

12 Leçon 125 : Extensions de corps. Exemples et applications.

I. Extension de corps

1. Généralités [PER]

Extension, degré de l'extension, théorème de la base télescopique, extension engendrée

2. Eléments et extensions algébriques [PER]

Eléments algébriques/transcendants, polynôme minimal, lien avec $K[\alpha]$ et $K(\alpha)$, extension finie, extension algébrique, corps des éléments algébriques

II. Extension de corps et polynômes

1. Corps de rupture [PER]

Corps de rupture, existence et unicité, exemple, contre-exemple scindé

2. Corps de décomposition [PER]

Corps de décomposition, existence et unicité, exemple

3. Clôture algébrique [GOZ]

Corps algébriquement clos, exemples, clôture algébrique, exemples

III. Corps particuliers

1. Corps finis [PER]

Sous-corps premier, caractéristique, morphisme de Frobenius, **DEV 1 : existence et unicité des corps finis**, construction de $\mathbb{F}_4$, inclusion des corps finis, cyclicité du groupe multiplicatif

2. Extensions cyclotomiques [GOZ] [PER]

Racines n -ièmes de l'unité, racines primitives n -ièmes de l'unité, corps cyclotomique, polynômes cyclotomiques et prop

DEV 2 : Irréductibilité de $\Phi_n(X)$ + polynôme minimal d'une racine primitive n -ième de l'unité

Intersection d'extensions, théorème de Dirichlet faible

Présentation :

- Le théorème de la base télescopique est crucial, car permet en pratique de trouver le degré d'une extension.
- Les corps de rupture permettent de passer d'un corps où le polynôme était irréductible, à un corps où celui-ci admet une racine. Cependant, il arrive que le polynôme ne soit toujours pas complètement scindé (il manque des racines dans le corps de rupture). On considère alors le corps de décomposition.
On aboutit alors aux corps algébriquement clos, ceux où tout polynôme est scindé.
- Se placer dans un corps plus grand contenant les racines d'un polynôme donné est une méthode très utile. On peut par exemple démontrer le théorème de Cayley-Hamilton en se plaçant dans un corps de décomposition du polynôme caractéristique.
- Les polynômes cyclotomiques sont directement définis à partir de leurs racines. Ces polynômes ont de nombreuses propriétés, et permettent de créer de nouvelles extensions de corps.

Développements :

- Existence et unicité des corps finis
 - Théorie de Galois, Gozard, p85
 - Algèbre Tome 4, Szpirglas, p85
- Irréductibilité des polynômes cyclotomiques + degré d'une extension cyclotomique
 - Théorie de Galois, Gozard, p69
 - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p384
 - Cours d'algèbre, Perrin, p80

Références :

- [PER] Cours d'algèbre, Perrin
- [GOZ] Théorie de Galois, Gozard

Leçon 125: Extension de corps. Exemples et applications

Tous les corps sont supposés commutatifs. Soit K, L, M des corps.

I Extension de corps

1) Généralités [PER]

Def 1: On dit que L est une extension de corps de K , notée L/K , lorsque $K \subset L$.

Exemple 2: $\mathbb{Q}$ est une extension de $\mathbb{R}$, $\mathbb{R}(x)$ est une extension de $\mathbb{R}$.

Prop 3: Si L/K extension de corps, L est un K -espace vectoriel.

Def 4: On appelle degré de l'extension L/K la dimension de L comme K -espace vectoriel. On la note $[L:K]$.

Remarque 5: On a donc $L \cong K^m$ si $m = [L:K] < +\infty$

Théorème 6 (de la base télescopique): Soit L/K et M/L des extensions de corps. Soit $(e_i)_{i \in I}$ une base de L sur K et $(f_j)_{j \in J}$ une base de M sur L . Alors la famille $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K .

Corollaire 7: Si les extensions sont finies, on a:

$$[M:K] = [M:L] \cdot [L:K].$$

Def 8: 1) Soit L/K une extension et A une partie de L . On dit que A engendre L sur K , notée $L = K(A)$, si L est le plus petit sous-corps de L contenant K et A .
Si $A = \{d_1, \dots, d_n\}$, on note $L = K(d_1, \dots, d_n)$.

2) On dit que L/K est menagène si $L = K(d)$ avec $d \in L$.

Notation 9: Si L/K est une extension et $d \in L$, on note $K[d]$ le sous-corps de L engendré par K et d .
On a $K[d] \subset K(d)$.

2) Eléments et extensions algébriques [PER]

Def 10: Soit L/K et $d \in L$. Soit $\ell: K[x] \rightarrow L$ le morphisme d'évaluation en d : $\ell(P(x)) = P(d) \forall P \in K[x]$.

1) Si ℓ est injectif, on dit que d est transcendant sur K .
2) Sinon, on dit que d est algébrique sur K . Ainsi il existe $P \in K[x]$ non nul tel que $P(d) = 0$.

Def 11: Si d algébrique sur K , il existe P non nul tel que $\ker(\ell) = (P)$, et on peut supposer P unitaire. On dit que P est le polynôme minimal de d sur K . Il est irréductible dans $K[x]$.

Exemple 12: 0 et π sont transcendents sur $\mathbb{Q}$, mais pas sur $\mathbb{R}$.

• $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, le polynôme minimal $x^2 - 2$.

• i est algébrique sur $\mathbb{Q}$, le polynôme minimal $x^2 + 1$.

Prop 13: Si d est transcendant, on a $K[d] \cong K[x]$ et $K(d) \cong K(x)$.

Théorème 14: Soit L/K extension et $d \in L$. On a équivalences:

1) d est algébrique sur K

$$2) K[d] = K(d)$$

$$3) [K(d):K] < +\infty.$$

Si P est le polynôme minimal de d sur K , on a $[K(d):K] = \deg(P)$. Cet entier s'appelle le degré de d .

Exemple 15: $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

Def 16: Soit L/K une extension

1) On dit que L/K est finie si $[L:K] < +\infty$

2) On dit que L/K est algébrique si pour tout $d \in L$, d est algébrique sur K .

Prop 17: Toute extension finie est algébrique.

Théorème 28: Soit L/K extension. On pose $M = \{x \in L; x \text{ est algébrique sur } K\}$. Alors M est un sous corps de L .
Contre-ex 19: Soit $\overline{\mathbb{Q}} = \{x \in \mathbb{C}; x \text{ algébrique sur } \mathbb{Q}\}$. Alors $\overline{\mathbb{Q}}$ est un corps algébrique sur $\mathbb{Q}$, mais $\overline{\mathbb{Q}}/\mathbb{Q}$ est de degré infini car il existe des éléments de $\overline{\mathbb{Q}}$ de degré arbitrairement grands.

II Extension de corps et polynômes

1) Corps de rupture [PER]

Déf 20: Soit $P \in K[X]$ un polynôme irréductible. Une extension L/K est appelée corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

Théorème 27: Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K , qui est unique à isomorphisme près.

Exemple 22: $\mathbb{Q} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1 sur $\mathbb{R}$.
 $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{R}[X]/(X^3-2)$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$.

Contre-ex 23: Si L est un corps de rupture de P , P n'est pas forcément scindé sur L . Prendre $K = \mathbb{Q}$ et $P(X) = X^3 - 2$. Alors P n'est pas scindé dans $L = \mathbb{Q}(\sqrt[3]{2})$.

2) Corps de décomposition [PER]

Déf 24: Soit $P \in K[X]$ de degré n . On appelle corps de décomposition de P sur K une extension L de K tel que:

- 1) P est scindé dans L
- 2) L est minimal pour cette propriété (L est engendré par les racines de P).

Théorème 25: Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K , unique à isomorphisme près.

On le note $D_K(P)$.

Exemple 26: Pour $K = \mathbb{Q}$, $P(X) = X^3 - 2$, $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.
 Pour $K = \mathbb{Q}$, $P(X) = X^4 - 2$, $D_K(P) = \mathbb{Q}(\sqrt[4]{2}, i)$

3) Clôture algébrique [G02]

Prop 27: On a équivalence entre:

- 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.

Déf 28: On dit alors que K est algébriquement clos.

Exemples 29: $\mathbb{C}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

Prop 30: Tout corps algébriquement clos est infini.

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

Déf 32: Soit L/K extension. On dit que L est une clôture algébrique de K si:

- 1) L est algébrique sur K .
- 2) L est algébriquement clos.

Exemple 33: $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
 $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème 34 (de Steinitz) Admis: Tout corps K admet une clôture algébrique, unique à K-isomorphisme près.

III Corps particuliers

1) Corps finis [PER]

Déf 35: On appelle sous-corps premier de K le plus petit sous corps de K

Def 36: Soit $\ell: \mathbb{Z} \rightarrow K$, $n \mapsto n \cdot 1_K$. Alors $\text{Ker}(\ell) = p\mathbb{Z}$. Le nombre p est appelé la caractéristique du corps K . Il est nul ou est un nombre premier. On la note $\text{car}(K)$.

Remarque 37: 1) Si $\text{car}(K) = 0$, $\mathbb{Q}$ est le sous-corps premier de K .
2) Si K est fini, le sous-corps premier de K est $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
De plus, son cardinal est une puissance de p .

Corollaire 38: Il n'y a pas de corps de cardinal 6.

Prop 39: Soit $\text{car}(K) = p > 0$. L'application

$F: K \rightarrow K$ est un morphisme de corps appelé morphisme de Frobenius

Si K est fini, c'est un automorphisme.

Si $K = \mathbb{F}_p$, c'est l'identité.

Théorème 40: Soit p premier et $n \in \mathbb{N}^*$. On pose $y = p^n$. Alors il existe un corps à y éléments, c'est le corps de décomposition du polynôme $X^y - X$ sur $\mathbb{F}_p$.
Il est unique à isomorphisme près, et est noté $\mathbb{F}_y$.

Exemple 41: On peut construire $\mathbb{F}_4$ de deux manières:

- Comme le corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$.
- Avec l'isomorphisme $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$.

Prop 42: On a: $\mathbb{F}_p \subset \mathbb{F}_{p^n} \iff n \mid m$.

Théorème 43: Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

2) Corps cyclotomiques [602][PER]

Def 44: Soit $n \in \mathbb{N}^*$. On pose $\mathbb{U}_n = \{z \in \mathbb{C}; z^n = 1\}$ l'ensemble des racines n -ièmes de l'unité. C'est un groupe cyclique d'ordre n .

Def 45: On appelle racine primitive n -ième de l'unité tout générateur de $\mathbb{U}_n$, c'est tout élément ξ de $\mathbb{U}_n$ tel que $\xi^d \neq 1 \forall d < n$. On note $\mathbb{U}_n^*$ cet ensemble, qui a

pour cardinal $\varphi(n)$ où φ est l'indicatrice d'Euler.

Def 46: On appelle corps cyclotomique d'indice n tout corps de la forme $\mathbb{Q}(\xi)$ avec $\xi \in \mathbb{U}_n^*$.

Def 47: Soit $n \in \mathbb{N}^*$. On appelle n -ième polynôme cyclotomique le polynôme: $\Phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$.

Remarque 48: Φ_n est unitaire et de degré $\varphi(n)$.

Lemme 49: On a: $\mathbb{U}_n = \bigcup_{d \mid n} \mathbb{U}_d^*$

Prop 50: On a la formule: $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Corollaire 51: On a: $n = \sum_{d \mid n} \varphi(d)$

Exemple 52: $\Phi_1(X) = X - 1$ $\Phi_2(X) = X + 1$

$\Phi_3(X) = X^2 + X + 1$ $\Phi_4(X) = X^2 + 1$

Corollaire 53: Si p est premier:

$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1$

Prop 54: $\forall n \in \mathbb{N}^*$, $\Phi_n(X) \in \mathbb{Z}[X]$

Lemme 55: Soit $p, a \in \mathbb{Q}[X]$ non nuls. On suppose que $p \mid a$ dans $\mathbb{Z}[X]$, et que p et a sont unitaires. Alors p et a sont dans $\mathbb{Z}[X]$.

Théorème 56: $\forall n \in \mathbb{N}^*$, $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$.

Corollaire 57: Si $\xi \in \mathbb{U}_n^*$, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_n(X)$, donc $[\mathbb{Q}(\xi): \mathbb{Q}] = \varphi(n)$.

Corollaire 58: Soit $d \in \mathbb{U}_n^*$ et $d' \in \mathbb{U}_n^*$ avec $\text{pgcd}(m, n) = 1$. Alors: $\mathbb{Q}(d) \cap \mathbb{Q}(d') = \mathbb{Q}$.

Théorème 59 (de Dirichlet faible): Soit $n > 1$. Alors il existe une infinité de nombres premiers p vérifiant: $p \equiv 1 \pmod{n}$.