Algebra and Discrete Mathematics
Volume 10 **(2010)**. Number 1. pp. 104 – 111

RESEARCH ARTICLE

On separable group rings

George Szeto and Lianyong Xue

Communicated by V. I. Sushchansky

Abstract. Let G be a finite non-abelian group, R a ring with 1, and $\overline{G}$ the inner automorphism group of the group ring RG over R induced by the elements of G. Then three main results are shown for the separable group ring RG over R: (i) RG is not a Galois extension of $(RG)^{\overline{G}}$ with Galois group $\overline{G}$ when the order of G is invertible in R, (ii) an equivalent condition for the Galois map from the subgroups H of G to $(RG)^H$ by the conjugate action of elements in H on RG is given to be one-to-one and for a separable subalgebra of RG having a preimage, respectively, and (iii) the Galois map is not an onto map.

1. Introduction

Galois extensions for rings and Hopf algebras have been intensively investigated ([3], [7], [8], [10], [11]) and many examples are constructed. In [8], the following question was asked: which Azumaya algebra with an automorphism group is also a Galois algebra? In [3], it was shown that any Azumaya projective group algebra RG_f over R is a central Galois algebra over R with an inner Galois group $\overline{G}$ induced by the base elements $\{U_g \mid g \in G\}$ of RG_f where $f : G \times G \longrightarrow \{\text{units of } R\}$ is a factor set ([3], Theorem 3). Recently, this fact was generalized to any separable projective group algebra RG_f ([9]), and equivalent conditions were found for Galois separable skew polynomial rings and Galois crossed products with an inner

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.

2000 Mathematics Subject Classification: *16S35, 16W20.*

Key words and phrases: *Galois extensions, Galois algebras, separable extensions, group rings, group algebras.*

Galois group ([6], [9]). The purpose of the present paper is to show that any separable group ring RG of a non-abelian group G is not a Galois extension of $(RG)^{\overline{G}}$ with an inner Galois group $\overline{G}$ induced by the elements of G. Then we discuss the Galois map $\alpha : H \longrightarrow (RG)^H$ by conjugation from the set of subgroups H of G to the set of separable subalgebras of RG. Also, an equivalent condition is obtained for α being one-to-one and for a separable subalgebra of RG having a preimage, respectively. Moreover, it is shown that α is not onto.

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 $\sum xa_i \otimes b_i = \sum a_i \otimes b_i x$ 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 ([5], Introduction or [8], Definition 2.2). Let G be a finite automorphism group of B and $B^G = \{x \in B \,|\, g(x) = x \text{ for all } g \in G\}$. 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. 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. The order of a group G is denoted by $|G|$. Let D be a subring of B. We denote $V_B(D)$ the centralizer subring of D in B and $G(D) = \{g \in G \,|\, g(d) = d \text{ for all } d \in D\}$.

Let R be a ring with identity 1 and G a finite group. Then RG denotes the group ring of G over R, and RG_f a projective group ring with a factor set $f : G \times G \longrightarrow \{$units in the center 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 $\{U_g \,|\, g \in G\}$ such that $U_g U_h = f(g, h)U_{gh}$; in particular, when R is commutative, a projective group ring RG_f is called a projective group algebra.

3. Group rings of non-abelian groups

In this section, let R be a ring with 1, G a finite non-abelian group of order n for some integer n invertible in R, RG the group ring of G over R, and $\overline{G}$ the inner automorphism group of RG over R induced by the elements of G. It is well known that RG is a separable extension of R. We shall show that the separable group ring RG over R is not a Galois extension of $(RG)^{\overline{G}}$ with Galois group $\overline{G}$. There are two cases in the proof: (i) R

is commutative and (ii) R is noncommutative. We begin with a group algebra RG over a commutative ring R.

Theorem 1. *Let RG be a group algebra of a finite non-abelian group over a commutative ring R and $\overline{G}$ the inner automorphism group of RG over R induced by the elements of G. Then RG is not a Galois extension of $(RG)^{\overline{G}}$ with Galois group $\overline{G}$.*

Proof. Let k be the number of conjugate classes of G and Z the center of G. Then $\overline{G} \cong G/Z$ and $|Z| < k < n$ for G is non-abelian where $|Z|$ is the order of Z and n is the order of G. Let C_i be the sum of all distinct conjugate elements of the ith conjugate class of G for $i = 1, 2, \ldots, k$, and C the center of RG. Then it is known that $C = \sum_{i=1}^{k} RC_i$ which is a free R-module of rank k. Now assume that RG is a Galois extension of $(RG)^{\overline{G}}$ with Galois group $\overline{G}$. Since $(RG)^{\overline{G}} = C$, RG is a central Galois algebra with an inner Galois group $\overline{G}$. Hence $RG = C\overline{G}_f$ which is a projective group algebra of $\overline{G}$ over C with a factor set $f : \overline{G} \times \overline{G} \longrightarrow \{\text{units of } C\}$ ([2], Theorem 6). Thus $n = \text{rank}_R(RG) = \text{rank}_R(C\overline{G}_f) = \text{rank}_R(C) \cdot \text{rank}_C(C\overline{G}_f) = k \cdot |\overline{G}| > |Z| \cdot n/|Z| = n$. This is a contradiction. Thus RG is not a Galois extension of $(RG)^{\overline{G}}$ with Galois group $\overline{G}$. □

Next, we want to extend Theorem 1 to the case of a non-commutative ring R. Let R_0 be the center of R, C the center of RG, and Z the center of G. We first show some properties of $\overline{G}$.

Lemma 1. *By keeping the notations in the above remarks, (1) the center of R_0G is C (the center of RG) and (2) the restriction of $\overline{G}$ to R_0G is isomorphic to $\overline{G}$, that is, $\overline{G}|_{R_0G} \cong \overline{G}$.*

Proof. (1) Let k be the number of conjugate classes of G and C_i the sum of all distinct conjugate elements of the ith conjugate class for $i = 1, 2, \ldots, k$. Then $C = V_{RG}(RG) = V_{\sum_{i=1}^{k} RC_i}(R) = \sum_{i=1}^{k} R_0C_i =$ the center of R_0G.

(2) Since $\overline{G}|_{R_0G} \cong G/Z \cong \overline{G}$, the statement holds. □

The following lemma which is Theorem 2.1 in [13] will play an important role.

Lemma 2. *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 $\sum_{g \in G} CU_g$ is a projective group algebra of G over C with a factor set $f : G \times G \longrightarrow \{\text{units of } C\}$.*

Now, we extend Theorem 1 to a separable group ring RG.

Theorem 2. *Let RG be a group ring of a non-abelian group G of order n invertible in R, R_0 the center of R, and C the center of RG. Then RG is not a Galois extension of $(RG)^{\overline{G}}$ with an inner Galois group $\overline{G}$ induced by the elements of G.*

Proof. Assume that RG is a Galois extension of $(RG)^{\overline{G}}$ with Galois group $\overline{G}$ induced by the elements of G. Then, by Lemma 2, $\sum_{\overline{g}\in\overline{G}} C\overline{g} = C\overline{G}_f$ which is a projective group algebra of $\overline{G}$ over C with factor set $f : \overline{G}\times\overline{G} \longrightarrow \{\text{units of } C\}$. Since $\overline{G} \cong G/Z$ where Z is the center of G, $R_0G = \sum_{\overline{g}\in\overline{G}} R_0Zg \subset \sum_{\overline{g}\in\overline{G}} Cg \subset \sum_{\overline{g}\in\overline{G}} R_0Gg = R_0G$ by Lemma 1. Hence $R_0G = \sum_{\overline{g}\in\overline{G}} Cg = C\overline{G}_f$. By Lemma 1 again, the center of R_0G is C, so the center of $C\overline{G}_f$ is also C. Moreover, since the order n of G is invertible in R, $C\overline{G}_f$ is a separable C-algebra. Thus $C\overline{G}_f$ is an Azumaya C-algebra; and so $C\overline{G}_f$ is a central Galois algebra over C with an inner Galois group $\overline{G}$ ([3], Theorem 3). Therefore the group algebra R_0G is a Galois algebra over C with an inner Galois group $\overline{G}$. This contradicts to Theorem 1, so RG is not a Galois extension of $(RG)^{\overline{G}}$ with an inner Galois group $\overline{G}$. □

4. The Galois map

It is well known that the fundamental theorem holds for any indecomposable commutative ring Galois extension S with Galois group G ([1]), that is, the Galois map $\alpha : H \longrightarrow S^H$ for a subgroup H of G is a one-to-one correspondence between the set of subgroups of G and the set of separable subalgebras of S. Moreover, Galois extensions of a ring satisfying the fundamental theorem were studied in [12]. In this section, we shall discuss two questions of the Galois map for a non-Galois extension RG of $(RG)^G$, $\alpha : H \longrightarrow (RG)^H$ for a subgroup H of G where the action of H on RG is the conjugation by the elements in H: (1) when does $H = G((RG)^H)$ where $G((RG)^H) = \{g \in G \mid g(x) = x \text{ for each } x \in (RG)^H\}$, that is, is α one-to-one? (2) which separable subalgebra A of RG is $(RG)^{G(A)}$, that is, is α onto? For a subgroup H of G, let H act on G by conjugation and O_i be the sum of all distinct conjugate elements of the ith conjugate class of G under the action of H, for $i = 1, 2, \ldots, h$ where h is the number of conjugate classes of G under the action of H.

Lemma 3. *By keeping the notations in the above remark, then $(RG)^H = \sum_{i=1}^{h} RO_i$.*

Proof. Since H is a subgroup of G and $\{g \mid g \in G\}$ is a basis for RG over R, $(RG)^H = \sum_{i=1}^{h} RO_i$ by a direct computation. □

Corollary 1. *Let H and L be subgroups of G. If $(RG)^H = (RG)^L$, then (1) $h = l$, where h and l are the numbers of conjugate classes of G under the conjugation action of H and L respectively, and (2) $\{O_1, O_2, \ldots, O_h\} = \{O'_1, O'_2, \ldots, O'_l\}$ where O_i is the sum of all distinct conjugate elements of the ith conjugate class of G under the action of H and O'_i is the sum of all distinct conjugate elements of the ith conjugate class of G under the action of L.*

Proof. (1) By Lemma 3, $(RG)^H = \sum_{i=1}^{h} RO_i$ and $(RG)^L = \sum_{i=1}^{l} RO'_i$, so $\sum_{i=1}^{h} RO_i = (RG)^H = (RG)^L = \sum_{i=1}^{l} RO'_i$. Since RG is a free R-module with basis $\{g \mid g \in G\}$, $(RG)^H$ is a free R-module with basis $\{O_1, O_2, \ldots, O_h\}$ and $(RG)^L$ is a free R-module with basis $\{O'_1, \ldots, O'_l\}$. Thus $h = l$.

(2) Since $(RG)^H = (RG)^L$, for each $i = 1, 2, \ldots, h$, $O_i \in (RG)^L = \sum_{j=1}^{l} RO'_j$. Hence $O_i = \sum_{j=1}^{l} r_j O'_j$ for some $r_j \in R$. Noting that $\{g \mid g \in G\}$ is a basis for RG over R, we have that r_j is either 0 or 1. Thus $O_i = \sum_{j \in J_i} O'_j$ for some subset J_i of $\{1, 2, \ldots, l\}$. But $\{J_i \mid i = 1, 2, \ldots, h\}$ are disjoint subsets of $\{1, 2, \ldots, l\}$ where $h = l$, so each J_i contains only one O'_j, that is, $O_i = O'_j$ for some j. Therefore $\{O_1, O_2, \ldots, O_h\} = \{O'_1, O'_2, \ldots, O'_l\}$. □

Now we show an equivalent condition for α being a one-to-one map: $(RG)^H = (RG)^L$ implies that $H = L$ for subgroups H and L of G.

Theorem 3. *Let H and L be subgroups of G. Then $H = L$ if and only if $(RG)^H = (RG)^L$ and there exists an element $x \in G$ such that $V_H(x) = V_L(x) = V_{HL}(x)$ where $V_T(x)$ is the centralizer of x in T for a subset T of G.*

Proof. ($\Longrightarrow$) Since $H = L$, the necessity is clear.

($\Longleftarrow$) Since $(RG)^H = (RG)^L$, we can assume that $O_i = O'_i$ for each i by Corollary 1. By hypothesis, there exists an element $x \in G$ such that $V_H(x) = V_L(x) = V_{HL}(x)$. Since x is a term of O_i for some i and $O_i = O'_i$, for any $a \in H$, $axa^{-1} = bxb^{-1}$ for some $b \in L$; and so $(b^{-1}a)x = x(b^{-1}a)$, that is, $b^{-1}a \in V_{HL}(x)$. But $V_L(x) = V_{HL}(x)$, so $b^{-1}a \in L$. Thus $a \in L$ for any $a \in H$. This implies that $H \subset L$. Similarly, $L \subset H$. Therefore $H = L$. □

We recall that for a subset $S \subset RG$, the set $\{g \in G \mid g(s) = s$ for all $s \in S\}$ is denoted by $G(S)$.

Corollary 2. *Let H be a subgroup of G. Then $H = G((RG)^H)$ if and only if there exists an element $x \in G$ such that $V_{G((RG)^H))}(x) \subset V_H(x)$.*

Proof. ($\Longrightarrow$) The necessity is clear.

($\Longleftarrow$) Since $(RG)^H = (RG)^{G((RG)^H)}$ and $H \subset G((RG)^H)$, the statement is an immediate consequence of Theorem 3. □

Since the order of G is invertible in R, RG is a separable group algebra over R; and so it is an Azumaya algebra over its center ([4], Example III, page 41 and Theorem 3.8, page 55). We shall show which separable subalgebra A of the Azumaya algebra RG is equal to $(RG)^{G(A)}$.

Proposition 1. *Assume the order of G is invertible in R. Then for any subgroup H of G, $(RG)^H$ is a separable R-subalgebra of RG.*

Proof. Let $|H| = n$ and $\mathrm{Tr}(x) = \sum_{g\in H} g(x) = \sum_{g\in H} gxg^{-1}$. Then the map $\pi : RG \longrightarrow (RG)^H$ by $\pi(x) = \mathrm{Tr}(n^{-1}x)$ is surjective as a bimodule homomorphism over $(RG)^H$. Hence π splits. Thus $(RG)^H$ is a direct summand of RG as a bimodule over $(RG)^H$. Since $|G|$ is invertible in R, RG is a projective separable R-algebra. This implies that $(RG)^H$ is also a separable R-subalgebra by the proof of Theorem 3.8 in [4] on page 55. □

Theorem 4. *Let C be the center of RG and A a separable subalgebra of the Azumaya algebra RG. Assume the order of G is invertible in R. Then $A = (RG)^{G(A)}$ if and only if $\mathrm{rank}_{C_p}(((RG)^{G(A)})_p) = \mathrm{rank}_{C_p}(A_p)$ for each prime ideal p of C.*

Proof. ($\Longrightarrow$) The necessity is clear.

($\Longleftarrow$) Since RG is an Azumaya algebra over C, it is a finitely generated and projective C-module. Noting that A is a separable subalgebra of RG over C, we have that A is a direct summand of RG as an A-bimodule. Hence $RG = A \oplus A'$ for some A-bimodule A'; and so $\mathrm{rank}_{C_p}(A_p)$ is defined for each prime ideal p of C ([4], page 27). Moreover, since the order of G is invertible in R, the group algebra $C(G(A))$ of $G(A)$ over C is a separable subalgebra of RG over C. Thus $V_{RG}(C(G(A)))$ is a separable subalgebra of RG over C by the commutator theorem for Azumaya algebras ([4], Theorem 4.3, page 57). But $V_{RG}(C(G(A))) = (RG)^{G(A)}$, so $(RG)^{G(A)}$ is a separable subalgebra of RG over C. Clearly, $A \subset (RG)^{G(A)}$, so $(RG)^{G(A)} = A \oplus (A' \cap (RG)^{G(A)})$ (for $RG = A \oplus A'$). By hypothesis, $\mathrm{rank}_{C_p}(((RG)^{G(A)})_p) = \mathrm{rank}_{C_p}(A_p)$ for each prime ideal p of C, so $\mathrm{rank}_{C_p}((A' \cap (RG)^{G(A)})_p) = 0$ for each prime ideal p of C. Thus $A' \cap (RG)^{G(A)} = \{0\}$. Therefore $A = (RG)^{G(A)}$. □

Next, we want to show that there are separable subalgebras of a group algebra RG of a non-abelian group G not satisfying Theorem 4, so the Galois map is not onto from the set of subgroups of G to the set of separable subalgebras of RG.

Theorem 5. *Let RG be a group algebra of a non-abelian group G whose order is invertible in R. Then the Galois map $\alpha : H \longrightarrow (RG)^H$ for a subgroup H of G is not onto from the set of subgroups of G to the set of separable subalgebras of RG.*

Proof. Let $g \neq e$ (the identity of G) and $R\langle g\rangle$ the subalgebra of RG generated by g. Since $|G|^{-1} \in R$, $R\langle g\rangle$ is a separable subalgebra of RG. By hypothesis, G is non-abelian, so $R\langle g\rangle$ is a proper separable subalgebra of RG. On the other hand, $G(R\langle g\rangle) = \{h \in G \,|\, hgh^{-1} = g\}$, so $G(R\langle g\rangle)$ is the commutator subgroup of $\langle g\rangle$ in G. Let $(RG)^{G(R\langle g\rangle)} = \oplus \sum_{i=1}^{k} O_i$ where k is the number of conjugate classes of G under the action of $G(R\langle g\rangle)$ and O_i is the sum of the distinct conjugate elements in the ith conjugate class of G under the action. Noting that each element in $\langle g\rangle$ is a conjugate class of G under the action of $G(R\langle g\rangle)$ and that $\langle g\rangle \neq G$, we have that $|\langle g\rangle| < k$. But $\mathrm{rank}_R(R\langle g\rangle) = |\langle g\rangle| =$ the order of $\langle g\rangle$ and $\mathrm{rank}_R((RG)^{G(R\langle g\rangle)}) = k =$ the number of conjugate classes of G under the action of $G(R\langle g\rangle)$, so $R\langle g\rangle \neq (RG)^{G(R\langle g\rangle)}$. Thus the separable subalgebra $R\langle g\rangle$ does not have a preimage of α; and so the Galois map α is not onto. □

We conclude the present paper with an example to show that the Galois map $\alpha : H \longrightarrow (RG)^H$ is one-to-one, but not onto.

Example 1. Let S_3 be the permutation group on 3 symbols $\{1, 2, 3, \}$, that is, $S_3 = \{e, (12), (13), (23), (123), (132)\}$, and R the field of real numbers. Then the group algebra RS_3 is not a Galois extension of $(RS_3)^{S_3}$ with an inner Galois group S_3 induced by the elements of S_3, and $\alpha : H \longrightarrow (RS_3)^H$ is one-to-one from the set of subgroups of S_3 to the set of separable subalgebras of the Azumaya algebra RS_3 over its center C where

(1) $C = Re \oplus R((12) + (13) + (23)) \oplus R((123) + (132))$,

(2) $S_3 \cong \overline{S}_3 =$ the inner automorphism group induced by the elements of S_3,

(3) $(RS_3)^{\langle e\rangle} = RS_3$,
$(RS_3)^{\langle (12)\rangle} = Re \oplus R(12) \oplus R((13) + (23)) \oplus R((123) + (132))$,
$(RS_3)^{\langle (13)\rangle} = Re \oplus R(13) \oplus R((12) + (23)) \oplus R((123) + (132))$,
$(RS_3)^{\langle (23)\rangle} = Re \oplus R(23) \oplus R((12) + (13)) \oplus R((123) + (132))$,
$(RS_3)^{\langle (123)\rangle} = Re \oplus R((12) + (13) + (23)) \oplus R(123) \oplus R(132)$,
$(RS_3)^{S_3} = C$.

(4) $Re \oplus R(12)$ is a separable subalgebra of RS_3 which is not an image under α, so α is not onto.

References

[1] S.U. Chase, D.K. Harrison, A. Rosenberg, *Galois Theory and Galois Cohomology of Commutative Rings*, Memoirs Amer. Math. Soc. No. 52, 1965.

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

[3] F.R. DeMeyer, *Galois Theory in Separable Algebras over Commutative Rings,* Illinois J. Math., **10** (1966), 287-295.

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

[5] F.R. DeMeyer and G.J. Janusz, *Group Rings which are Azumaya Algebras,* Trans. Amer. Math. Soc., **279**(1) (1983), 389-395.

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

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

[8] Nuss, Philippe, *Galois-Azumaya Extensions and the Brauer-Galois Group of a Commutative Ring,* Bull, Belg. Math. Soc., **13** (2006), 247-270.

[9] G. Szeto and L. Xue, *The general Ikehata theorem for H-separable crossed products,* International Journal of Mathematics and Mathematical Sciences, **23**(10) (2000), 657-662.

[10] G. Szeto and L. Xue, *The Commutator Hopf Galois Extensions,* Algebra and Discrete Mathematics, **3** (2003), 89-94.

[11] G. Szeto and L. Xue, *The Galois Algebra with Galois Group which is the Automorphism Group,* Journal of Algebra, **293**(1) (2005), 312-318.

[12] G. Szeto and L. Xue, *On Galois Extensions Satisfying the Fundamental Theorem,* International Mathematical Forum, **2**(36) (2007), 1773-1777.

[13] 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.

Contact information

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

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

Received by the editors: 04.05.2009
and in final form 04.05.2009.