Plan détaillé avec livres : $\boxed{141}$

• A = anneau) I) A)

[PER] p.53

Déf1 : irréductibilité d'un ~~anneau~~ élément dans un anneau

Ex2 : sur $\mathbb{Z}$,

~~Déf3 : Anneau factoriel~~

~~Ex4 : $\mathbb{Z}$, $k[X]$ avec k corps~~

~~Rem5 : Euclidien $\Rightarrow$ principal $\Rightarrow$ factoriel] 1)~~

~~En général on travaille sur $k[X]$ euclidien car k corps.~~

vrm utile ?

Rem6 : ⚠ dire dans quel anneau c'est irréd. ex $2X \in \mathbb{Z}[X] / \mathbb{Q}[X]$

[PER] p.9

Prop7 : Soit $P \in A[X]$

- Si P est de degré 1 et unitaire, P irréd
- Si $\deg(P) \geq 2$, irréd $\rightsquigarrow$ pas de racines dans A.

[GOM] p.378 [PER] p.202

Ex8 :
- D'Alembert-Gauss
- Irréductibles de $\mathbb{R}[X]$
- Pas de résultats sim. sur $\mathbb{Q}[X]$

B) Critères d'irréductibilité : On se place dans A factoriel, $K = \mathrm{Frac}(A)$.

[PER] p.10

Prop19 : Polyn de d° 2 ou 3 sur un corps... (en gén. pour $\mathbb{Q}$)

ex19' : polyn d° 2, 3 sur $\mathbb{F}_3$, $\mathbb{F}_2$ ...

Rem20 : Critère des "racines évidentes" sur $\mathbb{Q}[X]$

[PER] p.57-58

Déf21 : contenu / polynôme primitif

Prop22 Lemme de Gauss

PROP23 : irréd de $A[X]$ = irréd. de A + $P \in K[X]$ d° ≥ 1 primitifs

[PER] p.12

THM24 : Critère d'irréd. par réduction modulo un idéal premier

~~THM~~ Ex25 : $X^3 - 127X^2 + 3608X + 19$ irréd sur $\mathbb{Z}[X]$

[PER] p.13

THM25 : Eisenstein

APPLI26 : $\Phi_p = \sum_{i=0}^{p-1} X^i$, p premier irréd. sur $\mathbb{Z}[X]$.

Rem27 : il existe une infinité de poly irréd sur $\mathbb{Z}[X]$.

II) Extensions de corps : On note K un corps commutatif (tous les corps sont commutatifs)

A) Extensions algébriques :

[PER] p.73

Déf28 : extension de corps

Ex29 : $\mathbb{C}/\mathbb{R}$, $\mathbb{R}[X]/\mathbb{R}$, $\mathbb{Q}(i)/\mathbb{Q}$

Rem30 : $K \subseteq L$ ext. corps, L = K-ev

Déf31 : degré extension + ex

Thm32 : Base télescopique + multiplicativité des d°

[PER] p.75

Déf33 : nombre algébrique | transcendant (avec polynômes) + extension alg

Ex34 : i, $\sqrt{2}$, $\sqrt[3]{2}$ sur $\mathbb{Q}$, T sur $K(T)$...

Déf35 : Polynôme minimal (π_x)

Ex36 : des exemples de π_x...

Rem36 : π_x irréductible

THM37 : α alg sur $K \Leftrightarrow K[\alpha] = K(\alpha) \Leftrightarrow \dim_K K[\alpha] < +\infty$ et $\hat{m} = d°(\pi_\alpha)$

(passer par $\varphi : \begin{array}{l} K[T] \to K[\alpha] \\ P \mapsto P(\alpha) \end{array}$)

THM38 : $\{ x \in L \text{ alg sur } K \}$ ss-corps de L

Ex39 : $\overline{\mathbb{Q}}$ ↗

[PER] 75

Déf40 : Corps algébriquement clos

Rem41 : $\mathbb{C}$, $\overline{\mathbb{Q}}$

B) Corps de rupture et de décomposition :

[PER] p.78-79

DÉF42 : Corps de rupture

THM43 : Existence et unicité corps de rupture

Ex44 : $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$, $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3-2)$ ... Rem44' : construction d'ext. alg. $\boxed{K[X]/(\pi_\alpha) \simeq K(\alpha)}$

DÉF45 Corps de décomposition

THM46 : Existence et unicité

Ex47 : $\mathbb{R}(i)$ corps de déc. de X^2+1, $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j)$ de ~~$\mathbb{Q}(\sqrt[3]{2})$~~ $X^3 - 2$ sur $\mathbb{Q}$

DÉF48 : Clôture algébrique

Rem49 : sur $\overline{\mathbb{Q}}$ ↗

C) Critères d'irréductibilité grâce aux extensions :

REM50 : Si un polyn. est un polyn. mini d'un élément sur K, il est irréd sur K
↳ en pratique si on a le d° de l'ext. et qu'on sait que $\deg(P) = [K(\alpha):K]$ ~~et~~ et $P(\alpha) = 0$ alors $P = \pi_\alpha$ donc irréd.

[PER] p.88

THM51 : $P \in K[X]$ irréd, $[L:K] = m$, si $\deg(P) \wedge m = 1$, P irréd sur L

Ex52 : $X^3 + X + 1$ sur $\mathbb{Q}(i)$, sur $\mathbb{F}_{p^n}$ où $3 \nmid n$] $p = 2$ ou 5

~~$X^2 + 2X + 3$ irréd sur $\mathbb{Q}(\sqrt{2})$~~

Plan détaillé [141] suite

II) C)

[PER] p.87 THM52 : $P \in K[X]$. P irréd sur $K \iff P$ n'a pas de racines dans les extension L/K tq $[L:K] \leqslant \frac{\deg P}{2}$.

Ex53 : X^4+X+1 irréd sur $\mathbb{F}_2$, ~~$\mathbb{F}_4$~~] 11)

III) Applications et exemples :

B) Construction des corps finis :

p désigne un nombre premier
$q = p^n$, $n \in \mathbb{N}^*$

[PER] p.81 RAPPEL54 : déf caract + morphisme de Frobenius

THM54 : Existence et unicité des corps finis

[GOZ] p.87 REM55 : Construction en pratique à partir de corps de rupture :

THM56 : $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$, π irréd de d°n sur $\mathbb{F}_q$

juste dû à $\pi \mid X^{p^n}-X$ scindé sur $\mathbb{F}_{p^n}$

Cor57 : Corps de rupture = corps de déc. sur $\mathbb{F}_p$ pour π irréd

[GOZ] p.58 APPL58 : Construction de $\mathbb{F}_4$ (Annexe : table des lois)

[PER] p.82 THM59 : $\mathbb{F}_q^*$ cyclique ← utilise A)

Cor60 : élém^t primitif sur $\mathbb{F}_q$

[FRA] p.150 THM61 : $A(n,q) = \{$polyn. irréd, unitaire, de d°n sur $\mathbb{F}_q\}$, $I(n,q) = \# A(n,q)$

$$X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P$$

Cor62 : $q^n = \sum_{d \mid n} d\, I(d,q)$

Dév 2

Prop63 : • $I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu(n/d)\, q^d$, où μ fonction de Möbius (prop. admises)

• $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$.

(utilise A)

$\boxed{I(n,q) > 0}$ ⟸ regarder $I(n,q) \geq 1$ $\forall n$ ⟺ il existe des polyn. irréd de tout d° sur $\mathbb{F}_q$

OK

A) Polynômes cyclotomiques : (sur $\mathbb{Q}$)

[PER] p.89 DÉF64 : Polyn. cyclotomiques sur $\mathbb{Q}$

PROP65 : $X^n - 1 = \prod_{d \mid n} \Phi_d$

REM66 : Φ_n unitaire, de degré $\varphi(n)$, φ = ind. Euler

[GOZ] p.76 Ex64' : ex. de Φ_n

REM67 : Φ_p pour p 1er, on a déjà vu qu'il était irréd.

[PER] p.82 THM68 : • $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$

• Φ_n irréductible sur $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

Dév 1

Cor67 : Pour $\xi \in \mathbb{U}_n^*$, $[\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(n)$, Φ_n polyn. mini de ξ sur $\mathbb{Q}$

Réf : [PER] : Perrin, Cours d'Algèbre.

[GOZ] : Gozard, Théorie de Galois

[FRA] : Francinou, Gianella, Exercices de mathématiques pour l'agrégation

Idée de plan :

I) Polynômes irréductibles

A) Définitions et exemples

↳ $\underset{\text{cas gén.}}{\underline{\mathbb{R}\ \mathbb{C}\ \mathbb{Q}}}$, $\mathbb{F}_q$ (parler d'anneaux factoriels ?)

B) Critères d'irréductibilité (A factoriel)

→ d°2, 3
→ contenu + lemme de Gauss
→ irréductibilité sur $A[X]$
→ Eisenstein

II) Extensions de corps

A) Déf - extensions algébriques

→ base télescopique
→ déf élém^t alg. + déf polynôme mini

B) Corps de rupture et de décomposit°

→ existence et unicité (pour les 2)
→ racine de P dans extension
→ exemples $\boxed{\text{+ critères d'irréd. avec les extensions}}$ C
→ thm de l'élément primitif)

C) Clôture algébrique et corps alg clos

→ KR corps alg clos
→ exemples
→ ens {éléments de K alg sur k} = corps alg clos
↳ $\overline{\mathbb{Q}}$...
→ ex $\overline{\mathbb{F}_p}$?

III) Exemples et applicat°

A) Poly cyclotomiques

déf, prop, $\boxed{\text{irréductibilité}}$ dév1

B) Corps finis

→ corps rupt = corps décomp
→ déf $\mathbb{F}_q$, ss-corps de $\mathbb{F}_q$
→ $\boxed{\text{polyn irréductibles sur } \mathbb{F}_q \text{ dénombrem}^t}$

on se sert des poly cyclo !
dév2

Plan leçon [141]

« Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications »

Rapport du jury :

- ☒ Corps de rupture + corps de décomposition
- ☒ Exemples sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{F}_q$
- ☒ Exemples de polyn irréductibles sur $\mathbb{F}_2$, $\mathbb{F}_3$, de d° 2, 3, 4
- ☒ Critères d'irréductibilité
- ☒ Polynômes minimaux de quelques nombres algébriques
- ☐ Savoir montrer que {nbres alg. sur $\mathbb{Q}$} = corps alg. clos
- ☒ Thm base télescopique et applicat° à l'étude irréductibilité des polynômes

⚠

Dév. (1) Dénombrement des polynômes irréductibles unitaires sur $\mathbb{F}_q$

(2) Irréductibilité des polynômes cyclotomiques

Réf :
- Perrin
- Gozard