Extensions de corps
Exemples et applications

Tous les corps sont supposés commutatifs.

I Généralités

1) Définition et exemples

Déf : Soit E un corps. On appelle extension de corps de E un morphisme de corps $j : E \to F$ où F est un corps.

Rq : Un tel morphisme est injectif : pour $x \neq 0$ dans E, $j(x)\,j(1/x) = j(1) = 1 \neq 0$ donc $j(x) \neq 0$ par intégrité.
On peut écrire $\mathrm{Im}(j) \simeq F$. Désormais, on identifie F à $\mathrm{Im}(j)$ et l'extension $j : E \to F$ s'écrit $E \subseteq F$

Rq : L'extension $E \subseteq F$ est naturellement muni d'une structure de E-espace vectoriel.

Déf : Le degré de l'extension $E \subseteq F$ est la dimension de F comme E-espace-vectoriel. On la note $[F:E]$
On parle d'extension finie (resp. infinie) lorsque $[F:E] < +\infty$ (resp. $[F:E] = +\infty$)

Déf : Pour une extension donnée $E \subseteq G$, F est un corps intermédiaire pour $E \subseteq G$ si $E \subseteq F \subseteq G$.

Ex : 1/ $\mathbb{R} \subset \mathbb{C}$ est une extension finie de degré 2 ($(1,i)$ $\mathbb{R}$-base de $\mathbb{C}$)
2/ $\mathbb{Q} \subset \mathbb{R}$ est une extension infinie. Si $[\mathbb{R}:\mathbb{Q}] < +\infty$, $\mathbb{R}$ serait dénombrable comme $\mathbb{Q}$ ev de dim finie.
3/ Si E et F sont des corps finis, alors $|F| = |E|^{[F:E]}$
4/ $K \subset K(X)$ est une extension infinie.

2) Théorème de la base télescopique

Th : Soient $E \subseteq F$ et $F \subseteq G$ deux extensions de corps et soient $(e_i)_{i \in I}$ une E-base de F
$(f_j)_{j \in J}$ une E-base de G

Alors : • $E \subseteq G$ est une extension de corps tel que $(e_i f_j)_{(i,j) \in I \times J}$ est une E-base de G
• Si de plus, $[F:E]$ et $[G:F]$ sont finis, alors l'extension $E \subseteq G$ est finie et son degré vérifie :
$$\boxed{[G:E] = [G:F][F:E]} \quad \text{(multiplicativité du degré)}$$ (1)

Rq : La démonstration n'est pas difficile et pourtant ce théorème fournit un résultat de divisibilité très pratique.
On peut généraliser ce résultat à une suite finie d'extensions $E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$ où $n \in \mathbb{N}^*$: si $[E_i : E_{i-1}] < +\infty$ $\forall i \in [\![2,n]\!]$, alors $[E_n : E_1] = \prod_{i=2}^{n} [E_i : E_{i-1}]$

Application : Pour $p \in \mathcal{P}$ et $n \in \mathbb{N}$, les sous-corps de $\mathbb{F}_{p^n}$ sont les corps $\mathbb{F}_{p^d}$ où $d \mid n$.

3) Élément algébrique et polynôme minimal
C-L

Déf : Soient $E \subseteq F$ une extension de corps et $x \in F$.
L'élément x est algébrique sur E s'il existe un polynôme $P \in E[X]$ tel que P est non nul et $P(x) = 0$
Sinon l'élément x est dit transcendant sur E

Déf : L'extension $E \subseteq F$ est dite algébrique si tout élément de F est algébrique.

Ex : 1/ $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ (pour $\mathbb{Q} \subset \mathbb{R}$)
2/ $\sum_{n=0}^{+\infty} 10^{-n!}$ est transcendant sur $\mathbb{Q}$ selon le critère de Liouville
3/ Plus dur mais plus pertinent, e et π sont transcendants sur $\mathbb{Q}$ (2)

Rq : Bien qu'ils soient difficiles à trouver, il y a un nombre non dénombrable d'éléments transcendants sur $\mathbb{Q}$. En effet, nous savons déterminer (facilement) tous les nombres algébriques sur $\mathbb{Q}$ et $\{$Nb alg.$\} = \bigcup_{n \geq 1} \left(\bigcup_{P \in \mathbb{Q}_n[X]} Z(P) \right)$ est dénombrable.

Prop : Soit le morphisme d'anneaux $\varphi_x \left(\begin{array}{l} E[X] \to F \\ P \mapsto P(x) \end{array} \right)$ pour $x \in F$ fixé.
On définit $\mathrm{Im}(\varphi_x) = E[x]$.

Alors : • x transcendant $\Leftrightarrow \varphi_x$ injectif

Dans ce cas, $E(x)$ est une extension infinie de E.

• x algébrique $\Leftrightarrow \varphi_x$ non injectif

Dans ce cas, il existe un unique polynôme unitaire de degré minimal $\pi_x \in E[X]$ tel que $\pi_x(x) = 0$ et $(\pi_x) = \mathrm{Ker}(\varphi_x)$

Ce polynôme est irréductible et est appelé le polynôme minimal de x sur K. Enfin, $E[x]$ est une extension finie de E de degré $d°(\pi_x)$

Rq : $E(x) \simeq E[X]/(\pi_x)$ est donc un sous-corps de F où $E(x) = E[x]$ si x est algébrique.

Csq : Toute extension finie de corps est algébrique

L'ensemble de F des éléments algébriques de E est un sous-corps de F (en particulier, si x, y algébrique alors $x+y$, xy et $1/x$ pour $x \neq 0$ sont algébriques)

Ex : Pour $\mathbb{Q} \subset \mathbb{R}$, $\pi_{\sqrt{2}}(X) = X^2 - 2$ d'où $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

II Corps de décomposition et clôture algébrique

1) Corps de rupture

Def : Soient K un corps et P irréductible de degré ≥ 2.

Une extension L est un corps de rupture de P sur K si $\exists \alpha \in L$ tel que $P(\alpha) = 0$ et $L = K(\alpha)$

Rq : On veut une extension dans laquelle P admet au moins une racine

Prop : Pour $P \in K[X]$ irréductible, il existe un corps de rupture de P sur K unique à isomorphisme près.

Rq : On pourra considérer "le" corps de rupture de P : $K(\alpha) \simeq K[X]/(P)$

Si on ne spécifie pas la racine α de P, il y a plusieurs isomorphismes entre deux corps de rupture

Ppté : Dans $K(\alpha) = K[X]/(P)$, α est la classe de X : $\alpha = \overline{X}$

$[K(\alpha) : K] = d°(P)$ et $(1, \alpha, \dots, \alpha^{d°(P)-1})$ K-base de $K(\alpha)$

Ex : $\mathbb{C}$ est le corps de rupture de P où $P(X) = X^2 + 1$ sur $\mathbb{R}$

Appli : Si $q = p^n$, alors si $P \in \mathbb{F}_p[X]$ irréductible de degré n, on peut réaliser $\mathbb{F}_q$ comme le corps de rupture $\mathbb{F}_p[X]/(P)$

2) Corps de décomposition

Def : Soient K un corps et $P \in K[X]$ non scalaire de degré n et unitaire

Une extension L est un corps de décomposition de P sur K si $\exists (x_1, \dots, x_n) \in L^n$ tel que $P(X) = \prod_{i=1}^{n} (X - x_i)$ et tel que L est engendré par $(x_i)_{1 \leq i \leq n}$ comme extension : $L = K(x_1, \dots, x_n)$

Rq : Une définition équivalente est de dire que c'est un corps dans lequel P est scindé et qui est minimal pour cette propriété

Rq : On veut une extension dans laquelle P a toutes ses racines

Prop : Pour $P \in K[X]$, il existe un corps de décomposition de P sur K unique à isomorphisme près.

Rq : On peut le construire par une suite de corps de rupture pour obtenir toutes les racines une à une.

Ppté : On obtient alors $[K(x_1, \dots, x_n) : K] \mid n!$

Rq : Si P irréductible, "le" corps de décomposition peut être "le" corps de rupture mais il est souvent "plus gros".

Ex : Pour $K = \mathbb{Q}$ et $P(X) = X^3 - 2$: le corps $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(j, \sqrt[3]{2})$ est "le" corps de décomposition de P mais $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{2}, j)$ est "le" corps de rupture de P (prendre également $\mathbb{Q}(j\sqrt[3]{2})$)

Appli : Si $q = p^n$, on peut réaliser $\mathbb{F}_q$ comme le corps de décomposition de $P(X) = X^q - X$ sur $\mathbb{F}_p$.

3) Clôture algébrique

Def : Un corps K est algébriquement clos si tout polynôme non constant de $K[X]$ a une racine de K

Rq : Cela est équivalent à : "Tout polynôme est scindé sur K"

Ainsi, un corps algébriquement clos n'a pas d'extension algébrique sur K non triviale.

Def : Une clôture algébrique $\overline{K}$ de K est une extension algébrique sur K où $\overline{K}$ est un corps algébriquement clos

Th de Steinitz : • Tout corps admet une clôture algébrique
• Deux clôtures algébriques sont isomorphes

Th de d'Alembert-Gauss : $\mathbb{C}$ est algébriquement clos

Ex : $\mathbb{C} = \overline{\mathbb{R}}$ mais $\mathbb{C} \neq \overline{\mathbb{Q}}$ puisque e et π sont transcendants sur $\mathbb{Q}$!

$\mathbb{F}_{p^n}$ n'est pas algébriquement clos ($X^{p^n} - X + 1$ sans racine !) et admet $\bigcup_{k} \mathbb{F}_{p^{k!}}$ est "la" clôture algébrique de $\mathbb{F}_{p^n}$.

Per C-L

(6) ← Esc

C-L Cal

III Applications

1) Irréductibilité de polynômes

DEV1 Soit $q=p^l$, $p\in\mathcal{P}$ et $l\in\mathbb{N}$.
Soit $I_U(n,q)$ l'ensemble des polynômes unitaires de degré n irréductibles sur $\mathbb{F}_q$ et soit $I(n,q)=|I_U(n,q)|$. Alors

1/ $X^{q^n}-X=\prod_{d|n}\prod_{P\in I_U(d,q)} P$

2/ $I(n,q)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$ où μ désigne la fct. de Möbius

3/ $I(n,q)\geq 1$ pour tout $n\in\mathbb{N}^*$

4/ $I(n,q)\underset{n\to\infty}{\sim}\frac{q^n}{n}$

Lemme : $\mu\left(\begin{array}{l}\mathbb{N}^*\to\{0,\pm1\}\\ n\mapsto\mu(n)\end{array}\right)$ où $\mu(n)=\begin{cases}0 & \text{si } \exists p\in\mathcal{P} \text{ tq } p^2|n\\ 1 & \text{si } n=1\\ (-1)^r & \text{si } n=\prod_{i=1}^r p_i,\ p_i\neq p_j\end{cases}$

Pour $f:\mathbb{N}^*\to\mathbb{R}$ et si $g:\mathbb{N}^*\to\mathbb{R}$ tq $g(n)=\sum_{d|n}f(d)$
alors la 1° formule d'inversion de Möbius est vraie : $f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$

Rq : Voir $\mathbb{F}_q$ comme corps de rupture est possible.

Th : Soit $P\in K[X]$ irréductible de degré n et $K\subseteq L$ extension de degré m tq $m\wedge n=1$. Alors P irréductible sur L.

Ex : X^3+X+1 irréductible sur $\mathbb{Q}\Rightarrow$ irréductible sur $\mathbb{Q}(i)$

Th : Soit $P\in K[X]$ de degré $n>0$. Alors P irréductible sur K si et ssi P est sans racine dans toutes les extensions $K\subseteq L$ de degré $\leq\frac{n}{2}$.

Ex : X^4+1 est réductible dans $\mathbb{F}_p$, $\forall p\in\mathcal{P}$

2) Constructions à la règle et au compas

La définition d'un point constructible est rappelée oralement.

Déf : Un réel a est constructible s'il existe deux points constructibles M et N tel que $MN=|a|$

Prop : L'ensemble K des réels constructibles est un corps.
De plus, si $a\in K\cap\mathbb{R}_+$, $\sqrt{a}\in K$

Th de Wantzel : Le degré dans $\mathbb{Q}$ d'un réel constructible a est une puissance de 2 ie $[\mathbb{Q}(a):\mathbb{Q}]=2^k$, $k\in\mathbb{N}$

Th : Un réel a est constructible si et ssi $\exists(K_i)_{i\in[\![1,n]\!]}$ suite finie tq $K_{i+1}=K_i(a_{i+1})$ pour $i\in[\![1,n-1]\!]$ et $K_1=\mathbb{Q}(a_1)$ avec $[K_{i+1}:K_i]=2$ et $a\in K_n$.

Rq : Traduction algébrique d'un fait géométrique

Appli : La duplication du cube est impossible (puisque $\sqrt[3]{2}$ n'est pas constructible : $\pi_{\sqrt[3]{2}}(X)=X^3-2$ et $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$)
La quadrature du cercle est impossible (car π transcendant donc π et $\sqrt{\pi}$ non constructible)
La trisection de l'angle est impossible pour tout angle ($\frac{\pi}{3}$ n'est pas constructible)

Prop : Un point est constructible si et ssi ses coordonnées (dans un repère orthonormé) sont des réels constructibles

DEV2 : Si un polygône régulier à n côtés est constructible à la règle et au compas, alors n est de la forme $n=2^\alpha p_1\dots p_r$ où $\alpha\in\mathbb{N}$ et où les p_i sont des nombres premiers de Fermat (ie $p\in\mathcal{P}$ et $p=2^{2^k}+1$ où $k\in\mathbb{N}$)
Le pentagone régulier est constructible

Rq : La réciproque est vraie (appelé th. de Gauss) mais fait appel à la théorie de Galois qui est hors programme.

3) Un peu de théorie de Galois sans la nommer

Déf : Soit K un corps de caractéristique $p\in\mathcal{P}$.
L'application $F\left(\begin{array}{l}K\to K\\ x\mapsto x^p\end{array}\right)$ est appelé (morphisme de) Frobenius.

Prop : Si K est fini, F est un automorphisme

Prop : Soient les corps et l'extension $\mathbb{F}_q\subseteq\mathbb{F}_{q^n}$ où $q=p^l$, $p\in\mathcal{P}$ et $n\in\mathbb{N}^*$.
Alors le groupe des automorphismes de $\mathbb{F}_{q^n}$ qui laissent $\mathbb{F}_q$ invariant noté $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ est cyclique d'ordre n et est engendré par F.

Rq : En fait, $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ est le groupe de Galois de l'extension $\mathbb{F}_q\subseteq\mathbb{F}_{q^n}$

Coro : Le sous-corps $\mathbb{F}_{q^d}$ de $\mathbb{F}_{q^n}$ (où $d|n$) est l'ensemble des points fixes de $F^{n/d}$.

1) Démontrer avec les mains que $(\alpha_i \beta_j)$ base de G

2) Insister sur la difficulté de prouver qu'un élément est transcendant (surtout par rapport à prouver qu'un élément est algébrique !)

3) La théorie des anneaux ($K[X]$ anneau principal car K corps !) donne directement que π_x existe et son irréductibilité (idéaux principaux sont premiers !)

4) On va construire des extensions par adjonction de racines (à chaque fois on "augmente" le nombre de racines)

5) Exemples de $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1) \simeq \mathbb{R}(i)$
$Id \left(\begin{matrix} \mathbb{C} \longrightarrow \mathbb{C} \\ i \longmapsto i \end{matrix}\right) + \overline{Id} \left(\begin{matrix} \mathbb{C} \longrightarrow \mathbb{C} \\ i \longmapsto -i \end{matrix}\right)$

6) Dessiner la tour de corps de rupture

7) Par contraposée : si $P = QR$, on a $\deg(Q) = q < n$

$\Rightarrow$ $qm = ln$
$n \mid qm \underset{n \wedge m}{\Longrightarrow} n \mid q$ et $q < n$!

$$\begin{tikzcd} & L[X]/(Q) \arrow[dl, dash, "l"'] \arrow[dr, dash, "q"] & \\ K[X]/(P) \arrow[dr, dash, "n"'] & & L \arrow[dl, dash, "m"] \\ & K & \end{tikzcd}$$

8) Rappel def point constructible

9) $F^n = Id \Rightarrow \langle F \rangle \simeq \mathbb{Z}/n\mathbb{Z} < Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$
et $F^l \neq Id$, $l < n$

Or, $\mathbb{F}_{q^n}^*$ cyclique : $\mathbb{F}_{q^n} = \mathbb{F}_q(x)$
$\Rightarrow F^l(x) \neq F^k(x)$, $l \neq k$

– $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n \Rightarrow$ il y a au plus n auto car il y a n conjugués donné par les $F^k(x)$, $k \in [\![0, n-1]\!]$

Références :

[C-L] : Algèbre corporelle / Antoine CHAMBERT-LOIR

[Cal] : Extension de corps - théorie de Galois / Josette CALAIS

[Per] : Cours d'algèbre / Daniel PERRIN

[Aud] : Géométrie / Michèle AUDIN

[Car] : Théorie des corps - La règle et le compas / Jean-Claude CARREGA

[Esc] : Théorie de Galois / Jean-Pierre ESCOFIER

Dev 1 → Francinou Gianella 1 p°189 (+ Ramazanov pour l'interprétation)

Dev 2 → [Car] p°47 (+ Audin pour les défs et les dessins)