On Galois Extensions for Separable Group Rings

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 $R$ be a ring with 1, $G$ a group, and $RG$ a group ring with center $C$. Assume $RG$ is an Azumaya $C$-algebra. Then the inner automorphism group $G$ of $RG$ induced by the elements of $G$ is finite, and $RG$ is not a Galois extension of $(R)G$ with Galois group $G$. For a proper subgroup $K$ of $G$ with an invertible order, the following are equivalent:

1. $RG$ is a Galois extension of $(R)K$ with Galois group $K$;
2. $RG$ is a projective right $(R)K$-module and the centralizer of $(R)K$ is $\oplus \sum_{\gamma \in \mathbb{K}} J_{\gamma}$ where $J_{\gamma} = \{a \in R \mid ax = \gamma(x)a \text{ for each } x \in R\}$; and
3. $\{g \in G \mid g \text{ is a representative of } \gamma \in \mathbb{K}\}$ are linearly independent over $C$. Moreover, we call $f : \mathbb{K} \longrightarrow (R)K$ the Galois map from the set of subgroups of $G$ to the set of subalgebras of $RG$. Then $f$ is one-to-one from a set of Galois groups $\mathbb{K}$ of $RG$ to the set of separable subalgebras $(R)K$ of $RG$.

Mathematics Subject Classification: 16S35, 16W20

Keywords: Galois extensions, Group rings, separable extensions, Azumaya algebras

1 Introduction

Let $R$ be a ring with 1, $G$ a group, and $RG$ a group ring. F. R. DeMeyer and G. J. Janusz ([3], Theorem 1) studied an Azumaya group ring $RG$. When
$R$ is a field and $G$ is a finite group of a nonzero order in $R$. K. Hirata ([5], Proposition 6) proved that for a subgroup $K$ of $G$, $RG$ is a Hirata separable extension of the double centralizer of $RK$ in $RG$. This fact was extended to any Azumaya group ring $RG$ ([12], Lemma 4.2). In the present paper, we study some problems for Galois extensions in $RG$. Let $\mathcal{G}$ be the inner automorphism group of $RG$ induced by the elements of $G$. Then $\mathcal{G}$ is a finite group. We shall show that $RG$ is not a Galois extension of $(RG)^{\mathcal{G}}$ with Galois group $\mathcal{G}$ where $(RG)^{\mathcal{G}}$ is the subring of the elements fixed under each element in $\mathcal{G}$. Moreover, let $B$ be a proper subgroup of $\mathcal{G}$ with an invertible order in $R$. We shall show the following equivalent conditions: (1) $RG$ is a Galois extension of $(RG)^{\mathcal{G}}$, with Galois group $\mathcal{G}$; (2) $RG$ is a projective right $(RG)^{\mathcal{G}}$-module and the centralizer of $(RG)^{\mathcal{G}}$ is $\oplus \sum_{\eta \in \mathcal{K}} J_{\eta}$ where $J_{\eta} = \{a \in RG \mid ax = \eta(x)a \text{ for each } x \in RG\}$; and (3) Let $A$ be a set of representatives of elements of $\mathcal{K}$ in $G$. Then the elements in $A$ are linearly independent over $C$ where $C$ is the center of $RG$. Let $\mathcal{K}$ be a subgroup of $\mathcal{G}$, we call $f : \mathcal{K} \rightarrow (RG)^{\mathcal{G}}$ the Galois map from the set of subgroups of $\mathcal{G}$ to the set of subalgebras of $RG$ over $C$. Then $f$ is one-to-one from a set of Galois groups $\mathcal{K}$ as given in the equivalent conditions to the set of separable subalgebras of $RG$.

2 Basic Definitions and Notations

Let $B$ be a ring with 1 and $A$ a subring of $B$ with the same identity 1. Then $B$ is called a separable extension of $A$ if there exist $\{a_i, b_i \in B, i = 1, 2, ..., k \}$ 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 $B$ where $\otimes$ is over $A$. In particular, $B$ is called an Azumaya algebra if it is a separable extension over its center. A ring $B$ is called a Hirata 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. For more about Azumaya algebras and Hirata separable extensions, see [7] and [11]. Let $G$ be a finite automorphism group of $B$ and $B^G = \{x \in B \mid g(x) = x \text{ for all } g \in G\}$. Then $B$ is called a Galois extension of $B^G$ with Galois group $G$ if there exist elements $\{c_i, d_i \in B, i = 1, 2, ..., m \}$ for some integer $m$ such that $\sum c_i d_i = 1$ and $\sum c_i g(d_i) = 0$ for each $g \neq 1$ in $G$, and $\{c_i, d_i \}$ is called a $G$-Galois system for $B$ ([1]). A Galois extension $B$ of $B^G$ is called a Galois algebra if $B^G$ is contained in the center of $B$, and a central Galois algebra if $B^G$ is equal to the center of $B$ ([9], [10]). The order of a group $G$ is denoted by $|G|$. For a subring $A$ of $B$, we denote by $V_B(A)$ the centralizer (also called commutator) subring of $A$ in $B$. As given in [1], let $R$ be a commutative ring with 1, and $G$ a finite group. Then $\oplus \sum_{g \in G} RU_g$ is called a projective group algebra of $G$ over $R$ if $U_g U_h = f(g, h) U_{gh}$ for $g, h \in G$ and $f : G \times G \rightarrow \{\text{units of } R\}$ is a factor set.
3 Galois Extensions

Let $R$ be a ring with 1, $G$ a group, and $RG$ the group ring of $G$ over $R$ with center $C$. Assume $RG$ is an Azumaya $C$-algebra. We shall show that $RG$ is not a Galois extension of $(RG)^G$ with Galois group $G$ where $G$ is the inner automorphism group of $RG$ induced by the elements of $G$. Moreover, let $K$ be a proper subgroup of $G$ with an invertible order in $R$. We shall characterize a Galois extension $RG$ of $(RG)^K$ with Galois group $K$. Throughout this section, $RG$ is an Azumaya $C$-algebra, and $G$ is the inner automorphism group of $RG$ induced by the elements of $G$. We note that the order $|G|$ of $G$ is finite ([3], Theorem 1). We begin with a lemma.

**Lemma 3.1** Let $R_0$ be the center of $R$. Then $RG$ is a Galois extension of $(RG)^G$ with Galois group $G$ if and only if $R_0G$ is a Galois extension of $(R_0G)^G$ with Galois group $G$.

**(Proof.** ($\iff$) Since $R_0G$ is a Galois extension of $(R_0G)^G$ with Galois group $G$ restricted to $R_0G$, the Galois system for $R_0G$ is also a Galois system for $RG$ with Galois group $G$ isomorphic with $G$ restricted to $R_0G$. Thus $RG$ is a Galois extension of $(RG)^G$ with Galois group $G$.

($\Rightarrow$) By hypothesis, $RG$ is a Galois extension of $(RG)^G$ with Galois group $G$, so the crossed product with trivial factor set of $G$ over $RG$, $\Delta(RG, G) \cong \text{Hom}_{(RG)^G}(RG, RG)$ ([1], Theorem 1). But $RG$ is an Azumaya $C$-algebra, so $RG \cong R \otimes_{R_0} R_0G \cong (R \otimes_{R_0} C) \otimes_C R_0G$ where $C$ is also the center of $R_0G$. Since $R$ is an Azumaya $R_0$-algebra ([3], Theorem 1), $R \otimes_{R_0} C$ is an Azumaya $C$-algebra and $R \otimes_{R_0} C \cong RC$. Thus $\Delta(RG, G) \cong \Delta(RC \otimes_C R_0G, G) \cong \text{Hom}_{(RG)^G}(RC \otimes_C R_0G, RC \otimes_C R_0G)$. Next, $(RG)^G$ is the centralizer of $R_0G$ in $RG$, so $(RG)^G = RG$. This implies that $\Delta(RG, G) \cong \text{Hom}_{RG}(RC \otimes_C R_0G, RC \otimes_C R_0G)$. Noting that $\Delta(RG, G) \cong RC \otimes_C \Delta(R_0G, G)$ by the multiplication map, we have that $RC \otimes_C \Delta(R_0G, G) \cong RC \otimes_C \text{Hom}_C(R_0G, R_0G)$ as Azumaya $C$-algebras. Therefore $\Delta(R_0G, G) \cong \text{Hom}_C(R_0G, R_0G)$ by the commutator theorem for Azumaya algebras ([2], Theorem 4.3, page 57). Noting that $(R_0G)^G = C$ which is the center of the Azumaya algebra $R_0G$, we conclude that $R_0G$ is a Galois extension of $(R_0G)^G$ with Galois group $G$ restricted to $R_0G$ ([1], Theorem 1).

By Lemma 3.1, we can assume that $R$ is commutative to show that $RG$ is not a Galois extension of $(RG)^G$ with Galois group $G$.

**Theorem 3.2** Let $R$ be a commutative ring with 1, $G$ a nonabelian group, and $RG$ a group ring $RG$. If $RG$ is an Azumaya $C$-algebra, then $RG$ is not a Galois extension of $(RG)^G$ with Galois group $G$.}
Thus $RG$ is a Galois extension of $(RG)^G$ with Galois group $G$. Then, $RG$ is a central Galois algebra over $C$ with an inner Galois group $G$. Hence $RG = CG_f$ which is a projective group algebra of $G$ over $C$ ([1], Theorem 6). Thus $\text{rank}_{R}(RG) = |G|$, the order of $G$. Since $C = \oplus RO_i$ where $O_i$ is the sum of the distinct elements in the $i$th orbit of $G$ under the inner automorphism of the elements of $G$, $RZ$ is a direct summand of $C$ where $Z$ is the center of $G$. Hence for some prime ideal $p$ of $RZ$, $C_p$ is a free $(RZ)_p$-module of rank greater than 1, that is, $\text{rank}_{(RZ)_p}(C_p) > 1$ because $G$ is a nonabelian group. But $RG$ is also a free $RZ$-module of rank $|G/Z|$, so $\text{rank}_{RZ}(RG) = \text{rank}_{C}(RG) \cdot \text{rank}_{(RZ)_p}(C_p)$ implies that $|G/Z| = |G/Z| \cdot \text{rank}_{(RZ)_p}(C_p)$. Thus $\text{rank}_{(RZ)_p}(C_p) = 1$. This is a contradiction. Therefore $RG$ is not a Galois extension of $(RG)^G$ with Galois group $G$.

By keeping the notations in Theorem 3.2, let $K$ be a proper subgroup of $G$ with an invertible order in $R$. Next we characterize the Galois extension $RG$ of $(RG)^K$ with Galois group $K$.

**Theorem 3.3** Let $K$ be a proper subgroup of $G$ with an invertible order in $R$. Then the following statements are equivalent: (1) $RG$ is a Galois extension of $(RG)^K$ with Galois group $K$; (2) $RG$ is a projective right $(RG)^K$-module and the centralizer of $(RG)^K$ is $\oplus \sum_{\overline{g} \in K} J_{\overline{g}}$ where $J_{\overline{g}} = \{a \in RG \mid ax = \overline{g}(x)a \}$ for each $x \in RG$; and (3) Let $A = \{g \in G \mid \overline{g} \in K\}$ be a set of representatives of elements of $K$. Then the elements in $A$ are linearly independent over $C$ where $C$ is the center of $RG$.

**Proof.** (1) $\implies$ (2) Since $RG$ is a Galois extension of $(RG)^K$ with Galois group $K$, $RG$ is a projective right $(RG)^K$-module ([1], Theorem 1), and the centralizer of $(RG)^K$ is $\oplus \sum_{\overline{g} \in K} J_{\overline{g}}$ ([6], Proposition 1).

(2) $\implies$ (1) By hypothesis, $RG$ is a projective right $(RG)^K$-module where $RG$ is an Azumaya algebra, so $RG$ is a Hirata separable extension of $(RG)^K$ ([4], Theorem 1). Hence $RG$ is a finitely generated right $(RG)^K$ by the general Zelinsky-Rosenberg theorem as given in [13]. Moreover, $(RG)^K$ is a direct summand of $RG$ as a $(RG)^K$-bimodules ([12], Lemma 4.2), so $(RG)^K$ is a separable subalgebra of $RG$ by the proof of Theorem 3.8 on page 55 in [2]. Thus $(RG)^K$ is the double centralizer of itself ([2], Theorem 4.3, page 57). Now by hypothesis, the centralizer of $(RG)^K$ is $\oplus \sum_{\overline{g} \in K} J_{\overline{g}}$, so $RG$ is a Galois extension of $(RG)^K$ with Galois group $K$ ([7], Proposition 1-(2)).

(2) $\implies$ (3) By the proof of (2) $\implies$ (1), $RG$ is a Hirata separable extension of $(RG)^K$ and a Galois extension of $(RG)^K$ with Galois group $K$. Hence $J_{\overline{g}}$ is a
projective $C$-module of rank 1 for each $\overline{g} \in \overline{K}$ ([7], Theorem 2). Since $Cg = J_{\overline{g}}$ where $g \in G$ such that $\overline{g} \in \overline{K}$, $\{g \in G \mid \overline{g} \in \overline{K}\}$ are linearly independent over $C$.

(3) $\implies$ (2) Since $\{g \in G \mid \overline{g} \in \overline{K}\}$ are linearly independent over $C$, $\oplus \sum Cg = C\overline{K}_f$ is a projective group algebra of $\overline{K}$ over $C$ with a factor set $f : \overline{K} \times \overline{K} \to \{\text{units of } C\}$. But the order of $\overline{K}$ is a unit in $C$, so $C\overline{K}_f$ is a separable subalgebra of $RG$. Hence $(RG)\overline{K} (= V_{RG}(C\overline{K}_f)$, the centralizer of $C\overline{K}_f$ in $RG$) is also a separable subalgebra of $RG$. Thus $RG$ is a projective right $(RG)\overline{K}$-module by the lifting property of a projective module over a separable algebra ([2], Proposition 2.3, page 48). Moreover, since $C\overline{K}_f$ is a separable subalgebra of the Azumaya algebra $RG$, $C\overline{K}_f$ is the double centralizer of itself ([2], Theorem 4.3, page 57). Hence $C\overline{K}_f$ is the centralizer of $(RG)\overline{K}$. Thus the centralizer of $(RG)\overline{K}$ is $\oplus \sum_{\overline{g} \in \overline{K}} J_{\overline{g}}$ because $J_{\overline{g}} = Cg$ for each $\overline{g} \in \overline{K}$.

As given in [8], a Galois extension $B$ of $B^G$ with Galois group $G$ is called a commutator Galois extension with Galois group $G$ if the centralizer $V_B(B^G)$ of $B^G$ in $B$ is a Galois extension of $(V_B(B^G))^G$ with Galois group $G|_{V_B(B^G)} \cong G$.

**Corollary 3.4** Assume $RG$ satisfy an equivalent condition in Theorem 3.3. Then $RG$ is a commutator Galois extension with Galois group $\overline{K}$ if and only if the center of $C\overline{K}_f$ is $C$.

**Proof.** By the proof of Theorem 3.3, $C\overline{K}_f$ is the centralizer of $(RG)\overline{K}$ and $C\overline{K}_f$ is a projective group algebra of $\overline{K}$ over $C$. Noting that $C\overline{K}_f$ is a separable $C$-algebra, we have that $C\overline{K}_f (= V_{RG}((RG)\overline{K}))$ is an Azumaya $C$-algebra if and only if $C\overline{K}_f$ is a Galois extension with Galois group induced by and isomorphic with $\overline{K}$ ([1], Theorem 6).

**Corollary 3.5** Assume $RG$ satisfy an equivalent condition in Theorem 3.3 and $\overline{L}$ a subgroup of $\overline{K}$ such that $\overline{L} = \{\overline{g} \in \overline{K} \mid \overline{g}(a) = a \text{ for each } a \in C\overline{K}\}$. Then $\overline{L}$ is the center of $\overline{K}$ and $RG$ is a Galois and Hirata separable extension of $(RG)\overline{L}$ with Galois group $\overline{L}$.

**Proof.** Clearly, $\overline{L}$ is the center of $\overline{K}$. By Theorem 3.3, since $RG$ is a Galois and Hirata separable extension of $(RG)\overline{K}$, $RG$ is a Galois and Hirata separable extension of $(RG)\overline{L}$ ([7], Theorem 6-(1)).

### 4 The Galois Map

Let $RG$ be an Azumaya $C$-algebra and $\overline{K}$ a subgroup of $\overline{G}$. As studied in [9] and [10], we call the map $f : \overline{K} \to (RG)\overline{K}$ the Galois map from the set
of subgroups of $\mathcal{G}$ to the set of subalgebras of $RG$. Then $f$ induces a map $F : C\overline{K}_f \rightarrow (RG)\overline{K} (= V_{RG}(C\overline{K}_f))$. We shall show that (1) $F$ is one-to-one from the set of separable subalgebras $C\overline{K}_f$ to the set of separable subalgebras of $RG$, and (2) $f$ is one-to-one from the group of subgroups $\mathcal{K}$ with closed set product such that $|\mathcal{K}|^{-1} \in R$ and $RG$ is a Galois extension of $(RG)\overline{K}$ to the set of separable subalgebras of $RG$ as given in Theorem 3.3, that is, $f$ is one-to-one from the group of Galois subgroups $\overline{K}$ of $\mathcal{G}$ with set product to the set of separable subalgebras of $RG$ as given in Theorem 3.3.

**Theorem 4.1** Let $RG$ be an Azumaya C-algebra and $\mathcal{K}$ a subgroup of $\mathcal{G}$. Let $\mathcal{C} = \{C\overline{K}_f | C\overline{K}_f$ is a separable subalgebra of $RG\}$ and $\mathcal{S}$ the set of separable subalgebras of $RG$. Then $F : C\overline{K}_f \rightarrow (RG)\overline{K} (= V_{RG}(C\overline{K}_f))$ is one-to-one from $\mathcal{C}$ to $\mathcal{S}$.

**Proof.** Let $\overline{K}$ and $\overline{H}$ be subgroups of $\mathcal{G}$ such that $C\overline{K}_f$ and $C\overline{H}_f'$ are separable subalgebra of $RG$ and $F(C\overline{K}_f) = F(C\overline{H}_f')$. Then $V_{RG}(C\overline{K}_f) = (RG)\overline{K} = F(C\overline{K}_f) = F(C\overline{H}_f') = (RG)\overline{H} = V_{RG}(C\overline{H}_f')$. But $C\overline{K}_f$ and $C\overline{H}_f'$ are separable subalgebra of the Azumaya algebra $RG$, so $C\overline{K}_f = C\overline{H}_f'$ by the commutator theorem for Azumaya algebras ([2], Theorem 4.3, page 57). Thus $F$ is one-to-one from $\mathcal{C}$ to $\mathcal{S}$.

We call the subgroup $\overline{K}$ a Galois group of $RG$ as given in Theorem 3.3 if $|\overline{K}|^{-1} \in R$ and $RG$ is a Galois extension of $(RG)\overline{K}$, and the group of Galois subgroups of $\mathcal{G}$ with set product is denoted by $\mathcal{D}$.

**Theorem 4.2** Let $f : \overline{K} \rightarrow (RG)\overline{K}$ from a Galois group $\overline{K}$ in $\mathcal{D}$ to $(RG)\overline{K}$ in $\mathcal{S}$. Then $f$ is one-to-one from $\mathcal{D}$ to $\mathcal{S}$.

**Proof.** By Theorem 3.3, $\{g \in G | \overline{g} \in \overline{K}\}$ are linearly independent over $C$, so $C\overline{K}_f (= \oplus \sum Cg)$ is a projective group algebra of $\overline{K}$ over $C$. Now let $\overline{K}$ and $\overline{H}$ be two Galois groups in $\mathcal{D}$ such that $f(\overline{K}) = f(\overline{H})$. Then $C\overline{K}_f$ and $C\overline{H}_f'$ are projective group algebras. Since $|\overline{K}|^{-1}$ and $|\overline{H}|^{-1}$ are in $R$, $C\overline{K}_f$ and $C\overline{H}_f'$ are separable subalgebra of $RG$. Hence $C\overline{K}_f = C\overline{H}_f'$ by Theorem 4.1; and so $\overline{K} = \overline{H}$. Thus $f$ is one-to-one from $\mathcal{D}$ to $\mathcal{S}$.

**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**


Received: August, 2010