Cadre : Sauf indication contraire, $\Bbbk$, $\mathbb{K}$ et $\mathbb{L}$ sont des corps. Tous les corps seront commutatifs, sauf dans le Théorème 35.

I Généralités sur les corps finis

1) Caractéristiques, sous-corps premier

Définition 1. Soit $\mathbb{K}$ un corps, on appelle sous-corps premier de $\mathbb{K}$ l'intersection de tous ses sous-corps non nuls.

Exemple 2. *Le sous-corps premier de $\mathbb{R}$ et $\mathbb{C}$ est $\mathbb{Q}$.*

Définition 3. Soit A un anneau unitaire, il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 4. *La caractéristique est soit nulle soit un nombre premier.*

Corollaire 5. *Si $\operatorname{car}(K) = 0$, $\mathbb{K}$ est infini, mais la réciproque est fausse.*

Théorème 6. *Soient $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$ des extensions de corps. Alors $\mathbb{L}$ (resp. $\mathbb{K}$) est un espace vectoriel sur $\mathbb{K}$ (resp. $\Bbbk$). Si $(b_i)_{i\in I}$ est une $\Bbbk$-base de $\mathbb{K}$ et $(a_j)_{j\in J}$ est une $\mathbb{K}$-base de $\mathbb{L}$, alors $(a_j b_i)_{(i,j)\in I\times J}$ est une $\Bbbk$-base de $\mathbb{L}$.*

Corollaire 7. *Soit $\Bbbk \subseteq \mathbb{K}$ une extension finie. Alors $\mathbb{L} \cong \mathbb{K}^{[\mathbb{K}:\Bbbk]}$.*

Théorème 8. *Si $\mathbb{K}$ est un corps fini de caractéristique p, alors le sous-corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z}$. Ainsi $|\mathbb{K}|$ est une puissance de p.*

Exemple 9. *Il n'existe pas de corps de cardinal 57.*

Proposition 10. *Si $\operatorname{car}(\mathbb{K}) = p$, alors l'application $F : \mathbb{K} \to \mathbb{K}$ définie par $F(x) = x^p$ est un morphisme de corps, dit morphisme de Frobenius. Si $\mathbb{K}$ est fini, c'est un automorphisme, qui est l'identité si $\mathbb{K} = \mathbb{F}_q$.*

Corollaire 11 (Fermat)**.** *Soient $p \in \mathbb{Z}$ premier et $a \in \mathbb{Z}$, alors $a^p \equiv a\ [p]$.*

2) Existence et unicité des corps finis

Définition 12. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindé sur $\mathbb{L}[X]$, et si $\mathbb{L}$ est minimal pour cette propriété.

Théorème 13. *Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^\star$. Il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près.*

Théorème 14. *Soit p un nombre premier et soit $n \in \mathbb{N}^\star$. On pose $q = p^n$.*

(i) Il existe un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

(ii) De plus, $\mathbb{K}$ est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Proposition 15. *Soient $m, n \in \mathbb{N}^\star$, alors $(\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}) \Leftrightarrow n \mid m$.*

Exemple 16. *Les sous-corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$ et $\mathbb{F}_{16}$.*

3) Structure de $\mathbb{F}_q^\times$

Théorème 17. *Tout sous-groupe fini de $\mathbb{K}^\star$ est cyclique. En particulier, le groupe $\mathbb{F}_p^\times$ est cyclique.*

Remarque 18. *On ne sait pas en général trouver un générateur de $\mathbb{F}_q^\times$.*

Exemple 19. *$\mathbb{F}_8^\times \cong \mathbb{Z}/7\mathbb{Z}$, tout élément non neutre de $\mathbb{F}_8^\times$ est générateur.*

Théorème 20. *On considère l'extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. Il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} \cong \mathbb{F}_q(\alpha)$.*

II Polynômes sur un corps fini

1) Polynômes irréductibles

Théorème 21. *Soient $\mathbb{F}_p \subset \mathbb{K}$ une extension finie de degré $n \geqslant 1$ et $\xi \in \mathbb{K}$. Les assertions suivantes sont équivalentes :*

(i) $\mathbb{K} = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$

(ii) $(1, \xi, \xi^2, \dots, \xi^{n-1})$ est une base du $\mathbb{F}_p$-espace vectoriel $\mathbb{K}$.

(iii) $(1, \xi, \xi^2, \dots, \xi^{n-1})$ est une famille libre sur $\mathbb{F}_p$.

(iv) Le polynôme minimal de ξ sur $\mathbb{K}$ est de degré n.

Proposition 22. *Soient p premier, $n \in \mathbb{N}^\star$ et $q = p^n$. Soit $P \in \mathbb{F}_p[X]$ unitaire et irréductible de degré n. Alors $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_q$.*

Corollaire 23. *Soient p premier, $n \in \mathbb{N}^\star$ et $P \in \mathbb{F}_p[X]$ de degré n.*

(i) Il existe des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p[X]$.

(ii) Si P est unitaire et irréductible, $\mathbb{F}_{p^n}$ est un corps de rupture de P.

(iii) Si P est unitaire et irréductible, P divise $X^{p^n} - X$.

Lemme 24. *Soient $d, n \in \mathbb{N}^\star$ et $q = p^n$. Soit $P \in \mathbb{F}_p[X]$ unitaire et irréductible de degré d. Si P divise $X^q - X$, alors d divise n.*

Théorème 25. *Soient p premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 26 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 27. *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

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

2) Cyclotomie

Définition 28. On pose $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \,|\, \zeta^n = 1\}$ le groupe des racines n-ièmes de l'unité.

Proposition 29. *Tout sous-groupe de $\mathbb{K}^\star$ est cyclique.*

Définition 30. On pose $\mathbb{K}_n$ un corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$. Le groupe $\mu_n(\mathbb{K})$ est cyclique d'ordre n. On note $\mu_n^\star(\mathbb{K})$ l'ensemble des générateurs de $\mu_n(\mathbb{K})$, ses éléments sont les racines primitives n-ièmes de l'unité.

Remarque 31. $|\mu_n^\star(\mathbb{K}_n)| = \varphi(n)$

Définition 32. On définit le n-ième polynôme cyclotomique par :

$$\Phi_{n,\mathbb{K}} = \prod_{\zeta \in \mu_n^\star(\mathbb{K}_n)} (X - \zeta) \in \mathbb{K}[X]$$

Proposition 33. $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}}$

Proposition 34. *On a $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. De plus, pour $\sigma : \mathbb{Z} \to \mathbb{K}$ le morphisme canonique, on a $\Phi_{n,\mathbb{K}}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X))$. En particulier, $\Phi_{n,\mathbb{F}_p}$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction modulo p.*

Théorème 35 (Wedderburn)**.** *Tout corps fini est commutatif.*

III Applications

1) Irréductibilité des polynômes de $\mathbb{Z}[X]$

Proposition 36. *Soient $P, Q \in \mathbb{F}_p[X]$. Alors :*

$$(P+Q)^p = P^p + Q^p \quad \text{et} \quad (P(X))^p = P(X^p)$$

Définition 37. On définit le contenu de $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ par $c(P) = \mathrm{pgcd}(a_0, \dots, a_n)$. Un polynôme P est dit primitif si $c(P) = 1$.

Proposition 38. *Soient $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.*

Proposition 39. *Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :*

(i) Les polynômes constants, irréductibles dans $\mathbb{Z}$ (premiers).

(ii) Les polynômes non constants, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 40 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$. Soit un nombre premier p tel que $p \nmid a_n$, $\forall i < n, p | a_i$ et $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Z}[X]$.*

Application 41. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 42. On pose $(\mathbb{F}_q)^2 = \left\{x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q\right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 43. *Si $q = p^n$, on a :*

(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

(ii) Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$

Proposition 44. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 45. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 46. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 47. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \quad \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si \quad \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si \quad \overline{a} = 0 \end{cases}$$

Proposition 48. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 49. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$*

Théorème 50 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 51. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 52. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 53. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

Développements

— Polynômes unitaires irréductibles sur $\mathbb{F}_q$ (25,26,27) [Tau08]

— Étude des polynômes cyclotomiques (41) [Per96]

— Loi de réciprocité quadratique (50) [Ser13]

Références

[Per96] Daniel Perrin. *Cours d'Algèbre.* Ellipses, 1996
[Tau08] Patrice Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet, 2008
[Ser13] Jean-Pierre Serre. *Cours d'Arithmétique.* PUF, 2013