J. Math. Soc. Japan
Vol. 15, No. 2, 1963

Hasse's principle on quaternionic anti-hermitian forms

By Hiroaki HIJIKATA

(Received June 14, 1962)

In this paper we consider so called Hasse's principle concerning quaternionic anti-hermitian forms over an algebraic number field. Our main result will show that, when the number of variables is different from two, a quaternionic anti-hermitian form over an algebraic number field represents zero if and only if it represents zero in all local fields. We shall also show that two anti-hermitian forms which are equivalent in all local fields are not always equivalent in the original field. Thus Hasse's principle in the first sense is valid while that in the second sense is not. § 1 is preliminaries: the most part of it is devoted to resume the local theory of quaternionic anti-hermitian forms (Tsukamoto [3]). In § 2 we give results affirming Hasse's principle in the first sense and in § 3 a counter-example to Hasse's principle in the second sense.

§ 1. Preliminaries

Let k be a field of characteristic not two, and let D be a quaternion division algebra over k, having a basis: ε_0 (=the unit element of D), $\varepsilon_1, \varepsilon_2, \varepsilon_3$ satisfying $\varepsilon_1^2=c_1$, $\varepsilon_2^2=c_2$ ($c_1, c_2 \in k^*$), $\varepsilon_1\varepsilon_2=-\varepsilon_2\varepsilon_1=\varepsilon_3$. Sometimes we write: $D=(c_1, c_2/k)=(c_1, c_2)$.

D has an involution which fixes only the elements of k ('main involution') which transforms $\xi=\sum_{i=0}^{3}\varepsilon_i a_i$ to $\bar{\xi}=\varepsilon_0 a_0-\sum_{i=1}^{3}\varepsilon_i a_i$. The reduced norm $N(\xi)$ and the reduced trace $Tr(\xi)$ are defined by the formulae: $N(\xi)=\xi\bar{\xi}$, $Tr(\xi)=\xi+\bar{\xi}$. D^- denotes the set of all elements of D whose trace is zero, i.e. $D^-=\{\xi;\ Tr(\xi)=0\}$.

We consider a finite dimensional right vector space V over D. A sesquilinear form $\varphi: V\times V\to D$ is called anti-hermitian if it has the property:

$$\varphi(y,x)=-\overline{\varphi(x,y)} \quad \text{for any } (x,y) \text{ in } V\times V.$$

A mapping H from V to D is called an *anti-hermitian form* on V if the following two conditions are fulfilled:

1) $H(xa)=\bar{a}H(x)a$ for any (a,x) in $D\times V$.
2) There exists an anti-hermitian sesquilinear form φ satisfying

$$H(x+y)-H(x)-H(y)=\varphi(x,y)-\overline{\varphi(x,y)} \quad \text{for any } (x,y) \text{ in } V\times V.$$

We resume here some fundamental results in the local theory from Tsukamoto [3] which we shall use freely in the following.

PROPOSITION 1. *If $H(x)=0$ for all x in V, then $\varphi(x,y)=0$ for all (x,y) in $V\times V$. As a consequence, V has an orthogonal basis.*

PROPOSITION 2. 1) *Witt's theorem is valid, i.e. if W_1, W_2 are subspaces of V and if there exists a linear isomorphism ρ from W_1 onto W_2 such that $H(\rho(x))=H(x)$ for all x in W_1, then ρ can be extended to an automorphism of (V,H) (i.e. a linear isomorphism of V onto itself which preserves $H(x)$).* 2) *We have 'Witt's decomposition' of (V,H) i.e.*

$$V=V_0+\sum_{i=1}^{\nu}\{e_i, e_i'\} \qquad (\textit{orthogonal sum}),$$

where $H(e_i)=H(e_i')=0, \varphi(e_i, e_i')=1$ $(1\leqq i\leqq \nu)$ and V_0 is anisotropic.

This decomposition is *unique* up to an automorphism of (V,H). ν is called the *index* of (V,H), and the isomorphism class of V_0 is called the *type* of (V,H). The *discreminant* $\delta(V)$ of (V,H) is defined by

$$\delta(V)=(-1)^n N(\varphi(x_i, x_j)) \pmod{k^{*2}}$$

where (x_i) is a basis of V. It is easily seen that $\delta(V)$ thus defined is a type invariant and $\delta(V+V')=\delta(V)\delta(V')$.

Now we restrict our field to the local one.

PROPOSITION 3. *Let ξ and η be in D^-. Then ξ is equivalent to η (i.e. there exists an element α of D^* satisfying $\eta=\bar{\alpha}\xi\alpha$), if and only if $N(\xi)\equiv N(\eta)$* (mod k^{*2}). *From this we can deduce that any anti-hermitian space of dimension $\geqq 4$ is isotropic.*

PROPOSITION 4. *In case of the local field, (V,H) is completely determined by $(-1)^{\dim V}$ and $\delta(V)$, which can be prescribed arbitrarily. The list of all the anisotropic anti-hermitian spaces are as follows:*

	dim V	$\delta(V)$
(p-adic case)	0	1
	1	$c\not\equiv 1$ (mod k^{*2})
	2	$c\not\equiv 1$ (mod k^{*2})
	3	1
(the real case)	0	1
	1	$c\not\equiv 1$ (mod k^{*2})

Finally we introduce some notations for the later use. $\mathbf{H}_n^-(D)$ means the set of all non degenerate $n \times n$ anti-hermitian matrices over D, namely $\mathbf{H}_n^-(D) = \{X \in M_n(D)^*\,;\, {}^t\bar{X} = -X\}$.

If, for X, Y in $\mathbf{H}_n^-(D)$, there exists an element Z of $M_n(D)^*$ satisfying ${}^t\bar{Z}XZ = Y$, we say X is *equivalent* to Y, and express as $X \sim Y$.

Moreover if, for X, Y in $\mathbf{H}_n^-(D)$, there exist Z in $M_n(D)^*$ and c in k^* satisfying ${}^t\bar{Z}XZ = cY$, we say X is *multiplicatively equivalent* to Y, and use the notation $X \not\sim Y$. Both relations are clearly equivalence relations and there is a one-to-one correspondence between the elements of $\mathbf{H}_n^-(D)/\sim$ and the isomorphism classes of non-degenerate anti-hermitian spaces over D. In view of Weil's paper [1], $\mathbf{H}_n^-(D)/\not\sim$ corresponds to the isomorphism classes of quaternionic algebraic groups of type D_n.

§ 2. From now on k denotes exclusively an algebraic number field and D denotes a quaternion division algebra over k. $k_\mathfrak{p}$ means the completion of k with respect to a prime $\mathfrak{p}$ (finite or infinite) of k, and $D_\mathfrak{p}$ means the algebra over $k_\mathfrak{p}$ obtained from D by extending the field of coefficients from k to $k_\mathfrak{p}$. We consider everything over k as imbedded naturally in the corresponding thing over $k_\mathfrak{p}$, e. g. $V \subset V_\mathfrak{p}$ and $M_n(D) \subset M_n(D_\mathfrak{p})$, etc.

For the shortness of expressions we say "(H. I) is true for n" if the next proposition is true: "If $U \in \mathbf{H}_n^-(D)$ represents zero in $k_\mathfrak{p}$ (i. e. there exists a non-zero element $x_\mathfrak{p}$ of $V_\mathfrak{p}$ satisfying ${}^t\bar{x}_\mathfrak{p}Ux_\mathfrak{p} = 0$) for all $\mathfrak{p}$, then U represents zero in k (i. e. there exists a non-zero element x of V satisfying ${}^t\bar{x}Ux = 0$)."

In the same way we consider two more propositions: "(H. II) is true for n" means "U and U' in $\mathbf{H}_n^-(D)$ are equivalent by an element of $M_n(D)^*$ if and only if they are equivalent by an element of $M_n(D_\mathfrak{p})^*$ for all $\mathfrak{p}$."

The third proposition we consider is "U and U' in $\mathbf{H}_n^-(D)$ are multiplicatively equivalent by an element of $M_n(D)^*$ if and only if they are multiplicatively equivalent by an element of $M_n(D_\mathfrak{p})^*$ for all $\mathfrak{p}$."

Or symbolically we may express it as

(H. II) $$U \underset{k}{\sim} U' \Leftrightarrow U \underset{k_\mathfrak{p}}{\sim} U' \quad \text{for all } \mathfrak{p}$$

(H. III) $$U \underset{k}{\not\sim} U' \Leftrightarrow U \underset{k_\mathfrak{p}}{\not\sim} U' \quad \text{for all } \mathfrak{p}$$

where $\not\sim$ means the multiplicative equivalence introduced in § 1; (H. III) is nothing but the Hasse's principle for quaternionic algebraic groups of type D_n over k.

LEMMA 1. (H. III) *is true for* $n = 1$.

PROOF. Assume $u, v \in D^*$ and $u \not\sim v$ for all $\mathfrak{p}$, i. e. there exist for each $\mathfrak{p}$ $x_\mathfrak{p} \in D_\mathfrak{p}^*$ and $c_\mathfrak{p} \in k_\mathfrak{p}^*$ satisfying $\bar{x}_\mathfrak{p}ux_\mathfrak{p} = c_\mathfrak{p}v$. Then we have clearly $N(u)/N(v) \in k_\mathfrak{p}^{*2}$ for any $\mathfrak{p}$, and consequently $N(u)/N(v) \in k^{*2}$. So we can find c in k^*

with the property: $N(u)=N(cv)$, and u can be transformed to cv by an inner-automorphism of D, i.e. there exists $y\in D^*$ such that $y^{-1}uy=cv$, whence we get $\bar{y}uy=N(y)cv$. q.e.d.

LEMMA 2. (H. III) *is true for* $n=3$.

PROOF. We make use of the well-known isogeny between SO(6) and SL(4) over the universal domain Ω. Considering projective groups, we get the isomorphism

$$\mathrm{PO}(6)\cong\mathrm{PL}(4). \tag{1}$$

For a given element U of $\mathbf{H}_3^-(D)$, we construct an involutive algebra (A,α_U) with the underlying algebra $A=M_3(D)$ and the involution α_U defined by

$$\alpha_U: X\to U^{-1}\,{}^t\bar{X}U \qquad \text{for any } X \text{ in } A.$$

Let $G(U)$ be the connected component of the algebraic group consisting of all automorphisms of (A,α_U). Let U and U' be in $\mathbf{H}_n^-(D)$, then $G(U)$ is isomorphic to $G(U')$ as an algebraic group over k if and only if U is multiplicatively equivalent to U' over k:

$$G(U)\underset{k}{\cong}G(U')\Leftrightarrow U\underset{k}{\sim}U'.$$

On the other hand, from the isomorphism (1) $G(U)$ is isomorphic over k to one and only one (up to an isomorphism over k) group of type PL(4); we denote this group (of type PL(4) defined over k) by $G^*(U)$:

$$G(U)\cong G^*(U) \quad \text{over } k.$$

By the result of Weil [1], $G^*(U)$ is realized as the connected component of the automorphism group of an involutive algebra (B_U,β_U) which is isomorphic over the universal domain to $M_4(\Omega)\oplus M_4(\Omega)$ with the involution; $(x,y)\to({}^ty,{}^tx)$. It is easily shown that such an algebra (B_U,β_U) must be one of the following types:

1) $B_U=M_4(k)\oplus M_4(k)$ $\qquad\beta_U:(x,y)\to({}^ty,{}^tx)$

2) $B_U=M_2(D')\oplus M_2(D')$ $\qquad\beta_U:(x,y)\to({}^t\bar{y},{}^t\bar{x})$

where D' denotes a quaternion division algebra defined over k and $x\to\bar{x}$ denotes the main involution of D'.

3) $B_U=M_4(K)$ $\qquad\beta_U:x\to{}^t\bar{x}$

where K denotes a quadratic extension of k and $x\to\bar{x}$ denotes the conjugation of K over k.

4) $B_U=M_2(\mathfrak{D})$ $\qquad\beta_U:x\to{}^tx^\iota$

where $\mathfrak{D}$ denotes a quaternion division algebra over a quadratic extension K of k with the involution ι which does not fix the elements of K.

5) $$B_U = \mathfrak{D}' \qquad \beta_U : x \to x^\iota$$

where $\mathfrak{D}'$ denotes a division algebra of degree 4 over a quadratic extension K of k, with the involution ι which does not fix the elments of K.

Let (B, β) and (B', β) be two involutive algebras, isomorphic to one of the above types, and assume that they are isomorphic (as an involutive algebra over $k_\mathfrak{p}$) for all $\mathfrak{p}$, then we can conclude that they are isomorphic over k as an involutive algebra over k. For $(B, \beta) \cong (B', \beta')$ over $k_\mathfrak{p}$ means firstly $B \otimes k_\mathfrak{p} \cong B' \otimes k_\mathfrak{p}$ for all $\mathfrak{p}$, and this means by the Hasse's theorem in associative algebras that $B \cong B'$ over k. In case of 1), 2) there is nothing more to say; in case of 3), 4) and 5) the problem is reduced to the (H. III) type theorem in hermitian forms over involutive algebras which was proved by Landherr in ([2], p. 229, Satz 4).

Now let U and U' be in $\mathbf{H}_n^-(D)$, and suppose that U is multiplicatively equivalent to U' over $k_\mathfrak{p}$ for all $\mathfrak{p}$. Then $G(U)$ is isomorphic to $G(U')$ over $k_\mathfrak{p}$ for all $\mathfrak{p}$, and this means $G^*(U)$ is isomorphic to $G^*(U')$ over $k_\mathfrak{p}$ for all $\mathfrak{p}$.

We realize $G^*(U)$ and $G^*(U')$ as the automorphism groups of the involutive algebras (B_U, β_U) and $(B_{U'}, \beta_{U'})$, respectively, both algebras being chosen from the above list; Then these involutive algebras must be isomorphic over $k_\mathfrak{p}$ for all $\mathfrak{p}$, so that by the above argument they are isomorphic over k and consequently $G^*(U)$ is isomorphic to $G^*(U')$ over k. Finally this means that $G(U)$ is isomorphic to $G(U')$ over k and we have thus shown that U is multiplicatively equivalent to U' over k. q. e. d.

LEMMA 3. (H. I) *is true for* $n = 3$.

PROOF. Let U be in $\mathbf{H}_n^-(D)$ and represents zero in all $k_\mathfrak{p}$, Consider Witt's decomposition (proposition 2) in each $k_\mathfrak{p}$:

$$U \underset{k_\mathfrak{p}}{\sim} \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & \xi_\mathfrak{p} \end{pmatrix} \qquad \xi_\mathfrak{p} \in D_\mathfrak{p}^-, \text{ where } \xi_\mathfrak{p} \text{ is determined by } \delta(U) \equiv N(\xi_\mathfrak{p}) \pmod{k_\mathfrak{p}^{*2}}.$$

As $\delta(U)$ is a norm of the pure-quaternion in $D_\mathfrak{p}^-$ for each $\mathfrak{p}$, there exists ξ in D^- such that $N(\xi) = \delta(U)$.

Then ξ satisfies the equation $N(\xi) \equiv N(\xi_\mathfrak{p}) \pmod{k_\mathfrak{p}^{*2}}$ for each $\mathfrak{p}$, so by the argument in the proof of Lemma 1 we can find, for each $\mathfrak{p}$, an element $r_\mathfrak{p}$ of $k_\mathfrak{p}^*$ such that $r_\mathfrak{p}\xi \sim \xi_\mathfrak{p}$. We get

$$U \underset{k_\mathfrak{p}}{\sim} \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & r_\mathfrak{p}\xi \end{pmatrix} \underset{k_\mathfrak{p}}{\sim} r_\mathfrak{p} \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & \xi \end{pmatrix} \qquad \text{for every } \mathfrak{p}.$$

We can conclude from Lemma 2 that U is multiplicatively equivalent to

$\begin{pmatrix} 0 & 1 & 0 \\ -0 & 0 & 0 \\ 0 & 0 & \xi \end{pmatrix}$ over k, i.e. there exists r in k^* such that U is equivalent to $r\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & \xi \end{pmatrix}$. This shows that U represents zero in k. q.e.d.

LEMMA 4. *Let* $A=M_n(D)$, $U\in \mathbf{H}_n^-(D)$, $\alpha: X\to U^{-1}\,{}^t\bar{X}U$ $(X\in A)$, $D=(p, q/k)$, $K\supset k(\sqrt{q})$, $B=M_{2n}(K)$, $\beta: Y\to(\Phi(U)\mathbf{J})^{-1}\,{}^tY(\Phi(U)\mathbf{J})$.

Then $(A, \alpha)\otimes K$ *is isomorphic to* $(B, \beta)\otimes K$ *over* K.

Where $\Phi: M_n(D)\to M_{2n}(K)$ *is defined by* $\Phi(X)=(\varphi(x_{ij}))$ *and* $\varphi: D\to M_2(K)$ *is an injection defined by* $\varphi(\gamma)=\begin{pmatrix} a+c\sqrt{q} & p(b-d\sqrt{q}) \\ b+d\sqrt{q} & a-c\sqrt{q} \end{pmatrix}$ *for* $\gamma=a+b\varepsilon_1+c\varepsilon_2+d\varepsilon_3\in D$ *and* $\mathbf{J}=\mathrm{diag}(J, J, \cdots, J)$, $J=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

As a consequence, U represents zero (as an anti-hermitian form) in K, if and only if $\Phi(U)\mathbf{J}$ (as a quadratic form) represents zero in K.

In particular, $\gamma\in D^-$ represents zero in K if and only if $\varphi(\gamma)J$ represents zero in K. If K is the real field the last condition is equivalent that $N(\gamma)=\det(\varphi(\gamma)J)<0$ in K.

The proof is straightforward and is omitted.

Now we will give some supplementary definitions and notations.

DEFINITION 1. Let f be a definite quadratic form over the real field. We put $\mathrm{sgn}(f)=1$ if f is positive definite, and $\mathrm{sgn}(f)=-1$ if f is negative definite.

Let $\mathfrak{p}_i$ $(1\leqq i\leqq s)$ be all the finite primes of k at which D does not split, $\mathfrak{p}_{\infty,j}$ $(1\leqq j\leqq t)$ all the real primes of k at which D splits, $\mathfrak{p}_{\infty,j}$ $(t<j\leqq u)$ all the real primes of k at which D does not split. We use these notations in the next definition and Lemmas 5, 6, 7 and 8.

DEFINITION 2. Let $\xi\in D^-$, and $N(\xi)\equiv 1 \pmod{\mathfrak{p}_{\infty,j}}$, $\xi^{(j)}$ the image of ξ in $D\otimes k_{\mathfrak{p}_{\infty,j}}$. We fix an injection $\varphi_j: D\otimes k_{\mathfrak{p}_{\infty,j}}\to M_2(k_{\mathfrak{p}_{\infty,j}})$ once for all, and define as $\mathrm{sgn}_j(\xi)=\mathrm{sgn}(\varphi_j(\xi^{(j)})J)$ (notations of Lemma 4 and Definition 1).

By this definition and Lemma 4, we get

LEMMA 5. $\mathrm{diag}(\xi_1, \xi_2, \cdots, \xi_n)\in \mathbf{H}_n^-(D)$ *represents zero in* $k_{\mathfrak{p}_{\infty,j}}$ *if and only if one of the following two conditions be satisfied:*

1) *There exists* ξ_l, *such that* $N(\xi_l)\equiv -1 \pmod{\mathfrak{p}_{\infty,j}}$.

2) $N(\xi_l)\equiv 1 \pmod{\mathfrak{p}_{\infty,j}}$ *for all* l, *and there exist* ξ_l, ξ_m $(l\neq m)$ *such that* $\mathrm{sgn}_j(\xi_l)\neq \mathrm{sgn}_j(\xi_m)$.

LEMMA 6. *Let* ξ_l $(l=1, 2, 3)\in D^-$, *and* $N(\xi_l)\equiv 1 \pmod{\mathfrak{p}_{\infty,j}}$ *for all* l *if and only if* $j\leqq t_0\leqq t$. *Then* $\mathrm{diag}(\xi_1, \xi_2, \xi_3)\in \mathbf{H}_3^-(D)$ *represents zero in* k *if and only if*

the following two conditions are satisfied:

1) $\delta(\mathrm{diag}(\xi_1, \xi_2, \xi_3)) = -N(\xi_1)N(\xi_2)N(\xi_3) \not\equiv 1 \pmod{k_{\mathfrak{p}_i}^{*2}}$, $1 \leqq i \leqq s$.

2) *For each* $j \leqq t_0$, *there exist* ξ_l *and* ξ_m $(l \neq m)$ *such that*

$$\mathrm{sgn}_j(\xi_l) \neq \mathrm{sgn}_j(\xi_m).$$

PROOF. By Lemma 3, it is sufficient to show that $\mathrm{diag}(\xi_1, \xi_2, \xi_3)$ represents zero in all $k_{\mathfrak{p}}$. As any quadratic form of 6 variables over a $\mathfrak{p}$-adic field represents zero, this is a direct consequense of Proposition 4, Lemmas 4 and 5.

LEMMA 7. $U \in \mathbf{H}_4^-(D)$ *represents zero in* k *if and only if* U *represents zero in* $k_{\mathfrak{p}_{\infty,j}}$ $(1 \leqq j \leqq t)$.

PROOF. "Only if" part is clear, we will show "if" part. Let U be diagonalized as

$$U = \begin{pmatrix} \xi_1 & & & 0 \\ & \xi_2 & & \\ & & \xi_3 & \\ 0 & & & \xi_4 \end{pmatrix} = \mathrm{diag}(\xi_1, \xi_2, \xi_3, \xi_4),\ \xi_l \in D^-\quad (l = 1, 2, 3, 4).$$

As U represents zero in all $k_{\mathfrak{p}}$, we can find for each $\mathfrak{p}$, $\eta^{(\mathfrak{p})}$ and $x_l^{(\mathfrak{p})}$ $(l = 1, 2, 3, 4)$ such that

$$\bar{x}_1^{(\mathfrak{p})}\xi_1 x_1^{(\mathfrak{p})} + \bar{x}_2^{(\mathfrak{p})}\xi_2 x_2^{(\mathfrak{p})} = \bar{\eta}^{(\mathfrak{p})} = -\bar{x}_3^{(\mathfrak{p})}\xi_3 x_3^{(\mathfrak{p})} - \bar{x}_4^{(\mathfrak{p})}\xi_4 x_4^{(\mathfrak{p})}. \tag{2}$$

Where we can assume without loss of generality that $\eta^{(\mathfrak{p})} \neq 0$ for any $\mathfrak{p}$, because Witt's decomposition shows that a zero-form represents any element of the pure quaternion. Moreover we may assume that $N(\eta^{(\mathfrak{p}_{\infty,j})}) \equiv 1 \pmod{\mathfrak{p}_{\infty,j}}$ if and only if $1 \leqq j \leqq t_1 \leqq t$. Consider the set of equations:

$$\begin{cases} y \equiv N(\eta^{(\mathfrak{p}_i)}) \pmod{k_{\mathfrak{p}_i}^{*2}},\ 1 \leqq i \leqq s \\ y \equiv N(\eta^{(\mathfrak{p}_{\infty,j})}) \pmod{\mathfrak{p}_{\infty,j}},\ 1 \leqq j \leqq u. \end{cases} \tag{3}$$

By the approximation theorem, (3) has a solution y_1 in k. By Hasse's theorem on quadratic forms, there exists $\eta_1 \in D^-$, such that $N(\eta_1) = y_1$.

Let c_1 be a solution of

$$c \equiv \mathrm{sgn}(\eta^{(\mathfrak{p}_{\infty,j})})\,\mathrm{sgn}(\eta_1) \pmod{\mathfrak{p}_{\infty,j}},\ 1 \leqq j \leqq t_1. \tag{4}$$

Then $\eta = c_1\eta_1$ satisfies

$$\begin{cases} N(\eta) \equiv N(\eta^{(\mathfrak{p}_i)}) \pmod{k_{\mathfrak{p}_i}^{*2}}, & 1 \leqq i \leqq s \\ N(\eta) \equiv N(\eta^{(\mathfrak{p}_{\infty,j})}) \pmod{\mathfrak{p}_{\infty,j}}, & 1 \leqq j \leqq u \\ \mathrm{sgn}_j(\eta) = \mathrm{sgn}(\eta^{(\mathfrak{p}_{\infty,j})}) & 1 \leqq j \leqq t. \end{cases}$$

So it can readily be seen that $\mathrm{diag}(\xi_1, \xi_2, -\eta)$ and $\mathrm{diag}(-\xi_3, -\xi_4, -\eta)$ satisfy the condition 1) and 2) of Lemma 6, and both of them represent zero in k. q. e. d.

LEMMA 8. $U \in \mathbf{H}_n^-(D)$ $(n \geqq 4)$ *represents zero in* k *if and only if* U *represents*

zero in $k_{\mathfrak{p}_{\infty,j}}$ $(1 \leqq j \leqq t)$.

PROOF. Let $U = \mathrm{diag}(\xi_1, \xi_2, \cdots, \xi_n)$, $\xi_l \in D^-$ $(l = 1, 2, \cdots, n)$. Take, for each $\mathfrak{p}$ non-zero $\eta^{(\mathfrak{p})}$ such that

$$\bar{x}_1^{(\mathfrak{p})}\xi_1 x_1^{(\mathfrak{p})} + \bar{x}_2^{(\mathfrak{p})}\xi_2 x_2^{(\mathfrak{p})} = \eta^{(\mathfrak{p})} = -\bar{x}_3^{(\mathfrak{p})}\xi_3 x_3^{(\mathfrak{p})} - \cdots - x_n^{(\mathfrak{p})}\xi_n \bar{x}_n^{(\mathfrak{p})}.$$

Let η_1, c_1 be a solution of (3), (4) of Lemma 7 respectively, and $\eta = c_1\eta_1$.

Then by Lemma 5, 6, 7, and the mathematical induction on the numbers of variables n, $\mathrm{diag}(\xi_1, \xi_2, -\eta)$ and $\mathrm{diag}(-\xi_3, -\xi_4, \cdots, -\xi_n, -\eta)$ represent zero in k.

Now, (H. I) being trivially true for $n = 1$, we get by Lemmas 3 and 8.

THEOREM (H. I) *is true for* $n \neq 2$.

i.e. A quaternionic anti-hermitian form in $(n \neq 2)$ *variables over an algebraic number field represents zero if and only if it represents zero in all local fields.*

§ 3. Let D be a quaternion division algebra over a perfect field k. Let $A = M_2(D)$ and $U \in \mathbf{H}_2^-(D)$, $\alpha : X \to U^{-1}\,{}^t\bar{X}U$ $(X \in A)$ is an involution of A. Then $G(U) = \mathrm{Aut}_0(A, \alpha)$ is an algebraic group defined over k, and isomorphic to $\mathrm{PO}(4) = \mathrm{SO}(4)/\text{center}$ over the universal domain Ω. On the other hand, $\mathrm{SO}(4)$ is isogenious to $\mathrm{SL}(2) \times \mathrm{SL}(2)$ over Ω. Going to a projective group, we get:

$$\mathrm{PO}(4) \cong \mathrm{PL}(2) \times \mathrm{PL}(2) \quad \text{over } \Omega.$$

So $G(U)$ must be isomorphic to one and only one of the k-forms of $\mathrm{PL}(2) \times \mathrm{PL}(2)$. The complete list of the k-forms of $\mathrm{PL}(2) \times \mathrm{PL}(2)$ is as follows:

1) $\mathrm{PL}(2, k) \times \mathrm{PL}(2, k)$
2) $\mathrm{PL}(2, k) \times \mathrm{PL}(1, D')$ where D' is a quaternion division algebra over k.
3) $\mathrm{PL}(1, D') \times \mathrm{PL}(1, D'')$ where D', D'' is a quaternion division algebra over k.
4) $\mathrm{PL}(2, K)$ where K is a quadratic extension of k.
5) $\mathrm{PL}(1, \mathfrak{D})$ where $\mathfrak{D}$ is a quaternion division algebra over a quadratic extension K of k.

In the classical theory, it is known that any group of type 1) or 4) of the above list is a k-form of some orthogonal group defined over k, so our group $G(U)$ can not be isomorphic to 1) or 4). If the index $\nu(U)$ of U is not zero, then an easy calculation shows that $G(U)$ is isomorphic to a group of type 2) with $D' = D$ over k. If the discreminant $\delta(U)$ of U is not 1 (mod k^{*2}), then $\nu(U)$ is necessarily zero and it can be shown that $G(U)$ is isomorphic to a group of type 5) over k. The last case to consider is that $\delta(U) \equiv 1$ (mod k^{*2}) and $\nu(U) = 0$.

This corresponds to the type 3) of the above list, where some singularity occurs and Hasse's principle fails. Now we will determine explicitly the isomorphism over k of this case.

Let $\delta(U) \equiv 1$ (mod k^{*2}). Taking suitable basis $1, \xi, \eta, \zeta$, we may assume

$\xi^2=p, \eta^2=q, \xi\eta=-\eta\xi=\zeta$ $(p, q\in k^*)$, $D=(p, q/k)$ and $U=\mathrm{diag}(\xi, r\xi)\, r\in k^*$.

PROPOSITION, *If* $D=(p, q)$ *and* $U=\mathrm{diag}(\xi, r\xi)\in \mathbf{H}_n^-(D)$ *with* $\xi^2=p$, *then* $G(U)$ *is isomorphic to* $G=\mathrm{PL}(1, D_1)\times \mathrm{PL}(1, D_2)$ *over* k, *where* $D_1=(p, r/k)$ *and* $D_2=(p, rq/k)$.

PROOF. Let $K=k(\sqrt{r}\,)$, and

$$G=\mathrm{PL}(1, D_1)\times \mathrm{PL}(1, D_2)$$

$$G'=\mathrm{PL}(2, K)\times \mathrm{PL}(1, D)$$

$$G''=\mathrm{Aut}_0(M_2(D), \alpha_1) \qquad \alpha_1: X\to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} {}^t\bar{X} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Each group is defined over K and isomorphic to $\mathrm{PL}(2)\times \mathrm{PL}(2)$ over Ω.

Now we fix a basis of quaternions as follows:

the basis of $D=(p, q)$: $1, \xi, \eta$ and ζ

the basis of $D_1=(p, r)$: $1, \xi, \eta'=(\sqrt{r}/\sqrt{q}\,)\eta$ and $\zeta'=(\sqrt{r}/\sqrt{q}\,)\zeta$

the basis of $D_2=(p, rq)$: $1, \xi, \eta''=\sqrt{r}\,\eta$ and $\zeta''=\sqrt{r}\,\zeta$.

Let z be a generic point of G over K, then its affine representative $z=(x, y)$ is written as $x=x_0+x_1\xi+x_2\eta'+x_3\zeta', y=y_0+y_1\xi+y_2\eta''+y_3\zeta''$. Let z' be a generic point of G' over K with affine representative

$$z'=(x', y') \quad x'=(x'_{ij}) \quad y'=y'_0+y'_1\xi+y'_2\eta+y'_3\zeta.$$

Define the mapping from G to G' by $\psi(z)=\psi_1(x)\times\psi_2(y)$

$$\psi_1(x)=\begin{pmatrix} x_0+x_1\sqrt{r} & x_2+x_3\sqrt{r} \\ p(x_2-x_3\sqrt{r}\,) & x_0-x_1\sqrt{r} \end{pmatrix}$$

$$\psi_2(y)=y_0+y_1\xi+y_2\sqrt{r}\,\eta+y_3\sqrt{r}\,\zeta.$$

then ψ is a rational isomorphism defined over K,

Define $\pi: G'\to G''$ by $\pi(z')=i_1(x')i_2(y')$, where i_1 and i_2 denote respectively the canonical injections

$$i_1: \quad M_2(K)\to M_2(D)\otimes K,$$

$$i_2: \quad D\to M_2(D)\otimes K,$$

then π is a rational isomorphism defined over K.

Define φ: $G''\to G(U)$ by $\varphi(z'')=Si(z'')S^{-1}$, where $S=\begin{pmatrix} 1 & \xi/p \\ 1/\sqrt{r} & -1/\sqrt{r}\,\xi/p \end{pmatrix}$ and i denotes the identification of the underlying algebra of $(M_2(D), \alpha_1)$ and that of $(M_2(D), \alpha)$, then φ is also a rational isomorphism defined over K.

The composite $f=\varphi\circ\pi\circ\psi$ gives a rational isomorphism from G to $G(U)$ defined over K. We will show that f is actually defined over k, then the proposition is proved. Let σ be a generator of the Galois group of K over k. It is sufficient to show that $f^\sigma(z)=f(z)$. After trivial identifications we may

write $f(z)=\varphi(\psi_1(x)\psi_2(y))=S(\psi_1(x)\psi_2(y))S^{-1}$ and $f^\sigma(z)=S^\sigma(\psi_1^\sigma(x)\psi_2^\sigma(y))S^{-\sigma}$. Direct calculation shows:

$$\psi_1^\sigma(x)=\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}\psi_1(x)\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}^{-1} \qquad \psi_2^\sigma(y)=\xi\psi_2(y)\xi^{-1}$$

$$S^\sigma=S\xi^{-1}\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}^{-1}$$

but ξ commutes with $\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}$ and $\psi_1(x)$. Therefore we get $f^\sigma(z)=f(z)$.

q. e. d.

From this proposition we can easily construct the example in which (H. I) (and consequently (H. II) and (H. III)) is not valid.

COUNTER-EXAMPLE. Let $k=Q$ (rational number field), $p=-5$, $q=-13$ and $r=-3$, $U=\mathrm{diag}(\xi, r\xi)$, $U_0=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$. Then the above proposition shows

$$G(U)\cong \mathrm{PL}(1,(p,r))\times \mathrm{PL}(1,(p,rq)) \text{ over } Q$$

$$G(U_0)\cong \mathrm{PL}(2,Q)\times \mathrm{PL}(1,(p,q)) \text{ over } Q\,.$$

Now we calculate the Hilbert's symbol for p, q, r and rq:

$\mathfrak{p}$	$\left(\frac{p,q}{\mathfrak{p}}\right)$	$\left(\frac{p,r}{\mathfrak{p}}\right)$	$\left(\frac{p,rq}{\mathfrak{p}}\right)$
5	−1	−1	1
13	−1	1	−1
∞	−1	−1	1
2	−1	1	−1
3	1	1	1
other prime	1	1	1

The above table and the proposition in this § show that $G(U)$ *is isomorphic to* $G(U_0)$ *in all* $Q_\mathfrak{p}$, *but* $G(U)$ *is clearly not isomorphic to* $G(U_0)$ *over* Q, i. e. (H. III) is not valid for U and U_0. In this case corresponding group $G(U)$ or $G(U_0)$ is not simple over Q, so the failure of Hasse's principle is rather natural. But this example gives a simple group in which Hasse's principle fails. For instance, let $U_0=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ $U=\begin{pmatrix}\xi & 0\\ 0 & r\xi\end{pmatrix}$ and

$$U_1=\mathrm{diag}(U, U_0, \cdots, U_0)\in \mathbf{H}_{2n}^-(D)$$

$$U_1'=\mathrm{diag}(U_0, U_0, \cdots, U_0)\in \mathbf{H}_{2n}^-(D) \qquad n\geqq 2\,.$$

Then $G(U_1)$ and $G(U_1')$ are isomorphic to $\mathrm{PO}(4n)$ over Ω, and simple over Ω. U_1 is multiplicatively equivalent to U_1' in all $Q_\mathfrak{p}$ because $U\sim U_0$ for all $\mathfrak{p}$,

say $U\sim r_{\mathfrak{p}}U_0$, then $U_0\sim r_{\mathfrak{p}}U_0$ and $U_1\sim r_{\mathfrak{p}}U_1'$ (i.e. $G(U_1)$ is isomorphic to $G(U_1')$ over $Q_{\mathfrak{p}}$) but U_1 is not multiplicatively equivalent to U_1' (i.e. $G(U_1)$ is not isomorphic to $G(U_1')$ over Q).

Now we sum up the results which are easily seen from the above example.

PROPOSITION. I) (H. I) *is not valid for* $n=2$.

II) (H. II) *is not valid any* n.

III) (H. III) *is not valid for even* n.

(H. III) is true for $n=1$ and 3. It is likely to be true for any odd n, but we have no proof.

PROOF. I) $\mathrm{diag}(\xi, r\xi)$ in the above example gives a counter-example.

II) $\xi, r\xi\in\mathbf{H}_1^-(D)$ gives a counter-example for $n=1$. For general n, we consider any $U'\in\mathbf{H}_{n-1}^-(D)$ and let $U_1=\xi\oplus U'$ (direct sum) and $U_1'=r\xi\oplus U'$ (direct sum). Then $U_1\sim U_1'$ in all $Q_{\mathfrak{p}}$, but U_1 is not equivalent to U_1' over Q.

III) We have already given a counter-example for this. q.e.d.

Bibliography

[1] A. Weil, Algebras with involution and classical groups, J. Indian Math. Soc., (1961), 589-623.

[2] W. Landherr, Liesche Ringe vom Typus A über einem algebraischen Zahlkörper (Die lineare Gruppe) und hermitesche Formen über einem Schiefkörper, Abh. Math. Sem. Hansische Univ., 12 (1938), 200-241.

[3] T. Tsukamoto, On the local theory of quaternionic anti-hermitian forms, J. Math. Soc. Japan, 13 (1961), 387-400.