INEQUALITIES FOR IDEAL BASES IN ALGEBRAIC NUMBER FIELDS

K. MAHLER

(received 11 May 1964)

In a paper of nearly thirty years ago (Mahler 1937) I first studied approximation properties of algebraic number fields relative to their full system of inequivalent valuations. I now return to these questions with a slightly improved method and establish a number of existence theorems for such fields.

The main result of this paper (Theorem 1) states that every ideal has a basis such that *all* the valuations of *all* the basis elements lie below limits which can be given explicitly in terms of field constants and arbitrary parameters. Both this theorem and some of the consequences derived from it seem to be new; at least I have not found them in the recent treatments of algebraic number fields by E. Artin (1959), H. Hasse (1963), S. Lang (1964), or O. T. O'Meara (1963).

The paper of 1937 depended on Minkowski's theorem on the successive minima of convex bodies (see e.g. Cassels 1959). The present paper, on the other hand, is based on a classical inequality from the reduction theory of quadratic forms, or alternatively, on a basis theorem in the geometry of numbers which was not yet known in 1937. The new approach is more powerful and enables one to construct ideal bases rather than just a system of independent elements of the ideal.

I collect in § 1 the tools from the reduction theory of quadratic forms and from the geometry of numbers which are used in this paper. The next sections similarly contain the facts from valuation theory and ideal theory which are needed.

In a further paper I hope to treat algebraic function fields of one variable in a similar manner.

1.

Let $F(\boldsymbol{x}) = F(x_1, \cdots, x_n)$ be a symmetric convex distance function in n-dimensional real space, K the convex body K: $F(\boldsymbol{x}) \leqq 1$, and

$$V = \int \cdots \int_K dx_1 \cdots dx_n$$

the volume of K. As usual a lattice point denotes a point with rational integral coordinates.

A theorem due to myself (Mahler 1938) and H. Weyl (1942) states that there is a positive constant γ_n depending only on the dimension n of the space and not on the special distance function $F(\boldsymbol{x})$ or the body K, with the following property.

There exist n lattice points

$$\boldsymbol{g}_k = (g_{1k}, g_{2k}, \cdots, g_{nk}) \qquad (k = 1, 2, \cdots, n)$$

of determinant

$$\begin{vmatrix} g_{11}, \cdots, g_{n1} \\ \vdots \qquad\quad \vdots \\ g_{1n}, \cdots, g_{nn} \end{vmatrix} = 1$$

such that

$$\prod_{k=1}^{n} F(g_{1k}, g_{2k}, \cdots, g_{nk}) \leqq \frac{\gamma_n}{V}. \tag{1}$$

For all n the constant γ_n may be chosen equal to

$$\gamma_n = 2n!, \tag{2}$$

and for large n it is of lower order than $n!$ It would be of importance to determine the exact value of γ_n at least for small n.

Let in particular

$$\Phi(\boldsymbol{x}) = \Phi(x_1, \cdots, x_n) = \sum_{h=1}^{n} \sum_{k=1}^{n} \varphi_{hk} x_h x_k \qquad (\varphi_{hk} = \varphi_{kh})$$

be a positive definite quadratic form of discriminant

$$D_\Phi = \begin{vmatrix} \varphi_{11}, \cdots, \varphi_{1n} \\ \vdots \qquad\quad \vdots \\ \varphi_{n1}, \cdots, \varphi_{nn} \end{vmatrix} > 0,$$

and let

$$F(\boldsymbol{x}) = |\sqrt{\Phi(\boldsymbol{x})}|$$

be the positive square root of $\Phi(\boldsymbol{x})$. The body K is now the ellipsoid

$$K : \Phi(\boldsymbol{x}) \leqq 1$$

of volume

$$V = \pi^{n/2} \Gamma\left(\frac{n}{2} + 1\right)^{-1} D_\Phi^{-\frac{1}{2}}.$$

Hence in this case the inequality (1) takes the form

$$\prod_{k=1}^{n} \Phi(g_{1k}, g_{2k}, \cdots, g_{nk}) \leqq c_n D_\Phi, \tag{3}$$

where, by (1) and (2),

$$c_n = \gamma_n^2 \pi^{-n} \Gamma\left(\frac{n}{2}+1\right)^2 \leqq 4\pi^{-n} \Gamma\left(\frac{n}{2}+1\right)^2 (n!)^2 \leqq (n!)^3 \quad \text{for } n \geqq 2. \tag{4}$$

For small dimensions n better values for c_n are obtained from the reduction theory of positive definite quadratic form; see v. d. Waerden (1956), Kapitel 1. By this theory, one finds that one may choose

$$c_2 = \tfrac{4}{3},\ c_3 = 2,\ c_4 = 4,\ c_5 = 10,\ c_6 = 42,\ c_7 = 250; \tag{5}$$

here the values of c_2, c_3, and c_4 are best possible. Further

$$c_n \leqq \left(\frac{2}{\pi}\right)^n \Gamma\left(\frac{n}{2}+2\right)^2 \left(\tfrac{5}{4}\right)^{((n-3)(n-4))/2} \qquad \text{for } n \geqq 5,$$

but this upper bound is for large n not as good as (4).

While this paper is based on the inequality (3) for quadratic forms, a different choice of the distance function $F(x)$ might possibly be advantageous.

2.

Throughout this paper,

$$K = P(\vartheta), \quad \text{where} \quad F(\vartheta) = 0,$$

denotes a fixed algebraic number field of finite degree $n \geqq 2$ over the rational number field P. Here the polynomial $F(x)$ in $P[x]$ is assumed to be monic and irreducible over P.

Together with K we consider its isomorphic images in the complex number field C. Let $\vartheta^{(1)}, \cdots, \vartheta^{(n)}$ be the zeros of $F(x)$ in C numbered such that

$$\vartheta^{(1)}, \cdots, \vartheta^{(r_1)}$$

are real, but that

$$\vartheta^{(r_1+j)} \quad \text{and} \quad \vartheta^{(r_1+r_2+j)} \qquad (j = 1, 2, \cdots, r_2)$$

are non-real and complex conjugate. The isomorphism

$$\vartheta \to \vartheta^{(j)}$$

then maps K onto a subfield $K^{(j)}$ of C; let $\xi^{(j)}$, for every ξ in K, be its image in $K^{(j)}$. Then

$$|\xi^{(r_1+j)}| = |\xi^{(r_1+r_2+j)}| \qquad (j = 1, 2, \cdots, r_2),$$

and there are just

$$r_\infty = r_1 + r_2$$

distinct absolute values

$$|\xi^{(j)}| \qquad (j = 1, 2, \cdots, r_\infty)$$

in K. With each such absolute value $|\xi^{(j)}|$ we associate as usual an infinite prime divisor $\mathfrak{q}^{(j)}$, and we use the notation

$$|\xi^{(j)}| = |\xi|_{\mathfrak{q}^{(j)}} \qquad (j = 1, 2, \cdots, r_\infty).$$

We further put

$$r = r_\infty - 1, \qquad n_{\mathfrak{q}^{(j)}} = \begin{cases} 1 & \text{if } 1 \leqq j \leqq r_1, \\ 2 & \text{if } r_1 + 1 \leqq j \leqq r_\infty. \end{cases}$$

Then

$$\sum_{\mathfrak{q}} n_{\mathfrak{q}} = r_1 + 2r_2 = n, \quad \prod_{\mathfrak{q}} |\xi|_{\mathfrak{q}}^{n_{\mathfrak{q}}} = |N(\xi)|, \tag{6}$$

where both the sum and the product extend over all the infinite prime divisors

$$\mathfrak{q} = \mathfrak{q}^{(1)}, \mathfrak{q}^{(2)}, \cdots, \mathfrak{q}^{(r_\infty)}$$

of K. These r_∞ absolute values $|\xi|_{\mathfrak{q}}$ form all the inequivalent continuations to K of the absolute value $|x|$ in P.

3.

In addition to the r_∞ absolute values, K has countably many inequivalent non-archimedean discrete valuations, the $\mathfrak{r}$-adic valuations

$$|\xi|_{\mathfrak{r}}$$

where $\mathfrak{r}$ runs over all the finite prime divisors of K.

To each such prime divisor $\mathfrak{r}$ there belongs a unique (positive) prime

$$p = p_{\mathfrak{r}}$$

in P of which $\mathfrak{r}$ is a factor, and then the $\mathfrak{r}$-adic valuation $|\xi|_{\mathfrak{r}}$ is a continuation to K of the p-adic valuation $|x|_p$ of P. Conversely, when p is any (positive) prime in P, the p-adic valuation $|x|_p$ has a certain finite number r_p of inequivalent continuations $|\xi|_{\mathfrak{r}}$ where

$$\mathfrak{r} = \mathfrak{r}^{(1)}, \mathfrak{r}^{(2)}, \cdots, \mathfrak{r}^{(r_p)}$$

runs over all distinct prime divisor factors of p in K.

For each finite prime divisor $\mathfrak{r}$ denote by $e_{\mathfrak{r}}$ its order and by $f_{\mathfrak{r}}$ its degree, and put $n_{\mathfrak{r}} = e_{\mathfrak{r}} f_{\mathfrak{r}}$. The valuation $|\xi|_{\mathfrak{r}}$ can be written in the form

$$|\xi|_{\mathfrak{r}} = p_{\mathfrak{r}}^{-w_{\mathfrak{r}}(\xi)/e_{\mathfrak{r}}} \tag{7}$$

where $w_{\mathfrak{r}}(\xi)$ is the order of ξ with respect to $\mathfrak{r}$. The function $w_{\mathfrak{r}}(\xi)$ assumes exactly all rational integral values when ξ runs over the non-zero elements of K.

Next,

$$w_{\mathfrak{r}}(\mathfrak{p}_{\mathfrak{r}}) = e_{\mathfrak{r}}, \quad N(\mathfrak{r}) = p_{\mathfrak{r}}^{f_{\mathfrak{r}}}. \tag{8}$$

Furthermore, if $\mathfrak{p}$ is a prime in P, and $\mathfrak{r}$ runs over all the $r_{\mathfrak{p}}$ distinct prime divisor factors $\mathfrak{r}^{(j)}$ of $\mathfrak{p}$,

$$\sum_{\mathfrak{r}/\mathfrak{p}} n_{\mathfrak{r}} = n, \quad \prod_{\mathfrak{r}/\mathfrak{p}} |\xi|_{\mathfrak{r}}^{n_{\mathfrak{r}}} = |N(\xi)|_{\mathfrak{p}}. \tag{9}$$

From now on the letter $\mathfrak{p}$ will be used to denote all the prime divisors of K, both finite and infinite; on the other hand, $\mathfrak{q}$ will be restricted to the infinite and $\mathfrak{r}$ to the finite prime divisors.

For the whole of this paper the product formula

$$\prod_{\mathfrak{p}} |\xi|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = 1 \qquad \text{for all } \xi \neq 0 \text{ in } K \tag{10}$$

will be fundamental.

4.

Denote by $K_{\mathfrak{p}}$ the completion of K relative to the valuation $|\xi|_{\mathfrak{p}}$. Thus, $K_{\mathfrak{p}}$ is the real field R for $\mathfrak{p} = \mathfrak{q}^{(j)}$, $1 \leqq j \leqq r_1$; it is the complex field C for $\mathfrak{p} = \mathfrak{q}^{(j)}$, $r_1+1 \leqq j \leqq r_\infty$; and it is the $\mathfrak{r}$-adic field for $\mathfrak{p} = \mathfrak{r}$.

An adèle is an infinite dimensional vector $\boldsymbol{i} = \{i_{\mathfrak{p}}\}$ where to each prime divisor $\mathfrak{p}$ there corresponds a component $i_{\mathfrak{p}}$ of $\boldsymbol{i}$ which may be any element of $K_{\mathfrak{p}}$, subject to the condition that

$$|i_{\mathfrak{p}}|_{\mathfrak{p}} \leqq 1 \qquad \text{for all but finitely many } \mathfrak{p}.$$

If $i_{\mathfrak{p}} \neq 0$ for all $\mathfrak{p}$ and

$$|i_{\mathfrak{p}}|_{\mathfrak{p}} = 1 \qquad \text{for all but finitely many } \mathfrak{p},$$

$\boldsymbol{i}$ is called an idèle, and then

$$||\boldsymbol{i}|| = \prod_{\mathfrak{p}} |i_{\mathfrak{p}}|_{\mathfrak{p}}^{n_{\mathfrak{p}}}$$

is the *volume* of this idèle. The same notation is used for an adèle.

Such adèles and idèles will play only a subordinate role in this paper. Of much greater importance will be the notion of what I called a λ-function in my former paper (Mahler 1937), but which I shall now call a *ceiling*, a term suggested by my colleague B. H. Neumann.

A *ceiling* is a positive valued function $\lambda(\mathfrak{p})$ of the variable prime divisor $\mathfrak{p}$ with the following properties.

(A) *At all infinite prime divisors* $\mathfrak{q}$, $\lambda(\mathfrak{q})$ *may assume arbitrary positive values.*

(B) *At every finite prime divisor* $\mathfrak{r}$, $\lambda(\mathfrak{r})$ *is of the form*

$$\lambda(\mathfrak{r}) = p_{\mathfrak{r}}^{-l_{\mathfrak{r}}/e_{\mathfrak{r}}}$$

where $e_{\mathfrak{r}}$ *is the order of* $\mathfrak{r}$, $p_{\mathfrak{r}}$ *is the corresponding rational prime, and* $l_{\mathfrak{r}}$ *is any rational integer.*

(C) $\lambda(\mathfrak{p})$ *is equal to* 1 *except at finitely many prime divisors* $\mathfrak{p}$.

$$\text{(D)} \qquad \prod_{\mathfrak{p}} \lambda(\mathfrak{p})^{n_{\mathfrak{p}}} = 1.$$

From this definition, there exist to $\lambda(\mathfrak{p})$ infinitely many idèles $\boldsymbol{i}$ of volume $||\boldsymbol{i}|| = 1$ such that

$$\lambda(\mathfrak{p}) = |i_{\mathfrak{p}}|_{\mathfrak{p}} \qquad \text{for all } \mathfrak{p}.$$

This property might also have been used as the definition of a ceiling.

5.

If $\lambda(\mathfrak{p})$ is any ceiling, put

$$\text{(11)} \qquad \mathfrak{Q}_\lambda = \prod_{\mathfrak{q}} \lambda(\mathfrak{q})^{n_{\mathfrak{q}}}, \quad \mathfrak{R}_\lambda = \prod_{\mathfrak{r}} \lambda(\mathfrak{r})^{n_{\mathfrak{r}}},$$

so that

$$\text{(12)} \qquad \mathfrak{Q}_\lambda > 0, \quad \mathfrak{R}_\lambda > 0, \quad \mathfrak{Q}_\lambda \mathfrak{R}_\lambda = 1.$$

Further denote by $\mathfrak{a}_\lambda$ the finite divisor

$$\text{(13)} \qquad \mathfrak{a}_\lambda = \prod_{\mathfrak{r}} \mathfrak{r}^{l_{\mathfrak{r}}}$$

and by $[\mathfrak{a}_\lambda]$ the (fractional) ideal in K which consists of all field elements α that are divisible by $\mathfrak{a}_\lambda$, i.e. which satisfy the inequalities

$$|\alpha|_{\mathfrak{r}} \leqq \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r}.$$

Then $\mathfrak{a}_\lambda$ and $[\mathfrak{a}_\lambda]$ have the same norm

$$\text{(14)} \qquad N(\mathfrak{a}_\lambda) = N([\mathfrak{a}_\lambda]) = \prod_{\mathfrak{r}} N(\mathfrak{r})^{l_{\mathfrak{r}}} = \prod_{\mathfrak{r}} \lambda(\mathfrak{r})^{-n_{\mathfrak{r}}} = \frac{1}{\mathfrak{R}_\lambda} = \mathfrak{Q}_\lambda.$$

This relation between $\mathfrak{a}_\lambda$ and $[\mathfrak{a}_\lambda]$ is one-to-one, and every ideal $\mathfrak{a} \neq (0)$ is of the form $\mathfrak{a} = \mathfrak{a}_\lambda$ for at least one $\lambda(\mathfrak{p})$.

A basis of $\mathfrak{a}_\lambda$, or more exactly of $[\mathfrak{a}_\lambda]$, is a set of n elements $\alpha_1, \cdots, \alpha_n$ of K that are linearly independent over P and are such that every element α of $[\mathfrak{a}_\lambda]$ can be written in a unique way as a sum

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$$

with rational integral coefficients $x_1, \cdots, x_n$. The discriminant $d(\mathfrak{a}_\lambda)$ of both $\mathfrak{a}_\lambda$ and $[\mathfrak{a}_\lambda]$ is then given by

$$d(\mathfrak{a}_\lambda) = \begin{vmatrix} \alpha_1^{(1)}, \cdots, \alpha_n^{(1)} \\ \vdots \qquad\quad \vdots \\ \alpha_1^{(n)}, \cdots, \alpha_n^{(n)} \end{vmatrix}^2 = N(\mathfrak{a}_\lambda)^2 d = \mathfrak{Q}_\lambda^2 d, \tag{15}$$

where $d \neq 0$ is the field discriminant, and the upper suffixes denote the conjugates over C.

Two ceilings $\lambda(\mathfrak{p})$ and $\mu(\mathfrak{p})$ are said to be *associated* if

$$\lambda(\mathfrak{r}) = \mu(\mathfrak{r}) \qquad \text{for all } \mathfrak{r},$$

hence if and only if

$$\mathfrak{a}_\lambda = \mathfrak{a}_\mu.$$

Except when K is an imaginary quadratic field, there are always infinitely many ceilings that are equivalent to a given one.

A ceiling is called *principal* if there exist an element $\theta \neq 0$ of K and a positive integer H such that

$$\lambda(\mathfrak{p})^H = |\theta|_\mathfrak{p} \qquad \text{for all } \mathfrak{p}.$$

It is true only for imaginary quadratic fields that every ceiling is principal.

Under multiplication the ceilings form an abelian group of which the principal ceilings form a subgroup.

6.

The following two simple properties of ceilings will be applied repeatedly in this paper.

LEMMA 1. *Let $\xi \neq 0$ be an element of K, Γ a positive constant, and $\lambda(\mathfrak{p})$ a ceiling satisfying*

$$|\xi|_\mathfrak{q} \leqq \Gamma\lambda(\mathfrak{q}) \text{ for all } \mathfrak{q}, \qquad |\xi|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \text{ for all } \mathfrak{r}.$$

Then

$$|\xi|_\mathfrak{q} \geqq \Gamma^{-(n-1)}\lambda(\mathfrak{q}) \text{ for all } \mathfrak{q}, \qquad |\xi|_\mathfrak{r} \geqq \Gamma^{-n}\lambda(\mathfrak{r}) \text{ for all } \mathfrak{r}.$$

PROOF. By the fundamental equation (10) and by the property (D), for every divisor $\mathfrak{p}_0$,

$$|\xi|_{\mathfrak{p}_0}^{n\mathfrak{p}_0} = \Big\{\prod_{\mathfrak{p}\neq\mathfrak{p}_0} |\xi|_\mathfrak{p}^{n\mathfrak{p}}\Big\}^{-1}, \qquad \lambda(\mathfrak{p}_0)^{n\mathfrak{p}_0} = \Big\{\prod_{\mathfrak{p}\neq\mathfrak{p}_0} \lambda(\mathfrak{p})^{n\mathfrak{p}}\Big\}^{-1},$$

hence

$$\left(\frac{|\xi|_{\mathfrak{p}_0}}{\lambda(\mathfrak{p}_0)}\right)^{n_{\mathfrak{p}_0}} = \left\{\prod_{\mathfrak{p}\neq\mathfrak{p}_0}\left(\frac{|\xi|_{\mathfrak{p}}}{\lambda(\mathfrak{p})}\right)^{n_{\mathfrak{p}}}\right\}^{-1} \geqq \begin{cases} \prod_{\mathfrak{q}\neq\mathfrak{q}_0} \Gamma^{-n_{\mathfrak{q}}} = \Gamma^{-(n-1)} & \text{if } \mathfrak{p}_0 = \mathfrak{q}_0, \\ \prod_{\mathfrak{q}} \Gamma^{-n_{\mathfrak{q}}} = \Gamma^{-n} & \text{if } \mathfrak{p}_0 = \mathfrak{r}_0. \end{cases}$$

Since $n_{\mathfrak{p}_0} \geqq 1$, the assertion follows at once.

It is clear that the hypothesis of the lemma can hold only if $\Gamma \geqq 1$.

LEMMA 2. *Let the hypothesis be as in Lemma* 1, *and let* $\mathfrak{r}_0$ *be any finite prime divisor satisfying*

$$p_{\mathfrak{r}_0} > \Gamma^{n^2}.$$

Then

$$|\xi|_{\mathfrak{r}_0} = \lambda(\mathfrak{r}_0).$$

PROOF. If for any finite prime divisor $\mathfrak{r}$

$$|\xi|_{\mathfrak{r}} < \lambda(\mathfrak{r}),$$

then from the property (B),

$$|\xi|_{\mathfrak{r}} \leqq \lambda(\mathfrak{r}) p_{\mathfrak{r}}^{-1/e_{\mathfrak{r}}} \leqq \lambda(\mathfrak{r}) p_{\mathfrak{r}}^{-1/n}.$$

This would imply for $\mathfrak{r} = \mathfrak{r}_0$ that

$$|\xi|_{\mathfrak{r}_0} \leqq \lambda(\mathfrak{r}_0) p_{\mathfrak{r}_0}^{-1/n} < \Gamma^{-n}\lambda(\mathfrak{r}_0),$$

contrary to Lemma 1.

7.

We procede now to the proof of the main theorem of this paper. Let $\lambda(\mathfrak{p})$ be an arbitrary ceiling, $\mathfrak{a}_\lambda$ the corresponding finite divisor, and $\beta_1, \cdots, \beta_n$ an arbitrary basis of $[\mathfrak{a}_\lambda]$. We form the function

$$\Phi(\boldsymbol{x}) = \Phi(x_1, \cdots, x_n) = \sum_{\mathfrak{q}} \lambda(\mathfrak{q})^{-2} |x_1\beta_1 + \cdots + x_n\beta_n|_{\mathfrak{q}}^2 \tag{16}$$

of the real variables $x_1, \cdots, x_n$; here the $\mathfrak{q}$-adic values are defined by

$$|x_1\beta_1 + \cdots + x_n\beta_n|_{\mathfrak{q}} = |x_1\beta_1^{(j)} + \cdots + x_n\beta_n^{(j)}| \quad \text{for } \mathfrak{q} = \mathfrak{q}^{(j)},\ 1 \leqq j \leqq r_\infty,$$

where upper suffixes denote again conjugates. Naturally Φ depends on the choice of the basis $\beta_1, \cdots, \beta_n$.

Write

$$\beta_h^{(r_1+j)} = \gamma_h^{(r_1+j)} + i\gamma_h^{(r_1+r_2+j)} \qquad (h = 1, 2, \cdots, n;\ j = 1, 2, \cdots, r_2),$$

where the γ's are the real and the imaginary parts of the $\beta_h^{(r_1+j)}$. Then Φ becomes a sum of n squares of real linear forms,

$$\Phi(x) = \sum_{j=1}^{r_1} \lambda(\mathfrak{q}^{(j)})^{-2}(x_1\beta_1^{(j)} + \cdots + x_n\beta_n^{(j)})^2 +$$
$$+ \sum_{j=1}^{r_2} \lambda(\mathfrak{q}^{(r_1+j)})^{-2}\{(x_1\gamma_1^{(r_1+j)} + \cdots + x_n\gamma_n^{(r_1+j)})^2 +$$
$$+ (x_1\gamma^{(r_1+r_2+j)} + \cdots + x_n\gamma_n^{(r_1+r_2+j)})^2\},$$

and hence takes the form of a positive definite quadratic form. From this representation, it has the discriminant

$$D_\Phi = \Delta^2 \prod_{\mathfrak{q}} \lambda(\mathfrak{q})^{-2n_\mathfrak{q}} = \Delta^2 \mathfrak{Q}_\lambda^{-2} \tag{17}$$

where Δ denotes the determinant of order n in which the h-th column, for $h = 1, 2, \cdots, n$, consists of the consecutive elements

$$\beta_h^{(1)}, \beta_h^{(2)}, \cdots, \beta_h^{(r_1)}, \gamma_h^{(r_1+1)}, \gamma_h^{(r_1+2)}, \cdots, \gamma_h^{(n)}.$$

Denote by b the determinant of the $n \times n$ matrix with elements

$$b_{hk} = \begin{cases} +1 \text{ if } h = 1, 2, \cdots, r_\infty & \text{and } k = h, \\ +i \text{ if } h = r_1+1, r_1+2, \cdots, r_\infty & \text{and } k = h+r_2, \\ +1 \text{ if } h = r_\infty+1, r_\infty+2, \cdots, n & \text{and } k = h-r_2, \\ -i \text{ if } h = r_\infty+1, r_\infty+2, \cdots, n & \text{and } k = h, \text{ and} \\ 0 \quad \text{in all other cases.} \end{cases}$$

Then

$$b = (-2i)^{r_2}.$$

On multiplying the matrix of Δ on the left-hand side by (b_{hk}), we obtain

$$(-2i)^{r_2}\Delta = \begin{vmatrix} \beta_1^{(1)}, \cdots, \beta_n^{(1)} \\ \vdots \qquad\quad \vdots \\ \beta_1^{(n)}, \cdots, \beta_n^{(n)} \end{vmatrix} = d(\mathfrak{a}_\lambda)^{\frac{1}{2}} = N(\mathfrak{a}_\lambda)\sqrt{d} = \mathfrak{Q}_\lambda\sqrt{d},$$

and hence

$$\Delta^2 = \mp 2^{-2r_2}\mathfrak{Q}_\lambda^2 d.$$

Since D_Φ is positive, it follows then finally from (17) that

$$D_\Phi = 2^{-2r_2}|d|. \tag{18}$$

8.

We now apply to Φ the inequality (3) of § 1. By this formula there is an $n \times n$ matrix (g_{hk}) with rational integral elements and of determinant 1 such that

$$\prod_{k=1}^{n} \Phi(g_{1k}, g_{2k}, \cdots, g_{nk}) \leqq c_n D_\Phi, \tag{3}$$

with the values (4) or (5) for c_n. Put

$$\alpha_k = \sum_{h=1}^{n} \beta_h g_{hk}, \quad m_k = \sum_{\mathfrak{q}} \lambda(\mathfrak{q})^{-2} |\alpha_k|_{\mathfrak{q}}^2 \qquad (k = 1, 2, \cdots, n). \tag{19}$$

Then $\alpha_1, \cdots, \alpha_n$ form a basis of $[\mathfrak{a}_\lambda]$, and

$$m_k = \Phi(g_{1k}, g_{2k}, \cdots, g_{nk}) \qquad (k = 1, 2, \cdots, n).$$

Hence, by (3) and (18),

$$m_1 m_2 \cdots m_n \leqq 2^{-2r_2} c_n |d|. \tag{20}$$

The equation (19) for m_k may be written in the form

$$\frac{m_k}{n} = \frac{1}{n} \sum_{\mathfrak{q}} \lambda(\mathfrak{q})^{-2} n_{\mathfrak{q}} \frac{|\alpha_k|_{\mathfrak{q}}^2}{n_{\mathfrak{q}}}.$$

To this formula we apply the theorem on the arithmetic and geometric means, where we note that $n_{\mathfrak{q}}$ is equal to 1 for r_1 and equal to 2 for r_2 prime divisors $\mathfrak{q}$. Therefore

$$\Big\{ \prod_{\mathfrak{q}} (\lambda(\mathfrak{q})^{-2n_{\mathfrak{q}}} |\alpha_k|_{\mathfrak{q}}^{2n_{\mathfrak{q}}} n_{\mathfrak{q}}^{-n_{\mathfrak{q}}}) \Big\}^{1/n} \leqq \frac{m_k}{n},$$

where

$$\prod_{\mathfrak{q}} \lambda(\mathfrak{q})^{-2n_{\mathfrak{q}}} = \mathfrak{Q}_\lambda^{-2}, \quad \prod_{\mathfrak{q}} |\alpha_k|_{\mathfrak{q}}^{2n_{\mathfrak{q}}} = N(\alpha_k)^2, \quad \prod_{\mathfrak{q}} n_{\mathfrak{q}}^{-n_{\mathfrak{q}}} = 2^{-2r_2}.$$

It follows that

$$\prod_{\mathfrak{q}} |\alpha_k|_{\mathfrak{q}}^{n_{\mathfrak{q}}} = |N(\alpha_k)| \leqq 2^{r_2} \mathfrak{Q}_\lambda \left(\frac{m_k}{n} \right)^{n/2}, \tag{21}$$

where the square root is taken with the positive sign.

On the other hand, α_k is an element of a basis for $[\mathfrak{a}_\lambda]$, hence does not vanish and is divisible by $\mathfrak{a}_\lambda$, i.e.

$$|\alpha_k|_{\mathfrak{r}} \leqq \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r}. \tag{22}$$

Therefore

$$\prod_{\mathfrak{r}} |\alpha_k|_{\mathfrak{r}}^{n_{\mathfrak{r}}} \leqq \prod_{\mathfrak{r}} \lambda(\mathfrak{r})^{n_{\mathfrak{r}}} = \mathfrak{R}_\lambda.$$

We now multiply this inequality with the inequality (21) and apply the fundamental equation (10). The result is that

$$1 = \prod_{\mathfrak{p}} |\alpha_k|_{\mathfrak{p}}^{n_{\mathfrak{p}}} \leqq 2^{r_2} \mathfrak{Q}_\lambda \left(\frac{m_k}{n} \right)^{n/2} \cdot \mathfrak{R}_\lambda = 2^{r_2} \left(\frac{m_k}{n} \right)^{n/2},$$

and that therefore

$$m_k \geqq 2^{-2r_2/n} n \qquad (k = 1, 2, \cdots, n). \tag{23}$$

We finally substitute this lower bound for all but one of the factors m_k in (20) and then obtain also an upper bound, viz.

$$m_k \leqq 2^{-2r_2/n} n^{-(n-1)} c_n |d| \qquad (k = 1, 2, \cdots, n). \tag{24}$$

Since, by (19),

$$|\alpha_k|_{\mathfrak{q}}^2 \leqq m_k \lambda(\mathfrak{q})^2 \qquad \text{for all } \mathfrak{q},$$

it follows that

$$|\alpha_k|_{\mathfrak{q}} \leqq 2^{-r_2/n} n^{-(n-1)/2} |c_n d|^{\frac{1}{2}} \lambda(\mathfrak{q}) \qquad \text{for all } \mathfrak{q},$$

or, say,

$$|\alpha_k|_{\mathfrak{q}} \leqq C\lambda(\mathfrak{q}) \quad \text{for all } \mathfrak{q} \qquad (k = 1, 2, \cdots, n) \tag{25}$$

where from now on C denotes the field constant

$$C = 2^{-r_2/n} n^{-(n-1)/2} |c_n d|^{\frac{1}{2}}. \tag{26}$$

For the smallest values of n the following table for C is obtained from (5).

$$n = 2, \quad r_1 = 2, \quad r_2 = 0, \qquad C = \left(\frac{2d}{3}\right)^{\frac{1}{2}},$$

$$n = 2, \quad r_1 = 0, \quad r_2 = 1, \qquad C = \left|\frac{d}{3}\right|^{\frac{1}{2}},$$

$$n = 3, \quad r_1 = 3, \quad r_2 = 0, \qquad C = \left(\frac{2d}{9}\right)^{\frac{1}{2}},$$

$$n = 3, \quad r_1 = 1, \quad r_2 = 1, \qquad C = \left|\frac{2^{\frac{1}{2}} d}{9}\right|^{\frac{1}{2}},$$

$$n = 4, \quad r_1 = 4, \quad r_2 = 0, \qquad C = \left(\frac{d}{16}\right)^{\frac{1}{2}},$$

$$n = 4, \quad r_1 = 2, \quad r_2 = 1, \qquad C = \left|\frac{2^{\frac{1}{2}} d}{32}\right|^{\frac{1}{2}},$$

$$n = 4, \quad r_1 = 0, \quad r_2 = 2, \qquad C = \left(\frac{d}{32}\right)^{\frac{1}{2}}.$$

On applying Lemma 1 to the formulae (22) and (25), we obtain the further pair of inequalities

$$\left.\begin{aligned} |\alpha_k|_{\mathfrak{q}} &\geqq C^{-(n-1)} \lambda(\mathfrak{q}) \quad \text{for all } \mathfrak{q} \qquad (27)\\ |\alpha_k|_{\mathfrak{r}} &\geqq C^{-n} \lambda(\mathfrak{r}) \quad \text{for all } \mathfrak{r} \qquad (28) \end{aligned}\right\} \qquad (k = 1, 2, \cdots, n).$$

We also see that always

$$C \geqq 1,$$

and we may make use of Lemma 2. By combining these results we arrive at the following theorem.

THEOREM 2. *Let $\lambda(\mathfrak{p})$ be an arbitrary ceiling of K, and let $\mathfrak{a}_\lambda$ be the corresponding divisor. Then there exists a basis $\alpha_1, \cdots, \alpha_n$ of the ideal $[\mathfrak{a}_\lambda]$ such that*

$$\left.\begin{aligned} C^{-(n-1)}\lambda(\mathfrak{q}) \leqq |\alpha_k|_\mathfrak{q} \leqq C\lambda(\mathfrak{q}) \quad &\text{for all } \mathfrak{q} \\ C^{-n}\lambda(\mathfrak{r}) \leqq |\alpha_k|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \quad &\text{for all } \mathfrak{r} \end{aligned}\right\} \quad (k = 1, 2, \cdots, n).$$

Furthermore, if $p_\mathfrak{r}$ is the rational prime divisible by $\mathfrak{r}$,

$$|\alpha_k|_\mathfrak{r} = \lambda(\mathfrak{r}) \qquad \textit{for all } \mathfrak{r} \textit{ satisfying } p_\mathfrak{r} > C^{n^2}.$$

COROLLARY. *The norms of the basis elements satisfy the inequalities*

$$|N(\alpha_k)| \leqq C^* N(\mathfrak{a}_\lambda) \qquad (k = 1, 2, \cdots, n),$$

where C^* denotes the field constant

$$C^* = n^{-\frac{1}{2}n^2}|c_n d|^{\frac{1}{2}n}.$$

This last result is contained in (14), (21), and (24). For small n, C^* has the values

$$C^* = \left|\frac{d}{3}\right| \text{ if } n = 2; \quad C^* = \left|\frac{2d}{27}\right|^{\frac{1}{2}} \text{ if } n = 3; \quad C^* = \left|\frac{d}{64}\right|^2 \text{ if } n = 4.$$

The basis $\alpha_1, \cdots, \alpha_n$ given by Theorem 1 will from now on be called a *λ-basis*; and we shall later make use of the vector

$$\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)'$$

which has the basis elements as its components.

9.

As we remarked already, except when K is an imaginary quadratic field there are always infinitely many associated λ-functions. Hence, apart from this special case, theorem 1 establishes the existence of *infinitely many* different λ-bases of any given ideal $[\mathfrak{a}_\lambda] = \mathfrak{a}$. It has some interest to note that these λ-bases do *not* represent the most general type of basis of an ideal. This is obvious from the following theorem.

THEOREM 2. *There exists a finite set*

$$M = \{\kappa_1, \kappa_2, \cdots, \kappa_m\}$$

of elements of K with the following property.

If $\alpha_1, \cdots, \alpha_n$ is any λ-basis of K, then the quotients

$$\frac{\alpha_h}{\alpha_k} \qquad (h, k = 1, 2, \cdots, n)$$

belong to M.

PROOF. The principal ideals (α_h) and (α_k) are multiples of $[\mathfrak{a}_\lambda]$ and so can be written as

$$(\alpha_h) = [\mathfrak{a}_\lambda]\mathfrak{g}_h, \quad (\alpha_k) = [\mathfrak{a}_\lambda]\mathfrak{g}_k.$$

Here, by the Corrollary, $\mathfrak{g}_h$ and $\mathfrak{g}_k$ are integral ideals satisfying

$$1 \leqq N(\mathfrak{g}_h) \leqq C^*, \quad 1 \leqq N(\mathfrak{g}_k) \leqq C^*.$$

Hence both numerator and denominator of the ideal quotient

$$\left(\frac{\alpha_h}{\alpha_k}\right) = \frac{\mathfrak{g}_h}{\mathfrak{g}_k}$$

are bounded. Since this quotient is a principal ideal, it must then be equal to one of *finitely many* principal ideals

$$(\gamma_1), (\gamma_2), \cdots, (\gamma_w)$$

where the γ's depend only on the field K and are all distinct from 0.

Assume, say, that

$$\left(\frac{\alpha_h}{\alpha_k}\right) = (\gamma_\mu)$$

and that therefore a unit η exists for which

$$\frac{\alpha_h}{\alpha_k} = \gamma_\mu \eta.$$

By Theorem 1,

$$\left|\frac{\alpha_h}{\alpha_k}\right|_\mathfrak{q} = |\gamma_\mu|_\mathfrak{q} |\eta|_\mathfrak{q} \leqq \frac{C\lambda(\mathfrak{q})}{C^{-(n-1)}\lambda(\mathfrak{q})} = C^n \qquad \text{for all } \mathfrak{q}.$$

Hence

$$|\eta|_\mathfrak{q} \leqq C^n |\gamma_\mu|_\mathfrak{q}^{-1} \qquad \text{for all } \mathfrak{q}.$$

Now the γ's are finite in number, are distinct from zero, and they depend only on K. Therefore there exists an upper bound for all the absolute values $|\eta|_\mathfrak{q}$ of η that also depends only on K. Hence η is one of finitely many units

$$\eta_1, \eta_2, \cdots, \eta_w$$

that likewise depend only on K. The set M of all products

$$\gamma_\mu \eta_\nu \qquad (\mu = 1, 2, \cdots, u; \nu = 1, 2, \cdots, v)$$

evidently has the asserted properties.

This construction will in general give for M much too large a set. There would be some interest in establishing an algorithm for determining the smallest possible set M that belongs to a given field K.

The classical theorem on the finiteness of the ideal class number of K is a trivial consequence of Theorem 2. For let $\mathfrak{a}$ be an arbitrary (fractional) ideal $\neq(0)$ of K; let $\lambda(\mathfrak{p})$ be any ceiling such that $[\mathfrak{a}_\lambda] = \mathfrak{a}$, and let $\alpha_1, \cdots, \alpha_n$ be a λ-basis. Then the ideal

$$(\alpha_1)^{-1}\mathfrak{a} = \left(1, \frac{\alpha_2}{\alpha_1}, \cdots, \frac{\alpha_n}{\alpha_1}\right)$$

is equivalent to $\mathfrak{a}$, and it has only finitely many possibilities because all its generators lie in the finite set M.

10.

Let $\boldsymbol{i} = \{i_\mathfrak{p}\}$ be an arbitrary adèle of K, and $\lambda(\mathfrak{p})$ any ceiling. We shall prove that the adèle can be approximated by a number α of the field such that all the valuations $|\alpha - i_\mathfrak{p}|_\mathfrak{p}$ are at most of the order of $\lambda(\mathfrak{p})$. We begin with a weaker result.

LEMMA 3. *There exists an element β of K such that*

$$|\beta - i_\mathfrak{r}|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r}.$$

PROOF. Denote by $\mathscr{R}^*$ the set of those finite prime divisors $\mathfrak{r}$ for which at least one of the two numbers $|i_\mathfrak{r}|_\mathfrak{r}$ and $\lambda(\mathfrak{r})$ is distinct from 1, by $\mathscr{P}$ the set of all rational primes p of the form $p = p_\mathfrak{r}$ for some $\mathfrak{r}$ in $\mathscr{R}^*$, and by $\mathscr{R}$ and $\overline{\mathscr{R}}$ the sets of all finite prime divisors $\mathfrak{r}$ for which $p_\mathfrak{r}$ does, or does not, belong to $\mathscr{P}$, respectively. Let further Π be the product of all primes p in $\mathscr{P}$.

From these definitions,

$$|i_\mathfrak{r}|_\mathfrak{r} = \lambda(\mathfrak{r}) = |\Pi|_\mathfrak{r} = 1 \qquad \text{for } \mathfrak{r} \in \overline{\mathscr{R}}. \tag{29}$$

Choose for k so large a positive integer that

$$|\Pi^k i_\mathfrak{r}|_\mathfrak{r} \leqq 1 \qquad \text{for all } \mathfrak{r} \in \mathscr{R};$$

the finitely many numbers $\Pi^k i_\mathfrak{r}$, where $\mathfrak{r} \in \mathscr{R}$, are thus $\mathfrak{r}$-adic integers. By the approximation theorem for finitely many distinct $\mathfrak{r}$-adic valuations of K there exists then an algebraic integer γ in K such that

$$|\gamma - \Pi^k i_\mathfrak{r}|_\mathfrak{r} \leqq |\Pi^k|_\mathfrak{r} \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r} \in \mathscr{R}.$$

On putting

$$\beta = \Pi^{-k}\gamma,$$

it follows that

$$|\beta - i_\mathfrak{r}|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r} \in \mathfrak{R}.$$

On the other hand, it is obvious from (29) that

$$|\beta - i_\mathfrak{r}|_\mathfrak{r} = |\Pi^{-k}\gamma - i_\mathfrak{r}|_\mathfrak{r} \leqq \max(|\Pi^{-k}\gamma|_\mathfrak{r}, |i_\mathfrak{r}|_\mathfrak{r}) = 1 = \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r} \in \bar{\mathfrak{R}}.$$

These two sets of inequalities prove that β satisfies the assertion of the lemma.

11.

The system of inequalities

$$|\alpha - i_\mathfrak{r}|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r} \tag{30}$$

has not only the solution $\alpha = \beta$ just constructed, but is more generally satisfies by all elements α of K which are of the form

$$\alpha = \beta + x_1\alpha_1 + \cdots + x_n\alpha_n, \tag{31}$$

where $\alpha_1, \ldots, \alpha_n$ form a λ-basis, and $x_1, \cdots, x_n$ are arbitrary rational integers. For we have

$$|x_k|_\mathfrak{r} \leqq 1 \quad \text{and} \quad |\alpha_k|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \quad \text{for all } \mathfrak{r} \quad (k = 1, 2, \cdots, n),$$

and hence, by the construction of β,

$$|\alpha - i_\mathfrak{r}|_\mathfrak{r} \leqq \max\,(|\beta - i_\mathfrak{r}|_\mathfrak{r}, |x_k\alpha_k|_\mathfrak{r}) \leqq \lambda(\mathfrak{r}) \qquad \text{for all } \mathfrak{r}. \tag{32}$$

We can now choose the rational integers $x_1, \cdots, x_n$ in such a way that also the absolute values

$$|\alpha - i_\mathfrak{q}|_\mathfrak{q}, \text{ where } \mathfrak{q} = \mathfrak{q}^{(1)}, \mathfrak{q}^{(2)}, \cdots, \mathfrak{q}^{(r_\infty)},$$

allow simple upper estimates in terms of the values $\lambda(\mathfrak{q})$. For this purpose we note that, if upper indices as usual denote the conjugates, the numbers

$$\beta^{(j)}, i_{\mathfrak{q}^{(j)}}, \alpha_1^{(j)}, \cdots, \alpha_n^{(j)}$$

are real if $1 \leqq j \leqq r_1$, and they are complex if $r_1 + 1 \leqq j \leqq r_\infty$. The discriminant

$$d(\alpha_1, \cdots, \alpha_n) = \begin{vmatrix} \alpha_1^{(1)}, \cdots, \alpha_n^{(1)} \\ \vdots \qquad\quad \vdots \\ \alpha_1^{(n)}, \cdots, \alpha_n^{(n)} \end{vmatrix}^2$$

of the λ-basis is known to be real and distinct from zero. It follows then that there exist real numbers $\xi_1, \cdots, \xi_n$ such that

$$\beta^{(j)}-i_{\mathfrak{q}^{(j)}} = \xi_1\alpha_1^{(j)}+\cdots+\xi_n\alpha_n^{(j)} \qquad \text{for } j = 1, 2, \cdots, r_\infty.$$

We finally fix the rational integers $x_1, \cdots, x_n$ in (31) by the conditions

$$-\tfrac{1}{2} \leqq x_k+\xi_k < +\tfrac{1}{2} \qquad (k = 1, 2, \ldots, n).$$

Then

$$|\alpha-i_{\mathfrak{q}^{(j)}}|_{\mathfrak{q}^{(j)}} = |(x_1+\xi_1)\alpha_1^{(j)}+\cdots+(x_n+\xi_n)\alpha_n^{(j)}| \leqq$$
$$\leqq n\cdot\tfrac{1}{2}\max(|\alpha_1^{(j)}|, \cdots, |\alpha_n^{(j)}|) \qquad (j = 1, 2, \cdots, r_\infty),$$

and hence

$$|\alpha-i_{\mathfrak{q}}|_{\mathfrak{q}} \leqq \frac{nC}{2}\lambda(\mathfrak{q}) \qquad \text{for all } \mathfrak{q}. \tag{33}$$

By combining the estimates (32) and (33) we arrive at the following result.

THEOREM 3. *Let $\mathfrak{i} = \{i_\mathfrak{p}\}$ be any adèle and $\lambda(\mathfrak{p})$ any ceiling of K. Then there exists an element α of K such that*

$$|\alpha-i_\mathfrak{q}|_\mathfrak{q} \leqq \frac{nC}{2}\lambda(\mathfrak{q}) \text{ for all } \mathfrak{q}, \quad |\alpha-i_\mathfrak{r}|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \text{ for all } \mathfrak{r}.$$

COROLLARY. *These formulae imply that*

$$\prod_\mathfrak{p} |\alpha-i_\mathfrak{p}|_\mathfrak{p}^{n_\mathfrak{p}} \leqq \left(\frac{nC}{2}\right)^n.$$

Hence to every adèle $\mathfrak{i}$ there is a field element α with the property that the volume of the adèle $\alpha-\mathfrak{i}$ is not greater than $(nC/2)^n$.

Theorem 3 seems to be new; it is stronger than the approximation theorems in the books on algebraic numbers which have been referred to in the introduction.

12.

As an application of Theorem 3 we give here a short proof of a well-known density theorem (see e.g. Lang 1964, V, § 1, or O'Meara 1963, § 33 : 5.)

Denote by $\lambda(\mathfrak{p})$ an arbitrary ceiling, by t a parameter such that

$$t \geqq 8nC \tag{34}$$

and by $L(t)$ the number of field elements α satisfying

$$|\alpha|_\mathfrak{q} \leqq t\lambda(\mathfrak{q}) \text{ for all } \mathfrak{q}; \quad |\alpha|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) \text{ for all } \mathfrak{r}. \tag{35}$$

We shall prove that

$$L(t) \geqq (4nC)^{-n}t^n. \tag{36}$$

Put

$$\tau = \left[\frac{t}{4nC}\right],$$

where as usual the square brackets denote the integral part. Then, by (34),

$$\frac{t}{8nC} \leqq \frac{t}{4nC} - 1 < \tau \leqq \frac{t}{4nC}. \tag{37}$$

For each suffix $j = 1, 2, \cdots, n$ denote by g_j any one of the integers

$$0, \mp 1, \mp 2, \cdots, \mp \tau,$$

so that the system $\boldsymbol{g} = (g_1, \cdots, g_n)$ of these n integers has

$$(2\tau+1)^n > \left(\frac{t}{4nC}\right)^n$$

possibilities. With each system $\boldsymbol{g}$ we associate an adèle $\boldsymbol{i} = \boldsymbol{i}(\boldsymbol{g}) = \{i_\mathfrak{p}\}$ as follows. For every infinite prime divisor $\mathfrak{q} = \mathfrak{q}^{(j)}$ put

$$i_{\mathfrak{q}^{(j)}} = \begin{cases} 2nCg_j\lambda(\mathfrak{q}^{(j)}) & \text{if} \quad 1 \leqq j \leqq r_1, \\ 2nC(g_j + ig_{j+r_2})\lambda(\mathfrak{q}^{(j)}) & \text{if} \quad r_1+1 \leqq j \leqq r_\infty, \end{cases}$$

and for every finite prime divisor $\mathfrak{r}$ put

$$i_\mathfrak{r} = 0.$$

By Theorem 3 there exists to this adèle an element $\alpha = \alpha(\boldsymbol{g})$ of K for which

$$\begin{cases} |\alpha^{(j)} - 2nCg_j\lambda(\mathfrak{q}^{(j)})| \leqq \dfrac{nC}{2}\lambda(\mathfrak{q}^{(j)}) & \text{if} \quad 1 \leqq j \leqq r_1, \\ |\alpha^{(j)} - 2nC(g_j + ig_{j+r_2})\lambda(\mathfrak{q}^{(j)}| \leqq \dfrac{nC}{2}\lambda(\mathfrak{q}^{(j)}) & \text{if} \quad r_1+1 \leqq j \leqq r_\infty, \\ |\alpha|_\mathfrak{r} \leqq \lambda(\mathfrak{r}) & \text{for all } \mathfrak{r}. \end{cases} \tag{38}$$

Now, by (34) and (37),

$$\max\left(2nC|g_j| + \frac{nC}{2}, 2nC|g_j + ig_{j+r_2}| + \frac{nC}{2}\right) \leqq 2nC\tau\sqrt{2} + \frac{nC}{2} \leqq \frac{t}{\sqrt{2}} + \frac{t}{16} < t,$$

and so it follows from (38) that α is a solution of (35).

On the other hand, the numbers, α and α^* say, that belong to two distinct systems of integers $\boldsymbol{g}$ and $\boldsymbol{g}^*$, are themselves distinct. For let j be a suffix for which $g_j \neq g_j^*$ and hence $|g_j - g_j^*| \geqq 1$. Then both for $j \leqq r_1$ and for $j > r_1$,

$$|\alpha^{(j)}-\alpha^{*(j)}| \geqq 2nC \cdot 1 \cdot \lambda(\mathfrak{q}^{(j)})-2\frac{nC}{2}\lambda(\mathfrak{q}^{(j)}) > 0.$$

By means of our construction we have thus obtained $(2\tau+1)^n$ distinct solutions of the inequalities (35), and so we have proved the assertion.

13.

If x is a real variable, let as usual

$$\operatorname{sgn} x = +1 \text{ if } x > 0, \quad \operatorname{sgn} 0 = 0, \quad \text{and} \quad \operatorname{sgn} x = -1 \text{ if } x < 0.$$

THEOREM 4. *If $\lambda(\mathfrak{p})$ is any ceiling such that*

$$\lambda(\mathfrak{q}) \neq 1 \text{ for all } \mathfrak{q},$$

then there exists an element $\vartheta \neq 0$ of K for which

$$\operatorname{sgn}(|\vartheta|_{\mathfrak{p}}-1) = \operatorname{sgn}(\lambda(\mathfrak{p})-1) \text{ for all } \mathfrak{p}.$$

PROOF. Denote by l so large a positive integer that

$$\text{for every } \mathfrak{q} \text{ either } \lambda(\mathfrak{q})^l > C^n \text{ or } \lambda(\mathfrak{q})^l < C^{-n}.$$

The powers

$$\lambda(\mathfrak{p})^{ls}, \qquad s = 1, 2, 3, \cdots,$$

are again ceilings; for each s denote by $\alpha_1(ls), \cdots, \alpha_n(ls)$ a λ^{ls}-basis.

By Theorem 2, all the quotients

$$\frac{\alpha_k(ls)}{\alpha_1(ls)}, \qquad k = 2, 3, \cdots, n,$$

lie in the finite set M. Hence the system of these $n-1$ quotients has only finitely many possibilities, and there exist two positive integers s and t such that

$$s > t \geqq 1, \quad \frac{\alpha_k(ls)}{\alpha_1(ls)} = \frac{\alpha_k(lt)}{\alpha_1(lt)} \quad \text{for } k = 2, 3, \cdots, n.$$

Put

$$\vartheta = \frac{\alpha_1(ls)}{\alpha_1(lt)}.$$

Then $\vartheta \neq 0$ lies in K, and

$$\alpha_k(ls) = \vartheta\alpha_k(lt) \qquad (k = 1, 2, \cdots, n). \tag{39}$$

As before, denote by $\mathfrak{a}_\lambda$ the finite divisor belonging to $\lambda(\mathfrak{p})$. Then $\mathfrak{a}_\lambda^{ls}$ and $\mathfrak{a}_\lambda^{lt}$ are the analogous finite divisors that belong to $\lambda(\mathfrak{p})^{ls}$ and $\lambda(\mathfrak{p})^{lt}$, respectively. Since as ideals

$$[\mathfrak{a}_\lambda^{ls}] = (\alpha_1(ls), \cdots, \alpha_n(ls)) \quad \text{and} \quad [\mathfrak{a}_\lambda^{lt}] = (\alpha_1(lt), \cdots, \alpha_n(lt)),$$

the principal ideal (ϑ) satisfies the equation

$$[\mathfrak{a}_\lambda^{ls}] = (\vartheta)[\mathfrak{a}_\lambda^{lt}]$$

and hence also the equation

$$(\vartheta) = [\mathfrak{a}_\lambda^{l(s-t)}].$$

It follows therefore that

$$|\vartheta|_\mathfrak{r} = \lambda(\mathfrak{r})^{l(s-t)} \qquad \text{for all } \mathfrak{r},$$

whence

$$\operatorname{sgn}(|\vartheta|_\mathfrak{r} - 1) = \operatorname{sgn}(\lambda(\mathfrak{r}) - 1) \qquad \text{for all } \mathfrak{r}. \tag{40}$$

Next, for all $\mathfrak{q}$,

$$C^{-(n-1)}\lambda(\mathfrak{q})^{ls} \leqq |\alpha_k(ls)|_\mathfrak{q} \leqq C\lambda(\mathfrak{q})^{ls}, \quad C^{-(n-1)}\lambda(\mathfrak{q})^{lt} \leqq |\alpha_k(lt)|_\mathfrak{q} \leqq C\lambda(\mathfrak{q})^{lt} \qquad (k = 1, 2, \cdots, n),$$

hence, by (39),

$$C^{-n}\lambda(\mathfrak{q})^{l(s-t)} \leqq |\vartheta|_\mathfrak{q} \leqq C^n\lambda(\mathfrak{q})^{l(s-t)} \qquad \text{for all } \mathfrak{q}.$$

If $\lambda(\mathfrak{q}) > 1$, then $\lambda(\mathfrak{q})^l > C^n$ and hence

$$|\vartheta|_\mathfrak{q} \geqq C^{-n}\lambda(\mathfrak{q})^l > 1;$$

if, however, $\lambda(\mathfrak{q}) < 1$, then $\lambda(\mathfrak{q})^l < C^{-n}$ and therefore

$$|\vartheta|_\mathfrak{q} \leqq C^n\lambda(\mathfrak{q})^l < 1.$$

Thus, in either case,

$$\operatorname{sgn}(|\vartheta|_\mathfrak{q} - 1) = \operatorname{sgn}(\lambda(\mathfrak{q}) - 1) \qquad \text{for all } \mathfrak{q}. \tag{41}$$

The assertion of the theorem is contained in (40) and (41).

14.

Let

$$S = \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{s+1}\}, \qquad \text{where } s \geqq 1,$$

be a finite set of distinct prime divisors which, in particular, contains all infinite prime divisors. From the definition of a ceiling it is obvious that for all suffixes $\sigma = 1, 2, \cdots, s$ there exists a ceiling, $\lambda_\sigma(\mathfrak{p})$ say, with the following properties.

(a) $$\lambda_\sigma(\mathfrak{p}_\sigma) > 1.$$

(b) $$\lambda_\sigma(\mathfrak{p}) < 1 \text{ if } \mathfrak{p} \in S, \mathfrak{p} \neq \mathfrak{p}_\sigma.$$

(c) $$\lambda_\sigma(\mathfrak{p}) = 1 \text{ if } \mathfrak{p} \notin S.$$

Denote by ϑ_σ a field element given by Theorem 4 for the ceiling $\lambda_\sigma(\mathfrak{p})$. Thus

$$|\vartheta_\sigma|_{\mathfrak{p}_\sigma} > 1; \quad |\vartheta_\sigma|_{\mathfrak{p}} < 1 \text{ if } \mathfrak{p} \in S, \quad \mathfrak{p} \neq \mathfrak{p}_\sigma; \quad |\vartheta_\sigma|_{\mathfrak{p}} = 1 \text{ if } \mathfrak{p} \notin S.$$

It follows then from a theorem by Minkowski (see e.g. Hasse 1963, § 28) that the regulator

$$\begin{vmatrix} \log|\vartheta_1|_{\mathfrak{p}_1}, \cdots, \log|\vartheta_s|_{\mathfrak{p}_1} \\ \vdots \qquad\qquad \vdots \\ \log|\vartheta_1|_{\mathfrak{p}_s}, \cdots, \log|\vartheta_s|_{\mathfrak{p}_s} \end{vmatrix}$$

does not vanish. Hence no relation

$$\vartheta_1^{x_1} \cdots \vartheta_s^{x_s} = 1$$

with rational integral exponents $x_1, \cdots, x_n$ not all zero can hold.

In the special case when S consists only of the infinite prime divisors, this result contains the main part of Dirichlet's unit theorem: There are $r = r_\infty - 1$ independent units in K. In the general case the result just proved is due to Artin and Whaples (1945).

15.

Let $\lambda(\mathfrak{p})$, $\mu(\mathfrak{p})$, and $\nu(\mathfrak{p})$ be three ceilings connected by the equation

$$\nu(\mathfrak{p}) = \lambda(\mathfrak{p})\mu(\mathfrak{p}),$$

and let $\mathfrak{a}_\lambda$, $\mathfrak{a}_\mu$, and $\mathfrak{a}_\nu$ be the corresponding finite divisors. Then

$$\mathfrak{a}_\nu = \mathfrak{a}_\lambda \mathfrak{a}_\mu \quad \text{and} \quad [\mathfrak{a}_\nu] = [\mathfrak{a}_\lambda][\mathfrak{a}_\mu].$$

Denote by $\beta_1, \cdots, \beta_n$ and $\gamma_1, \cdots, \gamma_n$ a μ-basis and a ν-basis, respectively, and by

$$\beta = (\beta_1, \cdots, \beta_n)' \quad \text{and} \quad \gamma = (\gamma_1, \cdots, \gamma_n)'$$

the two column vectors of which these bases form the components.

Since the components of both β and γ are linearly independent over the rational field, there exists a unique matrix

$$U = (u_{hk})$$

with rational elements such that

$$\gamma_h = \sum_{k=1}^{n} u_{hk}\beta_k \qquad (h = 1, 2, \cdots, n), \tag{42}$$

or in matrix form,

$$\gamma = U\beta.$$

The matrix U is non-singular, i.e. its determinant

$$u = \det U$$

does not vanish. For from (42),

$$N(\mathfrak{a}_\nu) = |u| N(\mathfrak{a}_\mu),$$

whence

$$|u| = \frac{N(\mathfrak{a}_\nu)}{N(\mathfrak{a}_\mu)} = N(\mathfrak{a}_\lambda) \neq 0. \tag{43}$$

16.

We can further obtain some information about the single elements u_{hk} of U. Denote by a the smallest positive integer such that

$$a\mathfrak{a}_\lambda, = \mathfrak{a} \text{ sav},$$

is an integral divisor. Then

$$a\mathfrak{a}_\nu = \mathfrak{a}\mathfrak{a}_\mu, \quad [a\mathfrak{a}_\nu] = [\mathfrak{a}][\mathfrak{a}_\mu]$$

and hence

$$[a\mathfrak{a}_\nu] \text{ is a subset of } [\mathfrak{a}_\mu].$$

There exists then an $n \times n$ matrix

$$V = (v_{hk})$$

with rational *integral* elements such that

$$a\gamma_h = \sum_{k=1}^{n} v_{hk}\beta_k \qquad (h = 1, 2, \cdots, n).$$

On comparing this formula with (42) and remembering that U is unique, it follows that

$$aU = V \textit{ is a matrix with rational integral elements.} \tag{44}$$

Next, on changing over to the conjugates, the formulae (42) imply that

$$\gamma_h^{(j)} = \sum_{k=1}^{n} u_{hk}\beta_k^{(j)} \qquad (h, j = 1, 2, \cdots, n).$$

For fixed h, this is a system of n linear equations for

$$u_{h1}, u_{h2}, \cdots, u_{hn}$$

with the determinant

$$\Delta_0 = \begin{vmatrix} \beta_1^{(1)}, \cdots, \beta_n^{(1)} \\ \vdots \qquad\quad \vdots \\ \beta_1^{(n)}, \cdots, \beta_n^{(n)} \end{vmatrix} = d(\beta_1, \cdots, \beta_n)^{\frac{1}{2}} = N(\mathfrak{a}_\mu)\sqrt{d}. \tag{45}$$

Therefore, by Cramér's rule,

$$u_{hk} = \frac{\Delta_{hk}}{\Delta_0} \tag{46}$$

where Δ_{hk} denotes the determinant which is obtained from Δ_0 on replacing the h-th column of the latter determinant by the new column

$$\gamma_k^{(1)}, \cdots, \gamma_k^{(n)}$$

Now, by Theorem 1,

$$|\beta_k^{(j)}| \leqq C\mu(\mathfrak{q}^{(j)}), \quad |\gamma_k^{(j)}| \leqq C\nu(\mathfrak{q}^{(j)}) = C\lambda(\mathfrak{q}^{(j)})\mu(\mathfrak{q}^{(j)}).$$

Hence, on developing Δ_{hk} into a sum of $n!$ terms,

$$|\Delta_{hk}| \leqq n! C^n \Big(\prod_{\mathfrak{q}} \mu(\mathfrak{q})^{n\mathfrak{q}}\Big) \max_{\mathfrak{q}} \lambda(\mathfrak{q}).$$

Here

$$\prod_{\mathfrak{q}} \mu(\mathfrak{q})^{n\mathfrak{q}} = \mathfrak{Q}_\mu = N(\mathfrak{a}_\mu),$$

so that by (45) and (46),

$$|u_{hk}| \leqq \frac{n! C^n}{|d|^{\frac{1}{2}}} \max_{\mathfrak{q}} \lambda(\mathfrak{q}) \qquad (h, k = 1, 2, \cdots, n). \tag{47}$$

The properties (43), (44), and (47) enable us to find all possible matrices U; in particular, we obtain upper bounds for both the numerators and the denominators of the elements u_{hk} of U where these bounds depend only on the ceiling $\lambda(\mathfrak{p})$. We therefore arrive at the following result.

THEOREM 5. *To every ceiling $\lambda(\mathfrak{p})$ there exists a finite set*

$$S_\lambda = \{U^{(1)}, U^{(2)}, \cdots, U^{(L)}\}$$

of matrices $U^{(l)} = (u_{hk}^{(l)})$ with rational elements, all of the determinants $\mp N(\mathfrak{a}_\lambda)$, which have the following property.

If $\mu(\mathfrak{p})$ and $\nu(\mathfrak{p})$ are any two ceilings satisfying the relation

$$\nu(\mathfrak{p}) = \lambda(\mathfrak{p})\mu(\mathfrak{p}),$$

and if $\beta_1, \cdots, \beta_n$ and $\gamma_1, \cdots, \gamma_n$ are a μ-basis and a ν-basis, respectively, then

$$\gamma_h = \sum_{k=1}^{n} u_{hk}^{(l)} \beta_k \qquad (h = 1, 2, \cdots, n),$$

where $U^{(l)} = (u_{hk}^{(l)})$ is some element of S_λ.

17.

As an application of Theorem 5, consider the infinite sequence of ceilings

$$\lambda_l(\mathfrak{p}) = \lambda_0(\mathfrak{p})\mu(\mathfrak{p})^l \qquad (l = 0, 1, 2, \cdots), \tag{48}$$

where $\lambda_0(\mathfrak{p})$ and $\mu(\mathfrak{p})$ are two fixed ceilings. For every suffix l denote by $\alpha_{l,1}, \cdots, \alpha_{l,n}$ an arbitrary λ_l-basis, and by

$$U_l = (u_{l,hk}) \qquad (l = 0, 1, 2, \cdots)$$

the uniquely determined $n \times n$ matrix with rational elements for which

$$\alpha_{l+1,h} = \sum_{k=1}^{n} u_{l,hk}\alpha_{l,k} \qquad (h = 1, 2, \cdots, n). \tag{49}$$

By Theorem 5, the sequence of matrices

$$U_0, U_1, U_2, \cdots \tag{50}$$

consists then of only finitely many distinct elements, and these lie in a finite set which depends only on $\mu(\mathfrak{p})$ and not on $\lambda_0(\mathfrak{p})$. In the special case when

$$\lambda_0(\mathfrak{r}) = \mu(\mathfrak{r}) = 1 \qquad \text{for all } \mathfrak{r},$$

this result goes back to Minkowski (1899).

Minkowski also decided in this special case for which fields K the matrix chain (50) can be periodic; by this we mean that there exist two positive integers L and L' such that

$$U_{l+L} = U_l \qquad \text{for } l \geqq L'.$$

In the general case I solved this problem in my paper (Mahler 1937) by proving (in a slightly different notation) the following theorem.

In order that to the sequence (48) *of ceilings there exist a sequence of* λ_l*-bases* $\alpha_{l,1}, \cdots, \alpha_{l,n}$ *for which the sequence* (50) *of matrices is periodic, it is necessary and sufficient that the ceiling* $\mu(\mathfrak{q})$ *be principal.*

I also showed in this paper that to every ceiling $\mu(\mathfrak{p})$ there exist principal ceilings that are arbitrarily close to some integral power of $\mu(\mathfrak{p})$.

References

E. Artin, 1959, *Theory of algebraic numbers*, Mathematisches Institut, Göttingen.
E. Artin & G. Whaples, 1945, *Bull. Am. Math. Soc.* **51**, 469–492.
J. W. S. Cassels, 1959, *An introduction to the geometry of numbers*, Springer-Verlag, Berlin.
H. Hasse, 1963, *Zahlentheorie*, Akademie-Verlag, Berlin.
S. Lang, 1964, *Algebraic numbers*, Addison-Wesley Publishing Co., Reading, Mass.
K. Mahler, 1937, *Acta Mathematica* **68**, 109–144.

K. Mahler, 1938, *Proc. Koninkl. Akad. Wetensch. Amsterdam*, **41**, 634—637.
O. T. O'Meara, 1963, *Introduction to quadratic forms*, Springer Verlag, Berlin.
H. Minkowski, 1899, *Nachr. Ges. Wiss. Göttingen*, 64—66.
B. L. v. d. Waerden, 1956, *Acta Mathematica* **96**, 265—309.
H. Weyl, 1942, *Proc. London Math. Soc.* **47**, 268—289.

Mathematics Department,
Institute of Advanced Studies,
Australian National University,
Canberra, A.C.T., 28 April, 1964.