SUR LE PRODUIT DES CONJUGUÉS EXTÉRIEURS AU CERCLE UNITÉ D'UN ENTIER ALGÉBRIQUE

Autor(en): **Waldschmidt, Michel**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **26 (1980)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-51068

SUR LE PRODUIT DES CONJUGUÉS EXTÉRIEURS AU CERCLE UNITÉ D'UN ENTIER ALGÉBRIQUE

par Michel WALDSCHMIDT

English summary. This is a survey of some recent results, mainly due to D. Boyd, C. L. Stewart, and E. Dobrowolski, concerning conjectures of Lehmer, Schinzel and Zassenhaus. The problem is to give an effective version of a theorem of Kronecker, and to obtain a lower bound for the product of the conjugates outside the unit circle of an algebraic integer.

Soit α un entier algébrique. On note $d = [\mathbf{Q}(\alpha) : \mathbf{Q}]$ le degré de α, $\alpha_1, \ldots, \alpha_d$ les conjugués de α, et

$$M(\alpha) = \prod_{|\alpha_j| > 1} |\alpha_j| = \prod_{j=1}^{d} \max\{1, |\alpha_j|\}.$$

On remarque que $M(0) = 1$, et que $M(\zeta) = 1$ si ζ est une racine de l'unité. En 1857, Kronecker a démontré que si α est différent de 0 et non racine de l'unité, alors $M(\alpha) > 1$. Ce résultat est déjà implicite dans la démonstration du théorème des unités par Dirichlet en 1846. Il résulte du fait que si $M(\alpha) = 1$, alors, pour tout entier $k > 0$, α^k est racine d'un polynôme de degré $\leqslant d$ et de hauteur $\leqslant 2^d$, et ces polynômes sont en nombre fini.

En 1933, D. H. Lehmer pose la question suivante: est-il vrai que pour tout $\varepsilon > 0$ il existe un entier algébrique α vérifiant $1 < M(\alpha) < 1 + \varepsilon$? Lehmer précise qu'une recherche intensive mais non exhaustive parmi les polynômes symétriques de degré $\leqslant 14$ ne lui a pas permis de trouver une meilleure valeur que $M(\alpha_0) = 1,1762808\ldots$ pour α_0 racine du polynôme

$$P(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

On notera que $P(X) = X^5 Q\left(X + \frac{1}{X}\right)$ où

$$Q(Y) = (Y+1)^2 (Y-1)(Y+2)(Y-2) - 1.$$

Ce nombre α_0 est le plus petit nombre de Salem connu.

Cette question a été posée par Lehmer en liaison avec la recherche de grands nombres premiers (cf. [S]). Elle apparaît aussi en théorie ergodique (voir également [S]). Enfin elle est apparentée à la conjecture de Pisot: si $\theta > 1$ est un nombre réel tel qu'il existe $\lambda > 0$ pour lequel $\| \lambda \theta^n \| \to 0$ (où $\| \, . \, \|$ désigne la distance à l'entier le plus proche), alors θ est un nombre de Pisot. Le lien avec le problème de Lehmer se fait par l'intermédiaire de l'ensemble E des limites $\lim a_{n+1}/a_n$, pour $(a_0, a_1, \ldots)$ suite de Pisot:

$$a_{n+1} = N(a_n^2/a_{n-1}), \quad n \geqslant 1,$$

où $N(x) = \left[x + \frac{1}{2} \right]$, et a_0, a_1 sont des entiers, $0 < a_0 < a_1$. On sait que E est dense dans $[1, \infty]$, et que E contient l'ensemble S des nombres de Pisot et celui T des nombres de Salem. Si on avait $E = S \cup T$, on en déduirait d'une part $\inf T = 1$, ce qui répond à la question de Lehmer, et on en déduirait d'autre part la conjecture de Pisot. Cependant D. Boyd [B2], [B3] a obtenu des résultats qui suggèrent plutôt $E \neq S \cup T$.

Il est intéressant de noter qu'en 1936, après avoir donné à Paris un exposé sur la solution par Schneider du 7e problème de Hilbert sur la transcendance de a^b, C. L. Siegel signala à C. Pisot la question de D. H. Lehmer. Quarante ans après (comme nous allons le voir), la méthode de Schneider permet à Stewart et Dobrowolski de faire des progrès importants vers une réponse négative à la question de Lehmer.

Polynômes non réciproques

En 1970, C. J. Smyth a montré que si le polynôme minimal de α n'est pas réciproque (et $\alpha \neq 0$, $\alpha \neq 1$), alors $M(\alpha) \geqslant \theta_0$ où θ_0 est la racine réelle de $X^3 - X - 1$. Il en déduit le résultat de Siegel (1944): $\theta_0 = 1,32471795\ldots$ est le plus petit nombre de Pisot (l'existence du plus petit nombre de Pisot résulte du fait, démontré par Salem en 1944, que l'ensemble S est fermé). Il en déduit aussi un résultat de Chamfy (1957): si α est un entier algébrique non réel vérifiant $|\alpha| = |\bar{\alpha}| > 1$ et $|\alpha_j| < 1$ pour α_j conjugué de α avec $\alpha_j \neq \alpha$ et $\alpha_j \neq \bar{\alpha}$, alors $|\alpha| \geqslant \sqrt{\theta_0}$. Enfin si $\alpha \neq 0$, $\alpha \neq 1$ a un polynôme minimal non réciproque, on a

$$\max |\alpha_j| \geqslant 1 + \frac{\log \theta_0}{d}.$$

La question de Lehmer est donc résolue pour les polynômes non réciproques. Néanmoins l'étude de l'ensemble des valeurs de $M(\alpha)$ pour α non réciproque n'est pas terminée. Le plus petit point limite connu [B1, B2, B4] correspond aux polynômes $X^n + X + 1$:

$$\begin{aligned}\beta &= \exp \int_0^1 \int_0^1 \log \left| e^{2i\pi t_1} + e^{2i\pi t_2} + 1 \right| dt_1\, dt_2 \\ &= \exp \left\{ \frac{1}{\pi} \int_0^{\pi/3} - \log \left(2 \sin \frac{t}{2} \right) dt \right\} \\ &= 1{,}38135 \ \ldots\end{aligned}$$

On ignore si ce nombre est algébrique ou transcendant (cf. [B2]).

Remarque. Pour $P \in \mathbf{C}[z_1, \ldots, z_n]$, Mahler définit

$$M(P) = \exp \int_0^1 \ldots \int_0^1 \log \left| P(e^{2i\pi t_1}, \ldots, e^{2i\pi t_n}) \right| dt_1 \ldots dt_n .$$

La formule de Jensen montre que $M(\alpha) = M(P)$ si $P \in \mathbf{Z}[X]$ est le polynôme minimal de α. D'autre part soit $P(X, Y) \in \mathbf{C}[X, Y]$, et, pour $k \geqslant 0$, soit $Q_k(X) = P(X, X^k) \in \mathbf{C}[X]$. Alors on a (cf. [B1] théorème 2) $M(Q_k) \to M(P)$ quand $k \to \infty$.

Polynômes réciproques

D. W. Boyd a fait très récemment une recherche sur ordinateur qui lui a permis de vérifier que $M(\alpha) \geqslant \alpha_0$ si α est un nombre algébrique (non nul et non racine de l'unité) de degré $\leqslant 16$, ou bien de degré $\leqslant 26$ et de hauteur $\leqslant 1$ (i.e. dont le polynôme minimal a pour coefficients 0, 1 ou -1). D'autre part le plus petit point limite de l'ensemble des $M(\alpha)$ qu'il connaisse est

$$\begin{aligned}&M\left(Y^2(X+1) + Y(X^2+X+1) + X^2 + 1\right) \\ &= \exp \int_0^1 \int_0^1 \log \left| \zeta^2(1+z^{-1}) + \zeta(z+1+z^{-1}) + z + 1 \right| d\theta\, dt \\ &= 1{,}255425 \ \ldots\end{aligned}$$

(où on a écrit $\zeta = e^{2i\pi\theta}$, $z = e^{2i\pi t}$), correspondant par exemple aux polynômes

$$X^{2n}(1+X^{-1}) + X^n(X+1+X^{-1}) + X + 1 .$$

Enfin Boyd [B1] demande si $\beta = 1,38135\ldots$ est le plus petit élément du deuxième ensemble dérivé de $\{M(\alpha)\}$.

Le problème initial de Lehmer a fait l'objet de plusieurs travaux récents. Soit d un entier positif. Comme il n'existe qu'un nombre fini d'entiers algébriques de degré d et de mesure inférieure ou égale à 2^d, il existe une constante $C(d) > 1$ telle que si α est un entier algébrique non nul et non racine de l'unité de degré d, on ait $M(\alpha) > C(d)$. En notant $\lceil \alpha \rceil = \max_{1 \leq j \leq d} |\alpha_j|$ et en remarquant que

$$\lceil \alpha \rceil \leqslant M(\alpha) \leqslant \lceil \alpha \rceil^d,$$

on en déduit sous les mêmes hypothèses $\lceil \alpha \rceil > C(d)^{1/d}$, et même, si le polynôme minimal de α est réciproque, $\lceil \alpha \rceil > C(d)^{2/d}$.

A défaut de pouvoir minorer $C(d)$ par une constante absolue supérieure à 1 (ce qui correspondrait à une réponse négative à la question de Lehmer), on peut chercher à minorer $C(d)$ en fonction de d. Un tel résultat a été obtenu par Schinzel et Zassenhaus en 1965:

$$C(d) > 1 + \frac{c}{2^d}$$

où c est une constante absolue positive. Ils posaient alors le problème de l'existence d'une constante $c' > 0$ telle que $\lceil \alpha \rceil > 1 + \frac{c'}{d}$ sous les hypothèses précédentes (ce qui résulterait d'une réponse négative à la question de Lehmer, et serait le meilleur possible comme on le voit sur l'exemple $\alpha = 2^{1/d}$).

Une amélioration considérable a été obtenue par Blanksby et Montgomery en 1971:

$$C(d) > 1 + \frac{1}{52\, d \log 6d}$$

et par conséquent pour la conjecture de Schinzel et Zassenhaus

$$\lceil \alpha \rceil > 1 + \frac{1}{30\, d^2 \log 6d}\,.$$

En 1977, C. L. Stewart montra que la méthode de Thue conduit à la minoration

$$C(d) > 1 + \frac{1}{10^4\, d \log d}\,;$$

la constante est moins bonne, mais la méthode (on va le voir) très fructueuse.

Simultanément et indépendamment, E. Dobrowolski obtint par une méthode simple et élégante un nouveau progrès vers la conjecture de Zassenhaus:

$$\lceil \alpha \rceil > 1 + \frac{1}{4\,e\,d^2}\,.$$

Voici sa démonstration. Supposons que α soit un entier algébrique non nul tel que $\lceil \alpha \rceil \leqslant 1 + (4\,e\,d^2)^{-1}$. Soit p un nombre premier, $2\,e\,d < p < 4\,e\,d$. Pour k entier positif considérons la somme de Newton

$$S_k = \sum_{i=1}^{d} \alpha_i^k\,.$$

Pour $k \leqslant d$ on a

$$|\,S_k\,| \leqslant d\left(1 + \frac{1}{4\,e\,d^2}\right)^{d} < de$$

$$|\,S_{kp}| \leqslant d\left(1 + \frac{1}{4\,e\,d^2}\right)^{4ed2} < de\,,$$

donc

$$|\,S_k - S_{kp}\,| \leqslant 2\,d\,e < p\,.$$

Mais $S_k \equiv S_k^p \equiv S_{kp} \pmod p$, donc $S_k = S_{kp}$ pour $1 \leqslant k \leqslant d$, ce qui montre que α et α^p sont conjugués. On en déduit facilement que α est une racine de l'unité, ce qui termine la démonstration.

Peu après, Dobrowolski améliorait son résultat:

$$\lceil \alpha \rceil > 1 + \frac{\log d}{d^2 + o\,(d)} \quad \text{pour } d \to \infty\,.$$

Il choisit $3d \leqslant p \leqslant 6d$, et la partie nouvelle de la démonstration consiste à vérifier les récurrences

$$S_{kp} \equiv S_k \mod k \qquad \text{pour } 1 \leqslant k < d\,.$$

En 1978, Dobrowolski obtint une remarquable amélioration des résultats antérieurs:

$$C\,(d) > 1 + c_0\,(\log\log d/\log d)^3\,,$$

où c_0 est une constante absolue positive effectivement calculable.

Il a depuis montré que c_0 peut être choisi égal à $\dfrac{1}{1200}$, et même peut être

remplacé par $1 - \varepsilon$ si on se limite aux entiers d suffisamment grands: $d \geqslant d_0(\varepsilon)$. Par conséquent pour la conjecture de Schinzel Zassenhaus

$$\lceil \alpha \rceil > 1 + \frac{2 - \varepsilon}{d} \left(\frac{\log \log d}{\log d} \right)^3 .$$

Sa démonstration repose sur la méthode de Thue-Stewart, et utilise des congruences de manière un peu analogue à sa démonstration élémentaire précédente. Nous allons la présenter en y incorporant des simplifications introduites par Mignotte mais qui conduisent seulement à $c_0 = 10^{-6}$.

THÉORÈME (Dobrowolski). *Soit α un entier algébrique non nul et non racine de l'unité. Alors*

$$M(\alpha) > 1 + c_0 \left(\frac{\log \log d}{\log d} \right)^3$$

avec $c_0 \geqslant 10^{-6}$.

Pour présenter la démonstration de Dobrowolski, nous allons procéder par approximations successives; pour les résultats intermédiaires, voir Mignotte [M].

LEMME 1. *Soit α un entier algébrique non nul qui n'est pas racine de l'unité, de degré d et de hauteur $\leqslant H$. Alors*

$$M(\alpha) \geqslant 2^{1/(2dH)} > 1 + \frac{\log 2}{2\,d\,H} .$$

La deuxième inégalité résulte de $1 + x < e^x$ pour $x > 0$. Pour la première on considère un nombre premier p vérifiant $2\,d\,H \leqslant p \leqslant 4\,d\,H$. Soit f le polynôme minimal de α. On a par le petit théorème de Fermat

$$f(X^p) \equiv f(X)^p \mod p\,\mathbf{Z}[X]$$

donc p^d divise la norme de $f(\alpha^p)$. Comme α et α^p ne sont pas conjugués, on a $f(\alpha^p) \neq 0$. Donc

$$p^d \leqslant \left| \text{Norme } f(\alpha^p) \right| \leqslant (d\,H)^d\, M(\alpha)^{pd} .$$

Donc

$$M(\alpha) \geqslant (p/dH)^{1/p} .$$

L'étude de la fonction $(x/dH)^{1/x}$ sur l'intervalle $[2\,dH,\ 4\,dH]$ donne le résultat.

Au lieu d'utiliser le polynôme minimal de f on peut utiliser n'importe quel polynôme $F \in \mathbf{Z}[X]$, pourvu que $F(\alpha^p) \neq 0$. On aura une bonne minoration de la norme de $F(\alpha^p)$ si f (ou mieux, une puissance de f) divise F.

LEMME 2. *Soient α un entier algébrique non nul et non racine de l'unité, f son polynôme minimal, H sa hauteur, T un entier, p un nombre premier, et $F \in \mathbf{Z}[X]$ un polynôme de degré $< L$ tel que f^T divise F et $F(\alpha^p) \neq 0$. Alors*

$$M(\alpha)^{Lp}\ (LH)^d \geqslant p^{dT}\ .$$

En effet, on a

$$\left| N(F(\alpha^p)) \leqslant (L\,H)^d\ M(\alpha)^{Lp} \right.$$

et p^{dT} divise la norme de $F(\alpha^p)$.

Il reste à trouver un polynôme F vérifiant les hypothèses du lemme 2. On peut bien sûr choisir $F = f^T$, mais on ne trouve alors rien de mieux que le lemme 1. Le miracle vient de la méthode de Thue: en utilisant le lemme de Siegel, on peut construire un polynôme F tel que f^T divise F, et tel que la hauteur de F ne soit pas trop grande:

$$H(F) \leqslant 2 + \left(2^T\, L^{T^2 d} M(\alpha)^{TL}\right)^{1/(L-dT)}\ ,$$

pourvu que $L \geqslant 2\,dT$. Ainsi le degré de F risque d'être plus grand que celui de f^T, mais on gagne une bonne majoration de la hauteur de F. On choisit $T = [50\,(\log d)\,(\log\log d)^{-1}]$, et $L = dT^2$. On montre qu'il existe un nombre premier p dans l'intervalle $[T^2, 6\,T^2 \log T]$ tel que $F(\alpha^p) \neq 0$. On en déduit $\log M(\alpha) \geqslant (8\,T^3)^{-1}$ pour $d \geqslant 16$, ce qui démontre le théorème.

Dans un travail récent [D], E. Dobrowolski a obtenu des minorations de $M(P)$ pour $P \in \mathbf{Z}[X]$, $P(0) \neq 0$ et P non produit de polynômes cyclotomiques, en fonction seulement du nombre de coefficients non nuls de P.

ANALOGUE ELLIPTIQUE

Soit E une courbe elliptique définie sur le corps $\overline{\mathbf{Q}}$ des nombres algébriques. Soit $\hat{h}$ la hauteur de Néron Tate sur $E(\overline{\mathbf{Q}})$. M. Anderson a démontré dans le cas C.M. que pour tout $P \in E(\overline{\mathbf{Q}})$ non de torsion,

$$\hat{h}(P) > c_1\ D^{-4} (\log D)^{-3}\ ,$$

où c_1 est une constante positive ne dépendant que de g_2, g_3. Cet énoncé a été récemment amélioré par D. W. Masser (résultat annoncé en Mai 1979 aux journées sur les fonctions abéliennes et les nombres transcendants):

THÉORÈME (D. W. Masser). *Soit E une courbe elliptique définie sur $\overline{\mathbf{Q}}$ Il existe $c_2 > 0$ tel que si $P \in E(\overline{\mathbf{Q}})$ n'est pas de torsion, alors*

$$\hat{h}(P) > c_2 \; D^{-10} (\log D)^{-6} .$$

De plus si E a une multiplication complexe

$$\hat{h}(P) > c_2 \; D^{-3} (\log D)^{-2} .$$

REMARQUE FINALE

Soit α un *nombre* algébrique de polynôme minimal

$$a_0 X^d + \ldots = a_d = a_0 \prod_{j=1}^{d} (X - \alpha_j) .$$

On définit

$$M(\alpha) = |a_0| \prod_{j=1}^{d} \max(1, |\alpha_j|) .$$

Le résultat suivant, implicite chez Feldman, a été explicité par D. Bertrand:

$$M(\alpha) = \prod_{v} \max(1, |\alpha|_v)$$

où v décrit l'ensemble des valeurs absolues convenablement normalisées de $\mathbf{Q}(\alpha)$. La hauteur logarithmique absolue de α introduite par A. Weil peut alors être définie par

$$h(\alpha) = \frac{1}{[\mathbf{Q}(\alpha) : \mathbf{Q}]} \log M(\alpha) .$$

Dans les démonstrations de transcendance on a le choix entre plusieurs définitions de la « taille ». Il est maintenant généralement admis (depuis peu) que le meilleur choix est $h(\alpha)$.

RÉFÉRENCES

Nous ne mentionnons que les références qui ne se trouvent pas dans les bibliographies de [M] et [S].

[B1] BOYD, David W. *Pisot numbers and the width of meromorphic functions.* Privately circulated manuscript, Janvier 1977.

[B2] BOYD, David W. Variations on a theme of Kronecker. *Canad. Math. Bull. 21* (1978), 129-133.

[B3] —— Pisot sequences, Pisot numbers and Salem numbers. *Astérisque 61* (1979), 35-42.

[B4] —— *Reciprocal polynomials having small values* Manuscrit, Mai 1979.

[D] DOBROWOLSKI, Edouard. *On a question of Lehmer and the number of irreducible factors of a polynomial* Manuscrit.

[M] MIGNOTTE, Maurice. Entiers algébriques dont les conjugués sont proches du cercle unité. *Sém. Delange Pisot Poitou (théorie des nombres) 19* (1977/78), n° 39, 6 p.

[S] STEWART, Cameron L. On a theorem of Kronecker and a related question of Lehmer. *Sém. théorie des nombres.* Bordeaux, 1977/78, n° 7, 11 p.

(Reçu le 3 janvier 1980)

Michel Waldschmidt

Institut Henri-Poincaré
11, rue Pierre-et-Marie-Curie
75231 Paris Cédex 05