Leçon 125 : Extensions de corps. Exemples et applications.

Dans cette leçon, on appelle *corps* un anneau commutatif non nul dont tous les éléments non nuls sont inversibles.

1 Degré d'une extension de corps

Définition 1. Soit **K** un corps. On dit qu'un corps **L** est une extension de **K** s'il existe un morphisme de corps (nécessairement injectif) de **K** dans **L**. On note $\mathbf{L} : \mathbf{K}$ pour dire que **L** est une extension de **K**.

Remarque 2. Le corps **K** est alors isomorphe à un sous-corps de **L**. Quitte à identifier **K** et son image dans **L**, on supposera que $\mathbf{K} \subseteq \mathbf{L}$.

Définition 3. Soit **K** un corps, on considère le morphisme d'anneaux $n \in \mathbf{Z} \mapsto n\,1_{\mathbf{K}} \in \mathbf{K}$. Son noyau est un idéal de **Z**, donc de la forme $n\mathbf{Z}$ où $n \in \mathbf{N}$. Cet entier n est appelé la caractéristique du corps **K**, on le note car(**K**).

Proposition 4. *Soit* **K** *un corps et soit* $p = \mathrm{car}(\mathbf{K})$.
— *Si* $p = 0$, *alors* **K** *est une extension de* **Q**.
— *Si* $p \neq 0$, *alors* p *est premier et* **K** *est une extension de* $\mathbf{Z}/p\mathbf{Z}$.
Le corps **Q** *(resp.* $\mathbf{Z}/p\mathbf{Z}$*) est le plus petit sous-corps de* **K**, *on l'appelle le sous-corps premier de* **K**.

Proposition 5. *Soit* $\mathbf{L} : \mathbf{K}$ *une extension, alors* **L** *est naturellement muni d'une structure de* **K***–espace vectoriel. Sa dimension (éventuellement infinie) est appelée degré de* **L** *sur* **K** *et on note* $[\mathbf{L} : \mathbf{K}] = \dim_{\mathbf{K}} \mathbf{L}$.

Exemple 6.

1. **C** est une extension de degré 2 de **R**.
2. **R** est une extension infinie de **Q**.
3. Si **K** est un corps et $P \in \mathbf{K}[X]$ est irréductible alors $\mathbf{K}[X]/(P)$ est une extension de **K** de degré $\deg P$.
4. Si **K** est un corps alors $\mathbf{K}(X)$ est une extension infinie de **K**.

Théorème 7 (base télescopique)**.** *Soient* $\mathbf{L} : \mathbf{K}$ *et* $\mathbf{M} : \mathbf{L}$ *deux extensions. Soit* $\{x_i\}_{i\in I}$ *une base de* **L** *sur* **K** *et soit* $\{y_j\}_{j\in J}$ *une base de* **M** *sur* **L**. *Alors* **M** *est une extension de* **K** *et* $\{x_i y_j\}_{(i,j)\in I\times J}$ *est une base de* **M** *sur* **K**. *En particulier, on a la multiplicativité des degrés :*

$$[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}] \times [\mathbf{L} : \mathbf{K}]$$

2 Extensions algébriques, extensions transcendantes

Définition 8. Soit $\mathbf{L} : \mathbf{K}$ une extension et soit S une partie de **L**. Le plus petit sous-corps de **L** contenant $\mathbf{K} \cup S$ est noté $\mathbf{K}(S)$ et est appelé sous-corps de **L** obtenu par adjonction de S à **K**. Dans le cas où $S = \{\alpha_1, \ldots, \alpha_n\}$, on le notera plus simplement $\mathbf{K}(\alpha_1, \ldots, \alpha_n)$.

Définition 9. Soit $\mathbf{L} : \mathbf{K}$ une extension et soit $\alpha \in \mathbf{L}$. On dit que α est algébrique sur **K** s'il existe un polynôme non nul $P \in \mathbf{K}[X]$ tel que $P(\alpha) = 0$. Sinon, on dit que α est transcendant sur **K**.

Exemple 10.

1. Les nombres $\sqrt[3]{2}$, i et $\zeta_n = \exp(\frac{2i\pi}{n})$ sont algébriques sur **Q**.
2. Les nombres e et π sont transcendants sur **Q**. (Hermite et Lindemann, admis)
3. Si **K** est un corps alors dans $\mathbf{K}(T)$, l'élément T est transcendant sur **K**.

Définition 11. Soit $\mathbf{L} : \mathbf{K}$ une extension et soit $\alpha \in \mathbf{L}$ algébrique sur **K**. L'ensemble des polynômes de $\mathbf{K}[X]$ qui annulent α est un idéal non nul de $\mathbf{K}[X]$, il est donc engendré par un unique polynôme irréductible unitaire non nul $P \in \mathbf{K}[X]$. Ce polynôme est appelé le polynôme minimal de α sur **K**.

Théorème 12. *Soit* $\mathbf{L} : \mathbf{K}$ *une extension et soit* $\alpha \in \mathbf{L}$.

1. *Si* α *est algébrique sur* $\mathbf{K}$ *de polynôme minimal* P*, alors on a l'isomorphisme de corps* $\mathbf{K}(\alpha) \cong \mathbf{K}[X]/(P)$.
2. *Si* α *est transcendant sur* $\mathbf{K}$*, alors* $\mathbf{K}(\alpha) \cong \mathbf{K}(X)$.

Corollaire 13. *Soit* $\mathbf{L} : \mathbf{K}$ *une extension et soit* $\alpha \in \mathbf{L}$*. Alors* α *est algébrique sur* $\mathbf{K}$ *ssi* $[\mathbf{K}(\alpha) : \mathbf{K}] < \infty$*. Dans le cas où* α *est algébrique sur* $\mathbf{K}$ *de polynôme minimal* P*, on a* $[\mathbf{K}(\alpha) : \mathbf{K}] = \deg P$.

Définition 14. Soit $\mathbf{L} : \mathbf{K}$ une extension. On dit que c'est une extension finie si $[\mathbf{L} : \mathbf{K}] < \infty$. On dit que c'est une extension algébrique si tout élément de $\mathbf{L}$ est algébrique sur $\mathbf{K}$.

Proposition 15. *Toute extension finie est algébrique.*

Théorème 16. *Soient* $\mathbf{L} : \mathbf{K}$ *et* $\mathbf{M} : \mathbf{L}$ *deux extensions. Alors* $\mathbf{M} : \mathbf{K}$ *est algébrique ssi* $\mathbf{M} : \mathbf{L}$ *et* $\mathbf{L} : \mathbf{K}$ *sont algébriques.*

Théorème 17. *Soit* $\mathbf{L} : \mathbf{K}$ *une extension. On définit l'ensemble :*

$$\mathbf{M} = \{x \in \mathbf{L} \mid x \text{ algébrique sur } \mathbf{K}\}$$

Alors $\mathbf{M}$ *est un sous-corps de* $\mathbf{L}$ *et c'est une extension algébrique de* $\mathbf{K}$.

Exemple 18. L'ensemble $\overline{\mathbf{Q}} = \{x \in \mathbf{C} \mid x \text{ algébrique sur } \mathbf{Q}\}$ est un corps, c'est une extension algébrique infinie de $\mathbf{Q}$.

Théorème 19 (élément primitif, caractéristique 0)**.** *Soit* $\mathbf{K}$ *un corps de caractéristique* 0 *et soit* $\mathbf{L} : \mathbf{K}$ *une extension finie. Alors il existe* $\alpha \in \mathbf{L}$ *tel que* $\mathbf{L} = \mathbf{K}(\alpha)$.

Exemple 20. $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ est une extension de degré 6 de $\mathbf{Q}$. D'après le théorème précédent, il est engendré par un seul élément. En effet $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

3 Cyclotomie

Définition 21. On appelle racine n–ième de l'unité les racines du polynôme $X^n - 1$ dans $\mathbf{C}$, et on note $\mu_n(\mathbf{C})$ l'ensemble de ces racines. C'est un groupe cyclique d'ordre n, on appelle racine n–ième primitive un générateur de ce groupe et on note $\mu_n^*(\mathbf{C})$ l'ensemble des racines n–ièmes primitives. On définit le n–ième polynôme cyclotomique par :

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*(\mathbf{C})} (X - \zeta)$$

Proposition 22. $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Théorème 23. *Pour tout* $n \in \mathbf{N}^*$, $\Phi_n \in \mathbf{Z}[X]$ *et est irréductible dans* $\mathbf{Z}[X]$ *(et donc dans* $\mathbf{Q}[X]$*). Il est de degré* $\varphi(n)$.

Corollaire 24. *Si* $\zeta \in \mathbf{C}$ *est une racine primitive n–ième de l'unité, alors son polynôme minimal est* Φ_n*, donc* $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

4 Adjonction de racines

Définition 25. Soient $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ irréductible. Une extension $\mathbf{L} : \mathbf{K}$ est appelée un corps de rupture de P sur $\mathbf{K}$ s'il existe $\alpha \in \mathbf{L}$ tel que $\mathbf{L} = \mathbf{K}(\alpha)$ et $P(\alpha) = 0$.

Théorème 26. *Soient* $\mathbf{K}$ *un corps et* $P \in \mathbf{K}[X]$ *irréductible. Alors il existe* $\mathbf{L} = \mathbf{K}(\alpha)$ *un corps de rupture de* P *sur* $\mathbf{K}$*, unique au sens suivant : si* $\mathbf{L}' = \mathbf{K}(\alpha')$ *est un autre corps de rupture de* P *sur* $\mathbf{K}$*, alors il existe un unique isomorphisme* $\varphi : \mathbf{L} \to \mathbf{L}'$ *qui vérifie* $\varphi_{|\mathbf{K}} = \mathrm{id}_{\mathbf{K}}$ *et* $\varphi(\alpha) = \alpha'$.

Définition 27. Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ de degré $n \geqslant 1$. Une extension $\mathbf{L} : \mathbf{K}$ est appelée un corps de décomposition de P sur $\mathbf{K}$ si :

1. Il existe $\lambda, \alpha_1, \ldots, \alpha_n \in \mathbf{L}$ tels que dans $\mathbf{L}[X]$, $P = \lambda(X - \alpha_1) \cdots (X - \alpha_n)$.

2. $\mathbf{L} = \mathbf{K}(\alpha_1, \ldots, \alpha_n)$.

Théorème 28. *Soit* $\mathbf{K}$ *un corps et* $P \in \mathbf{K}[X]$ *un polynôme de degré* $n \geqslant 1$. *Alors il existe* $\mathbf{L}$ *un corps de décomposition de* P *sur* $\mathbf{K}$*, unique au sens suivant : si* $\mathbf{L}'$ *est un autre corps de décomposition de* P *sur* $\mathbf{K}$*, alors il existe un isomorphisme entre* $\mathbf{L}$ *et* $\mathbf{L}'$.

Proposition 29. *Soit* $\mathbf{L} : \mathbf{K}$ *une extension et soit* $P \in \mathbf{K}[X]$ *de degré* $n \geqslant 1$. *Si* $\mathbf{L}$ *est un corps de décomposition de* P *sur* $\mathbf{K}$ *alors* $[\mathbf{L} : \mathbf{K}] \leqslant n!$.

Exemple 30. $\mathbf{K} = \mathbf{Q}$ et $P = X^3 - 2$, alors $\mathbf{Q}(\sqrt[3]{2}, \mathrm{j})$ est « le » corps de décomposition de P sur $\mathbf{Q}$. De plus, son degré vaut 6, l'inégalité précédente est donc optimale.

Application 31 (Théorème de Cayley–Hamilton)**.** Soient $\mathbf{K}$ un corps, $n \in \mathbf{N}^*$ et $A \in \mathscr{M}_n(\mathbf{K})$. Soit $\chi_A(X) = \det(X\,\mathrm{I} - A)$ le polynôme caractéristique de A, alors $\chi_A(A) = 0$.

5 Corps finis

Théorème 32 (construction des corps finis)**.**

1. *Soit* $\mathbf{K}$ *un corps fini et soit* p *sa caractéristique. Alors il existe* $n \in \mathbf{N}^*$ *tel que* $|\mathbf{K}| = p^n$.
2. *Pour tout* $q = p^n$*, le corps de décomposition de* $X^q - X$ *est de cardinal* q *et il est unique à isomorphisme près. On note* $\mathbf{F}_q$ *ce corps.*

Proposition 33. *Soient* p *premier et* $d, n \in \mathbf{N}^*$. *Alors* $\mathbf{F}_{p^n}$ *est une extension de* $\mathbf{F}_{p^d}$ *ssi* d *divise* n.

Théorème 34. *Le groupe multiplicatif* $\mathbf{F}_q^*$ *est cyclique.*

Corollaire 35. *Soit* $\mathbf{F}_{q^n}$ *une extension de* $\mathbf{F}_q$*, alors il existe* $\alpha \in \mathbf{F}_{q^n}$ *tel que* $\mathbf{F}_{q^n} = \mathbf{F}_q(\alpha)$. *En particulier, pour tout* $n \in \mathbf{N}^*$*, il existe un polynôme irréductible dans* $\mathbf{F}_q[X]$ *de degré* n.

Définition 36. fonction de Möbius.

Proposition 37. *formule d'inversion de Möbius.*

Théorème 38 (dénombrement des polynômes irréductibles de $\mathbf{F}_q[X]$)**.** *Notons* $A(n,q)$ *l'ensemble des polynômes irréductibles unitaires de* $\mathbf{F}_q[X]$ *de degré* n *et notons* $I(n,q)$ *son cardinal. Alors :*

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

En particulier on a l'équivalent lorsque $n \to +\infty$, $I(n,q) \sim \frac{q^n}{n}$.

Développement

1. Théorème de l'élément primitif pour les corps de caractéristique 0. **[19]**
2. Dénombrement des polynômes irréductibles sur $\mathbf{F}_q$. **[38]**

Références

— CALAIS, *Extensions de corps – Théorie de Galois.*
— ELKIK, *Cours d'algèbre.*
— FRANCINOU et GIANELLA, *Exercices de mathématiques pour l'agrégation,* p. 189.
— GOURDON, *Les maths en tête, algèbre,* p. 89.
— PERRIN, *Cours d'algèbre.*