HUGH L. MONTGOMERY

Polynomials in many variables

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 17, nº 1 (1975-1976), exp. nº 7, p. 1-6

<http://www.numdam.org/item?id=SDPP_1975-1976__17_1_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
17e année, 1975/76, n° 7, 6 p.

POLYNOMIALS IN MANY VARIABLES

by Hugh L. MONTGOMERY

We concern ourselves with two completely unrelated topics, although polynomials in several variables are involved in both parts.

PART I. Zeros of Dirichlet polynomials

Let $\mathfrak{D}$ be the class of all generalized Dirichlet polynomials

$$D(s) = 1 + \sum_{n=1}^{N} a_n \exp(-\lambda_n s) ,$$

where $a_n \in \mathbb{Z}$, and $\lambda_n > 0$ for all n. Such Dirichlet polynomials have been known to arise as factors of Euler products. We ask : For $D \in \mathfrak{D}$, how far to the left can all the zeros of $D(s)$ be ? Recently, it was shown that for every $\varepsilon > 0$, $D(s)$ has a zero in the half-plane $\operatorname{Re} s > -\varepsilon$. Our object (realized in Theorem 3) is to sharpen this statement, and to determine the extremal $D(s)$.

In 1857, KRONECKER proved the following theorem.

THEOREM A. - *If* $F \in \mathbb{Z}[x]$, F *is monic, and* $F(x) \neq 0$ *for* $|x| > 1$, $x \in \mathbb{C}$, *then* F *is a product of cyclotomic polynomials ; all zeros of* F *are roots of unity*.

The above does not seem to present much prospect of being generalized to several variables, as in several variables it would be difficult to determine what a "monic" polynomial should be. However, we can reformulate Theorem A as the following.

THEOREM A'. - *If* $F \in \mathbb{Z}[x]$, $F(C) = 1$, $F(x) \neq 0$ *for* $|x| < 1$, $x \in \mathbb{C}$, *then* F *is a product of cyclotomic polynomials ; its zeros are roots of unity*.

This generalizes immediately, as a new theorem.

THEOREM 1. - *If* $F \in \mathbb{Z}[z_1, z_2, \ldots, z_n]$, $F(\underset{\sim}{0}) = 1$, $F(\underset{\sim}{z}) \neq 0$ *for* $\underset{\sim}{z} \in U^n$, *where* $U^n = \{\underset{\sim}{z} \in \mathbb{C}^n ;\ |z_i| < 1$ *for* $1 \leqslant i \leqslant n\}$, *then*

$$F(\underset{\sim}{z}) = \prod_{k=1}^{K} P_k(z_1^{a_{1k}} z_2^{a_{2k}} \ldots z_n^{a_{nk}}) ,$$

where the P_k *are cyclotomic polynomials and the* a_{ik} *are non-negative integers*.

In addition to my original proof of Theorem 1, which was very complicated, Bryan BIRCH and Atle SELBERG have found simpler proofs. We do not give a complete proof here, but indicate the spirit of my original proof, as modified by BIRCH.

We proceed by induction on n ; the case $n = 1$ is Theorem A' . Suppose that there is a non-constant term of $F(\underset{\sim}{z})$ which does not involve z_n . This is, of course, only a special case ; in general, we must make a multiplicative change of variables to bring about this favorable situation. Then

$$F(\underset{\sim}{z}) = \sum_{j=0}^{J} F_j(z_1 , z_2 , \ldots , z_{n-1}) \, z_n^j ,$$

and F_0 is non trivial. If $J = 0$, then we are done ; if $J > 0$, then we wish to show that F_0 is a factor of the other F_j . By the inductive hypothesis, F_0 is a product of polynomials $P(z_1^{a_1} z_2^{a_2} \ldots z_{n-1}^{a_{n-1}})$, P cyclotomic. Thus each factor of F_0 vanishes on a large set in $\overline{U}^{n-1}$, so to show that $F_0 | F_j$ it suffices to show that $F_j = 0$ in $\overline{U}^{n-1}$ whenever $F_0 = 0$. Let $F_0(\underset{\sim}{u}) = 0$, $|u_i| = 1$, $1 \leq i \leq n - 1$. Put

$$f_\lambda(y) = \sum_{j=0}^{J} F_j(\lambda \underset{\sim}{u}) \, y^j .$$

Suppose that $F_j(\underset{\sim}{u}) \neq 0$ for at least one j , $1 \leq j \leq J$. The coefficients of f_λ are continuous functions in λ , so that for λ near 1 there is a continuous function $y(\lambda)$ such that $y(1) = 0$, $f(y(\lambda)) = 0$. Then, for $\lambda < 1$, λ near 1 , we have $F(z) = 0$ for $\underset{\sim}{z} = (u_1 , \ldots , u_{n-1} , y(\lambda)) \in U^n$, a contradiction. Hence $F_j(\underset{\sim}{u}) = 0$, and we deduce that $F_0 | F$, as desired.

In his doctoral thesis, Harald BOHR demonstrated that the set of values of a generalized Dirichlet polynomial is connected to the set of values of an associated polynomial in several variables. Precisely, if $P \in \underset{\sim}{C}[z_1 , \ldots , z_n]$, and $\lambda_1 , \ldots , \lambda_n$ are positive linearly independent numbers, put

$$D(s) = P(\exp(- \lambda_1 s) , \ldots , \exp(- \lambda_n s)) .$$

Then

$$\{P(\underset{\sim}{z}) \; ; \; |z_i| = 1\} = \bigcap_{\delta>0} \{D(s) \; ; \; |\mathrm{Re}\, s| < \delta\} . \tag{1}$$

To this, we add a new result.

THEOREM 2. - <u>In the above notation,</u>

$$\{P(\underset{\sim}{z}) \; ; \; \underset{\sim}{z} \in U^n\} = \{D(s) \; ; \; 0 < \mathrm{Re}\, s \leq + \infty\} .$$

<u>Proof</u>. - Call the above sets X and Y , respectively. By appealing to (1) for each $\sigma > 0$, we see that $Y = Y'$, where

$$Y' = \bigcup_{\sigma>0} \{P(\underset{\sim}{z}) \; ; \; |z_i| = \exp(- \lambda_i \sigma)\} .$$

That $X = Y'$ now follows from a standard analytic completion argument : Suppose $P(\underset{\sim}{z}) = a$, $\underset{\sim}{z} \in U^n$, and let σ_0 be the supremum of those σ with the property that $a \in \{P(\underset{\sim}{z}) \; ; \; \underset{\sim}{z} \in U(\sigma)\}$, where $U(\sigma) = \{\underset{\sim}{z} \; ; \; |z_i| \leq \exp(- \lambda_i \sigma)\}$. For $\sigma > \sigma_0$ let $f(\sigma) = \min_{\underset{\sim}{z} \in U(\sigma)} |P(\underset{\sim}{z}) - a|$. Then $f(\sigma_0) = 0$, and f is continuous and increasing for $\sigma_0 > \sigma_0$. For $\sigma_0 > \sigma_0$, let $\underset{\sim}{z}(\sigma) \in U(\sigma)$ have the property that $|P(z(\sigma))| - a|$ has the minimal value $f(\sigma)$. By the minimum modulus theorem, $|z_i(\sigma)| = \exp(- \lambda_i \sigma)$. Let $\underset{\sim}{z}(\sigma_0)$ be a cluster point of the points $\underset{\sim}{z}(\sigma)$ as as $\sigma \longrightarrow \sigma_0^+$. Then $|z_i(\sigma_0)| = \exp(-\lambda_i\,\sigma_0)$, and $P(\underset{\sim}{z}(\sigma_0)) = a$, so that $X = Y'$.

Our objective is now within reach.

THEOREM 3. – *Let* $D(s) = 1 + \sum_{n=1}^{N} a_n \exp(-\lambda_n\, s)$, *where* $a_n \in \underset{\sim}{Z}$, *not all* a_n *vanish, and the* λ_n *are positive real numbers. Then* $D(s)$ *has zeros in the half-plane* $\operatorname{Re} s \geqslant 0$. *If* $D(s) \neq 0$ *for* $\operatorname{Re} s > 0$, *then*

$$D(s) = \prod_{k=1}^{K} P_k(\exp(-\mu_k\, s)) ,$$

where the P_k *are cyclotomic and the* μ_k *are positive real ; the zeros of* $D(s)$ *form a finite union of arithmetic progressions on* $\operatorname{Re} s = 0$.

Proof. – After BOHR, there is a polynomial $F \in \underset{\sim}{Z}[z_1, \ldots, z_n]$ and linearly independent positive real numbers $\nu_1, \ldots, \nu_n$ such that

$$D(s) = P(\exp(-\lambda_1\, s), \ldots, \exp(-\lambda_n\, s)) .$$

By Theorem 2, we are concerned with zeros of $P(\underset{\sim}{z})$ for $\underset{\sim}{z} \in U^n$. But $P(\underset{\sim}{0}) = 1$, so the result follows from Theorem 1.

PART II. Norms of products of polynomials

For $F \in \underset{\sim}{C}[z_1, z_2, \ldots, z_n]$, say

$$F(\underset{\sim}{z}) = \sum_{\underset{\sim}{m}} a(\underset{\sim}{m})\, z_1^{m_1} z_2^{m_2} \ldots z_n^{m_n} , \tag{1}$$

let

$$f = \deg F = \max_{\underset{\sim}{m},\, a(\underset{\sim}{m}) \neq 0} (m_1 + m_2 + \ldots + m_n) , \tag{2}$$

and put

$$\|F\| = \sum_{\underset{\sim}{m}} |a(\underset{\sim}{m})| . \tag{3}$$

By the triangle inequality, we have

$$\|FG\| \leqslant \|F\| . \|G\| , \tag{4}$$

$$\|F + G\| \leqslant \|F\| + \|G\| . \tag{5}$$

If $f = \deg F$, $g = \deg G$, and n are all held fixed, then by compactness there is a constant $c = c(f, g ; n) > 0$ such that

$$\|FG\| \geqslant c(f, g ; n) \|F\| . \|G\| .$$

Arguing more precisely, A. O. GEL'FOND showed that one can take $c(f,g;1)=C^{-f-g}$; later Kurt MAHLER demonstrated this with $A = 2$, which is sharp. However, for $n > 1$, their methods give bounds depending not on $\deg F$ as we have defined it in (2), but on

$$\sum_{i=1}^{n} \max_{\underset{\sim}{m},\, a(\underset{\sim}{m}) \neq 0} m_i ;$$

this gives some dependence on n, in addition to that on f and g. Of course, if n is allowed to be arbitrarily large then we no longer have compactness, so it is of interest that Per ENFLO has recently proved the following theorem.

THEOREM. - *There is a positive constant* $c(f, g)$, *independent of* n, *such that for all polynomials* F, G *in* n *variables, with degrees not exceeding* f *and* g, *respectively,*

$$\|FG\| \geqslant c(f, g)\|F\|.\|G\| .$$

This forms one of the steps in Enflo's recent disproof of the invariant subspace conjecture. His proof of the above theorem is very complicated ; we give here a proof which seems to be easier to understand, and which generalizes easily in a number of ways.

If $F^* = z_0^f F(z_1/z_0, \dots, z_n/z_0)$ then F^* is homogeneous of degree f, $\|F^*\| = \|F\|$, and $(FG)^* = F^* G^*$. Thus in proving the Theorem, we may assume without loss of generality that F and G are homogeneous. This allows us to employ the following simple lemma.

LEMMA 1 [EULER]. - *Let* $F_i = \partial F/\partial z_i$. *If* F *is homogeneous of degree* f, *then*

(6) $$\sum_{i=1}^{n} \|F_i\| = f\|F\| .$$

Let $c_r(f, g)$ be the largest real number such that

(7) $$\|F^r G\| \geqslant c_r(f, g)\|F\|^r \|G\|$$

for all polynomials F, G of degrees f, g, respectively.

Our proof proceeds by a complicated induction on r, f, and g. The two main inductive steps are provided by the following lemmas.

LEMMA 2. - *For* $r \geqslant 1$,

(8) $$c_{r+1}(f, 0) \geqslant c_1(f-1, fr)\, c_r(f, 0) .$$

Proof. - Using (7) twice, we see that

$$\begin{aligned}\|(r+1)F^r F_i\| &\geq (r+1)c_1(f-1, fr)\|F_i\|.\|F^r\| \\ &\geqslant (r+1)c_1(f-1, fr)\, c_r(f, 0)\|F_i\|.\|F\|^r .\end{aligned}$$

The left hand side is $= \|(F^{r+1})_i\|$, so we sum the above over i and apply lemma 1 to find that

$$f(r+1)\|F^{r+1}\| \geqslant (r+1)c_1(f-1, fr)\, c_r(f, 0)f\, \|F\|^{r+1} .$$

This gives (8)

LEMMA 3. - *For* $r \geqslant 1$, $g \geqslant 1$,

(9) $$c_r(f, g) \geqslant c_{r+1}(f, g-1)\, \frac{g}{2fr+g} .$$

Proof. - By (7),

(10) $$c_{r+1}(f\ ,\ g-1)\|F\|^{r+1}.\|G_i\| \leqslant \|F^{r+1}\ G_i\|\ .$$

But

$$\begin{aligned} F^{r+1}\ G_i &= F(F^r\ G_i + rF^{r-1}\ F_i\ G) - rF^r\ F_i\ G \\ &= F(F^r\ G)_i - rF^r\ F_i\ G\ , \end{aligned}$$

so the right hand side of (10) is

$$\begin{aligned} &\leqslant \|F(F^r\ G)_i\| + r\|F^r\ F_i\ G\| \\ &\leqslant \|F\|.\|(F^r\ G)_i\| + r\|F^r\ G\|.\|F_i\|\ , \end{aligned}$$

by (4) and (5). Summing over i, we find, from Lemma 1, that

$$c_{r+1}(f\ ,\ g-1)\|F\|^{r+1}.g.\|G\| \leqslant (fr+g)\|F\|.\|F^r\ G\| + fr\|F^r\ G\|.\|F\|\ .$$

This gives (9).

We now prove the Theorem, using Lemmas 2 and 3. Our first inductive hypothesis is that

(11) $$H(f)\ :\ c_1(f\ ,\ g) > 0 \ \text{ for all } \ g \geqslant 0\ .$$

We note that $c_1(0\ ,\ g) = 1$, which provides a basis for induction. We prove $H(f)$, assuming $H(f-1)$. Noting that $c_1(f\ ,\ 0) = 1$; we induct on r in Lemma 2 to find that $c_r(f\ ,\ 0) > 0$ for all $r \geqslant 1$. This provides the basis for an induction on g ; by Lemma 3, we see that $c_r(f\ ,\ g) > 0$ for all $g\ ,\ r$. This gives $H(f)$, which completes the induction on f .

The constants provided by our proof are very small. For example, we find that $c(3\ ,\ 4) > 2 \times 10^{-194}$. It would be interesting to know whether we could take $c(f\ ,\ g) = C^{-f-g}$.

Our proof extends in a number of directions. If K is a field of characteristic 0 having a valuation $\|\ \|_v$, then for F $K[z_1\ ,\ z_2\ ,\ \dots\ ,\ z_n]$, we may put

$$\|F\| = \sum_{\underset{\sim}{m}} \|a(\underset{\sim}{m})\|_v\ .$$

Then we still have the Theorem, although in general the constants may depend on v . If $\|m\|_v = m$ for all positive integers m , then the above proof applies without change. If we put

$$\|F\|_p = (\Sigma\ |a(\underset{\sim}{m})|^p)^{1/p}\ ,$$

then

(12) $$\|FG\|_p \geqslant c_p(f\ ,\ g)\|F\|_p\ \|G\|_p\ ;$$

the constant is uniform in p for $0 < \delta \leqslant p \leqslant +\infty$. Alternatively, if we put

$$\|F\|_q = \left(\int_0^1 \dots \int_0^1 |F(e(\theta_1)\ ,\ \dots\ ,\ e(\theta_n))|^q\ d\theta_1 \dots d\theta_n\right)^{1/q}\ ,$$

where $e(\theta) = \exp 2\pi i\theta$, we find that

$$\|FG\|_q \geqslant c_q(f\ ,\ g)\|F\|_q\ \|G\|_q \tag{13}$$

for $0 < q \leqslant +\infty$. In conclusion, we note an interesting difference between (12) and (13). If (13) holds for one $q < \infty$ then it follows for all other finite q , since there are constants a_i such that

$$a_1(q\ ,\ q')\|F\|_q \leqslant \|F\|_{q'} \leqslant a_2(q\ ,\ q')\|F\|_q$$

for $0 < q\ ,\ q' < \infty$. This is not the case in (12) ; the inequalities are genuinely distinct for distinct p .

(Texte reçu le 1er décembre 1975)

Hugh L. MONTGOMERY
Department of Mathematics
University of Michigan
ANN ARBOR, Mich. 48104
(Etats-Unis)