

Leçon 125 : Extensions de corps. Exemples et applications

Sauf si précisé les corps seront toujours commutatifs.

1 Généralités

1.1 Premières propriétés

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

Exemple 2. On a par exemple $\mathbb{R} \subset \mathbb{C}$ ou $\mathbb{Q} \subset \mathbb{Q}(i)$.

Proposition 3. Si $\mathbb{K}$ est un sous corps de $\mathbb{L}$ alors $\mathbb{L}$ est un $\mathbb{K}$ -espace vectoriel.

Définition 4. Lorsque $\dim_{\mathbb{K}}(\mathbb{L})$ est finie on pose $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$ le degré de $\mathbb{L}$ sur $\mathbb{K}$.

Théorème 5. (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 6. (Multiplicativité du degré) Dans la situation précédente on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 7. Soit $\mathbb{K} \subset \mathbb{L}$ une extension et $A \subset \mathbb{L}$. On dit que A engendre $\mathbb{L}$ sur $\mathbb{K}$ et on écrit $\mathbb{L} = \mathbb{K}(A)$ lorsque $\mathbb{L}$ est le plus petit sous corps de $\mathbb{L}$ contenant $\mathbb{K}$ et A . Si $A = \{a_1, \dots, a_n\}$ et on note $\mathbb{L} = \mathbb{K}(a_1, \dots, a_n)$.
L'extension $\mathbb{L}$ est dite monogène lorsqu'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

Remarque 8. Si on a une extension $\mathbb{K} \subset \mathbb{L}$ et $\alpha \in \mathbb{L}$ on note $\mathbb{K}[\alpha]$ le sous anneau de $\mathbb{L}$ engendré par $\mathbb{K}$ et α et on a $\mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$. Cependant $\mathbb{K}[\alpha]$ n'est en général pas isomorphe à $\mathbb{K}[T]$ l'anneau des polynômes.

1.2 Algébriques et transcendants

Définition 9. Soit $\mathbb{K} \subset \mathbb{L}$ et soit $\alpha \in \mathbb{L}$. Soit $\varphi : \mathbb{K}[T] \rightarrow \mathbb{L}$ le morphisme défini par $\varphi|_{\mathbb{K}} = Id_{\mathbb{K}}$ et $\varphi(T) = \alpha$.

- Si φ est injectif on dit que α est transcendant sur $\mathbb{K}$.
- Sinon on dit que α est algébrique sur $\mathbb{K}$. C'est à dire qu'il existe $P \in \mathbb{K}[T]$ non nul tel que $P(\alpha) = 0$. Plus précisément $\ker \varphi = (P)$ et si on le suppose unitaire on dit que P est le polynôme minimal de α sur $\mathbb{K}$.

Exemple 10. Les nombres e et π sont transcendants sur $\mathbb{Q}$. Les nombres $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs $X^2 - 2, X^2 + 1, X^3 - 2$.

Proposition 11. Si α est transcendant on a $\mathbb{K}[\alpha] \cong \mathbb{K}[T]$ et $\mathbb{K}(\alpha) \cong \mathbb{K}(T)$.

Théorème 12. Soit $\mathbb{K} \subset \mathbb{L}$ une extension et soit $\alpha \in \mathbb{L}$. Les propriétés suivantes sont équivalentes :

1. α est algébrique sur $\mathbb{K}$,
2. $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$,
3. $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$.

Précisément si P est le polynôme minimal de α , P est irréductible et $\dim_{\mathbb{K}}(\mathbb{K}[\alpha]) = [\mathbb{K}[\alpha] : \mathbb{K}] = \deg(P)$ appelé le degré de α .

Définition 13. 1. Une extension $\mathbb{K} \subset \mathbb{L}$ est dite finie lorsque $\dim_{\mathbb{K}}(\mathbb{L}) = [\mathbb{L} : \mathbb{K}]$.
2. Une extension $\mathbb{K} \subset \mathbb{L}$ est dite algébrique lorsque pour tout $\alpha \in \mathbb{L}$, α est algébrique sur $\mathbb{K}$.

Théorème 14. Soit $\mathbb{K} \subset \mathbb{L}$ une extension, alors $M = \{x \in \mathbb{L} \mid x \text{ est algébrique sur } \mathbb{K}\}$ est un sous corps de $\mathbb{L}$.

Exemple 15. Pour $\mathbb{K} = \mathbb{Q}$ et $\mathbb{L} = \mathbb{C}$, $\mathbb{M}$ est une extension algébrique de $\mathbb{Q}$ mais qui n'est pas finie car il existe des éléments de degré arbitrairement grands ($\sqrt[n]{2}$ annulé par $X^n - 2$ irréductible).

Définition 16. Un corps $\mathbb{K}$ est algébriquement clos lorsqu'il vérifie l'une des propriétés équivalentes suivantes :

1. Tout polynôme $P \in \mathbb{K}[X]$ de degré supérieur à 1 admet une racine dans $\mathbb{K}$.
2. Tout polynôme $P \in \mathbb{K}[X]$ est produit de polynôme de degré 1.
3. Les éléments irréductibles de $\mathbb{K}[X]$ sont les $X - \alpha$ avec $\alpha \in \mathbb{K}$.
4. Si une extension $\mathbb{K} \subset \mathbb{L}$ est algébrique alors $\mathbb{K} = \mathbb{L}$.

Exemple 17. $\mathbb{C}$ est algébriquement clos. Le corps $\mathbb{M}$ de l'exemple précédent est une extension algébriquement close de $\mathbb{Q}$.

2 Extensions et catégories

2.1 Corps de rupture et de décomposition

Définition 18. 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 19. Soit $P \in \mathbb{K}$ irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$ unique à isomorphisme près.

Définition 20. 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 21. 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 $D_{\mathbb{K}}(P)$.

Exemple 22. Dans $\mathbb{Q}$ on a $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(j, \sqrt[3]{2})$ et $D_{\mathbb{Q}}(X^4 - 2) = \mathbb{Q}(i, \sqrt[4]{2})$.

Définition 23. Une extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est appelée clôture algébrique lorsque $\overline{\mathbb{K}}$ est algébriquement clos et $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$.

Exemple 24. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, le corps $\mathbb{M}$ de 15 est une clôture algébrique de $\mathbb{Q}$.

2.2 Corps finis

Définition 25. 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 26. 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 27. 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 28. Si $\mathbb{K}$ est fini c'est un automorphisme et si $\mathbb{K} = \mathbb{F}_p$ c'est l'identité.

Théorème 29. 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 30. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique d'ordre $q - 1$.

3 Application à l'irréductibilité

3.1 Polynômes cyclotomiques

Définition 31. 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 32. Le n -ième polynôme cyclotomique de $\mathbb{K}$ est $\Phi_n(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$.

Remarque 33. 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 34. On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proposition 35. Dans $\mathbb{Q}$ on a $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 36. Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

3.2 Polynômes de $\mathbb{F}_p$

Lemme 37. *Le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.*

Théorème 38. *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 39. $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Définition 40. 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 41. (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 $\mathcal{U}_d(p) = \{P \in \mathbb{F}_p[X] \mid \deg(P) = d, \text{ irréductible et unitaire} \}$ pour tout $n \in \mathbb{N}^*$ et p premier fixé.

Lemme 42. *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 43. *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 44. *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 : Polynômes cyclotomiques irréductibles 35 et 36

Dev 2 : Dénombrement des polynômes irréductibles de $\mathbb{F}_q$ 41,42,43 et 44

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 :

Les extensions de degré fini, le théorème de la base télescopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. Il est souhaitable d'introduire la notion d'élément algébrique et d'extension algébrique en donnant des exemples. Il faut savoir calculer le polynôme minimal d'un élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon peut être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, ainsi que par des extensions cyclotomiques.

Pour aller plus loin, les candidates et candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos, par exemple en expliquant comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Il est possible de s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.