - 1} - 1$, ainsi que K, un surcorps de $\mathbb{F}_p$, sur lequel P est scindé. Alors K est de caractéristique p en tant que surcorps de $\mathbb{F}_p$.
Alors les racines de P dans K sont simples. En effet, soit $x \in \mathbb{F}_p$ tel que $x^{p^n - 1} = 1$, alors $x \neq 0$, or $P' = (p^n - 1)X^{p^n - 2} - 1$ a pour seule racine 0 (car $(p^n - 1) \neq 0$ car on est en caractéristique p), donc x est simple. Ainsi, il a exactement $p^n - 1$ racines.
Alors, $K' := \mathrm{Rac}_K(P) \cup \{0\} = \mathrm{Rac}_K(X^{p^n} - X)$ est un sous-corps de K, d'après le lemme 1. Ainsi, K' est un corps fini de cardinal p^n.

3.2 Démonstration de l'unicité

Lemme 2 Soit L un corps fini de cardinal p^n. Soit $P = X^{p^n} - X$. Alors $\mathrm{Rac}_L(P) = L$.

Preuve On a : $P = X(X^{p^n-1} - 1)$. Or, $(L^\times, \times)$ est un groupe cyclique car L est un corps fini, et $L^\times = L\backslash\{0_L\}$, donc $|L^\times| = p^n - 1$. Donc, les éléments de $L^\times$ constituent un ensemble de $p^n - 1$ racines de $X^{p^n-1}-1$, qui en admet au plus p^n-1. Donc, $\mathrm{Rac}_L(X^{p^n-1}-1) = L^\times$. Ainsi, $\mathrm{Rac}_L(P) = L$.

Soit L un corps de cardinal p^n. On note $K = \mathbb{F}_p$ et $P = X^{p^n} - X$, d'après le lemme 2, $\mathrm{Rac}_L(P) = L$.
But : Montrer que L est le plus petit élément (au sens de l'inclusion/injection entre corps) de $\{K|K$ surcorps de $\mathbb{F}_p$ sur lequel P est scindé$\}$.
Soit L' un surcorps de K sur lequel P est scindé. L' est de caractéristique p en tant que surcorps de K, donc $\mathrm{Rac}_{L'}(P)$ est un sous-corps de L' d'après le lemme 1.
De plus, on a : $\mathrm{Rac}_{L'}(P) \cap \mathrm{Rac}_{L'}(P') = \emptyset$, car PAinsi, comme P est scindé sur L', $|\mathrm{Rac}_{L'}(P')| = p^n$.
De plus, comme nous sommes en caractéristique p, l'ensemble $\mathrm{Rac}_{L'}(P)$ est stable par l'addition et la multiplication de L'. Donc, on peut injecter L dans L', en envoyant chaque élément de L sur une racine de L'. Et on peut donc injecter L dans tout surcorps L' de K sur lequel P est scindé. Ainsi, par le "corollaire" du théorème d'unicité d'un corps de décomposition, K est le corps de décomposition sur K de P, et il est unique à isomorphisme près, et on a bien montré le théorème.

3.3 Exemples

On note, pour tout $p \in \mathbb{N}^*$ premier, et $n \in \mathbb{N}^*$, $\mathbb{F}_{p^n}$ le corps fini à p^n éléments. On a notamment, pour tout p premier : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3.3.1 Construction d'exemples

La construction proposée précédemment est exclusivement théorique. En effet, la notion de corps de décomposition est abstraite, et il est difficile de faire des calculs dans un tel corps. En revanche, puisqu'on sait qu'il n'y a qu'un seul corps de cardinal p^n, il suffit d'en trouver un seul (appelons le K), et on pourra alors étudier la stucture de $\mathbb{F}_{p^n}$ en étudiant K. Par exemple :

Proposition : Soit p premier, et $n \in \mathbb{N}^*$. Soit $P \in \mathbb{F}_p[X]$ irréductible de degré n. Alors $\mathbb{F}_p[X]/(P)$ le corps fini de cardinal p^n.
Preuve : D'abord, $\mathbb{F}_p[X]/(P)$ est de caractéristique p, et est un corps fini, donc s'écrit sous la forme p^α, avec $\alpha \in \mathbb{N}$. Or, $\alpha = [\mathbb{F}_p[X]/(P) : \mathbb{F}_p] = n$ car $(1, ..., X^{n-1})$ (en classe d'équivalence) est une $\mathbb{F}_p$-base de $\mathbb{F}_p[X]/(P)$. Donc $|\mathbb{F}_p[X]/(P)| = p^n$.

Remarque : Ainsi, afin de trouver un corps de cardinal p^n, il "suffit" de trouver un polynôme irréductible de $\mathbb{F}_p$ de degré n.

Proposition : Soit p premier, et $n \in \mathbb{N}^*$. Alors il existe un polynôme irréductible de $\mathbb{F}_p[X]$ de degré n.

3.3.2 $\mathbb{F}_4$

1. On pose $Q = X^2 + X + 1$. Comme, le degré de Q est de degré inférieur ou égal à 3 et qu'il n'a pas de racines dans $\mathbb{F}_2[X]$, alors Q est irréductible. Donc $\mathbb{F}_4 = \mathbb{F}_2[X]/(Q)$. On a : $\mathbb{F}_4 = \{0, 1, X, X+1\}$.
2. $(1, X)$ engendre $\mathbb{F}_4$. On a : $X^2 = X + 1$. (car $-1 = 1$)
3. La loi additive du corps est :

$+$	1	X	$X+1$
1	0	$X+1$	X
X	$X+1$	0	1
$X+1$	X	1	0

4. La loi multiplicative du corps est :

$\times$	X	$X+1$
X	$X+1$	1
$X+1$	1	X

5. On remarque que $\mathbb{Z}/4\mathbb{Z}$ n'est pas $\mathbb{F}_4$! En effet :

	2	3
2	0	2
3	2	1

3.3.3 $\mathbb{F}_8$

- On pose $Q = X^3 + X + 1$. Encore une fois, le degré de P est inférieur ou égal à 3 et P n'admet pas de racines dans $\mathbb{F}_2$. Donc $\mathbb{F}_8 = \mathbb{F}_2[X]/(Q)$.
- Pour simplifer le calcul, regardons les multiplications des générateurs du corps :

1	X	X^2
X	X^2	$X+1$
X^2	$X+1$	X

- Calculons les itérés de X : $X \to X^2 \to X+1 \to X^2+X \to X^2+X+1 \to X^2+1 \to 1$. On savait déjà que $\mathbb{F}_8^*$ était cyclique. Et X en est un générateur (en fait, ils sont tous générateurs car 7 est premier)
- Regardons la loi de corps :

1	X	X^2	$X+1$	X^2+X	X^2+X+1	X^2+1
X	X^2	$X+1$	X^2+X	X^2+X+1	X^2+1	1
X^2	$X+1$	X^2+X	X^2+X+1	X^2+1	1	X
$X+1$	X^2+X	X^2+X+1	X^2+1	1	X	X^2
X^2+X	X^2+X+1	X^2+1	1	X	X^2	$X+1$
X^2+X+1	X^2+1	1	X	X^2	$X+1$	X^2+X
X^2+1	1	X	X^2	$X+1$	X^2+X	X^2+X+1

- On remarque que $\mathbb{F}_4$ ne s'injecte pas dans $\mathbb{F}_8$. En effet, il n'y a pas de sous-corps de cardinal 4 dans $\mathbb{F}_8$, car tout élément engendre multiplicativement $\mathbb{F}_8^*$.

3.3.4 $\mathbb{F}_9$

- On pose $Q = X^2 + 1$, irréductible car de degré inférieur ou égal à 3 et sans racines dans $\mathbb{F}_3$.
- On a $X^2 = 2$
- Calculons les itérés de X dans $\mathbb{F}_3[X]/(Q)$: $X \to 2 \to 2X \to 1$. Donc X n'engendre pas $\mathbb{F}_9^*$
- $X + 1$ en est un générateur en revanche : $X + 1 \to 2X \to 2X + 1 \to 2 \to 2X + 2 \to X \to X + 2 \to 1$.