

11 Leçon 123 : Corps finis. Applications.

I. Généralités sur les extensions de corps [PER]

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

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

Corps de décomposition, exemple, existence et unicité

II. Corps finis

1. Construction des corps finis [PER] [GOZ]

Sous-corps premier, caractéristique, morphisme de Frobenius, petit théorème de Fermat, DEV 1 : existence et unicité des corps finis

2. Eléments de structure [ULM] [PER] [GOZ]

Inclusion des corps finis, exemple, cyclicité de $\mathbb{F}_q^*$, autre construction de $\mathbb{F}_q$, corps de rupture = corps de décomposition pour les corps finis

3. Carrés dans un corps fini [PER]

Toutes les propriétés des carrés dans $\mathbb{F}_q$

III. Application à l'irréductibilité de polynômes [PER] [GOZ]

Critère d'Eisenstein, deux exemples, réduction modulo p , propriété avec les extensions de degré inférieur ou égal à $\frac{n}{2}$, racines primitives n -ièmes de l'unité, polynômes cyclotomiques, propriétés,

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

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.
- La question principale de cette leçon est de se demander si pour tout entier n il existe un corps à n éléments.
- Pour construire $\mathbb{F}_q$ où $q = p^n$, on a deux manières : soit passer par le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$, soit passer par le corps de rupture d'un polynôme $P \in \mathbb{F}_p[X]$ irréductible et de degré n sur $\mathbb{F}_p$.

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
- [ULM] Anneaux-corps-résultants, Ulmer

Selon 123: Corps finis. Applications

I Généralités sur les extensions de corps [PER]

Soit K, L, M des corps commutatifs

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

Prop 2: Si K est un sous-corps de L , L est un K -espace vectoriel.

Def 3: Si $\dim_K(L)$ est finie, on pose $[L:K] = \dim_K(L)$ que l'on appelle degré de L sur K .

Remarque 4: Si K et L sont des corps finis, on a $[L:K] = |K|^n$ avec $n = [L:K]$.

Théorème 5 (de la base télescopique): Soit $K \subset L \subset M$.

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 6: Si les degrés sont finis, on a: $[M:K] = [M:L] \times [L:K]$.

Def 7: Soit L/K extension et A une partie de L . On dit que A engendre L sur K et on écrit $L = K(A)$ si L est le plus petit sous-corps de L contenant K et A .
L'extension L/K est dite monogène si il existe $d \in L$ tel que $L = K(d)$.

Def 8: 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 $L = K(L)$ avec $P(L) = 0$.

Exemple 9: Le corps $\mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1 sur $\mathbb{R}$.

Théorème 10: Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K , unique à isomorphisme près.

Centre-ex 11: Si L est un corps de rupture de P , P n'est

pas forcément scindé sur L . Par exemple si $K = \mathbb{Q}$ et $P(X) = X^3 - 2$ alors $L = \mathbb{Q}(\sqrt[3]{2})$ n'est pas une racine de P ($\sqrt[3]{2}$ et $\sqrt[3]{2}\omega$ et $\sqrt[3]{2}\omega^2$) ne sont pas dans L .

Def 12: 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 $L[X]$

2) Les racines de P engendrent L .

Exemple 13: Pour $K = \mathbb{Q}$ et $P(X) = X^3 - 2$, son corps de décomposition est $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

Théorème 14: Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K . Il est unique à isomorphisme près.

II Corps finis

1) Construction des corps finis [PER][602]

Def 15: Soit K un corps. On appelle sous-corps premier de K le plus petit sous-corps de K .

Def 16: Soit $\ell: \mathbb{Z} \rightarrow K$ le morphisme d'anneaux tel que $\ell(n) = n \cdot 1_K$. Alors $\text{Ker}(\ell) = p\mathbb{Z}$.

Le nombre p est appelé la caractéristique du corps K . Elle vaut 0 ou un nombre premier. On la note $\text{car}(K)$.

Remarque 17: 0 Si $\text{car}(K) = 0$, K est infini et $\mathbb{Q}$ est le sous-corps premier de K .

Si K est fini, $\text{car}(K) = p > 0$ et le sous-corps premier de K est $\mathbb{Z}/p\mathbb{Z}$, noté $\mathbb{F}_p$.

Prop 18: Si K est fini, $\text{car}(K) = p > 0$ et $q = |K| = p^n$. Le cardinal d'un corps fini est une puissance de sa caractéristique.

Exemple 19: Il n'y a pas de corps de cardinal 6.

Prop 20: Soit K un corps de caractéristique $p > 0$.

L'application $F: K \rightarrow K$ définie par $F(a) = a^p$

est un morphisme de corps appelé morphisme de Frobenius.
 $\hookrightarrow K$ est fini, c'est un automorphisme.
 $\hookrightarrow K$ est $\mathbb{F}_p$, c'est l'identité.

Corollaire 21 (petit théorème de Fermat): Soit p premier.
 Alors: $\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}$.

Théorème 22: Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$. Alors il existe un corps fini à q éléments, il est corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$. Il est unique à $\mathbb{F}_p$ -isomorphisme près, et est noté $\mathbb{F}_q$. DEV 1

Corollaire 23: Le produit des éléments de $\mathbb{F}_q^*$ est égal à -1 .

2) Éléments de structure [ULM][VER][602]

Prop 24: Soit $d, n \in \mathbb{N}^*$. On a: $\mathbb{F}_p \subset \mathbb{F}_{p^n} \iff d \mid n$.

Exemple 25: Les sous-corps de $\mathbb{F}_{2^4}$ sont: $\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^4}$.
 $\mathbb{F}_{2^4}, \mathbb{F}_{2^2}$

Théorème 26: Soit $q = p^n$. Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Théorème 27: Soit $q = p^n$. Alors $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$. DEV 1

Corollaire 28: Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[x]$

Corollaire 29: Soit π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors π divise $x^{p^n} - x$ sur $\mathbb{F}_p[x]$ (car est stable sur $\mathbb{F}_p$: son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(\pi)$ est aussi son corps de décomposition).

Exemples 30: Il y a un unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$: $x^2 + x + 1$.
 Il y a 2 polynômes irréductibles de degré 3 sur $\mathbb{F}_2$:
 $x^3 + x + 1$ et $x^3 + x^2 + 1$.

3) Carrés dans un corps fini [VER]

Notation 31: Soit $q = p^n$. On pose $\mathbb{F}_q^* = \{x \in \mathbb{F}_q; \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^* \cap \mathbb{F}_q^*$.

Prop 32: Pour $p=2$, $\mathbb{F}_q^* = \mathbb{F}_q$.
 Pour $p>2$, $|\mathbb{F}_q^*| = \frac{q-1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Prop 33: Soit $p>2$. Alors on a:
 $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$

Exemple 34: 2 est un carré dans $\mathbb{F}_7$ mais pas 3.

Corollaire 35: -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \pmod{4}$ (avec $p>2$).

Application 36: Il existe une infinité de nombres premiers de la forme $4n+1$.

III Application à l'irréductibilité de polynômes [VER][602]

Théorème 37 (critère d'Eisenstein): Soit A un anneau factoriel et $K = \text{Frac}(A)$. Soit $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$. Soit $p \in A$ irréductible. On suppose que:

1) $p \nmid a_n$ 2) $\forall i \in \{0, \dots, n-1\}, p \mid a_i$ 3) $p^2 \nmid a_0$.

Alors P est irréductible dans $K[X]$ (et dans $A[X]$) si P est primitif.

Application 38: Avec $X^n - 2 \in \mathbb{Z}[X]$, on voit qu'il existe des polynômes irréductibles de tout degré sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Application 39: Soit $\phi_p(x) = x^{p-1} + \dots + x + 1$. Alors

Φ_p est irréductible sur $\mathbb{Z}$.

Théorème 40 (réduction modulo p): Soit A un anneau intègre et $K = \text{Frac}(A)$. Soit I un idéal premier de A et $\bar{p} = A/I$. Soit $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$ et $\bar{P}$ sa réduction modulo I . On suppose que $\bar{a}_n \neq 0$. Alors si $\bar{P}$ est irréductible sur $\bar{p}$, P est irréductible sur K .

Exemple 41: $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$.

Théorème 42: Soit $P \in \mathbb{C}[X]$ de degré $n > 0$. Alors P est irréductible sur $\mathbb{C}$ si et seulement si P n'a pas de racines dans les extensions K de $\mathbb{C}$ qui vérifient $[K:\mathbb{C}] \leq \frac{n}{2}$.

Contre-ex 43: Le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{F}_p$ pour tout p premier.

Déf 44: Soit $n \in \mathbb{N}^*$, on pose $\mathcal{U}_n = \{z \in \mathbb{C}; z^n = 1\}$ l'ensemble des racines n -ièmes de l'unité.

On appelle racine primitive n -ième de l'unité tout générateur de $\mathcal{U}_n$, c'est tout élément de $\mathcal{U}_n$ d'ordre n . On note $\mathcal{U}_n^*$ cet ensemble.

Déf 45: Soit $n \in \mathbb{N}^*$. On appelle n -ième polynôme cyclotomique le polynôme:

$$\Phi_n(X) = \prod_{z \in \mathcal{U}_n^*} (X - z)$$

Prop 46: Φ_n est unitaire de degré $\varphi(n)$ où φ est l'indicatrice d'Euler.

$$\Phi_n(X) = \prod_{d|n} \Phi_d(X)$$

Lemme 47: On trouve la formule:
$$n = \sum_{d|n} \varphi(d)$$

Prop 48: $\forall n \in \mathbb{N}^*, \Phi_n(X) \in \mathbb{Z}[X]$

Lemme 49: Soit $A, B \in \mathbb{Q}[X]$. On suppose que $A \in \mathbb{Z}[X]$ et que A et B sont mutuelles. Alors A et B sont dans $\mathbb{Z}[X]$.

Théorème 50: $\forall n \in \mathbb{N}^*, \Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

$\Delta \in \mathbb{V} \mathbb{Z}$

Corollaire 51: Soit $n \in \mathbb{N}^*$. Soit $w \in \mathcal{U}_n^*$. Alors le polynôme minimal de w sur $\mathbb{Q}$ est Φ_n et alors $[\mathbb{Q}(w):\mathbb{Q}] = \varphi(n)$.