

ON COMMUTATOR GALOIS EXTENSIONS

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 a finite automorphism group of B , B^G the subring of elements in B fixed under each element in G , and $\Delta = V_B(B^G)$ the commutator subring of B^G in B . A structure theorem of B is given when Δ is a Galois extension with Galois group $G|_{\Delta} \cong G$, which generalizes a structure of a Galois algebra, and the study of the commutator Galois extension B is reduced to the study of the Galois extension B with one orbit under the action of G on the isomorphic summands of B .

1. Introduction

Galois theory for fields was generalized for rings in the sixties. Several interesting classes of Galois extensions for noncommutative rings were studied ([2], [4], [6], [8]). Recently, the class of the DeMeyer-Kanzaki Galois extensions was generalized to the Azumaya Galois extensions ([1], [5]) and the class of center Galois extensions ([7]) respectively. In [9], a Galois algebra was shown to be a finite direct sum of central Galois algebras with

2000 Mathematics Subject Classification: 16S35, 16W20

Key Words and Phrases: Galois extensions, commutator Galois extensions, Galois algebras, central Galois algebras, and center Galois extensions.

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.

subgroups of G as Galois groups and a commutative Galois algebra with Galois group induced by and isomorphic with G . The purpose of the present paper is to generalize the above structure theorem for a Galois algebra to a commutator Galois extension. Let B be a Galois extension of B^G with Galois group G where B^G is the subring of elements in B fixed under each element in G , and $\Delta = V_B(B^G)$ the commutator subring of B^G in B . In section 3, we shall show that if B is a commutator Galois extension with Galois group G (that is, Δ is a Galois extension with Galois group $G|_{\Delta} \cong G$), then B is a finite direct sum of central commutator Galois extensions with subgroups of G as Galois groups and a center Galois extension with Galois group induced by and isomorphic with G . Moreover, by using the structure for a Galois algebra ([9], Theorem 3.8) we shall show that for a commutator Galois extension B with Galois group G , B is a direct sum of Galois extensions B_i and a center Galois extension with Galois groups all isomorphic with G such that each direct summand B_i is a direct sum of isomorphic ideals $\{Bf_{ij}\}$ generated by central orthogonal idempotents $\{f_{ij}\}$ and G acts on the set of isomorphic ideals $\{Bf_{ij}\}$ transitively, that is, $\{Bf_{ij}, j = 1, 2, \dots, n_i\}$ has one orbit under G . Consequently, the study of a commutator Galois extension B is reduced to the study of the type of Galois extensions B_i with Galois group isomorphic with G such that $B_i = \sum_{j=1}^{n_i} Bf_{ij}$ and G acts transitively on the summands $\{Bf_{ij}\}$ and a center Galois extension. In section 4, for a Galois algebra B of type B_i , we shall give an expression of the subring B^H of the elements fixed under each element in a subgroup H of G , and an equivalent condition under which a subring T is B^H for some subgroup H of G . This derives a one-to-one correspondence between a set of some subgroups of G and a set of some separable subalgebras.

2. 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 , 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. We denote $V_B(A)$ the commutator subring of A in B , Δ the commutator subring $V_B(B^G)$ of B^G in B , $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$, and $J_g^{(A)} = \{b \in A \mid bx = g(x)b \text{ for all } x \in A\}$ for each $g \in G$. We call B a separable extension of A if there exist $\{a_i, b_i \text{ in } B, i = 1, 2, \dots, m \text{ for some integer } m\}$ such that $\sum a_i b_i = 1$, and $b \sum a_i \otimes b_i = \sum a_i \otimes b_i b$ 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 $\{a_i, b_i \text{ in } B, i = 1, 2, \dots, m\}$ for some integer m such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1,g}$ for each $g \in G$, B is called a Galois algebra over R if B is a Galois extension of R which is contained in C , and B is called a central Galois extension if B is a Galois extension of C . We call B a center Galois extension of B^G ([7]) if C is a Galois algebra over C^G with Galois group $G|_C \cong G$, B is an Azumaya Galois extension of B^G ([1]) if it is a Galois extension of B^G which is a C^G -Azumaya algebra, B is called a DeMeyer-Kanzaki Galois extension with Galois group G ([2], [4]) if B is an Azumaya C -algebra and a center Galois extension with Galois group G . We call B a commutator Galois extension with Galois group G if Δ is a Galois extension with Galois group $G|_\Delta \cong G$, and a central commutator Galois extension if Δ is a central Galois algebra with Galois group $G|_\Delta \cong G$.

3. A Structure Theorems

In this section, we shall show a structure theorem mentioned in section 1, which generalizes the structure of a Galois algebra as given in [9], and show that a commutator Galois extension B can be reduced to the study of the type of Galois extensions with one orbit under the action of G on the isomorphic summands of B . Let $K = \{g \in G \mid g(d) = d \text{ for all } d \in \Delta\}$. It is easy to see that K is a normal subgroup of G and G/K is an automorphism group of Δ where $\bar{g}(d) = g(d)$ for all $\bar{g} \in G/K$ and $d \in \Delta$. We first show

that B^K is a commutator Galois extension with Galois group \overline{G} ($= G/K$), and give a structure theorem for B^K when Δ is a Galois extension of $\Delta^{\overline{G}}$ with Galois group \overline{G} . Then we generalize the following structure theorem for a Galois algebra as given in [9] to a commutator Galois extension.

Proposition 3.1. ([9], Theorem 3.8) *Let A be a Galois algebra over a commutative ring R with Galois group G . Then there exist central orthogonal idempotents $\{f_i \in C \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ and subgroups H_i of G such that $A = (\oplus \sum_{i=1}^m Af_i) \oplus Af$, where $f = 1 - \sum_{i=1}^m f_i$, Af_i is a central Galois algebra with Galois group $H_i|_{Af_i} \cong H_i$ for each $i = 1, 2, \dots, m$, and $Af = Cf$ which is a commutative Galois algebra with Galois group $G|_{Cf} \cong G$ in case $f \neq 0$.*

Lemma 3.2. *If A is a central Galois algebra over its center C with Galois group H , then $(D \otimes_C A)^{1 \otimes H} = D \otimes_C A^H$ for any C -algebra D .*

Proof. Since A is a central Galois algebra with Galois group H , the order of H is a unit in A ([4], Corollary 3). Let k be the order of H and $x (= \sum_{i=1}^l d_i \otimes a_i)$ be any element in $(D \otimes_C A)^{1 \otimes H}$ for some integer l . Then $kx = Tr_{1 \otimes H}(x) = \sum_{i=1}^l d_i \otimes Tr_H(a_i)$; and so $x = \sum_{i=1}^l d_i \otimes \frac{1}{k} Tr_H(a_i)$ which is contained in $D \otimes_C A^H$. Thus $(D \otimes_C A)^{1 \otimes H} \subset D \otimes_C A^H$. The other inclusion $D \otimes_C A^H \subset (D \otimes_C A)^{1 \otimes H}$ is clear, so the lemma is proved.

Theorem 3.3. *If Δ is a Galois extension of $\Delta^{\overline{G}}$ with Galois group \overline{G} , then (1) B^K is a commutator Galois extension of B^G with Galois group \overline{G} , and (2) there exist orthogonal idempotents $\{f_i \in Z \mid i = 1, 2, \dots, m \text{ for some integer } m\}$, where Z is the center of Δ , and subgroups \overline{H}_i of \overline{G} such that $B^K = (\oplus \sum_{i=1}^m B^K f_i) \oplus B^K f$ where $B^K f_i$ is a central commutator Galois extension with Galois group $\overline{H}_i|_{B^K f_i} \cong \overline{H}_i$ for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m f_i$, and $B^K f$ is a center Galois extension with Galois group $\overline{G}|_{B^K f} \cong \overline{G}$ in case $f \neq 0$.*

Proof. (1) Since $\Delta \subset V_{B^G \Delta}(B^G) \subset V_B(B^G) = \Delta$, we have that $V_{B^G \Delta}(B^G) = \Delta$. Thus, $B^G \Delta$ is a commutator Galois extension of B^G with Galois group $\overline{G}|_{B^G \Delta}$. Moreover, since $B^G \Delta \subset B^K$ such that $(B^K)^{\overline{G}} = B^G = (B^G \Delta)^{\overline{G}}$, both B^K and $B^G \Delta$ are Galois extensions of B^G with Galois group \overline{G} . Thus we conclude that $B^K = B^G \Delta$. Therefore, B^K is a commutator Galois extension of B^G with Galois group \overline{G} .

(2) We first show that $\Delta^{\overline{G}}$ is contained in Z . In fact, since B is a Galois extension of B^G with Galois group G , $\Delta = \bigoplus \sum_{g \in G} J_g$ ([4], Proposition 1). Hence for any $x \in \Delta^{\overline{G}} (= \Delta^G)$ and $d \in \Delta$, $d = \sum_{g \in G} b_g$ for some $b_g \in J_g$, so $b_g x = g(x) b_g = x b_g$ for each $g \in G$. Thus $dx = \sum_{g \in G} b_g x = \sum_{g \in G} x b_g = x \sum_{g \in G} b_g = xd$ for any $d \in \Delta$; and so, $x \in Z$ for any $x \in \Delta^{\overline{G}}$. Therefore, $\Delta^{\overline{G}} \subset Z$. But Δ is a Galois extension of $\Delta^{\overline{G}}$ by hypothesis, so Δ is a Galois algebra with Galois group \overline{G} . Hence, by Proposition 3.1, there exist orthogonal idempotents $\{f_i \in Z \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ and subgroups \overline{H}_i of \overline{G} such that $\Delta = (\bigoplus \sum_{i=1}^m \Delta f_i) \oplus \Delta f$ where Δf_i is a central Galois algebra with Galois group $\overline{H}_i|_{\Delta f_i} \cong \overline{H}_i$ for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m f_i$, and $\Delta f (= Zf)$ is a commutative Galois algebra with Galois group $\overline{G}|_{\Delta f} \cong \overline{G}$ in case $f \neq 0$. Since f_i and f are in the center of Δ , they are also in the center of $B^G \Delta$. Hence $B^K = B^G \Delta = (\bigoplus \sum_{i=1}^m B^G \Delta f_i) \oplus B^G \Delta f = (\bigoplus \sum_{i=1}^m B^K f_i) \oplus B^K f$. Since Δf_i is a central Galois algebra with Galois group $\overline{H}_i|_{\Delta f_i} \cong \overline{H}_i$, $B^K f_i (= B^G \Delta f_i)$ is a Galois extension with Galois group $\overline{H}_i|_{B^K f_i} \cong \overline{H}_i$. Next, by Lemma 3.2, we have

$$((B^G Z f_i) \otimes_{Z f_i} (\Delta f_i))^{1 \otimes \overline{H}_i} = (B^G Z f_i) \otimes_{Z f_i} (\Delta f_i)^{\overline{H}_i} = (B^G Z f_i) \otimes_{Z f_i} (Z f_i),$$

so $((B^G Z f_i) \otimes_{Z f_i} (\Delta f_i))^{\overline{H}_i} = (B^G Z f_i)(Z f_i)$. Hence

$$(B^K f_i)^{\overline{H}_i} = (B^G \Delta f_i)^{\overline{H}_i} = ((B^G Z f_i) \otimes_{Z f_i} (\Delta f_i))^{\overline{H}_i} = (B^G Z f_i)(Z f_i) = B^G Z f_i.$$

Moreover, noting that $B^K = B^G \Delta$, we have that $V_{B^K f_i}(B^G Z f_i) = \Delta f_i$. Thus $B^K f_i$ is a central commutator Galois extension with Galois group $\overline{H}_i|_{B^K f_i} \cong \overline{H}_i$ for each $i = 1, 2, \dots, m$. Furthermore, we claim that $B^K f$ is a center Galois extension with Galois group

$\overline{G}|_{B^K f} \cong \overline{G}$ in case $f \neq 0$. Since $\Delta f (= Zf)$ is a commutative Galois algebra with Galois group $\overline{G}|_{\Delta f} \cong \overline{G}$ in case $f \neq 0$ by Proposition 3.1, we only need to show that $\Delta f (= Zf)$ is the center of $B^K f$. In fact, $B^K = B^G \Delta$, so B^K and Δ have the same center Z . Thus, $B^K f$ has the center Zf . This completes the proof.

Now the structure theorem for a Galois algebra as given in Proposition 3.1 is generalized to a commutator Galois extension.

Corollary 3.4. *If B is a commutator Galois extension with Galois group G , then (1) $B = B^G \Delta$ and (2) there exist orthogonal idempotents $\{f_i \in Z \mid i = 1, 2, \dots, m \text{ for some integer } m\}$, where Z is the center of Δ , and subgroups H_i of G such that $B = (\oplus \sum_{i=1}^m B f_i) \oplus B f$ where $B f_i$ is a central commutator Galois extension with Galois group $H_i|_{B f_i} \cong H_i$ for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m f_i$, and $B f$ is a center Galois extension with Galois group $G|_{B f} \cong G$ in case $f \neq 0$.*

Next, by using the structure theorem for a Galois algebra ([9], Theorem 3.8) we show that the study of a commutator Galois extension B can be reduced to the Galois extensions with one orbit under the action of G on the isomorphic summands.

Lemma 3.5. *Let A be a Galois algebra with Galois group G . Then there exist central orthogonal idempotents $\{e_i \in C \mid i = 1, 2, \dots, k \text{ for some integer } k\}$ such that (1) $A = (\oplus \sum_{i=1}^k A e_i) \oplus A f$, where $f = 1 - \sum_{i=1}^k e_i$, $A e_i$ is a Galois algebra with Galois group $G|_{A e_i} \cong G$ for each $i = 1, 2, \dots, k$, $A f = C f$ which is a commutative Galois algebra with Galois group $G|_{C f} \cong G$ in case $f \neq 0$, and (2) $A e_i = \oplus \sum_{j=1}^{n_i} A f_{ij}$ which is a direct sum of isomorphic ideals $\{A f_{ij}\}$ generated by central orthogonal idempotents $\{f_{ij}\}$ such that G acts on the set of isomorphic ideals $\{A f_{ij}\}$ transitively, that is, $\{A f_{ij}, j = 1, 2, \dots, n_i\}$ has one orbit under G .*

Proof. (1) By the proof of Proposition 3.1 ([9], Theorem 3.8), $Af_i = A(\prod_{h_i \in H_i} J_{h_i})$ where H_i is a maximal subset of G such that $\prod_{h_i \in H_i} J_{h_i} \neq \{0\}$. We note that H_i is also a subgroup of G by Lemma 3.5 in [9]. Hence, for any $g \in G$, $Ag(f_i) = g(Af_i) = g(A(\prod_{h_i \in H_i} J_{h_i})) = A(\prod_{h_i \in H_i} J_{gh_i g^{-1}})$. This implies that $gH_i g^{-1}$ is a maximal subset (subgroup) of G such that $\prod_{h_i \in gH_i g^{-1}} J_{h_i} \neq \{0\}$. Thus, $g(Af_i) = Ag(f_i) = Af_j$, a direct summand of A . Therefore g permutes the direct summands of A , that is, g permutes the set of idempotents, $\{f_i \mid i = 1, 2, \dots, m\}$ denoted by F . Let $\{F_i \mid i = 1, 2, \dots, k$ for some integer $k\}$ be the distinct orbits of F under the action of G . Then $F = \cup_{i=1}^k F_i$, a disjoint union of orbits $\{F_i\}$, where $F_i = \{g(f_j) \mid g \in G \text{ for some } f_j\}$. Rewrite the index of elements in F_i by $F_i = \{f_{ij} \mid j = 1, 2, \dots, n_i \text{ for some integer } n_i\}$. Let $e_i = \sum_{j=1}^{n_i} f_{ij}$. Then $\{e_i \mid i = 1, 2, \dots, k\}$ are central orthogonal idempotents such that $g(e_i) = e_i$ for each $g \in G$, that is, $e_i \in C^G$ for each $i = 1, 2, \dots, k$. Hence Ae_i is a Galois algebra with Galois group $G|_{Ae_i} \cong G$ ([9], Lemma 3.7). Moreover, noting that $\sum_{i=1}^k e_i = \sum_{i=1}^k \sum_{j=1}^{n_i} f_{ij} = \sum_{i=1}^m f_i$, we have that $f = 1 - \sum_{i=1}^k e_i$. Thus, $Af = Cf$ which is a commutative Galois algebra with Galois group $G|_{Cf} \cong G$ in case $f \neq 0$ by Proposition 3.1, and $A = (\oplus \sum_{i=1}^k Ae_i) \oplus Af$.

(2) By the proof of part (1), $Ae_i = \oplus \sum_{j=1}^{n_i} Af_{ij}$ which is a direct sum of isomorphic ideals $\{Af_{ij}\}$ generated by central orthogonal idempotents $\{f_{ij}\}$ and G acts on the set of isomorphic ideals $\{Af_{ij}\}$ transitively. This completes the proof.

As a consequence of Lemma 3.5, we obtain an expression for a commutator Galois extension B^K with Galois group $\overline{G} (= G/K)$ where $K = \{g \in G \mid g(d) = d \text{ for all } d \in \Delta\}$ and B with Galois group G respectively.

Theorem 3.6. *Let B be a Galois extension of B^G with Galois group G such that Δ is a Galois extension with Galois group $\overline{G} (= G/K)$. Then there exist orthogonal idempotents $\{e_i \in Z \mid i = 1, 2, \dots, k \text{ for some integer } k\}$, where Z is the center of Δ , such that $B^K = (\oplus \sum_{i=1}^k B^K e_i) \oplus B^K f$ where $B^K e_i = \sum_{j=1}^{n_i} B^K f_{ij}$ which is a Galois*

extension with Galois group induced by and isomorphic with \overline{G} such that the action of \overline{G} on $\{f_{ij} \mid j = 1, 2, \dots, n_i\}$ has exactly one orbit; that is, $\{f_{ij} \mid j = 1, 2, \dots, n_i\}$ is transitive under the action of \overline{G} for each $i = 1, 2, \dots, k$, and $B^K f$ is a center Galois extension with Galois group $\overline{G}|_{B^K f} \cong \overline{G}$ in case $f \neq 0$.

Proof. By the proof of Theorem 3.3, Δ is a Galois algebra with Galois group \overline{G} , so, by Lemma 3.5, there exist orthogonal idempotents $\{e_i \in Z \mid i = 1, 2, \dots, k \text{ for some integer } k\}$ such that $\Delta = (\oplus \sum_{i=1}^k \Delta e_i) \oplus \Delta f$ where Δe_i is a Galois algebra with Galois group $\overline{G}|_{\Delta e_i} \cong \overline{G}$, $\Delta f (= Zf)$ is a commutative Galois algebra with Galois group $\overline{G}|_{\Delta f} \cong \overline{G}$ in case $f = 1 - \sum_{i=1}^k e_i \neq 0$, and $\Delta e_i = \sum_{j=1}^{n_i} \Delta f_{ij}$ such that the action of \overline{G} on $\{f_{ij} \mid j = 1, 2, \dots, n_i\}$ has exactly one orbit. By Theorem 3.3, $B^K = B^G \Delta$ which is a commutator Galois extension with Galois group \overline{G} , so, $B^K = B^G \Delta = (\oplus \sum_{i=1}^k B^G \Delta e_i) \oplus B^G \Delta f = (\oplus \sum_{i=1}^k B^K e_i) \oplus B^K f$ where $B^K e_i = \sum_{j=1}^{n_i} B^K f_{ij}$ which is a Galois extension with Galois group induced by and isomorphic with \overline{G} such that the action of \overline{G} on $\{f_{ij} \mid j = 1, 2, \dots, n_i\}$ has exactly one orbit, and $B^K f$ is a center Galois extension with Galois group $\overline{G}|_{B^K f} \cong \overline{G}$ in case $f \neq 0$.

Theorem 3.7. *Let B be a commutator Galois extension with Galois group G . Then there exist orthogonal idempotents $\{e_i \in Z \mid i = 1, 2, \dots, k \text{ for some integer } k\}$, where Z is the center of Δ , such that (1) $B = (\oplus \sum_{i=1}^m B e_i) \oplus Bf$, and (2) $B e_i = \sum_{j=1}^{n_i} B f_{ij}$ which is a Galois extension with Galois group induced by and isomorphic with G such that the action of G on $\{f_{ij} \mid j = 1, 2, \dots, n_i\}$ has exactly one orbit, and Bf is a center Galois extension with Galois group induced by and isomorphic with G in case $f \neq 0$.*

Proof. Since B is a commutator Galois extension with Galois group G , $K = \{1\}$. Thus Theorem 3.7 is a consequence of Theorem 3.6.

4. Invariant Subrings

In section 3, Lemma 3.5 reduces the study of a Galois algebra A to the study of the type of the Galois algebra Ae_i with Galois group induced by and isomorphic with G such that (1) $Ae_i = \sum_{i=1}^m Af_{ij}$ where $\{Af_{ij}\}$ are isomorphic ideals of A and $\{f_{ij}\}$ are central orthogonal idempotents, and (2) G acts transitively on the summands $\{Af_{ij}\}$ of Ae_i . In this section, we shall study a Galois algebra A of this type: $A = \sum_{i=1}^m Ae_i$ where $\{e_i\}$ are central orthogonal idempotents and G acts transitively on the summands $\{Ae_i\}$. We shall show an expression of each element in B^H for a subgroup H of G and give an equivalent condition under which a subring T is B^H for a subgroup H of G . We begin with a relation between G and the automorphism group of Ae_i for each i induced by G . Denote the set $\{\alpha_{ij} : Ae_i \rightarrow Ae_j \mid \alpha_{ij} = g|_{Ae_i} \text{ for some } g \in G\}$ by $G(i, j)$. Clearly $G(i, i)$ is an automorphism group of Ae_i for each i .

Theorem 4.1. *For any pair $1 \leq i, j \leq m$, there exists an $g \in G$ such that $G(j, j) = gG(i, i)g^{-1}$ and $G(i, j) = gG(i, i)$.*

Proof. Since G acts transitively on $\{e_i \mid i = 1, 2, \dots, m\}$, there exists an $g \in G$ such that $g(e_i) = e_j$. Hence $G(j, j) = g(g^{-1}G(j, j)g)g^{-1} \subset gG(i, i)g^{-1} \subset G(j, j)$. Thus, $G(j, j) = gG(i, i)g^{-1}$. Similarly, $G(i, j) = gG(i, i)$.

Next we show an expression of each element in A^H for a subgroup H and give an equivalent condition under which a subring T is B^H for a subgroup H of G . We denote the subset of $G(i, j)$, $\{\alpha \in G(i, j) \mid \alpha = h|_{Ae_i} \text{ for some } h \in H\}$ by $H(i, j)$ for a subgroup H of G .

Lemma 4.2. *Let H be a subgroup of G . Then $A^H = \{a \mid a = \sum_{i=1}^m a_i \text{ where } a_i \in Ae_i \text{ and } \alpha(a_i) = a_j \text{ for each } \alpha \in H(i, j), 1 \leq i, j \leq m\}$.*

Proof. Let $a \in A^H$. Then $a = \sum_{i=1}^m a_i$ for some $a_i \in Ae_i$. Since $h(a) = a$ for each $h \in H$, $\sum_{i=1}^m h(a_i) = \sum_{i=1}^m a_i$. But $A = \bigoplus \sum_{i=1}^m Ae_i$ where h permutes $\{e_i\}$, so h permutes $\{a_i\}$. Hence $h(a_i) = a_j$ if $h|_{Ae_i} \in H(i, j)$. This implies that $A^H \subset \{a \mid a = \sum_{i=1}^m a_i \text{ where } a_i \in Ae_i \text{ and } \alpha(a_i) = a_j \text{ for each } \alpha \in H(i, j), 1 \leq i, j \leq m\}$. The converse is clear.

Let T be a subring of A and $H = \{g \in G \mid g(t) = t \text{ for each } t \in T\}$. Then we have $T \subset A^H$. The following is an equivalent condition under which $T = A^H$.

Theorem 4.3. *Let T be a subring of A and $H = \{g \in G \mid g(t) = t \text{ for each } t \in T\}$. Then $T = A^H$ if and only if $Te_i = (Ae_i)^{H(i, i)}$ for some e_i in each orbit of $\{e_i \mid i = 1, 2, \dots, m\}$ under the action of H .*

Proof. (\implies) Let $T = A^H$. Then $T = A^H = \{a \mid a = \sum_{i=1}^m a_i \text{ where } a_i \in Ae_i \text{ and } \alpha(a_i) = a_j \text{ for each } \alpha \in H(i, j), 1 \leq i, j \leq m\}$ by Lemma 4.2. In particular, for $a = \sum_{i=1}^m a_i \in T$ where $a_i \in Ae_i$, $\alpha(a_i) = a_i$ for each $\alpha \in H(i, i)$, so $Te_i \subset (Ae_i)^{H(i, i)}$ for each i . On the other hand, for any $ae_i \in (Ae_i)^{H(i, i)}$, let $t = \sum_{j=1}^{n_i} h_j(ae_i)$ where $\{h_j(e_i) \mid h_j \in H \text{ and } j = 1, 2, \dots, n_i\}$ for some integer n_i is the orbit containing e_i under the action of H ; then $t \in A^H = T$. Thus $ae_i = te_i \in Te_i$, and so $(Ae_i)^{H(i, i)} \subset Te_i$.

(\impliedby) By Lemma 4.2, $A^H = \{a \mid a = \sum_{i=1}^m a_i \text{ where } a_i \in Ae_i \text{ and } \alpha(a_i) = a_j \text{ for each } \alpha \in H(i, j), 1 \leq i, j \leq m\}$. Hence $A^H e_i \subset \{a_i e_i \in Ae_i \mid \alpha(a_i) = a_i \text{ for each } \alpha \in H(i, i)\} \subset (Ae_i)^{H(i, i)}$ for each $i = 1, 2, \dots, m$. But $Te_i = (Ae_i)^{H(i, i)}$ for an e_i in each orbit of $\{e_i \mid i = 1, 2, \dots, m\}$ under the action of H by hypothesis, so for each $j = 1, 2, \dots, m$, there is an e_i in the same orbit of e_j and an $h \in H(i, j)$ such that $h(e_i) = e_j$. Thus $A^H e_j = A^H h(e_i) = h(A^H e_i) \subset h((Ae_i)^{H(i, i)}) = h(Te_i) = Te_j$; and so $A^H e_j = Te_j$ for each $j = 1, 2, \dots, m$. Hence $T = T \sum_{j=1}^m e_j = \sum_{j=1}^m Te_j = \sum_{j=1}^m A^H e_j = A^H$.

Let n , the order of G , be invertible in A . We shall show a set of some subgroups of G

is in a one-to-one correspondence with the set of separable subalgebras T of A such that $Te_i = (Ae_i)^{H(i,i)}$ for an e_i in each orbit of $\{e_i \mid i = 1, 2, \dots, m\}$ under the action of H .

Lemma 4.4. *Let A be a Galois algebra with Galois group G of order n invertible in A and H a subgroup of G . Then A^H is a separable subalgebra of A .*

Proof. Since A is a Galois algebra with Galois group G and H is a subgroup of G , A is a Galois extension of A^H with Galois group H . Hence A is finitely generated and projective left (or right) module over A^H . But n is invertible in A . Thus A^H is a direct summand of A as a A^H -bimodule. Therefore A^H is a separable subalgebra because A is so ([3], proof of Theorem 3.8, page 55).

Let H be a subgroup of G . We call H an I -maximal subgroup if $A^K = A^H$ for a subgroup K of G implies that $K \subset H$. We now show the set of the I -maximal subgroups of G and the set of separable subalgebras of A as given in Theorem 4.3 are in a one-to-one correspondence.

Theorem 4.5. *Let A be a Galois algebra with Galois group G of order n invertible in A . Then the set of the I -maximal subgroups of G is in a one-to-one correspondence with the set of separable subalgebras T of A such that $Te_i = (Ae_i)^{H(i,i)}$ for an e_i in each orbit of $\{e_i \mid i = 1, 2, \dots, m\}$ under the action of H , where $H = \{g \in G \mid g(t) = t \text{ for each } t \in T\}$.*

Proof. Let H be an I -maximal subgroup of G . Then, by Lemma 4.4, A^H is a separable subalgebra of A such that $A^H e_i = (Ae_i)^{H(i,i)}$ for an e_i in each orbit of $\{e_i \mid i = 1, 2, \dots, m\}$ under the action of H by Theorem 4.3; and so the map $\alpha : H \rightarrow A^H$ is well defined. Also, Theorem 4.3 and Lemma 4.4 imply that α is onto. Moreover, let K and H be two subgroups of G such that $\alpha(K) = \alpha(H)$, that is, $A^K = A^H$. Then $A^{\langle K, H \rangle} = A^K = A^H$

where $\langle K, H \rangle$ is the subgroup of G generated by elements of K and H . This implies that any subgroup is contained uniquely in an I -maximal subgroup, so α is one-to-one.

We conclude the present paper with an example to demonstrate the structure as given in Theorem 3.7.

Example 4.6. Let $R[i, j, k]$ be the real quaternion algebra over the field of real numbers R , $A = (R[i, j, k] \otimes_R R[i, j, k]) \oplus R[i, j, k] \oplus R[i, j, k] \oplus R[i, j, k] \oplus R[i, j, k] \oplus R[i, j, k]$, and $G = \langle H, K \rangle$ where $H = \{1, h_i, h_j, h_k\}$, $K = \{1, s_i, s_j, s_k\}$, and for all $(a \otimes b, a_1, a_2, a_3, a_4) \in A$

$$h_i(a \otimes b, a_1, a_2, a_3, a_4) = (iai^{-1} \otimes b, ia_1i^{-1}, ia_2i^{-1}, ia_3i^{-1}, ia_4i^{-1}),$$

$$h_j(a \otimes b, a_1, a_2, a_3, a_4) = (jaj^{-1} \otimes b, ja_1j^{-1}, ja_2j^{-1}, ja_3j^{-1}, ja_4j^{-1}),$$

$$h_k(a \otimes b, a_1, a_2, a_3, a_4) = (kak^{-1} \otimes b, ka_1k^{-1}, ka_2k^{-1}, ka_3k^{-1}, ka_4k^{-1}),$$

$$s_i(a \otimes b, a_1, a_2, a_3, a_4) = (a \otimes ibi^{-1}, a_2, a_1, a_4, a_3),$$

$$s_j(a \otimes b, a_1, a_2, a_3, a_4) = (a \otimes jbj^{-1}, a_3, a_4, a_1, a_2),$$

$$s_k(a \otimes b, a_1, a_2, a_3, a_4) = (a \otimes kbk^{-1}, a_4, a_3, a_2, a_1).$$

Then,

(1) A is a Galois extension with Galois group G .

(2) $A^G = \{(r_1 \otimes r_2, r, r, r, r) \mid r_1, r_2, r \in R\} \cong R \oplus R$.

(3) The center of A is $C = (R \otimes R) \oplus R \oplus R \oplus R \oplus R (\cong R \oplus R \oplus R \oplus R \oplus R)$.

(4) By (1), (2), and (3), A is a Galois algebra with Galois group G , but not a central Galois algebra with Galois group G .

(5) Let e_i be the idempotent with 1 at the i^{th} -component and 0 elsewhere for $i = 1, 2, 3, 4, 5$. Then $e_1 = (1 \otimes 1, 0, 0, 0, 0)$ and $e_2 + e_3 + e_4 + e_5 = (0, 1, 1, 1, 1)$ are orthogonal idempotents in A^G ; and so Ae_1 and $A(e_2 + e_3 + e_4 + e_5)$ are Galois algebras with Galois group induced by and isomorphic with G respectively ([9], Lemma 3.7).

(6) $A(e_2 + e_3 + e_4 + e_5) = \oplus \sum_{i=2}^5 Ae_i$, and the action of G on $\{e_i \mid i = 2, 3, 4, 5\}$ has exactly one orbit.

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, 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] M. Ouyang, Galois Extensions and Galois Correspondence, *Algebra Colloquium*, 7(1)(2000), 43-57.
- [6] K. Sugano, On a Special Type of Galois Extensions, *Hokkaido J. Math*, 9(1980), 123-128.
- [7] G. Szeto and L. Xue, On Characterizations of a Center Galois Extension, *International Journal of Mathematics and Mathematical Sciences*, 23(11)(2000), 753-758.
- [8] G. Szeto and L. Xue, On Central Commutator Galois Extensions of Rings, *International Journal of Mathematics and Mathematical Sciences*, Vol. 24(5)(2000), 289-294.
- [9] G. Szeto and L. Xue, The Structure of Galois Algebras, *Journal of Algebra*, 237(1)(2001), 238-246.