125. Extensions de corps. Exemples et applications.

Tous les corps sont considérés comme commutatifs. K et L désignent des corps. On supposera connues les notions de caractéristique d'un corps et de sous-corps premier.

I. Extension de corps

1) Définition et premières propriétés

Déf. (1): Soient K, L deux corps. On dit que L est une extension de K, noté $K \subset L$, s'il existe un morphisme de corps (nécessairement injectif) de K dans L.
L a alors une structure de K-espace vectoriel, et $\dim_K L$ est appelé degré de L sur K, noté $[K:L]$.

Ex. (2): • $\mathbb{R} \subset \mathbb{C}$ et $[\mathbb{C}:\mathbb{R}] = 2$
• $\mathbb{R} \subset \mathbb{R}(X)$ et $[\mathbb{R}(X):\mathbb{R}] = +\infty$

Prop. (3): Si $K \subset L$ et K et L sont finis, alors $|L| = |K|^n$ où $n = [L:K]$ [Per] 65

Coro (4): Si K est fini de caractéristique p, alors : $\exists n \in \mathbb{N}^* / |K| = p^n$

Th. (5): (base téléscopique)
Soient $K \subset L \subset \Pi$ des corps, $(e_i)_{i\in I}$ base de L sur K et $(f_j)_{j\in J}$ base de Π sur L. Alors $(e_i f_j)_{I\times J}$ est une base de Π sur K.

Coro (6): Si $K \subset L \subset \Pi$, alors $[\Pi:K] = [\Pi:L][L:K]$

2) Extension algébrique

Déf. (7): Soit $K \subset L$ et $(\alpha_1 \dots \alpha_n) \in L^n$.
1) On note $K[\alpha_1 \dots \alpha_n]$ le plus petit sous-anneau de L contenant K et $(\alpha_1 \dots \alpha_n)$ ——— sous-corps ———
66
2) On dit que $(\alpha_1 \dots \alpha_n)$ engendre L sur K si $L = K(\alpha_1 \dots \alpha_n)$, et que L est monogène sur K s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Rq (8): $K[\alpha] = \{P(\alpha), P \in K[X]\}$

$$K(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)},\ P, Q \in K[X] \text{ et } Q(\alpha) \neq 0 \right\}$$

Déf. / Prop. (9): Soit $K \subset L$ une extension et $\alpha \in L$.
On définit $\varphi : K[X] \to L$, $P \mapsto P(\alpha)$. φ est un morphisme d'anneaux.

1) Si φ est injectif, on dit que α est transcendant sur K.
On a alors $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$

2) Sinon, α est dit algébrique sur K. Il existe alors un unique $P \in K[X]$ unitaire, irréductible (donc de degré ≥ 1) tel que $\ker \varphi = (P)$.
P est appelé polynôme minimal de α sur K, et $\deg(P)$ est appelé degré de α sur K.

Ex. (10):
• $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, de polynôme minimal $X^2 - 2$ et de degré 2.
• $\sqrt{2} \in \mathbb{R}$ ——— $\mathbb{R}$, ——— $X - \sqrt{2}$ ——— 1.
• e et π sont transcendants sur $\mathbb{Q}$ (culturel). Plus généralement, $\overline{\mathbb{Q}} = \{\lambda \in \mathbb{C}, \lambda \text{ algébrique sur } \mathbb{Q}\}$ est dénombrable donc il existe une infinité (non dénombrable) de nombres transcendants sur $\mathbb{Q}$.

Th. (11): Soit $K \subset L$, $\alpha \in L$. Sont équivalentes
i) α est algébrique sur K ii) $K[\alpha] = K(\alpha)$ iii) $\dim_K K[\alpha] < +\infty$

Coro (12): Si $\alpha \in L$ est algébrique sur K de polynôme minimal P, alors $\dim_K K[\alpha] = \deg(P)$.

Déf. (13): 1) Une extension $K \subset L$ est dite finie si $[L:K] < +\infty$ 67
2) Une extension $K \subset L$ est dite algébrique si tout $\alpha \in L$ est algébrique sur K.

Ex. (14): $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ est finie

Rq (15): Une extension $K \subset L$ finie est algébrique, mais la réciproque est fausse (voir Ex. (17)).

Th. (16): Soit $K \subset L$ une extension et $\Pi = \{x \in L / x \text{ algébrique sur } K\}$
Alors, Π est un sous-corps de L.

Ex (17): $\mathbb{Q} \subset \overline{\mathbb{Q}}$ est une extension algébrique, mais pas une extension finie.

[Bos]

Prop. (18) : Soit $K \subset L$ une extension, $a, b \in L$ algébriques sur K de polynômes minimaux respectifs f et g. Alors

1) $S = \mathrm{Res}_X(f(X), g(T-X)) \in K[T]$ est un polynôme annulateur de $a+b$

125 2) $P = \mathrm{Res}_X(f(X), T^{\deg g} g\left(\frac{X}{T}\right)) \in K[T]$ ——— ab.

Exercice (19) : Déterminer un polynôme annulateur de $\sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$.
(réponse : (18).1) nous donne $S = T^4 - 10T^2 + 1$)

[Pu]

Déf. (20) : K est dit algébriquement clos si tout $P \in K[X]$ de

67 degré ≥ 1 admet une racine dans K.

Ex. (21) : • $\mathbb{C}$ est algébriquement clos (d'Alembert - Gauss)

• $\bar{\mathbb{Q}}$ ———

• $\mathbb{R}$ n'est pas algébriquement clos (X^2+1 par exemple)

68

II. Construction d'extension par adjonction de racine

1) Corps de rupture

Déf. (22) : Soit $P \in K[X]$ irréductible. Une extension $K \subset L$ est appelée

70 corps de rupture si $L = K(\alpha)$ est monogène et $P(\alpha) = 0$.

On a alors $[L:K] = \deg P$.

Th. (23) : Soit $P \in K[X]$ irréductible. Alors il existe un corps de rupture de P sur K, unique à isomorphisme près.

Rq (24) : P n'est pas nécessairement scindé sur un corps de rupture
($P = X^3 - 2 \in \mathbb{Q}[X]$, $L = \mathbb{Q}(\sqrt[3]{2})$).

2) Corps de décomposition

Déf. (25) : Soit $P \in K[X]$ (irréductible ou non). Un corps de

71 décomposition de P sur K est une extension $K \subset L$ telle que :

1) P est scindé sur L

2) L est engendré par les racines de P.

Th. (26) : Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, noté $D_K(P)$, unique à isomorphisme près.

Ex. (27) : $D_{\mathbb{Q}}(X^3-2) = \mathbb{Q}(j, \sqrt[3]{2})$ et $[\mathbb{Q}(j, \sqrt[3]{2}) : \mathbb{Q}] = 6$

Appli. (28) : Soit E un K-ev de dimension finie, $u \in \mathcal{L}(E)$ de polynôme [Gou] caractéristique χ_u. Alors $\chi_u(u) = 0$ (Cayley - Hamilton) 176

3) Critères d'irréductibilité d'un polynôme

[Per]

Th. (29) : (critère d'Eisenstein)

Soit A anneau factoriel, $K = Fr(A)$ et $P = a_n X^n + \dots + a_0 \in A[X]$, $n \geq 2$. 76

S'il existe $p \in A$ irréductible tel que :

i) $p \nmid a_n$

ii) $\forall\, 0 \leq i \leq n-1$, $p \mid a_i$

iii) $p^2 \nmid a_0$

Alors P est irréductible sur K (donc sur A si $c(P) = pgcd(a_0 \dots a_n) = 1$).

Ex. (30) : Si $p \in \mathbb{N}$ est premier, alors $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$. 77

Th. (31) : Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$, $n \geq 1$ et $p \in \mathbb{N}$ premier.
Si $\bar{a}_n \neq \bar{0}$ et $\bar{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$.

Rq (32) : pas nécessairement sur $\mathbb{Z}$! ($P = 2X$, $p = 3$)

Th. (33) : Soit $P \in K[X]$, $\deg P = n \geq 1$

Alors P est irréductible sur K SSI P n'admet pas de racine dans 78
toute extension $K \subset L$ telle que $[L:K] \leq n/2$

Ex. (34) : $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

III. Extensions cyclotomiques $n \in \mathbb{N}$, $n \geq 1$

Déf. (35) : Soit $\mu_n = \{\zeta \in \mathbb{C}, \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité, et $\mu_n^* = \{\zeta \in \mu_n / \forall\, 0 < d < n, \zeta^d \neq 1\}$ l'ensemble des racines primitives n-ièmes de l'unité.

[Per] 80

Prop. (36) : $|\mu_n^*| = \varphi(n)$ et si $\zeta \in \mu_n^*$ et $m \in \mathbb{N}$, alors $\zeta^m \in \mu_n^*$ ssi $m \wedge n = 1$.

Déf. (37) : Le n-ième polynôme cyclotomique est $\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta) \in \mathbb{C}[X]$

Prop. (38) : $X^n - 1 = \prod_{d|n} \Phi_d$

Ex. (39) : $\Phi_1 = X - 1$; $\Phi_2 = X + 1$; $\Phi_3 = X^2 + X + 1$; $\Phi_4 = X^2 + 1$ 81

$\Phi_p = X^{p-1} + \dots + X + 1$ pour p premier.

Th./Déf. (40) : $\Phi_n \in \mathbb{Z}[X]$. Pour p premier, on notera $\Phi_{n,\mathbb{F}_p}$ le projeté (canonique) de Φ_n sur $\mathbb{F}_p[X]$.

82 **Th. (41)** : Pour tout $n \geq 1$, Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$

Coro. (42) : Si $\zeta \in \mu_n^*$, alors son polynôme minimal sur $\mathbb{Q}$ est Φ_n, et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

DVP

[Cont] 169

Appli. (43) : Soit $\mathbb{Q} \subset K$ une extension finie. Alors K contient un nombre fini de racines de l'unité.

[Cyc] 70

Prop. (44) : Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. On note pour $k \in \mathbb{N}^*$ ζ_k une racine primitive k-ième de l'unité.

On a alors : $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$.

IV. Corps finis

$p \in \mathbb{N}$ premier, $n \in \mathbb{N}^*$

[Per] 73

Déf./Prop. (45) : Soit K un corps de caractéristique p.

Alors $F : K \to K$, $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Si K est fini, c'est un automorphisme. Si $K = \mathbb{F}_p$, $F = id_{\mathbb{F}_p}$.

Th. (46) : Soit $q = p^n$. Il existe un unique corps (à isomorphisme près) à q éléments, noté $\mathbb{F}_q$. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

74

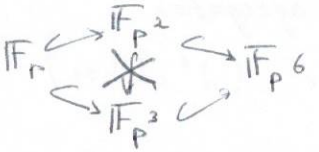
Th. (47) : $(\mathbb{F}_q^*, \cdot)$ est cyclique de cardinal $q - 1$.

Ex. (48) : $(\mathbb{F}_8^*, \cdot) \simeq (\mathbb{Z}/7\mathbb{Z}, +)$ et tout élément différent de 1 est un générateur de $\mathbb{F}_8^*$.

Prop. (49) : Soit $q = p^n$. Pour tout $m | n$, il existe un unique sous-corps de $\mathbb{F}_q$ de cardinal p^m. C'est l'ensemble des racines de $X^{p^m} - X$ dans $\mathbb{F}_q$.

Coro. (50) : $\mathbb{F}_{p',m} \subset \mathbb{F}_{p^n} \iff p = p'$ et $m | n$

Ex. (51) :



[Dm3] 220

Th. (52) : Soit $\mathbb{F}_q$ un corps fini et $n \geq 1$. $S = X^{q^n} - X$ est alors exactement le produit des polynômes unitaires irréductibles sur $\mathbb{F}_q$ dont le degré divise n.

De plus, en notant m_n le nombre de polynômes irréductibles de degré n, on a : $m_n \sim \frac{q^n}{n}$ quand $n \to +\infty$

DVP

Coro (53) : Soit $P \in \mathbb{F}_q[X]$, $\deg P = n \geq 1$. Alors

P irréductible sur $\mathbb{F}_q \iff$ i) $P \mid X^{q^n} - X$

ii) $\forall d | n$, d premier, $P \wedge (X^{q^{n/d}} - X) = 1$

[Beck] 244

Rq (54) : Le coro (53) nous donne un algorithme permettant de tester l'irréductibilité d'un polynôme sur $\mathbb{F}_q$. Si $P \in \mathbb{F}_q[X]$ n'est pas irréductible et est sans facteur carré, on peut utiliser l'algorithme de Berlekamp pour déterminer ses facteurs irréductibles.

Références :

- [Per] Perrin, Cours d'algèbre (80 %)
- [Bos] Bostan, Chyzak, Algorithmes efficaces en calcul formel
- [Ort] Ortiz, Exercices d'algèbre
- [Dmz] Demazure, Cours d'algèbre
- [Goz] Gozard, Théorie de Galois
- [Beck] Beck, Objectif agrégation
- [Gou] Gourdon, Algèbre (2e édition)