J. Math. Kyoto Univ. (JMKYAZ)
16-2 (1976) 325-350

The conjugacy classes in the unitary, symplectic and orthogonal groups over an algebraic number field

By

Teruaki ASAI

(Communicated by Prof. Nagata, July 7, 1975)

Introduction. Let k be a commutative field and σ be its involution, i.e. an automorphism of k such that $\sigma^2 = \text{identity}$. Let V be a symmetric bilinear (resp. symplectic; resp. Hermitian) space over k with respect to σ. Let $U(V)$ denote the group of all isometries of V. We shall concern with the conjugacy classes of the elements of $U(V)$. The problem has been studied by many mathematicians, and there are known substantial amount of results. First of all, there is a canonical injection from the set of all conjugacy classes of $U(V_0)$ for a symmetric bilinear (resp. symplectic; resp. Hermitian) space V_0 into the set of the equivalence classes of the pairs (V, x) consisting of symmetric bilinear (resp. symplectic; resp. Hermitian) spaces V and its isometries x (c.f. G. E. Wall [9] and J. Milnor [4]). The equivalence problem of the pairs (V, x) was solved by J. Williamson [10] under the assumption that the base field is perfect and of characteristic $\neq 2$, and then solved by G. E. Wall [9] under the weaker assumption called "trace condition". Then, to determine the conjugacy classes of $U(V)$ we must determine the image of the above canonical injection. The problem to determine this image can be reduced to the form of our Problem 3.3, § 3 (when k is perfect). When the base field k is finite, the latter problem is solved by G. E. Wall [9], in fact he gave an explicit description of all the conjugacy classes over finite fields. When k is a local field, J. Milnor [4] gave an answer to this problem. (See our Lemma 3.4.) Utilizing his results we get a similar answer when k is an algebraic number field (Theorem 3.6 and 3.7) and give a complete set of local invariants to each conjugacy classes. Since, it turns out that local invariants correspond to the local conjugacy classes, we can describe our results as the Hasse principle for the conjugacy classes (Theorem 4.7, 4.8 and 4.9). Namely the following map ι is injective and we can effectively characterize the image of ι in terms of local invariants.

$$\iota; \left\{\begin{matrix}\text{the conjugacy classes}\\ \text{in } U(V)\end{matrix}\right\} \longrightarrow \prod_v \left\{\begin{matrix}\text{the conjugacy classes}\\ \text{in } U(V_v)\end{matrix}\right\}$$

where v runs all the prime spots on $k_0=\{x\in k|{}^{\sigma}x=x\}$.

To our best knowledge, the injectiveness of the above ι was remarked for the first time by M. Eichler [0] (for the special case of regular conjugacy classes in the anisotropic orthogonal group $0(V)$), and its general validity was remarked by H. Hijikata [1].

In the first two sections, we shall sum up the known results, mostly from [4] and [7], in a form convenient for our later use.

This paper is preparatory to my subsequent paper to get the class number formula of positive definite quadratic forms by means of Selberg Trace Formula.

Finally I express my hearty gratitude to Professor H. Hijikata for his kind guidance and encouragement.

§1. The conjugacy classes of the unitary, symplectic and orthogonal groups

1.1. First we give some definitions. Let A be a commutative ring with 1. Let α be an involution of A (i.e. α is an automorphism of A and $\alpha^2=\text{identity}$). α may be identity. Let M be a finitely generated A-module. Let $\varepsilon=1$ or -1. An ε-Hermitian form on M over A with respect to α is a mapping F: $M\times M\rightarrow A$ satisfying

(i) $F(au+bv, w)=a F(u, w)+b F(v, w)$,

(ii) $F(u, v) = {}^{\alpha}F(v, u)$,

for any $u, v, w \in M$ and $a, b \in A$. We call the pair (M, F) an ε-Hermitian Module over A (with respect to α). If α = identity and $\varepsilon = 1$, we call F a symmetric bilinear form and (M, F) a symmetric bilinear module over A. If M is a free A-module, we call (M, F) an ε-Hermitian space over A. We often indicate ε-Hermitian spaces by M, $N, \ldots$ instead of $(M, F), (N, G), \ldots$ if there is no confusion.

Let (M, F) be an ε-Hermitian space over A. And let $\{e_1, \ldots, e_n\}$ be a basis of M over A. We say (M, F) is non-degenerate if the (n, n)-matrix $(F(e_i, e_j))$ is invertible. We often write $(M, F) = (F(e_i, e_j))$ for brevity.

Assume $A = \bigoplus_{i=1}^{r} A_i$ and ${}^{\alpha}A_i = A_i$. Let δ be an element of A such that $\delta = (\varepsilon_1, \ldots, \varepsilon_r) \in A_1 \oplus \cdots \oplus A_r$ with $\varepsilon_i = 1$ or $-1 \in A_i$. Even if we do not assume $\delta = 1$ or -1, we can similarly define δ-Hermitian forms over A as above. A δ-Hermitian module over $A = \bigoplus_{i=1}^{r} A_i$ is always a direct sum of ε_i-Hermitian modules over A_i.

1.2. Let k be a (commutative) field and σ be its involution. (σ may be identity.) We put $\varepsilon = 1$ or -1. Let (V, f) be an ε-Hermitian space over k with respect to σ and $U(V, f)$ denote the group of all isometries of (V, f).

For a monic polynomial $p(X) = X^n + c_1 X^{n-1} + \cdots + c_n$ with $c_n \neq 0$, we define its "dual" polynomial $p^*(X)$ by

$$p^*(X) = ({}^{\sigma}c_n)^{-1} X^n ({}^{\sigma}p)(X^{-1})$$

where $({}^{\sigma}p)(X) = X^n + {}^{\sigma}c_1 X^{n-1} + \cdots + {}^{\sigma}c_n$.

Let $m(X)$ be the minimal polynomial of $x \in U(V, f)$. For any polynomial $h(X) \in k[X]$, we have

$$f(h(x)u, v) = f(u, ({}^{\sigma}h)(x^{-1})v) \qquad \text{for any} \quad u, v \in v.$$

Thus we have

Lemma 1.1. (1) $m^*(X) = m(X)$.

(2) *Put $R = k[X]/m(X)$. Then V is an R-module by the mapping*

$(X\mapsto x)$. *There is an involution* α *of* R *such that* ${}^{\alpha}X=X^{-1}$ *and* $\alpha|_k=\sigma$. *And* $f(au, v)=f(u, {}^{\alpha}av)$ *for any* $u, v\in V$ *and* $a\in R$.

1.3. We define an equivalence relation in the set of the pairs $((V,f), x)$ consisting of the ε-Hermitian spaces (V,f) and its isometries x. Let $((V,f), x)$ and $((W, g), y)$ be such pairs. Then $((V,f), x)$ and $((W, g), y)$ are called equivalent if there exists a mapping $\varphi: (V,f)\to(W, g)$ which is an isomorphism as ε-Hermitian spaces and $\varphi(xu)=y\varphi(u)$ for any $u\in V$. We indicate this by the notation $((V,f), x)\simeq((w, g), y)$. Then we clearly have

Lemma 1.2. *Let* (V,f) *be an* ε*-Hermitian space over* k *with respect to* σ *and* $x, y\in U(v,f)$. *Then the following are equivalent.*

(1) x *and* y *are conjugate in* $U(V,f)$.

(2) $((V,f), x)\simeq((V,f), y)$.

1.4. Linear function ℓ. Let $m(X)$ be a monic polynomial whose constant term is not zero. We assume $m^*(X)=m(X)$. Put $R=k[X]/m(X)$. Since $m^*(X)=m(X)$, there exists a unique involution α of R such that ${}^{\alpha}X=X^{-1}$ and $\alpha|_k=\sigma$. Then $R=R_1\oplus\cdots\oplus R_r$ where $R_i(i=1,\dots, r)$ are α-indecomposable, i.e. R_i are not direct sums of non-trivial α-stable subalgebras. Since α stabilizes R_i, α induces the involution α_i of $R_i(i=1,\dots, r)$.

Let $\mathfrak{m}_i$ be the radical of R_i and d_i be the positive integer such that $\mathfrak{m}_i^{d_i}=\{0\}$ and $\mathfrak{m}_i^{d_i-1}\neq\{0\}$. α_i induces the involution $\bar{\alpha}_i$ of $\bar{R}_i=R_i/\mathfrak{m}_i$. If $\sigma\neq$identity, then obviously $\bar{\alpha}_i$ is not identity $(i=1,\dots, r)$. And if $\sigma=$identity and $\bar{\alpha}_i=$identity, then $R_i=k[X]/(X-1)^{d_i}$ or $k[X]/(X-1)^{d_i}$.

Lemma 1.3. (*Springer-Steinberg* [7], p. 254.) *We use the above notation. Assume that all* $\bar{\alpha}_i$*'s are not identity or char* $k\neq 2$. *Then there exists a* k*-valued linear function* ℓ *on* R *such that*

(1) *The symmetric bilinear form* $(u, v)\mapsto\ell(uv)$ *on* $R\times R$ *is non-degenerate.*

(2) $\ell({}^{\alpha}u)={}^{\sigma}(\ell(\delta u))$ *for any* $u\in R$

where $\delta=(\varepsilon_1,\dots, \varepsilon_r)\in R=R_1\oplus\cdots\oplus R_r$

with $\begin{cases} \varepsilon_i = 1 \text{ if } \bar{\alpha}_i \neq \text{identity}, \\ \varepsilon_i = (-1)^{d_i - 1} \text{ if } \bar{\alpha}_i = \text{identity}. \end{cases}$

Proof. We prove the above lemma only when $\bar{R}_i (i=1,\dots, r)$ are separable extension fields of k. (For the general proof, see Springer-Steinberg (loc, cit.).) $\mathfrak{m}_i$ is a principal ideal and $\mathfrak{m}_i$ is generated by an element π_i such that

$$\begin{cases} {}^{\alpha_i}\pi_i = \pi_i & \text{if } \bar{\alpha}_i \neq \text{identity}, \\ {}^{\alpha_i}\pi_i = -\pi_i & \text{if } \bar{\alpha}_i = \text{identity}. \text{ (c.f. Lemma 2.9.)} \end{cases}$$

Since R_i is a separable and commutative algebra, we can show that there exists a unique subalgebra E_i of R_i such that $E_i \simeq \bar{R}_i$. Then ${}^{\alpha}E_i = E_i$ by the uniqueness of E_i. (c.f. A. Malcev [3] and E. J. Taft [8].) Any element $a \in R$ can be written uniquely as $a = a_0 + a_1\pi_i + a_2\pi_i^2 + \cdots + a_{d-1}\pi_i^{d_i - 1}$ with $a_0, a_1, \dots, a_{d_i - 1} \in E_i$. We put $\ell_i(a) = Tr_{E_i/k}\, a_{d_i - 1}$. Then ℓ_i is a k-valued linear function on R_i which satisfies the required condition in case $R = R_i$. Define the k-valued linear function ℓ on R as follows.

$$\ell\colon R = R_1 \oplus \cdots \oplus R_r \longrightarrow k$$

$$(c_1, \dots, c_r) \longrightarrow \sum_{i=1}^{r} \ell_i(c_i).$$

Then ℓ satisfies the required condition.

1.5. Let V be a vector space over k and $x \in GL(V)$. $m(X)$ is the minimal polynomial of x. We assume $m^*(X) = m(X)$. The notation and the assumptions are as in 1.4. V is an R-module by the mapping $(X \mapsto x)$. We assume the assumption of Lemma 1.3, therefore there exists a k-valued linear function ℓ on R with those properties listed in Lemma 1.3. Hereafter we fix this function ℓ. We have the following three lemmas (c.f. Springer-Steinberg [7], p. 254).

Lemma 1.4. (1) *Let f be a (not necessarily non-degenerate) ε-Hermitian form on V over k such that $x \in U(V, f)$. Then there exists* *a unique δ-Hermitian form $F(f)$ on V over R with respect to α such that*

$$f(au, v)=\ell(aF(f)(u, v)) \quad \textit{for any} \quad u, v\in V \quad \textit{and} \quad a\in R.$$

(2) *f is non-degenerate if and only if $F(f)$ satisfies the following condition.*

$(*)$ *For any $u\neq 0\in V$, there exists $v\in V$ such that $F(f)(u, v)\neq 0$.*

Lemma 1.5. *Let f_1, f_2 be ε-Hermitian forms on V over k such that $x\in U(V, f_i)(i=1, 2)$. And let $F(f_i)(i=1, 2)$ be the uniquely determined δ-Hermitian forms on V over R by Lemma 1.4. Then the following are equivalent.*

(1) $((V, f_1), x)\simeq((V, f_2), x)$.

(2) $(V, F(f_1))\simeq(V, F(f_2))$ *(as δ-Hermitian modules over R).*

Lemma 1.6. *Let (V, F) be any δ-Hermitian module over R with respect to α. Since R is a k-algebra, V is a vector space over k. If we define $g\colon V\times V\to k$ by $g(u, v)=\ell(F(u, v))$, we get an ε-Hermitian space (V, g) over k with respect to σ and $x\in U(V, g)$ where x is the image of X in $R=k[X]/m(X)$.*

Definition 1.7. *Under the notation of Lemma 1.6, we put $\ell((V, F))=(V, g)$.*

1.6. *The problem in determining the conjugacy classes in $U(V, f)$.*

Let (V, f) be a non-degenerate ε-Hermitian space over k with respect to σ. We assume $\sigma\neq$identity or char $k\neq 2$.

Theorem 1.8. *Let C be a conjugacy class in $GL(V)$. Fix any element $x\in C$. $m(X)$ is the minimal polynomial of x. Then V is a module over $R=k[X]/m(X)$ by the mapping $(X\mapsto x)$.*

(I) *If $C\cap U(V, g)\neq\emptyset$ for some non-degenerate ε-Hermitian form g on V over k with respect to σ, then $m^*(X)=m(X)$.*

Conversely we assume $m^*(X)=m(X)$. Let α be an involution of R such that ${}^{\alpha}X=X^{-1}$, $\alpha|_k=\sigma$. Write $R=R_1\oplus\cdots\oplus R_r$, where R_i $(i=1,\dots, r)$ are α-indecomposable subalgebras of R (i.e. R_i are not direct sums of α-stable subalgebras). The radical of R_i is generated by an element π_i. d_i is the positive integer such that $\pi_i^{d_i}=0$ and $\pi_i^{d_i--}\neq 0$. And put $V_i=R_iV$. Then the following are equivalent.

(1) *$C\cap U(V, g)=\emptyset$ for some non-degenerate ε-Hermitian form g on V over k with respect to σ.*

(2) *For $1\leqslant i\leqslant r$, R_i-module V_i has the following form.*

$V_i=V_{i,0}\oplus\cdots\oplus V_{i,d_i-1}$ with

(i) *$V_{i,j}$ is a free module over $R_i/\pi_i^{d_i-1}R_i$, $(j=0,\dots, d_i-1)$.*

(ii) *If $\sigma=$ identity and $R_i=k[X]/(X\pm 1)^{d_i}$, then the rank of $V_{i,j}$ as a module over $R_i/\pi_i^{d_i-j}R_i$ must be an even number if $(-1)^{d_i-1+j}\varepsilon=-1$*

(II) *Assume C satisfies the above equivalent conditions. Put $\delta=(\varepsilon_1,\dots,\varepsilon_r)\in R$ where*

$$\begin{cases} \varepsilon_i=(-1)^{d_i-1}\in R_i & \text{if } \sigma=\text{identity and } R_i=k[X]/(X\pm 1)^{d_i},\\ \varepsilon_i=1\in R_i & \text{otherwise.}\end{cases}$$

Let $\{(V, F_i)|i\in I\}$ be the set of the representatives of the equivalence classes of the $\varepsilon\delta$-Hermitian forms on V over R satisfying the condition $(*)$ in Lemma 1.6.
Then

$$\left\{\begin{array}{l}\text{the conjugacy classes}\\ \text{in } U(V,f) \text{ which}\\ \text{are contained in } C\end{array}\right\} \xleftrightarrow{1-1} \left\{(V, F_i)\;\middle|\;\begin{array}{l} i\in I\\ \\ \ell((V, F_i))\simeq(V, f)\end{array}\right\}$$

where ℓ is a k-valued linear function satisfying the conditions listed in Lemma 1.3.

Proof. (I) By Lemma 1.4, 1.5 and 1.6, we see that (1) is equivalent to the following condition.

(3) There exists an $\varepsilon\delta$-Hermitian form F on V over R with respect

to α which satisfies the condition $(*)$ in Lemma 1.4.

The equivalence of (2) and (3) comes from Lemma 2.7 and corollary 2.12 in §2.

(II) is an easy result of Lemma 1.4, 1.5 and 1.6.

The above theorem shows that the problem to determine the conjugacy classes in $U(V, f)$ consists of the following problems.

(a) The equivalence problem of the Hermitian forms on V over R with respect to α satisfying the condition $(*)$ in Lemma 1.6.

(b) Let F be an $\varepsilon\delta$-Hermitian form on V over R with respect to α. Determine the isomorphism class of $\angle((V, F))$ from the isomorphism class of (V, F).

Remark 1.9. If $\sigma=$identity and $\varepsilon=-1$, then (V, f) is a symplectic space. The non-degenerate symplectic spaces having the same dimension are all isomorphic. So the problem (b) is trivial in this case. Thus in considering the problem (b), we may assume $\varepsilon=1$.

§2. Hermitian forms over local rings

Here we study the Hermitian modules of some type over the commutative rings which are the direct sums of complete local rings whose maximal ideals are principal. But first we consider the Hermitian spaces over more general rings.

2.1. *The trace condition* (G. E. Wall [9], p. 17). Let R be a not necessarily commutative ring with 1 and $\mathfrak{R}$ its (Jacobson) radical. We assume that the $\mathfrak{R}$-topology of R is Hausdorff and is complete. ($\mathfrak{R}$-topology of R is the topology which is obtained when we take $\{\mathfrak{R}^m | m=0, 1,...\}$ as a basis of neighbourhoods of $0\in R$. $\mathfrak{R}$-topology is Hausdorff$\Leftrightarrow \bigcap_m \mathfrak{R}^m=\{0\}$) Let α be an involution of R (i.e. α is an anti-automorphism and $\alpha^2=$id.).

Definition 2.1. (*c.f. G. E. Wall* [9], p. 17.) *We say the pair* (R, α) *satisfies the trace condition if the following is valid.*

(*Tr*) *For any positive integer* m, *if there exists* $x\in\mathfrak{R}^m$ *such that*

${}^{\alpha}x=\eta x$ $(\eta=\pm 1)$, then $x=y+\eta{}^{\alpha}y$ for some $y\in\mathfrak{R}^{m}$.

Remark 2.2. If 2 is an invertible element in R, R satisfies the trace condition. And there are some cases when R satisfies the trace condition even if 2 is not an invertible element in R (cf. [9], p. 18).

Let $R^{\times}$ denote the set of all invertible element in R. Define $(R^{\times})^{+}=\{x\in R^{\times}|{}^{\alpha}x=x\}$ and $(R^{\times})^{-}=\{x\in R^{\times}|{}^{\alpha}x=-x\}$. Put $\bar{R}=R/\mathfrak{R}$, and define $\bar{R}^{\times}$, $(\bar{R}^{\times})^{+}$, $(\bar{R}^{\times})^{-}$ similarly. Denote φ: $R\to\bar{R}$ the canonical mapping. Then we have the following lemma due to G. E. Wall.

Lemma 2.3. (*Approximation Theorem.* [9], p. 18.) *Assume R satisfies the trace condition, then*

(1) *The canonical mappings $(R^{\times})^{+}\to(\bar{R}^{\times})^{+}$ and $(R^{\times})^{-}\to(\bar{R}^{\times})^{-}$ are both surjective.*

(2) *For any $x, y\in(R^{\times})^{+}$ (resp. $(R^{\times})^{-}$), if there exists $\bar{a}\in\bar{R}^{\times}$ such that $\bar{a}\varphi(x){}^{\alpha}\bar{a}=\varphi(y)$, then there exists $a\in R^{\times}$ such that $a x{}^{\alpha}a=y$.*

2.2. Non-degenerate Hermitian spaces. Let A be a commutative ring with 1 and $\mathfrak{m}$ its (Jacobson) radical. Let α be an involution of A. We assume that the $\mathfrak{m}$-topology of A is Hausdorff and is complete. Remark that this condition is satisfied if A is a complete local ring. Now let (M, F) be any non-degenerate ε-Hermitian space of rank n over A $(\varepsilon=\pm 1)$. If we put $\bar{M}=M/\mathfrak{m}M$, $\bar{M}$ is a module over $\bar{A}=A/\mathfrak{m}$. And F induces canonically the ε-Hermitian form $\bar{F}$ on $\bar{M}$ with respect to the involution of $\bar{A}$ induced by α.

Lemma 2.4. *Define an involution $*$ of a matrix algebra $M(n, A)$ as following:*

For $C=(c_{ij})\in M(n, A)$, let $C^{*}=({}^{\alpha}c_{ji})$. Then $(M(n, A), *)$ satisfies the trace condition if and only if (A, α) satisfies the trace condition.

Proof. It is an easy matter to show the lemma if we notice that the radical of $M(n, A)$ is $M(n, \mathfrak{m})$ and that $(M(n, \mathfrak{m}))^{s}=M(n, \mathfrak{m}^{s})$ for any positive integer s.

Combining Lemma 2.3 and Lemma 2.4 we get the following Proposition.

Proposition 2.5. *Assume that A satisfies the trace condition. Then*

(1) *Any non-degenerate ε-Hermitian space over $\bar{A}$ is induced by some non-degenerate ε-Hermitian space over A.*

(2) *Let (M, F) and (M', F') be non-degenerate ε-Hermitian spaces over A. Then (M, F) and (M', F') are isomorphic if and only if $(\bar{M}, \bar{F})$ and $(\bar{M}', \bar{F}')$ are isomorphic.*

2.3. The Hermitian module which satisfies the condition $(*)$. (See below.) Let A be a direct sum of (commutative) complete local rings whose maximal ideals are principal and α be any involution of A. The following lemma is obvious.

Lemma 2.6. *If A is α-indecomposable (i.e. A is not a direct sum of non-trivial α-stable subrings), then (A, α) is one of the following two types.*

(I) *A is a complete local ring whose maximal ideal is principal and α is any involution.*

(II) *$A=B\oplus B$ where B is a complete local ring whose maximal is principal. And α is given by*

$$\alpha\colon B\oplus B \longrightarrow B\oplus B \quad ((x, y)\longmapsto (y, x)).$$

Let $A=\bigoplus_{i=1}^{r} A_i$ where A_i $(i=1,\dots, r)$ are α-indecomposable. Then α induces the involution α_i on each A_i. Now, let $\delta=(\varepsilon_1,\dots, \varepsilon_r)\in A$ be given, where $\varepsilon_i=1$ or $-1\in A_i$ for $i=1,\dots, r$. We study here the δ-Hermitian module (N, G) which satisfies the following condition.

$(*)$ For any $u\neq 0\in N$, there exists $v\in N$ such that $G(u, v)\neq 0$. Obviously we have the following lemma, and thus we may assume A is α-indecomposable.

Lemma 2.7. *Let (M, F) be any δ-Hermitian module over A with respect to α. If we put $M_i=A_iM$, then the δ-Hermitian form F*

induces ε_i-Hermitian form F_i on each M_i over A_i (with respect to α_i).

Conversely, let (M_i, F_i) be any ε_i-Hermitian module over A_i $(i=1,\dots, r)$. Then we obtain a δ-Hermitian module (M, F) over A. Moreover (M, F) satisfies the condition $(*)$ if and only if each (M_i, F_i) satisfies the condition $(*)$.

2.4. *The trace condition* (continued). Hereafter in this §, we assume that (A, α) is one of the two types listed in Lemma 2.6. Let $\mathfrak{m}$ be the radical of A. When A is of type I (in Lemma 2.6), $\mathfrak{m}$ is the maximal ideal. When A is of type II (in Lemma 2.6), $\mathfrak{m}=\mathfrak{m}'\oplus\mathfrak{m}'$ where $\mathfrak{m}'$ is the maximal ideal of B. We put $\bar{A}=A/\mathfrak{m}$. α induces the involution $\bar{\alpha}$ of $\bar{A}$, since α stabilizes $\mathfrak{m}$. Any ε-Hermitian module (M, F) over A induces an ε-Hermitian $(\bar{M}, \bar{F})$ over $\bar{A}$.

Lemma 2.9. *Assume (A, α) satisfies the trace condition, then there exists a generator π of $\mathfrak{m}$ such that ${}^{\alpha}\pi=\eta\pi$, where* $\begin{cases} \eta=-1 & \textit{if } \bar{\alpha} \textit{ is identity and } \alpha \textit{ is not identity,} \\ \eta=1 & \textit{otherwise} \end{cases}$

Proof. We may assume $\mathfrak{m}\neq\{0\}$. Let π be any generator of $\mathfrak{m}$. Then ${}^{\alpha}\pi=u\pi$ for some $u\in A^{\times}$. Since $\alpha^2=\text{id.}$, $u{}^{\alpha}u\equiv 1 \pmod{\mathfrak{m}}$. Therefore if $\bar{\alpha}$ is not identity, there exists an element $v\in A^{\times}$ such that $u \equiv v({}^{\alpha}v)^{-1} \pmod{\mathfrak{m}}$ by Hilbert's Theorem 90. Thus ${}^{\alpha}(v\pi)\equiv(v\pi) \pmod{\pi^2}$. If $\bar{\alpha}$ is identity, $u\equiv\pm 1 \pmod{\pi^2}$. So, in any case we may assume ${}^{\alpha}\pi \equiv\eta\pi \pmod{\pi^2}$. Then ${}^{\alpha}\pi-\eta\pi\in\mathfrak{m}^2$. Since ${}^{\alpha}({}^{\alpha}\pi-\eta\pi)=(-\eta)({}^{\alpha}\pi-\eta\pi)$, there exists an element $b\in\mathfrak{m}^2$ such that ${}^{\alpha}\pi-\eta\pi=b+(-\eta){}^{\alpha}b$. Then we have ${}^{\alpha}(\pi+\eta b)=\eta(\pi+\eta b)$. Moreover $\pi+\eta b$ is a generator of $\mathfrak{m}$, so we may assume ${}^{\alpha}\pi=\eta\pi$ $(\eta=\pm 1)$. But if $\bar{\alpha}$ is identity and ${}^{\alpha}\pi=\pi$, then α is identity. This completes the proof.

Proposition 2.10. (1) *If $\bar{\alpha}$ is not identity, (A, α) satisfies the trace condition.*

(2) *Assume that $\bar{\alpha}$ is identity and $\mathfrak{m}\neq\{0\}$. Then (A, α) satisfies the trace condition if and only if 2 is an invertible element in A.*

Proof. (1) Assume there exists an element $x \in \mathfrak{m}^s$ such that ${}^\alpha x = \eta x$ $(\eta = \pm 1)$. Since $\bar{\alpha} \neq \mathrm{id.}$, there exists $a \in A^\times$ such that $a + {}^\alpha a = b \in A^\times$. Then $x = b^{-1}bx = b^{-1}(a + {}^\alpha a)x = b^{-1}ax + \eta^\alpha(b^{-1}ax)$. Thus the trace condition is satisfied.

(2) Assume A satisfies the trace condition. Since $\bar{\alpha}$ is identity, A is of type I (in Lemma 2.6.) Let π be a generator of $\mathfrak{m}$ such that ${}^\alpha\pi = -\pi$ (c.f. Lemma 2.6). $\pi \neq 0$, since $\mathfrak{m} \neq \{0\}$. There exists an element $u\pi \in \mathfrak{m} = \pi A$ such that $\pi = (u\pi) - {}^\alpha(u\pi)$ by the trace condition. Therefore $\pi \equiv 2u\pi \pmod{\pi^2}$. Thus 2 is an invertible element in A.

2.5. *Jordan splittings.* (See O. T. O'Meara [6], p. 243 and Springer-Steinberg [7], p. 256.) A is a commutative ring and α is its involution. We assume that (A, α) is one of the two types listed in Lemma 2.6, and that (A, α) satisfies the trace condition. Let π be a generator of the radical $\mathfrak{m}$ such that ${}^\alpha\pi = \eta\pi$ $(\eta = \pm 1)$. (See Lemma 2.9.) Let (M, F) be an ε-Hermitian module over A (with respect to α) which satisfies the condition $(*)$ in 2.3. We now give the decomposition of (M, F) which we call *the Jordan splitting* of (M, F).

Theorem 2.11. (*Jordan splittings and their uniqueness.*)

Case 1. *When $\pi^n \neq 0$ for any positive integer n, M is an A-free module and (M, F) has the following decomposition.*

$$M = M_0 \oplus \cdots \oplus M_m \quad (\textit{as } A\textit{-modules}) \textit{ with}$$

(a) $i \neq j \Rightarrow F(M_i, M_j) = \{0\}$.

(b) $F(M_i, M_i) \subseteq \pi^i A$ *for any* i *and if we put*

$F_i(x, y) = \pi^{-i}F(x, y) \in A$ *for* $x, y \in M_i$, *then* (M_i, F_i) *is a non-degenerate* $\eta^i\varepsilon$*-Hermitian space over* A.

The sequence of the isomorphism classes of the Hermitian spaces $\{(M_i, F_i) | i = 0, 1, \ldots, m\}$ *are uniquely determined. Conversely the sequence of the isomorphism classes of the Hermitian spaces* $\{(M_i, F_i) | i = 0, 1, \ldots, m\}$ *determines the isomorphism class of* (M, F).

Case 2. *When $\pi^d = 0$ and $\pi^{d-1} \neq 0$ for some positive integer d, (M, F) has the following decomposition.*

$$M=M_0\oplus\cdots\oplus M_{d-1} \quad \textit{(as A-modules) with}$$

(a) $i\neq j\Rightarrow F(M_i, M_j)=\{0\}$,

(b) $\pi^{d-i}M_i=0$ *and* M_i *is a free module over* $A/\pi^{d-i}A$.

And for any $x, y\in M_i$, $\pi^{d-i}F(x, y)=0$, *therefore we can write* $F(x, y)=\pi^i F_i(x, y)$ *with* $F_i(x, y)\in A/\pi^{d-i}A$. *Then* (M_i, F_i) *is a non-degenerate* $\eta^i\varepsilon$*-Hermitian space over* $A/\pi^{d-i}A$ *with respect to the involution induced by* α.

The sequence of the isomorphism classes of the Hermitian spaces $\{(M_i, F_i)|i=0, 1,\dots, d-1\}$ *are uniquely determined. Conversely the sequence of the isomorphism classes of the Hermitian spaces* $\{(M_i, F_i)|i=0, 1,\dots, m\}$ *determines the isomorphism class of* (M, F).

In any case, the sequence of the isomorphism classes of $\{(M_i, F_i)|i=0, 1,\dots\}$ *or* $\{(\overline{M}_i, \overline{F}_i)|i=0, 1,\dots\}$ *is a complete invariant for the isomorphism class of* (M, F).

Proof. $(\overline{M}, \overline{F})$ is an ε-Hermitian module over $\bar{A}$ with respect to $\bar{\alpha}$. Put $\overline{N}=\{\bar{x}\in\overline{M}|F(\bar{x}, \overline{M})=0\}$. Then there exists a subspace $\overline{M}_0$ of $\overline{M}$ such that $\overline{M}=\overline{M}_0\oplus\overline{N}$ as $\bar{A}$-modules. Then $(\overline{M}_0, F|_{\overline{M}_0})$ is a non-degenerate Hermitian space. Let $\{\bar{e}_1,\dots, \bar{e}_r\}$ be a basis of $\overline{M}_0$ over $\bar{A}$. Choose a representative element e_i in M which is mapped onto $\bar{e}_i\in\overline{M}_0$ $(i=1,\dots, r)$. If we put $M_0=Ae_1+\cdots+Ae_r$, then M_0 is an A-free module and $(M_0, F|_{M_0})$ is a non-degenerate Hermitian space over A. So we can decompose M into $M=M_0\oplus M'$ where $M'=\{x\in M|F(M_0, x)=0\}$. Then $F(M', M')\subseteq\pi A$. Thus we may assume $F(M, M)\subseteq\pi A$ from the beginning.

Assume that $\pi^n\neq 0$ for any positive integer n (Case 1). Then A is a domain if A is of type I (in Lemma 2.6), and if A is of type II in Lemma 2.6, B is a domain. So in any case, $(u, v)\mapsto\frac{1}{\pi}F(u, v)$ defines an $\varepsilon\eta$-Hermitian form on M.

Assume that $\pi^d=0$ and $\pi^{d-1}\neq 0$ for some positive integer d (Case 2). In this case $F(M, M)\subseteq\pi A$ implies that $\pi^{d-1}M=0$ by the condition $(*)$. So M is a module over $A/\pi^{d-1}A$. Moreover if we put $F(u, v)=\pi G(u, v)$ for any $u, v\in M$, then $G(u, v)$ is determined as an element in $A/\pi^{d-1}A$. And $(u, v)\mapsto G(u, v)$ is an $\varepsilon\eta$-Hermitian form over $A/\pi^{d-1}A$.

If we repeat the above process, we get the required decomposition.

Give such a decomposition $M=M_0\oplus M_1\oplus\cdots\oplus M_r$. Let $M(i)=\{x\in M|F(x, M)\subseteq\pi^iA\}$. Then $M(i)=\pi^iM_0\oplus\pi^{i-1}M_1\oplus\cdots\oplus M_i\oplus M_{i+1}\oplus\cdots\oplus M_r$.

Assume that $\pi^n\neq 0$ for any positive integer n (Case 1). Then $(u, v)\mapsto\frac{1}{\pi^i}F(u, v)$ defines an $\varepsilon\eta^i$-Hermitian form on $M(i)$. This induces an $\varepsilon\eta^i$-Hermitian form G_i on the $\bar{A}$-module $N_i=M(i)/\{M(i+1)+\pi M(i-1)\}$. (We put $M(-1)=0$.) Then we can easily show that

$(N_i, G_i)\simeq(\overline{M}_i, \bar{F}_i)$ as Hermitian modules $(i=0, 1, 2,\dots)$. Thus the isomorphism classes of $\{(M_i, F_i)|i=0, 1,\dots, r\}$ do not depend on the particular decomposition. (See Proposition 2.5.)

Similarly we can show the uniqueness of the Jordan splittings, when $\pi^d=0$ and $\pi^{d-1}\neq 0$ for some d (Case 2). (See Springer-Steinberg [7], p. 256.)

Corollary 2.12. *We assume $\pi^d=0$ and $\pi^{d-1}\neq 0$ for some positive integer d. Let N be any A-module. Then the following are equivalent.*

(1) *There exists an ε-Hermitian form F on N which satisfies the condition* (*).

(2) *$N=N_0\oplus\cdots\oplus N_{d-1}$ (as A-modules) with*

(i) *N_j is a free module over $A/\pi^{d-j}A$.*

(ii) *When $\bar{\alpha}=$identity, the rank of N_j as a module over $A/\pi^{d-j}A$ must be an even number if $\varepsilon(-1)^j=-1$.*

Proof. This comes from the above theorem and the following fact. "Let $\varepsilon'=1$ or -1. Then there exists an ε'-Hermitian space of any rank over $\bar{A}$ with respect $\bar{\alpha}$ except when $\bar{\alpha}=$identity and $\varepsilon'=-1$. When $\bar{\alpha}=$identity and $\varepsilon'=-1$, the rank must be even."

Definition 2.13. *Under the notation of Theorem 2.11, we write*

$$(M, F)=\bigoplus_{i=1}^{r}(M_i, \pi^iF_i).$$

This is called the Jordan splitting of (M, F).

§3. To determine the isomorphism class of $\ell((V, F))$ from the isomorphism class of (V, F)

3.1. We keep the notation and assumption of §1. In this §, we assume k is perfect. And when $\sigma=\mathrm{id.}$, we assume $\mathrm{char}\, k\neq 2$ in addition. The k-valued linear function ℓ on R is the one constructed in the proof of Lemma 1.3. ℓ depends on the choice of π_i $(i=1, .., r)$. (See the proof of Lemma 1.3.) (V, F) is an $\varepsilon\delta$-Hermitian module over R with respect to α. So (V, F) is a direct sum of $\varepsilon\varepsilon_i$-Hermitian modules (V_i, F_i) over R_i with respect α_i, where $V_i=R_iV$ and $\alpha_i=\alpha|_{R_i}$ $(i=1,\dots, r)$. Let $(V_i, F_i)=\overset{d_i-1}{\underset{j=0}{\oplus}} (V_{i,j}, \pi_i^j F_{i,j})$ be the Jordan splitting of (V_i, F_i).

Put $\eta^i=\begin{cases} -1 \text{ if } \sigma=\text{identity and } R_i=k[X]/(X\pm 1)^{d_i}, \\ 1 \text{ otherwise} \end{cases}$

Then we easily have the following lemma whose proof is omitted.

Lemma 3.1. (1) $\ell((V, F))=\overset{r}{\underset{i=1}{\oplus}} \ell_i((V_i, F_i))$, *where* $\ell_1, .., \ell_r$ *are as in the proof of Lemma* 1.5.

(2) $\ell_i((V_i, F_i))=\overset{d_i-1}{\underset{j=0}{\oplus}} l_i((V_{i,j}, \pi_i^j F_i))$.

(3) *When* d_i-j *is an even integer, then*

$$\ell_i((V_{i,j}, \pi_i^j F_i))=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus\cdots\oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(4) *When* d_i-j *is an odd integer* $2s+1$, *then*

$$\ell_i((V_{i,j}, \pi_i^j F_i))=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus\cdots\oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \eta_i^s Tr_{\overline{R}_i/k}((\overline{V}_{i,j}, \overline{F}_{i,j})),$$

where $\eta_i^s Tr_{\overline{R}_i/k}((\overline{V}_{i,j}, \overline{F}_{i,j}))$ *is* $\overline{V}_{i,j}$ *considered as a vector space over* k *with the Hermitian form* $(u, v)\mapsto \eta_i^s Tr_{\overline{R}_i/k}\overline{F}_{i,j}(u, v)$ *with respect to* σ. *(See Definition* 1.7)

(4) *When* $\overline{R}_i$ *is a direct sum of two fields, then*

$$\eta_i^s Tr_{\bar{R}_i/k}((\bar{V}_{i,j}, \bar{F}_{i,j})) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By Theorem 1.8, Theorem 2.11 and Lemma 3.1, we have

Theorem 3.2. *We use the notation of Theorem* 1.8. *Let C be a conjugacy class in $GL(V)$ which satisfies the equivalent conditions in Theorem* 1.8, (*I*). *Assume $\bar{R}_i$ is a finite extension field of k for $1 \leqslant i \leqslant s$ and $\bar{R}_i$ is a direct sum of two copies of finite extension field of k for $s+1 \leqslant i \leqslant r$.*
Put $n_{i,j} = \dim_{\bar{R}_i} \bar{V}_{i,j}$ and

$$\eta_i = \begin{cases} -1 \text{ if } \sigma = \text{identity and } R_i = k[X]/(X \pm 1)^{d_i}, \\ 1 \text{ otherwise.} \end{cases}$$

Then there is a following 1−1 *correspondence.*

$$\left\{ \begin{array}{l} \text{The conjugacy classes in } U(V, f) \\ \text{which is contained in } C. \end{array} \right\}$$

$$\xleftrightarrow{1-1} \left\{ (\ldots, H_{i,j}, \ldots) \;\middle|\; \begin{array}{ll} \text{(a)} & H_{i,j}\ (1 \leqslant i \leqslant s,\ 0 \leqslant j \leqslant d_i - 1) \text{ runs the} \\ & \text{equivalence classes of } n_{i,j}\text{-dimensional} \\ & \varepsilon\eta_i^{d_i - j - 1}\text{-Hermitian spaces over } \bar{R}_i \text{ with} \\ & \text{respect to } \alpha_i, \\ \text{(b)} & \oplus \left\{ Tr_{\bar{R}_i/k} H_{i,j} \;\middle|\; \begin{array}{l} 1 \leqslant i \leqslant s,\ 0 \leqslant j \leqslant d_i - 1, \\ d_i - j \text{ is odd.} \end{array} \right\} \\ & \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots\cdots\cdots\cdots \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \simeq (V, f) \end{array} \right\}$$

For the definition of $Tr_{\bar{R}_i/k} H_{i,j}$, see Lemma 3.1, (4). *When σ = identity and $\varepsilon = -1$, the condition* (b) *in the right side of the above correspondence is unnecessary.*

We must solve the following problem.

Problem 3.3. Let k be a field and E a finite extension field of k. Let α be an involution ($\neq$identity) of E such that ${}^{\alpha}k = k$. Put

$\sigma=\alpha|_k$. Given any non-degenerate s-simensional Hermitian space (W, F) over E with respect to α. Determine the isomorphism class of the Hermitian space $Tr_{E/k}(W, F)$ over k with respect to σ from the isomorphism class of (W, F), where $Tr_{E/k}(W, F)$ is W considered as a vector space over k with the Hermitian form $(u, v)\mapsto Tr_{E/k}F(u, v)$ with respect to σ.

J. Milnor [4] gave an answer to the above problem when k is a local field and $\sigma=$identity. (See Lemma 3.5.) In the following, utilizing his results we give a similar answer when k is an algebraic number field.

3.2. We introduce some notation and conventions. Let k be a field and R a finite (commutative) k-algebra. $Tr_{R/k}$ (resp. $N_{R/k}$) denote the trace (resp. the norm) of the regular representation. If k is an algebraic number field and v is a prime spot on k, and if W is a δ-Hermitian module over R (with respect to some involution α of R), then W induces the δ-Hermitian module W_v over $R_v=R\otimes_k k_v$ with respect to the involution of R_v induced by α.

If V is a symmetric bilinear space over a local field, $S(V)$ means the Hasse symbol of V. If V is a symmetric bilinear space over an algebraic number field F and if v is any prime spot on F, then $S_v(V)=S(V_v)$.

Now we consider the problem 3.3. We use the notation of Problem 3.3. We write W instead of (W, F). Let W_0 be the Hermitian space of the same rank s as W over E with respect to α such that $W_0=\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

Put $K=\{x\in E|{}^{\alpha}x=x\}$ and $k_0=\{x\in k|{}^{\sigma}x=x\}$.

Lemma 3.4. (1) *When $\sigma=$identity,*

$$\det(Tr_{E/k}W)\equiv\det(Tr_{E/k}W_0) \bmod (k^{\times})^2.$$

(2) *When $\sigma\neq$identity,*

$$\det(Tr_{E/k}W)\equiv N_{K/k_0}(\det W)\det(Tr_{E/k}W_0) \bmod N_{k/k_0}(k^{\times}).$$

Proof. (1) See J. Milnor [4], Lemma 2.2 and Theorem 2.7. (2) is similar to (1).

Lemma 3.5. *(See J. Milnor* [4], §2.) *Assume k is a local field and $\sigma=id.$.*

(1) *The Hasse symbol $S(Tr_{E/k}W)$ of the symmetric bilinear space $Tr_{E/k}W$ is given by $S(Tr_{E/k}W)=S(Tr_{E/k}W_0)dW$, where dW is the Hermitian invariant of W, i.e. $dW=1$ or -1 according as* $\det W\in N_{E/k}(E^{\times})$ *or not.*

(2) *When k is the field of real numbers and E is the field of complex numbers, the index $I(Tr_{E/k}W)$ of $Tr_{E/k}W$ (i.e. the number of negative entries when we put $Tr_{E/k}W$ into a diagonal symmetric matrix) is given by $I(Tr_{E/k}W)=2I(W)$, where $I(W)$ is the index of W (i.e. the number of negative entries when we put W into a diagonal Hermitian matrix).*

Lemma 3.6. *Assume k is a local field and $\sigma=$ identity. The Hermitian invariant of the Hermitian space $Tr_{E/k}W$ over k with respect to σ is given by $d(Tr_{E/k}W)=dWd(Tr_{E/k}W_0)$, where dW is the Hermitian invariant of W.*

Proof. By the local class field theory,

$$(x, E/K)|_k=(N_{K/k_0}(x), k/k_0) \qquad \text{for any} \quad x\in K^{\times}.$$

Thus $\det W\in N_{E/K}(E^{\times})$ if and only if $N_{K/k_0}(\det W)\in N_{k/k_0}(k^{\times})$. Therefore we have the lemma from Lemma 3.4, (2)

Theorem 3.7. *Assume k is an algebraic number field and $\sigma=$ identity. Let v be any prime spot on k and $\{w_1,\dots, w_g\}$ be the set of all prime spots on K which divide v. Then*

$$S_v(Tr_{E/k}W)=S_v(Tr_{E/k}W_0)\{\prod_{i=1}^{g} dW_{w_i}\},$$

where $dW_{w_i}=1$ *or* -1 *according as* $\det W_{w_i}\in N_{E_{w_i}/K_{w_i}}(E^\times_{w_i})$ *or not.*

When v *is a real spot, we may assume* $\{w_1,\dots, w_r\}=\{w_i|E\otimes_K K_{w_i}\simeq$ *the field of complex numbers*$\}$. *Then*

$$I_v(Tr_{E/k}W)=2\sum_{i=1}^{r} I_{w_i}(W)+s([K:k]-r).$$

where $I_v(Tr_{E/k}W)$ *(resp.* $I_{w_i}(W)$*) is the index of* $(Tr_{E/k}W)_v$ *(resp.* W_{w_i}*).*

Proof. $(Tr_{E/k}W)_v=Tr_{E_v/k_v}W_v$

$$=Tr_{E_v/k_v}(\bigoplus_{i=1}^{g} W_{w_i}) \quad (\because \quad E_v=E\otimes_k k_v\simeq \bigoplus_{i=1}^{g} E_{w_i})$$

$$=\bigoplus_{i=1}^{g}(Tr_{E_{w_i}/k_v}W_{w_i}) \quad (\because \quad Tr_{E_v/k_v}=\bigoplus_{i=1}^{g} Tr_{E_{w_i}/k_v})$$

Thus $S_v(Tr_{E/k}W)=S((Tr_{E/k}W)_v)=S(\bigoplus_{i=1}^{g}(Tr_{E_{w_i}/k_v}W_{w_i}))$
$=\{\prod_{i<j}(\det(Tr_{E_{w_i}/k_v}W_{w_i}), \det(Tr_{E_{w_j}/k_v}W_{w_j}))\}\{\prod_{i=1}^{g}S(Tr_{E_{w_i}/k_v}W_{w_i})\}$,
where (,) denotes the Hilbert's symbol.
Similarly

$$S_v(Tr_{E/k}W_0)$$

$$=\{\prod_{i<j}(\det(Tr_{E_{w_i}/k_v}(W_0)_{w_i}), \det(Tr_{E_{w_j}/k_v}(W_0)_{w_j}))\}\{\prod_{i=1}^{g}S(Tr_{E_{w_i}/k_v}(W_0)_{w_i})\}$$

Thus $S_v(Tr_{E/k}W)S_v(Tr_{E/k}W_0)=\{\prod_{i=1}^{g}S(Tr_{E_{w_i}/k_v}W_{w_i})\}\{\prod_{i=1}^{g}S(Tr_{E_{w_i}/k_v}(W_0)_{w_i}\}$.
So we get the first assertion of the theorem if we prove

$$S(Tr_{E_{w_i}/k_v}W_{w_i})=S(Tr_{E_{w_i}/k_v}(W_0)_{w_i})\,dW_{w_i} \qquad \text{for any } i.$$

But this is Lemma 3.6, if E_{w_i} is a field. And if E_{w_i} is a direct sum of two copies of K_{w_i}, we clearly have $W_{w_i}\simeq(W_0)_{w_i}$ and $dW_{w_i}=1$, therefore the above equation is trivially valid.

The second equation of the theorem is easy and we omit the proof.

Similarly we can prove

Theorem 3.8. *Assume k is an algebraic number field and $\sigma \neq$ identity. Let v be any prime spot on $k_0 = \{x \in k | {}^\sigma x = x\}$ and $\{w_1, \ldots, w_g\}$ be the set all prime spots on K which divides v. Then*

$$\mathrm{d}((Tr_{E/k} W)_v) = \mathrm{d}((Tr_{E/k} W_0)_v) \{ \prod_{i=1}^{q} dW_{w_i} \}.$$

Remark 3.9. (1) Under the notation of Theorem 3.6, $S_v(Tr_{E/k} W_0) = 1$ if v is non-dyadic and any prime spot on E which divides v is unramified over v.

(2) Under the notation of Theorem 3.7, $\mathrm{d}((Tr_{E/k} W_0)) = 1$ if v is non-dyadic and any prime spot on E which divides v is unramified over v.

§4. Hasse principle for the conjugacy classes

4.1. Hasse principle for the Hermitian forms over a k-algebra. Let k be an algebraic number field. Let R be a finite k-algebra generated by one element (i.e. $R = k[X]/m(X)$ with $m(X) \neq$constant). Let α be an involution of R such that ${}^\alpha k = k$. Put $\sigma = \alpha|_k$ and $k_0 = \{x \in k | {}^\alpha x = x\}$. Write $R = \bigoplus_{i=1}^{r} R_i$, where R_i $(i = 1, \ldots, r)$ are α-indecomposable subalgebras. Let $\mathfrak{m}_i$ be the radical of R_i $(i = 1, \ldots, r)$. d_i is the positive integer such that $\mathfrak{m}_i^{d_i} = \{0\}$, $\mathfrak{m}_i^{d_i - 1} \neq \{0\}$. α induces the involution α_i on each R_i and thus induces the involution $\bar{\alpha}_i$ on each $\bar{R}_i = R_i/\mathfrak{m}_i$. $\mathfrak{m}_i$ is generated by an element π_i such that ${}^{\alpha_i}\pi_i = \eta_i \pi_i$ where $\eta_i = -1$ or 1 according as $\bar{\alpha}_i =$identity or not. (See Lemma 2.9.) We assume $\bar{R}_i$ is a finite extension field of k for $1 \leqslant i \leqslant s$ and $\bar{R}_i$ is a direct sum of two copies of a finite extension field of k for $s+1 \leqslant i \leqslant r$. Let $\delta = (\varepsilon_1, \ldots, \varepsilon_r) \in R$ with $\varepsilon_i = 1$ or $-1 \in R_i$ $(i = 1, \ldots, r)$. Let (M, F) be a δ-Hermitian module over R with respect to α satisfying the condition $(*)$. (See 2.3.) Then (M, F) induces canonically a δ-Hermitian module over $R_v = R \otimes_{k_0} (k_0)_v$ for any prime spot v on k_0. We indicate this Hermitian module by (M_v, F_v) or $(M, F)_v$.

Proposition 4.1. *Let (M, F) and (N, G) be δ-Hermitian modules. Then the following are equivalent.*

(1) $(M, F) \simeq (N, G)$.

(2) $(M, F)_v \simeq (N, G)_v$ *for any prime spot* v *on* k_0.

Proof. (1)$\Rightarrow$(2) is trivial.

(2)$\Rightarrow$(1). Put $M_i = R_i M$ and $F_i = F|_{M_i}$. Then $(M, F) = \bigoplus_{i=1}^{r} (M_i, F_i)$. Similarly we write $(N, G) = \bigoplus_{i=1}^{r} (N_i, G_i)$. Then $(M, F)_v \simeq (N, G)_v$ implies $(M_i, F_i)_v \simeq (N_i, G_i)_v$ $(i = 1, \dots, r)$. Let $(M_i, F_i) = \bigoplus_{j=0}^{d_i - 1} (M_{i,j}, \pi_i^j F_{i,j})$ (resp. $(N_i, G_i) = \bigoplus_{j=0}^{d_i - 1} (N_{i,j}, \pi_i^j G_{i,j})$) be the Jordan splitting of (M_i, F_i) (resp. (N_i, G_i)). $(R_i)_v$ is not α-indecomposable in general. But if we apply the uniqueness of the Jordan splittings very carefully, we see that $(M_i, F_i)_v \simeq (N_i, G_i)_v$ implies $(M_{i,j}, F_{i,j})_v \simeq (N_{i,j}, G_{i,j})_v$ for $0 \leqslant j \leqslant d_i - 1$. Thus $(\overline{M}_{i,j}, \overline{F}_{i,j})_v \simeq (\overline{N}_{i,j}, \overline{G}_{i,j})_v$ for any i, j and v. On the other hand $(M, F) \simeq (N, G) \Leftrightarrow (\overline{M}_{i,j}, \overline{F}_{i,j}) \simeq (\overline{N}_{i,j}, \overline{G}_{i,j})$ for any i, j. Therefore it suffices to prove that $(\overline{M}_{i,j}, \overline{F}_{i,j}) \simeq (\overline{N}_{i,j}, \overline{G}_{i,j})$ if and only if $(\overline{M}_{i,j}, \overline{F}_{i,j})_v \simeq (\overline{N}_{i,j}, \overline{G}_{i,j})_v$ for any v. But this is trivial when $\overline{R}_i$ is a direct sum of two copies of some algebraic extension field of k. Thus our assertion comes from the following lemma.

Lemma 4.2. *Let* E *be a finite extension field of* k *and* α *be an involution (maybe identity) of* E *such that* ${}^{\alpha}k = k$. *Put* $\sigma = \alpha|_k$, $K = \{x \in E | {}^{\alpha}x = x\}$ *and* $k_0 = \{x \in k | {}^{\sigma}x = x\}$.

(1) *Let* v *be any prime spot on* k_0 *and* $\{w_1, \dots, w_g\}$ *be the set of prime spots on* K *which divide* v. *Then any Hermitian space over* $E_v = E \otimes_k k_v$ *with respect to* α *is a direct sum of Hermitian spaces over* $E_{w_i} = E \otimes_K K_{w_i}$ $(i = 1, \dots, g)$.

(2) *Let* V *and* W *be non-degenerate Hermitian spaces over* E *with respect to* α. *Then* $V \simeq W$ *if and only if* $V_v \simeq W_v$ *for any prime spot* v *on* k_0.

Proof. Since $E_v = \bigoplus_{i=1}^{g} E_{w_i}$, (1) is trivial. (1) implies that if $V_v \simeq W_v$ for any prime spot v on k_0, then $V_w \simeq W_w$ for any prime spot w on K, therefore $V \simeq W$ by the usual Hasse principal for the Hermitian or quadratic spaces. (See W. Landherr [2] and O. T. O'Meara [6].)

Now we ask the following question.

Problem 4.3. For any prime spot v on k_0 there corresponds a δ-Hermitian module $(M, F)_{(v)}$ over R_v with respect to α. When does there exist a δ-Hermitian module (M, F) over R such that $(M, F)_v \simeq (M, F)_{(v)}$ for any prime spot v on k_0?

To answer the above problem we give a preparatory lemma without proof, which is easily derived from Theorem 2.11. (See also the proof of Proposition 4.1.)

Lemma 4.4. *Let M_i be an R_i-module. Let G be any ε_i-Hermitian form on $(M_i)_v = M_i \otimes_k k_v$ over $(R_i)_v = R_i \otimes_k k_v$ with respect to α_i which satisfies the condition $(*)$ in 2.3. Then $((M_i)_v, G)$ has the following decomposition.*

$(M_i)_v = (M_i)_{v,0} \oplus \cdots \oplus (M_i)_{v,d_i-1}$ (as R_i-modules) with

(a) $j \neq j' \Rightarrow G((M_i)_{v,j}, (M_i)_{v,j'}) = \{0\}$,

(b) *$\pi_i^{d_i-j}(M_i)_{v,j} = 0$ and $(M_i)_{v,j}$ is a free module over $(R_i/\pi_i^{d_i-j}R_i)_v$. And for any $x, y \in (M_i)_{v,j}$, $\pi_i^{d_i-j}G(x, y) = 0$, therefore we can write $G(x, y) = \pi_i^j G_i(x, y)$ with $G_i(x, y) \in (R_i/\pi_i^{d_i-j}R_i)_v$. Then $((M_i)_{v,j}, G_j)$ is a non-degenerate $\eta_i^j\varepsilon_i$-Hermitian space over $(R_i/\pi_i^{d_i-j}R_i)_v$ with respect to the involution induced by α_i.*

The sequence of the isomorphism classes of the Hermitian spaces $\{((M_i)_{v,j}, G_j)\}$ is uniquely determined. $((M_i)_{v,j}, G_j)$ induces canonically the $\eta_i^j\varepsilon_i$-Hermitian space $(\overline{(M_i)_{v,j}}, \overline{G_j})$ over $(\overline{R_i})_v = (R_i/\pi_i R_i)_v$. And the sequence of the isomorphism classes of the Hermitian spaces $\{(\overline{(M_i)_{v,j}}, \overline{G_j}) \mid j = 0, \ldots, d_i - 1\}$ is a complete invariant for the isomorphism class of $((M_i)_v, G)$. We write $((M_i)_v, G) = \bigoplus_{j=0}^{d_i-1} ((M_i)_{v,j}, \pi_i^j G_j)$.

We easily have the following two propositions. Combining them we see that Problem 4.3 is solved completely by the usual Hasse principle for the Hermitian spaces or symmetric bilinear spaces. (See W. Landherr [2] and O. T. O'Meara [6].)

Proposition 4.5. *Let M be any R-module. Put $M_i = R_i M$ ($i = 1, \ldots, r$). Then $M = M_1 \oplus \cdots \oplus M_r$. Assume for any prime spot v on*

k_0 there corresponds a δ-Hermitian form $F_{(v)}$ on M_v over $R_v=R\otimes_k k_v$ (with respect to α). $F_{(v)}$ induces ε_i-Hermitian form $(F_i)_{(v)}$ on each $(M_i)_v$, and $(M_v, F_{(v)})=\bigoplus_{i=1}^{r}((M_i)_v, (F_i)_{(v)})$. Let $((M_i)_v, (F_i)_{(v)})=\bigoplus_{j=0}^{d_i-1}((M_i)_{v,j}, \pi_i^j(F_i)_{(v),j})$ be the decomposition as in Lemma 4.3. Then the following are equivalent.

(1) *There exists a δ-Hermitian form F on M over R such that $(M_v, F_v)\simeq(M_v, F_{(v)})$ for any prime spot v on k.*

(2) *For $i=1,\dots, s$ and $j=0,\dots, d_i-1$, there exists an $\eta_i^j\varepsilon_i$-Hermitian space $W_{i,j}$ over R_i such that*

$$(W_{i,j})_v\simeq((M_i)_{v,j}, (F_i)_{(v),j}) \text{ for any prime spot } v \text{ on } k_0.$$

Proposition 4.6. *We use the notation and assumption of Lemma 4.2. Assume that for any prime spot v on k_0 there corresponds a Hermitian space $V_{(v)}$ over E_v with respect to α. Let $\{w_1,\dots, w_g\}$ be the set of prime spots on K which divide v. Since $V_{(v)}$ is a direct sum of Hermitian spaces $V_{(w_i)}$ over $E_{w_i}=E\otimes_K K_{w_i}$ $(i=1,\dots, g)$, so for any prime spot w on K there corresponds a unique Hermitian space $V_{(w)}$ over E_w. Then the following are equivalent.*

(1) *There exists a Hermitian space W over E such that $V_{(v)}\simeq W_v$ for any prime spot v on k_0.*

(2) *There exists a Hermitian space W over E such that $V_{(w)}\simeq W_w$ for any prime spot w on K.*

4.2. Hasse principle for the conjugacy classes. Let (V, f) be a non-degenerate ε-Hermitian space over k. Put $G=U(V, f)$ and $GL=GL(V)$. We consider G and GL as algebraic groups defined over k_0, where $k_0=\{x\in k|{}^\sigma x=x\}$. For example, $G(k_0)$ is the k_0-rational points of G. Then Proposition 4.1 and Theorem 1.8 shows

Theorem 4.7. (*H. Hijikata* [1]) *For $x_1, x_2\in G(k_0)$, x_1 and x_2 are conjugate in $G(k_0)$ if and only if x_1 and x_2 are conjugate in $G((k_0)_v)$ for any prime spot v on k_0.*

By Theorem 1.8 and Proposition 4.5, we have

Theorem 4.8. *We use the notation of Theorem* 1.8 *and Theorem* 3.2. *Let C be a conjugacy class of $GL(k_0)$ which satisfies the equivalent conditions in Theorem* 1.8, (I). *For any prime spot v on k_0, C determines the conjugacy class C_v of $GL((k_0)_v)$ and each conjugacy class D of $G(k)$ determines the conjugacy class D_v of $G((k_0)_v)$.*

(I) *There is a following* $1-1$ *correspondence.*

$$\left\{\begin{array}{l}\textit{The conjugacy classes in } G((k_0)_v)\\ \textit{which is contained in } C_v.\end{array}\right\}\xleftrightarrow{1-1}$$

$$\left\{(\dots,(H_{i,j})_{(v)},\dots)\;\middle|\;\begin{array}{ll}\text{(a)} & (H_{i,j})_{(v)}\ (1\leqslant i\leqslant s,\ 0\leqslant j\leqslant d_i-1)\ \textit{runs the}\\ & \textit{isomorphism classes of } n_{i,j}\textit{-dimensional}\\ & \eta_i^{d_i-j-1}\textit{-Hermitian spaces over } (\bar{R}_i)_v\\ & \textit{with respect to } \bar{\alpha}_i,\\ \text{(b)} & \oplus\{Tr_{\bar{R}_i/k}(H_{i,j})_{(v)}|1\leqslant i\leqslant s,\ 0\leqslant j\leqslant d_i-1\}\\ & \oplus\begin{pmatrix}0&1\\1&0\end{pmatrix}\oplus\cdots\oplus\begin{pmatrix}0&1\\1&0\end{pmatrix}\simeq(V,f)_v\end{array}\right\}$$

When $\varepsilon=-1$ and $\sigma=$ identity, the condition (b) *in the right side of the above correspondence is unnecessary.*

(II) *Assume for any prime spot v on k_0 there corresponds a conjugacy class $D_{(v)}$ of $G((k_0)_v)$ which is contained in C_v. And we assume*

$$D_{(v)}\longleftrightarrow(\dots,(H_{i,j})_{(v)},\dots)$$

by the above correspondence. Then the following are equivalent.

(1) *There exists a conjugacy class D of G_k such that $D_v=D_{(v)}$ for any prime spot v on k_0.*

(2) *For $1\leqslant i\leqslant s$, $0\leqslant j\leqslant d_i-1$, there exists $\eta_i^{d_i-j-1}$-Hermitian form $W_{i,j}$ over $\bar{R}_i$ with respect to $\bar{\alpha}_i$ such that $(W_{i,j})_v\simeq(H_{i,j})_{(v)}$ for any prime spot v on k_0.*

For semisimple elements in the orthogonal group, the existence theorem of prescribed local behaviour (the second part of the above theorem) has another form. The minimal polynomial of the semisimple element has the following form.

$$m(X)=\prod_{i=1}^{r} m_i(X) \quad \text{where}$$

(i) For $1\leqslant i\leqslant s$, $m_i(X)$ is a monic irreducible polynomial and $m_i(X)=m_i^*(X)$.

(ii) For $s+1\leqslant i\leqslant r$, $m_i(X)=p_i(X)p_i^*(X)$ with $p_i(X)$ is a monic irreducible polynomial and $p_i^*(X)\neq p_i(X)$.

(iii) $i\neq j\Rightarrow m_i(X)\neq m_j(X)$.

Theorem 4.9. *Let G be an orthogonal group and $m(X)$ be the polynomial as above. Assume that for any prime spot v on k there corresponds $x_v\in G(k_v)$ whose minimal polynomial is $m(X)$. Put $(V_v)_{m_i(x_v)}=\{u\in V_v|m_i(x_v)u=0\}$. Assume $\dim_{k_v}(V_v)_{m_i(x_v)}$ $(i=1,\dots,r)$ are independent of v, i.e. the elementary divisors of x_v are independent of v. Then there exists $x\in G(k)$ such that x and x_v are conjugate in $G(k_v)$ if and only if the following conditions are satisfied.*

(i) *$S((V_v)_{m_i(x_v)})=1$ for almost all v $(i=1,\dots,s)$.*

(ii) *$\prod_v S((V_v)_{m_i(x_v)})=1$ $(i=1,\dots,s-1)$.*

(iii) *If $(X-1)(X+1)$ divides $m(X)$, then there exists $d\in k^\times$ such that $\det(V_v)_{(x_v-1)}\equiv d \bmod (k_v^\times)^2$.*

Proof. This comes from the following lemma whose proof is omitted. (c.f. the proof of Theorem 3.6.)

Lemma 4.10. *Let E be a finite extension field of k and α an involution of E such that $\alpha|_k=$ identity. Assume that for any prime spot v on k there corresponds a Hermitian space $W_{(v)}$ of rank s over E_v with respect to α. Then the following are equivalent.*

(i) *There exists a Hermitian space W of rank s over E such that $W_v\simeq W_{(v)}$ for any prime spot v on k.*

(ii) $W_{(v)}\simeq \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ *for almost all v, and $\prod_v S(Tr_{E_v/k_v} W_{(v)})=1$.*

There is an analogue of Theorem 4.9 for semisimple element in the unitary group.

UNIVERSITY OF OSAKA PREFECTURE

References

[0] M. Eichler, Zur Algebra der orthogonalen Gruppen, Math. Zeit. 53, 11–20 (1950).

[1] H. Hijikata, Hasse principle for the conjugacy classes of the orthogonal group (in Japanese), Reports of the symposium on algebraic groups held at Yamanaka-Kyodo-Kensyujo, 1973.

[2] W. Landherr, Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper, Abh. Math. Sem. Hamburg Univ. 11, 245–248 (1935).

[3] A. Malcev, On the representation of an algebra as a direct sum of the radical and a semisimple algebra, Dokl. Akad. Nauk SSSR 36 (1942), 42–45.

[4] J. Milnor, On isometries of inner product spaces, Inv. Math., Vol. 8 (1969), 83–97.

[5] J. Milnor and D. Husemoller, Symmetric bilinear forms, Springer-Verlag, 1973.

[6] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, 1963.

[7] T. A. Springer and R. Steinberg, Conjugacy classes, Seminar on algebraic groups and related finite groups, Springer Lecture Notes 131 (1970).

[8] E. J. Taft, Orthogonal conjugacies in associative and Lie algebras, Trans. Amer. Math. Soc. 113 (1964), 18–29.

[9] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austr. Math. Soc., Vol. 3 (1963), 1–62.

[10] J. Williamson, Normal matrices over an arbitrary field of characteristic zero, Amer. J. Math. 61 (1939), 335–356.