

On Galois Algebras with a Unique Galois Group

Xiaolong Jiang, George Szeto, and Lianyong Xue*

Department of Mathematics

Bradley University

Peoria, Illinois 61625

E-mail: szeto@bradley.edu, lxue@bradley.edu

ABSTRACT

Equivalent conditions for a central Galois algebra to admit a unique Galois group are given, and a classification of semiconnected Galois extensions with a unique Galois group is also obtained.

1. Introduction

Let F be a field finite Galois extension of F^G with Galois group G . It is well known that $G = \text{Aut}_{F^G}(F)$, the F^G -automorphism group of F . This fact was extended to an indecomposable commutative ring finite Galois extension S ; that is, S is a commutative ring Galois extension with no idempotents but 0 and 1 with a finite Galois group G , then $G = \text{Aut}_{S^G}(S)$ ([1], Theorem 3.5). This fact implies that S admits a unique Galois group G . By noting that there are Galois extensions of a ring with more than one Galois group (see Examples in section 4), the purpose of the present paper is to show two equivalent conditions for a central Galois algebra to admit a unique Galois group. Moreover, a class of semiconnected Galois extensions with a unique Galois group is investigated, and examples are given to demonstrate the results.

* Corresponding author

AMS 2000 Subject Classification Codes: 16S35, 16W20

Key Words and Phrases: Galois extensions, Galois algebras, Semiconnected Galois extensions, Galois groups.

This paper was written under the support of a Caterpillar Fellowship at Bradley University and during the visit of the first author to Bradley University from Zhongshan University, P. R. China supported by Lingnan Foundation. She would like to thank Bradley University for her hospitality.

2. Basic Definitions and Notations

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 , and A a subring of B with the same identity 1. The commutator subring of A in B is denoted by $V_B(A)$. We call B a Galois extension of B^G with Galois group G if there exist elements $\{a_i, b_i$ 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 $g \in G$. Such a set $\{a_i, b_i\}$ is called a G -Galois system for B . A ring 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 algebra if B is a Galois extension of C . An automorphism α of B is called a Galois element if there exist elements $\{x_i, y_i$ in B , $i = 1, 2, \dots, r\}$ for some integer r such that $\sum_{i=1}^r x_i \alpha(y_i) = \delta_{1,\alpha}$. We call B semiconnected if it contains only finitely many central idempotents.

Throughout this paper, we assume that B is a Galois extension of B^G with Galois group G , C the center of B , $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$, and $J_\alpha = \{b \in B \mid bx = \alpha(x)b \text{ for all } x \in B\}$ for $\alpha \in \text{Aut}_{B^G}(B)$.

3. Characterizations

In this section, two characterizations of a central Galois algebra with a unique Galois group are given. Moreover, a sufficient condition is given for a Galois algebra to admit a unique Galois group. Let B be a Galois extension of A with Galois group G . The expression of the commutator subring of A in B , $V_B(A)$, as given in [3] will play an important role.

Proposition 3.1. ([3], Proposition 1) *Let B be a Galois extension of A with Galois group G . Then*

$$V_B(A) = \oplus \sum_{g \in G} J_g.$$

Proposition 3.2. ([5], Proposition 4) *Let B be a central Galois algebra over its center C with Galois group G . Then J_g is a projective rank one C -module for each $g \in G$.*

We recall that an element $\alpha \in \text{Aut}_A(B)$ is called a Galois element if there exist $\{x_i, y_i$ in $B, i = 1, 2, \dots, r\}$ for some integer r such that $\sum_{i=1}^r x_i \alpha(y_i) = \delta_{1,\alpha}$. Hence for a subgroup G_β of $\text{Aut}_A(B)$, G_β is a Galois group for B if each element $g \in G_\beta$ is a Galois element with the same set $\{x_i, y_i$ in $B, i = 1, 2, \dots, r\}$ such that $\sum_{i=1}^r x_i g(y_i) = \delta_{1,g}$ for each $g \in G_\beta$. We denote $\cup G_\beta$ by \mathcal{S} where G_β is a Galois group for B over A and β in some index set I .

Theorem 3.3. *Let B be a central Galois algebra over C with Galois group G . Then the following statements are equivalent:*

(1) *The Galois group is unique.*

(2) *B is a direct sum of rank one projective C -modules $\{J_g \mid g \in H\}$ for a Galois group H over C unique up to the order of summands and gh is a Galois element for B for all $g, h \in \mathcal{S}$.*

(3) *B is a direct sum of rank one projective C -modules $\{J_g \mid g \in H\}$ for a Galois group H over C unique up to the order of summands and $I_{gh} = B$ for all $g, h \in \mathcal{S}$ such that $gh \neq 1$ where I_{gh} is the left ideal generated by $\{b - gh(b) \mid b \in B\}$.*

Proof. (1) \implies (2) Since B is a central Galois algebra over C with Galois group G , $B = \oplus \sum_{g \in G} J_g$ by Proposition 3.1. Moreover, by hypothesis, G is unique, so $\mathcal{S} = G$. Hence the direct sum is unique up to the order of summands. On the other hand, since $\mathcal{S} = G$, it is clear that gh is a Galois element for B for all $g, h \in \mathcal{S}$.

(2) \implies (3) We only need to show that $I_{gh} = B$ for all $g, h \in \mathcal{S}$ such that $gh \neq 1$. By hypothesis, gh is a Galois element for B . Let $\{a_i, b_i$ in $B, i = 1, 2, \dots, m$ for some integer $m\}$ be a gh -Galois system. Then $\sum_{i=1}^m a_i gh(b_i) = \delta_{1,gh}$. Thus $\sum_{i=1}^m a_i (b_i - gh(b_i)) = 1$, and so the left ideal $I_{gh} = B$.

(3) \implies (1) Assume there is another Galois group H for B over C . Then $B = \bigoplus \sum_{g \in G} J_g = \bigoplus \sum_{h \in H} J_h$ by Proposition 3.1. By hypothesis, the direct sum is unique up to the order of summands. Hence for each $g \in G$, there exists an $h \in H$ such that $J_g = J_h$. We claim that $g = h$. Assume $g \neq h$. Then $g^{-1}h \neq 1$. Now for any $a \in J_g = J_h$, $ax = g(x)a = h(x)a$, and so $(g(x) - h(x)) \cdot a = 0$ for all $x \in B$. Thus $(x - g^{-1}h(x)) \cdot g^{-1}(a) = 0$ for all $x \in B$. Since $I_{g^{-1}h} = B$ for all $g^{-1}h \in \mathcal{S}$ such that $g^{-1}h \neq 1$, $g^{-1}(a) = 0$; and so $a = 0$. But J_g is a rank one projective C -module by Proposition 3.2, so $J_g \neq \{0\}$. This contradiction implies that $g = h$. Therefore $G \subset H$. Similarly, $H \subset G$. Thus $G = H$.

Next we show a sufficient condition under which a Galois algebra has a unique Galois group.

Theorem 3.4. *Let B be a Galois algebra (not necessarily central) over R . If for an idempotent $e \neq 0, 1$ in R , Be and $B(1 - e)$ are Galois algebras over Re and $R(1 - e)$, respectively, with unique Galois groups, then B has a unique Galois group.*

Proof. Assume that B has two Galois groups G and H over R . Then by Lemma 3.7 in [7], Be is a Galois algebra over Re and with Galois groups $G|_{Be} \cong G$ and $H|_{Be} \cong H$, respectively. By hypothesis, Be is a Galois algebra over Re with a unique Galois group. Hence $G|_{Be} = H|_{Be}$. Similarly, $G|_{B(1-e)} = H|_{B(1-e)}$, so $G = H$.

4. Semiconnected Galois Extensions

Let B be a semiconnected Galois extension with finitely many central idempotents and Galois group G , $I = \{e_i \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ the set of minimal central idempotents of B , and $G(e_i) = \{g \in G \mid g(e_i) = e_i\}$ for each e_i . We note that $G(e_i)$ can be identified as $G(e_i)|_{Be_i}$ for each e_i (see Lemma 4.1 below). In this section, the set of Galois groups H for B is computed such that $H(e_1) = G(e_1)$ and $G(e_i) \cong H(e_i) = H$ for each minimal central idempotent e_i , and thus the Galois extensions B with a unique Galois group H are classified.

Let $I = \cup_{i=1}^k O_i$ for some integer k be the union of orbits O_i of I under the G -action on $\{e_i \mid i = 1, 2, \dots, m\}$ and $E_i = \sum_{e_j \in O_i} e_j$. Then $B = \oplus \sum_{i=1}^m B e_i = \oplus \sum_{i=1}^k B E_i$. Thus we can reduce the study of B to a semiconnected Galois extension $B E_i$ with a transitive Galois group $G(E_i)|_{B E_i} \cong G$ (see Lemma 4.1 below or [7], Lemma 3.7) where $G(E_i) = \{g \in G \mid g(E_i) = E_i\}$. A Galois group G is called transitive if $I (= O_1)$ has one orbit.

Lemma 4.1. *If e is a nonzero central idempotent of B , then $G(e) \cong G(e)|_{B e}$.*

Proof. (see [7], Lemma 3.7).

By Lemma 4.1, $B E_i$ is a semiconnected Galois extension with Galois group $G(E_i)|_{B E_i} \cong G$. Thus we can reduce the study of B to a semiconnected Galois extension $B E_i$ with a transitive Galois group $G(E_i)|_{B E_i} \cong G$.

Theorem 4.2. *Let $I = \cup_{i=1}^k O_i$ for some integer k be the union of orbits of I under the G -action and $E_i = \sum_{e_j \in O_i} e_j$. Then $B = \oplus \sum_{i=1}^k B E_i$ such that $B E_i$ is a Galois extension with a transitive Galois group $G(E_i)|_{B E_i}$ for each i , and $G(E_i)|_{B E_i} \cong G(E_i) = G$.*

Proof. Since $g(E_i) = E_i$ for each $g \in G$, Theorem 4.2 is an immediate consequence of Lemma 4.1.

Theorem 4.3. *Let B be a semiconnected Galois extension with a transitive Galois group G . Then B is a groupoid; that is, $B = \oplus \sum_{i=1}^m B e_i$ such that*

- (i) $B e_i \cong B e_j$ for all i and j ,
- (ii) $G(e_j) = g G(e_i) g^{-1}$ for some $g \in G$ such that $g(e_i) = e_j$,
- (iii) $B e_i$ is a Galois extension with Galois group $G(e_i)$ if $G(e_i) \neq \{1\}$.

Proof. This is a consequence of the Theorem in [6], Theorem 13 and Theorem 15 in [4].

We remark that $G(e_j) = g G(e_i) g^{-1}$ is independent of the choice of $g \in G$ such that $g(e_i) = e_j$. Theorem 4.3 yields Galois group $G(e_i)$ for $B e_i$ from Galois group G for B .

Next we discuss how to construct more Galois groups H for B from $G(e_i)$. We begin with an expression of a Galois group H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$ which will play an important role to construct Galois groups for B .

Theorem 4.4. *Let B be a semiconnected Galois extension with a transitive Galois group G and $f_j \in G$ such that $f_j(e_1) = e_j$ for $j = 1, 2, \dots, m$. Assume $G(e_1) \neq \{1\}$. If H is a Galois group for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$, then there exists an element $(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$, the Cartesian product of $m - 1$ copies of $\text{Aut}(G(e_1))$ such that $H = \{h \in H \mid h = h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta_j(h_1) f_j^{-1}) \text{ where } h_1 \in G(e_1)\}$.*

Proof. Since $H = H(e_j)$ for each $j = 1, 2, \dots, m$, for each $h \in H$, $h(e_j) = e_j$ for each j . Hence $h = \oplus \sum_{j=1}^m h|_{Be_j}$. Also $H \cong H|_{Be_j} \cong G(e_j)|_{Be_j} \cong G(e_j)$, so $\{h|_{Be_j} \mid h \in H\} \cong G(e_j)|_{Be_j} \cong G(e_j)$. By Theorem 4.3(ii), $G(e_j) = f_j G(e_1) f_j^{-1}$ for an $f_j \in G$ such that $f_j(e_1) = e_j$, so $h|_{Be_j} = f_j h_j f_j^{-1}$ for some $h_j \in G(e_1)$. Hence for any $h \in H$, $h = \oplus \sum_{j=1}^m f_j h_j f_j^{-1}$ for some $h_j \in G(e_1)$. As given by Theorem 4.3(ii) again, f_1 can be taken as the identity of G . But then $H = \{h \in H \mid h = h_1 \oplus (\oplus \sum_{j=2}^m f_j h_j f_j^{-1}) \text{ where } h_1 = h|_{Be_1}\}$. Thus from the isomorphism $G(e_1) \cong H \cong H|_{Be_j} \cong G(e_j) = f_j G(e_1) f_j^{-1} \cong G(e_1)$ by $h_1 \longrightarrow h \longrightarrow h|_{Be_j} \longrightarrow f_j h_j f_j^{-1} \longrightarrow h_j$, we obtain an automorphism β_j of $G(e_1)$, that is, $\beta_j : G(e_1) \longrightarrow G(e_1)$ by $\beta_j(h_1) = h_j$ for each $h_1 (= h|_{Be_1}) \in G(e_1)$ for $j = 2, \dots, m$. Therefore, we obtain an expression of each element in H such that $H = \{h \in H \mid h = h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta_j(h_1) f_j^{-1}) \text{ where } h_1 = h|_{Be_1} \in G(e_1)\}$.

Theorem 4.4 implies that any Galois group H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$ induces an element $(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$, the Cartesian product of $m - 1$ copies of $\text{Aut}(G(e_1))$. Next we show that any $(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$ induces a Galois group H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$.

Theorem 4.5. *Let B be a semiconnected Galois extension with a transitive Galois group G and $f_j \in G$ such that $f_j(e_1) = e_j$ for $j = 2, \dots, m$. Assume $G(e_1) \neq \{1\}$. If*

$(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$, then $H = \{x \oplus (\oplus_{j=2}^m f_j \beta_j(x) f_j^{-1}) \mid x \in G(e_1)\}$ is a Galois group for B such that $H(e_1) = G(e_1)$, $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$, and $B^H = \oplus_{j=1}^m B^G e_j$.

Proof. Firstly, it is easy to check that H is an automorphism group of B under the componentwise multiplication. In fact, for any $\alpha, \beta \in H$, $\alpha = x \oplus (\oplus_{j=2}^m f_j \beta_j(x) f_j^{-1})$ and $\beta = y \oplus (\oplus_{j=2}^m f_j \beta_j(y) f_j^{-1})$ for some $x, y \in G(e_1)$, so $\alpha \cdot \beta = (xy) \oplus (\oplus_{j=2}^m f_j \beta_j(xy) f_j^{-1}) \in H$. Moreover, let $\alpha = 1$ in H , then $x \oplus (\oplus_{j=2}^m f_j \beta_j(x) f_j^{-1}) = 1$. Hence $x = 1$. On the other hand, if $\alpha = x \oplus (\oplus_{j=2}^m f_j \beta_j(x) f_j^{-1})$ such that $f_j \beta_j(x) f_j^{-1} = 1$ in $G(e_j)$ for some j , then $\beta_j(x) = 1$ in $G(e_1)$; and so $x = 1$. Thus $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$. Next we claim that B is a Galois extension with Galois group H . Let $\{a_t, b_t \in B \mid t = 1, 2, \dots, k \text{ for some integer } k\}$ be a Galois system for B with Galois group G . Then for each $\alpha \in H$, $\alpha = x \oplus (\oplus_{j=2}^m f_j \beta_j(x) f_j^{-1})$ for some $x \in G(e_1)$, and so

$$\begin{aligned} \sum_{t=1}^k a_t \alpha(b_t) &= \sum_{j=1}^m \sum_{t=1}^k a_t \alpha(b_t e_j) = \sum_{j=1}^m \sum_{t=1}^k a_t (f_j \beta_j(x) f_j^{-1})(b_t e_j) \\ &= \sum_{j=1}^m \left(\sum_{t=1}^k a_t (f_j \beta_j(x) f_j^{-1})(b_t) \right) (f_j \beta_j(x) f_j^{-1})(e_j) \\ &= \sum_{j=1}^m \left(\sum_{t=1}^k a_t (f_j \beta_j(x) f_j^{-1})(b_t) \right) e_j \quad (\text{for } f_j \beta_j(x) f_j^{-1} \in G(e_j)) \\ &= \sum_{j=1}^m \delta_{1, f_j \beta_j(x) f_j^{-1}} e_j = \sum_{j=1}^m \delta_{1, x} e_j = \delta_{1, x} = \delta_{1, \alpha}. \end{aligned}$$

because $\alpha = 1$ in H if and only if $x = 1$ in $G(e_1)$. Hence H is a Galois group for B . Furthermore, noting that $H|_{Be_j} = f_j G(e_1) f_j^{-1} = G(e_j)$, we have that $B^H = \oplus_{j=1}^m (Be_j)^H = \oplus_{j=1}^m (Be_j)^{G(e_j)} = \oplus_{j=1}^m B^G e_j$ ([4], Lemma 9).

By Theorems 4.4 and 4.5, we have a relation between the set of Galois groups H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$ and the set $(\text{Aut}(G(e_1)))^{m-1}$ by $\lambda : H \rightarrow (\beta_2, \dots, \beta_m)$ where $(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$ as given in Theorem 4.4 such that $H = \{h \in H \mid h = h_1 \oplus (\oplus_{j=2}^m f_j \beta_j(h_1) f_j^{-1}) \text{ where } h_1 \in G(e_1)\}$. Now we want to show that λ is a bijection.

Theorem 4.6. *Let B be a semiconnected Galois extension with a transitive Galois group G . Assume $G(e_1) \neq \{1\}$. Then there exists a one-to-one correspondence between the set $(\text{Aut}(G(e_1)))^{m-1}$ and the set of Galois groups H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$.*

Proof. By Theorem 4.4, any Galois group H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$ induces an element

$$(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$$

such that $H = \{h \in H \mid h = h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta_j(h_1) f_j^{-1}) \text{ where } h_1 \in G(e_1)\}$. We define a map $\lambda : H \rightarrow (\beta_2, \dots, \beta_m)$ from the set of Galois groups H for B such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$ to the set $(\text{Aut}(G(e_1)))^{m-1}$. We claim that λ is well defined. In fact, let $(\beta_2, \dots, \beta_m) \in (\text{Aut}(G(e_1)))^{m-1}$ and $(\beta'_2, \dots, \beta'_m) \in (\text{Aut}(G(e_1)))^{m-1}$ such that

$$H = H_\beta = \{h \in H \mid h = h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta_j(h_1) f_j^{-1}) \text{ where } h_1 \in G(e_1)\}$$

and

$$H = H_{\beta'} = \{h \in H \mid h = h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta'_j(h_1) f_j^{-1}) \text{ where } h_1 \in G(e_1)\}.$$

Then $\beta'_j(h_1) = \beta_j(h_1)$ for $h_1 \in G(e_1)$. But $H(e_1) = G(e_1)$, so $\beta'_j = \beta_j$ for each $j = 2, \dots, m$. This implies that λ is well defined and one-to-one. Moreover, by Theorem 4.5, λ is onto. Thus λ is a bijection.

Theorem 4.6 leads to a classification of the semiconnected Galois extensions B with a unique Galois group H .

Theorem 4.7. *By keeping the notations as given in Theorem 4.6, the Galois extension B with a unique Galois group H if and only if B is one of the following classes: (1) $m = 1$ and $G (= H)$ is unique, and (2) $m \geq 2$ and $|\text{Aut}(G(e_1))| = 2$.*

Proof. Since $H = \{h = h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta_j(h_1) f_j^{-1}) \mid h_1 \in G(e_1)\}$ where $\beta_j \in \text{Aut}(G(e_1))$ by Theorem 4.6. The Galois group H is unique if and only if either (1) $m = 1$ (that is, $B = Be_1$) and H is unique, or (2) $m \geq 2$, there are two cases: case (i), $\text{Aut}(G(e_1)) = \{1, \beta\}$; we have that $H = \{h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta(h_1) f_j^{-1}) \mid h_1 \in G(e_1)\}$, and case (ii), $\text{Aut}(G(e_1)) = \{1, \beta, \beta', \dots\}$; we have that $H_\beta = \{h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta(h_1) f_j^{-1}) \mid h_1 \in G(e_1)\} \neq H_{\beta'} = \{h_1 \oplus (\oplus \sum_{j=2}^m f_j \beta'(h_1) f_j^{-1}) \mid h_1 \in G(e_1)\}$. Thus for $m \geq 2$, the uniqueness of H is equivalent to case (i), that is $|\text{Aut}(G(e_1))| = 2$.

Applying Theorem 4.5, we can generalize the following theorem for Galois algebras with no central idempotents but 0 and 1 as given by F. R. DeMeyer ([2], Theorem 1): Let $K = \{g \in G \mid g(c) = c \text{ for each } c \in C\}$. Then B is a central Galois algebra with Galois group K and C is a Galois algebra with Galois group H/K .

Corollary 4.8. *Let B be a semiconnected Galois algebra over R with a transitive Galois group G . Assume $G(e_1) \neq \{1\}$. Then there exists a Galois group H such that B is a central Galois algebra with Galois group K and C is a Galois algebra with Galois group H/K where $K = \{g \in H \mid g(c) = c \text{ for each } c \in C\}$.*

Proof. Since $G(e_1) \neq \{1\}$, there exists a Galois group H such that $H(e_1) = G(e_1)$ and $G(e_j) \cong H(e_j) = H$ for each $j = 1, 2, \dots, m$ and $B^H = \oplus \sum_{i=1}^m B^{H(e_i)} e_i$ by Theorem 4.5. Noting that Be_i is a Galois extension of $(Be_i)^{G(e_i)} = B^G e_i = Re_i$ ([4], Lemma 9 or Lemma 9'), we have that Be_i is a Galois algebra over Re_i with a Galois group $G(e_i)$ ($\cong H(e_i) = H$). Since Be_i contains no central idempotents but 0 and e_i , it is a central Galois algebra with Galois group K_i where $K_i = \{g \in G(e_i) \mid g(ce_i) = ce_i \text{ for each } c \in C\}$ and Ce_i is a Galois algebra over Re_i with Galois group $G(e_i)|_{K_i}$ ([2], Theorem 1). But $K = K(e_i) \cong K|_{Be_i} = K_i$, so B is a central Galois algebra with Galois group K and C is a Galois algebra with Galois group H/K .

We conclude the present paper with several examples to demonstrate the results.

EXAMPLE 1.

Let Q be the field of rational numbers, $B = Q[i] \oplus Q[i]$ where $i^2 = -1$, and $G = \{(1, 1), (\alpha, \alpha)\}$ where $\alpha(a + bi) = a - bi$ for all $a + bi \in Q[i]$. Then B is a Galois algebra over $Q \oplus Q$ with a G -Galois system $\{a_1 = (1, 1), a_2 = (i, i); b_1 = (\frac{1}{2}, \frac{1}{2}), a_2 = (-\frac{1}{2}i, -\frac{1}{2}i)\}$. Also $B(1, 0) \cong Q[i]$ and $B(0, 1) \cong Q[i]$, so they are Galois algebra over $Q \oplus \{0\}$ and $\{0\} \oplus Q$ with a unique Galois group. Thus G is unique by Theorem 3.4. But $(\alpha, 1) \in \text{Aut}_{Q \oplus Q}(B)$, so $G \neq \text{Aut}_{Q \oplus Q}(B)$.

EXAMPLE 2.

Let $B = R \oplus R \oplus R \oplus R$, a direct sum of four fields of real numbers R , $G = \{1, g, g^2, g^3\}$ such that $g(r_1, r_2, r_3, r_4) = (r_2, r_3, r_4, r_1)$ for all $(r_1, r_2, r_3, r_4) \in B$, and $G' = \{1, h, h^2, h^3\}$ such that $h(r_1, r_2, r_3, r_4) = (r_2, r_4, r_1, r_3)$ for all $(r_1, r_2, r_3, r_4) \in B$. Then, B is a Galois extension with Galois groups G and G' respectively with the same Galois system $\{a_1 = b_1 = (1, 0, 0, 0), a_2 = b_2 = (0, 1, 0, 0), a_3 = b_3 = (0, 0, 1, 0), a_4 = b_4 = (0, 0, 0, 1)\}$. We can check that $B^G = B^{G'} = \{(r, r, r, r) | r \in R\} \cong R$, and $G \cong G'$ but $G \neq G'$.

EXAMPLE 3.

Let $B = R \oplus R \oplus R \oplus R$, a direct sum of four fields of real numbers R , $G = \{1, g, g^2, g^3\}$ such that $g(r_1, r_2, r_3, r_4) = (r_2, r_3, r_4, r_1)$ for all $(r_1, r_2, r_3, r_4) \in B$, and $G' = \{1, g_1, g_2, g_1g_2\}$ such that $g_1(r_1, r_2, r_3, r_4) = (r_2, r_1, r_4, r_3)$ and $g_2(r_1, r_2, r_3, r_4) = (r_3, r_4, r_1, r_2)$ for all $(r_1, r_2, r_3, r_4) \in B$. Then, B is a Galois extension with Galois groups G and G' respectively with the same Galois system $\{a_1 = b_1 = (1, 0, 0, 0), a_2 = b_2 = (0, 1, 0, 0), a_3 = b_3 = (0, 0, 1, 0), a_4 = b_4 = (0, 0, 0, 1)\}$. It can be checked that $B^G = B^{G'} = \{(r, r, r, r) | r \in R\} \cong R$. But G is a cyclic group of order 4 and G' is Klein 4-group, so $G \not\cong G'$.

References

- [1] Chase, S.U., Harrison, D.K. and Rosenberg, A., *Galois Theory and Galois Cohomology of Commutative Rings*, Memoirs Amer. Math. Soc. No. 52, 1965.

- [2] DeMeyer, F.R., Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.* **10** (1966), 287-295.
- [3] Kanzaki, T., On Galois Algebra Over A Commutative Ring, *Osaka J. Math.* **2** (1965), 309-317.
- [4] Kishimoto, K. and Nagahara, T., *On G-extensions of a semi-connected ring*, Math. J. Okayama Univ. **32** (1990), 25–42.
- [5] Rosenberg, A. and Zelinsky, D., Automorphisms of Separable Algebras, *Pacific J. Math.*, **11**(1961), 1109-1117.
- [6] Villamayor, O. and Zelinsky, D., *Galois theory for rings with finitely many idempotents*, Nagoya Math. J. **27**(1966), 721-731.
- [7] Szeto, G. and Xue, L., The structure of Galois algebras, *Journal of Algebra*, **237**(1) (2001), 238-246.