

141: Pol. irr. à une indéterminée corps de coefficients etc. et applis

I. Polynômes et irréductibilité Anneau, intègre, commutatif. $P \in A[X]$
 K en corps. k en corps

a) Notion d'irréductibilité

Def. 1: On dit que P est irr. si $P \in A[X]^* = A^* \setminus \{0\}$, si $P \neq 0$ et si il n'est divisible que par $\lambda \in A^*$ ou λP .

Ex. 2: Si $P \in k[X]$ de deg. 1 alors P est irr.

Si $P \in \mathbb{R}[X]$ de discriminant négatif alors P est irr.

Prop. 3: Un pol. de deg. 2 ou 3 est réductible dans $K[X]$ ssi il admet au moins une racine dans K .

Prop. 5: Si un pol. de $K[X]$ de deg ≥ 2 est irréductible alors il n'a pas de racines dans K .

b) L'anneau des polynômes et notions de contenu

Prop. 6: $A[X]$ est principal ssi A est un corps

Def. 7: On appelle contenu de P noté $c(P)$ ou $c(P) = \text{pgcd}(a_0, \dots, a_n)$ où $P = a_n X^n + \dots + a_0$. Si $c(P) = 1$ on dit que P est primitif.

Rmq. 8: Le contenu est défini modulo A^* .

Lemme 9: (Gauss) $P, Q \in A[X]$ $c(PQ) = c(P)c(Q)$ modulo A^* .

Prop. 10: $\mathbb{Q}[X]$ primitif non constant

P est irr. dans $\mathbb{Q}[X]$ ssi P irr. dans $\text{Frac}(A[X])$

Thm. 11: (Gauss) Si A est factoriel alors $A[X]$ est factoriel.

c) Critère d'irréductibilité $K = \text{Frac}(A)$

Thm. 12: (Eisenstein) A factoriel. $P = a_n X^n + \dots + a_0$. $P \in A$ irréductible.

Si :

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

Alors P est irréductible dans $K[X]$ (et dans $A[X]$ si $c(P) = 1$)

Ex. 13: $X^2 + 3X + 12$ est irréductible dans $\mathbb{Q}[X]$.

Thm. 14: A factoriel. I idéal premier de A et $B := A/I$, $I = \text{Frac}(B)$

$P = a_n X^n + \dots + a_0 \in A[X]$. Soit $\bar{P}$ sa réduction modulo I .

Si $\bar{a}_n \neq 0$ et $\bar{P}$ irr. sur B alors P est irr. sur K .

Rmq. 13: Le cas d'utilisation fréquent est $A = \mathbb{Z}$, $I = (p)$, $B = \mathbb{F}_p$

Ex. 16: $X^3 + 462X^2 + 2433X - 6769$ irr. sur $\mathbb{Z}$. En effet réduit mod. 2 il reste $X^3 + X + 1$ qui est irr. sur $\mathbb{F}_2$

Thm. 17: $P \in k[X]$ de deg. m . P est irr. sur k ssi P n'a pas de racines dans les extensions K/k tq $[K:k] \leq \frac{m}{2}$.

Thm. 18: $P \in k[X]$ irr. de deg. m et K/k de deg. n tq $\text{pgcd}(m, n) = 1$ alors P est irr. sur K .

II. Polynômes et extensions de corps M, L, K corps commutatifs

a) Extensions et éléments algébriques

cf. L12S LPER p. 65-67

et L18S p. 755

15 points

ROY
p. 368
- 369

LPER
p. 50
- 51

33

b) Corps de rupture et décomposition

cf L12S EPERS p 70-72

6 points

39

b) Cloture algébrique

cf L12S EPERS p. 67 et p 72

3 points

42

III. Un exemple de polynômes irréductible: polynômes cyclotomiques

 $\mu_n = \{ \zeta \in \mathbb{C} \mid \zeta^n = 1 \}$, μ_n^* les générateurs de ce groupe.Def. 44: $n \in \mathbb{N}^*$, on définit le n -ème pol cyclotomique:

$$\Phi_n = \prod_{\zeta \in \mu_n^*} (x - \zeta)$$

Prop. 45: $x^n - 1 = \prod_{d \mid n} \Phi_d$ Prop. 46: Φ_n est unitaire de deg $\phi(n)$ Prop. 47: avec 45 on a $\Phi_n = \frac{x^n - 1}{\prod_{d \mid n, d < n} \Phi_d}$ Ex. 48: $\Phi_3 = x^2 + x + 1$, $\Phi_5 = x^4 + x^3 + x^2 + x + 1$...Prop. 49: $\Phi_n \in \mathbb{Z}[X]$ Thm. 50: Φ_n est irr. sur $\mathbb{Z}[X]$ Cor. 51: $\zeta \in \mu_n^*$ le pol. min de ζ sur $\mathbb{Q}$ est Φ_n et $[\mathbb{Q}(\zeta), \mathbb{Q}] = \phi(n)$

Thm. 52: (Wedderburn) tout corps fini est commutatif.

IV. Application: Construction des corps finis K , k des corps, p premier et $q = p^n$ avec $n \in \mathbb{N}^*$ Def. 53: On appelle sous corps premier de K , le plus petit sous corps de K .Def. 54: $f: \mathbb{Z} \rightarrow K$. Le générateur de $\text{Ker}(f)$ est appelé caractéristique de K noté $\text{car}(K)$.Prop. 55: $\text{car}(K)$ est nul ou bien est un nombre premier. Si• $\text{car}(K) = 0$ alors K est infini et contient $\mathbb{Q}$ • $\text{car}(K) = p$ le sous corps premier de K est $\mathbb{F}_p$.Prop. 56: Si K est fini et $\text{car}(K) = p$ alors $|K| = p^n$ avec $n \in \mathbb{N}^*$ EPERS
p. 80-81DEV
p. 83
EPERSEPERS
p. 72-73

Thm. 57: Il existe un corps à q éléments. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Il est unique à isomorphisme près.

Def. 58: Notons $m = \prod_{i=1}^r p_i^{a_i}$ sa décomposition en facteur premier. On appelle fonction de Möbius :

$$\mu(m) = \begin{cases} 1 & \text{si } m=1 \\ (-1)^r & \text{si } m = \prod_{i=1}^r p_i \text{ (sans facteur carré)} \\ 0 & \text{sinon} \end{cases}$$

Thm. 59: (Inversion de Möbius) $u, v: \mathbb{N}^* \rightarrow \mathbb{R}$, D_n ensemble des diviseurs de n .
 $\forall m \in \mathbb{N}^* \quad u(m) = \sum_{d|m} v(d) \quad \text{ssi} \quad \forall m \in \mathbb{N}^*, \quad v(m) = \sum_{d|m} \mu(d) u\left(\frac{m}{d}\right)$

Notons $P_m := X^q - X \in \mathbb{F}_p[X]$, $U_n(p)$ l'ens. des pol. unités de deg. n irr. dans $\mathbb{F}_p[X]$.
Lemme. 60: Tout diviseur irréductible de P_m dans $\mathbb{F}_p[X]$ est de degré diviseur m . Réciproquement, pour tout diviseur d de m , tout polynôme $P \in U_d(p)$ divise P_m .

Thm. 61: P_m est sans facteur carré dans $\mathbb{F}_p$ et

$$P_m = \prod_{d|m} \prod_{P \in U_d(p)} P$$

Thm. 62: $\forall m \in \mathbb{N}^*, \quad |U_n(p)| = \frac{1}{n} \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d$.

COURS: Rombaldi, Algèbre et géométrie par Lagrey
CPERS: Perrin, cours d'algèbre
CBERS: Berhuy, Algèbre le grand combat

ZKOHJ

p. 331
- 332

ZKOHJ

p. 423
- 424

DEV. 2