6. Simultaneous approximation to real numbers by rationals

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

and

$$\sigma = \frac{(\alpha^{(k)} - \alpha^{(j)})\,\beta^{(l)}}{(\alpha^{(j)} - \alpha^{(l)})\,\beta^{(k)}}\,.$$

Now $|\beta| = |\beta^{(1)}|$ is small by hypothesis, and it is clear that there is a conjugate $\beta^{(k)}$ with $|\beta^{(k)}| \geqq c_0(\alpha)|q|$. We now put $l = 1$ and pick j distinct from k, l. The quotient $|\beta^{(l)}/\beta^{(k)}|$ and hence $|\sigma|$ is then small. Therefore the left hand side of (5.6) will be small and

$$|\, b_1 \log \alpha_1 + \dots + b_r \log \alpha_r - \log \alpha_{r+1} - k\pi i\,|$$

will be small for some integer k. Since $\pi i = \log(-1)$, this expression is of the type (5.5). One can choose the associate γ of β such that all the quotients $|\gamma^{(k)}/\gamma^{(j)}|$ $(1 \leqq k, j \leqq d)$ are bounded independently of p, q, and hence α_{r+1} as well as $\alpha_1, \dots, \alpha_r$ and their conjugates are bounded. Substituting explicit values for the estimates and using his lower bounds for (5.5), Baker obtains a contradiction if $\beta = q\alpha - p$ is too small, and thereby he proves Theorem 5A.

A more quantitative discussion of this argument as it applies in the proof of Theorem 5C is given by Baker (1971). There is an anticipation of the argument at the end of Gelfond's (1952) book. Gelfond dealt with certain cubic Thue equations $F(x, y) = 1$ and pointed out that a lower bound for (5.5) (which then was not known) would provide upper bounds for the size of solutions of these equations.

6. Simultaneous approximation to real numbers by rationals

6.1. In this section we shall provide the background for the more special problem of simultaneous approximation to real algebraic numbers, which will be discussed in §7. Using the same general principles that were used in the proof of Theorem 1A and its corollary, Dirichlet (1842) proved the following two theorems and their corollaries.

Theorem 6A. *Let $\alpha_1, \dots, \alpha_l$ be real numbers and suppose Q is an integer greater than* 1. *Then there exist integers $q, p_1, \dots, p_l$ with*

(6.1) $\quad 1 \leqq q < Q^l \quad$ *and* $\quad |\alpha_i q - p_i| \leqq Q^{-1} \quad (i = 1, \dots, l)\,.$

COROLLARY 6B. *Suppose at least one of* $\alpha_1, \dots, \alpha_l$ *is irrational. Then there are infinitely many rational l-tuples* $(p_1/q, \dots, p_l/q)$ *with* $q > 0$ *and* $(q, p_1, \dots, p_l)$ [1] $= 1$ *and such that*

$$\left| \alpha_i - \frac{p_i}{q} \right| < q^{-1-(1/l)} \qquad (i = 1, \dots, l). \tag{6.2}$$

The restriction in Theorem 6A that Q is an integer can be removed by using a slightly different proof. Essentially the theorem says that if $\alpha_0, \alpha_1, \dots, \alpha_l$ are real numbers, not all zero, then there exist non-zero integer $(l+1)$-tuples $(q, p_1, \dots, p_l)$ which are fairly proportional to $(\alpha_0, \alpha_1, \dots, \alpha_l)$. Put differently, it says that if $(\alpha_0, \alpha_1, \dots, \alpha_l)$ is a non-zero vector in $(l+1)$-dimensional space, then there are non-zero integer vectors in that space whose direction is fairly close to that of $(\alpha_0, \alpha_1, \dots, \alpha_l)$.

THEOREM 6C. *Suppose* $\alpha_1, \dots, \alpha_l$ *and* Q *are as in Theorem* 6A. *Then there exist integers* $q_1, \dots, q_l, p$ *with*

$$\begin{aligned} &1 \leqq \max(|q_1|, \dots, |q_l|) < Q^{1/l} \quad \textit{and} \\ &|\alpha_1 q_1 + \dots + \alpha_l q_l + p| \leqq Q^{-1}. \end{aligned} \tag{6.3}$$

COROLLARY 6D. *Suppose* $1, \alpha_1, \dots, \alpha_l$ *are linearly independent over the rationals. Then there are infinitely many* $(l+1)$*-tuples of coprime integers* $q_1, \dots, q_l, p$ *with* $q = \max(|q_1|, \dots, |q_l|) > 0$ *and with*

$$|\alpha_1 q_1 + \dots + \alpha_l q_l + p| < q^{-l}. \tag{6.4}$$

Again the restriction in Theorem 6C that Q is an integer can be removed. A geometric interpretation is that if we have a hyperplane in $(l+1)$-dimensional space defined by an equation $\alpha_0 x_0 + \alpha_1 x_1 + \dots + \alpha_l x_l = 0$, then there are integer points $(p, q_1, \dots, q_l)$ which almost satisfy this equation and which therefore in some sense are fairly close to the hyperplane.

6.2. Let us say that $(\alpha_1, \dots, \alpha_l)$ is *badly approximable of the first type* if Corollary 6B cannot be improved by an arbitrary factor, i.e. if there is a constant $c = c(\alpha_1, \dots, \alpha_l) > 0$ such that

$$\max\left(\left|\alpha_1 - \frac{p_1}{q}\right|, \dots, \left|\alpha_l - \frac{p_l}{q}\right|\right) > cq^{-1-(1/l)}$$

[1] I.e. the greatest common divisor of $q, p_1, \dots, p_l$.

for every rational l-tuple $(p_1/q, \ldots, p_l/q)$. Let us say that $(\alpha_1, \ldots, \alpha_l)$ is *very well approximable of the first type* if the exponent in Corollary 6B can be improved, i.e. if there is a $\delta = \delta(\alpha_1, \ldots, \alpha_l) > 0$ such that the system of inequalities

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

has infinitely many solutions $(p_1/q, \ldots, p_l/q)$. Similarly we shall say that $(\alpha_1, \ldots, \alpha_l)$ is *badly approximable of the second type* if there is a $c' = c'(\alpha_1, \ldots, \alpha_l) > 0$ such that

$$| \alpha_1 q_1 + \ldots + \alpha_l q_l + p | > c' q^{-l}$$

for any integers $q_1, \ldots, q_l, p$ with $q = \max(|q_1|, \ldots, |q_l|) > 0$, and that it is *very well approximable of the second type* if there is a $\delta' = \delta'(\alpha_1, \ldots, \alpha_l) > 0$ such that the inequality

$$| \alpha_1 q_1 + \ldots + \alpha_l q_l + p | < q^{-l-\delta'}$$

has infinitely many solutions.

Theorems 6A and 6C and their corollaries are usually considered *dual* to each other, and usually if one has a refinement of one of them one can prove a refinement of the other. In fact Khintchine (1925, 1926a) proved a *transference principle* which contains the following theorem as a special case.

THEOREM 6E. *An l-tuple $(\alpha_1, \ldots, \alpha_l)$ is badly approximable of the first type if and only if it is badly approximable of the second type. It is very well approximable of the first type precisely if it is very well approximable of the second type.*

The first of the four assertions of this theorem had earlier been proved by Perron (1921). In view of the theorem we may speak of *badly approximable* and of *very well approximable* l-tuples.

6.3. Now suppose that $\alpha_1, \ldots, \alpha_l$ are real algebraic numbers and that $1, \alpha_1, \ldots, \alpha_l$ is a basis of a number field K of degree $n = l + 1$. There is a rational integer $a > 0$ such that $a\alpha_1, \ldots, a\alpha_l$ are algebraic integers, and hence for any rational integers $q_1, \ldots, q_l, p$ which are not all zero, the norm

$$\mathcal{N}(a(\alpha_1 q_1 + \ldots + \alpha_l q_l + p))$$

is a non-zero rational integer and hence has absolute value at least 1. The conjugate factors $\alpha_1^{(i)} q_1 + \ldots + \alpha_l^{(i)} q_l + p$ have absolute values $\leqq c_1 \max(|q_1|. \ldots, |q_l|, |p|)$, and this implies that

$$|\alpha_1 q_1 + \ldots + \alpha_l q_l + p| \geqq c_2 (\max(|q_1|, \ldots, |q_l|, |p|))^{-l}.$$

Now if $|\alpha_1 q_1 + \ldots + \alpha_l q_l + p|$ is small, then $q = \max(|q_1|, \ldots, |q_l|) \geqq c_3 \max(|q_1|, \ldots, |q_l|, |p|)$, and we get $|\alpha_1 q_1 + \ldots + \alpha_l q_l + p| \geqq c_4 q^{-l}$. Thus we have

THEOREM 6F. *l-tuples* $(\alpha_1, \ldots, \alpha_l)$ *such that* $1, \alpha_1, \ldots, \alpha_l$ *is a basis of a real number field, are badly approximable.*

In particular badly approximable l-tuples exist, and Corollaries 6B and 6D can be improved at most by constant factors. In fact they can be improved by respective factors $c_5(l) < 1$, $c_6(l) < 1$, but the best value for these factors is known only when $l = 1$, when $c_5(l) = c_6(l) = \frac{1}{\sqrt{5}}$ by Theorem 1C. It is possible but there is no strong evidence that the extreme cases are attained by the l-tuples of Theorem 6F, and that therefore the optimal values of $c_5(l)$, $c_6(l)$ are algebraic of degree $l + 1$. The latest information on $c_5(l)$, $c_6(l)$ may be found in Cassels (1955) and the references given there.

The following " metrical " theorem is a consequence of a more general theorem of Khintchine (1926b).

THEOREM 6G. *Almost no l-tuple* $(\alpha_1, \ldots, \alpha_l)$ *(in the sense of Lebesgue measure) is either badly approximable or very well approximable.*

We saw that Corollary 6B cannot be improved by more than a constant factor. Combining the inequalities (6.2) we obtain

$$|\alpha_1 - (p_1/q)| \ldots |\alpha_l - (p_l/q)| < q^{-l-1}$$

or

$$|q| \cdot |\alpha_1 q - p_1| \ldots |\alpha_l q - p_l| < 1,$$

and therefore

$$|q| \cdot \|\alpha_1 q\| \ldots \|\alpha_l q\| < 1, \tag{6.5}$$

where $\| \xi \|$ denotes the distance from a real number ξ to the nearest integer. It is possible that (6.5) can be improved by more than a constant factor if $l > 1$. This is in fact a famous conjecture of Littlewood, which is usually stated in the form that for $l > 1$ and arbitrary real numbers $\alpha_1, ..., \alpha_l$,

$$\liminf_{q \to \infty} q \, \| \alpha_1 q \| \dots \| \alpha_l q \| = 0 .$$

6.4. Dirichlet's principle in the proof of Theorems 6A, 6C may be replaced by Minkowski's Convex Body Theorem:

THEOREM 6H (Minkowski 1896). *Suppose K is a convex set in Euclidean E^n, symmetric at $\mathbf{0}$ (i.e. if a point $\mathbf{x} \in K$ then also $-\mathbf{x} \in K$) and with volume $V(K) > 2^n$. Then K contains an integer point different from $\mathbf{0}$.*

Sometimes one needs a more general version of this result in which the set of integer points is replaced by a *point lattice* Λ. Namely, such a lattice Λ is any discrete subgroup of the vector space E^n which contains n linearly independent vectors. It is easy to see that Λ is obtained from the set of integer points by a non-singular linear transformation A, and although A is not determined by Λ, the absolute value of the determinant of A is. This absolute value is called the *determinant* of the lattice Λ and will be denoted by $d(\Lambda)$. Theorem 6H remains true if the integer points are replaced by a lattice Λ and if the inequality $V(K) > 2^n$ is replaced by $V(K) > 2^n d(\Lambda)$.)

A special case of Theorem 6H is when K is a parallelepiped given by inequalities

$$(6.6) \qquad | L_i(\mathbf{x}) | < R_i \qquad (i = 1, ..., n)$$

where $L_i(\mathbf{x}) = c_{i1}x_1 + ... + c_{in}x_n$ $(i = 1, ..., n)$ are linear forms of determinant 1 and where the R_i's are positive constants with $R_1 R_2 \dots R_n > 1$. Continuity arguments show that the conclusion is still true if $R_1 R_2 \dots R_n = 1$ and if one of the inequalities in (6.6) is replaced by $\leqq$. Thus we have

THEOREM 6I (Minkowski's Linear Forms Theorem). *Suppose $L_1, ..., L_n$ are linear forms with determinant 1 and suppose that $R_1, ..., R_n$ are positive with $R_1 \dots R_n \geqq 1$. There is an integer point $\mathbf{x} \neq \mathbf{0}$ with*

$$| L_1(\mathbf{x}) | \leqq R_1 , \ | L_2(\mathbf{x}) | < R_2, ..., | L_n(\mathbf{x}) | < R_n .$$

Now suppose $l \geqq 1$ and put $n = l + 1$, and for vectors $\mathbf{x} = (q, p_1, ..., p_l)$ put $L_1(\mathbf{x}) = \alpha_1 q - p_1, ..., L_l(\mathbf{x}) = \alpha_l q - p_l$, but $L_n(\mathbf{x}) = q$. We obtain

Theorem 6A by applying Minkowski's Linear Forms Theorem to these linear forms and to $R_1 = \dots = R_l = Q^{-1}$ and $R_n = Q^l$.

6.5. For later applications it will be convenient to state explicitly two other simple applications of Minkowski's Linear Forms Theorem. Suppose $1 \leqq m < n$ and let $L_1(\mathbf{x}), \dots, L_m(\mathbf{x})$ be linearly independent linear forms. Assume without loss of generality that $L_1, \dots, L_m, x_1, \dots, x_{n-m}$ are linearly independent, and that these n linear forms have determinant d. By Theorem 6I there is for every $Q > 1$ an integer point $\mathbf{x} \neq \mathbf{0}$ with

$$| d |^{-1/n} \, | L_i(\mathbf{x}) | \leqq Q^{-(n-m)} \qquad (i = 1, \dots, m)$$

and

$$| d |^{-1/n} \, | x_j | \leqq Q^m \qquad (j = 1, \dots, n-m) .$$

Then if the norm $|\mathbf{x}|$ of $\mathbf{x} = (x_1, \dots, x_n)$ is defined by

$$|\mathbf{x}| = \max(|x_1|, \dots, |x_n|) , \tag{6.7}$$

we have $|\mathbf{x}| \leqq c_1 Q^m$ and

$$| L_i(\mathbf{x}) | \leqq c_2 \, |\mathbf{x}|^{-(n-m)/m} \qquad (i = 1, \dots, m) \tag{6.8}$$

where c_1, c_2 depend on $L_1, \dots, L_m$ only. Since Q may be chosen arbitrarily large, it follows that there are infinitely many integer points $\mathbf{x} \neq \mathbf{0}$ with (6.8). More generally, it can be shown that if $L_1(\mathbf{x}), \dots, L_m(\mathbf{x})$ are linear forms of rank r (i.e. there are r but not $r+1$ linearly independent ones among them) with $1 \leqq r < n$, then the exponent in (6.8) may be replaced by $-(n-r)/r$. Therefore the following holds.

Corollary 6J. *Suppose $L_1, \dots, L_m$ are linear forms of rank r with $1 \leqq r < n$. There is a $c_3 = c_3(L_1, \dots, L_m)$ such that there are infinitely many integer points $\mathbf{x} \neq \mathbf{0}$ with*

$$| L_i(\mathbf{x}) | \leqq c_3 \, |\mathbf{x}|^{-(n-r)/r} \qquad (i = 1, \dots, m) .$$

Corollary 6J essentially implies Corollaries 6B, 6D, i.e. it implies versions of these corollaries involving constants such as c_3. Finally Theorem 6I yields

Corollary 6K. *Suppose $L_1(\mathbf{x}), \dots, L_n(\mathbf{x})$ are linear forms of determinant $d \neq 0$. Suppose $\gamma_1, \dots, \gamma_n$ are reals with $\gamma_1 + \dots + \gamma_n = 0$. For any $Q > 0$ there is an integer point $\mathbf{x} \neq \mathbf{0}$ with*

$$| L_i(\mathbf{x}) | \leqq | d |^{1/n} Q^{\gamma_i} \qquad (i=1, ..., n).$$

6.6. An important special case of Theorem 6C is when $\alpha_1 = \alpha$, $\alpha_2 = \alpha^2, ..., \alpha_l = \alpha^l$. Changing our notation from l to d, we obtain a solution of the inequalities

$$1 \leqq \max(|q_1|, ..., |q_d|) < Q^{1/d}, \quad | q_d\alpha^d + ... + q_1\alpha + q_0 | \leqq Q^{-1}.$$

The polynomial $P(x) = q_d x^d + ... + q_1 x + q_0$ has height $H(P) \leqq c_1 Q^{1/d}$ and $| P(\alpha) | \leqq Q^{-1}$, whence

$$| P(\alpha) | \leqq c_2 H(P)^{-d},$$

where c_1, c_2 depend on α and on d only. Now one can show that unless $| P'(\alpha) |$ is extremely small, there is a real root β of P with

$$| \alpha - \beta | \leqq c_3 | P(\alpha) | / | P'(\alpha) | \leqq c_2 c_3 H(P)^{-d} | P'(\alpha) |^{-1}.$$

In general it is likely that $| P'(\alpha) |$ is of about the same order of magnitude as $H(P)$, and then we obtain

$$| \alpha - \beta | \leqq c_4 H(P)^{-d-1} \leqq c_5 H(\beta)^{-d-1}.$$

(The defining polynomial of β is a divisor of P, and this implies that $H(\beta) \leqq c_6 H(P)$ by, e.g., Theorem 4-3 in vol. 2 of LeVeque (1955)). Unfortunately we don't know whether $| P'(\alpha) |$ is large. At any rate one is tempted to conjecture that for every real α which is not itself algebraic of degree $\leqq d$, there are infinitely many real algebraic β of degree $\leqq d$ such that

$$| \alpha - \beta | \leqq c_7 H(\beta)^{-d-1}. \tag{6.9}$$

A weaker conjecture is that for every α as above and every $\varepsilon > 0$ there are infinitely many real algebraic numbers β of degree $\leqq d$ with

$$| \alpha - \beta | < H(\beta)^{-(d+1-\varepsilon)}. \tag{6.10}$$

The conjecture related to (6.9) is true for $d = 1$ by Dirichlet's Theorem, and it was shown to be true for $d = 2$ by Davenport and Schmidt (1967). For general d, Wirsing (1961) showed that there are infinitely many β of degree $\leqq d$ with

$$| \alpha - \beta | \leqq c_8 H(\beta)^{-(d+3)/2}.$$

He also showed that if $(\alpha, \alpha^2, ..., \alpha^d)$ is not very well aproximable, then (6.10) does have infinitely many solutions for every $\varepsilon > 0$.

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

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

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