

Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : Polynômes irréductibles à une indéterminée. Corps de rupture.
Exemples et applications.

Autre sujet :

A est un anneau factoriel et $k = \text{frac}(A)$
 K est une extension de k .

I Polynômes irréductibles

1 Definition

DEF 1 Un polynôme $P \in A[X]$ est dit irréductible si $\nexists P = A \cdot B$ et si P est un élément irréductible de l'anneau $A[X]$.

Rq2 $k[X]$ est euclidien, donc principal,
donc factoriel

DEF/PROP3 $\forall p \in h[x]$.

$\alpha \in K$ est une racine de P si $P(\alpha) = 0$.
La multiplicité de α comme racine de P est le plus grand $n \in \mathbb{N}$ tel que $(X - \alpha)^n$ divise P dans $K[X]$.

La somme des multiplicités des racines de P dans K est inférieure au degré de P .
Il y a égalité ssi P est scindé dans $K[X]$.

PROP4 [Inductibilité dans $k[x]$]

- Tout polynôme de degré 1 est irréductible.
- Un polynôme irréductible de degré > 1 n'a aucune racine dans K .
- La réciproque est vérifiée pour les degrés 2 et 3.

EX5 $(X^2+1)^2$ est réductible sans racines dans $\mathbb{R}$

Rq 6 Si P est irréductible dans $K[X]$ alors
il est irréductible dans $k[X]$.

DEF 7 Le contenu de $P \in A[X]^+ \setminus \{0\}$, noté $c(P)$, est le pgcd des coefficients de P .

P est dit primitif, si $c(P)=1$.

$P = \sum_{n=0}^{\infty} a_n X^n$ est dit unitaire si $a_n = 1$.

LEM 8 [Gauss]

- $c(P) = c(Q) = 1 \Rightarrow c(PQ) = 1$
- $\forall P, Q \in A[x]^* \setminus \{0\}, c(PQ) = c(P) \cdot c(Q).$

2 Critères d'irréductibilité

Th9 Soit $P \in A[X]$, $d^0 P \geq 1$.

P est irréductible dans $k[x]$ et $c(P) = 1$
 $\Leftrightarrow P$ est irréductible dans $A[x]$.

TH10 [Kritik d' Eisenstein]

Satz $P = \sum_{i=0}^n a_i X^i \in A[X]$, $d^\circ P \geq 1$.

On suppose qu'il existe $p \in A$ irréductible
tel que $p \nmid a_n$ & $\forall i \in [0; n-1], p \nmid a_i$ & $p^2 \nmid a_0$.
Alors P est irréductible dans $k[x]$.

EX14 $\forall n \geq 1, X^n - 2$ est irréductible dans $\mathbb{Q}[X]$

TH12 [critère de réduction]

Satz $P = \sum_{i=0}^n a_i X^i \in A[X]$, $d^0 P \geq 1$.

Soit I un idéal premier de A , $B = A/I$ et $L = \text{frac}(B)$.
Si $\bar{a}_n \neq \bar{0}$ et $\bar{P}$ est irréductible dans $L[X]$
alors P est irréductible dans $A[X]$.

EX13 $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$ (étudier modulo 2)

3 Polynôme minimal

DEF 14 Zeit & EK.

α est dit algébrique sur k s'il existe $P \in k[X] \setminus \{0\}$ tel que $P(\alpha) = 0$.

DEF/PROP 15 Soit $\alpha \in K$ algébrique sur k .

On appelle polynôme minimal de α sur k , noté $\text{Irr}(\alpha, k)$, le générateur unitaire de l'idéal non trivial des polynômes de $k[X]$ qui annulent α .

NOM : Prénom : Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

G0Z] p31

EX16 $d^0(\text{Irr}(\alpha, k)) = 1 \iff \text{Irr}(\alpha, k) = X - \alpha \iff \alpha \in k$

La notation $\text{Irr}(\alpha, k)$ est justifiée par :

PROP17 Soit $P \in k[X]$.

P est irréductible dans $k[X]$, unitaire et $P(\alpha) = 0$
 $\iff P = \text{Irr}(\alpha, k)$.

Ø

EX18 $\forall m \geq 1, \text{Irr}(\sqrt[m]{2}, \mathbb{Q}) = X^m - 2$.

D'où $\forall m \geq 2, \sqrt[m]{2} \notin \mathbb{Q}$.

G0Z] p33

TH19 Soit $\alpha \in K$ algébrique sur k .

Alors $\dim_k k(\alpha) = [k(\alpha) : k] = d^0(\text{Irr}(\alpha, k))$.

II Extensions de corps

1 Corps de rupture

G0Z] p57

DEF20 Soit $P \in k[X]$ irréductible.

On dit que le corps K est un corps de rupture de P si $K = k(\alpha)$ avec $P(\alpha) = 0$.

TH21 Soit $P \in k[X]$ irréductible.

• Il existe un corps de rupture de P .

• Soient $k(\alpha)$ et $k(\beta)$ deux corps de rupture de P .

Alors il existe un unique k -isomorphisme

$\iota : k(\alpha) \rightarrow k(\beta)$ tel que $\iota(\alpha) = \beta$.

p58

Rq22 $P = \text{Irr}(\alpha, k)$

EX23 $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ et $i = \bar{X}$

p59

PROP24 Soit $P \in k[X]$ de degré $n \geq 2$.

P est irréductible dans $k[X] \iff$

P n'a pas de racine dans les extensions L de k telles que $[L : k] \leq n/2$.

G0Z] p22

TH25 Soit E un K -espace vectoriel.

Alors $\dim_k E = (\dim_K E)(\dim_k K)$.

p59

PROP26 Soit $P \in k[X]$ irréductible, $d^0 P = n$.

Si $[K : k] = m$ et $\text{pgcd}(m, n) = 1$ alors

P est irréductible dans $K[X]$.

2 Corps de décomposition

DEF27 Soit $P \in k[X]$.

On dit que K est un corps de décomposition de P sur k si

• $\exists \alpha \in K, \exists (\alpha_1, \dots, \alpha_m) \in K^m, P = a(X - \alpha_1) \dots (X - \alpha_m)$

• $K = k(\alpha_1, \dots, \alpha_m)$.

Rq28 Comme K est engendré par les α_i ,
 K est un corps minimal où P est scindé.

TH29 Soit $P \in k[X]$ avec $d^0 P \geq 1$.

• Il existe un corps de décomposition L de P sur k avec $[L : k] \leq m!$.

• Si L et L' sont deux corps de décomposition de P sur k alors il existe un k -isomorphisme de L sur L' .

3 Clôture algébrique

DEF/PROP30 On a équivalence entre :

• Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K .

• Tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine dans K .

• Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.

• Toute extension algébrique de K est égale à K .

On dit alors que K est algébriquement clos.

PROP31 Tout corps algébriquement clos est infini.

TH32 $\mathbb{C}$ est algébriquement clos.

DEF33 On dit que K est une clôture algébrique de k si K est algébrique sur k et K est algébriquement clos.

TH34 [Steinitz]

Tout corps commutatif admet une clôture algébrique (on admet : unique à isomorphisme près).

p60

p62

p63

NOM :

Prénom :

Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

GOZ] p63

PROP35 Soit E un corps algébriquement clos.
Soit K un sous-corps de E .

L'ensemble $\bar{K}$ des éléments de E algébriques sur K (= fermeture algébrique de K dans E) est une clôture algébrique de K .

EX36 La fermeture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$ est une clôture algébrique de $\mathbb{Q}$.

III Applications

1 Corps finis

[PER]

↑72

DEF37 Soit K un corps quelconque.
On appelle sous-corps premier de K le plus petit sous-corps de K .

PROP38 Si $\text{car } K = 0$ alors le sous-corps premier de K est isomorphe à $\mathbb{Q}$.

Si $\text{car } K = p > 0$ alors le sous-corps premier de K est isomorphe à $\mathbb{F}_p$.

COR39 Si K est un corps fini alors $|K| = p^n$ avec $n \in \mathbb{N}^*$ et p premier.

↑73

TH40 Soit p premier et $n \in \mathbb{N}^*$. $q = p^n$.
Il existe un corps à q éléments, unique à $\mathbb{F}_p$ -isomorphisme près. On le note $\mathbb{F}_q$.

GOZ] p58

EX41 $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 - X - 1) \simeq \{0, 1, i, i^2\}$

↑91

TH42 Soient p premier, $n \in \mathbb{N}^*$ et $q = p^n$.
 K est un sous-corps de $\mathbb{F}_q$ ssi il existe $d|m$ tel que $|K| = p^d$.

↑92

TH43 Soit p premier. Soit $n \in \mathbb{N}^*$. $q = p^n$.
La clôture algébrique de $\mathbb{F}_q$ est

$$\bar{\mathbb{F}}_q = \bigcup_{i=1}^{+\infty} \mathbb{F}_{q^i} = \bigcup_{i=1}^{+\infty} \mathbb{F}_{p^{ni}}.$$

2 Polynômes cyclotomiques

NOT44 Soit k un corps.

On note $\mu_n(k)$ l'ensemble des racines n -èmes de l'unité dans k .

On note K_n un corps de décomposition de $X^n - 1$ sur k .

[PER]

↑80

DEF45 Une racine n -ème primitive de 1 est un élément ζ de K_n tel que $\zeta^n = 1$ et $\forall d < n, \zeta^d \neq 1$.

On note leur ensemble $\mu_n^*(K_n)$.

DEF46 Le n -ième polynôme cyclotomique est $\Phi_{n,k} = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$.

PROP47 $X^n - 1 = \prod_{d|n} \Phi_{d,k}(X)$.

EX48 $\Phi_{n,k} = X^{\frac{n}{2}} + 1, \dots$

↑81

PROP49 • $\Phi_{n,\alpha} \in \mathbb{Z}[X]$

• si on note $\sigma: \mathbb{Z} \rightarrow k$ alors $m \mapsto m \cdot 1_k$

$$\Phi_{n,k} = \sigma(\Phi_{n,\alpha})$$

TH50 Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$

DEV2

↑82

[GOZ] GOZARD, Théorie de Galois (++)

[PER] PERRIN, Cours d'algèbre (++)

[OX] OUVX X-ENS, Algèbre 1 (-)