Leçon 125 : Extension de corps
Exemples et applications

Ouvrages : Perrin, Gozard

I - Généralités sur les corps

1) Premières définitions et propriétés

2) Extensions de corps

II - Extensions algébriques

1) Éléments algébriques et transcendants

2) Polynômes irréductibles

3) Cyclotomie

III - Adjonction de racines

1) Corps de rupture

2) Corps de décomposition

3) Clôture algébrique

IV - Extensions de corps finis

V - Constructions géométriques à la règle et au compas

DEV 1 : Irréductibilité de Φ_n + lemme

DEV 2 : Dénombrement des polynômes irréductibles de degré n sur $\mathbb{F}_q$ (avec la fonction de Möbius).

Leçon 125 : Extensions de corps. Exemples et applications

On considère des corps (souvent notés K, L) commutatifs.

I - Généralités sur les corps

1) Premières définitions, premiers exemples [PER] [GOZ]

PROP 1 : Soit A un anneau commutatif, $A \neq \{0\}$. Les assertions suivantes sont équivalentes :
- Les seuls idéaux de A sont $\{0\}$ et A
- Tout élément non nul de A est inversible.

DEF 2 : Si A vérifie ces conditions, on dit que A est un corps

EX 3 : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps, $\mathbb{Z}$ n'est pas un corps

PROP 4 : Soit A un anneau commutatif, I un idéal de A :
I est un idéal maximal de $A \Leftrightarrow A/I$ est un corps.

PROP 5 : Un corps est intègre

PROP 6 : Si K est un corps, $K^* = \{x \in K, x \neq 0\}$ est un groupe appelé groupe des inversibles de K.

peut être remplacé par les [illegible]

DEF 7 : Soient A, B deux anneaux commutatifs et $f : A \to B$. On dit que f est un morphisme d'anneaux lorsque
$\cdot f(1_A) = 1_B$, $\forall x, y \in A$, $f(x+y) = f(x) + f(y)$, $f(xy) = f(x) f(y)$.
On parle de morphismes de corps lorsque $A = L_1$, $B = L_2$ sont des corps. On parle de K-morphisme lorsque $K \subset L_1$, $K \subset L_2$ et $f_{|K} = Id$.

REM 8 : Un morphisme de corps est injectif

EX 9 : $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$

2) Extensions de corps [PER]

DEF 10 : Soient K, L des corps. Lorsque $K \subset L$, on parle d'extension de corps et on la note L/K.

EX 11 : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; $\mathbb{R} \subset \mathbb{R}(T)$

DEF 12 : On appelle degré de l'extension L/K la dimension de L en tant que K-espace vectoriel. On la note $[L:K]$.

REM 13 : Si $[L:K] = n$, on a $L \simeq K^n$ → utile pour les corps finis.

THM 14 (de la base télescopique) : Soient $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ une K-base de L, $(f_j)_{j \in J}$ une L-base de M. Alors $(e_i f_j)_{(i,j) \in I \times J}$ est une K-base de M

COR 15 : Si les degrés sont finis, on a l'égalité : $[M:K] = [M:L][L:K]$ qui permet de faire des raisonnements arithmétiques.

DEF 16 : Soit L/K une extension et $A \subset L$. On dit que A engendre L sur K et on écrit $L = K(A)$ lorsque L est le plus petit sous-corps de L qui contient A et K. Si $A = \{a_1, \dots, a_n\}$, on note $L = K(a_1, \dots, a_n)$.

II - Extensions algébriques

1) Éléments algébriques et transcendants [PER]

DEF 17 : Soit L/K une extension et $\alpha \in L$. Soit $\varphi : K[T] \to L$ défini par $\varphi_{|K} = Id_K$ et $\varphi(T) = \alpha$.
- Si φ est injectif, on dit que α est transcendant sur K
- Sinon, on dit que α est algébrique sur K. Le générateur (unitaire) de l'idéal $\ker(\varphi)$ est appelé polynôme minimal de α et noté μ_α.

EX 18 : Les nombres $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ et $\mu_{\sqrt{2}} = X^2 - 2$, $\mu_i = X^2 + 1$, $\mu_{\sqrt[3]{2}} = X^3 - 2$.
Les nombres e et π sont transcendants sur $\mathbb{Q}$ (ADMIS).

THM 19 : Soit L/K une extension et $\alpha \in L$. Les assertions suivantes sont équivalentes.
- α est algébrique sur K
- $K[\alpha] = K(\alpha)$
- $[K(\alpha) : K] < \infty$,

De plus, dans ce cas, μ_α est irréductible et $[K(\alpha):K] = \deg(\mu_\alpha)$.

DEF 20 : Lorsque $[L:K] < \infty$, on dit que L/K est finie, lorsque $\forall \alpha \in L$, α est algébrique sur K, on dit que L/K est algébrique.

PROP 21 : Toute extension finie est algébrique

THM 22 : Soit L/K une extension, $M = \{x \in L \mid x \text{ algébrique sur } K\}$. Alors M est un sous-corps de L.

EX 23 : $\sqrt[3]{5} + \sqrt[3]{7}\sqrt[5]{3}$ est algébrique sur $\mathbb{Q}$

2) Polynômes irréductibles [GOZ]

DEF 24 : Soit A un anneau commutatif, $P \in A[X]$. On dit que P est irréductible lorsque $P \notin A[X]^\times (= A^\times)$ et $P = AB \Rightarrow A \in A[X]^\times$ ou $B \in A[X]^\times$. [PER]

PROP 25 : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, $a_n \neq 0$, $a_0 \neq 0$. Soit $\alpha \in \mathbb{Q}$, $\alpha = \frac{p}{q}$, $p \wedge q = 1$ tq $P(\alpha) = 0$. Alors $q \mid a_n$ et $p \mid a_0$.

THM 26 : (Critère d'Eisenstein) Soit A un anneau factoriel et $K = \mathrm{Frac}(A)$ son corps des fractions. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, $n \geq 1$. On suppose qu'il $\exists\, p$ irréductible dans A (donc premier) tel que $p \nmid a_n$, $\forall k \in [\![0; n-1]\!]$, $p \mid a_k$ et $p^2 \nmid a_0$. Alors P est irréductible dans $K[X]$.

EX 27 : $\forall n \in \mathbb{N}$, $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.

DEF 28 : Soit A un anneau factoriel. Soit $P \in A[X] \setminus \{0\}$, on appelle contenu de P et on note $c(P)$ le PGCD des coefficients de P. On dit que P est primitif lorsque $c(P) = 1$.

THM 29 : Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$. Soit $P \in A[X]$, $\deg(P) \geq 1$. P est irréductible dans $A[X]$ si et seulement s'il l'est dans $K[X]$ et $c(P) = 1$.

THM 30 : Soit $P \in \mathbb{Z}[X]$, $\deg(P) \geq 1$, P unitaire. S'il existe p premier tel que P est irréductible dans $\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.

EX 31 : $X^3 - 7X + 3$ est irréductible dans $\mathbb{F}_2[X]$ donc dans $\mathbb{Z}[X]$.

3) Cyclotomie [PER]

DEF 32 : Soit K corps et $n \in \mathbb{N}^*$ tel que $\mathrm{car}(K) \nmid n$. On note $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité i.e. racines de $P_n(X) = X^n - 1$.

DEF 33 : Une racine n-ième primitive de l'unité est un élément $\zeta \in K$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. C'est un élément de μ_n d'ordre exactement n. On note $\mu_n^*(K)$ l'ensemble des racines n-ièmes primitives de l'unité.

DEF 34 : On définit le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\zeta \in \mu_n^*(K)} (X - \zeta)$, $\forall n \in \mathbb{N}^*$.

PROP 35 : On a Φ_n unitaire et $\deg(\Phi_n) = \varphi(n)$ $\forall n \in \mathbb{N}^*$. De plus $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$, φ désigne l'indicatrice d'Euler.

PROP 36 : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

EX 37 : $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_5 = X^4 + X^3 + X^2 + X + 1$

PROP 38 : En prenant les degrés dans l'égalité donnée par PROP 35, on a $n = \sum_{d \mid n} \varphi(d)$

DEV 1 [GOZ]

PROP 39 : Soient $P, A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P \in \mathbb{Z}[X]$, que $P = AB$ et que P et A sont unitaires. Alors A et B sont dans $\mathbb{Z}[X]$.

THM 40 : $\forall n \in \mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Q}[X]$.

COR 41 : Soit $n \in \mathbb{N}^*$ et ζ une racine primitive n-ième de l'unité, alors ζ est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

III - Adjonction de racines

1) Corps de rupture [PER]

DEF 42 : Soit K un corps, $P \in K[X]$ irréductible. Une extension L/K est appelée corps de rupture de P sur K lorsque $L = K(\alpha)$ avec $P(\alpha) = 0$.

EX 43 : $\mathbb{Q}(\sqrt[3]{2})$ pour $X^3 - 2$; $\mathbb{Q}(i)$ pour $X^2 + 1$.

THM 44 : Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

THM 45 : Soit $P \in K[X]$ irréductible de degré n et L/K une extension, $[L:K] = m$ et $n \wedge m = 1$. Alors P est encore irréductible sur L.

EX 46 : $X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.

2) Corps de décomposition [PER]

DEF 47 : Soit $P \in K[X]$, $\deg(P) = n$. On appelle corps de décomposition de P sur K une extension L de K telle que :
- Dans $L[X]$, P est produit de facteurs de degré 1
- Le corps est minimal pour cette propriété (les racines de P engendrent L).

THM 48 : Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près. On le note $D_K(P)$.

EX 49 : $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, j)$; $D_{\mathbb{Q}}(X^4 - 2) = \mathbb{Q}(\sqrt[4]{2}, i)$.

3) Clôture algébrique

PROP 50 : Soit K un corps. Les assertions suivantes sont équivalentes :
(1) Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K
(2) Tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine dans K
(3) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1
(4) Toute extension algébrique de K est identique à K.

DEV 2

DEF 51: On dit alors que K est algébriquement clos.

EX 52: $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos

PROP 53: Tout corps algébriquement clos est infini.

THM 54: Le corps $\mathbb{C}$ est algébriquement clos.

DEF 55: Soit L/K une extension. On dit que L est une clôture algébrique de K si et seulement si L est algébrique sur K et L est algébriquement close.

THM 56 (Steinitz): • Tout corps commutatif admet une clôture algébrique $\tilde{K}$.
• Si $\tilde{K}_1$ et $\tilde{K}_2$ sont deux clôtures algébriques de K, alors il existe un K-isomorphisme de $\tilde{K}_1$ sur $\tilde{K}_2$. (ADMIS).

IV - Extensions de corps finis [PER] [GOZ]

THM 57: Soit F un corps fini. Alors il existe $p \in \mathbb{N}$ premier tel que F soit un $\mathbb{F}_p$-espace vectoriel. Donc $\#F = p^n$ avec $n \in \mathbb{N}$.

THM 58: Soit $p \in \mathbb{N}^*$ premier, $n \in \mathbb{N}^*$, $q = p^n$. Alors :
• Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.
• En particulier, K est unique, à isomorphisme près. On le note $\mathbb{F}_q$.

EX 59: $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$.

THM 60: On a l'inclusion $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \Leftrightarrow d \mid n$

EX 61: On a le treillis des corps finis de caractéristique 2 :

$$\begin{tikzcd}
 & \mathbb{F}_{64} & \mathbb{F}_{16} \\
\mathbb{F}_8 \arrow[ur, dash] & & \mathbb{F}_4 \arrow[u, dash] \arrow[ul, dash] \\
 & \mathbb{F}_2 \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

DEF 62: On définit $\mu : \mathbb{N}^* \to \{0; 1; -1\}$ la fonction de Möbius par $\mu(1) = 1$, $\mu(n) = 0$ si n contient un facteur carré et $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \dots, p_r$ sont des nombres premiers distincts.

PROP 63: $\forall n \geq 2, \sum_{d \mid n} \mu(d) = 0$ [FRA 1]

THM 64: Soit $g : n \in \mathbb{N}^* \mapsto \sum_{d \mid n} f(d)$, alors $\forall n \geq 1$,
$f(n) = \sum_{d \mid n} \mu(\frac{n}{d}) g(d) = \sum_{d \mid n} \mu(d) g(\frac{n}{d})$.

THM 65: On note $A(n,q)$ l'ensemble des polynômes ~~irréductibles~~ de $\mathbb{F}_q[X]$ irréductibles unitaires de degré n, $I(n,q) = \#A(n,q)$
$$X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P(X)$$

THM 66: On a $I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu(\frac{n}{d}) q^d$, $I(n,q) \sim \frac{q^n}{n}$.

V - Constructions géométriques à la règle et au compas [GOZ]

Soit P un plan affine euclidien orienté, $\mathcal{R} = (O, \vec{i}, \vec{j})$ un repère orthonormé direct.

DEF 67: Soit $X \subset P$, $\#X \geq 2$. On dit que $M = (x,y) \in P$ est constructible en un pas à partir de X lorsque M est un point d'intersection soit de deux droites, soit de deux cercles, soit d'une droite et d'un cercle.

PROP 68: Soit $x \in \mathbb{R}$. $(x,0)$ est constructible si et seulement si $(0,x)$ est constructible.

DEF 69: Lorsque $(x,0)$ (ou $(0,x)$) est constructible, on dit que x est constructible.

PROP 70: • Tout élément de $\mathbb{Q}$ est constructible.
• $M = (x,y)$ est constructible ssi x et y le sont.

THM 71 (Wantzel): Soit $t \in \mathbb{R}$, t est constructible si et seulement si il existe $(L_0, \dots, L_p)$ une suite finie de sous-corps telle que $L_i \subset L_{i+1}$ $\forall i \in [\![1; p]\!]$ et :
• $L_0 = \mathbb{Q}$
• $\forall i \in [\![0; p-1]\!]$, $[L_{i+1} : L_i] = 2$
• $t \in L_p$.

COR 72: Si x est constructible, $\exists e \in \mathbb{N}$, $[\mathbb{Q}(x) : \mathbb{Q}] = 2^e$

APPLICATION 73: • Impossibilité de la quadrature du cercle : $\sqrt{\pi}$ n'est pas constructible (car transcendant)
• Impossibilité de la duplication du cube car $\sqrt[3]{2}$ n'est pas constructible.