THE SPACE OF $\mathfrak{p}$-ADIC NORMS

BY

O. GOLDMAN and N. IWAHORI

Institute for Advanced Study, Princeton, N. J., U. S. A. (1)

Introduction

The symmetric space associated to the orthogonal group of a real indefinite quadratic form φ can be described, as is well known, as the set M of positive definite quadratic forms ψ which are minimal with respect to the property $|\varphi| \leqslant \psi$. The orthogonal group $O(\varphi)$ of the form φ acts transitively on M, and the isotropy group of any $\psi \in M$ is a maximal compact subgroup of $O(\varphi)$. A similar statement holds for the symplectic group.

A. Weil raised the question of the $\mathfrak{p}$-adic analogue of this phenomenon, and suggested the use of norms (sec. 1) in place of the positive definite quadratic forms. If φ is a non-degenerate quadratic form on a vector space E over a $\mathfrak{p}$-adic field we associate to φ the set $\mathcal{M}(\varphi)$ (see sec. 4) of norms α on E which are minimal with respect to the property $|\varphi| \leqslant \alpha^2$. Then again the orthogonal group $O(\varphi)$ of φ acts transitively on $\mathcal{M}(\varphi)$. However, the isotropy group of an element $\alpha \in \mathcal{M}(\varphi)$, while still compact, is no longer a maximal compact subgroup.

The study of norms on $\mathfrak{p}$-adic vector spaces it not new. (See for example Cohen [1] and Monna [3].) These authors were concerned with the metric topology induced on the vector space by a norm on that space. We are here concerned with the intrinsic structure that is carried by the set $\mathcal{N}(E)$ of *all* norms on a given vector space E. We define a natural metric on $\mathcal{N}(E)$, and in sec. 2 of the present paper describe some of the properties of $\mathcal{N}(E)$ as a metric space. For example, $\mathcal{N}(E)$ is a complete, locally compact arc-wise connected space, and is even contractible to a point.

---

(1) This research was partially supported by the National Science Foundation through Brandeis University, the University of California at Berkeley, Harvard University and the Institute for Advanced Study.

The group Aut (E) of linear automorphisms of E acts, in a natural way, on $\mathfrak{N}(E)$ leaving the metric invariant. In sec. 3 we give some of the properties of this action. The isotropy group of any point of $\mathfrak{N}(E)$ is a compact open subgroup of Aut (E), while the orbit of any point is a closed discrete subspace. The quotient space Aut $(E)\backslash\mathfrak{N}(E)$ is proved to be canonically homeomorphic to the symmetric product of n circles, where n is the dimension of E. In the same section we describe invariants for the conjugacy of two elements of $\mathfrak{N}(E)$ with respect to the isotropy group of a preassigned norm.

In sec. 4 we consider some relations between quadratic forms and norms and give a characterization of the elements of $\mathfrak{M}(\varphi)$. In this we make use of the relations, developed in sec. 1, between norms and lattices in E. Using this criterion of minimality, we obtain an explicit description of the elements of $\mathfrak{M}(\varphi)$ from which the transitivity of $O(\varphi)$ on $\mathfrak{M}(\varphi)$ follows easily. To some extent, our technique in this section is a variation of the method used by Eichler [2] in his study of the action of $O(\varphi)$ on certain lattices in E associated to φ.

In the fifth section we introduce the notion of the discriminant of a quadratic form with respect to a norm and describe some of the properties and applications of this concept.

We have given such a detailed description of $\mathfrak{N}(E)$ as a metric space and of the action of Aut (E) on $\mathfrak{N}(E)$ because we feel that there are possibilities of using these structures to study other types of arithmetic problems which may be formulated in the $\mathfrak{p}$-adic domain.

We should like to thank A. Weil for suggesting this line of investigation and for his help during the course of our work.

Section 1. Lattices and Norms

The following notation will have a fixed meaning throughout this paper:

K is a field complete in a discrete valuation, having a finite residue class field, hence locally compact.

q is the number of elements in that residue class field.

$|\,|$ is the valuation of K normalized so as to assume all integral powers of q on K^*.

$\mathfrak{O}$ is the valuation ring of K.

$\mathfrak{p}=\pi\mathfrak{O}$ is the maximal ideal of $\mathfrak{O}$.

E is a vector space over K of finite dimension n, topologized in the only natural topology over K, so that E is locally compact.

$P(E)$ is the projective space of E, so that $P(E)$ is compact.

By a *lattice* in E will be meant a finitely generated $\mathfrak{O}$-submodule L of E which spans E over K. Alternatively, L may be described as an $\mathfrak{O}$-submodule of E which is compact and open.

Let L be a lattice on E. If x is any non-zero element of E, the set of elements $a \in K$ such that $ax \in L$ is a fractional ideal of $\mathfrak{O}$, and so has the form $\mathfrak{p}^m$. We set $\alpha(x) = q^m$. We complete the definition of α by setting $\alpha(0) = 0$. Then, it is readily verified that α has the following properties:

1. if $x \neq 0$, then $\alpha(x) > 0$.
2. $\alpha(ax) = |a| \alpha(x)$, $a \in K$.
3. $\alpha(x + y) \leqslant \sup(\alpha(x), \alpha(y))$.

Any real-valued function on E having these three properties will be called a *norm* on E. In particular, every lattice determines a norm, and conversely, if α is the norm associated to a lattice L, then L is in turn determined by α through the relation $L = \{x \in E \mid \alpha(x) \leqslant 1\}$. It will be seen shortly that not every norm is determined by a lattice. We denote by $\mathcal{N}$, or by $\mathcal{N}(E)$, the set of all norms on E, and by $\mathcal{L}$, the set of norms determined by the lattices of E.

It follows immediately from the definition that each norm is a continuous function on E. If a norm is multiplied by a positive real number, the result is again a norm. Finally, $\mathcal{N}$ is partially ordered by the relation $\alpha \leqslant \beta$ means $\alpha(x) \leqslant \beta(x)$ for all $x \in E$.

Let L be a lattice. As $\mathfrak{O}$ is a principal ideal ring, L is a free $\mathfrak{O}$-module; let $x_1, \ldots, x_n$ be a set of free generators of L. If α is the norm associated to L, it is clear that $\alpha(\sum a_i x_i) = \sup(|a_i|)$.

PROPOSITION 1.1. *Let α be any norm on E. Then there is a basis $\{x_i\}$ of E, and positive real numbers r_i such that*

$$\alpha(\sum a_i x_i) = \sup(r_i |a_i|).$$

Proof. We prove the proposition by induction on the dimension of E. If $\dim E = 1$, let x be any non-zero element of E. Then, $\alpha(ax) = \alpha(x)|a|$, and the assertion is verified in that case. Assume that $\dim E = n$, and that the proposition is valid for spaces of dimension less than n. Let E_1 be a subspace of dimension $n - 1$ of E. It is clear that the restriction of α to E_1 lies in $\mathcal{N}(E_1)$, so that α restricted to E_1 has the form described in the proposition.

Let λ be a linear functional on E having E_1 for its kernel. With x any non-zero element of E, consider the quotient $|\lambda(x)|/\alpha(x)$. First of all this quotient is continuous. Secondly, it is a homogeneous function of degree 0. Hence it defines a continuous function on the projective space $P(E)$. As $P(E)$ is compact, this function assumes its maximum. Thus, there is an element $x_1 \in E$ such that

$$\frac{|\lambda(x)|}{\alpha(x)} \leqslant \frac{|\lambda(x_1)|}{\alpha(x_1)}, \quad \text{all} \quad x \in E.$$

It is clear that x_1 cannot be in E_1. Hence, E is the direct sum of Kx_1 and E_1.

Let $y \in E$; then $y = x_1 \lambda(y)/\lambda(x_1) + z$, with $z \in E_1$. We have, on the one hand,

$$\alpha(y) \leqslant \sup\left(\frac{|\lambda(y)|}{|\lambda(x_1)|}\alpha(x_1),\ \alpha(z)\right),$$

and, on the other hand, from the definition of x_1, that

$$\alpha(y) \geqslant \frac{|\lambda(y)|}{|\lambda(x_1)|}\alpha(x_1).$$

It follows that
$$\alpha(y) = \sup\left(\frac{|\lambda(y)|}{|\lambda(x_1)|}\alpha(x_1),\ \alpha(z)\right).$$

From the inductive assumption, there is a basis $x_2, \ldots, x_n$ of E_1 and positive real numbers $r_2, \ldots, r_n$ such that

$$\alpha\left(\sum_2^n a_i x_i\right) = \sup\left(r_2|a_2|, \ldots, r_n|a_n|\right).$$

If we set $r_1 = \alpha(x_1)$, then the argument above shows that $\alpha(\sum_1^n a_i x_i) = \sup(r_i|a_i|)$.

If $\alpha \in \mathfrak{N}(E)$, and $\{x_i\}$ is a basis such that $\alpha(\sum a_i x_i) = \sup(r_i|a_i|)$, then we shall say that α is *canonical* with respect to $\{x_i\}$.

We denote by E^* the dual space of E. We shall now describe a useful mapping from $\mathfrak{N}(E)$ to $\mathfrak{N}(E^*)$. Let $\alpha \in \mathfrak{N}(E)$. If $\lambda \in E^*$, we have already considered in the proof above, the quotient $|\lambda(x)|/\alpha(x)$ for non-zero $x \in E$. The continuity of this quotient and the compactness of $P(E)$ enable us to set

$$\alpha^*(\lambda) = \sup_x \frac{|\lambda(x)|}{\alpha(x)}.$$

There is no difficulty in verifying that α^* is a norm on E^*.

PROPOSITION 1.2. *The mapping $\alpha \to \alpha^*$ has the following properties:*

1. $(a\alpha)^* = 1/a\alpha^*$ *for* $a > 0$.
2. *if* $\alpha \leqslant \beta$, *then* $\beta^* \leqslant \alpha^*$.
3. *if* α *is canonical with respect to a basis* $\{x_i\}$, *and* $\{\lambda_i\}$ *is the dual basis of* $\{x_i\}$, *then* α^* *is canonical with respect to* $\{\lambda_i\}$ *and* $\alpha^*(\lambda_i) = \alpha(x_i)^{-1}$.
4. $\alpha^{**} = \alpha$.

Proof. These assertions are all trivial consequences of the definition of α^*. The fourth statement follows from the third by making use of Prop. 1.1.

PROPOSITION 1.3.(1) *Let α and β be any two norms. Then there is a basis of E with respect to which both α and β are canonical.*

Proof. The proof is by induction on $\dim E$; the case where $\dim E = 1$ is trivial. Suppose the assertion valid for spaces of dimension less than n. We consider the quotient $\alpha(x)/\beta(x)$ for non-zero $x \in E$. This defines a continuous function on $P(E)$, hence attains its maximum somewhere. Thus there is a non-zero $x_1 \in E$ such that

$$\frac{\alpha(x)}{\beta(x)} \leqslant \frac{\alpha(x_1)}{\beta(x_1)} \quad \text{all} \quad x \in E. \tag{1}$$

From the fact that $\alpha = \alpha^{**}$, we have

$$\alpha(x_1) = \sup_\lambda \frac{|\lambda(x_1)|}{\alpha^*(\lambda)},$$

and as $P(E^*)$ is compact, the supremum is attained somewhere. Thus, there is a $\lambda_1 \in E^*$, with

$$\alpha(x_1) = \frac{|\lambda_1(x_1)|}{\alpha^*(\lambda_1)}. \tag{2}$$

Clearly $\lambda_1(x_1) \neq 0$. Using the definition of α^*, we have from (2)

$$\frac{|\lambda_1(x)|}{|\lambda_1(x_1)|} \leqslant \frac{\alpha(x)}{\alpha(x_1)}. \tag{3}$$

Since from (1) we have $\beta(x)/\beta(x_1) \geqslant \alpha(x)/\alpha(x_1)$, it follows that

$$\frac{|\lambda_1(x)|}{|\lambda_1(x_1)|} \leqslant \frac{\beta(x)}{\beta(x_1)}. \tag{4}$$

(1) This theorem was given by A. Weil in a course in algebraic number theory at Princeton University.

Let E_1 be the kernel of λ_1. Since $\lambda_1(x_1) \neq 0$, E is the direct sum of E_1 and Kx_1. From the inductive assumption, there is a basis $\{x_2, \ldots, x_n\}$ of E_1 with respect to which $\alpha|_{E_1}$ and $\beta|_{E_1}$ are canonical. It follows immediately from (3) and (4) that α and β are canonical with respect to the basis $\{x_1, \ldots, x_n\}$.

COROLLARY 1.4. *Let L and L' be lattices in E. Then there is a set of free generators $\{x_1, \ldots, x_n\}$ of L such that for suitable $a_i \in K^*$, $\{a_1x_1, \ldots, a_nx_n\}$ is a set of free generators of L'.*

Proof. Let α, α' be respectively the norms of the lattices L, L'. By Proposition 1.3 there is a basis $y_1, \ldots, y_n$ of E with respect to which α and α' are both canonical. Since the values assumed by α and α' are integral powers of q, there are elements $b_i \in K^*$ such that $\alpha(y_i) = |b_i|$. Set $x_i = b_i^{-1}y_i$. Then it is clear that $\{x_1, \ldots, x_n\}$ is a set of free generators for L. If we choose $a_i \in K^*$ such that $\alpha'(x_i) = |a_i|^{-1}$, then $\{a_1x_1, \ldots, a_nx_n\}$ will be a set of free generators of L'.

Let $\{\alpha_j; j \in J\}$ be an indexed family of elements of $\mathcal{N}$ which has the following property: for each $x \in E$, the set $\{\alpha_j(x)\}$ of real numbers is bounded. If we then put $\beta(x) = \sup_{j \in J}\{\alpha_j(x)\}$, then there is no difficulty in verifying that β is again a norm. We shall write $\sup_{j \in J}\{\alpha_j\}$ for β. This operation has all the usual properties of a supremum. In particular, $\sup\{\alpha_j\}$ is always defined for finite sets J.

Suppose $\{\alpha_j; j \in J\}$ is again an indexed family of elements of $\mathcal{N}(E)$, but assume this time that $\sup_{j \in J}\{\alpha_j^*\}$ is defined (in $\mathcal{N}(E^*)$). In that case, we set

$$\inf\{\alpha_j\} = (\sup \alpha_j^*)^*.$$

In contrast to the sup operation, it is not true in general that $\inf\{\alpha_j\}(x) = \inf\{\alpha_j(x)\}$, not even when the indexing set J is finite.

We conclude this section with a description of some relations between norms and lattices which will be used later in studying quadratic forms.

Let α be a norm and let $L_\alpha = \{x \in E \mid \alpha(x) \leq 1\}$. Then L_α is a lattice, and is the largest lattice on which the values of α do not exceed 1. We denote by $[\alpha]$ the norm of the lattice L_α. It is clear from the definition that $\alpha \leq [\alpha] \leq q\alpha$. $[\alpha]$ may also be characterized as $\inf\{\beta \in \mathcal{L} \mid \alpha \leq \beta\}$.

PROPOSITION 1.5.

(a) $\alpha \leq \beta \Rightarrow [\alpha] \leq [\beta]$.

(b) $[q\alpha] = q[\alpha]$.

(c) $\alpha(x) = \inf q^{-t}[q^t\alpha](x)$, *the inf being taken over all t or over the set $0 \leq t \leq 1$.*

(d) *for each $x \in E$, the function of t defined by $[q^t\alpha](x)$ is continuous from the left.*

Proof.

(a) If $\alpha \leqslant \beta$, then $L_\alpha \supset L_\beta$ from which we find $[\alpha] \leqslant [\beta]$.

(b) We have $L_{q\alpha} = \pi L_\alpha$ and hence $[q\alpha] = q[\alpha]$.

(c) We note first that $q^t \alpha \leqslant [q^t \alpha]$ so that $\alpha \leqslant q^{-t}[q^t \alpha]$. Hence $\inf q^{-t}[q^t \alpha]$ exists, and $\alpha \leqslant \inf q^{-t}[q^t \alpha]$. It follows from (b) above, that $q^{-t}[q^t \alpha]$ is periodic in t with period 1 so that inf over all t is the same as inf over the interval $0 \leqslant t \leqslant 1$. Now, let x be any non-zero element of E, and set $\alpha(x) = q^{-t_1}$. Then, $[q^{t_1} \alpha](x) = 1$, so that $q^{-t_1}[q^{t_1}\alpha](x) = \alpha(x)$. Hence,

$$\alpha(x) = \inf q^{-t} [q^t \alpha] (x),$$

which proves (c).

(d) If $x \neq 0$, then one readily verifies that $[q^t \alpha] (x)$ is the smallest integral power of q which is not less than $q^t \alpha(x)$. Continuity of $[q^t \alpha](x)$ from the left follows immediately.

It should be remarked that as a consequence of (a), $[q^t \alpha]$ is a monotonic increasing function of t.

LEMMA 1.6. *Let $\alpha_t \in \mathfrak{L}$ for $0 \leqslant t \leqslant 1$ be such that:*

(1) *α_t is monotonic increasing in t.*

(2) $\alpha_1 = q\alpha_0$.

Then there is a basis of E with respect to which all α_t are canonical.

Proof. Let l_t be the lattice $\{x \mid \alpha_t(x) \leqslant 1\}$. Then

(a) $t_1 \leqslant t_2 \Rightarrow l_{t_1} \supset l_{t_2}$

(b) $l_1 = \pi l_0$,

so that also $l_0 \supset l_t \supset \pi l_0$.

Now $l_0/\pi l_0$ is an n-dimensional vector space over $\mathfrak{O}/\pi\mathfrak{O}$, and $l_t/\pi l_0$ form a descending family of subspaces of $l_0/\pi l_0$. We may imbed the family $\{l_t/\pi l_0\}$ in a maximal descending chain $l_0/\pi l_0 = V_1 \supset V_2 \supset \dots \supset V_{n+1} = 0$, with $\dim V_i/V_{i+1} = 1$. For each t, $l_t/\pi l_0 = V_i$, for suitable i. Let $y_1, \dots, y_n$ be a basis for V_1 chosen so that $y_i, y_{i+1}, \dots, y_n$ is a basis for V_i. Let $x_1, \dots, x_n$ be elements of l_0 such that x_i maps onto y_i in the homomorphism $l_0 \to l_0/\pi l_0 = V_1$. Clearly $x_1, \dots, x_n$ is a set of free generators of l_0. Furthermore, for each t, there is an index i such that $l_t = \pi l_0 + \sum_{j=i}^n \mathfrak{O} x_j$, and therefore $\{\pi x_1, \dots, \pi x_{i-1}, x_i, \dots, x_n\}$ is a set of free generators for l_t. It is now clear that all the α_t are canonical with respect to the basis $\{x_i\}$.

PROPOSITION 1.7. *Let, for all real t, $\alpha_t \in \mathcal{L}$ be chosen such that:*

(a) $t_1 \leqslant t_2 \Rightarrow \alpha_{t_1} \leqslant \alpha_{t_2}$

(b) $\alpha_{t+1} = q\alpha_t$

(c) *for each x, $\alpha_t(x)$ is continuous from the left.*

Then there is a unique $\alpha \in \mathcal{N}$ such that $\alpha_t = [q^t \alpha]$.

Proof. By lemma 1.6 above there is a basis $\{x_i\}$ with respect to which all α_t are canonical. We have then $\alpha_t(\sum a_i x_i) = \sup_i \{q^{\mu_i(t)} |a_i|\}$, where

1. $\mu_i(t) \in Z$
2. $t_1 \leqslant t_2 \Rightarrow \mu_i(t_1) \leqslant \mu_i(t_2)$
3. $\mu_i(t+1) = \mu_i(t) + 1$.

Now define
$$d_i = \inf_{0 \leqslant t \leqslant 1} \{\mu_i(t) - t\} = \inf_t \{\mu_i(t) - t\},$$
set $r_i = q^{d_i}$ and $\alpha(\sum a_i x_i) = \sup \{r_i |a_i|\}$. Then $\alpha \in \mathcal{N}$, and we shall show that $[q^t \alpha] = \alpha_t$. It is clearly sufficient to consider only $0 \leqslant t \leqslant 1$. We note also that from condition (c), $d_i = \mu_i(t) - t$ for some t with $0 \leqslant t < 1$.

We have $[q^t \alpha] = \inf \{\beta \in \mathcal{L} \mid \beta \geqslant q^t \alpha\}$. From the definition of α we have $\alpha \leqslant q^{-t} \alpha_t$, so that $[q^t \alpha] \leqslant \alpha_t$. Hence we must show that $\alpha_t \leqslant [q^t \alpha]$.

Now $[q^t \alpha]$ is the norm of the lattice $\{x \mid \alpha(x) \leqslant q^{-t}\}$. Hence the desired inequality $\alpha_t \leqslant [q^t \alpha]$ will follow if we prove the implication: $\alpha_t(x) > 1 \Rightarrow \alpha(x) > q^{-t}$.

Suppose then that $\alpha_t(x) > 1$. Since $\alpha_t \in \mathcal{L}$, the values assumed by α_t on the non-zero elements of E are integral powers of q. Hence we have $\alpha_t(x) \geqslant q$. With $x = \sum a_i x_i$, there is an index i such that $q^{\mu_i(t)} |a_i| \geqslant q$. Now, for some t' with $0 \leqslant t' < 1$, we have $d_i = \mu_i(t') - t'$. We consider
$$q^{d_i} |a_i| = q^{\mu_i(t') - t'} |a_i|.$$
Suppose first that $t \leqslant t'$. Then, $\mu_i(t) \leqslant \mu_i(t')$ so that
$$q^{d_i} |a_i| \geqslant q^{\mu_i(t) - t'} |a_i| \geqslant q^{1-t'} > q^{-t}.$$
On the other hand, suppose that $t' < t$. Then,
$$\mu_i(t) \leqslant \mu_i(1) = \mu_i(0) + 1 \leqslant \mu_i(t') + 1,$$
and hence
$$q^{d_i} |a_i| \geqslant q^{\mu_i(t) - 1 - t'} |a_i| \geqslant q^{-t'} > q^{-t}.$$
Thus, in either event
$$\alpha(x) \geqslant q^{d_i} |a_i| > q^{-t}.$$
This shows that $\alpha_t \leqslant [q^t \alpha]$ and hence $\alpha_t = [q^t \alpha]$. The uniqueness of α follows from Proposition 1.5.

Remark. It follows from the above that there are at most n distinct norms among the $[q^t\alpha]$ for $0 \leqslant t < 1$.

Let $E = E_1 + E_2$ (direct sum), and let $\alpha \in \mathcal{N}$. We shall say that E_1 and E_2 are *orthogonal* with respect to α if $\alpha(x_1 + x_2) = \sup(\alpha(x_1), \alpha(x_2))$, whenever $x_i \in E_i$.

LEMMA 1.8. *Let $E = E_1 + E_2$ (direct sum) and let f be the projection of E onto E_1. Let $\alpha \in \mathcal{N}$. Then E_1 and E_2 are orthogonal with respect to α if, and only if, $\alpha(x) \geqslant \alpha(f(x))$ for all $x \in E$.*

Proof. Suppose E_1 and E_2 are orthogonal with respect to α. Then $\alpha(x) = \sup(\alpha(f(x)), \alpha(x - f(x)))$, hence $\alpha(x) \geqslant \alpha(f(x))$. Suppose now that $\alpha(x) \geqslant \alpha(f(x))$ for all $x \in E$. Since $\alpha(x) < \sup(\alpha(f(x)), \alpha(x - f(x)))$ only if $\alpha(f(x)) = \alpha(x - f(x))$, it follows that $\alpha(x) = \sup(\alpha(f(x)), \alpha(x - f(x)))$, so that E_1 and E_2 are orthogonal with respect to α.

COROLLARY 1.9. *Let $E = E_1 + E_2$ (direct sum) and let $\alpha \in \mathcal{N}$. Then E_1 and E_2 are orthogonal with respect to α if, and only if, E_1 and E_2 are orthogonal with respect to $[q^t\alpha]$ for all t.*

Proof. Let f be the projection of E onto E_1. Then $\alpha(x) \geqslant \alpha f(x) \Leftrightarrow [q^t\alpha](x) \geqslant [q^t\alpha](f(x))$ for all t and the result follows from Lemma 1.8.

Section 2. The topological structure of $\mathcal{N}(E)$

We introduce a metric in the set $\mathcal{N}$ of all norms on E. If $\alpha, \beta \in \mathcal{N}$ consider, for non-zero x, the quotient $\alpha(x)/\beta(x)$. As we have already seen, this defines a continuous function on the compact space $P(E)$. As $\alpha(x) > 0$ for non-zero x, the function $|\log(\alpha(x)/\beta(x))|$ is bounded on $P(E)$, and we define

$$d(\alpha, \beta) = \sup_{x \neq 0} \left| \log \frac{\alpha(x)}{\beta(x)} \right|.$$

There is no difficulty in verifying that d is a metric on $\mathcal{N}$.

There is an explicit formula for d which will be useful later.

PROPOSITION 2.1. *Let α and β be norms such that α is canonical with respect to a basis $\{x_i\}$ and β is canonical with respect to $\{y_i\}$. Then,*

$$d(\alpha, \beta) = \sup_{i,j} \left\{ \log \frac{\beta(x_i)}{\alpha(x_i)}, \log \frac{\alpha(y_j)}{\beta(y_j)} \right\}.$$

Proof. It is clear from the definition of d that

$$d(\alpha, \beta) = \sup \left\{ \sup_{x \in E} \log \frac{\beta(x)}{\alpha(x)}, \sup_{y \in E} \log \frac{\alpha(y)}{\beta(y)} \right\}.$$

Now,

$$\sup_{x\in E}\log\frac{\beta(x)}{\alpha(x)}=\sup\log\frac{\beta(\sum a_i x_i)}{\alpha(\sum a_i x_i)},$$

with the supremum being taken over all $a_1, \ldots, a_n \in K$, not all 0. Hence,

$$\sup_{x\in E}\frac{\beta(x)}{\alpha(x)}\geqslant\sup_i\frac{\beta(x_i)}{\alpha(x_i)}.$$

Let $m=\alpha(\sum a_i x_i)=\sup_i(|a_i|\,\alpha(x_i))$. Then, $|a_i|\leqslant m/\alpha(x_i)$. Hence,

$$\beta(\sum a_i x_i)\leqslant\sup_i(|a_i|\,\beta(x_i))\leqslant\sup_i\left(m\,\frac{\beta(x_i)}{\alpha(x_i)}\right),$$

so that

$$\frac{\beta(\sum a_i x_i)}{\alpha(\sum a_i x_i)}\leqslant\sup_i\frac{\beta(x_i)}{\alpha(x_i)}.$$

Thus

$$\sup_{x\in E}\log\frac{\beta(x)}{\alpha(x)}=\sup_i\log\frac{\beta(x_i)}{\alpha(x_i)}.$$

In the same way, we obtain

$$\sup_{y\in E}\log\frac{\alpha(y)}{\beta(y)}=\sup_j\log\frac{\alpha(y_j)}{\beta(y_j)},$$

and the assertion follows immediately.

From now on, when we speak of the topology of $\mathcal{N}$ it will be understood to mean the metric topology defined by d.

THEOREM 2.2. *$\mathcal{N}$ is complete.*

Proof. Let $\{\alpha_n\}$ be a Cauchy sequence in $\mathcal{N}$. Let β be any element of $\mathcal{N}$, and set $f_n(x)=\log(\alpha_n(x)/\beta(x))$, for $x\neq 0$ in E. Then the f_n are continuous functions on $P(E)$ and form a Cauchy sequence in the uniform topology on $P(E)$. Hence $g(x)=\lim_{n\to\infty}f_n(x)$ exists, where g is continuous on $P(E)$, and the convergence is uniform.

Set $\alpha(x)=\beta(x)\,e^{g(x)}$ on E, defining $\alpha(0)=0$. Then, for $x\neq 0$ we have $\alpha(x)>0$, also $\alpha(ax)=|a|\,\alpha(x)$ for $a\in K$. We have $\log(\alpha(x)/\alpha_n(x))=g(x)-f_n(x)$, so that

$$\lim_{n\to\infty}|\log\alpha(x)-\log\alpha_n(x)|=0,$$

uniformly for non-zero x.

Now suppose that for some x and y we have $\alpha(x+y)>\sup(\alpha(x),\alpha(y))$. Clearly then none of the elements $x, y, x+y$ is 0. Choose $\varepsilon>0$ such that $\varepsilon<\frac{1}{2}(\log\alpha(x+y)-\log\alpha(x))$ and also $\varepsilon<\frac{1}{2}(\log\alpha(x+y)-\log\alpha(y))$. Then, there is an n such that $|\log\alpha(z)-\log\alpha_n(z)|<\varepsilon$ for all non-zero z. In particular,

$$\log \alpha(x+y) - \log \alpha_n(x+y) < \varepsilon$$
$$-\log \alpha(x) + \log \alpha_n(x) < \varepsilon$$

and therefore, $\log \alpha_n(x+y) - \log \alpha_n(x) > 0$, or $\alpha_n(x+y) > \alpha_n(x)$. In exactly the same way, we find $\alpha_n(x+y) > \alpha_n(y)$. But this contradicts the fact that α_n is a norm. Thus, we must have $\alpha(x+y) \leqslant \sup(\alpha(x), \alpha(y))$, and hence α is a norm. It follows immediately from the definition of α, that $\lim_{n\to\infty} d(\alpha, \alpha_n) = 0$. This completes the proof that $\mathcal{N}$ is complete.

THEOREM 2.3. *$\mathcal{N}$ is locally compact. More precisely, if $\alpha \in \mathcal{N}$, and $b > 0$, then $\{\beta \in \mathcal{N} \mid d(\alpha, \beta) \leqslant b\}$ is compact.*

Proof. Let $D = \{\beta \in \mathcal{N} \mid d(\alpha, \beta) \leqslant b\}$. By Theorem 2.2, D is complete. Let X be a subset of E having the following properties: $0 \notin X$, X compact, and if x is a non-zero element of E, then $ax \in X$ for some $a \in K$. Such a set X may be obtained in the following manner: let $\{x_i\}$ be a basis of E, and set $X = \{\sum a_i x_i \mid \sup\{|a_i|\} = 1\}$.

Denote by F the space of functions on X described by the restriction to X of $\log \beta$, with $\beta \in D$. The metric topology in D coincides with the uniform topology in F. We shall show that F consists of uniformly bounded, uniformly equicontinuous functions on X.

Because, for $\beta \in D$, $\mathrm{d}(\alpha, \beta) \leqslant b$, we have

$$e^{-b}\alpha(x) \leqslant \beta(x) \leqslant e^{b}\alpha(x),$$

for all $x \in X$, so that

$$|\log \beta(x)| \leqslant b + |\log \alpha(x)|.$$

Since $\log \alpha(x)$ is bounded on X, it follows that the elements of F are uniformly bounded on X.

Also, since $\alpha(x)$ is bounded away from 0 on X, all $\beta \in D$ are uniformly bounded away from 0, so that the uniform equicontinuity of $\{\log \beta\}$ is the same as uniform equicontinuity of $\{\beta\}$. Now,

$$|\beta(x) - \beta(y)| \leqslant \beta(x-y) \leqslant e^{b}\alpha(x-y),$$

and because α is uniformly continuous on X, the result follows. Hence by the theorem of Ascoli-Arzela, F is compact, and hence D is also compact.

We consider now the connectedness properties of $\mathcal{N}$.

THEOREM 2.4. *Let α, β be two norms, and let $0 \leqslant t \leqslant 1$. Let*

$$P(t) = \{\gamma \in \mathcal{N} \mid \gamma(x) \leqslant \alpha(x)^{1-t}\beta(x)^{t}, \text{ all } x \in E\}.$$

Then, $P(t)$ is not empty. Set $\pi_t = \sup\{\gamma \mid \gamma \in P(t)\}$. Then, π_t has the following properties:

(a) $\pi_0 = \alpha$, $\pi_1 = \beta$

(b) $d(\pi_{t_1}, \pi_{t_2}) = |t_1 - t_2| \, d(\alpha, \beta)$

(c) *If $\{x_i\}$ is a basis with respect to which both α and β are canonical, then π_t is also canonical with respect to $\{x_i\}$, and $\pi_t(x_i) = \alpha(x_i)^{1-t}\beta(x_i)^t$.*

Proof. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical. Define γ_t by:

$$\gamma_t(\sum a_i x_i) = \sup_i \{|a_i| \, \alpha(x_i)^{1-t}\beta(x_i)^t\},$$

so that $\gamma_t \in \mathfrak{N}$. We shall show first that $\gamma_t \in P(t)$.

We have $|a_i| \, \alpha(x_i) \leqslant \alpha(\sum a_i x_i)$, so that

$$|a_i|^{1-t}\alpha(x_i)^{1-t} \leqslant \alpha(\sum a_i x_i)^{1-t}.$$

Similarly,
$$|a_i|^t \beta(x_i)^t \leqslant \beta(\sum a_i x_i)^t,$$

so that
$$|a_i| \, \alpha(x_i)^{1-t}\beta(x_i)^t \leqslant \alpha(\sum a_i x_i)^{1-t}\beta(\sum a_i x_i)^t.$$

Since this is so for all i, it follows that $\gamma_t \in P(t)$. Furthermore, for each x, $\gamma(x)$ is bounded from above, as γ ranges through $P(t)$, so that π_t is defined. We have, of course, $\gamma_t \leqslant \pi_t$.

We shall now show that actually $\gamma_t = \pi_t$. Namely,

$$\pi_t(x_i) \leqslant \alpha(x_i)^{1-t}\beta(x_i)^t,$$

so that
$$\pi_t(\sum a_i x_i) \leqslant \sup(|a_i| \, \pi_t(x_i)) \leqslant \sup(|a_i| \, \alpha(x_i)^{1-t}\beta(x_i)^t) = \gamma_t(\sum a_i x_i).$$

Thus, $\pi_t \leqslant \gamma_t$ or $\pi_t = \gamma_t$. This proves assertion (c).

The assertion (a) is obvious, while (b) follows immediately from the formula of Proposition 2.1.

As an immediate corollary, we have:

COROLLARY 2.5. *$\mathfrak{N}$ is arcwise connected.*

Proof. With α and β given, construct π_t as above. It follows from (b) that the map $t \to \pi_t$ is a continuous mapping of the unit interval into $\mathfrak{N}$. Since $\pi_0 = \alpha$ and $\pi_1 = \beta$, the result follows.

PROPOSITION 2.6. *$\mathfrak{N}$ is contractible.*

Proof. Let $\alpha_0 \in \mathfrak{N}$ be given. If $\alpha \in \mathfrak{N}$, let $\pi_t(\alpha)$ be the arc described by Theorem 2.4, with $\pi_0(\alpha) = \alpha_0$ and $\pi_1(\alpha) = \alpha$. Let I be the closed interval $0 \leqslant t \leqslant 1$, and define

$f: I \times \mathfrak{N} \to \mathfrak{N}$ by $f(t, \alpha) = \pi_t(\alpha)$. Then, $f(0, \alpha) = \alpha_0$ while $f(1, \alpha) = \alpha$. Thus, the result will follow when we prove that f is continuous.

We have
$$d(f(t_1, \alpha_1), f(t_2, \alpha_2)) = d(\pi_{t_1}(\alpha_1), \pi_{t_2}(\alpha_2)$$
$$\leqslant d(\pi_{t_1}(\alpha_1), \pi_{t_1}(\alpha_2)) + d(\pi_{t_1}(\alpha_2), \pi_{t_2}(\alpha_2)),$$
so that
$$d(f(t_1, \alpha_1), f(t_2, \alpha_2)) \leqslant d(\pi_{t_1}(\alpha_1), \pi_{t_1}(\alpha_2)) + |t_1 - t_2| \, d(\alpha_2, \alpha_0).$$

We shall now show that
$$d(\pi_t(\alpha), \pi_t(\beta)) \leqslant t d(\alpha, \beta),$$
from which everything will follow.

Let $\{x_i\}$ be a basis with respect to which both α_0 and α are canonical, $\{y_j\}$ a basis with respect to which α_0 and β are canonical. Then, $\pi_t(\alpha)$ is canonical with respect to $\{x_i\}$, while $\pi_t(\beta)$ is canonical with respect to $\{y_j\}$. Furthermore,

$$\pi_t(\alpha)(x_i) = \alpha_0(x_i)^{1-t} \alpha(x_i)^t$$
$$\pi_t(\alpha)(y_j) \leqslant \alpha_0(y_j)^{1-t} \alpha(y_j)^t$$
$$\pi_t(\beta)(x_i) \leqslant \alpha_0(x_i)^{1-t} \beta(x_i)^t$$
$$\pi_t(\beta)(y_j) = \alpha_0(y_j)^{1-t} \beta(y_j)^t.$$

Combining these relations with the formula of Proposition 2.1 gives immediately $d(\pi_t(\alpha), \pi_t(\beta)) \leqslant t d(\alpha, \beta)$. This completes the proof.

Let $\alpha \in \mathfrak{N}$. Denote by $C(\alpha)$ the set of real numbers $\{\log \alpha(x) \mid x \in E, x \neq 0\}$. Choose a basis $\{x_i\}$ with respect to which α is canonical. Then

$$\alpha(\sum a_i x_i) = \sup (m_i |a_i|),$$

and for each non-zero $x \in E$, we have $\log \alpha(x) = \log m_i + \log |a|$, for some $a \in K^*$, some i. This shows that $C(\alpha)$ is the union of a finite number of cosets of $\mathbf{R}/Z \log q$, the number of cosets being no more than $n = \dim E$. We shall call the number of these cosets the *rank* of α, and shall denote it by $r(\alpha)$. In the next section we shall associate multiplicities to the cosets of $C(\alpha)$.

The set $C(\alpha)$ is uniformly discrete in the following sense: there exist positive real numbers d such that, if $r, s \in C(\alpha)$ and $|r - s| \leqslant d$, then $r = s$. We shall call such numbers d *separating numbers* of α.

PROPOSITION 2.7. *Let $\alpha \in \mathfrak{N}$, and let d be a separating number of α. If $\beta \in \mathfrak{N}$ and $d(\alpha, \beta) \leqslant \frac{1}{2} d$, then $r(\beta) \geqslant r(\alpha)$.*

Proof. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical,

$$\alpha(\sum a_i x_i) = \sup (m_i |a_i|), \ \beta(\sum a_i x_i) = \sup (m_i' |a_i|).$$

Then, Proposition 2.1 shows that $d(\alpha, \beta) = \sup |\log m_i - \log m_i'|$. Hence, $|\log m_i - \log m_i'| \leqslant \frac{1}{2} d$, $1 \leqslant i \leqslant n$.

Let $r(\alpha) = r$, and renumber the x_i so that $\log m_1, \ldots, \log m_r$ are incongruent mod $Z \log q$. From the choice of d as a separating number of α, it follows that $\log m_1', \ldots, \log m_r'$ are incongruent mod $Z \log q$, so that $r(\beta) \geqslant r = r(\alpha)$.

COROLLARY 2.8. *The set of* $\beta \in \mathcal{N}$ *for which* $r(\beta) = n$ *is open and everywhere dense in* $\mathcal{N}$.

Proof. Proposition 2.7 shows immediately that the set under consideration is open. To see that the set is everywhere dense, let $\alpha \in \mathcal{N}$ and let $\{x_i\}$ be a basis with respect to which α is canonical. Set $m_i = \alpha(x_i)$. Let $\varepsilon > 0$, and choose real numbers t_i as follows:

$$|t_i| < \varepsilon, \quad \text{and} \quad t_1 + \log m_1, \ldots, t_n + \log m_n$$

are incongruent mod $Z \log q$. Now put

$$\beta(\sum a_i x_i) = \sup (e^{t_i} m_i |a_i|).$$

Then, $\beta \in \mathcal{N}$ and $d(\alpha, \beta) = \sup |t_i| < \varepsilon$. Finally, it is clear that $r(\beta) = n$. Thus, the set of norms of rank n is everywhere dense in $\mathcal{N}$.

THEOREM 2.9. *Let* $\alpha \in \mathcal{N}$ *have rank* n, *let* d *be a separating number of* α, *and let* $\{x_i\}$ *be a basis with respect to which* α *is canonical. Then, if* $d(\alpha, \beta) \leqslant \frac{1}{2} d$, β *is also canonical with respect to* $\{x_i\}$.

Proof. Set $\alpha(x_i) = m_i$. Since $r(\alpha) = n$, and $\alpha(\sum a_i x_i) = \sup (m_i |a_i|)$, the numbers $\log m_1, \ldots, \log m_n$ are incongruent mod $Z \log q$. Because $d(\alpha, \beta) \leqslant \frac{1}{2} d$, we have $|\log \beta(x_i) - \log m_i| \leqslant \frac{1}{2} d$, and since d is a separating number of α, it follows that $\log \beta(x_1), \ldots, \log \beta(x_n)$ are incongruent mod $Z \log q$. Let $x = \sum a_i x_i$ be any non-zero element of E. From the incongruence, mod $Z \log q$, of $\{\log \beta(x_i)\}$, we find that those of the numbers $\beta(x_i) |a_i|$ which are non-zero are distinct. Hence

$$\beta(\sum a_i x_i) = \sup (\beta(x_i) |a_i|),$$

or β is canonical with respect to $\{x_i\}$.

COROLLARY 2.10. *Let* $\mathcal{N}'$ *be the set of all* $\alpha \in \mathcal{N}$ *with* $r(\alpha) = n$. *Then* $\mathcal{N}'$ *is locally Euclidean of dimension* n.

Proof. Let $\alpha\in\mathcal{N}'$, let d be a separating number of α and let $\{x_i\}$ be a basis with respect to which α is canonical. Set $D=\{\beta\,|\,d(\alpha,\beta)<\frac{1}{2}d\}$. Then $D\subset\mathcal{N}'$ is a neighborhood of α, and Theorem 2.9 shows that each element of D is canonical with respect to $\{x_i\}$. Define $f:D\to R^n$ by

$$f(\beta)=\{\log\beta(x_1),\ \dots,\ \log\beta(x_n)\}.$$

Then f is a homeomorphism of D with the open subset of R^n defined by

$$\{(r_1,\ \dots,\ r_n)\,|\,|r_i-\log\alpha(x_i)|<\tfrac{1}{2}d\}.$$

PROPOSITION 2.11. *Let $\{x_i\}$ be a basis of E. Let A be the set of all norms which are canonical with respect to $\{x_i\}$. Then A is a closed subspace of $\mathcal{N}$.*

Proof. Suppose $\alpha\notin A$. Then there are $a_i\in K$, not all 0, such that

$$\sup_i\{\log\alpha(a_ix_i)-\log\alpha(\textstyle\sum a_ix_i)\}=d>0.$$

Now suppose that $\beta\in\mathcal{N}$ such that $d(\alpha,\beta)\leqslant\frac{1}{3}d$. Then, for all non-zero x, we have $|\log\alpha(x)-\log\beta(x)|\leqslant\frac{1}{3}d$, and combining this with the definition of d gives

$$\sup\{\log\beta(a_ix_i)-\log\beta(\textstyle\sum a_ix_i)\}\leqslant\tfrac{2}{3}d.$$

Thus also $\beta\notin A$ which shows that A is closed.

COROLLARY 2.12. *Let $\mathcal{N}'$ be again the set of $\alpha\in\mathcal{N}$ with $r(\alpha)=n$, and let X be a connectedness component of $\mathcal{N}'$. Let $\{x_i\}$ be a basis with respect to which some element of X is canonical. Then every element of X is canonical with respect to $\{x_i\}$.*

Proof. Let A be the set of all norms which are canonical with respect to $\{x_i\}$. Then by Proposition 2.11, $\mathcal{N}'\cap A$ is a closed subset of $\mathcal{N}'$. However, Theorem 2.9 shows that $\mathcal{N}'\cap A$ is open in $\mathcal{N}'$. The assertion follows immediately.

Section 3. The action of Aut (E) on $\mathcal{N}(E)$

We denote by Aut (E) the group of linear automorphisms of E with its natural locally compact topology. Aut (E) acts on $\mathcal{N}(E)$ as follows: if $\sigma\in\mathrm{Aut}\,(E)$ and $\alpha\in\mathcal{N}(E)$, then $\sigma\alpha(x)=\alpha(\sigma^{-1}x)$. It is clear from the definition of the metric on $\mathcal{N}$, that the elements of Aut (E) are represented by *isometries* of $\mathcal{N}$. It is also clear that the subset $\mathcal{L}$ of $\mathcal{N}$ is stable under the action of Aut (E).

PROPOSITION 3.1. *The kernel of the representation of* Aut(E) *by transformations of* $\mathcal{N}(E)$ *consists of the automorphisms* $x \to cx$, *with* $|c| = 1$.

Proof. If for some $x \in E$ the elements x and $\sigma(x)$ are linearly independent, then there exist norms α so that $\alpha(x) \neq \alpha(\sigma x)$. Hence x and $\sigma(x)$ are linearly dependent for all $x \in E$, from which it follows that $\sigma(x) = cx$ with c a fixed element of K. As we have $\alpha(cx) = |c|\alpha(x)$, we conclude that $|c| = 1$. Conversely, it is obvious that any automorphism of the form $x \to cx$, $|c| = 1$ is represented by the identity on $\mathcal{N}$.

If $\alpha \in \mathcal{N}$, we denote by G_α the *isotropy group* of α in Aut(E).

PROPOSITION 3.2. $G_\alpha = \bigcap_t G_{[q^t\alpha]}$.

Proof. The assertion is an immediate consequence of the definition of $[\alpha]$, and Proposition 1.5 (c).

COROLLARY 3.3. *For each* $\alpha \in \mathcal{N}(E)$, *the isotropy group* G_α *is a compact open subgroup of* Aut(E).

Proof. Let L be a lattice and β its norm. If $\{x_i\}$ is a set of free generators of L and σ is in Aut(E) with $\sigma x_i = \sum a_{ij} x_j$, then $\sigma \in G_\beta$ if, and only if, all a_{ij} are in $\mathfrak{O}$ and det (a_{ij}) is a unit in $\mathfrak{O}$. It follows immediately that G_β is a compact open subgroup of Aut(E) (and is in fact a maximal compact subgroup).

If α is any norm, then by the remark following Prop. 1.7, only finitely many of the norms $[q^t\alpha]$ are distinct. Hence, because of Prop. 3.2, G_α is also a compact open subgroup of Aut(E).

Remark. Proposition 2.1 may be used to give an explicit description of the elements of G_α. Let $\{x_i\}$ be a basis with respect to which α is canonical. Let $\sigma \in$ Aut(E), and suppose $\sigma(x_i) = \sum_j a_{ji} x_j$. Then, $\sigma \in G_\alpha$ if, and only if,

$$|a_{ji}| \leq \alpha(x_i)\,\alpha(x_j)^{-1}, \quad i, j = 1, 2, \ldots, n$$

and $|\det(a_{ji})| = 1$.

COROLLARY 3.4. *The map* Aut$(E) \times \mathcal{N}(E) \to \mathcal{N}(E)$ *is continuous.*

Proof. We have

$$d(\sigma\beta, \tau\alpha) \leq d(\sigma\beta, \sigma\alpha) + d(\sigma\alpha, \tau\alpha) = d(\beta, \alpha) + d(\alpha, \sigma^{-1}\tau\alpha).$$

Hence, if $\sigma^{-1}\tau \in G_\alpha$, we obtain $d(\sigma\beta, \tau\alpha) \leq d(\beta, \alpha)$. Since G_α is open, the assertion follows.

PROPOSITION 3.5. *Let α and β be elements of $\mathcal{N}$, and let d be a positive real number. Let X_α be the orbit of α under the action of* $\operatorname{Aut}(E)$, *and let* $D = \{\gamma \in \mathcal{N} \mid d(\beta, \gamma) \leqslant d\}$. *Then $X_\alpha \cap D$ is finite.*

Proof. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical. Set $\alpha(x_i) = r_i$ and $\beta(x_i) = s_i$. Suppose $\sigma \in \operatorname{Aut}(E)$ is such that $\sigma\alpha \in D$. Set

$$\sigma^{-1}(x_i) = \sum_j a_{ij} x_j. \text{ Then } \sigma\alpha(x_i) = \sup_j \{r_j |a_{ij}|\}.$$

From the fact that $d(\sigma\alpha, \beta) \leqslant d$, we get

$$\left| \log \frac{\sigma\alpha(x_i)}{\beta(x_i)} \right| \leqslant d$$

and therefore $$e^{-d} s_i \leqslant \sup_j \{r_j |a_{ij}|\} \leqslant e^d s_i.$$

Hence $|a_{ij}| \leqslant e^d s_i / r_j$. It follows that the set of $\sigma \in \operatorname{Aut}(E)$ for which $\sigma\alpha \in D$ lies in a compact subset of $M_n(K)$. However, the map $\operatorname{Aut}(E) \to \mathcal{N}$ defined by $\sigma \to \sigma\alpha$ is continuous. Hence the set $\{\sigma \in \operatorname{Aut}(E) \mid \sigma\alpha \in D\}$ is a closed subset of $\operatorname{Aut}(E)$, so that it is compact. Since G_α is an open subgroup of $\operatorname{Aut}(E)$, it follows that $X_\alpha \cap D$ is finite.

As an immediate consequence, we have:

COROLLARY 3.6. *The orbit X_α is a closed discrete subset of $\mathcal{N}$.*

Let $\alpha \in \mathcal{N}$ and let $\{x_i\}$ be a basis with respect to which α is canonical. Set $\alpha(x_i) = m_i$. Then, the numbers $\log m_1, \ldots, \log m_n$ are representatives (with possible repetitions) of the cosets of $C(\alpha)$ mod $Z \log q$. Let $r = r(\alpha)$, and suppose the x_i have been renumbered so that $\log m_1, \ldots, m_r$ are incongruent mod $Z \log q$. Let, for $1 \leqslant i \leqslant r$, E_i be the space spanned by all x_j which are such that $\log m_j \equiv \log m_i \pmod{Z \log q}$. Then, E is the direct sum of $E_1, \ldots, E_r$. Furthermore, there is a lattice norm $\lambda_i \in \mathcal{L}(E_i)$ such that the restriction of α to E_i is $m_i \lambda_i$.

The dimension of the space E_i does not depend on the choice of the basis $\{x_i\}$. Namely, suppose $E = E_1' + \ldots + E_r'$ (direct sum). Suppose further that there is a $\lambda_j' \in \mathcal{L}(E_j')$, and a positive real number m_j' such that $\alpha | E_i' = m_i' \lambda_i'$ and $\log m_i \equiv \log m_i'$ $\pmod{Z \log q}$. Let f_i be the projection of E onto E_i, and let x be a non-zero element of E_i'. We have $\alpha(x) = m_i' \lambda_i'(x)$, so that $\log \alpha(x) \equiv \log m_i \pmod{Z \log q}$. At the same time, the non-zero numbers among $m_j \lambda_j f_j(x)$ are distinct, hence $\alpha(x) = \sup_j (m_j \lambda_j f_j(x))$, so that in particular, $f_i(x) \neq 0$. Thus, the restriction of f_i to E_i' maps E_i' monomorphically into E_i, so that $\dim E_i' \leqslant \dim E_i'$. From the symmetry, it follows that $\dim E_i' =$

$\dim E_i$. We shall call $\dim E_i$ the *multiplicity* of the coset (in $C(\alpha)$) which is represented by $\log m_i$. We shall also use the notation $C_m(\alpha)$ to denote the set $C(\alpha)$ together with the assigned multiplicities. It is clear that the sum of the multiplicities of the cosets which comprise $C(\alpha)$ is n.

THEOREM 3.7. *Let α and β be elements of $\mathcal{N}$. Then, a necessary and sufficient condition that α and β be conjugate under the action of* $\mathrm{Aut}(E)$ *is that* $C_m(\alpha) = C_m(\beta)$.

Proof. Suppose first that $\beta = \sigma\alpha$, with $\sigma \in \mathrm{Aut}(E)$. Let $\{x_i\}$ be a basis with respect to which α is canonical, and let $y_i = \sigma^{-1}x_i$. Then β is canonical with respect to $\{y_i\}$, and $\beta(y_i) = \alpha(x_i)$. It is clear that $C_m(\alpha) = C_m(\beta)$.

Now suppose $C_m(\alpha) = C_m(\beta)$. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical, and furthermore such that

$$1 \leqslant \alpha(x_1) \leqslant \alpha(x_2) \leqslant \dots \alpha(x_n) < q.$$

Then each $\alpha(x_i)$ occurs in the set $\{\alpha(x_1, \dots, \alpha(x_n)\}$ as often as the multiplicity of the associated coset in $C(\alpha)$. The numbers $\beta(x_i)$ are not necessarily in increasing order. However, there is an element $\sigma \in \mathrm{Aut}(E)$, such that with $\gamma = \sigma\beta$, we have

$$1 \leqslant \gamma(x_1) \leqslant \gamma(x_2) \leqslant \dots \gamma(x_n) < q.$$

Furthermore, σ is a product of a diagonal transformation with a permutation of the x_i, so that γ is still canonical with respect to $\{x_i\}$. As we have $C_m(\gamma) = C_m(\beta) = C_m(\alpha)$, it follows that $\gamma(x_i) = \alpha(x_i)$ all i. Hence $\gamma = \alpha$, or α and β are conjugate under $\mathrm{Aut}(E)$.

COROLLARY 3.8. *The orbit space* $\mathrm{Aut}(E)\backslash\mathcal{N}(E)$ *is naturally homeomorphic to the symmetric product of n circles.*

Proof. Set $T = R/Z\log q$ so that T is a circle, and let S be the symmetric product of n copies of T. We define a map $h: \mathcal{N}(E) \to S$ as follows: given $\alpha \in \mathcal{N}(E)$, $C(\alpha)/Z\log q$ is a subset of T consisting of $r(\alpha)$ points, each with an assigned multiplicity, the sum of the multiplicities being n. If $t_1, \dots, t_r$ are those points of T, and $\nu_1, \dots, \nu_r$ are their multiplicities, set

$$h(\alpha) = (t_1, t_1, \dots, t_r), \text{ each } t_i \text{ appearing } \nu_i \text{ times.}$$

It is clear that h maps $\mathcal{N}(E)$ onto S. It follows from Theorem 3.7 that the inverse image of a point of S is precisely one orbit of $\mathcal{N}(E)$ under the action of $\mathrm{Aut}(E)$. Hence h defines a $1-1$ map h' of $\mathrm{Aut}(E)\backslash\mathcal{N}(E)$ onto S. To show that h' is a homeomorphism, we shall show that h is a continuous open map.

We show first that h is an open map. Let $\alpha \in \mathcal{N}$, let $d > 0$ be given, and set $D = \{\beta \mid d(\alpha, \beta) < d\}$. Let $\{x_i\}$ be a basis with respect to which α is canonical and such that

$$1 \leqslant \alpha(x_1) \leqslant \alpha(x_2) \leqslant \ldots \leqslant \alpha(x_n) < q.$$

Suppose that $(t_1, \ldots, t_n) \in S$ is such that $t_1 \leqslant t_2 \leqslant \ldots \leqslant t_n$, $|t_i - \log \alpha(x_i)| < d$. Define $\beta \in \mathcal{N}$ by

$$\beta(\sum a_i x_i) = \sup (e^{t_i} |a_i|).$$

Then

$$d(\alpha, \beta) = \sup_i \{|t_i - \log \alpha(x_i)|\} < d,$$

so that $\beta \in D$, while $h(\beta) = (t_1, \ldots, t_n)$. Thus the image of D contains an open set, which contains $h(\alpha)$, so that h is an open map.

To see that h is continuous, let $\alpha, \beta \in \mathcal{N}$ with $d(\alpha, \beta) = d$. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical. Then

$$|\log \alpha(x_i) - \log \beta(x_i)| \leqslant d.$$

Hence, by choosing d sufficiently small, we can make $h(\beta)$ lie in any prescribed neighborhood of $h(\alpha)$. Thus, h is continuous and the proof is complete.

Remark. The structure of the orbit space $\mathrm{Aut}(E) \backslash \mathcal{N}(E)$ makes it possible to define an integration on $\mathcal{N}(E)$ which is invariant under the action of $\mathrm{Aut}(E)$. Namely, let f be a complex-valued function on $\mathcal{N}(E)$ which is continuous with compact support. Let $\alpha \in \mathcal{N}$, and define for $\sigma \in \mathrm{Aut}(E)$, $g(\sigma, \alpha) = f(\sigma\alpha)$. Then, g is a continuous function on $\mathrm{Aut}(E)$ (α is fixed) with compact support. The continuity of g is immediate. Suppose D is the support of f. Then, since the orbit of α is discrete, there are only a finite number of norms $\sigma\alpha$ in D. Hence, g vanishes outside a finite union of cosets mod G_α, and since G_α is compact, it follows that g has compact support. With a Haar measure chosen on $\mathrm{Aut}(E)$, form

$$h(\alpha) = \int_{\mathrm{Aut}(E)} g(\sigma, \alpha)\, d\sigma.$$

Then, h depends only on the orbit of α under $\mathrm{Aut}(E)$, so that it defines a function $\bar{h}$ on the symmetric product of n circles. The ordinary product T_n of n-circles, being a group, carries a Haar measure. We lift $\bar{h}$ to a function h' on T_n, and then define $\int_{T_n} h'$ to be the integral of f on $\mathcal{N}$.

We have shown above that $C_m(\alpha)$ gives a complete set of invariants for equivalence of norms with respect to the group $\mathrm{Aut}(E)$. We now consider the question of equivalence with respect to the elements of the isotropy group G_α of a preassigned norm α. In order to describe the invariants for this type of equivalence we must first consider the extensions of norms from E to the exterior algebra of E.

We denote by ΛE the exterior algebra of E, by $\Lambda_r E$ the homogeneous component of ΛE of degree r. In particular, $\Lambda_0 E = K$ and $\Lambda_1 E = E$. If $\alpha \in \mathfrak{N}(E)$, we shall associate to α a norm $\Lambda_r \alpha$ on $\Lambda_r E$, for $r \geqslant 1$.

Let λ be an element of the dual space E^* of E. Then there is defined a derivation d_λ of ΛE which maps $\Lambda_r E$ into $\Lambda_{r-1} E$, and which coincides with λ on E. Hence, if $\omega \in \Lambda_r E$ and $\lambda_1, \ldots, \lambda_r$ are elements of E^*, then $d_{\lambda_1} \ldots d_{\lambda_r}(\omega) \in K$. For $\alpha \in \mathfrak{N}(E)$, we define, for $\omega \in \Lambda_r E$,

$$\Lambda_r(\alpha)(\omega) = \sup \frac{|d_{\lambda_1} \ldots d_{\lambda_r}(\omega)|}{\alpha^*(\lambda_1) \ldots \alpha^*(\lambda_r)},$$

as $\lambda_1, \ldots, \lambda_r$ range independently over the non-zero elements of E^*. As we have already seen in section 1, the existence of such a supremum lies in the compactness of the space $P(E^*)$. It follows from Prop. 1.2 that $\Lambda_1 \alpha = \alpha$.

It follows without difficulty from the definition that, for $r \geqslant 1$, and $\omega \in \Lambda_{r+1}(E)$, we have

$$\Lambda_{r+1}(\alpha)(\omega) = \sup_{\lambda \in E^*} \frac{\Lambda_r(\alpha)(d_\lambda \omega)}{\alpha^*(\lambda)}.$$

We leave to the reader the details of the verification of the following properties of $\Lambda_r(\alpha)$.

PROPOSITION 3.9. *If α is a norm of E, then $\Lambda_r(\alpha)$ is a norm of $\Lambda_r E$. If α is canonical with respect to the basis $\{x_i\}$ of E, then $\Lambda_r(\alpha)$ is canonical with respect to the basis $\{x_{i_1} \wedge \ldots \wedge x_{i_r}\}$, $(i_1 < i_2 < \ldots < i_r)$ of $\Lambda_r E$, and*

$$\Lambda_r(\alpha)(x_{i_1} \wedge \ldots \wedge x_{i_r}) = \alpha(x_{i_1}) \ldots \alpha(x_{i_r}).$$

If $\sigma \in \mathrm{Aut}(E)$ and $\alpha \in \mathfrak{N}(E)$, then it follows directly from the definition that $\Lambda_r(\sigma\alpha) = \sigma_r \Lambda_r(\alpha)$, where σ_r is the automorphism of $\Lambda_r E$ induced by σ.

Let α and β be two norms of E. We define, for $1 \leqslant r \leqslant n$, the *r-discriminant* $\Delta_r(\beta, \alpha)$ of β with respect to α by

$$\Delta_r(\beta, \alpha) = \sup_{\omega \in \Lambda_r E} \frac{\Lambda_r(\beta)(\omega)}{\Lambda_r(\alpha)(\omega)},$$

where ω ranges over the non-zero elements of $\Lambda_r E$. As usual, the supremum exists because of the compactness of the projective space $P(\Lambda_r E)$.

PROPOSITION 3.10. *Let $\{x_i\}$ be a basis with respect to which both α and β are canonical, and suppose that the elements of the basis are arranged so that*

$$\frac{\beta(x_1)}{\alpha(x_1)} \geqslant \frac{\beta(x_2)}{\alpha(x_2)} \geqslant \dots \geqslant \frac{\beta(x_n)}{\alpha(x_n)}.$$

Then

$$\Delta_r(\beta, \alpha) = \prod_{j=1}^{r} \frac{\beta(x_j)}{\alpha(x_j)}.$$

Proof. Since $\Lambda_r(\alpha)$ is canonical with respect to the basis

$$\{x_{i_1} \wedge \dots \wedge x_{i_r}\} \; (i_1 < i_2 < \dots < i_r) \text{ of } \Lambda_r E,$$

we have

$$\Delta_r(\beta, \alpha) = \sup \frac{\Lambda_r(\beta)(x_{i_1} \wedge \dots \wedge x_{i_r})}{\Lambda_r(\alpha)(x_{i_1} \wedge \dots \wedge x_{i_r})},$$

the supremum being taken over the set of r-tuples $(i_1 < \dots < i_r)$. However, we have

$$\frac{\Lambda_r(\beta)(x_{i_1} \wedge \dots \wedge x_{i_r})}{\Lambda_r(\alpha)(x_{i_1} \wedge \dots \wedge x_{i_r})} = \prod_{j=1}^{r} \frac{\beta(x_{i_j})}{\alpha(x_{i_j})}.$$

It follows immediately from the fact that

$$\frac{\beta(x_1)}{\alpha(x_1)} \geqslant \frac{\beta(x_2)}{\alpha(x_2)} \geqslant \dots \geqslant \frac{\beta(x_n)}{\alpha(x_n)},$$

that the supremum occurs for the r-tuple $(1, 2, \dots, r)$, and hence that

$$\Delta_r(\beta, \alpha) = \prod_{j=1}^{r} \frac{\beta(x_j)}{\alpha(x_j)}.$$

Using the same notation as above, it follows from the proposition that the numbers $\beta(x_j)/\alpha(x_j)$ are determined by the discriminants $\Delta_r(\beta, \alpha)$ and do not depend on the choice of the basis $\{x_i\}$. Thus, if α and β are two norms, and $\{x_i\}$ is a basis with respect to which both α and β are canonical, then the unordered n-tuple $\{\beta(x_1)/\alpha(x_1), \dots, \beta(x_n)/\alpha(x_n)\}$ is completely determined, including multiplicities, by α and β, and does not depend on the choice of the basis. We shall call that (unordered) n-tuple of real numbers the *invariants* of β with respect to α, and shall denote it by $I(\beta, \alpha)$. If $0 \leqslant t \leqslant 1$ we consider also the invariants $I(\beta, [q^t\alpha])$. Considered as a function of t, the invariants $I(\beta, [q^t\alpha])$ will be called the *elementary divisors* of β with respect to α.

If $\sigma \in \mathrm{Aut}(E)$, then the definition of $I(\beta, \alpha)$ shows immediately that $I(\sigma\beta, \sigma\alpha) = I(\beta, \alpha)$. In particular, the elementary divisors of $\sigma\beta$ with regard to $\sigma\alpha$ are the same as those of β with respect to α.

We shall use the elementary divisors to give a criterion for the equivalence of two norms with respect to the isotropy group of a third norm.

LEMMA 3.10. *Let α and β be two norms and let $\{x_i\}$ be a basis with respect to which α is canonical. Then, there is a $\sigma \in G_\alpha$ such that $\sigma\beta$ is canonical with respect to $\{x_i\}$.*

Proof. Let $\{y_i\}$ be a basis with respect to which both α and β are canonical. According to our description of $C_m(\alpha)$, the set of n numbers $\{\log \alpha(x_1), \ldots, \log \alpha(x_n)\}$ represent the same cosets, $\mathrm{mod}\, Z \log q$, as do the numbers $\{\log \alpha(y_1), \ldots, \log \alpha(y_n)\}$, each coset being represented the same number of times in the first set as in the second. Hence, by renumbering the y_i, we have $\alpha(x_i) = q^{h_i} \alpha(y_i)$, with $h_i \in Z$.

Define $\sigma \in \mathrm{Aut}(E)$ by $\sigma(y_i) = \pi^{h_i} x_i$. Then, because α is canonical with respect to $\{y_i\}$, $\sigma\alpha$ is canonical with respect to $\{x_i\}$. At the same time,

$$\sigma\alpha(x_i) = \alpha(\sigma^{-1} x_i) = q^{h_i} \alpha(y_i) = \alpha(x_i),$$

and hence $\sigma \in G_\alpha$. Finally, because β is canonical with respect to $\{y_i\}$, it follows that $\sigma\beta$ is canonical with respect to $\{x_i\}$.

We choose a norm α which will be fixed for the rest of this section. Let $\{x_i\}$ be a basis with respect to which α is canonical, and such that

$$\frac{1}{q} < \alpha(x_1) \leqslant \alpha(x_2) \leqslant \ldots \leqslant \alpha(x_n) \leqslant 1.$$

This basis will also be kept fixed. With respect to the basis $\{x_i\}$, we have $[\alpha](x_i) = 1$.

Using the basis $\{x_i\}$ we identify $\mathrm{Aut}(E)$ with $GL(n, K)$ as follows: to $\sigma \in \mathrm{Aut}(E)$ we associate the matrix (a_{ji}) given by $\sigma x_i = \sum a_{ji} x_j$.

Let g be the rank of α, and let $\nu_1, \ldots, \nu_g$ be the multiplicities of the $\alpha(x_i)$. Namely,

$$\alpha(x_1) = \ldots = \alpha(x_{\nu_1}) < \alpha(x_{\nu_1+1}) = \ldots = \alpha(x_{\nu_1+\nu_2}) < \text{etc}.$$

We place along the main diagonal of a generic $n \times n$ matrix square blocks of size $\nu_1, \nu_2, \ldots, \nu_g$. Then, the elements of G_α are the matrices with coefficients in $\mathfrak{O}$, whose determinant is a unit in $\mathfrak{O}$ and whose elements to the left of the aforementioned diagonal blocks are in $\mathfrak{p}$. In passing, we observe that the elements $\sigma \in \mathrm{Aut}(E)$ having the property $\sigma\alpha \geqslant \alpha$ are exactly those matrices with the properties just described for the elements of G_α except for the condition on the determinant.

The symmetric group $\mathfrak{S}_n$ of degree n is considered as a subgroup of $\operatorname{Aut}(E)$ acting by permutation of the x_i. The group $\mathfrak{S}_n$ is a subgroup of $G_{[\alpha]}$. We consider also the direct product $\mathfrak{S}_\alpha = \mathfrak{S}_{\nu_1} \times \ldots \times \mathfrak{S}_{\nu_g}$ as a subgroup of $\mathfrak{S}_n$ in the obvious fashion. Clearly $\mathfrak{S}_n \cap G_\alpha = \mathfrak{S}_\alpha$.

LEMMA 3.11. *Let β and γ be two norms each of which is canonical with respect to $\{x_i\}$. If $I(\beta, [q^t\alpha]) = I(\gamma, [q^t\alpha])$ for all t, then there is a $\sigma \in \mathfrak{S}_\alpha$ such that $\gamma = \sigma\beta$.*

Proof. For convenience, we set $\mu_j = \nu_1 + \ldots + \nu_j$. Suppose $0 \leqslant t \leqslant 1$, and $q^t\alpha(x_{\mu_j}) \leqslant 1$, $q^t\alpha(x_{\mu_j+1}) > 1$. Then it is easy to verify that $[q^t\alpha](x_i) = 1$ for $i \leqslant \mu_j$ and $[q^t\alpha](x_i) = q$ for $i > \mu_j$. Hence, the hypothesis on β and γ implies that for $j = 1, \ldots, g$ we have

$$\{\beta(x_1), \ldots, \beta(x_{\mu_j}),\ q^{-1}\beta(x_{\mu_j+1}), \ldots, q^{-1}\beta(x_n)\} = \{\gamma(x_1), \ldots, \gamma(x_{\mu_j}),\ q^{-1}\gamma(x_{\mu_j+1}), \ldots, q^{-1}\gamma(x_n)\}.$$

By equality, we mean multiplicity of repetitions but disregarding order.

Let h be any positive integer. We form the sum of the hth powers of the elements of the two sets just considered. Then, we have

$$\sum_{i=1}^{\mu_j} \beta(x_i)^h + q^{-h} \sum_{i>\mu_j} \beta(x_i)^h = \sum_{i=1}^{\mu_j} \gamma(x_i)^h + q^{-h} \sum_{i>\mu_j} \gamma(x_i)^h.$$

Assigning to j successively the values $1, 2, \ldots, g$ leads to the following:

$$\sum_{i=1}^{\nu_1} \beta(x_i)^h = \sum_{i=1}^{\nu_1} \gamma(x_i)^h, \quad \sum_{i=\nu_1+1}^{\nu_1+\nu_2} \beta(x_i)^h = \sum_{i=\nu_1+1}^{\nu_1+\nu_2} \gamma(x_i)^h,$$

and so on. Since these relations hold for all $h \geqslant 0$, we conclude that

$$\{\beta(x_1), \ldots, \beta(x_{\nu_1})\} = \{\gamma(x_1), \ldots, \gamma(x_{\nu_1})\},$$

$\{\beta(x_{\nu_1+1}), \ldots, \beta(x_{\nu_1+\nu_2})\} = \{\gamma(x_{\nu_1+1}), \ldots, \gamma(x_{\nu_1+\nu_2})\}$, etc. Thus, there is an element $\sigma \in \mathfrak{S}_\alpha$ such that $\sigma\beta(x_i) = \gamma(x_i)$ for all i. Since β is canonical with respect to $\{x_i\}$, the same is the case for $\sigma\beta$, and since γ is also canonical with respect to $\{x_i\}$, we conclude finally that $\gamma = \sigma\beta$.

COROLLARY 3.12. *Let β and γ be two norms. Then, the following statements are equivalent:*

(i) *There is a $\tau \in G_\alpha$ with $\gamma = \tau\beta$*

(ii) *$I(\beta, [q^t\alpha]) = I(\gamma, [q^t\alpha])$, for all t.*

Proof.

(i) ⇒ (ii).

This implication follows immediately from the definition of the elementary divisors.

(ii) ⇒ (i).

By Lemma 3.10 we can find elements $\varrho, \sigma, \in G_\alpha$ such that $\varrho\beta$ and $\sigma\gamma$ are canonical with respect to $\{x_i\}$. Since $I(\varrho\beta, [q^t\alpha]) = I(\beta, [q^t\alpha])$, with a similar statement for γ, Lemma 3.11 may be applied to give the desired conclusion.

We denote by D the group of diagonal matrices whose elements are powers of π and by $\mathfrak{G}$ the group generated by D and $\mathfrak{S}_n$. Clearly D is a normal subgroup of $\mathfrak{G}$ and $\mathfrak{G}$ is the semi-direct product of D and $\mathfrak{S}_n$.

PROPOSITION 3.13. $\mathfrak{G} \cap \mathfrak{G}_\alpha = \mathfrak{S}_\alpha$.

Proof. Obviously $\mathfrak{S}_\alpha \subset \mathfrak{G} \cap \mathfrak{G}_\alpha$. Suppose $\delta\omega \in \mathfrak{G} \cap G_\alpha$ with $\delta \in D$ and $\omega \in \mathfrak{S}_n$. Since $1/q < \alpha(x_i) \leqslant 1$, it follows immediately that $\delta = 1$ and hence that $\omega \in \mathfrak{S}_\alpha$.

THEOREM 3.14. $\mathrm{Aut}(E) = G_\alpha \mathfrak{G} G_\alpha$.

Proof. Let $\sigma \in \mathrm{Aut}(E)$ and set $\beta = \sigma\alpha$. By lemma 3.10, there is a $\varrho \in G_\alpha$ such that $\varrho\beta = \varrho\sigma\alpha$ is canonical with respect to $\{x_i\}$. Hence, from the properties of $C_m(\alpha)$, there is a $\tau \in \mathfrak{G}$ such that $\tau\varrho\sigma\alpha = \alpha$. But this shows that $\tau\varrho\sigma \in G_\alpha$ or $\sigma \in G_\alpha \mathfrak{G} G_\alpha$.

The theorem just proved asserts that each double coset of $\mathrm{Aut}(E)$ with respect to G_α is represented by an element of $\mathfrak{G}$. We consider now the question of when two elements of $\mathfrak{G}$ represent the same double coset.

THEOREM 3.15. *Suppose that ϱ and σ are in $\mathfrak{G}$ with $\varrho \in G_\alpha \sigma G_\alpha$. Then $\varrho \in \mathfrak{S}_\alpha \sigma \mathfrak{S}_\alpha$.*

Proof. We have $\varrho = \lambda\sigma\mu$ with $\lambda, \mu \in G_\alpha$. Hence, $\varrho\alpha = \lambda\sigma\alpha$ so that $I(\varrho\alpha, [q^t\alpha]) = I(\sigma\alpha, [q^t\alpha])$, for all t. Also, because $\varrho, \sigma \in \mathfrak{G}$, both $\varrho\alpha$ and $\sigma\alpha$ are canonical with respect to $\{x_i\}$. It follows from Lemma 3.11 that $\varrho\alpha = \tau\sigma\alpha$, with $\tau \in \mathfrak{S}_\alpha$. Hence, $\sigma^{-1}\tau^{-1}\varrho \in G_\alpha$, while clearly $\sigma^{-1}\tau^{-1}\varrho \in \mathfrak{G}$. Since $\mathfrak{G} \cap G_\alpha = \mathfrak{S}_\alpha$, we find that $\varrho \in \mathfrak{S}_\alpha \sigma \mathfrak{S}_\alpha$.

Section 4. Quadratic forms

From now on we assume that the characteristic of K is not 2. By a *non-degenerate quadratic form* we shall mean a mapping $\varphi: E \to K$ which is such that

$$\varphi(ax) = a^2\varphi(x), \text{ and } B(x, y) = \varphi(x+y) - \varphi(x) - \varphi(y)$$

is a non-degenerate bilinear form on E. We shall say that φ is *definite* if $\varphi(x)=0$ implies $x=0$, otherwise φ is *indefinite*. We denote the orthogonal group of φ by $O(\varphi)$.

THEOREM 4.1. *Let φ be a definite quadratic form. Then $|\varphi|^{\frac{1}{2}}$ is a norm on E.*

Proof. It is clear that we need only prove that $|\varphi(x+y)|\leqslant \sup(|\varphi(x)|, |\varphi(y)|)$. Suppose the contrary is the case for a pair of elements x, y of E, i.e., $|\varphi(x+y)|>\sup(|\varphi(x)|, |\varphi(y)|)$. Then it is clear that x and y are linearly independent. Set $\varphi(x)=a$, $\varphi(y)=c$ and $B(x,y)=b$. Then we have $|b|>|a|$ and also $|b|>|c|$. With t an arbitrary element of K, we have

$$\frac{c}{b^2}\varphi\left(x+\frac{b}{c}ty\right)=t^2+t+\frac{ac}{b^2}.$$

(Note that we have tacitly assumed that $c\neq 0$. That is so because φ is definite.) Now $|ac/b^2|<1$, so that the polynomial t^2+t+ac/b^2 has a simple zero in the field $\mathfrak{O}/\pi\mathfrak{O}$, hence by Hensel's lemma it has a zero in K. This contradicts the fact that φ is definite and therefore we conclude that $|\varphi|^{\frac{1}{2}}$ is indeed a norm.

Given φ, we denote by $\mathcal{N}(\varphi)$ the set of those norms α on E having the property $|\varphi(x)|^{\frac{1}{2}}\leqslant\alpha(x)$, all $x\in E$. It is easy to see that $\mathcal{N}(\varphi)$ is not empty. For, let β be any norm on E. Then $|\varphi(x)|^{\frac{1}{2}}/\beta(x)$, $x\neq 0$ defines a continuous function on the compact space $P(E)$, and is therefore bounded. Hence there is some positive real number c such that $c\beta\in\mathcal{N}(\varphi)$. We shall also use that notation $\mathcal{L}(\varphi)$ for $\mathcal{L}\cap\mathcal{N}(\varphi)$. It is clear that both $\mathcal{N}(\varphi)$ and $\mathcal{L}(\varphi)$ are stable under the action of $O(\varphi)$.

We shall be interested in the set of elements of $\mathcal{N}(\varphi)$ which are minimal (in that set) in the partial ordering of $\mathcal{N}$. In order to prove that such minimal elements exist, it will be useful to extend the notion of norm by defining a *semi-norm* on E to be a real-valued function α on E such that:

(1) $\alpha(x)\geqslant 0$

(2) $\alpha(ax)=|a|\,\alpha(x)$

(3) $\alpha(x+y)\leqslant\sup(\alpha(x),\alpha(y))$.

Let $\mathcal{S}$ be the set of all semi-norms, and let

$$\mathcal{S}(\varphi)=\{\alpha\in\mathcal{S}\mid |\varphi(x)|^{\frac{1}{2}}\leqslant\alpha(x),\quad\text{all}\quad x\in E\}.$$

LEMMA 4.2. $\mathcal{S}(\varphi)=\mathcal{N}(\varphi)$.

Proof. Let α be a semi-norm such that $|\varphi(x)|\leqslant\alpha(x)^2$ for all x, and suppose that $\alpha(y)=0$. If x is any element of E and a any element of K, we have $\alpha(x+ay)\leqslant\alpha(x)$. Now,

$$|B(x, ay)| = |\varphi(x+ay) - \varphi(x) - \varphi(ay)|$$

and,
$$|\varphi(x+ay)| \leqslant \alpha(x+ay)^2 \leqslant \alpha(x)^2,$$

$$|\varphi(x)| \leqslant \alpha(x)^2, \text{ while } \varphi(ay) = 0.$$

Hence,
$$|a|\,|B(x, y)| = |B(x, ay)| \leqslant \alpha(x)^2.$$

Since this relation holds for all $a \in K$ and all $x \in E$, we have $B(x, y) = 0$ for all x, so that $y = 0$ from the fact that φ is non-degenerate. Thus, α is a norm and

$$\mathcal{S}(\varphi) = \mathcal{N}(\varphi).$$

LEMMA 4.3. *Let $\mathcal{S}'$ be any totally ordered subset of $\mathcal{S}$, and let*

$$\beta(x) = \inf\,\{\alpha(x) \,|\, \alpha \in \mathcal{S}'\}.$$

Then $\beta \in \mathcal{S}$.

Proof. It is clear that β satisfies the first two conditions above in the definition of semi-norm; we must verify that the third condition holds. Suppose on the contrary that $\beta(x+y) > \sup\,(\beta(x), \beta(y))$ for some pair of elements of E. Choose a positive real ε such that

$$\varepsilon < \beta(x+y) - \sup\,(\beta(x), \beta(y)).$$

Then, there exist α and α' in S' such that

$$\alpha(x) \leqslant \beta(x) + \varepsilon$$

$$\alpha'(y) \leqslant \beta(y) + \varepsilon.$$

If we replace either α or α' by a smaller element of $\mathcal{S}'$, these relations will remain valid. As $\mathcal{S}'$ is totally ordered, one of the inequalities $\alpha \leqslant \alpha'$, $\alpha' \leqslant \alpha$ must be valid; let us suppose that it is the latter relation. Thus,

$$\alpha'(x) \leqslant \beta(x) + \varepsilon$$

$$\alpha'(y) \leqslant \beta(y) + \varepsilon$$

while
$$\alpha'(x+y) \leqslant \sup\,(\alpha'(x), \alpha'(y)) \leqslant \sup\,(\beta(x), \beta(y)) + \varepsilon < \beta(x+y).$$

This is impossible from the definition of β. Thus, β is a semi-norm.

COROLLARY 4.4. *If $\alpha \in \mathcal{N}(\varphi)$, then there is a minimal element $\beta \in \mathcal{N}(\varphi)$ with $\beta \leqslant \alpha$. Hence in particular, $\mathcal{N}(\varphi)$ has minimal elements.*

Proof. We apply Zorn's lemma. If S' is a totally ordered subset of $\mathcal{N}(\varphi)$, and we set $\beta(x)=\inf\{\gamma(x)\,|\,\gamma\in S'\}$, then by Lemma 4.3 β is a semi-norm. At the same time it is clear that $\beta\in S(\varphi)$. But by Lemma 4.2 this shows that β is in fact in $\mathcal{N}(\varphi)$. This shows that Zorn's lemma may be applied to the set $\{\gamma\in\mathcal{N}(\varphi)\,|\,\gamma\leqslant\alpha\}$ and hence shows that this set has a minimal element.

We shall denote by $\mathcal{M}(\varphi)$ the set of minimal elements of $\mathcal{N}(\varphi)$. The same argument as above shows also that $\mathcal{L}(\varphi)$ has minimal elements; we shall denote by $\mathcal{L}_m(\varphi)$ the set of minimal elements of $\mathcal{L}(\varphi)$. One should not suppose that $\mathcal{L}_m(\varphi)$ coincides with $\mathcal{L}(\varphi)\cap\mathcal{M}(\varphi)$; in general these sets are distinct. It is clear that both $\mathcal{M}(\varphi)$ and $\mathcal{L}_m(\varphi)$ are stable under the action of $O(\varphi)$.

Theorem 4.1 shows that $\mathcal{M}(\varphi)$ has only one element when φ is definite. As a consequence, we have:

THEOREM 4.5. *If φ is definite, then $O(\varphi)$ is compact.*

Proof. Since $\mathcal{M}(\varphi)$ is stable under the action of $O(\varphi)$, we have immediately $O(\varphi)\subset G_{|\varphi|^{\frac{1}{2}}}$. However, $G_{|\varphi|^{\frac{1}{2}}}$ is compact and $O(\varphi)$ is closed, hence $O(\varphi)$ is compact. (See Ono [4].)

The converse of Theorem 4.5 is trivial.

There is an intimate connection between $\mathcal{M}(\varphi)$ and the function $|\varphi|$. We have:

PROPOSITION 4.6. *For each $x\in E$, we have*

$$|\varphi(x)|=\inf_{\alpha\in\mathcal{M}(\varphi)}\alpha(x)^2.$$

Proof. It follows immediately from Corollary 4.4. that $\inf_{\alpha\in\mathcal{M}(\varphi)}\alpha(x)^2=\inf_{\beta\in\mathcal{N}(\varphi)}\beta(x)^2$. Let x be a non-isotropic vector of φ. Then, there is a basis $\{x_i\}$ such that $x_1=x$ and φ is diagonal with respect to $\{x_i\}$; $\varphi(\sum a_i x_i)=\sum_i \varkappa_i a_i^2$. Define $\beta\in\mathcal{N}$ by $\beta(\sum a_i x_i)=\sup_i\{|\varkappa_i|^{\frac{1}{2}}|a_i|\}$. Clearly, $\beta\in\mathcal{N}(\varphi)$, and $|\varphi(x_1)|=\beta(x_1)^2$.

Suppose now that $x\neq 0$ is an isotropic vector of φ. Choose y isotropic with $B(x,y)=1$. Let $H=Kx+Ky$, and let H' be the orthogonal complement of H with respect to φ. We note the following. Suppose $\alpha\in\mathcal{N}(\varphi|_H)$ and $\beta\in\mathcal{N}(\varphi|_{H'})$. Define γ through $\gamma(z+z')=\sup(\alpha(z),\beta(z'))$, where $z\in H$ and $z'\in H'$. Then, $\gamma\in\mathcal{N}(\varphi)$. Thus, we are reduced to the case where $E=H$.

Let h be any integer; define

$$\beta(ax+by)=\sup(q^h|a|,\,q^{-h}|b|).$$

Then, it is easy to check that $\beta\in\mathcal{N}(\varphi)$. At the same time, $\beta(x)=q^h$, while h is arbitrary. The result follows immediately.

A much stronger form of this proposition will be proved at the end of this section when more detailed information about the structure of $\mathfrak{M}(\varphi)$ will be available

It will be convenient for later purposes to note the following: with α any norm we have:

$$\alpha \in \mathfrak{N}(\varphi) \Leftrightarrow q^{\frac{1}{2}} \alpha \in \mathfrak{N}(\pi^{-1}\varphi)$$

$$\alpha \in \mathfrak{M}(\varphi) \Leftrightarrow q^{\frac{1}{2}} \alpha \in \mathfrak{M}(\pi^{-1}\varphi).$$

PROPOSITION 4.7. *Let L be a lattice in E and let α be its norm. Then, a necessary and sufficient condition that $\alpha \in \mathfrak{L}(\varphi)$ is that $|\varphi| \leqslant 1$ on L. A necessary and sufficient condition that $\alpha \in \mathfrak{L}_m(\varphi)$ is that L be maximal in the set of lattices with the above property.*

Proof. Suppose $\alpha \in \mathfrak{L}(\varphi)$. If $x \in L$, we have $|\varphi(x)|^{\frac{1}{2}} \leqslant \alpha(x) \leqslant 1$. Suppose now that $|\varphi| \leqslant 1$ on L. Let x be any non-zero element of E; determine the integer h such that $\pi^h x \in L$ but $\pi^{h-1} x \notin L$. Then, $\alpha(x) = q^h$. Now $|\varphi(\pi^h x)| \leqslant 1$, whence $|\varphi(x)| \leqslant q^{2h} = \alpha(x)^2$ or $\alpha \in \mathfrak{L}(\varphi)$. The second assertion follows immediately from the first.

We now use some of the relations between norms and lattices described in section 1.

PROPOSITION 4.8. *Let $\alpha \in \mathfrak{N}$. Then the following statements are equivalent:*

(i) $\alpha \in \mathfrak{N}(\varphi)$

(ii) (a) $[\alpha] \in \mathfrak{L}(\varphi)$

(b) $[q^t \alpha] \in \mathfrak{L}(\pi^{-1}\varphi)$ for $0 < t \leqslant \frac{1}{2}$

(c) $[q^t \alpha] \in \mathfrak{L}(\pi^{-2}\varphi)$ for $\frac{1}{2} < t \leqslant 1$.

Proof.

(i) $\Rightarrow$ (ii):

We have $|\varphi(x)| \leqslant \alpha(x)^2$ and $\alpha(x) \leqslant q^{-t}[q^t \alpha](x)$. In particular, for $t = 0$ we get $[\alpha] \in \mathfrak{L}(\varphi)$. Suppose $0 < t \leqslant \frac{1}{2}$. Then $[q^t \alpha](x)^2 \geqslant q^{2t}|\varphi(x)|$, while both $[q^t \alpha](x)$ and $|\varphi(x)|$ are integral powers of q (unless $\varphi(x) = 0$). Hence $[q^t \alpha](x)^2 \geqslant q|\varphi(x)|$, i.e., $[q^t \alpha] \in \mathfrak{L}(\pi^{-1}\varphi)$.

Statement (c) follows from (b) by replacing φ by $\pi^{-1}\varphi$ and α by $q^{\frac{1}{2}}\alpha$.

(ii) $\Rightarrow$ (i):

We have

$$\alpha(x) = \inf_{0 \leqslant t < 1} q^{-t}[q^t \alpha](x).$$

We need only show that $q^{-2t}[q^t \alpha](x)^2 \geqslant |\varphi(x)|$, to obtain the desired result. But this inequality follows immediately from ii.

THEOREM 4.9.[1] *Let* $\alpha \in \mathcal{N}$. *Then the following conditions are equivalent:*

(i) $\alpha \in \mathcal{M}(\varphi)$

(ii) (a) $[\alpha] \in \mathcal{L}_m(\varphi)$

(b) $[q^{\frac{1}{2}}\alpha] \in \mathcal{L}_m(\pi^{-1}\varphi)$

(c) $[q^t\alpha] = [q^{\frac{1}{2}}\alpha]$ for $0 < t \leq \frac{1}{2}$

(d) $[q^t\alpha] = q[\alpha]$ for $\frac{1}{2} < t \leq 1$.

Proof.

(i) $\Rightarrow$ (ii):

It follows from Proposition 4.8 that $[\alpha] \in \mathcal{L}(\varphi)$ and that $[q^{\frac{1}{2}}\alpha] \in \mathcal{L}(\pi^{-1}\varphi)$. If $0 < t \leq \frac{1}{2}$, then $[q^t\alpha] \leq [q^{\frac{1}{2}}\alpha]$, while, again by Proposition 4.8, $[q^t\alpha] \in \mathcal{L}(\pi^{-1}\varphi)$. Hence (b) $\Rightarrow$ (c). In a similar fashion (a) $\Rightarrow$ (d). By replacing φ by $\pi^{-1}\varphi$ and α by $q^{\frac{1}{2}}\alpha$, we see also that (a) $\Rightarrow$ (b). Thus, we must prove (a).

Let $\mu \in \mathcal{L}(\varphi)$ be such that $\mu \leq [\alpha]$. We shall show that $\mu = [\alpha]$. Define

$$L_0 = \{x \mid \alpha(x) \leq 1\}$$
$$L_{\frac{1}{2}} = \{x \mid \alpha(x) \leq q^{-\frac{1}{2}}\}$$
$$L_0' = \{x \mid \mu(x) \leq 1\}$$
$$L_{\frac{1}{2}}' = L_{\frac{1}{2}} + \pi L_0'.$$

Then $[\alpha]$ is the norm of L_0, $[q^{\frac{1}{2}}\alpha]$ is the norm of $L_{\frac{1}{2}}$. Also $\pi L_0 \subset L_{\frac{1}{2}} \subset L_0$, $\pi L_0' \subset L_{\frac{1}{2}}' \subset L_0'$ and $L_0 \subset L_0'$.

Denote by ν the norm of the lattice $L_{\frac{1}{2}}'$.

Set
$$\beta_t = \begin{cases} \mu & t = 0 \\ \nu & 0 < t \leq \frac{1}{2} \\ q\mu & \frac{1}{2} < t \leq 1. \end{cases}$$

Then by Proposition 1.7 there is a $\beta \in \mathcal{N}$ such that $[q^t\beta] = \beta_t$. Clearly $\beta_t \leq [q^t\alpha]$, hence $\beta \leq \alpha$. We shall show that $\beta \in \mathcal{N}(\varphi)$. Since $\alpha \in \mathcal{M}(\varphi)$, it will follow that $\beta = \alpha$ and hence that $\mu = [\alpha]$. This will show that $[\alpha] \in \mathcal{L}_m(\varphi)$.

In order to show that $\beta \in \mathcal{N}(\varphi)$, Proposition 4.8 requires that we prove that $\beta_0 \in \mathcal{L}(\varphi)$ and that $\beta_{\frac{1}{2}} \in \mathcal{L}(\pi^{-1}\varphi)$. That $\beta_0 \in \mathcal{L}(\varphi)$ is so by the choice of μ. Hence we are left with proving that $\nu \in \mathcal{L}(\pi^{-1}\varphi)$, or because of Proposition 4.7, with proving that $|\pi^{-1}\varphi| \leq 1$ on $L_{\frac{1}{2}}'$.

Let $y \in L_{\frac{1}{2}}$ and $z \in L_0'$. Then

---

[1] We wish to thank M. Sato for suggesting the possibility of characterizing the elements $\alpha \in \mathcal{M}(\varphi)$ by properties of $[q^t\alpha]$.

$$\varphi(y+\pi z)=\varphi(y)+\pi^2\varphi(z)+\pi B(y,z)$$
$$=\varphi(y)+\pi^2\varphi(z)+\pi\varphi(y+z)-\pi\varphi(y)-\pi\varphi(z)$$

so that

$$|\pi^{-1}\varphi(y+\pi z)|\leqslant \sup\{|\pi^{-1}\varphi(y)|,\ |\pi\varphi(z)|,\ |\varphi(y+z)|,\ |\varphi(y)|,\ |\varphi(z)|\}.$$

Now,

$$y\in L_{\frac{1}{2}}\Rightarrow|\pi^{-1}\varphi(y)|\leqslant 1$$
$$z\in L_0'\Rightarrow|\varphi(z)|\leqslant 1\Rightarrow|\pi\varphi(z)|\leqslant 1$$
$$y+z\in L_{\frac{1}{2}}+L_0'\subset L_0'\Rightarrow|\varphi(y+z)|\leqslant 1.$$

Hence

$$|\pi^{-1}\varphi(y+\pi z)|\leqslant 1 \text{ as desired.}$$

(ii) $\Rightarrow$ (i):

Suppose that $\beta\leqslant\alpha$ with $\beta\in\mathfrak{N}(\varphi)$. Then $[q^t\beta]\leqslant[q^t\alpha]$ for all t. Hence by Proposition 4.8 we conclude that $[\beta]=[\alpha]$ and $[q^{\frac{1}{2}}\beta]=[q^{\frac{1}{2}}\alpha]$. Let $0<t\leqslant\frac{1}{2}$. Again by Proposition 4.8, $[q^t\beta]\in\mathfrak{L}(\pi^{-1}\varphi)$ while

$$[q^t\beta]\leqslant[q^{\frac{1}{2}}\beta]=[q^{\frac{1}{2}}\alpha],\ \text{so that}\ [q^t\beta]=(q^{\frac{1}{2}}\beta].$$

Similarly, if $\frac{1}{2}<t\leqslant 1$, then $[q^t\beta]=q[\beta]$. This shows that $\alpha\in\mathfrak{M}(\varphi)$ and completes the proof of the theorem.

The theorem just proved shows that $\mathfrak{M}(\varphi)$ may be identified with a subset of $\mathfrak{L}_m(\varphi)\times\mathfrak{L}_m(\pi^{-1}\varphi)$. Namely with the set of $(\alpha,\beta)\in\mathfrak{L}_m(\varphi)\times\mathfrak{L}_m(\pi^{-1}\varphi)$ for which $\alpha\leqslant\beta\leqslant q\alpha$.

PROPOSITION 4.10. *Let φ be an indefinite non-degenerate quadratic form and $y\neq 0$ an isotropic vector of φ. Let $\alpha\in\mathfrak{L}_m(\varphi)$. Then, $\alpha(y)=\sup\{|B(x,y)|\}$, the sup being taken over the lattice $L=\{x|\alpha(x)\leqslant 1\}$.*

Proof. According to Proposition 4.7, $|\varphi|\leqslant 1$ on L and L is a maximal lattice with respect to this property. Define the integer m by $\alpha(y)=q^m$, and set $y_1=\pi^m y$. Then $\alpha(y_1)=1$, and $y_1\in L$. Hence, for all $x\in L$ we have $|\varphi(x+y_1)|\leqslant 1$. It follows immediately that

$$|B(x,y_1)|\leqslant 1,\quad \text{for all}\quad x\in L.$$

Set

$$\sup_{x\in L}|B(x,y_1)|=q^h,\ \text{and}\ y_2=\pi^h y_1.$$

Then, $|B(x,y_2)|\leqslant 1$ for $x\in L$. It follows from this, that $|\varphi|\leqslant 1$ on the lattice $L+\mathfrak{O}y_2$ and hence that $y_2\in L$ from the maximality of L. Hence $\alpha(y_2)\leqslant 1$, or $h\geqslant 0$. However we have $|B(x,y_1)|\leqslant 1$, for $x\in L$, so that $h\leqslant 0$. Thus, $h=0$ and hence

$$\sup_{x\in L}|B(x,y_1)|=1,\ \text{or}\ \sup_{x\in L}|B(x,y)|=\alpha(y).$$

THEOREM 4.11. *Let* φ *be an indefinite non-degenerate quadratic form, and let* $\alpha \in \mathcal{M}(\varphi)$. *Then there exist isotropic vectors* y_1 *and* y_2 *such that:*

(1) $B(y_1, y_2) = 1$

(2) $[\alpha](y_1) = 1, \quad [\alpha](y_2) = 1$

(3) $[q^{\frac{1}{2}}\alpha](\pi^j y_1) = 1, \quad [q^{\frac{1}{2}}\alpha](\pi^{1-j} y_2) = 1,$ *where* j *is either* 0 *or* 1 *(depending on* α*).*

Furthermore, y_1 *may be chosen, up to multiplication by an element of* K^*, *as any non-zero isotropic vector.*

Proof. Set $L = \{x \mid \alpha(x) \leqslant 1\}$ and $L' = \{x \mid \alpha(x) \leqslant q^{-\frac{1}{2}}\}$. Then $[\alpha]$ and $[q^{\frac{1}{2}}\alpha]$ are, respectively, the norms of the lattices L and L'.

Let w be any non-zero isotropic vector of φ, define m by $[\alpha](w) = q^m$, and set $y_1 = \pi^m w$. Then, $[\alpha](y_1) = 1$ so that, by Proposition 4.10, we have $\sup_{x \in L} |B(x, y_1)| = 1$.

Define j by $[q^{\frac{1}{2}}\alpha](y_1) = q^j$. Since

$$1 = [\alpha](y_1) \leqslant [q^{\frac{1}{2}}\alpha](y_1) \leqslant q[\alpha](y_1) = q, \text{ we have}$$
$$j = 0 \text{ or } 1.$$

Again by Proposition 4.10,

$$\sup_{x \in L} |\pi^{-1} B(x, y_1)| = q^j, \text{ i.e., } \sup_{x \in L} |B(x, y_1)| = q^{j-1}.$$

If $j = 0$, choose $x_1 \in L$ so that $B(x_1, y_1) = 1$. If $j = 1$, choose $x_1 \in L'$ so that $B(x_1, y_1) = 1$. Then of course x_1 is also in L. Now set $y_2 = x_1 - \varphi(x_1) y_1$. Then y_2 is isotropic, and $B(y_1, y_2) = 1$. As $x_1 \in L$, we have $|\varphi(x_1)| \leqslant 1$, and therefore also, $y_2 \in L$. If follows again from Proposition 4.10 that $[\alpha](y_2) = 1$.

In case $j = 0$, we have $y_1 \in L'$ and $\pi y_2 \in L'$, with $\pi^{-1} B(y_1, \pi y_2) = 1$. If $j = 1$, then $\pi y_1 \in L'$ and $|\varphi(x_1)| \leqslant 1/q$, so that $y_2 \in L'$. Again $\pi^{-1} B(\pi y_1, y_2) = 1$. In either case, we find $[q^{\frac{1}{2}}\alpha](\pi^j y_1) = [q^{\frac{1}{2}}\alpha](\pi^{1-j} y_2) = 1$.

Before continuing with the general case, we shall apply the theorem just proved to describe $\mathcal{M}(\varphi)$ when φ is indefinite, and dim $E = 2$.

THEOREM 4.12. *Suppose that* φ *is indefinite and* dim $E = 2$. *Let* x_1 *and* x_2 *be a basis of* E *consisting of isotropic vectors for which* $B(x_1, x_2) = 1$. *Let* h *be any integer and let* $\beta_h \in \mathcal{N}(E)$ *be defined by* $\beta_h(a_1 x_1 + a_2 x_2) = \sup\, (q^{\frac{1}{2}h} |a_1|,\ q^{-\frac{1}{2}(h+1)} |a_2|)$. *Then* $\mathcal{M}(\varphi)$ *is the set* $\{\beta_h;\ h \in Z\}$. *Finally,* $O(\varphi)$ *is transitive on* $\mathcal{M}(\varphi)$.

Proof. Let g be any integer. Define $\sigma \in \operatorname{Aut}(E)$ by $\sigma(x_1) = \pi^g x_1$, $\sigma(x_2) = \pi^{-g} x_2$. Then, $\sigma \in O(\varphi)$, and $\sigma\beta_0 = \beta_{2g}$. Now define $\tau \in \operatorname{Aut}(E)$ by $\tau(x_1) = x_2$, $\tau(x_2) = x_1$ so that

τ is also in $O(\varphi)$, and $\sigma\tau\beta_0=\beta_{2g-1}$. Thus, each β_h is conjugate to β_0 by some element of $O(\varphi)$. However, $O(\varphi)$ is generated by the automorphisms σ and τ as described, together with the automorphisms $x_1\to cx_1$, $x_2\to c^{-1}x_2$ with $|c|=1$. Those automorphisms however leave fixed each β_h. Thus, $\{\beta_h\}$ is stable under $O(\varphi)$ and $O(\varphi)$ is transitive on that set. The full assertion of the theorem will follow when we show that $\mathfrak{M}(\varphi)$ is contained in $\{\beta_h\}$.

Let $\alpha\in\mathfrak{M}(\varphi)$. We apply Theorem 4.11 to α. Thus, $y_1=bx_1$ for some $b\in K^*$. Since all isotropic vectors in E are multiples either of x_1 or x_2, it follows that $y_2=b^{-1}x_2$.

Set $|b|=q^{-m}$. Now, bx_1 and $b^{-1}x_2$ form a set of free generators for L. Hence

$$[\alpha](a_1x_1+a_2x_2)=\sup(q^m|a_1|, q^{-m}|a_2|).$$

At the same time, $\pi^j bx_1$ and $\pi^{1-j}b^{-1}x_2$ form a set of free generators for L'. Therefore,

$$[q^{\frac{1}{2}}\alpha](a_1x_1+a_2x_2)=\sup(q^{m+j}|a_1|, q^{-m+1-j}|a_2|).$$

If follows from Proposition 1.5 and Theorem 4.8 that

$$\alpha=\inf\{[\alpha], q^{-\frac{1}{2}}[q^{\frac{1}{2}}\alpha]\}.$$

Hence,
$$\alpha(a_1x_1+a_2x_2)=\sup\{d_1|a_1|, d_2|a_2|\},$$

where
$$d_1=q^m\inf\{1, q^{j-\frac{1}{2}}\}, d_2=q^{-m}\inf\{1, q^{\frac{1}{2}-j}\}.$$

Thus, we find that $\alpha=\beta_{2m-1}$ when $j=0$, and $\alpha=\beta_{2m}$ when $j=1$. This completes the description of $\mathfrak{M}(\varphi)$ in the indefinite case of dimension two.

We return to the general case of an indefinite quadratic form φ. Using the same notation as in Theorem 4.11, we have:

PROPOSITION 4.13. *Let H be the space spanned by y_1 and y_2, and let H' be the orthogonal complement of H with respect to φ. Then H and H' are orthogonal with respect to α.*

Proof. We apply Corollary 1.9; because of Theorem 4.9, we have to show only that H and H' are orthogonal with respect to $[\alpha]$ and with respect to $[q^{\frac{1}{2}}\alpha]$. Let f be the projection of E onto H, then $f(x)=B(x,y_2)y_1+B(x,y_1)y_2$. According to Lemma 1.8, the desired result will follow when we prove that $[q\alpha](x)\geqslant[\alpha](f(x))$ and also that $[q^{\frac{1}{2}}\alpha](x)\geqslant[q^{\frac{1}{2}}\alpha](f(x))$. Furthermore, it is clearly sufficient to prove the first of these inequalities for $[\alpha](x)=1$, and the second for $[q^{\frac{1}{2}}\alpha](x)=1$. Now if $[\alpha](x)=1$, then

$x \in L$, so that $|B(x, y_1)| \leqslant 1$ and $|B(x, y_2| \leqslant 1$. Since y_1 and y_2 are in L, it follows that $f(x) \in L$ or that $[\alpha](f(x)) \leqslant 1$. In the second case, $x \in L'$, we have

$$|\pi^{-1} B(x, \pi^j y)| \leqslant 1 \text{ and } |\pi^{-1} B(x, \pi^{1-j} y_2)| \leqslant 1,$$

so that again
$$f(x) = B(x, y_2) y_1 + B(x, y_1) y_2 \in L'$$

and the assertion follows.

In order to use the result just proved to obtain further information on the structure of the set $\mathfrak{M}(\varphi)$, we need a preliminary lemma.

LEMMA 4.14. *Let $\alpha \in \mathfrak{M}(\varphi)$, and let $E = E_1 + E_2$ be such that E_1 and E_2 are orthogonal with respect to φ as well as with respect to α. Then, $\alpha|_{E_i} \in \mathfrak{M}(\varphi|_{E_i})$.*

Proof. Let $\beta_i \in \mathfrak{N}(\varphi|_{E_i})$ with $\beta_i \leqslant \alpha|_{E_i}$. Define $\gamma \in \mathfrak{N}$ by $\gamma(x_1 + x_2) = \sup(\beta_1(x_1), \beta_2(x_2))$. That γ is in fact a norm on E is clear. From the fact that E_1 and E_2 are orthogonal with respect to φ, we find $\gamma \in \mathfrak{N}(\varphi)$. And, from the fact that E_1 and E_2 are orthogonal with respect to α, we obtain $\gamma \leqslant \alpha$. As $\alpha \in \mathfrak{M}(\varphi)$, it follows that $\gamma = \alpha$ and hence that $\beta_i = \alpha|_{E_i}$. Thus, $\alpha|_{E_i} \in \mathfrak{M}(\varphi|_{E_i})$.

Combining Proposition 4.13 and the lemma allows us to use induction on the dimension of E to conclude the following:

THEOREM 4.15. *Let $\alpha \in \mathfrak{M}(\varphi)$. Then, there is a direct sum decomposition*

$$E = E_0 + E_1 + \ldots + E_g$$

into subspaces which are mutually orthogonal with respect to φ as well as with respect to α such that:

(a) *$\varphi|_{E_0}$ is definite*
(b) *For $1 \leqslant i \leqslant g$, $\dim E_i = 2$, and $\varphi|_{E_i}$ is indefinite*
(c) *$\alpha|_{E_i} \in \mathfrak{M}(\varphi|_{E_i})$ $0 \leqslant i \leqslant g$.*

As an immediate corollary we obtain:

THEOREM 4.16. *$O(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$.*

Proof. Let α and α' be elements of $\mathfrak{M}(\varphi)$, and let $E = \sum E_i = \sum E_i'$ be decompositions of E of the type described in Theorem 4.15 corresponding respectively to α and α'. By Witt's Theorem, there is an element $\tau \in O(\varphi)$ such that $\tau E_i' = E_i$. Set $\beta = \tau\alpha'$. Then $\sum E_i$ is a decomposition of E of the type under consideration corresponding to β. Since $\varphi|_{E_0}$ is definite, $\mathfrak{M}(\varphi|_{E_0})$ has only one element (Theorem 4.1), so that $\beta|_{E_0} = \alpha|_{E_0}$. Let $1 \leqslant i \leqslant g$. Then, $O(\varphi|_{E_i})$ is transitive on $\mathfrak{M}(\varphi|_{E_i})$ (Theorem 4.11), so that there is a $\sigma_i \in O(\varphi|_{E_i})$ such that $\beta|_{E_i} = \sigma_i \alpha|_{E_i}$. Defining σ as the direct sum of σ_i (and the identity on E_0), we see that $\sigma \in O(\varphi)$ and $\beta = \sigma\alpha$. Thus, $O(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$.

As an immediate corollary we obtain a result already proved by Eichler [2].

COROLLARY 4.17. *$O(\varphi)$ is transitive on $\mathfrak{L}_m(\varphi)$.*

Proof. Let $\alpha \in \mathfrak{L}_m(\varphi)$. By Corollary 4.4 there is a $\beta \in \mathfrak{M}(\varphi)$ such that $\beta \leqslant \alpha$. It follows immediately from Theorem 4.9 that $\alpha = [\beta]$. Now let α' be another element of $\mathfrak{L}_m(\varphi)$, and choose $\beta' \in \mathfrak{M}(\varphi)$ such that $\beta' \leqslant \alpha'$. Then, there is a $\sigma \in O(\varphi)$ such that $\beta' = \sigma\beta$. Hence $\sigma\alpha = \sigma[\beta] = [\sigma\beta] = [\beta'] = \alpha'$, which shows that $O(\varphi)$ is transitive on $\mathfrak{L}_m(\varphi)$.

If g is a positive integer, we denote by $\mathfrak{N}_g$ the set of those $\alpha \in \mathfrak{N}$ with the property that $\alpha(x)^g$ is an integral power of q, for all non-zero $x \in E$. Thus, for example, $\mathfrak{N}_1 = \mathfrak{L}$. It follows from Proposition 1.5 and Theorem 4.9 that $\mathfrak{M}(\varphi) \subset \mathfrak{N}_2$. Note that if E' is a subspace of E, the restriction mapping from $\mathfrak{N}(E)$ to $\mathfrak{N}(E')$ maps $\mathfrak{N}_g(E)$ into $\mathfrak{N}_g(E')$.

We shall now prove a strengthened form of Proposition 4.6.

THEOREM 4.18. *Let E' be a totally isotropic subspace of E (i.e., $\varphi(x) = 0$, all $x \in E'$) and let $\gamma \in \mathfrak{N}_2(E')$. Then there exists an $\alpha \in \mathfrak{M}(\varphi)$ such that $\alpha|_{E'} = \gamma$.*

Proof. It is clearly sufficient to prove the theorem in the case where E' is a maximal totally isotropic subspace of E. Let $x_1, \dots, x_g$ be a basis of E' with respect to which γ is canonical. Since $\gamma \in \mathfrak{N}_2(E')$, we have $\gamma(x_i) = q^{\frac{1}{2}h_i}$, with h_i integers.

Choose $y_i \in E$ such that

1. $\varphi(y_i) = 0$
2. $B(x_i, y_j) = \delta_{ij}$.

Let E'' be the space spanned by $y_1, \dots, y_g$. Then $E' \cap E'' = 0$. Furthermore, the restriction of φ to $E' + E''$ is non-degenerate. Let E_0 be the orthogonal complement, with respect to φ, of $E' + E''$. Then, $E = E' + E'' + E_0$ is a direct sum, and the restriction of φ to E_0 is definite.

Set $\delta(y_i) = q^{-\frac{1}{2}(h_i+1)}$, and define $\delta \in \mathfrak{N}(E'')$ by

$$\delta(\sum a_i y_i) = \sup\,(|a_i|\,\delta(y_i)).$$

Also, set $\delta_0 = |\varphi|^{\frac{1}{2}}$ in E_0. Finally, define $\alpha \in \mathfrak{N}(E)$ by

$$\alpha(x + y + z) = \sup\,(\gamma(x), \delta(y), \delta_0(z)),$$

where $x \in E'$, $y \in E''$, $z \in E_0$.

Let H_i be the space spanned by x_i and y_i. Then, E is the orthogonal direct sum of $E_0, H_1, \ldots, H_g$, and these spaces are also orthogonal with respect to α. It follows from Theorem 4.12 that the restriction of α to H_i is in $\mathcal{M}(\varphi|_{H_i})$. Hence from the description of $\mathcal{M}(\varphi)$ we conclude that $\alpha \in \mathcal{M}(\varphi)$. Since we have $\alpha|_{E'} = \gamma$, the result follows.

We conclude this section with several supplementary remarks concerning the relations between quadratic forms and norms which are valid in general only under the hypothesis that the characteristic of the residue class field $\mathfrak{O}/\mathfrak{p}$ is not 2.

PROPOSITION 4.19. *Let L be a lattice and φ a non-degenerate quadratic form. If $2 \nmid q$, there is a set of free generators $\{x_i\}$ of L such that φ is diagonal with respect to $\{x_i\}$.*

Proof. It is clear that we may replace φ by $c\,\varphi$ with c any element of K^*. Hence we may suppose that $|\varphi| \leqslant 1$ on L and that equality holds for some element of L. We shall prove the proposition by induction on $n = \dim E$. The case where $n = 1$ is trivial.

Let $x_1 \in L$ be such that $|\varphi(x_1)| = 1$. Let E' be the orthogonal complement, with respect to φ, of Kx_1. Let $L' = L \cap E'$. It is clear that we shall be done when we prove that $L = \mathfrak{O}x_1 + L'$.

Obviously, $\mathfrak{O}x_1 + L' \subset L$. Suppose $x \in L$; then $x = ax_1 + y$ with $y \in E'$. Here, $a = B(x, x_1)/2\varphi(x_1)$. Thus, everything follows from $|a| \leqslant 1$. As we suppose that $2 \nmid q$, and as we have $|\varphi(x_1)| = 1$, we must show that $|B(x, x_1)| \leqslant 1$. But,

$$B(x, x_1) = \varphi(x + x_1) - \varphi(x) - \varphi(x_1),$$

and $|\varphi| \leqslant 1$ on L, so that indeed we have $|B(x, x_1)| \leqslant 1$ and the proof is complete.

PROPOSITION 4.20. *Let φ be a definite form and let $\mu = |\varphi|^{\frac{1}{2}}$. Assume that $2 \nmid q$. If $\{x_i\}$ is a basis with respect to which φ is diagonal, then μ is canonical with respect to $\{x_i\}$.*

Proof. We have $\varphi(\sum a_i x_i) = \sum \varkappa_i a_i^2$. If we replace each x_i by $c_i x_i$ with $c_i \in K^*$, then φ is still diagonal, and if μ is canonical with respect to $\{c_i x_i\}$ it will be canonical with respect to $\{x_i\}$. Thus, we may suppose that $|\varkappa_i|$ is either 1 or $1/q$. We set $\varkappa_i = u_i \pi^{h_i}$, with $|u_i| = 1$ and $h_i = 0$ or 1. Now suppose that μ is not canonical with respect to $\{x_i\}$. Then, there are elements $a_i \in K$ such that $|\sum \varkappa_i a_i^2| < \sup\{|\varkappa_i|\,|a_i|^2\}$. Set $a_i = v_i \pi^{g_i}$, where $|v_i| = 0$ or 1. Thus,

$$\left|\sum u_i v_i^2 \pi^{h_i + 2g_i}\right| < \sup\{|v_i|\, q^{-(h_i + 2g_i)}\}.$$

Let i_0 be an index for which $|\varkappa_{i_0}||a_{i_0}|^2$ is maximal, and let J be the set of all indices i such that $|\varkappa_i||a_i|^2=|\varkappa_{i_0}||a_{i_0}|^2$. Then, we note first that J must have at least two elements. Secondly, for $i\in J$, we have $|v_i|=1$. Also since $h_i=0$ or 1, the equality, for $i\in J$, $h_i+2g_i=h_{i_0}+2g_{i_0}$ implies immediately that $h_i=h_{i_0}$ and $g_i=g_{i_0}$. Hence we have $|\sum_{i\in J}u_iv_i^2|<1$.

Since u_i and v_i are all units in $\mathfrak{O}$, and $2\nmid q$, Hensel's lemma asserts that there are units $w_i\in\mathfrak{O}$, for $i\in J$, such that $\sum_{i\in J}u_iw_i^2=0$. This contradicts the hypothesis that φ is definite, from which we conclude that μ is canonical with respect to $\{x_i\}$.

For the final proposition we refer to the notation of Theorem 4.15 and say that φ has *maximal index* if $E_0=0$. This is equivalent to the condition that E is a direct sum of mutually orthogonal hyperbolic planes.

We denote by $SO(\varphi)$ the *special orthogonal group* consisting of the elements $\sigma\in O(\varphi)$ with $\det\sigma=1$. It is well known that $[O(\varphi):SO(\varphi)]=2$. We consider the question of the transitivity of $SO(\varphi)$ on $\mathfrak{M}(\varphi)$. Suppose $\alpha\in\mathfrak{M}(\varphi)$. Then it is clear that $SO(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$ if, and only if, $O(\varphi)\cap G_\alpha\not\subset SO(\varphi)$.

PROPOSITION 4.21. *Suppose that $2\nmid q$. Then, $SO(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$ if, and only if, φ does not have maximal index.*

Proof. Choose $\alpha\in\mathfrak{M}(\varphi)$ and decompose E according to Theorem 4.15: $E=E_0+E_1+\ldots+E_g$. Suppose that $E_0\neq 0$. Then, there is an element $\sigma\in O(\varphi|_{E_0})$ with $\det\sigma=-1$. If we extend σ to E by defining it to be 1 on E_i, for $1\leqslant i\leqslant g$, then we find $\sigma\in O(\varphi)\cap G_\alpha$. Since $\det\sigma=-1$, it follows that $O(\varphi)\cap G_\alpha\not\subset SO(\varphi)$ so that $SO(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$. (Note that for this part of the proposition we need not assume that $2\nmid q$.)

Now suppose that $E_0=0$ and that $2\nmid q$. Let x_i, y_i be a basis of E_i consisting of isotropic vectors with $B(x_i,y_j)=\delta_{ij}$. If we set $z_i=x_i$ for $1\leqslant i\leqslant g$ and $z_i=y_{i-g}$ for $g+1\leqslant i\leqslant n$, then with respect to this basis of E, the elements of G_α are represented by the matrices of the form

$$\sigma=\begin{pmatrix} A & B \\ \pi C & D\end{pmatrix}$$

with A, B, C, D arbitrary $g\times g$ matrices with coefficients in $\mathfrak{O}$ and such that $\det\sigma$ is a unit in $\mathfrak{O}$. If we impose the condition that such a matrix represent an element of $O(\varphi)$ we find that ${}^tAD\equiv 1 \pmod{\mathfrak{p}}$. Hence, $\det\sigma\equiv 1 \pmod{\mathfrak{p}}$, while $2\nmid q$. It follows that $G_\alpha\cap O(\varphi)\subset SO(\varphi)$ and hence $SO(\varphi)$ is not transitive on $\mathfrak{M}(\varphi)$.

Section 5. Discriminants

Let α be a norm on E. In section 3 we described an extension of α to a norm on the exterior algebra ΛE of E. As a consequence of Proposition 3.9 we obtain the following useful fact:

PROPOSITION 5.1. *Let α be a norm on E and let $\{x_i\}$, $\{y_i\}$ be two bases of E with respect to which α is canonical. Let $\sigma \in \operatorname{Aut}(E)$ be defined by $y_i = \sigma(x_i)$. Then,*

$$\prod_{i=1}^{n} \alpha(y_i) = |\det \sigma| \prod_{i=1}^{n} \alpha(x_i).$$

Proof. It follows from Proposition 3.9 that

$$\Lambda_n(\alpha)(x_1 \wedge \ldots \wedge x_n) = \prod \alpha(x_i)$$

and, at the same time,
$$\Lambda_n(\alpha)(y_1 \wedge \ldots \wedge y_n) = \prod \alpha(y_i).$$

However,
$$y_1 \wedge \ldots \wedge y_n = (\det \sigma)(x_1 \wedge \ldots \wedge x_n),$$

and the assertion follows.

Let $\alpha \in \mathfrak{N}(E)$ and let φ be a non-degenerate quadratic form. Let $\{x_i\}$ be a basis with respect to which α is canonical. Set

$$\Delta(\varphi, \alpha) = |\det B(x_i, x_j)| \left\{\prod_{i=1}^{n} \alpha(x_i)\right\}^{-2}.$$

It follows immediately from Proposition 5.1 that $\Delta(\varphi, \alpha)$ is independent of the choice of $\{x_i\}$; we call $\Delta(\varphi, \alpha)$ the *discriminant* of φ with respect to α.

PROPOSITION 5.2. *If $\sigma \in \operatorname{Aut}(E)$, then*

$$\Delta(\varphi\sigma^{-1}, \sigma\alpha) = \Delta(\varphi, \alpha).$$

Proof. Let $\{x_i\}$ be a basis with respect to which α is canonical, and set $y_i = \sigma x_i$. Then $\sigma\alpha$ is canonical with respect to $\{y_i\}$ and $\sigma\alpha(y_i) = \alpha(x_i)$, while $B\sigma^{-1}(y_i, y_j) = B(x_i, x_j)$. The result follows immediately.

THEOREM 5.3. *Let φ be a non-degenerate quadratic form. Then, $\Delta(\varphi, \alpha)$ is the same for all α in $\mathfrak{M}(\varphi)$. Let $d(\varphi)$ be the value assumed by $\Delta(\varphi, \alpha)$ for $\alpha \in \mathfrak{M}(\varphi)$. If $\beta \in \mathfrak{N}(\varphi)$, then $\Delta(\varphi, \beta) \leqslant d(\varphi)$, and equality holds only when $\beta \in \mathfrak{M}(\varphi)$.*

Proof. Since $O(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$, it follows immediately from Proposition 5.2 that $\Delta(\varphi, \alpha)$ is the same for all $\alpha \in \mathfrak{M}(\varphi)$.

Let $\beta \in \mathcal{N}(\varphi)$. Then, there is an $\alpha \in \mathcal{M}(\varphi)$ with $\alpha \leqslant \beta$. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical. Then, $\alpha(x_i) \leqslant \beta(x_i)$, and $\prod_{i=1}^{n} \alpha(x_i) = \prod_{i=1}^{n} \beta(x_i)$ can hold only for $\alpha = \beta$. Thus, $\Delta(\varphi, \beta) \leqslant \Delta(\varphi, \alpha)$ and equality holds only for $\alpha = \beta$.

Remark. The value of $d(\varphi)$ may be determined explicitly in case the characteristic of $\mathfrak{O}/\mathfrak{p}$ is not 2. If g is the index of φ, namely the dimension of a maximal totally isotropic subspace of E, then $d(\varphi) = q^g$. We use the notation of Theorem 4.15: $E = E_0 + \ldots + E_g$ where $\varphi|_{E_0}$ is definite and for $1 \leqslant i \leqslant g$, E_i is a hyperbolic plane. If, for $1 \leqslant i \leqslant g$, x_i, y_i form a basis of E_i consisting of isotropic vectors with $B(x_i, y_i) = 1$, then we have $\alpha(x_i)\,\alpha(y_i) = q^{-\frac{1}{2}}$ (Theorem 4.12). Also, if $z_1, \ldots, z_n$ is a basis of E_0 with respect to which φ/E_0 is diagonal, then it follows from Proposition 4.19 that

$$\alpha|_{E_0}(\sum a_i z_i) = \sup(|\varphi(z_i)|^{\frac{1}{2}}\,|a_i|).$$

Then, the determinant of B with respect to the basis $\{x_i, y_j, z_k\}$ has an absolute value of $\prod_k |\varphi(z_k)|$, while the product of the values of α^2 on this basis is $q^{-g}\prod|\varphi(z_k)|$. Hence, $\Delta(\varphi, \alpha) = q^g$.

Let $\{x_i\}$ be a basis of E. If φ is a quadratic form, there is some basis in which φ is diagonal. This may be expressed by the statement that there is a $\sigma \in \mathrm{Aut}(E)$ such that $\varphi\sigma$ is a diagonal in the basis $\{x_i\}$. If ψ is a diagonal in $\{x_i\}$, with $\psi(\sum a_i x_i) = \sum \varkappa_i a_i^2$, then by replacing ψ by $\psi\tau$, with τ suitably chosen in $\mathrm{Aut}(E)$, we may keep ψ diagonal and change each $\varkappa_i$ modulo K^{*2}. Since K^*/K^{*2} is a finite group, we arrive at the following result:

PROPOSITION 5.4. *There are only a finite number of orbits of quadratic forms under the action of* $\mathrm{Aut}(E)$.

As an immediate consequence of this result, we have:

THEOREM 5.5. *Let α be a given norm, and let X be the set of all non-degenerate quadratic forms φ such that $\alpha \in \mathcal{M}(\varphi)$. Then X is stable under the action of G_α and decomposes, under that action, into a finite number of orbits.*

Proof. Suppose that φ and ψ are in X and are equivalent in $\mathrm{Aut}(E)$, i.e., $\psi = \varphi\sigma$ with $\sigma \in \mathrm{Aut}(E)$. Then, $\sigma\alpha \in \mathcal{M}(\varphi)$ while at the same time $\alpha \in \mathcal{M}(\varphi)$. Since $O(\varphi)$ is transitive on $\mathcal{M}(\varphi)$, we have $\sigma\alpha = \varrho\alpha$ with $\varrho \in O(\varphi)$, and hence $\sigma = \varrho\tau$ with $\tau \in G_\alpha$. Thus,

$$\psi = \varphi\sigma = \varphi\varrho\tau = \varphi\tau,$$

or φ and ψ are in the same orbit under G_α. The result now follows from Proposition 5.4.

We need several preliminary propositions in preparation for the main result of this section.

If φ is a non-degenerate quadratic form and $\alpha \in \mathfrak{M}(\varphi)$, we have seen in Theorem 5.3 that $\Delta(\varphi, \alpha)$ depends only on φ and not on the choice of α; we set $d(\varphi) = \Delta(\varphi, \alpha)$.

PROPOSITION 5.6. *As φ ranges over all non-degenerate quadratic forms, $d(\varphi)$ ranges over a finite set.*

Proof. If $\alpha \in \mathfrak{M}(\varphi)$ and $\sigma \in \operatorname{Aut}(E)$, then $\sigma\alpha \in \mathfrak{M}(\varphi\sigma^{-1})$, and by Proposition 5.2, $\Delta(\varphi\sigma^{-1}, \sigma\alpha) = \Delta(\varphi, \alpha)$. Thus, $d(\varphi\sigma^{-1}) = d(\varphi)$, and the assertion follows from Proposition 5.4.

Let α and β be norms on E, and let $\{x_i\}$ be a basis with respect to which both α and β are canonical. It follows from Proposition 3.10 that the n-discriminant

$$\Delta_n(\alpha, \beta) = \frac{\prod_i \alpha(x_i)}{\prod_i \beta(x_i)}.$$

Since we shall use $\Delta_r(\alpha, \beta)$ only for $r = n$, we shall write $\Delta(\alpha, \beta)$ in place of $\Delta_n(\alpha, \beta)$. It is clear that

$$\Delta(\varphi, \beta) = \Delta(\varphi, \alpha)\,\Delta(\alpha, \beta)^2,$$

where φ is any non-degenerate quadratic form.

LEMMA 5.7. *If $\alpha \leqslant \beta$, then $\Delta(\alpha, \beta)\ \beta \leqslant \alpha$.*

Proof. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical. Then, $\alpha(x_i) \leqslant \beta(x_i)$, and

$$\Delta(\alpha, \beta)\,\beta(x_i) = \prod_{j \neq i} \frac{\alpha(x_j)}{\beta(x_j)}\,\alpha(x_i) \leqslant \alpha(x_i).$$

COROLLARY 5.8. *Let β be a given norm, and c a given real number with $0 < c \leqslant 1$. Then the set of all α such that $\alpha \leqslant \beta$ and $\Delta(\alpha, \beta) = c$ is compact.*

Proof. For fixed β, the function of α given by $\Delta(\alpha, \beta)$ is clearly continuous. Hence the set of α for which $\Delta(\alpha, \beta) = c$ is closed. By Lemma 5.7, each α under consideration has the property $c\beta \leqslant \alpha \leqslant \beta$. But this is the same as the statement $d(\alpha, c^{\frac{1}{2}}\beta) \leqslant \log c^{-\frac{1}{2}}$. The set of all α with the latter property is compact, from which we obtain the desired conclusion.

LEMMA 5.9. *For a given integer g, the set $\mathfrak{N}_g$ is uniformly discrete. Explicitly, if $\alpha \neq \beta$ are in $\mathfrak{N}_g$, then $d(\alpha, \beta) \geqslant g^{-1} \log q$.*

Proof. Suppose that α and β are in $\mathcal{N}_g$ with $d(\alpha,\beta)<g^{-1}\log q$. Let $\{x_i\}$ be a basis with respect to which both α and β are canonical. Then,

$$d(\alpha,\beta)=\sup_i\left|\log\frac{\alpha(x_i)}{\beta(x_i)}\right|,$$

so that, for each i,
$$\left|\log\frac{\alpha(x_i)}{\beta(x_i)}\right|<\frac{1}{g}\log q.$$

It follows from the hypothesis $\alpha,\beta\in\mathcal{N}_g$, that $\alpha(x_i)=\beta(x_i)$ or that $\alpha=\beta$.

After these preliminaries, we arrive at the main result of this section:

THEOREM 5.10. *Let β be a given norm and c a given positive real number. Let Y be the set of all non-degenerate quadratic forms which satisfy the following two conditions:*

(1) $\beta\in\mathcal{N}(\varphi)$

(2) $\Delta(\varphi,\beta)=c$.

Then, Y is stable under the action of G_β and decomposes, under that action, into a finite number of orbits.

Proof. Let $\varphi\in Y$. Then there is an $\alpha\in\mathcal{M}(\varphi)$ with $\alpha\leqslant\beta$. We have,

$$\Delta(\alpha,\beta)^2=\Delta(\varphi,\beta)\,\Delta(\varphi,\alpha)^{-1}=c\,d(\varphi)^{-1}.$$

According to Proposition 5.6, the values of $d(\varphi)$ lie in a finite set, hence the values of $\Delta(\alpha,\beta)$ lie in a finite set.

Let A be the set of all α which arise in the above manner; it follows from Corollary 5.8 that A is compact. However, $A\subset\mathcal{N}_2$, so that by Lemma 5.9, A is discrete. Thus, A is a finite set. Let $\alpha_1,\ldots,\alpha_h$ be the elements of A. For $i=1,2,\ldots,h$ let Y_i be the set of those $\varphi\in Y$ for which $\alpha_i\in\mathcal{M}(\varphi)$. (These sets are not necessarily disjoint.) Then Y is the union of $Y_1,\ldots,Y_h$. Clearly, each Y_i is stable under the action of $G_{\alpha_i}\cap G_\beta$. Since both G_{α_i} and G_β are compact open subgroups of Aut(E), the index of $G_{\alpha_i}\cap G_\beta$ in G_{α_i} is finite. Applying Theorem 5.5, we conclude that Y_i decomposes into a finite number of orbits under the action of $G_{\alpha_i}\cap G_\beta$, from which it follows immediately that Y decomposes into a finite number of orbits under the action of G_β.

There is a sort of dual to Theorem 5.10.

THEOREM 5.11. *Let φ be a non-degenerate quadratic form and let c be a positive number. Let U be the set of those norms $\alpha\in\mathcal{N}(\varphi)$ for which $\Delta(\varphi,\alpha)=c$. Then U is stable under the action of $O(\varphi)$ and the quotient space of U mod $O(\varphi)$ is compact.*

Proof. Let β be an element of $\mathfrak{M}(\varphi)$, and let U' be the subset of U of those α for which $\alpha \geqslant \beta$. Let α be any element of U. Then, there is a $\gamma \in \mathfrak{M}(\varphi)$ with $\gamma \leqslant \alpha$. Since $O(\varphi)$ is transitive on $\mathfrak{M}(\varphi)$, it follows that every orbit of U under the action of $O(\varphi)$ meets U', so that we need only prove that U' is compact. Now, U' is clearly closed. At the same time, if $\alpha \in U'$ we have $\beta \leqslant \alpha \leqslant \Delta(\alpha,\beta)\beta$ and

$$\Delta(\alpha,\beta)^2 = \Delta(\varphi,\beta)\,\Delta(\varphi,\alpha)^{-1},$$

or $\Delta(\alpha,\beta) = (d(\varphi)/c)^{\frac{1}{2}}$. But the set of all norms α satisfying these inequalities is compact, so that U' is also compact.

References

[1]. I. S. Cohen, On non-Archimedean normed spaces. *Indag. Math.*, 10 (1948), 244–249.
[2]. M. Eichler, *Quadratische Formen und Orthogonale Gruppen*. Springer, Berlin, 1952.
[3]. A. F. Monna, Sur les espaces linéaires normés I–IV, *Indag. Math.*, 8 (1946), 643–660, 682–700.
[4]. T. Ono, On the compacity of the orthogonal groups. *Nagoya Math. J.*, 7 (1954), 111–114.

Received April 15, 1962