7. SIMULTANEOUS APPROXIMATION TO ALGEBRAIC NUMBERS BY RATIONALS

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Inequalities as above in which β is an algebraic *integer* are more difficult. Here one has to deal with polynomials $x^d + q_{d-1} x^{d-1} + \dots + q_1 x + q_0$, and hence one has to deal with an inhomogeneous approximation problem. One might conjecture that if $d \geqq 2$ and if α is not an algebraic integer of degree d and is not algebraic of degree $\leqq d - 1$, then for every $\varepsilon > 0$ there are infinitely many real algebraic integers β of degree $\leqq d$ with

$$(6.11) \qquad | \alpha - \beta | < H(\beta)^{-(d-\varepsilon)} .$$

This conjecture is true if $(\alpha, \alpha^2, \dots, \alpha^{d-1})$ is not very well approximable. Davenport and Schmidt (1969) showed a result with (6.11) replaced by

$$| \alpha - \beta | \leqq c_9 H(\beta)^{-[(d+1)/2]} .$$

6.7. We have discussed approximation properties of general l-tuples $\alpha_1, \dots, \alpha_l$ and of l-tuples $\alpha, \alpha^2, \dots, \alpha^l$. Interesting questions arise if one asks about approximation properties of special l-tuples. For example, $(e, e^2, \dots, e^l)$ is not very well approximable (Popken (1929); see Schneider (1957), Kap. 4). A more general result (which is analogous to Theorem 7A below) concerning the l-tuple $\alpha_1 = e^{r_1}, \dots, \alpha_l = e^{r_l}$ with distinct non-zero rationals $r_1, \dots, r_l$ was proved by Baker (1965). For the behavior of l-tuples $\log \alpha_1, \dots, \log \alpha_l$ where $\alpha_1, \dots, \alpha_l$ are algebraic, see Baker (1966, 1967b, 1967c, 1968a) and Feldman (1968a, 1968b). In the next section we shall turn to l-tuples of real algebraic numbers.

7. Simultaneous approximation to algebraic numbers by rationals

7.1. We have already seen (Theorem 6F) that $(\alpha_1, \dots, \alpha_l)$ is badly approximable if $1, \alpha_1, \dots, \alpha_l$ is a basis of a real algebraic number field. In the same way one can show that if $1, \alpha_1, \dots, \alpha_l$ are linearly independent over the field of rationals and if they generate a field of degree d, then

$$| \alpha_1 q_1 + \dots + \alpha_l q_l + p | \geqq c_1 | \mathbf{q} |^{-d+1}$$

for every non-zero integer point $\mathbf{q} = (q_1, \dots, q_l, p)$. Here $c_1 = c_1(\alpha_1, \dots, \alpha_l) > 0$ is easily computable. The case $l = 1$ of this inequality yields Liouville's Theorem 2A.

Cassels and Swinnerton-Dyer (1955) have shown that Littlewood's conjecture is true for l-tuples $(\alpha_1, \dots, \alpha_l)$ such that $1, \alpha_1, \dots, \alpha_l$ is a basis of a real number field. (This conjecture applies only if $l > 1$.) Peck (1961) showed for such l-tuples with $l > 1$ that there are infinitely many rational l-tuples $\left(\frac{p_1}{q}, \dots, \frac{p_l}{q}\right)$ with

$$\left| \alpha_1 - \frac{p_1}{q} \right| < c_2 q^{-1-(1/l)},$$

$$\left| \alpha_i - \frac{p_i}{q} \right| < c_2 q^{-1-(1/l)} (\log q)^{-1/(l-1)} \qquad (i=2, \dots, l).$$

Schmidt (1966) derived an asymptotic formula for the number $\nu(N)$ of solutions with $q \leqq N$ of $\left| \alpha_i - \frac{p_i}{q} \right| < \psi(q)$ $(i=1, \dots, l)$ for such l-tuples and for certain functions $\psi(q)$. Earlier Lang (1965b, 1965c, 1966a) had done this for $l = 1$ and for a wider class of numbers α_1. Adams (1967) replaced our special l-tuples by badly approximable l-tuples and proved (1969a, 1969b, to appear) other results of this type.

7.2. As in §6.3, $\| \xi \|$ will denote the distance from a real number ξ to the nearest integer.

THEOREM 7A. *Suppose $\alpha_1, \dots, \alpha_l$ are real algebraic numbers such that $1, \alpha_1, \dots, \alpha_l$ are linearly independent over the rationals, and suppose $\delta > 0$. There are only finitely many positive integers q with*

$$q^{1+\delta} \| \alpha_1 q \| \dots \| \alpha_l q \| < 1 . \tag{7.1}$$

The inequalities

$$\left| \alpha_i - \frac{p_i}{q} \right| < q^{-1-(1/l)-\delta} \qquad (i=1, \dots, l) \tag{7.2}$$

imply that $\| \alpha_i q \| < q^{-(1/l)-\delta}$ $(i=1, \dots, l)$ and hence they imply (7.1). Therefore (7.2) has only finitely many solutions, and we obtain

COROLLARY 7B. *Suppose $\alpha_1, \dots, \alpha_l$ and δ are as in Theorem 7A. Then there are only finitely many rational l-tuples $\left(\frac{p_1}{q}, \dots, \frac{p_l}{q}\right)$ with* (7.2).

THEOREM 7C. *Again assume that $\alpha_1, \dots, \alpha_l$ and δ are as in Theorem* 7A. *Then there are only finitely many l-tuples of non-zero integers $q_1, \dots, q_l$ with*

(7.3) $$| q_1 q_2 \dots q_l |^{1+\delta} \| \alpha_1 q_1 + \dots + \alpha_l q_l \| < 1 .$$

By applying Theorem 7C to all the non-empty subsets of $\alpha_1, \dots, \alpha_l$ one deduces

COROLLARY 7D. *If again $\alpha_1, \dots, \alpha_l$; δ are as in Theorem 7A, then there are only finitely many $(l+1)$-tuples of integers $q_1, \dots, q_l, p$ with $q = \max(|q_1|, \dots, |q_l|) > 0$ and with*

(7.4) $$| \alpha_1 q_1 + \dots + \alpha_l q_l + p | < q^{-l-\delta} .$$

By Corollaries 6B and 6D the exponents in Corollaries 7B and 7D are best possible. In view of Khintchine's Transference Principle (Theorem 6E), the Corollaries 7B and 7D say the same, namely that $\alpha_1, \dots, \alpha_l$ is not very well approximable. The case $l = 1$ of these corollaries is Roth's Theorem. Theorems 7A and 7C and their corollaries were proved by Schmidt (1970). They had been anticipated by a weaker version of the case $l = 2$ and by the case $l = 2$ itself (Schmidt 1965 and 1967a, respectively).

Before Roth's Theorem was known Hasse (1939) used Siegel's method to derive estimates for simultaneous approximation. Baker (1967a), Feldman (1970a) and Osgood (1970) proved weaker but effective versions of Corollary 7D for special algebraic numbers $\alpha_1, \dots, \alpha_l$.

7.3. Corollary 7B shows that the exponent in Corollary 6B is best possible for algebraic numbers $\alpha_1, \dots, \alpha_l$, and Corollary 7D does the same for Corollary 6D. We shall now examine Corollaries 6J and 6K in the special case when the coefficients of the linear forms involved are algebraic. Suppose $1 \leqq m < n$ and $L_1(\mathbf{x}), \dots, L_m(\mathbf{x})$ are linear forms with real algebraic coefficients. We shall call $L_1, \dots, L_m$ a *Roth System* if for every $\delta > 0$ the inequalities

(7.5) $$| L_i(\mathbf{x}) | < | \mathbf{x} |^{-((n-m)/m)-\delta} \qquad (i = 1, \dots, m)$$

have only finitely many solutions in integer points $\mathbf{x} \neq \mathbf{0}$. Roth's Theorem says that for $n = 2$, $m = 1$, the linear form $L(\mathbf{x}) = \alpha x_1 - x_2$ with a real algebraic irrational α is a Roth System.

THEOREM 7E (Schmidt (1971a)). *Linear forms $L_1(\mathbf{x}), \dots, L_m(\mathbf{x})$ with real algebraic coefficients and with $m < n$ are a Roth System if and only if their restrictions to every rational subspace S^d of dimension d with $1 \leqq d \leqq n$ have rank r satisfying*

(7.6) $$r \geqq dm/n\,.$$

This theorem contains Corollaries 7B and 7D. For suppose $m = 1$, $n = l + 1$ and $L(\mathbf{x}) = L_1(\mathbf{x}) = \alpha_1 x_1 + \ldots + \alpha_l x_l + x_n$ where the numbers $\alpha_1, \ldots, \alpha_l$, 1 are algebraic and linearly independent over the rationals. Then $L(\mathbf{x}) \neq 0$ for every integer point $\mathbf{x} \neq \mathbf{0}$, and hence L has rank $r = 1$ on every rational subspace $S^d \neq \mathbf{0}$. Since $dm/n = d/n \leqq 1$, the inequality (7.6) is always satisfied, and $L(\mathbf{x})$ is a Roth System. Hence there are only finitely many integer points $\mathbf{x} \neq \mathbf{0}$ with $|L(\mathbf{x})| < |\mathbf{x}|^{-(n-1)-\delta} = |\mathbf{x}|^{-l-\delta}$, and Corollary 7D follows. Corollary 7B can be similarly derived.

The necessity of the condition (7.6) in Theorem 7E is easy to see: A rational subspace S^d is a d-dimensional Euclidean space, and the integer points in such a space form a lattice Λ. By applying a result analogous to Corollary 6J to the restrictions of $L_1, \ldots, L_m$ to S^d and to the lattice Λ, we obtain infinitely many integer points $\mathbf{x} \neq \mathbf{0}$ in S^d with

$$|L_i(\mathbf{x})| \leqq c_1 |\mathbf{x}|^{-(d-r)/r} = c_1 |\mathbf{x}|^{1-(d/r)} \qquad (i = 1, \ldots, m)\,.$$

Now if $r < dm/n$, say if $r = dmn^{-1}(1+\delta)^{-1}$, then

$$|L_i(\mathbf{x})| \leqq c_1 |\mathbf{x}|^{1-(n/m)(1+\delta)} \leqq c_1 |\mathbf{x}|^{-((n-m)/m)-\delta} \qquad (i = 1, \ldots, m)\,,$$

and we don't have a Roth System.

Suppose $L_1(\mathbf{x}), \ldots, L_n(\mathbf{x})$ are linear forms with real algebraic coefficients and suppose $\gamma_1, \ldots, \gamma_n$ are reals with $\gamma_1 + \ldots + \gamma_n = 0$. In view of Corollary 6K the following definition is natural. We shall call $(L_1, \ldots, L_n; \gamma_1, \ldots, \gamma_n)$ a *General Roth System* if for every $\delta > 0$ there is a $Q_0 = Q_0(L_1, \ldots, L_n; \gamma_1, \ldots, \gamma_n; \delta)$ such that for $Q > Q_0$ there is no integer point $\mathbf{x} \neq \mathbf{0}$ with

$$|L_i(\mathbf{x})| < Q^{\gamma_i - \delta} \qquad (i = 1, \ldots, n)\,.$$

Roth's Theorem says that for $n = 2$ and an algebraic irrational α, the system $(L_1(\mathbf{x}) = \alpha x_1 - x_2, L_2(\mathbf{x}) = x_1; \gamma_1 = -1, \gamma_2 = 1)$ is a General Roth System. Schmidt (1971a) derives necessary and sufficient conditions for General Roth Systems which contain Theorem 7E as a special case.

7.4. We shall briefly discuss an inhomogeneous approximation problem. Suppose $l > 1$ and suppose $1, \alpha_1, \ldots, \alpha_l$ are algebraic and linearly independent over the rational field $\mathbf{Q}$. The special case $q_l = 1$ of Theorem 7C shows that there are only finitely many integer l-tuples $q_1, \ldots, q_{l-1}, p$ with $q = \max(|q_1|, \ldots, |q_{l-1}|) > 0$ and with

$$|\alpha_1 q_1 + \ldots + \alpha_{l-1} q_{l-1} + p + \alpha_l| < q^{-(l-1)-\delta}\,.$$

One can easily show that more generally this is still true if α_l is not of the type $\alpha_l = \alpha_1 x_1 + \ldots + \alpha_{l-1} x_{l-1} + x_0$ with rational integers $x_0, x_1, \ldots, x_{l-1}$. Changing the notation we obtain

COROLLARY 7F. *Suppose $\alpha_1, \ldots, \alpha_l, \beta$ are real algebraic numbers such that β is not a linear combination of $\alpha_1, \ldots, \alpha_l$ with rational integer coefficients. Then for every $\delta > 0$ there are only finitely many integer l-tuples $q_1, \ldots, q_l$ with $q = \max(|q_1|, \ldots, |q_l|) > 0$ and with*

$$| \alpha_1 q_1 + \ldots + \alpha_l q_l + \beta | < q^{-(l-1)-\delta} .$$

This holds also when $l = 1$, but is trivial in this case. The case when $l = 2$ and α_1/α_2 is quadratic was proved by Mahler (1963). Combining Corollary 7D with certain transference theorems (see, e.g., Cassels (1957), ch. V) one obtains

COROLLARY 7G. *Suppose $\alpha_1, \ldots, \alpha_l$ are real, algebraic and linearly independent over* $\mathbf{Q}$. *Then for every real β and every $\varepsilon > 0$ there are infinitely many integer l-tuples $(q_1, \ldots, q_l)$ with $q = \max(|q_1|, \ldots, |q_l|) > 0$ and*

$$| \alpha_1 q_1 + \ldots + \alpha_l q_l + \beta | < q^{-(l-1-\varepsilon)} .$$

7.5. Suppose α is a real algebraic number. Assume at first that it is not algebraic of degree $\leqq d$ where d is a given positive integer. Then $1, \alpha, \ldots, \alpha^d$ are linearly independent over the rationals, and by Corollary 7D there are only finitely many integer solutions of

$$| q_d \alpha^d + \ldots + q_1 \alpha + q_0 | < q^{-d-\delta} \; (q = \max(|q_1|, \ldots, |q_d|) > 0)$$

for any given $\delta > 0$. Thus there are only finitely many polynomials $P(x)$ of degree at most d with rational integer coefficients and with

$$| P(\alpha) | < H(P)^{-d-\delta} .$$

Now if β is a root of $P(x)$ and if, say, $P(x) = a(x-\beta)(x-\beta_2) \ldots (x-\beta_e)$, then $|P(\alpha)| = |\alpha - \beta| \, |a(\alpha-\beta_2) \ldots (\alpha-\beta_e)| \leqq |\alpha - \beta| (|\alpha|+1)^{e-1} c_1 H(P)$ by the well known inequality $|a| (1+|\beta|)(1+|\beta_2|) \ldots (1+|\beta_e|) \leqq c_1 H(P)$ where $c_1 = c_1(e)$. (See e.g. LeVeque (1955), vol. 2, Theorem 4.2.) Thus $|\alpha - \beta| < H(P)^{-d-1-\delta}$ would imply that $|P(\alpha)| < c_2 H(P)^{-d-\delta}$, which has only finitely many solutions. Thus we see that the inequality

$$(7.7) \qquad | \alpha - \beta | < H(\beta)^{-d-1-\delta}$$

has for every $\delta > 0$ only finitely many solutions in algebraic numbers β of degree $\leqq d$. It can be shown that the assumption on the degree of α can be removed, and we obtain

THEOREM 7H. *Suppose α is a real algebraic number, d a positive integer, $\delta > 0$. There are only finitely many (real or complex) algebraic numbers β of degree at most d with* (7.7).

This supersedes Wirsing's Theorem 4B. Suppose α is real and algebraic but not algebraic of degree $\leqq d$. Then by Corollary 7D the d-tuple $(\alpha, \alpha^2, \ldots, \alpha^d)$ is not very well approximable. Using a result of Wirsing (1961) mentioned in §6.6, we obtain a theorem which complements Theorem 7H.

THEOREM 7I. *Suppose α is algebraic of some degree greater than d. Then for every $\varepsilon > 0$ there are infinitely many real algebraic numbers β of degree $\leqq d$ with* (6.10), *i.e. with*

$$|\alpha - \beta| < H(\beta)^{-d-1+\varepsilon}.$$

In order to obtain results about approximation by algebraic *integers* β, one has to apply Corollary 7F with $l = d$ and $\alpha_1 = 1, \alpha_2 = \alpha, \ldots, \alpha_{d-1} = \alpha^{d-2}, \alpha_d = \alpha^{d-1}, \beta = \alpha^d$.

THEOREM 7J. *Suppose α, d, δ are as in Theorem* 7H. *There are only finitely many (real or complex) algebraic integers β of degree at most d with*

$$|\alpha - \beta| < H(\beta)^{-d-\delta}.$$

Using certain transference principles (see Davenport and Schmidt (1969)) together with the results of this section one can prove

THEOREM 7K. *Suppose $d \geqq 2$ and α is a real algebraic number of some degree $\geqq d$ but is not an algebraic integer of degree d. Then for every $\varepsilon > 0$ there are infinitely many real algebraic integers β of degree $\leqq d$ with*

$$|\alpha - \beta| < H(\beta)^{-d+\varepsilon}.$$

7.6. In the course of his classification of algebraic and transcendental real numbers, Mahler (1932) defines $\omega_d = \omega_d(\alpha)$ as the supremum of the numbers ω such that there are infinitely many polynomials P with rational integer coefficients of degree $\leqq d$ and with

$$0 < |P(\alpha)| < H(P)^{-\omega}.$$

By Corollary 6D it is clear that $\omega_d \geqq d$ unless α is algebraic of degree $\leqq d$. Furthermore if α is algebraic of degree n, then one can show using the norm of $P(\alpha)$ that $\omega_d \leqq n-1$ $(d=1, 2, \ldots)$. Thus Mahler could characterize the algebraic numbers α by the property that $\omega_d(\alpha)$ $(d=1, 2, \ldots)$ remains bounded.

Koksma (1939) defines $\omega_d^* = \omega_d^*(\alpha)$ as the supremum of the numbers ω^* such that there are infinitely many algebraic numbers β of degree $\leqq d$ with

$$|\alpha - \beta| < H(\beta)^{-1-\omega^*}.$$

It is easy to see that $\omega_d^* \leqq \omega_d$ and Wirsing (1961) showed that $\omega_d^* \geqq \frac{1}{2}(\omega_d + 1)$ if α is transcendental. Hence the algebraic numbers can also be characterized by the property that $\omega_d^*(\alpha)$ $(d=1, 2, \ldots)$ is bounded. We have $\omega_d^* \leqq \omega_d \leqq n-1$ if α is algebraic of degree n, and the results of the last section show that $\omega_d^* = d$ if $d \leqq n-1$. Since ω_d^* and ω_d increase with d, we have for algebraic α of degree n,

$$\omega_d = \omega_d^* = \begin{cases} d & \text{if } d \leqq n-1 \\ n-1 & \text{if } d \geqq n. \end{cases}$$

Thus the exponent in Theorem 7H is best possible precisely if $d < n$.

Another characterization of algebraic numbers by approximation properties was given by Gelfond (1952, §III.4, Lemma VII) and refined by Lang (1965a) and Tijdeman (1971, Lemma 6). This lemma was slightly improved by D. Brownawell (unpublished).

8. Tools from the Geometry of Numbers

8.1. To prove the theorems enunciated in the last section one needs certain results from the Geometry of Numbers. This field was first investigated under this name by Minkowski (1896). Other books on the Geometry of Numbers are Cassels (1959) and Lekkerkerker (1969).

Let K be a symmetric [1]) convex set in Euclidean E^n. For convenience let us assume that K is compact and has a non-empty interior. For $\lambda > 0$ let λK be the set consisting of the points $\lambda \mathbf{x}$ with $\mathbf{x} \in K$. Minkowski defines

[1]) I.e. if $\mathbf{x} \in K$, then also $-\mathbf{x} \in K$.