Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Maurice Mignotte

Entiers algébriques dont les conjugués sont proches du cercle unité

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 2 (1977-1978), exp. n° 39, p. 1-6

<http://www.numdam.org/item?id=SDPP_1977-1978__19_2_A13_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 39, 6 p.

8 mai 1978

ENTIERS ALGÉBRIQUES DONT LES CONJUGUÉS SONT PROCHES DU CERCLE UNITÉ

par Maurice MIGNOTTE

1. Introduction.

Etant donné un entier algébrique α non nul de degré D, de conjugués $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_D$, on considère la mesure $M(\alpha)$ donnée par

$$M(\alpha) = \prod_{i=1}^{D} \max\{1, |\alpha_i|\} .$$

KRONECKER [4] démontra en 1857 que, si $M(\alpha) = 1$, alors α est une racine de l'unité ; la réciproque est triviale. Du fait qu'il n'existe qu'un nombre fini d'entiers algébriques de degré D et de mesure bornée, pour tout entier D, il existe une constante $C(D) > 1$ telle que tout entier algébrique non nul, de degré D et de mesure majorée par $C(D)$, est une racine de l'unité.

En 1933, D. H. LEHMER [6], en liaison avec une méthode pour découvrir de grands nombres premiers, posa la question suivante : A-t-on $\liminf C(D) = 1$? A l'heure actuelle, il semble qu'aucun entier algébrique α n'ait été découvert qui vérifie $1 < M(\alpha) < M(\alpha_0)$, où α_0 est le nombre de Salem (donc $M(\alpha_0) = \alpha_0$) racine de l'équation

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 = 0 ,$$

$\alpha_0 = 1{,}17628081\ldots$, exemple déjà signalé par LEHMER.

En 1971, C. J. SMYTH [9], améliorant des résultats de SALEM, SIEGEL, CASSELS ..., démontra qu'un entier algébrique non nul α qui n'est pas conjugué à α^{-1} vérifie $M(\alpha) \geqslant \beta_0 = 1{,}32471795\ldots$, où β_0 est la racine réelle de l'équation $x^3 - x - 1 = 0$.

Jusqu'au début de cette année, le meilleur résultat connu était celui de BLANKSBY et MONTGOMERY [1],

$$C(D) > 1 + (52\, D \log 6D)^{-1} , \tag{1}$$

leur démonstration utilisait l'analyse de Fourier. Un résultat sensiblement équivalent a été prouvé par C. L. STEWART [10] par la méthode de Thue, utilisée habituellement en théorie des nombres transcendants. Depuis DOBROWOLSKI [3] a obtenu la minoration

$$C(D) > 1 + C_1 \left(\frac{\log \log D}{\log D}\right)^3 ,$$

où C_1 est une constante positive (calculable).

Notons que la quantité $C(D)$ joue un rôle important dans l'étude des relations multiplicatives entre nombres algébriques ou, ce qui est bien sûr équivalent, des formes linéaires dégénérées de logarithmes de nombres algébriques. Ce fait, mis en évidence par STARK, a été ensuite précisé par LOXTON et Van der POORTEN [7] et sur-

tout par M. WALDSCHMIDT [11].

Signalons enfin que l'assertion

$$\liminf C(D) > 1$$

est équivalente à une conjecture en dynamique topologique concernant l'existence de groupes localement compacts munis d'un automorphisme vérifiant certaines propriétés de caractère ergodique (voir [5]).

Les résultats originaux qui figurent dans cet exposé ont été obtenus en collaboration avec C. L. STEWART et M. WALDSCHMIDT.

2. Le théorème de Kronecker.

THÉORÈME 1. - *Un entier algébrique α non nul, dont tous les conjugués appartiennent au disque unité, est une racine de l'unité.*

Nous donnons deux preuves de ce résultat.

Première démonstration. - Considérons la suite des nombres algébriques α , α^2 , α^3 , ... Ses éléments ayant un degré borné et une mesure égale à 1 , elle ne peut prendre qu'un nombre fini de valeurs. D'où l'existence d'un entier positif k tel que $\alpha^k = 1$.

Seconde démonstration. - Considérons la suite des entiers $\mathrm{Trace}(\alpha^n)$, $n = 0 , 1 , 2 , \ldots$ C'est une suite récurrente linéaire d'entiers bornée ; on vérifie facilement qu'elle est purement périodique. D'où l'existence d'un entier k tel que $\mathrm{Trace}(\alpha^k) = \mathrm{Trace}(\alpha^0)$; ce qui s'écrit $\alpha_1^k + \alpha_2^k + \ldots + \alpha_D^k = D$, avec $|\alpha_i| \leqslant 1$, pour $i = 1 , \ldots , D$, et implique $\alpha^k = \alpha_1^k = 1$.

3. Résultats élémentaires.

PROPOSITION 1. - *Soit α un entier algébrique qui n'est pas une unité. Alors, sa mesure est au moins égale à deux.*

On a en effet

$$M(\alpha) \geqslant |\alpha_1 \ldots \alpha_D| \geqslant 2 .$$

Le résultat suivant s'inspire d'une remarque de P. BATEMAN citée en [2].

PROPOSITION 2. - *Si α est un entier algébrique, alors le discriminant Δ du corps $\mathbb{Q}(\alpha)$ vérifie*

$$|\Delta| \leqslant (\sqrt{D}\, M(\alpha))^{2D} , \text{ où } D = \deg(\alpha) .$$

En effet,

$$|\Delta| \leqslant \mathrm{Disc}(1 , \alpha , \dots , \alpha^{D-1})| = \begin{vmatrix} 1 & \alpha_1 & \alpha_2^2 & \dots & \alpha_1^{D-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{D-1} \\ \dots & & & & \\ 1 & \alpha_D & \alpha_D^2 & \dots & \alpha_D^{D-1} \end{vmatrix}^2$$

et on majore le déterminant grâce à l'inégalité de Hadamard.

COROLLAIRE 1. - Si K est un corps de nombres de degré D dont le discriminant a une valeur absolue au moins égale à $(2D)^D$, alors tout entier algébrique α, qui engendre K et qui n'est pas une racine de l'unité, vérifie $M(\alpha) \geqslant \sqrt{2}$.

Le théorème suivant, démontré en [2], améliore un résultat de R. M. ROBINSON.

PROPOSITION 3. - Soit α un entier algébrique irrationnel, de conjugués $\alpha_1 = \alpha , \alpha_2 , \dots , \alpha_D$. Supposons que la conjugaison complexe commute avec les éléments du groupe de Galois de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ et que l'on ait $|\alpha_i| \leqslant \sqrt{2}$, pour $i = 1 , \dots , D$, alors α est une racine de l'unité.

Le nombre $\theta = \alpha\bar{\alpha} - 1$ est un entier algébrique dont les conjugués sont les nombres $\alpha_i \bar{\alpha}_i - 1 = |\alpha_i|^2 - 1$. Donc $|\mathrm{Norme}(\theta)| < 1$, puis $\theta = 0$. On a donc $|\alpha_i| = 1$, pour $i = 1 , \dots , D$, et on conclut grâce au théorème de Kronecker.

Le résultat suivant généralise le théorème 2 de [2].

PROPOSITION 4. - Soit α une unité algébrique de degré D qui n'est pas une racine de l'unité. Soit p un nombre premier non ramifié dans le corps $\mathbb{Q}(\alpha)$, et soit L le p. p. c. m. des degrés résiduels des idéaux premiers de ce corps au-dessus de p. On a alors l'inégalité

$$p^D \leqslant f \prod_{i, |\alpha_i - 1| < 1} |\alpha_i - 1| \; 2^D M^f(\alpha) , \text{ où } f = p^L - 1 .$$

On a d'une part

$$p^D \leqslant |\mathrm{Norme}(\alpha^f - 1)|$$

puisque chaque idéal premier au-dessus de p divise $\alpha^f - 1$, que p n'est pas ramifié et $\alpha^f - 1 \neq 0$. D'autre part, cette norme est trivialement majorée par le membre de droite de l'inégalité cherchée.

COROLLAIRE 2. - Si p est un nombre premier impair non ramifié et totalement décomposé dans le corps $\mathbb{Q}(\alpha)$, où α vérifie les hypothèses de la proposition 4, on a

$$M(\alpha) \geqslant 2^{-1/3} (p/2)^{(D-1)/(p-1)} ; \tag{1}$$

donc, si de plus p vérifie $p \leqslant D \log D$, alors on a

$$M(\alpha) \geqslant 1,2 .$$

La proposition ci-dessous introduit une idée de DOBROWOLSKI que nous retrouverons au paragraphe suivant.

PROPOSITION 5. - Soit α un entier algébrique qui n'est pas une racine de l'unité, $L(\alpha)$ sa longueur (i. e. la somme des valeurs absolues des coefficients du polynôme minimal de α), on a alors

$$M(\alpha) \geq 2^{1/(2L(\alpha))} .$$

Soit P le polynôme minimal de α , et soit p un nombre premier vérifiant $2L(\alpha) \leq p \leq 4L(\alpha)$. On a

$$P(X^p) = F(X)^p + p\, G(X) \text{ , avec } G \in \mathbb{Z}[X] ,$$

donc p^D divise l'entier $\text{Norme}(P(\alpha^p))$. Du fait que α n'est pas une racine de l'unité on a $P(\alpha^p) \neq 0$ (lemme 1). Par conséquent,

$$p^D \leq L(\alpha)^D M(\alpha)^{pD} ,$$

ou

$$M(\alpha) \geq (p/L(\alpha))^{1/p} \geq 2^{1/(2L(\alpha))} .$$

4. Le théorème de Dobrowolski.

Démontrons d'abord le lemme déjà utilisé plus haut.

LEMME 1. - Soient α un nombre algébrique non nul, α' un conjugué de α . S'il existe des entiers r et s non nuls avec $|r| \neq |s|$ et $\alpha'^r = \alpha^s$, alors α est une racine de l'unité.

Soit σ un isomorphisme du corps $\mathbb{Q}(\alpha_1 , \ldots , \alpha_D)$ tel que $\sigma(\alpha) = \alpha'$. On a alors

$$\sigma^2(\alpha)^{r^2} = \sigma(\sigma(\alpha)^r)^r = \sigma(\alpha)^{rs} = \alpha^{s^2} ,$$

et plus généralement

$$\sigma^k(\alpha)^{r^k} = \alpha^{s^k} \text{ , pour } k \geq 2 .$$

La conclusion est obtenue en choisissant pour k un entier tel que $\sigma^k(\alpha) = \alpha$.

Le résultat suivant nous sera utile

LEMME 2. - Soient α un nombre algébrique non nul et p un nombre premier. Alors, si le nombre α^p a un degré inférieur à celui de α , il existe un nombre algébrique β de degré plus petit que α et de mesure majorée par celle de α .

Soit K le corps $\mathbb{Q}(\alpha^p)$. Si α est de degré p sur K , l'assertion du lemme a lieu en prenant $\beta = \alpha^p$, les mesures de α et β sont alors égales. Considérons maintenant le cas contraire. Il existe alors un entier r , $0 < r < p$, et une racine p-ième de l'unité tels que $\alpha^r \zeta$ appartienne à K (faire le produit des conjugués de α sur K). Comme le degré de ζ sur K est inférieur à p , il en résulte qu'il existe un entier s premier à p tel que α^s appartienne à K (faire le produit des conjugués de α^r sur K). La relation de Bezout $us + vp = 1$ permet d'en déduire que α^p est égal à γ^p , pour un élément γ de

K . On vérifie alors l'assertion du lemme en choisissant $\beta = \gamma$.

Nous sommes maintenant en mesure de démontrer le résultat suivant.

THÉORÈME 2. - Si α est un entier algébrique irrationnel de degré D qui n'est pas une racine de l'unité, on a

$$M(\alpha) \geqslant 1 + 10^{-6} (\log \log D/\log D)^3 .$$

1° Réduction. - On raisonne par récurrence sur D . D'après (1) (ou la proposition 5), cette inégalité a lieu pour $D \leqslant 16$. D'après le lemme 2 et le fait que la fonction $D \longmapsto (\log \log D/\log D)^3$ est décroissante pour $D \geqslant 16$, on peut supposer que, pour tout p premier, le degré de α^p est égal à celui de α .

2° Construction d'une fonction auxilliaire. - On construit un polynôme non nul à coefficients entiers

$$F(X) = \sum_{i=0}^{N-1} a_i X^i$$

divisible par $P(X)^T$, P désignant le polynôme minimal de α , N et T sont des entiers positifs qui seront précisés plus loin soumis à la condition $N \geqslant 2DT$. La version du lemme de Siegel qui figure en [8] assure l'existence d'un tel polynôme avec des coefficients pas trop gros, en fait avec

$$\max_{1 \leqslant i < N} \{|a_i|\} \leqslant 2 + (2^T N^{T^2 D} M(\alpha)^{TN})^{1/(N-TD)} .$$

3° Conclusion. - D'après le lemme 1 et la réduction, les polynômes minimaux des α^p sont distincts. Il existe donc un nombre premier $N/D \leqslant p \leqslant 3(N/D) \log(N/D)$ tel que $F(\alpha^p)$ soit non nul.

D'après l'argument utilisé dans la démonstration de la proposition 5, p^D divise la norme de $P(\alpha^p)$ donc p^{TD} divise la norme de $F(\alpha^p)$.

D'autre part, on a la majoration évidente

$$|\text{Norme}(F(\alpha^p))| \leqslant (N \max\{|a_i|\})^D M(\alpha)^{Np} .$$

Après quelques calculs, on déduit de ce qui précède l'inégalité

$$T \log p \leqslant \log(KD) + 2 + 2(T^2/K) \log(KD) + K(p + 1) \log M(\alpha) , \text{ où } K = N/D .$$

Choisissons $K = T^2$, compte tenu des contraintes vérifiées par p , l'inégalité précédente implique

$$2T \log T \leqslant 5 \log(T^2 D) + 8T^4 \log T \log M(\alpha) .$$

En choisissant $T = [50(\log D/\log \log D)]$ pour $D \geqslant 16$, on en déduit

$$\log M(\alpha) \geqslant 1/(8T^3) \geqslant 10^{-6}(\log D/\log \log D)^3 .$$

BIBLIOGRAPHIE

[1] BLANKSBY (P. E.) and MONTGOMERY (H. L.). - Algebraic integers near the unit circle, Acta Arithm., Warszawa, t. 18, 1971, p. 355-369.

[2] CALLAHAN (T.), NEWMAN (M.) and SHEINGORN (M.). - Fields with large Kronecker constants, J. of number Theory, t. 9, 1977, p. 182-186.

[3] DOBROWOLSKI (E.). - Manuscrit non publié .

[4] KRONECKER (L.). - Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, J. für reine und angew. Math., t. 53, 1857, p. 173-175.

[5] LAWTON (W.). - Heights of algebraic numbers and Szegö's theorem, Proc. Amer. math. Soc., t. 49, 1975, p. 47-50.

[6] LEHMER (D. H.). - Factorization of certain cyclotomic functions, Annals of Math., Series 2, t. 34, 1933, p. 461-479.

[7] LOXTON (J. H.) and van der POORTEN (A. J.). - Multiplicative relations in number fields , Bull Australian math. Soc., t. 16, 1977, p. 83-98, et t. 17, 1977, p. 151-155.

[8] MIGNOTTE (M.) et WALDSCHMIDT (M.). - Linear forms in two logarithms and Schneider's method, Math. Annalen, t. 231, 1978, p. 241-267.

[9] SMYTH (C. J.). - On the product of the conjugates outside the unit circle of an algebraic integer, Bull. London math. Soc., t. 3, 1971, p. 169-175.

[10] STEWART (C. L.). - Algebraic integers whose conjugates lie near the unit circle, Bull. Soc. math. France, t. 106, 1978 (à paraître).

[11] WALDSCHMIDT (M.). - A lower bound for linear forms in logarithms, Acta Arithm., Warszawa (à paraître).

(Texte reçu le 31 mai 1978)

Maurice MIGNOTTE
Centre de Calcul
Université Louis Pasteur
67084 STRASBOURG CEDEX