Leçon 125 : Extensions de corps. Exemples et applications

Tout corps sera, sauf mention contraire, supposé commutatif.
[Ulm18]

I Généralités

Soit k un corps.

I.1 Premières définitions

Déf 1. Un sous-corps de k est un sous-anneau F de k, qui est un corps.

Déf 2. Une extension de corps de k, notée $k \hookrightarrow K$ ou K/k, est une paire (K, φ) où K est un corps, et $\varphi : k \to K$ un morphisme de corps.

Rq 3. Tout morphisme de corps $\varphi : k \to K$ est injectif. On peut alors identifier k à $\varphi(k)$, et utiliser par abus la notation $k \subseteq K$ pour une extension de corps.

Ex 4. Tout corps de caractéristique 0 possède un corps premier isomorphe à $\mathbb{Q}$, et tout corps de caractéristique non nulle possède un corps premier isomorphe à $\mathbb{Z}/p\mathbb{Z}$, avec p premier. Un corps est donc soit une extension de corps de $\mathbb{Q}$, soit une extension de corps de $\mathbb{Z}/p\mathbb{Z}$.

Thm 5. Soit K/k une extension de corps. Le corps K est un k-espace vectoriel.

Déf 6. Soit K/k une extension de corps. On appelle degré d'extension de K/k, notée $[K : k]$, la dimension de K en tant que K-espace vectoriel. Une extension de corps est dite finie, si son degré d'extension est fini.

Ex 7. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{C} : \mathbb{Q}] = \infty$.

Déf 8. Soit K/k une extension de corps, et $\alpha_1, \dots, \alpha_r \in K$. Le corps $k(\alpha_1, \dots, \alpha_r)$ est le plus petit sous-corps de K contenant tous les α_i et k. Une extension de la forme $k(\alpha)$ est appelée extension monogène.

Prop 9. Soit $f \in k[X]$ irréductible. Alors $K := k[X]/(f)$ est une extension de corps de k, $[K : k] = \deg f$ et la classe $\overline{X}$ de X est une racine de f. Pour $\alpha = \overline{X}$, nous avons $K = k[X]/(f) = k(\alpha)$.

I.2 Nombres algébriques. Extensions algébriques.

Notation 10. Soit K/k une extension de corps et $\alpha \in K$, On note $ev_\alpha : k[X] \to K$, $P \mapsto P(\alpha)$ le morphisme d'évaluation en α.

Prop 11. Soit K/k une extension de corps, et $\alpha \in K$.

1. Si $\operatorname{Ker} ev_\alpha = (0)$, alors l'image $k[\alpha] = \operatorname{Im}(ev_\alpha) \simeq k[X]$ est un k-espace vectoriel de dimension infinie, de base $(1, \alpha, \alpha^2, \dots)$ et $k(\alpha) \simeq Frac(k[X])$.
2. Si $\operatorname{Ker} ev_\alpha \neq (0)$, alors $\operatorname{Ker} ev_\alpha$ est de la forme (f) avec f irréductible dans $k[X]$. Le générateur unitaire de $\operatorname{Ker} ev_\alpha$ est le polynôme minimal de α sur k, noté $m_{\alpha,k}$. Le polynôme $m_{\alpha,k}$ divise tout polynôme de $k[X]$ qui s'annule en α. Le corps $k(\alpha)$ est un k-espace vectoriel de dimension $m := \deg m_{\alpha,k}$, de base $(1, \alpha, \dots, \alpha^{m-1})$, et $k(\alpha) = k[\alpha] \simeq k[X]/(m_{\alpha,k})$.

Déf 12. Soit K/k une extension de corps, et $a \in K$. Si le noyau $\operatorname{Ker} ev_a$ n'est pas l'idéal nul, alors a est dit algébrique sur k. Sinon, a est dit transcendant sur k. Si tous les éléments a de K sont algébriques sur k, alors l'extension de corps K/k est dite algébrique.

Ex 13. $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. π est transcendant sur $\mathbb{Q}$.

Cor 14. Soit K/k une extension de corps et $\alpha \in K$. Si α est transcendant sur k, alors $k(\alpha) \simeq Frac(k[X])$. Si α est algébrique sur k, alors $k(\alpha) = k[\alpha] \simeq k[X]/(m_{\alpha,k})$.

Ex 15. Soit $f = X^5 + 2X + 2 \in \mathbb{Q}[X]$ et soit α son unique racine réelle. f est irréductible sur $\mathbb{Q}$, donc $m_{\alpha,\mathbb{Q}} = f$, et donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$.

Prop 16. Soit K/k une extension de corps. Un élément $\alpha \in K$ est algébrique sur k, si et seulement si, α appartient à un sous-corps $L \subseteq K$ de degré fini sur k.

Thm 17 (Base téléscopique)**.** Soit $K/L/k$ des extension de corps. Alors $[K : k] < \infty$, si et seulement si, $[L : k] < \infty$ et $[K : L] < \infty$. Dans ce cas : $[K : k] = [K : L][L : k]$.

De plus, si $(v_1, \dots, v_n)$ est une L-base de K, et $(w_1, \dots, w_m)$ une k-base de L, alors $\mathcal{B} = (v_i w_j)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ est une k-base de K.

Ex 18. Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ une extension de $\mathbb{Q}$. $[K : \mathbb{Q}(\sqrt{3})] = 2$ et $[\mathbb{Q}(\sqrt{3} : \mathbb{Q}] = 2$, donc $[K : \mathbb{Q}] = 4$.

Thm 19. Soit K/k une extension de corps. L'ensemble des éléments de K algébriques sur k, est un sous-corps de K.

II Corps de rupture

Soit k un corps

II.1 Corps de rupture, corps de décomposition

Déf 20. Soient K/k et L/k deux extension de corps. Un isomorphisme $\varphi : K \to L$ qui fixe tous les éléments de k est appelé k-isomorphisme.

Déf 21. Soit $f \in k[X]$ de degré $n \geq 1$. Un corps de rupture de f sur k est une extension de corps K/k telle que f possède une racine α dans K, et que K est l'extension monogène $k(\alpha)$.

Prop 22. Soit $f \in k[X]$ irréductible.

1. Il existe un corps de rupture K/k de f sur k, unique à k-isomorphisme près. C'est le corps $K = k[X]/(f)$. Pour tout corps de rupture $k(\alpha)$, nous avons $k(\alpha) \simeq k[X]/(f)$. En particulier, $[k(\alpha) : k] = \deg f$.

Prop 23. Si $k(\alpha_1)$ et $k(\alpha_2)$ sont deux corps de rupture de f sur k, alors il existe un unique k-isomorphisme $\varphi : k(\alpha_1) \to k(\alpha_2)$ avec $\varphi(\alpha_1) = \alpha_2$.

Ex 24. Soit $j = e^{\frac{2i\pi}{3}} \in \mathbb{C}$ et soit $\alpha = \sqrt[3]{2}$. $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ et $\mathbb{Q}(j\alpha) \not\subseteq \mathbb{R}$, sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$. Bien qu'isomorphes à $\mathbb{Q}[X]/(X^3 - 2)$, ils sont distincts.

Déf 25. Soit $f \in k[X]$ de degré $n \geq 1$. Un corps de décomposition de f sur k est une extension de corps K/k telle que :

1. f est scindé sur K, c'est à dire que K contient toutes les racines de f.
2. K est exactement le sous corps $k(\alpha_1, \ldots, \alpha_m)$ de K, engendré par k et les racines $\alpha_1, \ldots, \alpha_m$ de f dans K.

Thm 26. Pour tout $f \in k[X]$ non constant, il existe, à k-isomorphisme près, un unique corps de décomposition de f sur k, de degré d'extension inférieur à $\deg(f)!$.

Déf 27. Soit K/k une extension de corps. On note $\mathrm{Aut}(K/k)$ le groupe des k-automorphismes de K. Si G est un groupe d'automorphisme d'un corps K, le corps fixe de G, noté K^G, est l'ensemble des éléments de K laissés fixe par G.

Prop 28. Si $f \in k[X]$ possède n racines dans un corps de décomposition K de f sur k, alors $\mathrm{Aut}(K/k)$ permute les n racines de f, et est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Thm 29 (Artin)**.** Soit K/k une extension de corps finie, et G un sous-groupe fini de $\mathrm{Aut}(K)$. Alors $G = \mathrm{Aut}(K/K^G)$ et $|\mathrm{Aut}(K/K^G)| = [K : K^G]$.

II.2 Construction des corps finis

Soit p premier, $n \in \mathbb{N}^*$ et $q = p^n$.

Thm 30 (Existence et "unicité" d'un corps fini)**.**
1. Le corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$ de $X^q - X$ est un corps fini de cardinal q.
2. Si $\mathbb{K}$ et $\mathbb{K}'$ sont deux corps finis de cardinal q, alors ils sont $\mathbb{Z}/p\mathbb{Z}$–isomorphes.

Notation 31. On notera $\mathbb{F}_q$ le corps fini de cardinal q, unique à $\mathbb{Z}/p\mathbb{Z}$–isomorphe près.

Rq 32. $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \ldots, \alpha_q) = \{\alpha_1, \ldots, \alpha_q\}$ où $\alpha_1, \ldots, \alpha_q$ sont les racines de $X^q - X \in \mathbb{F}_p[X]$

Ex 33. $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$ où α est une racine de $X^4 - X \in \mathbb{F}_2[X]$ différente de 0 et 1.

Thm 34. Soit α un générateur de $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p(\alpha)$

Thm 35. Il existe au moins un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n, et on a alors que $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$.

Ex 36. $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$, et il vient que $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. Soit α une racine de $X^2 + X + 1$, alors $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{a + b\alpha : a, b \in \mathbb{F}_2\} = \{0, 1, \alpha, 1 + \alpha\}$.

II.3 Un exemple : extensions cyclotomiques

Soit $n \in \mathbb{N}^*$.

Déf 37. On note $\mathbb{U}_n := \{z \in \mathbb{C} : z^n = 1\}$ l'ensemble des racines n-ième de l'unité. On note $\mathbb{V}_n = \{\zeta \in \mathbb{U}_n : \mathrm{ord}(\zeta) = n\}$ l'ensemble des racines $n^{\text{ième}}$ primitives de l'unité.

Déf 38. Le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}[X]$ est défini par : $\Phi_n(X) = \prod_{\zeta \in \mathbb{V}_n} (X - \zeta)$. On a $\deg(\Phi_n) = \varphi(n)$.

Thm 39 (DEV 1)**.** Φ_n est irréductible sur $\mathbb{Q}$.

C-ex 40. $\Phi_8 = X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$ pour tout p premier.

Cor 41. Soit m premier avec n, $\zeta \in \mathbb{V}_n$ et $\zeta \in \mathbb{V}_m$. On a alors :

1. Φ_n est le polynôme minimal de ζ sur $\mathbb{Q}$. En particulier, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. On appelle extension cyclotomique une telle extension.
2. $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\zeta') = \mathbb{Q}$

App 42 (Théorème de Wedderburn)**.** Tout corps fini est commutatif.

III Construction à la règle et au compas

Thm 43. L'ensemble des nombres complexes constructibles à la règle et au compas est un sous-corps de $\mathbb{C}$, stable par racine carrée.

Ex 44. $\zeta = e^{\frac{2i\pi}{5}}$ est constructible à la règle et au compas. Il vient que le pentagone régulier est constructible à la règle et au compas.

Fig 45 (Construction du pentagone régulier)**.**

Thm 46 (Wantzel)**.** Un nombre $\alpha \in \mathbb{C}$ est constructible si et seulement si il existe une tour d'extension $\mathbb{L}_0 \subseteq \cdots \subseteq \mathbb{L}_n$ telle que $\mathbb{L}_0 = \mathbb{Q}$, $\alpha \in \mathbb{L}_n$ et $[\mathbb{L}_{i+1} : \mathbb{L}_i] = 2 \ \forall i \in [\![0, n-1]\!]$

Cor 47. Tout nombre constructible est algébrique sur $\mathbb{Q}$, et son degré est une puissance de 2.

Ex 48.
— π n'étant pas algébrique sur $\mathbb{Q}$, π n'est pas constructible.
— $X^3 - 2$ étant irréductible sur $\mathbb{Q}$, ses racines : $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ ne sont pas constructibles.
— La réciproque est fausse : une racine réelle de $X^4 - X - 1$ n'est pas constructible.

App 49 (Réponse aux trois problèmes de l'Antiquité)**.** La quadrature du cercle, la duplication du cube et la trisection de l'angle, sont fausses.

Déf 50. p est un nombre premier de Fermat s'il est premier et qu'il existe un entier positif n tel que $p = 2^{2^n} + 1$.

Ex 51. Pour $n \in \{0, 1, 2, 3, 4\}$, $2^{2^n} + 1$ est un nombre premier de Fermat. Pour $n = 5$, il n'est pas premier.

Thm 52 (DEV 2)**.** Si p est un nombre premier de Fermat, alors $\zeta := e^{\frac{2i\pi}{p}}$ est constructible à la règle et au compas.

Cor 53 (Gauss-Wantzel)**.** Soit $n \in \mathbb{N}^*$, le polygone régulier à n côtés est constructible si et seulement si soit $n = 2^m$ où $m \geq 2$, soit $n = 2^m p_1 \dots p_r$ où $m \in \mathbb{N}$, $r \geq 1$ et les p_i sont des nombres premiers de Fermat distincts.

Ex 54.
— Le polygone régulier à 17 côtés est constructible à la règle et au compas.
— Le polygone régulier à 19 côtés n'est pas constructible à la règle et au compas.

Bibliographie

[Ulm18] Felix Ulmer. *Anneaux, corps, résultants*. ellipses, 2018.