Chapitre Premier CORPS FINIS (RAPPELS)

CHAPITRE PREMIER

CORPS FINIS (RAPPELS)

Ce chapitre résume les propriétés générales des corps finis. Rappelons que d'après le *théorème de Wedderburn*, tout corps fini est commutatif (pour une démonstration, voir par exemple [**1**], pp. 35-37, ou [**19**], p. 1).

§ 1. *Classification des corps finis.*

1.1. Soit k un corps fini. Sa caractéristique est certainement différente de 0; c'est un nombre premier p, et le sous-corps premier de k s'identifie à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Notons f le degré de l'extension $k/\mathbf{F}_p$; k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, au produit direct de f exemplaires de $\mathbf{F}_p$; en particulier:

PROPOSITION 1. — *Si q désigne le nombre d'éléments de k, on a $q = p^f$.*

Considérons alors k^*, groupe multiplicatif de k; il est d'ordre $q - 1$; on a donc, pour tout élément a de k^*, $a^{q-1} = 1$, et a fortiori $a^q = a$; comme cette égalité reste vraie pour $a = 0$, elle est vérifiée par tout élément de k; en conséquence:

PROPOSITION 2. — *Si Ω désigne une clôture algébrique de k (donc aussi de $\mathbf{F}_p$), k est égal à l'ensemble des racines dans Ω du polynôme $X^q - X$. En particulier, k est le corps de décomposition dans Ω du polynôme $X^q - X$, et tout corps fini ayant même nombre d'éléments q (donc même caractéristique p) que k est nécessairement isomorphe à k.*

Pour $k = \mathbf{F}_p$, l'identité $a^q = a$ s'écrit $a^p = a$, et constitue le *petit théorème de Fermat* sur les restes modulo p. Pour k quelconque, la proposition 2 permet d'écrire

$$X^{q-1} - 1 = \prod_{a \in k^*} (X - a); \quad X^q - X = \prod_{a \in k} (X - a);$$

la première de ces deux égalités montre que les fonctions symétriques élémentaires des éléments de k^* *autres que le produit* sont toutes nulles, et que le produit de tous les éléments de k^* est égal à -1; pour $k = \mathbf{F}_p$, cette dernière propriété constitue le *théorème de Wilson* sur les restes modulo p.

1.2. Soient maintenant p un nombre premier, f un entier $\geqslant 1$, et posons $q = p^f$. Désignons par Ω une clôture algébrique de $\mathbf{F}_p$, et notons k l'ensemble des racines dans Ω du polynôme $X^q - X$. Ce polynôme ayant toutes ses racines simples (son dérivé vaut -1), on voit que card $(k) = q$; de plus, q étant une puissance de la caractéristique, on a, quels que soient a et b dans k, $(a+b)^q = a^q + b^q = a + b$; on a évidemment aussi $(ab)^q = a^q b^q = ab$, et k est un sous-corps de Ω; en particulier:

PROPOSITION 3. — *Quels que soient p premier et $f \geqslant 1$, il existe un corps fini possédant exactement $q = p^f$ éléments.*

Ce corps est unique à isomorphisme près (prop. 2); on le note généralement $\mathbf{F}_q$.

1.3. Mêmes données que dans la section précédente. Soient f_1 et f_2 deux entiers $\geqslant 1$, et posons, pour $i = 1, 2$,

$$q_i = q^{f_i}; \qquad k_i = \mathbf{F}_{q_i} \subset \Omega;$$

on a alors évidemment $[k_i : \mathbf{F}_q] = f_i$. Si $k_1 \subset k_2$, la multiplicativité du degré montre que f_1 divise f_2. Inversement, supposons que f_1 divise f_2; on peut écrire $f_2 = mf_1$, donc $q_2 = {q_1}^m$; si $a \in k_1$, on a alors $a^{q_1} = a$ (prop. 2), donc $a^{{q_1}^m} = a^{q_2} = a$, et par conséquent $a \in k_2$ (prop. 2); ainsi, $k_1 \subset k_2$. Au total (et en conservant ces notations):

PROPOSITION 4. — *L'inclusion $k_1 \subset k_2$ équivaut à la relation f_1 divise f_2, donc à la relation q_2 est une puissance de q_1.*

COROLLAIRE 1. — *Soient respectivement f' et f'' le p.g.c.d. et le p.p.c.m. de f_1 et f_2. Posons $q' = q^{f'}$, $q'' = q^{f''}$, $k' = \mathbf{F}_{q'}$, $k'' = \mathbf{F}_{q''}$. Alors l'intersection et le composé de k_1 et k_2 sont respectivement k' et k''.*

§ 2. *Groupe additif et groupe multiplicatif d'un corps fini.*

Soit k un corps fini à $q = p^f$ éléments.

2.1. L'extension $k/\mathbf{F}_p$ étant de degré f, k est isomorphe, en tant qu'espace vectoriel sur $\mathbf{F}_p$, et a fortiori en tant que groupe additif, au produit direct de f exemplaires de $\mathbf{F}_p$; en conséquence:

PROPOSITION 5. — *Le groupe additif k^+ de k est un groupe de type $(p, ..., p)$ (f fois).*

2.2. Passons au groupe multiplicatif k^*; il est commutatif, d'ordre $q-1$; si N désigne le p.p.c.m. des ordres des éléments de k^*, on vérifie sans peine qu'il existe dans k^* un élément g d'ordre exactement égal à N (c'est là une propriété générale des groupes commutatifs d'ordre fini). Tout élément de k^* est évidemment racine du polynôme $X^N - 1$; ce polynôme, de degré N, possède donc au moins $q-1$ racines, d'où $N \geqslant q-1$; or, par construction même, N divise $q-1$; ainsi, $N = q-1$; mais alors g est d'ordre $q-1$, c'est un générateur de k^*, et on peut énoncer:

PROPOSITION 6. — *Le groupe multiplicatif k^* de k est un groupe cyclique d'ordre $q-1$.*

Pour une autre démonstration de ce résultat, utilisant les propriétés de l'indicatrice d'Euler, voir [**17**], pp. 12-13.

2.3. Soit d un entier $\geqslant 1$; on se propose d'étudier le groupe des puissances d-ièmes et le groupe des racines d-ièmes de l'unité dans k^*, c'est-à-dire l'image et le noyau de l'homomorphisme $u_d: k^* \to k^*$, défini par $u_d(x) = x^d$ $(x \in k^*)$. Posons $\delta = (q-1, d)$, $u_\delta(x) = x^\delta$ $(x \in k^*)$ et notons g un générateur de k^* (prop. 6). L'identité de Bezout $a(q-1) + bd = \delta$ montre que u_d et u_δ ont même noyau (noter que $x^{q-1} = 1$ pour tout $x \in k^*$); k^* étant fini, il en résulte que l'image de u_d et celle de u_δ ont même ordre; mais la première est évidemment contenue dans la seconde: u_d et u_δ ont donc aussi même image. Maintenant, comme δ divise $q-1$, il est clair que l'image de u_δ est le sous-groupe de k^* engendré par g^δ, et que le noyau de u_δ est le sous-groupe de k^* engendré par $g^{(q-1)/\delta}$ (pour le voir, identifier par exemple k^* à $\mathbf{Z}/(q-1)\,\mathbf{Z}$, g s'identifiant à la classe de 1 (mod $q-1$)). En résumé:

PROPOSITION 7. — *Soient k un corps fini à q éléments, g un générateur de k^*, d un entier $\geqslant 1$, et posons $\delta = (q-1, d)$. Alors:*

(i) *Dans k^*, les puissances d-ièmes et les puissances δ-ièmes forment un même sous-groupe, cyclique, engendré par g^δ, et d'ordre égal à $(q-1)/\delta$.*

(ii) *De même, les racines d-ièmes et les racines δ-ièmes de l'unité forment un même sous-groupe, cyclique, engendré par $g^{(q-1)/\delta}$, et d'ordre égal à δ.*

COROLLAIRE 1. — *Le groupe quotient k^*/k^{*d} est cyclique, d'ordre égal à δ.*

COROLLAIRE 2. — *Pour qu'un élément a de k^* soit une puissance d-ième, il faut et il suffit que $a^{(q-1)/\delta} = 1$.*

Pour $k = \mathbf{F}_p$, p impair, et $d = \delta = 2$, le corollaire 2 coïncide avec le *critère d'Euler* sur les restes et non-restes quadratiques modulo p.

§ 3. *Extensions algébriques d'un corps fini.*

Soit toujours k un corps fini à q éléments.

3.1. Soit K une extension algébrique de k, de degré fini m; il est clair que $\mathrm{card}\,(K) = q^m$, et donc que $K = \mathbf{F}_{q^m}$. Soit alors i un entier $\geqslant 0$; comme q^i est une puissance de la caractéristique de K, l'application σ_i: $K \to K$, définie par $\sigma_i(x) = x^{q^i}$ $(x \in K)$, est un automorphisme de K, et même, puisque $k = \mathbf{F}_q$, un k-automorphisme de K (prop. 2); si j est un autre entier $\geqslant 0$, on a évidemment $\sigma_{i+j} = \sigma_i \circ \sigma_j$; enfin, si (par exemple) $i \leqslant j$, l'ensemble des $x \in K$ tels que $\sigma_i(x) = \sigma_j(x)$, donc tels que $x^{q^{j-i}} = x$, est évidemment égal à $K \cap \mathbf{F}_{q^{j-i}}$, et ne peut par conséquent être égal à $K = \mathbf{F}_{q^m}$ que si $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^{j-i}}$, donc (prop. 4) si $i \equiv j \pmod m$; en particulier, les m k-automorphismes σ_i avec $0 \leqslant i < m$ sont distincts, et on peut affirmer:

PROPOSITION 8. — *L'extension K/k est galoisienne; son groupe de Galois est cyclique, d'ordre m, engendré par l'automorphisme* (dit de Frobenius) $x \mapsto x^q$.

Le fait que K/k est galoisienne peut se voir plus directement: en effet, k étant évidemment parfait, K/k est séparable, et il suffit de prouver que K/k est normale, ce qui résulte du fait que K est le corps de décomposition, dans une clôture algébrique de k, du polynôme $X^{q^m} - X$ (prop. 2).

3.2. Mêmes données que ci-dessus. Soit $Tr : K \to k$, l'application *trace*. La proposition 8 montre que, pour tout élément x de K, on a

$$Tr(x) = x + x^q + \ldots + x^{q^{m-1}}. \tag{3.2.1}$$

En outre:

PROPOSITION 9. — *L'application $Tr : K \to k$, est surjective. Si $x \in K$, les deux assertions suivantes sont équivalentes:*

(a) $Tr(x) = 0$;

(b) *il existe $y \in K$ tel que $x = y^q - y$.*

Démonstration. — Considérons K comme espace vectoriel sur k; Tr est alors une forme linéaire, et cette forme linéaire n'est pas nulle (si elle l'était, (3.2.1) impliquerait que le polynôme $X + X^q + \ldots + X^{q^{m-1}}$, de

degré q^{m-1}, admet pour racines les q^m éléments de K: absurde): elle est donc surjective, ce qui prouve la première assertion, et ce qui montre en outre que le noyau de Tr est un hyperplan de K; comme $Tr(y^q - y) = 0$ pour tout élément y de K, il reste, pour établir l'équivalence de (a) et (b), à prouver que l'ensemble des éléments de la forme $y^q - y$ ($y \in K$) est également un hyperplan de K; et il suffit pour cela de remarquer que l'application $y \mapsto y^q - y$ de K dans K est k-linéaire et de rang $m - 1$, puisque son noyau (formé des $y \in K$ tels que $y^q = y$, donc égal à k: prop. 2, ou prop. 8) est de dimension 1.

3.3. Mêmes données et notations que ci-dessus. Soit maintenant $N: K \to k$, l'application *norme*. La proposition 8 montre que, pour tout élément x de K, on a

$$N(x) = x.x^q \dots x^{q^{m-1}} = x^{(q^m-1)/(q-1)}. \tag{3.3.1}$$

En outre:

PROPOSITION 10. — *L'application $N: K^* \to k^*$, est surjective. Si $x \in K^*$, les deux assertions suivantes sont équivalentes:*

(a) $N(x) = 1$;

(b) *il existe $y \in K^*$ tel que $x = y^{q-1}$.*

Démonstration. — N est un homomorphisme du groupe K^* dans le groupe k^*, et il résulte de (3.3.1) et de la proposition 7 (avec $d=(q^m-1)/(q-1)$) que le noyau de N est d'ordre $(q^m-1)/(q-1)$; comme l'ordre de K^* est égal à $q^m - 1$, l'image de N est nécessairement d'ordre $q - 1 = \text{card}(k^*)$, d'où la surjectivité de N. Le noyau de N contenant évidemment tous les éléments de K^* de la forme y^{q-1} ($y \in K^*$), qui en constituent un sous-groupe, il reste donc, pour établir l'équivalence de (a) et (b), à montrer que ce sous-groupe est précisément d'ordre $(q^m-1)/(q-1)$; mais il suffit pour cela de remarquer que l'application $y \mapsto y^{q-1}$ de K^* dans K^* est un homomorphisme dont le noyau (formé des $y \in K^*$ tels que $y^{q-1} = 1$, donc égal à k^*) est d'ordre $q - 1$, et dont l'image est alors effectivement d'ordre $(q^m-1)/(q-1)$, puisque K^* est lui-même d'ordre $q^m - 1$.

Notes sur le chapitre premier

Théorème de Wedderburn: pour la démonstration originale, voir Wedderburn (1905); l'idée d'utiliser (comme dans [**1**] ou [**19**]) les propriétés des polynômes cyclotomiques pour simplifier cette démonstration est due à Witt (1931).

§ **1**: la classification des corps (commutatifs) finis (« champs de Galois ») remonte essentiellement à Galois (1830).

§ **2**: le fait que le groupe multiplicatif du corps $\mathbf{F}_p$ est cyclique est dû à Euler (1760); sa démonstration utilisait les propriétés de l'« indicatrice d'Euler ». Ce résultat est un ingrédient essentiel de la théorie des restes quadratiques (Euler, Legendre, Gauss), cubiques (Jacobi, Eisenstein), biquadratiques (Gauss, Jacobi), et plus généralement des restes de puissances quelconques (Kummer, etc.); à ce sujet, voir par exemple Dickson, *History of the Theory of Numbers.*

§ **3**: les propositions 9 et 10 sont des cas particuliers du *théorème* 90 de Hilbert relatif aux extensions cycliques (voir [**10**], pp. 213-215).

CHAPITRE 2

POLYNÔMES ET IDÉAUX DE POLYNÔMES

On sait que si K est un corps *infini*, et si F est un polynôme à une ou plusieurs variables, à coefficients dans K, et *identiquement nul* sur K, alors F est *nul*: tous ses coefficients sont nuls. Ceci n'est plus vrai pour un corps fini: ainsi, sur $k = \mathbf{F}_q$, le polynôme $X^q - X$, non nul, est pourtant identiquement nul (chap. 1, sect. 1.1 et 1.2); c'est à cette particularité des corps finis qu'est consacré le présent chapitre.

Dans tout le cours de ce chapitre (ainsi que dans les chapitres suivants), k désignera un corps fini à $q = p^f$ éléments, n un entier $\geqslant 1$, $X = (X_1, ..., X_n)$ une famille de n variables, et $k[X] = k[X_1, ..., X_n]$ l'anneau des polynômes en $X_1, ..., X_n$ à coefficients dans k; d'autre part, les éléments $\mathbf{a} = (a_1, ..., a_n)$ de k^n seront appelés *points* (ou *points rationnels sur* k, si cette précision est nécessaire); si $F \in k[X]$, si $\mathbf{a}$ est un point de k^n, et si $F(\mathbf{a}) = 0$, on dira que $\mathbf{a}$ est un *zéro* de F.

§ 1. *Polynômes réduits et polynômes identiquement nuls.*

1.1. Soit F un élément de $k[X]$.