

On Indecomposable Separable Algebras with a Finite Automorphism Group

George Szeto

Department of Mathematics, Bradley University
Peoria, Illinois 61625, USA
szeto@bradley.edu

Abstract

Let B be a separable extension of B^G which is a separable C^G -algebra with a finite automorphism group G where C is the center of B with no idempotents but 0 and 1, and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. Then B is a projective Hirata separable extension of $B^G C$ and $B^G C$ is a Galois extension of B^G with Galois group G/K . Moreover, equivalent conditions are given under which B is a Galois extension of $B^G C$ with Galois group K .

Mathematics Subject Classification: 16S35, 16W20

Keywords: Separable extensions, Galois extensions, indecomposable separable algebras, Hirata separable extensions.

1 Introduction

It has been well known that an indecomposable commutative separable algebra A over A^G with a finite automorphism group G is a Galois algebra ([4], Proposition 1.2, page 80), and the fundamental theorem of Galois extensions for fields holds also for A ; that is, there exists a one-to-one correspondence between the set of subgroups of G and the set of separable subalgebras of A ([2], Theorem 3.5). More investigations of the general Galois extensions of rings were given in [1], [7], [8], and [9]. The purpose of the present paper is to generalize the above two results to a noncommutative separable algebra. Let B be a separable extension of B^G which is a separable C^G -algebra with a finite automorphism group G where C is the center of B with no idempotents but 0 and 1, and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. We shall show that B is a projective Hirata separable extension of $B^G C$ and $B^G C$ is a Galois extension of B^G with Galois group G/K . Moreover, some equivalent conditions are given

under which B is a Galois extension of $B^G C$ with Galois group K . Also, it will be shown that the fundamental theorem holds for the Galois extension $B^G C$ with Galois group G/K ; that is, there exists a one-to-one correspondence between the set of subgroups of G containing K and the set of separable extensions of B^G in $B^G C$. This derives a one-to-one correspondence between the set of separable extensions of $B^G C$ in B and the set of subgroups of G containing K .

2 Indecomposable Separable Algebras

Following the definitions as given in [1], 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 . For a subring A of B with the same identity 1, $V_B(A)$ denotes the commutator subring of A in B . We call B a separable extension of A if there exist $\{a_i, b_i$ in B , $i = 1, 2, \dots, p$ for some integer $p\}$ 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 , $i = 1, 2, \dots, p\}$ for some integer p such that $\sum_{i=1}^p a_i g(b_i) = \delta_{1,g}$ 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 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.

In this section, we assume that C is the center of B with no idempotents but 0 and 1 (that is, B is indecomposable), B is a separable extension of B^G which is a separable C^G -algebra with a finite automorphism group G , and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$.

Theorem 2.1 *Let B be an indecomposable separable extension of B^G which is a separable C^G -algebra with a finite automorphism group G . Then B is a projective Hirata separable extension of $B^G C$ and $B^G C$ is a Galois extension of B^G with Galois group G/K .*

Proof. Since B is a separable extension of B^G which is a separable C^G -algebra, it is a separable C^G -algebra by the transitivity of separable extensions. Hence 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). Thus $B^G C$ is a Galois extension of B^G with Galois group G/K with the same Galois system as C . Moreover, noting that B^G and C are separable C^G -algebras, we have that $B^G C$ is also a separable C^G -algebra. Thus $B^G C$ is a separable C -algebra because $C^G \subset C \subset B^G C$. But B is an Azumaya C -algebra, so it is a projective C -module. Therefore B is also a projective

$B^G C$ -module ([4], Proposition 2.3, page 48). Consequently, B is a projective Hirata separable extension of $B^G C$ ([5], Theorem 1).

Let B be an indecomposable separable C^G -algebra as given in Theorem 2.1. Then B is a projective Hirata separable extension of $B^G C$. Next, we show some equivalent conditions under which B is also a Galois extension of $B^G C$ with Galois group K .

Theorem 2.2 *Let B be as given in Theorem 2.1. Then the following statements are equivalent:*

- (1) B is a Galois extension of $B^G C$ with Galois group K .
- (2) B is a Galois extension of B^G with Galois group G .
- (3) $V_B(B^G) = \oplus \sum_{g \in K} J_g$ where $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$.

Proof. (1) \implies (2) Since C is a Galois algebra over C^G with Galois group G/K , C has a Galois system $\{c_i, d_i \text{ in } C, i = 1, 2, \dots, p \text{ for some integer } p\}$ such that $\sum_{i=1}^p c_i g(d_i) = 1$ for each $g \in K$ and $\sum_{i=1}^p c_i g(d_i) = 0$ for each $g \notin K$. Now, by hypothesis, B is a Galois extension of $B^G C$ with Galois group K . Let $\{a_i, b_i \text{ in } B, i = 1, 2, \dots, q \text{ for some integer } q\}$ be a Galois system for B with Galois group K , that is, $\sum_{i=1}^q a_i g(b_i) = \delta_{1,g}$ for each $g \in K$. Then we claim that $\{a_i c_j, b_i d_j, i = 1, 2, \dots, q, j = 1, 2, \dots, p\}$ is a Galois system for B with Galois group G . In fact, $\sum_{i=1}^q \sum_{j=1}^p (a_i c_j)(b_i d_j) = \sum_{i=1}^q a_i b_i \sum_{j=1}^p c_j d_j = 1$ and $\sum_{i=1}^q \sum_{j=1}^p (a_i c_j)g(b_i d_j) = \sum_{i=1}^q a_i g(b_i) \sum_{j=1}^p c_j g(d_j) = 0$ for each $g \neq 1$ in G . This implies that B is a Galois extension of B^G with Galois group G .

(2) \implies (1) Since B is a Galois extension of B^G with Galois group G , it is a Galois extension of B^K with Galois group K . Hence it suffices to show that $B^K = B^G C$. Clearly, $B^G C \subset B^K$ and $(G/K)|_{B^G C} \cong (G/K)|_{B^K} \cong G/K$ by the definition of K . Moreover, since C is a Galois algebra over C^G with Galois group G/K , $B^G C$ and B^K are Galois extensions of B^G with Galois group $(G/K)|_{B^G C} \cong (G/K)|_{B^K} \cong G/K$ with the same Galois system as C . Hence $B^G C = B^K$. Thus B is a Galois extension of $B^G C$ with Galois group K .

(1) \implies (3) Since B is a Galois extension of $B^G C$ with Galois group K , $V_B(B^G) = V_B(B^G C) = \oplus \sum_{g \in K} J_g$ ([6], Proposition 1).

(3) \implies (1) As shown in the proof of (2) \implies (1), since $B^G C \subset B^K$ and C is a Galois algebra over C^G with Galois group G/K , $B^G C$ and B^K are Galois extensions of B^G with Galois group $(G/K)|_{B^G C} \cong (G/K)|_{B^K} \cong G/K$. Thus $B^G C = B^K$. On the other hand, B is a projective Hirata separable extension of $B^G C$ by Theorem 2.1, so that $V_B(B^G) = V_B(B^G C) = \oplus \sum_{g \in K} J_g$ implies that B is a Galois extension of $B^G C$ with Galois group K ([7], Proposition 1). This completes the proof.

Theorem 2.3 *Let $\mathcal{C} = \{H \mid H \text{ is a subgroup of } G \text{ containing } K\}$ and $\mathcal{D} = \{B^G E \mid E \text{ is a separable subalgebra of } C \text{ over } C^G\}$. Then $\alpha : H \longrightarrow B^G C^H$ is a one-to-one correspondence between \mathcal{C} and \mathcal{D} .*

Proof. For a subgroup H of G containing K , H/K is a subgroup of G/K such that $C^{H/K} = C^H$ which is a separable C^G -algebra ([4], Corollary 1.7 on page 89). Therefore $\alpha : H \longrightarrow B^G C^H$ is well defined from \mathcal{C} to \mathcal{D} . Next we claim that α is one-to-one. In fact, let $\alpha(H) = \alpha(L)$ for $H, L \in \mathcal{C}$. Then $B^G C^H = B^G C^L$; and so $C^H = (B^G C^H) \cap C = (B^G C^L) \cap C = C^L$. Thus $C^{H/K} = C^H = C^L = C^{L/K}$. Therefore $H/K = L/K$ by the fundamental theorem for the commutative Galois algebra C ([4], Corollary 1.7 on page 89). Noting that $K \subset H \subset LK = L$ and $K \subset L \subset HK = H$, we have $H = L$. Now let E be a separable subalgebra of C over C^G . Then $E = C^{H/K}$ for some subgroup of G containing K by the fundamental theorem for indecomposable commutative Galois algebra C again. Thus $\alpha(H) = B^G C^H = B^G C^{H/K} = B^G E$; and so α is onto.

Now we show that $B^G C$ satisfies the fundamental theorem.

Theorem 2.4 *By keeping the notations as given in Theorem 2.3, the map $\beta : H \longrightarrow (B^G C)^H$ is a one-to-one correspondence between the set of subgroups of G containing K and the set of separable extensions of B^G in $B^G C$.*

Proof. At first, we claim that $(B^G C)^H = B^G C^H$ for each subgroup of G containing K . In fact, since C is a commutative Galois algebra over C^G with Galois group G/K , C is also a Galois algebra over C^H with Galois group H/K . Hence there exists an element $c \in C$ such that $\text{Tr}_{H/K}(c) = 1$ where $\text{Tr}_{H/K} = \sum_{\bar{h} \in H/K} \bar{h}$ ([4], Corollary 1.3, page 85). Let $\sum_{i=1}^k b_i c_i \in (B^G C)^H$ for some $b_i \in B^G$, $c_i \in C$, and some integer k . Then $\sum_{i=1}^k b_i c_i = \text{Tr}_{H/K}(c) \sum_{i=1}^k b_i c_i = \text{Tr}_{H/K}(c \sum_{i=1}^k b_i c_i) = \sum_{i=1}^k b_i \text{Tr}_{H/K}(c c_i) \in B^G C^H$. Thus $(B^G C)^H \subset B^G C^H$. Also, the converse is clear, $B^G C^H \subset (B^G C)^H$, so $(B^G C)^H = B^G C^H$. Thus by Theorem 2.3, β is a one-to-one correspondence between the set of subgroups of G containing K and the set of separable extensions $(B^G C)^H$. Next we want to show that any separable extension A of B^G in $B^G C$ is $(B^G C)^H$ for some subgroup H of G containing K . Let Z be the center of $B^G C$. Then $B^G C$ is an Azumaya algebra over Z and $C \subset Z$. Since C is a Galois algebra with Galois group G/K , Z is also a Galois algebra with Galois group G/K (that is, $B^G C$ is a DeMeyer-Kanzaki Galois extension of B^G with Galois group G/K). But then $A = B^G \cdot (A \cap Z) = B^G Z^H$ where $H = \{g \in G \mid g(a) = a \text{ for all } a \in A\}$ ([3], page 120). Moreover, noting that $Z = Z_0 C$ where Z_0 is the center of B^G , we have that $Z^H = Z_0 C^H$; and so $A = B^G Z^H = B^G C^H$. Therefore the map $\beta : H \longrightarrow (B^G C)^H$ is a one-to-one correspondence between the set

of subgroups of G containing K and the set of separable extensions of B^G in $B^G C$.

In Theorem 2.4, since $B^G C$ may be decomposable and $B^G C$ may not be Azumaya algebra over C , Theorem 2.4 generalizes Theorem 3 in [3].

Corollary 2.5 ([3], Theorem 3) *By keeping the notations as given in Theorem 2.3, the map $\beta : H \rightarrow (B^G C)^H$ is a one-to-one correspondence between the set of subgroups of G containing K and the set of separable extensions of B^G in $B^G C$.*

3 Examples

In this section, we shall give two examples of indecomposable separable extension with an automorphism group, one a Galois extension but the other not a Galois extension. We begin with a decomposable separable extension.

Example 3.1 *Let S_3 be the permutation group on 3 symbols, Q the rational field, and QS_3 the group algebra of S_3 over Q .*

(1) *Since 6 (the order of S_3) is invertible in Q , QS_3 is a separable algebra over Q .*

(2) *Let G be the inner automorphism group of QS_3 induced by the elements in S_3 . The center of S_3 is the identity 1, so there are at least two conjugate classes of S_3 . Hence the center Z of QS_3 is a free module over Q of rank greater than two.*

(3) *QS_3 is not a Galois extension of $(QS_3)^G$ with Galois group G . Assume QS_3 is a Galois extension of $(QS_3)^G$ with Galois group G . Since G is inner, $(QS_3)^G = Z$ (= the center of QS_3); and so QS_3 is a central Galois algebra over Z with an inner Galois group G . Thus $QS_3 = ZG_f$, which is a projective group algebra of G over Z with a factor set $f : G \times G \rightarrow \text{units of } Z$. But then $\text{rank}_Q(QS_3) = 6 = \text{rank}_Q(ZG_f) = \text{rank}_Q(Z) \cdot \text{rank}_Z(QS_3) \geq 2 \cdot 6 = 12$. This is impossible. Therefore QS_3 is not a Galois algebra over Z .*

Noting that QS_3 is decomposable, we let $\{e_i | i = 1, 2, \dots, m \text{ for some integer } m\}$ be the set of minimal central idempotents of QS_3 . Then $QS_3 = \sum_{i=1}^m (QS_3)e_i$ where $(QS_3)e_i$ is an indecomposable separable algebra over Ze_i for each i .

Example 3.2 Let $(QS_3)e_i$ be a noncommutative component of QS_3 as given in the above remark. Then $(QS_3)e_i$ is an indecomposable separable extension of $((QS_3)e_i)^{G_i}$ where $G_i = G/(QS_3)e_i$, but not a Galois extension. In fact, since $e_i \in Z$ and $Z = (QS_3)^G$, $G((QS_3)e_i) = (QS_3)e_i$. Hence the order of G_i is 1, 2, 3, or 6, and $((QS_3)e_i)^{G_i} = Ze_i$.

(1) Clearly, $(QS_3)e_i$ is an indecomposable separable algebra over Ze_i ($= ((QS_3)e_i)^{G_i}$).

(2) Assume $(QS_3)e_i$ is a Galois algebra over Ze_i with Galois group G_i . Then the order of G_i is 1, 2, 3, or 6. By hypothesis, $(QS_3)e_i$ is noncommutative, the order of G_i is not 1, 2, or 3. Also, the order of G_i is not 6 (a square free integer) because $(QS_3)e_i$ is a central semisimple algebra over Ze_i . Thus $(QS_3)e_i$ is not a Galois algebra over Ze_i with Galois group G_i .

Next is an indecomposable Galois extension as given by Theorem 2.2.

Example 3.3 Let D be the field of complex numbers, $M_2(D)$ the matrix ring of order 2 over D , $B = M_2(D)[i, j, k]$ the quaternion ring over $M_2(D)$, and $G = \{1, g_i, g_j, g_k, \alpha, g_i\alpha, g_j\alpha, g_k\alpha\}$ where $g_i(b) = ibi^{-1}$, $g_j(b) = jbj^{-1}$, $g_k(b) = kbk^{-1}$, and $\alpha(b) = \bar{a}_0 + \bar{a}_1i + \bar{a}_2j + \bar{a}_3k$ for $b = a_0 + a_1i + a_2j + a_3k \in B$ where $\bar{a} = \begin{pmatrix} \bar{d}_1 & \bar{d}_2 \\ \bar{d}_3 & \bar{d}_4 \end{pmatrix}$ for $a = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix} \in M_2(D)$ and \bar{d}_i is the conjugate of the complex number d_i . Then,

(1) the center of B is $C = \left\{ \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \mid d \in D \right\} \cong D$.

(2) $K = \{1, g_i, g_j, g_k\}$ and $G/K = \{1, \alpha\}$.

(3) $B^G = M_2(R)$, the matrix ring of order 2 over the field of real numbers R .

(4) $B^G C = B^K = M_2(D)$.

(5) B is a Galois extension of $M_2(D)$ with Galois group $K = \{1, g_i, g_j, g_k\}$.

(6) B is a Galois extension of $M_2(R)$ with Galois group G .

(7) $M_2(D)$ is a Galois extension of $M_2(R)$ with Galois group $G/K = \{1, \alpha\}$.

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

References

- [1] R. Alfaro and G. Szeto, On Galois Extensions of an Azumaya Algebra, *Comm. in Algebra*, **25**(6)(1997), 1873-1882.

- [2] S.U. Chase, D.K. Harrison, A. Rosenberg, Galois Theory and Galois Cohomology of Commutative Rings, *Memoirs Amer. Math. Soc.* Volume 52. 1965.
- [3] F.R. DeMeyer, Some Notes on the General Galois Theory of Rings, *Osaka J. Math.*, **2** (1965), 117 - 127.
- [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 a Special Type of Galois Extensions, *Hokkaido J. Math.*, **9** (1980), 123-128.
- [8] G. Szeto and L. Xue, On Galois Extensions Satisfying the Fundamental Theorem, *International Mathematical Forum*, **2**(36) (2007), 1773-1777.
- [9] G. Szeto and L. Xue, On Galois Extensions of a Separable Algebra, *International Mathematical Forum*, to appear.

Received: December 11, 2007