

Leçon 123 : Corps finis. Applications

1 Construction

1.1 Rappels sur les extension de corps

Définition 1. Soient $\mathbb{K}$ et $\mathbb{L}$ des corps. On dit que $\mathbb{L}$ est une extension de $\mathbb{K}$ lorsque $\mathbb{K} \subset \mathbb{L}$.

Théorème 2. (Base télescopique) Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des corps, $(e_i)_{i \in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j \in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors la famille $(e_i f_j)_{(i,j) \in I \times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

Corollaire 3. (Multiplicativité du degré) Dans la situation précédente on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 4. Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible. Une extension $\mathbb{L} \supset \mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ lorsque $\mathbb{L}$ est une extension monogène $\mathbb{L} = \mathbb{K}[\alpha]$ avec $P(\alpha) = 0$.

Théorème 5. Soit $P \in \mathbb{K}$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$ unique à isomorphisme près.

Définition 6. Soit $P \in \mathbb{K}[X]$ de degré n (irréductible ou non). On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :

1. Dans $\mathbb{L}[X]$, P est produit de polynôme de degré 1 (ou alors P a toutes ses racines dans $\mathbb{L}$).
2. Le corps $\mathbb{L}$ est minimal pour cette propriété (ou alors les racines de P engendrent $\mathbb{L}$).

Théorème 7. Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près que l'on note $D_{\mathbb{K}}(P)$.

1.2 Existence et unicité

Définition 8. Soit $\varphi : \mathbb{Z} \rightarrow \mathbb{K}$; $n \mapsto 1 + \dots + 1$ morphisme d'anneau. Son noyau est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec p premier ou $p = 0$. Ce nombre est appelé caractéristique de $\mathbb{K}$ noté $\text{car}(\mathbb{K})$

Remarque 9. Si $\text{car}(\mathbb{K}) = 0$ alors $\mathbb{K}$ contient $\mathbb{Z}$ (et $\mathbb{Q}$) donc est infini. Si $\mathbb{K}$ est fini alors $\text{car}(\mathbb{K}) > 0$, son sous corps premier est $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ et $|\mathbb{K}| = p^n$.

Proposition 10. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. L'application $F : \mathbb{K} \rightarrow \mathbb{K}$; $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Théorème 11. Si $\mathbb{K}$ est fini c'est un automorphisme et si $\mathbb{K} = \mathbb{F}_p$ c'est l'identité.

Théorème 12. Soit p premier et $n \in \mathbb{N}^*$, on pose $q = p^n$. Il existe un corps $\mathbb{K}$ à q éléments, unique à isomorphisme près noté $\mathbb{F}_q = D_{\mathbb{F}_p}(X^q - X)$.

Théorème 13. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique d'ordre $q - 1$.

2 Propriétés

2.1 Inclusions et automorphismes

Théorème 14. (Wedderburn) Tout corps fini est commutatif.

Proposition 15. Soit $\mathbb{K}$ un corps fini de caractéristique p et de cardinal $q = p^n$ on a :

1. Si $\mathbb{L}$ est une extension finie de $\mathbb{K}$, alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$.
2. Si $\mathbb{M}$ est un sous corps de $\mathbb{K}$ alors $|\mathbb{M}| = p^m$ avec m divise n .
3. Soit $d|n$ alors il existe un unique sous corps $\mathbb{M}$ de $\mathbb{K}$ tel que $|\mathbb{M}| = p^d$. On a $\mathbb{M} = \{x \in \mathbb{K} | x^{p^d} = x\}$ et $\mathbb{M}$ est isomorphe à $\mathbb{F}_{p^d}$.

Proposition 16. Soit $\mathbb{K}$ corps fini de cardinal q , $\overline{\mathbb{K}}$ une clôture algébrique et $m \in \mathbb{N}^*$. Alors il existe une unique extension $\mathbb{L}$ de $\mathbb{K}$ telle que $[\mathbb{L} : \mathbb{K}] = m$, de plus $|\mathbb{L}| = q^m$ et $\mathbb{L} = \{x \in \overline{\mathbb{K}} | x^{q^m} = x\}$.

Proposition 17. Pour tout $m, n \in \mathbb{N}^*$ on a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$.

2.2 Carrés dans $\mathbb{F}_q$

Pour $q = p^n$ on pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 18. Pour $p = 2$ on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Proposition 19. Pour $p > 2$ on a $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Corollaire 20. Pour $p > 2$ on a $-1 \in \mathbb{F}_q^{*2} \iff (-1)^{\frac{q-1}{2}} = 1 \iff \frac{q-1}{2} \text{ pair} \iff q \equiv 1 \pmod{4}$.

Application 21. Il existe une infinité de nombre premier de la forme $4m + 1$.

3 Applications à l'irréductibilité des polynômes

Théorème 22. (Critère d'Eisenstein) Soit A anneau factoriel et $\mathbb{K}$ son corps des fractions. Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $p \in A$ irréductible. Si on a les conditions suivantes :

1. $p \nmid a_n$,
2. $p \mid a_i$ pour $i \in \{0, \dots, n-1\}$,
3. $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{K}[X]$ (donc si $\text{pgcd}(a_i) = 1$ il l'est dans $A[X]$).

Exemple 23. Pour p premier dans $\mathbb{N}$, $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$.

Pour tout $n \in \mathbb{N}^*$ le polynôme $X^n - 2$ est irréductible sur $\mathbb{Z}$.

Remarque 24. Le deuxième exemple nous donne l'existence d'extensions de $\mathbb{Q}$ de n'importe quel degré puis l'existence des nombres transcendants sur $\mathbb{R}$.

Théorème 25. (Réduction) Soient A un anneau factoriel et $\mathbb{K}$ son corps des fractions, I idéal premier de A et $B = A/I$ intègre de corps des fractions L . Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $\bar{P}$ sa réduction modulo I . On suppose que $\bar{a}_n \neq 0$ dans B . Si $\bar{P}$ est irréductible sur B ou $\mathbb{L}$ alors P est irréductible sur $\mathbb{K}$.

Exemple 26. Si $A = \mathbb{Z}$ et $I = (p)$ avec p premier alors $B = \mathbb{F}_p$ est un corps. Par exemple $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ en réduisant modulo 2 dans $\mathbb{F}_2$.

Lemme 27. Le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Théorème 28. Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$, alors P irréductible si et seulement si P n'a pas de racines dans les extensions de $\mathbb{K}$ de degré inférieur ou égal à $n/2$.

Exemple 29. $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Définition 30. Une racine n -ième primitive de l'unité de $\mathbb{K}$ est un élément $\zeta \in \mathbb{K}$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. C'est un générateur de $\mu_n(\mathbb{K})$ de sorte qu'il y ait $\varphi(n)$ racines primitives de l'unité, leur ensemble est noté $\mu_n^*(\mathbb{K})$.

Définition 31. Le n -ième polynôme cyclotomique de $\mathbb{K}$ est $\Phi_n(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$.

Remarque 32. Si $\zeta \in \mu_n^*(\mathbb{K})$ alors les ζ^d avec $\text{pgcd}(d, n) = 1$. Le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 33. On a $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Proposition 34. Dans $\mathbb{Q}$ on a $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 35. Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

4 Dénombrement sur les corps finis

4.1 Sur les espaces de matrices

Lemme 36. Pour tout entier $p \in \{1, \dots, n\}$ il y a $\prod_{k=1}^p (q^n - q^{k-1}) = q^{\frac{p(p-1)}{2}} \prod_{k=n-p+1}^n (q^k - 1)$ familles formées de p vecteurs linéairement indépendants dans un $\mathbb{F}_q$ espace vectoriel de dimension n .

Théorème 37. Pour tout $\mathbb{F}_q$ espace vectoriel E on a :

1. $\text{card}(GL(E)) = \prod_{k=1}^n (q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^n (q^k - 1)$
2. $\text{card}(SL(E)) = q^{n-1} \prod_{k=1}^n (q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=2}^n (q^k - 1)$

On note $D_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de taille n de $\mathbb{F}_q$.

Lemme 38. On a $D_n(\mathbb{F}_q) = \{A \in GL_n(\mathbb{F}_q) | A^q = A\}$.

Lemme 39. Pour tout $A \in D_n(\mathbb{F}_q)$ on a $\mathbb{F}_q^n = \bigoplus_{k=1}^{q-1} \ker(A - \lambda_k I_n)$
où λ_k sont les valeurs propres de A .

Définition 40. On pose $\mathcal{F} = \{(E_1, \dots, E_{q-1}) | \mathbb{F}_q^n = \bigoplus_{k=1}^{q-1} E_k\}$ et
 $\mathcal{F}_{(n_1, \dots, n_{q-1})} = \{(E_1, \dots, E_{q-1}) \in \mathcal{F} | \dim(E_i) = n_i, 1 \leq i \leq q-1\}$
ce qui nous donne une partition de $\mathcal{F}$.

Lemme 41. L'application $\varphi : D_n(\mathbb{F}_q) \rightarrow \mathcal{F} ; A \mapsto (\ker(A - \lambda_1 I_n), \dots, \ker(A - \lambda_{q-1} I_n))$ est bijective.

Lemme 42. Pour $(n_k)_{1 \leq k \leq q-1} \in \mathbb{N}^{q-1}$ fixé tel que
 $\sum_{k=1}^{q-1} n_k = n$ l'application : $GL(\mathbb{F}_q^n) \times \mathcal{F}_{(n_1, \dots, n_{q-1})} \rightarrow$
 $\mathcal{F}_{(n_1, \dots, n_{q-1})} ; (g, (E_1, \dots, E_{q-1})) \mapsto (g(E_1), \dots, g(E_{q-1}))$ définit
une action transitive de $GL(\mathbb{F}_q^n)$ vers $\mathcal{F}_{(n_1, \dots, n_{q-1})}$

Lemme 43. Pour $(n_k)_{1 \leq k \leq q-1} \in \mathbb{N}^{q-1}$ fixé tel que $\sum_{k=1}^{q-1} n_k = n$
et $(E_k)_{1 \leq k \leq q-1} \in \mathcal{F}_{(n_1, \dots, n_{q-1})}$, le stabilisateur de $(E_k)_{1 \leq k \leq q-1}$
est de cardinal $\prod_{k=1}^{q-1} \text{card}(GL(E_k))$ et $\text{card}(\mathcal{F}_{(n_1, \dots, n_{q-1})}) =$
 $\frac{\text{card}(GL_n(\mathbb{F}_q^n))}{\prod_{k=1}^{q-1} \text{card}(GL(E_k))}$

Théorème 44. Avec la convention $\text{card}(GL_0(\mathbb{F}_q)) = 0$ on a :

$$\text{card}(D_n(\mathbb{F}_q)) = \sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1 + \dots + n_{q-1} = n}} \frac{\text{card}(GL_n(\mathbb{F}_q))}{\text{card}(GL_{n_1}(\mathbb{F}_q)) \dots \text{card}(GL_{n_{q-1}}(\mathbb{F}_q))}$$

4.2 Polynômes irréductibles de $\mathbb{F}_p$

Définition 45. On définit la fonction de Möbius comme $\mu(1) = 1$,
 $\mu(n) = (-1)^r$ si $n = \prod_{i=1}^r p_i$ dans sa décomposition en facteurs carrés
et $\mu(n) = 0$ sinon.

Théorème 46. (Möbius) Soient $(u_n)_{n \in \mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*}$ des
suites réelles alors $\forall n \in \mathbb{N}^*, u_n = \sum_{d|n} v_d \iff \forall n \in \mathbb{N}^*, v_n =$

$$\sum_{d|n} \mu(d) u_{\frac{n}{d}}.$$

On pose $P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ et $\mathcal{U}_d(p) = \{P \in \mathbb{F}_p[X] | \deg(P) = d, \text{irréductible et unitaire}\}$ pour tout $n \in \mathbb{N}^*$
et p premier fixé.

Lemme 47. Tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est
de degré divisant n . Réciproquement pour tout diviseur d de n
tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n .

Théorème 48. Le polynôme P_n est sans facteur carré dans
 $\mathbb{F}_p[X]$ et on a $X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P(X)$.

Théorème 49. Pour tout entier $n \in \mathbb{N}^*$ on a $|\mathcal{U}_n(p)| =$
 $\frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$.

Dev 1 : Dénombrement des matrices diagonalisables de $\mathbb{F}_q$ 39 et
41, 42, 43 et 44

Dev 2 : Dénombrement des polynômes irréductibles de $\mathbb{F}_p$ 46, 47, 48
et 49

Dev 3 : Polynômes cyclotomiques irréductibles 34 et 35

Références

- [PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.
[TAU07] Patrice TAUVEL : Corps commutatifs et théorie de
Galois : cours et exercices. Calvage et Mounet, 2007.

- [17] Jean Étienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Supérieur, 2017.

RAPPORT DU JURY :

La construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Le calcul des degrés des extensions, le théorème de la base télescopique, les injections des divers F_q sont incontournables. La structure du groupe multiplicatif doit aussi être connue. Des applications des corps finis (y compris pour F_q avec q non premier!) ne doivent pas être oubliées. Par exemple, l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont des pistes intéressantes.

Les candidates et candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductibilité des polynômes à coefficients dans un corps fini.