J. Math. Soc. Japan
Vol. 31, No. 1, 1979

On Hasse principle for division of quadratic forms

By Takashi ONO and Hiroyuki YAMAGUCHI

(Received June 20, 1977)

Introduction.

Let (A, α), (B, β) be algebras with involution over a global field K of characteristic$\neq 2$. Denote by $\mathrm{Hom}((A, \alpha), (B, \beta))$ the set of all algebra homomorphisms $\pi : A \rightarrow B$ sending the identity of A to that of B such that $\pi(a^{\alpha})=\pi(a)^{\beta}$. For each place v of K denote by $\mathrm{Hom}_v((A, \alpha), (B, \beta))$ the similar set obtained by regarding (A, α), (B, β) as algebras over the local field K_v at v. By the Hasse principle for (A, α), (B, β) we shall mean the following statement

$$\text{(H)} \qquad \mathrm{Hom}((A, \alpha), (B, \beta))\neq\emptyset \Leftrightarrow \mathrm{Hom}_v((A, \alpha), (B, \beta))\neq\emptyset \qquad \text{for all } v.$$

Since the algebra with involution appears in many interesting scenes of mathematics, we are anxious to know to what extent (H) is true. The main result of this paper ((4.8) Theorem) says that (H) holds when A, B are the matrix algebras over K. For the proof, the case where both of α and β are "symmetric" is most important and, in this case, (H) is equivalent to the Hasse principle for the division of quadratic forms ((3.1) Theorem), a special case of which appeared in Ono [1]. When $A=C=C(q_V)$, the Clifford algebra of a quadratic form q_V over a space V, and $\alpha=$the involution $-$ of C which changes the sign of vectors in V, and $(B, \beta)=(\mathrm{End}\ Y, *)$, where Y is a vector space and $*$ is a symmetric involution associated to a quadratic form q_Y on Y, the set $\mathrm{Hom}((C, -), (\mathrm{End}\ Y, *))$ is essentially the same as the set of solutions $\beta : X\times Y \rightarrow Y$ (bilinear) to the Hurwitz equation $q_Y(\beta(x, y))=q_X(x)q_Y(y)$, where (X, q_X) is closely related to (V, q_V) ((5.6) Theorem). Thus (H) swallows up the Hasse principle for the Hurwitz equations. In §6, the younger author considers the case where $q_X=x_1^2+\cdots+x_p^2$, $q_Y=$arbitrary form and reduces the Hasse principle for the Hurwitz equation for q_X, q_Y to the older author's (4.8) Theorem, whereby extending the scope of the validity of (H). The contents of §1$\sim$§5 grew out of the course of lectures (Spring term, 1977) by the older author.

§ 1. Preliminaries.

Throughout this section, K will denote any field of characteristic$\neq 2$. We shall use the same symbol $\sim$ for the following three equivalence relations. Firstly, in the multiplicative group $K^\times$, we write $a\sim b$ when $ab^{-1}\in(K^\times)^2$. Secondly, we write $A\sim B$ when central simple algebras A, B over K are similar. Lastly, we write $f\sim g$ when quadratic forms f, g over K are congruent.

The symbol (a, b), $a, b\in K^\times$, means the quaternion algebra over K with basis 1, i, j, k such that $i^2=a$, $j^2=b$, $k=ij=-ji$. The quaternion algebra gives rise to a symmetric bilinear map

$$(,): K^\times/(K^\times)^2\times K^\times/(K^\times)^2 \longrightarrow B(K),$$

where $B(K)$ is the Brauer group of K. We know the identities $(a, -a)\sim 1$, $(a, a)\sim(a, -1)$.

There are three basic invariants for the non-degenerate quadratic form f: the rank $r(f)$, the determinant $d(f)$ and the Hasse algebra $h(f)$. Here, $r(f)$=dimension of the vector space where f is defined, $d(f)$=determinant of the symmetric matrix associated with f and $h(f)\sim\bigotimes_{i<j}(a_i, a_j)$ when $f\sim\langle a_1, \cdots, a_n\rangle$, the diagonal form $a_1x_1^2+\cdots+a_nx_n^2$ on the space K^n, $n=r(f)$. These are invariants in the sense that $r(f)=r(g)$, $d(f)\sim d(g)$ and $h(f)\sim h(g)$ whenever $f\sim g$.

Let X, Y be vector spaces for non-degenerate quadratic forms f, g, respectively. The direct sum $f\oplus g$ is the quadratic form on $X\oplus Y$ such that $(f\oplus g)(x+y)=f(x)+g(y)$ and the tensor product $f\otimes g$ is the quadratic form on $X\otimes Y$ such that $(f\otimes g)(x\otimes y)=f(x)g(y)$. The set of all equivalence classes of non-degenerate quadratic forms over K together with the operation induced by $f\oplus g$ and $f\otimes g$ forms a commutative semiring. Under these operations, the invariants behave as follows:

$$(1.1)\qquad \begin{cases} r(f\oplus g)=r(f)+r(g), & r(f\otimes g)=r(f)r(g), \\ d(f\oplus g)\sim d(f)d(g), & d(f\otimes g)\sim d(f)^{r(g)}d(g)^{r(f)}, \\ h(f\oplus g)\sim(d(f), d(g))\otimes h(f)\otimes h(g). & \end{cases}$$

The formula for $h(f\otimes g)$ is not explicit in the literature. To get this, we need a little preparation. First of all, for any integer n, put $n^*=(1/2)n(n-1)$. We define the discriminant of f by $\varDelta(f)=(-1)^{r(f)^*}d(f)$. Next, suppose that $f\sim\langle a_1, \cdots, a_{r(f)}\rangle$. Then, for $c\in K^\times$, we have

$$(1.2)\qquad h(cf)\sim(c, \varDelta(f)d(f)^{r(f)})\otimes h(f).$$

Next, by induction, one generalizes (1.1) to get

$$h(f_1\oplus\cdots\oplus f_n)\sim h(\langle d(f_1),\cdots,d(f_n)\rangle)\otimes\bigotimes_{i=1}^{n}h(f_i). \tag{1.3}$$

Finally, since $f\otimes g\sim\langle a_1,\cdots,a_{r(f)}\rangle\otimes g\sim(\langle a_1\rangle\oplus\cdots\oplus\langle a_{r(f)}\rangle)\otimes g\sim a_1g\oplus\cdots\oplus a_{r(f)}g$, it follows from (1.2), (1.3) that $h(f\otimes g)\sim h(a_1g\oplus\cdots\oplus a_{r(f)}g)\sim h(\langle a_1{}^{r(g)}d(g),\cdots,a_{r(f)}^{r(g)}d(g)\rangle)\otimes\bigotimes_{i=1}^{r(f)}h(a_ig)\sim h(d(g)\langle a_1{}^{r(g)},\cdots,a_{r(f)}^{r(g)}\rangle)\otimes\bigotimes_{i=1}^{r(f)}((a_i,\Delta(g)d(g)^{r(g)})\otimes h(g))\sim(d(g),\Delta(f)d(f)^{r(f)r(g)+r(g)+1})\otimes h(f)^{r(g)}\otimes(d(f),\Delta(g)\cdot d(g)^{r(g)})\otimes h(g)^{r(f)}$, and we get the following formula:

$$\begin{aligned}h(f\otimes g)\sim(d(f),\Delta(g))\otimes(d(g),\Delta(f))\otimes(d(f),d(g))^{r(f)r(g)+1}\\ \otimes h(f)^{r(g)}\otimes h(g)^{r(f)}.\end{aligned} \tag{1.4}$$

We shall say that a non-degenerate quadratic form f divides another such form g and write $f|g$ if there is a quadratic form q such that $g\sim q\otimes f$. If $f|g$, one must have $r(f)|r(g)$ by (1.1). When K is algebraically closed, since there is one and only one class of forms of given rank, we have

$$f\,|\,g\Leftrightarrow r(f)|r(g),$$

and so the divisibility of quadratic forms is the same as that of natural numbers.

§2. Local fields.

We shall first consider the case $K=\boldsymbol{R}$. Let f be a non-degenerate quadratic form over $\boldsymbol{R}$. When $f\sim\langle\underbrace{1,\cdots,1}_{m},\underbrace{-1,\cdots,-1}_{n}\rangle$, the signature $\sigma(f)$ is the number $m-n$. It is well-known that

$$f\sim g\Longleftrightarrow r(f)=r(g)\quad\text{and}\quad\sigma(f)=\sigma(g).$$

One verifies easily that

$$\sigma(f\oplus g)=\sigma(f)+\sigma(g),\quad\sigma(f\otimes g)=\sigma(f)\sigma(g). \tag{2.1}$$

As for the divisibility, we have the following criterion:

(2.2) PROPOSITION. *For non-degenerate quadratic forms f, g over $\boldsymbol{R}$, we have*

$$f|g\Longleftrightarrow\begin{cases}\text{(i)} & r(f)|r(g)\ \textit{and}\\ \text{(ii)} & \textit{either}\ \ \sigma(f)=\sigma(g)=0\ \ \textit{or}\ \ \sigma(f)\neq0\\ & \textit{and}\ \ \sigma(f)|\sigma(g),\ \ |\sigma(g)\sigma(f)^{-1}|\leqq r(g)r(f)^{-1},\\ & \sigma(g)\sigma(f)^{-1}\equiv r(g)r(f)^{-1}\ (\text{mod.}\,2).\end{cases}$$

PROOF. ($\Rightarrow$) Suppose that $g \sim q \otimes f$. Then, by (2.1), we have $\sigma(g) = \sigma(q)\sigma(f)$ and so $\sigma(g)=0$ when $\sigma(f)=0$. Assume now that $\sigma(f) \neq 0$. Then, obviously $\sigma(f) | \sigma(g)$, and $|\sigma(g)\sigma(f)^{-1}| \leqq r(g)r(f)^{-1}$ since $|\sigma(q)| \leqq r(q)$. The last relation follows from $\sigma(q) \equiv r(q)$ (mod. 2).

($\Leftarrow$) When $\sigma(f)=\sigma(g)=0$, we have $\sigma(g)=\sigma(q)\sigma(f)$ for any q such that $r(q)=r(g)r(f)^{-1}$. Hence $g \sim q \otimes f$ and so $f|g$. When $\sigma(f) \neq 0$, put $s=\sigma(g)\sigma(f)^{-1}$. Since $|s| \leqq r(g)r(f)^{-1}$ and $s \equiv r(g)r(f)^{-1}$ (mod. 2), there is a number k, $0 \leqq k \leqq r(g)r(f)^{-1}$, such that $s=2k-r(g)r(f)^{-1}$. Let q be a quadratic form of rank $r(g)r(f)^{-1}$ such that $q \sim \langle \underbrace{1, \cdots, 1}_{k}, -1, \cdots, -1 \rangle$. Then, $\sigma(q)=k-(r(g)r(f)^{-1}-k) = s$, and so $g \sim q \otimes f$, q. e. d.

From now on, in this section, let K be a non-discrete, non-connected commutative locally compact field of characteristic $\neq 2$; for simplicity, we shall call such K a $\mathfrak{p}$-adic field, where $\mathfrak{p}$ stands for the unique maximal ideal of the unique maximal compact subring of K. Over such a field K, it is well-known that two non-degenerate quadratic forms f, g are equivalent $f \sim g$ if and only if $r(f)=r(g)$, $d(f) \sim d(g)$ and $h(f) \sim h(g)$. Hence, we have $f|g$ if and only if[*] there exists a quadratic form q such that

$$(2.3) \quad \begin{cases} r(g)=r(q)r(f), \\ d(g) \sim d(q)^{r(f)}d(f)^{r(q)}, \\ h(g) \sim (d(q), \Delta(f)) \otimes (d(f), \Delta(q)) \otimes (d(q), d(f))^{r(q)r(f)+1} \\ \qquad \otimes h(q)^{r(f)} \otimes h(f)^{r(q)} \\ \quad \sim (d(q), \Delta(f)d(f)^{r(q)r(f)}) \otimes (d(f), -1)^{r(q)^*} \otimes h(q)^{r(f)} \otimes h(f)^{r(q)}. \end{cases}$$

We need to state the criterion for $f|g$ separately according to the parity of $r(f)$.

(2.4) PROPOSITION. *Let f, g be non-degenerate quadratic forms over a $\mathfrak{p}$-adic field K. When $r(f) \equiv 0$ (mod. 2), we have*

$$f|g \Longleftrightarrow \begin{cases} \text{(i)} \quad r(f)|r(g) \quad \textit{and} \\ \text{(ii)} \quad d(g) \sim d(f)^{r(g)r(f)^{-1}} \quad \textit{when} \quad \Delta(f) \nsim 1, \\ \qquad d(g) \sim d(f)^{r(g)r(f)^{-1}} \quad \textit{and} \\ \qquad h(g) \sim (d(f), -1)^{(r(g)r(f)^{-1})^*} \otimes h(f)^{r(g)r(f)^{-1}} \\ \qquad \textit{when} \quad \Delta(f) \sim 1. \end{cases}$$

[*] Needless to say that the "only if"-part works for any field of characteristic $\neq 2$. Similar remark applies to the "only if"-part of (2.4), (2.5) and (2.6).

Proof. We only have to prove the "if"-part ($\Leftarrow$). When $\Delta(f)\sim 1$, take any q such that $r(g)=r(q)r(f)$. The conditions (i), (ii) then imply (2.3). When $\Delta(f)\not\sim 1$, we first take $a\in K^{\times}$ such that

$$(a,\ \Delta(f))\sim(d(f),\ -1)^{(r(g)r(f)^{-1})^{*}}\otimes h(g)\otimes h(f)^{r(g)r(f)^{-1}}.$$

This is possible because the symmetric bilinear mapping $(\ ,\ )$: $K^{\times}/(K^{\times})^{2}\times K^{\times}/(K^{\times})^{2}\rightarrow B(K)$ is non-degenerate when K is $\mathfrak{p}$-adic. Next, take q such that $q\sim\langle a,1,\cdots,1\rangle$ and $r(g)=r(q)r(f)$. Then, since $d(q)\sim a$, the conditions (i), (ii) imply again (2.3), q.e.d.

Assume now that $r(f)\equiv 1$ (mod. 2). From (2.3), it follows that $f|g$ if and only if there exists a q such that

$$(2.5)\qquad \begin{cases} r(q)=r(g)r(f)^{-1}, \\ d(q)\sim d(g)d(f)^{r(g)r(f)^{-1}}, \\ h(q)\sim h(g)\otimes h(f)^{r(g)r(f)^{-1}}\otimes(d(g)d(f)^{r(g)r(f)^{-1}},\ \Delta(f)d(f)^{r(g)r(f)^{-1}}) \\ \qquad\otimes(d(f),\ -1)^{(r(g)r(f)^{-1})^{*}}. \end{cases}$$

In what follows, we shall use the fact: In order that there exists a quadratic form q over K of rank r such that $d(q)\sim d$ and $h(q)\sim\varepsilon$, it is necessary and sufficient that $r=1$, $\varepsilon\sim 1$; or $r=2$, $d\not\sim -1$; or $r=2$, $\varepsilon\sim 1$; or $r\geqq 3$, where ε means an element in $B(K)\approx\boldsymbol{Q}/\boldsymbol{Z}$ of order 1 or 2. (We shall often identify with -1 the element of order 2 in $B(K)$).

(2.6) Proposition. *Let f, g be non-degenerate quadratic forms over a $\mathfrak{p}$-adic field K. Assume that $r(f)\equiv 1$ (mod. 2). Then we have*

$$f|g\Longleftrightarrow\begin{cases} \text{(i)}\quad r(f)|r(g)\ \ \textit{and}\ \ r(g)r(f)^{-1}\geqq 3,\ \ \textit{or} \\ \text{(ii)}\quad r(g)=r(f)\ \ \textit{and}\ \ h(g)\otimes h(f)\otimes(d(g)d(f),\ -1)^{r(f)^{*}}\sim 1, \\ \textit{or} \\ \text{(iii)}\quad r(g)=2r(f)\ \ \textit{and either}\ \ d(g)\not\sim -1\ \ \textit{or} \\ \qquad h(g)\otimes(d(g),\ \Delta(f))\otimes(d(f),\ -1)\sim 1. \end{cases}$$

Proof. We only have to prove the "if"-part. In case (i), by the above remark, we can find q such that $r(q)=r(g)r(f)^{-1}$, $d(q)\sim d(g)d(f)^{r(g)r(f)^{-1}}$ and $h(q)\sim$ the algebra on the right hand side of (2.5). Then $f|g$ by (2.5). In case (ii), take q such that $r(q)=1$ and $q\sim\langle d(g)d(f)\rangle$. Then, since $h(q)\sim 1$, we have (2.5) and so $f|g$. In case (iii), we can find q such that $r(q)=2$, $d(q)\sim d(g)$ and $h(q)\sim h(g)\otimes(d(g),\ \Delta(f))\otimes(d(f),\ -1)$ and hence $f|g$, again, by (2.5), q.e.d.

§ 3. Hasse principle for division of quadratic forms.

In this section, K will denote a global field of characteristic$\neq 2$. For a place v of K we denote by K_v the completion of K at v. We shall reserve the symbol $\sim$ exclusively for objects (field elements, quadratic forms, central simple algebras etc.) over the global field K. For objects defined over local field K_v, we shall write $\underset{v}{\sim}$ for the equivalences. For quadratic forms f, g over K_v, we shall write $f\underset{v}{|}g$ when f divides g.

(3.1) Theorem. *Let f, g be non-degenerate quadratic forms over a global field K of characteristic $\neq 2$. Then, $f|g$ if and only if $f\underset{v}{|}g$ for all places v.*

We recall here some necessary facts on global fields.

(3.2) (Theorem 4.5.10 of Scharlau [1]). *Let q_v be a quadratic form for each v, with a fixed rank. There exists a quadratic form q over K such that $q\underset{v}{\sim}q_v$ for all v if the following conditions are satisfied:*

(i) *there is a $d\in K^\times$ such that $d(q_v)\underset{v}{\sim}d$ for all v,*

(ii) *$h(q_v)\underset{v}{\sim}1$ for almost all v,*

(iii) *the number of v where $h(q_v)\underset{v}{\nsim}1$ is even.*

(3.3) (A special case of Exercise 2.16, p. 355 of Cassels-Fröhlich [1]). *Let $a\in K^\times$ and let $\varepsilon_v=\pm 1$ for each v. There exists $x\in K^\times$ such that $(a, x)\underset{v}{\sim}\varepsilon_v$ for all v if the following conditions are satisfied:*

(i) *$\varepsilon_v=1$ for almost all v,*

(ii) *the number of v where $\varepsilon_v=-1$ is even,*

(iii) *there is an $x_v\in(K_v)^\times$ such that $(a, x_v)\underset{v}{\sim}\varepsilon_v$ for all v.*

(3.4) (Lemma 5 of Ono [1]). *Let K be an algebraic number field and L be a quadratic extension: $L=K(\sqrt{d})$. Let M be a subset of the set of all real infinite places of K such that d is positive in K_v. Then, there exists an element $c\in L$ such that $N_{L/K}(c)$ has an arbitrarily given sign in each K_v, $v\in M$.*

Proof of (3.1) Theorem. We only have to prove the "if"-part.

Case 1. $r(f)\equiv 1$ (mod. 2).

For each v, the assumption of the "if"-part implies that there is a q_v such thea $g\underset{v}{\sim}q_v\otimes f$, and so

$$(3.5)\quad \begin{cases} r(q_v)=r(g)r(f)^{-1}, \\ d(q_v)\underset{v}{\sim}d(g)d(f)^{r(g)r(f)^{-1}}, \\ h(q_v)\underset{v}{\sim}h(g)\otimes h(f)^{r(g)r(f)^{-1}}\otimes(d(g)d(f)^{r(g)r(f)^{-1}}, \varDelta(f)d(f)^{r(g)r(f)^{-1}}) \\ \qquad\qquad \otimes(d(f), -1)^{(r(g)r(f)^{-1})^*}. \end{cases}$$

Hence, if we put $d=d(g)d(f)^{r(g)r(f)^{-1}}$ then (i) of (3.2) follows from (3.5). The conditions (ii), (iii) of (3.2) hold since $h(q_v)$ is equivalent to an algebra given globally as the right hand side of (3.5). Hence, there exists a q over K such that $q \underset{v}{\sim} q_v$ for all v. We have then $g \underset{v}{\sim} q \otimes f$ for all v. By the Hasse-Minkowski theorem on quadratic forms, we have $g \sim q \otimes f$, i.e. $f|g$.

Case 2. $r(f)\equiv 0 \pmod{2}$, $\varDelta(f) \sim 1$.

The assumption that $f \underset{v}{|} g$ implies that

$$(3.6)\qquad \begin{cases} d(g) \underset{v}{\sim} d(f)^{r(g)r(f)^{-1}}, \\ h(g) \underset{v}{\sim} (d(f), -1)^{(r(g)r(f)^{-1})^*} \otimes h(f)^{r(g)r(f)^{-1}}. \end{cases}$$

Let E be the set of all real infinite places of K for which the signature $\sigma_v(f)\neq 0$. By the independence of valuations, one can find a form q over K such that $r(q)=r(g)r(f)^{-1}$ and $\sigma_v(q)=\sigma_v(g)\sigma_v(f)^{-1}$ for all $v\in E$. Then we have $g \underset{v}{\sim} q \otimes f$ for all infinite places v of K. As for a finite place $v=\mathfrak{p}$, (3.6) implies that

$$\begin{cases} d(g) \underset{\mathfrak{p}}{\sim} d(f)^{r(q)}, \\ h(g) \underset{\mathfrak{p}}{\sim} (d(f), -1)^{r(q)^*} \otimes h(f)^{r(q)}, \end{cases}$$

and by (2.3) we see that $q \underset{\mathfrak{p}}{\sim} g \otimes f$. Therefore, by the Hasse-Minkowski theorem, we have $g \sim q \otimes f$.

Case 3. $r(f)\equiv 0 \pmod{2}$, $\varDelta(f) \nsim 1$.

The assumption implies that for each v there is a q_v such that

$$(3.7)\qquad \begin{cases} d(g) \underset{v}{\sim} d(f)^{r(g)r(f)^{-1}}, \\ h(g) \underset{v}{\sim} (d(f), -1)^{(r(g)r(f)^{-1})^*} \otimes (d(q_v), \varDelta(f)) \otimes h(f)^{r(g)r(f)^{-1}}. \end{cases}$$

By (3.3) and (3.7) with $x_v=d(q_v)$, one can find an element $t\in K^\times$ such that

$$(3.8)\qquad h(g) \sim (d(f), -1)^{(r(g)r(f)^{-1})^*} \otimes (t, \varDelta(f)) \otimes h(f)^{r(g)r(f)^{-1}}.$$

For each real infinite place v, denote by $s_v(\varphi)$ the number of negative coefficients in the diagonal form of a quadratic form φ. So, we have the relations

$$(3.9)\qquad \begin{cases} \sigma_v(\varphi)=r(\varphi)-2s_v(\varphi), \\ d(\varphi) \underset{v}{\sim} (-1)^{s_v(\varphi)}, \\ h(\varphi) \underset{v}{\sim} (-1)^{s_v(\varphi)^*}. \end{cases}$$

From (3.7), (3.9), we have

$$(-1)^{s_v(g)^*}=((-1)^{s_v(f)}, -1)_v^{(r(g)r(f)^{-1})^*}(t, (-1)^{r(f)^*+s_v(f)})_v \times(-1)^{s_v(f)^*r(g)r(f)-1}, \tag{3.10}$$

where $(,)_v$ means the Hilbert symbol at v.

Let E be as before, the set of all real infinite places of K for which $\sigma_v(f)\neq 0$. We have then

$$s_v(q_v)=\frac{1}{2}\left(\frac{r(g)}{r(f)}-\frac{r(g)-2s_v(g)}{r(f)-2s_v(f)}\right). \tag{3.11}$$

Now, let M (resp. N) be the set of places $v\in E$ for which $\Delta(f)\underset{v}{>}0$ (resp. $\Delta(f)\underset{v}{<}0$). By (3.4), there is an element $c\in L^\times$, $L=K(\sqrt{\Delta(f)})$ such that

$$\mathrm{sign}_v(tNc)=(-1)^{s_v(q_v)} \quad \text{for all} \quad v\in M.$$

Since one can replace t by tNc in $(t, \Delta(f))$, one can assume without loss of generality that

$$\mathrm{sign}_v(t)=(-1)^{s_v(q_v)} \quad \text{for all} \quad v\in M.$$

Next, we claim that

$$\mathrm{sign}_v(t)=(-1)^{s_v(q_v)} \quad \text{for all} \quad v\in N.$$

In fact, since $\Delta(f)\underset{v}{<}0$ for $v\in N$, we have

$$1\equiv r(f)^*+s_v(f)\equiv\frac{1}{2}r(f)-s_v(f) \ (\mathrm{mod.}\ 2), \quad v\in N. \tag{3.12}$$

We also have

$$(t, \Delta(f))_v=(t, -1)_v=\mathrm{sign}_v(t), \quad v\in N. \tag{3.13}$$

Substituting (3.13) in (3.10), we get

$$\mathrm{sign}_v(t)=(-1)^{s_v(g)^*+s_v(f)^*r(g)r(f)^{-1}}((-1)^{s_v(f)}, -1)^{(r(g)r(f)^{-1})^*}. \tag{3.14}$$

Now, one sees easily from (3.11) that

$$s_v(q_v)=\frac{(1/2)(s_v(g)-s_v(f)r(g)r(f)^{-1})}{(1/2)r(f)-s_v(f)}. \tag{3.15}$$

Since the denominator of (3.15) is odd by (3.12), we get

$$(-1)^{s_v(q_v)}=(-1)^{1/2(s_v(g)-s_v(f)r(g)r(f)^{-1})}=\mathrm{sign}_v(t), \quad v\in N,$$

by a straightforward calculation using (3.14). In other words, we have proved that

$$\mathrm{sign}_v(t)=(-1)^{s_v(q_v)} \qquad \text{for all} \quad v\in E=N\cup M.$$

Now, by the independence of valuations, one can find a form q over K such that $r(g)=r(q)r(f)$, $q\sim\langle a_1\cdots a_{r(q)-1}, t(a_1,\cdots,a_{r(q)})^{-1}\rangle$ and $s_v(q)=s_v(q_v)$ for all $v\in E$. Note that $d(q)\sim t$. We have then $\sigma_v(q)=\sigma_v(g)\sigma_v(f)^{-1}$, $v\in E$, i.e. $\sigma_v(g)=\sigma_v(q\otimes f)$, $v\in E$. Since this last equality is trivially true for real infinite $v\notin E$, we have $g\underset{v}{\sim}q\otimes f$ for all infinite places. On the other hand, (3.7), (3.8) imply that $d(g)\underset{\mathfrak{p}}{\sim}d(f)^{r(q)}\underset{\mathfrak{p}}{\sim}d(q\otimes f)$ for all $\mathfrak{p}$ and $h(g)\sim(d(f),-1)^{r(q)^*}\otimes(d(q),\Delta(f))\otimes h(f)^{r(q)}$. Therefore, we have $g\underset{\mathfrak{p}}{\sim}q\otimes f$ for all $\mathfrak{p}$. Hence, again by the Hasse-Minkowski theorem, we have $g\sim q\otimes f$, i.e. $f|g$, q.e.d.

§ 4. Hasse principle for the matrix algebras with involutions.

Let K be a field of characteristic $\neq 2$ and A, B are algebras with 1 over K. By a homomorphism of A to B we always mean an algebra homomorphism sending 1 onto 1. We denote by $\mathrm{Hom}(A, B)$ the set of all homomorphisms. Let α, β be involutions of A, B respectively. We denote by $\mathrm{Hom}((A,\alpha),(B,\beta))$ the subset of $\mathrm{Hom}(A, B)$ consisting of homomorphisms π satisfying $\pi(a^\alpha)=\pi(a)^\beta$, $a\in A$. In this section, we shall consider exclusively the case where A, B are the matrix algebras: $A=K_m$, $B=K_n$. Obviously, we have

$$\mathrm{Hom}(K_m, K_n)\neq\emptyset \Longleftrightarrow m|n. \tag{4.1}$$

Since we are looking for the criterion for $\mathrm{Hom}((K_m,\alpha),(K_n,\beta))\neq\emptyset$, we may assume by (4.1) that $n=qm$, $q\in\boldsymbol{Z}$.

As is well-known, one can write

$$a^\alpha=F^{-1}{}^t aF,\quad a\in K_m,\quad F\in(K_m)^\times,\quad {}^tF=(\mathrm{sgn}\,\alpha)F=\pm F \quad\text{and}$$

$$b^\beta=G^{-1}{}^t bG,\quad b\in K_n,\quad G\in(K_n)^\times,\quad {}^tG=(\mathrm{sgn}\,\beta)G=\pm G.$$

When $\mathrm{sgn}\,\alpha=-1$, m must be even and α may be replaced, without extending the ground field, by the standard involution $j=j_{m/2}$:

$$a^j=J^t aJ^{-1},\quad J=J_{m/2}=\begin{pmatrix} 0 & -1_{m/2} \\ -1_{m/2} & 0 \end{pmatrix}.$$

(4.2) Proposition. $\mathrm{Hom}((K_m,\alpha),(K_n,\beta))\neq\emptyset\Leftrightarrow G\sim U\otimes F$ *for some* $U\in(K_q)^\times$.

PROOF. Call π_0 the representation in $\mathrm{Hom}(K_m, K_n)$ given by $\pi_0(a)=1_q\otimes a$. Since K_m is a simple algebra, any other representation π in $\mathrm{Hom}(K_m, K_n)$ can be written as

$$\pi(a)=T\pi_0(a)T^{-1} \qquad \text{for some} \quad T\in(K_n)^\times.$$

Then we have

$$\pi\in\mathrm{Hom}((K_m, \alpha), (K_n, \beta)) \Longleftrightarrow \pi(a^\alpha)=\pi(a)^\beta,\ a\in K_m$$
$$\Longleftrightarrow T\pi_0(a^\alpha)T^{-1}=(T\pi_0(a)T^{-1})^\beta.$$

Now, we have

$$T\pi_0(a^\alpha)T^{-1}=T(1_q\otimes F^{-1t}aF)T^{-1}=T(1_q\otimes F^{-1})(1_q\otimes {}^ta)(1_q\otimes F)T^{-1}$$

and

$$(T\pi_0(a)T^{-1})^\beta=G^{-1t}(T\pi_0(a)T^{-1})G=G^{-1t}T^{-1}(1_q\otimes {}^ta)^tTG.$$

Hence ${}^tTGT(1_q\otimes F^{-1})$ commutes with $1_q\otimes {}^ta$ for all $a\in K_m$ and so it must be of the form $U\otimes 1_m$ for some $U\in(K_q)^\times$. We have thus ${}^tTGT=U\otimes F$, q. e. d.

From (4.2) we deduce the following results on $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))$, with $n=qm$.

(4.3) *If* $\mathrm{sgn}\,\alpha=\mathrm{sgn}\,\beta=-1$, *then* $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))\neq\emptyset$.

In fact, replacing α, β by the involution j, i.e. replacing F, G by $J_{m/2}$, $J_{n/2}$, respectively, we have $J_{n/2}\sim U\otimes J_{m/2}$ with $U=1_q$.

(4.4) *If* $\mathrm{sgn}\,\alpha\neq\mathrm{sgn}\,\beta$ *and* $q\equiv1$ (mod. 2), *then* $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))=\emptyset$.

In fact, if there exists U such that $G\sim U\otimes F$, then U must be skew-symmetric, but this is impossible since q is odd.

(4.5) *If* $\mathrm{sgn}\,\alpha=1$, $\mathrm{sgn}\,\beta=-1$ *and* $q\equiv0$ (mod. 2), *then* $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))\neq\emptyset$.

In fact, put $U=J_{q/2}$. Then one has $G\sim J_{n/2}\sim J_{q/2}\otimes F$.

(4.6) *If* $\mathrm{sgn}\,\alpha=-1$, $\mathrm{sgn}\,\beta=1$, $q\equiv0$ (mod. 2) and $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))\neq\emptyset$, *then* $G\sim J_{q/2}\otimes J_{m/2}$.

In fact, let $U\in(K_q)^\times$ be such that $G\sim U\otimes F$. Since F is skew-symmetric and G is symmetric, U must be skew-symmetric and so $U\sim J_{q/2}$.

(4.7) *If* $\mathrm{sgn}\,\alpha=\mathrm{sgn}\,\beta=1$, *then* $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))\neq\emptyset$ *if and only if* $F|G$ *in the sense of* § 1.

Now, let K be a global field of characteristic$\neq 2$ and (A, α), (B, β) be algebras with involution over K. We put $\mathrm{Hom}_v((A, \alpha), (B, \beta))=\mathrm{Hom}((A_v, \alpha), (B_v, \beta))$ where $A_v=K_v\otimes A$, $B_v=K_v\otimes B$. By the Hasse principle for (A, α), (B, β) we shall mean the statement:

(H) $\mathrm{Hom}((A, \alpha), (B, \beta))\neq\emptyset \Longleftrightarrow \mathrm{Hom}_v((A, \alpha), (B, \beta))\neq\emptyset$ *for all* v.

(4.8) THEOREM. *Let m, n be any natural numbers and (K_m, α), (K_n, β) be matrix algebras with involutions. Then* (H) *holds for these algebras.*

PROOF. We only have to prove ($\Leftarrow$). The assumption implies that $m|n$ and so we put $n=qm$. In view of (4.3), (4.4), (4.5), it remains to consider the cases (i) $\mathrm{sgn}\,\alpha=-1$, $\mathrm{sgn}\,\beta=1$, $q\equiv 0$ (mod. 2) and (ii) $\mathrm{sgn}\,\alpha=\mathrm{sgn}\,\beta=1$. In case (i), by (4.6), applied for K_v, we have $G\underset{v}{\sim}J_{q/2}\otimes J_{m/2}$ for all v. Hence by the Hasse-Minkowski theorem, we have $G\sim J_{q/2}\otimes J_{m/2}\sim J_{q/2}\otimes F$ and so $\mathrm{Hom}((K_m, \alpha), (K_n, \beta))\neq\emptyset$ by (4.2). In case (ii), by (4.7), our assertion is nothing else than (3.1) Theorem, q.e.d.

§5. Hurwitz equations.

Let K be a field of characteristic$\neq 2$, X a vector space over K of dimension $p\geqq 1$, q_X a non-degenerate quadratic form on X, Y another vector space over K of dimension $n\geqq 1$ and q_Y a non-degenerate quadratic form on Y. We shall assume that there is an $e\in X$ such that $q_X(e)=1$ and fix such an element once for all. Denote by B the set of all bilinear maps $\beta: X\times Y\to Y$ satisfying the Hurwitz equation:

$$q_Y(\beta(x, y))=q_X(x)q_Y(y). \tag{5.1}$$

Our problem is to find a criterion for $B\neq\emptyset$. As the first reduction of the problem, we have

(5.2) PROPOSITION. *Put $B_0=\{\beta\in B, \beta(e, y)=y, y\in Y\}$. Then, $B\neq\emptyset\to B_0\neq\emptyset$.*

PROOF. ($\Leftarrow$) is trivial. To prove ($\Rightarrow$), put $s(y)=\beta(e, y)$. Then, (5.1) implies that $s\in O(q_Y)$, the orthogonal group of q_Y. Obviously, the map $\beta_0(x, y)=s^{-1}(\beta(x, y))$ belongs to B_0, q.e.d.

Before stating the second reduction of the problem, we need some preparations. First, decompose the space X as the orthogonal sum $X=Ke\perp V$ and put $q_V=-q_X|V$. Let $C=C(q_V)$ the Clifford algebra of q_V and let $x\mapsto\bar{x}$ be the unique involution of C such that $\bar{v}=-v$ for all $v\in V$. Next, let $\alpha\mapsto\alpha^*$ be the involution of the algebra $\mathrm{End}\,Y$ of endomorphisms of Y such that $(\alpha y, y')=(y, \alpha^* y')$, $y, y'\in Y$, where $(y, y')=(1/2)(q_Y(y+y')-q_Y(y)-q_Y(y'))$.

(5.3) PROPOSITION. *There is a bijection* $\mathrm{Hom}((C, -), (\mathrm{End}\,Y, *))\approx B_0$.

PROOF. First, we consider $X=Ke\perp V$ as a subset of $C=K\oplus V\oplus\cdots$ by the identification $e=1\in K$. For $\pi\in\mathrm{Hom}((C,-),(\mathrm{End}\,Y,*))$, put $\beta(x,y)=\pi(x)y$, $x\in X$, $y\in Y$. We claim that $\pi\mapsto\beta$ is the bijection we are looking for. In fact, we have $q_Y(\beta(x,y))=q_Y(\pi(x)y)=(\pi(x)y,\pi(x)y)=(y,\pi(x)*\pi(x)y)=(y,\pi(\bar{x})\pi(x)y)=(y,\pi(\bar{x}x)y)$. Write $x=x_0+v$, $x_0\in K$, $v\in V$. Then, we have $\bar{x}x=x_0{}^2-v^2=x_0{}^2-q_V(v)=q_X(x)$ and so $q_Y(\beta(x,y))=(y,q_X(x)y)=q_X(x)q_Y(y)$. Obviously, β is bilinear and satisfies $\beta(e,y)=y$, hence $\beta\in B_0$. Since C is generated by 1 and V, clearly the map $\pi\mapsto\beta$ is injective. Conversely, take any $\beta\in B_0$ and consider a linear map $\lambda: X\rightarrow\mathrm{End}\,Y$ defined by $\lambda(x)y=\beta(x,y)$. Put $\lambda_0=\lambda|V$. The relation (5.1) implies that

$$\lambda(x)*\lambda(x)=q_X(x). \tag{5.4}$$

Writing $x=x_0+v$ as above, we get, from (5.4), $x_0{}^2-q_V(v)=x_0{}^2+x_0(\lambda_0(v)+\lambda_0(v)*)+\lambda_0(v)*\lambda_0(v)$, or

$$\lambda_0(v)+\lambda_0(v)*=0,\quad \lambda_0(v)*\lambda_0(v)=-q_V(v), \tag{5.5}$$

which implies that $\lambda_0(v)^2=q_V(v)$. Hence, by the universal property of the Clifford algebra, we can extend λ_0 to a representation π of C. Now, by (5.5), we have $\pi(-v)*=-\lambda_0(v)*=\lambda_0(v)=\pi(v)$, $v\in V$. Since C is generated by V, we have $\pi\in\mathrm{Hom}((C,-),(\mathrm{End}\,Y,*))$, q.e.d.

Combining (5.2) and (5.3), we get

(5.6) THEOREM. *Notation being as above, we have*

$$B\neq\emptyset \Longleftrightarrow \mathrm{Hom}((C,-),(\mathrm{End}\,Y,*))\neq\emptyset.$$

When K is a global field of characteristic $\neq 2$, denote by B_v the set of all bilinear maps $\beta: X_v\times Y_v\rightarrow Y_v$ satisfying the condition (5.1), where $X_v=K_v\otimes X$, $Y_v=K_v\otimes Y$. By the Hasse principle for the ordered pair (q_X, q_Y) we shall mean the statement:

$$B\neq\emptyset \Longleftrightarrow B_v\neq\emptyset \quad \text{for all } v. \tag{5.7}$$

From (4.8), (5.6), (5.7), we deduce the following

(5.8) THEOREM. *Notation being as above, the Hasse principle for* (q_X, q_Y) *holds whenever* $C(q_V)\approx K_{2m}$, $m=\dim V$, $q_V=-q_X|V$.

(5.9) The assumption of (5.8) is satisfied if, e.g., m is even and q_V has the maximal index. As for other examples, see (6.4).

§ 6. The case $q_X = x_1^2 + \cdots + x_p^2$.

We put $m=p-1$, $q_V=-x_1'^2-\cdots-x_m'^2$ and denote by $(C_m, -)$ the Clifford algebra of q_V. We shall determine the structure of $(C_m, -)$ and prove the Hasse principle (H) for $\mathrm{Hom}((C_m, -), (K_n, *))\neq\emptyset$, which in turn implies the validity of the Hasse principle for our Hurwitz problem.

(6.1) LEMMA. $(C_m, -)\otimes(C_4, -)\approx(C_{m+4}, -)$, *for* $m=1, 2, 3, \cdots$.

PROOF. Suppose $\{e_1, e_2, e_3, e_4\}$, $\{e_1', \cdots, e_m'\}$ are sets of generators of C_4, C_m with the relations

$$e_i^2=e_k'^2=-1, \quad e_i e_j=-e_j e_i \ (i\neq j),$$
$$e_k' e_h'=-e_h' e_k' \ (k\neq h).$$

Put

$$e_i''=1\otimes e_i, \quad 1\leqq i\leqq 4,$$
$$e_i''=e_{i-4}'\otimes e_1 e_2 e_3 e_4, \quad 4<i\leqq m+4.$$

Then, $e_i'' e_j''=-e_j'' e_i''$ $(i\neq j)$ and $e_i''^2=-1$. Moreover, $\overline{e_i''}=-e_i''$, q. e. d.

This lemma reduces our problem to that of determining $(C_m, -)$ for $m\leqq 4$.

(6.2) LEMMA. *If* $D=(-1, -1)_K$ *is not trivial,*

$$(C_1, -)\approx(L, -)$$
$$(C_2, -)\approx(D, -)$$
$$(C_3, -)\approx(D\oplus D, -\oplus -)$$
$$(C_4, -)\approx(D_2, t-), \ \textit{where}$$

$L=K(\sqrt{-1})$ *and* $-$ *in* $(L, -)$ *denotes the non-trivial automorphism of* L *over* K; $t-$ *is the involution* $-\otimes t$ *of* $D\otimes K_2\approx D_2$.

PROOF. If C_3^+ is the even part of C_3, $C_3\approx C_3^+\oplus C_3^+$. $C_3^+=K+Ke_1e_2+Ke_2e_3+Ke_3e_1\approx D$, and therefore $(C_3, -)\approx(D\oplus D, -\oplus -)$. $C_4\approx C_4'\otimes C_4''$ where

$$C_4'=K+Ke_2e_3+Ke_2e_4+Ke_3e_4$$
$$C_4''=K+Ke_1+Ke_2e_3e_4+Ke_1e_2e_3e_4.$$

Since $C_4'\approx D$, $C_4''\approx K_2$, we have $C_4\approx D_2$. The rest follows easily, q. e. d.

(6.3) LEMMA. (i) *If* D *is not trivial,*

$$(D, -)\otimes(D, -)\approx(K_4, t)$$
$$(D, -)\otimes(L, -)\approx(L_2, t-).$$

(ii) *If D is trivial,*

$$(D, -)\approx(K_2, j_0),$$

j_0 being the involution $Z\mapsto\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}{}^tZ\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^{-1}$.

PROOF. Let $\{1, i, j, k\}$ be a basis of D with $i^2=j^2=-1$ and $k=ij=-ji$. Let $\{1, i', j', k'\}$ be another copy of the basis. Then, $D\otimes D\approx A_1\otimes A_2$, where

$$A_1=K+KI+KJ+KIJ$$

$$A_2=K+KI'+KJ'+KI'J'$$

$$I=i\otimes 1,\quad J=j\otimes j',\quad I'=1\otimes j',\quad J'=i\otimes k'.$$

Since $A_1\approx A_2\approx K_2$, $D\otimes D\approx K_4$. Moreover, the involution $-\otimes-$ of $D\otimes D$ corresponds to t under the identification

$$I, I'\longleftrightarrow\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix};\quad J, J'\longleftrightarrow\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Next, $D\otimes L\rightarrow L_2$ is given by

$$(x_0+x_1i+x_2j+x_3k)\otimes z\longmapsto z\begin{pmatrix}x_0+x_1\sqrt{-1} & x_2+x_3\sqrt{-1}\\ -x_2+x_3\sqrt{-1} & x_0-x_1\sqrt{-1}\end{pmatrix}.$$

Finally, if D is trivial, $-r^2-s^2=1$ for some $r, s\in K$, and $(D, -)\approx(K_2, j_0)$ under the identification

$$i\longleftrightarrow\begin{pmatrix}-r & s\\ s & r\end{pmatrix},\quad j\longleftrightarrow\begin{pmatrix}-s & -r\\ -r & s\end{pmatrix},$$

q. e. d.

By combining the above lemmas, we can prove

(6.4) PROPOSITION. (i) *If D is not trivial, then $(C_m, -)$ is isomorphic to*

$$\begin{array}{lll}
(K(2^{m/2}), t) & \textit{if}\ m=8c & \textit{for some integer } c\\
(L(2^{(m-1)/2}), t-) & \phantom{\textit{if}\ m}=8c+1 & \\
(D(2^{(m-2)/2}), t-) & \phantom{\textit{if}\ m}=8c+2 & \\
(D(2^{(m-3)/2})\oplus D(2^{(m-3)/2}), t-\oplus t-) & \phantom{\textit{if}\ m}=8c+3 & \\
(D(2^{(m-2)/2}), t-) & \phantom{\textit{if}\ m}=8c+4 & \\
(L(2^{(m-1)/2}), t-) & \phantom{\textit{if}\ m}=8c+5 & \\
(K(2^{m/2}), t) & \phantom{\textit{if}\ m}=8c+6 & \\
(K(2^{(m-1)/2})\oplus K(2^{(m-1)/2}), t\oplus t) & \phantom{\textit{if}\ m}=8c+7. &
\end{array}$$

(ii) *If D is trivial, then $(C_m, -)$ is isomorphic to*

$$\begin{array}{lll} (K(2^{m/2}),\ \lambda_c) & & \textit{if}\ \ m=4c \\ (L(2^{(m-1)/2}),\ \lambda_c -) & \textit{if}\ -1\notin (K^{\times})^2 \left.\vphantom{\begin{array}{l}a\\a\end{array}}\right\} & =4c+1 \\ (K(2^{(m-1)/2})\oplus K(2^{(m-1)/2}),\ \tau\lambda_c) & \textit{if}\ -1\in (K^{\times})^2 & \\ (K(2^{m/2}),\ \lambda_{c+1}) & & =4c+2 \\ (K(2^{(m-1)/2})\oplus K(2^{(m-1)/2}),\ \lambda_{c+1}\oplus\lambda_{c+1}) & & =4c+3. \end{array}$$

In this list, $K(a)$, $L(a)$, $D(a)$ mean K_a, L_a, D_a, respectively, and $\lambda_c=t$ if c is even and $\lambda_c=j_0$ if c is odd, where j_0 is the involution $Z\mapsto J\,{}^tZJ^{-1}$, $J=\begin{pmatrix} 0 & I \\ -I & 0\end{pmatrix}$; also $(X, Y)^{\tau\lambda_c}=(Y^{\lambda_c}, X^{\lambda_c})$.

(6.5) THEOREM. *Let α' be an arbitrary involution of K_m. Then, the Hasse principle for* $\mathrm{Hom}((A, \alpha), (K_n, *))\neq\emptyset$ *holds for the following (A, α):*

(1) $A=D_m=D\otimes K_m$, $\alpha=-\otimes\alpha'$.

(2) $A=K_m\oplus K_m$, $(X, Y)^{\alpha}=(Y^{\alpha'}, X^{\alpha'})$.

(3) $A=L_m=L\otimes K_m$, $\alpha=-\otimes\alpha'$, *if* $-1\notin(K^{\times})^2$ *and* $L=K(\sqrt{-1})$.

In particular, the Hasse principle for $\mathrm{Hom}((C_m, -), (K_n, *))\neq\emptyset$ is true for all $m, n\geqq 1$ and all involutions $*$ of K_n in view of (6.4) proposition. We remark that the theorem is true for $(A, \alpha)=(K_m\oplus K_m, \alpha'\oplus\alpha')$ or $(D_m\oplus D_m, \beta\oplus\beta)$ if it is true for $(A, \alpha)=(K_m, \alpha')$ or (D_m, β), respectively.

PROOF. There exists an involutorial homomorphism of (A, α) into $(K_n, *)$ if and only if K_n has a subalgebra isomorphic to A on which $*$ restricts to an involution equivalent to α, provided that (A, α) is one of the types described in the statement of the theorem. In this case, we shall say that $(K_n, *)$ *contains* (A, α) for the sake of simplicity in this proof. We assume that $((K_v)_n, *)$ contains (A_v, α) for each valuation v of K and show that $(K_n, *)$ contains (A, α) over K.

(1) $(A, \alpha)=(D_m, -\otimes\alpha')$. First assume $D_v\not\sim 1$. Then $n=4mh$ for some integer h and $(K_v)_n\approx(D_v)_m\otimes(D_v)_h$. Since $*$ leaves $(D_v)_m$ invariant, it leaves its centralizer $(D_v)_h$ in $(K_v)_n$ invariant. There exists some $F\in(D_v)_h$ such that $Z^*=F\,{}^t\bar{Z}F^{-1}$ for all $Z\in(D_v)_h$ and ${}^t\bar{F}=\pm F$. If ${}^t\bar{F}=F$, ${}^t\bar{S}FS$ is diagonal for some invertible $S\in(D_v)_h$ and we may assume that F itself is diagonal without loss of generality. In particular, $F\in(K_v)_h$ and $*$ leaves $(K_v)_h$ and therefore the factor $(D_v)_m\otimes D_v$ invariant in the factorization $(K_v)_n\approx(D_v)_m\otimes(D_v)_h$. Thus, $((K_v)_n, *)$ contains $((D_v)_m\otimes D_v, -\otimes\alpha'\otimes -)\approx((K_v)_{4m}, \alpha'\otimes t)$. In this case, $\operatorname{sgn}*=\operatorname{sgn}\alpha'$. If ${}^t\bar{F}=-F$, then, for some invertible $S\in(D_v)_h$, ${}^t\bar{S}FS$ is of the form

$$\left(\begin{array}{cc|c} \begin{array}{c|c} & I_r \\ \hline -I_r & \end{array} & & \\ \hline & & \begin{array}{ccc} u_1 & & \\ & \ddots & \\ & & u_s \end{array} \end{array}\right), \quad \bar{u}_i=-u_i, \quad 2r+s=h.$$

Let $\tilde{F}$ be the matrix in $(K_v)_{4h}\approx D_v\otimes(D_v)_h$ corresponding to $1\otimes F$. Then $\tilde{F}$ is skew-symmetric and $Z^*=\tilde{F}\,{}^tZ\tilde{F}^{-1}$ for all $Z\in(K_v)_{4h}$. In this case, $\mathrm{sgn}\,*=-\mathrm{sgn}\,\alpha'$, $\tilde{F}$ is similar to $\begin{pmatrix} 0 & I_{2h} \\ -I_{2h} & 0 \end{pmatrix}$, and therefore $((K_v)_n, *)$ contains $((K_v)_{4m}, \alpha'\otimes j_0)$, where $Z^{j_0}=J\,{}^tZJ^{-1}$, $J=\begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$. Next, assume $D_v\sim 1$. By (ii) of (6.3) lemma, $((K_v)_n, *)$ contains $((K_v)_{2m}, \alpha'\otimes j_0)$. If $\mathrm{sgn}\,*=\mathrm{sgn}\,\alpha'$, then $((K_v)_n, *)$ must contain $((K_v)_{4m}, \alpha'\otimes j_0\otimes j_0)\approx((K_v)_{4m}, \alpha'\otimes t)$. In all cases, if $\mathrm{sgn}\,*=\mathrm{sgn}\,\alpha'$, $((K_v)_n, *)$ contains $((K_v)_{4m}, \alpha'\otimes t)$, and therefore, by (4.8) theorem, $(K_n, *)$ contains $(K_{4m}, \alpha'\otimes t)$, which contains $(D_m, \alpha'\otimes -)$. If $\mathrm{sgn}\,*=-\mathrm{sgn}\,\alpha'$ and $D\not\sim 1$, then $D_v\not\sim 1$ for some v and therefore $4m$ divides n, and $(K_n, *)$ contains $(K_{4m}, \alpha'\otimes j_0)$, which contains $(D_m, \alpha'\otimes -)$ because $(D, -)\otimes(D, \alpha_1)\approx(K_4, j_0)$ if $z^{\alpha_1}=u\bar{z}u^{-1}$ and $\bar{u}=-u\neq 0$. If $D\sim 1$, (4.8) theorem applies directly.

(2) We first note that the extensions of the involution $(x, y)^\tau=(y, x)$ of $K\oplus K\approx\left\{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix};\ x, y\in K\right\}$ to K_2 are precisely j_0 and j_0' given by

$$Z^{j_0}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}{}^tZ\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}, \quad Z^{j_0'}=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}{}^tZ\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}.$$

We settle the case $m=1$ first. If $((K_v)_n, *)$ contains $(K_v\oplus K_v, \tau)$, we may identify $(x, y)\in K_v\oplus K_v$ with $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}\otimes I_h$, $n=2h$, because the unipotent elements $(1, 0)$, $(0, 1)$ must have the same rank in $(K_v)_n$. $*$ leaves invariant the centralizer $\left\{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix};\ x, y\in K_v\right\}\otimes(K_v)_h$ of $K_v\oplus K_v$. Put $X'=X^\gamma$ if

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\otimes X\right)^*=\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\otimes X\right)^*\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\otimes I_h\right)^*$$

$$=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\otimes X'.$$

Similarly, define δ by

$$\left(\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\otimes X\right)^{*}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\otimes X^{\delta}.$$

Then, γ, δ are antiautomorphisms of $(K_v)_h$ and $\delta=\gamma^{-1}$. There exists some $S\in(K_v)_h$ such that $X^{\gamma}=S^{-1}{}^tXS$ and $X^{\delta}={}^tS^{-1}{}^tX{}^tS$ by Skolem-Noether theorem. By conjugating $(K_v)_n\approx(K_v)_2\otimes(K_v)_h$ by $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\otimes I_h+\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\otimes S$, we may assume that $\left(\begin{pmatrix}x & 0\\ 0 & y\end{pmatrix}\otimes X\right)^{*}=\begin{pmatrix}y & 0\\ 0 & x\end{pmatrix}\otimes{}^tX$ for all x, $y\in K_v$ and $X\in(K_v)_h$. Since $*$ leaves the second factor $(K_v)_h$ invariant, it leaves the first factor $(K_v)_2$ invariant. The remark at the beginning implies that $((K_v)_n, *)$ contains $((K_v)_2, j_0')$ if $\operatorname{sgn}*=1$ and $((K_v)_2, j_0)$ if $\operatorname{sgn}*=-1$. We can show similarly that, for any m, $((K_v)_n, *)$ contains $((K_v)_{2m}, \alpha'\otimes j_0')$ if $\operatorname{sgn}*=\operatorname{sgn}\alpha'$ and $((K_v)_{2m}, \alpha'\otimes j_0)$ if $\operatorname{sgn}*=-\operatorname{sgn}\alpha'$.

(3) As above, it suffices to study the case $m=1$. We first note that the extensions of the involution $\begin{pmatrix}x & y\\ -y & x\end{pmatrix}\mapsto\begin{pmatrix}x & -y\\ y & x\end{pmatrix}$ of $L\approx\left\{\begin{pmatrix}x & y\\ -y & x\end{pmatrix};\ x,\ y\in K\right\}$ to K_2 are precisely (K_2, t) and (K_2, j_0). First assume $-1\notin(K_v^{\times})^2$. Then $L_v=L\otimes K_v=K_v(\sqrt{-1})$ is a field. If $(K_v)_n$ contains L_v, 2 divides n and we may assume that $x+\sqrt{-1}\,y\in L_v$ is identified with $\begin{pmatrix}x & y\\ -y & x\end{pmatrix}\otimes I_h\in(K_v)_2\otimes(K_v)_h\approx(K_v)_n$, $n=2h$. As before, there exists some $F\in(L_v)_h$ such that $Z^*=F{}^t\bar{Z}F^{-1}$ for all $Z\in(L_v)_h$ and ${}^t\bar{F}=\pm F$. If ${}^t\bar{F}=F$, ${}^t\bar{S}FS$ is diagonal for some invertible $S\in(L_v)_h$ and we may assume $F\in(K_v)_h$. Then $*$ leaves the first factor $(K_v)_2$ invariant. If $\operatorname{sgn}*=1$, $((K_v)_n, *)$ contains $((K_v)_2, t)$ and if $\operatorname{sgn}*=-1$, it contains $((K_v)_2, j_0)$. If ${}^t\bar{F}=-F$, we may assume that F is of the form

$$\left(\begin{array}{cc|c}
 & I_r & \\
-I_r & & \\
\hline
 & & \begin{matrix}a_1\sqrt{-1} & & \\ & \ddots & \\ & & a_s\sqrt{-1}\end{matrix}
\end{array}\right),\quad a_i\in K_v,\ 2r+s=h.$$

Put

$$H_1=\left(\begin{array}{cc|c} & I_r & \\ \hline -I_r & & \\ \hline & & 0 \end{array}\right), \quad H_2=\left(\begin{array}{cc|c} & 0 & \\ \hline 0 & & \\ \hline & & \begin{matrix} a_1 & & \\ & \ddots & \\ & & a_s \end{matrix} \end{array}\right),$$

and $\tilde{F}=I_2\otimes H_1+\begin{pmatrix}0&1\\-1&0\end{pmatrix}\otimes H_2$. Then $Z^*=\tilde{F}\,{}^tZ\tilde{F}^{-1}$ for all $Z=\begin{pmatrix}x&y\\-y&x\end{pmatrix}\otimes X$. Therefore $Z^*=T\tilde{F}\,{}^tZ\tilde{F}^{-1}T^{-1}$ for all $Z\in(K_v)_n$ for some T, which commutes with all elements of the form $\begin{pmatrix}x&y\\-y&x\end{pmatrix}\otimes X$ and therefore is in L_v; $T=\begin{pmatrix}x_0&y_0\\-y_0&x_0\end{pmatrix}\otimes I_h$. $T\tilde{F}=\begin{pmatrix}x_0&y_0\\-y_0&x_0\end{pmatrix}\otimes H_1+\begin{pmatrix}-y_0&x_0\\-x_0&-y_0\end{pmatrix}\otimes H_2$. If $\mathrm{sgn}*=1$, $T\tilde{F}$ must be symmetric and hence $x_0=0$. In this case, $T\tilde{F}$ is similar to $I_2\otimes F_0$ for some F_0, i.e., $((K_v)_n, *)$ contains $((K_v)_2, t)$. If $\mathrm{sgn}*=-1$, $T\tilde{F}$ is skew-symmetric and we must have $y_0=0$. In this case, $((K_v)_n, *)$ contains $((K_v)_2, j_0)$. Next, assume $-1\in(K_v^\times)^2$. In this case, $(L_v, -)\approx(K_v\oplus K_v, \tau)$ and the argument in (2) implies that $((K_v)_n, *)$ contains $((K_v)_2, j_0')$ if $\mathrm{sgn}*=1$ and $((K_v)_2, j_0)$ if $\mathrm{sgn}*=-1$. Since -1 is a square in K_v, $\begin{pmatrix}0&1\\1&0\end{pmatrix}\sim\begin{pmatrix}1&0\\0&-1\end{pmatrix}\sim\begin{pmatrix}1&0\\0&1\end{pmatrix}$ and j_0' is equivalent to t. Combining all the cases, we see that $(K_n, *)$ contains (K_2, t) or (K_2, j_0) both of which contain $(L, -)$, and this completes the proof of the theorem.

(6.7) REMARK. A slight modification of the above proof shows that (6.5) theorem remains true if we replace $((-1, -1)_K, -)$, $(K(\sqrt{-1}), -)$ by more general $((a, b)_K, -)$, $(K(\sqrt{a}), -)$.

References

W. Sharlau

[1] Quadratic forms, Queen's papers on pure and applied mathematics, 22, Kingston, Ontario, 1969.

J.W.S. Cassels and A. Fröhlich

[1] Algebraic number theory, Thompson Book Co., Washington D.C., 1967.

T. Ono

[1] Arithmetic of orthogonal groups, J. Math. Soc. Japan, 7 (1955), 79-91.

Takashi ONO
Department of Mathematics
The Johns Hopkins University
Baltimore, Maryland
U.S.A.

Hiroyuki YAMAGUCHI
Department of Mathematics
The Johns Hopkins University
Baltimore, Maryland
U.S.A.

Added in Proof: In a recent letter Dr. A. Wadsworth remarked that one can prove Theorem (3.1) of this paper by induction on the number $n=r(g)/r(f)$ starting with the statement for $n=1$ which is the main theorem of Ono [1].