Chapitre VI — Corps finis - Construction

L'objectif de ce chapitre est de construire les corps finis et de donner quelques applications à la cryptographie. On admettra dans toute la suite le résultat suivant, dont la démonstration dépasserait le niveau de ce cours :

Théorème 6.1 (Wedderburn). *Tout corps fini est commutatif.*

Les premiers exemples de corps finis sont les quotients de l'anneau $\mathbb{Z}$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z},$$

où p est un nombre premier. Compte tenu du chapitre précédent, d'autres exemples sont fournis par les quotients

$$\mathbb{F}_p[X]/(F),$$

où F est un polynôme irréductible de $\mathbb{F}_p[X]$. Ce sont en effet des corps (cor. 5.5), et ils sont finis, puisqu'ils sont de dimension finie sur $\mathbb{F}_p$. Nous reviendrons sur ce point, et démontrerons que l'on obtient de la sorte tous les corps finis. On prouvera dans les sept premiers paragraphes les énoncés suivants :

1) tout corps fini contient un sous-corps isomorphe à un corps $\mathbb{F}_p$.
2) Le cardinal d'un corps fini est une puissance d'un nombre premier.
3) Le groupe multiplicatif d'un corps fini est cyclique.
4) Tout corps fini K de cardinal p^n est isomorphe à $\mathbb{F}_p[X]/(F)$, où F est un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.
5) Pour tout nombre premier p et tout entier $n \geq 1$, il existe un corps à p^n éléments et il est unique à isomorphisme près.

Il est assez simple de démontrer les quatre premiers résultats, notamment les 1, 2 et 4. Le cinquième l'est beaucoup moins.

1. Caractéristique d'un anneau

Soit A un anneau. Notons 1_A l'élément neutre multiplicatif de A. Soit $f : \mathbb{Z} \to A$ l'application de $\mathbb{Z}$ dans A définie par

$$f(m) = m1_A \quad \text{pour tout } m \in \mathbb{Z}. \tag{1}$$

C'est un homomorphisme d'anneaux de $\mathbb{Z}$ dans A (et d'ailleurs le seul). Son noyau est un idéal de $\mathbb{Z}$. Il existe donc un unique entier naturel n tel que l'on ait

$$\mathrm{Ker}(f) = n\mathbb{Z}.$$

Définition 6.1. *L'entier n est la caractéristique de A.*

Lemme 6.1. *Si A est intègre, sa caractéristique est nulle ou est un nombre premier. Tel est en particulier le cas si A est un corps commutatif.*

Démonstration : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-anneau de A, à savoir l'image de f (th. 3.2). Puisque A est intègre, il en est donc de même de $\mathbb{Z}/n\mathbb{Z}$. Si n n'est pas nul, $\mathbb{Z}/n\mathbb{Z}$ est alors un corps (prop. 3.2), et n est un nombre premier (cor. 4.2).

Théorème 6.2. *Soit K un corps commutatif d'élément neutre multiplicatif 1_K. Soit m un entier relatif.*

1) *Supposons K de caractéristique zéro. On a $m1_K = 0$ si et seulement si $m = 0$. Dans ce cas, K contient un unique sous-corps isomorphe à $\mathbb{Q}$.*
2) *Supposons K de caractéristique un nombre premier p. On a $m1_K = 0$ si et seulement si p divise m. Dans ce cas, K contient un unique sous-corps isomorphe à $\mathbb{F}_p$.*

Démonstration : Supposons K de caractéristique 0. L'homomorphisme $f : \mathbb{Z} \to K$ défini par (1) est alors injectif, d'où l'équivalence annoncée. L'application de $\mathbb{Q}$ dans K qui à $a/b \in \mathbb{Q}$ associe $a1_K(b1_K)^{-1}$, prolonge f de $\mathbb{Z}$ à $\mathbb{Q}$, et est un homomorphisme de corps. (Notons que b étant non nul, on a $b1_K \neq 0$, et l'on vérifie que cette application est bien définie). Son image est donc un sous-corps de K isomorphe à $\mathbb{Q}$. Par ailleurs, soient Q_1 et Q_2 deux sous-corps de K isomorphes à $\mathbb{Q}$. L'intersection $Q_1 \cap Q_2$ est un sous-corps de Q_1 et de Q_2. Puisque $\mathbb{Q}$ ne contient pas de sous-corps autres que lui-même, tel est aussi le cas de Q_1 et Q_2, d'où $Q_1 \cap Q_2 = Q_1 = Q_2$, et l'unicité annoncée. Si K est de caractéristique p, le noyau de f est l'idéal $p\mathbb{Z}$. Par suite, on a $m1_K = 0$ i.e. m appartient au noyau de f si et seulement si p divise m. L'image de f est un sous-corps de K isomorphe à $\mathbb{F}_p$. L'unicité d'un tel sous-corps résulte, comme ci-dessus, du fait que $\mathbb{F}_p$ n'a pas d'autres sous-corps que lui-même.

Par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique 0. Pour tout p premier, $\mathbb{F}_p$ est de caractéristique p. On obtient aussitôt les résultats 1 et 2 énoncés précédemment :

Corollaire 6.1. *Soit K un corps fini. La caractéristique de K est un nombre premier p et K contient un unique sous-corps isomorphe à $\mathbb{F}_p$. De plus, il existe un entier $n \geq 1$ tel que le cardinal de K soit p^n.*

Démonstration : Puisque K est fini, K ne contient pas de sous-corps isomorphe à $\mathbb{Q}$. La caractéristique de K est donc un nombre premier p et K contient un unique sous-corps isomorphe à $\mathbb{F}_p$ (th. 6.2). Par suite, K est naturellement muni d'une structure d'espace vectoriel sur $\mathbb{F}_p$ (cf. exemples 5.1, 3). Le corps K étant fini, la dimension de K sur $\mathbb{F}_p$ est

aussi finie. Si n est cette dimension, K est donc isomorphe, comme espace vectoriel, à $\mathbb{F}_p^n$, et K est de cardinal p^n [32].

Corollaire 6.2. *Soit K un corps fini de cardinal p. Alors, K est isomorphe à $\mathbb{F}_p$.*

Démonstration : C'est immédiat vu que K contient un sous-corps isomorphe à $\mathbb{F}_p$.

Corollaire 6.3. *Soient K un corps fini, de caractéristique p, et F un polynôme irréductible de degré n dans $K[X]$. Alors, $K[X]/(F)$ est un corps fini, de caractéristique p, et son cardinal est $|K|^n$.*

Démonstration : Le corps $K[X]/(F)$ contenant un sous-corps isomorphe à K (remarque 5.6), sa caractéristique est la même que celle de K i.e. est p. Par ailleurs, le K-espace vectoriel $K[X]/(F)$ est de dimension n (th. 5.9), donc est isomorphe à K^n, d'où le résultat.

2. Groupe multiplicatif d'un corps fini

Démontrons dans ce paragraphe le résultat 3 annoncé.

Théorème 6.3. *Soient K un corps commutatif et H un sous-groupe fini de K^*. Alors, H est un groupe cyclique.*

En particulier :

Corollaire 6.4. *Si K est un corps fini, le groupe multiplicatif K^* est cyclique.*

Démonstration du théorème 6.3 : On utilise les deux lemmes ci-dessous.

Lemme 6.2. *Soient G un groupe abélien multiplicatif, et x, y deux éléments de G d'ordre m et n premiers entre eux. Alors, xy est d'ordre mn.*

Démonstration : On a déjà démontré ce résultat dans un cadre plus général au bas de page numéro 13. Démontrons ici ce lemme directement. Puisque G est abélien, on a $(xy)^{mn} = e$, où e est l'élément neutre de G. L'ordre de xy divise donc mn. Par ailleurs, il existe u et v dans $\mathbb{Z}$ tels que l'on ait $mu + nv = 1$ (Bézout). On a

$$(xy)^{um} = y^{um} = y^{1-vn} = y \quad \text{et} \quad (xy)^{vn} = x^{vn} = x^{1-um} = x.$$

Considérons alors un entier $r \geq 1$ tel que $(xy)^r = e$. On a $(xy)^{rum} = y^r = e$, et de même $x^r = e$. Il en résulte que r est un multiple de m et n, donc aussi de mn vu que l'on a $\text{pgcd}(m, n) = 1$, d'où le résultat.

[32] Rappelons que deux espaces vectoriels sur un corps sont isomorphes si et seulement si ils ont la même dimension. En particulier, tout espace vectoriel de dimension n sur K est isomorphe à K^n (le fait que K soit fini n'intervient pas ici). Pour justifier que $|K| = p^n$, on peut aussi choisir une base de K sur $\mathbb{F}_p$. Les coordonnées des éléments de K étant dans $\mathbb{F}_p$, il y a p choix possibles pour chaque coordonnée, d'où les p^n éléments attendus, puisque tout élément de K s'écrit de façon unique comme une combinaison linéaire des vecteurs d'une base.

Lemme 6.3. *Soient G un groupe abélien fini et x, y deux éléments de G. Il existe dans G un élément dont l'ordre est le ppcm des ordres de x et y.*

Démonstration : Notons multiplicativement la loi de composition de G. Soient α l'ordre de x et β celui de y. Soit R l'ensemble des diviseurs premiers de α pour lesquels on a $v_p(\alpha) > v_p(\beta)$, et S l'ensemble des diviseurs premiers de β pour lesquels on a $v_p(\beta) \geq v_p(\alpha)$. Posons

$$a = \prod_{p \in R} p^{v_p(\alpha)} \quad \text{et} \quad b = \prod_{p \in S} p^{v_p(\beta)}.$$

Il existe deux entiers r et s tels que l'on ait

$$\alpha = ar \quad \text{et} \quad \beta = bs.$$

Posons alors

$$z = x^r y^s \in G.$$

L'élément x^r est d'ordre a et y^s est d'ordre b (prop. 2.8). Par ailleurs, a et b sont premiers entre eux. Puisque G est abélien, z est donc d'ordre ab (lemme 6.2), qui n'est autre que le ppcm de α et β.

Le théorème 6.3 se déduit comme suit : soit m l'ordre de H. Puisque H est fini, il existe un élément de H d'ordre maximum n. Le corps K étant commutatif, H est en particulier abélien, donc pour tout élément de H d'ordre d, il existe un élément de H d'ordre le ppcm de d et n (lemme 6.3). Par suite, on a $\text{ppcm}(d, n) = n$, donc d divise n. Ainsi, les ordres de tous les éléments de H divisent n. Le polynôme $X^n - 1 \in K[X]$ ayant au plus n racines dans K, on en déduit que l'on a $m \leq n$. Puisque n divise m, on a donc $m = n$. Il existe ainsi un élément d'ordre m dans H, ce qui établit le théorème[33].

Corollaire 6.5. *Soit K un corps fini de cardinal q. Le groupe K^* possède exactement $\varphi(q-1)$ générateurs, où φ est la fonction indicatrice d'Euler. De plus, si α est un générateur*

[33] On peut aussi utiliser le résultat suivant : soit G un groupe multiplicatif fini d'ordre n, d'élément neutre e. On suppose que pour tout diviseur d de n, l'ensemble des éléments $y \in G$ tels que $y^d = e$, est de cardinal au plus d. Alors, G est cyclique d'ordre n.

En effet, Soit d un diviseur de n. Vérifions que l'ensemble des éléments de G d'ordre d est vide ou bien que son cardinal est $\varphi(d)$, où φ est la fonction indicatrice d'Euler. Supposons qu'il existe $x \in G$ d'ordre d. Le sous-groupe $< x >$ de G engendré par x est cyclique d'ordre d. Soit T l'ensemble des éléments $y \in G$ tels que $y^d = e$. Le groupe $< x >$ est contenu dans T, et d'après l'hypothèse faite sur G, on a donc $T =< x >$. Il en résulte que l'ensemble des éléments d'ordre d de G est formé des générateurs de $< x >$, et il y en a $\varphi(d)$ (th. 2.5). D'où l'assertion. Pour tout diviseur d de n, notons alors Φ_d l'ensemble des éléments d'ordre d de G. Le groupe G étant la réunion disjointe de Φ_d, on a donc

$$n = \sum_{d|n} \left|\Phi_d\right| \leq \sum_{d|n} \varphi(d).$$

de K^*, alors l'ensemble des générateurs de K^* est

$$\Big\{\alpha^k \mid 1 \leq k \leq q-1 \text{ et } \operatorname{pgcd}(k, q-1) = 1\Big\}.$$

Démonstration : C'est une conséquence directe du théorème 2.5 et du corollaire 6.4.

Exercice 1. On considère le polynôme $P = X^4 + X + 1 \in \mathbb{F}_2[X]$.

1) Montrer que $K = \mathbb{F}_2[X]/(P)$ est un corps.
2) Quelle est la caractéristique de K, le cardinal de K ?
3) Soit α la classe de X modulo (P). Montrer que α est un générateur de K^*. Combien il y a-t-il de générateurs dans K^* ? Déterminer leurs coordonnées dans la base $(1, \alpha, \alpha^2, \alpha^3)$ de K sur $\mathbb{F}_2$.

3. Corps finis comme quotients de $\mathbb{F}_p[X]$

Voici le quatrième résultat annoncé :

Théorème 6.4. *Soit K un corps fini de cardinal p^n. Il existe un polynôme $F \in \mathbb{F}_p[X]$ irréductible de degré n tel que les corps K et $\mathbb{F}_p[X]/(F)$ soient isomorphes.*

Démonstration : Soit α un générateur de K^*. On considère l'application

$$\psi : \mathbb{F}_p[X] \to K$$

définie pour tout $P = \sum a_i X^i \in \mathbb{F}_p[X]$ par l'égalité

$$\psi(P) = \sum a_i \alpha^i,$$

où l'on identifie ici $a_i \in \mathbb{F}_p$ avec n'importe quel entier relatif dont la classe modulo p est a_i. Cela est licite car K est de caractéristique p. C'est un homomorphisme d'anneaux. Il est surjectif vu que α est un générateur de K^*. Le noyau de ψ est un idéal I de $\mathbb{F}_p[X]$ et $\mathbb{F}_p[X]/I$ est donc un anneau isomorphe à K. L'idéal I n'est pas nul, sinon K serait isomorphe à $\mathbb{F}_p[X]$, or $\mathbb{F}_p[X]$ n'est pas un corps (ou plus simplement K est fini et $\mathbb{F}_p[X]$

S'il existait un diviseur d de n tel que $\left|\Phi_d\right| = 0$, on aurait ainsi

$$n < \sum_{d|n} \varphi(d),$$

et une contradiction (lemme 2.5). En particulier, Φ_n n'est pas vide, autrement dit, il existe dans G un élément d'ordre n i.e. G est cyclique d'ordre n.

Le théorème 6.3. se déduit alors du fait que pour tout diviseur d de l'ordre de H, le polynôme $X^d - 1 \in K[X]$ a au plus d racines dans K, donc en particulier dans H.

ne l'est pas). Il existe donc un polynôme $F \in \mathbb{F}_p[X]$ tel que $I = (F)$ (th. 5.2). Puisque $\mathbb{F}_p[X]/(F)$ est un corps, F est donc irréductible (cor. 5.4). Par ailleurs, si m est le degré de F, le cardinal de $\mathbb{F}_p[X]/(F)$ est p^m (cor. 6.3), d'où $m = n$ et le résultat.

Il en résulte que les corps finis de cardinal p^n s'obtiennent exclusivement à partir de polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$. Par conséquent, compte tenu du corollaire 6.3 et du théorème 6.4, on obtient l'énoncé suivant :

Proposition 6.1. *Soient p un nombre premier et n un entier ≥ 1. Les deux assertions suivantes sont équivalentes :*

1) il existe un corps à p^n éléments.

2) Il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.

Il s'agit donc maintenant de démontrer l'existence de polynômes irréductibles de tout degré $n \geq 1$ dans $\mathbb{F}_p[X]$. Il s'agira aussi de démontrer que si U et V sont deux polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$, alors les corps $\mathbb{F}_p[X]/(U)$ et $\mathbb{F}_p[X]/(V)$ sont isomorphes (unicité à isomorphisme près des corps à p^n éléments).

Exercice 2. Démontrer l'existence de corps à 27, puis à 125 éléments.

4. Construction et unicité des corps à p^2 éléments

Soit p un nombre pemier. On va démontrer directement l'énoncé suivant, qui est un cas particulier de celui que l'on a en vue.

Théorème 6.5. *Il existe, à isomorphisme près, un unique corps de cardinal p^2.*

Démonstration : Supposons $p = 2$. Le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ étant irréductible sur $\mathbb{F}_2$, l'anneau

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1),$$

est donc un corps à quatre éléments. Puisqu'il n'existe qu'un seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$, le corps $\mathbb{F}_4$ est donc le seul corps à isomorphisme près de cardinal 4.

Supposons désormais p impair. On a vu en exercice qu'il existe $p(p-1)/2$ polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_p[X]$[34]. Il existe donc des corps à p^2 éléments.

Vérifions l'unicité annoncée. Considérons pour cela deux corps de cardinal p^2. Il s'agit de montrer qu'ils sont isomorphes, autrement dit, que si U et V sont deux polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_p[X]$, les corps

$$K = \mathbb{F}_p[X]/(U) \quad \text{et} \quad K' = \mathbb{F}_p[X]/(V),$$

[34] On procède comme suit. Tout d'abord, il y a p^2 polynômes unitaires de degré 2 dans $\mathbb{F}_p[X]$. Ceux qui sont réductibles sur $\mathbb{F}_p$ sont de la $(X-a)(X-b)$ avec a et b dans $\mathbb{F}_p$. Il y en a p pour lesquels $a = b$ et $p(p-1)/2$ pour lesquels $a \neq b$. On obtient ainsi $p^2 - p - p(p-1)/2 = p(p-1)/2$ polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_p[X]$.