THEORY OF REDUCTION FOR ARITHMETICAL EQUIVALENCE. II[1]

BY

HERMANN WEYL

1. **Introduction. Lattices over the unit lattice.** Given n linearly independent vectors $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ in an n-dimensional vector space E^n, the formula

$$\mathfrak{x} = y_1\mathfrak{b}_1 + \cdots + y_n\mathfrak{b}_n \tag{1}$$

yields all vectors of the space E^n or of a lattice $\mathfrak{L}$ in E^n if the coordinates y_i range over all real numbers or all integers, respectively. We take the viewpoint that the lattice $\mathfrak{L}$ is given but the choice of its basis arbitrary. The several bases are connected with one another by unimodular transformations. If $f(\mathfrak{x})$ is a gauge function assigning a "length" $f(\mathfrak{x})$ to each vector $\mathfrak{x}$ the problem of reduction requires normalization of the lattice basis in terms of the given f. A solution is sought for all possible gauge functions or at least for some important class. The most significant class is obtained by running f^2 over all positive quadratic forms.

Following in Dirichlet's and Hermite's footsteps, Minkowski developed such a method of reduction for quadratic forms and established the decisive facts about it. In R1 I approached the same problem in that geometric way which Minkowski had initiated but then abandoned for unknown reasons.

The question may be put in a slightly different form. All linear mappings of E^n carrying $\mathfrak{L}$ into itself carry $f(\mathfrak{x})$ into equivalent gauge functions. The task is to pick out by a universal rule in each class of equivalent gauge functions one particular $f(\mathfrak{x})$ which is called the reduced function of its class. Let $\mathfrak{R}_0$, $\mathfrak{R}$, $\mathfrak{C}$ in the future denote the fields of all rational, real and complex numbers, respectively. Complex numbers are written in the form $\xi = x_0 + x_1 i$ (x_0, x_1 real). It is convenient to insert between the full vector space and the lattice $\mathfrak{L}$, the set E_0^n of all vectors (1) with *rational* coefficients y_i, a set which we describe as an n-dimensional vector space over $\mathfrak{R}_0$. Crystallography has found this advisable in distinguishing between the macroscopic and atomistic symmetries of a crystal, and in the theory of algebraic numbers one puts the *field* before the *ring* of its integers.

Let a lattice $\mathfrak{L}$ in E_0^n be given. With respect to any basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of E_0^n, formula (1), the function $f(\mathfrak{x})$ is represented by a function $g(y_1, \cdots, y_n)$ and the lattice $\mathfrak{L}$ by a "numerical lattice" Λ whose vectors are n-uples $(y_1, \cdots, y_n)$

Presented to the Society, January 1, 1941; received by the editors December 11, 1940.

(1) The first part, which appeared under the same title in these Transactions, vol. 48 (1940), pp. 126–164, is cited as R1.

of rational numbers. (Only if $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ is a true basis of $\mathfrak{L}$ will Λ be the unit lattice I whose elements are the n-uples of integers.) Hence $f(\mathfrak{x})$ with respect to $\mathfrak{L}$ is represented by g/Λ. All representations g/Λ of $f(\mathfrak{x})/\mathfrak{L}$ are equivalent, i.e., they arise from one another by linear transformations of the coordinates with rational coefficients. In each class of equivalent g/Λ we are to pick one individual, the "reduced" g/Λ. Suppose we have succeeded in doing this by some universal rule. We then have to select, for each Λ that may occur in a reduced g/Λ, a definite basis $\mathfrak{b}_1^*, \cdots, \mathfrak{b}_n^*$ in terms of which $\mathfrak{L}$ is represented by Λ. The equation

$$f^*(\mathfrak{x}) = g(y_1, \cdots, y_n) \quad \text{for} \quad \mathfrak{x} = y_1\mathfrak{b}_1^* + \cdots + y_n\mathfrak{b}_n^*$$

then defines the reduced gauge function f^* in its class. By the first step of reducing g/Λ no essential progress has been made unless the lattices Λ which may occur in a reduced g/Λ are limited to a finite number of possibilities. For only then is the selection of a basis $\mathfrak{b}_1^*, \cdots, \mathfrak{b}_n^*$ for each of these Λ essentially simpler than the original problem.

The Dirichlet-Hermite-Minkowski method of reduction by admitting only bases $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of $\mathfrak{L}$ always represents $\mathfrak{L}$ by the one lattice $\Lambda = \mathrm{I}$, the unit lattice. Thus it provides the ideal solution. Minkowski's construction of consecutive shortest distances in the lattice

$$f(\mathfrak{b}_1) = M_1, \cdots, f(\mathfrak{b}_n) = M_n$$

(for which he obtains the inequality $M_1 \cdots M_n V \leqq 2^n$) falls under our more general scheme. That theorem which he describes as indicating a certain "Oekonomie der Strahldistancen" states exactly that there is only an *a priori* limited number of possibilities for Λ with which to count in a reduced g/Λ. In R1 I carried the first method over to those other fields and quasi-fields which have not more than one infinite prime spot, and I found that it works only under the hypothesis that the class number for ideals is 1. Simultaneously Siegel observed that the rougher second method, by which incidentally Minkowski had proved that the class number of positive quadratic forms with *integral* coefficients and a given discriminant is finite, operates without this restrictive hypothesis(2). I add the remark that an argument making no use of the bases of a lattice need not even assume their existence. In an algebraic number field $\mathfrak{F}$ we consider any "order" $[\mathfrak{F}]$; in general there are several classes of lattices belonging to this order. The theory is limited neither to the principal class nor to the principal order. Following a suggestion by Siegel, P. Humbert generalized the investigation of quadratic forms to an arbitrary algebraic number field $\mathfrak{F}$ with several infinite prime spots(2). No doubt the whole problem thereby loses much of its simplicity. But once upon this track one ought to include the quaternions and thus deal also with those noncom-

(2) See P. Humbert, Commentarii Mathematici Helvetici, vol. 12 (1939–1940), pp. 263–306.

mutative division algebras of finite degree over $\mathfrak{R}_0$ for which the concept of infinite prime spots goes through. I resume here the rougher method of reduction with these further generalizations by the same geometric approach as in R1. I am not only interested in the fact that certain numbers are finite; I wish to ascertain reasonably low explicit upper bounds for them. The geometric method yields good results in this regard.

Before concluding this introduction I remind the reader of some simple facts about lattices in E_0^n. A vector $\mathfrak{x}$ in E_0^n is defined as an n-uple $(x_1, \cdots, x_n)$ of rational numbers. The unit vectors $\mathfrak{e}_k = (e_{1k}, \cdots, e_{nk})$ are the columns of the unit matrix $\|e_{ik}\|$. The word lattice means any set of vectors such that $\mathfrak{a} - \mathfrak{b}$ is contained in the set every time $\mathfrak{a}$ and $\mathfrak{b}$ are. We assume that the lattice is n-dimensional, i.e., contains n linearly independent vectors; and discrete, i.e., we require that for any given positive integer q there are not more than a finite number of lattice vectors satisfying the inequalities

$$|x_1| \leqq q, \cdots, |x_n| \leqq q.$$

From now on the term lattice refers only to discrete lattices which have the full dimensionality of their vector space. By a familiar argument one shows that one can find n linearly independent vectors $\mathfrak{l}_1, \cdots, \mathfrak{l}_n$ in a given lattice $\mathfrak{L}$ such that every lattice vector

$$\mathfrak{x} = u_1\mathfrak{l}_1 + \cdots + u_n\mathfrak{l}_n$$

has integral components u_i. By the same construction one adapts the basis $\mathfrak{l}_1, \cdots, \mathfrak{l}_n$ of any lattice Λ containing the unit lattice I to the basis $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$ of I:

$$\begin{aligned}
\mathfrak{e}_1 &= c_1\mathfrak{l}_1, \\
\mathfrak{e}_2 &= c_{21}\mathfrak{l}_1 + c_2\mathfrak{l}_2, \\
&\cdots\cdots\cdots\cdots, \\
\mathfrak{e}_n &= c_{n1}\mathfrak{l}_1 + \cdots + c_{n,n-1}\mathfrak{l}_{n-1} + c_n\mathfrak{l}_n.
\end{aligned}$$

The integers c_k are positive and the integral skew coefficients c_{ki} $(i<k)$ may be normalized by

$$0 \leqq c_{ki} < c_i \qquad (k = i+1, \cdots, n);$$

then $(\mathfrak{l}_1, \cdots, \mathfrak{l}_n)$ is uniquely determined. The index $j = [\Lambda : \mathrm{I}]$, i.e., the number of vectors in Λ which are incongruent modulo I, equals $c_1 \cdots c_n$. Let $\Lambda^{(k)}$ denote the part of Λ lying in the linear subspace $x_{k+1} = \cdots = x_n = 0$. The index $j_k = [\Lambda^{(k)} : \mathrm{I}^{(k)}]$ equals $c_1 \cdots c_k$. Hence these two lemmas:

LEMMA 1. *j_k is a divisor of j_h for $k<h$.*

LEMMA 2. *The number $h_n(j)$ of different lattices Λ over I of given index $j = [\Lambda : \mathrm{I}]$ is finite.*

Indeed, it equals the sum

$$\sum c_1^{n-1} c_2^{n-2} \cdots c_n^{0}$$

extended over all factorizations $c_1 c_2 \cdots c_n = j$ of j. (Incidentally, the numbers $h_n(j)$ for $j = 1, 2, \cdots$ have as their generating function the Dirichlet series

$$\sum_{j=1}^{\infty} h_n(j) \cdot j^{-s} = \zeta(s)\zeta(s-1) \cdots \zeta(s-n+1)$$

convergent in the half-plane $\Re s > n$.)

2. **Vector space and lattice over an algebraic field.** Let $\mathfrak{J}$ be any field of finite degree f over $\mathfrak{R}_0$. By carefully putting all factors in their proper places we shall see to it that all arguments and formulas in this and the following two sections remain valid for any division algebra, whether commutative or not, of finite degree over $\mathfrak{R}_0$. We choose a basis $\sigma_1, \cdots, \sigma_f$ of $\mathfrak{J}/\mathfrak{R}_0$ so that each number ξ of $\mathfrak{J}$ is uniquely represented by

$$\xi = x_1\sigma_1 + \cdots + x_f\sigma_f \qquad (x_a \text{ rational}). \tag{2}$$

Any n-uple $(\xi_1, \cdots, \xi_n)$ of numbers ξ_i in $\mathfrak{J}$ is a vector of the n-dimensional vector space E^n over $\mathfrak{J}$. The fundamental operations are addition of two vectors, $\mathfrak{x} + \mathfrak{x}'$, and multiplication $\delta\mathfrak{x}$ of a vector $\mathfrak{x}$ by a number δ (the numerical factor always in front of the vector!). Thus we may write

$$\mathfrak{x} = (\xi_1, \cdots, \xi_n) = \xi_1\mathfrak{e}_1 + \cdots + \xi_n\mathfrak{e}_n.$$

k linearly independent vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_k$ span a linear subspace $[\mathfrak{d}_1, \cdots, \mathfrak{d}_k]$ consisting of all vectors of the form $\eta_1\mathfrak{d}_1 + \cdots + \eta_k\mathfrak{d}_k$. Any n linearly independent vectors $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$ form a basis of $E^n/\mathfrak{J}$ in terms of which each vector is uniquely expressible as

$$\mathfrak{x} = \eta_1\mathfrak{d}_1 + \cdots + \eta_n\mathfrak{d}_n. \tag{3}$$

The original coordinates ξ_i are connected with the η_i by that nonsingular linear transformation D,

$$\xi_i = \sum_k \eta_k \delta_{ik}, \tag{4}$$

whose matrix $\|\delta_{ik}\|$ has for its columns the vectors $\mathfrak{d}_k = (\delta_{1k}, \cdots, \delta_{nk})$.

Expressing each component ξ_i in terms of the basis σ of $\mathfrak{J}$,

$$\xi_i = x_{i1}\sigma_1 + \cdots + x_{if}\sigma_f,$$

we identify $E^n/\mathfrak{J}$ with the (nf)-dimensional vector space E_0^{nf} over $\mathfrak{R}_0$. The rational numbers x_{ia} are the coordinates of $\mathfrak{x}$ with respect to the basis $\sigma_a\mathfrak{e}_i$. One has to distinguish between linear dependence in $\mathfrak{J}$ and in $\mathfrak{R}_0$.

We suppose we are given a lattice $\mathfrak{L}$ in E_0^{nf}. It will have a basis $\mathfrak{l}_\mu$

($\mu = 1, \cdots, nf$) in terms of which each vector $\mathfrak{x}$ of $\mathfrak{L}$,

$$\mathfrak{x} = \sum_{\mu} u_{\mu} \mathfrak{l}_{\mu} \tag{5}$$

has rational *integral* components u_{μ}. A number δ of $\mathfrak{J}$ is said to be a *multiplier* of $\mathfrak{L}$ if the operation $\mathfrak{x} \to \delta\mathfrak{x}$ carries each lattice vector $\mathfrak{x}$ into a lattice vector $\delta\mathfrak{x}$. The multipliers of $\mathfrak{L}$ form an *order* $[\mathfrak{J}]$. This assertion is meant to imply the following four properties(3):

1°. The number 1 is in $[\mathfrak{J}]$.

2°. $[\mathfrak{J}]$ is a ring.

3°. Any given number δ in $\mathfrak{J}$ may be multiplied by a positive rational integer m such that $m\delta$ is in $[\mathfrak{J}]$.

4°. Each number in $[\mathfrak{J}]$ is an integer.

1° and 2° are evident. To prove 3° and 4° we write

$$\delta\mathfrak{l}_{\mu} = \sum_{\nu} d_{\nu\mu}\mathfrak{l}_{\nu} \qquad (d_{\mu\nu} \text{ rational}).$$

If δ is any number and m a common denominator of the coefficients $d_{\mu\nu}$, then $m\delta$ is a multiplier. If δ happens to be a multiplier, then the $d_{\mu\nu}$ are rational integers and δ satisfies the equation

$$\left| \delta e_{\nu\mu} - d_{\nu\mu} \right| = 0.$$

In the same manner as for the "principal order" consisting of all integers of $\mathfrak{J}$ one proves(4) that any order $[\mathfrak{J}]$ is a discrete f-dimensional lattice in the f-dimensional vector space $\mathfrak{J}/\mathfrak{R}_0$, and hence has a basis $\sigma_1, \cdots, \sigma_f$ in terms of which every number ξ of $[\mathfrak{J}]$ appears in the form (2) with rational *integral* coefficients x_i.

The transformation D, (4), maps $\mathfrak{L}$ upon a lattice Λ: If $\mathfrak{x} = (\xi_1, \cdots, \xi_n)$ is in $\mathfrak{L}$, then $(\eta_1, \cdots, \eta_n)$ is in Λ, and *vice versa*. We call two lattices *equivalent* and admit them to the same *class* if one is carried into the other by a non-singular transformation D. The lattices Λ of one class express a given lattice $\mathfrak{L}$ in terms of different bases $(\mathfrak{d}_1, \cdots, \mathfrak{d}_n)$ of $E^n/\mathfrak{J}$. Obviously two equivalent lattices have the same multipliers.

A lattice $\mathfrak{L}$ is said to belong to the order $[\mathfrak{J}]$ if every number of that order is a multiplier of $\mathfrak{L}$. (For $n = 1$ this notion coincides with that of an ideal in $[\mathfrak{J}]$, and our classes of lattices with the classes of ideals.) Given an order $[\mathfrak{J}]$, the n-uples $(\xi_1, \cdots, \xi_n)$ of numbers ξ_i in $[\mathfrak{J}]$ form a lattice I which belongs to the order $[\mathfrak{J}]$; we call it the *unit lattice* for $[\mathfrak{J}]$. The lattices belonging to a given order $[\mathfrak{J}]$ are distributed over a number of classes, the class of I being the principal class.

(3) Notion and name are due to Dedekind. Hilbert in his Zahlbericht introduced the word "ring" for this purpose, but since ring has now acquired a wider meaning I revert, in agreement with such authorities as Artin and Chevalley, to Dedekind's terminology.

(4) Cf. H. Weyl, *Algebraic Theory of Numbers*, Princeton, 1940, pp. 145–146.

Let $\sigma_1, \cdots, \sigma_f$ be a basis of $[\mathfrak{J}]$ and $\mathfrak{l}_\mu$ $(\mu = 1, \cdots, nf)$ a basis of Λ. If Λ contains I the vectors $\sigma_a \mathfrak{e}_k$, which span I, are linear combinations of the $\mathfrak{l}_\mu$ with integral rational coefficients, and their absolute determinant, i.e., the absolute determinant of the transformation connecting the coordinates u_μ with the x_{ka} $(k = 1, \cdots, n; a = 1, \cdots, f)$ is the index $j = [\Lambda : \mathrm{I}]$.

Those vectors $(\xi_1, \cdots, \xi_n)$ in Λ for which $\xi_{k+1} = \cdots = \xi_n = 0$ form a lattice $\Lambda^{(k)}$ in the k-dimensional space $E^k/\mathfrak{J}$ with the coordinates $\xi_1, \cdots, \xi_k$. Considering Λ as a lattice in E_0^{nf} and using the arrangement

$$x_{11}, \cdots, x_{1f}; x_{21}, \cdots, x_{2f}; \cdots$$

of the coordinates in E_0^{nf} one can apply Lemma 1 to kf and $(k+1)f$ instead of k and h and thus one derives a corresponding proposition in $\mathfrak{J}$ instead of $\mathfrak{R}_0$:

LEMMA 3. *In the row of indices*

$$j_k = [\Lambda^{(k)} : \mathrm{I}^{(k)}] \qquad (k = 1, \cdots, n) \tag{6}$$

each number is a divisor of its successor.

The set of vectors $(\xi_1, \cdots, \xi_n)$ in Λ outside $[\mathfrak{e}_1, \cdots, \mathfrak{e}_{k-1}]$, i.e., for which $(\xi_k, \cdots, \xi_n) \neq (0, \cdots, 0)$, will be denoted Λ_k. Thus Λ_k and $\Lambda^{(k-1)}$ are complements in Λ.

We have seen that the number of different lattices Λ over a given lattice I with a given index $[\Lambda : \mathrm{I}] = j$ is finite, namely $h_{nf}(j)$. More exactly, one finds by the same argument that the number $H_f(j_1, \cdots, j_n)$ of different lattices Λ over I with given indices (6) has as its generating function the Dirichlet series of n variables $s_1, \cdots, s_n$:

$$\mathrm{Z}_f(s_1 + s_2 + \cdots + s_n - nf) \cdot \mathrm{Z}_f(s_2 + \cdots + s_n - (n-1)f) \cdots \mathrm{Z}_f(s_n - f) = \sum_{j_1, \cdots, j_n} H_f(j_1, \cdots, j_n) \cdot j_1^{-s_1} \cdots j_n^{-s_n}$$

where

$$\mathrm{Z}_f(s) = \zeta(s+1) \cdots \zeta(s+f).$$

Hence *a fortiori*:

LEMMA 4. *We have found upper bounds for the number of lattices Λ belonging to a given order $[\mathfrak{J}]$ which contain the unit vectors $\mathfrak{e}_1, \cdots, \mathfrak{e}_n$ and hence the unit lattice* I *for $[\mathfrak{J}]$ and which, moreover, have either a given index $j = [\Lambda : \mathrm{I}]$ or a given row of indices $j_1, \cdots, j_n$.*

3. **Preliminaries about reduction.** Suppose an order $[\mathfrak{J}]$ and a basis $\sigma_1, \cdots, \sigma_f$ of $[\mathfrak{J}]$ to be given. We consider a real-valued function

$$f(\mathfrak{x}) = f(\xi_1, \cdots, \xi_n)$$

which depends on a variable vector $\mathfrak{x}$ in $E^n/\mathfrak{J}$ and is positive except for $\mathfrak{x} = 0$, and we assume:

(i_0) For each positive q one can ascertain a positive q' such that the inequality $f(\mathfrak{x}) < q$ implies the nf inequalities

$$|x_{ia}| < q' \qquad (i = 1, \cdots, n;\ a = 1, \cdots, f) \tag{7}$$

for the components x_{ia} of the ξ_i.

Let $\mathfrak{L}$ be a lattice belonging to the fixed order $[\mathfrak{F}]$. n vectors $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of $\mathfrak{L}$ which are linearly independent with respect to $\mathfrak{F}$ constitute a semi-basis of $\mathfrak{L}$. Because of the discreteness of $\mathfrak{L}$ there is but a finite number of vectors $\mathfrak{x}$ in $\mathfrak{L}$ satisfying the inequalities (7). Hence Minkowski's construction of consecutive minima of f in $\mathfrak{L}$ is applicable. It yields a semi-basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of $\mathfrak{L}$ such that

$$f(\mathfrak{x}) \geqq f(\mathfrak{b}_k) = M_k$$

for every vector $\mathfrak{x}$ in $\mathfrak{L}$ outside $[\mathfrak{b}_1, \cdots, \mathfrak{b}_{k-1}]$ (*reduced semi-basis*). Obviously

$$M_1 \leqq M_2 \leqq \cdots \leqq M_n. \tag{8}$$

The mapping

$$\mathfrak{x} = \eta_1\mathfrak{b}_1 + \cdots + \eta_n\mathfrak{b}_n \rightarrow (\eta_1, \cdots, \eta_n) \tag{3}$$

carries $f(\mathfrak{x})$ into a function $g(\eta_1, \cdots, \eta_n)$ and $\mathfrak{L}$ into a lattice Λ which contains the unit lattice I for $[\mathfrak{F}]$. The function $g(\xi_1, \cdots, \xi_n)$ is *reduced with respect to* Λ, i.e.,

$$g(\xi_1, \cdots, \xi_n) \geqq g(e_{1k}, \cdots, e_{nk}) \tag{9}$$

whenever $(\xi_1, \cdots, \xi_n)$ is in Λ_k.

The M_k are uniquely determined by f and $\mathfrak{L}$; the situation is somewhat less favorable for $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$. Suppose $\mathfrak{b}_1', \cdots, \mathfrak{b}_n'$ is another set constructed according to our prescription. If M_k is actually lower than M_{k+1} then $[\mathfrak{b}_1', \cdots, \mathfrak{b}_k'] = [\mathfrak{b}_1, \cdots, \mathfrak{b}_k]$. (Analogues of Theorems 8 and 9 in R1.)

Being given n real numbers p_k,

$$1 \leqq p_1 \leqq \cdots \leqq p_n,$$

we say that the semi-basis $\mathfrak{b}_1', \cdots, \mathfrak{b}_n'$ of $\mathfrak{L}$ has the property $B(p_1, \cdots, p_n)$ if

$$f(\mathfrak{x}) \geqq \frac{1}{p_k} f(\mathfrak{b}_k')$$

for any vector $\mathfrak{x}$ in $\mathfrak{L}$ outside $[\mathfrak{b}_1', \cdots, \mathfrak{b}_{k-1}']$. Accordingly we ascribe the property $B(p_1, \cdots, p_n)$ to a function $g(\xi_1, \cdots, \xi_n)$ in conjunction with a lattice Λ over I if

$$g(\xi_1, \cdots, \xi_n) \geqq \frac{1}{p_k} \cdot g(e_{1k}, \cdots, e_{nk})$$

whenever $(\xi_1, \cdots, \xi_n)$ is in Λ_k.

If $\mathfrak{b}_k'$ is a semi-basis of $\mathfrak{L}$ with the property $B(p_1, \cdots, p_n)$, then

$$M_k' = f(\mathfrak{b}_k') \leqq p_k M_k.$$

(Analogue of Theorem 8_p.) Indeed, let $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ be a reduced semi-basis of $\mathfrak{L}$, $f(\mathfrak{b}_k) = M_k$. At least one of the k linearly independent vectors $\mathfrak{b}_1, \cdots, \mathfrak{b}_k$, say $\mathfrak{b}_i$, lies outside $[\mathfrak{b}_1', \cdots, \mathfrak{b}_{k-1}']$; hence

$$f(\mathfrak{b}_i) \geqq \frac{1}{p_k} \cdot f(\mathfrak{b}_k')$$

or

$$M_k' \leqq p_k M_i \leqq p_k M_k.$$

With the same notations I maintain that $[\mathfrak{b}_1', \cdots, \mathfrak{b}_k'] = [\mathfrak{b}_1, \cdots, \mathfrak{b}_k]$ provided $M_{k+1} > p_k M_k$. (Analogue of Theorem 9_p.) Proof: Suppose that one of the vectors $\mathfrak{b}_1', \cdots, \mathfrak{b}_k'$, say $\mathfrak{b}_i'$, is not in $[\mathfrak{b}_1, \cdots, \mathfrak{b}_k]$. Then

$$f(\mathfrak{b}_i') \geqq M_{k+1}.$$

Vice versa, if all k numbers $M_1', \cdots, M_k'$ are less than M_{k+1} then $\mathfrak{b}_1', \cdots, \mathfrak{b}_k'$ lie in $[\mathfrak{b}_1, \cdots, \mathfrak{b}_k]$. The observation that $M_i' \leqq p_i M_i \leqq p_k M_k$ finishes the proof.

The notation of *properly reduced* bases depends on a given multiplicative group U of numbers ϵ in $\mathfrak{J}$ and deals with functions f which satisfy the further condition:

(ii_0) $f(\epsilon \mathfrak{x}) = f(\mathfrak{x})$ (ϵ in U).

The semi-basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of $\mathfrak{L}$ is said to be properly reduced provided the inequality

$$f(\mathfrak{x}) > f(\mathfrak{b}_k)$$

holds with the sign $>$ for any vector $\mathfrak{x}$ of $\mathfrak{L}$ outside $[\mathfrak{b}_1, \cdots, \mathfrak{b}_{k-1}]$ except for the vectors of the special form

$$\mathfrak{x} = \epsilon \mathfrak{b}_k \qquad (\epsilon \text{ in } U).$$

Accordingly $g(\xi_1, \cdots, \xi_n)$ is properly reduced with respect to the lattice Λ over I if

$$g(\xi_1, \cdots, \xi_n) > g(e_{1k}, \cdots, e_{nk})$$

for all vectors $(\xi_1, \cdots, \xi_n)$ in Λ_k except the special vectors

$$\epsilon(e_{1k}, \cdots, e_{nk}) \qquad (\epsilon \text{ in } U).$$

With $\mathfrak{b}_k$ the vectors

$$\mathfrak{b}_k' = \epsilon_k \mathfrak{b}_k \qquad (\epsilon_k \text{ in } U)$$

form a reduced semi-basis of $\mathfrak{L}$ under the sole assumption that they lie in $\mathfrak{L}$.

Because $\mathfrak{x} = \epsilon_k \mathfrak{b}_k$ satisfies

$$f(\mathfrak{x}) = f(\mathfrak{b}_k), \quad \text{a fortiori} \quad f(\mathfrak{x}) \leqq f(\mathfrak{b}_k),$$

there is then, according to (i_0), only a finite number of possibilities for ϵ_k. We set

$$\eta_1 \mathfrak{b}_1 + \cdots + \eta_n \mathfrak{b}_n = \mathfrak{x} = \eta_1' \mathfrak{b}_1' + \cdots + \eta_n' \mathfrak{b}_n'$$

and denote by Λ, Λ' the corresponding images of $\mathfrak{R}$:

$$(\eta_1, \cdots, \eta_n) \quad \text{in } \Lambda \cdot \rightleftarrows \cdot \mathfrak{x} \quad \text{in } \mathfrak{R} \cdot \rightleftarrows \cdot (\eta_1', \cdots, \eta_n') \quad \text{in } \Lambda'.$$

The "special transformation"

$$\eta_k = \eta_k' \epsilon_k \qquad (\epsilon_k \text{ in } U) \tag{10}$$

carries Λ into Λ'. We count in the same *family* any two lattices Λ and Λ' arising from each other by such a special transformation. Given the lattice Λ over I there is only a finite number of special transformations such that the transformed lattice Λ' also contains I. In particular, the group $\{J_\Lambda\}$ of all special transformations J_Λ leaving Λ invariant is finite. If h is its degree, one has $\epsilon_k^h = 1$ $(k = 1, \cdots, n)$ for each J_Λ; hence the ϵ_k are roots of unity in $\mathfrak{J}$. The roots of unity in a field $\mathfrak{J}$ form a finite cyclic group; in particular, if $\mathfrak{J}$ has at least one real spot, the only such roots are ± 1. (However, in noncommutative division algebras the group of the roots of unity is, generally speaking, neither Abelian nor finite.)

The simple argument in R1, p. 136, shows:

If $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ *is a properly reduced semi-basis and* $\mathfrak{b}_1', \cdots, \mathfrak{b}_n'$ *any semi-basis of* $\mathfrak{R}$, *then the sequence of the values* $f(\mathfrak{b}_1), \cdots, f(\mathfrak{b}_n)$ *is lower than* $f(\mathfrak{b}_1'), \cdots, f(\mathfrak{b}_n')$. *If* $\mathfrak{b}_1', \cdots, \mathfrak{b}_n'$ *is reduced and* $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ *properly reduced, then*

$$\mathfrak{b}_1' = \epsilon_1 \mathfrak{b}_1, \cdots, \mathfrak{b}_n' = \epsilon_n \mathfrak{b}_n \qquad (\epsilon_i \text{ in } U).$$

4. **Extension to the ground field $\mathfrak{R}$. Minkowski's inequality.** So far the function $f(\mathfrak{x})$ has been defined merely for the vectors in the space $E^n/\mathfrak{J}$. In order to introduce geometry we assign to the variables x_a in (2) arbitrary *real* values:

$$\xi^* = x_1 \sigma_1 + \cdots + x_f \sigma_f. \tag{2*}$$

Sticking to the multiplication table of the basic elements σ_a, we thus extend $\mathfrak{J}/\mathfrak{R}_0$ to a commutative algebra $\mathfrak{J}^*$ over $\mathfrak{R}$. But only in the two cases treated in R1, where $\mathfrak{J}$ is $\mathfrak{R}_0$ itself or an imaginary quadratic field over $\mathfrak{R}_0$, is $\mathfrak{J}^*$ again a field. In general it is not. However, any n-uple $\mathfrak{x}^* = (\xi_1^*, \cdots, \xi_n^*)$ of elements ξ_i^* in $\mathfrak{J}^*$ may be considered as a vector in an (nf)-dimensional vector space E^{nf} over $\mathfrak{R}$ with the real coordinates x_{ia}:

$$\xi_i^* = x_{i1}\sigma_1 + \cdots + x_{if}\sigma_f.$$

We now assume $f(\mathfrak{x}^*)$ to be a *gauge function*, i.e., a continuous real-valued function in this space, having the following properties:

(i) $f(\mathfrak{x}^*) > 0$ except for $\mathfrak{x}^* = 0$.
(ii) $f(t\mathfrak{x}^*) = |t| \cdot f(\mathfrak{x}^*)$ for any real factor t.
(iii) $f(\mathfrak{x}_1^* + \mathfrak{x}_2^*) \leqq f(\mathfrak{x}_1^*) + f(\mathfrak{x}_2^*)$.

The gauge body

$$K: \quad f(\xi_1^*, \cdots, \xi_n^*) < 1$$

and also the solid qK defined by $f(\xi_1^*, \cdots, \xi_n^*) < q$ are bounded; hence postulate (i_0) of the previous section is fulfilled. Let V^* be the volume of K computed in terms of the coordinates x_{ia}.

Again we fix an order $[\mathfrak{F}]$ and a basis $\sigma_1, \cdots, \sigma_f$ of $[\mathfrak{F}]$. Let Λ be a lattice belonging to this order and containing the unit lattice I for $[\mathfrak{F}]$ and let $f(\xi_1, \cdots, \xi_n)$ be reduced with respect to Λ. The volume of K in terms of the coordinates u_μ as introduced by (5), i.e., measured against the fundamental parallelepiped of Λ, equals $V^* \cdot [\Lambda : \mathrm{I}]$. Hence by the simple argument explained in R1, p. 140, Minkowski's second inequality leads to this formula holding for a gauge function $f(\xi_1^*, \cdots, \xi_n^*)$ which is reduced with respect to Λ:

$$(M_1 \cdots M_n)^f \cdot V^* [\Lambda : \mathrm{I}] \leqq 2^{nf}$$

where

$$M_k = f(e_{1k}, \cdots, e_{nk}).$$

5. **Splitting. The number of reduced lattices is finite.** Up to now everything has worked for a division algebra of degree f over $\mathfrak{R}_0$ just as well as for a field $\mathfrak{F}$. Further progress depends on the structure of $\mathfrak{F}^*$. If $\mathfrak{F}$ is a field, then $\mathfrak{F}^*$ is isomorphic to the direct sum of a number of components $\mathfrak{R}$ and $\mathfrak{C}$. We first study this case.

The decomposition of $\mathfrak{F}^*$ is brought about by conjugation. One knows that $\mathfrak{F}/\mathfrak{R}_0$ has a determining number θ whose powers $1, \theta, \cdots, \theta^{f-1}$ constitute a basis for $\mathfrak{F}$. The number θ satisfies an irreducible equation in $\mathfrak{R}_0$ of degree f. Let θ^α and $\theta^\beta, \bar{\theta}^\beta$ (or in one row: $\theta^{(1)}, \cdots, \theta^{(f)}$) denote its r real and s pairs of complex conjugate roots. They define the f conjugations

$$\xi \to \xi^\alpha; \qquad \xi \to \xi^\beta, \qquad \xi \to \bar{\xi}^\beta$$

each of which projects $\mathfrak{F}$ isomorphically into $\mathfrak{R}$ or $\mathfrak{C}$. We use the notations

$$\xi^\alpha = x^\alpha, \qquad \xi^\beta = x_0^\beta + ix_1^\beta \qquad (\bar{\xi}^\beta = x_0^\beta - ix_1^\beta)$$

and call the $r+s$ numbers ξ^α, ξ^β the *splits*, and the f real numbers x^α; x_0^β, x_1^β

the *splitting coordinates* of ξ. The same applies to any element ξ^* of $\mathfrak{J}^*$. The product $\zeta^* = \xi^*\eta^*$ has the splits

$$\zeta^\alpha = \xi^\alpha\eta^\alpha, \qquad \zeta^\beta = \xi^\beta\eta^\beta.$$

The arithmetician speaks of the different values of the indices α and β as the r real and s imaginary (*infinite prime*) *spots* of $\mathfrak{J}$; for the sake of brevity we often drop the adjectives in parentheses. If a definite arrangement is desired, we write $\alpha = \alpha_1, \cdots, \alpha_r$; $\beta = \beta_1, \cdots, \beta_s$.

The splitting coordinates x^α; x_0^β, x_1^β are connected with the components $x_1, \cdots, x_f$ of ξ^* by the linear substitution

$$\Sigma = \|\sigma_1, \cdots, \sigma_f\| \tag{11}$$

where in the symbol on the right side each term stands for the column of its splitting coordinates (in a definite arrangement). The splitting of $\mathfrak{J}^*$ into r components $\mathfrak{R}$ and s components $\mathfrak{C}$ is established as soon as it is certain that the absolute determinant

$$\Delta = \text{abs.}\,|\,\sigma_1, \cdots, \sigma_f\,|$$

of the matrix Σ is different from zero. For the particular basis $1, \theta, \cdots, \theta^{f-1}$ one sees that $(-2i)^s \cdot \Delta$ is the Vandermonde determinant of $\theta^{(1)}, \cdots, \theta^{(f)}$, and hence indeed $\Delta \neq 0$. This fact carries over to any basis $\sigma_1, \cdots, \sigma_f$ of $\mathfrak{J}$.

The number in $\mathfrak{J}^*$ with the splitting coordinates x^α; x_0^β, $-x_1^\beta$ is denoted by $\bar{\xi}^*$. As absolute value $|\xi^*|$ we introduce the greatest of the $r+s$ numbers $|\xi^\alpha|$, $|\xi^\beta|$. One could agree on other definitions, but this one is most convenient for our future applications. What usually is called a *unit* in $\mathfrak{J}$ is a number of $\mathfrak{J}$ which is a unity at all *finite* prime spots. None but the infinite prime spots matter for our investigation; hence we take the liberty of using the term "*unit*" for those numbers ϵ of $\mathfrak{J}$ which are unities at all infinite prime spots, i.e., for which the $r+s$ equations $|\epsilon^\alpha| = 1$, $|\epsilon^\beta| = 1$ hold.

For any element δ^* of $\mathfrak{J}^*$ one introduces the real matrix $\|d_{ab}\|$ of the linear operation $\xi^* \to \xi^*\delta^*$ in $\mathfrak{J}^*$:

$$x_a \to \sum_b d_{ab}x_b \qquad \left(\sigma_a\delta^* = \sum_b d_{ba}\sigma_b\right)$$

and its characteristic polynomial

$$|\,te_{ab} - d_{ab}\,| = t^f - d_1t^{f-1} + \cdots \pm d_f.$$

d_1 and d_f are called trace (tr) and norm (Nm), respectively. In terms of the splitting coordinates our operation of multiplication splits into the transformations

$$x^\alpha \to x^\alpha d^\alpha; \qquad \xi^\beta \to \xi^\beta\delta^\beta,$$

each corresponding to a real or imaginary spot α or β. Of course, $\xi^\beta \to \xi^\beta \delta^\beta$ stands for

$$x_0^\beta \to x_0^\beta d_0^\beta - x_1^\beta d_1^\beta, \qquad x_1^\beta \to x_0^\beta d_1^\beta + x_1^\beta d_0^\beta.$$

Hence

$$\operatorname{tr}(\delta^*) = \sum_\alpha d^\alpha + 2\sum_\beta d_0^\beta,$$

$$\operatorname{Nm}(\delta^*) = \prod_\alpha d^\alpha \cdot \prod_\beta \{(d_0^\beta)^2 + (d_1^\beta)^2\}.$$

If $\delta^* = \delta$ is in $\mathfrak{J}$ the d_{ab} are rational numbers. For a unit ϵ in $\mathfrak{J}$ our formulas show that the determinant $\operatorname{Nm}(\epsilon)$ of the transformation $\xi^* \to \xi^* \epsilon$ is of absolute value 1 and hence as a rational number equal to ± 1.

Considering the trace $\operatorname{tr}(\xi^2)$ one readily verifies that $(2^\delta \Delta)^2$ is rational for any basis $\sigma_1, \cdots, \sigma_f$ and especially a rational integer for a basis of an order $[\mathfrak{J}]$.

The transformation (4) in E^{nf},

$$\xi_i^* = \sum_k \eta_k^* \delta_{ik} \qquad (\delta_{ik} \text{ numbers in } \mathfrak{J}) \tag{4}$$

splits into the components

$$\xi_i^\alpha = \sum_k \eta_k^\alpha \delta_{ik}^\alpha, \qquad \xi_i^\beta = \sum_k \eta_k^\beta \delta_{ik}^\beta,$$

each α-component involving n, each β-component $2n$ real variables:

$$\xi_k^\alpha = x_k^\alpha; \qquad \xi_k^\beta = x_{k0}^\beta + i x_{k1}^\beta.$$

How closely can one approximate an element ξ^* of $\mathfrak{J}^*$ by a number γ of our order $[\mathfrak{J}]$ with the basis $\sigma_1, \cdots, \sigma_f$? For an appropriate γ in $[\mathfrak{J}]$ the real components x_a' of $\xi^* - \gamma$,

$$\xi^* - \gamma = x_1' \sigma_1 + \cdots + x_f' \sigma_f,$$

will satisfy the inequalities $|x_a'| \leqq \frac{1}{2}$, and thus

$$|\xi^* - \gamma| \leqq \rho$$

where

$$\rho = \tfrac{1}{2} \cdot \max_{\alpha,\beta} (|\sigma_1^\alpha| + \cdots + |\sigma_f^\alpha|, \ |\sigma_1^\beta| + \cdots + |\sigma_f^\beta|).$$

The "circles" of radius ρ around all numbers γ of $[\mathfrak{J}]$ cover the whole $\mathfrak{J}^*$. (Such a radius was denoted by the letter r in R1, which now serves a different purpose.)

Let us now return to the situation explained at the end of the previous section and let V be the volume of K computed in terms of the splitting coordinates of $\xi_1^*, \cdots, \xi_n^*$. Then $V = V^*/\Delta^n$. Moreover we observe that

$f(\xi_1^*, \cdots, \xi_k^*, 0, \cdots, 0)$ is reduced with respect to the lattice $\Lambda^{(k)}$, and denoting by V_k the volume of the solid

$$f(\xi_1^*, \cdots, \xi_k^*, 0, \cdots, 0) < 1$$

in E^{kf} computed in terms of the splitting coordinates of $\xi_1^*, \cdots, \xi_k^*$, we obtain these fundamental inequalities for $M_k = f(e_{1k}, \cdots, e_{nk})$:

THEOREM I. *For a reduced* $f(\xi_1, \cdots, \xi_n)/\Lambda$ *one has*

$$(M_1 \cdots M_n)^f \cdot V[\Lambda : \mathrm{I}] \leqq (2^f\Delta)^n, \tag{12}$$

more generally

$$(M_1 \cdots M_k)^f \cdot V_k[\Lambda^{(k)} : \mathrm{I}^{(k)}] \leqq (2^f\Delta)^k. \tag{12$_k$}$$

At this point we introduce the further assumption:

(ii*) $f(\tau^*\mathfrak{x}^*) \leqq |\tau^*| \cdot f(\mathfrak{x}^*)$ (τ^* any element of $\mathfrak{J}^*$),

and henceforth the term "gauge function" is to be taken in this restricted sense. Following Minkowski's own argument, we then prove

THEOREM II. *For a reduced* $f(\xi_1, \cdots, \xi_n)/\Lambda$ *one always has*

$$j = [\Lambda : \mathrm{I}] \leqq (nf)! \left(\frac{4}{\pi}\right)^{ns} \cdot \left(\frac{\Delta}{f!}\right)^n \tag{13}$$

and more generally

$$j_k = [\Lambda^{(k)} : \mathrm{I}^{(k)}] \leqq (kf)! \left(\frac{4}{\pi}\right)^{ks} \left(\frac{\Delta}{f!}\right)^k \qquad (k = 1, \cdots, n). \tag{13$_k$}$$

Hence in any class of lattices belonging to the order $[\mathfrak{J}]$ there is always a lattice Λ which contains I and satisfies (13) and (13$_k$). Together with Lemma 2 this proves(5):

THEOREM III. *The number of classes of lattices belonging to a given order* $[\mathfrak{J}]$ *is finite.*

---

(5) This theorem is well known. We are concerned only with those lattices Λ over I which are in the class of $\mathfrak{L}$, but as our bounds (13) or the sharper bounds (35) depend on the order rather than on the special class it seemed worth while to mention Theorem III in passing. For a commutative field $\mathfrak{J}$ and its principal order $[\mathfrak{J}]$ E. Steinitz, Mathematische Annalen, vol. 71 (1912), pp. 328–354, and vol. 72 (1912), pp. 297–345, proved that the number for classes of any n is the same as for $n=1$, namely equal to the number of classes of ideals. See also I. Schur, Mathematische Annalen, vol. 71 (1912), pp. 355–367; W. Franz, Journal für die reine und angewandte Mathematik, vol. 171 (1934), pp. 149–161; C. Chevalley, *L'Arithmétique dans les Algèbres de Matrices*, Actualités Scientifiques et Industrielles, no. 323, 1936, in particular Theorems 3, 7 and 8.

(The proposition implies the corresponding one about classes of ideals.) Any gauge function will do for the proof, for instance

$$f(\xi_1^*, \cdots, \xi_n^*) = |\xi_1^*| + \cdots + |\xi_n^*|.$$

We shall soon see that much better upper bounds for the number of classes are obtained by using for f^2 the trace of a positive Hermitian form. However, our present Theorem II goes far beyond Theorem III because it deals with any gauge function f in conjunction with a lattice rather than with lattices alone.

Proof. Observe that the "octahedron"

$$|\xi_1^*| + \cdots + |\xi_n^*| < 1$$

contains no vector of Λ except the zero vector. Hence owing to Minkowski's chief inequality we find this upper bound for its volume W:

$$Wj \leqq (2^l\Delta)^n.$$

Let $(\xi_1, \cdots, \xi_n)$ be a vector in Λ and ξ_k be the last nonvanishing one among its coordinates ξ_i. Then by the definition of reduction

$$f(\xi_1, \cdots, \xi_n) \geqq M_k = f(e_{1k}, \cdots, e_{nk}). \tag{14}$$

On the other hand the assumptions (iii) and (ii*) imply

$$\begin{aligned} f(\xi_1 e_1 + \cdots + \xi_n e_n) &\leqq M_1|\xi_1| + \cdots + M_n|\xi_n| \\ &= M_1|\xi_1| + \cdots + M_k|\xi_k|. \end{aligned} \tag{15}$$

Because of (8) the relations (14) and (15) are incompatible unless

$$|\xi_1| + \cdots + |\xi_n| = |\xi_1| + \cdots + |\xi_k| \geqq 1.$$

We base our computation of W upon the following general remark about gauge functions f in an n-dimensional vector space over $\mathfrak{R}$. If V is the volume of the gauge body $K: f(\mathfrak{x}) < 1$, then the integral $\int$ of e^{-f} over the whole space equals $n!V$. One simply evaluates the integral by decomposing the space into the infinitely thin shells

$$q \leqq f(\mathfrak{x}) < q + dq$$

and thus finds

$$\int = V \cdot \int_0^\infty e^{-q} \cdot nq^{n-1} dq = n!V.$$

Applying this remark to the gauge function $|\xi_1^*| + \cdots + |\xi_n^*|$ in our (nf)-dimensional vector space and to the gauge function $|\xi^*|$ in the f-dimensional space $\mathfrak{F}^*$, one gets this double value for $\int$:

$$(nf)!W = (f!w)^n,$$

w being the volume of the "cylinder" defined by

$$|\xi^*| < 1, \qquad \text{or by} \quad |x^\alpha| < 1, \quad (x_0^\beta)^2 + (x_1^\beta)^2 < 1.$$

Therefore $w = 2^r\pi^s$.

(ii*) entails the property (ii$_0$) of §3, provided U is the group of units in our sense. From now on we shall abide by this convention and interpret the term "properly reduced" accordingly. Then the transformation $\xi^* \to \xi^* \cdot \epsilon$ (ϵ in U) and hence every special transformation (10) has the determinant ± 1 and thus the indices j_k for two lattices Λ and Λ' over I which are in the same family coincide: $j_k = j_k'$ for $k = 1, \cdots, n$.

The values γ^* of a *Hermitian form* in $\mathfrak{F}^*$,

$$\gamma^*(\mathfrak{x}^*) = \sum_{i,k} \xi_i^* \gamma_{ik}^* \bar{\xi}_k^* \qquad (\gamma_{ki}^* = \bar{\gamma}_{ik}^*) \tag{16}$$

are totally real in the sense that $\bar{\gamma}^* = \gamma^*$, or that even the β-splits $\gamma^\beta = g_0^\beta + ig_1^\beta = g^\beta$ of γ^* are real. What such a Hermitian form does is to associate a quadratic form $\{g_{ik}^\alpha\}$ with each real spot α and a Hermitian form $\{\gamma_{ik}^\beta\}$ with every imaginary spot β. The splits of $\gamma^*(\mathfrak{x}^*)$ are

$$g^\alpha = \sum_{i,k} x_i^\alpha g_{ik}^\alpha x_k^\alpha, \qquad g^\beta = \sum_{i,k} \xi_i^\beta \gamma_{ik}^\beta \bar{\xi}_k^\beta \tag{17}$$

where $x_i^\alpha = \xi_i^\alpha$ and ξ_i^β are the splits of ξ_i^*. The form $\gamma^*(\mathfrak{x}^*)$ is said to be positive if each of the r quadratic forms $\{g_{ik}^\alpha\}$ and each of the s Hermitian forms $\{\gamma_{ik}^\beta\}$ is positive definite.

We now apply our theory to the gauge function f introduced by

$$f^2 = \operatorname{tr}(\gamma^*(\mathfrak{x}^*)). \tag{18}$$

In terms of the splits (17) one has

$$f^2 = \sum_\alpha g^\alpha + 2\sum_\beta g^\beta. \tag{19}$$

The properties (i) to (iii) of §4 are readily verified; (ii*) is also fulfilled because of

$$f^2(\tau^*\mathfrak{x}^*) = \sum_\alpha |\tau^\alpha|^2 g^\alpha + 2\sum_\beta |\tau^\beta|^2 g^\beta.$$

6. **Quaternion algebra of totally positive norm over a totally real field.** Turning to noncommutative division algebras, we denote by $\mathfrak{Q}$ the quasi-field of quaternions

$$a = a_0 + a_1 i_1 + a_2 i_2 + a_3 i_3$$

whose components a_0, a_1, a_2, a_3 are arbitrary real numbers, and use the notations $\bar{a}$ and $|a|$ in the customary manner:

$$a\bar{a} = |a|^2 = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

For which of the noncommutative division algebras of finite degree over $\mathfrak{R}_0$ does the concept of infinite prime spots work in a way similar to that in the previous section for fields? I am going to describe one such situation without discussing the question whether or not it is the only one (though, as a matter of fact, it is).

Suppose we are given a field $\mathcal{E}$ of degree e over $\mathfrak{R}_0$ and two numbers ω_1, ω_2 in $\mathcal{E}$. We put $\omega_3 = \omega_1\omega_2$ and form the quaternion algebra $\mathcal{J}$ over $\mathcal{E}$ whose elements ξ are quadruples $(\xi_0, \xi_1, \xi_2, \xi_3)$ of numbers in $\mathcal{E}$,

$$\xi = \xi_0 + \xi_1\iota_1 + \xi_2\iota_2 + \xi_3\iota_3, \tag{20}$$

with this multiplication table for the unities $\iota_1, \iota_2, \iota_3$:

$$\iota_1^2 = -\omega_1, \qquad \iota_2^2 = -\omega_2, \qquad \iota_3^2 = -\omega_3;$$

$$\iota_1\iota_2 = -\iota_2\iota_1 = \iota_3, \qquad \iota_3\iota_1 = -\iota_1\iota_3 = \omega_1\iota_2, \qquad \iota_2\iota_3 = -\iota_3\iota_2 = \omega_2\iota_1.$$

The conjugate $\bar{\xi}$ is $\xi_0 - \xi_1\iota_1 - \xi_2\iota_2 - \xi_3\iota_3$ and

$$\xi\bar{\xi} = \xi_0^2 + \omega_1\xi_1^2 + \omega_2\xi_2^2 + \omega_3\xi_3^2.$$

If the equation

$$\xi_0^2 + \omega_1\xi_1^2 + \omega_2\xi_2^2 + \omega_3\xi_3^2 = 0 \tag{21}$$

has no solution $(\xi_0, \xi_1, \xi_2, \xi_3)$ in $\mathcal{E}$ except $(0, 0, 0, 0)$, then $\mathcal{J}$ is a division algebra of degree 4 over $\mathcal{E}$ and of degree $f = 4e$ over $\mathfrak{R}_0$. We assume $\mathcal{E}$ to be totally real (to have no imaginary infinite prime spot) and ω_1, ω_2 to be totally positive numbers in $\mathcal{E}$ (i.e., their e conjugates $\omega_1^\alpha, \omega_2^\alpha$ are all positive). Then the quadratic form of the variables $\xi_0, \xi_1, \xi_2, \xi_3$ at the left of (21) is positive definite in each conjugate $\mathcal{E}^\alpha$ of $\mathcal{E}$ and hence (21) has no solution except 0. Denoting as before by τ^α the conjugate of any number τ in $\mathcal{E}$ corresponding to the spot α of $\mathcal{E}$, we map (20) upon the element

$$\xi^\alpha = \xi_0^\alpha + \xi_1^\alpha(\omega_1^\alpha)^{1/2} \cdot i_1 + \xi_2^\alpha(\omega_2^\alpha)^{1/2} \cdot i_2 + \xi_3^\alpha(\omega_3^\alpha)^{1/2} \cdot i_3 \tag{22}$$

in $\mathfrak{Q}$. This "conjugation" is an isomorphic mapping and defines the "infinite quaternion prime spot" α of $\mathcal{J}$. (22) are the splits, and the $4e = f$ real numbers

$$x_0^\alpha = \xi_0^\alpha, \qquad x_1^\alpha = \xi_1^\alpha(\omega_1^\alpha)^{1/2}, \qquad x_2^\alpha = \xi_2^\alpha(\omega_2^\alpha)^{1/2}, \qquad x_3^\alpha = \xi_3^\alpha(\omega_3^\alpha)^{1/2}$$

are the "splitting coordinates," of ξ. Application to the elements ξ^*, equation (2*), of $\mathcal{J}^*$ is immediate.

There is only one thing to settle: The splitting coordinates $x_0^\alpha, x_1^\alpha, x_2^\alpha, x_3^\alpha$ arise from the components x_a by the substitution (11), each σ_a standing for

the column of its splitting coordinates. Is its determinant, whose absolute value will again be denoted by Δ, different from zero? To answer the question, let $(\tau_1, \cdots, \tau_e)$ be a basis of $\mathcal{E}$ and set $\Delta_0 = \text{abs.}|\tau_1, \cdots, \tau_e|$. From it we obtain the following basis of $\mathfrak{J}$:

$$\tau_a, \qquad \tau_a\iota_1, \qquad \tau_a\iota_2, \qquad \tau_a\iota_3 \qquad\qquad (a = 1, \cdots, e).$$

The Δ of this particular basis is given by

$$\Delta = \prod_{\alpha} (\omega_1^{\alpha}\omega_2^{\alpha})\cdot\Delta_0^4 = \text{Nm}\ \omega_3\cdot\Delta_0^4.$$

Thus $\Delta \neq 0$ for this and consequently for any basis.

Incidentally Δ is a rational number for any basis of $\mathfrak{J}$ and $4^e\cdot\Delta$ a rational integer if $\sigma_1, \cdots, \sigma_f$ is a basis of $[\mathfrak{J}]$. The characteristic equation of the multiplication $\xi^* \to \xi^*\cdot\delta$ considered as a linear operation in $\mathfrak{J}^*$ is the square of a polynomial (of degree $2e$), and so is the characteristic polynomial of the linear substitution (4) in E^{nf}.

The notion of unit and the absolute value $|\xi^*|$ of any element ξ^* of $\mathfrak{J}^*$ are introduced as before. The constant on the right side of (13_k) is to be changed into

$$(kf)!\left(\frac{32}{\pi^2}\right)^{ek}\left(\frac{\Delta}{f!}\right)^k.$$

As gauge functions f we employ in particular those whose square equals

$$\tfrac{1}{4}\ \text{tr}\ (\gamma^*) = \sum_{\alpha} g^{\alpha}$$

where γ^* is any positive Hermitian form (16) in $\mathfrak{J}^*$.

7. **The theorems of finiteness for quadratic forms.** After so many preliminaries which stake out the ground covered by our investigation, I now come to the core of the matter, which may be explained fairly completely by the simplest example $\mathfrak{J} = \mathfrak{R}_0$. Here we have only one order $[\mathfrak{J}]$ consisting of the ordinary integers $0, \pm 1, \pm 2, \cdots$ and only one class of lattices. For any given lattice Λ over I and any positive quadratic form

$$f^2(\mathfrak{x}) = \sum g_{ik}x_ix_k \qquad\qquad (g_{ki} = g_{ik})$$

the conditions of reduction read:

$$f^2(\mathfrak{x}) \geqq g_{kk} \qquad \text{whenever } \mathfrak{x} = (x_1, \cdots, x_n) \text{ is in } \Lambda_k.$$

Each of them is a linear inequality for the coefficients g_{ij}.

With the notation used in R1 we carry out Jacobi's transformation:

$$f^2 = q_1z_1^2 + \cdots + q_nz_n^2.$$

The volume V of the ellipsoid $f^2 < 1$ is given by

$$V^2 = \omega_n^2/q_1 \cdots q_n,$$

ω_n being the volume of the n-dimensional sphere. Hence the inequality (12),

$$M_1 \cdots M_n V[\Lambda:\mathrm{I}] \leqq 2^n, \tag{23}$$

turns into

$$g_{11} \cdots g_{nn}[\Lambda:\mathrm{I}]^2 \leqq (2^n/\omega_n)^2 \cdot q_1 \cdots q_n. \tag{24}$$

As Minkowski observed, (23) may be proved much more easily for quadratic forms than for an arbitrary gauge function. By an argument similar to the one employed in proving Theorem II we see that the ellipsoid

$$f'^2 = \frac{q_1}{M_1^2} z_1^2 + \cdots + \frac{q_n}{M_n^2} z_n^2 < 1$$

contains no lattice vector except zero. Hence its volume V' satisfies the inequality

$$V'[\Lambda:\mathrm{I}] \leqq 2^n, \quad \text{and} \quad V' = M_1 \cdots M_n \cdot V.$$

If κ_n is a number such that the part of space covered by impenetrable n-dimensional spheres in any lattice arrangement may never exceed the proportion $\kappa_n:1$ then we can even write $\kappa_n 2^n$ instead of 2^n and thus replace ω_n in (24) by $\pi_n = \omega_n/\kappa_n$. The most primitive choice is $\kappa_n = 1$; however, according to Blichfeldt's ingenious device([6]),

$$\kappa_n = (n+2) \cdot 2^{-1-n/2}$$

is a permissible and better value.

Making use of the inequalities

$$g_{ii} \geqq q_i$$

on the left side of (24) we get for the index $j = [\Lambda:\mathrm{I}]$ this upper bound

$$j \leqq 2^n/\pi_n \tag{25}$$

which is a considerable improvement over (13), $j \leqq n!$ For $n = 1, 2, 3$ it yields the result $j = 1$, to which the theory of reduction for binary and ternary forms owes its comparative simplicity.

For similar reasons

$$g_{11} \cdots g_{kk} \cdot j_k^2 \leqq (2^k/\pi_k)^2 \cdot q_1 \cdots q_k, \tag{24$_k$}$$

$$j_k \leqq 2^k/\pi_k \qquad (k = 1, \cdots, n). \tag{25$_k$}$$

Unless the lattice Λ satisfies the n inequalities (25$_k$) for its indices $j_k = [\Lambda^{(k)}:\mathrm{I}^{(k)}]$ there can be no Λ-reduced forms.

([6]) H. F. Blichfeldt, Mathematische Annalen, vol. 101 (1929), pp. 605–608.

Dividing (24_k) by

$$g_{11} \cdots g_{k-1,k-1} \geqq q_1 \cdots q_{k-1}$$

we find that our reduced form satisfies the fundamental relations

$$q_k \geqq \lambda_k g_{kk} \tag{26}$$

where

$$\lambda_k = (j_k \pi_k / 2^k)^2. \tag{27}$$

This lower bound for q_k is much better than the corresponding one holding for the method of reduction studied in R1.

The *first theorem of finiteness* deals with the subset $\Lambda_k(=)$ of Λ_k to which a vector $\mathfrak{x}$ in Λ_k belongs if there exists a Λ-reduced positive quadratic form f^2 satisfying the *equation* $f^2(\mathfrak{x}) = g_{kk}$. *The set* $\Lambda_k(=)$ *is finite.* The proof is as in R1, but the upper bounds arrived at are a good deal lower. The first part of the proof yields the bounds

$$\lambda_i z_i^2 \leqq 1 \qquad (\text{for } i = k, k+1, \cdots, n)$$

where the λ_i are now defined by (27). In the second part one replaces the vector $\mathfrak{x}$ in $\Lambda_k(=)$ by $\mathfrak{x} - \mathfrak{x}_h$ where $\mathfrak{x}_h$ is any vector in $\Lambda^{(h)}$ $(h<k)$ and observes that

$$f^2(\mathfrak{x} - \mathfrak{x}_h) \geqq g_{kk}.$$

This is true in particular if $\mathfrak{x}_h$ is in $\mathrm{I}^{(h)}$, and as in R1 one thus derives the relations

$$\lambda_h z_h^2 \leqq \rho^2 h \qquad (\rho = 1/2;\ h = 1, \cdots, k-1).$$

Once the discrete lattice Λ is given, the resulting universal upper bounds for $|x_n|, \cdots, |x_1|$ leave only a limited number of possibilities for a vector $\mathfrak{x} = (x_1, \cdots, x_n)$ in Λ.

The *second theorem of finiteness* shall be restated in a more natural and slightly more general form. Let $p \geqq 1$ and $w \geqq 0$ be given. With respect to the lattice Λ over I the positive quadratic form f^2 will be said to have the property $B(p, w)$ provided

$$f^2(\mathfrak{x}) \geqq \frac{1}{p} \cdot f^2(\mathfrak{e}_k) \tag{28}$$

for any vector $\mathfrak{x}$ in Λ_k, and

$$f^2(\mathfrak{e}_k - \mathfrak{x}_h) \geqq f^2(\mathfrak{e}_k) - w \cdot f^2(\mathfrak{e}_h) \tag{28'}$$

for $h<k$ and any vector $\mathfrak{x}_h$ in $\Lambda^{(h)}$. Again, each of these conditions is a linear inequality for the coefficients g_{ij} of f^2. We maintain:

Given two lattices Λ *and* Λ' *over* I, *there is only a limited number of linear*

transformations carrying Λ into Λ' and at the same time capable of carrying an unspecified Λ-reduced form f^2 into an unspecified f'^2 which has the property $B(p, w)$ with respect to Λ'.

We write the transformation as

$$\mathfrak{x} = \sum_i x_i \mathfrak{e}_i = \sum_i y_i \mathfrak{d}_i:$$

if $(x_1, \cdots, x_n)$ is in Λ, then $(y_1, \cdots, y_n)$ is in Λ', and *vice versa*. In particular, the $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$ are vectors in Λ. (p, $\mathfrak{e}_i$, $\mathfrak{d}_i$ were denoted in R1 by ρ^2, $\mathfrak{d}_i$, $\mathfrak{s}_i$.) More explicitly as has been done in R1, we divide the row of indices $1, \cdots, n$ into a number of sections by means of the subspaces

$$E_k = [\mathfrak{e}_1, \cdots, \mathfrak{e}_k], \qquad E_k' = [\mathfrak{d}_1, \cdots, \mathfrak{d}_k] \qquad (k = 0, 1, \cdots, n).$$

We pick out those $k = l_0, l_1, \cdots, l_v$,

$$0 = l_0 < l_1 < \cdots < l_{v-1} < l_v = n$$

for which $E_k = E_k'$, and divide the range of k into the v sections

$$l_{u-1} < k \leqq l_u \qquad (u = 1, \cdots, v).$$

We then study the possibilities for transformations $(\mathfrak{d}_1, \cdots, \mathfrak{d}_n)$ with given $l_1, \cdots, l_{v-1}$.

By the analogues of Theorems 8_p and 9_p we have

$$g'_{kk} \leqq p g_{kk} \qquad (k = 1, \cdots, n) \tag{29}$$

and moreover

$$g_{i+1,i+1} \leqq p g_{ii} \tag{30}$$

whenever i and $i+1$ are in the same section. Consider a $\mathfrak{d}_k$ of the last section ($l_{v-1} < k \leqq n$). The first part of the proof in R1 yields for $\mathfrak{x} = \mathfrak{d}_k$ the simple upper bounds

$$\lambda_h z_h^2 \leqq p^{\{k-h\}+1}$$

if h also belongs to the last section, $\{k\}$ denoting 0 or k according as $k \leqq 0$ or $k > 0$. The second part requires a slight modification. Suppose h lies in the uth section ($u < v$), and set for the moment $l_u = l$. Since $E_l = E_l'$, the vectors in $\Lambda^{(l)}$ are obtained from the expression $y_1\mathfrak{d}_1 + \cdots + y_l\mathfrak{d}_l$ by running $(y_1, \cdots, y_l, 0, \cdots, 0)$ over $\Lambda'^{(l)}$. Hence, according to the postulate (28'):

$$f'^2(\mathfrak{e}_k - \mathfrak{y}') \geqq g'_{kk} - w g'_{ll}$$

for any vector $\mathfrak{y}'$ in $\Lambda'^{(l)}$, or

$$f^2(\mathfrak{d}_k - \mathfrak{x}') \geqq g'_{kk} - w g'_{ll}$$

for any vector $\mathfrak{x}'$ in $\Lambda^{(l)}$, *a fortiori* for any vector in $\Lambda^{(h)}$, *a fortiori* for any vector $\mathfrak{x}'$ in $\mathrm{I}^{(h)}$. Following the same argument as in R1, one gets the inequality

$$wg'_{ll} + \rho^2 h g_{hh} \geqq \lambda_h g_{hh} z_h^2 \qquad (\rho = 1/2).$$

But because h and l are in the same section, (30) and (29) lead to

$$g_{ll} \leqq p^{l-h} g_{hh}, \qquad g'_{ll} \leqq p g_{ll} \leqq p^{l-h+1} g_{hh}$$

and thus finally

$$\lambda_h z_h^2 \leqq h\rho^2 + w \cdot p^{l_u - h + 1} \qquad (l_{u-1} < h \leqq l_u;\ u = 1, \cdots, v-1).$$

It is clear how the same procedure applies to a k in the lower sections. Denoting the values of the variables $z_1, \cdots, z_n$ for $\mathfrak{x} = \mathfrak{d}_k$ by $z_{1k}, \cdots, z_{nk}$, one finds:

$z_{hk} = 0$ if h is in a higher section than k;

$\lambda_h z_{hk}^2 \leqq p^{[k-h]+1}$ if h and k are in the same section;

$\lambda_h z_{hk}^2 \leqq h\rho^2 + w \cdot p^{l-h+1}$ if h is in a lower section than k which ends with l.

8. **Modifications in arbitrary fields and quasi-fields.** Our next concern is to examine whether any serious modifications of the procedure just described arise in the two general cases of a field and a quaternion algebra over a field. Take the case of the field first. With a positive Hermitian form γ^* in $\mathfrak{F}^*$ we combine its trace f^2:

$$(31) \qquad f^2(\xi_1^*, \cdots, \xi_n^*) = \sum_\alpha \sum_{i,k} g_{ik}^\alpha x_i^\alpha x_k^\alpha + 2 \sum_\beta \sum_{i,k} \gamma_{ik}^\beta \xi_i^\beta \bar{\xi}_k^\beta \qquad (\xi_k^\beta = x_{k0}^\beta + i x_{k1}^\beta).$$

γ^* is called reduced with respect to Λ if the gauge function f is, i.e., if

$$(32) \qquad f^2(\xi_1, \cdots, \xi_n) \geqq \mathrm{tr}\,(\gamma_{kk}^*) = M_k^2$$

for any vector $(\xi_1, \cdots, \xi_n)$ in Λ_k. Each part is subjected to its Jacobi transformation:

$$\sum_{i,k} g_{ik}^\alpha x_i^\alpha x_k^\alpha = \sum_i q_i^\alpha (z_i^\alpha)^2,$$

$$\sum_{i,k} \gamma_{ik}^\beta \xi_i^\beta \bar{\xi}_k^\beta = \sum_i q_i^\beta \left| \zeta_i^\beta \right|^2.$$

Besides

$$\mathrm{tr}\,(q_i) = \sum_\alpha q_i^\alpha + 2 \sum_\beta q_i^\beta, \qquad \mathrm{Nm}\,(q_i) = \prod_\alpha q_i^\alpha \cdot \prod_\beta (q_i^\beta)^2$$

we introduce the mean value $\langle q_i \rangle$ by

$$f \cdot \langle q_i \rangle = \mathrm{tr}\,(q_i).$$

In terms of the coordinates x_k^α; x_{k0}^β, x_{k1}^β the volume V of the ellipsoid $f^2(\mathfrak{x}^*)<1$ is

$$\omega_{nf} \text{ divided by } 2^{ns}\left(\prod_i \mathrm{Nm}\, q_i\right)^{1/2}.$$

Instead of applying Minkowski's second inequality to the present gauge function we again consider the ellipsoid

$$f'^2(\mathfrak{x}^*) = \mathrm{tr}\left(\sum_i \frac{q_i}{M^2}\,\zeta_i\bar{\zeta}_i\right) < 1$$

which contains no lattice vector except zero, and thus establish the inequality

$$\prod_i (\mathrm{tr}\,\gamma_{ii}^*)^f \cdot [\Lambda:\mathrm{I}]^2 \leqq \frac{(4^{r+s}\Delta^2)^n}{\pi^{2}_{nf}} \cdot \prod_i \mathrm{Nm}\, q_i \tag{33}$$

for any reduced γ^*/Λ.

Now enters the only new feature: Making use of the inequality between arithmetic and geometric means in the form

$$\mathrm{Nm}\, q_i \leqq \langle q_i\rangle^f$$

we infer from

$$q_i^\alpha \leqq g_{ii}^\alpha, \qquad q_i^\beta \leqq \gamma_{ii}^\beta$$

the relation

$$\langle\gamma_{ii}^*\rangle^f \geqq \langle q_i\rangle^f \geqq \mathrm{Nm}\, q_i,$$

and then (33) yields the following upper bound for $j=[\Lambda:\mathrm{I}]$:

$$j \leqq 1/\mu_n \quad \text{with the abbreviation} \quad \mu_n = \frac{\pi_{nf}\cdot f^{nf/2}}{(2^{r+s}\Delta)^n}.$$

For the same reasons

$$\prod_{i=1}^k \langle\gamma_{ii}^*\rangle^f (\mu_k j_k)^2 \leqq \prod_{i=1}^k \mathrm{Nm}\, q_i \tag{34}$$

and hence

$$\mu_k j_k \leqq 1. \tag{35}$$

These estimates are an improved substitute for Theorem II. Combining (34) with

$$\prod_{i=1}^{k-1} \langle\gamma_{ii}^*\rangle^f \geqq \prod_{i=1}^{k-1} \langle q_i\rangle^f \geqq \prod_{i=1}^{k-1} \mathrm{Nm}\, q_i$$

one gets

$$\text{Nm } q_k \geqq (\mu_k j_k)^2 \cdot \langle \gamma_{kk}^* \rangle^f. \tag{36}$$

Not only does this inequality establish a lower bound for the trace of q_k,

$$\text{tr } q_k \geqq (\mu_k j_k)^{2/f} \cdot \text{tr } \gamma_{kk}^*,$$

but it also shows that the geometric mean of the conjugates of q_k is not much smaller than their arithmetic mean. Therefore none of the conjugates can be much smaller than their arithmetic mean. We have a special case of the situation dealt with by the following

LEMMA 5. *Let $f_1, \cdots, f_m$ be positive integers and $u_1, \cdots, u_m$; $v_1, \cdots, v_m$ two rows of positive numbers. We set*

$$f = f_1 + \cdots + f_m,$$
$$f \cdot \langle u \rangle = f_1 u_1 + \cdots + f_m u_m,$$
$$\text{Nm } u = u_1^{f_1} \cdots u_m^{f_m}.$$

If $u_\alpha \leqq v_\alpha$ $(\alpha = 1, \cdots, m)$ and

$$\text{Nm } u \geqq \mu \cdot \langle v \rangle^f \tag{37}$$

with some constant $\mu \geqq 1$, then

$$u_\alpha \geqq \lambda_\alpha \cdot \langle v \rangle$$

where λ_α depends on μ but not on the u and v.

(In our case r among the weights f_α are 1 and s of them equal 2.)

Proof. In the trivial case $m = 1$ one determines λ by

$$\lambda^f = \mu. \tag{38}$$

If $m > 1$ we set $u_1 = \lambda \cdot \langle v \rangle$ and assume $\lambda \leqq 1$. Then

$$\text{Nm } u = \lambda^{f_1} \langle v \rangle^{f_1} \cdot u_2^{f_2} \cdots u_m^{f_m} \leqq \lambda^{f_1} \langle v \rangle^{f_1} \langle u \rangle_1^{f - f_1}.$$

Here $\langle u \rangle_1$ denotes the arithmetic mean of $u_2, \cdots, u_m$ formed with the weights $f_2, \cdots, f_m$ of sum $f - f_1$:

$$(f - f_1) \cdot \langle u \rangle_1 = f_2 u_2 + \cdots + f_m u_m = f \cdot \langle u \rangle - f_1 u_1$$
$$= f \cdot \langle u \rangle - f_1 \lambda \langle v \rangle \leqq (f - f_1 \lambda) \langle v \rangle.$$

Therefore

$$\text{Nm } u \leqq \mu \cdot \langle v \rangle^f$$

where

$$\mu = \lambda^{f_1}\left(\frac{f - f_1\lambda}{f - f_1}\right)^{f-f_1}. \tag{39}$$

As its logarithmic derivative shows,

$$\frac{d\mu}{\mu} = \frac{f_1(1-\lambda)}{f - f_1\lambda}\cdot\frac{f d\lambda}{\lambda}; \tag{40}$$

this function $\mu(\lambda)$ maps the interval $0 \leqq \lambda \leqq 1$ monotonically upon $0 \leqq \mu \leqq 1$ and thus will assume the given value μ ($\leqq 1$) for a certain $\lambda = \lambda_1$ ($\leqq 1$). Thus we cannot have $u_1 < \lambda_1 \cdot \langle v \rangle$ under the condition (37).

(We wish to obtain the best value for the constant λ_1. If one is content with a little less, one may choose λ_1 according to the equation

$$\lambda_1^{f_1}\cdot\left(\frac{f}{f-f_1}\right)^{f-f_1} = \mu,$$

or even, as

$$\left(1 + \frac{f_1}{f-f_1}\right)^{(f-f_1)/f_1} < e \qquad (= \text{basis of natural logarithms}),$$

$$(\lambda_1 e)^{f_1} = \mu.$$

Incidentally, formula (40) holds good also for the function (38) which rules the trivial case $m = 1, f_1 = f$.)

In this way we ascertain constants λ_k, λ_k' such that

$$\text{each } q_k^{\alpha} \geqq \lambda_k \cdot \langle \gamma_{kk}^{*} \rangle \text{ and each } q_k^{\beta} \geqq \lambda_k' \cdot \langle \gamma_{kk}^{*} \rangle.$$

In case there is only one infinite prime spot, λ_k and λ_k' are determined by the relation

$$(\mu_k j_k)^2 = \lambda_k = \lambda_k'^2$$

in case of several spots by the equations

$$(\mu_k j_k)^2 = \lambda_k\left(\frac{f-\lambda_k}{f-1}\right)^{f-1} = \lambda_k'^2\left(\frac{f-2\lambda_k'}{f-2}\right)^{f-2}$$

together with $\lambda_k \leqq 1$ and $\lambda_k' \leqq 1$.

Similarly for the other case studied in §6, that of a quaternion algebra $\mathfrak{Z}$ with totally positive relative norm over a totally real field. The constants μ_k, λ_k in the inequalities

$$\mu_k j_k \leqq 1 \quad \text{and} \quad q_k^{\alpha} \geqq \lambda_k \cdot \langle \gamma_{kk}^{*} \rangle$$

are then given by

$$\mu_k = \pi_{4ke}\, \Delta^{-k}(e/4)^{2ke},$$

$$(\mu_k j_k)^{1/2} = \lambda_k \quad \text{or} \quad \lambda_k\left(\frac{e-\lambda_k}{e-1}\right)^{e-1} \qquad (\lambda_k \leqq 1),$$

according as $e=\frac{1}{4}f$ is 1 or is greater than 1.

After this the proofs for the first and second theorems of finiteness roll along as before.

9. **The pattern of equivalent cells.** The Hermitian forms $\{\gamma_{ik}^*\}$ constitute a linear space of

$$N = f\cdot\tfrac{1}{2}n(n-1) + (r+s)n = f\cdot\tfrac{1}{2}n(n+1) - sn \qquad (\text{field } \mathfrak{F})$$

or

$$N = en(2n-1) \qquad (\text{quasi-field } \mathfrak{F})$$

dimensions, the positive ones a convex cone G in that space. G is an open set; we operate within G throughout. "Form" means any positive Hermitian form.

Let Λ be a lattice over I. A Λ-reduced form γ^* has been characterized by the inequalities

$$f^2(\xi_1, \cdots, \xi_n) \geqq f^2(e_{1k}, \cdots, e_{nk}) \tag{32}$$

holding for $f^2=\text{tr}\ (\gamma^*)$ whenever $(\xi_1, \cdots, \xi_n)$ is in Λ_k. For a given vector $(\xi_1, \cdots, \xi_n)$ the equality sign in (32) will hold identically for all Hermitian forms γ^* only if

$$(\xi_1, \cdots, \xi_n) = \epsilon\cdot(e_{1k}, \cdots, e_{nk}) \qquad (\epsilon \text{ a unit}),$$

as follows at once from the expression (31). For any other vector $(\xi_1, \cdots, \xi_n)$ the equation determines a $(N-1)$-dimensional hyperplane in our N-dimensional linear space of forms. This remark justifies our definition of "properly reduced" in terms of the group U of units.

The forms γ^* which are reduced with respect to Λ make up a convex cone G_Λ in G. The properly reduced forms are the inner points of G_Λ; see R1, p. 150. G_Λ may be empty; indeed it will be so unless the indices j_k of Λ satisfy the inequalities (35). Even if it is not empty it may be without inner points. Theorem 10 in R1, together with the first theorem of finiteness, proves:

THEOREM IV. *If G_Λ has inner points, then G_Λ is a convex pyramid defined within G by a limited number of linear inequalities.*

A linear mapping $\mathfrak{x}\to\mathfrak{x}'$ of $E^n/\mathfrak{F}$ upon itself is one satisfying the conditions $(\mathfrak{x}_1+\mathfrak{x}_2)'=\mathfrak{x}_1'+\mathfrak{x}_2'$ and $(\delta\cdot\mathfrak{x})'=\delta\cdot\mathfrak{x}'$ for any number δ in $\mathfrak{F}$. We also require that $\mathfrak{x}=0$ is the only vector whose image $\mathfrak{x}'$ equals 0. If $\mathfrak{d}_1, \cdots, \mathfrak{d}_n$ is any basis of $E^n/\mathfrak{F}$ the mapping S may be defined by giving the images $\mathfrak{d}_i'=\mathfrak{d}_iS$ of the $\mathfrak{d}_i$. The mapping S carries a form γ^* into a form γ_S^* according to the equation $\gamma_S^*(\mathfrak{x}S)=\gamma^*(\mathfrak{x})$. An order $[\mathfrak{F}]$ in $\mathfrak{F}$ and a lattice $\mathfrak{L}$ belonging to the order $[\mathfrak{F}]$ are supposed to be given. The linear mappings S which leave $\mathfrak{L}$ invariant are

said to form the *modular group*(7). In terms of a basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of $E^n/\mathfrak{J}$ the lattice $\mathfrak{L}$ is represented by Λ:

$$\mathfrak{x} = \eta_1\mathfrak{b}_1 + \cdots + \eta_n\mathfrak{b}_n \quad \text{in} \quad \mathfrak{L} \cdot \rightleftarrows \cdot (\eta_1, \cdots, \eta_n) \quad \text{in} \quad \Lambda,$$

and a form $\gamma^*(\mathfrak{x})$ is represented by a form $\Gamma^*(\eta_1, \cdots, \eta_n)$:

$$\gamma^*(\eta_1\mathfrak{b}_1 + \cdots + \eta_n\mathfrak{b}_n) = \Gamma^*(\eta_1, \cdots, \eta_n). \tag{41}$$

The linear mapping defined by $\mathfrak{b}_i \to \mathfrak{b}_i'$ carries $\eta_1\mathfrak{b}_1 + \cdots + \eta_n\mathfrak{b}_n$ into $\eta_1\mathfrak{b}_1' + \cdots + \eta_n\mathfrak{b}_n'$; hence it leaves $\mathfrak{L}$ invariant and thus belongs to the modular group if and only if $\Lambda = \Lambda'$, Λ and Λ' being the representations of $\mathfrak{L}$ in terms of $\mathfrak{b}_i$ and $\mathfrak{b}_i'$. For a vector $\mathfrak{b}$ in $\mathfrak{L}$ there are not more than a finite number of units ϵ such that $\epsilon\mathfrak{b}$ also is in $\mathfrak{L}$. Indeed, for the splits of $\mathfrak{x} = \epsilon\mathfrak{b}$ one finds

$$|\xi^\alpha| = |\delta^\alpha|, \quad |\xi^\beta| = |\delta^\beta|, \quad \text{a fortiori} \quad |\xi^\alpha| \leqq |\delta^\alpha|, \quad |\xi^\beta| \leqq |\delta^\beta|,$$

which in view of the discrete nature of $\mathfrak{L}$ proves the point.

We want to divide G without gaps and overlappings into domains which are mutually equivalent under the modular group. We shall introduce these cells first as entities which have nothing to do with Hermitian forms, adopting a criterion of identity other than the set-theoretic one. The systematic place for this introduction would have been at the end of §3. Only afterwards shall we explain the meaning of the phrase "a form lies in a cell." Here are the definitions:

A semi-basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ of $\mathfrak{L}$ determines a cell $Z(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$; the semi-basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ is said to determine the same cell if

$$\mathfrak{b}_i = \epsilon_i\mathfrak{b}_i \qquad (\epsilon_i \text{ units}). \tag{42}$$

Let S be an operation of the modular group. The image Z_S of $Z = Z(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ is defined as $Z(\mathfrak{b}_1', \cdots, \mathfrak{b}_n')$ where $\mathfrak{b}_i' = \mathfrak{b}_i S$. (Notice that if Z is written as $Z(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$, $\mathfrak{b}_i = \epsilon_i\mathfrak{b}_i$, then $Z(\mathfrak{b}_1', \cdots, \mathfrak{b}_n')$ is the same Z_S because $\mathfrak{b}_i' = \epsilon_i\mathfrak{b}_i'$; thus Z_S is independent of the fixation of the defining semi-basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$.) Those S of the modular group for which $Z_S = Z$ shall be denoted by J_Z; they form a finite group $\{J_Z\}$. Indeed, for such an $S = J_Z$ one must have

$$\mathfrak{b}_i' = \mathfrak{b}_i S = \sigma_i\mathfrak{b}_i \qquad (\sigma_i \text{ a unit}), \tag{43}$$

and the J_Z are those mappings of the special form (43) which leave $\mathfrak{L}$ invariant. (In terms of another defining semi-basis $\mathfrak{b}_i = \epsilon_i\mathfrak{b}_i$ the same J_Z is expressed by $\mathfrak{b}_i' = \epsilon_i\sigma_i\epsilon_i^{-1} \cdot \mathfrak{b}_i$.) Any operation S of the modular group has the same effect upon Z as $J_Z S$.

(7) If one feels that this term ought to be reserved for the group which is fundamental in the theory of the modules of the theta functions then a new word, say "lattice group," is indicated for our purpose.

In terms of $(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ the lattice $\mathfrak{L}$ is represented by an admissible lattice Λ, i.e., by a lattice Λ over I which is equivalent to $\mathfrak{L}$. Hence to the cell $Z=Z(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ there corresponds a family of admissible lattices Λ, and the same family to each equivalent cell Z_S. We have a one-to-one correspondence between the classes of equivalent cells on the one hand, and the families of admissible lattices Λ on the other. We distinguish them by different colors. The operations J_Z are represented by the operations J_Λ in terms of the basis $(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$.

Now we come to the realization of cells as point sets in G. A form γ^* is said to lie in $Z=Z(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ if $(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ is reduced with respect to γ^*, i.e., if for $f^2=\mathrm{tr}(\gamma^*)$ one has $f^2(\mathfrak{x}) \geqq f^2(\mathfrak{b}_k)$ whenever $\mathfrak{x}$ is in $\mathfrak{L}$ and outside $[\mathfrak{b}_1, \cdots, \mathfrak{b}_{k-1}]$. Because (42) implies

$$f^2(\mathfrak{b}_k) = f^2(\mathfrak{b}_k), \qquad [\mathfrak{b}_1, \cdots, \mathfrak{b}_{k-1}] = [\mathfrak{b}_1, \cdots, \mathfrak{b}_{k-1}],$$

the definition is independent of the fixation of the defining semi-basis $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$. If γ^* lies in $Z=Z(\mathfrak{b}_1, \cdots, \mathfrak{b}_n)$ then the transform Γ^* introduced by (41) lies in G_Λ, and γ_S^* lies in Z_S.

The fact that there always exists a reduced semi-basis for a given γ^* and the concluding sentence of §3 can now be stated thus:

(a) Every point γ^* lies in at least one cell Z.

(b) An inner point of a cell Z cannot lie in a cell Z' unless Z' is the same as Z (or briefly: different cells have no inner points in common).

The fact (a) will of course not be altered by suppressing all *empty* cells and their colors. Thus we have to look only for those admissible Λ whose indices satisfy the conditions (35); and this brings the colors down to a limited number. Will (a) still prevail after suppressing all cells without inner points and their colors? The answer is affirmative because there is no inner clustering of cells in G. This is a consequence of the second theorem of finiteness, which now takes on the following form. Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be a semi-basis of $\mathfrak{L}$, $p \geqq 1$ and $w \geqq 0$. The form γ^* is said to lie in $Z(\mathfrak{a}_1, \cdots, \mathfrak{a}_n | p, w)$ if

$$f^2(\mathfrak{x}) \geqq \frac{1}{p} \cdot f^2(\mathfrak{a}_k)$$

whenever $\mathfrak{x}$ is in $\mathfrak{L}$ and outside $[\mathfrak{a}_1, \cdots, \mathfrak{a}_{k-1}]$, and if, moreover,

$$f^2(\mathfrak{a}_k - \mathfrak{x}_h) \geqq f^2(\mathfrak{a}_k) - w \cdot f^2(\mathfrak{a}_h)$$

whenever $h<k$ and $\mathfrak{x}_h$ is in $\mathfrak{L}$ and $[\mathfrak{a}_1, \cdots, \mathfrak{a}_h]$.

THEOREM V. *There is only a finite number of operations S of the modular group such that the image Z_S into which a given cell Z is thrown by S will have points in common with the domain $Z(\mathfrak{a}_1, \cdots, \mathfrak{a}_n | p, w)$.*

Application to $p=1$, $w=0$ proves in particular that a cell borders on not more than a finite number of other cells. And since $Z(\mathfrak{a}_1, \cdots, \mathfrak{a}_n | p, w)$ sweeps

over the whole G if p and w increase to infinity we are sure that the cells cluster around no point in the interior of G ("the modular group is properly discontinuous in G"). We therefore definitely admit only those colors whose cells are N-dimensional solids, i.e., have inner points. In our summary we talk of them as point sets in G.

THEOREM VI. (a) *G is divided into a pattern of cells, each cell bearing a color out of a finite palette of colors. The cells cover G without gaps and overlappings. Each cell is a solid convex pyramid (in G). The mappings of the modular group leave this design, including its coloring, invariant. Any two cells of the same color can be carried one into the other by an operation of the modular group.*

(b) *Given a point in G and a cell Z one can assign a neighborhood $\mathfrak{N}$ to the point such that there is only a limited number of operations S of the modular group for which the image Z_S penetrates into $\mathfrak{N}$.*

(c) *The operations of the modular group which carry a cell into itself form a finite subgroup. This group of linear operations in the vector space $E^n/\mathfrak{F}$ is equivalent (in $\mathfrak{F}$) to a group whose elements are of the special form*

$$\xi_1 \to \xi_1\epsilon_1, \cdots, \xi_n \to \xi_n\epsilon_n \qquad (\epsilon_i \text{ units}).$$

(Of course, in view of statement (c) the statement (b) could have been replaced by the simpler one that only a finite number of cells penetrate into $\mathfrak{N}$.)

We form a *nucleus* by selecting one cell Z_c of each color c. All cells adjacent to the nuclear cells form a *wreath* around the nucleus. Here the word "adjacent" may be interpreted either in the wide sense of "having a point in common," or in the narrower sense of "having a wall of $N-1$ dimensions in common."

THEOREM VII. *Determine for each cell Z_c' of color c in the wreath an operation S_c' of the modular group which maps the nuclear cell Z_c of color c into Z_c'. The S_c' thus selected, together with the operations J_c of the modular group which carry Z_c into itself, generate the whole group if all colors c are taken into account.*

Were it not for the groups $\{J_\Lambda\}$ the nucleus would form a fundamental domain. As it is, one has first to replace in our construction each G_Λ by a part G_Λ' which in G_Λ is a fundamental domain for the finite group of special transformations

$$J_\Lambda: \quad \xi_k \to \xi_k\epsilon_k \qquad (\epsilon_k \text{ a unit})$$

carrying G_Λ into itself. The effect of J_Λ upon the coefficient $\overset{*}{\gamma}{}_{ik}^{\alpha}$ is described by

$$\overset{*}{\gamma}{}_{ik}^{\alpha} \to \epsilon_i \overset{*}{\gamma}{}_{ik}^{\alpha} \bar{\epsilon}_k.$$

If in one split α the transformation of the variable $\gamma_{ik}^{\alpha} = \Xi$,

$$\Xi \to \epsilon_i^{\alpha} \Xi \bar{\epsilon}_k^{\alpha} = \epsilon_i^{\alpha} \Xi (\epsilon_k^{\alpha})^{-1},$$

is the identity, then the same is true of every split. Hence it is sufficient to consider one split α only, and after choosing it we write simply $\gamma_{ik}^{\alpha}=\gamma_{ik}$, $\epsilon_i^{\alpha}=\epsilon_i$. If the transformation $\Xi\to\epsilon_1\Xi\epsilon_2^{-1}$ is the identity, one must have $\epsilon_1=\epsilon_2$ as the specialization $\Xi=1$ shows, and $\Xi\to\epsilon_2\Xi\epsilon_1^{-1}$ is also the identity. Moreover, if $\Xi\to\epsilon_1\Xi\epsilon_2^{-1}$ and $\Xi\to\epsilon_2\Xi\epsilon_3^{-1}$ are identities, then $\Xi\to\epsilon_1\Xi\epsilon_3^{-1}$ is. Consequently we may well limit ourselves first to the coefficients γ_{ik} $(i<k)$ on one side of the diagonal, and then more particularly to

$$\Xi_1=\gamma_{12},\ \Xi_2=\gamma_{23},\ \cdots,\ \Xi_{n-1}=\gamma_{n-1,n}.$$

Let us at once consider the most disagreeable case, that of a quaternion quasi-field $\mathfrak{F}$ as described in §6.

The group $\{J_\Lambda\}$ induces a group of transformations of the type

$$\Xi\to\epsilon_1\Xi\bar{\epsilon}_2 \qquad (|\epsilon_1|=|\epsilon_2|=1)$$

for $\gamma_{12}=\Xi_1=\Xi$. This is a finite group of orthogonal transformations J in the space of the four components X_0, X_1, X_2, X_3 of the variable quaternion Ξ. Denote by ΞJ the transform of Ξ by J. The simplest way of ascertaining a fundamental domain for this group $\{J\}$ is as follows: One chooses a point $\Xi=\mathrm{A}$ which differs from all its transforms $\mathrm{A}J$ ($J\neq$identity). The fundamental domain consists of all points Ξ which are nearer to the center A than to the other equivalent centers $\mathrm{A}J$ and is thus characterized by the inequalities

$$\Xi\cdot\overline{\mathrm{A}-\mathrm{A}J}+(\mathrm{A}-\mathrm{A}J)\cdot\bar{\Xi}\geqq 0.$$

Fortunately these are linear inequalities, namely of the form

$$a_0X_0+a_1X_1+a_2X_2+a_3X_3\geqq 0$$

(a_0, a_1, a_2, a_3 being the components of $\mathrm{A}-\mathrm{A}J$). After having done this we limit ourselves to those operations J_Λ which leave Ξ_1 unchanged. They form a subgroup and we study its influence upon $\Xi_2,\cdots,\Xi_{n-1}$. The next step would consist in singling out Ξ_2. By induction we thus obtain a finite number of subsidiary linear inequalities each concerned with the four components of one of the variables $\gamma_{12},\cdots,\gamma_{n-1,n}$ only, and by them we define the fundamental domain G_Λ' in G_Λ for the group $\{J_\Lambda\}$.

I set little store by this whittling down of G_Λ to G_Λ'. It seems less artificial to operate with the whole cells Z; in doing so one has to keep in mind that the modular group in its influence upon Z matters only modulo $\{J_Z\}$.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.