J. Math. Kyoto Univ.
10-3 (1970) 433-437

A remark on the group of orthogonal similitudes

By

Hiroaki HIJIKATA and Akiko YOSHIOKA

(Received April 9, 1970)

Let (V, Q) be a *quadratic space* over a field k, namely V is a finite dimensional vector space over k supplied with a quadratic form $Q: V\rightarrow k$. Let $\Phi(x, y)=Q(x+y)-Q(x)-Q(y)$ denote the associated bilinear form. For any subspace W of V, we set $W^{\perp}=\{x\in V; \Phi(x, w)=0$ for any $w\in W\}$. A vector x in V is called *singular* if $Q(x)=0$, and the set of all the singular vectors in $V^{\perp}$ make up a subspace V' called the *radical* of (V, Q). A quadratic space (V, Q) is called *non-degenerate* [resp. *strongly* non-degenerate] if V' [resp. $V^{\perp}$] consists of the single vector 0.

A linear automorphism $u\in GL(V)$ of V is called a (orthogonal) *similitude* of (V, Q), if there exists a scalar μ called the *multiplicator* of u, such that $Q(u(x))=\mu Q(x)$ for any $x\in V$. Let $GO(V, Q)$ denote the subgroup of $GL(V)$ consisting of all the similitudes of (V, Q).

A similitude with the multiplicator 1 is called a *rotation* (some authors restrict the name rotation for the one with the determinant 1), and the rotations make up a subgroup $O(V, Q)$ called the *orthorgonal group* of (V, Q).

If the multiplicator μ of u is a square $(=\nu^2)$ in k, then we can find a rotation σ such that σu is a homothecy h_{ν}, i.e. $h_{\nu}(x)=\nu x$ for any $x\in V$. If μ is not a square, u can not be a homothecy modulo $O(V, Q)$. It is the purpose of this note to prove the following theorem which gives a normal form modulo $O(V, Q)$ for a similitude with a non-square multiplicator.

Theorem. *Let* (V, Q) *be a non-degenerate quadratic space over*

k of dimension n. If a similitude $u \in GO(V, Q)$ has a non-square multiplicator μ, then n is even $(=2m)$, and there exists a rotation σ and a base $\{e_1, \cdots, e_m, e'_1, \cdots, e'_m\}$ of V satisfying the following: $\sigma u(e_i)=e'_i$ and $\sigma u(e'_i)=\mu e_i$ for $i=1, \cdots, m$.

This result is obtained by the second named author of this note under the assumption that (V, Q) is strongly non-degenerate, and its special case when k is of characteristic two has been published in her previous paper, Structure du groupe des similitudes orthogonales, Nagoya Math. J. 1970. The generalization to the present form and a simplification of the proof due to the first named author.

The assumption of non-degeneracy of (V, Q) is nothing essential for this problem. Indeed, consider a (V, Q) with a non-trivial radical V', $\dim V'=r>0$. Let V_1 be an arbitrarily chosen complement of V', $V=V_1+V'$, $V_1\cap V'=\{0\}$, and $\pi_1: V\to V_1$, $\pi': V\to V'$ be the projections according to the decomposition.

If $u\in GO(V, Q)$, then $u(V')\subset V'$ hence

$$\pi_1 u\pi' = 0 \qquad \cdots\cdots\cdots\cdots(1)$$

If w is a linear endomorphism of V such that $w(V)\subset V'$, then $1+w\in O(V, Q)$, in particular

$$1-\pi' u\pi_1 u^{-1}\in \mathrm{O}(V, Q) \qquad \cdots\cdots\cdots\cdots(2)$$

By (1) and the identity $1=\pi_1+\pi'$, we have,

$$u = \pi_1 u\pi_1+\pi' u\pi_1+\pi' u\pi'$$

Set $u'=(1-\pi' u\pi_1 u^{-1})u$, then $u'=\pi_1 u\pi_1+\pi' u\pi'$ i.e. u' stabilizes both V_1 and V'. Since $GO(V', Q_{|V'})=O(V', Q_{|V'})=GL(V')$, we apply our theorem to $u'_{|V_1}$ and get the following.

Corollary. *In the assumptions of the above theorem, drop the non-degeneracy of (V, Q). Let $\{e_1^0, \cdots, e_r^0\}$ be an arbitrary base of the radical V', then it can be extended by $\{e_1, \cdots, e_m, e_1', \cdots, e'_m\}$ to a base of V which together with some $\sigma\in O(V, Q)$ satisfies the following:*

$$\sigma u(e_i) = e_i', \quad \sigma u(e_i') = \mu e_i \ \ i = 1, \cdots, m, \ \ \sigma u(e_i^0) = e_i^0 \ \textit{for} \ i = 1, \cdots, r.$$

Now we start to the proof of Theorem with a series of elementary lemmas, where the second one is quite obvious.

Lemma 1. *If k has at least three elements, and if Φ is not identically zero on $V\times V$, then we can find a pair of vectors x and y in V, such that*

$$Q(x)Q(y)\Phi(x, y) \neq 0 .$$

Proof. Since Φ is not identically O, we can find $x, y\in V$ such $\Phi(x, y)=a\neq 0$. If $Q(x)Q(y)\neq 0$, we have nothing to prove. Suppose $Q(y)=0$. Then, for any $\xi, \eta\in k$, we have $Q(x+\xi y)=Q(x)+\xi a$, $Q(x+\eta y)=Q(x)+\eta a$ and $\Phi(x+\xi y, x+\eta y)=2Q(x)+(\xi+\eta)a$. Let $b=a^{-1}Q(x)$, c and d be three distinct elements of k. If $c+d\neq 2b$, we choose ξ and η as $\xi=c$, $\eta=d$. If $c+d=2b$, then $2d=(d+c)-(c-d)\neq 2b$ and we choose as $\xi=\eta=d$. Then replace the pair x, y by $x+\xi y$, $x+\eta y$, and the latter has the required properties.

Lemma 2. *Let (V, Q) be a quadratic space [non-degenerate or not], and W be a subspace of V. If the restriction $\Phi_{|W\times W}$ of Φ on W is non-degenerate, i.e. $(W, Q_{|W})$ is strongly non-degenerate, then*

$$V = W+W^{\perp} \quad \textit{and} \quad W\cap W^{\perp} = \{0\} .$$

Lemma 3. *Suppose Φ is not identically 0 on $V\times V$, and there exists a similitude $u\in GO(V, Q)$ with a non-square multiplicator μ, then we can find a vector e of V and a symmetry σ such that $\Phi(e, \sigma u(e))\neq 0$.*

Furthermore let W be a subspace of V spanned by thus chosen e and $\sigma u(e)$, then $(W, Q_{|W})$ is storongly non-degenerate.

Proof. Suppose our first statement is false, i.e. $\Phi(x, \sigma u(x))=0$ for any $x\in V$ and any symmetry σ. Then for any $x, y\in V$, $0=\Phi(\sigma u(x)+y,\ \sigma u(\sigma u(x)+y))=\Phi(\sigma u(x),\ \sigma u(y))+\Phi(y,\ (\sigma u)^2 x)$ $=\Phi(y,\ \mu x+(\sigma u)^2 x)$, i.e. $\mu x+(\sigma u)^2 x\in V^{\perp}$. In other words, denoting by h_μ the homothecy, Image $(h_\mu+(\sigma u)^2)\subset V^{\perp}$. In particular, Image $(h_\mu+u^2)\subset V^{\perp}$. Hence, Image $((\sigma u)^2-u^2)\subset V^{\perp}$, or equivalently,

$$\text{Image}\,(\sigma u-u\sigma^{-1})\subset V^{\perp} \qquad \cdots\cdots\cdots\cdots(1)$$

Since the existence of non-square μ eliminates the possibility that

k has only two elements, we can take x and y as in Lemma 1. By the definition, the symmetry σ_y with respect to y is given by $\sigma_y(z)=z-Q(y)^{-1}\Phi(z, y)y$ for any $z\in V$. Hence we have $(\sigma_y u-u\sigma_y)x =Q(y)^{-1}\Phi(x, y)(u(y)-\Phi(x, y)^{-1}\Phi(u(x), y)y)$. Putting $c=\Phi(x, y)^{-1} \times\Phi(u(x), y)$, the above (1) implies

$$u(y)-cy\in V^{\perp}, \tag{2}$$

Now, $\mu\Phi(x, y)=\Phi(u(x), u(y))$ is equal to $\Phi(u(x), cy)$ by (2), we get $\mu\Phi(x, y)=c\Phi(u(x), y)=c^2\Phi(x, y)$ i.e. $\mu=c^2$, a contradiction.

To prove the second statement, the matrix of Φ with respect to the base $\{e, \sigma u(e)\}$ should be computed, and it is equal to $(2Q(e))^2\mu-(\Phi(e, \sigma u(e))^2$ which never vanish since μ is not a square.

Lemma 4. *Snppose (V, Q) be non-degenerate, and Φ be identically zero i.e. $V=V^{\perp}$. Let u be a similitude with a non-square multiplicator μ, then $u^2(x)=\mu x$ for any $x\in V$. Furthermore V admits a base S of the form $S=\{e_1, u(e_1), \cdots, e_m, u(e_m)\}$, thus dim $V=2m$.*

Proof. Our assumptions on (V, Q) implies that the characteristic of k is two and V has no singular vector other than 0. Since $Q(u^2(x)-\mu(x)=Q(u^2(x))-\mu^2Q(x)=0$, we get $u^2(x)=\mu x$ for any $x\in V$.

Let $S=\{e_1, u(e_1), \cdots, e_m, u(e_m)\}$ be a set of vectors with the following two properties. (i) S is linearly independent. (ii) S is maximal among such sets, namely $\{x, u(x)\}\cap S$ is not linearly independent for any $x\in V$. Such a set S certainly exists, and what we need to prove is that S spans V.

For any $x\in V$, we have a non-trivial relation $\xi x+\eta u(x)=\sum_{i=1}^{m} \times(\xi_i e_i+\eta_i u(e_i))$ with ξ or η to be non-zero. Setting $\zeta=\xi+\eta\sqrt{\mu}$, $\zeta_i=\xi_i+\eta_i\sqrt{\mu}$ for $i=1, \cdots, m$ and applying Q to the both sides of the above equation, we get $\zeta^2Q(e)=\sum_{i=1}^{m}\zeta_i^2Q(e_i)$, hence $Q(e)=\sum_{i=1}^{m}(\zeta^{-1}\zeta_i)^2 \times Q(e_i)$. Set $\zeta^{-1}\zeta_i=\xi_i'+\eta_i'\sqrt{\mu}$, then $Q(e)=\sum_{i=1}^{m}(Q(\xi_i'e_i)+Q(\eta_i'u(e_i)))$, hence $e=\sum_{i=1}^{m}(\xi_i'e_i+\eta_i'u(e_i))$.

Proof of Theorem. We proceed by the induction on $d(V)$

$=dim\, V - dim\, V^{\perp}$. When $d(V)=0$, the situation is that of Lemma 4, we can take $\sigma=1$ and $u(e_i)$ of lemma as e_i' of the theorem for $i=1, \cdots, m$.

Suppose $d(V)>0$, i.e. Φ is not identically zero, and let e, σ and W be that we have got in Lemma 3. By Lemma 2, we have $V=W+W^{\perp}$, $W\cap W^{\perp}=\{0\}$. Let u_1 denote the composite σu, it is a similitude with the same multiplicator μ as u. Let $\tilde{\sigma}: u_1(W)\to W$ be a linear isomorphism defined by $\tilde{\sigma}: u_1^2(e)\mapsto \mu e$, $u_1(e)\mapsto u_1(e)$. Since $Q(u_1^2(e))=Q(\mu e)$, $\Phi(u_1^2(e), u_1(e))=\Phi(\mu e, u_1(e))$ and since $u_1(W)\cap V^{\perp}=u_1(W\cap V^{\perp})=\{0\}$, by Witt theorem $\tilde{\sigma}$ can be extended to a rotation $\sigma_1\in O(V, Q)$.

Since $\sigma_1 u_1(e)=u_1(e)$, $\sigma_1 u_1(u_1(e))=\mu e$, $\sigma_1 u_1$ stabilizes W hence $W^{\perp}$. If $dim W^{\perp}>0$, the restriction $\sigma_1 u_{1|W^{\perp}}$ of $\sigma_1 u_1$ to $W^{\perp}$ is a similitude of the quadratic space $(W^{\perp}), Q_{|W^{\perp}})$ with the same multiplicator μ. Hence, by the induction assumption, $dim\, W^{\perp}$ is even $(=2(m-1))$ and $W^{\perp}$ admits a base $\{e_2, \cdots, e_m, e_2', \cdots, e_m'\}$ such that $\sigma_1 u_1(e_i)=e_i'$, $\sigma_1 u_1(e_i')=\mu e_i$ for $i=2, \cdots, m$. By putting $e_1=e$ and $e_1'=\sigma_1 u_1(e)$, we have completed the proof.

KYOTO UNIVERSITY
UNIVERSITY OF OSAKA PREFECTURE