

Title	A note on the orthogonal group of a quadratic module of rank two over a commutative ring
Author(s)	Kanzaki, Teruo
Citation	Osaka Journal of Mathematics. 1973, 10(3), p. 607-609
Version Type	VoR
URL	<a href="https://doi.org/10.18910/3711">https://doi.org/10.18910/3711</a>
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

## A NOTE ON THE ORTHOGONAL GROUP OF A QUADRATIC MODULE OF RANK TWO OVER A COMMUTATIVE RING

TERUO KANZAKI

(Received April 24, 1973)

Let  $A$  be an arbitrary commutative ring with the identity element. This note will give an elementary property on the orthogonal group of a non-degenerate quadratic  $A$ -module of rank two. Throughout this paper, we will assume that  $(V, q)$  is a non-degenerate quadratic  $A$ -module such that  $V$  is a finitely generated projective  $A$ -module and  $[V_m: A_m]=2$  for all maximal ideal  $m$  of  $A$ . The Clifford algebra  $C(V, q)$  is a quadratic extension of  $C_0(V, q)$ , the set of homogeneous elements of degree 0 in  $C(V, q)$ , and  $C_0(V, q)$  is a commutative and separable quadratic extension of  $A$  (cf. [3], [4]). Set  $B=C_0(V, q)$ .  $B$  is a Galois extension of  $A$  with a Galois group  $G=\{I, \tau\}$ , and  $\tau$  is the unique  $A$ -algebra automorphism of  $B$  such that the fixed subring of  $B$  is  $A$  ([4], [5]). By [3],  $V$  is an invertible  $B$ -bimodule, and  $(V, \phi)$ ,  $\phi: V \times V \rightarrow B$ ;  $\phi(x, y)=xy$  in  $C(V, q)$  for  $x, y \in V$ , is a non-degenerate hermitian  $B$ -module ((2.4) in [3]). We denote by  $I(A)$  the set of idempotents in  $A$ , which is an abelian group with respect to the product  $*$ ;  $e * e' = e + e' - 2ee'$  for  $e, e' \in I(A)$ . Then, by [1], the group  $\text{Aut}(B/A)$  of all  $A$ -algebra automorphisms of  $B$  is  $\{e\tau + (1-e)I; e \in I(A)\}$ , and is isomorphic to  $I(A)$  by the isomorphism  $\mu: I(A) \rightarrow \text{Aut}(B/A); e \mapsto \mu = e\tau + (1-e)I$ . Let  $O(V, q)$  be the orthogonal group of  $(V, q)$ , i.e.  $O(V, q) = \{\rho \in \text{Hom}_A(V, V); q(\rho v) = q(v) \text{ and } \rho(V) = V\}$ . For any  $\rho \in O(V, q)$ ,  $\rho$  is extended to an  $A$ -algebra automorphism  $\tilde{\rho}$  of  $C(V, q)$  which induces an automorphism of  $B$ . Accordingly, there exists a group homomorphism  $\eta: O(V, q) \rightarrow I(A); \rho \mapsto \mu^{-1}(\rho|B)$ . We put  $O^+(V, q) = \{\rho \in O(V, q); \rho|B=I\}$  and  $O^-(V, q) = \{\rho \in O(V, q); \tilde{\rho}|B \neq I\}$ .

REMARK 1. Let  $V$  be a free  $A$ -module with the basis  $\{u, v\}$ ,  $V=Au \oplus Av$ . For  $\rho \in O(V, q)$ , let  $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  denote the matrix of  $\rho$  with respect to the basis  $\{u, v\}$ . Then  $(\det \rho)^2 = 1$ . If  $\rho$  is in  $O^+(V, q)$  then  $\det \rho = 1$ . If  $\tilde{\rho}|B = \tau$  then  $\det \rho = -1$ .

Proof. Since  $C(V, q) = A \oplus Au v \oplus Au \oplus Av$  and  $B = A \oplus Au v$ , we have  $\tilde{\rho}(uv) = (au + bv)(cu + dv) = B_q(cu, bv) + acq(u) + bdq(v) + (\det \rho)uv$ . Since  $(uv)^2 = B_q(u, v)uv - q(u)q(v)$ , we have  $B = C^+(V, q) = (A, B_q(u, v), -1)$  and  $\tau(uv) = B_q(u, v)$

$-uv$  (cf. Proposition 3 in [2]). If  $\tilde{\rho}|B=I$  then  $\det \rho=1$  and  $B_q(cu, bv)+acq(u)+bdq(v)=0$ . If  $\tilde{\rho}|B=\tau$  then  $\det \rho=-1$  and  $(cb-1)B_q(u, v)+acq(u)+bdq(v)=0$ .

Let  $N: U(B)\rightarrow U(A)$  be a group homomorphism of the unit group of  $B$  to the unit group of  $A$  defined by  $N(b)=b\tau(b)$ .

**Proposition 1.**  $O^+(V, q)$  is an abelian group, and is isomorphic to  $\text{Ker } N$ .

Proof. Since  $C(V, q)=B\oplus V$  and  $V$  is an invertible  $B$ -bimodule, if  $\rho$  is in  $O^+(V, q)$ , then  $\tilde{\rho}|B=I$ , and  $\tilde{\rho}|V=\rho$  induces an isometry of the hermitian  $B$ -module  $(V, \phi)$  onto itself, hence there exists an element  $b$  in  $U(B)$  such that  $\rho(v)=bv$  for all  $v\in V$ . Accordingly,  $\phi(x, y)=\phi(\rho(x), \rho(y))=\phi(bx, by)=b\tau(b)\phi(x, y)=N(b)\phi(x, y)$ , and we have  $N(b)=1$ , since  $B$  is generated by  $\phi(V, V)$ . The correspondence  $\rho \rightsquigarrow b$  is a group monomorphism of  $O^+(V, q)$  to  $\text{Ker } N$ . Conversely, for any  $b$  in  $\text{Ker } N$ , it is easily obtained that  $b$  induces an isometry of  $(V, q)$  onto itself. Therefore,  $O^+(V, q)\approx \text{Ker } N$ .

**Corollary 1.**  $O(V, q)=\bigcup_{\tilde{\rho}_e|B=\mu_e\in \text{Aut}(B/A)} \rho_e \circ O^+(V, q)$  and the following sequence is exact;

$$(1) \longrightarrow \text{Ker } N \longrightarrow O(V, q) \xrightarrow{\eta} I(A).$$

**Proposition 2.** Let  $\rho_0$  be an element in  $O^-(V, q)$  such that  $\tilde{\rho}_0|B=\tau$ . Then, there exist  $\alpha$  in  $A$  such that  $\rho_0^2=\alpha I$  and  $\alpha^2=1$ . For every  $\rho\in O^-(V, q)$  such that  $\tilde{\rho}|B=\tau$ , we have  $\rho^2=\rho_0^2=\alpha I$ .

Proof. Let  $\rho_0$  be an element in  $O^-(V, q)$  such that  $\tilde{\rho}_0|B=\tau$ ,  $\rho_0^2$  is in  $O^+(V, q)$ , hence there is  $\alpha$  in  $\text{Ker } N$  such that  $\rho_0^2(v)=\alpha v$  for all  $v\in V$ . Since  $\alpha\rho_0(v)=\rho_0^3(v)=\rho_0(\alpha v)=\tau(\alpha)\rho_0(v)$  for all  $v\in V$  and  $V$  is faithful over  $B$ , we have that  $\tau(\alpha)=\alpha$  is in  $B^\tau=A$  and  $\alpha^2=N(\alpha)=1$ . For any  $\rho\in O^-(V, q)$  such that  $\tilde{\rho}|B=\tau$ ,  $\rho\circ\rho_0^{-1}$  is in  $O^+(V, q)$ , and so there exists  $b$  in  $\text{Ker } N$  such that  $\rho(v)=b\rho_0(v)$  for all  $v\in V$ . Accordingly, we have  $\rho^2=b\rho_0b\rho_0=b\tau(b)\rho_0^2=\rho_0^2$ .

**Corollary 2.** If  $A$  has no idempotents other than 0 and 1, and if  $O(V, q)\neq O^+(V, q)$ , then there exists  $\alpha$  in  $U(A)\cap \text{Ker } N$  such that  $\rho^2=\alpha I$  for every  $\rho$  in  $O^-(V, q)$ . Furthermore, if 2 is invertible in  $A$ , then  $\alpha=1$ .

Proof. We assume that  $A$  has no idempotents other than 0 and 1,  $\frac{1}{2}$  is in  $A$ , and  $O^-(V, q)\neq \phi$ . Since  $\text{Aut}(B/A)=G=\{I, \tau\}$ , there exists  $\alpha$  in  $A$  such that  $\alpha^2=1$  and  $\rho^2=\alpha I$  for every  $\rho\in O^-(V, q)$ .  $\frac{1+\alpha}{2}$  becomes an idempotent in  $A$ . Therefore,  $\frac{1+\alpha}{2}$  is 1 or 0, that is,  $\alpha$  is 1 or  $-1$ . We will show  $\alpha=1$ . Assume  $\alpha=-1$ . For any maximal ideal  $m$  of  $A$ , we consider the localization  $(V_m, q_m)$

$=A_m u \oplus A_m v$ , and the induced isometry  $\rho$  on  $(V_m, q_m)$  for  $\rho \in O^-(V, q)$ . Let  $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  denote the matrix of  $\rho$  with respect to the basis  $u, v$ . For the fact that  $\det \rho = ad - bc = -1$  and  $\begin{pmatrix} a & b \\ d & c \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ , we obtain that  $a(a+d) = -2$  and  $b=c=0$ , and so  $\rho(u) = au$  and  $a^2 = -1$ . Accordingly,  $q_m(u) = q_m(\rho(u)) = q_m(au) = a^2 q_m(u) = -q_m(u)$ . Since we can choose  $u$  such that  $q_m(u) \neq 0$ , this is a contradiction. Consequently,  $\alpha = 1$ .

**Proposition 3.** *Let  $A$  be a commutative ring such that  $A$  has no idempotents other than 0 and 1, 2 is invertible in  $A$ . If  $O(V, q) \neq O^+(V, q)$ , then for every  $\rho \in O^-(V, q)$ , there exists an invertible  $A$ -submodule  $U$  of  $V$  such that  $\rho|U = -I, \rho|U^\perp = I$  and  $V = U \oplus (U)^\perp$ .*

*Proof.* If  $\rho$  is in  $O^-(V, q)$ , by Corollary 2,  $\rho^2 = I$ , hence we have that  $\frac{I-\rho}{2}$  and  $\frac{I+\rho}{2}$  are idempotents and  $I = \frac{I-\rho}{2} + \frac{I+\rho}{2}$ . Since  $\rho|B = \tau$ , we have  $\rho \neq I$ , hence  $\frac{I-\rho}{2}$  is neither 0 nor  $I$ . This mention is held for the localization with respect to every maximal ideal of  $A$ . Therefore,  $U = \frac{I-\rho}{2}(V)$  and  $U' = \frac{I+\rho}{2}(V)$  are finitely generated projective  $A$ -modules of rank one, and we can check that  $U$  and  $U'$  are mutually orthogonal,  $V = U \oplus U'$  and  $U' = U^\perp$ . Since  $\rho \circ \frac{I-\rho}{2} = -\left(\frac{I-\rho}{2}\right)$  and  $\rho \circ \frac{I+\rho}{2} = \frac{I+\rho}{2}$ , we have  $\rho|U = -I, \rho|U' = \rho|U^\perp = I$  and  $V = U \oplus U^\perp$ .

**REMARK 2.** Let  $A$  be as Proposition 3. If we call such an isometry in Proposition 3 a symmetry of  $(V, q)$ , then  $O(V, q)$  is an abelian group having no symmetries, or every element of  $O(V, q)$  is a product of one or two symmetries.

OSAKA CITY UNIVERSITY

---

**References**

- [1] S.U. Chase, D.K. Harrison and A. Rosenberg: *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 15-33.
- [2] T. Kanzaki: *On the quadratic extensions and the extended Witt ring of a commutative ring*, Nagoya Math. J. **49** (1973), 127-141.
- [3] T. Kanzaki: *On non-commutative quadratic extensions of a commutative ring*, Osaka J. Math. **10** (1973), 597-605.
- [4] A. Micali and O.E. Villamayor: *Sur les algebres de Clifford. II*, J. Reine Angew. Math. **242** (1970), 61-90.
- [5] C. Small: *The group of quadratic extensions*, J. Pure Appl. Algebra **2** (1972), 83-105.

