125 EXTENSIONS DE CORPS. EXEMPLES ET APPLICATIONS.

I. Généralités sur les extensions de corps

[Per96, §III, p65] [Cog00, §2.1, p60–62]

On ne considère que des corps commutatifs.

Définition 1. [Extension de corps, degré]
Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-e.v.. Lorsque $\dim(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est finie.

Exemple 2. $\mathbb{R} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{Q}(i)$.

Une extension de corps est un espace vectoriel sur le corps de base. On note $[\mathbb{L} : \mathbb{K}]$ le degré de cet espace vectoriel (éventuellement infini). Exemples

Théorème 3. [Théorème de la base télescopique]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ 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 $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Sous-corps contenant une partie. Exemple

Définition 4. [Élément algébrique, transcendant]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\phi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\phi_{|\mathbb{K}} = \mathrm{id}$ et $\phi(T) = \alpha$.
Si ϕ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\phi) = (P)$. P est appelé polynôme minimal de α.

Exemple 5. $\sqrt{2}, i$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Théorème 6. [Caractérisation d'un algébrique]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty$$

Théorème 7. *Pour tout entier $n \in \mathbb{N}$ et toute famille $p_1, \dots, p_n$ d'entiers supérieurs ou égaux à 2, tous sans facteur carré, et premiers deux à deux, on a :*

$$[\mathbb{Q}[\{\sqrt{p_i}\}_{1\leq i\leq n}] : \mathbb{Q}] = 2^n$$

Dans le cas transcendant, isomorphisme $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(X)$
Extension algébrique
Lorsque $[\mathbb{L} : \mathbb{K}] < +\infty$, l'extension est algébrique

II. Extensions de corps et polynômes

[Per96, §III.1.c, p70]

II. A. Corps de rupture

Corps de rupture d'un polynôme irréductible
Il existe un unique corps de rupture à isomorphisme près.
Exemple de $\mathbb{C}$, de $\mathbb{Q}[\sqrt{2}]$
Degré du corps de rupture

II. B. Corps de décomposition

Corps de décomposition
Existence et unicité à isomorphisme près
Exemple de $\mathbb{Q}(i, \sqrt{2})$
Théorème de l'élément primitif

II. C. Clôture algébrique

Corps algébriquement clos. Formulations équivalentes
Théorème de D'Alembert-Gauss [Rom17, p378]
Application : toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable
Polynôme ne s'annulant pas sur un corps fini $\rightarrow$ tout corps fini n'est pas algébriquement clos
Clôture algébrique
Tout corps admet une clôture algébrique unique à isomorphisme près

III. Applications

III. A. Irréductibilité de polynômes et réduction

[Per96, §3.3-3.4, p76–85] [Rom17, §12.11.4, p381–383]

Soit A un anneau factoriel. On note $K = \mathrm{Frac}(A)$

Proposition 8. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $A[X]$ si et seulement si il est de contenu 1 et irréductible dans $K[X]$.*

Proposition 9. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 10. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 11. *Soit I un idéal premier de A et $B = A/I$. Soit $P = \sum_{i=0}^{r} a_i X^i \in A[X]$ et $\overline{P}$ la réduction de P modulo I. Si $\overline{a_n}$ dans B, et si $\overline{P}$ est irréductible sur B ou $\mathrm{Frac}(B)$, alors P est irréductible sur K.*

Que l'on reformule dans le cas $A = \mathbb{Z}$, $I = (p)$, $B = \mathbb{F}_p$:

Proposition 12. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 13. $X^3+462X^2+2433X-67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme X^p-X-1 pour tout $p \in \mathcal{P}$.

Liens entre irréductibilité et degré des extensions [Per96, p78–79]

III. B. Cyclotomie

[Per96, §3.4, p80] [Rom17, §12.11.5, p383]

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

Définition 14. [polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Proposition 15.
(i) Φ_n *est unitaire de degré* $\varphi(n) = \mathrm{card}(\{k \in [1,n] \mid k \wedge n = 1\})$.
(ii) $X^n - 1 = \prod_{d|n} \Phi_d$. *En particulier, si n est premier :* $\Phi_n = X^n - 1$.

Corollaire 16.
- *On en déduit la fameuse formule* $\phi(n) = \sum_{d \mid n} \phi(d)$.
- *Pour* $n \geq 2$, $\sum_{\omega \in \mathbb{U}_n} \omega = 0$.

Proposition 17. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 18. Φ_n *est irréductible sur* $\mathbb{Z}$ *et donc sur* $\mathbb{Q}$.

Corollaire 19. *On a* $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.

ANNEXE

Schémas d'extensions de corps avec leur degré.

BIBLIOGRAPHIE

[Cog00] M. Cognet : *Algèbre linéaire*. Bréal, 2000.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.