On Galois Algebras with an Inner Galois Group

George Szeto and **Lianyong Xue**

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

Abstract

Let B be a Galois algebra with an inner Galois group G and center C. Then there exist orthogonal central idempotents $\{e_i \in C | i = 1, 2, ..., m$ for some integer $m\}$ and some subgroups $\{H_i | i = 1, 2, ..., m\}$ of G such that $B = \oplus \sum_{i=1}^{m} Be_i$ where Be_i is a projective group algebra $(Ce_i)(H_i)_{f_i}$ with a factor set f_i, $i = 1, 2, ..., m$. This generalizes the structure of a central Galois algebra with an inner Galois group as given by F. R. DeMeyer. Consequently, a structure of Galois algebras over a semi-local ring is derived.

1. Introduction

Let A be a central Galois algebra with an inner Galois group G, that is, A is a Galois algebra over its center C and $G = \{g_i \,|\, i = 1, 2, ..., n\}$ for some integer n such that $g_i(a) = U_i a U_i^{-1}$ for some invertible element $U_i \in A$, for each $a \in A$ and $i = 1, 2, ..., n$. Then F. R. DeMeyer ([1]) showed that $A \cong CG_f$ which is an Azumaya projective group algebra over C with a factor set f; that is, CG_f is a free C-module with a basis $\{U_i \,|\, i = 1, 2, ..., n\}$ such that $U_i U_j = U_k \cdot f(g_i, g_j)$ where $g_i g_j = g_k$ and $f(g_i, g_j) = U_i U_j U_k^{-1}$ for $i, j = 1, 2, ..., n$ ([1], Theorem 6). The purpose of the present paper is to generalize the above theorem to a Galois algebra (not necessarily central) with an inner Galois group. Let B be a Galois algebra over a commutative ring R with an inner Galois group G. Then we shall show that

(2000) Mathematics Subject Classification: 13B02, 16W20.

Key Words and Phrases: Galois algebras, Separable algebras, Azumaya algebras, Projective group algebras.

there exist orthogonal idempotents $\{e_i \in C \mid i = 1, 2, ..., m$ for some integer $m\}$ and some subgroups of G, $\{H_i \mid i = 1, 2, ..., m\}$, such that $B = \oplus \sum_{i=1}^{m} Be_i$ where Be_i is a projective group algebra of H_i restricted to Be_i over Ce_i for each $i = 1, 2, ..., m$. Moreover, for a Galois algebra B over a semi-local ring R, using the general Wedderburn Theorem for Azumaya algebras over a semi-local ring with no idempotents but 0 and 1 ([2], Corollary 1), we have a further description of the structure of each direct summand Be_i for $i = 1, 2, ..., m$.

2. Basic Definitions and Notations

Let F be a ring with 1 and E a subring of F. Then F is called a separable extension of E if there exist $\{a_i, b_i$ in F, $i = 1, 2, ..., k$ for some integer $k\}$ such that $\sum a_i b_i = 1$ and $\sum x a_i \otimes b_i = \sum a_i \otimes b_i x$ for all x in F where $\otimes$ is over E. In particular, F is called an Azumaya algebra if it is a separable extension over its center. Let G be a finite automorphism group of F and $F^G = \{x \in F \mid g(x) = x$ for all $g \in G\}$. Then F is called a Galois extension of F^G with Galois group G if there exist elements $\{c_i, d_i$ in F, $i = 1, 2, ..., t$ for some integer $t\}$ such that $\sum c_i d_i = 1$ and $\sum c_i g(d_i) = 0$ for each $g \neq 1$ in G, a Galois algebra over F^G if F is a Galois extension of F^G which is contained in the center of F, and a central Galois algebra over F^G if F is a Galois extension of F^G which is equal to the center of F. Let R be a commutative ring with identity 1; then RG_f is called a projective group algebra induced by a group $G = \{g_1, g_2, ..., g_q\}$ for some integer q with a factor set f, which is a map from $G \times G$ to $\{$units of $R\}$, such that $f(gh, l)f(g, h) = f(g, hl)f(h, l)$, if RG_f is a free R-module with a basis $\{x_i \mid i = 1, 2, ..., q\}$ such that $x_i x_j = x_k \cdot f(g_i, g_j)$ where $g_i g_j = g_k$ for $i, j = 1, 2, ..., q$ ([1]).

3. Galois Algebras with an Inner Galois Group

Let B be a Galois algebra over a commutative ring R with an inner Galois group G. We shall generalize the structure theorem for a central Galois algebra as shown by F. R. DeMeyer ([1], Theorem 6). This derives a structure theorem for Galois algebras over a semi-local ring R. We first recall the structure theorem as given by F. R. DeMeyer.

Proposition 3.1. ([1], Theorem 6) *Let B be a central Galois algebra over its center C with an inner Galois group G. Then $B = CG_f$, a projective group algebra with a factor set f.*

Theorem 3.2. *Let B be a Galois algebra over R with an inner Galois group G and C the center of B. Then there exist orthogonal central idempotents $\{e_i \mid i = 1, 2, ..., m$ for some integer $m\}$ and subgroups of G, $\{H_i \mid i = 1, 2, ..., m\}$, such that $B = \oplus \sum_{i=1}^{m} Be_i$ where Be_i is a projective group algebra of H_i over Ce_i for each $i = 1, 2, ..., m$.*

Proof. Let $J_g = \{b \in B \mid bx = g(x)b$ for all $x \in B\}$ for each $g \in G$. Then J_gB is an ideal of B such that $J_gB = Be_g$ for some central idempotent $e_g \in C$ ([4], Proposition 2 and Lemma 2), and there exist orthogonal central idempotents $\{e_i \mid i = 1, 2, ..., m$ for some integer $m\}$ and subgroups $\{H_i \mid i = 1, 2, ..., m\}$ of G such that Be_i is a central Galois algebra over Ce_i with Galois group H_i for each $i = 1, 2, ..., m$ ([6], Theorem 3.8). Moreover, let $e_0 = 1 - \sum_{i=1}^{m} e_i$. Then $e_0 = 0$ or $Be_0 = Ce_0$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G ([6], Theorem 3.8). Since G is an inner automorphism group, $G|_C = \{1\}$. Thus $e_0 = 0$. But then $\{e_i\}$ are orthogonal idempotents summing to 1 ([6], Theorem 3.8); and so $B = \oplus \sum_{i=1}^{m} Be_i$. Now, for any $g \in H_i$, by hypothesis, g is an inner automorphism of B, so $g(x) = U_g x U_g^{-1}$ for some invertible element $U_g \in B$ for all $x \in B$. Thus $g(xe_i) = U_g(xe_i)U_g^{-1} = (U_g e_i)(xe_i)(U_g^{-1}e_i) = (U_g e_i)(xe_i)(U_g e_i)^{-1}$ where $(U_g e_i)^{-1}$ is the inverse of $U_g e_i$ in Be_i. Therefore $g|_{Be_i}$ is also an inner automorphism group of Be_i for each $g \in H_i$; and so $H_i|_{Be_i}$ is an inner automorphism group of Be_i. Consequently, by Proposition 3.1, Be_i is a projective group algebra of $H_i|_{Be_i}$ over Ce_i for each $i = 1, 2, ..., m$.

In particular, when B is a central Galois algebra with an inner Galois group G, $BJ_g = B$ for each $g \in G$ ([4], Lemma 1). Hence $e_g = 1$ for each $g \in G$. Noting that $e_i = \pi_{g \in H_i} e_g$ for each i ([6], Theorem 3.8), we have that $m = 1$, $e_1 = 1$, and $H_1 = G$

in Theorem 3.2. Thus $B = Be_1$ is a projective group algebra of G over C. Therefore Theorem 3.2 recovers Theorem 6 in [1].

Next, we shall derive a structure theorem for Galois algebras over a semi-local ring R. The following results for Azumaya algebras over a semi-local ring with no idempotents but 0 and 1 will play an important role.

Proposition 3.3. ([2], Theorem 1) *Let R be a semi-local ring with no idempotents but 0 and 1, and A an Azumaya algebra over R. Then any two indecomposable finitely generated and projective A-modules are isomorphic.*

Proposition 3.4. ([2], Corollary 1) *If R is a semi-local ring with no idempotents but 0 and 1, then every element in $B(R)$, the Brauer group of R, is represented by a unique (up to isomorphic) Azumaya R-algebra D with no idempotents but 0 and 1. Moreover, if A is equivalent to D in $B(R)$, then $A \cong M_n(D)$ for a uniquely determined integer n.*

Lemma 3.5. *Let A be a projective separable algebra over a semi-local ring R and C the center of A. Then C is a semi-local ring.*

Proof. Since A is a separable algebra over R, it is an Azumaya C-algebra and C is a separable R-algebra ([3], Theorem 3.8 on page 55). Noting that C is a direct summand of A as a C-module ([3], Lemma 3.1 on page 51), we have that C is a finitely generated and projective R-module (for A is a projective separable R-algebra). But R is a semi-local ring, so C/JC is a direct sum of projective separable algebras over fields where J is the Jacobson radical of R. Thus C is a semi-local ring.

Lemma 3.6. *Let P be a finitely generated and projective module of rank one over a semi-local ring R. Then $P \cong R$.*

Proof. Since R is semi-local, there are minimal idempotents $\{e_i \,|\, i = 1, 2, ..., m$ for some integer $m\}$ summing to 1. Hence $R = \oplus \sum_{i=1}^{m} Re_i$ such that each Re_i is a semi-local ring with no idempotents but 0 and e_i. Thus $P = \oplus \sum_{i=1}^{m} Pe_i$ such that each Pe_i is a finitely generated and projective module of rank one over a semi-local ring Re_i with no idempotents but 0 and e_i. Noting that Pe_i is indecomposable finitely generated and projective module of rank one over Re_i, we have that $Pe_i \cong Re_i$ by Proposition 3.3 for each i. Therefore $P = \oplus \sum_{i=1}^{m} Pe_i \cong \oplus \sum_{i=1}^{m} Re_i = R$.

Theorem 3.7. *If B is a Galois algebra over a semi-local ring R with Galois group G, then B is a direct sum of projective group algebras or a direct sum of projective group algebras and a commutative Galois algebra with Galois group induced by and isomorphic with G.*

Proof. Since B is a Galois algebra over R, by Theorem 3.8 in [6], there exist orthogonal central idempotents $\{e_i \,|\, i = 0, 1, 2, ..., m$ for some integer $m\}$ and subgroups of G, $\{H_i \,|\, i = 1, 2, ..., m\}$, such that $B = \oplus \sum_{i=0}^{m} Be_i$ where Be_i is a central Galois algebra over Ce_i with Galois group $H_i|_{Be_i}$ for each $i = 1, 2, ..., m$ and $e_0 = 1 - \sum_{i=1}^{m} e_i$ such that $e_0 = 0$ or $Be_0 = Ce_0$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G where C is the center of B. Since B is a Galois algebra over R again, it is projective separable over the semi-local ring R. Hence C is also semi-local by Lemma 3.5. Thus Ce_i is semi-local for each i. Now, for each $g \in H_i$, let $J_g^{Be_i} = \{be_i \in Be_i \,|\, bx = g(x)b$ for all $x \in Be_i\}$. Then $J_g^{Be_i}$ is a finitely generated and projective module of rank one over Ce_i which is semi-local for each $g \in H_i$ (for Be_i is a central Galois algebra over Ce_i with Galois group $H_i|_{Be_i}$). This implies that $J_g^{Be_i} \cong Ce_i$ by Lemma 3.6. Therefore $g|_{Be_i}$ is inner ([5], Lemma 5) for each $g \in H_i$, that is, $H_i|_{Be_i}$ is inner; and so Be_i is a projective group algebra $(Ce_i)(H_i)_{f_i}$ with a factor set $f_i : H_i \times H_i \longrightarrow \{\text{units of } Ce_i\}$ for each $i = 1, 2, ..., m$. This completes the proof.

Corollary 3.8. *Let B be a Galois algebra over a semi-local ring R with Galois group G and C the center of B. If there is a $g \neq 1$ in G such that $g|_C = 1$, then B is a direct sum* *of projective group algebras.*

Proof. Since there is a $g \neq 1$ in G such that $g|_C = 1$, $G|_C \not\cong G$. Thus e_0 as given in Theorem 3.7 must be 0. Therefore $B = \oplus \sum_{i=1}^{m} Be_i$ which is a direct sum of projective group algebras by Theorem 3.7.

Note: The condition that there is a $g \neq 1$ in G such that $g|_C = 1$ in Corollary 3.8 can not be dropped as illustrated by the example at the end of this paper.

Next, we give a further description of each Be_i as given in Theorem 3.7 by using the general Wedderburn Theorem for an Azumaya algebra over a semi-local ring with no idempotents but 0 and 1 as given by Proposition 3.4 ([2], Corollary 1).

Theorem 3.9. *Let B be a Galois algebra over a semi-local ring R with Galois group G. Then for each e_i as given in Theorem 3.7, $Be_i = \oplus \sum_{j=1}^{k_i} Bf_{ij}$, $i = 1, 2, ..., m$ for some k_i, where f_{ij} are minimal central idempotents in Ce_i, such that $Bf_{ij} \cong M_{n_j}(D_j)$, a matrix ring of order n_j over an indecomposable Azumaya Cf_{ij}-algebra D_j for some integer n_j, where C is the center of B.*

Proof. Since B is a Galois algebra over R, B is projective separable over the semi-local ring R. Hence C is semi-local by Lemma 3.5. Thus Ce_i is semi-local for each i. Therefore Ce_i has finite number of minimal idempotents $\{f_{ij} \mid j = 1, 2, ..., k_i \text{ for some integer } k_i\}$ summing to e_i; and so $Ce_i = \oplus \sum_{j=1}^{k_i} Cf_{ij}$ where Cf_{ij} is a semi-local ring with no idempotents but 0 and f_{ij} for each j and Bf_{ij} is an Azumaya Cf_{ij}-algebra. Consequently, $Bf_{ij} \cong M_{n_j}(D_j)$ which is a matrix ring of order n_j for some n_j over an Azumaya Cf_{ij}-algebra D_j with no idempotents but 0 and f_{ij} by Proposition 3.4 ([2], Corollary 1).

Let R be a commutative ring with no idempotents but 0 and 1 and Spec(R) the spectrum of R. It is well known that the rank of a projective R-module M is defined as the number of copies of M_p over R_p for each $p \in \text{Spec}(R)$, where R_p is the local ring of R at $p \in \text{Spec}(R)$ (see [3], page 26). Next, we show that the rank of each direct summand Bf_{ij} of Be_i over Cf_{ij} in Theorem 3.9 is the order of H_i for each $j = 1, 2, ..., k_i$

Theorem 3.10. *Let $Be_i = \oplus \sum_{j=1}^{k_i} Bf_{ij}$, $i = 1, 2, ..., m$, for some k_i as given in Theorem 3.9. Then $\text{rank}_{Cf_{ij}}(Bf_{ij}) = \text{rank}_{Ce_i}(Be_i)$ = the order of H_i for each $j = 1, 2, ..., k_i$.*

Proof. Since Be_i is a central Galois algebra over Ce_i with Galois group H_i, $\text{rank}_{Ce_i}(Be_i)$ is the order of H_i (for the skew group ring $Be_i * H_i \cong \text{Hom}_{Ce_i}(Be_i, Be_i)$). Thus $\text{rank}_{(Ce_i)_p}(Be_i)_p$ = the order of H_i for each $p \in \text{Spec}(Ce_i)$. Noting that $\text{Spec}(Ce_i) = \cup_{j=1}^{k_i} \text{Spec}(Cf_{ij})$, we have that $(Be_i)_p \cong (Bf_{ij})_p$ for each $p \in \text{Spec}(Cf_{ij})$. Thus

$$\text{rank}_{Ce_i}(Be_i) = \text{rank}_{Cf_{ij}}(Bf_{ij}) = \text{the order of } H_i \text{ for each } j = 1, 2, ..., k_i.$$

We conclude the present paper with an example to illustrate the structure in Theorem 3.7.

EXAMPLE. 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) $B^G = R \oplus (R \otimes R) \cong R \oplus R$ which is a semi-local ring.

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

(4) $C = R \oplus (D \otimes_R D)$ which is also a semi-local ring.

(5) Let $e_1 = (1, 0)$ and $e_0 = 1 - e_1$. Then $B = Be_1 \oplus Be_0$ where $Be_1 = R[i, j, k] = RG_f$ which is a projective group algebra of $G|_{Be_1}$ over R $(= Ce_1)$ with a trivial factor set f and $Be_0 = D \otimes_R D = Ce_0$ which is a commutative Galois algebra with Galois group $G|_{Ce_0} \cong G$.

Acknowledgements. This paper was written under the support of a Caterpillar Fellowship at Bradley University. The authors would like to thank Caterpillar Inc. for the support.

References

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

[2] F.R. DeMeyer, Projective Modules over Central Separable Algebras, *Canadian J. Math.,* **21**(1969) 117-127.

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

[4] T. Kanzaki, On Galois Algebra over a Commutative Ring, *Osaka J. Math.,* **2**(1965), 309-317.

[5] A. Rosenberg and D. Zelinsky, Automorphisms of Separable Algebras, Pacific J. Math., **11**(1961), 1109-1117.

[6] G. Szeto and L. Xue, The Structure of Galois Algebras, *Journal of Algebra,* **237**(1)(2001), 238-246.