ON A COMPOSITION OF GALOIS EXTENSIONS

George Szeto\textsuperscript{1}, Lianyong Xue\textsuperscript{2} \textsuperscript{§}

\textsuperscript{1,2}Department of Mathematics
Bradley University
1501 West Bradley Avenue, Peoria, Illinois, 61625, USA
\textsuperscript{1}e-mail: szeto@bradley.edu
\textsuperscript{2}e-mail: lxue@bradley.edu

Abstract: Let $B$ be a Galois extension of $B^G$ with Galois group $G$ such that $B^G$ is a separable $C^G$-algebra, where $C$ is the center of $B$. Then an equivalent condition is given for $B$ as a composition of a Hirata Galois extension $B$ of $B^G C$ with Galois group $K$ and a DeMeyer-Kanzaki Galois extension $B^G C$ of $B^G$ with Galois group $G/K$, where $K = \{ g \in G \mid g(c) = c \text{ for all } c \in C \}$. Properties of separable subextensions are also given.

AMS Subject Classification: 16S35, 16W20

Key Words: separable extensions, Galois extensions, Hirata separable extensions, Hirata Galois extensions, DeMeyer-Kanzaki Galois extensions

1. Introduction

Let $B$ be an indecomposable Galois algebra over a commutative ring $R$ with Galois group $G$, $C$ the center of $B$, and $K = \{ g \in G \mid g(c) = c \text{ for all } c \in C \}$. In [2], it was shown that $B$ is a central Galois algebra over $C$ with Galois group $K$, and $C$ is a commutative Galois extension of $C^G$ with Galois group $G/K$ (see [2], Theorem 1). This fact was generalized to an indecomposable Galois extension $B$ of $B^G$ with Galois group $G$ such that $B^G$ is separable over $C^G$ (see [10], Theorem 3.2). By noting that this fact fails for decomposable Galois extensions, the purpose of the present paper is to give an equivalent condition for a Galois extension $B$ (not necessarily indecomposable) of $B^G$
which is separable over $C^G$ such 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 $G/K$. Let $J_g = \{b \in B \mid bx = g(x)b \text{ for each } x \in B\}$ for a $g \in G$. We shall show that $B$ is a composition of the above two Galois extensions $B \supset B^G C \supset B^G$ with Galois group $K$ and $G/K$ respectively if and only if $J_g = \{0\}$ for each $g \not\in K$ and the order of $K$ is a unit in $B$. Moreover, let $B$ be a Galois extension satisfying the above conditions. We shall give two one-to-one correspondences, one between the set of separable extensions of $B^G C$ in $B$ and the set of separable $C$-subalgebras of $\bigoplus_{g \in K} J_g$, and the other one between the set of separable extensions of $B^G$ in $B^G C$ and the set of separable subalgebras of $Z$ over $Z^G$, where $Z$ is the center of $B^G C$.

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 $\{a_i, b_i \in B, i = 1, 2, \ldots, m\}$ 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. We call $B$ a Galois extension of $B^G$ with Galois group $G$ if there exist elements $\{a_i, b_i \in B, i = 1, 2, \ldots, m\}$ 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 $C$ (see [9], [10]). 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 of $B^G$ if it is a Galois and a Hirata separable extension of $B^G$ (see [6]). $B$ is called a center Galois extension of $B^G$ if $C$ is a Galois algebra over $C^G$ with Galois group $G|_C \cong G$. A Galois extension $B$ is called a DeMeyer-Kanzaki Galois extension with Galois group $G$ if $B$ is an Azumaya $C$-algebra and a center Galois extension with Galois group $G$. A ring $B$ is called decomposable if it contains more than two central idempotents and 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 $B$, $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$, $J_g = \{b \in B \mid bx = g(x)b \text{ for each } x \in B\}$ for a $g \in G$, and for a subring $A$ of $B$, $V_B(A)$ denotes the commutator subring of $A$ in $B$.
3. Equivalent Conditions

In this section, we shall give an equivalent condition for a Galois extension $B$ of a separable algebra $B^G$ over $C^G$ such 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 $G/K$. We shall employ the following two useful results of a Hirata separable extension as given in [5] and [6].

**Proposition 3.1.** (see [6], Proposition 4.3) Let $B$ be a Hirata Galois extension of $B^G$ with Galois group $G$. Then $B^G$ is a direct summand of $B$ as an $B^G$-bimodule if and only if the order of $G$ is a unit in $B$.

**Proposition 3.2.** (see [4], Theorem 1) Let $A$ be an Azumaya $C$-algebra. If $D$ is a subalgebra of $A$ such that $A$ is projective as a left $D$-module, then $A$ is a Hirata separable extension of $D$.

Now we show the necessity of the main theorem.

**Theorem 3.3.** Let $B$ be a Galois extension of $B^G$ with Galois group $G$ such that $B^G$ is separable over $C^G$. If $B$ is a Hirata Galois extension of $B^G C$ with Galois group $K$, then the order of $K$ is a unit in $B$ and $J_g = \{0\}$ for each $g \not\in K$.

**Proof.** Since $B$ is a Galois extension of $B^G$ such that $B^G$ is separable over $C^G$, $B$ is a separable extension of $B^G$; and so $B$ is a separable $C^G$-algebra by the transitivity property of separable extensions. Hence $B$ is an Azumaya $C$-algebra and $C$ is a separable $C^G$-algebra (see [3], Theorem 3.8, p. 55). Thus the homomorphic image of $B^G$ and $C$, $B^G C$ is also a separable $C^G$-algebra, and so $B^G C$ is a separable subalgebra of the Azumaya $C$-algebra $B$. But then $B^G C$ is a direct summand of $B$ as an $B^G C$-bimodule. By hypothesis, $B$ is a Hirata Galois extension of $B^G C$ with Galois group $K$. Hence the order of $K$ is a unit in $B$ by Proposition 3.1. Next, we show that $J_g = \{0\}$ for each $g \not\in K$. In fact, since $B$ is a Galois extension of $B^G C$ with Galois group $K$, $V_B(B^G C) = \bigoplus_{g \in K} J_g = V_B(B^K)$ (see [5], Proposition 1). On the other hand, since $V_B(B^G C) = V_B(B^G) = \oplus \sum_{g \in G} J_g$, $\oplus \sum_{g \in K} J_g = \oplus \sum_{g \in G} J_g$. Thus $J_g = \{0\}$ for each $g \not\in K$. This completes the proof.

Next is the converse of Theorem 3.3.

**Theorem 3.4.** Let $B$ be a Galois extension of $B^G$ with Galois group $G$ such that $B^G$ is separable over $C^G$. If the order of $K$ is a unit in $B$ and $J_g = \{0\}$ for each $g \not\in K$, then $B$ 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 $G/K$.

**Proof.** Let $\{a_i, b_i \in B, i = 1, 2, ..., m\}$ for some integer $m$ be a $G$-Galois system for $B$ and $r$ the order of $K$. Since $r$ is a unit in $B$ by hypothesis,
we can check that \( \{ \text{Tr}_{K}(a_i), \frac{1}{r} \text{Tr}_{K}(b_i) \mid i = 1, 2, ..., m \} \) is a \( G/K \)-Galois system for \( B^K \) where \( \text{Tr}_{K}( ) = \sum_{g \in K} g( ) \). Hence \( B^K \) is a Galois extension of \( B^G \) with Galois group \( G/K \). But \( B^G \) is separable over \( C^G \) by hypothesis, so \( B^K \) is a separable \( C^G \)-algebra by the transitivity property of separable extensions. Noting that \( C \subset B^K \), we have that \( B^K \) is a separable subalgebra of the Azumaya \( C \)-algebra \( B \). Next, since \( J_g = \{0\} \) for each \( g \notin K \), \( V_B(B^G C) = V_B(B^G) = \oplus \sum_{g \in G} J_g = \oplus \sum_{g \in K} J_g = V_B(B^K) \). Since \( B^G C \) and \( B^K \) are separable subalgebras of the Azumaya \( C \)-algebra \( B \), we have that \( B^G C = V_B(V_B(B^G C)) = V_B(V_B(B^K)) = B^K \) by the double centralizer property for Azumaya algebras (see [3], Theorem 4.3, p. 57). This implies that \( B \) is a Galois extension of \( B^G C (= B^K) \) with Galois group \( K \) and \( B^G C \) is a Galois extension of \( B^G \) with Galois group \( G/K \). Moreover, we claim 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 fact, since \( B \) is a left finitely generated projective \( B^G C \)-module, \( B \) is a Hirata separable extension of \( B^G C \) by Proposition 3.2. Thus \( B \) is a Hirata Galois extension of \( B^G C \) with Galois group \( K \). Also, let \( Z \) be the center of \( B^G C \). Then clearly, \( C \subset Z \) implies that \( B^G C \) is an Azumaya \( Z \)-algebra (for \( B^G C \) is a separable \( C \)-algebra). Noting that \( B^G C = B^G Z \) which is a Galois extension of \( B^G \) with Galois group \( G/K \), we have that \( B^G Z \) is a center Galois extension of \( B^G \) with Galois group \( G/K \) (see [8], Theorem 3.2). Therefore \( B^G C \) is a DeMeyer-Kanzaki Galois extension of \( B^G \) with Galois group \( G/K \).

**Corollary 3.5.** Let \( B \) be a Galois algebra over a commutative ring \( R \) with Galois group \( G \). Then \( B \) is a central Galois algebra over \( C \) with Galois group \( K \) and \( C \) is a commutative Galois extension of \( B^G \) with Galois group \( G/K \) if and only if the order of \( K \) is a unit in \( B \) and \( J_g = \{0\} \) for each \( g \notin K \).

### 4. Separable Subrings

Let \( B \) be a Galois extension of \( B^G \) with Galois group \( G \) such that \( B^G \) is separable over \( C^G \) as given in Theorem 3.4. By Theorem 3.4, \( B \) is a composition of a Hirata Galois extension \( B \) of \( B^G C \) with Galois group \( K \) and a DeMeyer-Kanzaki Galois extension \( B^G C \) of \( B^G \) with Galois group \( G/K \). In this section, we shall give some properties of the class of the separable subalgebras comparable with \( B^G C \).

**Theorem 4.1.** Let \( B \) be given in Theorem 3.4, \( S = \{ A \subset B \mid A \) is a separable extension of \( B^G C \} \), and \( T = \{ D \subset \oplus \sum_{g \in K} J_g \mid D \) is a separable \( C \)-algebra \} \). Then \( \alpha : A \to V_B(A) \) is a one-to-one correspondence between \( S \).
and $T$.

Proof. By Theorem 3.4, $B$ is a Hirata Galois extension of $B^G C$ with Galois group $K$, so $B$ is a Hirata separable extension and a left finitely generated and projective module over $B^G C$. Hence $\alpha : A \rightarrow V_B(A)$ is a one-to-one correspondence between the set of separable extensions $A$ of $B^G C$ such that $A$ is a direct summand of $B$ as an $A$-bimodule and the set of $C$-separable subalgebras of $V_B(B^G C)$ (see [7], Theorem 1). But for any separable extension $A$ of $B^G C$ in $B$, $A$ is a separable subalgebra of the Azumaya $C$-algebra $B$, so $A$ is a direct summand of $B$ as an $A$-bimodule. Thus, noting that $V_B(B^G C) = V_B(B^K) = \bigoplus_{g \in K} J_g$, we conclude that $\alpha : A \rightarrow V_B(A)$ is a one-to-one correspondence between $S$ and $T$.

Let $B$ be given in Theorem 3.4. By Theorem 3.4, $B^G C$ is a DeMeyer-Kanzaki Galois extension of $B^G$ with Galois group $G/K$, that is, $B^G C$ is an Azumaya algebra over its center $Z$ and $Z$ is a commutative Galois algebra over $Z^G$ with Galois group $G/K$. Let $P = \{ A \subset B^G C | A$ is a separable extension of $B^G \}$ and $Q = \{ D | D$ is a separable subalgebra of $Z$ over $Z^G \}$. Then $\beta : A \rightarrow A \cap Z$ is a one-to-one correspondence between $P$ and $Q$. 

Next we give a new proof of the expression of a separable algebra $A \in P$ as given in [1].

**Lemma 4.2.** By keeping the above notations, for any $A \in P$, $A = B^G \cdot (A \cap Z)$.

Proof. Since $A \in P$, $B^G \subset A$. Hence $A$ is a two sided module over $B^G$. But $B^G C = B^G Z$ has center $Z$, so the center of $B^G$ is $Z^G$. Noting that $B^G$ is separable over $Z^G$, we have that $B^G C$ is an Azumaya algebra over $Z^G$. Thus $A \cong B^G \otimes_{Z^G} V_A(B^G) = B^G \otimes_{Z^G} (A \cap V_{B^G C}(B^G)) = B^G \otimes_{Z^G} (A \cap Z)$ by the multiplication map (see [3], Corollary 3.6, p. 54). Therefore $A = B^G \cdot (A \cap Z)$.

**Theorem 4.3.** By keeping the above notations, $\beta : A \rightarrow A \cap Z$ is a one-to-one correspondence between $P$ and $Q$.

Proof. Since $\beta$ is the restriction map of the equivalent functor from the category of the bimodules over the Azumaya algebra $B^G$ and the category of the modules over the center $Z^G$ of $B^G$, $\beta : A \rightarrow A \cap Z$ is a one-to-one correspondence.

We conclude the present paper with three examples to demonstrate the main results in Section 3. Examples 1 and 2 show the existence of decomposable Galois algebras and extensions which are composition of two Galois extensions as given in Theorem 3.3 and 3.4, and Example 3 is a decomposable Galois extension which is not a composition of two Galois extensions as given in Theorem 3.3 and 3.4.
Example 1. Let $A = R[i,j,k]$ be the quaternion algebra over the real field $R$, $B = A \times A$, and $G = \{1, g_i, g_j, g_k, g, gg_i, gg_j, gg_k\}$, where $g_i(x, y) = (ixi^{-1}, iyi^{-1})$, $g_j(x, y) = (jxj^{-1}, jyj^{-1})$, $g_k(x, y) = (kxk^{-1}, kyk^{-1})$, and $g(x, y) = (y, x)$ for all $(x, y)$ in $B$. Then:

1. $B$ is a Galois extension with a $G$-Galois system: \( \{a_1 = (1, 0), a_2 = (i, 0), a_3 = (j, 0), a_4 = (k, 0), a_5 = (0, 1), a_6 = (0, i), a_7 = (0, j), a_8 = (0, k)\}$; \( b_1 = \frac{1}{2}(1, 0), b_2 = -\frac{1}{2}(i, 0), b_3 = -\frac{1}{2}(j, 0), b_4 = -\frac{1}{2}(k, 0), b_5 = \frac{1}{2}(0, 1), b_6 = -\frac{1}{2}(0, i), b_7 = -\frac{1}{2}(0, j), b_8 = -\frac{1}{2}(0, k)\);

2. $B^G = \{(r, r) \mid r \in R\} \cong R$;

3. by (1) and (2), $B$ is a Galois algebra over $R$ with Galois group $G$;

4. $C = R \times R$;

5. $K = \{1, g_i, g_j, g_k\}$;

6. $B^K = B^G C = R \times R$; and

7. by (6), $B$ is a composition of a central Galois algebra $B$ over $C$ with Galois group $K$ and $C$ is a commutative Galois extension of $C^G$ with Galois group $G/K$.

Example 2. Let $B = A \times A$ and $L = \{1, g_i, g_j, g_k\} \subset G$ as given in Example 1. Then:

1. $L$ is a subgroup of $G$;

2. $B$ is a Galois extension of $B^L$ with Galois group $L$;

3. $B^L = \{(x, x) \mid x \in R[i]\} \cong R[i]$ which is a separable $R$-algebra;

4. $K = \{1, g_i\}$;

5. $B^K = B[i] \times R[i]$;

6. $C = R \times R \subset R[i] \times R[i] = B^K = B^G C$; and

7. $B$ is a composition of a Hirata Galois extension (not a Galois algebra) of $B^L C$ with Galois group $K$ and a DeMeyer-Kanzaki Galois extension $B^L C$ of $B^L$ with Galois group $L/K$.

Example 3. Let $S$ be a commutative Galois algebra with Galois group $G$, $S \ast G$ the skew group ring (the crossed product with trivial factor set), $B = S \times (S \ast G)$, and $\overline{G} = \{(g, I_g) \mid g \in G\}$, where $I_g(x) = g x g^{-1}$ for each $x \in S \ast G$. Then:

1. $B$ is a Galois extension of $B^G$ with Galois group $\overline{G}$;

2. the center $C$ of $B$ is $S \times S^G$;

3. $B^G = S^G \times (S \ast G)^{\overline{G}}$;

4. $B^G C = S \times (S \ast G)^{\overline{G}}$;

5. $K = \{1\}$;

6. $B^K = B \neq B^G C$; and

7. $B$ is not a composition of $B \ni B^K$ and $B^K \ni B^G$. 

Acknowledgements

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.

References


