Cadre : Sauf indication contraire, $\Bbbk$, $\mathbb{K}$ et $\mathbb{L}$ sont des corps.

I Extensions de corps

1) Définitions et premières propriétés

Définition 1. Soit $\mathbb{K}$ un corps. On appelle extension de $\mathbb{K}$ un corps $\mathbb{L}$ tel qu'il existe un morphisme de corps $\mathbb{K} \to \mathbb{L}$.

Exemple 2. *On a la tour d'extensions* $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Remarque 3. *Tout morphisme de corps est injectif. Quitte à identifier* $\mathbb{K}$ *et son image dans* $\mathbb{L}$*, on peut supposer que* $\mathbb{K}$ *est un sous-corps de* $\mathbb{L}$.

Définition 4. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. Alors $\mathbb{L}$ est muni d'une structure de $\mathbb{K}$-espace vectoriel. Sa dimension est appelée degré de $\mathbb{L}$ sur $\mathbb{K}$, notée $[\mathbb{L} : \mathbb{K}]$.

Exemple 5. $[\mathbb{C} : \mathbb{R}] = 2$ *et* $[\mathbb{R} : \mathbb{Q}] = \infty$.

Définition 6. Soit $\mathbb{K}$ un corps. 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 7. *Soit* $\mathbb{K}$ *un corps, et soit* $p = \operatorname{car}(\mathbb{K})$.

(i) Si $p = 0$*, alors* $\mathbb{K}$ *est une extension de* $\mathbb{Q}$.

(ii) Si $p \neq 0$*, alors* p *est premier et* $\mathbb{K}$ *est une extension de* $\mathbb{Z}/p\mathbb{Z}$.

Exemple 8. *Si* $\operatorname{car}(\mathbb{K}) = 0$*,* $\mathbb{Q}$ *est le plus petit sous-corps de* $\mathbb{K}$*. Si* $\operatorname{car}(\mathbb{K}) \neq 0$*, c'est* $\mathbb{Z}/p\mathbb{Z}$.

Théorème 9 (Base téléscopique)**.** *Soit* $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$ *une tour d'extension. Soient* $(\alpha_j)_{j\in J}$ *une* $\mathbb{K}$*-base de* $\mathbb{L}$ *et* $(\beta_i)_{i\in I}$ *une* $\Bbbk$*-base de* $\mathbb{K}$*. Alors* $(\alpha_j\beta_i)_{(i,j)\in I\times J}$ *forme une* $\Bbbk$*-base de* $\mathbb{L}$.

Corollaire 10 (Extensions emboîtées)**.** *Soit* $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$ *une tour d'extension, où* $\Bbbk$*,* $\mathbb{K}$ *et* $\mathbb{L}$ *sont finis. Alors* $[\mathbb{L} : \mathbb{K}]\,[\mathbb{K} : \Bbbk] = [\mathbb{L} : \Bbbk]$.

Remarque 11. *On a* $[\mathbb{K} : \Bbbk] = 1$ *si, et seulement si,* $\mathbb{K} = \Bbbk$.

2) Extensions algébriques

Définition 12. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit S une partie de $\mathbb{L}$. Le plus petit sous-corps de $\mathbb{L}$ contenant S est noté $\mathbb{K}(S)$ et est appelé sous-corps de $\mathbb{L}$ engendré par S dans $\mathbb{K}$. Si $S = \{\alpha_1, \dots, \alpha_n\}$, on notera $\mathbb{K}(\alpha_1, \dots, \alpha_n)$.

Définition 13. Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$. On considère l'application $\varphi : \mathbb{K}[X] \to \mathbb{L}$ définie par $\varphi|_{\mathbb{K}} = Id_{\mathbb{K}}$ et $\varphi(X) = \alpha$.

(i) S'il existe $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$, on dit que α est algébrique.

(ii) Sinon, φ est injective, et on dit que α est transcendant sur $\mathbb{K}$.

Exemple 14. $\sqrt{2}$ *et* $e^{\frac{2i\pi}{n}}$ *sont algébriques sur* $\mathbb{Q}$*,* e *et* π *y sont algébriques.*

Définition 15. Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. L'ensemble des polynômes de $\mathbb{K}[X]$ qui annulent α est un idéal non nul de $\mathbb{K}[X]$. On appelle polynôme minimal de α sur $\mathbb{K}$, noté π_α, l'unique polynôme unitaire non nul qui engendre cet idéal.

Théorème 16. *Soient* $\mathbb{L}$ *une extension d'un corps* $\mathbb{K}$ *et* $\alpha \in \mathbb{L}$*. Alors :*

(i) Si α *est algébrique sur* $\mathbb{K}$*, alors* $\mathbb{K}(\alpha) \cong \mathbb{K}[X]/(\pi_\alpha)$.

(ii) Si α *est transcendant sur* $\mathbb{K}$*, alors* $\mathbb{K}(\alpha) \cong \mathbb{K}[X]$.

Corollaire 17. *Soient* $\mathbb{L}$ *une extension d'un corps* $\mathbb{K}$ *et* $\alpha \in \mathbb{L}$*. Alors* α *est algébrique sur* $\mathbb{K}$ *si, et seulement si,* $[\mathbb{K}(\alpha) : \mathbb{K}]$ *est fini. Dans ce cas, on a* $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg \pi_\alpha$.

Définition 18. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. On dit qu'elle est finie si son degré est fini. On dit qu'elle est algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Proposition 19. *Toute extension finie est algébrique.*

Théorème 20. *Soit* $\Bbbk \subseteq \mathbb{K} \subseteq \mathbb{L}$ *des extensions. Alors* $\Bbbk \subseteq \mathbb{L}$ *est algébrique si, et seulement si,* $\mathbb{K} \subseteq \mathbb{L}$ *et* $\Bbbk \subseteq \mathbb{K}$ *sont algébriques.*

Définition 21. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. On appelle fermeture algébrique, notée $\overline{\mathbb{K}}$, le sous-corps de $\mathbb{L}$ des éléments algébriques sur $\mathbb{K}$. C'est une extension algébrique sur $\mathbb{K}$.

II Corps de rupture, de décomposition

1) Corps de rupture

Définition 22. Soit $P \in \mathbb{K}[X]$ irréductible. Une extension monogène $\mathbb{L}$ de $\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si elle est engendré par $\mathbb{K}$ et par une racine α de P.

Remarque 23. *$\mathbb{L}$ est alors une extension de $\mathbb{K}$ de degré le degré de P.*

Exemple 24. *Si P est de degré 1, $\mathbb{K}$ est un corps de rupture de P.*

Théorème 25. *Tout polynôme irréductible sur $\mathbb{K}$ admet un corps de rupture, qui est unique à $\mathbb{K}$-isomorphisme près.*

Exemple 26. *$\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$.*

Exemple 27. *Le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$ a 4 éléments.*

Corollaire 28. *Pour tout polynôme sur $\mathbb{K}$, il existe une extension de $\mathbb{K}$ dans laquelle il admet au moins une racine.*

2) Corps de décomposition

Définition 29. 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 $\mathbb{L} = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$ avec $\alpha_k \in \mathbb{L}$ des racines de P.

Remarque 30. *Un corps de décomposition est une extension finie.*

Exemple 31. *$\mathbb{Q}[\sqrt{2}]$ est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.*

Théorème 32. *Soit $P \in \mathbb{K}[X]$ non constant. Alors P admet un corps de décomposition, unique à isomorphisme près, de degré au plus* $(\deg P)!$.

Exemple 33. *$\mathbb{Q}[\sqrt[3]{2}]$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais ce n'est pas un corps de décomposition.*

Théorème 34. *Soit $\mathbb{K}$ un corps de caractéristique nulle, et soit $P \in \mathbb{K}[X]$ irréductible. Si $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$, alors P est à racines simples dans $\mathbb{L}$.*

Théorème 35 (Élément primitif en caractéristique nulle)**.** *Toute extension finie d'un corps de caractéristique nulle est monogène.*

Application 36. *Soient p, q premiers. Alors $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p}+\sqrt{q})$.*

Exemple 37. *$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est une extension de degré 4 de $\mathbb{Q}$ engendrée par $\sqrt{2}+\sqrt{3}$.*

III Corps finis

Proposition 38. *Soit $\mathbb{K}$ un corps fini de caractéristique p non nulle. Alors il existe $n \in \mathbb{N}^\star$ tel que $|\mathbb{K}| = p^n$.*

Définition 39. Soient p premier, $n \in \mathbb{N}^\star$ et $q = p^n$. Le corps de décomposition de $X^q - X$ est de cardinal q. On note $\mathbb{F}_q$ ce corps.

Proposition 40. *Soient p premier et $d, n \in \mathbb{N}^\star$. Alors $\mathbb{F}_{p^n}$ est une extension de $\mathbb{F}_{p^d}$ si, et seulement si, d divise n.*

Théorème 41. *Le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique.*

Corollaire 42. *Soit $\mathbb{F}_{q^n}$ une extension de $\mathbb{F}_q$, alors il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. En particulier, pour $n \in \mathbb{N}^\star$, il existe un polynôme irréductible dans $\mathbb{F}_q[X]$ de degré d.*

IV Applications

1) Polynômes cyclotomiques

Définition 43. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 44. *Pour $n \in \mathbb{N}^\star$, Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 45. *Pour $n \in \mathbb{N}^\star$, $X^n - 1 = \prod_{d|n} \Phi_d(n)$*

Exemple 46. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Lemme 47. *Soient $A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P = AB \in \mathbb{Z}[X]$. Si A et P sont unitaires, alors A et B sont à coefficients entiers.*

Proposition 48. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 49. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

2) Polynômes irréductibles

Théorème 50. *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 51. *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 52. *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 53. *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 54. *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 :*

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

Proposition 55 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d \mid n} g(d)$. Alors :*

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

Corollaire 56. *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

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

3) Nombres constructibles

Définition 57. Soient $A \subset \mathbb{R}^2$ et $M \in \mathbb{R}^2$. On dit que M est constructible en un pas à partir de A s'il existe deux éléments distincts, droites ou cercles, tels que M est un point d'intersection de ces éléments.

Définition 58. Soit $M \in \mathbb{R}^2$. On dit que M est constructible s'il existe $A_0 \subset A_1 \subset \ldots \subset A_n$ des parties de $\mathbb{R}^2$, avec $A_0 = \{(0,0),(1,0)\}$, $M \in A_n$ et $A_i = A_{i-1} \cup \{M_i\}$ où M_i est constructible en un pas à partir de A_{i-1}.

Définition 59. Un réel x est dit constructible si $(x, 0)$ est constructible.

Proposition 60. *Tout rationnel est constructible.*

Proposition 61. *Si $x > 0$ est constructible, alors $\sqrt{x}$ est constructible.*

Théorème 62. *Soit $x \in \mathbb{R}$ constructible. Alors x est algébrique sur $\mathbb{Q}$, et $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2.*

Application 63. *La duplication du cube, la trisection de l'angle et la quadrature du cercle sont impossibles à la règle et au compas. Autrement dit, $\sqrt[3]{2}$, $\sqrt{\pi}$ et $\cos\left(\frac{\pi}{9}\right)$ ne sont pas constructibles.*

Développements

— Étude des polynômes cyclotomiques (48,49) [Per96]

— Polynômes unitaires irréductibles sur $\mathbb{F}_q$ (54,55,56) [Tau08]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet