Zeitschrift: 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
DOI: https://doi.org/10.5169/seals-45369

CRITÈRES D'IRRÉDUCTIBILITÉ DE POLYNOMES SUR UN CORPS DE NOMBRES

par Maurice MIGNOTTE

I. INTRODUCTION

Désignons par K un corps de nombres et par A l'anneau des entiers de K. Nous ne considérerons que des polynômes unitaires à coefficients dans A.

Un élément x de A sera dit irréductible s'il n'est pas inversible dans A et s'il n'est pas égal au produit de deux éléments non inversibles de A. Un polynôme unitaire P à coefficients dans A sera dit irréductible s'il n'est pas constant et s'il n'est pas égal au produit de deux polynômes non constants et à coefficients dans A. Du fait que l'anneau A est intégralement clos, un polynôme unitaire à coefficients dans A est irréductible dans A si et seulement s'il est irréductible sur K. Dans toute la suite, il importera de ne pas confondre le fait qu'un polynôme P est irréductible et le fait, qu'en un point x de A, la valeur $P(x)$ est un élément irréductible de A.

Les deux critères d'irréductibilité qui font l'objet de ce travail sont de même nature: si un polynôme unitaire et à coefficients dans A prend en certains points de A suffisamment de valeurs qui sont des unités ou des éléments irréductibles de A, alors P est nécessairement irréductible.

Le point de départ consiste à remarquer que si P est le produit de deux polynômes P_1 et P_2 à coefficients dans A et si x est un point de A tel que $P(x)$ soit une unité ou un élément irréductible de A, alors l'un au moins des polynômes P_1 et P_2 prend au point x une valeur qui est une unité de A. Ceci conduit à chercher des majorations du nombre de points x, contenus dans certains domaines, où un polynôme Q peut prendre des valeurs qui sont des unités. Ces majorations font intervenir la hauteur des coefficients de Q; pour les appliquer aux polynômes P_1 et P_2 il est nécessaire de trouver une majoration des hauteurs des polynômes P_1 et P_2 en fonction de celle du polynôme P.

Nous choisirons deux domaines différents pour les points x; dans le premier cas les points considérés auront une hauteur bornée, dans le second cas chacun de leurs conjugués sera assez grand. Dans le premier cas nous

utiliserons le plongement logarithmique du corps K et le fait que l'image par ce plongement du groupe des unités est un réseau; il suffira de majorer la norme des images de $Q(x)$ pour des points x de hauteur bornée. Dans le second cas, nous utiliserons simplement le fait que si x a tous ses conjugués assez grands il en est de même de $Q(x)$ et donc que $Q(x)$ ne peut pas être une unité.

II. Une remarque préliminaire

Soit P un polynôme unitaire à coefficients dans A qui soit le produit de deux polynômes P_1 et P_2 à coefficients dans A. Les valeurs de ces polynômes en un point x de A donnent lieu à des remarques évidentes: Si $P(x)$ est un élément irréductible de A, l'un des deux éléments $P_1(x)$ et $P_2(x)$ au moins est une unité; si $P(x)$ est une unité, les deux éléments $P_1(x)$ et $P_2(x)$ de A sont des unités; d'où l'inégalité [1]):

Lemme 1:. *En désignant, pour chaque partie E de A, et tout polynôme Q sur A, par $u(Q,E)$ et $i(R,E)$ le nombre d'éléments de E où la valeur de Q est une unité, respectivement un élément irréductible, on a l'inégalité*

$$i(P,E) + 2u(P,E) \leq u(P_1,E) + u(P_2,E).$$

III. Majoration des hauteurs de P_1 et P_2

Considérons provisoirement un polynôme g à coefficients complexes et qui ne s'annule pas à l'origine.

Posons

$$g = a_0X^d + a_1X^{d-1} + \ldots + a_d.$$

Pour simplifier, nous supposerons g unitaire. Si g est le produit de deux polynômes unitaires g_1 et g_2, nous cherchons à majorer les coefficients de g_1 et g_2. Pour ceci, on utilisera le fait que les coefficients de g_1 sont certaines fonctions des racines du polynôme g. Plus précisément, la somme des coefficients de g_1 est égale à la somme de 2^{d_1} (d_1 désigne le degré de g_1)

---

[1]) Pour plus de détails, voir (1).

produits de certaines racines de g affectés du coefficient ± 1 [1]). Il est clair que chacun de ces produits est majoré en module par le produit des modules des racines de g qui ont un module supérieur à 1. Pour majorer ce produit nous utiliserons un lemme classique de la théorie des fonctions analytiques.

LEMME 2. *Soit* $f(z) = \sum_0^\infty b_m z^m$ *une fonction holomorphe dans le disque* $|z| \leq 1$ *et telle que* $f(0)$ *soit non nulle. Soient* $\zeta_1, \ldots, \zeta_\nu$ *les racines de* f *dans le disque* $|z| < 1$ *(répétées chacune autant de fois que son ordre de multiplicité). On a l'inégalité :*

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

Démonstration :

Posons

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

La fonction h est holomorphe dans le disque $|z| \leq 1$. De plus, les modules de f et de h coïncident sur le cercle $|z| = 1$. D'où l'égalité:

$$\frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\theta})|^2 \, d\theta = \frac{1}{2\pi} \int_0^{2\pi} |h(e^{i\theta})|^2 \, d\theta .$$

En appliquant la formule de Parseval, on en déduit la relation

$$\sum_0^\infty |b_m|^2 = \sum_0^\infty |c_m|^2$$

Mais on a l'égalité

$$|c_0| = |h(0)| = |b_0| \left(\prod_{j=1}^{\nu} |\zeta_j|\right)^{-1} .$$

En reportant cette valeur de $|c_0|$ dans l'égalité précédente, on obtient immédiatement l'inégalité

---

[1]) Si g_1 est de la forme $\alpha_0 X^{d_1} + \alpha_1 X^{d_1 - 1} + \ldots + \alpha_{d_1}$ et si $\zeta_1, \zeta_2, \ldots, \zeta_{d_1}$ désignent les zéros de g_1 (chaque racine figurant un nombre de fois égal à son ordre multiplicité), on sait qu'au signe près, chaque coefficient α_k de g_1 est la somme de tous les produits de la forme $\zeta_{j1} \ldots \zeta_{jk}$, où les indices $j_1, \ldots, j_k$ sont tous distincts. Ainsi α_k est la somme de $\binom{d_1}{k}$ produits de cette forme. La somme des α_k est donc égale à la somme de 2^{d_1} produits du type $(-1)^k \zeta_{j1} \ldots \zeta_{jk}$.

$$|b_0|\left(\prod_{j=1}^{\nu}|\zeta_j|\right)^{-1} \leq \left(\sum_{0}^{\infty}|b_m|^2\right)^{\frac{1}{2}}.$$

Ceci achève la démonstration du lemme.

Revenons au polynôme g. D'après le lemme 2, le produit des racines de g situées dans le disque $|z| \leq 1$ a un inverse dont le module est majoré par la quantité $\left(\sum_{0}^{d}|a_i|^2\right)^{\frac{1}{2}}|a_0|^{-1}$. Puisque g est unitaire le produit de toutes ses racines a pour module $|a_d|$. Ceci montre que le produit de racines de g situées à l'extérieur du disque $|z| \leq 1$ a un module majoré par $\left(\sum_{0}^{d}|a_i|^2\right)^{\frac{1}{2}}$. De cette majoration et des remarques qui précèdent le lemme 2, on déduit que la somme des modules des coefficients du polynôme g_1 est majorée par $2^{d_1}\left(\sum_{0}^{d}|a_i|^2\right)^{\frac{1}{2}}$. D'où:

LEMME 3. *Soit* $g = a_0X^d + a_1X^{d-1} + \ldots + a_d$ *un polynôme unitaire à coefficients complexes qui ne s'annule pas à l'origine. Soit* g_1 *un polynôme unitaire de degré* d_1 *qui divise* g. *Alors, la somme des modules des coefficients de* g_1 *est majorée par* $2^{d_1}\left(\sum_{0}^{d}|a_i|^2\right)^{\frac{1}{2}}$.

Cette majoration va nous permettre de majorer les hauteurs des polynômes P_1 et P_2 en fonction de celle de P. Auparavant, il nous faut introduire plusieurs définitions.

Soit n le degré du corps de nombres K. On sait qu'il y a exactement n isomorphismes distincts σ_i du corps K dans le corps des complexes.

Soit Q un polynôme unitaire à coefficients dans K. Si Q est égal à $b_0X^d + b_1X^{d-1} + \ldots + b_d$, on pose

$$|Q|_1 = \max_i \sum_{0}^{d}|\sigma_i(b_j)|, \quad |Q|_2 = \max_i\left(\sum_{0}^{d}|\sigma_i(b_j)|^2\right)^{\frac{1}{2}}.$$

Soit P un polynôme unitaire à coefficients dans A et qui ne s'annule pas à l'origine et soit P_1 un polynôme unitaire à coefficients dans A qui divise P. En appliquant le lemme 3 aux différents polynômes σ_iP et σ_iP_1 (notations évidentes !), on obtient la majoration suivante:

LEMME 4. *Soit* P *un polynôme unitaire à coefficients dans* A *qui ne s'annule pas à l'origine. Soit* P_1 *un polynôme unitaire à coefficients dans* A *et qui divise* P. *On a l'inégalité:*

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

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 σ_i soit inclue dans le corps des réels; alors les autres indices sont en nombre pair $2r_2$. On peut numéroter les σ_i de sorte que l'image de σ_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

$$x \to (\mathrm{Log}\,|\sigma_1(x)|, \ldots, \mathrm{Log}\,|\sigma_{r_1+r_2}(x)|) .$$

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

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

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

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

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:

$$u_a(Q) \leq w \,.\, \deg Q \,.\, \mathrm{card}\,(J \cap R)\,, \tag{1}$$

où on a posé

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

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 ≥ 1 qui sera fixé ultérieurement. On suppose que le polynôme satisfait à la condition

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

Désignons par $\|\ \|$ 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 :*

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

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

$$\| L(x') \| \leq (r_1 + r_2) \max_i \left(|\, \mathrm{Log}\, |\, \sigma_i(x') \,| \,| \right).$$

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

— *majoration des* $|\sigma_i(x')|$.

Reprenons la notation

$$Q = b_0X^d + b_1X^{d-1} + \ldots + b_d .$$

On a alors l'inégalité

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

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

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

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

$$|\operatorname{Log}|\sigma_i(x')|| \leq n \,.\, \operatorname{Log}(Sa^d) .$$

D'où l'inégalité

$$||L(x')|| \leq (r_1+r_2)\,n \,.\, \operatorname{Log}(Sa^d) .$$

Si on pose

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

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

$$\operatorname{Log}(Sa^d) \leq \lambda \operatorname{Log} a .$$

D'où finalement l'inégalité

$$||L(x')|| \leq \deg Q \,.\, C_0 \,.\, \operatorname{Log} a$$

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 $b = \deg Q \cdot C_0 \cdot \operatorname{Log} a$. Remarquons que b est au moins égal à $\operatorname{Log} 2$.

Deuxième étape.

LEMME 6. *Soit b un réel au moins égal à $\operatorname{Log} 2$. 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

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

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

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

Comme b est au moins égal à $\operatorname{Log} 2$, le nombre $b + S$ est majoré par μb où μ vaut $1 + \dfrac{S}{\operatorname{Log} 2}$.

D'où l'inégalité

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

où on a posé

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

On voit que connaissant K on peut calculer explicitement S et 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 $a \geqq 2$, 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 :*

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

(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

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

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

$$\begin{aligned} u_a(P_1) + u_a(P_2) &\leqq w\, C_1 (C_0 \operatorname{Log} a)^r \left((\deg P_1)^{r+1} + (\deg P_2)^{r+1}\right) \\ &\leqq 2w\, C_1 (C_0 \operatorname{Log} a)^r (\deg P)^{r+1} . \end{aligned}$$

Ceci achève la démonstration du théorème.

Remarque. L'inégalité $a \geqq 2$ n'a été introduite que pour éviter des complications inutiles. Le théorème reste vrai pourvu que l'on suppose $a \geqq \alpha_0$ avec α_0 fixé, $\alpha_0 > 1$, mais cette fois la constante C dépend de α_0.

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

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

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.*

Pour tout entier x, dont tous les conjugués sont strictement supérieurs à S, l'élément $P(x)$ est réductible dans A.

Démonstration :

D'après le lemme 4 nous savons que si P_1 désigne un diviseur de P, alors $|P_1|_1$ est majoré par S. Soit alors σ_i un isomorphisme quelconque de K dans $\mathbf{C}$ et soit x un entier dont tous les conjugués sont supérieurs à S. Nous avons les inégalités suivantes

$$|\sigma_i(P_1(x)(| \geqq |\sigma_i(x)|^{d_1} - (|P_1|_1 - 1)\,|\sigma_i(x)|^{d_1-1}$$
$$\geqq |\sigma_i(x)|^{d_1-1}(|\sigma_i(x)| + 1 - S) > S^{d_1-1} \geqq 1\,.$$

Ceci étant vrai pour tout i, la norme de $P_1(x)$ a un module strictement supérieur à 1; autrement dit $P_1(x)$ n'est pas une unité. Si P est égal au produit de P_1 et d'un polynôme P_2, la même démonstration montre que $P_2(x)$ n'est pas une unité. Dans ces conditions, il est clair que l'élément $P(x)$ est réductible dans l'anneau A.

Du théorème résultent immédiatement les deux critères suivants:

CRITÈRE 2. *Soit P un polynôme unitaire à coefficients dans A et qui ne s'annule pas en zéro et de degré d. S'il existe un élément x entier dont tous les conjugués ont un module strictement supérieur à $2^{d-1}|P|_2$ et tel que l'élément $P(x)$ soit irréductible dans A, alors le polynôme P est irréductible sur K.*

CRITÈRE 2'. *Avec les mêmes notations que ci-dessus, s'il existe un entier rationnel x de module strictement supérieur à $2^{d-1}|P|_2$ et tel que $P(x)$ soit irréductible dans A, alors le polynôme P est irréductible dans $K[X]$.*

RÉFÉRENCE

[1] MIGNOTTE, M. Un critère d'irréductibilité des polynômes. *Enseignement mathématique*, tome 17 (1971), pp. 213-214.

(Reçu le 24 février 1971)

Maurice Mignotte
Centre Scientifique
Place du 8 mai 45
F-93 - Saint-Denis