

123: Corps finis. Applications.

Tous les corps considérés ici sont supposés commutatifs. K et L sont des corps.

1 Propriétés et construction des corps finis

1.1 Caractéristique, sous-corps premier, cardinal

Proposition 1. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier. Dans ce cas, on note $\mathbb{F}_p$ ce corps.

Définition 2. Soit K un corps. On appelle caractéristique de K l'unique entier naturel n tel que le noyau du morphisme d'anneaux de $\mathbb{Z}$ dans K soit $n\mathbb{Z}$.

Proposition 3. La caractéristique d'un corps est soit 0, soit un nombre premier.

Proposition 4. Le plus petit sous-corps de K , appelé sous-corps premier, est:

- Isomorphe à $\mathbb{Q}$ si K est de caractéristique nulle.
- Isomorphe à $\mathbb{F}_p$ si K est de caractéristique p .

Remarque 5. Si K est un corps fini, sa caractéristique est un nombre premier. La réciproque est fautive: $\mathbb{F}_p(X)$ est infini de caractéristique p .

Proposition 6. Soit $K \rightarrow L$ une extension de corps. Alors L peut être muni d'une structure de K -espace vectoriel. On note $[L : K]$ sa dimension.

Corollaire 7. Si K est un corps fini de caractéristique p , alors il existe $n \in \mathbb{N}^*$ tel que $\text{Card}(K) = p^n$: le cardinal de tout corps fini est une puissance d'un nombre premier.

Proposition 8. (Base télescopique) Si $k \subset K \subset L$, si $(\alpha_i)_{i \in I}$ est une K -base de L , et $(\beta_j)_{j \in J}$ une k -base de K , alors $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ est une k -base de L .
Et $[L : k] = [L : K][K : k]$ (y compris si l'un vaut $+\infty$).

Proposition 9. Soit K un corps de caractéristique p premier. L'application $K \rightarrow K, x \mapsto x^p$ est un morphisme de corps, appelé morphisme de Frobenius. Si K est fini, alors ce morphisme est un automorphisme.

1.2 Construction

Théorème 10. Soit $P \in K[X]$. Il existe un corps de décomposition de P sur K , unique à K -isomorphisme près.

Théorème 11. Soit p premier, et soit $n \in \mathbb{N}^*$. Il existe, à isomorphisme près, un unique corps à p^n éléments, qui est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_{p^n}$.

Proposition 12. On a un morphisme de corps $\mathbb{F}_q \rightarrow \mathbb{F}_{q'}$ si et seulement si q' est une puissance de q .

Exemple 13. Le seul sous-corps de $\mathbb{F}_8$ distinct de $\mathbb{F}_8$ est $\mathbb{F}_2$.

Lemme 14. La clôture algébrique de $\mathbb{F}_p$, notée $\overline{\mathbb{F}_p}$, coïncide avec celle de $\mathbb{F}_{p^n}$.

Théorème 15.

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}.$$

1.3 Groupe $(\mathbb{F}_q^*, \times)$

Théorème 16. (Wedderburn) Tout corps fini est commutatif.

Lemme 17. L'indicatrice d'Euler φ satisfait $\forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d)$.

Proposition 18. $\mathbb{F}_q^*$ est un groupe cyclique, automatiquement isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Proposition 19. Soit K un corps fini de caractéristique p , et soit α un générateur de K^* . Alors $K = \mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha]$, et si $n = [K : \mathbb{F}_p]$, alors $K = \bigoplus_{i=0}^{n-1} \mathbb{F}_p \alpha^i$.

2 Polynômes irréductibles

2.1 Polynômes irréductibles et dénombrement

Théorème 20. $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(P)$ où P est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Corollaire 21. Pour tout $n \in \mathbb{N}^*$, il existe un polynôme de degré n irréductible sur $\mathbb{F}_p$.

Définition 22. On définit la fonction de Möbius $\mu : \mathbb{N}^* \rightarrow \mathbb{C}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n admet un facteur carré, et $\mu(p_1 \cdots p_r) = (-1)^r$ pour $p_1, \dots, p_r$ premiers deux à deux distincts.

DÉVELOPPEMENT : 1

Théorème 23. (Formule d'inversion de Möbius) Soit $f : \mathbb{N}^* \rightarrow \mathbb{C}$. On définit $g : \mathbb{N}^* \rightarrow \mathbb{C}$, $n \mapsto \sum_{d|n} f(d)$. Alors :

$$f(n) = \sum_{d|n} \mu(n/d)g(d) = \sum_{d|n} \mu(d)g(n/d).$$

Théorème 24. On note $A(n, q)$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbb{F}_q[X]$, et $I(n, q) = \text{Card } A(n, q)$. On a :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d, q)} P(X).$$

$$\text{Ainsi } q^n = \sum_{d|n} dI(n, q), \text{ et } I(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{n \rightarrow +\infty}{\sim} \frac{q^n}{n}.$$

2.2 Application à l'irréductibilité sur $\mathbb{Z}$ ou $\mathbb{Q}$

Théorème 25. (Critère d'Eisenstein) Soient A un anneau factoriel, et K son corps des fractions. Soit $P = \sum_{k=0}^n a_k X^k \in A[X]$ tel qu'il existe $p \in A$ irréductible vérifiant:

- p divise $a_0, a_1, \dots, a_{n-1}$
- p ne divise pas a_n
- p^2 ne divise pas a_0

Alors P est irréductible dans $K[X]$.

Exemple 26. Pour p premier, $\Phi_p(X) = 1 + X + \dots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$.

Théorème 27. Soient $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ et p premier tels que $a_n \not\equiv 0 \pmod{p}$. Si $\bar{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Application 28. $X^p - X - 1$ est irréductible sur $\mathbb{Q}$.

Remarque 29. La réciproque est fautive: $X^4 + 1$ est irréductible sur $\mathbb{Z}$, mais réductible sur chaque $\mathbb{F}_p$.

3 Carrés dans $\mathbb{F}_q$

Proposition 30. a est un carré modulo $n = \prod_{i=1}^r p_i^{\alpha_i}$ si, et seulement si, c'est un carré modulo chaque $p_i^{\alpha_i}$.

Proposition 31. n premier avec p est un carré modulo p^α si, et seulement si :

- n est un carré modulo p (cas p impair).
- $n \equiv 1 \pmod{4}$ (cas $p = 2, \alpha = 2$).
- $n \equiv 1 \pmod{8}$ (cas $p = 2, \alpha \geq 3$).

Proposition 32. On suppose $\text{car}(\mathbb{F}_q) \neq 2$. Pour $(a, b, c) \in \mathbb{F}_q^* \times \mathbb{F}_q^2$, l'équation $ax^2 + bx + c$ admet des solutions dans $\mathbb{F}_q$ si, et seulement si, $b^2 - 4ac$ est un carré dans $\mathbb{F}_q$.

Définition 33. On note $\mathbb{F}_q^{(2)} = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*(2)} = \mathbb{F}_q^{(2)} \setminus \{0\}$.

Proposition 34.

- Si $p = 2$, alors $\mathbb{F}_q^{(2)} = \mathbb{F}_q$.
- Si $p \geq 3$, alors $\text{Card}(\mathbb{F}_q^{*(2)}) = \frac{q-1}{2}$.

Corollaire 35. Si $p \geq 3$, alors $x \in \mathbb{F}_q^{*(2)} \iff x^{(q-1)/2} = 1$.

Corollaire 36. Si $p \geq 3$, $-1 \in \mathbb{F}_q^{*(2)} \iff q \equiv 1 \pmod{4}$.

Application 37. Il existe une infinité de nombres premiers de la forme $4n + 1$.

Définition 38. (Symbole de Legendre) Soient p un nombre premier impair et $a \in \mathbb{F}_p$. On définit

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a \in \mathbb{F}_p^{*(2)} \\ -1 & \text{sinon} \end{cases}$$

Remarque 39. On étend cette définition aux entiers relatifs: $a \in \mathbb{Z}$ premier avec p est un carré modulo p si $\left(\frac{a}{p}\right) = 1$.

Proposition 40. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Corollaire 41. L'application $\mathbb{F}_p^* \rightarrow \{-1, 1\}, x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupes.

DÉVELOPPEMENT : 2

Théorème 42. (Loi de réciprocité quadratique) Pour p, q deux nombres premiers impairs distincts, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Proposition 43. Pour p premier impair, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Remarque 44. Ces résultats permettent de calculer $\left(\frac{a}{p}\right)$ pour tous a, p par réductions successives.

4 Algèbre linéaire et algèbre bilinéaire sur $\mathbb{F}_q$

4.1 Algèbre linéaire

Proposition 45. $\text{Card}(\mu_n(\mathbb{F}_q)) = \text{PGCD}(n, q-1)$.

Proposition 46.

$$\text{Card}(GL_n(\mathbb{F}_q)) = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

$$\text{Card}(PGL_n(\mathbb{F}_q)) = \text{Card}(SL_n(\mathbb{F}_q)) = (q^n - 1)(q^n - q) \dots (q^n - q^{n-2})q^{n-1}$$

$$\text{Card}(PSL_n(\mathbb{F}_q)) = \text{Card}(SL_n(\mathbb{F}_q)) / \text{PGCD}(n, q-1).$$

Application 47. Soient $p \geq 3$ premier, $n \in \mathbb{N}^*$, et $q = p^n$. Alors:

$$SO_2(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré dans } \mathbb{F}_q^* \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

Proposition 48. Le nombre de matrices diagonalisables de $M_n(\mathbb{F}_q)$ est donné par :

$$D_n = \sum_{\substack{n_1 + \dots + n_q = n \\ n_i \geq 0}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)| \times \dots \times |GL_{n_q}(\mathbb{F}_q)|}$$

4.2 Formes quadratiques

Ici, K est un corps fini de caractéristique distincte de 2, et E est un K -espace vectoriel de dimension finie n .

f est une forme quadratique non dégénérée sur E .

Lemme 49. Pour $a, b \in \mathbb{F}_q^*$, l'équation $ax^2 + by^2 = 1$ admet toujours au moins une solution dans $\mathbb{F}_q^2$.

Théorème 50. Soit $\alpha \in K^* \setminus K^{*(2)}$. Alors f est équivalente à l'une des deux formes quadratiques suivantes:

- $f_1(x) = x_1^2 + \cdots + x_{n-1}^2 + x_n^2$
- $f_2(x) = x_1^2 + \cdots + x_{n-1}^2 + \alpha x_n^2$

Une forme quadratique f est dans l'une ou l'autre de ces classes suivant si son discriminant est un carré dans $\mathbb{F}_q$ ou non.

Corollaire 51. Il y a deux orbites pour l'action par congruence de $GL_n(\mathbb{F}_q)$ sur $S_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$.