International Journal of Algebra, Vol. 5, 2011, no. 5, 233 - 239

A Structure of Galois Extensions with an Inner Galois Group

George Szeto

Department of Mathematics
Bradley University
Peoria, Illinois 61625, USA
szeto@bradley.edu

Lianyong Xue

Department of Mathematics
Bradley University
Peoria, Illinois 61625, USA
lxue@bradley.edu

Abstract

Let B be a Galois extension of B^G with an inner Galois group G where $G = \{g_i \,|\, g_i(x) = U_i x U_i^{-1}$ for some $U_i \in B$ and for all $x \in B$, $i = 1, 2, \cdots, n$ for some integer n invertible in $B\}$. Then B is a composition of two Galois extensions $B \supset B^K$ with an inner Abelian Galois group K and $B^K \supset B^G$ with an inner Galois group G/K where $K = \{g \in G \,|\, g(U_i) = U_i$ for each $i\}$. Descriptions of $B \supset B^K$ and $B^K \supset B^G$ are given.

Mathematics Subject Classification: 13B05, 16W20

Keywords: Galois extensions, Galois algebras, central Galois algebras, Azumaya algebras, projective group algebras

1 Introduction

The class of central Galois algebras over a commutative ring with an inner Galois Group has been investigated ([1], [2]). It was shown that any central Galois algebra B over R with an inner Galois group G is an Azumaya projective group algebra RG_f of G over R with a factor set $f\colon G \times G \longrightarrow$ units of R ([1], Theorem 6). Conversely, any Azumaya projective group algebra RG_f over

R with a factor set f: $G \times G \longrightarrow$ units of R is a central Galois algebra with an inner Galois group induced by the basis elements of RG_f ([2], Theorem 3). In case R is indecomposable, in [2], all central Galois algebras with an Abelian inner Galois group G are found, and an application to the commutative theory is obtained by giving a Kummer type theorem for Abelian extensions. Moreover some types of Galois extensions of a ring (not necessarily commutative) with an inner Galois group have been studied such as crossed products, skew polynomial rings, and Hirata separable extensions ([5], [8], [9], [10]). The purpose of the present paper is to continue the study of a Galois extension B of a ring B^G with an inner Galois group G where $G = \{g_i \,|\, g_i(x) = U_i x U_i^{-1}$ for some $U_i \in B$ and for all $x \in B$, $i = 1, 2, \cdots, n$ for some integer n invertible in $B\}$. We shall show that B is a composition of two Galois extensions: (1) $B \supset B^K$ with an Abelian inner Galois group K as studied in [2], where $K = \{g \in G \,|\, g(U_i) = U_i$ for each $i\}$ such that B^K is a central algebra over CK_f and contains B^G and CG_f as commutator subalgebras of B over C, and (2) $B^K \supset B^G$ with an inner Galois group G/K. Moreover, characterizations are given for B^K being a projective group ring of G/K over B^G.

Throughout this paper, we assume that B is a ring with 1, G a finite automorphism group of B of order n for some integer n invertible in B, C the center of B, B^G the set of elements in B fixed under each element in G. 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 $g \in G$. A ring B is called a Galois algebra over R if B is a Galois extension of R which is contained in C, and a central Galois algebra over C if B is a Galois extension of C. Let A be a subring of B with the same identity 1. The commutator subring of A in B is denoted by $V_B(A)$. For the definitions of a separable or a Hirata separable extension and an Azumaya algebra, see [3] and [7]. As given in [1], a projective group ring RG_f of a group G of order n over a ring R with a factor set f: $G \times G \longrightarrow$ units of R is a ring with an R-basis $\{U_i,\, i = 1, 2, \cdots, n \,|\, rU_i = U_i r$ for each $r \in R$ and $U_i U_j = U_k f(g_i, g_j)$ where $g_i g_j = g_k \in G\}$.

2 A Composition of 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, C the center of B, and $K = \{g \in G \,|\, g(U_i) = U_i$ for each $i = 1, 2, \cdots, n\}$. Then we shall show that B is a composition of two Galois extensions: (i) B is a Galois extension of B^K with an Abelian inner Galois group K such that B^K is a central algebra over CK_f where CK_f is a projective group algebra of K over C with a factor set f: $K \times K \longrightarrow$ units of C, and B^K contains B^G and CG_f as commutator subalgebras of B over C, and (ii) $B^K \supset B^G$ with an inner Galois group G/K. We begin with a lemma to show that B contains a projective group algebra CG_f, and that G contains a normal Abelian inner subgroup K.

Lemma 2.1 *Let B be a Galois extension of B^G with an inner Galois group G, $G = \{g_i \,|\, g_i(x) = U_i x U_i^{-1},\ U_i \in B$ and for all $x \in B$, $i = 1, 2, \cdots, n$ for some integer n invertible in $B\}$. Then (i) B contains a separable projective group algebra CG_f of G over C with factor set $f : G \times G \longrightarrow$ units of C where $f(g_i, g_j) = U_i U_j U_k^{-1}$ and $g_i g_j = g_k$, and (ii) K is an Abelian normal subgroup of G.*

Proof. (i) By Theorem 2.1 in [10], B contains a separable projective group algebra CG_f of G over C with factor set $f : G \times G \longrightarrow$ units of C where $f(g_i, g_j) = U_i U_j U_k^{-1}$ and $g_i g_j = g_k$. Moreover, since the order n of G is invertible in B, CG_f is separable over C.

(ii) Since CG_f is invariant under the action of G and $K = \{g_j \in G \,|\, g_j(U_i) = U_i$ for each $i = 1, 2, \cdots, n\}$, $U_j U_i = U_i U_j$ for each $g_j \in K$ and each $i = 1, 2, \cdots, n$, that is, $g_j g_i = g_i g_j$ and $f(g_j, g_i) = f(g_i, g_j)$ for each $g_j \in K$ and for all $i = 1, 2, \cdots, n$. Thus K is a normal Abelian inner subgroup of G.

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 C the center of B. Then B is a composition of two Galois extensions: (1) B is a Galois extension of B^K with an Abelian inner Galois group K such that B^K is a central algebra over CK_f and contains B^G and CG_f as commutator subalgebras of B over C, and (2) B^K is a Galois extension of B^G with an inner Galois group G/K.*

Proof. (1) Since B is a Galois extension of B^G with an inner Galois group G, B is a Galois extension of B^K with an Abelian inner Galois group K by Lemma 2.1-(ii). Next, we claim that B^K is a central algebra over CK_f and contains B^G and CG_f as commutator subalgebras of B over C. In fact, since B is a Galois extension of B^G with an inner Galois group G, B is a Hirata separable extension of B^G ([7], Corollary 3). Since B is a Galois extension of B^G again, B is left or right B^G-finitely generated projective. Moreover, since n is invertible in B by hypothesis, B^G is a direct summand of B as a B^G-bimodule. Hence $V_B(V_B(B^G) = B^G$ and $V_B(B^G)$ is a separable C-algebra ([6], Theorem 1) for B^G is separable over itself. Noting that CG_f is a separable C-subalgebra of $V_B(B^G)$, we have $CG_f = V_B(V_B(CG_f)$ ([6], Theorem 1). But $V_B(CG_f) = B^G$, so $V_B(B^G) = CG_f$. Thus B^G and CG_f are commutator subalgebras of B over C. Similarly, the pair B^K and CK_f are commutator subalgebras of B over C because B is a Galois extension of B^K with an inner Galois group K of an order invertible in B. Thus $V_B(B^K) = CK_f \subset B^K$, so

$V_{B^K}(B^K) = CK_f$, that is, CK_f is the center of B^K; and so B^K is a central algebra over CK_f.

(2) Since n is a unit in B and K is a normal subgroup of G by Lemma 2.1, B^K is a Galois extension of B^G with inner Galois group G/K.

3 The Galois Subring B^K

In this section, B^K as given in Theorem 2.2 is described. Equivalent conditions are given for B^K which is a projective group ring of G/K over B^G. Thus more properties of B^K can be found. We shall keep all notations as given in section 2 for a Galois extension B of B^G with an inner Galois group G of order n invertible in B.

Theorem 3.1 *The following statements are equivalent:*
(1) The projective group algebra CG_f is a central Galois algebra over CK_f with Galois group G/K;
(2) CG_f is a central algebra over CK_f;
(3) B^G is a central algebra over CK_f;
(4) $B^K = B^G(G/K)_{\overline{f}}$ which is a projective group ring of G/K over B^G with factor set $\overline{f} : G/K \times G/K \longrightarrow$ units of C where $\overline{f}$ is induced by f;
(5) $B^K = \sum_{g \in G} B^G U_g$.

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

(2)$\Longrightarrow$(1) Let $S = \{U_{\overline{g}} \,|\, \overline{g} \in G/K\}$ where $U_{\overline{g}} = U_g$ for an element $g \in G$. We claim that S are linearly independent over CK_f. In fact, let $\sum_{U_{\overline{g}} \in S} a_{\overline{g}} U_{\overline{g}} = 0$ for some $a_{\overline{g}} \in CK_f$. Then $a_{\overline{g}} = \sum_{h \in K} c_{g,h} U_h$ for some $c_{g,h} \in C$; and so $\sum_{U_{\overline{g}} \in S} \sum_{h \in K} c_{g,h} U_h U_{\overline{g}} = 0$, that is, $\sum_{U_{\overline{g}} \in S} \sum_{h \in K} c_{g,h} f(h,g) U_{hg} = 0$. Thus $c_{g,h} f(h,g) = 0$. Since $f(h,g)$ is a unit in C, $c_{g,h} = 0$ for each $U_{\overline{g}} \in S$ and $h \in K$. Therefore $a_{\overline{g}} = 0$ for each $U_{\overline{g}} \in S$. This implies that S are linearly independent over CK_f; and so $CG_f = (CK_f)(G/K)_{\overline{f}}$, a projective group algebra G/K over CK_f with factor set $\overline{f} : G/K \times G/K \longrightarrow$ units of C induced by $f : G \times G \longrightarrow$ units of C. Noting that n, the order of G, is a unit in C, we conclude that $(CK_f)(G/K)_{\overline{f}}$ is a separable CK_f-algebra. Moreover, by hypothesis, CK_f is the center of CG_f, so CG_f is an Azumaya CK_f-algebra. Consequently, CG_f $(= (CK_f)(G/K)_{\overline{f}})$ is a central Galois algebra over CK_f with Galois group G/K ([2], Theorem 3).

(2)$\Longleftrightarrow$(3) By Theorem 2.2, B^G and CG_f are commutator subalgebras of B, so it can be verified that B^G and CG_f have the same center.

(1)$\Longrightarrow$(4) Since CG_f is a central Galois algebra over CK_f with Galois group G/K, $B^G(CG_f)$ is a Galois extension of B^G with Galois group G/K. On the other hand, B^K is also a Galois extension of B^G with Galois group

G/K such that $B^G(CG_f) \subset B^K$, so $B^G(CG_f) = B^K$ from the fact that the Galois group of $B^G(CG_f)$ is induced by and isomorphic with G/K. Therefore $B^K = B^G(CG_f) = B^G(CK_f)(G/K)_{\overline{f}} = B^G(G/K)_{\overline{f}}$.

(4)$\Longrightarrow$(5) It is clear because $CK_f \subset B^G$.

(5)$\Longrightarrow$(2) By hypothesis, $B^K = \sum_{g\in G} B^G U_g$, so $B^K = B^G G_f = B^G(CG_f)$. By Theorem 2.2, B^G and CG_f are commutator subalgebras of B, so that $B^K = B^G(CG_f)$ implies that B^K, B^G, and CG_f have the same center. But the center of B^K is CK_f by Theorem 2.2 again, so CK_f is the center of CG_f.

Theorem 3.1 implies some consequences in two special cases: (i) $K = \langle 1 \rangle$, and (ii) B^G is a separable CK_f-algebra. In case $K = \langle 1 \rangle$, Theorem 3.1 derives a result for a projective group ring, $B = B^G G_f$ which generalizes the structure theorem for an Azumaya projective group algebra as given in [2]. In case B^G is a separable CK_f-algebra, Theorem 3.1 gives a stronger structure theorem for B^K.

Corollary 3.2 *By keeping the notations of Theorem 3.1, the following statements are equivalent:*

(1) CG_f is a central Galois algebra over CK_f with Galois group G/K and B^G is a separable CK_f-algebra;

(2) CG_f is a central algebra over CK_f and B^G is a separable CK_f-algebra;

(3) B^G is an Azumaya algebra over CK_f;

(4) $B^K = B^G(G/K)_{\overline{f}}$ as Azumaya algebras over CK_f;

(5) $B^K = \sum_{g\in G} B^G U_g$ as Azumaya algebras over CK_f.

We note that B is an Azumaya C-algebra if and only if B^K is a separable C-algebra. We shall show that B is a Hirata separable extension of CG_f and CK_f respectively.

Theorem 3.3 *Assume B is an Azumaya C-algebra. Then B is a Hirata separable extension of both CG_f and CK_f respectively such that both CG_f and CK_f are direct summands of B as a bimodule over themselves, respectively.*

Proof. Since n is a unit in B, CG_f and CK_f are separable C-subalgebras of B. By hypothesis, B is an Azumaya C-algebra, so B is projective over CG_f and CK_f respectively ([3], Proposition 2.3, page 48). Hence B is a Hirata separable extension of both CG_f and CK_f respectively ([4], Theorem 1). Moreover, both CG_f and CK_f are separable C-subalgebras of the Azumaya algebra B, so they are direct summands of B as a bimodule over themselves.

We conclude the present paper with two examples to demonstrate Galois extensions with an inner Galois group and an Abelian inner Galois group, respectively.

Example 1. Let R be a central Galois algebra with Galois group G and $B = \Delta(R, G, f)$ the crossed product of G over R with a trivial factor set f. Then (1) B is a Galois extension of $B^{\overline{G}}$ with an inner Galois group $\overline{G}$ induced by G;

(2) the center of $\Delta(R, G, f) = R_0 =$ the center of $R^G G_f$ where R_0 is the center of R;

(3) B contains $R_0 G_f$, a projective group algebra of G over R_0;

(4) $R_0 G_f$ is not a central Galois algebra with Galois group $\overline{G}$ induced by G where $\overline{G} = G/K$ and K is the center of G;

(5) $B^K = R^G G_f$; and

(6) $B \supset B^K$ is a Galois extension with an Abelian Galois group K but $B^K \supset B^G$ is not a Galois extension with Galois group G/K.

Example 2. Let R be a commutative Galois algebra with a cyclic Galois group $\langle\rho\rangle$ of order n invertible in R, and $B = R[x, \rho] = R[X, \rho]/\langle X^n - a\rangle$ for some a invertible in R^ρ where $\langle X^n - a\rangle$ is the ideal of $R[X, \rho]$ generated by $X^n - a$. Then

(1) $B = R[x, \rho]$ is a separable skew polynomial ring over R with a basis $\{1, x, x^2, \cdots, x^{n-1} \mid x^n = a\}$ where $xr = \rho(r)x$ for any $r \in R$;

(2) $B \cong R\langle\rho\rangle_f$, a crossed product of $\langle\rho\rangle$ over R with factor set $f : \langle\rho\rangle \times \langle\rho\rangle \longrightarrow$ units of R by $f(\rho^i, \rho^j) = \begin{cases} 1 & \text{if } i + j < n \\ a & \text{if } i + j \geq n; \end{cases}$

(3) $B \supset B^\rho$ is a Galois extension with an Abelian inner Galois group $\langle\overline{\rho}\rangle$ induced by ρ;

(4) the center of B is R^ρ;

(5) B contains $R^\rho\langle\overline{\rho}\rangle_f$, a projective group algebra of $\langle\overline{\rho}\rangle$ over R^ρ with factor set f;

(6) $R^\rho\langle\overline{\rho}\rangle_f$ is a commutative separable R^ρ-algebra, so $K = \langle 1\rangle$; and hence $B^K = B$.

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, 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] S. Ikehata, Note on Azumaya Algebras and H-Separable Extensions, *Math. J. Okayama Univ.,* **23** (1981), 17-18.

[5] S. Ikehata, On H-separable polynomials of prime degree, *Math. J. Okayama Univ.* **33** (1991), 21-26.

[6] K. Sugano, On Centralizers In Separable Extensions II, *Osaka J. Math.*, **8** (1971), 465-469.

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

[8] G. Szeto and L. Xue, Skew Group Rings which are Galois, *International Journal of Mathematics and Mathematical Sciences,* **23**(4) (1999), 279-283.

[9] G. Szeto and L. Xue, On Splitting Rings for Azumaya Skew Polynomial Rings, *Algebra Colloquium,* **8**(1) (2001), 25-32.

[10] G. Szeto and L. Xue, On Galois Extensions with an Inner Galois Group, *Recent Developments in Algebra and Related Area*, ALM 8, 239-245, Higher Education Press and International Press Beijing-Boston, 2008.

Received: September, 2010