Kanzaki, T.
Osaka J. Math.
13 (1976), 503–512

NOTE ON QUATERNION ALGEBRAS OVER A COMMUTATIVE RING

Dedicated to Professor Mutsuo Takahashi on his 60th birthday

TERUO KANZAKI

(Received September 10, 1975)

Let R be a commutative ring. In [3] we defined a generalization $D(B, V, \varphi)$ of quaternion algebra over R. In this note we use a notation $\left(\frac{B,\varphi}{R}\right)$ instead of $D(B, V, \varphi)$, where $\varphi=(V, \varphi)$. The first object in this paper is to show the following generalizations of the well known classical formulas;

$$\left(\frac{B,\varphi}{R}\right)\otimes_R\left(\frac{B,\varphi'}{R}\right)\sim\left(\frac{B,\varphi\otimes\varphi'}{R}\right),$$

$$\left(\frac{B, i_B\circ\varphi_0}{R}\right)\otimes_R\left(\frac{B', i_{B'}\circ\varphi_0}{R}\right)\sim\left(\frac{B^*B', i_{B*B'}\circ\varphi_0}{R}\right)$$ for a symmetric bilinear R-module $\varphi_0=(U, \varphi_0)$. From the formulas, it is deduced that every element in Quat (R), the subgroup of Brauer group generated by quaternion algebras, is expressed as $\left[\frac{B_1,\varphi_1}{R}\right]\left[\frac{B_2,\varphi_2}{R}\right]\cdots\left[\frac{B_n,\varphi_n}{R}\right]$ for $n<|Q_s(R)|$, where $Q_s(R)$ is the quadratic extension group. The second object is to investigate on a quaternion R-algebra $\left(\frac{B,\varphi}{R}\right)$ such that $\left(\frac{B,\varphi}{R}\right)\sim R$. We shall show that if $\left(\frac{B,\varphi}{R}\right)\sim R$ then φ is R-free i.e. $\varphi=\langle a\rangle$ for some unit a in R, furthermore, if 2 is invertible in R then $\left(\frac{B,\varphi}{R}\right)\sim R$ implies $\left(\frac{B,\varphi}{R}\right)\cong\left(\frac{a,b}{R}\right)$ for some unite a and b in R, i.e. R-free quaternion algebra. Finally, we give a condition for $\left(\frac{B,\varphi}{R}\right)$ to be $\left(\frac{B,\varphi}{R}\right)\cong R_2$; $\left(\frac{B,\varphi}{R}\right)$ is isomorphic to a matrix ring R_2 if and only if there is a quadratic extension B' of R such that $[B']$ is identity element in $Q_s(R)$ and $\left(\frac{B,\varphi}{R}\right)\supset B'\supset R$. Particularly, if 2 is invertible in R, we have some equivalent conditions for $\left(\frac{B,\varphi}{R}\right)\cong R_2$, and as a corollary we have $\mathrm{Hom}_R(B, B)\cong R_2$ for every $[B]$ in $Q_s(R)$. Throughout this paper, we assume that R is a commutative ring, every ring has identity element, and every subring and extension ring of a ring have a common identity element.

1. Definitions and preliminary

Let B be an extension ring of R. If the residue R-bimodule B/R is invertible, then B is called a quadratic extension of R. As well known, if B is an R-algebra and quadratic extension of R then B is commutative (cf. [8]). And, if B is a separable commutative quadratic extension, then $B\supset R$ is a Galois extension with Galois group $G=\{I, \tau\}$, where τ is characterized as the unique R-algebra automorphism of B such that $B^{\tau}(=\{b\in B; \tau(b)=b\})=R$ (cf. [8]). Then every R-algebra automorphism of B is expressed as $e\tau+(1-e)I$ for some idempotent e in R and identity map I on B, and is an involution (cf. [4]). Therefore, we shall call the automorphism τ the main involution of B, and denote it by $\tau(b)=\bar{b}$ for $b\in B$. For a separable commutative quadratic extension $B\supset R$, we consider a hermitian left B-module $\varphi=(V, \varphi)$ defined by a finitely generated projective left B-module V and a hermitian form φ: $V\times V\to B$, satisfied $\varphi(v, v')=\overline{\varphi(v', v)}$ and $\varphi(au+bv, v')=a\,\varphi(u, v')+b\,\varphi(v, v')$ for $u, v, v'\in V$ and $a, b\in B$. When V is an invertible left B-module, we shall call $\varphi=(V, \varphi)$ a rank one hermitian left B-module. If $\varphi_i=(V_i, \varphi_i)$, $i=1,2$ are hermitian left B-modules, then the tensor product $\varphi_1\otimes\varphi_2=(V_1\otimes_B V_2, \varphi_1\otimes\varphi_2)$ is a hermitian left B-module defined by $\varphi_1\otimes\varphi_2$: $V_1\otimes_B V_2\times V_1\otimes_B V_2\to B$; $(b_1\otimes b_2, b_1'\otimes b_2')\rightsquigarrow \varphi_1(b_1, b_1')\varphi_2(b_2, b_2')$. If $\varphi_0=(U, \varphi_0)$ is a symmetric bilinear left R-module, then $i_B\circ\varphi_0=(B\otimes_R U, i_B\circ\varphi_0)$ is a hermitian left B-module defined by $i_B\varphi_0(b\otimes u, b'\otimes u')=b\,\varphi_0(u, u')\bar{b}'$ for $b\otimes u$, $b'\otimes u'$ in $B\otimes_R U$. A ring D is called a quaternion R-algebra if D satisfies the following conditions;

1) D is an Azumaya R-algebra,

2) there is a subring B of D such that $D\supset B$ is a quadratic extension and $B\supset R$ is a separable quadratic extension.

If D is a quaternion R-algebra and B is such a subring of D as above definition, then B is a maximal commutative subring of D and there is a rank one non degenerate hermitian left B-module $\varphi=(V, \varphi)$ such that $D=B\oplus V$ and the multiplication in D is characterized by $(b+v)(b'+v')=bb'+bv'+\bar{b}'v+\varphi(v, v')$ for $b+v$, $b'+v'\in B\oplus V$, (cf. [3]) Then D is denoted by $\left(\frac{B, \varphi}{R}\right)$. In the Brauer group $B(R)$ of R, we denote by n Quat(R) the subgroup of $B(R)$ generated by classes of quaternion R-algebras. We define an integer $L_Q(R)$ as follows; for any integer n, $L_Q(R)\leqq n$ if and only if every element of Quat (R) is expressed as a class of a tensor product of m quaternion R-algebras for some integer $m\leqq n$.

The set $Q_s(R)$ of isomorphism classes $[B]$'s of separable commutative quadratic extensions B's of R is an abelian group under the product $[B_1][B_2]=[B_1*B_2]$, where $B_1*B_2=(B_1\otimes_R B_2)^{\tau_1\times\tau_2}$ for the main involution τ_i of B_i, $i=1, 2$. The identity element of $Q_s(R)$ is $[R\times R]$, (cf. [8]).

2. Tensor product of quaternion R-algebras

In [3] we showed that a quaternion R-algebra $\left(\frac{B,\varphi}{R}\right)$ is a generalized crossed product of B and $G=G(B/R)=\{I,\tau\}$. Using an idea of Hattori [2], we have

Theorem 1. *We have Brauer equivalence*

$$\left(\frac{B,\varphi_1}{R}\right)\otimes_R\left(\frac{B,\varphi_2}{R}\right)\sim\left(\frac{B,\varphi_1\otimes\varphi_2}{R}\right).$$

Proof. Let $G=\{I,\tau\{$ be the Galois group of $B\supset R$, and $x_1,\cdots x_n, y_1,\cdots y_n$ a G-Galois system of B, i.e. it satisfies $\sum_i x_iy_i=1$, $\sum_i x_i\tau(y_i)=0$ in B. Then $e_1=\sum_i x_i\otimes y_i$ and $e_2=\sum_i x_i\otimes\tau(y_i)=\sum_i\tau(x_i)\otimes y_i=1\otimes 1-e_1$ are orthgonal idempotents in $\left(\frac{B,\varphi_1}{R}\right)\otimes_R\left(\frac{B,\varphi_2}{R}\right)$. It is known that

$$\left(\frac{B,\varphi_1}{R}\right)\otimes_R\left(\frac{B,\varphi_2}{R}\right)\sim e_1\left(\left(\frac{B,\varphi_1}{R}\right)\otimes_R\left(\frac{B,\varphi_2}{R}\right)\right)e_1=e_1((B\oplus V_1)\otimes_R(B\oplus V_2))e_1$$

$=e_1(B\otimes_R B)e_1\oplus e_1(B\otimes_R V_2)e_1\oplus e_1(V_1\otimes_R B)e_1\oplus e_1(V_1\otimes_R V_2)e_1=e_1(B\otimes_R B)\oplus e_1$ $(V_1\otimes_R V_2)\cong B\oplus V_1\otimes_B V_2=\left(\frac{B,\varphi_1\otimes\varphi_2}{R}\right)$, where $\varphi_i=(V_i,\varphi_i)$ $i=1,2$.

Theorem 2. *Let $\varphi_0=(U,\varphi_0)$ be a rank one non degenerate symmetric bilinear R-module. Then we have*

$$\left(\frac{B_1, i_{B_1}\circ\varphi_0}{R}\right)\otimes_R\left(\frac{B_2, i_{B_2}\circ\varphi_0}{R}\right)\cong\left(\frac{B_1*B_2, i_{B_1*B_2}\circ\varphi_0}{R}\right)\otimes_R\left(\frac{B_1, i_{B_1}\circ\varphi_0\otimes\varphi_0}{R}\right),$$

and

$$\left(\frac{B_1, i_{B_1}\circ\varphi_0\otimes\varphi_0}{R}\right)\cong\left(\frac{B_1, (i_{B_1}\circ\varphi_0)\otimes(i_{B_1}\circ\varphi_0)}{R}\right)\cong\mathrm{Hom}_R(B_1, B_1)\sim R.$$

Proof. From the definition of $\left(\frac{B, i_B\circ\varphi_0}{R}\right)$, we can put $\left(\frac{B_1, i_{B_1}\circ\varphi_0}{R}\right)=B_1\oplus B_1\otimes_R U$, $\left(\frac{B_2, i_{B_2}\circ\varphi_0}{R}\right)=B_2\oplus B_2\otimes_R U$, and the tensor product $D=\left(\frac{B_1, i_{B_1}\circ\varphi_0}{R}\right)\otimes_R\left(\frac{B_2, i_{B_2}\circ\varphi_0}{R}\right)=B_1\otimes_R B_2\oplus B_1\otimes_R B_2\otimes_R U\oplus B_1\otimes_R U\otimes_R B_2\oplus B_1\otimes_R U\otimes_R B_2\otimes_R U$. Since B_1*B_2 is a subring of $B_1\otimes_R B_2$, $D=\left(\frac{B_1, i_{B_1}\circ\varphi_0}{R}\right)\otimes_R\left(\frac{B_2, i_{B_2}\circ\varphi_0}{R}\right)$ contains $D_1=B_1*B_2\oplus(B_1*B_2)\otimes_R U=\left(\frac{B_1*B_2, i_{B_1*B_2}\circ\varphi_0}{R}\right)$ and $D_2=B_1\otimes_R R\oplus B_1\otimes_R U\otimes_R R\otimes_R U\cong\left(\frac{B_1, i_{B_1}\circ\varphi_0\otimes\varphi_0}{R}\right)$ as subrings. Every element of $B_1*B_2=(B_1\otimes_R B_2)^{\tau_1\times\tau_2}$ commutes with every element of $B_1\otimes_R U\otimes_R B_2\otimes_R U$, therefore $(B_1*B_2)\otimes_R U$ and $B_1\otimes_R U\otimes_R R\otimes_R U$ commute elementwise, and so are $B_1\otimes_R R$

and $(B_1 * B_2)\otimes_R U$. Accordingly, subrings D_1 and D_2 of D commute elementwise, and so a ring homomorphism $D_1\otimes_R D_2 \to D$ is defined by the contraction. Using the following lemma and the fact that $D_1\otimes_R D_2$ and D are Azumaya R-algebras, we can check that $D_1\otimes_R D_2\to D$ is an isomorphism. Namely, since $(B_1\otimes_R R)(B_1 * B_2)=(B_1\otimes_R B_2)^{I\times\tau_2}(B_1\otimes_R B_2)^{\tau_1\times\tau_2}=B_1\otimes_R B_2$, we have $D_1 D_2=D$. From the definition of hermitian module, we have $i_{B_1}\circ(\varphi_0\otimes\varphi_0)\cong(i_{B_1}\circ\varphi_0)\otimes(i_{B_1}\circ\varphi_0)$, therefore by [3], (2.10), we have $\left(\frac{B_1,\, i_{B_1}\circ(\varphi_0\otimes\varphi_0)}{R}\right)\cong \mathrm{Hom}_R(B\otimes_R U,\, B\otimes_R U)\cong \mathrm{Hom}_R(B,\, B)\sim R$.

Lemma 1. *Let $A\supset B$ be a G-Galois extension of commutative rings. If G is a direct product of normal subgroups G_1 and G_2, then we have*

$$A=A^{G_1}A^{G_2}\cong A^{G_1}\otimes_B A^{G_2}\,.$$

Proof. This is obtained immediately from Theorem 3.4 in [1] applying to the contract ring homomorphism $A^{G_1}\otimes_B A^{G_2}\to A$.

Lemma 2. *Let B_1 and B_2 be separable commutative quadratic extensions such that $[B_1]=[B_2]$ in $Q_s(R)$, and σ: $B_1\to B_2$ an R-algebra isomorphism. If $\varphi_1=(V_1,\varphi_1)$ and $\varphi_2=(V_2,\varphi_2)$ are rank one non degenerate hermitian left B_1- and B_2-modules, respectively, such that there is a σ-semi-linear isomorphism h: $V_1\to V_2$ making the following diagram commut;*

$$\begin{array}{ccc} V_1\times V_1 & \xrightarrow{h\times h} & V_2\times V_2 \\ \downarrow{\scriptstyle\varphi_1} & & \downarrow{\scriptstyle\varphi_2} \\ B_1 & \xrightarrow{\sigma} & B_2 \end{array}$$

then there is an R-algebra isomorphism f: $\left(\frac{B_1,\,\varphi_1}{R}\right)\to\left(\frac{B_2,\,\varphi_2}{R}\right)$, and f induces σ and h on B_1 and V_1 respectively.

Proof. From the definitions of $\left(\frac{B_i,\,\varphi_i}{R}\right)$ $i=1, 2$, f is immediately defined by σ and h, (cf. [5], Prop. 3).

Propsotion 1. *Let $\left(\frac{B_1,\,\varphi_1}{R}\right)$ and $\left(\frac{B_2,\,\varphi_2}{R}\right)$ be quaternion algebras such that $[B_1]=[B_2]$ in $Q_s(R)$. Then there is a quaternion R-algebra $\left(\frac{B_1,\,\varphi_2'}{R}\right)$ such that $\left(\frac{B_1,\,\varphi_2'}{R}\right)\cong\left(\frac{B_2,\,\varphi_2}{R}\right)$. Therefore, we have*

$$\left(\frac{B_1,\,\varphi_1}{R}\right)\otimes_R\left(\frac{B_2,\,\varphi_2}{R}\right)\sim\left(\frac{B_1,\,\varphi_1\otimes\varphi_2'}{R}\right),\ \textit{provided } [B_1]=[B_2] \textit{ in } Q_s(R)\,.$$

Proof. Suppose $[B_1]=[B_2]$ in $Q_s(R)$. There is an R-algebra isomorphism $\sigma: B_2 \to B_1$. Then, by change of ring, there is a rank one non degenerate hermitian B_1-module $\varphi_2'=(B_1\otimes_{B_2}V_2, \sigma\varphi_2)$ for $\varphi_2=(V_2, \varphi_2)$. From σ and a σ-semilinear isomorphism $h: V_2 \to B_1\otimes_{B_2}V_2$; $v \leadsto 1\otimes v$, one can construct an R-algebra isomorphism $f: \left(\frac{B_2, \varphi_2}{R}\right) \to \left(\frac{B_1, \varphi_2'}{R}\right)$ by Lemma 2. Accordingly, by Theorem 1 we have $\left(\frac{B_1, \varphi_1}{R}\right)\otimes_R\left(\frac{B_2, \varphi_2}{R}\right)\simeq\left(\frac{B_1, \varphi_1}{R}\right)\otimes_R\left(\frac{B_1, \varphi_2'}{R}\right)\sim\left(\frac{B_1, \varphi_1\otimes\varphi_2'}{R}\right)$.

Let us denote by $|Q_s(R)|$ the cardinal number of the set $Q_s(R)$.

Theorem 3. *We have*

$$L_Q(R)\leqq |Q_s(R)|-1\ .$$

Proof. Suppose $|Q_s(R)|=n<\infty$, and $Q_s(R)=\{[B_0]=1, [B_1], \cdots [B_{n-1}]\}$. By Proposition 1, every element $[A]$ in Quat(R) is expressed as $A\sim\left(\frac{B_1, \varphi_1}{R}\right)\otimes_R \left(\frac{B_2, \varphi_2}{R}\right)\otimes\cdots\otimes_R\left(\frac{B_{n-1}, \varphi_{n-1}}{R}\right)$ for suitable $\varphi_1, \varphi_2, \cdots \varphi_{n-1}$.

3. Quaternion algebra of split type

Theorem 4. *For any quaternion R-algebra $\left(\frac{B, \varphi}{R}\right)$, if $\left(\frac{B, \varphi}{R}\right)\sim R$ then $\varphi=(V, \varphi)$ is R-free, i.e. there is a unit a in R such that $\varphi=\langle a\rangle$. Then $\left(\frac{B, \varphi}{R}\right)$ is denoted by $\left(\frac{B, a}{R}\right)$.*

Proof. Put $\left(\frac{B, \varphi}{R}\right)=B\oplus V$, $\varphi=(V, \varphi)$. Then $VV=B$ in $\left(\frac{B, \varphi}{R}\right)$, (cf. [3], (2.1)). Suppose $\left(\frac{B, \varphi}{R}\right)\simeq \mathrm{Hom}_R(P, P)$ for a finitely generated projective and faithful R-module P. Then, P may be regarded as a faithful left $\left(\frac{B, \varphi}{R}\right)$-module and also a faithful B-module. Since B is a maximal commutative subring of $\left(\frac{B, \varphi}{R}\right)=\mathrm{Hom}_R(P, P)$, P becomes an invertible left B-module. From $VV=B$, we have $P=VP\simeq V\otimes_B P$. Since P is invertible as B-module, it means that V is B-free.

From Theorem 1 and 2, we have $\left(\frac{B, a}{R}\right)\otimes_R\left(\frac{B, b}{R}\right)\sim\left(\frac{B, ab}{R}\right)$, and $\left(\frac{B_1, a}{R}\right)\otimes_R \left(\frac{B_2, a}{R}\right)\simeq\left(\frac{B_1*B_2, a}{R}\right)\otimes_R\left(\frac{B_1, a^2}{R}\right)\sim\left(\frac{B_1*B_2, a}{R}\right)$.

A quaternion R-algebra $\left(\frac{B, \varphi}{R}\right)=B\oplus V$ has an involution $\left(\frac{B, \varphi}{R}\right)\to\left(\frac{B, \varphi}{R}\right)$;

$d \leadsto \bar{d}$ defined by $\overline{(b+v)}=\bar{b}-v$ for $b\in B$, $v\in V$. Then, the norm N: $\left(\frac{B,\varphi}{R}\right)\to R$; $d\leadsto d\bar{d}$ defines a non degenerate quadratic R-module $\left(\left(\frac{B,\varphi}{R}\right), N\right)=(B, N|B)\perp(V, N|V)$, (cf. [3], (2.7)).

Corollary 1. *For a quaternion R-algebra $\left(\frac{B,\varphi}{R}\right)$, the following conditions are equivalent*:

1) *There is a unit a contained in $N(B)=\{b\bar{b}; b\in B\}$ such that $\left(\frac{B,\varphi}{R}\right)\cong\left(\frac{B,a}{R}\right)$.*

2) $\left(\frac{B,\varphi}{R}\right)\cong \mathrm{Hom}_R(B, B)$.

Proof. 1)$\Rightarrow$2): Since $\left(\frac{B,a}{R}\right)$ is a crossed product of a cylic group $G=G(B/R)$ and B with the trivial factor set $a\in N(B)$, we have $\left(\frac{B,a}{R}\right)=\Delta(G, B)\cong \mathrm{Hom}_R(B, B)$, where $\Delta(G, B)$ means a twisted group ring of G and B. 2)$\Rightarrow$1): By theorem 4, $\left(\frac{B,\varphi}{R}\right)\cong \mathrm{Hom}_R(B, B)\sim R$ implies $\varphi=\langle a\rangle$ for some unit a in R. Then, $\left(\frac{B,a}{R}\right)$ is a crossed product of $G=G(B/R)$ and B with the factor set a, and $\left(\frac{B,a}{R}\right)\cong \mathrm{Hom}_R(B, B)\cong\Delta(G, B)$. Therefore, a is in $N(B)$.

Lemma 3. ([3], (2.13)). *Let $\left(\frac{B,\varphi}{R}\right)=B\oplus V$ be a quaternion R-algebra and put $q=-N|V$, i.e. $q(v)=-N(v)$ for $v\in V$. Then (V, q) is hyperbolic if and only if $[B]=1$ in $Q_s(R)$. If $[B]=1$ in $Q_s(R)$ then $\left(\frac{B,\varphi}{R}\right)\sim R$.*

Proof. Suppose (V, q) is hyperbolic. Then there are totally isotropic R-submodules V_1 and V_2 such that $V=V_1\oplus V_2$ and V_i is invertible, $i=1, 2$. Since $0=q(v)=-N(v)=-v\bar{v}=v^2$ for every $v\in V$, we have $V_iV_i=0$, $i=1, 2$, and so $B=VV=V_1V_2+V_2V_1$. Put $\mathfrak{a}_1=V_1V_2$ and $\mathfrak{a}_2=V_2V_1$. Then we have $B=\mathfrak{a}_1+\mathfrak{a}_2$. Therefore, there are $e_1\in\mathfrak{a}_1$ and $e_2\in\mathfrak{a}_2$ such that $e_1+e_2=1$. Since $\mathfrak{a}_1\mathfrak{a}_2=\mathfrak{a}_2\mathfrak{a}_1=0$, e_1 and e_2 are orthogonal idempotents and $\mathfrak{a}_i=e_iB$, $i=1, 2$. Applying the main involution τ of B, we have $\tau(e_1B)=\tau(V_1V_2)=\tau(\varphi(V_1, V_2))=\varphi(V_2, V_1)=V_2V_1=e_2B$ and $B=e_1B\oplus e_2B$, therefore $[B]=1$ in $Q_s(R)$. Conversely, if $[B]=1$ in $Q_s(R)$, there are orthogonal idempotents e_1 and e_2 such that $B=e_1B\oplus e_2B$ and $\bar{e}_1=e_2$. Then we have $V=e_1V\oplus e_2V$ and e_1V, e_2V are totally isotropic R-submodule of (V, q), because of $q(e_1v)=e_1ve_1v=e_1\bar{e}_1v^2=0$ for every $e_1v\in e_1V$. If $[B]=1$ in $Q_s(R)$, then the Clifford algebra $C(V, q)$ of (V, q) is similar to R and isomorphic to $\left(\frac{V,\varphi}{R}\right)$, (cf. [3], (2.8)), and so $\left(\frac{B,\varphi}{R}\right)\sim R$.

Proposition 2. *If a quaternion R-algebra* $\left(\frac{R,\varphi}{R}\right)$ *contains a separable quadratic extension B′ of R, then there is a rank one non degenerate hermitian B′-module* φ' *such that* $\left(\frac{B,\varphi}{R}\right)=\left(\frac{B',\varphi'}{R}\right)$.

Proof. Firstly we shall show that B' is a maximal commutative subring of $\left(\frac{B,\varphi}{R}\right)$. Since B' is a separable subalgebra of the Azumaya R-algebra $\left(\frac{B,\varphi}{R}\right)$, the commutor ring $B''=\left\{b\in\left(\frac{B,\varphi}{R}\right);\ bb'=b'b \text{ for all } b'\in B'\right\}$ is also separable over R, (cf. [6], Theorem 2). Then we have that $\left(\frac{B,\varphi}{R}\right)\supset B''\supset B'\supset R$, B'' is a direct summand of $\left(\frac{B,\varphi}{R}\right)$ as left B''-module, and so is B' as left B'-module. When we consider $\left(\frac{B,\varphi}{R}\right)\otimes_R R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of R, we have $\left(\frac{B,\varphi}{R}\right)\otimes_R R/\mathfrak{m}\supset B''\otimes_R R/\mathfrak{m}\supset B'\otimes_R R/\mathfrak{m}\supset R/\mathfrak{m}$, therefore we may assume that R is a field. If $B''\neq B'$, then B'' becomes a commutative subring of $\left(\frac{B,\varphi}{R}\right)$ having $[B'':R]=3$. This is imposible for the simple ring $\left(\frac{B,\varphi}{R}\right)$ with $\left[\left(\frac{B,\varphi}{R}\right):R\right]=4$. Accordingly, B' is a maximal commutative subring of $\left(\frac{B,\varphi}{R}\right)$. By [7], Proposition 3 and [3], (2,.1) and (2.2), we have $\left(\frac{B,\varphi}{R}\right)=\left(\frac{B',\varphi'}{R}\right)$ for some rank one non degenerate hermitian left B'-module $\varphi'=(V',\varphi')$.

Theorem 5. *A quaternion R-algebra* $\left(\frac{B,\varphi}{R}\right)$ *is isomorphic to a matrix ring* R_2 *of degree two if and only if there is a quadratic extension B′ of R such that* $\left(\frac{B,\varphi}{R}\right)\supset B'\supset R$ *and* $[B']=1$ *in* $Q_s(R)$.

Proof. Suppose that there is a quadratic extension B' such that $[B']=1$ in $Q_s(R)$ and $\left(\frac{B,\varphi}{R}\right)\supset B'\supset R$. By Proposition 2, we may assume $[B]=1$ in $Q_s(R)$ for $\left(\frac{B,\varphi}{R}\right)$, i.e. $B=Re_1\oplus Re_2$, where e_1 and e_2 are orthogonal idempotents. Then by Lemma 3 we have $\left(\frac{B,\varphi}{R}\right)\sim R$ and by Theorem 4 $\left(\frac{B,\varphi}{R}\right)=\left(\frac{B,a}{R}\right)=B\oplus Bv$, where $v^2=\varphi(v,v)=a$ is unit in R. We have also an R-algebra isomorphism from the matrix R_2 to $\left(\frac{B,a}{R}\right)=B\oplus Bv=Re_1\oplus Re_2\oplus Re_1v\oplus Re_2v$ defined by

$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \rightsquigarrow e_1$, $\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} \rightsquigarrow e_2$, $\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \rightsquigarrow a^{-1}e_1 v$ and $\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} \rightsquigarrow e_2 v$. The converse is easily obtained from that $B'=\begin{pmatrix}R & 0\\ 0 & R\end{pmatrix}\subset R_2$ is a quadratic extension such that $[B']=1$ in $Q_s(R)$.

Corollary 2. *For any quaternion R-algebra* $\left(\frac{B, \varphi}{R}\right)$, *we have*

$$\left(\frac{B, \varphi}{R}\right)\otimes_R B \cong B_2 .$$

Proof. This is clear from $\left(\frac{B, \varphi}{R}\right)\otimes_R B \cong \left(\frac{B\otimes_R B,\ i_{B\otimes_R B}\circ\varphi}{B}\right)$ and $[B\otimes_R B]=1$ in $Q_s(B)$.

Corollary 3. *If a quaternion R-algebra* $\left(\frac{B, \varphi}{R}\right)$ *satisfies either* $[B]=1$ *in* $Q_s(R)$ *or* $\varphi=\langle a\rangle$ *for some unit a in R contained in* $N(B)$, *then the quadratic R-module* $\left(\left(\frac{B, \varphi}{R}\right), N\right)$ *is hyperbolic.*

Proof. If $[B]=1$ in $Q_s(R)$, $(V, N\,|\,V)$ and $(B, N\,|\,B)$ are hyperbolic by Lemma 3, therefore $\left(\left(\frac{B, \varphi}{R}\right), N\right)=(V, N\,|\,V)\perp(B, N\,|\,B)$ is so. If $\left(\frac{B, \varphi}{R}\right) =\left(\frac{B, a}{R}\right)$ and $a\in N(B)$ then a can be replaced by 1 and so $\left(\frac{B, 1}{R}\right)=B\oplus Bv$ for $v^2=1$. Then, we have $\left(\left(\frac{B, \varphi}{R}\right), N\right)=(B, N\,|\,B)\perp(Bv, N\,|\,Bv)\cong(B, N\,|\,B)\perp (B, -N\,|\,B)$, therefore this is hyperbolic.

4. In case 2 is invertible

In this section we assume that 2 is invertible in R.

Proposition 3. *If* $\left(\frac{B, \varphi}{R}\right)\sim R$ *then* $\left(\frac{B, \varphi}{R}\right)$ *is R-free, i.e. there are units a and b in R such that* $\left(\frac{B, \varphi}{R}\right)=\left(\frac{a, b}{R}\right)=R\oplus Ri\oplus Rj\oplus Rij$, $i^2=a$, $j^2=b$ *and* $ij=-ij$.

Proof. If $\left(\frac{B, \varphi}{R}\right)\sim R$, by Theorem 4 φ is B-free, i.e. there is a unit a in R satisying $\varphi=\langle a\rangle$, and $\left(\frac{B, \varphi}{R}\right)=B\oplus Bi$, $i^2=a$. Since 2 is invertible, $B'=R[i] \cong R[X]/(X^2-a)$ is a separable quadratic extension of R. By Proposition 2, we have $\left(\frac{B, \varphi}{R}\right)=\left(\frac{B', \varphi'}{R}\right)$ for some φ', and φ' is also B'-free, i.e. $\varphi'=\langle b\rangle=(B'j, \varphi')$

for some unit b in R. This means $\left(\frac{B,\ \varphi}{R}\right)=\left(\frac{B',\ \varphi'}{R}\right)=B'\oplus B'j=R\oplus Ri\oplus Rj \oplus Rij$, and $i^2=a$, $j^2=b$, $ji=\bar{i}j=-ij$.

Theorem 6. *For a quaternion R-algebra* $\left(\frac{B,\ \varphi}{R}\right)$, *the following conditions are equivalent*;

1) $\left(\frac{B,\ \varphi}{R}\right)\cong R_2$,

2) *there is an element u in* $\left(\frac{B,\ \varphi}{R}\right)$ *such that* $u^2=1$ *and* $R[u]=R+Ru$ *is a maximal commutative subring of* $\left(\frac{B,\ \varphi}{R}\right)$,

3) *there is a quadratic extension* B' *of* R *such that* $\left(\frac{B,\ \varphi}{R}\right)\cong\left(\frac{B',\ \varphi'}{R}\right)$ *and* $[B']=1$ *in* $Q_s(R)$,

4) *there is a unit a in R such that* $\left(\frac{B,\ \varphi}{R}\right)\cong\left(\frac{B',\ a}{R}\right)$ *for a separable quadratic extension* B' *and* $a\in N(B')$,

5) $\left(\frac{B,\ \varphi}{R}\right)\cong\left(\frac{b,\ 1}{R}\right)$ *for some unit b in R.*

Proof. 1) ⇒ 2): The element $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=u$ in R_2 satisfies the condition 2). 2) ⇒ 3): For a u satisfying the condition 2), $B'=R[u]$ is a quadratic extension of R. Because, $D=\left(\frac{B,\ \varphi}{R}\right)$ is a finitely generated projective left $R[u]\otimes_R D^\circ$-module, defined by $(a\otimes d^\circ)y=ayd$ for $y\in D$, $a\otimes d^\circ\in R[u]\otimes_R D^\circ$, since $R[u]\otimes_R D^\circ$ is a separable R-algebra. And a maximal commutaive subring of D is $R[u]=\mathrm{Hom}_{R[u]\otimes_R D^\circ}(D,\ D)$. Therefore, every maximal ideal $\mathfrak{p}$ of R, $R[u]_\mathfrak{p}$ is a maximal commutative subring of $D_\mathfrak{p}$. Hence $[R[u]_\mathfrak{p}\colon R_\mathfrak{p}]=2$. $B'R[u]$ is a separable qaudratic extension of R such that $[B']=1$ in $Q_s(R)$. By Proposition 2, we have $\left(\frac{B,\ \varphi}{R}\right)=\left(\frac{B',\ \varphi'}{R}\right)$ for some φ'. 3) ⇒ 1) and 2) ⇒ 5) are easily obtained from Theorem 5 and Proposition 3. 5) ⇒ 4) is clear. 4) ⇒ 2): Put $\left(\frac{B'\ a}{R}\right)=B'\oplus B'v$, $v^2=a$. Since $a\in N(B')$, there is a b in B' such that $a=N(b)=b\bar{b}$. Put $u=b^{-1}v$, then $u^2=1$ and $R[u]$ is a maximal commutative subring of $\left(\frac{B',\ a}{R}\right)$.

Corollary 4. *If* $[B]$ *is any element of* $Q_s(R)$, *the twisted group ring* $\Delta(G,\ B)$ *of B and the Galois group* $G=G(B/R)$ *is isomorphic to a matrix ring* R_2. *Therefore we have* $Hom_R(B,\ B)\cong R_2$.

Proof. Since $\Delta(G, B)=B\oplus B\tau\cong\left(\frac{B, 1}{R}\right)$, ($\tau$ is the main involution of B), by Theorem 6 we conclude $\mathrm{Hom}_R(B, B)\cong\Delta(G, B)\cong\left(\frac{B, 1}{R}\right)\cong R_2$.

OSAKA WOMEN'S UNIVERSITY

References

[1] S.U. Chase, D.K. Harrison and A. Rosenberg: *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. 52 (1965), 15–33.

[2] A. Hattori: *Certain cohomology associated with Galois extensions of commutative rings*, Sci. Papers College Gen. Ed. Univ. Tokyo **24** (1974), 79–91.

[3] T. Kanzaki: *On non commutative quadratic extensions of a commutative ring*, Osaka J. Math. **10** (1973), 597–604.

[4] ————: *A note on the orthogonal group of a quadratic module of rank two over a commutative ring*, Osaka J. Math. **10** (1973), 607–609.

[5] ————: *On the quadratic extension and the extended Witt ring of a commutative ring*, Nagoya Math. J. **49** (1973), 127–141.

[6] ————: *On commutor ring and Galois theory of separable algebras*, Osaka J. Math. **1** (1964), 103–115.

[7] ————: *On generalized crossed product and Brauer group*, Osaka J. Math. **5** (1968), 175–188.

[8] C. Small: *The group of quadratic extensions*, J. Pure Appl. Algebra **2** (1972), 83–105.