ON CENTRAL COMMUTATOR GALOIS EXTENSIONS OF RINGS

GEORGE SZETO and LIANYONG XUE

Abstract. Let B be a ring with 1, G a finite automorphism group of B of order n for some integer n, B^G the set of elements in B fixed under each element in G, and $\Delta = V_B(B^G)$, the commutator subring of B^G in B. Then the type of central commutator Galois extensions is studied. This type includes the types of Azumaya Galois extensions and Galois H-separable extensions. Several characterizations of a central commutator Galois extension are given. Moreover, it is shown that when G is inner, B is a central commutator Galois extension of B^G if and only if B is a H-separable projective group ring $B^G G_f$. This generalizes the structure theorem for central Galois algebras with an inner Galois group proved by F. R. DeMeyer.

Keywords: Azumaya algebras, Galois extensions, central Galois extensions, Azumaya Galois extensions, center Galois extensions, and H-separable extensions.

AMS 1991 Subject Classification Codes: 16S35; 16W20

1. Introduction. Galois theory for commutative rings were studied in the sixties and seventies ([2], chapter 3), and several Galois extensions of noncommutative rings were also investigated ([3], [5], [6], [8]). Recently, central Galois extensions and the DeMeyer-Kanzaki Galois extensions were generalized to the Azumaya Galois extensions and center Galois extensions respectively ([1], [9], [10], [11]). B is called an Azumaya Galois extension of B^G with Galois group G if B is a Galois extension of B^G which is an Azumaya algebra over C^G where C is the center of B, and B is called a center Galois extension of B^G if C is a Galois algebra with Galois group $G|_C \cong G$. The purpose of the present paper is to study a type of Galois extensions which is strictly between the types of Azumaya Galois extensions and Galois H-separable extensions. Let $\Delta = V_B(B^G)$, the commutator subring of B^G in B. We call B a commutator Galois extension of B^G if Δ is a Galois extension with Galois group $G|_\Delta \cong G$, and B is a central commutator Galois extension of B^G if Δ is a central Galois algebra with Galois group $G|_\Delta \cong G$. We shall characterize a central commutator Galois extension in terms of a Galois H-separable extension B of B^G as studied by K. Sugano ([8]) and the C-modules $\{J_g \mid g \in G\}$ where $J_g = \{b \in B \mid ba = g(a)b$ for all $a \in B\}$. Moreover, it will be shown that B is a central commutator Galois extension of B^G with an inner Galois group G if and only if B is a H-separable projective group ring $B^G G_f$ where $B^G G_f = \sum_{g \in G} B^G U_g$ such that $\{U_g \,|\, g \in G\}$ are free over B^G, $bU_g = U_g b$ for all $b \in B^G$ and $g \in G$, and $U_g U_h = U_{gh} f(g,h)$ where $f : G \times G \longrightarrow$ units of C^G is a factor set. This generalizes the structure theorem for a central Galois algebra with an inner Galois group proved by F. R. DeMeyer ([4]). This paper was written under the support of a Caterpillar Fellowship at Bradley University. We would like to thank Caterpillar Inc. for the support.

2. Basic Definitions and Notations.

Throughout this paper, B will represent a ring with 1, C the center of B, G a finite automorphism group of B of order n for some integer n, B^G the set of elements in B fixed under each element in G, and $\Delta = V_B(B^G)$, the commutator subring of B^G in B.

Let A be a subring of a ring B with the same identity 1. 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 $\sum b a_i \otimes b_i = \sum a_i \otimes b_i b$ for all b in B where $\otimes$ is over A, and a ring B is called a H-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. An Azumaya algebra is a separable extension of its center. 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 $\sum_{i=1}^{m} c_i g(d_i) = \delta_{1,g}$ for $g \in G$. The set $\{c_i, d_i\}$ is called a G-Galois system for B. B is called a DeMeyer-Kanzaki Galois extension of B^G if B is an Azumaya C-algebra and C is a Galois algebra with Galois group $G|_C \cong G$. If C is a Galois algebra with Galois group $G|_C \cong G$, we call B a center Galois extension of B^G. B is called an Azumaya Galois extension if it is a Galois extension of B^G that is an Azumaya C^G-algebra, and B is called a Galois H-separable extension if it is a Galois and a H-separable extension of B^G (see [8]). We call B a commutator Galois extension of B^G if Δ is a Galois extension with Galois group $G|_\Delta \cong G$, and B is a central commutator Galois extension of B^G if Δ is a central Galois algebra with Galois group $G|_\Delta \cong G$. For each $g \in G$, let $J_g = \{b \in B \mid bx = g(x)b$ for all $x \in B\}$ and $J_g^A = \{a \in A \mid ax = g(x)a$ for all $x \in A\}$ for a subring A of B.

3. Central Commutator Galois Extensions.

In this section, we shall give several characterizations of a central commutator Galois extension in terms of Galois H-separable extensions and Azumaya Galois extensions respectively, and prove the converse of a theorem for a Galois H-separable extension as given in [8]. We begin with some properties of a commutator Galois extension.

Lemma 3.1. *If B is a commutator Galois extension of B^G, then Δ is a Galois algebra over C^G.*

Proof. Since Δ is a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$, B and $B^G\Delta$ are also Galois extensions of B^G with Galois group G and $G|_{B^G\Delta}$. But $B^G\Delta \subset B$ and $G \cong G|_{B^G\Delta}$, so $B = B^G\Delta$. Thus, the center of Δ is C; and so $\Delta^G = B^G \cap \Delta = C^G$.

Lemma 3.2. *If B is a commutator Galois extension of B^G, then $J_g = J_g^\Delta$ for each $g \in G$.*

Proof. Since $J_g = \{b \in B \mid ba = g(a)b$ for all $a \in B\} \subset \{b \in B \mid ba = g(a)b$ for all $a \in B^G\} = \Delta$, $J_g \subset J_g^\Delta$.

Conversely, for any $x \in J_g^\Delta$, $xd = g(d)x$ for all $d \in \Delta$. Since Δ is a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$, $B = B^G\Delta$ by the proof of Lemma 3.1. So for any $b \in B$, $b = \sum_{i=1}^m b_i d_i$ for some $b_i \in B^G$, $d_i \in \Delta$ and some integer m, we have that $xb = x\sum_{i=1}^m b_i d_i = \sum_{i=1}^m b_i x d_i = \sum_{i=1}^m b_i g(d_i)x = g(\sum_{i=1}^m b_i d_i)x = g(b)x$. Thus, $J_g^\Delta \subset J_g$; and so $J_g = J_g^\Delta$.

Theorem 3.3. *The following are equivalent:*

(1) B is a central commutator Galois extension of B^G.

(2) B is a commutator Galois extension of B^G and $J_g J_{g^{-1}} = C$ for each $g \in G$.

(3) B is a Galois H-separable extension of B^G, $B = B^G\Delta$, and $n^{-1} \in B$.

Proof. (1) $\Longrightarrow$ (2) It is clear.

(2) $\Longrightarrow$ (1) By Lemma 3.1, $\Delta^G = C^G$, so Δ is a Galois algebra with Galois group $G|_\Delta \cong G$. By hypothesis, $J_gJ_{g^{-1}} = C$ for each $g \in G$ and by Lemma 3.2, $J_g = J_g^\Delta$ for each $g \in G$, so Δ is a central Galois algebra ([5], Theorem 1).

(1) $\Longrightarrow$ (3) Since Δ is a central Galois C^G-algebra, we have $B = B^G\Delta$, $J_g = J_g^\Delta$ for each $g \in G$ by Lemma 3.2 and $J_g^\Delta J_{g^{-1}}^\Delta = C$ ([6], Lemma 2). Hence $J_gJ_{g^{-1}} = C$ for each $g \in G$. But B is a Galois extension of B^G with the same Galois system for Δ, so B is a Galois H-separable extension of B^G ([8], Theorem 2 (iii)$\Longrightarrow$(i)). Moreover, $n^{-1} \in B$ ([6], Corollary 3), so (3) holds.

(3) $\Longrightarrow$ (1) Since $B = B^G\Delta$, the group $H = \{g \in G \mid g|_\Delta \text{ is an identity}\} = \{1\}$. Thus, Δ is a central Galois algebra over Δ^G ([8], Theorem 6, (3) (ii)$\Longrightarrow$(iii)) where $\Delta^G = C^G$ by Lemma 3.1.

We remark that (1) $\Longrightarrow$ (3) in Theorem 3.3 is the converse of Theorem 6 in [8]; that is, if Δ is a central Galois algebra with Galois group $G|_\Delta \cong G$, then (i) $n^{-1} \in B$, (ii) $B = B^G\Delta$, and (iii) B is a Galois H-separable extension of B^G.

In next theorem, we give a characterization of a central commutator Galois extension in terms of Azumaya Galois extensions

Theorem 3.4. *The following are equivalent:*

(1) B is a central commutator Galois extension of B^G and B^G is a separable C^G-algebra.

(2) B is an Azumaya Galois extension with Galois group G.

(3) B is a central commutator Galois extension and a separable extension of Δ.

Proof. (1) $\Longrightarrow$ (2) Since B is a central commutator Galois extension, B is a Galois H-separable extension of B^G by Theorem 3.3-(3). Thus, $V_B(V_B(B^G)) = B^G$ ([8], Proposition 4-(1)). This implies that $C \subset B^G$; and so $C = C^G$. Moreover, by Theorem 3.3-(3) again, $B = B^G\Delta$, so the center of B^G is C^G, the center of B. Thus, B^G is an Azumaya C^G-algebra. By noting that B is a Galois extension of B^G, (2) holds.

(2) $\Longrightarrow$ (1) is a consequence of Lemma 1 in [1].

(1) $\Longrightarrow$ (3) Since B is a separable extension of B^G (for it is a Galois extension) and B^G is a separable C^G-algebra, B is a separable C^G-algebra by the transitivity property of separable extensions. Thus, B is a separable extension of Δ because $C^G \subset \Delta \subset B$.

(3) $\Longrightarrow$ (1) Since Δ is a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$, Δ is a separable extension of Δ^G. By Lemma 3.1, $\Delta^G = C^G = C$ (for C is the center of Δ). By hypothesis, B is a separable extension of Δ. Hence B is a separable extension of C, that is, B is an Azumaya C-algebra. By Lemma 3.1 again, $B = B^G\Delta$ such that B^G and Δ are C-subalgebras of the Azumaya C-algebra B. Hence, they are Azumaya C-algebras by the commutator theorem for Azumaya algebras ([2], Theorem 4.3, page 57). Since Δ is a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$, B is a Galois extension of B^G which is an Azumaya C^G-algebra. This completes the proof.

4. *H*-separable Projective Group Rings.

In [4], it was shown that B is a central Galois algebra with an inner Galois group G if and only if B is an Azumaya projective group algebra C^GG_f over C^G where $C^GG_f = \sum_{g\in G} C^GU_g$ such that $\{U_g\,|\,g\in G\}$ are free over C^G, $cU_g = U_gc$ for all $c \in C^G$ and $g \in G$, and $U_gU_h = U_{gh}f(g,h)$, $f : G\times G \longrightarrow$ units of C^G is a factor set ([4]). We shall generalize this fact to a central commutator Galois extension with an inner Galois group.

Theorem 4.1. *B is a central commutator Galois extension of B^G with an inner Galois group G if and only if $B = B^GG_f$ which is a H-separable extension of B^G and $n^{-1} \in B$.*

Proof. ($\Longrightarrow$) By Theorem 3.3 (1)$\Longrightarrow$(3), $B = B^G\Delta$ which is a Galois H-separable extension of B^G and $n^{-1} \in B$, so it suffices to shown that $B = B^GG_f$, a projective group ring with coefficient ring B^G. Since Δ is a central Galois C^G-algebra, by Theorem 2 in [4], $\Delta = C^GG_f$, a projective group algebra over C^G where $f : G\times G \longrightarrow$ units of C^G is a factor set such that $f(g,h) = U_gU_hU_{gh}^{-1}$ for all $g,h \in G$. Noting that $bU_g = U_gb$ for all $b \in B^G$ and $g \in G$, we claim that $\{U_g\,|\,g \in G\}$ are independent over B^G. Assume $\sum_{g\in G} b_gU_g = 0$ for some $b_g \in B^G$ and $g \in G$. Since Δ is a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$, there exists a G-Galois system $\{c_i, d_i,\ i = 1, 2, ..., m$ for some integer $m\}$ for Δ such that $\sum_{i=1}^m c_ig(d_i) = \delta_{1,g}$ for $g \in G$. Hence $b_1 = \sum_{g\in G}\delta_{1,g}b_gU_g = \sum_{g\in G}\sum_{i=1}^m c_ig(d_i)b_gU_g = \sum_{g\in G}\sum_{i=1}^m c_ib_gg(d_i)U_g = \sum_{g\in G}\sum_{i=1}^m c_ib_gU_gd_i = \sum_{i=1}^m c_i(\sum_{g\in G} b_gU_g)d_i = 0$. So $\sum_{g\in G} b_gU_g = 0$ for some $b_g \in B^G$ and $g \in G$ implies that $b_1 = 0$. Now for any $h \in G$, since $\sum_{g\in G} b_gU_g = 0$, $0 = \sum_{g\in G} b_gU_gU_{h^{-1}} = \sum_{g\in G} b_gf(g,h^{-1})U_{gh^{-1}}$. Thus, $b_hf(h,h^{-1}) = 0$, and so $b_h = 0$. This proves that $\{U_g\,|\,g \in G\}$ are independent over B^G.

($\Longleftarrow$) Since $B^G G_f (\cong B^G \otimes_{C^G} C^G G_f)$ is a H-separable extension of B^G and B^G is a direct summand of $B^G G_f$ as a left B^G-module, $V_{B^G G_f}(V_{B^G G_f}(B^G)) = B^G$. This implies that the center of $B^G G_f$ is C^G. Moreover, G is inner induced by $\{U_g \,|\, g \in G\}$, so $J_g = C^G U_g$ for each $g \in G$. But then $C^G G_f = \oplus \sum_{g \in G} C^G U_g = \oplus \sum_{g \in G} J_g$ such that $J_g J_{g^{-1}} = (C^G U_g)(C^G U_{g^{-1}}) = C^G$ for all $g \in G$. By hypothesis, $n^{-1} \in C^G$, so $C^G G_f$ is a separable algebra over C^G. Thus, $\Delta (= C^G G_f)$ is a central Galois algebra ([5], Theorem 1) with an inner Galois group $\bar{G}$ induced by $\{U_g \,|\, g \in G\}$. Thus, B is a central commutator Galois extension of B^G with an inner Galois group G.

By Theorem 1.2 in [7], we derive a one-to-one correspondence between some sets of separable subextensions in a central commutator Galois extension B of B^G. Let $\mathcal{S} = \{\mathcal{A} \mid \mathcal{A}$ is a separable subextension of B containing B^G which is a direct summand of B as a bimodule $\}$ and $\mathcal{T} = \{\mathcal{D} \mid \mathcal{D}$ is a separable subalgebra of Δ over $C^G\}$.

Theorem 4.2. *Let B be a central commutator Galois extension of B^G. Then, there exists a one-to-one correspondence between $\mathcal{S}$ and $\mathcal{T}$ by $A \longrightarrow V_B(A)$.*

Proof. By Theorem 3.3-(4), B is a H-separable extension of B^G, so the correspondence holds by Theorem 1.2 in [7].

We conclude this paper with two examples of Galois extension B to show that

(1) B is a central commutator Galois extension but not an Azumaya Galois extension (see Theorem 3.4), and

(2) B is a Galois H-separable extension but not a central commutator Galois extension (see Theorem 3.3).

Example 1. Let $A = Q[i,j,k]$ be the quaternion algebra over the rational field Q, $B = \{\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \mid a_1, a_2, a_3 \in A\}$, the ring of all 2 by 2 upper triangle matrices over A and $G = \{1,\ g_i,\ g_j,\ g_k\}$ where $g_i(a) = iai^{-1}$, $g_j(a) = jaj^{-1}$, $g_k(a) = kak^{-1}$ for all a in A and $g\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} = \begin{pmatrix} g(a_1) & g(a_2) \\ 0 & g(a_3) \end{pmatrix}$ for $g \in G$. Then

(1) $A^G = Q$.

(2) $B^G = \{\begin{pmatrix} q_1 & q_2 \\ 0 & q_3 \end{pmatrix} \mid q_1, q_2, q_3 \in Q\}$, the ring of all 2 by 2 upper triangle matrices over Q.

(3) $\Delta = V_B(B^G) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in A\} \cong A$.

(4) Δ is a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$ and a Galois system $\{1,\ i,\ j,\ k;\ \frac{1}{4},\ -\frac{1}{4}i,\ -\frac{1}{4}j,\ -\frac{1}{4}k\}$.

(5) $\Delta^G = Q$ is the center of Δ.

(6) By (4) and (5), B is a central commutator Galois extension of B^G.

(7) The center of B^G is Q.

(8) B^G is not a separable extension of its center Q, and so B^G is not an Azumaya algebra. In fact, suppose that B^G is a separable extension of Q. Then, there exists a separable idempotent

$$e = \sum_{\substack{1 \le i \le j \le 2 \\ 1 \le k \le l \le 2}} q_{ijkl}(e_{ij} \otimes e_{kl}),$$

where $e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, and $q_{ijkl} \in Q$ such that $\sum_{\substack{1 \le i \le j \le 2 \\ 1 \le k \le l \le 2}} q_{ijkl}e_{ij}e_{kl} = I_2$, the identity 2 by 2 matrix, and $be = eb$ for all $b \in B^G$. By $e_{11}e = ee_{11}$, we have

$$\sum_{\substack{1 \le j \le 2 \\ 1 \le k \le l \le 2}} q_{1jkl}(e_{1j} \otimes e_{kl}) = \sum_{1 \le i \le j \le 2} q_{ij11}(e_{ij} \otimes e_{11}).$$

Hence $q_{2211} = 0$ and $q_{1jk2} = 0$ for all j, k, that is, $q_{1112} = q_{1122} = q_{1212} = q_{1222} = 0$. By $e_{12}e = ee_{12}$, we have

$$\sum_{1 \le k \le l \le 2} q_{22kl}(e_{12} \otimes e_{kl}) = \sum_{1 \le i \le j \le 2} q_{ij11}(e_{ij} \otimes e_{12}).$$

Hence $q_{22kl} = 0$ if $(k, l) \ne (1, 2)$ and $q_{ij11} = 0$ if $(i, j) \ne (1, 2)$, that is, $q_{2211} = q_{2222} = 0$ and $q_{1111} = q_{2211} = 0$. Therefore, $e = q_{1211}(e_{12} \otimes e_{11}) + q_{2212}(e_{22} \otimes e_{12})$. Thus, $I_2 = \sum_{\substack{1 \le i \le j \le 2 \\ 1 \le k \le l \le 2}} q_{ijkl}e_{ij}e_{kl} = q_{1211}e_{12}e_{11} + q_{2212}e_{22}e_{12} = 0$. This contradiction shows that B^G is not a separable extension of Q.

Example 2 Let $B = Q[i, j, k]$ be the quaternion algebra over the rational field Q and $G = \{1,\ g_i\}$ where $g_i(x) = ixi^{-1}$ for all x in B. Then

(1) B is a Galois extension of B^G with Galois group G and a Galois system $\{1,\ i,\ j,\ k;\ \frac{1}{4},\ -\frac{1}{4}i,\ -\frac{1}{4}j,\ -\frac{1}{4}k\}$.

(2) Since G is inner, B is a H-separable extension of B^G.

(3) By (1) and (2), B is a Galois H-separable extension of B^G.

(4) $\Delta = V_B(B^G) = Q[i]$ is not a Galois extension of Δ^G with Galois group $G|_\Delta \cong G$, and so B is not a central commutator Galois extension of B^G.

REFERENCES

[1] R. Alfaro, S. Szeto, On Galois Extensions of an Azumaya Algebra, Comm. in Algebra, **25(6)** (1997) 1873-1882.

[2] F.R. DeMeyer, E. Ingraham, Separable Algebras over Commutative Rings, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.

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

[4] F.R. DeMeyer, Galois Theory in Separable Algebras over Commutative Rings, Illinois J. Math.,10: 287-295, 1966.

[5] M. Harada, Supplementary Results on Galois Extension, Osaka J. Math., 2 (1965), 343-350.

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

[7] K. Sugano, On Centralizers In Separable Extensions, Osaka J. Math., 7(1970), 29-41.

[8] K. Sugano, On a Special Type of Galois Extensions, Hokkaido J. Math., **9** (1980) 123-128.

[9] G. Szeto and L. Ma, On center Galois extensions over rings, Glasnik Matematicki, Vol 24(1989), 11-16.

[10] S. Szeto, L. Xue, On Three types of Galois Extensions of rings, Southeast Asian Bulletin of Mathematics, 23(1999) 1-6.

[11] S. Szeto, L. Xue, On Characterizations of a Center Galois Extension, International Journal of Mathematics and Mathematical Sciences, to appear.

GEORGE SZETO and LIANYONG XUE
Mathematics Department, Bradley University, Peoria, Illinois 61625, USA
Email: szeto@hilltop.bradley.edu and lxue@hilltop.bradley.edu