4. SOME GENERALIZATIONS OF ROTH'S THEOREM

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **17 (1971)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

defined for $d = 3, 4, \ldots$ with $\kappa_0(3) = 1 + \sqrt{3}$ and with $|\kappa_0(d) - \frac{1}{2}d| \leqq c_1$ such that for an algebraic number α of degree d and for $\kappa > \kappa_0(d)$ there is a computable constant $c_2 = c_2(\alpha, \kappa)$ such that the inequality $\left|\alpha - \frac{p}{q}\right| < q^{-\kappa}$ has at most one solution p/q with $(p, q) = 1$ and $q > c_2$. But earlier Schinzel (1967) had pointed out that this is true with $\kappa > 3\sqrt{d/2}$ in place of $\kappa > \kappa_0(d)$. If d is large, then $\kappa_0(d) > 3\sqrt{d/2}$, and hence in this case Schinzel's result is better than Davenport's. Earlier Siegel (1937) and Hyyrö (1964) had shown results of this kind for numbers α of the type $\alpha = \sqrt[d]{(a/b)}$, or rather for the corresponding Thue's equation $ax^d - by^d = m$.

4. Some generalizations of Roth's Theorem

4.1. In this section we shall discuss several generalizations of Roth's Theorem, but not the generalization to simultaneous approximation, which will be taken up in §7.

The *height* $H(\beta)$ of an algebraic number β is defined by $H(\beta) = H(P)$, where P is the defining polynomial of β. Roth (1955b) enunciated and LeVeque ((1955), vol. 2, ch. 4) proved

Theorem 4A. *Let α be algebraic, K an algebraic number field and $\delta > 0$. There are only finitely many elements β of K with*

$$|\alpha - \beta| < H(\beta)^{-2-\delta}. \tag{4.1}$$

Neither α nor K need to be real here. When K is the field **Q** of rationals, then Theorem 4A reduces to Roth's Theorem. Since every number field contains **Q** as a subfield, it follows from Dirichlet's Theorem that the number 2 in the exponent in (4.1) is best possible if α is real.

In fact if α and K are real, then the exponent is best possible in a somewhat less trivial sense: Suppose K is a real or complex number field of degree t and β in K has degree d. Then d is a divisor of t. Define the *field height* $H_K(\beta)$ of β by $H_K(\beta) = H(P^{t/d})$, where P is the defining polynomial of β. One can show (LeVeque (1955), vol. 2, ch. 4.2) that $c_1(K)\, H(\beta)^{t/d} \leqq H_K(\beta) \leqq c_2(K)\, H(\beta)^{t/d}$, and hence Theorem 4A remains true a fortiori if (4.1) is replaced by

$$|\alpha - \beta| < H_K(\beta)^{-2-\delta}. \tag{4.2}$$

One can show that if both α and K are real and if $\alpha \notin K$, then there are infinitely many β in K with

$$(4.3) \qquad | \alpha - \beta | < c_3 (K) H_K (\beta)^{-2} .$$

Thus the exponent on the right hand side of (4.2) is best possible. Now if α is algebraic, then by Theorem 4A and since $H_K (\beta) \geqq c_1 (K) H (\beta)^{t/d}$, the inequality (4.3) can hold for only finitely many elements β of K of degree $d < t$. Hence if α is a real algebraic number and if the field K is real, then there are infinitely many primitive elements β of K (i.e. elements of K of degree t) with (4.3), i.e. with $| \alpha - \beta | < c_3 (K) H (\beta)^{-2}$. Hence Theorem 4A remains best possible if one restricts oneself to primitive elements β of K.

If α is a real or complex number which does not lie in a complex number field K, then there are infinitely many β in K with

$$(4.4) \qquad | \alpha - \beta | < c_4 (K) H_K (\beta)^{-1} .$$

We shall see in §4.4 that the exponent in (4.2) may be improved to $- 1 - \delta$ in this case.

4.2. The field K of Theorem 4A can be enlarged to contain α, and hence there is no loss of generality in this theorem if one assumes that $\alpha \in K$. One could try to give a lower bound for $| \alpha - \beta |$ where both α, β vary in K. In fact I can show (unpublished) that there is a number $c_1 (d, \delta)$ defined for $d = 1, 2, \ldots$ and for $\delta > 0$ such that in every number field K of degree d there are only finitely many pairs of elements α, β with

$$H (\beta) > H (\alpha)^{c_1} \quad \text{and} \quad | \alpha - \beta | < H (\beta)^{-2-\delta} .$$

For example, if $0 < \delta < 1$, one may put $c_1 = e^{c2}$ with $c_2 = d^{10^4 \delta^{-2}}$. This implies the existence of a (non-effective) constant $c_3 = c_3 (K, \delta)$ such that $| \alpha - \beta | > (H (\alpha) H (\beta))^{-2-\delta}$ if either $H (\beta) > H (\alpha)^{c3}$ or if $H (\alpha) > H (\beta)^{c3}$. It is conceivable that there is a $c_4 = c_4 (K, \delta) > 0$ such that

$$| \alpha - \beta | > c_4 (H (\alpha) H (\beta))^{-2-\delta}$$

for any two distinct elements α, β of K.

S. Schanuel (oral communication) also has a version of Theorem 4A in which both α and β are allowed to vary. It should be remarked that the inequalities of this subsection, when both α and β lie in K, would become quite trivial if we had substituted field heights for heights. In fact it is easy to see that

$$|\alpha - \beta| > c_5(K)(H_K(\alpha)\, H_K(\beta))^{-1}$$

if α, β are distinct elements of K.

4.3. A rather different question is that of approximation to an algebraic number α by algebraic numbers β of fixed degree d. Siegel (1921a) already had given some estimates, and using the method of Roth, Ramachandra (1966) had improved these estimates. Wirsing was the first to prove (but published only in (1971)) a result in which the exponent depends on d only, namely the following.

THEOREM 4B. *Suppose α is a real or complex algebraic number and suppose $d \geqq 1$, $\delta > 0$. There are only finitely many (real or complex) algebraic numbers β of degree d with*

$$|\alpha - \beta| < H(\beta)^{-2d-\delta} \tag{4.5}$$

Wirsing's Theorem becomes Roth's Theorem when $d = 1$. As we shall see in §7.5, the exponent $-2d - \delta$ in (4.5) may be replaced by $-d - 1 - \delta$. Nevertheless we shall now discuss the interesting idea underlying Wirsing's proof.

If one attempts to generalize Roth's method to prove Theorem 4B, a difficulty arises in part (b). One has to show that

$$P(\beta_1, \ldots, \beta_m) = 0$$

where P is a polynomial with rational integer coefficients constructed in part (a), and where $\beta_1, \ldots, \beta_m$ are certain algebraic numbers of degree d satisfying (4.5). In general the degree of the field

$$\mathbf{Q}(\beta_1, \ldots, \beta_m)$$

generated by $\beta_1, \ldots, \beta_m$ may be as large as d^m.

Suppose now that this is the case. The number

$$(b_1 \ldots b_m)\, d^{m-1} \mathcal{N}(P(\beta_1, \ldots, \beta_m))\,, \tag{4.6}$$

where $b_1, \ldots, b_m$ are the leading coefficients of the defining polynomials of $\beta_1, \ldots, \beta_m$ and where $\mathcal{N}$ denotes the norm of $\mathbf{Q}(\beta_1, \ldots, \beta_m)$ over $\mathbf{Q}$, is rational. The conjugates of $P(\beta_1, \ldots, \beta_m)$ are $P(\beta_1^{(i_1)}, \ldots, \beta_m^{(i_m)})$ where $1 \leqq i_h \leqq d$ ($h = 1, \ldots, m$) and where $\beta_h = \beta_h^{(1)}, \beta_h^{(2)}, \ldots, \beta_h^{(m)}$ are the distinct conjugates of β_h. Since each number β_h and each of its conjugates occurs at most to the power d^{m-1}, and since $b_h \beta_h^{(i_1)} \ldots \beta_h^{(i_t)}$ is an algebraic integer if $i_1, \ldots, i_t$ are distinct (see Schneider (1957), Hilfssatz 17 or LeVeque (1955), vol. 2, p. 64), the number (4.6) is a rational integer. One can estimate a factor $P(\beta_1^{(i_1)}, \dots, \beta_m^{(i_m)})$ of (4.6) well only if many of the superscripts $i_1, \dots, i_m$ equal 1. Wirsing in his proof used the fact that for most of the d^m factors, about $\frac{m}{d}$ of these superscripts equal 1. This enabled him to show that under suitable conditions the number (4.6) has absolute value less than 1, and hence is zero.

4.4. Let K be a number field of degree t and let $\alpha_1, \dots, \alpha_t$ be arbitrary real or complex algebraic numbers. For $\beta \in K$, Mahler puts

$$f(\beta) = \prod_{j=1}^{t} \min(1, |\alpha_j - \beta^{(j)}|),$$

where $\beta^{(1)}, \dots, \beta^{(t)}$ are the conjugates of β corresponding to the conjugates $\omega^{(1)} = \omega, \dots, \omega^{(t)}$ of a fixed generator (i.e. primitive element) ω of K.

THEOREM 4C (*Mahler* 1963).[1] *Suppose $K, \alpha_1, \dots, \alpha_t, f(\beta)$ are as above, and suppose that $\delta > 0$. There are only finitely many β in K with*

$$f(\beta) < H_K(\beta)^{-2-\delta}.$$

Since $f(\beta) \leqq |\alpha_1 - \beta|$, it is easy to see that Theorem 4C sharpens Theorem 4A. Suppose now that K is complex and that for every β of K, $\beta^{(2)}$ is the complex conjugate $\bar{\beta}$ of β. Also suppose that $\alpha_2 = \bar{\alpha}_1$. By Theorem 4C there are only finitely many β in K with

$$|\alpha_1 - \beta^{(1)}| \, |\alpha_2 - \beta^{(2)}| < H_K(\beta)^{-2-\delta},$$

i.e. with

$$|\alpha_1 - \beta| < H_K(\beta)^{-1-(\delta/2)}.$$

Hence if K is complex, then the exponent $-2-\delta$ in (4.2) may be replaced by $-1-\delta$. It follows that in general if α is a complex (non-real) algebraic number, then the exponent $-2-\delta$ in (4.1) may be replaced by $-1-\delta$. By (4.4) the exponent $-1-\delta$ is best possible in this case.

Suppose β is an element of K of degree d. If b_0 is the leading coefficient of the defining polynomial P of β, then $c_0 = b_0^{t/d}$ is the leading coefficient

[1] See also Mahler (1961), Appendix C, Assertion (2.II).

of the polynomial $P^{t/d}$ used in the definition of $H_K(\beta)$. For every σ in $0 \leqq \sigma \leqq 1$, let $\mathscr{C}(\sigma)$ be the class of β in K with

$$|c_0| \leqq H_K(\beta)^\sigma .$$

Mahler (1963) proved a result which contains Theorem 4C, namely

THEOREM 4D. *Suppose K, $\alpha_1, \ldots, \alpha_t, f(\beta)$, δ are as above, and suppose $0 \leqq \sigma \leqq 1$. There are only finitely many β in $\mathscr{C}(\sigma)$ with*

$$f(\beta) < H_K(\beta)^{-1-\sigma-\delta} .$$

Of particular interest is the case when $\sigma = 0$, because $\mathscr{C}(0)$ consists precisely of the integers of K. Therefore given an algebraic number α, there are only finitely many integers β of K with $|\alpha - \beta| < H_K(\beta)^{-1-\delta}$, and by applying this to K and its subfields it follows that there are only finitely many integers β of K with

$$|\alpha - \beta| < H(\beta)^{-1-\delta} . \tag{4.7}$$

The exponent $-1-\delta$ in (4.7) may be replaced by $-\frac{1}{2}-\delta$ if α is complex.

Mahler also proved some " inhomogeneous " theorems, which are contained in more recent and more general results to be stated in §7.4.

4.5. The first one to recognize the importance of p-adic diophantine approximations was K. Mahler. He developed an extensive theory and in particular he proved (1933a, b) the following

THEOREM 4E (Mahler (1933a). *Suppose $F(x, y)$ is a binary form as in Theorem 2C and suppose $p_1, \ldots, p_r$ are distinct rational primes. There are only finitely many rational integers $x, y, z_1, \ldots, z_r$ with*

$$F(x, y) = p_1^{z1} \ldots p_r^{z_r} .$$

Mahler (1933c) gave an asymptotic formula for the number $N(m)$ of solutions of

$$|F(x, y)|\,|F(x, y)|_{p_1} \cdots |F(x, y)|_{p_r} \leqq m$$

where $|\;|_p$ denotes the p-adic valuation. His results were generalized to algebraic number fields by Parry (1940, 1950). For a sharper version of Theorem 4E see Theorem 5E and the remarks below it. Using Roth's method, Ridout (1957) proved (but see also Schneider (1957), Satz 6) a result which can be formulated as follows.

THEOREM 4F. *Let α be a real algebraic number distinct from zero and let $p_1, \ldots, p_r, q_1, \ldots, q_r$ be distinct rational primes. Suppose $\delta > 0$. There are only finitely many rationals p/q* with

$$p = p_1^{a_1} \ldots p_r^{a_r} p', \quad q = q_1^{b_1} \ldots q_s^{b_s} q'$$

where $a_1, \ldots, a_r, b_1, \ldots, b_s$ are non-negative integers and where p', q' are non-zero integers such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{| p' q' | \cdot | pq |^{\delta}} . \tag{4.8}$$

The case $p' = q' = 1$ of this theorem is due to Mahler (1936). In this paper Mahler also proved a weaker version of Theorem 4F, of the type of Schneider's Theorem mentioned in §2.4. For a rather better recent estimate in this case see Theorem 5B. Bounds for the number of solutions of inequalities of the type (4.8) were given by Fraenkel (1962). More general versions of Theorem 4F were given by Stepanov (1967) and Walliser (1969).

Now let α be a real algebraic irrational. Recall that the convergents p_n/q_n to α satisfy $| \alpha - p_n/q_n | < q_n^{-2}$. It follows from Mahler's (1936) result that the greatest prime factor of $p_n q_n$ tends to infinity, and it follows from Theorem 4F that in fact the greatest prime factor of p_n as well as that of q_n tends to infinity.

Let $K = \mathbf{Q}(\omega)$ be a number field of degree t. We shall recall some well known facts about valuations of K. Suppose that $t = r + 2s$ and that $\omega^{(1)}, \ldots, \omega^{(r)}$ are real and $\omega^{(r+1)}, \ldots, \omega^{(r+s)}, \omega^{(r+s+1)}, \ldots, \omega^{(t)}$ are complex with $\omega^{(r+s+j)}$ the complex conjugate of $\omega^{(r+j)}$ $(j = 1, \ldots, s)$. Let Ω be the set consisting of the integers $1, 2, \ldots, r + s$ and of the prime ideals of the ring of integers of K. If $v \in \Omega$, $1 \leqq v \leqq r + s$ and if $\alpha \in K$, then we put $| \alpha |_v = | \alpha^{(v)} |$ where $| \;|$ denotes the ordinary absolute value. Now suppose v is a prime ideal $\mathfrak{p}$. The norm $\mathcal{N}(\mathfrak{p})$ equals $p^{N_\mathfrak{p}}$ where p is a rational prime and where $N_\mathfrak{p}$ is a positive rational integer. If $\alpha \in K$, $\alpha \neq 0$, then the fractional ideal (α) may uniquely be written $(\alpha) = \mathfrak{p}^a \mathfrak{p}_2^{a_2} \ldots \mathfrak{p}_k^{a_k}$ where $a, a_2, \ldots, a_k$ are rational integers and where $\mathfrak{p}, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ are distinct prime ideals. We now put $| \alpha |_v = p^{-a}$ and we put $| 0 |_v = 0$. It is clear that $| \alpha\beta |_v = | \alpha |_v \, | \beta |_v$ and that if $\alpha \neq 0$, then $| \alpha |_v = 1$ for all but finitely many $v \in \Omega$. The mappings $\alpha \rightarrow | \alpha |_v$ where $v \in \Omega$ are all the inequivalent valuations of K, and the Archimedean valuations are those where $v = 1, 2, \ldots, r + s$. For every $v \in \Omega$, there is a completion K_v of K with respect to $| \;|_v$.

Put $N_v = 1$ or $N_v = 2$ if $1 \leqq v \leqq r$ or if $r + 1 \leqq v \leqq r + s$, respectively; N_v was defined above when v is a prime ideal. Put $\| \alpha \|_v = | \alpha |_v^{N_v}$. It is clear that the definition of $| \alpha |_v$ and of $\| \alpha \|_v$ can be extended to $\alpha \in K_v$. The product formula

$$\prod_{v \in \Omega} \| \alpha \|_v = 1$$

holds for every non-zero α in K. One can show that

$$c_1 (K) H_K (\beta) \leqq \prod_{v \in \Omega} \max (1, \| \beta \|_v) \leqq c_2 (K) H_K (\beta) . \tag{4.9}$$

Theorem 4G. *Let S be a finite subset of Ω. For each $v \in S$, let α_v be an element of K_v which is algebraic over K. For $\beta \in K$ put*

$$g (\beta) = \prod_{v \in S} \min (1, \| \alpha_v - \beta \|_v) .$$

Then for every $\delta > 0$ there are only finitely many $\beta \in K$ with

$$g (\beta) < H_K (\beta)^{-2-\delta} .$$

A more general version of this theorem may be found in Mahler ((1961), Appendix C, Assertion (2,I)). See also Lang ((1962), ch. 6). In its present form Theorem 4G does not contain Theorem 4F, but Mahler's generalization of it does. The case of Theorem 4G when K is the field of rationals is due to Ridout (1958). It may be seen that Mahler's Theorem 4C is equivalent with the case of Theorem 4G when $S = \{1, 2, ..., r + s\}$, i.e. when we are considering only Archimedean valuations. Lang and Ridout also gave p-adic versions of Theorem 2C and thus sharpened Theorem 4E. Like Roth's Theorem, the results discussed here do not permit to give an estimate for the " size " (say $H (\beta)$) of the solutions, and hence they are non-effective. For weaker but effective p-adic results see Theorem 5B, 5D and 5E. For an effective weaker version of Theorem 4G see Sprindžuk (1970b, 1971a).

5. Effective methods. Baker's Theorem

5.1. All the results obtained by the method of Thue, Siegel and Roth share the disadvantage that they are non-effective. Although they show that certain inequalities and equations have only finitely many integer solutions, they do not give bounds for the size of the solutions and hence give no method to compute all the solutions.