PORTUGALIAE MATHEMATICA
Vol. 54 Fasc. 4 – 1997

ON H-SEPARABLE AND GALOIS EXTENSIONS OF RINGS

George Szeto

Abstract: Let S be a ring with 1, G a finite automorphism group of S of order n, and S^*G the skew group ring of G over S. Assume n is a unit in S. If S is a G-Galois and an H-separable extension of S^G, then S^*G is an Azumaya algebra if and only if S is Azumaya. Moreover, the structure theorem for a central Galois algebra of F.R. DeMeyer is generalized to a G-Galois extension with an inner Galois group.

1 – Introduction

Galois extensions of rings and Galois algebras have been intensively investigated (see References). In particular, central Galois algebras with an inner Galois group was shown to be Azumaya projective group algebras ([2] and [3]), and the concept of a central Galois algebra was generalized to an H-separable Galois extension of a noncommutative ring ([8]). The purpose of the present paper is to characterize an H-separable Galois extension in terms of skew group rings and to generalize the structure theorem of a central Galois algebra with an inner Galois group as given by F.R. DeMeyer ([2] and [3]) to an H-separable Galois extension. Let S be a ring with 1, G a finite automorphism group of S, C the center of S, S^G the subring of the elements fixed under each element in G, and S^*G the skew group ring of G over S. Assume S is an H-separable extension of S^G. If the order of G is a unit in S we show that S is an Azumaya algebra if and only if so is S^*G. In this case, S is Galois over S^G with Galois group G. Moreover, if S is a G-Galois extension of S^G with an inner Galois group G, we give a sufficient and necessary condition for the commutator subring of S^G in S to be a central Galois

Received: April 4, 1996; *Revised*: August 20, 1996.
AMS Classification: 16S30, 16W20.
Keywords and Phrases: Galois extensions of rings, H-separable extensions, Azumaya algebras, Skew group rings.

algebra with an inner Galois group. This generalizes the structure theorem of a central Galois algebra with an inner Galois group of F.R. DeMeyer ([2]).

2 – Definitions and notations

Throughout, we let S be a ring with 1, G a finite automorphism group of S, $S^G = \{s \text{ in } S \;/\; g(s) = s \text{ for each } g \text{ in } G\}$, and S^*G the skew group ring such that $g\,s = g(s)\,g$ for each s in S and g in G. Then S is called a G-Galois extension of S^G if there exist $\{a_i, b_i \text{ in } S,\ i = 1, 2, ..., m, \text{ for some integer } m\}$ such that $\sum a_i\,b_i = 1$ and $\sum a_i\,g(b_i) = 0$ for each $g \neq 1$ in G. The set $\{a_i, b_i\}$ is called a G-Galois system for S. A ring extension $R \subset T$ is called a separable extension if there exist $\{s_i, t_i \text{ in } T,\ i = 1, 2, ..., k, \text{ for some integer } k\}$ such that $\sum a\,s_i \otimes t_i = \sum s_i \otimes t_i\,a$ for all a in T where $\otimes$ is over R, and $\sum a_i\,b_i = 1$. $R \subset T$ is called an H-separable extension if $T \otimes_R T$ is isomorphic to a direct summand of a finite direct sum of T as a T-bimodule (see [5]). It is known that an H-separable extension is a separable extension. A separable algebra over its center is also called an Azumaya algebra.

3 – Azumaya skew group rings

In this section, if the order of G is a unit in S we characterize an Azumaya skew group ring S^*G in terms of the Azumaya algebra S. Let $\Delta = V_S(S^G)$, the commutator subring of S^G in S, $C =$ the center of S, $C' =$ the center of Δ, and $Z =$ the center of S^*G.

Lemma 3.1. *If S is an H-separable and G-Galois extension of S^G, then $S^*G \cong \Delta \otimes_C S^\circ$ where S° is the opposite ring of S. Moreover, the center of $S^G = C' =$ the center of Δ.*

Proof: Since S is a G-Galois extension of S^G, $S^*G \cong \mathrm{Hom}_{S^G}(S, S)$ ([3], Theorem 1). Since S is an H-separable extension of S^G, $\mathrm{Hom}_{S^G}(S, S) \cong \Delta \otimes_C S^\circ$ ([8], Definition 1 or [9], p. 106) and $V_S(V_S(S^G)) = S^G$ ([8], Proposition 4). Hence $V_S(\Delta) = S^G$. Thus $C' = V_\Delta(\Delta) \subset S^G$. Moreover, noting that $\Delta = V_S(S^G)$, we have that $C' \subset$ the center of S^G and that $C' \supset$the center of S^G; and so $C' =$the center of S^G. ∎

In the following, the order of G, n is assumed to be a unit in S.

Theorem 3.2. *Let S be an H-separable extension of S^G and faithful over S^*G. If S^*G is an Azumaya algebra, then S is also an Azumaya algebra and a G-Galois extension of S^G.*

Proof: Since S is projective as a left S-module, it is also projective as a left S^*G-module. This follows because n is a unit in S. That is, for any exact sequence of left S^*G-modules, $p\colon M \to S \to 0$, there exists a splitting S-homomorphism $q: S \to M$. Then it is straightforward to check that $q': S \to M$ by $q'(s) = \frac{1}{n}\sum g_i\, q(g_i^{-1}s)$ for all s in S and g_i in G is a left S^*G-splitting homomorphism of p, where $g_i\, s = g_i(s)$. But S^*G is an Azumaya algebra over Z, so S is finitely generated and projective over Z by the transitivity of finitely generated and projective modules. Since Z is a commutative ring and S is faithful over Z, S is a progenerator Z-module. Noting that S^*G is an Azumaya Z-algebra, we have that S is also a progenerator S^*G-module ([6], Lemma 1). But then, by Morita's theorem, $S^G \cong \mathrm{Hom}_{S^*G}(S,S)$ implies that $S^*G \cong \mathrm{Hom}_{S^G}(S,S)$ and S is a finitely generated and projective right S^G-module. This proves that S is a G-Galois extension of S^G. Moreover, since S is an H-separable extension of S^G, Δ is a finitely generated and projective C-module ([8], Proposition 4). By Lemma 3.1, $S^*G \cong \Delta \otimes_C S^\circ \cong \Delta \otimes_{C'} C' \otimes_C S^\circ$ so the center of $\Delta \otimes_{C'} C' \otimes_C S^\circ$ is C'. Thus Δ and $C' \otimes_C S^\circ$ are Azumaya algebras over C' ([4], Theorem 4.4). Since Δ is an Azumaya C'-algebra, C' is a C'-direct summand of Δ. Hence C' is a finitely generated and projective C-module because Δ is so over C ([8], Proposition 4). Noting that C' is faithful over C, we have that C' is a progenerator over C. Thus C is a C-direct summand of C'. Therefore, that $C' \otimes_C S^\circ$ is separable over C' implies that S is separable over C ([4], Theorem 3.8, p. 55). Thus S is an Azumaya C-algebra. ∎

In the proof of Theorem 3.2, we note that S is a G-Galois extension of S^G. Next is the converse of the theorem.

Theorem 3.3. *Let S be an H-separable and G-Galois extension of S^G. If S is an Azumaya algebra, then so is S^*G.*

Proof: Since S is an H-separable and G-Galois extension of S^G, $S^*G \cong \mathrm{Hom}_{S^G}(S,S) \cong \Delta \otimes_C S^\circ \cong \Delta \otimes_{C'} (C' \otimes_C S^\circ)$ as given in the proof of Theorem 3.2. By hypothesis, S is an Azumaya C-algebra, $C' \otimes_C S^\circ$ is an Azumaya C'-algebra ([4], Lemma 5.1). Moreover, since n is a unit in S, Δ is a separable algebra over C ([8], Proposition 4). But then Δ is an Azumaya C'-algebra ([4], Theorem 3.8). Thus $\Delta \otimes_{C'} (C' \otimes_C S^\circ)$ is an Azumaya C'-algebra; and so S^*G is an Azumaya algebra.

4 – Galois extensions

In this section, we shall generalize the structure theorem of a central Galois algebra with an inner Galois group to a Galois extension with an inner Galois group. We recall that KG_f is a projective group algebra of a group G over a commutative ring K if it is a K-algebra with a K-basis $\{U_i \;/\; g_i \text{ in } G\}$ such that $U_i U_j = U_{ij}\, f(g_i, g_j)$ where $f\colon\, G \times G \to$ the group of units in K is a factor set. A similar definition of a projective group ring of G over a ring with 1 is defined where the factor set f has images in the group of units in the center of the ring ([2) and [10]). We keep the notations as given in Section 3: $\Delta = V_S(S^G)$ and $C' =$ the center of Δ.

Lemma 4.1. *Let $J_i = \{a \text{ in } S \;/\; a\,s = g_i(s)\,a \text{ for all } s \text{ in } S\}$ for each g_i in G. If S is a G-Galois extension of S^G, then $\Delta = \sum J_i\, C'$ for all g_i in G.*

Proof: By Proposition 1 in [7], p. 311, $\Delta = \sum \bigoplus J_i$. Since $C \subset C'$, the lemma holds. ∎

Clearly, Δ is a G-invariant subring of S. Let $I_\Delta = \{g_i \;/\; g_i(d) = d \text{ for all } d \text{ in } \Delta\}$. Then I_Δ is a normal subgroup of G, and we denote the quotient group G/I_Δ by G'. K. Sugano ([8]) gives several equivalent conditions for a central G'-Galois extension Δ. Next is another one when S is a G-Galois extension with an inner Galois group G. This generalizes the structure theorem of F.R. DeMeyer for a central Galois algebra with an inner Galois group ([2]).

Theorem 4.2. *Let S be a G-Galois extension of S^G with an inner Galois group G. Then, Δ is a central G'-Galois extension of C' if and only if $\{U_i \;/\; g'_i$ in $G'\}$ are linearly independent over C' where $g'_i(s) = U_i\, s\, U_i^{-1}$.*

Proof: Since S is a G-Galois extension with an inner Galois group G such that $g'_i(s) = U_i\, s\, U_i^{-1}$ for some U_i in S and all s in S, S is an H-separable extension of S^G ([8], Corollary 3). For any g_i in G, since $g_i(t) = t$ for each t in S^G, so U_i is in Δ (for $\Delta = V_S(S^G)$). Hence Δ is a G-invariant subring of S. Now for g_i in I_Δ, $g_i(d) = d$ for each d in Δ, so U_i is in C'. Also, clearly, if U_i is in C', then g_i is in I_Δ. Thus G' is an inner automorphism group of Δ such that $g'_i(d) = U_i\, d\, U_i^{-1}$ for each d in Δ. Moreover, since the order of G is a unit in S, Δ is an Azumaya C'-algebra ([8], Proposition 4). But then $J_i^{-1} = U_i\, C'$, where $J'_i = \{d \text{ in } \Delta \;/\; da = g'_i(a)\, d \text{ for all } a \text{ in } \Delta\}$ ([8]). Furthermore, since S is G-Galois over S^G, $\Delta = \bigoplus \sum J_i$ as C-modules for all g_i in G_i ([7], Proposition 1, p. 311). Noting that $J_i \subset J'_i$ for each g_i in G, we have that $\Delta = \sum J'_i$ for all g'_i in G' as a sum of C'-modules. Thus $\Delta = \sum U_i\, C'$ for all g'_i in G'. Therefore, $\{U_i \;/\; g'_i \text{ in } G'\}$

are linearly independent over C' if and only if the sum is direct, $\Delta = \bigoplus \sum U_i C'$ for g_i' in G'. This is equivalent to that Δ is a central G'-Galois algebra over C' (for $J_i' J_j' = C'$ where $g_j' = (g_i')^{-1}$) ([7], Theorem 1, p. 344).

Corollary 4.3. *Let S be a G-Galois extension of S^G with an inner Galois group G. If $\{U_i \ / \ g_i' \text{ in } G'\}$ are linearly independent over C', then $V_S(C') = S^G G'_f$, a projective group ring of G' over S^G.*

Proof: By Theorem 4.2, Δ is a central G'-Galois algebra with an inner Galois group G', so it is a projective group algebra over C', $C' G'_f$ ([2], Theorem 3). Since the order of G is a unit in S, $V_S(C') = S^G \Delta \cong S^G \otimes_C \Delta$ ([8], Theorem 6). This is a projective group ring of G' over S^G. ∎

Corollary 4.4. *By keeping the hypotheses of Corollary 4.3, if $G \cong G'$, then $S \cong S^G G_f$, the skew group ring of G over S^G.*

Proof: By Theorem 4.2, Δ is a central G'-Galois algebra. Now $G \cong G'$, $S^G \Delta$ is a G-Galois extension of S^G. But S is also a G-Galois extension of S^G, so $S = S^G G_f$. ∎

The following are more consequences of Theorem 4.2 on the skew group ring S^*G. Let S be a G-Galois extension of S^G with Galois group G not necessarily inner. Then G induces an inner automorphism group G^* of S^*G; that is, for any g_i in G, and $\sum s_i g_i$ in S^*G, $g_j(\sum s_i g_i) = \sum g_j(s_i)(g_j g_i g_j^{-1}) = g_j(\sum s_i g_i) g_j^{-1}$. Using the G-Galois system for S as a G^*-Galois system for S^*G, we conclude that S^*G is also a G^*-Galois extension of $(S^*G)^{G^*}$. Denote $V_{S^*G}((S^*G)^{G^*})$ by Δ^*, its automorphism group $(G^*)'$ induced by G^*, and center by $(C^*)'$.

Corollary 4.5. *Let S be a G-Galois extension of S^G. If Δ^* is a $(G^*)'$-Galois extension, then it is a central $(G^*)'$-Galois algebra over $(C^*)'$ and $V_{S^*G}((C^*)')$ is a projective group ring of $(G^*)'$ over $(C^*)'$.*

Proof: Since S is a G-Galois extension, S^*G is a G^*-Galois extension with an inner Galois group G^* by the above remark. Hence S^*G is also an H-separable extension of $(S^*G)^{G^*}$ ([8], Corollary 3). By hypothesis, Δ^* is a $(G^*)'$-Galois extension, so it is a central $(G^*)'$-Galois extension by Corollary 4.3 and $V_{S^*G}((C^*)')$ is a projective group ring of $(G^*)'$ over $(C^*)'$ by Corollary 4.3. ∎

Corollary 4.6. *If S^*G is an Azumaya Z-algebra, then the subalgebra ZG generated by the elements of G is a projective group algebra of $(G^*)'$ over the center of ZG, where $(G^*)'$ is the automorphism group of ZG induced by G^*.*

Proof: Since S^*G is an Azumaya Z-algebra, S is a G-Galois extension by the proof of Theorem 3.2. The order of G is a unit in S, so ZG is a separable Z-algebra. Hence $ZG = V_{S^*G}(V_{S^*G}(ZG))$ ([4], Theorem 4.3). Noting that $V_{S^*G}(ZG) = (S^*G)^{(G^*)'}$ we have that $ZG = V_{S^*G}((S^*G)^{(G^*)'})$. Thus by Corollary 4.5, ZG is a projective group algebra. ∎

We remark that Corollary 4.4 is a generalization of the structure theorem of a central Galois algebra with an inner Galois group as given by F.R. DeMeyer ([3], Theorem 6).

5 – Examples

In this section, we give two examples of Galois extensions, one H-separable and the other not an H-separable extension.

(I) Let J be the ring of integers, $Q = J[i,j,k]$ the quaternion ring over J, $S = Q \times Q$ the direct product of Q, and $g\colon S \to S$ by $g(a,b) = (b,a)$ for all (a,b) in S.

Then g is an automorphism of S of order 2.

Let $G = \{1, g\}$. Then,

(**1**) $S^G = \{(a,a) \;/\; a \text{ in } Q\}$.

(**2**) S is a G-Galois extension of S^G because $\{a_1 = (1,0),\ a_2 = (0,1);\ b_1 = (1,0),\ b_2 = (0,1)\}$ is a G-Galois system for S.

(**3**) The center C of $S = J \times J$.

(**4**) S is not an H-separable extension of S^G, because C is not contained in S^G.

(II) Let $Q = R[i,j,k]$ be the quaternion ring over the real field R, $S = Q \times Q$, $g\colon S \to S$ by $g(a,b) = (b,a)$ for all (a,b) in S, and $G = \{1, g\}$. Then

(**1**) S is a G-Galois extension but not an H-separable extension of S^G.

(**2**) The order of G is a unit in S.

(**3**) S is an Azumaya algebra over C.

(**4**) S^*G is an Azumaya algebra over C^G.

(**5**) S^*G is a G-Galois extension of $(S^*G)^{G^*}$ where G^* is an inner Galois group induced by G. Thus S^*G is also an H-separable extension (see Corollary 4.6).

ACKNOWLEDGEMENT – The major portion of the present paper was done during the visit of Professor K. Sugano to Bradley University in fall, 1995. The author would like to thank him for many valuable discussions. The author would also like to thank the referee for his valuable suggestions.

REFERENCES

[**1**] ALFARO, R. and SZETO, G. – Skew group rings which are Azumaya, *Comm. in Algebra,* 23(6) (1995), 2255–2261.

[**2**] DEMEYER, F.R. – Galois theory in separable algebras over commutative rings, *Illinois J. Math.,* 10(2) (1966), 287–295.

[**3**] DEMEYER, F.R. – Some notes on the general Galois theory of rings, *Osaka J. Math.,* 2 (1965), 117–127.

[**4**] DEMEYER, F.R. and INGRAHAM, E. – *Separable Algebras Over Commutative Rings*, Vol. 181, Springer-Verlag, Berlin, 1971.

[**5**] HIRADA, K. – Some types of separable extensions, *Nagoya J. Math.,* 33 (1968), 107–115.

[**6**] IKEHATA, S. – Note on Azumaya algebras and H-separable extensions, *Math. J. Okayama Univ.,* 23 (1981), 17–18.

[**7**] KANZAKI, T. – On Galois algebra over a commutative ring, *Osaka J. Math.,* 2 (1965), 309–317.

[**8**] SUGANO, K. – On a special type of Galois extensions, *Hokkaido J. Math.,* 9 (1980), 123–128.

[**9**] SUGANO, K. – Note on automorphisms in separable extension of noncommutative ring, *Hokkaido J. Math.,* 9 (1980), 268–274.

[**10**] SUGANO, K. – Separable Frobenius extensions, *Hokkaido J. Math.,* 24 (1995), 105–111.

George Szeto,
Mathematics Department, Bradley University,
Peoria, Illinois 61625 – U.S.A.