On Galois Extensions with an Inner Galois Group

George Szeto
Department of Mathematics, Bradley University
Peoria, Illinois 61625, U.S.A.
E-mail: szeto@bradley.edu

Lianyong Xue
Department of Mathematics, Bradley University
Peoria, Illinois 61625, U.S.A.
E-mail: lxue@bradley.edu

Abstract

Let B be a Galois extension of B^G with an inner Galois group G, $G = \{g \mid g(x) = U_g x U_g^{-1}$ for some $U_g \in B$ and for all $x \in B\}$. Then it is shown that B contains a projective group algebra CG_f of G over the center C of B where $f : G \times G \longrightarrow$ units of C is a factor set. Characterizations for B generated by $\{U_g \mid g \in G\}$ over B^G, and for a Galois CG_f are given respectively.

1 Introduction

Let B be a ring with 1, G a finite automorphism group of B, C the center of B, and B^G the set of elements in B fixed under each element in G. Following the definitions and notations in [9], we call B 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. A Galois extension B of B^G is called a Galois algebra if B^G is contained in C, and a central Galois algebra if $B^G = C$. Let A be a subring of B with the same identity 1. We denote $V_B(A)$ the commutator (also called centralizer) subring of A in B, that is, $V_B(A) = \{b \in B | bx = xb$ for all $x \in A\}$. 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 $\sum ba_i \otimes b_i = \sum a_i \otimes b_i b$ for all b in B where $\otimes$ is over A. An Azumaya algebra is a separable extension of its center. Let R be a commutative ring with 1 and $U(R)$ the set of units of R. As in [1], for a factor set (also called 2-cocycle) f: $G \times G \longrightarrow U(R)$ (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 U_g is an invertible element for each $g \in G$, the multiplications are given by $(r_g U_g)(r_h U_h) = r_g r_h U_g U_h$ and $U_g U_h = f(g,h) U_{gh}$ for $r_g, r_h \in R$ and $g, h \in G$; that is, $f(g,h) = U_g U_h U_{gh}^{-1}$. Noting that $U_g U_h U_{gh}^{-1}$ is in the center of RG_f and that $(G, \cdot)$ is associative, we can check that f: $G \times G \longrightarrow U(R)$ is a 2-cocycle. Let $Z^2(G,R)$ be the group of 2-cocycles and $B^2(G,R)$ be the group of 2-coboundaries. Then the second cohomology group $H^2(G,R) = Z^2(G,R)/B^2(G,R)$. It is known that $RG_f \cong RG_{f'}$ for $f, f' \in Z^2(G,R)$ if and only if f and f' are cohomologous cocycles in $Z^2(G,R)$, that is, $[f] = [f']$ in $H^2(G,R)$. Thus RG_f corresponds to $[f]$ in $H^2(G,R)$. For more detail, see [2].

Galois algebras with an inner Galois group have been intensively investigated ([1], [4], [5], [6], [7], [8]). It was shown that any central Galois algebra B over C with an inner Galois group G is an Azumaya projective group algebra CG_f of G over C ([1], Theorem 6). The converse also holds: any Azumaya projective group algebra CG_f over C is a central Galois algebra with an inner Galois group $\overline{G}$ induced by G ([2], Theorem 3). In [7], it was shown that any Galois algebra with an inner Galois group G is either a direct sum of Azumaya projective group algebras or a direct sum of Azumaya projective group algebras and a commutative Galois algebra. The purpose of the present paper is to study any Galois extension B of B^G with an inner Galois group G whose order $|G|$ is invertible in B, where $G = \{g \mid g(x) = U_g x U_g^{-1}$ for some $U_g \in B$ and for all $x \in B\}$. We shall show that B contains a projective group algebra CG_f. Thus several characterizations are obtained for B generated by $\{U_g \mid g \in G\}$ over B^G. These characterizations generalize the results for a central Galois algebra with an inner Galois group G ([1], Theorem 6). Moreover, when B is an Azumaya algebra, properties of the commutator subring $V_B(B^G)$ of B^G in B are given.

2 Galois Extensions

In this section, let B be a Galois extension of B^G with an inner Galois group G of order n invertible in B for some integer n, $G = \{g \mid g(x) = U_g x U_g^{-1}$ for some $U_g \in B$ and for all $x \in B\}$, C the center of B, and B^G the elements in B fixed under each $g \in G$. We shall show that B contains a projective group algebra CG_f, that is, $CG_f = \oplus_{g \in G} CU_g$, $U_g U_{g'} = U_{gg'} f(g,g')$ for $g, g' \in G$ where $f : G \times G \longrightarrow$ units of C is a factor set.

Theorem 2.1. *Let B be a Galois extension of B^G with an inner Galois group G, $G = \{g \mid g(x) = U_g x U_g^{-1}$ for some $U_g \in B$ and for all $x \in B\}$,* *and C the center of B. Then B contains a projective group algebra CG_f of G over C with a factor set $f : G \times G \longrightarrow$ units of C.*

Proof. Since B is a Galois extension of B^G with Galois group G, B has a G-Galois system $\{x_i, y_i \in B \,|\, i = 1, 2, ..., m$ for some integer $m\}$ such that $\sum_{i=1}^m x_i g(y_i) = \delta_{1,g}$ for each $g \in G$. We claim that $\{U_g \,|\, g \in G\}$ are linearly independent over C. In fact, let $\sum_{g \in G} a_g U_g = 0$ for some $a_g \in C$. Then

$$\sum_{i=1}^{m} x_i \sum_{g \in G} a_g U_g h^{-1}(y_i) = 0 \text{ for each } h \in G \text{ and}$$

$$\sum_{g \in G} a_g \sum_{i=1}^{m} x_i g h^{-1}(y_i) U_g = \sum_{g \in G} a_g \delta_{1, gh^{-1}} U_g = a_h U_h.$$

Noting that $a_g \in C$ and $U_g h^{-1}(y_i) = g h^{-1}(y_i) U_g$, we have that

$$\sum_{i=1}^{m} x_i \sum_{g \in G} a_g U_g h^{-1}(y_i) = \sum_{g \in G} a_g \sum_{i=1}^{m} x_i g h^{-1}(y_i) U_g;$$

and so $a_h U_h = 0$. But U_h is invertible in B, so $a_h = 0$ for each $h \in G$. Thus $\{U_g \,|\, g \in G\}$ are linearly independent over C. Moreover, for any $g, h \in G$, $U_{gh} x U_{gh}^{-1} = gh(x) = U_g U_h x U_h^{-1} U_g^{-1}$ for all $x \in B$, so $x U_{gh}^{-1} U_g U_h = U_{gh}^{-1} U_g U_h x$ for all $x \in B$. Hence $U_{gh}^{-1} U_g U_h \in C$ for any $g, h \in G$. Now define $f : G \times G \longrightarrow$ units of C by $f(g, h) = U_{gh}^{-1} U_g U_h$. Since $(G, \cdot)$ is associative, f is a factor set such that $U_g U_h = U_{gh} f(g, h)$. Therefore $\sum_{g \in G} C U_g = C G_f$, a projective group algebra of G over C with factor set f. □

Next we show an equivalent condition for a Galois projective group algebra CG_f to be contained in B as given in Theorem 2.1.

Lemma 2.1. *Let B and CG_f be given in Theorem 2.1, Z the center of G, and $\overline{G}$ the restriction of G to CG_f. Then $\overline{G} \cong G/K$ where $K = \{g \in Z \,|\, f(g, h) = f(h, g)$ for all $h \in G\}$.*

Proof. Since CG_f is invariant under each $g \in G$, $\overline{G}$ is a group. Let $\overline{g} = \overline{1} \in \overline{G}$. Then $g(U_h) = U_g U_h U_g^{-1} = U_h$ for each $h \in G$. Hence $U_g U_h = U_h U_g$. Thus $U_{gh} f(g, h) = U_{hg} f(h, g)$. This is equivalent to that $gh = hg$ and $f(g, h) = f(h, g)$ for each $h \in G$, that is, $g \in K$. Noting that $g \longrightarrow \overline{g}$ is a group homomorphism, we have that $\overline{G} \cong G/K$. □

Theorem 2.2. *Let B be a Galois extension of B^G with an inner Galois group G of order n invertible in B and CG_f as given in Theorem 2.1.*

Then CG_f is a central Galois algebra with an inner Galois group $\overline{G}$ (the restriction of G to CG_f) if and only if $\{U_{\overline{g}}\,|\,\overline{g}\in\overline{G}\}$ are linearly independent over S where $U_{\overline{g}}=U_g$ for each $g\in G$ and S is the center of CG_f.

Proof. ($\Longrightarrow$) Since the order of G is invertible in B, CG_f is a separable algebra over C. Hence CG_f is an Azumaya S-algebra ([3], Theorem 3.8, page 55). By hypothesis, CG_f is a central Galois algebra with an inner Galois group $\overline{G}$, so $CG_f = S\overline{G}_{\overline{f}}$ ([1], Theorem 6), a projective group algebra of $\overline{G}$ over S with a factor set $\overline{f}:\overline{G}\times\overline{G}\longrightarrow$ units of the center of S induced by $f: G\times G\longrightarrow$ units of C. Thus $\{U_{\overline{g}}\,|\,\overline{g}\in\overline{G}\}$ are linearly independent over S.

($\Longleftarrow$) By hypothesis, $\{U_{\overline{g}}\,|\,\overline{g}\in\overline{G}\}$ are linearly independent over S, so $S\overline{G}_{\overline{f}}=\oplus_{\overline{g}\in\overline{G}}SU_{\overline{g}}$ is a projective group algebra of $\overline{G}$ over S with factor set $f:\overline{G}\times\overline{G}\longrightarrow$ units of S induced by $f: G\times G\longrightarrow$ units of C. By Lemma 2.1, $\{U_g\,|\,\overline{g}=\overline{1}\in\overline{G}\}=\{U_g\,|\,g\in K\}$, so $\{U_g\,|\,g\in K\}\subset S$. Hence $CG_f=\oplus_{\overline{g}\in\overline{G}}SU_{\overline{g}}=S\overline{G}_{\overline{f}}$. Noting that CG_f is an Azumaya S-algebra, we conclude that $S\overline{G}_f$ is an Azumaya S-algebra. But then $S\overline{G}_f$ is a central Galois S-algebra with an inner Galois group $\overline{G}$ ([2], Theorem 3). Thus CG_f is a central Galois algebra over S with an inner Galois group $\overline{G}$. □

By using Theorem 2.2, we obtain several characterizations for a Galois extension B generated by $\{U_g\,|\,g\in G\}$ over B^G. We recall that C is the center of B, S the center of CG_f, Z the center of G, and $K=\{g\in Z\,|\,f(g,h)=f(h,g)$ for all $h\in G\}$.

Theorem 2.3. *Let B be a Galois extension of B^G with an inner Galois group G of order n invertible in B. Then the following are equivalent:*

(1) $B=\sum_{g\in G}B^GU_g$, i.e., B is generated by $\{U_g\,|\,g\in G\}$ over B^G;

(2) $B=B^GG_f$, a projective group ring of G over B^G with factor set $f:G\times G\longrightarrow$ units of C;

(3) $C=S$;

(4) $\sum_{g\in G}CU_g$, the subring of B generated by $\{U_g\,|\,g\in G\}$ over C, is a central Galois C-algebra with Galois group $\overline{G}\cong G$;

(5) $\sum_{g\in G}CU_g$ is an Azumaya C-algebra;

(6) $K=\langle 1\rangle$ and $\{U_{\overline{g}}\,|\,\overline{g}\in\overline{G}\}$ are linearly independent over S.

Proof. (1) $\Longrightarrow$ (3) Since $C\subset B^G$ and since $B=\sum_{g\in G}B^GU_g$, $B=B^G(\sum_{g\in G}CU_g)$. Moreover, since $g(x)=U_gxU_g^{-1}=x$ for all $x\in B^G$ and $g\in G$, we have that $S\subset C$. Hence $S=C$.

(3) $\Longrightarrow$ (4) Since $\sum_{g\in G}CU_g=CG_f$ by Theorem 2.1, CG_f is an Azumaya S-algebra. By hypothesis, $S=C$, so CG_f is an Azumaya C-

algebra. Hence $\sum_{g\in G} CU_g$ $(= CG_f)$ is a central Galois C-algebra with Galois group $\overline{G} \cong G$ ([2], Theorem 3).

(4) $\Longrightarrow$ (5) It is clear.

(5) $\Longrightarrow$ (2) Since $\sum_{g\in G} CU_g = CG_f$ by Theorem 2.1, statement (5) implies that CG_f is a central Galois C-algebra with Galois group $\overline{G} \cong G$ ([2], Theorem 3). Noting that $CG_f \subset \sum_{g\in G} B^G U_g$, we have that $\sum_{g\in G} B^G U_g$ is a Galois extension of B^G with a same G-Galois system as CG_f. But B is a Galois extension of B^G with Galois group G, so $B = \sum_{g\in G} B^G U_g$. Moreover, since CG_f is a central Galois C-algebra with Galois group $\overline{G} \cong G$, there exists a G-Galois system $\{x_i, y_i \in CG_f \,|\, i = 1, 2, ..., m$ for some integer $m\}$ such that $\sum_{i=1}^m x_i g(y_i) = \delta_{1,g}$ for each $g \in G$. Noting that $bx_i = x_i b$ for all $b \in B^G$, we can show that $\{U_g \,|\, g \in G\}$ are linearly independent over B^G by the same proof of Theorem 2.1. Thus $B = \sum_{g\in G} B^G U_g = B^G G_f$.

(2) $\Longrightarrow$ (1) It is clear.

(3) $\Longrightarrow$ (6) Since $\overline{G} \cong G$ and $\overline{G} \cong G/K$, we have that $K = \langle 1 \rangle$. Moreover, since $\sum_{g\in G} CU_g$ is a central Galois C-algebra and $C = S$, $\{U_{\overline{g}} \,|\, \overline{g} \in \overline{G}\}$ are linearly independent over S.

(6) $\Longrightarrow$ (3) Since $K = \langle 1 \rangle$ and $\overline{G} \cong G/K$, we have that $\overline{G} \cong G$. Moreover, since $\sum_{g\in G} CU_g$ is a separable C-algebra, $\sum_{g\in G} CU_g$ is an Azumaya S-algebra ([3], Theorem 3.8, page 55). By hypothesis, $\{U_{\overline{g}} \,|\, \overline{g} \in \overline{G}\}$ are linearly independent over S, so $\sum_{g\in G} CU_g = \sum_{g\in G} SU_g = SG_{\overline{f}}$ which is an Azumaya S-algebra. But then $SG_{\overline{f}}$ is a central Galois S-algebra with an inner Galois group $\overline{G}$ ([2], Theorem 3). Noting that $\overline{G} \cong G$, we have that $C = S$. This completes the proof. □

3 The Commutator Subring

By keeping the notations in section 2, let B be a Galois extension of B^G with an inner Galois group G of order n invertible in B, $G = \{g \,|\, g(x) = U_g x U_g^{-1}$ for some $U_g \in B$ and for all $x \in B\}$, C the center of B, Z the center of G, and $K = \{g \in Z \,|\, f(g,h) = f(h,g)$ for all $h \in G\}$. In this section, we shall study the commutator (also called centralizer) subring $V_B(B^G)$ of B^G in B. Assume that B is an Azumaya C-algebra. It will be shown that $V_B(B^G)$ is a central Galois algebra with an inner Galois group $\overline{G}$ $(= G/K)$ if and only if $B^K = B^G \cdot (CG_f)$.

Theorem 3.1. *Let B be a Galois extension of B^G with an inner Galois group G of order n invertible in B. If B is an Azumaya C-algebra, then $V_B(B^G) = CG_f$.*

Proof. Since n, the order of G, is invertible in B, the projective group algebra CG_f is a separable subalgebra of the Azumaya C-algebra B. Hence $V_B(V_B(CG_f)) = CG_f$ by the double centralizer property of Azumaya algebras ([3], Theorem 4.3, page 57). Noting that $V_B(CG_f) = B^G$, we have that $V_B(B^G) = CG_f$. □

As given in Theorem 2.2, the central Galois algebra CG_f is characterized in terms of the freeness property of $\{U_{\overline{g}} \,|\, \overline{g} \in \overline{G}\}$ over the center of CG_f. Next we show a characterization of the central Galois algebra CG_f in terms of the Galois extension B^K over B^G.

Theorem 3.2. *Let B be an Azumaya C-algebra and a Galois extension of B^G with an inner Galois group G of order n invertible in B. Then CG_f is a central Galois algebra with Galois group $\overline{G}$ if and only if $B^K = B^G \cdot (CG_f)$.*

Proof. ($\Longrightarrow$) Since CG_f is a central Galois algebra with Galois group $\overline{G}$ $(= G/K)$, CG_f has a $\overline{G}$-Galois system. Clearly, $CG_f \subset B^G \cdot (CG_f) \subset B^K$ and $(B^G \cdot (CG_f))^G = (B^K)^G = B^G$, so $B^G \cdot (CG_f)$ and B^K are also Galois extensions with the same Galois system as CG_f by noting that the restrictions of G to $B^G \cdot (CG_f)$ and B^K are isomorphic with $\overline{G}$ of G to CG_f. Thus $B^K = B^G \cdot (CG_f)$.

($\Longleftarrow$) By hypothesis, B is a Galois extension of B^G with an inner Galois group G of order n invertible in B, so B^K is a Galois extension of B^G with an inner Galois group G/K. Let S be the center of CG_f. Since CG_f is a separable C-subalgebra of the Azumaya C-algebra B, $V_B(V_B(CG_f)) = CG_f$. Hence CG_f, B^G $(= V_B(CG_f))$, and $B^G \cdot (CG_f)$ have the same center S. By hypothesis, $B^K = B^G \cdot (CG_f)$. Thus S is the center of B^K. But B^K is a Galois extension of B^G with an inner Galois group $\overline{G}$ $(= G/K)$, so B^K contains the separable projective group algebra $S\overline{G}_{\overline{f}}$ where $f : \overline{G} \times \overline{G} \longrightarrow$ units of S induced by $f : G \times G \longrightarrow$ units of C by Theorem 2.1. Thus $\{U_{\overline{g}} \,|\, \overline{g} \in \overline{G}\}$ are linearly independent over S. Therefore CG_f is a central Galois algebra with Galois group $\overline{G}$ by Theorem 2.2. □

Corollary 3.1. *Let B be an Azumaya C-algebra and a Galois extension of B^G with an inner Galois group G of order n invertible in B. Then B^K is a Galois projective group ring of $\overline{G}$ over $B^G S$ with factor set $\overline{f} : \overline{G} \times \overline{G} \longrightarrow$ units of C.*

Proof. By Theorem 3.2, $B^K = B^G \cdot (CG_f)$ and $CG_f = S\overline{G}_{\overline{f}}$, so $B^K = B^G \cdot (CG_f) = B^G(S\overline{G}_{\overline{f}}) = (B^G S)\overline{G}_{\overline{f}}$ which is a Galois projective group ring of $\overline{G}$ over $B^G S$ with factor set $\overline{f} : \overline{G} \times \overline{G} \longrightarrow$ units of C. □

We conclude the present paper with two examples to illustrate the results for Theorem 2.1 and Theorem 2.3.

Example 3.1. (See Examples 1 and 2 in [4]) Let A be any noncommutative ring with 4 invertible in A, C the center of A, $B = M_2(A)$, the 2 by 2 matrix ring over A, and $G = \{g_1, g_2, g_3, g_4\}$ where $g_i(x) = U_i x U_i^{-1}$, $i = 1, 2, 3, 4$, for all $x \in B$ and $U_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $U_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $U_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $U_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then

(1) The center of B is $\{\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \mid c \in C\} \cong C$,

(2) $B^G = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in A\} \cong A$,

(3) B is a Galois extension of B^G with an inner Galois group G of order 4 invertible in B, and

(4) B contains the projective group algebra $C\overline{G}_f$ of $\overline{G}$ over C. □

Example 3.2. Let $B = M_2(R[i, j, k])$ be the 2×2 matrix ring over the real quaternion $R[i, j, k]$ with the inner automorphism group $G = \{1, g_i, g_j, g_k\}$ induced by iI, jI, kI, the scalar matrices. Then

(1) $B^G = M_2(R)$ and the center of B is R,

(2) $RG_f = R \oplus Ri \oplus Rj \oplus Rk$, a projective group algebra with center R, and so it is a central Galois algebra over R with an inner Galois group $\overline{G} \cong G$, and

(3) $B = B^G[i, j, k] = B^G\overline{G}_f$, a Galois projective group ring of $\overline{G}$ over B^G. □

Acknowledgment

This paper was revised under the suggestions of the referee and written under the support of a Caterpillar Fellowship at Bradley University. The authors would like to thank the referee for the valuable suggestions and 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, Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.*, **10** (1966), 287-295.

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

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

[5] G. Szeto and Y.-F. Wong, On Azumaya projective group rings, *Azumaya Algebras, Actions, and Modules* (Bloomington, IN, 1990), Contemporary Math. **124**, Amer. Math. Soc., Providence, RI, 1992, 251-256.

[6] G. Szeto and L. Xue, Skew Group Rings which are Galois, *International Journal of Mathematics and Mathematical Sciences*, **23** (1999), no. 4, 279-283.

[7] G. Szeto and L. Xue, The Structure of Galois Algebras, *Journal of Algebra*, **237** (2001), no. 1, 238-246.

[8] G. Szeto and L. Xue, On Galois Algebras with an Inner Galois Group, *East-West Journal of Mathematics*, Special Volume (2004), 101-106.

[9] G. Szeto and L. Xue, The Galois Algebra with Galois Group which is the Automorphism Group, *Journal of Algebra*, **293** (2005), no. 1, 312-318.