COLLOQUIUM MATHEMATICUM

VOL. L 1985 FASC. 1

ON A THEOREM OF DOBROWOLSKI ABOUT THE PRODUCT OF CONJUGATE NUMBERS

BY

ULRICH RAUSCH (MARBURG)

1. Let α be an algebraic integer of degree n over Q, different from zero and roots of unity. We consider

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

where $\alpha_1, \ldots, \alpha_n$ denote the conjugates of α. Dobrowolski ([1]) has shown that

$$M(\alpha) > 1+(1-\varepsilon)\left(\frac{\log\log n}{\log n}\right)^3$$

for arbitrary positive ε and $n > n_0(\varepsilon)$. His proof depends on the construction of an auxiliary polynomial with small coefficients, for which purpose a sharpened version of Siegel's lemma is employed. But, instead of the coefficients, it suffices to control the *values* of that polynomial at certain points. This observation enables us to simplify the argument considerably by replacing Siegel's lemma with Minkowski's theorem on linear forms. A slight improvement of the result is obtained too, namely

THEOREM.

$$M(\alpha) > 1+(2-\varepsilon)\left(\frac{\log\log n}{\log n}\right)^3 \quad (\varepsilon > 0;\ n > n_0(\varepsilon)).$$

2. We state three lemmas, the first of which is due to Dobrowolski.

LEMMA 1.

$$\alpha_i^r \neq \alpha_j^s \quad \textit{for} \quad r, s \in N,\ r \neq s,\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n; \tag{1}$$

$$\Big|\prod_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} (\alpha_i^p - \alpha_j)\Big| \geqslant p^n \quad \textit{for prime numbers } p. \tag{2}$$

LEMMA 2. *Let $Q \subset N$ be a finite set such that*

(3) $$\deg(\alpha^q) = n \quad \text{for} \quad q \in Q$$

and let $R_q \in N$ for $q \in Q$. Moreover, let λ_{qr} be positive real numbers having the property that for arbitrary $F(x) \in Z[x]$ the inequalities

(4) $$\Big|\prod_{i=1}^{n} F^{(r)}(\alpha_i^q)\Big| < \lambda_{qr} \quad (q \in Q;\ r = 0, \ldots, R_q - 1)$$

imply already

(5) $$F(\alpha^q) = F'(\alpha^q) = \ldots = F^{(R_q-1)}(\alpha^q) = 0 \quad (q \in Q).$$

Then

$$\log M(\alpha) > \frac{\Lambda - \frac{1}{2}(\sum R_q^2)\log(n \sum R_q)}{(\sum R_q)(\sum qR_q)},$$

where the sums are extended over $q \in Q$ and

$$\Lambda = \frac{1}{n}\log \prod_{q \in Q} \prod_{r=0}^{R_q-1} \lambda_{qr}.$$

Proof. Let $N = n \sum R_q$ and consider a polynomial in x of degree $N-1$ with indeterminate coefficients x_j:

$$\Phi(x; x_j) = \sum_{j=0}^{N-1} x_j \cdot x^j.$$

The terms

$$\frac{d^r}{dx^r}\Phi(x; x_j)\Big|_{x=\alpha_i^q} = \sum_{j=r}^{N-1} j(j-1)\ldots(j-r+1)\alpha_i^{q(j-r)} x_j$$

$$(q \in Q;\ r = 0, \ldots, R_q - 1;\ i = 1, \ldots, n)$$

constitute a system of N linear forms in the x_j's. We denote the absolute value of its determinant by D. Then

$$\prod_{q \in Q} \prod_{r=0}^{R_q-1} \lambda_{qr} \leqslant D,$$

since otherwise Minkowski's theorem (which is easily extended to cover the case $D = 0$) would supply numbers

$$a_0, \ldots, a_{N-1} \in Z, \quad \text{not all zero},$$

such that

$$F(x) := \Phi(x; a_j) \in Z[x] \setminus \{0\}$$

would satisfy (4) and hence also (5). This means (cf. (1))

$$\prod_{q\in Q} f_q(x)^{R_q} \mid F(x),$$

$f_q(x)$ signifying the minimal polynomial of α^q. By (3) we obtain a contradiction:

$$N-1 \geqslant \deg F(x) \geqslant \deg \prod_{q\in Q} f_q(x)^{R_q} = N.$$

On the other hand, Hadamard's inequality yields

$$\begin{aligned} D &\leqslant \prod_{q\in Q} \prod_{r=0}^{R_q-1} \prod_{i=1}^{n} \Big\{ \sum_{j=r}^{N-1} |j(j-1)\ldots(j-r+1)\alpha_i^{q(j-r)}|^2 \Big\}^{1/2} \\ &< \prod_{q\in Q} \prod_{r=0}^{R_q-1} \prod_{i=1}^{n} \{N^{r+1/2} \max(1, |\alpha_i|)^{qN}\} \\ &= N^{n\sum R_q^2/2} \cdot M(\alpha)^{N\sum qR_q}, \end{aligned}$$

and the assertion follows. □

It remains to prepare a tool for dealing with condition (3). Although Lemma 3 of [1] would suffice for our present purpose, the following lemma may be of independent interest.

Lemma 3. *Let p be a prime and $\deg(\alpha^p) = d < n$. Then $M(\alpha) = M(\alpha^p)$ or else there is a p-th root of unity ζ such that $\deg(\zeta\alpha) = d$ and $M(\alpha) > M(\zeta\alpha)$.*

This implies that one may assume

(6) $$\deg(\alpha^p) = n \quad \text{for all primes } p$$

in most cases when lower bounds for $M(\alpha)$ are concerned. Indeed, suppose we have proved

(7) $$M(\alpha) > 1 + \Theta(n)$$

for all α subject to (6) and all n, Θ being a positive non-increasing function. Then induction on n yields immediately that (7) generally holds. If (7) is known only for $n > n_0$, we apply the same argument to $\Theta^*(n) = \min(\Theta(n), c)$, where c is some positive constant such that

$$M(\alpha) > 1 + c \quad \text{for} \quad 1 \leqslant n \leqslant n_0,$$

and observe that $\Theta^*(n) = \Theta(n)$ for large n if, additionally, $\Theta(n)$ tends to zero for $n \to \infty$.

Proof of Lemma 3. If $n/d = [Q(\alpha): Q(\alpha^p)] = p$, then each conjugate of α^p occurs exactly p times among the numbers $\alpha_1^p, \ldots, \alpha_n^p$; thus

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

Now let $n/d \neq p$. Then the equation $x^p - \alpha^p = 0$ is reducible over $Q(\alpha^p)$, say

$$x^p - \alpha^p = g(x)h(x), \quad g(x),\ h(x) \in Q(\alpha^p)[x], \quad 1 \leqslant \deg g(x) =: t < p.$$

Since

$$x^p - \alpha^p = \prod_{s=1}^{p} (x - \alpha e^{2\pi i s/p}),$$

it follows by considering the constant term of $g(x)$ that

$$\xi\alpha^t \in Q(\alpha^p), \quad \xi \text{ a } p\text{th root of unity.}$$

But $kt + lp = 1$ for suitable $k, l \in Z$, and so

$$\zeta\alpha = (\xi\alpha^t)^k (\alpha^p)^l \in Q(\alpha^p), \quad \text{where } \zeta := \xi^k.$$

Thus we have $Q(\zeta\alpha) = Q(\alpha^p)$, i.e., $\deg(\zeta\alpha) = d$, and $\zeta \in Q(\alpha)$. If $\zeta_1, \ldots, \zeta_n$ are the conjugates of ζ relative to $Q(\alpha)$, then each conjugate of $\zeta\alpha$ over Q occurs exactly n/d times among the numbers $\zeta_1\alpha_1, \ldots, \zeta_n\alpha_n$; hence

$$M(\alpha) = \prod_{i=1}^{n} \max(1, |\zeta_i \alpha_i|) = M(\zeta\alpha)^{n/d} > M(\zeta\alpha). \ \square$$

3. Proof of the theorem. We assume (6) and choose in Lemma 2 $Q = \{1\} \cup P$, where P is the set of all prime numbers $p \leqslant u$. Further we put $R_1 = R$, $R_p = 1$ for $p \in P$. Then the numbers

$$\lambda_{1r} = 1 \quad (r = 0, \ldots, R-1),$$
$$\lambda_{p0} = p^{nR} \quad (p \in P)$$

satisfy the required conditions: (4) implies first

$$F(\alpha) = F'(\alpha) = \ldots = F^{(R-1)}(\alpha) = 0, \quad \text{i.e.,} \quad f_1(x)^R \mid F(x),$$

and then, by (2), $F(\alpha^p) = 0$ for $p \in P$. Hence

$$\log M(\alpha) > \frac{R \sum_{p \leqslant u} \log p - \frac{1}{2}\{R^2 + \pi(u)\} \log(n\{R + \pi(u)\})}{\{R + \pi(u)\}\{R + \sum_{p \leqslant u} p\}}.$$

Finally, setting

$$R = \left[\frac{\log n}{\log\log n}\right], \quad u = \frac{(\log n)^2}{\log\log n},$$

we obtain by means of the prime number theorem

$$\log M(\alpha) > 2\left(\frac{\log\log n}{\log n}\right)^3 (1 + o(1)) > (2 - \varepsilon)\left(\frac{\log\log n}{\log n}\right)^3$$

if n is sufficiently large. This proves the assertion. $\square$

REFERENCE

[1] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arithmetica 34 (1979), p. 391–401.

FACHBEREICH MATHEMATIK
UNIVERSITÄT MARBURG
MARBURG, BUNDESREPUBLIK DEUTSCHLAND

Reçu par la Rédaction le 12.01.1981

Annex. In view of the proof of Lemma 2, one will naturally suppose that the determinant considered there can be explicitly expressed by a product of differences, similar to the Vandermondian. This is in fact true, and E. Dobrowolski has just sent me an elegant proof which I shall record here.* As a consequence, the preceding proof may be rearranged so that Minkowski's theorem as well as any reminiscence of transcendence theory is avoided.

Dobrowolski argues as follows: Consider the vector valued function

$$\varphi\colon C \to C^N, \qquad \varphi(z) = (1, z, \ldots, z^{N-1})^T$$

together with its derivatives $\varphi^{(r)}$. The determinant in question is of the form

$$D = \det[\varphi(z_1), \ldots, \varphi^{(L_1-1)}(z_1), \ldots, \varphi(z_m), \ldots, \varphi^{(L_m-1)}(z_m)]$$

with $\sum_{j=1}^{m} L_j = N$.

(In Lemma 2: $z_1 = \alpha_1^{q_1}, \ldots, z_n = \alpha_n^{q_1}$, $z_{n+1} = \alpha_1^{q_2}, \ldots, z_{2n} = \alpha_n^{q_2}, \ldots$ and $L_1 = \ldots = L_n = R_{q_1}$, $L_{n+1} = \ldots = L_{2n} = R_{q_2}, \ldots$ if $Q = \{q_1, q_2, \ldots\}$.) Now, for given h, let

$$(\Delta_0 \varphi)(z) = \varphi(z), \qquad (\Delta_{r+1} \varphi)(z) = (\Delta_r \varphi)(z+h) - (\Delta_r \varphi)(z) \qquad (r \geqslant 0).$$

Then

$$(\Delta_r \varphi)(z) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \varphi(z + (r-k)h) \tag{8}$$

* Editors' note: As pointed out by A. Schinzel, the determinant in question was evaluated by C. Meray in 1867 (cf. M. Shibayama, Tôhoku Mathematical Journal 2 (1912), p. 143–146).

and

$$\lim_{h \to 0} h^{-r} (\Delta_r \varphi)(z) = \varphi^{(r)}(z).$$

Hence

$$D = \lim_{h \to 0} h^{-M} \det [\Delta_0 \varphi(z_1), \ldots, \Delta_{L_1-1} \varphi(z_1), \ldots$$
$$\ldots, \Delta_0 \varphi(z_m), \ldots, \Delta_{L_m-1} \varphi(z_m)],$$

where $M = \sum_{j=1}^{m} \sum_{i=1}^{L_j-1} i$.

From (8) it follows, on taking linear combinations of the columns, that

$$D = \lim_{h \to 0} h^{-M} \det \big[\varphi(z_1), \varphi(z_1+h), \ldots, \varphi\big(z_1+(L_1-1)h\big), \ldots$$
$$\ldots, \varphi(z_m), \ldots, \varphi\big(z_m+(L_m-1)h\big)\big],$$

and this is Vandermonde's determinant. So

$$D = \prod_{i>j} (z_i - z_j)^{L_i L_j} \prod_{k=1}^{m} [(L_k-1)!(L_k-2)! \ldots 2!\,1!].$$

Reçu par la Rédaction le 15.03.1981