

## An Inequality About Factors of Polynomials

By M. Mignotte

**Abstract.** A sharp inequality is proved about the product of some roots of a polynomial. It is used to bound the height of the factors of a polynomial. Applications are given to the problem of factorization and numerical examples show that these bounds strongly improve the previous ones.

**I. Introduction.** If  $R = \sum_{j=0}^d c_j X^j$  is a polynomial with complex coefficients, we put

$$\|R\| = \left(\sum |c_j|^2\right)^{1/2}, \quad L(R) = \sum |c_j|, \quad H(R) = \max |c_j|.$$

We shall first prove:

**THEOREM 1.** Let  $P = \sum_{i=0}^d a_i X^i$  be a polynomial with complex coefficients. Let  $z_1, z_2, \dots, z_k$  be those zeros of  $P$  (counted with their multiplicities), such that  $1 \leq |z_1| \leq |z_2| \leq \dots \leq |z_k|$ . Then

$$|a_d| \prod_{i=1}^k |z_i| \leq \|P\|.$$

This inequality improves a result of Mahler [1] who obtained  $L(P)$  instead of  $\|P\|$  on the right-hand side.

**THEOREM 2.** Let  $Q$  be a polynomial with rational integer coefficients. If  $Q_1 \cdots Q_m R = Q$ , where  $Q_1, \dots, Q_m, R$  are polynomials with rational integer coefficients, then

$$(1) \quad \prod_{j=1}^m L(Q_j) \leq 2^D \|Q\|, \quad \text{where } D = \sum_{j=1}^m \deg(Q_j),$$

and, if for example  $Q_1 = b_0 + b_1 X + \dots + b_1 X^1$ , then

$$(2) \quad |b_i| \leq \binom{1}{i} \|Q\|.$$

(This result also holds for Gaussian integer coefficients.)

These inequalities can be used in the theory of transcendental numbers, but we

---

Received June 28, 1973.

AMS (MOS) subject classifications (1970). Primary 12D05.

Key words and phrases. Inequality, roots of polynomial, factorization.

Copyright © 1974, American Mathematical Society

shall not speak of this here. They are also useful in the problem of factorization of polynomials over  $\mathbf{Z}$  as we shall see now.

We recall the method of H. Zassenhaus [3]. Put

$$F(X) = X^n + a_1X^{n-1} + \dots + a_n, \quad a_i \in \mathbf{Z},$$

and assume that

$$G(X) = X^m + b_1X^{m-1} + \dots + b_m, \quad b_j \in \mathbf{Z}, m \leq n/2,$$

is a factor of  $F$ .

Suppose that we find  $M$  such that for any such  $G$  we have  $H(G) \leq M$ . We take a prime number  $p$ , not dividing the discriminant of  $F$ , and choose  $r$  such that  $p^r > 2M$ . Then, starting with a factorization into monic polynomials

$$F \equiv F_1 \cdots F_k \pmod{p},$$

we get, with the help of Hensel's lemma, well-defined  $\bar{F}_i \in \mathbf{Z}(X)$  such that

$$F \equiv \bar{F}_1 \cdots \bar{F}_k \pmod{p^r}, \quad \text{with } \bar{F}_i \equiv F_i \pmod{p}, \quad i = 1, \dots, r,$$

and such that the coefficients of the  $\bar{F}_i$  belong to the interval  $] -p^r/2, p^r/2[$ .

It is now clear that we are able to factorize  $F$  over  $\mathbf{Z}$ . The problem is now to find a value for  $M$ .

Zassenhaus remarked that, if  $|z| \leq A$  for any root  $z$  of  $F$ , then

$$|b_j| \leq \binom{m}{j} A^j.$$

It is well known that we can take

$$(3) \quad A = \max |a_i| + 1.$$

Zassenhaus also used the bound

$$(4) \quad A = \max_{1 \leq i \leq n} \left| \frac{|a_i|}{\binom{n}{i}} \right|^{1/i} / (2^{1/n} - 1).$$

To show the strength of (2), we take two examples given in [4] to compare (3) and (4).

Put

$$F_1(X) = X^{15} + 30X^{14} + 5X^{13} + 2X^{12} + 5X + 2,$$

and

$$F_2(X) = X^8 + 8X^7 + 21X^6 + 21X^5 + 42X^4 + 13X^3 + 12X^2 - 14X + 12.$$

For  $F_1$ , we get

$$M_1 \leq 2.8 \cdot 10^{10} \quad \text{by (3),}$$

$$M_1 \leq 2.7 \cdot 10^9 \quad \text{by (4),}$$

and, for  $F_2$ ,

$$M_2 \leq 3.5 \cdot 10^6 \quad \text{by (3),}$$

$$M_2 \leq 1.4 \cdot 10^5 \quad \text{by (4);}$$

whereas (2) gives

$$M_1 \leq 1083 \quad \text{and} \quad M_2 \leq 348.$$

(In fact,  $F_1$  is irreducible: Rouché's theorem shows that all its roots but one lie in the disk  $|z| < 1$ .)

**II. Proof of Theorem 1.** A proof can be found in [2], but we prefer to deduce it from the following elementary lemma which gives a stronger result.

LEMMA 1. *Let  $P(X)$  be a polynomial with complex coefficients and  $\alpha$  be a nonzero complex number. Then*

$$\|(X + \alpha)P(X)\| = |\alpha| \|(X + \bar{\alpha}^{-1})P(X)\|.$$

*Proof.* Write

$$P(X) = \sum_{k=0}^m a_k X^k,$$

$$Q(X) = (X + \alpha)P(X) = \sum_{k=0}^{m+1} (a_{k-1} + \alpha a_k) X^k,$$

$$R(X) = (X + \bar{\alpha}^{-1})P(X) = \sum_{k=0}^{m+1} (a_{k-1} + \bar{\alpha}^{-1} a_k) X^k,$$

with  $a_{-1} = a_{m+1} = 0$ .

Then

$$\|Q\|^2 = \sum_{k=0}^{m+1} |a_{k-1} + \alpha a_k|^2 = \sum_{k=0}^{m+1} (a_{k-1} + \alpha a_k) \overline{(a_{k-1} + \alpha a_k)}$$

which expands to

$$\sum_{k=0}^{m+1} (|a_{k-1}|^2 + \alpha a_k \bar{a}_{k-1} + \bar{\alpha} a_{k-1} \bar{a}_k + |\alpha|^2 |a_k|^2).$$

Expanding  $|\alpha|^2 \|R\|^2$  yields the same sum.

Thus we have  $\|Q\| = |\alpha| \|R\|$ , which proves the lemma.

LEMMA 2. Let  $x_1, x_2, \dots, x_m$  be complex numbers,

$$0 < |x_1| \leq \dots \leq |x_q| < 1 \leq |x_{q+1}| \leq \dots \leq |x_m|, \quad q \geq 0.$$

Put

$$S(X) = (X - x_1) \cdots (X - x_m),$$

$$T(X) = (X - \bar{x}_1^{-1}) \cdots (X - \bar{x}_q^{-1})(X - x_{q+1}) \cdots (X - x_m).$$

Then

$$(5) \quad \|S\| = |x_1 \cdots x_q| \|T\|.$$

*Proof.* By induction on  $q$ . For  $q = 0$ , (5) holds. Assume  $q > 0$  and put

$$\bar{S}(X) = S(X)/(X - x_1), \quad \bar{T}(X) = T(X)/(X - \bar{x}_1^{-1}).$$

Then

$$\begin{aligned} \|S\| &= \|(X - x_1)\bar{S}(X)\| = |x_1| \|(X - \bar{x}_1^{-1})\bar{S}(X)\| \quad (\text{by Lemma 1}) \\ &= |x_1| |x_2 \cdots x_q| \|(X - \bar{x}_1^{-1})\bar{T}(X)\| \quad (\text{by induction hypothesis}) \\ &= |x_1 \cdots x_q| \|T\|. \end{aligned}$$

This implies the following refinement of Theorem 1.

PROPOSITION. Let  $P(X) = a_m X^m + \cdots + a_0 = a_m (X - x_1) \cdots (X - x_m)$  where  $x_1, \dots, x_m$  are complex numbers such that

$$|x_1| \leq \dots \leq |x_q| < 1 \leq |x_{q+1}| \leq \dots \leq |x_m|, \quad q \geq 0.$$

Then

$$\|P\|^2 \geq |a_m|^2 |x_{q+1} \cdots x_m|^2 + |a_0|^2 |x_{q+1} \cdots x_m|^{-2}.$$

*Proof.* Put

$$Q(X) = a_m \prod_{i=1}^q (X - \bar{x}_i^{-1}) \prod_{i=q+1}^m (X - x_i) = b_m X^m + \cdots + b_0.$$

First assume  $x_1 \neq 0$ . Then by Lemma 2,  $\|P\| = |x_1 \cdots x_q| \|Q\|$ , hence

$$\|P\|^2 \geq |x_1 \cdots x_q|^2 (|b_m|^2 + |b_0|^2),$$

from which the result follows.

If  $x_1 = \dots = x_n = 0$  ( $n \leq q$ ), then  $a_0 = 0$ , so we just have to prove  $\|P\|^2 \geq |a_m|^2 |x_{q+1} \cdots x_m|^2$ . But, in fact, replacing  $P(X)$  by  $P(X)/X^n$  in the above argument yields the stronger result

$$\|P\|^2 \geq |a_m|^2 |x_{q+1} \cdots x_m|^2 + |a_n|^2 |x_{q+1} \cdots x_m|^{-2}.$$

*Remarks.* (1) The proof of Theorem 1 is quite elementary while the previous inequalities were weaker and based on transcendental results such as Jensen's or Parseval's formula. We leave an analytic proof of Lemma 2 as exercise to the reader.

(2) In a certain sense, Theorem 1 is the best possible: the inequality is not always true if we replace  $\|P\|$  by  $(\sum |a_j|^e)^{1/e}$  for  $e > 2$ . (Take for example  $P(X) = X^2 - 2aX - 1$  where  $a$  is a sufficiently large positive number.)

**III. Proof of Theorem 2.** The well-known expression of the coefficients of a polynomial gives:

LEMMA 3. *Let  $P$  be as in Theorem 1. Then*

$$|a_i| \leq \binom{d}{i} |z_1 \cdots z_k| |a_d|,$$

and

$$\sum_{i=0}^d |a_i| \leq 2^d |z_1 \cdots z_k| |a_d|.$$

The theorem follows easily from Lemma 3 and Theorem 1.

**Acknowledgement.** I would like to thank the referee for several helpful comments.

Université Paris-Nord  
 Département de Mathématiques  
 Centre Scientifique et Polytechnique  
 Place du 8 Mai 1945  
 93 Saint-Denis 93206, France

1. K. MAHLER, "An application of Jensen's formula to polynomials," *Mathematika*, v. 7, 1960, pp. 98–100. MR 23 #A1779.
2. M. MIGNOTTE, "Critères d'irréductibilité des polynômes sur un corps de nombres," *Enseignement Math.*, v. 18, 1972, pp. 191–200.
3. H. ZASSENHAUS, "On Hensel factorization. I," *J. Number Theory*, v. 1, 1969, pp. 291–311. MR 39 #4120.
4. H. G. ZIMMER, *Computational Problems, Methods and Results in Algebraic Number Theory*, Lecture Notes in Math., vol. 269, Springer-Verlag, Berlin, 1972.