The Fundamental Theorem for Azumaya Automorphism and Galois Extensions of Rings

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

ABSTRACT. Let B be a ring with 1, G an automorphism group of B of order n for some integer n invertible in B, C the center of B, and B^G the set of elements in B fixed under each element in G. Then, B is called an Azumaya automorphism extension of B^G with group G if $B \cong B^G \otimes_{C^G} V_B(B^G)$ as Azumaya C^G-algebras under the multiplication map. In this paper we establish a one-to-one correspondence between the set of subgroups of G and the set of minimal central factors of some Azumaya automorphism subextensions of B when B is an Azumaya automorphism and a Galois extension of B^G with Galois group G. Consequently, the fundamental theorem for Galois extension is derived for B.

1. Introduction.

In [1], B is called a DeMeyer-Kanzaki Galois extension of B^G with Galois group G if B is an Azumaya algebra over C which is a Galois algebra with Galois group induced by and isomorphic with G. The class of DeMeyer-Kanzaki Galois extensions was investigated in [2] and [4], and it was generalized to the class of Azumaya Galois extensions [1] and the class of center Galois extensions [5], [6], and [7] respectively. We note that the structure of both DeMeyer-Kanzaki Galois extension and Azumaya Galois extension are similar; that

---

AMS 1991 Subject Classification Codes: 16S35; 16W20

This work was done under the support of a Caterpillar Fellowship at Bradley University. The authors would like to thank Caterpillar Inc. for the support.

is, $B \cong B^G \otimes_{C^G} V_B(B^G)$ as C^G-algebras under the multiplication map where B^G is an Azumaya C^G-algebra and $V_B(B^G)$ is a central Galois algebra with Galois group induced by and isomorphic with G ([1], Theorem 1 and Theorem 2). Removing the Galois condition on B, we define a class of ring extensions B called an Azumaya automorphism extension of B^G with group G if $B \cong B^G \otimes_{C^G} V_B(B^G)$ as Azumaya C^G-algebras under the multiplication map. For an Azumaya automorphism extension B with group G both B^G and $V_B(B^G)$ are Azumaya C^G-algebras by the commutator theorem for Azumaya algebras and $(V_B(B^G))^G = C^G$ since $B^G \cap V_B(B^G) = C^G$. We call $V_B(B^G)$ the central factor of such a B. The purpose of the present paper is to show a one-to-one correspondence between the set of subgroups of G and the set of minimal central factors of some Azumaya automorphism subextensions of B if B is an Azumaya automorphism and a Galois extension of B^G with Galois group G. Consequently, the fundamental theorem for B can be derived.

2. Definitions and Notations.

Throughout, B will represent a ring with 1, G an automorphism group of B of order n for some integer n invertible in B, C the center of B, and B^G the set of elements in B fixed under each element in G.

Let A be a subring of a ring B with the same identity 1. $V_B(A)$ is 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 $\sum b a_i \otimes b_i = \sum a_i \otimes b_i b$ for all b in B where $\otimes$ is over A. 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 $\{a_i, b_i$ in B, $i = 1, 2, ..., m\}$ for some integer m such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. Such a set $\{a_i, b_i\}$ is called a G-Galois system for B. B is called an Azumaya Galois extension if B is a Galois extension with Galois group G over an Azumaya C^G-algebra B^G. We call B a DeMeyer-Kanzaki Galois extension of B^G with Galois group G if B is an Azumaya

C-algebra and C is a Galois algebra with Galois group $G|_C \cong G$. We call B an Azumaya automorphism extension of B^G with group G if $B \cong B^G \otimes_{C^G} V_B(B^G)$ as Azumaya C^G-algebras under the multiplication map, and $V_B(B^G)$ is called the central factor of such a B.

3. The Fundamental Theorem.

Let B be an Azumaya automorphism and a Galois extension of B^G with Galois group G. Then, a one-to-one correspondence between the set of subgroups of G and the set of minimal central factors of some Azumaya automorphism subextensions of B is given. This derives the fundamental theorem for Galois extension B. Throughout this section, we assume that B is an Azumaya automorphism and a Galois extension of B^G with Galois group G. Let S be a commutative separable subalgebra of B over C^G. We shall first give an equivalent condition for $V_B(S)$ being an Azumaya automorphism extension with group induced by a subgroup K of G.

Theorem 3.1

Let S be a commutative separable subalgebra of B over C^G. Then,

(1) $V_B(S)$ is an Azumaya S-algebra.

(2) $V_B(S)$ is an Azumaya automorphism extension with group induced by a subgroup K of G if and only if $(V_B(S))^K$ is an Azumaya S-algebra.

PROOF. (1) Since B is an Azumaya automorphism extension with group G, B is an Azumaya C^G-algebra. But, by hypothesis, S is a separable C^G-algebra, so $V_B(S)$ is a separable C^G-algebra such that $V_B(V_B(S)) = S$ by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). This implies that $V_B(S)$ is an Azumaya S-algebra ([3], Theorem 3.8, page 55).

(2) ($\Longrightarrow$) Denote $V_B(S)$ by Δ. By (1), $\Delta(= V_B(S))$ is an Azumaya S-algebra. But, by hypothesis, Δ is an Azumaya automorphism extension with group induced by K. Hence $\Delta \cong \Delta^K \otimes_S V_\Delta(\Delta^K)$ as Azumaya S-algebras. Thus, Δ^K is an Azumaya S-algebra ([3], Theorem 4.4, page 58).

($\Longleftarrow$) Since $(V_B(S))^K$ is an Azumaya S-algebra, $S \subset (V_B(S))^K \subset B^K$. Thus, $V_B(S)$ is invariant under K, that is, $k(V_B(S)) = V_B(S)$ for each $k \in K$. Moreover, by (1), $\Delta(= V_B(S))$ is an Azumaya S-algebra and Δ^K is an Azumaya S-algebra by hypothesis, so Δ^K is an Azumaya S-subalgebra of Δ. Hence $\Delta \cong \Delta^K \otimes_S V_\Delta(\Delta^K)$ as Azumaya S-algebras by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). Thus, noting that $S = S^K$, Δ is an Azumaya automorphism extension with group induced by K.

By Theorem 3.1, we can identify the Azumaya automorphism subextensions arising from subgroups of G.

Corollary 3.2

Let K be a subgroup of G and S the center of B^K. Assume S is a separable C^G-algebra. Then $B^K \cdot V_B(B^K)$ is an Azumaya automorphism extension of B^K with group induced by K if and only if B^K is an Azumaya S-algebra.

PROOF. ($\Longrightarrow$) Since $B^K \cdot V_B(B^K)$ is an Azumaya automorphism extension of B^K with group induced by K and S is the center of B^K, $B^K\big(= (B^K \cdot V_B(B^K))^K\big)$ is an Azumaya S-algebra.

($\Longleftarrow$) Since S is a commutative separable subalgebra of B over C^G, $V_B(S)$ is an Azumaya S-algebra by Theorem 3.1-(1). Moreover, by hypothesis, B^K is an Azumaya S-algebra, so B^K is a separable C^G-algebra by the transitivity of separable extensions. Hence $V_B(V_B(B^K)) = B^K$ by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). This implies that B^K, $V_B(B^K)$, and $B^K \cdot V_B(B^K)$ $\big(\cong B^K \otimes_S V_B(B^K)\big)$ have the same center S. Thus, $B^K \cdot V_B(B^K)$ is an Azumaya S-subalgebra of $V_B(S)$ which we denote by Δ. Therefore, by the commutator theorem for Azumaya algebras, $\Delta \cong (B^K \cdot V_B(B^K)) \otimes_S V_\Delta(B^K \cdot V_B(B^K))$. But, $S \subset V_\Delta(B^K \cdot V_B(B^K)) \subset V_B(B^K \cdot V_B(B^K)) = S$ since $V_B(V_B(B^K)) = B^K$ and the center of B^K is S; and so $\Delta \cong (B^K \cdot V_B(B^K)) \otimes_S V_\Delta(B^K \cdot V_B(B^K)) = (B^K \cdot V_B(B^K)) \otimes_S S \cong B^K \cdot V_B(B^K)$. Consequently, $B^K \cdot V_B(B^K) = \Delta = V_B(S)$ and $(V_B(S))^K = (B^K \cdot V_B(B^K))^K = B^K$ which is an Azumaya S-algebra. Thus, by theorem 3.1-(2), $B^K \cdot V_B(B^K) (= V_B(S))$ is an Azumaya automorphism extension of B^K with group induced by K.

To establish a one-to-one correspondence between the set of subgroups K of G and the set of "some" separable subalgebras of B over C^G, we need the notion of minimal central factor of an Azumaya automorphism subextension of B with group induced by K.

Definition 1

Let $\mathcal{C}_K$ be the set of Azumaya automorphism subextensions of B of the form $V_B(S)$ with group induced by K for a subgroup K of G where S is a commutative separable subalgebra of B over C^G.

Definition 2

Let $\Delta = V_B(S) \in \mathcal{C}_K$ where S is a commutative separable subalgebra of B over C^G. $V_\Delta(\Delta^K)$ is called a minimal central factor in $\mathcal{C}_K$ if for any $\Delta' = V_B(S') \in \mathcal{C}_K$ where S' is a commutative separable subalgebra of B over C^G, $V_{\Delta'}((\Delta')^K) \subset V_\Delta(\Delta^K)$ implies that $V_{\Delta'}((\Delta')^K) = V_\Delta(\Delta^K)$

We shall show a one-to-one correspondence between the set of subgroups K of G and the set of minimal central factors in $\mathcal{C}_K$ for subgroups K of G. We begin with some properties of $\mathcal{C}_K$.

Lemma 3.3

Let $\Delta = V_B(S) \in \mathcal{C}_K$ where S is a commutative separable subalgebra of B over C^G. Then $V_\Delta(\Delta^K) = V_B(\Delta^K)$.

PROOF. Since S is a commutative separable subalgebra of B over C^G, $\Delta(= V_B(S))$ is an Azumaya S-algebra by Theorem 3.1-(1). Moreover, since $\Delta = V_B(S) \in \mathcal{C}_K$, $\Delta \cong \Delta^K \otimes_S V_\Delta(\Delta^K)$ as Azumaya S-algebras. Hence Δ^K is an Azumaya S-algebra ([3], Theorem 4.4, page 58); and so $S \subset \Delta^K$. Therefore, $V_B(\Delta^K) \subset V_B(S) = \Delta$. Thus, $V_\Delta(\Delta^K) = V_B(\Delta^K)$.

Lemma 3.4

Let B be an Azumaya automorphism and a Galois extension of B^G with Galois group G, K a subgroup of G, and S the center of B^K. Then B^K is an Azumaya S-algebra and S is a separable algebra over C^G.

PROOF. Since B is a Galois extension of B^G with Galois group G, B is also a Galois extension of B^K with Galois group K. Hence B is a finitely generated and projective left (or right) B^K-module. But B is an Azumaya automorphism extension of B^G with group G, so B is an Azumaya C^G-algebra. Moreover, noting that $|G|^{-1} \in B$, we have $|K|^{-1} \in B$, and so B^K is a direct summand of B as a B^K-bimodule. Therefore, B^K is a separable algebra over C^G by the proof of Theorem 3.8 on page 55 in [3]. Consequently, B^K is an Azumaya S-algebra and S is a separable algebra over C^G ([3], Theorem 3.8, page 55).

Lemma 3.5

Let B be given in Lemma 3.4. Then, for any subgroup K of G,

(1) $B^K \cdot V_B(B^K) \in \mathcal{C}_K$, and

(2) $V_B(B^K)$ is the unique minimal central factor in $\mathcal{C}_K$.

PROOF. (1) Let S be the center of B^K. Then, B^K is an Azumaya S-algebra and S is a separable algebra over C^G by Lemma 3.4. Hence $B^K \cdot V_B(B^K)$ is an Azumaya automorphism extension with group induced by K by Corollary 3.2. Moreover, by the proof of Corollary 3.2, $B^K \cdot V_B(B^K) = V_B(S)$. Thus, $B^K \cdot V_B(B^K) \in \mathcal{C}_K$.

(2) Let $\Delta \in \mathcal{C}_K$. Then $\Delta = \Delta^K \cdot V_\Delta(\Delta^K)$ is an Azumaya automorphism extension with group induced by K. Since $\Delta^K \subset B^K$, $V_B(B^K) \subset V_B(\Delta^K) = V_\Delta(\Delta^K)$ by Lemma 3.3. Thus, $V_B(B^K)$ is contained in every central factor in $\mathcal{C}_K$. Moreover, by (1), $B^K \cdot V_B(B^K) \in \mathcal{C}_K$. Denote $B^K \cdot V_B(B^K)$ by F. Then $V_F(F^K) = V_B(F^K)$ by Lemma 3.3. But, $F^K = B^K$, so $V_B(B^K) = V_F(F^K)$ is a central factor in $\mathcal{C}_K$. This implies that $V_B(B^K)$ is the unique minimal central factor in $\mathcal{C}_K$.

We now show a one-to-one correspondence theorem.

Theorem 3.6

Let B be an Azumaya automorphism and a Galois extension of B^G with Galois group G. Then, there exists a one-to-one correspondence between the set of subgroups K of G and the set of minimal central factors in $\mathcal{C}_K$ for subgroups K of G.

PROOF. By Lemma 3.5-(2), the map $\alpha : K \longrightarrow V_B(B^K)$ is well defined and onto. Next, we claim that α is one-to-one. In fact, let $\alpha(K) = \alpha(H)$ for some subgroups K and H of G. Then $V_B(B^K) = V_B(B^H)$. But, by Lemma 3.4, B^K and B^H are separable C^G-subalgebras of the Azumaya C^G-algebra B, so $V_B(V_B(B^K)) = B^K$ and $V_B(V_B(B^H)) = B^H$ by the commutator theorem for Azumaya algebras. Thus, $B^K = B^H$. Denote $\langle K, H\rangle$ the subgroup of G generated by the elements in K and H. Then, since B is a Galois extension of B^G with Galois group G, B is also a Galois extension of B^K with Galois group K, a Galois extension of B^H with Galois group H, and a Galois extension of $B^{\langle K,H\rangle}$ with Galois group $\langle K, H\rangle$. Thus, $B * K \cong \mathrm{Hom}_{B^K}(B, B)$, $B * H \cong \mathrm{Hom}_{B^H}(B, B)$, and $B * \langle K, H\rangle \cong \mathrm{Hom}_{B^{\langle K,H\rangle}}(B, B)$ ([2], Theorem 1). But, $B^K = B^H = B^{\langle K,H\rangle}$, so $B * K \cong B * H \cong B * \langle K, H\rangle$. Hence the order of K, H, and $\langle K, H\rangle$ are same. Therefore. $K = H = \langle K, H\rangle$. Thus, α is one-to-one.

By Theorem 3.6, the well known fundamental theorem for Galois extension is derived for B.

Theorem 3.7

Let B be given in Theorem 3.6. Then, there exists a one-to-one correspondence between the set of subgroups K of G and the set of commutators of the minimal central factors in $\mathcal{C}_K$ for subgroups K of G.

PROOF. By Theorem 3.6, $\alpha : K \longrightarrow V_B(B^K)$ is a bijection, and $\beta : V_B(B^K) \longrightarrow V_B(V_B(B^K)) = B^K$ (the set of commutators of the minimal central factors in $\mathcal{C}_K$ for subgroups K of G) is a bijection by the commutator theorem for Azumaya algebras. Thus, $\beta \circ \alpha : K \longrightarrow B^K$ is a bijection between the set of subgroups K of G and the set of B^K which are commutators of the minimal central factors $V_B(B^K)$ in $\mathcal{C}_K$ for subgroups K of G.

We conclude the present paper with an example to demonstrate our results.

Example 1

Let $A = Q[i,j,k]$ be the quaternion algebra over the rational field Q, $B = M_2(A)$ the 2×2 matrix ring over A, and $G = \{1, g_i, g_j, g_k\}$ where
$g_i(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} iai^{-1} & ibi^{-1} \\ ici^{-1} & idi^{-1} \end{pmatrix}$, $g_j(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} jaj^{-1} & jbj^{-1} \\ jcj^{-1} & jdj^{-1} \end{pmatrix}$, and
$g_k(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} kak^{-1} & kbk^{-1} \\ kck^{-1} & kdk^{-1} \end{pmatrix}$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in B$. Then,

(1) The center of B is $C = \{\begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} | q \in Q\} \cong Q$, and $Q^G = Q$.

(2) $B^G = M_2(Q)$, the 2×2 matrix ring over Q. Hence B^G is an Azumaya Q-algebra.

(3) $V_B(B^G) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} | a \in A\} \cong A$ which is a Galois extension of Q with Galois group induced by and isomorphic with G with a Galois system: $\{\frac{1}{2},\ \frac{1}{2}i,\ \frac{1}{2}j,\ \frac{1}{2}k;\ \frac{1}{2},\ -\frac{1}{2}i,\ -\frac{1}{2}j,\ -\frac{1}{2}k\}$.

(4) $B \cong B^G \otimes_Q V_B(B^G)$ as Azumaya Q-algebras under the multiplication map.

(5) By (3), B is a Galois extension with Galois group G.

(6) B is an Azumaya automorphism and a Galois extension of B^G with Galois group G by (4) and (5).

(7) The nontrivial subgroups of G are $K_i = \{1, g_i\}$, $K_j = \{1, g_j\}$, and $K_k = \{1, g_k\}$.

(8) $B^{K_i} = M_2(Q[i])$ with center $S_i = \{\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} |s \in Q[i]\} \cong Q[i]$,

$B^{K_j} = M_2(Q[j])$ with center $S_j = \{\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} |s \in Q[j]\} \cong Q[j]$, and

$B^{K_k} = M_2(Q[k])$ with center $S_k = \{\begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} |s \in Q[k]\} \cong Q[k]$.

(9) $V_B(B^{K_i}) = S_i$ which is the minimal central factor in $\mathcal{C}_{K_i}$,

$V_B(B^{K_j}) = S_j$ which is the minimal central factor in $\mathcal{C}_{K_j}$, and

$V_B(B^{K_k}) = S_k$ which is the minimal central factor in $\mathcal{C}_{K_k}$.

(10) $\alpha : K \longrightarrow V_B(B^K)$ is a one-to-one correspondence between the set of subgroups K of G and the set of minimal central factors in $\mathcal{C}_K$ for subgroups K of G.

REFERENCES

1. R. Alfaro and G. Szeto, Skew Group Rings Which Are Azumaya, Comm. in Algebra, 23(6) (1995), 2255-2261.

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, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.

4. T. Kanzaki, On Galois Algebra over A Commutative Ring, Osaka J. Math., 2 (1965), 309-317.

5. G. Szeto and L. Xue, On The Ikehata Theorem for H-separable Skew Polynomial Rings, Mathematical Journal of Okayama University, 40(1998), 27-32[2000].

6. G. Szeto and L. Xue, The General Ikehata Theorem for H-separable Crossed Products, International Journal of Mathematics and Mathematical Sciences, to appear.

7. G. Szeto and L. Xue, On Characterizations of A Center Galois Extension, International Journal of Mathematics and Mathematical Sciences, to appear.