

# 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](http://www.numdam.org/item?id=SDPP_1971-1972__13_1_A6_0)

© Séminaire Delange-Pisot-Poitou. Théorie des nombres  
(Secrétariat mathématique, Paris), 1971-1972, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## CRITÈRES D'IRRÉDUCTIBILITÉ DES POLYNÔMES

par Maurice MIGNOTTE

### I. Introduction

#### 1. Généralités.

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

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.

$\underline{A}$  : anneau intègre commutatif,

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

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

$n = \text{card } \underline{U}$ ,

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

$k = \text{card } \underline{D}$ .

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

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

$$u_E(P) = \text{card}\{x \in E \mid P(x) \in \underline{U}\},$$

$$i_E(P) = \text{card}\{x \in E \mid P(x) \in \underline{I}\}.$$

Si  $E = \underline{A}$ , on supprimera l'indice  $E$ .

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

#### 3. Une inégalité fondamentale.

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

$$x \in \underline{A} \text{ et } P(x) \text{ irréductible} \implies P_1(x) \text{ ou } P_2(x) \text{ unité,}$$

$x \in \underline{A}$  et  $P(x)$  unité  $\implies P_1(x)$  et  $P_2(x)$  unités.

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

**LEMME J.1.** - Si  $P$  réductible alors

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

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

Sous certaines conditions,

$$(a) \quad u_E(Q) \leq M , \text{ pour tout } Q \in \underline{A}[X] \text{ tel que } 1 \leq \deg Q \leq \deg P .$$

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

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

D'où le critère : si  $P$  vérifie

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

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  $\underline{A}$ .

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

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

### 1. Cas général.

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

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

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

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

D'où le critère suivant.

**CRITÈRE 1.** - Si  $P$  vérifie

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

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

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

### 2. Cas où $D$ est fini.

Soient  $e_1, \dots, e_n$  les éléments de  $\underline{U}$ . On note

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

On peut supposer  $u_1(Q) \geq \dots \geq u_n(Q)$ .

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

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

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

où  $R \in \underline{A}[X]$ .

Soit  $x \in \underline{A}$  tel que  $Q(x) = e_i$ ,  $i \geq 2$ , alors

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

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

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

$$u_2(Q) + \dots + u_n(Q) \leq k.$$

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

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

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

La seconde ne sera pas utilisée.

**CRITÈRE 2.** - Si  $P$  vérifie

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

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

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

### 3. Applications.

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

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

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

III. Cas des corps quadratiques imaginaires.

$\tilde{K}$  désigne un corps quadratique imaginaire,  
 $\tilde{K} = \mathbb{Q}(\sqrt{-C})$  avec  $C$  entier positif quadratfrei,  
 $\tilde{A}$  désigne l'anneau des entiers de  $\tilde{K}$ .

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

**LEMME III.1. - Si  $P$  est réductible, alors**

$$(2) \quad i(P) + 2u(P) \leq f(P_1) + f(P_2) + \deg(P).$$

Et le lemme II.2 prend la forme suivante.

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

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	$\geq 8$
$C \neq 1$ et $\neq 3$	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  $\tilde{U} = \{1, -1\}$ ,  
 $\tilde{D} = \{1, -1, 2, -2\}$ .

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

Si  $\deg Q = 2$ , on a  $f(Q) \leq n \deg Q - \deg Q = 2$ , 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  $u_2 \leq 1$ , 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  $(x - a_1)(x - a_2)(x - a_3) \in \tilde{D}$ , 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  $u_2 \leq 1$ . Si  $u_1 \geq 4$ , on utilise le fait qu'il n'existe aucun  $x$  tel que

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

ce qui est évident.

Revenons à la démonstration initiale.

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

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

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  $\underline{A}[X]$  .

Remarque. - Si  $\underline{A} = \underline{Z}$  , 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  $a_1, \dots, a_d$  des entiers rationnels distincts, quelles sont les valeurs de  $d$  telles que le polynôme  $P = (X - a_1) \dots (X - a_d) + 1$  soit irréductible sur  $\underline{Z}$  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  $\underline{Z}$  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  $\underline{Z}$  . Si  $d \geq 5$  , le tableau montre que  $P$  est irréductible, en effet,  $f(P) \geq 5$  . 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  $d \geq 6$  , le tableau permet de conclure à l'irréductibilité de  $P$  , sauf peut-être si  $K = \underline{Q}(\sqrt{-3})$  . 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  $a_1, \dots, a_6$  .

#### IV. Cas des corps de nombres.

##### 1. Notations et préliminaires.

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

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

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

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

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

avec  $n = r_1 + 2r_2$  .

On considère l'application

$$L : \underline{\tilde{K}}^* \rightarrow \underline{\tilde{R}}^r, \quad r = r_1 + r_2,$$

$$x \mapsto L(x) = (\log |\sigma_1(x)|, \dots, \log |\sigma_n(x)|).$$

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

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

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

$$S(P) = \max_i \sum_{k=0}^d |\sigma_i(a_k)|,$$

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

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  $|z| \leq 1$  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

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

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  $|z| \leq 1$ , 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

$$S(P_1) \leq 2^{d_1} |P|,$$

$$S(P_2) \leq 2^{d_2} |P|.$$

## 3. Premier choix de $E$ .

Soit  $\| \cdot \|$  la norme euclidienne de  $\underline{\tilde{R}}^r$ , on pose

$$E(a) = \{x \in \underline{\tilde{A}} \mid h(x) \leq a\}, \quad \text{où } h(x) = \max_i |\sigma_i(x)|,$$

$$B(b) = \{y \in \underline{\tilde{R}}^r \mid \|y\| \leq b\},$$

$$u_a(P) = \{x \in E(a) \mid P(x) \in \underline{U}\},$$

$$i_a(P) = \{x \in E(a) \mid P(x) \text{ irréductible dans } \underline{A}\}.$$

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

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

On a les inégalités suivantes

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

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

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

$$(\alpha) \quad J \subset B(b) \quad (\text{lemme 2})$$

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

On obtient alors

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

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

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

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

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

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

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

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  $\underline{K}$ , telle que

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

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  $P \in \underline{A}[X]$  unitaire et réductible, il existe une constante  $C$ , calculable explicitement qui ne dépend que de  $\deg P$ ,  $|P|$  et  $\underline{K}$  telle que

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



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

$$i_a(P) + 2u_a(P) > C(\log a)^3,$$

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

4. Deuxième choix de  $E$ .

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

Si on pose

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

on voit que

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

Ceci est vrai pour tout  $\sigma_i$ , il en résulte que

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

de même

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

D'où le théorème ci-dessous.

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

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

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

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

(Texte reçu le 13 décembre 1971)

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