ON A THEOREM BY E. BOMBIERI

BY

K. MAHLER

(Communicated by Prof. J. POPKEN at the meeting of January 30, 1960)

A. BRAUER, in 1929 (Jber. D. Math. Ver. 38 (1929), 47), proved that if α is a fixed algebraic number of degree m and $\beta \neq \alpha$ is a variable algebraic number of degree n and height $H(\beta)$, then

$$|\alpha-\beta| > C^n H(\beta)^{-m},$$

where the constant $C>0$ depends only on α. This result has recently been greatly improved by E. BOMBIERI (Boll. Unione Mat. Ital. (III), 13 (1958), 351–354) who obtained the following theorem.

Let α and β be two distinct algebraic numbers which are not conjugates of one another and are of degrees m and n and of heights $H(\alpha)$ and $H(\beta)$, respectively. Then

$$|\alpha-\beta| > (4mn)^{-3mn} H(\alpha)^{-n} H(\beta)^{-m}.$$

A study of Bombieri's very elegant proof shows that its restriction to algebraic numbers is inessential and that it may be applied to the zeros of polynomials with arbitrary *real or complex coefficients*. In this note I use Bombieri's method to establish two theorems on such polynomials which contain his theorem, and its extension to the case of conjugate algebraic numbers, as special cases.

In the first theorem it is assumed that the resultant $R(f, g)$ of two arbitrary polynomials f and g does not vanish. Then a lower bound for the difference $|\alpha-\beta|$ between any zero α of f and any zero β of g is determined which depends only on $R(f, g)$ and on the degrees and heights of f and g. If these polynomials have integral coefficients and are irreducible, one comes back to Bombieri's theorem.

In the second theorem one assumes instead that the discriminant of the arbitrary polynomial f is not zero. It is then possible to obtain a lower bound for the difference $|\alpha_1-\alpha_2|$ of any two two distinct zeros of f that depends only on $D(f)$ and the degree and the height of f. In the special case when f has integral coefficients and is irreducible, this theorem establishes a lower bound for the difference of any two conjugate algebraic numbers.

1. If
$$f(z)=a_0z^m+a_1z^{m-1}+\ldots+a_m, \qquad \text{where } a_0\neq 0,$$
is an arbitrary polynomial with real or complex coefficients, denote by
$$\delta(f)=m \text{ and } H(f)=\max(|a_0|,|a_1|,\ldots,|a_m|)$$
its degree and its height, respectively. It is obvious that

(1) $$\delta\left(\frac{1}{k!}\frac{d^kf}{dz^k}\right)=m-k,\; H\left(\frac{1}{k!}\frac{d^kf}{dz^k}\right)\leqslant\binom{m}{k}H(f) \qquad (k=0,1,2,\ldots,m).$$

Let now A be an arbitrary real or complex number satisfying
$$|A|\geqslant 1,$$
and let further
$$f^*(z)=f(z+A).$$
Naturally
$$\delta(f^*)=\delta(f)=m.$$

Next, by Taylor's formula.
$$f^*(z)=\frac{f^{(m)}(A)}{m!}z^m+\frac{f^{(m-1)}(A)}{(m-1)}z^{m-1}+\ldots+f(A).$$
Here, by (1),
$$\left|\frac{f^{(k)}(A)}{k!}\right|\leqslant H\left(\frac{1}{k!}\frac{d^kf}{dz^k}\right)(1+|A|+|A|^2+\ldots+|A|^{m-k})\leqslant\binom{m}{k}H(f)\cdot(m+1)\,|A|^{m-k}.$$
Further
$$\binom{m}{k}|A|^{-k}\leqslant\sum_{k=0}^{m}\binom{m}{k}|A|^{-k}=(1+|A|^{-1})^m$$
and therefore
$$\binom{m}{k}|A|^{m-k}\leqslant(|A|+1)^m.$$
It follows therefore that

(2) $$H(f^*)\leqslant(m+1)(|A|+1)^mH(f) \qquad \text{if } |A|\geqslant 1.$$

2. Lemma 1. *If $\alpha_1,\ldots,\alpha_m$ are m real or complex numbers, there exists a real or complex number A such that*
$$1\leqslant|A|\leqslant\sqrt{m+1}, \qquad \min_{1\leqslant\mu\leqslant m}|\alpha_\mu-A|\geqslant 1.$$

When all numbers $\alpha_1,\ldots,\alpha_m$ are real, we may take $A=i$.

Proof: With the $m+1$ numbers $0,\alpha_1,\ldots,\alpha_m$ associate the circles
$$C_0: |z|<1, \text{ and } C_\mu: |z-\alpha_\mu|<1 \qquad (\mu=1,2,\ldots,m)$$
in the z-plane. Each of these circles has the area π; the area of the union of the $m+1$ circles hence does not exceed $\pi(m+1)$. On the other hand, the circle
$$C: |z|\leqslant\sqrt{m+1}$$
has exactly the area $\pi(m+1)$. There is then at least one point A of C which does not belong to any one of the circles $C_0, C_1, \ldots, C_m$. – The assertion for real numbers $\alpha_1,\ldots,\alpha_m$ is obvious.

3. Let
$$f(z)=a_0z^m+a_1z^{m-1}+\ldots+a_m=a_0(z-\alpha_1)(z-\alpha_2)\ldots(z-\alpha_m) \qquad (a_0\neq 0),$$
$$g(z)=b_0z^n+b_1z^{n-1}+\ldots+b_n=b_0(z-\beta_1)(z-\beta_2)\ldots(z-\beta_n) \qquad (b_0\neq 0)$$
be any two polynomials with real or complex coefficients which satisfy the condition that their resultant
$$R(f,g)=a_0^n\,b_0^m\prod_{\mu=1}^{m}\prod_{\nu=1}^{n}(\alpha_\mu-\beta_\nu)$$
does not vanish. This assumption implies that the minimum distance
$$\Delta(f,g)=\min_{\substack{1\leqslant\mu\leqslant m\\1\leqslant\nu\leqslant n}}|\alpha_\mu-\beta_\nu|$$
between the zeros of the two polynomials is a positive number. Our aim is to establish a lower bound for $\Delta(f,g)$ in terms of
$$\delta(f),\ \delta(g),\ H(f),\ H(g),\ R(f,g).$$

Let A be the number of Lemma 1, thus satisfying
$$1\leqslant|A|\leqslant\sqrt{m+1}, \qquad \min_{1\leqslant\mu\leqslant m}|\alpha_\mu-A|\geqslant 1.$$
Then put
$$f^*(z)=f(z+A),\ g^*(z)=g(z+A);\ \alpha_\mu^*=\alpha_\mu-A,\ \beta_\nu^*=\beta_\nu-A\ (1\leqslant\mu\leqslant m,\ 1\leqslant\nu\leqslant n)$$
so that
$$f^*(z)=a_0(z-\alpha_1^*)(z-\alpha_2^*)\ldots(z-\alpha_m^*),$$
$$g^*(z)=b_0(z-\beta_1^*)(z-\beta_2^*)\ldots(z-\beta_n^*).$$
Since $\alpha_\mu^*-\beta_\nu^*=\alpha_\mu-\beta_\nu$, it is obvious that

(3) $$R(f^*,g^*)=R(f,g),\quad \Delta(f^*,g^*)=\Delta(f,g).$$

Further

(4) $$|\alpha_\mu^*|\geqslant 1 \qquad (\mu=1,2,\ldots,m),$$

and by (2)

(5) $$H(f^*)\leqslant(m+1)(|A|+1)^mH(f),\quad H(g^*)\leqslant(n+1)\,(|A|+1)^nH(g).$$

From now on we assume, without loss of generality, that

$$(6) \qquad \Delta(f, g) \leqslant 1$$

and choose the notation such that

$$(7) \qquad \Delta(f, g) = |\alpha_1 - \beta_1| = |\alpha_1^* - \beta_1^*|.$$

The resultant may be written in the form

$$(8) \qquad R(f, g) = a_0{}^n \prod_{\mu=1}^{m} g^*(\alpha_\mu{}^*).$$

Here, by (4),

$$|g^*(\alpha_\mu{}^*)| \leqslant H(g^*)(1 + |\alpha_\mu{}^*| + |\alpha_\mu{}^*|^2 + \ldots + |\alpha_\mu{}^*|^n) \leqslant (n+1)|\alpha_\mu{}^*|^n H(g^*),$$

whence, by the second inequality (5),

$$(9) \qquad |g^*(\alpha_\mu{}^*)| \leqslant (n+1)^2(|A|+1)^n|\alpha_\mu{}^*|^n H(g) \qquad (\mu = 1, 2, \ldots, m).$$

Replace now on the right-hand side of (8) all factors $g^*(\alpha_\mu{}^*)$ except the one with $\mu = 1$ by this upper bound (9). It follows then that

$$(10) \qquad |R(f, g)| \leqslant |a_0|^n |g^*(\alpha_1{}^*)| \prod_{\mu=2}^{m} \{(n+1)^2(|A|+1)^n|\alpha_\mu{}^*|^n H(g)\}.$$

4. An upper bound for the remaining factor $g^*(\alpha_1{}^*)$ may be obtained from the identity

$$(11) \qquad g^*(\alpha_1{}^*) = g^*(\alpha_1{}^*) - g^*(\beta_1{}^*) = \int_{\beta_1{}^*}^{\alpha_1{}^*} \frac{dg^*(z)}{dz}\, dz,$$

where the integration extends over the line segment L joining $\beta_1{}^*$ to $\alpha_1{}^*$. Every point on L is of the form

$$z = (1-t)\alpha_1{}^* + t\beta_1{}^* = \alpha_1{}^* - t(\alpha_1{}^* - \beta_1{}^*)$$

where t is a real number between 0 and 1. It follows then, on applying the formulae (4), (6) and (7), that for all points on L,

$$|z| \leqslant |\alpha_1{}^*| + |\alpha_1{}^* - \beta_1{}^*| \leqslant |\alpha_1{}^*| + 1 \leqslant 2|\alpha_1{}^*|.$$

Next, by (1) and (5),

$$H\left(\frac{dg^*}{dz}\right) \leqslant nH(g^*) \leqslant n(n+1)(|A|+1)^n H(g).$$

Hence, when z runs over L,

$$\left|\frac{dg^*(z)}{dz}\right| \leqslant n(n+1)(|A|+1)^n H(g) \,.\, (1 + |2\alpha_1{}^*| + |2\alpha_1{}^*|^2 + \ldots + |2\alpha_1{}^*|^{n-1}).$$

Here

$$1 + |2\alpha_1{}^*| + |2\alpha_1{}^*|^2 + \ldots + |2\alpha_1{}^*|^{n-1} \leqslant (1 + 2 + 2^2 + \ldots + 2^{n-1})|\alpha_1{}^*|^{n-1} < \\ < 2^n|\alpha_1{}^*|^n,$$

and hence

$$(12) \qquad \left|\frac{dg^*(z)}{dz}\right| \leqslant n(n+1)2^n(|A|+1)^n|\alpha_1{}^*|^n H(g) \qquad \text{if } z \in L.$$

The integral (11) implies the estimate

$$|g^*(\alpha_1{}^*)| \leqslant |\beta_1{}^* - \alpha_1{}^*| \max_{z \in L} \left|\frac{dg^*(z)}{dz}\right|.$$

Thus, finally, it follows from (7) and (12) that

$$(13) \qquad |g^*(\alpha_1{}^*)| \leqslant \Delta(f, g) \,.\, n(n+1)2^n(|A|+1)^n|\alpha_1{}^*|^n H(g).$$

5. Now substitute this upper bound in (10). We find that

$$|R(f, g)| \leqslant |a_0|^n \Delta(f, g) n(n+1) 2^n(|A|+1)^n|\alpha_1{}^*|^n H(g) \,. \\ \cdot \prod_{\mu=2}^{m} \{(n+1)^2(|A|+1)^n|\alpha_\mu{}^*|^n H(g)\} \\ \leqslant |a_0\alpha_1{}^*\alpha_2{}^*\ldots\alpha_m{}^*|^n (n+1)^{2m} 2^n (|A|+1)^{mn} H(g)^m \Delta(f, g).$$

Here

$$a_0\alpha_1{}^*\alpha_2{}^*\ldots\alpha_m{}^*$$

is the constant term of $f^*(z)$; its absolute value does not then exceed the height of this polynomial, and hence

$$|a_0\alpha_1{}^*\alpha_2{}^*\ldots\alpha_m{}^*| \leqslant H(f^*) \leqslant (m+1)(|A|+1)^m H(f).$$

The last inequality therefore becomes

$$(14) \qquad |R(f, g)| \leqslant c_1(f, g) H(f)^n H(g)^m \Delta(f, g)$$

where we have put

$$c_1(f, g) = (m+1)^n (n+1)^{2m} 2^n (|A|+1)^{2mn}.$$

It is convenient to replace $c_1(f, g)$ by a larger, but simpler expression. First, since $m \geqslant 1$ and $|A| \geqslant 1$,

$$2^n \leqslant (m+1)^n, \quad |A|+1 \leqslant 2|A|,$$

and so $c_1(f, g)$ is not greater than the expression $c_2(f, g)$ given by

$$c_2(f, g) = (m+1)^{2n}(n+1)^{2m} 2^{2mn} |A|^{2mn}.$$

When all the zeros of $f(z)$ are real, we may simply put $A = i$ and hence $|A| = 1$, when $c_2(f, g)$ obtains the value

$$(m+1)^{2n}(n+1)^{2m}2^{2mn}.$$

Excluding this trivial choice, we may always take for A a number satisfying $|A| \leqslant \sqrt{m+1}$, and then $c_2(f, g)$ becomes

$$\leqslant (m+1)^{2n}(n+1)^{2m}2^{2mn}(m+1)^{mn}.$$

Finally, we may always interchange the polynomials $f(z)$ and $g(z)$ in our proof, which means that also m and n are interchanged. We obtain therefore finally the following result.

Theorem 1. *Let $f(z)$ and $g(z)$ be two polynomials with real or complex coefficients, of degrees $\delta(f)=m$ and $\delta(g)=n$, of heights $H(f)$ and $H(g)$, and with zeros $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$, respectively. Assume that the resultant $R(f, g)$ of the two polynomials does not vanish, and put*

$$\Delta(f,g) = \min_{\substack{1\leqslant\mu\leqslant m\\ 1\leqslant\nu\leqslant n}} |\alpha_\mu - \beta_\nu|.$$

Finally, let

$$C(f, g) = (m+1)^{2n}(n+1)^{2m}4^{mn}c(f, g)^{mn}$$

where $c(f, g)$ is 1 when at least one of the two polynomials has only real zeros, and where otherwise $c(f, g)$ denotes the smaller one of the two numbers $m+1$ and $n+1$. Then either

$$\Delta(f, g) \geqslant 1$$

or

$$\Delta(f, g) \geqslant \{C(f, g)H(f)^n H(g)^m\}^{-1}|R(f, g)|.$$

Remark: When the two polynomials $f(z)$ and $g(z)$ have rational integral coefficients, $R(f, g)$ becomes an integer distinct from zero, and so $|R(f, g)| \geqslant 1$. Theorem 1 becomes therefore now the theorem of E. Bombieri.

6. Theorem 1 has an analogue involving the zeros $\alpha_1, \ldots, \alpha_m$ of the single polynomial $f(z)$ which, as before, may have any real or complex coefficients. It will now be assumed that the discriminant

$$D(f) = a_0^{2m-2} \prod_{1\leqslant\mu<\nu\leqslant m} (\alpha_\mu - \alpha_\nu)^2$$

of $f(z)$ does not vanish; thus all the zeros of $f(z)$ are distinct, and the minimum distance

$$\Delta(f) = \min_{1\leqslant\mu<\nu\leqslant m} |\alpha_\mu - \alpha_\nu|$$

of these zeros is positive.

Our aim is to find a lower bound for $\Delta(f)$ in terms of

$$\delta(f),\ H(f),\ D(f).$$

To do so, we shall essentially repeat the proof of Theorem 1, but now the second polynomial

$$g(z) = f'(z)$$

will be identified with the derivative of the first, and we shall apply the identity

$$D(f) = (-1)^{\frac{1}{2}m(m-1)} a_0^{m-1} \prod_{\mu=1}^{m} f'(\alpha_\mu). \tag{15}$$

Let again A be chosen such that

$$1 \leqslant |A| \leqslant \sqrt{m+1}, \qquad \min_{1\leqslant\mu\leqslant m} |\alpha_\mu - A| \geqslant 1.$$

Further put

$$f^*(z) = f(z+A),\ g^*(z) = g(z+A) = f'(z+A),\ \alpha_\mu^* = \alpha_\mu - A \quad (\mu = 1, 2, \ldots, m),$$

so that

$$f^*(z) = a_0(z-\alpha_1^*)(z-\alpha_2^*)\ldots(z-\alpha_m^*), \qquad |\alpha_\mu^*| \geqslant 1 \quad (\mu = 1, 2, \ldots, m).$$

Since

$$n = \delta(g) = \delta\left(\frac{df}{dz}\right) = m-1, \qquad H(g) = H\left(\frac{df}{dz}\right) \leqslant mH(f),$$

the inequalities (5) now take the form

$$H(f^*) \leqslant (m+1)(|A|+1)^m H(f), \qquad H(g^*) \leqslant m^2(|A|+1)^{m-1}H(f),$$

and hence the inequalities (9) change into

$$|g^*(\alpha_\mu^*)| \leqslant m^3(|A|+1)^{m-1}|\alpha_\mu^*|^{m-1}H(f) \qquad (\mu = 1, 2, \ldots, m). \tag{16}$$

From the definition,

$$\alpha_\mu^* - \alpha_\nu^* = \alpha_\mu - \alpha_\nu, \text{ hence } D(f^*) = D(f), \quad \Delta(f^*) = \Delta(f),$$

so that, by(15), also

$$D(f) = (-1)^{\frac{1}{2}m(m-1)} a_0^{m-1} \prod_{\mu=1}^{m} g^*(\alpha_\mu^*). \tag{17}$$

Replace here all factors $g^*(\alpha_\mu^*)$ except the one with $\mu = 1$ by their upper bounds (16). It follows then that

$$|D(f)| \leqslant |a_0|^{m-1}|g^*(\alpha_1^*)| \prod_{\mu=2}^{m} \{m^3(|A|+1)^{m-1}|\alpha_\mu^*|^{m-1}H(f)\}. \tag{18}$$

7. From here onwards a slightly different method has to be used. The proof depends on a simple lemma due to C. L. Siegel.

Lemma 2: *Let $F(z)$ be a polynomial of degree M with arbitrary real or complex coefficients, and let ζ be a zero of $F(z)$. If $|\zeta| \geqslant 1$, and $G(z)$ denotes the quotient polynomial $F(z)/(z-\zeta)$, then* [1]

$$H(G) \leqslant MH(F).$$

Proof: Let, in explicit form,

$$F(z) = A_0 + A_1 z + \ldots + A_M z^M, \quad G(z) = B_0 + B_1 z + \ldots + B_{M-1} z^{M-1}.$$

---

[1] The lemma holds without the restriction on ζ, but the weaker assertion suffices for our purpose.

When $|z|$ is sufficiently small,

$$\frac{1}{z-\zeta} = -\left(\frac{1}{\zeta}+\frac{z}{\zeta^2}+\frac{z^2}{\zeta^3}+\dots\right)$$

and hence, identically,

$$G(z) = -\left(\frac{1}{\zeta}+\frac{z}{\zeta^2}+\frac{z^2}{\zeta^3}+\dots\right) F(z).$$

On multiplying out and comparing the coefficients of equal powers of z on both sides, we obtain the equations

$$-B_\mu = \frac{A_0}{\zeta^{\mu+1}}+\frac{A_1}{\zeta^\mu}+\dots+\frac{A_\mu}{\zeta} \qquad (\mu=0, 1, \dots, M-1).$$

Since $|1/\zeta|\leqslant 1$, these show immediately that

$$|B_\mu| \leqslant (\mu+1)H(F) \qquad (\mu=0, 1, \dots, M-1),$$

giving the assertion.

This lemma will now be applied to the polynomial $f^*(z)$. Put

$$h(z)=a_0(z-\alpha_2^*)(z-\alpha_3^*)\dots(z-\alpha_m^*), \quad k(z)=a_0(z-\alpha_3^*)\dots(z-\alpha_m^*),$$

so that

$$h(z)=\frac{f^*(z)}{z-\alpha_1^*}, \quad k(z)=\frac{h(z)}{z-\alpha_2^*}.$$

By Lemma 2,

$$H(h)\leqslant mH(f^*),$$

and a second application of this lemma gives

$$H(k)\leqslant m(m-1)H(f^*)<m^3(|A|+1)^m H(f). \tag{19}$$

Consider now the factor $g^*(\alpha_1^*)$ that was left in the formula (18). On differentiating $f^*(z)$ and putting $z=\alpha_1^*$, evidently

$$g^*(\alpha_1^*)=a_0(\alpha_1^*-\alpha_2^*)(\alpha_1^*-\alpha_3^*)\dots(\alpha_1^*-\alpha_m^*). \tag{20}$$

There is now no loss of generality in assuming that the zeros α_μ had been numbered such that

$$\Delta(f)=|\alpha_1-\alpha_2|=|\alpha_1^*-\alpha_2^*|.$$

The identity (20) implies then that

$$|g^*(\alpha_1^*)|=\Delta(f)|k(\alpha_1^*)|$$

and here, similarly as before,

$$|k(\alpha_1^*)|\leqslant H(k)(1+|\alpha_1^*|+|\alpha_1^*|^2+\dots+|\alpha_1^*|^{m-2})\leqslant(m-1)H(k)|\alpha_1^*|^{m-2}.$$

Since $|\alpha_1^*|\geqslant 1$, we deduce then from (19) that

$$|g^*(\alpha_1^*)|\leqslant\Delta(f)\,.\,m^4(|A|+1)^m|\alpha_1^*|^{m-1}H(f). \tag{21}$$

We finally replace the factor $|g^*(\alpha_1^*)|$ in (18) by this upper bound. This leads to the inequality

$$|D(f)|\leqslant|a_0|^{m-1}\Delta(f)\,m^4(|A|+1)^m|\alpha_1^*|^{m-1}H(f)\prod_{\mu=2}^{m}\{m^3(|A|+1)^{m-1}|\alpha_\mu^*|^{m-1}H(f)\}$$

and hence to the result

$$|D(f)|\leqslant|a_0\alpha_1^*\alpha_2^*\dots\alpha_m^*|^{m-1}\Delta(f)m^{3m+1}(|A|+1)^{m^2-m+1}H(f)^m.$$

Here, just as in § 5,

$$|a_0\alpha_1^*\alpha_2^*\dots\alpha_m^*|\leqslant H(f^*)\leqslant(m+1)(|A|+1)^m H(f),$$

so that

$$|D(f)|\leqslant(m+1)^{m-1}m^{3m+1}(|A|+1)^{2m^2-2m+1}\Delta(f)H(f)^{2m-1}.$$

We can finally again distinguish between the general case when $|A|\leqslant\sqrt{m+1}$, and the special case when all zeros $\alpha_1, \dots, \alpha_m$ are real so that A may be taken to be i. With a slight simplification of the constant we arrive at the following conclusion.

Theorem 2. *Let $f(z)$ be a polynomial with real or complex coefficients, of degree $\delta(f)=m$, of height $H(f)$, and with zeros $\alpha_1, \dots, \alpha_m$. Assume that the discriminant $D(f)$ of $f(z)$ does not vanish, and put*

$$\Delta(f)=\min_{1\leqslant\mu<\nu\leqslant m}|\alpha_\mu-\alpha_\nu|.$$

Denote by $\Gamma(f)$ the constant

$$\Gamma(f)=(m+1)^{4m}4^{m^2}\gamma(f)^{m^2}$$

where $\gamma(f)$ is 1 when all zeros of $f(z)$ are real, and otherwise $\gamma(f)$ has the value $m+1$. Then

$$\Delta(f)\geqslant\{\Gamma(f)H(f)^{2m-1}\}^{-1}|D(f)|.$$

Remark: Assume again that $f(z)$ has rational integral coefficients. The discriminant $D(f)$ is then an integer distinct from zero, hence satisfies $|D(f)|\geqslant 1$. It follows therefore now that

$$|\alpha_1-\alpha_2|\geqslant\{\Gamma(f)H(f)^{2m-1}\}^{-1},$$

where α_1 and α_2 are any two distinct zeros of $f(z)$; i.e., α_1 and α_2 are algebraic conjugates. It follows then that Bombieri's theorem remains valid, even in a slightly strengthened form, when the algebraic numbers are conjugate.

Mathematics Department,
University of Manchester