Séminaire Delange-Pisot-Poitou. Théorie des nombres

Maurice Mignotte

Critères d'irréductibilité des polynômes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, n° 1 (1971-1972), exp. n° 7, p. 1-8

<http://www.numdam.org/item?id=SDPP_1971-1972__13_1_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
13e année, 1971/72, n° 7, 8 p.

6 décembre 1971

CRITÈRES D'IRRÉDUCTIBILITÉ DES POLYNOMES

par Maurice MIGNOTTE

I. Introduction

1. Généralités.

Dans le cas où P est un polynôme à coefficients dans $\underset{\sim}{Z}$, les critères qui suivent sont du type suivant : si P prend "assez" de valeurs qui sont des nombres premiers ou ± 1, alors P est irréductible sur $\underset{\sim}{Z}$.

La nature de tous ces critères n'est pas effective en ce sens que, pour montrer que l'un d'entre eux s'applique, il faut, a priori, un nombre de vérifications arbitrairement grand. Par contre, ils ne font intervenir que les valeurs prises par P.

2. Notations.

$\underset{\sim}{A}$: anneau intègre commutatif,

$\underset{\sim}{K}$: corps des fractions de $\underset{\sim}{A}$, on suppose $\underset{\sim}{K} \neq \underset{\sim}{A}$ (ce qui implique $\underset{\sim}{A}$ infini),

$\underset{\sim}{U}$: ensemble des "unités" de $\underset{\sim}{A}$ (éléments de A inversibles dans $\underset{\sim}{A}$),

$n = \operatorname{card} \underset{\sim}{U}$,

$\underset{\sim}{D}$: ensembles des diviseurs des éléments $e - e'$, où e et e' parcourent $\underset{\sim}{U}$ avec $e \neq e'$,

$k = \operatorname{card} \underset{\sim}{D}$.

Un élément x de $\underset{\sim}{A}$ est dit irréductible si, pour toute égalité $x = yz$, y et z dans $\underset{\sim}{A}$, on a $y \in \underset{\sim}{U}$ ou $z \in \underset{\sim}{U}$. On note $\underset{\sim}{I}$ l'ensemble des éléments irréductibles de $\underset{\sim}{A}$. P désignera toujours un polynôme de $\underset{\sim}{A}[X]$ de degré $\deg(P)$.

Soit E un sous-ensemble de $\underset{\sim}{A}$, on pose

$$u_E(P) = \operatorname{card}\{x \in E \mid P(x) \in \underset{\sim}{U}\},$$
$$i_E(P) = \operatorname{card}\{x \in E \mid P(x) \in \underset{\sim}{I}\}.$$

Si $E = A$, on supprimera l'indice E.

On dira que le polynôme P est irréductible dans $\underset{\sim}{A}[X]$ si, pour toute égalité $P = P_1 P_2$, P_1 et P_2 dans $\underset{\sim}{A}[X]$, on a $\deg(P_1) = 0$ ou $\deg(P_2) = 0$. Si P n'est pas irréductible, il sera dit réductible (dans $\underset{\sim}{A}[X]$).

3. Une inégalité fondamentale.

Supposons P réductible, $P = P_1 P_2$ avec P_1 et P_2 dans $\underset{\sim}{A}[X]$, on peut remarquer que :

$x \in \underset{\sim}{A}$ et $P(x)$ irréductible $\Longrightarrow$ $P_1(x)$ ou $P_2(x)$ unité,

$x \in \underset{\sim}{A}$ et $P(x)$ unité $\Longrightarrow$ $P_1(x)$ et $P_2(x)$ unités.

Avec les notations précédentes, on en déduit le lemme suivant.

LEMME I.1. - Si P réductible alors

$$i_E(P) + 2u_E(P) \leqslant u_E(P_1) + u_E(P_2) \quad (1)$$

Pour obtenir un critère d'irréductibilité, la démarche sera la suivante.

Sous certaines conditions,

(a) $u_E(Q) \leqslant M$, pour tout $Q \in \underset{\sim}{A}[X]$ tel que $1 \leqslant \deg Q \leqslant \deg P$.

Si P est réductible, alors d'après les inégalités (1) et (a), il vient

(b) $i_E(P) + 2u_E(P) \leqslant 2M$.

D'où le critère : si P vérifie

(c) $i_E(P) + 2u_E(P) > 2M$,

alors P est irréductible.

Le but de toute la suite sera donc de trouver des situations dans lesquelles la condition (a) soit vérifiée.

On distinguera plusieurs cas suivant la nature de $\underset{\sim}{A}$.

Dans toute la suite, Q désignera un polynôme de $\underset{\sim}{A}[X]$ tel que $1 \leqslant \deg Q \leqslant \deg P$.

II. Cas d'un anneau ayant un nombre fini d'unités.

1. Cas général.

Du fait que $\underset{\sim}{A}$ est intègre, on a le lemme suivant.

LEMME II.1. - Tout polynôme Q non constant vérifie $u(Q) \leqslant n \deg Q$.

En appliquant ce lemme au cas où $Q = P_1$ et $Q = P_2$, on déduit de (1) l'inégalité

$$i(P) + 2u(P) \leqslant n \deg P .$$

D'où le critère suivant.

CRITÈRE 1. - Si P vérifie

$$i(P) + 2u(P) > n \deg P ,$$

alors P est irréductible dans $\underset{\sim}{A}[X]$.

Exemple 1. - Si $a_1, \ldots, a_d$ sont des éléments distincts de $\underset{\sim}{A}$ et si $n = 1$, alors le polynôme $P = (X - a_1) \ldots (X - a_d) + 1$ est irréductible dans $\underset{\sim}{A}[X]$.

2. Cas où $\underset{\sim}{D}$ est fini.

Soient $e_1, \ldots, e_n$ les éléments de $\underset{\sim}{U}$. On note

$$u_i(Q) = \operatorname{card}\{x \in A \mid Q(x) = e_i\} .$$

On peut supposer $u_i(Q) \geqslant \ldots \geqslant u_n(Q)$.

LEMME II.2. - Pour tout polynôme Q non constant, on a $u(Q) \leqslant \deg(Q) + k$.

Démonstration. - Si $u(Q) - \deg(Q) \leqslant 0$, c'est fini. Sinon, on a $u_2 \geqslant 1$. Désignons par a_1 , ... , a_{u_1} les éléments x de $\underset{\sim}{A}$ tels que $Q(x) = e_1$. Q est donc de la forme

$$Q(X) = (X - a_1) \ldots (X - a_{u_1}) R(X) + e_1 ,$$

où $R \in \underset{\sim}{A}[X]$.

Soit $x \in \underset{\sim}{A}$ tel que $Q(x) = e_i$, $i \geqslant 2$, alors

$$(x - a_1) \ldots (x - a_{u_1}) R(x) + e_1 = e_i .$$

Ainsi les $(x - a_\lambda)$ sont des éléments de $\underset{\sim}{D}$. Ceci montre deux choses :

1° $(x - a_1)$ peut prendre au plus k valeurs distincte, donc il y a au plus k valeurs de x possibles. Autrement dit,

$$u_2(Q) + \ldots + u_n(Q) \leqslant k .$$

2° Les éléments $(x - a_1)$, ... , $(x - a_{u_1})$ étant distincts, on a $u_1 \leqslant k$.

La première remarque, jointe au fait que $u_1 \leqslant \deg(Q)$, montre que

$$u(Q) \leqslant \deg(Q) + k .$$

La seconde ne sera pas utilisée.

CRITÈRE 2. - Si P vérifie

$$i(P) + 2u(P) > \deg(P) + 2k ,$$

alors P est irréductible dans $\underset{\sim}{A}[X]$.

Exemple 2. - Si a_1 , ... , a_d sont des éléments distincts de $\underset{\sim}{A}$ et si $d > 2k$, le polynôme $P = (X - a_1) \ldots (X - a_d) + 1$ est irréductible dans $\underset{\sim}{A}[X]$.

3. Applications.

Dans ce paragraphe, on suppose de plus que $\underset{\sim}{A}$ est intégralement clos. Cette hypothèse implique que si $P \in \underset{\sim}{A}[X]$ est irréductible dans $\underset{\sim}{A}[X]$ et unitaire, alors P est irréductible dans $\underset{\sim}{K}[X]$. Les exemples 1 et 2 ont pour conséquences respectives les applications suivantes.

APPLICATION 1. - Si $n = 1$, le corps $\underset{\sim}{K}$ admet des extensions algébriques de degré quelconque.

APPLICATION 2. - Si k est fini, le corps $\underset{\sim}{K}$ admet des extensions algébriques de degré quelconque $> 2k$.

III. Cas des corps quadratiques imaginaires.

$\underset{\sim}{K}$ désigne un corps quadratique imaginaire,

$\underset{\sim}{K} = \mathbb{Q}(\sqrt{-C})$ avec C entier positif quadratfrei,

$\underset{\sim}{A}$ désigne l'anneau des entiers de K.

On pose $f(P) = u(P) - \deg(P)$, avec ces notations le lemme I.1 devient, avec $E \subset \underset{\sim}{A}$, le lemme suivant.

LEMME III.1. - Si P est réduit alors

$$i(P) + 2u(P) \leqslant f(P_1) + f(P_2) + \deg(P) . \tag{2}$$

Et le lemme II.2 prend la forme suivante.

LEMME III.2. - Pour tout polynôme non constant, on a $f(Q) \leqslant k$.

En fait, dans le cas présent, on peut améliorer très sensiblement cette majoration. On doit distinguer trois cas : $C \neq 1$ et $\neq 3$, $C = 1$, $C = 3$.

Voici un tableau donnant le maximum de $f(Q)$ suivant $\deg(Q)$.

deg Q	1	2	3	4	5	6	7	$\geqslant 8$
$C \neq 1$ et 3	1	2	1	0	0	0	0	0
$C = 1$	3	4	2	2	1	1	0	0
$C = 3$	5	3	3	2	1	1	1	0

Démontrons ce résultat dans le premier cas ($C \neq 1$ et $\neq 3$). On a $\underset{\sim}{U} = \{1 , -1\}$, $\underset{\sim}{D} = \{1 , -1 , 2 , -2\}$.

Si $\deg Q = 1$, alors $f(Q) \leqslant n \deg Q - \deg Q = 1$, valeur atteinte pour $Q = X$.

Si $\deg Q = 2$, on a $f(Q) \leqslant n \deg Q - \deg Q = 2$, valeur atteinte pour $Q = X^2 + X - 1$.

Reprenons les notations du lemme II.2, on a alors le lemme suivant.

LEMME III.1.- Si $u_1 = 3$, alors $u_2 \leqslant 1$, et si $u_1 > 3$, alors $u_2 = 0$.

Démonstration. - Si $u_1 = 3$, Q se met sous la forme

$$Q = (X - a_1)(X - a_2)(X - a_3)\, R(X) + e_1 ,$$

et si $Q(x) = e_2$, alors $(x - a_1)(x - a_2)(x - a_3) \in \underset{\sim}{D}$, du fait que les a_i sont distincts, il est facile de voir qu'il y a au plus un choix de x convenable, soit $u_2 \leqslant 1$. Si $u_1 \geqslant 4$, on utilise le fait qu'il n'existe aucun x tel que

$$(x - a_1)(x - a_2)(x - a_3)(x - a_4) \in \underset{\sim}{D} ,$$

ce qui est évident.

Revenons à la démonstration initiale.

Si $\deg(Q) = 3$ et si $u_1 \leqslant 2$, on a clairement $f \leqslant 2n - 3 = 1$, sinon on a $u_1 = 3$ et $u_2 = 1$ et $f \leqslant 3 + 1 - 3 = 1$ (atteint pour $Q = X^3 + 2X^2 - X - 1$).

Si $\deg(Q) \geqslant 4$, on utilise encore le lemme III.3, d'où $f \leqslant 0$.

Posons

$$F(q) = \max_{\deg Q = q} f(Q) .$$

On obtient alors le raffinement suivant du critère 2 de II.2.

CRITÈRE 3. - Si P vérifie

$$i(P) + 2u(P) > \deg P + \max_{d_1+d_2=\deg P} (F(d_1) + F(d_2)) ,$$

alors, P est irréductible dans $\underset{\sim}{A}[X]$.

Remarque. - Si $\underset{\sim}{A} = \underset{\sim}{Z}$, les résultats sont les mêmes que pour le premier cas ($C \neq 1$ et $\neq 3$).

Une application. - Nous nous proposons de résoudre le problème suivant : Soient $a_1 , \ldots , a_d$ des entiers rationnels distincts, quelles sont les valeurs de d telles que le polynôme $P = (X - a_1) \ldots (X - a_d) + 1$ soit irréductible sur $\underset{\sim}{Z}$ et sur tous les corps quadratiques imaginaires ? Montrons que P est irréductible, sauf peut-être pour $d = 2$ ou 4 .

Remarquons avant tout que, si P est irréductible sur $\underset{\sim}{Z}$ et réductible dans un corps quadratique K , la décomposition de P sur K est de la forme $P_1 P_2$, où P_1 et P_2 ont le même degré, en particulier P a un degré pair.

Résolvons d'abord le problème sur $\underset{\sim}{Z}$. Si $d \geqslant 5$, le tableau montre que P est irréductible, en effet, $f(P) \geqslant 5$. Si $d = 1$, P est irréductible. Si $d = 2$, il se peut que P ne soit pas irréductible $((X - 1)(X + 1) + 1 = X^2)$, de même pour $d = 4$ $((X - 2)(X - 1) X(X + 1) + 1 = (X^2 - X - 1)^2)$.

Si $d = 3$, le polynôme P ne peut avoir de racine, car le produit de trois nombres entiers distincts ne peut être égal à $- 1$, P est irréductible.

Dans le cas d'un corps quadratique, il suffit de considérer le cas où d est pair. Si $d \geqslant 6$, le tableau permet de conclure à l'irréductibilité de P , sauf peut-être si $K = \underset{\sim}{Q}(\sqrt{-3})$. Si $d = 6$, on voit facilement qu'un diviseur éventuel P_1 (de degré 3) ne peut prendre des valeurs unitaires en 6 points entiers $a_1 , \ldots , a_6$.

IV. Cas des corps de nombres.

1. Notations et préliminaires.

$\underset{\sim}{K}$: corps de nombres de degré n ,

$\underset{\sim}{A}$: anneau des entiers de K ,

$\underset{\sim}{U}$: ensemble des unités de K .

Il y a n isomorphismes distincts $\sigma_i : \underset{\sim}{K} \longrightarrow \underset{\sim}{C}$, on peut les numéroter de telle sorte que $\sigma_i(\underset{\sim}{K}) \subset \underset{\sim}{R}$ pour $i = 1 , \ldots , r_1$, et $\sigma_{i+r_2} = \overline{\sigma_i}$ pour

$$i = r_1 + 1 , \ldots , r_1 + r_2 ,$$

avec $n = r_1 + 2r_2$.

On considère l'application

$$L : \underset{\sim}{K}^* \to \underset{\sim}{R}^r , \quad r = r_1 + r_2 ,$$
$$x \mapsto L(x) = (\log|\sigma_1(x)| , \dots , \log|\sigma_n(x)|) .$$

On sait que le noyau de la restriction de L à $\underset{\sim}{A}^*$ est constitué par les w racines de l'unité contenues dans $\underset{\sim}{K}$ et que $L(U)$ est un sous-groupe discret R de $\underset{\sim}{R}^r$ de rang $s = r - 1$.

On considérera toujours des polynômes unitaires de $\underset{\sim}{A}[X]$ qui ne s'annulent pas à l'origine.

Si $P = a_0 X^d + a_1 X^{d-1} + \dots + a_d$, on pose

$$S(P) = \max_i \sum_{k=0}^{d} |\sigma_i(a_k)| ,$$
$$|P| = \max_i \left(\sum_{k=0}^{d} |\sigma_i(a_k)|^2\right)^{1/2} .$$

Si $P = P_1 P_2$, nous allons majorer $S(P_1)$ et $S(P_2)$ en fonction de $|P|$.

2. Majorations de $S(P_1)$ et $S(P_2)$.

LEMME IV.1. - Soit $f(z) = \sum_0^\infty b_m z^m$ une fonction holomorphe pour $|z| \leqslant 1$ telle que $f(0) \neq 0$. Soient $\zeta_1 , \dots , \zeta_\nu$ les racines de f dans le disque $|z| < 1$ (chacune répétée autant de fois que son ordre de multiplicité), on a alors

$$|b_0| \prod_{j=1}^{\nu} |\zeta_j|^{-1} \leqslant \left(\sum_0^\infty |b_m|^2\right)^{1/2} .$$

Démonstration. - Posons

$$g(z) = f(z) \prod_{j=1}^{\nu} (1 - \bar{\zeta}_j z)/(z - \zeta_j) = \sum_0^\infty c_m z^m .$$

g est holomorphe pour $|z| \leqslant 1$, de plus $|g(z)| = |f(z)|$ si $|z| = 1$. On en déduit

$$\sum_0^\infty |b_m|^2 = 1/2\pi \int_0^{2\pi} |f(e^{i\delta})|^2 \, d\delta = 1/2\pi \int_0^{2\pi} |g(e^{i\delta})|^2 \, d\delta = \sum_0^\infty |c_m|^2 .$$

Mais on a

$$|c_0| = |b_0| \prod_{j=1}^{\nu} |\zeta_j|^{-1} ,$$

d'où le lemme.

En appliquant ce résultat au polynôme $\sigma_i P$, on obtient facilement les inégalités

$$S(P_1) \leqslant 2^{d_1} |P| ,$$
$$S(P_2) \leqslant 2^{d_2} |P| .$$

3. Premier choix de E .

Soit $\| \ \|$ la norme euclidienne de $\underset{\sim}{R}^r$, on pose

$E(a) = \{x \in \underset{\sim}{A} \mid h(x) \leqslant a\}$, où $h(x) = \max_i |\sigma_i(x)|$,
$B(b) = \{y \in \underset{\sim}{R}^r \mid \|y\| \leqslant b\}$,

$u_a(P) = \{x \in E(a) \mid P(x) \in \underset{\sim}{U}\}$,
$i_a(P) = \{x \in E(a) \mid P(x)$ irréductible dans $\underset{\sim}{A}\}$.

Soit Q un polynôme non constant de degré $< d$ tel que $S(Q) \leq S$ avec $S = 2^{d-1} |P|$.

Soit $E^*(a) = \{x \in E(a) \mid Q(x) \neq 0\}$.

On a les inégalités suivantes

$$u_a(Q) \leq \deg Q \ \mathrm{card}(Q(E^*(a)) \cap U) ,$$

$$\mathrm{card}(Q(E^*(a)) \cap U) < w.\mathrm{card}(J \cap R) , \text{ avec } J = L(Q(E^*(a))) .$$

Pour majorer card $J \cap R$, on procèdera en deux étapes

(α) $J \subset B(b)$ (lemme 2)

(β) on majore $m = \mathrm{card}(B(b) \cap R)$ (lemme IV.3 ci-dessous).

On obtient alors

$$u_a(Q) \leq \deg Q.w.m .$$

Cette inégalité s'applique aux polynômes P_1 et P_2 , d'où

$$u_a(P_1) + u_a(P_2) \leq \deg P.w.m .$$

LEMME IV.2. - Pour tout $a \geq e$, on a

$$Q(x) \neq 0 \text{ et } h(x) \leq a \Rightarrow \|L(Q(x))\| \leq r_n(\deg(Q) + \log S) \log a .$$

Démonstration. - Posons $x' = Q(x)$.

On a les inégalités successives

$$\|L(x')\| \leq r \max_i |\log|\sigma_i(x')|| ,$$

$$|\sigma_i(x')| \leq S a^{\deg Q} \text{ pour } i = 1 , \dots , r ,$$

$$|\sigma_i(x')| \geq \prod_{j \neq i} (\sigma_j(x'))^{-1} \text{ (du fait que } |\mathrm{norme}(x')| \geq 1) .$$

Le lemme en résulte aussitôt.

LEMME IV.3. - Pour tout $b \geq 1$, il existe une constante C_0 explicite, qui ne dépend que de $\underset{\sim}{K}$, telle que

$$m = \mathrm{card}(B(b) \cap R) \leq C_0 b^s .$$

C'est évident : il s'agit de majorer le nombre de points d'un réseau de rang s contenu dans une boule de rayon b ; de plus, on peut calculer explicitement le volume et le diamètre de la maille du réseau R .

Grâce qu lemme I.1, on obtient finalement le théorème suivant.

THÉORÈME IV.1. - Soit $P \in \underset{\sim}{A}[X]$ unitaire et réductible, il existe une constante C , calculable explicitement qui ne dépend que de deg P , $|P|$ et $\underset{\sim}{K}$ telle que

$$i_a(P) + 2u_a(P) \leq C(\log a)^s , \text{ si } a \geq e .$$

CRITÈRE 1. - S'il existe $a \geq e$ tel que

$$i_a(P) + 2u_a(P) > C(\log a)^s ,$$

alors P est irréductible dans $\underset{\sim}{K}[X]$.

4. Deuxième choix de E.

On reprend les notations du n° 2. En particulier, on a $S \geq 1$.

Si on pose

$$E'(S) = \{x \in A \mid |\sigma_i(x)| > S , \ i = 1 , \ldots , r\} ,$$

on voit que

$$x \in E'(S) \Rightarrow |\sigma_i(P_1(x)| \geq |\sigma(x)|^{d_1} - (\mathcal{M}(P_1) - 1) \ |\sigma(x)|^{d_1-1} > S^{d_1-1} \geq 1 .$$

Ceci est vrai pour tout σ_i, il en résulte que

$$x \in E'(S) \Rightarrow P_1(x) \notin \underset{\sim}{U} ,$$

de même

$$x \in E'(S) \Rightarrow P_2(x) \notin \underset{\sim}{U} .$$

D'où le théorème ci-dessous.

THÉORÈME IV.2. - Si P est réductible, pour $S = 2^{d-1} |P|$, on a

$$x \in E'(S) \Rightarrow P(x) \text{ est réductible dans } \underset{\sim}{A} .$$

CRITÈRE 2. - S'il existe $x \in E'(S)$ tel que P(x) soit irréductible dans $\underset{\sim}{A}$, alors P est irréductible dans $\underset{\sim}{K}[X]$ (P est unitaire).

CRITÈRE 3. - S'il existe $x \in \underset{\sim}{Z}$ tel que $|x| > 2^{d-1} |P|$ et que P(x) soit irréductible dans $\underset{\sim}{A}$, alors P est irréductible dans $\underset{\sim}{K}[X]$.

(Texte reçu le 13 décembre 1971)

Maurice MIGNOTTE
Université de Paris-Nord
Centre Scientifique universitaire
Place du 8 mai 1945
93 SAINT-DENIS.