NOM : LAVIGNE Prénom : Florian Jury : N° 141

Algèbre ← Entourez l'épreuve → Analyse

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

Autre sujet :

17 (6) critères d'irréductibilité : Procédé (16 pages !!)...

Soit A anneau, K corps et $\mathcal{P}$ l'ens. des nombres premiers

I - Irréductibilité

A) Définitions

Déf 1 : Un polynôme $P \in A[X]$ est irréductible (dans $A[X]$) si $P \notin A$ et si $Q \in A[X]$ avec $Q | P$ alors :
$\exists u \in A^\times$, $Q = uP$ ou $Q = u$.

Prop 2 : Si P irr. alors λP l'est pour $\lambda \in A^\times$.

Prop 3 : Soit $P \in K[X]$
- $\deg P = 1 \Rightarrow P$ irr.
- Si P irr., alors P n'a pas de racine dans K.
- Si P est de degré 2 ou 3 et n'a pas de racine dans K, alors P est irr. dans $K[X]$
- P irr. $\Leftrightarrow K[X]/(P)$ est un corps.

Ex 4 : $(X^2+1)^2$ n'a pas de racine dans $\mathbb{R}$ et est réductible dans $\mathbb{R}[X]$.

Rq 5 : Soit $P \in K[X]$ irr. sur $K[X]$ et L/K ext. P peut être réductible sur $L[X]$.

Ex 6 : X^2+1 est irr. sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$.

Rq 7 : L'anneau $A[X]$ est factoriel si A l'est.

Th 8 : Tout polynôme de $A[X]$ pour A factoriel s'écrit comme produit de polynômes irréductibles

Ex 9 : $X^3+2X^2+X+2 = (X^2+1)(X+2)$ dans $\mathbb{R}[X]$
$= (X-i)(X+i)(X+2)$ dans $\mathbb{C}[X]$

Appli 10 : Si A est factoriel, via th. 8, on peut trouver un pgcd, un ppcm de deux polynômes. On peut aussi effectuer la DES.

Cor 11 : L'ensemble des polynômes irréductibles de $K[X]$ est infini.

B) Critères d'irréductibilité

Ici A est factoriel et $K = \mathrm{Frac}(A)$.

Déf 12 : Soit $P \in A[X]$. Le contenu de P, noté $C(P)$, est le pgcd des coefficients de P.

Déf 13 : $P \in A[X]$ est primitif si $C(P) = 1$.

Ex 14 : $C(X^3+2) = 1$. Donc X^3+2 est primitif.

Lemme 15 : (Gauss)
(i) Le produit de deux polynômes primitifs est primitif.
(ii) Soit $(P, Q) \in A[X]$. Alors $C(PQ) = C(P) \cdot C(Q)$.

Th 16 : (Eisenstein) DEV
Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ avec $n \geq 1$. Soit $p \in A$ irr. avec $p \nmid a_n$, $p | a_k$ pour $k < n$, $p^2 \nmid a_0$. Alors P est irr. sur $K[X]$.

Ex 17 : Soit $n \in \mathbb{N}^*$, $p \in \mathcal{P}$. Soit $a \in \mathbb{Z}$ avec $p | a$, $p^2 \nmid a$. Alors $X^n + a$ est irr. sur $\mathbb{Q}[X]$

Th 18 : Soit $P \in A[X]$, $\deg P \geq 1$. Alors P irr. dans $A[X]$ ssi (P irr. dans $K[X]$ et $C(P) = 1$)

Ex 19 : X^3+2 est irr. sur $\mathbb{Z}[X]$.

Prop 20 : Soit $p \in \mathcal{P}$. Alors $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ irr. sur $\mathbb{Z}[X]$.

Th 21 : Soit I idéal premier de A. On pose $B = A/I$ et $L = \mathrm{Frac}(B)$. Soit $P \in A[X] \setminus A$ de coefficient dominant $a_n \notin I$. Si (P mod I) est irr. dans $L[X]$, alors P est irr. dans $K[X]$.

Ex 22 : $X^3 - 257X^2 + 27134X + 13$ est irr. dans $\mathbb{Z}[X]$

II - Extensions de corps et polynômes

A) Nombres algébriques

Rq 23 : Soit $a \in K$. Alors eval_a est un morphisme de K-algèbres

Déf 24 : Si eval_a n'est pas injectif, a est dit algébrique. Sinon il est dit transcendant.

Déf 25 : Soit $a \in K$ algébrique. Alors $\mathrm{Ker}(\mathrm{eval}_a)$ est

Réf : * Tauvel, Corps commutatifs et Théorie de Galois
* Gozard, Théorie de Galois
* Beck, Objectif Agrégation
* Perrin, Cours d'Algèbre
* Francinou Gianella, Exercices pour l'agrégation, Algèbre 1

NOM : LAVIGNE Prénom : Florian Jury : N°141

(Algèbre) ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

NOM : LAVIGNE Prénom : Florian Jury : N°141

(Algèbre) ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

3/4

Annexe

Annexe 1 : Opérations dans $\mathbb{F}_4$.

Soit j la classe de X dans L. Alors :

+	0	1	j	j^2
0	0	1	j	j^2
1	1	0	j^2	j
j	j	j^2	0	1
j^2	j^2	j	1	0

×	0	1	j	j^2
0	0	0	0	0
1	0	1	j	j^2
j	0	j	j^2	1
j^2	0	j^2	1	j

Annexe 2 : Algorithme de Berlekamp

Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés. On pose :

$$S_p : \begin{cases} \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P) \\ (Q \bmod P) \longmapsto Q(X^q) \bmod P \ (= Q^q \bmod P) \end{cases}$$

On note $P = P_1 \dots P_r$ avec P_i irréductible et $K_i = \mathbb{F}_q[X]/(P_i)$ corps.
On définit l'isomorphisme de K-algèbres :

$$\varphi : \begin{cases} \mathbb{F}_q[X]/(P) \longrightarrow K_1 \times \dots \times K_r \\ Q \bmod P \longmapsto (Q \bmod P_1, \dots, Q \bmod P_r) \end{cases}$$

Soit $x = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$ et $\mathcal{B} = (1, x, \dots, x^{\deg P - 1})$ base de $\mathbb{F}_q[X]/(P)$. Alors le processus suivant s'arrête et décompose P :

(i) On calcule la matrice $S_p - id$ dans $\mathcal{B}$, et on passe à (ii)

(ii) Soit r = nbre d'irr. décomposant P. Alors $r = \dim(\ker(S_p - id))$
Si $r = 1$, P est irr. et on s'arrête. Sinon on passe à (iii)

(iii) Soit $V \in \mathbb{F}_q[X]$ non congru à une constante mod P
et $V \bmod P \in \ker(S_p - id)$. Alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{PGCD}(P, V - \alpha)$.

- Justifier l'irréductibilité, mentionner la factorialité
  Une des 2 justif ou les corps de rupture — irred de deg ≤ 3 (⇔ avoir une ρ)

- "spécialisation"

- Berlekamp : expliquer pquoi c'est bien. Efficacité ?

- Thm de la base télescopique

- Le corps de rupt c'est le + pt tel qu'on obtient une ρ

- Applica° : * corps finis → la plus grosse appli à mettre

  (codes correcteurs (cycliques))

  * irr de ℝ ou ℂ → histoires de réduc°, trigonalisa° di ℂ
    → irr de ℂ ⇒ tête des irr de ℝ
    appli : réduc° des endomorφ normaux
    CH + Lemme noyau ...

  dev possible → D'Alembert Gauss

  */ dev possible

  * thm de l'élt prim
    thm de prolongemt des morφ } dev possible } appli alg.

  dev possible | * polygones constructibles à la règle et au compas
    Gauss Wantzel
    ← n ème poly cyclotomique est irréductible

- Dev possibles : * # d'irred de deg n de $\mathbb{F}_q$ — cf Demazure
  ↳ à quoi ça sert ? permet de savoir combien on a de chance d'en avoir un en tirant au hasard

- Polygone de Newton : généralise Eisenstein

$P \in \mathbb{Z}[X]$ eg $2X^5+2X^4+6X^3+8X^2+1$

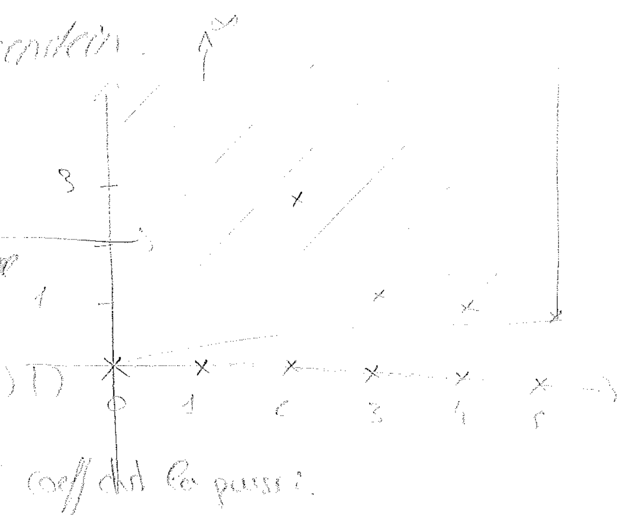
ℓ premier eg $\ell = 2$

Critère de Dumas (Prasolov)

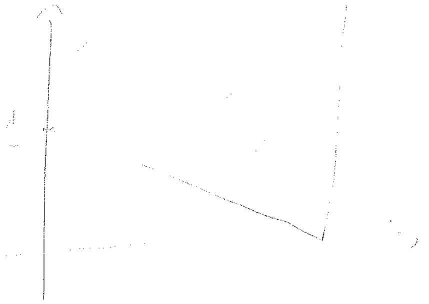
polygone = enveloppe convexe du gphe

$(i, \text{val } \ell\text{-adique}(\ldots))$

une pente ⇒ irr



Cas particulier : eisenstein :
Ifs de cette forme
une pente ⇒ irr.



Exercices

1 || p premier ≠ 2. Mq p est irred ds $\mathbb{Z}[i]$ ssi X^2+1 irred ds $\mathbb{Z}/p\mathbb{Z}[X]$

$\mathbb{Z}[i]$ eucl car 1.1 ⇒ ppal ⇒ (irr ⇔ premier)
⇕
idéal engendré premier
⇕
A/idéal engendré intègre

$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$

$\mathbb{Z}[i]/(p) \simeq \left(\mathbb{Z}[X]/(X^2+1)\right)/(p) = \mathbb{Z}[X]/(p, X^2+1)$ ← idéal engendré par p et X^2+1
↑ idéal

Et $\mathbb{Z}[X]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X]$ donc ↳ $\simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1) = \mathbb{F}_p[X]/(X^2+1)$

Donc p irred ⇔ p premier ⇔ $\mathbb{Z}[i]/(p)$ intègre ⇔ $\mathbb{F}_p[X]/(X^2+1)$ intègre
⇔ X^2+1 irr ds $\mathbb{F}_p[X]$
↑ encore l'histoire de $\mathbb{F}_p[X]$ ppal ⇒ (irr ⇔ premier)
↑ car $\mathbb{F}_p$ = corps.

|| En déduire que p somme de 2 carrés ssi $p \equiv 1\ (4)$

Rappels : carrés ds $\mathbb{F}_p$: $\forall a \in \mathbb{F}_p^*$, $a^{p-1} \equiv 1\ (p) \Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1\ (p)$
↑ pt thm de Fermat ↑ p impair ↑ $X^2-1 = (X-1)(X+1)$ + intègre.

Si $x = y^2$ alors $x^{p-1/2} = y^{p-1} = 1\ (p)$.

$\prod_{x \in \mathbb{F}_p^*} (X - x) = X^{p-1} - 1 = (X^{p-1/2} - 1)(X^{p-1/2} + 1)$ #{carrés} = $\frac{p-1}{2}$ = #{non carrés}
↑ S = carrés ↑ S' = non carrés

Donc $\forall a \in \mathbb{F}_p^*$ $\left(\frac{a}{p}\right) \equiv a^{p-1/2}\ (p)$
= 1 si a carré, $a \in \mathbb{F}_p^*$
-1 si a non carré, $a \in \mathbb{F}_p^*$
0 si p | a

p somme de 2 carrés $\Leftrightarrow p = a^2+b^2 = (a+ib)(a-ib)$, $a,b \in \mathbb{Z}$

$\Leftrightarrow X^2+1$ red dans $\mathbb{F}_p[X]$

irred de deg ≤ 3 $\Rightarrow$ $\exists a \in \mathbb{F}_p$, $a^2 = -1\ [p] \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1\ [p]$

$\Leftrightarrow \frac{p-1}{2} \in 2\mathbb{Z} \Leftrightarrow p = 1\ [4]$

non inv car inv de $\mathbb{Z}[i]$ $= \pm 1$ et $\pm i$

-1 = carré dans $\mathbb{F}_p$

Ex1 Soit $u \in End_{\mathbb{R}}(E)$, $\dim(E) = n < +\infty$. Alors il existe une droite ou un plan de E fixé par u

Utiliser la décomp en irr de χ_u + lemme des noyaux

3 Soit $P \in \mathbb{Z}[X]$, $\alpha_1 \dots \alpha_n$ les racines de P dans $\mathbb{C}$. $m = \max |\alpha_i|$

Pq Il existe $x_0 \in \mathbb{Z}$, $|x_0| > m+1$ tq $P(x_0)$ premier alors P irred dans $\mathbb{Z}[X]$

Si $P = QR$ dans $\mathbb{Z}[X]$. $P(x_0) = Q(x_0)R(x_0)$ donc $\begin{cases} Q(x_0) = 1 \\ R(x_0) = p \end{cases}$ (OPS).

$|x_0 - \alpha_i| > 1$ donc $\left|\prod_{i \in I \subset [\![1,n]\!]} (x_0 - \alpha_i)\right| > 1$ or $Q = \prod_{i \in I} (X - \alpha_i)$ pr un certain I.

$I \neq \emptyset$

Donc $I = \emptyset$ et $Q = 1$.

4 Soit $P = p_n X^n + \dots + p_0$ $\quad m = Ent(n+\frac{1}{2})$

Supposons qu'il existe $\alpha_1 \dots \alpha_n \in \mathbb{Z}$ tq $0 < |P(\alpha_i)| < m!/2^m$

Pq P irred dans $\mathbb{Z}[X]$

LAVIGNE Florian

N°141

dvt 1
1/1

DV 1 : Critère d'Eisenstein
(Cassini, Algèbre 1)

Dém du lemme de Gauss

(i) On pose $P = \sum_{k=0}^{n} a_k X^k$; $Q = \sum_{k=0}^{m} b_k X^k$; $PQ = \sum_{k=0}^{n+m} c_k X^k$.

Raisonnons par l'absurde et donc supposons que $c(PQ) \neq 1$. Il existe alors $p \in A$ premier avec $p \mid a_k$, pour tout $k \in [\![0; n+m]\!]$. On a alors dans $A/(p)[X]$:

$0 = \overline{PQ} = \overline{P}.\overline{Q}$. Comme p est premier, $A/(p)[X]$ est intègre. On aurait donc $\overline{P} = 0$ ou $\overline{Q} = 0$ ce qui est impossible, car P et Q sont primitifs

(ii) On remarque que $PQ = c(P)\,c(Q) \cdot \frac{P}{c(P)} \cdot \frac{Q}{c(Q)}$, avec $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ primitifs. Par (i), $c\left(\frac{P}{c(P)} \frac{Q}{c(Q)}\right) = 1$. Donc :

$$c(PQ) = c(P)\,c(Q).$$

Dém du critère

Raisonnons par l'absurde et supposons que P (et a fortiori $\tilde{P} := \frac{1}{c(P)} P$) est réductible dans $K[X]$.

$\exists R, S \in K[X]$, $\tilde{P} = RS$.

On a : $\exists \alpha, \beta \in A \setminus \{0\}$, $\alpha R \in A[X]$, $\beta S \in A[X]$.

De plus, comme $\alpha\beta \tilde{P} = (\alpha R).(\beta S)$, on a :

$$\alpha\beta = c(\alpha R).c(\beta S).$$

Ainsi : $P = \frac{c(P)}{\alpha\beta} \alpha\beta \tilde{P} = \underbrace{\left[\frac{c(P)}{c(\alpha R)} \alpha R\right]}_{=:U} . \underbrace{\left[\frac{1}{c(\beta S)} \beta S\right]}_{=:W}$

On sait que $U, W \in A[X]$. Donc P est réductible dans $A[X]$

De plus, $\overline{P} = \overline{a_n} X^n = \overline{U}.\overline{W}$. Si on écrit $U = \sum_{k=0}^{i} u_k X^k$ et $W = \sum_{k=0}^{j} w_k X^k$, on trouve $\overline{u_i}.\overline{w_j} = \overline{a_n} \neq 0$. Alors $\deg \overline{U} = i$ et $\deg \overline{W} = j$. Par unicité de la décomposition en irréductibles, $\overline{U} = \overline{u_i} X^i$ et $\overline{W} = \overline{w_j} X^j$. Dans ce cas, $p \mid u_0$ et $p \mid w_0$. On aurait $p^2 \mid u_0 w_0 = a_0$ ce qui est impossible.

LAVIGNE Florian

N°141
dvl2
1/2

DVL : Algorithme de Berlekamp (Beck, Objectif Agrégation)

On pose $P = P_1 \dots P_r \in \mathbb{F}_q[X]$, avec P_i irréductibles sur $\mathbb{F}_q[X]$ et pour $i \neq j$, $P_i \neq P_j$.

* Montrons que $r = \dim(\ker(S_p - id))$

Soit $\tilde{S}_p = \varphi \circ S_p \circ \varphi^{-1} : K_1 \times \dots \times K_r \to K_1 \times \dots \times K_r$
$(x_1, \dots, x_r) \mapsto (x_1^q, \dots, x_r^q)$

Alors $(x_1, \dots, x_r) \in \ker(\tilde{S}_p - id) \iff (x_1^q, \dots, x_r^q) = (x_1, \dots, x_r)$
$\iff \forall i \in [\![1, r]\!], x_i^q = x_i$ [dans K_i]

Soit $i : \mathbb{F}_q \hookrightarrow K$ extension de corps. Montrons que : $i(\mathbb{F}_q) = \{x \in K, x^q = x\} =: \dots$

Par le théorème de Lagrange, on a :

$$\forall x \in \mathbb{F}_q^\times, \quad x^{q-1} = 1$$

Donc $\mathbb{F}_q \subseteq E$. Or le polynôme $X^q - X$ admet au plus q racines. On sait que $\#\, i(\mathbb{F}_q) = q$. Donc $E = i(\mathbb{F}_q)$.

Ainsi : $(x_1, \dots, x_r) \in \ker(\tilde{S}_p - id) \iff \forall i \in [\![1, r]\!], x_i \in \mathbb{F}_q$.

Cela revient à dire que $\ker(\tilde{S}_p - id) = \mathbb{F}_q^r$.

Comme $\ker(S_p - id) \xrightarrow{\varphi} \ker(\tilde{S}_p - id)$, on a :

$$\dim \ker(S_p - id) = \dim \ker(\tilde{S}_p - id) = r$$

On a bien : $r = \dim(\ker(S_p - id))$.

** Supposons que $r > 1$ par la suite. On sait que l'ensemble des polynômes $U \bmod P$, avec U non constante modulo P, est la droite vectorielle de $\mathbb{F}_q[X]/(P)$ dirigée par 1.

Comme $\dim \ker(S_p - id) > 1$, il existe V.

** Montrons que pour $\alpha \in \mathbb{F}_q$, $\mathrm{PGCD}(V - \alpha, P) = \prod_{i, P_i \mid V - \alpha} P_i$.

En effet, $\mathrm{PGCD}(V - \alpha, P) \mid P$. Donc :

$\exists I_\alpha \subseteq [\![1, r]\!]$, $\mathrm{PGCD}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$.

On $\mathrm{PGCD}(P, V - \alpha) \mid V - \alpha$. Par le lemme de Gauss, $P_i \mid V - \alpha$, pour $i \in I_\alpha$.

On a donc bien $\mathrm{PGCD}(P, V - \alpha) = \prod_{i, P_i \mid V - \alpha} P_i$.

Or $(V \bmod P) \in \ker(S_p - id) \Leftrightarrow V \bmod P_i \in \mathbb{F}_q$, $\forall i \in [\![1, r]\!]$ d'après

$\Leftrightarrow \forall i, \exists \alpha_i \in \mathbb{F}_q, P_i \mid V - \alpha_i$.

Ainsi : $\alpha_i = \alpha \Leftrightarrow V - \alpha = 0 \bmod P_i \Leftrightarrow P_i \mid V - \alpha$.

Donc $I_\alpha = \{ i \in [\![1, r]\!], \alpha_i = \alpha \}$.

Alors $P = \prod_\alpha \prod_{i \in I_\alpha} P_i = \prod_\alpha PGCD(P, V - \alpha)$ (*)

** <u>Montrons que l'algorithme se termine.</u>

Si pour tout $i \neq j$, $\alpha_i = \alpha_j = \alpha$, alors $V \equiv \alpha [P]$, par le lemme chinois, ce qui est impossible.

Ainsi parmis les polynômes dans (*) il en existe deux qui ne sont pas triviaux.

Donc $\#\{Q$ irréductible, $Q \mid PGCD(P, V-\alpha)\} < r$.

<u>Commentaires</u> :

- ajouter cmt on se ramène à P sans facteurs carrés
  - ↳ prendre PGCD(P,P') et diviser P par ce PGCD (en faisant un peu attention)
- aller + vite sur la première partie
- Efficacité : Pivot de Gauss