

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 18 (1972)  
**Heft:** 1: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** CRITÈRES D'IRRÉDUCTIBILITÉ DE POLYNOMES SUR UN CORPS DE NOMBRES  
**Autor:** Mignotte, Maurice  
**Kapitel:** IV. Premier choix de E  
**DOI:** <https://doi.org/10.5169/seals-45369>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

**Download PDF:** 19.01.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

$$|P_1|_1 \leq 2^{d_1} |P|_2,$$

où  $d_1$  désigne le degré de  $P_1$ .

#### IV. PREMIER CHOIX DE $E$

Si  $x$  est un élément de  $A$ , on définit la hauteur de  $x$  par la formule

$$h(x) = \max_i |\sigma_i(x)|.$$

Soit  $Q$  un polynôme unitaire à coefficients dans  $A$  et qui ne s'annule pas à l'origine. Nous nous proposons de majorer le nombre de points  $x$  de  $A$  de hauteur au plus égale à  $a$  et tels que  $Q(x)$  soit une unité.

Nous allons utiliser le plongement logarithmique de  $K^*$ . Il nous faut encore introduire quelques définitions.

Soit  $r_1$  le nombre des indices  $i$  tels que l'image de  $K$  par  $\sigma_i$  soit incluse dans le corps des réels; alors les autres indices sont en nombre pair  $2r_2$ . On peut numéroter les  $\sigma_i$  de sorte que l'image de  $\sigma_i$  soit contenue dans  $\mathbf{R}$  pour  $i \leq r_1$  et que  $\sigma_{j+r_2} = \bar{\sigma}^j$  pour  $r_1 + 1 \leq j \leq r_1 + r_2$ .

Le plongement logarithmique de  $K^*$  dans  $\mathbf{R}^{r_1+r_2}$  est l'application  $L$  définie par la flèche

$$x \rightarrow (\text{Log } |\sigma_1(x)|, \dots, \text{Log } |\sigma_{r_1+r_2}(x)|).$$

Soient  $A^*$  l'ensemble des entiers non nuls et  $U$  l'ensemble des unités de  $A$ . On sait que le noyau de la restriction de  $L$  à  $A^*$  est constitué par les racines de l'unité contenues dans  $K$ .

L'image  $L(U)$  est contenue dans l'hyperplan  $W$  d'équation

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0.$$

Ceci ne fait que traduire le fait que  $x$  est une unité si et seulement si sa norme a pour module 1.

On montre facilement que l'image  $L(U)$  est un sous-groupe discret de  $W$ ; son rang est donc majoré par  $r = r_1 + r_2 - 1$ . En fait le théorème de Dirichlet dit que le rang de  $L(U)$  est exactement  $r$ , mais cette majoration nous suffira.

Revenons au polynôme  $Q$  et posons

$$u_a(Q) = \text{Card} \{ x \mid x \in A, h(x) \leq a \text{ et } Q(x) \in U \}$$

Nous cherchons à majorer  $u_a(Q)$ .

Un polynôme de degré donné ne peut prendre une certaine valeur qu'un nombre de fois au plus égal à son degré.

D'où l'inégalité

$$u_a(Q) \leq \deg Q \cdot \text{card}(\{Q(x) \mid x \in A \text{ et } h(x) \leq a\} \cap U).$$

Désignons par  $w$  le nombre de racines de l'unité contenues dans  $K$ . D'après la caractérisation du noyau de  $L|_U$  et l'inégalité précédente, on obtient:

$$(1) \quad u_a(Q) \leq w \cdot \deg Q \cdot \text{card}(J \cap R),$$

où on a posé

$$J = L(\{Q(x) \mid x \in A \text{ et } h(x) \leq u\}), \quad R = L(U).$$

Pour majorer le nombre d'éléments de  $J \cap R$ , nous procéderons en deux étapes:

- 1° L'image  $J$  est contenue dans une certaine boule  $B$  de l'espace  $\mathbf{R}^{r_1+r_2}$ .
- 2° On majore le nombre d'éléments de  $R$  contenus dans la boule  $B$ .

*Première étape.*

Soit  $S$  un réel  $\geq 1$  qui sera fixé ultérieurement. On suppose que le polynôme satisfait à la condition

$$\|Q\|_1 \leq S.$$

Désignons par  $\|\cdot\|$  la norme euclidienne de  $\mathbf{R}^{r_1+r_2}$ .

Démontrons le résultat suivant:

LEMME 5. *Soit  $a \geq 2$ . Il existe une constante  $C_0$  explicite, qui ne dépend que de  $S$  et de  $K$ , telle que si  $x$  vérifie  $h(x) \leq a$  et si  $Q(x)$  est non nul on ait l'inégalité:*

$$\|L(Q(x))\| \leq C_0 \cdot \text{Log } a \cdot \deg Q.$$

*Démonstration:*

Posons  $x' = Q(x)$  pour un certain  $x$  de hauteur majorée par  $a$  et tel que  $Q(x)$  soit non nul.

On a d'abord l'inégalité évidente

$$\|L(x')\| \leq (r_1 + r_2) \max_i (|\text{Log } |\sigma_i(x')||).$$

Pour majorer  $|\text{Log } |\sigma_i(x')||$ , on majore  $\text{Log } |\sigma_i(x')|$  puis on le minore. Autrement dit, on encadre  $|\sigma_i(x')|$ .

— *majoration des  $|\sigma_i(x')|$ .*

Reprenons la notation

$$Q = b_0 X^d + b_1 X^{d-1} + \dots + b_d.$$

On a alors l'inégalité

$$|\sigma_i(x')| \leq \sum_{j=0}^d |\sigma_i(b_j x^{d-j})|.$$

On en déduit facilement l'inégalité

$$|\sigma_i(x')| \leq S a^d.$$

— *minoration des  $|\sigma_i(x')|$ .*

Le procédé est classique. Du fait que  $x'$  est entier non nul, il a une norme au moins égale à 1 en module. D'où l'inégalité

$$|\sigma_i(x')| \geq \prod_{j \neq i} |\sigma_j(x')|^{-1}.$$

Grâce à la majoration précédente des  $|\sigma_j(x')|$ , on obtient l'inégalité

$$|\sigma_i(x')| \geq |S a^d|^{1-n} \geq |S a^d|^{-n}.$$

De cet encadrement des  $|\sigma_i(x')|$ , on déduit la majoration

$$|\text{Log } |\sigma_i(x')|| \leq n \cdot \text{Log}(S a^d).$$

D'où l'inégalité

$$\|L(x')\| \leq (r_1 + r_2) n \cdot \text{Log}(S a^d).$$

Si on pose

$$\lambda = 1 + \frac{\text{Log } S}{\text{Log } 2},$$

en tenant compte de l'hypothèse  $a \geq 2$ , on voit que l'on a

$$\text{Log}(S a^d) \leq \lambda \text{Log } a.$$

D'où finalement l'inégalité

$$\|L(x')\| \leq \text{deg } Q \cdot C_0 \cdot \text{Log } a$$

où on a posé

$$C_0 = n(r_1 + r_2) \cdot \lambda.$$

Ceci achève la démonstration du lemme.

Le lemme équivaut à dire que  $J$  est contenu dans la boule  $B$  de rayon  $b = \deg Q \cdot C_0 \cdot \text{Log } a$ . Remarquons que  $b$  est au moins égal à  $\text{Log } 2$ .

*Deuxième étape.*

LEMME 6. *Soit  $b$  un réel au moins égal à  $\text{Log } 2$ . Il existe une constante  $C_1$  explicite, qui ne dépend que de  $K$ , telle que le nombre d'éléments du réseau  $R$  contenus dans la boule  $B$  de rayon  $b$  soit majoré par  $C_1 b^r$ .*

*Démonstration :*

Soit  $D$  le parallélotope fondamental de  $R$ .

Il est clair que le nombre  $m$  de points de  $R$  contenus dans la boule  $B$  est majoré par le nombre de mailles de  $R$  qui rencontrent  $B$ . De plus toutes les mailles qui rencontrent  $B$  sont contenues dans la boule  $B'$  de rayon  $b + S$ , où  $S$  désigne le diamètre de  $D$ .

En comparant les volumes (calculés dans  $W$ ), on obtient l'inégalité

$$m \cdot \text{vol}(D) \leq \text{vol } B'.$$

Soit  $V$  le volume de la boule unité. L'inégalité précédente conduit à

$$m \leq V(b + S)^r (\text{vol } D)^{-1}.$$

Comme  $b$  est au moins égal à  $\text{Log } 2$ , le nombre  $b + S$  est majoré par  $\mu b$

où  $\mu$  vaut  $1 + \frac{S}{\text{Log } 2}$ .

D'où l'inégalité

$$m \leq C_1 b^r,$$

où on a posé

$$C_1 = V\mu (\text{vol } D)^{-1}.$$

On voit que connaissant  $K$  on peut calculer explicitement  $S$  et  $\text{vol } D$ , donc  $C_1$  est bien explicite. Ceci achève la démonstration du lemme.

*Conclusion.*

THÉORÈME 1. Soit  $P$  un polynôme unitaire à coefficients entiers et qui ne s'annule pas à l'origine. Pour tout  $a \geq 2$ , il existe une constante  $C$  calculable explicitement et qui ne dépend que de  $\deg P$ ,  $|P|_2$  et  $K$ , telle que si  $P$  est réductible alors on a l'inégalité :

$$i_a(P) + 2u_a(P) \leq C (\text{Log } a)^r .$$

(Où  $i_a(P)$  désigne le nombre de points  $x$  de hauteur majorée par  $a$  et tels que  $P(x)$  soit un élément irréductible de  $A$ ).

*Démonstration :*

Soient  $P_1$  et  $P_2$  deux polynômes à coefficients dans  $A$  et de produit  $P$ . D'après le lemme 1, nous avons l'inégalité

$$i_a(P) + 2u_a(P) \leq u_a(P_1) + u_a(P_2) .$$

Soit  $S$  le nombre  $2^{d-1} |P|_2$ ; le lemme 4 montre que  $|P_1|_1$  et  $|P_2|_1$  sont majorés par  $S$ .

Nous pouvons maintenant appliquer les lemmes 5 et 6 aux polynômes  $P_1$  et  $P_2$ . En tenant compte de l'inégalité (1), nous obtenons les majorations

$$\begin{aligned} u_a(P_1) + u_a(P_2) &\leq w C_1 (C_0 \text{Log } a)^r ((\deg P_1)^{r+1} + (\deg P_2)^{r+1}) \\ &\leq 2w C_1 (C_0 \text{Log } a)^r (\deg P)^{r+1} . \end{aligned}$$

Ceci achève la démonstration du théorème.

*Remarque.* L'inégalité  $a \geq 2$  n'a été introduite que pour éviter des complications inutiles. Le théorème reste vrai pourvu que l'on suppose  $a \geq \alpha_0$  avec  $\alpha_0$  fixé,  $\alpha_0 > 1$ , mais cette fois la constante  $C$  dépend de  $\alpha_0$ .

CRITÈRE 1. S'il existe  $a \geq 2$  tel que l'on ait l'inégalité

$$i_a(P) + 2u_a(P) > C (\text{Log } a)^r$$

alors le polynôme  $P$  est irréductible dans  $K[X]$ .

## V. DEUXIÈME CHOIX DE $E$

THÉORÈME 2. Soit  $P$  un polynôme unitaire réductible qui ne s'annule pas à l'origine et à coefficients dans  $A$ . Désignons par  $S$  le nombre  $2^{d-1} |P|_2$ , où  $d$  est le degré de  $P$ .