125 Extensions de corps. Exemples et applications.

Introduction : Les extensions de corps sont des constructions algébriques ayant de nombreuses applications, parfois surprenantes, telles que l'étude de la résolubilité par radicaux d'équations polynomiales ou les constructions à la règle et au compas. On présentera les propriétés fondamentales et les méthodes de construction de ces structures, avec une application aux constructions géométriques.

1 Généralités

1.1 Définition et premières propriétés

Définition 1. Soit K un corps. On appelle extension du corps K la donnée de (L, i) où L est un corps et $i : K \to L$ est un homomorphisme de corps. On note L/K cette extension.

Remarque 2. i est alors nécessairement injectif, et K est isomorphe à $i(K)$.

Proposition 3. L est alors muni d'une structure de K-algèbre via le produit externe $\lambda \cdot v = i(\lambda)v$.

Définition 4. On définit alors le degré de l'extension L/K par $[L : K] = \dim_K(L)$. Si ce degré est fini, on dit que l'extension L/K est finie.

***Exemple* 5.**
- $\mathbb{C}$ *est une extension de* $\mathbb{R}$*, et* $[\mathbb{C} : \mathbb{R}] = 2$.
- $\mathbb{R}$ *est une extension de* $\mathbb{Q}$ *et* $[\mathbb{R} : \mathbb{Q}] = \infty$.
- $K(X)$ *est une extension de* K *et* $[K(X) : K] = \infty$.

Proposition 6. Soit L/K une extension, soit E un L-espace vectoriel. Soient $(e_i)_{i\in I}$ base de L sur K, et $(f_j)_{j\in J}$ base de E sur L. Alors E a une structure de K-espace vectoriel, de base $(e_i f_j)_{(i,j)\in I\times J}$.

Corollaire 7. Si $L/K, M/L$ sont deux extensions de corps, alors M/K est une extension de corps, et son degré s'obtient par $[M : K] = [M : L][L : K]$.

Proposition 8. Soit L/K une extension, soit A partie de L. Il existe un plus petit sous-corps de L contenant K et A. On le note $K(A)$.

Définition 9. On dit que L est monogène s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

***Exemple* 10.** $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *est monogène, engendrée par* $\sqrt{2} + \sqrt{3}$.

Définition 11. Si $L/K, L'/K$ sont deux extensions, on appelle K-morphisme tout morphisme de corps $\varphi : L \to L'$ qui induit l'identité sur K.

1.2 Algébricité et transcendance

Définition 12. Soit L/K une extension, soit $a \in L$. On dit qu'il est algébrique sur K s'il existe $P \in K[X]$ tel que $P(a) = 0$. Il est dit transcendant s'il n'est pas algébrique. On dit que l'extension L/K est algébrique si tous les éléments de L sont algébriques sur K.

***Exemple* 13.** i *est algébrique sur* $\mathbb{R}$, $\sqrt{2}$ *est algébrique sur* $\mathbb{Q}$, π *est transcendant sur* $\mathbb{Q}$.

Proposition 14. a algébrique sur K ssi $K(a) = K[a]$ ssi $[K(\alpha) : K] < \infty$.

Proposition 15. Si $[L : K] < \infty$ alors l'extension L/K est algébrique.

Corollaire 16. Si a, b sont algébriques sur K, alors $a + b$ et ab algébriques sur K.

Définition 17. Soit $a \in L$ algébrique sur K. L'ensemble $\{P \in K[X], P(a) = 0\}$ est un idéal de $K[X]$, il est donc engendré par un unique polynôme unitaire : celui-ci est appelé polynôme minimal de a sur K, et noté π_a.

***Exemple* 18.** *Le polynôme minimal de* $\sqrt{2}$ *est* $X^2 - 2$ *sur* $\mathbb{Q}$ *et* $X - \sqrt{2}$ *sur* $\mathbb{R}$.

Proposition 19. Si $a \in L$ algébrique sur K, on a $\deg(\pi_a) = [K(a) : K]$.

2 Adjonction de racines

2.1 Corps de rupture et de décomposition

Définition 20. Soit K corps, soit $P \in K[X]$ irréductible. On appelle corps de rupture de P un corps L dans lequel P admet une racine et tel qu'il existe $a \in L, P = K(a)$.

***Exemple* 21.** $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ *sont des corps de rupture de* $X^3 - 2$.

Proposition 22. Soit $P \in K[X]$ irréductible. Alors $L = K[X]/P$ est un corps de rupture de P, de degré $\deg(P)$, et $L = K(\overline{X})$. De plus, P est le polynôme minimal de $\overline{X}$ sur K.

***Exemple* 23.** $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ *est un corps de rupture de* $X^2 + 1$.

Théorème 24. Si $L = K(a), L' = K(b)$ sont deux corps de rupture de P, il existe un K-isomorphisme $\sigma : L \to L'$ tel que $\sigma(a) = b$.

Définition 25. Soit K corps, $P \in K[X]$ irréductible de degré n.
L est dit corps de décomposition de P s'il existe $a_1, \cdots, a_n \in L, \lambda \in K$ tels que $L = K(a_1, \cdots, a_n)$ et $P = \lambda \prod_{i=1}^{n} (X - a_i)$.

Théorème 26. P possède un corps de décomposition L, unique à K-isomorphisme près, et $[L : K] \leq n!$.

***Application* 27** (Théorème de l'élément primitif)**.** *Soit K un corps de caractéristique nulle, soit L extension de K de degré fini. Alors il existe $x \in L$ tel que $L = K(x)$. De plus, L extension de K, on a $[L : K] \leq n \Leftrightarrow \forall x \in L, [K(x) : K] \leq n$.*

2.2 Clôture algébrique

Lemme 28. Soit K un corps. On a équivalence entre :

(i). Tout $P \in K[X]$ a une racine dans K.

(ii). Tout $P \in K[X]$ est scindé sur K.

(iii). La seule extension algébrique de K est K.

Définition 29. On dit alors que K est algébriquement clos.

***Exemple* 30.** *$\mathbb{C}$ est algébriquement clos.*

Définition 31. Si L extension de K, on dit que c'est une clôture algébrique de K si L algébriquement clos et algébrique sur K.

***Exemple* 32.** *$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$.*

3 Exemples fondamentaux

3.1 Corps finis

Théorème 33. Soit F corps fini. Alors sa caractéristique est un nombre premier p, et il existe $n \in \mathbb{N}^*, |F| = p^n$. Réciproquement, pour tout p premier, il existe un unique corps (à isomorphisme près) de cardinal p^n. On le note $\mathbb{F}_{p^n}$.

Proposition 34. Si F corps fini, F^* est cyclique.

***Application* 35.** *Si $n \in \mathbb{N}^*$, l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est monogène.*

Proposition 36. Si $q = p^n$, $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

3.2 Corps cyclotomiques

Définition 37. Soit $m \in \mathbb{N}^*$, soit $\omega_m = e^{2i\pi/m}$. $\mathbb{Q}(\omega_m)$ est appelé corps cyclotomique d'indice m. On appelle polynôme cyclotomique d'indice m le polynôme $\Phi_m = \prod_{\substack{k \leq m \\ k \wedge m = 1}} (X - \omega_m^k)$.

Proposition 38. On a $X^m - 1 = \prod_{d|m} \Phi_d$, et $\Phi_m \in \mathbb{Z}[X]$.

Théorème 39. $\deg(\Phi_m) = \varphi(m)$ et Φ_m est irréductible dans $\mathbb{Q}[X]$.

Corollaire 40. Φ_m est le polynôme minimal de ω_m, et $[\mathbb{Q}(\omega_m) : \mathbb{Q}] = \varphi(m)$.

4 Constructions à la règle et au compas

4.1 Le théorème de Wantzel

On note $\mathcal{P}$ le plan affine euclidien orienté.

Définition 41. Soit X partie de $\mathcal{P}$ avec $|X| \geq 2$, soit $M \in \mathcal{P}$. On dit que M est constructible en un pas à partir de X si M est point d'intersection de deux droites, une droite et un cercle, ou deux cercles déterminés à partir des points de X. On dit que M est constructible s'il existe une suite d'ensembles $\mathcal{B}_0, \cdots, \mathcal{B}_n$ tels que $\mathcal{B}_0 = \{O, I\}$ et pour tout $n, \mathcal{B}_{n+1} = \mathcal{B}_n \cup \{A_n\}$ où A_n constructible en un pas à partir de $\mathcal{B}_{n-1}$, et tels que $M \in \mathcal{B}_n$.

***Exemple* 42.** *$J = (0, 1)$ est constructible.*

Définition 43. On dit que $x \in \mathbb{R}$ est constructible si $(x, 0)$ est constructible. On dit qu'un angle θ est constructible si $\cos(\theta)$ est constructible.

***Exemple* 44.** *Tous les rationnels sont constructibles.*

Proposition 45. L'ensemble des réels constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

Théorème 46 (Wantzel)**.** Soit $x \in \mathbb{R}$. x est constructible si et seulement si il existe une suite finie $L_0, \cdots, L_q$ de sous-corps de $\mathbb{R}$ tels que $L_0 = \mathbb{Q}, x \in L_q$ et $\forall k \leq q - 1, [L_{k+1} : L_k] = 2$.

Théorème 47 (Gauss-Wantzel)**.** Soit $n \in \mathbb{N}^*$. L'angle $\frac{2\pi}{n}$ est constructible si et seulement si n est de la forme $2^\alpha p_1 \cdots p_r$ où les p_i sont des nombres premiers de la forme $1 + 2^{(2^\beta)}$.

***Exemple* 48.** *Les polygones réguliers à 5, 8 et 17 côtés sont constructibles.*

4.2 Applications aux problèmes grecs classiques

Lemme 49. Tout réel constructible est algébrique sur $\mathbb{Q}$.

***Application* 50.** *$\sqrt{\pi}$ n'est pas constructible, et la quadrature du cercle est impossible.*

Proposition 51. $\sqrt[3]{2}$ n'est pas constructible, et la duplication du cube est impossible.

Développements

— Théorème de l'élément primitif.
— Théorème de Gauss-Wantzel.

Références

[1] J.-P. Escofier, Théorie de Galois, Dunod.
[2] I. Gozard, Théorie de Galois, Ellipses.