125

Extensions de corps. Exemples et applications.

Soit $\mathbb{K}$, $\mathbb{L}$, k corps, $n\in\mathbb{N}^*$, $p\in\mathbb{N}$ premier

I] Extensions de corps et extensions algébriques

1] Notion d'extension de corps

[Goz] II.1

Définition 1 : On dit que $\mathbb{K}$ est une extension de k s'il existe un morphisme de corps $j : k\to\mathbb{K}$. On note $\mathbb{K}/k$.

Remarque 2 : (1) Si k est un sous-corps de $\mathbb{K}$, alors $\mathbb{K}/k$ par l'injection canonique.
(2) Réciproquement, tout morphisme de corps est injectif i.e. $j(k)$ est isomorphe à un sous-corps de $\mathbb{K}$.

Exemple 3 : $\mathbb{C}/\mathbb{R}$ et $\mathbb{R}/\mathbb{Q}$.

2] Extension et degré

[Goz] II.1

Proposition 4 : Soit $\mathbb{K}/k$.
Alors : il existe un morphisme de corps $j : k\to\mathbb{K}$ muni d'une loi. $\forall\lambda\in k, \forall x\in\mathbb{K}, \lambda x = j(\lambda).x$ rendant $\mathbb{K}$ une k-algèbre.

Définition 5 : Soit $\mathbb{K}/k$. On appelle degré de $\mathbb{K}/k$: $[\mathbb{K}:k]=\dim_k(\mathbb{K})$ la dimension de $\mathbb{K}$ comme k-espace vectoriel.

Exemple 6 : $[\mathbb{C}:\mathbb{R}]=2$ et $[\mathbb{R}:\mathbb{Q}]=+\infty$

Théorème 7 : (de la base télescopique) Soit $k\subseteq\mathbb{K}\subseteq\mathbb{L}$ extensions de corps, $(x_i)_{i\in I}$ base de $\mathbb{K}$ sur k et $(\beta_j)_{j\in J}$ base de $\mathbb{L}$ sur $\mathbb{K}$.
Alors : $(x_i\beta_j)_{i,j\in I\times J}$ est une base de $\mathbb{L}$ sur k.
$[\mathbb{L}:k]=[\mathbb{L}:\mathbb{K}][\mathbb{K}:k]$ (multiplicativité du degré)

Définition 8 : On appelle tour d'extensions toute suite finie de corps croissante pour l'inclusion : $\mathbb{K}_1\subseteq\dots\subseteq\mathbb{K}_r$.

3] Extension de type fini

[Goz] II.2

Définition 9 : Soit $\mathbb{L}/k$ et $P\subseteq\mathbb{L}$. On appelle sous-extension de $\mathbb{L}/k$ engendrée par P le plus petit élément, au sens de l'inclusion, des sous-corps de $\mathbb{L}$ contenant k. Noté $k(P)$.
On dit que $\mathbb{L}$ est une extension de type fini de k s'il existe une partie finie $\{x_1;\dots;x_n\}\in\mathbb{L}^n$ telle que $\mathbb{L}=k(x_1;\dots;x_n)$.
On dit que $\mathbb{L}$ est monogène si $n=1$.

Proposition 10 : Une extension $\mathbb{L}$ de degré fini de $\mathbb{K}$ est de type fini sur $\mathbb{K}$.

Contrexemple 11 : La réciproque est fausse.
$\mathbb{K}(X)$ est de type fini sur $\mathbb{K}$ mais pas de degré fini sur $\mathbb{K}$.

Proposition 12 : Soit $\mathbb{L}/k$ avec $[\mathbb{L}:k]$ premier.
Alors : $\mathbb{L}$ est une extension monogène de k i.e. $\exists x\in\mathbb{L}\ \backslash\ \mathbb{L}=k(x)$.

4] Éléments algébriques et transcendants

[Goz] III.1

Définition 13 : Soit $a\in\mathbb{K}$, $\mathbb{K}/k$ et $ev_a : k[X]\to\mathbb{K}$, $P\mapsto P(a)$ morphisme d'évaluation, $\ker(ev_a)$ l'idéal annulateur de a, $k[a]=\mathrm{Im}(ev_a)$:
(i) Si $\ker(ev_a)\neq\{0\}$, alors a est un élément algébrique sur k et on note $\Pi_a\in k[X]$ tel que $\ker(ev_a)=\langle\Pi_a\rangle$.
(ii) Si $\ker(ev_a)=\{0\}$, alors a est un élément transcendant sur k.

Exemple 14 : (1) e et π sont transcendants sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$.
(2) $\sqrt{2}$; i; $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs X^2-2 ; X^2+1 et X^3-2.

Théorème 15 : (caractérisation des éléments algébriques) Soit $\mathbb{L}/\mathbb{K}$ et $a\in\mathbb{L}$.
Alors : a est algébrique sur $\mathbb{K}$ ssi $[\mathbb{K}[a]:\mathbb{K}]<+\infty$
ssi $k[a]=k(a)$

III.3 [Goz]

5] Extensions algébriques

Définition 16: Soit $\mathbb{K}/k$. On dit que $\mathbb{K}$ est une extension algébrique de k si tous les éléments de $\mathbb{K}$ sont algébriques sur k.

Exemple 17: $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$

Proposition 18: Toute extension de degré fini de k est algébrique sur k.

Proposition 19: Soit $\mathbb{L}=\mathbb{K}(x_1,\dots,x_s)$ extension de type fini de $\mathbb{K}$, telle que les x_i sont algébriques sur $\mathbb{K}$.
Alors: $[\mathbb{L}:\mathbb{K}]<+\infty$ et $\mathbb{L}=\mathbb{K}[x_1,\dots,x_s]$

Théorème 20: (transitivité de l'algébricité) Soit $k\subseteq\mathbb{K}\subseteq\mathbb{L}$ extensions.
Alors: $\mathbb{L}$ est algébrique sur k ssi $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et $\mathbb{K}$ est algébrique sur k.

II] Construction de corps, lien avec les polynômes

V.1 [Goz]

1] Corps de rupture

Définition 21: Soit $f\in\mathbb{K}[X]$ irréductible. On dit que $\mathbb{L}$ est un corps de rupture de f si $\mathbb{L}$ est une extension de $\mathbb{K}$ engendrée par $\mathbb{K}$ et une racine x de f : $\mathbb{L}=\mathbb{K}(x)$.

Exemple 22: Si $\deg(f)=1$, alors $\mathbb{K}$ est un corps de rupture de f

Théorème 23: Soit $f\in\mathbb{K}[X]$ irréductible.
Alors: (1) il existe un corps de rupture de f,
(2) Si $\mathbb{K}(\alpha)$ et $\mathbb{K}(\beta)$ sont deux corps de rupture de f, alors il existe un unique $\mathbb{K}$-isomorphisme $\sharp:\mathbb{K}(\alpha)\to\mathbb{K}(\beta)$ tel que $\sharp(\alpha)=\beta$.

V.1 [Goz]

Application 24: $\mathbb{C}\simeq \mathbb{R}[X]/\langle X^2+1\rangle$ et $\mathbb{F}_4\simeq \mathbb{F}_2[X]/\langle X^2+X+1\rangle$

Proposition 25: Soit $P\in\mathbb{K}[X]$ tel que $\deg(P)=n$.
Alors: P est irréductible sur $\mathbb{K}$ ssi P n'a pas de racine dans les extensions $\mathbb{L}$ de $\mathbb{K}$ telles que $[\mathbb{L}:\mathbb{K}]\leq\frac{n}{2}$.

Proposition 26: Soit $P\in\mathbb{K}[X]$ irréductible tel que $\deg(P)=n$, soit $\mathbb{L}$ extension de $\mathbb{K}$ telle que $[\mathbb{L}:\mathbb{K}]=m$ tel que $m\wedge n=1$.
Alors: P est irréductible sur $\mathbb{L}$

Exemple 27: X^3+X+1 est irréductible sur $\mathbb{Q}(i)$ et $\mathbb{Q}$

Contrexemple 28: L'hypothèse $m\wedge n=1$ est vitale ! X^4+1 est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Q}(i)$: $X^4+1=(X^2+i)(X^2-i)$

V.2 [Goz]

2] Corps de décomposition

Définition 29: Soit $\mathbb{L}/\mathbb{K}$, $P\in\mathbb{K}[X]$ tel que $\deg(P)=n$. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si :
$\exists\, a;\alpha_1;\dots;\alpha_n\in\mathbb{L}^{n+1} \mid P(X)=a(X-\alpha_1)\dots(X-\alpha_n)$ et $\mathbb{L}=\mathbb{K}(\alpha_1,\dots,\alpha_n)$

Exemple 30: (1) $\mathbb{C}$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$.
(2) $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.

Théorème 31: Soit $P\in\mathbb{K}[X]\setminus\mathbb{K}$.
Alors: (1) il existe un corps de décomposition Σ de P sur $\mathbb{K}$ tel que $[\Sigma:\mathbb{K}]\leq n!$
(2) Si Σ et Σ' sont deux corps de décomposition de P sur $\mathbb{K}$, alors : il existe un $\mathbb{K}$-isomorphisme de Σ dans Σ'.

Notation 32: On note $D_{\mathbb{K}}(P)$ l'unique corps de décomposition de P sur $\mathbb{K}$ à isomorphisme près.

VIII.3

Théorème 33: (de l'élément primitif) Soit $\mathbb{L}/\mathbb{K}$ tel que $[\mathbb{L}:\mathbb{K}]<+\infty$ et $\mathbb{L}$ séparable.
Alors: $\exists x\in\mathbb{L} \mid \mathbb{L}=\mathbb{K}(x)$

3) Clôture algébrique

IV.3

Définition 34 : On dit que $\mathbb{K}$ est algébriquement clos si tout polynôme de $\mathbb{K}[X]\setminus\mathbb{K}$ est scindé sur $\mathbb{K}$.

Exemple 35 : $\mathbb{Q}$; $\mathbb{R}$ et $\mathbb{F}_p$ ne sont pas algébriquement clos.

Proposition 36 : Tout corps algébriquement clos est infini.

Théorème 37 : (de Gauss) $\mathbb{C}$ est algébriquement clos.

Application 38 : Toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable.

Définition 39 : Soit $\mathbb{L}/\mathbb{K}$. On dit que $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$ si $\mathbb{L}$ est algébrique sur $\mathbb{K}$ et $\mathbb{L}$ algébriquement clos.

[Goz]

Exemple 40 : (1) $\mathbb{C}$ est une clôture algébrique de $\mathbb{Q}$.
(2) L'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème 41 : (de Steinitz) (1) Tout corps commutatif $\mathbb{K}$ admet une clôture algébrique $\widetilde{\mathbb{K}}$.
(2) Si $\widetilde{\mathbb{K}}_1$ et $\widetilde{\mathbb{K}}_2$ sont deux clôtures algébriques de $\mathbb{K}$, alors il existe un $\mathbb{K}$-isomorphisme de $\widetilde{\mathbb{K}}_1$ dans $\widetilde{\mathbb{K}}_2$.

III] Corps finis

1] Existence et unicité des corps finis

XIII.4

Notation 42 : On note $\mathcal{U}_n(p)$ l'ensemble des polynômes unitaires, irréductibles de degré n sur $\mathbb{F}_p$.

Théorème 43 : $\forall P \in \mathcal{U}_n(p)$, $\mathbb{F}_p[X]/\langle P\rangle$ est une $\mathbb{F}_p$-algèbre de dimension n de base $(\overline{X}^k)_{k=0}^{n-1}$ et c'est un corps fini de cardinal p^n.

Exemple 44 : $\forall \lambda \in \mathbb{F}_p$, $X-\lambda \in \mathcal{U}_1(p)$ et $\mathbb{F}_p[X]/\langle X-\lambda\rangle$ est un corps isomorphe à $\mathbb{F}_p$.

[Rau]

XIII.4 [Rau]

Lemme 45 : Tout diviseur irréductible de $X^{p^n}-X$ dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, $\forall d|n$, $\forall P \in \mathcal{U}_d(p)$, $P \mid X^{p^n}-X$.

Théorème 46 : $X^{p^n}-X$ est sans facteurs carrés dans $\mathbb{F}_p[X]$ et

$$X^{p^n}-X = \prod_{d|n}\ \prod_{P\in\mathcal{U}_d(p)} P$$

Théorème 47 : À un isomorphisme près, il n'existe qu'un seul corps à p^n éléments $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/\langle P\rangle$ avec $P \in \mathcal{U}_n(p)$.

[Isen]

Proposition 48 : Soit $q=p^n$ et $S : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$, $Q \mapsto Q^q$.
Alors : S est un $\mathbb{F}_q$-endomorphisme de $\mathbb{F}_q[X]$.

Lemme 49 : Soit $\mathbb{L}$ extension de $\mathbb{F}_q$ et $x \in \mathbb{L}$.
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$.

Théorème 50 : Soit $q=p^n$, $P \in \mathbb{F}_q[X]$ sans facteurs carrés et $P = \prod_{i=1}^r P_i$ sa décomposition en irréductibles dans $\mathbb{F}_q[X]$.
Alors : (1) Si $r=1$, alors P est irréductible.
(2) Sinon, $\exists a \in \mathbb{F}_q \mid \exists V \in \mathbb{F}_q[X] \mid \mathrm{PGCD}(P, V-a)$ est facteur non-trivial de P.

2] Application aux polynômes cyclotomiques

[Per]

Définition 51 : On note $\mu_n = \{z\in\mathbb{C} \mid z^n = 1\}$ l'ensemble des racines n-ièmes de l'unité, $\mu_n^\times = \{z\in\mathbb{C} \mid \forall p\wedge n=1,\ p<n \Rightarrow z^p \neq 1 \text{ et } z^n=1\}$ l'ensemble des racines primitives n-ièmes de l'unité.
On appelle n-ième polynôme cyclotomique : $\Phi_n(X) = \prod_{\xi\in\mu_n^\times}(X-\xi)$

Théorème 52 : $X^n - 1 = \prod_{d|n}\Phi_d(X)$

Théorème 53 : Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$.

Références :

[Goz] Théorie de Galois – Gozard

[Ram] Mathématiques pour l'agrégation Algèbre et Géométrie – Ramsaldi

[Isen] L'oral à l'agrégation de mathématiques – Isenmann

[Per] Cours d'algèbre – Perrin