# The Structure of Galois Algebras

**George Szeto**

Department of Mathematics, Bradley University
Peoria, Illinois 61625 – U.S.A.
Email: szeto@hilltop.bradley.edu

**and**

**Lianyong Xue**
Department of Mathematics, Bradley University
Peoria, Illinois 61625 – U.S.A.
Email: lxue@hilltop.bradley.edu

Let $B$ be a ring with 1 and $G$ an automorphism group of $B$ of order $n$ for some integer $n$. It is shown that if $B$ is a Galois algebra with Galois group $G$, then $B$ is either a direct sum of central Galois algebras or a direct sum of central Galois algebras and a commutative Galois algebra. Moreover, when $G$ is inner, $B$ is either a direct sum of Azumaya projective group algebras or a direct sum of Azumaya projective group algebras and a commutative Galois algebra. Examples are given for these structures.

## 1. INTRODUCTION

T. Kanzaki ([6]), M. Harada ([4]), and F. R. DeMeyer ([3]) investigated Galois algebras. K. Sugano ([7]) studied the type of Galois $H$-separable extensions, and several other types of Galois Extensions were recently discussed ([1, 7, 8, 9, 10]). In [6], many interesting properties were found. It was shown that if $B$ is a Galois algebra over a commutative ring $R$ with Galois group $G$, then $B = \oplus \sum_{g\in G} J_g$ where $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ ([6, Theorem 1]), $J_g J_h = I_g J_{gh}$ where $I_g = BJ_g \cap C$ and $C$ the center of $B$, $I_g^2 = I_g$, $I_g J_g = J_g$ ([6, Proposition 2]), and $J_g J_{g^{-1}} = e_g C$ for some idempotent $e_g$ in $C$ ([6, Theorem 2]). In particular, if $B$ is a central Galois algebra, then $J_g J_h = J_{gh}$ and $I_g = C$ ([6, Corollary 1]), and its converse was also shown by M. Harada ([4, Theorem 1]): if $B = \oplus \sum_{g\in G} J_g$ such that $J_g J_{g^{-1}} = C$ and $B$ is a separable $R$-algebra, then $B$ is a central Galois algebra. The purpose of the present paper is to show the following structure theorem for a Galois algebra over $R$: if $B$ is a Galois algebra over $R$ with Galois group $G$, then there exist orthogonal idempotents $\{e_i \in C | i = 1, 2, ..., m$ for some integer $m\}$ and some subgroups $H_i$ of G such that $Be_i$ is a central Galois algebra with Galois group $H_i$ for each $i = 1, 2, ..., m$ and $B = \oplus \sum_{i=1}^{m} Be_i$ or $B = (\oplus \sum_{i=1}^{m} Be_i) \oplus A$ for some commutative Galois algebra $A$ with Galois group $G|_A \cong G$. When $G$ is inner, $B$ is either a direct sum of Azumaya projective group algebras as defined by F. R. DeMeyer ([3, Theorem 6]) or a direct sum of Azumaya projective group algebras and a commutative Galois algebra. This paper was revised under the suggestions of the referee and written under the support of a Caterpillar Fellowship at Bradley University. We would like to thank the referee for the valuable suggestions and Caterpillar Inc. for the support.

## 2. DEFINITIONS AND NOTATIONS

Throughout this paper, $B$ will represent a ring with 1, $G$ an automorphism group of $B$ of order $n$ for some integer $n$, $C$ the center of $B$, and $B^G$ the set of elements in $B$ fixed under each element in $G$. We denote $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ and $I_g = BJ_g \cap C$ for each $g \in G$.

Let $A$ be a subring of a ring $B$ with the same identity 1. We call $B$ a separable extension of $A$ if there exist $\{a_i, b_i$ in $B$, $i = 1, 2, ..., m$ for some integer $m\}$ such that $\sum a_i b_i = 1$, and $\sum b a_i \otimes b_i = \sum a_i \otimes b_i b$ for all $b$ in $B$ where $\otimes$ is over $A$. An Azumaya algebra is a separable extension of its center. $B$ is called a Galois extension of $B^G$ with Galois group $G$ if there exist elements $\{a_i, b_i$ in $B$, $i = 1, 2, ..., m\}$ for some integer $m$ such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. Such a set $\{a_i, b_i\}$ is called a $G$-Galois system for $B$. $B$ is called a Galois algebra over $R$ if $B$ is a Galois extension of $R$ which is contained in $C$, and $B$ is called a central Galois extension if $B$ is a Galois extension of $C$. A ring $B$ is called a $H$-separable extension of $A$ if $B \otimes_A B$ is isomorphic to a direct summand of a finite direct sum of $B$ as a $B$-bimodule, and $B$ is called a Galois $H$-separable extension if it is a Galois and a $H$-separable extension of $B^G$ (see [7]).

## 3. THE STRUCTURE THEOREM

In this section, we shall show a structure theorem for a Galois algebra $B$ over $R$ with Galois group $G$. We begin with some properties of the $C$-module $J_g$ for $g \in G$.

**LEMMA 3.1.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$, then*

*(1) $B(J_gJ_h) = B(J_hJ_g)$ for all $g, h \in G$.*

*(2) $BJ_g^2 = BJ_g$ for all $g \in G$.*

*Proof.* (1) Since $B$ is a Galois algebra over $R$, $R \subset C$ and $B$ is a separable extension of $R$. Hence $B$ is an Azumaya $C$-algebra ([2, Theorem 3.8, page 55]). Noting that $BJ_g$ is an ideal of $B$ and $I_g = BJ_g \cap C$ is an ideal of $C$, we have that $BJ_g = BI_g$ ([2, Corollary 3.7, page 54]). Hence $B(J_gJ_h) = (BJ_g)(BJ_h) = (BI_g)(BI_h) = (BI_h)(BI_g) = (BJ_h)(BJ_g) = B(J_hJ_g)$.

(2) By Proposition 2 in [6], $I_g^2 = I_g$ for all $g \in G$. Hence $BJ_g^2 = (BJ_g)(BJ_g) = (BI_g)(BI_g) = BI_g^2 = BI_g = BJ_g$ for all $g \in G$.

**Lemma 3.2.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$ and $H$ is a subgroup of $G$, then*

*(1) $B(\Pi_{h\in H}J_h)$ is invariant under $H$, that is, $g(B(\Pi_{h\in H}J_h)) = B(\Pi_{h\in H}J_h)$ for each $g\in H$.*

*(2) $B(\Pi_{h\in H}J_h) = Be$ for some idempotent $e$ in $C$.*

*(3) If $\Pi_{h\in H}J_h \neq \{0\}$, $H|_{Be}\cong H$.*

*Proof.* (1) It is easy to check that $g(J_h) = J_{ghg^{-1}}$ for all $g,h\in G$, so $g(B\Pi_{h\in H}J_h) = B(\Pi_{h\in H}J_{ghg^{-1}})$. But $\{ghg^{-1}\,|\,h\in H\} = H$ for each $g\in H$. So $g(B(\Pi_{h\in H}J_h)) = B(\Pi_{h\in H}J_h)$ for each $g\in H$ by Lemma 3.1.

(2) By Theorem 2 in [6], $J_hJ_{h^{-1}} = e_hC$ for some idempotent $e_h$ in $C$. So by Lemma 3.1, $B(\Pi_{h\in H}J_h) = B(\Pi_{h\in H}J_h^2) = B(\Pi_{h\in H}J_hJ_{h^{-1}}) = B(\Pi_{h\in H}e_h)$. Noting $\Pi_{h\in H}e_h$ by $e$, we have $B(\Pi_{h\in H}J_h) = Be$ where $e$ is an idempotent in $C$.

(3) By (1) $B(\Pi_{h\in H}J_h)$ is invariant under $H$ and by (2) $B(\Pi_{h\in H}J_h) = Be$, so for $h\in H$, $h(e)=e$ (for $e$ is the identity of $Be$). Since $B$ is a Galois algebra over $R$ with Galois group $G$, there exists a $G$-Galois system $\{a_i, b_i$ in $B$, $i=1,2,...,m\}$ for some integer $m$ such that $\sum_{i=1}^m a_ig(b_i) = \delta_{1,g}$ for each $g\in G$. Hence $e\sum_{i=1}^m a_ih(b_i) = e\delta_{1,h}$; and $\sum_{i=1}^m (ea_i)h(eb_i) = e\delta_{1,h}$ for each $h\in H$. Therefore, $e = \sum_{i=1}^m (ea_i)(h(eb_i)-(eb_i))$ for each $h\neq 1$ in $H$. Now by hypothesis, $\Pi_{h\in H}J_h\neq\{0\}$, so $e\neq 0$. This implies that $h|_{Be}\neq 1$ whenever $h\neq 1$ in $H$. Thus, $H|_{Be}\cong H$.

**LEMMA 3.3.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$, $H$ a subgroup of $G$, $e$ the same as in Lemma 3.2, and $J_h' = \{b\in Be\,|\,bx = h(x)b$ for all $x\in Be\}$ for each $h\in H\cong H|_{Be}$. Then, $J_h' = eJ_h$ for each $h\in H\cong H|_{Be}$.*

*Proof.* It is clear that $eJ_h\subset J_h'$. Conversely, for any $b\in J_h'$, $b = eb$ and $bx = h(x)b$ for each $x\in Be$. Hence for any $y\in B$, $by = (eb)y = b(ye) = h(ye)b = h(y)eb = h(y)b$. Therefore, $b\in J_h$. So, $b = eb\in eJ_h$. Thus, $J_h' = eJ_h$.

Next are two "local" structure theorems for $B(\Pi_{h\in H}J_h)$ where $H$ is a subgroup of $G$ such that $\Pi_{h\in H}J_h\neq\{0\}$.

**Theorem 3.4.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$. If $H$ is a subgroup of $G$ such that $\Pi_{h\in H}J_h \neq \{0\}$, then $B(\Pi_{h\in H}J_h)(= Be)$ is a Galois $H$-separable extension with Galois group $H|_{Be} \cong H$.*

*Proof.* By Lemma 3.2-(2), $B(\Pi_{h\in H}J_h) = Be$ for some idempotent $e$ in $C$, and by the proof of Lemma 3.2-(1) and (3), $\sum_{i=1}^{m}(ea_i)h(eb_i) = e\delta_{1,h}$ for each $h \in H \cong H|_{Be}$. Hence $Be$ is a Galois extension with Galois group $H|_{Be} \cong H$. Moreover, by Theorem 2 in [6], $J_hJ_{h^{-1}} = e_hC$ for some idempotent $e_h$ in $C$ and $e_he = e$ by the proof of Lemma 3.2. Therefore, by Lemma 3.3, $J'_hJ'_{h^{-1}} = (eJ_h)(eJ_{h^{-1}}) = eJ_hJ_{h^{-1}} = ee_hC = eC$ which is the center of $Be$. Thus, $Be$ is a Galois $H$-separable extension with Galois group $H|_{Be} \cong H$ ([7, Theorem 2]).

With the maximality property of the subset $H$ of $G$ such that $\Pi_{h\in H}J_h \neq \{0\}$, we show that $H$ is indeed a subgroup of $G$ and that $B(\Pi_{h\in H}J_h)$ becomes a central Galois algebra, a stronger Galois extension than the Galois $H$-separable extension as given in Theorem 3.4.

**LEMMA 3.5.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$ and $H$ a maximal subset of $G$ such that $\Pi_{h\in H}J_h \neq \{0\}$. Then $H$ is a subgroup of $G$.*

*Proof.* For any $g, h \in H$, we claim that $gh \in H$. In fact, suppose that $gh \notin H$. Then $(\Pi_{h\in H}J_h)J_{gh} = \{0\}$ by the maximality property of $H$. Hence $B(\Pi_{h\in H}J_h)J_{gh} = \{0\}$. Since $g, h \in H$ and $BJ_h^2 = BJ_h$ for all $h \in H$ by Lemma 3.1,

$$\begin{aligned}\{0\} &= B(\Pi_{h\in H}J_h)J_{gh} = B(\Pi_{h\in H}J_h)(J_gJ_h)J_{gh}\\ &= B(\Pi_{h\in H}J_h)(I_gJ_{gh})J_{gh} \quad ([6, \text{Proposition } 2])\\ &= B(\Pi_{h\in H}J_h)(I_gJ_{gh}) = B(\Pi_{h\in H}J_h)(J_gJ_h) = B(\Pi_{h\in H}J_h)\\ &\neq \{0\}.\end{aligned}$$

This is a contradiction. Thus, $gh \in H$. But then $H$ is a subgroup of $G$ for $G$ is finite.

**Theorem 3.6.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$. If $H$ is a maximal subset of $G$ such that $\Pi_{h\in H}J_h \neq \{0\}$, then $H$ is a subgroup of $G$ and $B(\Pi_{h\in H}J_h)(= Be)$ is a central Galois algebra with Galois group $H|_{Be} \cong H$.*

*Proof.* By Lemma 3.5, $H$ is a subgroup of $G$. Since $B$ is a Galois algebra over $R$ with Galois group $G$, $B = \oplus\sum_{g\in G} J_g$. Hence $Be = \oplus\sum_{g\in G} eJ_g = (\oplus\sum_{h\in H} eJ_h) \oplus (\oplus\sum_{g\notin H} eJ_g)$. by Lemma 3.3, $J'_h = eJ_h$ for each $h \in H \cong H|_{Be}$. By the maximality property of $H$, $BeJ_g = B(\Pi_{h\in H}J_h)J_g = \{0\}$ for each $g \notin H$. Hence $eJ_g = \{0\}$ for each $g \notin H$. Thus, $Be = \oplus\sum_{h\in H} J'_h$. Also, $J'_hJ'_{h^{-1}} = (eJ_h)(eJ_{h^{-1}}) = eJ_hJ_{h^{-1}} = eC$ which is the center of $Be$. Moreover, $B$ is a Galois $R$-algebra, so it is a separable $R$-algebra. Thus, $Be$ is a separable algebra over $Re$ ([2, Proposition 1.11, page 46]). Therefore, $Be$ is a central Galois algebra over $Ce$ ([4, Theorem 1]).

To obtain a structure theorem for a Galois algebra, we need a lemma.

**LEMMA 3.7.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$ and $e$ a nonzero idempotent in $C^G$. Then $Be$ is a Galois algebra over $Re$ with Galois group $G|_{Be} \cong G$.*

*Proof.* Since $e \in C^G$, $Be$ is invariant under $G$. By hypothesis, $B$ is a Galois algebra over $R$ with Galois group $G$, so there exists a $G$-Galois system for $B$ $\{a_i, b_i$ in $B$, $i = 1, 2, ..., m\}$ for some integer $m$ such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. Hence $e\sum_{i=1}^m a_i g(b_i) = e\delta_{1,g}$; and $\sum_{i=1}^m (a_i e)g(b_i e) = e\delta_{1,g}$ for each $g \in G$. Therefore, $\{a_i e, b_i e$ in $Be$, $i = 1, 2, ..., m\}$ is a $G$-Galois system for $Be$ and $e = \sum_{i=1}^m (a_i e)(g(b_i e) - b_i e)$ for each $g \neq 1$ in $G$. But $e \neq 0$, so $g|_{Be} \neq 1$ whenever $g \neq 1$ in $G$. Thus, $Be$ is a Galois algebra over $Re$ with Galois group $G|_{Be} \cong G$.

**THEOREM 3.8.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$. Then there are orthogonal idempotents $\{e_i \,|\, i = 1, 2, ..., m$ for some integer $m\}$ in $C$ and subgroups $H_i$*

*of $G$ such that $Be_i$ is a central Galois algebra with Galois group $H_i$ for each $i = 1, 2, ..., m$ and $B = \oplus \sum_{i=1}^{m} Be_i$ or $B = (\oplus \sum_{i=1}^{m} Be_i) \oplus Ce$ where $e = 1 - \sum_{i=1}^{m} e_i$ and $Ce = Be$ is a commutative Galois algebra with Galois group $G|_{Ce} \cong G$.*

*Proof.* Let $H_1$ be a maximal subset of $G$ such that $\Pi_{h\in H_1} J_h \neq \{0\}$. Then $H_1$ is a subgroup of $G$ by Lemma 3.5. By Theorem 3.6, there exists an idempotent $e_1$ in $C$ such that $B(\Pi_{h\in H_1} J_h)(= Be_1)$ is a central Galois algebra over $Ce_1$ with Galois group $H_1|_{Be_1} \cong H_1$. Let $H_1$, $H_2 = g_2 H_1 g_2^{-1}$, ..., $H_k = g_k H_1 g_k^{-1}$ be all the distinct conjugates of $H_1$ in $G$ for some $g_i \in G$ (if $H_1$ is a normal subgroup of $G$, $k = 1$ and $g_1 = 1$). Since for each $i = 2, 3, ..., k$, $\Pi_{h_i\in H_i} J_{h_i} = \Pi_{h\in H_1} J_{g_i h g_i^{-1}} = g_i(\Pi_{h\in H_1} J_h)$, $H_i$ is also a maximal subset (subgroup) of $G$ such that $\Pi_{h_i\in H_i} J_{h_i} \neq \{0\}$ by the maximality property of $H_1$. Hence, by Theorem 3.6 again, for each $i = 2, 3, ..., k$, there exists an idempotent $e_i$ in $C$ such that $B(\Pi_{h_i\in H_i} J_{h_i})(= Be_i)$ is a central Galois algebra over $Ce_i$ with Galois group $H_i|_{Be_i} \cong H_i$. Moreover, $(Be_i)(Be_j) = B(\Pi_{h_i\in H_i} J_{h_i})B(\Pi_{h_j\in H_j} J_{h_j}) = Be_i\delta_{ij}$ by Lemma 3.1 and the maximality property of $H_i$ and $H_j$; and so $e_1$, $e_2$, ..., $e_k$ are orthogonal. Thus, $B = (\oplus \sum_{i=1}^{k} Be_i) \oplus B(1 - \sum_{i=1}^{k} e_i)$. In case that $\sum_{i=1}^{k} e_i = 1$, we have $B = \oplus \sum_{i=1}^{k} Be_i$, and so we are done. In case that $\sum_{i=1}^{k} e_i \neq 1$, we have $1 - \sum_{i=1}^{k} e_i \neq 0$. Since $\{H_1, H_2, ..., H_k\} = \{g_i H_1 g_i^{-1} \mid i = 1, 2, ...k\}$ are all the distinct conjugates of $H_1$ in $G$, $\{gH_1g^{-1}, gH_2g^{-1}, ..., gH_kg^{-1}\} = \{H_1, H_2, ..., H_k\}$ for any $g \in G$. Hence, that $g(B(\Pi_{h_i\in H_i} J_{h_i})) = B(\Pi_{h_i\in H_i} J_{gh_ig^{-1}})$ implies that $\{g(e_1), g(e_2), ..., g(e_k)\} = \{e_1, e_2, ..., e_k\}$ for all $g \in G$. Hence, $g(1 - \sum_{i=1}^{k} e_i) = 1 - \sum_{i=1}^{k} e_i$ for all $g \in G$, and so $1 - \sum_{i=1}^{k} e_i$ a nonzero idempotent in $C^G$. Thus, by Lemma 3.7 $B(1 - \sum_{i=1}^{k} e_i)$ is a Galois algebra over $R(1 - \sum_{i=1}^{k} e_i)$ with Galois group $G|_{B(1-\sum_{i=1}^{k} e_i)} \cong G$. Let $e = 1 - \sum_{i=1}^{k} e_i$. Then $Be$ is a Galois algebra over $Re$ with Galois group $G|_{Be} \cong G$. In case that $eJ_g = \{0\}$ for each $g \neq 1$ in $G$, we have that $Be = \oplus \sum_{g\in G} eJ_g = eJ_1 = eC$. Thus, $Be$ is a commutative Galois algebra with Galois group $G|_{Be} \cong G$, and so we are done. In case that $eJ_g \neq \{0\}$ for some $g \neq 1$ in $G$, we can obtain a subgroup $H_{k+1}$ and an idempotent $e_{k+1}$ in $C$ such that $Be_{k+1}$ is a central Galois algebra with Galois group $H_{k+1}|_{Be_{k+1}} \cong H_{k+1}$. Let $E = \{e_g \mid g \in G$ and $J_g J_{g^{-1}} = e_g C\}$.

By the proof of Lemma 3.2-(2), each $e_i$ is contained in the Boolean algebra generated by the elements in $E$ which is finite. Consequently, in finite steps, we have orthogonal idempotents $e_i$ in $C$ and subgroups $H_i$, $i = 1, 2, ..., m$ for some integer $m$ such that $Be_i$ is a central Galois algebra with Galois group $H_i$ for each $i = 1, 2, ..., m$ and $B = \oplus \sum_{i=1}^m Be_i$ or $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ where $e = 1 - \sum_{i=1}^m e_i$ and $Ce$ is a commutative Galois algebra with Galois group $G|_{Ce} \cong G$. This completes the proof.

If we further assume in Theorem 3.8 that $J_g \neq \{0\}$ for each $g \neq 1$ in $G$, then we can show that $G = \cup_{i=1}^m H_i$.

**THEOREM 3.9.** *Let $B$ be a Galois algebra over $R$ with Galois group $G$ and $J_g \neq \{0\}$ for each $g \neq 1$ in $G$. Then there are orthogonal idempotents $\{e_i \,|\, i = 1, 2, ..., m$ for some integer $m\}$ in $C$ and subgroups $H_i$ of $G$ such that $G = \cup_{i=1}^m H_i$, $Be_i$ is a central Galois algebra with Galois group $H_i$ for each $i = 1, 2, ..., m$, and $B = \oplus \sum_{i=1}^m Be_i$ or $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ where $e = 1 - \sum_{i=1}^m e_i$ and $Ce$ is a commutative Galois algebra with Galois group $G|_{Ce} \cong G$.*

*Proof.* By Theorem 3.8, there are orthogonal idempotents $\{e_i \,|\, i = 1, 2, ..., m$ for some integer $m\}$ in $C$ and subgroup $H_i$ of $G$ such that $Be_i$ is a central Galois algebra over $Ce_i$ with Galois group $H_i|_{Be_i} \cong H_i$ for each $i = 1, 2, ..., m$ and $B = \oplus \sum_{i=1}^m Be_i$ or $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ where $e = 1 - \sum_{i=1}^m e_i$ and $Ce$ is a commutative Galois algebra with Galois group $G|_{Ce} \cong G$. Moreover, $H_i$'s are maximal subsets (subgroups) of $G$ such that $\Pi_{h \in H_i} J_h \neq \{0\}$. In case that $B = \oplus \sum_{i=1}^m Be_i$, for any $g \neq 1$ in $G$, $\{0\} \neq BJ_g = \oplus \sum_{i=1}^m Be_i J_g = \oplus \sum_{i=1}^m B(\Pi_{h_i \in H_i} J_{h_i}) J_g$. Hence, there is some $H_i$ such that $(\Pi_{h_i \in H_i} J_{h_i}) J_g \neq \{0\}$. Therefore, $g$ is contained in some $H_i$ by the maximality property of $H_i$. Thus, $G = \cup_{i=1}^m H_i$. In case that $B = \oplus \sum_{i=1}^m Be_i \oplus Ce$, we have $eJ_1 = \oplus \sum_{g \in G} eJ_g$. Hence, $eJ_g = \{0\}$ for any $g \neq 1$ in $G$. Therefore, for any $g \neq 1$ in $G$,

$\{0\} \neq BJ_g = (\oplus \sum_{i=1}^m Be_iJ_g) \oplus CeJ_g = \oplus \sum_{i=1}^m Be_iJ_g = \oplus \sum_{i=1}^m B(\Pi_{h_i \in H_i} J_{h_i})J_g$. Thus, similar to the above argument, $G = \cup_{i=1}^m H_i$. This completes the proof.

In [3], let $f$: $G \times G \longrightarrow U(R)$ be a factor set from $G \times G$ to the set of units of R, that is, $f(g,h)f(gh,k) = f(h,k)f(g,hk)$ for all $g$, $h$, and $k$ in $G$. $RG_f = \sum_{g \in G} RU_g$ is called a projective group algebra over $R$ if $RG_f$ is an algebra with a free basis $\{U_g \mid g \in G\}$ over $R$ where the multiplications are given by $(r_gU_g)(r_hU_h) = r_gr_hU_gU_h$ and $U_gU_h = f(g,h)U_{gh}$ for $r_g, r_h \in B$ and $g, h \in G$. It was shown that if $B$ is a central Galois algebra over $C$ with inner Galois group $G$, then $B$ is an Azumaya projective group algebra over $C$ ([3, Theorem 6]). We next generalize the above structure theorem for a central Galois algebra with an inner Galois group given by F. R. DeMeyer.

**THEOREM 3.10.** *If $B$ is a Galois algebra over $R$ with an inner Galois group $G$, then $B$ is either a direct sum of Azumaya projective group algebras or a direct sum of Azumaya projective group algebras and a commutative Galois algebra.*

*Proof.* By Theorem 6 in [3], a central Galois algebra with an inner Galois group is an Azumaya projective group algebra, so this is a consequence of Theorem 3.8.

We conclude the present paper with two examples of a Galois algebra $B$ which is not a central Galois algebra with Galois group $G$ such that $J_g \neq \{0\}$ for some $g \in G$ and $J_h = \{0\}$ for some $h \in G$, and $B = \oplus \sum_{i=1}^m Be_i$ or $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ as given in Theorem 3.8.

**EXAMPLE 1.** Let $R[i,j,k]$ be the real quaternion algebra over $R$, $B = R[i,j,k] \oplus R[i,j,k]$, and $G = \{1, g_i, g_j, g_k, g, gg_i, gg_j, gg_k\}$ where $g_i(a_1, a_2) = (ia_1i^{-1}, ia_2i^{-1})$, $g_j(a_1, a_2) = (ja_1j^{-1}, ja_2j^{-1})$, $g_k(a_1, a_2) = (ka_1k^{-1}, ka_2k^{-1})$, and $g(a_1, a_2) = (a_2, a_1)$ for all $(a_1, a_2)$ in $B$. Then,

(1) $B$ is a Galois extension with a $G$-Galois system: $\{a_1 = (1,0),\ a_2 = (i,0),\ a_3 = (j,0),\ a_4 = (k,0),\ a_5 = (0,1),\ a_6 = (0,i),\ a_7 = (0,j),\ a_8 = (0,k);\ b_1 = \frac{1}{4}(1,0),\ b_2 = -\frac{1}{4}(i,0),\ b_3 = -\frac{1}{4}(j,0),\ b_4 = -\frac{1}{4}(k,0),\ b_5 = \frac{1}{4}(0,1),\ b_6 = -\frac{1}{4}(0,i),\ b_7 = -\frac{1}{4}(0,j),\ b_8 = -\frac{1}{4}(0,k)\}$.

(2) $B^G = \{(r,r)\,|\,r \in R\} \cong R$.

(3) By (1) and (2) $B$ is a Galois algebra over $R$ with Galois group $G$.

(4) $C = R \oplus R$.

(5) By (3) and (4) $B$ is not a central Galois algebra with Galois group $G$.

(6) $J_1 = C = R \oplus R$, $J_{g_i} = (Ri) \oplus (Ri)$, $J_{g_j} = (Rj) \oplus (Rj)$, $J_{g_k} = (Rk) \oplus (Rk)$, and $J_g = J_{gg_i} = J_{gg_j} = J_{gg_k} = \{0\}$.

(7) $H_1 = \{1,\ g_i,\ g_j,\ g_k\}$ is a maximal subset (subgroup) of $G$ such that $\Pi_{h\in H_1} J_h \neq \{0\}$, and $B(\Pi_{h\in H_1} J_h)(= Be_1 = B)$ is a central Galois algebra over $C$ with Galois group $H_1|_{Be_1} \cong H_1$, and so $B = \oplus \sum_{i=1}^m Be_i$ where $m = 1$ and $Be_i$ is a central Galois algebra over $Ce_i$ with Galois group $H_i|_{Be_i} \cong H_i$ for each $i$. But $\cup_{i=1}^m H_i = H_1 \neq G$.

**EXAMPLE 2.** Let $R[i,j,k]$ be the real quaternion algebra over $R$, $D$ the field of complex numbers, $B = R[i,j,k] \oplus (D \otimes_R D)$, and $G = \{1,\ g_i,\ g_j,\ g_k\}$ where $g_i(a, d_1 \otimes d_2) = (iai^{-1}, \bar{d}_1 \otimes d_2)$, $g_j(a, d_1 \otimes d_2) = (jaj^{-1}, d_1 \otimes \bar{d}_2)$, and $g_k(a, d_1 \otimes d_2) = (kak^{-1}, \bar{d}_1 \otimes \bar{d}_2)$ for all $(a, d_1 \otimes d_2)$ in $B$, where $\bar{d}$ is the conjugate of the complex number $d$. Then,

(1) $B$ is a Galois extension with a $G$-Galois system: $\{a_1 = (1,0),\ a_2 = (i,0),\ a_3 = (j,0),\ a_4 = (k,0),\ a_5 = (0, 1 \otimes 1),\ a_6 = (0, \sqrt{-1} \otimes 1),\ a_7 = (0, 1 \otimes \sqrt{-1}),\ a_8 = (0, \sqrt{-1} \otimes \sqrt{-1});\ b_1 = \frac{1}{4}(1,0),\ b_2 = -\frac{1}{4}(i,0),\ b_3 = -\frac{1}{4}(j,0),\ b_4 = -\frac{1}{4}(k,0),\ b_5 = \frac{1}{4}(0, 1 \otimes 1),\ b_6 = -\frac{1}{4}(0, \sqrt{-1} \otimes 1),\ b_7 = -\frac{1}{4}(0, 1 \otimes \sqrt{-1}),\ b_8 = \frac{1}{4}(0, \sqrt{-1} \otimes \sqrt{-1})\}$.

(2) $B^G = R \oplus (R \otimes R) \cong R \oplus R$.

(3) By (1) and (2) $B$ is a Galois algebra over $R \oplus R$ with Galois group $G$.

(4) $C = R \oplus (D \otimes_R D)$.

(5) By (3) and (4) $B$ is not a central Galois algebra with Galois group $G$.

(6) $J_1 = C = R \oplus (D \otimes_R D)$, $J_{g_i} = R(i,0)$, $J_{g_j} = R(j,0)$, $J_{g_k} = R(k,0)$.

(7) $H_1 = \{1, g_i, g_j, g_k\} = G$ is a maximal subset (subgroup) of $G$ such that $\Pi_{h\in H_1} J_h \neq \{0\}$, and $B(\Pi_{h\in H_1} J_h)(= B(1,0) = R[i,j,k])$ is a central Galois algebra over $C(1,0)(= R)$ with Galois group $H_1|_{B(1,0)} \cong H_1$. Let $e_1 = (1,0)$ and $e = (0, 1\otimes 1)$. Then $B = (\oplus \sum_{i=1}^{m} Be_i) \oplus Ce$ where $m = 1$, $Be_i$ is a central Galois algebra over $Ce_i$ with Galois group $H_i|_{Be_i} \cong H_i$ for each $i = 1, 2, ..., m$ and $Ce = Be$ is a commutative Galois algebra with Galois group $G|_{Ce} \cong G$.

## REFERENCES


[1] R. Alfaro and G. Szeto, On Galois Extensions of an Azumaya Algebra, *Comm. in Algebra,* **25(6)**(1997) 1873-1882.

[2] F.R. DeMeyer and E. Ingraham, “Separable algebras over commutative rings”, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.

[3] F.R. DeMeyer, Some Notes on the General Galois Theory of Rings, *Osaka J. Math.,* **2**(1965) 117-127.

[4] M. Harada, Supplementary Results on Galois Extension, *Osaka J. Math.,* **2**(1965), 343-350.

[5] S. Ikehata and G. Szeto: On $H$-skew polynomial rings and Galois extensions, “Rings, Extension and Cohomology” 113-121, Lecture Notes in Pure and Appl. Math., 159, Dekker, New York, 1994.

[6] T. Kanzaki, On Galois Algebra Over A Commutative Ring, *Osaka J. Math.,* **2**(1965), 309-317.

[7] K. Sugano, On a Special Type of Galois Extensions, *Hokkaido J. Math.,* **9**(1980) 123-128.

[8] G. Szeto and L. Ma, On center Galois extensions over rings, *Glasnik Matematicki,* **24**(1989), 11-16.

[9] G. Szeto and L. Xue, On Three types of Galois Extensions of rings, *Southeast Asian Bulletin of Mathematics,* **23**(1999) 731-736.

[10] G. Szeto and L. Xue, On Characterizations of a Center Galois Extension, *International Journal of Mathematics and Mathematical Sciences,* Vol. 23, No. **11**(2000) 753-758.