The Invariant Subrings of an Azumaya Galois Extension

George Szeto and Lianyong Xue
Department of Mathematics, Bradley University
Peoria, Illinois 61625 – U.S.A.
Email: szeto@bradley.bradley.edu and lxue@bradley.bradley.edu

AMS 1991 Subject Classification Codes: 16S30; 16W20

Abstract. Let B be an Azumaya Galois extension or a DeMeyer-Kanzaki Galois extension with Galois group G. Equivalent conditions are given for a separable subextension of a Galois extension in the skew group ring $B * G$ being an invariant subring of a subgroup of the Galois group G.

1. Introduction

The fundamental theorem for the Galois extension of a field was generalized to a commutative ring with no idempotents but 0 and 1 ([4], Chapter 3). For a Galois extension of noncommutative ring, there exist some one-to-one correspondences between certain subsets of separable subextensions ([2], [3]). Let B be a Galois extension of B^G with Galois group G of order n invertible in B for some integer n, and K a subgroup of G. Then it can be shown that the invariant subring $B^K = \{b \in B \mid k(b) = b \text{ for each } k \in K\}$ is a separable extension of B^G. We note that there are separable extensions of B^G in B which are not invariant under a subgroup of G. It is interesting to know which separable extension of B^G in B is invariant under a subgroup of G. In the present paper, we shall give some equivalent conditions for a separable extension S of B^G in B (or of C^G in C) such that S is invariant under a subgroup of G for a DeMeyer-Kanzaki Galois extension B where B is called a DeMeyer-Kanzaki Galois extension of B^G with Galois group G if the center C of B is a Galois algebra over C^G with Galois group induced by and isomorphic with G, and B is an Azumaya C-algebra (see [4]). Moreover, assume that B is an Azumaya Galois extension with Galois group G, that is, B is a Galois extension of B^G with Galois group G

and B^G is an Azumaya C^G-algebra (see [1]). We note that the skew group ring $B*G$ is also a Galois extension of $(B*G)^{\bar{G}}$ with Galois group $\bar{G}$ where $\bar{G}$ is the inner automorphism group of $B*G$ induced by G. Equivalent conditions are given for a separable extension S of $(B*G)^{\bar{G}}$ in $B*G$ such that $S=(B*G)^{\bar{K}}$ for some subgroup $\bar{K}$ of $\bar{G}$.

2. Basic Definitions and Notations

Throughout this paper, B will represent a ring with 1, G an automorphism group of B of order n invertible in B for some integer n, 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 $\sum a_ib_i=1$, and $\sum ba_i\otimes b_i=\sum a_i\otimes b_ib$ for all b in B where $\otimes$ is over A. An Azumaya algebra is a separable extension of its center. 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 $\sum_{i=1}^m c_ig(d_i)=\delta_{1,g}$. As defined in [1], 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, and B is called a DeMeyer-Kanzaki G-Galois extension if B is an Azumaya C-algebra and C is a $G|_C$-Galois algebra with $G|_C\cong G$ (see [4]). It can be shown that a DeMeyer-Kanzaki Galois extension is an Azumaya Galois extension. For a B-module M, we denote $\mathrm{Ann}_B(M)=\{b\in B\mid bm=0 \text{ for all } m\in M\}$.

3. DeMeyer-Kanzaki Galois extensions

In this section, let B be a DeMeyer-Kanzaki Galois extension. We shall give an equivalent condition for a separable subring T being invariant under a subgroup K of G when (i) $B^G\subset T\subset B$ and (ii) $C^G\subset T\subset C$ respectively. We begin with the commutator theorem for Azumaya algebras and the structure theorem for a DeMeyer-Kanzaki Galois extension which will take an important role.

Proposition 3.1. ([4], Theorem 4.3, p.57) *Let A be an Azumaya algebra over its center C and E a separable subalgebra of A. Then*
(1) $V_B(E)$ is a separable subalgebra such that $V_A(V_A(E)) = E$.
(2) If E has center C, then $V_A(E)$ has center C such that $A \cong E \otimes_C V_A(E)$.

Proposition 3.2. *Let A be an Azumaya algebra over its center C and E a separable subalgebra of A with center D. Then $V_A(E)$ is an Azumaya D-algebra such that $V_A(D) \cong E \otimes_D V_A(E)$ as Azumaya D-algebra.*

Proof. Since E is a separable subalgebra of A, $V_B(E)$ is a separable subalgebra such that $V_A(V_A(E)) = E$ by Proposition 3.1. Hence $D = V_E(E) = E \cap V_A(E) = V_A(V_A(E)) \cap V_A(E) = V_{V_A(E)}(V_A(E))$ = the center of $V_A(E)$. Thus both E and $V_A(E)$ are Azumaya D-algebras. Since E is a separable subalgebra of A with center D, D is a separable subalgebra of A with itself as center (see [4], Theorem 3.8, p.55). Hence, by the above argument, $V_A(D)$ is an Azumaya D-algebra such that E is an Azumaya subalgebra of $V_A(D)$. Thus $V_A(D) \cong E \otimes_D V_A(E)$ as Azumaya D-algebras by Proposition 3.1.

Proposition 3.3. ([3], Lemma 2, p.120) *Let B be a DeMeyer-Kanzaki Galois extension of B^G with Galois group G. Then $B = B^G C \cong B^G \otimes_{C^G} C$ by the multiplication map such that B^G is an Azumaya C^G-algebra.*

Theorem 3.4. *Let B be a DeMeyer-Kanzaki Galois extension of B^G, $B^G \subset T$, a separable extension of B^G in B, and $K = \{g \in G \mid g(t) = t \text{ for all } t \in T\}$. Then, $T = B^K$ if and only if $Ann_C(T_g) = \{0\}$ for each $g \notin K$ where T_g is the C-module generated by $\{t - g(t) \mid t \in T\}$.*

Proof. Since B is a DeMeyer-Kanzaki Galois extension with Galois group G, $B * G$ is an Azumaya C^G-algebra ([1], Theorem 3.1). But T and B^K are separable C^G-subalgebras of $B * G$, so by Proposition 3.1, $T = B^K$ is equivalent to $V_{B*G}(T) = V_{B*G}(B^K)$. Since $V_{B*G}(B^G) = V_B(B^G) * G = C * G$ by Proposition 3.3, $V_{B*G}(B^K) \subset V_{B*G}(B^G) = C * G$. This implies that $V_{B*G}(B^K) = V_{C*G}(B^K)$ which is $C * K$ by the definition of K. Thus, we only need to show that $V_{B*G}(T) = C * K$ if and only if $\text{Ann}_C(T_g) = \{0\}$ for each $g \notin K$.

Assume that $V_{B*G}(T) = C * K$. Let $cT_g = \{0\}$ for some $c \in C$ and $g \in G$. Then $tc = ct = cg(t)$ for all $t \in T$. Hence $t(cg) = (tc)g = cg(t)g = (cg)t$ for all $t \in T$, that is, $cg \in V_{B*G}(T) = C * K$. Thus, c must be 0 if $g \notin K$. This proves that $\text{Ann}_C(T_g) = \{0\}$

for each $g \notin K$. Conversely, for any $\sum_{g\in G} b_g g \in V_{B*G}(T)$, $t(\sum_{g\in G} b_g g) = (\sum_{g\in G} b_g g)t = \sum_{g\in G} b_g g(t)g$, so $tb_g = b_g g(t)$ for all $t \in T$. But $B^G \subset T$, so $tb_g = b_g t$ all $t \in B^G$. Hence $b_g \in V_B(B^G)$ which is C by Proposition 3.3. Thus $b_g t = tb_g = b_g g(t)$ for all $t \in T$, and so $b_g(t - g(t)) = 0$ for all $t \in T$. This implies that $b_g T_g = \{0\}$. Therefore, if $\mathrm{Ann}_C(T_g) = \{0\}$ for each $g \notin K$, then $b_g = 0$ for each $g \notin K$. We have $V_{B*G}(T) \subset C * K$. Clearly, $C * K \subset V_{B*G}(T)$, so $V_{B*G}(T) = C * K$.

As given in Theorem 3.4, for a separable subring T of B over B^G, we have a subgroup $K_T = \{g \in G \mid g(t) = t \text{ for all } t \in T\}$. Let $\mathcal{C} = \{T = \text{a separable extension of } B^G \text{ in } B \mid \mathrm{Ann}_C(T_g) = \{0\} \text{ for each } g \notin K_T\}$. We have a correspondence theorem for the set of subgroups of G.

Corollary 3.5. *Let B be a DeMeyer-Kanzaki Galois extension of B^G with Galois group G. Then there exists a one-to-one correspondence between $\mathcal{C}$ and the set of subgroups of G.*

Let T be given in Theorem 3.4, by the one-to-one correspondence as given in [3], $T = B^G(T \cap C)$ ([3], Lemma 2, p.120). We then derive another characterization of T equal to B^K for some subgroup K of G.

Theorem 3.6. *Let T be given in Theorem 3.4. Then $T = B^K$ if and only if $T \cap C = C^K$.*

Proof. Assume that $T = B^K$. Then $T \cap C = B^K \cap C = C^K$. Conversely, if $T \cap C = C^K$, then $T = B^G(T \cap C) = B^G C^K = (B^G C)^K = B^K$.

Next we give an equivalent condition for a separable subring W such that $C^G \subset W \subset C$ being invariant under a subgroup K of G. We begin with a Lemma.

Lemma 3.7. *Let B be a DeMeyer-Kanzaki Galois extension of B^G with Galois group G. Then $V_{B*G}(B) = C$.*

Proof. We first claim that $V_{B*G}(C) = B$. In fact, it is clear that $B \subseteq V_{B*G}(C)$. 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 ([4], Proposition 1.2-(5)). Thus $b_g = 0$ for each $g \neq 1$. But then $\sum_{g \in G} b_g g = b_1 \in B$. Hence $V_{B*G}(C) \subseteq B$, and so $V_{B*G}(C) = B$. Therefore, $V_{B*G}(B) = C$ by Proposition 3.1 for the Azumaya C^G-algebra $B * G$.

Theorem 3.8. *Let B be a DeMeyer-Kanzaki Galois extension of B^G, $C^G \subset W$ a separable C^G-subalgebra of C and $K = \{g \in G \mid g(w) = w$ for all $w \in W\}$. Then, $W = C^K$ if and only if $Ann_B(W_g) = \{0\}$ for each $g \notin K$ where W_g is the B-module generated by $\{w - g(w) \mid w \in W\}$.*

Proof. Observing that $V_{B*G}(B) = C$ by Lemma 3.7, we have $V_{B*G}(B * K) = C^K$. But $V_{B*G}(V_{B*G}(C^K)) = C^K$ by Proposition 3.1 for the Azumaya C^G-algebra $B * G$, so $V_{B*G}(V_{B*G}(C^K)) = V_{B*G}(B * K)$. Hence $V_{B*G}(C^K) = B * K$ by Proposition 3.1 again. Therefore, $W = C^K$ if and only if $V_{B*G}(W) = V_{B*G}(C^K) = B * K$. Thus we only need to show that $V_{B*G}(W) = B * K$ if and only if $\mathrm{Ann}_B(W_g) = \{0\}$ for each $g \notin K$.

Assume that $V_{B*G}(W) = B * K$. If $b \in \mathrm{Ann}_B(W_g)$ for a $g \notin K$, that is, $bW_g = \{0\}$ for some $b \in B$ and $g \notin K$, then $wb = bw = bg(w)$ for all $w \in W$. Hence $w(bg) = (wb)g = bg(w)g = (bg)w$; and so $bg \in V_{B*G}(W) = B * K$. Therefore, b must be 0 if $g \notin K$. This proves that $\mathrm{Ann}_B(W_g) = \{0\}$ for each $g \notin K$.

Conversely, for any $\sum_{g \in G} b_g g \in V_{B*G}(W)$, $w(\sum_{g \in G} b_g g) = (\sum_{g \in G} b_g g)w = \sum_{g \in G} b_g g(w) g$. This implies that $wb_g = b_g g(w)$ for all $w \in W$, that is, $b_g W_g = \{0\}$. Thus that $\mathrm{Ann}_B(W_g) = \{0\}$ for each $g \notin K$ implies that $V_{B*G}(W) \subset B * K$. On the other hand, it is clear that $B * K \subset V_{B*G}(W)$, so $V_{B*G}(W) = B * K$. This completes the proof.

Corollary 3.9. *Let B, W, and W_g be given in Theorem 3.8, $K_W = \{g \in G \mid g(w) = w$ for all $w \in W\}$, and $\mathcal{D} = \{W =$ a separable extension of C^G in $C \mid Ann_B(W_g) = \{0\}$ for each $g \notin K_W\}$. Then there exists a one-to-one correspondence between $\mathcal{D}$ and the set of subgroups of G.*

4. Azumaya Galois Extensions

In this section, we consider an Azumaya Galois extension B with Galois group G. We note that $(B * G)^{\bar{G}} \subset B * G$ is a Galois extension with Galois group $\bar{G}$. By Theorem 3.1 in [1], we also note that $B * G$ is an Azumaya C^G-algebra. Next are two equivalent conditions for a separable extension of $(B*G)^{\bar{G}}$ in $B*G$ which is invariant under a subgroup $\bar{K}$ of $\bar{G}$.

Theorem 4.1. *Let B be an Azumaya Galois extension of B^G, S a separable subalgebra of $B*G$ such that $(B*G)^{\bar{G}}\subset S$, $K=\{g\in G \mid \bar{g}(s)=s$ for all $s\in S\}$, and D the center of S. Then $S=(V_{B*G}(D))^{\bar{K}}$ if and only if $(V_{B*G}(S))^{\bar{K}}=D$.*

Proof. By the definition of K, $S\subset(B*G)^{\bar{K}}$, so $V_{B*G}(S)\supset V_{B*G}((B*G)^{\bar{K}})=V_{B*G}(V_{B*G}(C^GK))=C^GK$ by Proposition 3.1 (for C^GK is a separable subalgebra of the Azumaya C^G-algebra $B*G$). Similarly, since S is a separable subalgebra of $B*G$, $V_{B*G}(S)$ is also a separable subalgebra of $B*G$ and $V_{B*G}(V_{B*G}(S))=S$. Hence $V_{B*G}(S)$ and S have the same center D by Proposition 3.2. Thus, $V_{B*G}(S)$ is an Azumaya D-algebra. Noting that DK is a separable subalgebra of $V_{B*G}(S)$, by Proposition 3.1 for the Azumaya D-algebra $V_{B*G}(S)$, $V_{V_{B*G}(S)}(V_{V_{B*G}(S)}(DK))=DK$. Now assume $(V_{B*G}(S))^{\bar{K}}=D$. Then $V_{V_{B*G}(S)}(DK)=(V_{B*G}(S))^{\bar{K}}=D$. Hence $DK=V_{V_{B*G}(S)}(V_{V_{B*G}(S)}(DK))=V_{V_{B*G}(S)}(D)=V_{B*G}(S)$. Thus $S=V_{B*G}(V_{B*G}(S))=V_{B*G}(DK)=(V_{B*G}(D))^{\bar{K}}$. Conversely, assume $S=(V_{B*G}(D))^{\bar{K}}$. Then $S=(V_{B*G}(D))^{\bar{K}}=S(V_{B*G}(S))^{\bar{K}}\cong S\otimes_D(V_{B*G}(S))^{\bar{K}}$ as an Azumaya D-algebra by Proposition 3.2. Thus $(V_{B*G}(S))^{\bar{K}}\cong D$.

Next is another equivalent condition for $S=(B*G)^{\bar{K}}$.

Theorem 4.2. *Let B be an Azumaya Galois extension of B^G, S a separable subalgebra such that $(B*G)^{\bar{G}}\subset S\subset B*G$, $K=\{g\in G\mid \bar{g}(s)=s$ for all $s\in S\}$, $f_g: S\longrightarrow B*G$ by $f_g(s)=(s-\bar{g}(s))g$ for all $s\in S$ and each $g\in G$. Then*
(1) $f_g\in Hom_{C^G}(S,B*G)$ for each $g\in G$.
(2) $S=(B*G)^{\bar{K}}$ if and only if $\{f_g\mid g\notin K\}$ are linearly independent over C^G, that is, $\sum_{g\notin K}c_gf_g=0$ for some $c_g\in C^G$ implies that $c_g=0$ for each $g\notin K$.

Proof. (1) is clear.

(2) Observing that $B*G$ is an Azumaya C^G-algebra, we have that $S=(B*G)^{\bar{K}}$ if and only if $V_{B*G}(S)=V_{B*G}((B*G)^{\bar{K}})=V_{B*G}(V_{B*G}(C^GK))=C^GK$ by Proposition 3.1. Therefore, we only need to show that $V_{B*G}(S)=C^GK$ if and only if $\{f_g\mid g\notin K\}$ are linearly independent over C^G. Now assume that $V_{B*G}(S)=C^GK$. If $\sum_{g\notin K}c_gf_g=0$, that is, $\sum_{g\notin K}c_gf_g(s)=0$ for some $c_g\in C^G$ and all $s\in S$, then $\sum_{g\notin K}c_g(s-\bar{g}(s))g=0$. Hence $s\sum_{g\notin K}c_gg=\sum_{g\notin K}c_gsg=\sum_{g\notin K}c_g\bar{g}(s)g=\sum_{g\notin K}c_ggs$. Thus $\sum_{g\notin K}c_gg\in V_{B*G}(S)=$

$C^G K$. Therefore, c_g must be 0 for each $g \notin K$. This proves that $\{f_g \mid g \notin K\}$ are linearly independent over C^G. Conversely, since $(B*G)^{\bar{G}} \subset S$, $V_{B*G}(S) \subset V_{B*G}((B*G)^{\bar{G}})$. But $V_{B*G}((B*G)^{\bar{G}}) = V_{B*G}(V_{B*G}(C^G G)) = C^G G$ by Proposition 3.1, so $V_{B*G}(S) \subset C^G G$. For any $\sum_{g\in G} c_g g \in V_{B*G}(S)$ where $c_g \in C^G$, $s(\sum_{g\in G} c_g g) = (\sum_{g\in G} c_g g)s = \sum_{g\in G} c_g \bar{g}(s) g$. Hence $\sum_{g\in G} c_g(s-\bar{g}(s))g = 0$. Since $\bar{k}(s) = s$ for $k \in K$ and $s \in S$, $\sum_{g\notin K} c_g(s-\bar{g}(s))g = 0$ for all $s \in S$, that is, $\sum_{g\notin K} c_g f_g = 0$. By hypothesis, $\{f_g \mid g \notin K\}$ are linearly independent over C^G, so $c_g = 0$ for each $g \notin K$. Therefore, $V_{B*G}(S) = C^G K$.

Corollary 4.3. *Let* B*,* S*, and* K *be given in Theorem 4.2 and* S_g *the* C^G*-module generated by* $\{s - \bar{g}(s) \mid s \in S\}$*. If* $\sum_{g\notin K} S_g g$ *is a direct sum of faithful* C^G*-modules* $\{S_g g \mid g \notin K\}$*, then* $S = (B*G)^{\bar{K}}$*.*

Proof. By the proof of Theorem 4.2, for any $\sum_{g\in G} c_g g \in V_{B*G}(S)$, $\sum_{g\notin K} c_g(s-\bar{g}(s))g = 0$ for all $s \in S$. Since $\sum_{g\notin K} S_g g$ is a direct sum, $c_g(s-\bar{g}(s))g = 0$ for each $g \notin K$ and all $s \in S$. Hence $c_g S_g g = \{0\}$. But $S_g g$ is a faithful C^G-module, so $c_g = 0$ for each $g \notin K$. Thus $V_{B*G}(S) = C^G K$. Therefore, $S = V_{B*G}(V_{B*G}(S)) = V_{B*G}(C^G K) = (B*G)^{\bar{K}}$.

Corollary 4.4. *Let* B*,* S*, and* K *be given in Theorem 4.2. If* $S = (B*G)^{\bar{K}}$*, then* $Ann_{C^G}(S_g) = \{0\}$ *for each* $g \notin K$ *where* S_g *is the* C^G*-module generated by* $= \{s - \bar{g}(s) \mid s \in S\}$*.*

Proof. Since $S = (B*G)^{\bar{K}}$, $V_{B*G}(S) = C^G K$. As given in the proof of Corollary 4.3, $cS_g = \{0\}$ for a $c \in C^G$ implies that $c = 0$ for each $g \notin K$.

References

1. Alfaro R. and Szeto G.: On Galois extensions of an Azumaya algebra, Comm. in Algebra, 25(6): 1873-1882 (1997).
2. Alfaro R. and Szeto G.: Skew group rings which are Azumaya, Comm. in Algebra, 23(6): 2255-2261 (1995).
3. DeMeyer F.R.: Some notes on the general Galois theory of rings, Osaka J. Math., 2: 117-127 (1965).
4. DeMeyer F.R. and Ingraham E.: Separable Algebras over Commutative Rings, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.