

[Per]

[Goz]

123. Corps finis applications

K, L, M corps commutatifs

I - Généralités sur les extensions de corps [Per] 65-70

- def + ex $\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q}$
- L/K alors L/K ev
- degré + ex
- base télescopique
- $[M:K] = [M:L][L:K]$
- $L = K(A)$
- monogène
- corps de rupture + Th + ex
- corps de décomposition + Γ + ex

II - Corps finis

1) Construction [Per] 72-73

- sous corps
- caractéristique
- morphisme de Frobenius
- existence corps à q éléments

Dev 1

2) Structure [Per] 74 [Goz] 87-89

- $\mathbb{F}_p \subset \mathbb{F}_{p^n} \Leftrightarrow d|n$ + ex
- $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$
- $\mathbb{F}_q \cong \mathbb{F}_p[X]/(\pi)$ π irred de deg n
- π de deg n irred divise $X^{p^n} - X$
- dans $\mathbb{F}_2$ $X^2 + X + 1$

III - Polynômes sur les corps finis

1) Polynômes irréductibles [Per] 76

- Critère d'Eisenstein + ex Φ_n
- réduction modulo + ex

2) Polynômes cyclotomiques

[G02] 67-69

- def $\mathbb{Q}_n$ $\mathbb{Q}_n^*$
- def Φ_n
- deg Φ_n
- $\Phi_n(x) \in \mathbb{Z}[x]$
- Φ_n irréductible sur $\mathbb{Q}[x]$
- Dirichlet faible

DEV 2

123: Corps finis. Applications

Soit K, L, M des corps commutatifs

I - Généralités sur les extensions de corps

Définition 1: On dit que L est une extension de corps de K noté L/K lorsque $K \subset L$

Exemple 2: $\mathbb{C}$ est une extension de $\mathbb{R}$ et $\mathbb{R}$ de $\mathbb{Q}$

Propriété 3: Si L/K extension de corps, L est un K -ev.

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

Exemple 5: $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}:\mathbb{Q}] = +\infty$

Théorème 6: (Base télescopique)

Soit $K \subset L \subset M$. Soit $(e_i)_{i \in I}$ base de L sur K , $(f_j)_{j \in J}$ 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:

$$[M:K] = [M:L] [L:K]$$

Définition 8: Soit L/K 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/K est dite monogène s'il existe $\alpha \in L$ tel que $L = K(\alpha)$

Définition 9: 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 10: Soit $P \in K[X]$ irréductible, il existe un corps de rupture de P sur K , unique à isomorphisme près

Exemple 11: $\mathbb{C} = \mathbb{R}[X]_{(X^2+1)}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$

Définition 12: Soit $P \in K[X]$ polynôme de degré n . On appelle corps de décomposition de P sur K une extension L de K telle que:

1) P est scindé dans L

2) L est minimal pour cette propriété.

Théorème 13: $\forall P \in K[X]$, il existe un corps de décomposition de P sur K , unique à isomorphisme près

Exemple 14: $\mathbb{Q}(3\sqrt{2}, i)$ est le corps de décomposition de $P(X) = X^3 - 2$ sur $\mathbb{Q}$

II - Corps finis

1) Construction

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

Définition 16: Soit $\varphi: \mathbb{Z} \rightarrow K \mapsto n \cdot 1_K$. Alors $\ker \varphi = p\mathbb{Z}$. Le nombre p est appelé la caractéristique du corps

K . Il est nul ou premier. On le note $\text{car}(K)$

Remarque 17: Si $\text{car}(K)=0$, $\forall (Z) \simeq \mathbb{Z} \subset K$, K est infini. Le sous corps premier de K est $\mathbb{Q}$. Si K est fini, $\text{car}(K)=p>0$. Le sous corps premier de K est $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. De plus son cardinal est une puissance de p .

Proposition 18: Soit K un corps de caractéristique $p>0$. L'application $F: K \rightarrow K$ définie par $F(x)=x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Théorème 19: Pour tout $q=p^n$ avec p premier et $n \in \mathbb{N}^*$, il existe un corps fini $\mathbb{F}_q$ tel que $|\mathbb{F}_q|=q$. C'est le corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$. $\mathbb{F}_q$ est unique à isomorphisme près.

2) Structure

Proposition 20: Soit $d, n \in \mathbb{N}^*$. On a $|\mathbb{F}_d| \subset |\mathbb{F}_n| \iff d|n$

Exemple 21: Les sous-corps de $\mathbb{F}_{2^4}$ sont $\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}, \mathbb{F}_{2^4}, \mathbb{F}_4$.

Théorème 22: Soit $q=p^n$. Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Corollaire 23: Soit $q=p^n$. Alors $|\mathbb{F}_q| = |\mathbb{F}_p[x]|_{(\pi)}$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Corollaire 24: Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors π divise $x^{p^n} - x$ dans $\mathbb{F}_p[x]$ donc est scindé sur $\mathbb{F}_{p^n}$: son corps de rupture $\mathbb{F}_{p^n} = (\mathbb{F}_p[x]/(\pi))$ est aussi son corps de décomposition.

Exemple 25: Il y a un unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$: $x^2 + x + 1$

III - Polynômes sur les corps finis

1) Polynômes irréductibles

Théorème 26: (Critère d'Eisenstein) Soit A un anneau factoriel et $K = \text{Frac}(A)$. Soit $P = \sum_{i=1}^n a_i x^i \in A[x]$. Soit $P \in A$ irréductible. On suppose que:

- 1) $p \nmid a_n$ 2) $\forall i \in [1, n-1]$ $p \mid a_i$ 3) $p^2 \nmid a_0$

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

Application 27: Soit $\phi_p(x) = x^{p^2} + \dots + x + 1$ alors ϕ_p est irréductible sur $\mathbb{Z}$.

Théorème 28: Soit A un anneau factoriel et $K = \text{Frac}(A)$.

Soit I un idéal premier de A et $B = A/I$. 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 $\bar{P}$ irréductible sur B

P est irréductible sur K .

Exemple 29: $X^3 + 462X^2 + 2433X - 67691$ est irréductible

sur $\mathbb{Z}$

2) Polynômes cyclotomiques

Définition 30: Soit $n \in \mathbb{N}^*$. On pose $M_n = \{z \in \mathbb{C} \mid z^n = 1\}$

L'ensemble des racines n -ième de l'unité.

On appelle racine primitive n -ième de l'unité tout générateur de M_n , c'est à dire tout élément de M_n d'ordre n . On note M_n^* cet ensemble

Définition 31: Soit $n \in \mathbb{N}^*$. On appelle n -ième polynôme cyclotomique le polynôme:

$$\Phi_n(X) = \prod_{z \in M_n^*} (X - z)$$

Proposition 32: Φ_n est unitaire de degré $\varphi(n)$

où φ est l'indicatrice d'Euler.

$$\text{On a } X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Proposition 33: $\forall n \in \mathbb{N}^* \quad \Phi_n(X) \in \mathbb{Z}[X]$

Théorème 34: $\forall n \in \mathbb{N}^* \quad \Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$

Application 35: (Théorème de Dirichlet faible) DEV2

Il existe une infinité de nombres premiers congrus à 1 modulo n pour $n \in \mathbb{N}^*$

Question principale:
existe-t-il un corps à
 n éléments $\forall n \in \mathbb{N}$?

Avant ça il faut
définir les extensions
de corps

$K \subset L$ ex $\mathbb{R} \subset \mathbb{C}$

$\hookrightarrow$ degré $[L:K]$

Th base télescopique
crucial

123: Corps finis

Applications

Application avec
les polynômes

critères

irréductibilité

Eisenstein

Modulo

Poly

cyclotomique

$$\phi_n = \prod_{j \in \mathbb{Z}_n^*} (x - \zeta_n^j)$$

Dichotomie
DEV2

$$\mathbb{F}_p^d \subset \mathbb{F}_{p^n} \Leftrightarrow d \mid n$$

π de deg n irréductible
divise $x^{p^n} - x$

structure et
prop de ces corps

Construction

$\rightarrow$ Qu'est-ce qu'un ss corps?
Quels sont ses caractéristiques

Existence des corps à
 q éléments DEV1

$$q = p^n$$

Corps de rupture

P irréductible dans ce corps

Corps de décomposition

P scindé sur ce corps

utile pour l'étude
des corps finis

$\rightarrow$ Existence et unicité