P. Maurer
ENS Rennes

Leçon 123. Corps finis. Exemples et applications.

Devs :

- Polynômes cyclotomiques
- Loi de réciprocité quadratique

Références :

1. Perrin, Cours d'algèbre
2. Gozard, Théorie de Galois
3. Combes, Algèbre et géométrie
4. Caldero, H2G2

Dans tout ce qui suit, p est un nombre premier et on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On rappelle que $\mathbb{F}_p$ est un corps a p éléments.

1 Construction des corps finis

1.1 Caractéristique et extensions de corps

Définition 1. *On dit que L est une extension de K si K est un sous-corps de L, i.e s'il existe un morphisme de corps injectif $\rho: K \to L$. Dans ce cas, on peut voir L comme K-espace vectoriel. On note $[L:K]$ la dimension de L en tant que K-ev, si cette dernière est finie.*

Théorème 2. *(Base télescopique)*

Soit $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K, $(f_j)_{j\in J}$ une base de M sur L. Alors $(e_i f_j)_{i\in I, j\in J}$ est une base de M sur K. En particulier, $[M:K] = [M:L][L:K]$.

Proposition 3. *Soit K un corps, et $\varphi: \mathbb{Z} \to K$ l'homomorphisme d'anneau défini par $\varphi(n) = n \cdot 1 = 1 + \cdots + 1$. L'ensemble $\operatorname{Ker}\varphi$ est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ et comme $\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{Im}(\varphi) \subset K$ est intègre, $p\mathbb{Z}$ est un idéal premier. Il y a donc deux cas : p est nul ou p est premier.*

Définition 4. *On appelle caractéristique de K l'entier p tel que $\operatorname{Ker}\varphi = p\mathbb{Z}$, et on le note $\operatorname{car}(K)$. On a donc $\operatorname{car}(K) = 0$ ou $\operatorname{car}(K) \in \mathbb{P}$.*

Proposition 5. *Si $\operatorname{car}(K) = p > 0$, alors pour tout $x \in K$, on a $px = 0$.*

Exemple 6. Les corps de caractéristique nulle sont infinis.

Exemple 7. Si K est fini, alors $\operatorname{car}(K) = p > 0$, et $\mathbb{F}_p \subset K$. Le théorème de la base téléscopique donne alors $|K| = q = p^n$ pour un certain $n \geq 1$.

Proposition 8. *Soit K un corps de caractéristique $p > 0$. L'application $F: K \to K$ définie par $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme, et si $K = \mathbb{F}_p$, c'est l'identité.*

1.2 Existence et unicité

Définition 9. *Soit K un corps et L une extension de K. Soit $P \in K[X]$, avec $\deg(P) = n \in \mathbb{N}^*$. On dit que L est un corps de décomposition de P sur K si P s'écrit $P(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ avec $a, \alpha_1, \ldots, \alpha_n \in L$ et si $L = K(\alpha_1, \ldots, \alpha_n)$.*

Exemple 10. $\mathbb{C} = \mathbb{R}(i)$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$, et $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$.

$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $\sqrt[3]{2}$ sur $\mathbb{Q}$ mais pas un corps de décomposition.

Théorème 11. *Soit $P \in K[X]$ de degré $n \geq 1$.*

1. *Il existe un corps de décomposition L de P sur K, avec $[L:K] \leq n!$*
2. *Si L et L' sont deux corps de décomposition de P sur K, alors il existe un K-isomorphisme de L dans L'.*

Théorème 12. *Soit $n \in \mathbb{N}^*$. On pose $q = p^n$. Alors il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. En particulier, K est unique à isomorphisme près.*

Théorème 13. *(Wedderburn). Tout corps fini est commutatif.*

Proposition 14. *Soit $n, m \in \mathbb{N}$. Alors $\mathbb{F}_{p^n}$ s'injecte dans $\mathbb{F}_{p^m}$ si et seulement si $n|m$.*

Exemple 15. Les sous-corps de $\mathbb{F}_6$ sont $\mathbb{F}_4$ et $\mathbb{F}_2$.

Dans tout ce qui suit, on se donne $n \in \mathbb{N}$ et on note $q = p^n$.

1.3 Le groupe $\mathbb{F}_q^*$

Définition 16. *On note $\mathbb{F}_q^*$ le groupe des inversibles de $\mathbb{F}_q$, donc $\mathbb{F}_q \setminus \{0\}$. On a ainsi $|\mathbb{F}_q^*| = q - 1$.*

Lemme 17. *On note φ l'indicatrice d'Euler. Alors $\varphi(n) = \sum_{d|n} \varphi(d)$.*

Théorème 18. *Le groupe $(\mathbb{F}_q^*, \times)$ est cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.*

Remarque 19. En général, il est difficile d'exhiber un générateur de $\mathbb{F}_q^*$.

Corollaire 20. *(Théorème de l'élément primitif pour les corps finis).*
Soit $L/\mathbb{F}_q$ une extension finie du corps fini $\mathbb{F}_q$. Alors il existe $\alpha \in L$ tel que $L = \mathbb{F}_q(\alpha)$.

2 Carrés dans $\mathbb{F}_q$

2.1 Propriétés de $\mathbb{F}_q^2$

Notation 21. *On pose $\mathbb{F}_q^2 := \{y \in \mathbb{F}_q : \exists x \in \mathbb{F}_q,\ y = x^2\}$, et $\mathbb{F}_q^{*2} := \mathbb{F}_q^* \cap \mathbb{F}_q^2$.*

Proposition 22. *Si $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p > 2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.*

Proposition 23. *On suppose $p > 2$ et on se donne $a \in \mathbb{F}_q^*$. Alors*

$$a^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^* \end{cases}.$$

Corollaire 24. *Soit $p > 2$ premier. Alors -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1[4]$.*

Application 25. *Soit $n \in \mathbb{Z}$. Alors n est somme de deux carrés si et seulement si*

$$\forall p \in \mathbb{P} \quad v_p(n) \equiv 0[2],$$

où $\mathbb{P}$ désigne l'ensemble des nombres premiers et $v_p(n)$ est la valuation p-adique de n.

2.2 Symbole de legendre

Définition 26. *On définit le symbole de Legendre pour $p > 2$ et $a \in \mathbb{F}_p$ par*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^*, \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^*, \\ 0 & \text{si } a = 0. \end{cases}$$

Remarque 27. D'après ce qui précède, pour $a \neq 0$ on a donc $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. En particulier, le symbole de Legendre est multiplicatif, au sens où $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proposition 28. *Soit p un nombre premier impair et a un élément de $\mathbb{F}_p^*$. On a*

$$|\{x \in \mathbb{F}_p : ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Développement 1 :

Théorème 29. *(Loi de réciprocité quadratique)*
Soit p et q deux nombres premiers impairs distincts. Alors on a

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Exemple 30. Calcul du symbol de Legendre :
$\left(\frac{23}{59}\right) = (-1)^{11.29} \left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = \cdots = \left(\frac{2}{3}\right) = -1.$

Lemme 31. *Pour tout nombre premier p impair, 8 divise $p^2 - 1$.*

Proposition 32. *Pour tout nombre premier p impair, on a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

2.3 Résolution des équations de degré 2

Proposition 33. *Trouver des solutions à l'équation $ax^2 + bx + c \equiv 0[p]$ avec $a, b, c \in \mathbb{Z}$ revient à trouver les racines du polynôme $\bar{a}X^2 + \bar{b}X + \bar{c} \in \mathbb{F}_p[X]$.*

Proposition 34. *Le polynôme $\bar{a}X^2 + \bar{b}X + \bar{c}$ a des racines dans $\mathbb{F}_p$ si et seulement si son discriminant $\Delta = \bar{b}^2 - 4\bar{a}\bar{c}$ appartient à $\mathbb{F}_p^2$.*

Proposition 35. *Si $\Delta \in \mathbb{F}_p^2$, en notant $\alpha \in \mathbb{F}_p$ tel que $\Delta = \alpha^2$, alors $\bar{a}X^2 + \bar{b}X + \bar{c}$ a pour racines α et $-\alpha$.*

3 Applications

3.1 Polynômes sur $\mathbb{F}_q$

Définition 36. *Un corps K est dit algébriquement clos si tout polynôme de $K[X]$ non constant admet une racine dans K.*

Remarque 37. $\mathbb{F}_q$ n'est pas algébriquement clos car $X^q - X + 1$ n'a aucune racine dans $\mathbb{F}_q$.

Proposition 38. *$F := \bigcup_{m \geq 1} \mathbb{F}_{p^{m!}}$ est un corps algébriquement clos contenant $\mathbb{F}_q$. On dit que F est une clotûre algébrique de $\mathbb{F}_q$.*

Théorème 39. *Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$, et $\bar{P}$ sa réduction sur $\mathbb{F}_p$ avec p premier, c'est-à-dire $\bar{P} = \sum_{i=0}^n \bar{a_i} X^i$. Si $\bar{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Z}$.*

Remarque 40. La réciproque est fausse, par exemple en prenant $P=X^4+1$.

Proposition 41. *Le polynôme X^p-X-1 est irréductible sur $\mathbb{F}_p$.*

3.2 Cyclotomie

Dans ce qui suit, K est un corps et $n\in\mathbb{N}^*$ est un entier tel que $\operatorname{car}(K)\nmid n$.

Définition 42. *On appelle groupe des racines $n^{\text{èmes}}$ de l'unité dans K, et on note $\mu_n(K)$ l'ensemble $\{\zeta\in K:\zeta^n=1\}$. Une racine $n^{\text{ème}}$ de l'unité est dite primitive si de plus, pour tout k divisant n, on a $\zeta^k\neq 1$. On note $\mu_n^*(K)$ l'ensemble des racines primitives $n^{\text{èmes}}$ de l'unité.*

Définition 43. *Le $n^{\text{ème}}$ polynôme cyclotomique sur K est défini par :*

$$\Phi_{n,K}(X):=\prod_{\zeta\in\mu_n^*(K)} X-\zeta.$$

Lemme 44. *$\Phi_{n,K}(X)$ est unitaire, de degré $\varphi(n)$, et vérifie $X^n-1=\prod_{d|n}\Phi_{d,K}(X)$.*

Développement 2 :

Théorème 45. *(Polynômes cyclotomiques rationnels)*

i. $\Phi_{n,\mathbb{Q}}(X)$ est à coefficients dans $\mathbb{Z}$.

ii. $\Phi_{n,\mathbb{Q}}(X)$ est irréductible sur $\mathbb{Z}$.

Théorème 46. *(Cas des corps finis)*
Les propositions suivantes sont équivalentes :

i. Il existe p premier, avec $p\wedge n=1$, tel que $\Phi_{n,\mathbb{F}_p}(X)$ soit irréductible sur $\mathbb{F}_p$.

ii. $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

3.3 Groupes linéaires sur $\mathbb{F}_q$

Définition 47. *Pour $n\in\mathbb{N}$, on note $U_n(k)$ l'ensemble des matrices triangulaires supérieures dont les coefficients diagonaux sont tous égaux à 1. C'est un sous-groupe de $\mathrm{GL}_n(k)$.*

Proposition 48. *Soit p un nombre premier et $n\in\mathbb{N}$. Alors on a :*

- $|\mathrm{GL}_n(\mathbb{F}_p)|=(p^n-1)\cdots(p^n-p^{n-1})=m\,p^{\frac{n(n-1)}{2}}$,
- $|\mathrm{SL}_n(\mathbb{F}_p)|=(p^n-1)\cdots(p^n-p^{n-2})\cdot p^{n-1}$,
- $|U_n(\mathbb{F}_p)|=p^{\frac{n(n-1)}{2}}$.

Où $m=(p-1)\cdots(p^n-1)$ est premier avec p.

Définition 49. *Soit G un groupe d'ordre $p^\alpha m$ avec $p\nmid m$. On dit que $H<G$ est un p-Sylow de G si c'est un sous-groupe d'ordre p^α.*

Proposition 50. *Le groupe $\mathrm{GL}_n(\mathbb{F}_p)$ admet pour p-Sylow le sous-groupe $U_n(\mathbb{F}_p)$.*

Théorème 51. ***(Sylow)***
Soit G un groupe d'ordre $p^\alpha m$ avec $p\nmid m$. Alors :

1. *G possède au moins un p-Sylow.*
2. *Les p-Sylow sont tous conjugués entre eux.*
3. *En notant k le nombre de p-Sylow, on a $k\equiv 1 \pmod p$ et k divise m.*

Proposition 52.
Le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ est :

$$\sum_{n_1+\cdots+n_q=n}\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q|\mathrm{GL}_{n_i}(\mathbb{F}_q)|}$$

Théorème 53. *(isomorphismes exceptionnels)*
On a les isomorphismes suivants :

- $\mathrm{GL}_2(\mathbb{F}_2)=\mathrm{SL}_2(\mathbb{F}_2)=\mathrm{PSL}_2(\mathbb{F}_2)\simeq\mathcal{S}_3$,
- $\mathrm{PGL}_2(\mathbb{F}_3)\simeq\mathcal{S}_4$ *et* $\mathrm{PSL}_2(\mathbb{F}_3)\simeq\mathcal{A}_4$,
- $\mathrm{PGL}_2(\mathbb{F}_4)=\mathrm{PSL}_2(\mathbb{F}_4)\simeq\mathcal{A}_5$,
- $\mathrm{PGL}_2(\mathbb{F}_5)\simeq\mathcal{S}_5$ *et* $\mathrm{PSL}_2(\mathbb{F}_5)\simeq\mathcal{A}_5$.