SOME CORRESPONDENCES FOR A CENTER GALOIS EXTENSION

GEORGE SZETO and LIANYONG XUE
Department of Mathematics, Bradley University
Peoria, Illinois 61625 – U.S.A.

Abstract

Let B be a ring with 1, G a finite automorphism group of B, C the center of B, B^G the set of elements in B fixed under each element in G. $B*G$ a skew group ring in which the multiplication is given by $gb = g(b)g$ for $b \in B$ and $g \in G$. Assume C is a Galois algebra with Galois group $G|_C \cong G$. Two correspondence theorems are given between some sets of separable extensions in the skew group ring $B*G$. Moreover, a sufficient and necessary condition is given for a subring S of B over B^G such that $S = B^K$ for some subgroup K of G. Consequently, a correspondence is established between the set of subgroups of G and a set of subrings of B over B^G.

Key Words and Phrases. Galois extensions, Center Galois extensions, Azumaya algebras, Separable extensions, H-separable extensions.

AMS Subject Classification Codes. 16S35, 16W20

1. INTRODUCTION

Let B be a ring with 1, C the center of B, G a finite automorphism group of B, and B^G the set of elements in B fixed under each element in G. B is called a DeMeyer-Kanzaki G-Galois extension if B is an Azumaya C-algebra and C is a Galois algebra with Galois group $G|_C \cong G$ ([2]). It was shown that there exists a one-to-one correspondence between the set of separable subalgebras of C over C^G and the set of separable subrings of B over B^G ([2], Theorem 3). This fact was generalized to an Azumaya Galois extension where B is called an Azumaya Galois extension of B^G if B is a G-Galois extension of B^G which is an Azumaya C^G-algebra ([1], Theorem 2). A ring B is called a center Galois extension of B^G if C is a Galois algebra over C^G with Galois group $G|_C \cong G$. Clearly, a DeMeyer-Kanzaki G-Galois extension is a center Galois extension. Many properties of a center Galois extension have been found in [5], [6], [7], and [10]. The purpose of the present paper is to continue the study of a center Galois extension. Two correspondence theorems are given between some sets of separable extensions in the skew group ring $B * G$. One of the correspondences implies the correspondence between the set of subgroups of G and a set of certain separable extensions each of which is invariant under a subgroup of G. Then a characterization of an invariant subring of B under a subgroup of G is obtained. This work was supported by a Caterpillar Fellowship at Bradley University. We would like to thank Caterpillar Inc. for the support.

2. BASIC NOTATIONS AND DEFINITIONS

Throughout this paper, B will represent a ring with 1, G an automorphism group of B, C the center of B, $B * G$ a skew group ring in which the multiplication is given by $gb = g(b)g$ for $b \in B$ and $g \in G$, B^G the set of elements in B fixed under G, and $\bar{G}$ the inner automorphism group of $B*G$ induced by G, that is, $\bar{g}(f) = gfg^{-1}$ for each $f \in B*G$ and $g \in G$. We note that $\bar{G}$ restricted to B is G.

Let A be a subring of a ring B with the same identity 1. We denote $V_B(A)$ the commutator subring of A in B. 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. A ring F is called a H-separable extension of B if $F \otimes_B F$ is isomorphic to a direct summand of a finite direct sum of F as a F-bimodule. B is called a G-Galois extension of B^G if there exist elements $\{c_i, d_i$ in B, $i = 1, 2, ..., m\}$ for some integer m such that $\sum_{i=1}^m c_i g(d_i) = \delta_{1,g}$ for each $g \in G$. Such a set $\{c_i, d_i\}$ is called a G-Galois system for B. B is called a DeMeyer-Kanzaki G-Galois extension if B is an Azumaya C-algebra and C is a Galois algebra with Galois group $G|_C \cong G$. B is called an Azumaya Galois extension of B^G if B is a G-Galois extension of B^G which is an Azumaya C^G-algebra. We call B a center Galois extension of B^G if C is a Galois algebra over C^G with Galois group $G|_C \cong G$. S is called a D-S-separable extension of E in B if S is a separable extension of E in B and a direct summand of a finite direct sum of B as a bimodule over S. For a B-module M, we denote $\text{Ann}_B(M) = \{b \in B \mid bm = 0 \text{ for all } m \in M\}$.

3. CORRESPONDENCE THEOREMS

In this section, we shall give two correspondences between some sets of separable extensions in the skew group ring $B*G$. We begin with the expressions of several commutator subrings.

LEMMA 3.1.

If B is a center Galois extension of B^G, then

(1) $V_{B*G}(C) = B$.

(2) $V_{B*G}(B) = C$.

(3) $V_{B*G}(B*G) = C^G$.

(4) $B = B^G C$.

(5) $V_{B*G}(B^G) = C*G$.

PROOF. (1) It is clear that $B \subset V_{B*G}(C)$. Conversely, for each $\sum_{g\in G} b_g g$ in $V_{B*G}(C)$, we have $c(\sum_{g\in G} b_g g) = (\sum_{g\in G} b_g g)c$ for each c in C, so $cb_g = b_g g(c)$, that is, $b_g(c - g(c)) = 0$ for each $g \in G$ and $c \in C$. But C is a commutative G-Galois extension of C^G, so the ideal of C generated by $\{c - g(c) \mid c \in C\}$ is C for each $g \neq 1$ ([3], Proposition 1.2-(5), page 80). Thus $b_g = 0$ for each $g \neq 1$. But then $\sum_{g\in G} b_g g = b_1 \in B$. Hence $V_{B*G}(C) \subset B$, and so $V_{B*G}(C) = B$.

(2) By (1), $V_{B*G}(C) = B$, so $V_{B*G}(B) \subset V_{B*G}(C) = B$. Thus $V_{B*G}(B) = V_B(B) = C$.

(3) By (2), $V_{B*G}(B) = C$, so $V_{B*G}(B*G) = (V_{B*G}(B))^{\bar{G}} = C^G$.

(4) Since C is a Galois algebra with Galois group $G|_C \cong G$, B and $B^G C$ are Galois extensions of B^G with Galois group $G|_{B^G C} \cong G$. Noting that $B^G C \subset B$, we conclude that $B = B^G C$.

(5) By (4), $B = B^G C$, so $V_B(B^G) = V_B(B^G C) = V_B(B) = C$. Thus, $V_{B*G}(B^G) = V_B(B^G) * G = C * G$.

LEMMA 3.2.

Let B be a center Galois extension of B^G with Galois group G. Then $B * G$ is H-separable over B^G and left (or right) B^G-finitely generated projective.

PROOF. Since C is a Galois algebra over C^G with Galois group $G|_C \cong G$, B is a Galois extension of B^G. Hence B is B^G-finitely generated projective. Therefore, by the transitivity of finitely generated and projective modules, $B * G$ is B^G-finitely generated projective since $B * G$ is B-finitely generated projective. Moreover, since C is a Galois algebra over C^G with Galois group $G|_C \cong G$ again, $C * G$ is an Azumaya C^G-algebra ([4], Theorem 2). Hence $C * G$ is H-separable over C^G. Thus, $B^G \otimes_{C^G} (C * G)$ is H-separable over $B^G \otimes_{C^G} C^G (\cong B^G)$. Noting that the map $B^G \otimes_{C^G} (C * G) \longrightarrow B^G(C * G)(= B * G$ by Lemma 3.1-(4)) by multiplication is a ring homomorphism, we have that $B * G$ is H-separable over B^G.

The correspondence given by Sugano ([9], Theorem 1) will play an important role. For convenience, we state it in the following:

PROPOSITION 3.3.

Let A be a H-separable extension of E. Then if A is left or right E-finitely generated projective, there exists a one-to-one correspondence $V : S \longrightarrow V_A(S)$ such that V^2 is an identity between the set of D-S-separable extensions of E in A and the set of $Z(A)$-separable subalgebras of $V_A(E)$ where $Z(A)$ is the center of A.

THEOREM 3.4.

Let B be a center Galois extension of B^G with Galois group G. Then there exists a one-to-one correspondence between the set of all separable subalgebras of $C * G$ over C^G and the set of all D-S-separable extensions of B^G in $B * G$.

PROOF. By Lemma 3.2, $B * G$ is H-separable over B^G and B^G-finitely generated projective, so, by Proposition 3.3, there exists a one-to-one correspondence between the set of all D-S-separable extensions of B^G in $B * G$ and the set of all C^G-separable subalgebras of $V_{B*G}(B^G)$ where C^G is the center of $B*G$ by Lemma 3.1-(4) and $V_{B*G}(B^G) = C*G$ by Lemma 3.1-(5). This completes the proof.

The second correspondence theorem is for the D-S-separable extensions of $(B*G)^{\bar{G}}$ in $B*G$. We first give a lemma.

LEMMA 3.5.
Let B be a center Galois extension of B^G with Galois group G. Then $B*G$ is H-separable over $(B*G)^{\bar{G}}$ and $(B*G)^{\bar{G}}$-finitely generated projective.

PROOF. Since C is a Galois algebra over C^G with Galois group $G|_C \cong G$, $B*G$ is a Galois extension of $(B*G)^{\bar{G}}$ with the same Galois system for C. Hence $B*G$ is finitely generated projective over $(B*G)^{\bar{G}}$. Moreover, since the elements in $\bar{G}$ are inner, $B*G$ is H-separable over $(B*G)^{\bar{G}}$ by Corollary 3 in [8].

THEOREM 3.6.
Let B be a center Galois extension of B^G with Galois group G of order n invertible in B. Then there exists a one-to-one correspondence between the set of all D-S-separable extensions of $(B*G)^{\bar{G}}$ in $B*G$ and the set of all C^G-separable subalgebras of $C^G G$.

PROOF. By Lemma 3.5, $B*G$ is H-separable over $(B*G)^{\bar{G}}$ and $(B*G)^{\bar{G}}$-finitely generated projective. Hence, by Proposition 3.3, there exists a one-to-one correspondence between the set of all D-S-separable extensions of $(B*G)^{\bar{G}}$ in $B*G$ and the set of all C^G-separable subalgebras of $V_{B*G}((B*G)^{\bar{G}})$. Since n is invertible in C^G, $C^G G$ is separable over C^G; and so $C^G G$ is a C^G-separable subalgebra of $V_{B*G}((B*G)^{\bar{G}})$. Thus, by Proposition 3.3, $V_{B*G}(V_{B*G}(C^G G)) = C^G G$. But $V_{B*G}((B*G)^{\bar{G}}) = V_{B*G}(V_{B*G}(C^G G))$, so $V_{B*G}((B*G)^{\bar{G}}) = C^G G$. This completes the proof.

4. THE INVARIANT SUBRINGS

In this section, let $J_g^{(S)}$ be the C-module generated by $\{s - g(s) \mid s \in S\}$ for a subring S of B for a $g \in G$. We are going to characterize, in terms of $J_g^{(S)}$, an invariant subring S of B over B^G under some subgroup K of G, that is, $S = B^K$. Consequently, we derive a one-to-one correspondence between the set of all subgroups of G and a set of certain separable extensions of B^G in B.

We begin with the double centralizer property of a skew group ring $C * K$ in $B * G$ for any subgroup K of G.

LEMMA 4.1.

Let K be a subgroup of G. If B is a center Galois extension of B^G with Galois group G, then $C * K$ satisfies the double centralizer property in $B * G$.

PROOF. Since C is a commutative Galois extension of C^G with Galois group G, C is a Galois extension of C^K with Galois group K with the same Galois system. Hence $C * K$ is an Azumaya C^K-algebra and C^K is separable over C^G, and so $C * K$ is a separable C^G-algebra by the transitivity of separable extensions. Thus, the one-to-one correspondence in Theorem 3.4 implies that $V_{B*G}(V_{B*G}(C * K)) = C * K$ for $C * K$ is a separable C^G-subalgebra of $C * G$.

LEMMA 4.2.

Let B be a center Galois extension of B^G with Galois group G, S a subring of B over B^G, and $K = \{g \in G \mid g(s) = s \text{ for all } s \in S\}$. Then, $J_g^{(S)}$ is a faithful C-module for each $g \notin K$ if and only if $V_{B*G}(S) = C * K$.

PROOF. Since $B^G \subset S$, $V_{B*G}(S) \subset V_{B*G}(B^G) = C * G$ by Lemma 3.1-(5). Thus, $V_{B*G}(S) = V_{C*G}(S)$. By a direct computation, $V_{C*G}(S) = C * K \oplus \sum_{g \notin K} I_g g$ where $I_g = \{c \in C \,|\, c(s - g(s)) = 0 \text{ for each } s \in S\} = \text{Ann}_C(J_g^{(S)})$. Therefore, $J_g^{(S)}$ is a faithful C-module for each $g \notin K$ if and only if $V_{B*G}(S) = C * K$.

THEOREM 4.3.

Let B be a center Galois extension of B^G with Galois group G, S a subring of B over B^G, and $K = \{g \in G \mid g(s) = s \text{ for all } s \in S\}$. Then, $S = B^K$ if and only if $J_g^{(S)}$ is a faithful C-module for each $g \notin K$ and S satisfies the double centralizer property in $B * G$.

PROOF. ($\Longleftarrow$) Since $J_g^{(S)}$ is a faithful C-module for each $g \notin K$, $V_{B*G}(S) = C * K$ by Lemma 4.2. Hence $V_{B*G}(V_{B*G}(S)) = V_{B*G}(C * K) = (V_{B*G}(C))^{\bar{K}} = B^K$ by Lemma 3.1-(1). But $V_{B*G}(V_{B*G}(S)) = S$ by hypothesis, so $S = B^K$.

($\Longrightarrow$) By Lemma 3.1-(1), $V_{B*G}(C) = B$. Hence $V_{B*G}(C * K) = (V_{B*G}(C))^{\bar{K}} = B^K$. But $S = B^K$ by hypothesis, so $V_{B*G}(C * K) = S$. Thus $V_{B*G}(S) = V_{B*G}(V_{B*G}(C * K))$.

Since $C * K$ satisfies the double centralizer property in $B * G$ by Lemma 4.1, $V_{B*G}(S) = C * K$. Therefore, $J_g^{(S)}$ is a faithful C-module for each $g \notin K$ by Lemma 4.2. Moreover, $V_{B*G}(V_{B*G}(S)) = V_{B*G}(C * K) = S$. This completes the proof.

COROLLARY 4.4.

Let B be a center Galois extension of B^G with Galois group G, S a D-S-separable extension of B^G in B, and $K = \{g \in G \mid g(s) = s \text{ for all } s \in S\}$. Then, $S = B^K$ if and only if $J_g^{(S)}$ is a faithful C-module for each $g \notin K$.

PROOF. Since B is a center Galois extension of B^G with Galois group G, Theorem 3.4 implies that every D-S-separable extension S of B^G in $B*G$ satisfies the double centralizer property in $B * G$. Thus, the Corollary is immediate from Theorem 4.3.

Corollary 4.4 induces a one-to-one correspondence between the set of all subgroups of G and the set of all D-S-separable extensions of B^G in B.

COROLLARY 4.5.

Let B be a center Galois extension of B^G with Galois group G. Then there is a one-to-one correspondence between the set of all subgroups of G and the set of all D-S-separable extensions S of B^G in B such that $J_g^{(S)}$ is a faithful C-module for each $g \notin K$ where $K = \{g \in G \mid g(s) = s \text{ for all } s \in S\}$.

PROOF. Let $\alpha : K \longrightarrow B^K$ for each subgroup K of G. We claim that

(i) α is one-to-one,

(ii) $K = \{g \in G \mid g(s) = s \text{ for all } s \in B^K\}$,

(iii) B^K is a D-S-separable extension of B^G in B such that $J_g^{(B^K)}$ is a faithful C-module for each $g \notin K$, and

(iv) α is onto the set of all D-S-separable extensions S of B^G in B such that $J_g^{(S)}$ is a faithful C-module for each $g \notin K$.

Proof of (i). Let K and H be two subgroups of G such that $\alpha(K) = \alpha(H)$, that is, $B^K = B^H$. Then $B^{\langle K,H\rangle} = B^K = B^H$ where $\langle K, H\rangle$ is the subgroup of G generated by K and H. Since B is a Galois extension of B^G with Galois group G, B is a Galois extension of B^K with Galois group K and a Galois extension of $B^{\langle K,H\rangle}$ with Galois group $\langle K, H\rangle$. Hence, $B * K \cong \text{Hom}_{B^K}(B, B) = \text{Hom}_{B^{\langle K,H\rangle}}(B, B) \cong B * \langle K, H\rangle$ ([2], Theorem 1). Therefore, $K = \langle K, H\rangle$. Similarly, $H = \langle K, H\rangle$. Thus $K = H$.

Proof of (ii). Let $H = \{g \in G \mid g(s) = s \text{ for all } s \in B^K\}$. Then $K \subset H$. Hence $B^H \subset B^K$. But $B^K \subset B^H$ by the definition of H, so $B^K = B^H$. Thus $K = H$ by (i).

Proof of (iii). By Theorem 4.3, $J_g^{(B^K)}$ is a faithful C-module for each $g \notin K$ and B^K satisfies the double centralizer property in $B*G$ for $S = B^K$ being a subring of B over B^G. Hence $V_{B*G}(B^K) = C*K$ by Lemma 4.2. Therefore, $V_{B*G}(C*K) = V_{B*G}(V_{B*G}(B^K)) = B^K$. But, by the proof of Lemma 4.1, $C*K$ is a separable C^G-subalgebra of $C*G$, so $V_{B*G}(C*K)(= B^K)$ is a D-S-separable extension of B^G in $B*G$ by Theorem 3.4.

Proof of (iv). α is onto by Corollary 4.4.

We conclude the present paper with a center Galois extension B that is not a DeMeyer-Kanzaki Galois extension.

Let Z be the ring of integers, $C = \oplus\sum_1^n Z$, the direct sum of n copies of Z for some integer n, $Z[i,j,k]$ the integer quaternion ring, $B = Z[i,j,k]C(= \oplus\sum_1^n Z[i,j,k])$, and $g(b_1, b_2, \cdots, b_n) = (b_n, b_1, b_2, \cdots, b_{n-1})$ for any $(b_1, b_2, \cdots, b_n) \in B$. Then

(1) C is a commutative Galois algebra with Galois group $G = \langle g \rangle$ generated by g with a Galois system $\{e_1, e_2, \cdots, e_n;\ e_1, e_2, \cdots, e_n\}$ where $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ with 1 in the i^{th} component such that $\sum_{j=1}^n e_j g^p(e_j) = \delta_{0,p}$, $p = 0, 1, \cdots, n-1$.

(2) $C^G = \{(a, a, \cdots, a) \mid a \in Z\}(\cong Z)$.

(3) The center of B is C since the center of $Z[i,j,k]$ is Z.

(4) B is a center Galois extension of B^G with Galois group G by (1) and (3), where $B^G = \{(b, b, \cdots, b) \mid b \in Z[i,j,k]\}(\cong Z[i,j,k])$.

(5) $Z[i,j,k]$ is not a separable Z-algebra (for 2 is not a unit in Z), so B^G is not an Azumaya C^G-algebra. Hence B is not an Azumaya C-algebra. Thus, B is not a DeMeyer-Kanzaki Galois extension.

(6) Let K be a subgroup of G. Then $K = \langle g^m \rangle$ for some integer $m|n$ and $B^K = \{(b_1, b_2, \cdots, b_m, b_1, b_2, \cdots, b_m, \cdots\cdots, b_1, b_2, \cdots, b_m) \mid b_p \in Z[i,j,k], \text{ for } 1 \le p \le m\}$.

(7) By Corollary 4.5, $B^K = \{(b_1, b_2, \cdots, b_m, b_1, b_2, \cdots, b_m, \cdots\cdots, b_1, b_2, \cdots, b_m) \mid b_p \in Z[i,j,k], \text{ for } 1 \le p \le m\}$ is a D-S-separable extension of B^G in B such that $J_g^{(B^K)}$ is a faithful C-module for each $g \notin K$.

(8) Let S be a D-S-separable extension of B^G in B. Then $J_g^{(S)}$ is C-faithful for $g \neq 1$. Hence, by Corollary 4.5, every D-S-separable extension S of B^G in B has form $S = B^K$ for some subgroup K of G.

(9) By Theorem 4.3, for any $S = \{(b_1, b_2, \cdots, b_m, b_1, b_2, \cdots, b_m, \cdots\cdots, b_1, b_2, \cdots, b_m) \mid b_p \in Z[i,j,k], \text{ for } 1 \le p \le m\}$ where $m|n$, S satisfies the double centralizer property in $B*G$ and $V_{B*G}(S)$ is a Z-separable subalgebras of $C*G$.

REFERENCES

1. R. Alfaro and G. Szeto, On Galois Extensions Of An Azumaya Algebra, Comm. in Algebra, 25(6), (1997), 1873-1882.
2. F.R. DeMeyer, Some Notes On The General Galois Theory Of Rings, Osaka J. Math. 2(1965), 117-127.
3. F.R. DeMeyer and E. Ingraham, Separable Algebras Over Commutative Rings, Vol. 181, Springer-Verlag, Berlin,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. S. Ikehata and G. Szeto, On H-Separable Polynomials In Skew Polynomial Rings Of Automorphism Type, Math. J. Okayama Univ. 34(1992), 49-55.
7. S. Ikehata and G. Szeto, On H-Skew Polynomial Rings And Galois Extensions, Rings, Extension and Cohomology, 113-121, Lecture Notes in Pure and Appl. Math., 159, Dekker, New York, 1994.
8. K. Sugano, On A Special Type Of Galois Extensions, Hokkaido J. Math., 9(1980), 123-128.
9. K. Sugano, On Centralizers In Separable Extensions II, Osaka J. Math., 8(1971), 465-469.
10. G. Szeto and L. Xue, On The Ikehata Theorem For H-Separable Skew Polynomial Rings, Mathematical Journal of Okayama University, Vol. 40, 1998(2000), 27-32.