Journal of the Mathematical Society of Japan Vol. 7, No. 1, January, 1955

Arithmetic of Orthogonal Groups.

By Takashi ONO

(Received, June 28, 1954)

Three decades ago, H. Hasse discovered in his fundamental research on the arithmetic of quadratic forms[1] a remarkable principle, which may be stated as follows in its most general form: Let K be an abstract field, k an algebraic number field or a field of algebraic functions of one variable over a finite field, $\mathfrak{p}$ a place of k and $k_{\mathfrak{p}}$ the $\mathfrak{p}$-completion of k. Let furthermore $O(K)$ be an object related to K and Π a property of $O(K)$ (e.g. $O(K)$ may be a quadratic form f, and Π the representability of zero by f). If K is in particular specialized to k, then $O(K)$ will represent an object $O(k)$ related to k. Let $O_{\mathfrak{p}}$ be the object constructed naturally from $O(k)$ by transition to $k_{\mathfrak{p}}$ from k. By the 'Hasse principle' we shall mean this statement: *The assertion '$O(k)$ has the property Π' follows from the fact that '$O_{\mathfrak{p}}$ has the property Π for every place $\mathfrak{p}$ of k'*. Theorems of this form will be called theorems of Hasse type. Hasse has proved some important theorems of this type, concerning quadratic forms, cyclic extensions of algebraic number field, etc.[2]

Now the question arises: to what extent is this principle valid? In the present paper we shall investigate this question in connection with the orthogonal groups, as they are in closest relation to quadratic forms. In fact these groups can be treated in the same time with the corresponding quadratic forms by the geometrical method of Dieudonné, Eichler[3] and others.

Thus, in § 1 we introduce preliminary notions such as the similarity of forms, the indices and coindices of forms and the Clifford algebra of forms. We prove a lemma (Lemma 1) which shows that the similarity of forms is more natural than the congruence from geometric-

1) Hasse [1] and [2].
2) Deuring [3] Chap. VII and Witt [4].
3) Dieudonné [5] and Eichler [6].

al viewpoint. Except in the final remark on the topological linear spaces, the ground field K in § 1 may be any field of characteristic $\neq 2$. Then, in § 2 we assume the field K to be locally compactly valued. We consider the local properties of quadratic forms and orthogonal groups: the determination of indices of forms (Lemma 2), the characterization of local similarity of forms by means of their indices and discriminants (Lemma 3) and the relation between indices of forms and the local isomorphism of their orthogonal groups (Lemma 4). The results on the automorphisms of classical groups due to Dieudonné are used. Finally, in § 3 we shall establish certain theorems of Hasse type for quadratic forms and orthogonal groups over a field of algebraic numbers, or a field of algebraic functions of one variable over a finite field of characteristic $\neq 2$. Thus, we prove, firstly, the principle for similarity of forms, where the arithmetic of central simple algebra is used (Theorem 1). Secondly, using Lemma 1, we transfer the thus obtained principle to that of orthogonal groups (Theorem 2). Lastly, we prove another theorem for groups under a somewhat weaker assumption and there a result from the class field theory is used (Theorem 3). It seems interesting to the writer that the algebraic property, i. e. the conjugateness of groups, comes from the continuity for all topologies induced by places in K.

§ 1. Preliminary notations.

Let K be a field of characteristic $\neq 2$, and let V be an n-dimensional vector space over K. We denote by E the algebra of endomorphisms of V over K, and by $GL(V)$ the group of automorphisms of V over K. Let f be a non-degenerate symmetric bilinear form on V. For any $\sigma \in GL(V)$, we define another bilinear form f^σ as follows: $f^\sigma(x, y)=f(\sigma x, \sigma y)$ for all $x, y \in V$. It is easy to see that $f^{\sigma\tau}=(f^\sigma)^\tau$, $(af)^\sigma=af^\sigma$ for $\sigma, \tau \in GL(V)$, $a \in K^*$[4]. We say that two forms[5] f and g are *congruent*: $f \sim g$, if $g=f^\sigma$ for some $\sigma \in GL(V)$ and that they are *similar*: $f \backsim g$, if $g \sim af$ for some $a \in K^*$. We denote by $O(V, f)$ the set of all $\sigma \in GL(V)$ such that $f^\sigma=f$ and call it the *orthogonal group*

4) K^* is the set of all non-zero elements in K.

5) For brevity, we often omit the long adjective: "non-degenerate symmetric bilinear". We also denote the quadratic form corresponding to f simply by the same notation.

corresponding to f. It is easy to see that $O(V, af)=O(V,f)$ and $O(V,f^\sigma)=\sigma^{-1}O(V,f)\sigma$ for $a\in K^*$, $\sigma\in GL(V)$. This means that if $f\backsim g$ then their groups $O(V,f)$ and $O(V,g)$ are conjugate in $GL(V)$. We can show that the converse is also true (Lemma 1). This is one of the important relations between forms and their groups.

LEMMA 1. *Let K and V be as above. Let f and g be two forms on V. Then, their orthogonal groups $O(V,f)$ and $O(V,g)$ are conjugate in $GL(V)$ if and only if f and g are similar in K: $f\backsim g$.*

PROOF. It suffices to show the necessity of the condition. If $O(V,g)=\tau^{-1}O(V,f)\tau$, then $O(V,g)=O(V,f^\tau)$. Thus, we may assume from the first that $O(V,f)=O(V,g)$. We devide the proof into two cases.

Case A. ($K\neq GF(3)$). Let a be any non-isotropic vector (in the sense of f) in V and let $\sigma_{\langle a\rangle}^f$ be the symmetry with respect to the hyperplane $\langle a\rangle^f$ which is composed of all $x\in V$ such that $f(a,x)=0$.[6] Thus, we have an orthogonal decomposition, $V=\langle a\rangle\oplus\langle a\rangle^f$. On the other hand, the involution $\sigma_{\langle a\rangle}^f$, considered as an element in $O(V,g)$, determines a non-isotropic subspace U of V such that $\sigma_{\langle a\rangle}^f(u)=-u$, $u\in U$ and $\sigma_{\langle a\rangle}^f(v)=v$, $v\in U^g$, where U^g is the conjugate of U in the sense of g.[7] We also have another orthogonal decomposition, $V=U\oplus U^g$. Since $\langle a\rangle^f$ is a hyperplane, we have $U^g\subset\langle a\rangle^f$. Conversely let x be any vector $\in\langle a\rangle^f$. Set $x=y+z$, $y\in U$, $z\in U^g$. Then, we get $x=\sigma_{\langle a\rangle}^f(x)=-y+z$. Hence, it follows that $y=0$, and so $x=z\in U^g$. Thus, we have $U=\langle b\rangle$ and $\langle b\rangle^g=\langle a\rangle^f$. We may also write $\sigma_{\langle a\rangle}^f$ as $\sigma_{\langle b\rangle}^g$. Now, set $b=\mu a+x$, $\mu\in K$, $x\in\langle a\rangle^f$. Then, since $\sigma_{\langle a\rangle}^f(b)=\sigma_{\langle b\rangle}^g(b)$, we get $x=0$, and we have $\langle a\rangle=\langle b\rangle$. Thus, we have $\langle a\rangle^f=\langle a\rangle^g$ for all non-isotropic vectors (in the sense of f). By exchanging the roles of f and g in the above argument we see that we need not distinguish the non-isotropic vectors in the senses of f and g. For a fixed nen-isotropic a, since $\langle a\rangle^f$ and $\langle a\rangle^g$ are the null-spaces of the linear functionals $\varphi_a:\varphi_a(x)=f(a,x)$ and $\psi_a:\psi_a(x)=g(a,x)$, $x\in V$, respectively, we know that $\langle\varphi_a\rangle=\langle\psi_a\rangle$ in the dual space of V. Thus, we get $\psi_a=\lambda_a\cdot\varphi_a$, namely, $g(a,x)=\lambda_a f(a,x)$, $x\in V$, $\lambda_a\in K^*$. If a and a' are non-isotropic and $f(a,a')\neq 0$, then we have $g(a,a')=\lambda_a f(a,a')$ and $g(a',a)=\lambda_{a'}f(a',a)$. Since f and g are symmetric forms,

6) $\langle a\rangle$ denotes the line spanned by a.

7) [5] p. 19 Prop. 7.

we get $\lambda_a=\lambda_{a'}$. Now, let a_i, $i=1,\cdots,n$ be a fixed orthogonal basis of V for f. Since K contains at least 5 elements, there exists a $\mu\in K^*$ such that $\mu^2 f(a_1,a_1)+\sum_{i=2}^{n} f(a_i,a_i)\neq 0$. Using this μ, put $a=\mu a_1+\sum_{i=2}^{n} a_i$. Then, $f(a,a)\neq 0$, $f(a,a_i)\neq 0$ $i=1,\cdots,n$. Therefore, by the above argument, we have $\lambda_{a_i}=\lambda_a$, $i=1,\cdots,n$. Now, let $x=\sum_{i=1}^{n}\mu_i a_i$ be any vector $\in V$. Then, $g(x,y)=\sum_{i=1}^{n}\mu_i g(a_i,y)=\sum_{i=1}^{n}\mu_i\lambda_{a_i} f(a_i,y)=\lambda_a f(x,y)$ for all $y\in V$. Thus, we get $g=\lambda_a f$. This settles Case A.

Case B. $(K=GF(3))$ If n is odd, we have nothing to prove since then any two forms are congruent. If n is even, we have two cases: $f_1\sim x_1^2+\cdots+x_{n-1}^2+x_n^2$ or $f_2\sim x_1^2+\cdots+x_{n-1}^2-x_n^2$. But, since the order of $O(V,f_1)$: $2\left(3^{n-1}-(-1)^{\frac{n}{2}}3^{\left(\frac{n}{2}-1\right)}\right)(3^{n-2}-1)3^{n-3}\cdots(3^2-1)3$ and that of $O(V,f_2)$: $2\left(3^{n-1}+(-1)^{\frac{n}{2}}3^{\left(\frac{n}{2}-1\right)}\right)(3^{n-2}-1)3^{n-3}\cdots(3^2-1)3$ are different, $O(V,f_1)$ and $O(V,f_2)$ cannot be conjugate in $GL(V)$.[8] Thus, we also know the validity of our statement in Case B.

After Dieudonné, we say that a form f is of *index* ν if ν is the maximum dimension of $U\subset V$ such that $U\subset U^*$, where U^* is the conjugate of U with respect to f.[9] A form f of index ν is congruent to $g=\sum_{i=1}^{\nu}(x_i^2-y_i^2)+f^*$, where the index of f^* is zero. From Witt's theorem, such f^* is determined uniquely up to congruence by f, and we call it the *kernel* of f.[10] We also call the rank of f^* (which is equal to $n-2\nu$) the *coindex* of f and denote it by $\nu^*(f)$. Since $x^2-y^2\sim a(x^2-y^2)$ for all $a\in K^*$, we get immediately that $f^*\backsim g^*$ if and only if $f\backsim g$.

Suppose that V be of dimension 2 over K. Let e_i, $i=1,2$ be some orthogonal basis of V with respect to a form f on V. Then, the associative algebra of rank 4 over K with basis 1, ω_1, ω_2, $\omega_1\omega_2$ such that $\omega_i^2=f(e_i,e_i)=a_i$, $\omega_i\omega_k+\omega_k\omega_i=0$ $(i\neq k)$ $i,k=1,2$, is called the *quaternion algebra* of f.[11] This algebra is central simple over K. It is easily

8) Dickson [7] Chap. VII §§ 169-170.

9) [5] p. 17.

10) [4] Satz 5.

11) This algebra is called by Witt [4] the Clifford algebra of f. But we shall adopt a modified definition of Clifford algebras; see below.

verified that this algebra is determined up to isomorphism by f. We denote it by (a_1, a_2). We see that if one of a_1, a_2 is a square in K then $(a_1, a_2) \cong K_2$: the full matric algebra of degree 2 over K, and if one of them, say a_2, is not a square in K then $(a_1, a_2) \cong \left(a_1, K(\sqrt{a_2}), \sigma\right)$: a cyclic algebra with respect to the quadratic extension $K(\sqrt{a_2})$ with Galois group $<\sigma>$.[12] Thus, we get the following relations for their algebra classes: $(a, b) \sim (b, a)$, $(a, -a) \sim 1$ and $(a, c) \otimes (b, c) \sim (ab, c)$, where $\otimes$ means the tensor product of two algebras over K. Now, let, again, V be an n-dimensional vector space over K, and let f be a form on V. For some fixed orthogonal basis $e_i (i=1, \cdots, n)$, put $a_i = f(e_i, e_i)$ and $d_i = a_1 \cdots a_i$. Then, we define the *Clifford algebra* $\mathfrak{C}(f)$ of f as a tensor product over K: $\mathfrak{C}(f) = (a_1, d_1) \otimes (a_2, d_2) \otimes \cdots \otimes (a_n, d_n)$.[13] This is, of course, central simple over K. It can be seen from the above properties of (a, b) that $f \sim g$ implies that $\mathfrak{C}(f) \sim \mathfrak{C}(g)$ and we know that the algebra class of $\mathfrak{C}(f)$ is independent of the choice of orthogonal basis e_i.[14] By simple computations we get $\mathfrak{C}(af) \sim \left(a, (-1)^{\frac{n(n+1)}{2}} d(f)^{n+1}\right) \otimes \mathfrak{C}(f)$, where $a \in K^*$ and $d(f)$ denotes the discriminant of f relative to some basis of V,[15] and $\mathfrak{C}(f+g) \sim \left(d(f), d(g)\right) \otimes \mathfrak{C}(f) \otimes \mathfrak{C}(g)$. For the special quadratic form of type $f \sim \sum_{i=1}^{r} (x_i^2 - y_i^2)$, we have $d(f) \sim (-1)^r$ and $\mathfrak{C}(f) \sim \left(-1, (-1)^{\frac{r(r+1)}{2}}\right)$.

We shall close this section with some topological remarks. Suppose that K has a non-trivial valuation $|\ |$. Let $u_i (i=1, \cdots, n)$ be some fixed basis of V over K. If we define *norm* of $x = \sum_{i=1}^{n} x_i u_i \in V$ by $\|x\| = \max_{i=1, \cdots, n} |x_i|$ and that of $X = (x_{ij}) \in E$ by $\|X\| = \max_{i, j=1, \cdots, n} |x_{ij}|$ then V and E are topologized as usual.[16] A subset S of such a topological linear space is called *bounded* if for some $b > 0$ we have $\|x\| < b$ for all $x \in S$.

---

12) $<*>$ denotes the cyclic group generated by $*$.

13) The Clifford algebra defined here is slightly different from the habitual one. That is the one denoted as $S(f)$ in [4]. We define, inspired by Jones [8], $\mathfrak{C}(f)$ as a product of (a, b)'s directly.

14) See the argument in [8] pp. 32-35.

15) The class of $d(f)$ modulo K^{*2} is independent of the choice of basis. We denote $a \sim b$ if $ab^{-1} \in K^{*2}$.

16) Artin [9] p. 18.

It is easy to see that boundedness is independent of the choice of basis u_i. It is obvious that the group $O(V,f)$ is a closed subset of E and $f \backsim g$ implies that their groups $O(V,f)$ and $O(V,g)$ are homeomorphically isomorphic. If K is locally compact, then so are V and E, and a bounded closed subset of V or E is the same thing as a compact subset.

§ 2. Local considerations.

In this §, we assume that K is a locally compactly valued field of characteristic $\neq 2$. Let V be an n-dimensional vector space over K and f be a non-degenerate symmetric bilinear form on V. If K is the comptex number field, then $\nu=[n/2]$ always, where $[*]$ means the integral part of $*$. If K is the real number field, then we get easily $\nu=\min(\iota, n-\iota)$, where ι is the number of positive coefficients in a canonical form of f. On the other hand, if K is non-archimedean, then we know that for $n \geqq 5$, every f is a zero form.[17] Thus, in this case, the coindices $\nu^* \leqq 4$ and more precisely $\nu^*=1$ or 3 if n is odd, $\nu^*=0, 2$ or 4 if n is even. For non-archimedean fields it is also known that $d(f)$ and $\mathfrak{C}(f)$ form a complete system of invariants for forms on V.[18] As to the coindices for the non-archimedean cases we get the following

LEMMA 2. *If n is odd, then $\nu^*=1$ if and only if $\mathfrak{C}(f) \sim \left(-1, (-1)^{\frac{n^2-1}{8}} d^{\frac{n+1}{2}}\right)$, where d is the discriminant of f for some basis in V. If n is even, then $\nu^*=0$ if and only if $(-1)^{\frac{n}{2}} d$ is a square in K and $\mathfrak{C}(f) \sim \left(-1, (-1)^{\frac{n^2+2n}{8}}\right)$, and $\nu^*=2$ if and only if $(-2)^{\frac{n}{2}} d$ is not a square in K.*

PROOF. Case 1. (n: odd). $\nu^*=1$ means that $f \sim g = \sum_{i=1}^{\frac{n-1}{2}} (x_i^2 - y_i^2) + (-1)^{\frac{n-1}{2}} dx$. This congruence, however, is equivalent to the condition $\mathfrak{C}(f) \sim \mathfrak{C}(g) \sim \left((-1)^{\frac{n-1}{2}}, (-1)^{\frac{n-1}{2}} d\right) \otimes \left(-1, (-1)^{\frac{n^2-1}{8}}\right) \otimes \left(-1, (-1)^{\frac{n-1}{2}} d\right) \sim \left(-1, (-1)^{\frac{n^2-1}{8}} d^{\frac{n+1}{2}}\right)$.

17) [4] Satz 16 or [6] p. 42 Satz 7.3.

18) [4] Satz 17.

Case 2. (n: even). First, $\nu^*=0$ means that $f\sim g=\sum_{i=1}^{\frac{n}{2}}(x_i^2-y_i^2)$. This congruence holds if and only if $d\sim(-1)^{\frac{n}{2}}$ and $\mathfrak{C}(f)\sim\left(-1,(-1)^{\frac{n^2+2n}{8}}\right)$. Next, suppose $\nu^*=2$. By definition we have $\nu(f^*)=0$ and so $-d^*$ is not a square in K. Since $d\sim(-1)^{\frac{n}{2}-1}d^*=(-1)^{\frac{n}{2}}(-d^*)$, $(-1)^{\frac{n}{2}}d$ is also not a square in K. Finally, suppose $\nu^*=4$. Then, $d\sim(-1)^{\frac{n}{2}-2}d^*=(-1)^{\frac{n}{2}}d^*$. Since $\nu(f^*)=0$, $(-1,-1)\otimes\mathfrak{C}(f^*)$ does not split in $K(\sqrt{d^*})$.[19] As every quaternion algebra splits by any quadratic extension over our K,[20] d^* should be a square in K. Thus, we get $(-1)^{\frac{n}{2}}d\sim 1$. Therefore our lemma is proved.

For the archimedean case, it is a trivial fact that the similarity of two forms is characterized by their indices. As an analogue of this we prove the following

LEMMA 3. *Let K be a non-archimedean field. In order to have $f\backsim g$ it is necessary and sufficient that: $\nu(f)=\nu(g)$, if n is odd; $\nu(f)=\nu(g)$ and $d(f)\sim d(g)$, if n is even.*[21]

PROOF. The necessity is trivial. Now, assume that $\nu(f)=\nu(g)$ for an odd n. If $\nu^*(f)=\nu^*(g)=1$, then $f^*\backsim g^*$ and it follows that $f\backsim g$. If $\nu^*(f)=\nu^*(g)=3$, then $\nu(f^*)=\nu(g^*)=0$, and $(-1,-1)\otimes\mathfrak{C}(f^*)$ and $(-1,-1)\otimes\mathfrak{C}(g^*)$ do not split in K.[22] As there exists only one algebra class of order 2 over our K,[23] we get $\mathfrak{C}(f^*)\sim\mathfrak{C}(g^*)$. Let a be an element in K^* such that $d(f^*)\sim d(ag^*)$. Since $\mathfrak{C}(ag^*)\sim\mathfrak{C}(g^*)$, we see that $f^*\sim ag^*$, namely $f^*\backsim g^*$. Therefore we get $f\backsim g$. Next, assume that $\nu(f)=\nu(g)$ and $d(f)\sim d(g)$ for an even n. If $\nu^*(f)=\nu^*(g)=0$ or 4, then from Lemma 2 we have $d(f)\sim d(g)\sim(-1)^{\frac{n}{2}}$ and $\mathfrak{C}(f)\sim\mathfrak{C}(g)$. If $\nu^*(f)=\nu^*(g)=2$, then from the condition on the discriminants we have $d(f^*)\sim d(g^*)$. Since f^* and g^* are binary forms, this implies that $f^*\backsim g^*$. Thus, we again have $f\backsim g$. This settles the sufficiency.[24]

19) [4] Satz 14.
20) [3] p. 113.
21) The condition about the discriminats for an even n is trivial except the case $\nu^*(f)=\nu^*(g)=2$.
22) [4] Satz 13.
23) [3] p. 112 Satz 3.
24) This proof was inspired by Mr. Tsuzuku.

For Lorentz groups, we can see by topological considerations that if two groups are homeomorphically isomorphic then their corresponding forms have equal indices. The analogue of this holds also for our general field K as a consequence of Dieudonné's result on the automorphisms of orthogonal groups. We get the following

LEMMA 4.[24'] *Let K be a locally compact field as described above. If there exists a homeomorphical isomorphism φ between $O(V,f)$ and $O(V,g)$, then we have $\nu(f)=\nu(g)$.*

PROOF. Since φ is a homeomorphism, if one of the groups is compact, so is the other. This implies that if one of the indices is zero, so is the other.[25] Suppose that $n\leqq 3$, then the indices $\leqq[3/2]=1$ and the statement is proved. Thus, we may assume that $n\geqq 4$ and both indices are $\geqq 1$. For such a case, it is known that φ induces a $1-1$ mapping Φ of the set of all lines in V onto itself such that if a line $<x>$ is orthogonal to another line $<y>$ with respect to f then $\Phi<x>$ is orthogonal to $\Phi<y>$ with respect to g and furthermore $\Phi<x>=<sx>$. where s is a $1-1$ semi-linear transformation of V onto itself.[26] Therefore the image of the basis of a totally isotropic subspace of V for f spans also a totally isotropic subspace of V for g whose dimension is the same as the former one. Thus, we have $\nu(f)=\nu(g)$, and our lemma is proved.

§ 3. Hasse principle.

Hereafter, we assume that K is either a field of algebraic numbers or a field of algebraic functions of one variable over a finite field of characteristic $\neq 2$. Let $K_\mathfrak{p}$ be a $\mathfrak{p}$-adic completion of K with respect to a place $\mathfrak{p}$ in K. Then, $K_\mathfrak{p}$ satisfies the conditions of K in §2 and conversely a field K in § 2 is a $K_\mathfrak{p}$ with a suitable K (in our present sense) and a suitable place $\mathfrak{p}$ in K. We denote by $V_\mathfrak{p}$ the scalar extension of V with respect to $K_\mathfrak{p}$, and by $E_\mathfrak{p}$, $GL(V_\mathfrak{p})$ the corresponding algebra and group. Suppose that a form f is given on V. Naturally

---

24') See the addendum at the end of the paper.

25) Ono [10] Th. 2.

26) Dieudonné [11] Chap. X, §§ 32-33. Though only the automorphism is treated there, we can see that the same argument shows the existence of the above Φ for the case of an isomorphism.

f may be considered as a form on $V_\mathfrak{p}$ for any place $\mathfrak{p}$ in K, and we may consider $O(V,f)$ as a subgroup of $O(V_\mathfrak{p},f)$ for any place $\mathfrak{p}$ in K. Let $\nu_\mathfrak{p}, \nu_\mathfrak{p}^*$ be the local index and coindex of f respectively for a place $\mathfrak{p}$. The Hasse principle for indices is expressed as $\nu=\min_\mathfrak{p} \nu_\mathfrak{p}$, where $\mathfrak{p}$ runs over all places in K. For a real infinite place $\mathfrak{p}$, let $\iota_\mathfrak{p}$ be the number of positive coefficients in a canonical form of f in $K_\mathfrak{p}$. In general, we denote by $\mathfrak{A}_\mathfrak{p}$ the scalar extension of an algebra $\mathfrak{A}$ over K to $K_\mathfrak{p}$.

First we prove the following theorem of Hasse type on the similarity of forms.

THEOREM 1. *Let K be a field of algebraic numbers or a field of algebraic functions of one variable over a finite field of characteristic $\neq 2$, and let V be an n-dimensional vector space over K. Let f and g be two non-degenerate symmetric bilinear forms on V. Then $f \backsim g$ in K ifand only if $f \backsim g$ in $K_\mathfrak{p}$ for every place $\mathfrak{p}$ in K.*

To get this theorem we prove the following lemma.

LEMMA 5. *Let K be a field of algebraic numbers, and let L be a quadratic extension of K: $L=K(\sqrt{d})$. Let $\mathfrak{M}$ be the set of all reat infinite places in K such that d is positive in $K_\mathfrak{p}$. Then, there exists an element $c \in L$ such that $N_{L/K}(c)$ has an arbitrarily given (positive or negative) sign in each $K_\mathfrak{p}$, $\mathfrak{p} \in \mathfrak{M}$.*

PROOF of lemma. Let $\mathfrak{p}$'s and $\mathfrak{q}$'s be places in $\mathfrak{M}$ corresponding to the given positive and negative signs respectively. By the independency of valuations in K, there exists an $x \in K$ such that $|x|_\mathfrak{p} > \sqrt{|d|_\mathfrak{p}}$ and $|x|_\mathfrak{q} < \sqrt{|d|_\mathfrak{q}}$.[27] Since d is positive in $K_\mathfrak{p}$, $\mathfrak{p} \in \mathfrak{M}$, this means that $x_\mathfrak{p}^2 > d_\mathfrak{p}$, $x_\mathfrak{q}^2 < d_\mathfrak{q}$, where $x_\mathfrak{p}$ and $d_\mathfrak{p}$ mean respectively the conjugates of x and d with respect to $\mathfrak{p}$. Thus, if we put $c=x+\sqrt{d}$, then $N_{L/K}c = x^2-d$ satisfies the required condition.

PROOF of theorem. The necessity is trivial. We prove the sufficiency separately for two cases.

Case 1. (n: odd). Suppose that $f \backsim g$ in $K_\mathfrak{p}$ for any place $\mathfrak{p}$ in K. Then, we have $\nu_\mathfrak{p}(f)=\nu_\mathfrak{p}(g)$ for any $\mathfrak{p}$. Put $a=d(f)\,d(g)^{-1}$, then $d(ag) \sim a\, d(g)=d(f)$ since n is odd. We also have $\nu_\mathfrak{p}(ag)=\nu_\mathfrak{p}(g)=\nu_\mathfrak{p}(f)$ for any $\mathfrak{p}$. Thus, we may assume from the first that $\nu_\mathfrak{p}(f)=\nu_\mathfrak{p}(g)$ and

27) [9] p. 8.

$d(f)\sim d(g)$ in $K_\mathfrak{p}$ for any $\mathfrak{p}$. Now, let $\mathfrak{p}$ be a real infinite place. Then, we have $\iota_\mathfrak{p}(f)=\iota_\mathfrak{p}(g)$ or $n-\iota_\mathfrak{p}(g)$. Suppose that $\iota_\mathfrak{p}(f)=n-\iota_\mathfrak{p}(g)$ for some real infinite $\mathfrak{p}$. Since $d(f)\sim d(g)$, it follows that $(-1)^{n-\iota_\mathfrak{p}(f)}=(-1)^{n-\iota_\mathfrak{p}(g)}=(-1)^{\iota_\mathfrak{p}(f)}$. Therefore, $(-1)^n=1$ in $K_\mathfrak{p}$. This contradicts to the assumption that n is odd. Thus, we have $\iota_\mathfrak{p}(f)=\iota_\mathfrak{p}(g)$ for all real infinite places $\mathfrak{p}$. Therefore we have $f\sim g$ in $K_\mathfrak{p}$ for all infinite places $\mathfrak{p}$. Now, let $\mathfrak{p}$ be any finite place in K. Since $\nu_\mathfrak{p}(f)=\nu_\mathfrak{p}(g)$ and $d(f)\sim d(g)$ in $K_\mathfrak{p}$. we get $\mathfrak{C}_\mathfrak{p}(f)\sim\mathfrak{C}_\mathfrak{p}(g)$ from Lemma 2. Therefore $f\sim g$ in $K_\mathfrak{p}$ for all finite places $\mathfrak{p}$. Thus, we get $f\sim g$ in $K_\mathfrak{p}$ for any place $\mathfrak{p}$ in K. According to the Hasse principle for the congruence of forms,[28] we get $f\sim g$ in K.

Case 2. (n: even). From the assumption we have $\nu_\mathfrak{p}(f)=\nu_\mathfrak{p}(g)$ and $d(f)\sim d(g)$ in $K_\mathfrak{p}$ for any $\mathfrak{p}$. Now, for any real infinite place $\mathfrak{p}$, we set $\varepsilon_\mathfrak{p}=0$ if $\iota_\mathfrak{p}(g)=\iota_\mathfrak{p}(f)$ and $\varepsilon_\mathfrak{p}=1$ if $\iota_\mathfrak{p}(g)=n-\iota_\mathfrak{p}(f)$. Then, we may select an element $b\in K$ such that b is of sign $(-1)^{\varepsilon_\mathfrak{p}}$ in $K_\mathfrak{p}$ for any real infinite place $\mathfrak{p}$. Then, we see that $\nu_\mathfrak{p}(f)=\nu_\mathfrak{p}(bg)$ for any place $\mathfrak{p}$, in particular $\iota_\mathfrak{p}(f)=\iota_\mathfrak{p}(bg)$ for any real infinite place $\mathfrak{p}$ and $d(f)\sim d(bg)$ since n is even. Thus, from the first was may assume that $\nu_\mathfrak{p}(f)=\nu_\mathfrak{p}(g)$ for any place $\mathfrak{p}$, $\iota_\mathfrak{p}(f)=\iota_\mathfrak{p}(g)$ for any real infinite place $\mathfrak{p}$ and $d(f)\sim d(g)$ in K. Now, for infinite places $\mathfrak{p}$, since $f\sim g$ in $K_\mathfrak{p}$, we get $\mathfrak{C}_\mathfrak{p}(f)\cong\mathfrak{C}_\mathfrak{p}(g)$ and for finite places $\mathfrak{p}$ such that $\nu_\mathfrak{p}^*(f)=\nu_\mathfrak{p}^*(g)=0$ or 4, i.e. $(-1)^{\frac{n}{2}}d(f)\sim(-1)^{\frac{n}{2}}d(g)\sim 1$ in $K_\mathfrak{p}$, we get $\mathfrak{C}_\mathfrak{p}(f)\sim\mathfrak{C}_\mathfrak{p}(g)$ from Lemma 2. Thus, $\big(\mathfrak{C}(f)\otimes\mathfrak{C}(g)\big)_\mathfrak{p}=\mathfrak{C}_\mathfrak{p}(f)\otimes\mathfrak{C}_\mathfrak{p}(g)\sim 1$ for the above mentioned places $\mathfrak{p}$. If, moreover, $\mathfrak{C}_\mathfrak{p}(f)\sim\mathfrak{C}_\mathfrak{p}(g)$ for all such places $\mathfrak{p}$ that $\nu_\mathfrak{p}^*(f)=\nu_\mathfrak{p}^*(g)=2$[29], then we have $f\sim g$ in $K_\mathfrak{p}$ for all places $\mathfrak{p}$ in K. Thus, we have $f\sim g$ in K as in Case 1. If not, then the algebra $\mathfrak{C}(f)\otimes\mathfrak{C}(g)$ over K is of exponent 2, i.e. of Schur index 2.[30] Therefore we see that $\mathfrak{C}(f)\otimes\mathfrak{C}(g)\sim\big(a, K(\sqrt{\beta}), \sigma\big)$ where a, $\beta\in K^*$, σ is a generator of Galois group of $K(\sqrt{\beta})$ over K. Thus, $\mathfrak{C}(f)\otimes\mathfrak{C}(g)\sim 1$ in $K(\sqrt{\beta})$. For the above mentioned non-exceptional places $\mathfrak{p}$, obviously we have $\mathfrak{C}(f)\otimes\mathfrak{C}(g)\sim 1$ in $K_\mathfrak{p}\big(\sqrt{(-1)^{\frac{n}{2}}d(f)}\big)$. On the other hand, for

28) [4] Satz 20.
29) We call such a finite place *exceptional*.
30) [3] p. 119, Satz 6, 7.

the exceptional places $\mathfrak{p}$, since $(-1)^{\frac{n}{2}}d(f)$ is not a square in $K_{\mathfrak{p}}$, we also have $\mathfrak{C}(f)\otimes\mathfrak{C}(g)\sim 1$ in $K_{\mathfrak{p}}\left(\sqrt{(-1)^{\frac{n}{2}}d(f)}\right)$. Thus, we get from the fundamental statement on algebra classes, $\mathfrak{C}(f)\otimes\mathfrak{C}(g)\sim 1$ in $L=K\left(\sqrt{(-1)^{\frac{n}{2}}d(f)}\right)$.[31] Then, we also have $L=K(\sqrt{\beta})$.[32] Thus, we get $\mathfrak{C}(f)\otimes\mathfrak{C}(g)\sim(a,L,\sigma)=\left(a,(-1)^{\frac{n}{2}}d(f)\right)$. Our next task is to replace a by an element $\in K^*$ which is totally positive. To do this, let $\mathfrak{M}$ be the set of all real infinite places $\mathfrak{p}$ in K such that $d=(-1)^{\frac{n}{2}}d(g)$ is positive in $K_{\mathfrak{p}}$. Then from the above Lemma 5, there exists $c\in L$ such that $aN_{L/K}c$ is positive in $K_{\mathfrak{p}}$ for all $\mathfrak{p}\in\mathfrak{M}$. As $(N_{L/K}c, L, \sigma)\sim 1$,[33] we may assume that $\left(\mathfrak{C}(f)\otimes\mathfrak{C}(g)\right)\sim\left(a,(-1)^{\frac{n}{2}}d(g)\right)$, where a is positive in $K_{\mathfrak{p}}$ for all $\mathfrak{p}\in\mathfrak{M}$. On the other hand, for all real infinite places $\mathfrak{p}$ such that $\mathfrak{p}\notin\mathfrak{M}$, a must be positive in $K_{\mathfrak{p}}$, since $1\sim\left(\mathfrak{C}(f)\otimes\mathfrak{C}(g)\right)_{\mathfrak{p}}\sim\left(a,(-1)^{\frac{n}{2}}d(g)\right)_{\mathfrak{p}}$ for these places $\mathfrak{p}$. Therefore, we have $\omega_{\mathfrak{p}}(f)=\omega_{\mathfrak{p}}(ag)$ for all real infinite places $\mathfrak{p}$. From the above formula of equivalence we get $\mathfrak{C}(f)\sim\left(a,(-1)^{\frac{n}{2}}d(g)\right)\otimes\mathfrak{C}(g)\sim\mathfrak{C}(ag)$. Therefore, we have $\mathfrak{C}_{\mathfrak{p}}(f)\sim\mathfrak{C}_{\mathfrak{p}}(ag)$ and $d(f)\sim d(ag)$ for all finite places $\mathfrak{p}$. This means that $f\sim ag$ in $K_{\mathfrak{p}}$ for all finite places $\mathfrak{p}$. Together with the above equality on $\omega_{\mathfrak{p}}$, we get from the Hasse principle for congruences, $f\sim ag$ in K. This proves our statement.

We get immediately from Lemma 1 in §1 the following theorem of Hasse type for orthogonal groups.

THEOREM 2. *Let K and V be as described in Theorem* 1. *Let f and g be forms on V. Then the orthogonal groups $O(V,f)$ and $O(V,g)$ are conjugate in $GL(V)$ if and only if $O(V_{\mathfrak{p}},f)$ and $O(V_{\mathfrak{p}},g)$ are conjugate in $GL(V_{\mathfrak{p}})$ for all places $\mathfrak{p}$ in K.*

Finally we prove the following theorem for orthogonal groups.

THEOREM 3. *Let K and V be as described in Theorem* 1. *Let f and g be forms on V. If their local orthogonal groups $O(V_{\mathfrak{p}},f)$ and $O(V_{\mathfrak{p}},g)$ are homeomorphically isomorphic for every place $\mathfrak{p}$ in K, then the global groups $O(V,f)$ and $O(V,g)$ are conjugate in $GL(V)$.*

---

31) [3] p. 118, Satz 2.
32) [3] p. 122, Satz 11.
33) [3] p. 65, Satz 3.

PROOF. From Lemma 4, we have $\nu_{\mathfrak{p}}(f)=\nu_{\mathfrak{p}}(g)$ for any place $\mathfrak{p}$ in K. If n is odd, we get $f\backsim g$ in $K_{\mathfrak{p}}$ for any $\mathfrak{p}$ by Lemma 3. Thus, it follows from Theorem 1 that $f\backsim g$ in K. On the other hand, if n is even, again we have $\nu_{\mathfrak{p}}(f)=\nu_{\mathfrak{p}}(g)$ for any $\mathfrak{p}$. Lemma 2 implies that $(-1)^{\frac{n}{2}}d(f)$ is a square in $K_{\mathfrak{p}}$ if and only if $(-1)^{\frac{n}{2}}d(g)$ is so. This means that the set of all finite places in K which split completely relative to the quadratic extension $K\left(\sqrt{(-1)^{\frac{n}{2}}d(f)}\right)$ coincides with such set relative to the extension $K\left(\sqrt{(-1)^{\frac{n}{2}}d(g)}\right)$. Therefore, both quadratic extensions are the class fields over the same ideal class group in K, and so they coincide.[34] Thus, we get $d(f)\sim d(g)$. Then, we have $f\backsim g$ in $K_{\mathfrak{p}}$ for any $\mathfrak{p}$, from Lemma 3. Thus, we get $f\backsim g$ in K from Theorem 1. Therefore we have the conjugateness of two groups.

Nagoya University.

Reference

[1] H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Crelle, Bd. 152, pp. 129-148, 1923.
[2] H. Hasse, Über die Äquivalenz quadratischer Formen im Kōrper der rationalen Zahlen, Crelle, ibid. pp. 205-224.
[3] M. Deuring, Algebren, Ergebn. d. Math. IV, 1. Berlin, 1935.
[4] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, Crelle, Bd. 176, pp. 31-44, 1937.
[5] J. Dieudonné, Sur les groupes classiques, Actual. Scient. et Ind., no. 1040, Paris (Hermann), 1948.
[6] M. Eichler, Quadratische Formen und Orthogonale Gruppen, Berlin (Springer), 1952.
[7] L. E. Dickson, Linear groups, Leipzig (Teubner), 1901.
[8] B. W. Jones, The Arithmetic Theory of Quadratic Forms, New York, 1950.
[9] E. Artin, Algebraic numbers and algebraic functions I, Princeton, 1951.
[10] T. Ono, On the Compacity of the Orthogonal groups, Nagoya Math. Journ., vol. 7, 1954.
[11] J. Dieudonné, On the automorphisms of the classical groups, Memoirs of the Amer. Math. Soc. vol. 2., 1952.
[12] C. Chevalley, Sur la théorie du corps de classes dans les corps finis et les corps locaux, Journ. Fac. Sci. Tokyo II, pp. 365-474, 1933.

34) Chevalley [12] Chapitre VI. We know that this property is also valid for the function field case.

[13] C. E. Rickart, Isomorphic groups of linear transformations II, Amer. Journ, of Math. vol. 73., pp. 697-716, 1951.

Addendum

(Received Nov. 8, 1954)

After this paper had been prepared, Prof. J. Dieudonné has kindly communicated to the writer that our lemma 4 is true without any topological assumptions provided $n \geqq 3$. His remark is as follows:

The first thing to do is to characterize the extremal involutions of the orthogonal groups by the method of C. E. Rickart.[35] There is nothing to do for $n=3$, and for $n=4, 5$, Rickart's proof works as well as for $n \geqq 6$. This being done we can see that there is no isomorphism between $O(V, f)$ and $O(V, g)$ if the index is 0 for one of them and $\neq 0$ for the other by the arguments of [11][36]. We are thus reduced to the case where both indices are >0 and $n \geqq 4$; this is done by the same arguments as those of [11].[37]

By this remark, we can further weaken the assumption of our Theorem 3 (for $n \geqq 3$) to get

THEOREM 3′. *Let K and V be as described in Theorem* 1. *If the local groups $O(V_\mathfrak{p}, f)$ and $O(V_\mathfrak{p}, g)$ are (abstractlly) isomorphic for every place $\mathfrak{p}$ in K, thethe global groups $O(V, f)$ and $O(V, g)$ are conjugate in $GL(V)$.*

---

35) Richart [13] p. 703. Th. 1.4.
36) [11] p. 48.
37) [11] p. 48-51.