Corps finis. Applications.

Mohamed NASSIRI

RACONTE TA LIFE.

Références

[GOUal] Les maths en tête : Algèbre, Xavier Gourdon
[PER] Cours d'algèbre, Daniel Perrin ♠
[OTZ] Exercices d'algèbre, Pascal Ortiz
[GOZ] Théorie de Galois, Ivan Gozard ♠
[ML3al] Mathématiques L3 Algèbre, Aviva Szpirglas
[FGNal1] Oraux X-ENS - Algèbre 1, Serge Francinou, Hervé Gianella et Serge Nicolas
[H2G2t1] Histoires hédonistes de groupes et de géométries - Tome 1, Philippe Caldero et Jérôme Germoni

Développements

Existence et unicité des corps finis
Théorème de Wedderburn
Théorème des deux carrés de Fermat
Théorème de Dirichlet (version faible)

Dans cette leçon, $n \in \mathbb{N}^*$, p est un nombre premier et $q = p^n$.

0 Caractéristique d'un anneau, d'un corps

Rappel 1 *Soit $p \in \mathbb{N}$, $p \geq 2$. Les asserstions suivantes sont équivalentes :*
(i) p est un nombre premier
(ii) $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre
(iii) $\mathbb{Z}/p\mathbb{Z}$ est un corps

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ et c'est un corps fini, $|\mathbb{F}_p| = p$. **[GOZ] p.3**

0.1 La caractéristique et ses propriétés [GOZ] p.6-7

Définition 2 *Soit A un anneau. Il existe un unique morphisme d'anneaux*

$$f : \mathbb{Z} \to A$$
$$n \mapsto \underbrace{1_A + ... + 1_A}_{n \ fois}$$

$\mathrm{Ker}(f)$ est un idéal de $\mathbb{Z}$, donc il existe un unique entier $c \in \mathbb{N}\backslash\{1\}$ tel que $\mathrm{Ker}(f) = c\mathbb{Z}$. Ce nombre c est appelé la caractéristique de A et on note $c = \mathrm{car}(A)$.

Exemple 3 *La caractéristique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est n.*

Proposition 4 *Soit A un anneau fini. Alors $\mathrm{car}(A) \neq 0$ et $\mathrm{car}(A) \mid \mathrm{card}(A)$*

Proposition 5 *Soit A un anneau intègre. Alors $\mathrm{car}(A)$ est soit nulle, soit un nombre premier.*

Corollaire 6 *Soit k un corps. Alors $\mathrm{car}(k)$ est soit nulle, soit un nombre premier.*

Proposition 7 *Soit p un nombre premier et A un anneau de caractéristique p. Alors*

$$\forall a, b \in A, \quad (a+b)^p = a^p + b^p$$

0.2 Sous-corps premier d'un corps [GOZ] p.7-8

Définition 8 *Un corps K est dit premier si et seulement si K n'a pas d'autre sous-corps que lui-même.*

Exemple 9 *$\mathbb{Q}$ est un corps premier.*
$\mathbb{F}_p$ est un corps premier.

Définition 10 *Soit K un corps. Notons P le sous-corps de K engendré 1_K, c'est-à-dire l'intersection de tous les sous-corps de K. Le corps P est bien sûr un corps premier. On l'appelle le sous-corps premier de K.*

Remarque 11 1) *K est un corps premier si et seulement si $P = K$.*
2) *Un corps et l'un quelconque de ses sous-corps ont le même sous-corps premier.*

Proposition 12 *Soit K un corps, P son sous-corps premier, et c sa caractéristique. On a :*
(i) Soit $c = 0$, et alors P est isomorphe à $\mathbb{Q}$
(ii) Soit c est un nombre premier p et alors P est isomorphe à $\mathbb{F}_p$.

Remarque 13 *Dans tous les cas, que K soit ou non commutatif, P est commutatif.*

Proposition 14 *Soit p un nombre premier. Tout corps fini de cardinal p est isomorphe à $\mathbb{F}_p$.*

1 Existence et constructions

1.1 Structure de $\mathbb{F}_p$-e.v. Commutativité [GOZ] p.81-82

Remarque 15 *On s'affranchit provisoirement, jusqu'au théorème de Wedderburn, de l'hypothèse de commutativité des anneaux et corps considérés*

Proposition 16 *Tout anneau intègre ayant un nombre fini $n \geq 2$ d'éléments est un corps.*

Théorème 17 *Soit F un corps fini. Alors :*
(i) La caractéristique de F est un nombre premier.
(ii) Son sous-corps premier est isomorphe à $\mathbb{F}_p$.
(iii) Il existe un $n \in \mathbb{N}^*$ tel que $\mathrm{card}(F) = p^n$.

Remarque 18 *- Pour p premier, le corps $\mathbb{F}_p(X)$ est un corps infini de caractéristique p.*
- Il n'existe pas de corps à 6 éléments.

Théorème 19 ♠ *Théorème de Wedderburn* ♠
Tout corps fini est commutatif. **[PER] p.82**

1.2 Groupe multiplicatif K^* [GOZ] p.83-84

Théorème 20 *Soit K un corps commutatif. Tout sous-groupe fini du groupe multiplicatif K^* est cyclique.*

Corollaire 21 *Le groupe multiplicatif d'un corps fini est cyclique.*

Remarque 22 1) *Pour p premier, $\mathbb{F}_p^*$ est cyclique. Le tableau suivant donne, pour p premier avec $p \leq 25$, la valeur de*

$$g = \min\{k \in [\![1, p-1]\!] \mid \overline{k} \text{ engendre } \mathbb{F}_p^*\}$$

p	2	3	5	7	11	13	17	19	23
g	1	2	2	3	2	2	3	2	5

2) *On ne sait en général pas déterminer explicitement un tel générateur ...*

Proposition 23 *Soit F un corps fini de caractéristique p, ξ un générateur de F^*. Alors $F = \mathbb{F}_p(\xi) = \mathbb{F}_p[\xi]$, et, en notant $n = [F : \mathbb{F}_p]$, on a :*

$$F = \mathbb{F}_p \oplus \mathbb{F}_p\xi \oplus ... \oplus \mathbb{F}_p\xi^{n-1}$$

Remarque 24 *La réciproque est fausse : on peut avoir $F = \mathbb{F}_p(\theta) = \mathbb{F}_p[\theta]$ sans que θ soit un générateur du groupe cyclique F^*.*

1.3 Existence et unicité [GOZ] p.85 → 89

Théorème 25 ♠ *Existence et unicité des corps finis* ♠
Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
(1) Il existe un unique corps fini à q éléments. Il est le corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$. On le note $\mathbb{F}_q$
(2) $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$, où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.
(3) Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\pi(x) \mid X^q - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_q$.

Remarque 26 *L'assertion (3) se traduit par le fait que, dans les corps finis, le corps de rupture est égal au corps de décomposition.*

Exemple 27 $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.
Comme j est racine de $X^2 + X + 1$, on a

$$\mathbb{F}_4 = \mathbb{F}_2(j) = \{0, 1, j, j^2 = 1 + j\}$$

2 Structure

2.1 Extensions de corps et sous-corps d'un corps fini

Théorème 28 *Théorème de l'élément primitif pour les corps finis*
Soit K un corps fini. Soit L une extension de degré fini de K. Alors L est monogène (i.e.) il existe $\xi \in L$ tel que $L = K(\xi)$. Un tel élément ξ est appelé un élément primitif de l'extension L de K.

Théorème 29 *Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$.*
Tout corps intermédiaire $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^n}$ est un corps $\mathbb{F}_{q^d}$ à q^d éléments où d est un diviseur de n et que, pour chaque diviseur d de n, il existe un unique corps intermédiaire de cardinal q^d. **[OTZ] p.141-142**

2.2 Carrés de $\mathbb{F}_q$

2.2.1 Généralités [GOZ] p.93

Proposition 30 *On pose*

$$\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\} \quad et \quad \mathbb{F}_q^{*2} = \mathbb{F}_q^* \cap \mathbb{F}_q^2$$

$\mathbb{F}_q^{*2}$ *est un sous-groupe de* $\mathbb{F}_q^*$.

Proposition 31 1) *Si* $p = 2$, *alors*

$$\mathbb{F}_q^2 = \mathbb{F}_q, \ donc \ \mathbb{F}_q^{*2} = \mathbb{F}_q^*$$

2) *Si* $p > 2$, *alors*
(*i*) $\mathbb{F}_q^{*2}$ *est un sous-groupe d'indice 2 de* $\mathbb{F}_q^*$ *; donc*

$$|\mathbb{F}_q^{*2}| = \frac{q-1}{2} \quad et \quad |\mathbb{F}_q^2| = \frac{q+1}{2}$$

(*ii*) $\mathbb{F}_q^{*2}$ *est le noyau de l'endomorphisme*

$$\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*, \quad x \mapsto x^{\frac{q-1}{2}}$$

(*iii*) $-1 \in \mathbb{F}_p^{*2} \Leftrightarrow p \equiv 1 \pmod 4$

2.2.2 ♠ Théorème des deux carrés ♠ [PER] p.56 → 58, 74-75

Définition 32 *On pose* $\Sigma = \{n \in \mathbb{N} \mid n = a^2+b^2 = n\}$

Lemme 33 $\mathbb{Z}[i] = \{a+ib, \ a, b \in \mathbb{N}\}$ *est un anneau euclidien* $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Lemme 34

$$p \in \Sigma \Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i] \Leftrightarrow -1 \in \mathbb{F}_p^{*2}$$

Théorème 35 $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \pmod 4$

3 Applications

3.1 Théorème de Dirichlet (version faible)

Théorème 36 *Théorème de Dirichlet (version faible) :* ♠
a) $\Phi_n(X)$ *désigne le n-ième polynôme cyclotomique. Si un nombre premier p divise* $\Phi_n(a)$ *pour un certain* $a \in \mathbb{N}$, *mais aucun des* $\Phi_d(a)$ *où* $d \mid n$, $d < n$, *alors* $p \equiv 1 \pmod n$
b) Il existe une infinité de nombres premiers de la forme $1 + \lambda n$, $\lambda \in \mathbb{N}^*$. **[GOZ] p.84**

3.2 Irréductibilité des polynômes

Théorème 37 *Critère de réduction modulo p :*
Soit p un nombre premier. Soit $P = a_nX^n + ... + a_1X + a_0 \in \mathbb{Z}[X]$ *et* $\overline{P} = \overline{a_n}X^n + ... + \overline{a_1}X + \overline{a_0}$, *où* $\overline{a_i}$ *est la classe des* a_i *dans* $\mathbb{Z}/p\mathbb{Z}$
Alors si $\overline{P}$ *est irréductible sur* $\mathbb{F}_p$, P *est irréductible sur* $\mathbb{Z}$.
Si $c(P) = 1$, *alors* P *est irréductible dans* $\mathbb{Z}[X]$. **[ML3ag] p.550**

Exemple 38 $P(X) = X^3+462X^2+2433X-67691$ *est irréductible dans* $\mathbb{Z}[X]$ **[PER] p.77**

Proposition 39 *Soit* $P \in K[X]$ *un polynôme de degré* $n \geq 1$. *P(X) est irréductible dans K[X] si et seulement si P(X) n'a pas de racine dans les extensions L de K telles que* $[L : K] \leq n/2$. **[GOZ] p.59**

Exemple 40 X^4+X+1 *est irréductible sur* $\mathbb{F}_2$ *car il n'a pas de racines dans* $\mathbb{F}_2$, *ni* $\mathbb{F}_4$. **[PER] p.78**

3.3 Algèbre linéaire et bilinéaire

Proposition 41 *Sur un corps fini* $\mathbb{F}_q$ *à q éléments et pour un entier m donné, les ensembles suivants ont pour cardinaux :*
(*i*) *Espace vectoriel :*

$$|\mathbb{F}_q^m| = q^m$$

(*ii*) *Groupe linéaire :*

$$|\mathrm{GL}_m(\mathbb{F}_q)| = (q^m-1)(q^m-q)...(q^m-q^{m-1}) = (q^m-1)(q^{m-1}-1)...(q-1)q^{m(m-1)/2}$$

C'est aussi le nombre de bases de $\mathbb{F}_q^m$.
(*ii*) *Groupe spécial linéaire :*

$$|\mathrm{SL}_m(\mathbb{F}_q)| = \frac{(q^m-1)(q^m-q)...(q^m-q^{m-1})}{q-1} = (q^m-1)(q^{m-1}-1)...(q^2-1)q^{m(m-1)/2}$$

[H2G2t1] p.250-252, [FGNal1] p.17

Proposition 42 *Soit q une puissance d'un nombre premier impair. On a un isomorphisme :*

$$\mathrm{SO}_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} \ si \ -1 \in \mathbb{F}_p^{*2} \\ \mathbb{Z}/(q+1)\mathbb{Z} \ si \ -1 \notin \mathbb{F}_p^{*2} \end{cases}$$

Proposition 43 *Soit* $\mathbb{K}$ *un corps commutatif fini à q éléments, E un* $\mathbb{K}$*-e.v. de dimension finie et* $f \in \mathcal{L}(E)$. *Montrer que f est diagonalisable dans E si et seulement si* $f^q = f$. **[GOUal] p.178**

Théorème 44 *Soit* $k = \mathbb{F}_q$ *un corps fini de caractéristique différente de 2, et E un k-espace vectoriel de dimension n.*
Soit $\alpha \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}$. *Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur E, de matrices*

$$Q_1 = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \quad \text{et}$$

$$Q_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \dots & 0 & \alpha \end{pmatrix}$$

[PER] p.130

Illustrations

Questions

Exercice :

Solution :

Exercice :

Solution :

Exercice :

Solution :