

On Galois Extensions with Automorphism Group as Galois Group

George Szeto and Lianyong Xue

Department of Mathematics

Bradley University

Peoria, Illinois 61625

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

ABSTRACT

Let B be a ring Galois extension of B^G with Galois group G such that B^G is a projective separable C^G -algebra where C is the center of B . Then it is shown that $G = \text{Aut}_{B^G}(B)$ and $K = \langle 1 \rangle$ where $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$ if and only if either B is an indecomposable DeMeyer-Kanzaki Galois extension of B^G or $B = B^G e \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B . This is a generalization of the case for Galois algebras. Moreover, the class of indecomposable Galois extensions are also studied.

Key Words and phrases. Separable extensions, Galois extensions, Galois algebras, Hirata Galois extensions, DeMeyer-Kanzaki Galois extensions.

2000 Mathematics Subject Classification. Primary 16S35, 16W20.

1. Introduction

Let B be a field Galois extension of B^G with Galois group G . It is well known that $G = \text{Aut}_{B^G}(B)$, the B^G -automorphism of B . In [1], this fact was extended to an indecomposable commutative Galois extension (with no idempotents but 0 and 1). Recently, the converse problem for a Galois algebra was studied ([10], Theorem 4.6). Let B be a Galois algebra over a commutative ring R with Galois group G . Then $G = \text{Aut}_R(B)$

if and only if either B is indecomposable commutative or $B = Re \oplus R(1 - e)$ where B is commutative, e and $1 - e$ are minimal idempotents of B . The purpose of the present paper is to generalize this result to a Galois extension (not necessarily a Galois algebra). Let B be a Galois extension of B^G with Galois group G such that B^G is projective separable over C^G where C is the center of B , and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. In section 3, we shall show that $G = \text{Aut}_{B^G}(B)$ and $K = \langle 1 \rangle$ if and only if either B is an indecomposable DeMeyer-Kanzaki Galois extension of B^G or $B = B^G e \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B , where B is called a DeMeyer-Kanzaki Galois extension if B is an Azumaya algebra over C and C is a Galois algebra over C^G with Galois group induced by and isomorphic with G ([2], [6]). We note that $K = \langle 1 \rangle$ and B^G is projective separable over C^G for the Galois algebra case. We also generalize the structure theorem for an indecomposable Galois algebra as given by F. R. DeMeyer ([3], Theorem 1). Let B be an indecomposable Galois extension of B^G with Galois group G such that B^G is separable over C^G . Then B is a Hirata Galois extension of $B^G C$ with Galois group K (that is, B is a Galois and a Hirata separable extension), and $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K . Then, in section 4, some properties of an indecomposable Galois extension are given. In section 5, the Galois correspondence is shown for the Hirata Galois extension B of $B^G C$ as given in section 3.

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

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. 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 $\sum b a_i \otimes b_i = \sum a_i \otimes b_i b$ for all b in B where \otimes is over A . An Azumaya algebra is a separable extension of its center. 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 $g \in G$ ([2]). 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 ([9]). A Galois extension B of B^G with Galois group G is called a DeMeyer-Kanzaki Galois extension if B is an Azumaya algebra over C which is a Galois algebra over C^G with Galois group induced by and isomorphic with G ([2], [6]). A ring B is called a Hirata 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, and B is called a Hirata Galois extension if it is a Galois and a Hirata separable extension of B^G ([8]). A ring B is called indecomposable if it contains no central idempotents but 0 and 1.

Throughout this paper, we assume that B is a Galois extension of B^G with Galois group G , C the center of B , $V_B(B^G)$ the commutator subring of B^G in B , $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$, and $G(A) = \{g \in G \mid g(a) = a \text{ for all } a \in A\}$ for a subring A of B .

3. The Generalization

In this section, let B be a Galois extension of B^G with Galois group G such that B^G is separable over C^G . We shall show that $G = \text{Aut}_{B^G}(B)$ and $K = \langle 1 \rangle$ if and only if either B is an indecomposable DeMeyer-Kanzaki Galois extension of B^G or $B = B^G e \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B . This generalizes the case for Galois algebras ([10], Theorem 4.6). We begin with a lemma to determine which automorphism in $\text{Aut}_{B^G}(B)$ is not in G .

Lemma 3.1. *Let B be a Galois extension of B^G with Galois group G and $\lambda \in \text{Aut}_{B^G}(B)$. If $e \neq 0$ is a central idempotent in B such that $\lambda|_{B^G e}$ is identity and $\lambda|_{B^G(1-e)}$ is not identity, then $\lambda \notin G$.*

Proof. See the proof of Lemma 4.1 in [10].

In [3], it was shown that an indecomposable Galois algebra B with Galois group G is a composition of two Galois extensions: (1) B is a central Galois algebra with Galois group K , and (2) C is a commutative Galois algebra over C^G with Galois group G/K ([3], Theorem 1). We want to generalize the above result to an indecomposable Galois extension.

Theorem 3.2. *Let B be an indecomposable Galois extension of B^G with Galois group G such that B^G is separable over C^G . Then (1) B is a Hirata Galois extension of $B^G C$ with Galois group K , and (2) $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K .*

Proof. (1) By hypothesis, B is a Galois extension of B^G such that B^G is separable over C^G . Hence B is a separable C^G -algebra. Thus B is an Azumaya C -algebra and C is a separable C^G -algebra ([4], Theorem 3.8, page 55). But C contains no idempotents but 0 and 1, so C is a Galois algebra over C^G with Galois group G/K ([4], Proposition 1.2(1), page 80). Hence, noting that $C \subset B^G C \subset B^K$, we have that $B^G C$ and B^K are Galois extensions of B^G with Galois group G/K with the same Galois system as C . Therefore $B^G C = B^K$. Moreover, since B is a Galois extension of B^G with Galois group G , B is a Galois extension of B^K with Galois group K . But $B^G C = B^K$, so B is a Galois extension of $B^G C$ with Galois group K . Furthermore, we want to show that B is a Hirata separable extension of $B^G C$. In fact, since B is a Galois extension of $B^G C$, B is a finitely generated and projective right $B^G C$ -module. But B is an Azumaya C -algebra, so B is a Hirata separable extension of $B^G C$ ([5], Theorem 1). Thus B is a Hirata Galois extension of $B^G C$ with Galois group K .

(2) Let Z be the center of $B^G C$. Noting that C is a Galois algebra over C^G with Galois group G/K and that $C \subset Z \subset B^G C$, we conclude that Z is Galois extension of

$Z^{G/K}$ ($= Z^G$) with Galois group G/K with the same Galois system as C , that is, $B^G C$ is a Galois extension of B^G with Galois group G/K such that Z is a Galois algebra over Z^G with Galois group induced by and isomorphic with G/K . Moreover, since B^G is separable over C^G , we can see that $B^G C$ is separable over C^G . Hence $B^G C$ is an Azumaya Z -algebra. Thus $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K .

Next Lemma shows that there are at most two central minimal idempotent in B when $|G|$, the order of G , is 2.

Lemma 3.3. *Let B be a Galois extension of B^G with Galois group G and a projective separable C^G -algebra. If $G = \text{Aut}_{B^G}(B)$ and $|G| = 2$, then B contains at most two minimal central idempotents.*

Proof. We first claim that C^G contains no idempotents but 0 and 1. In fact, let $e \in C^G$ such that $e^2 = e \neq 0, 1$ and $G = \{1, g\}$. Then $B = Be \oplus B(1 - e)$ such that $g(e) = e$. Hence $g(Be) = Be$ and $g(B(1 - e)) = B(1 - e)$. Since $g \neq 1$ in G , $g|_{Be} \neq 1$ or $g|_{B(1-e)} \neq 1$. Without loss of generality, assume $g|_{Be} \neq 1$. Then $\lambda = g|_{Be} \oplus 1 \in \text{Aut}_{B^G}(B)$ but $\lambda \notin G$ by Lemma 3.1. Thus $|\text{Aut}_{B^G}(B)| > |G|$. This is a contradiction; and so C^G contains no idempotents but 0 and 1. Next we show that B contains at most two minimal central idempotents. By hypothesis, B is a projective separable C^G -algebra, so it is a finitely generated C^G -module ([4], Proposition 2.1, page 47) and an Azumaya algebra over C ([4], Theorem 3.8, page 55). Hence C is a direct summand of B ([4], Lemma 3.1, page 51); and so C contains only finitely many minimal idempotents $\{e_i \mid i = 1, 2, \dots, q\}$ for some integer q . We want to show that $q \leq 2$. Since g is an automorphism of B , g permutes the minimal central idempotents $\{e_i \mid i = 1, 2, \dots, q\}$. Hence $g(e_1) = e_j$ for some j . We have two cases. Case 1: $g(e_1) = e_1$. Then, noting that $G = \{1, g\}$, we have that e_1 is an idempotent in C^G . But C^G contains no idempotents but 0 and 1, so $e_1 = 1$. Thus $q = 1$. Case 2: $g(e_1) = e_j$ for some $j \neq 1$. Then, noting that g is of order 2, we have that

$g(Be_1 \oplus Be_j) = Be_1 \oplus Be_j$ and $g|_{Be_1 \oplus Be_j} \neq 1$. If $q \geq 3$, then we have a $\lambda \in \text{Aut}_{B^G}(B)$ such that $\lambda|_{Be_1 \oplus Be_j} = g|_{Be_1 \oplus Be_j} \neq 1$ and $\lambda|_{\bigoplus_{i \neq 1, j} Be_i} = 1$. But $\lambda \notin G$ by Lemma 3.1, so this contradicts to the hypothesis that $G = \text{Aut}_{B^G}(B)$. Hence $q \leq 2$. Thus B contains at most two minimal central idempotents.

We recall that a Galois extension B of B^G with Galois group G is called a DeMeyer-Kanzaki Galois extension if B is an Azumaya algebra over C and C is a Galois algebra over C^G with Galois group $G|_C \cong G$ ([2],[6]). Now we show the main theorem.

Theorem 3.4. *Let B be a Galois extension of B^G with Galois group G such that B^G is a projective separable C^G -algebra. Then, $G = \text{Aut}_{B^G}(B)$ and $K = \langle 1 \rangle$ if and only if either B is an indecomposable DeMeyer-Kanzaki Galois extension of B^G , or $B = B^G e \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B .*

Proof. (\implies) There are 2 cases:

Case 1: $|G| > 2$. Since $G = \text{Aut}_{B^G}(B)$ and $|G| > 2$, B is indecomposable ([10], Lemma 4.3). Hence $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K by Theorem 3.2. By hypothesis, $K = \langle 1 \rangle$, so $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group $G|_{B^G C} \cong G$. But B is also a Galois extension of B^G with Galois group G , so $B = B^G C$, an indecomposable DeMeyer-Kanzaki Galois extension of B^G .

Case 2: $|G| = 2$. By Lemma 3.3, B contains either no central idempotents but 0 and 1, or exactly 2 minimal central idempotents. If B contains no central idempotents but 0 and 1, then B is given by Case 1 again. If B contains exactly 2 minimal central idempotents $\{e, 1 - e\}$, then $B = Be \oplus B(1 - e)$. Let $G = \{1, g\}$. Then g permutes $\{e, 1 - e\}$. We claim that $g(e) = 1 - e$. In fact, assume that $g(e) = e$. Then $g(Be) = Be$ and $g(B(1 - e)) = B(1 - e)$. Since $g \neq 1$ in G , either $g|_{Be} \neq 1$ or $g|_{B(1 - e)} \neq 1$. Without

loss of generality, assume $g|_{Be} \neq 1$. Then $\lambda = g|_{Be} \oplus 1 \in \text{Aut}_{B^G}(B)$ but $\lambda \notin G$ by Lemma 3.1. Thus $|\text{Aut}_{B^G}(B)| > |G|$. This contradicts to the hypothesis that $G = \text{Aut}_{B^G}(B)$. Hence $g(e) = 1 - e$. Now we show that $B^G = \{be + g(b)(1 - e) \mid b \in B\}$. Since

$$g(be + g(b)(1 - e)) = g(b)(1 - e) + g^2(b)e = be + g(b)(1 - e),$$

$\{be + g(b)(1 - e) \mid b \in B\} \subset B^G$. Conversely, let $b \in B^G$. Since $B = Be \oplus B(1 - e)$, $b = b_1e + b_2(1 - e)$ for some $b_1, b_2 \in B$. Hence

$$b_1e + b_2(1 - e) = b = g(b) = g(b_1e + b_2(1 - e)) = g(b_1)(1 - e) + g(b_2)e.$$

Since $B = Be \oplus B(1 - e)$, we have that $b_2(1 - e) = g(b_1)(1 - e)$. Hence $b = b_1e + b_2(1 - e) = b_1e + g(b_1)(1 - e) \in \{be + g(b)(1 - e) \mid b \in B\}$. Thus $B^G = \{be + g(b)(1 - e) \mid b \in B\}$. Now for any $x \in B$, $x = ae + b(1 - e)$ for some $a, b \in B$, so

$$x = ae + b(1 - e) = (ae + g(a)(1 - e))e + (g(b)e + b(1 - e))(1 - e) \in B^Ge \oplus B^G(1 - e).$$

Thus $B = B^Ge \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B .

(\Leftarrow) In case B is an indecomposable DeMeyer-Kanzaki Galois extension of B^G . Then $B = B^GC$ ([2], Lemma 2) and C is a commutative Galois algebra over C^G with no idempotents but 0 and 1 and with Galois group G/K $G|_C \cong G$. Thus $G \cong G|_C = \text{Aut}_{C^G}(C)$ ([1], Theorem 3.5). Noting that $B = B^GC$, we have that $\text{Aut}_{B^G}(B) \cong \text{Aut}_{C^G}(C) \cong G$. Therefore $G = \text{Aut}_{B^G}(B)$. Moreover, since $G|_C \cong G$, $K = \langle 1 \rangle$.

In case $B = B^Ge \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B . Then B contains exactly 2 minimal central idempotents e and $1 - e$. Thus for any $\alpha \in \text{Aut}_{B^G}(B)$, α permutes $\{e, 1 - e\}$. If $\alpha(e) = e$, then $\alpha = 1 \in G$. Hence for any $\alpha \neq 1$ in $\text{Aut}_{B^G}(B)$, $\alpha(e) = 1 - e$. We have that $\alpha(ae + b(1 - e)) = a(1 - e) + be$ for any $x = ae + b(1 - e) \in B$ where $a, b \in B^G$. Therefore $|\text{Aut}_{B^G}(B)| = 2$; and so $G = \text{Aut}_{B^G}(B)$ and $K = \langle 1 \rangle$.

4. Indecomposable Galois Extensions

Throughout this section, we assume that B is an indecomposable Galois extension of B^G with Galois group G such that B^G is a separable C^G -algebra. Then Theorem 3.2 shows that B is a Hirata Galois extension of $B^G C$ with Galois group K and $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K . In this section, we shall show a one-to-one correspondence between the following sets in B : (i) $\mathcal{P} = \{B^H \mid H \text{ is a subgroup of } K\}$ and (ii) $\mathcal{Q} = \{A \mid A \text{ is a separable subalgebra of } B \text{ over } C \text{ such that } A = \sum_{g \in H} J_g \text{ for some subgroup } H \text{ of } K\}$. Moreover, in case $K \neq \langle 1 \rangle$, some properties of the Hirata Galois extension B of $B^G C$ are also obtained. We need a property of $|K|$, the order of K .

Lemma 4.1. *The order of K is a unit in B .*

Proof. By Theorem 3.2, $B^G C$ is a Galois extension of B^G , and B^G is a separable C^G -algebra by hypothesis, so $B^G C$ is a separable C^G -algebra by the transitivity property of separable extensions. Hence $B^G C$ is a separable subalgebra of the Azumaya C -algebra B . Thus $V_B(B^G C)$ is a separable C -algebra ([4], Theorem 4.3, page 57). By Theorem 3.2 again, B is a Hirata Galois extension of $B^G C$ with Galois group K , so $|K|$ is a unit in B ([8], Proposition 4(3)).

Lemma 4.2. *Let H be a subgroup of K . Then (1) B is a Hirata Galois extension of B^H such that B^H is a direct summand of B as a B^H -bimodule, and (2) B^H is a separable algebra over C^G .*

Proof. (1) Since H is a subgroup of K , $C \subset B^H \subset B$. Noting that B is a Galois extension of B^H with Galois group H , we have that B is a finitely generated and projective right B^H -module. But B is an Azumaya C -algebra, so B is a Hirata separable extension of B^H ([5], Theorem 1). Thus B is a Hirata Galois extension of B^H with Galois group H .

Since H is a subgroup of K again, $|H|$ is a unit in B by Lemma 4.1. This implies that B^H is a direct summand of B as a B^H -bimodule.

(2) Since B is a Galois extension of B^H , B is a projective separable extension of B^H . On the other hand, by hypothesis, B is a Galois extension of B^G which is a separable C^G -algebra, so B is a separable C^G -algebra. Now B^H is a direct summand of B as a B^H -bimodule by part (1), so B^H is a separable algebra over C^G by the proof of Theorem 3.8 on page 55 in [4].

Next is the correspondence between \mathcal{P} and \mathcal{Q} .

Theorem 4.3. *Let $\mathcal{P} = \{B^H \mid H \text{ is a subgroup of } K\}$ and $\mathcal{Q} = \{A \mid A \text{ is a separable subalgebra of } B \text{ over } C \text{ such that } A = \oplus \sum_{g \in H} J_g \text{ for some subgroup } H \text{ of } K\}$. Then $\alpha : B^H \longrightarrow \oplus \sum_{g \in H} J_g$ is a one-to-one correspondence between \mathcal{P} and \mathcal{Q} .*

Proof. By Theorem 3.2, B is a Hirata separable extension of $B^G C$. Let H be a subgroup of K . Then B^H is a separable algebra over C^G by Lemma 4.2-(2). Hence B^H is a separable extension of $B^G C$. Moreover, B^H is a direct summand of B as a B^H -bimodule by Lemma 4.2-(1). This implies that the map $\alpha : B^H \longrightarrow V_B(B^H)$ is a one-to-one correspondence from \mathcal{P} to the set of separable subalgebras of $V_B(B^G)$ over C ([7], Theorem 1). But B is a Galois extension of B^H with Galois group H , so $V_B(B^H) = \oplus \sum_{g \in H} J_g$ ([6], Proposition 1). Thus $\alpha : B^H \longrightarrow \oplus \sum_{g \in H} J_g$ is a one-to-one correspondence between \mathcal{P} and \mathcal{Q} .

Next are some properties of the Hirata Galois extension B of $B^G C$ with Galois group K . We recall that $V_B(B^G)$ is the commutator subring of B^G in B . Let $L = \{g \in G \mid g(a) = a \text{ for all } a \in V_B(B^G)\}$. Then we can see that L is a normal group of G and $L \subset K$.

Lemma 4.4. *By keeping the above notations, B is a Galois extension of B^L with Galois group L and B^L is a Galois extension of B^K with Galois group K/L .*

Proof. Since B^G and C are separable C^G -algebras, $B^G C$ is a separable C^G -algebra; and so $B^G C$ is a separable C -algebra. Hence $V_B(B^G)$ ($= V_B(B^G C)$) is a separable C -algebra since B is an Azumaya C -algebra. Moreover, B is a Hirata Galois extension of $B^G C$ with Galois group K by Theorem 3.2, and $|K|$ is a unit in B by Lemma 4.1, so $|L|$ is a unit in B . Hence B is a Galois extension of B^L with Galois group L and B^L is a Galois extension of B^K ($= B^G C$) with Galois group K/L .

Theorem 4.5. *By keeping the above notations, $B^L = B^G \cdot V_B(B^G)$ if and only if $V_B(B^G)$ is a central Galois algebra with Galois group $(K/L)|_{V_B(B^G)} \cong K/L$.*

Proof. By Theorem 3.2, B is a Hirata Galois extension of B^K with Galois group K and $B^K = B^G C$. Noting that $L \subset K$, $B^K \subset B^L \subset B$, we have that $V_B(B^K) = V_B(B^G C) = V_B(B^G)$. Hence $L = \{g \in G \mid g(a) = a \text{ for all } a \in V_B(B^G)\} = \{g \in G \mid g(a) = a \text{ for all } a \in V_B(B^K)\}$. Thus $B^L = B^K \cdot V_B(B^K)$ if and only if $V_B(B^K)$ is a central Galois algebra with Galois group $(K/L)|_{V_B(B^K)} \cong K/L$ ([8], Theorem 6), that is, $B^L = (B^G C) \cdot V_B(B^G C) = B^G \cdot C \cdot V_B(B^G) = B^G \cdot V_B(B^G)$ if and only if $V_B(B^G)$ is a central Galois algebra with Galois group $(K/L)|_{V_B(B^G)} \cong K/L$.

The following are consequences for two special cases: (i) $L = \langle 1 \rangle$ and (ii) $L = K$.

Corollary 4.6. *By keeping the notations of Theorem 4.5, (1) $L = \langle 1 \rangle$; then, $B = B^G \cdot V_B(B^G)$ if and only if $V_B(B^G)$ is a central Galois algebra with Galois group $K|_{V_B(B^G)} \cong K$, and (2) $L = K$; then, $B^K = B^G \cdot V_B(B^G) = B^G C$ which is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K .*

Proof. (1) Since $L = \langle 1 \rangle$, part (1) is an immediate consequence of Theorem 4.5.

(2) Since $L = K$, $V_B(B^G) \subset B^L = B^K$. Noting that $B^K = B^G C$ by Theorem 3.2, we have that $B^G C \subset B^G \cdot V_B(B^G) \subset B^K = B^G C$. Hence $B^K = B^G \cdot V_B(B^G) = B^G C$ which is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K by Theorem 3.2.

5. The Galois Correspondence

In this section, let B be an indecomposable Galois extension of B^G with Galois group G such that B^G is a separable C^G -algebra as given in section 4. Then Theorem 3.2 gives a Galois correspondence between K and B^K ; that is, $G(B^K) = K$. In this section, we shall show that there exists a Galois correspondence between the set of subgroups of K and the set of separable extensions A of $B^G C$ in B such that $V_B(A) = \bigoplus \sum_{g \in G(A)} J_g$, where $G(A) = \{g \in G \mid g(a) = a \text{ for all } a \in A\}$.

Lemma 5.1. *Let \mathcal{C} be the set of subgroups of K and \mathcal{D} the set of separable extensions A of $B^G C$ in B such that $V_B(A) = \bigoplus \sum_{g \in G(A)} J_g$. Then for any $H \in \mathcal{C}$, $B^H \in \mathcal{D}$.*

Proof. By Lemma 4.2-(2), B^H is a separable algebra over C^G , so B^H is a separable extension of $B^G C$. Moreover, by the definition of $G(B^H)$, $H \subset G(B^H)$, so $B^{G(B^H)} \subset B^H$. Also, $B^{G(B^H)} \supset B^H$ by the definition of $G(B^H)$. Hence $B^{G(B^H)} = B^H$. Thus $V_B(B^H) = V_B(B^{G(B^H)})$. Since B is a Galois extension of $B^{G(B^H)}$ with Galois group $G(B^H)$, $V_B(B^{G(B^H)}) = \bigoplus \sum_{g \in G(B^H)} J_g$ ([6], Proposition 1). Hence

$$V_B(B^H) = V_B(B^{G(B^H)}) = \bigoplus \sum_{g \in G(B^H)} J_g.$$

Thus $B^H \in \mathcal{D}$.

Now we show that $\alpha : H \rightarrow B^H$ is a one-to-one correspondence between \mathcal{C} and \mathcal{D} .

Theorem 5.2. *Let $\alpha : \mathcal{C} \rightarrow \mathcal{D}$ by $\alpha(H) = B^H$. Then α is a bijection, and the inverse of α is $\alpha^{-1} : \mathcal{D} \rightarrow \mathcal{C}$.*

Proof. By Lemma 5.1, α is well defined. Now, let $H, L \in \mathcal{C}$ such that $\alpha(H) = \alpha(L)$. Then $B^H = B^L$ such that $V_B(B^H) = \oplus \sum_{g \in H} J_g = V_B(B^L) = \oplus \sum_{g \in L} J_g$ ([6], Proposition 1). Since B is a Hirata Galois extension of $B^G C$ with Galois group K , $J_g \neq \{0\}$ for each $g \in K$ ([8], Theorem 2(iii)). But $H, L \subset K$, so $\oplus \sum_{g \in H} J_g = \oplus \sum_{g \in L} J_g \subset \oplus \sum_{g \in K} J_g$. This implies that $H = L$; and so α is a one-to-one. Next we claim that α is onto. Let $A \in \mathcal{D}$. Then A is a separable extension of $B^G C$ such that $V_B(A) = \oplus \sum_{g \in G(A)} J_g$. By Theorem 3.2, $B^K = B^G C$, so $B^G C (= B^K)$ is a separable C^G -algebra by Lemma 4.2-(2). Thus A is a separable C^G -algebra by the transitivity property of separable extensions. Therefore A is a separable subalgebra of the Azumaya C -algebra B ; and so $A = V_B(V_B(A))$ by the double centralizer property for Azumaya algebras ([4], Theorem 4.3, page 57). Moreover, since B is a Galois extension of $B^{G(A)}$ with Galois group $G(A)$, $V_B(B^{G(A)}) = \oplus \sum_{g \in G(A)} J_g = V_B(A)$. Noting that $G(A)$ is a subgroup of K , we have that $B^{G(A)} = \alpha(G(A)) \in \mathcal{D}$; and so $V_B(V_B(B^{G(A)})) = B^{G(A)}$ by the above argument. Hence $A = V_B(V_B(A)) = V_B(V_B(B^{G(A)})) = B^{G(A)}$; that is, $\alpha(G(A)) = A$. Thus α is onto. Therefore α is a bijection with the inverse $\alpha^{-1} : A \rightarrow G(A)$.

Next, we want to show the Galois correspondence for the DeMeyer-Kanzaki Galois extension $B^G C$ of B^G with Galois group G/K . Let Z be the center of $B^G C$. We first claim that Z contains only finitely many idempotents so that the Galois correspondence theorem for Z as given by Villamayor and Zelinsky can be applied.

Lemma 5.3. *Let B be an indecomposable Galois extension of B^G with Galois group G such that B^G is a separable C^G -algebra and Z the center of $B^G C$. Then Z is a commutative Galois algebra over Z^G with Galois group G/K with only finitely many idempotents.*

Proof. By Theorem 3.2, B is a Galois extension of $B^G C$ with Galois group K , and $|K|$ is a unit in B by Lemma 4.1, so $B^G C$ is a direct summand of B as a $B^G C$ -bimodule. Noting that B is an Azumaya C -algebra and $C \subset B^G C$, we have that $B^G C$ is a finitely

generated C -module. But C contains no idempotents but 0 and 1, so $B^G C$ contains only finitely many central idempotents. On the other hand, by Theorem 3.2, $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K , so Z is a commutative Galois algebra over Z^G with Galois group G/K with only finitely many idempotents.

By the Theorem in [11], Lemma 5.3 gives a one-to-one correspondence between the set of the fat groups of subgroups of G/K and the set of separable subalgebras of Z over Z^G by $\overline{H} \rightarrow Z^{\overline{H}}$, where \overline{H} is the fat group of H . Next we derive the Galois correspondence for the DeMeyer-Kanzaki Galois extension $B^G C$ of B^G with Galois group G/K .

Theorem 5.4. *Let \mathcal{E} be the set of the fat groups of subgroups of G containing K and \mathcal{F} the set of separable extensions of B^G in $B^G C$. Then $\beta : \overline{H} \rightarrow (B^G C)^{\overline{H}}$ is a one-to-one correspondence between \mathcal{E} and \mathcal{F} .*

Proof. Let \mathcal{F}_Z be the set of separable subalgebras of Z over Z^G . Since Z is a commutative Galois algebra over Z^G with Galois group G/K with only finitely many idempotents by Lemma 5.3, $\overline{H} \rightarrow Z^{\overline{H}}$ is a one-to-one correspondence between \mathcal{E} and \mathcal{F}_Z ([11], Theorem). Moreover, since $B^G Z (= B^G C)$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K by Theorem 3.2, $A \rightarrow B^G A$ for each $A \in \mathcal{F}_Z$ is a one-to-one correspondence from \mathcal{F}_Z to \mathcal{F} ([2], Lemma 2). But $A = Z^{\overline{H}}$ for some subgroup H of G containing K by the correspondence theorem for Z , so the composition of $\overline{H} \rightarrow Z^{\overline{H}} \rightarrow B^G Z^{\overline{H}}$ gives a one-to-one correspondence $\overline{H} \rightarrow B^G Z^{\overline{H}} = (B^G C)^{\overline{H}}$ between \mathcal{E} and \mathcal{F} .

References

- [1] S.U. Chase, D.K. Harrison, A. Rosenberg, "Galois Theory and Galois Cohomology of Commutative Rings", *Memoirs Amer. Math. Soc.* No. 52, 1965.
- [2] F.R. DeMeyer, Some Notes on the General Galois Theory of Rings, *Osaka J. Math.* **2** (1965), 117-127.

- [3] F.R. DeMeyer, Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.* **10** (1966), 287-295.
- [4] F.R. DeMeyer and E. Ingraham, "Separable algebras over commutative rings", Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.
- [5] S. Ikehata, Note on Azumaya Algebras and H -Separable Extensions, *Math. J. Okayama Univ.*, **23** (1981), 17-18.
- [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 II, *Osaka J. Math.*, **8** (1971), 465-469.
- [8] K. Sugano, On a Special Type of Galois Extensions, *Hokkaido J. Math.*, **9**(1980) 123-128.
- [9] G. Szeto and L. Xue, The structure of Galois algebras, *Journal of Algebra*, **237**(1) (2001), 238-246.
- [10] G. Szeto and L. Xue, The Galois Algebra with Galois Group which is the Automorphism Group. *Journal of Algebra*, to appear.
- [11] O. E. Villamayor and D. Zelinsky, Galois Theory for Rings with Finitely Many Idempotents, *Nagoya Math. J.* **27** (1966), 721-731.