

# On Galois Extensions of a Separable Algebra

George Szeto and Lianyong Xue

Department of Mathematics

Bradley University

Peoria, Illinois 61625, USA

Email: szeto@bradley.edu lxue@bradley.edu

## Abstract

Characterizations for a Galois extension of a separable algebra are given, and applications are derived for Azumaya Galois extensions and Hirata separable Galois extensions.

**2000 Mathematics Subject Classification:** 16S35, 16W20

## 1 Introduction

Galois extensions over an Azumaya algebra have been studied in [1], [2], [3], [7], and [8], that is,  $B$  is a Galois extension of  $B^G$  with Galois group  $G$  such that  $B^G$  is an Azumaya algebra over  $C^G$  where  $C$  is the center of  $B$ . In the present paper, replacing the condition of Azumaya  $C^G$ -algebra  $B^G$  by a separable  $C^G$ -algebra  $B^G$ , we shall study a broader class of Galois extension  $B$  with Galois group  $G$  of  $B^G$  which is a separable  $C^G$ -algebra. Such a  $B$  is characterized in terms of the center  $Z$  of the skew group ring  $B * G$ . The following statements are equivalent: (1)  $B$  is a Galois extension with Galois group  $G$  of  $B^G$  which is a separable  $C^G$ -algebra; (2)  $B * G$  is a separable  $C^G$ -algebra and  $B$  is a left generator of  $Z$  where  $Z$  is the center of  $B * G$ ; and (3)  $B * G$  is a separable  $C^G$ -algebra and there exist  $\{x_i, y_i \in B \mid i = 1, 2, \dots, m \text{ for some integer } m\}$  such that  $\alpha : D \cong Z$  by  $\alpha(d) = \sum_{g \in G} \sum_{i=1}^m x_i dg(y_i) U_g$  for  $d \in D$  where  $D$  is the center of  $B^G$  and  $\{U_g \mid g \in G\}$  is a canonical bases for  $B * G$ . Thus these results can be applied to the class of Azumaya Galois extensions and the class of Hirata separable Galois extensions of a separable algebra.

## 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  $B$ ,  $i = 1, 2, \dots, m$  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  $B$ ,  $i = 1, 2, \dots, m\}$  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  $B$ . An Azumaya Galois extension of  $B^G$  with Galois group  $G$  is a Galois extension of  $B^G$  with Galois group  $G$  such that  $B^G$  is an Azumaya algebra over  $C^G$ . 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  $C$ . 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 separable Galois extension if it is a Galois and a Hirata separable extension of  $B^G$ .

## 3. Main Results

Throughout this section, let  $B$  be a Galois extension of  $B^G$  with Galois group  $G$ ,  $C$  the center of  $B$ ,  $B * G$  the skew group ring with a canonical basis  $\{U_g | g \in G\}$ ,  $Z$  the center of  $B * G$ , and  $D$  the center of  $B^G$ . We shall characterize a Galois extension  $B$  of  $B^G$  which is a separable  $C^G$ -algebra.

### Theorem 3.1.

The following statements are equivalent: (1)  $B$  is a Galois extension with Galois group  $G$  of  $B^G$  which is a separable  $C^G$ -algebra; (2)  $B * G$  is a separable  $C^G$ -algebra and  $B$  is a left generator of  $Z$ ; and (3)  $B * G$  is a separable  $C^G$ -algebra and there exist

$\{x_i, y_i \in B \mid i = 1, 2, \dots, m \text{ for some integer } m\}$  such that  $\alpha : D \cong Z$  as  $C^G$ -algebra by  $\alpha(d) = \sum_{g \in G} \sum_{i=1}^m x_i dg(y_i)U_g$  for  $d \in D$ .

*Proof.* (1)  $\implies$  (2) Since  $B$  is a Galois extension of  $B^G$  with Galois group  $G$ ,  $B * G \cong \text{Hom}_{B^G}(B, B)$  and  $B$  is a finitely generated and projective left  $B^G$ -module. Moreover, by hypothesis,  $B^G$  is a separable  $C^G$ -algebra, so  $\text{Hom}_{B^G}(B, B)$  is a separable  $C^G$ -algebra ([6], Theorem 1). Thus,  $B * G$  is a separable  $C^G$ -algebra; and so  $B * G$  is an Azumaya  $Z$ -algebra ([4], Theorem 3.8 on page 55). But then  $Z$  is a direct summand of  $B * G$  ([4], Lemma 3.1 on page 51). This implies that  $B * G$  is a generator of  $Z$ . Again,  $B$  is a Galois extension of  $B^G$ , so  $B$  is a generator of  $B * G$ . Therefore,  $B$  is a left generator of  $Z$  by the transitivity of generator modules.

(2)  $\implies$  (1) By hypothesis,  $B * G$  is a separable  $C^G$ -algebra, so  $B * G$  is an Azumaya  $Z$ -algebra ([4], Theorem 3.8 on page 55). Thus, noting that  $Z$  is a generator of itself, we have that  $Z$  is a generator of  $B * G$ . But  $B$  is a left generator of  $Z$  by hypothesis, so  $B$  is also a left generator of  $B * G$  by the transitivity of generator modules. This proves that  $B$  is a Galois extension of  $B^G$  with Galois group  $G$ . Moreover, since  $B * G$  is a separable  $C^G$ -algebra,  $B * G$  is a separable extension of  $B$ . Hence there exists an element  $c \in C$  such that  $\text{Tr}_G(c) = 1$  where  $\text{Tr}_G(\cdot) = \sum_{g \in G} g(\cdot)$ . Thus  $B^G$  is a direct summand of  $B$  as a  $B^G$ -bimodule; and so the group ring  $B^G * G$  is a direct summand of  $B * G$  as a  $B^G$ -bimodule. But  $B^G$  is a direct summand of  $B^G * G$  as a  $B^G$ -bimodule, so  $B^G$  is also a direct summand of  $B * G$  as a  $B^G$ -bimodule. On the other hand, since  $B$  has been shown to be Galois extension of  $B^G$  with Galois group  $G$ ,  $B$  is a finitely generated and projective left  $B^G$ -module. But then  $B * G$  is a finitely generated and projective left  $B^G$ -module such that  $B^G$  is also a direct summand of  $B * G$  as a  $B^G$ -bimodule. Now,  $B * G$  is a separable  $C^G$ -algebra by hypothesis, so  $B^G$  is also a separable  $C^G$ -algebra by the argument as given on page 55 in [4]. This completes the proof.

(1)  $\implies$  (3) Since  $B$  is a Galois extension of  $B^G$  with Galois group  $G$ ,

$$\alpha : \text{Hom}_{B^G}(B, B) \cong B * G$$

where  $B$  is a finitely generated and projective right  $B^G$ -module, and

$$\alpha(f) = \sum_{g \in G} \sum_{i=1}^m f(x_i)g(y_i)U_g$$

for a  $G$ -Galois system  $\{x_i, y_i\}$  ([3], Theorem 1). But  $B^G$  is a separable  $C^G$ -algebra by hypothesis, so  $\text{Hom}_{B^G}(B, B)$  is a separable  $C^G$ -algebra ([6], Theorem 1). Considering  $B$  as a right  $B^G$ -module, we can verify that the center of  $\text{Hom}_{B^G}(B, B)$  is  $f_D$  where  $f_D = \{f_d \in D \mid f_d(b) = bd \text{ for each } b \in B\}$ . In fact, for any  $h \in \text{Hom}_{B^G}(B, B)$  and  $b \in B$ ,  $(f_d \cdot h)(b) = f_d(h(b)) = h(b)d = h(db) = (h \cdot f_d)(b)$ , so  $f_d$  is contained in the center of  $\text{Hom}_{B^G}(B, B)$ . Also, for any  $h$  in the center of  $\text{Hom}_{B^G}(B, B)$ , noting that  $L_b$  the left multiplication map by  $b$  is in  $\text{Hom}_{B^G}(B, B)$ , we have that  $h \cdot L_b(1) = L_b \cdot h(1)$  because  $h \cdot L_b = L_b \cdot h$ . Thus  $h(b \cdot 1) = b \cdot h(1)$  for each  $b \in B$ . In particular, for each  $b \in B^G$ ,  $h(b \cdot 1) = b \cdot h(1) = h(1 \cdot b) = h(1) \cdot b$ . Now, let  $h(1) = d$ . Then  $bd = db$  for each  $b \in B^G$ , that is  $d \in D$ . Thus  $h = f_d \in f_D$ ; and so the center of  $\text{Hom}_{B^G}(B, B) = f_D$  where  $D$  is the center of  $B^G$ . Next, since  $\alpha : \text{Hom}_{B^G}(B, B) \cong B * G$  where  $\alpha(f) = \sum_{g \in G} \sum_{i=1}^m f(x_i)g(y_i)U_g$  for a  $G$ -Galois system  $\{x_i, y_i \in B \mid i = 1, 2, \dots, m \text{ for some integer } m\}$  for  $B$ . The restriction of  $\alpha$  to  $f_D$  is given by  $\alpha(f_d) = \sum_{g \in G} \sum_{i=1}^m f_d(x_i)g(y_i)U_g$  for each  $d \in D$ , which is equal to  $\sum_{g \in G} \sum_{i=1}^m (x_i d)g(y_i)U_g \in Z$ , the center of  $B * G$ . Thus  $\alpha : D \cong Z$  as  $C^G$ -algebra.

(3)  $\implies$  (1) Since  $\alpha : D \cong Z$  from the center of  $B^G$  to the center  $Z$  of  $B * G$  by  $\alpha(d) = \sum_{g \in G} \sum_{i=1}^m x_i d g(y_i)U_g$  for  $d \in D$  for some  $\{x_i, y_i \in B \mid i = 1, 2, \dots, m\}$ ,  $\alpha(1) = 1 = \sum_{g \in G} \sum_{i=1}^m x_i \cdot 1 \cdot g(y_i)U_g$ . Hence  $\sum_{i=1}^m x_i g(y_i) = \delta_{1,g}$ ; and so  $\{x_i, y_i \in B \mid i = 1, 2, \dots, m\}$  is a  $G$ -Galois system for  $B$ . Thus  $B$  is a Galois extension of  $B^G$  with Galois group  $G$ . Moreover,  $B * G$  is a separable  $C^G$ -algebra by hypothesis, so by the proof in (2)  $\implies$  (1), that  $B * G$  is a separable  $C^G$ -algebra implies that  $B^G$  is a separable  $C^G$ -algebra. Thus the proof is complete.

In [9], the class of Hirata separable Galois extensions was studied. By Theorem 3.1, we can derive some characterizations for a Hirata separable Galois extension  $B$  of  $B^G$  which is a separable  $C^G$ -algebra.

**Theorem 3.2.**

Let  $B$  be a Galois extension of  $B^G$  with Galois group  $G$  such that  $B^G$  is a separable  $C^G$ -algebra. Then the following statements are equivalent: (1)  $B$  is a Hirata separable Galois extension of  $B^G$ ; (2)  $B^G$  satisfies the double centralizer property in  $B$ , that is,  $V_B(V_B(B^G)) = B^G$ ; and (3)  $B$  is an Azumaya  $C^G$ -algebra.

*Proof.* (1)  $\implies$  (2) Since  $B$  is a Hirata separable Galois extension of  $B^G$ ,  $V_B(V_B(B^G)) = B^G$  ([9], Proposition 4).

(2)  $\implies$  (3) Since  $V_B(V_B(B^G)) = B^G$ ,  $C = C^G$ . Thus the separable  $C^G$ -algebra  $B$  becomes an Azumaya  $C^G$ -algebra.

(3)  $\implies$  (1) Since  $B$  is a Galois extension of  $B^G$  with Galois group  $G$ ,  $B$  is a finitely generated and projective left  $B^G$ -module. Moreover, by hypothesis,  $B$  is an Azumaya  $C^G$ -algebra, so  $B$  is a Hirata separable Galois extension of  $B^G$  ([5], Theorem 1).

By Theorem 3.1, some equivalent conditions for an Azumaya Galois extension can also be obtained.

**Theorem 3.3.**

By keeping the notations of Theorem 3.1, let  $B$  be a Galois extension of  $B^G$  with Galois group  $G$  such that  $B^G$  is a separable  $C^G$ -algebra. Then the following statements are equivalent: (1)  $D = C^G$ ; (2)  $Z = D$  where  $Z$  is the center of  $B * G$ ; and (3) there exist  $\{x_i \in V_B(D), y_i \in B \mid i = 1, 2, \dots, m \text{ for some integer } m\}$  such that  $\alpha : D \cong Z$  as  $C^G$ -algebra by  $\alpha(d) = \sum_{g \in G} \sum_{i=1}^m x_i dg(y_i) U_g$  for  $d \in D$ .

*Proof.* (1)  $\implies$  (2) Since  $D = C^G$ ,  $B^G$  is an Azumaya  $C^G$ -algebra. Hence  $B$  is an Azumaya Galois extension of  $B^G$  with Galois group  $G$ . Thus  $D = C^G = Z$  ([2], Theorem 1).

(2)  $\implies$  (1) Since  $Z = D$ ,  $Z \subset B^G \subset B$ . Thus  $Z = C^G$  ([2], Theorem 1).

(1)  $\implies$  (3) By hypothesis,  $D = C^G$ , so  $V_B(D) = V_B(C^G) = B$ . Thus  $x_i \in V_B(D)$  for each  $i$  where  $\{x_i, y_i \in B \mid i = 1, 2, \dots, m\}$  are as given in Theorem 3.1.

(3)  $\implies$  (2) By Theorem 3.1,  $\alpha : D \cong Z$  by  $\alpha(d) = \sum_{g \in G} \sum_{i=1}^m x_i dg(y_i)U_g$  for  $d \in D$ . In particular, let  $d = 1$ ; then  $\alpha(1) = 1 = \sum_{g \in G} \sum_{i=1}^m x_i g(y_i)U_g$ . Thus  $\{x_i, y_i \in B \mid i = 1, 2, \dots, m\}$  is a  $G$ -Galois system for  $B$ ; that is,  $\sum_{i=1}^m x_i g(y_i) = \delta_{1,g}$ . Now by hypothesis,  $x_i \in V_B(D)$  for each  $i$ , so  $\alpha(d) = \sum_{g \in G} \sum_{i=1}^m x_i dg(y_i)U_g = \sum_{g \in G} \sum_{i=1}^m dx_i g(y_i)U_g = d$ . Therefore  $D = Z$ .

We conclude the present paper with three examples of Galois extensions  $B$  of a separable algebra to demonstrate the results: (1)  $B$  is an Azumaya Galois extension of  $B^G$  and  $B$  is also a Hirata separable Galois extension of  $B^G$ , (2)  $B$  is an Azumaya Galois extension of  $B^G$  but  $B$  is not a Hirata separable Galois extension of  $B^G$ , and (3)  $B$  is a Galois extension of a separable algebra  $B^G$  but not an Azumaya Galois extension. First, we show a theorem.

**Theorem 3.4.**

Let  $B$  be an algebra over  $R$ ,  $G$  a finite automorphism group of  $B$ ,  $C$  the center of  $B$ , and  $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$ . If  $B$  is a central Galois algebra over  $C$  with Galois group  $K$  and  $C$  is a commutative Galois algebra over  $R$  with Galois group  $G/K$ , then  $B$  be a Galois algebra over  $R$  with Galois group  $G$ .

*Proof.* Let  $\{a_i, b_i \in B \mid i = 1, 2, \dots, m\}$  for some integer  $m$  be a Galois system for  $B$  over  $C$  with Galois group  $K$  and  $\{c_j, d_j \in C \mid j = 1, 2, \dots, k\}$  for some integer  $k$  a Galois system

for  $C$  over  $R$  with Galois group  $G/K$ . Then it can be checked that  $\{a_i c_j, b_i d_j \in B \mid i = 1, 2, \dots, m, j = 1, 2, \dots, k\}$  is a Galois system for  $B$  over  $R$  with Galois group  $G$ .

**Example 1.**

Let  $A = C[i, j, k]$  be the quaternion algebra over the complex field  $C$ ,

$$H = \{1, \alpha_i, \alpha_j, \alpha_k \mid \alpha_l(x) = lxl^{-1}, \text{ for } l = i, j, k \text{ and for each } x \in A\},$$

$\tau(a + b_i i + c_j j + d_k k) = \bar{a} + \bar{b}_i i + \bar{c}_j j + \bar{d}_k k$  for  $a, b, c, d \in C$ , and  $G = \langle \tau, H \rangle$  the automorphism group generated by  $\tau$  and the elements in  $H$ . Then (1)  $A$  is a central Galois algebra over  $C$  with Galois group  $H$  and  $C$  is a commutative Galois algebra over the real field  $R$  with Galois group  $G/H \cong \{1, \tau\}$ ; (2)  $A$  is a Galois algebra over  $R$  with Galois group  $G$  by Theorem 3.4; and (3) let  $B = M_2(C) \otimes_C A$  where  $M_2(C)$  is the matrix algebra of order 2 over  $C$ . Then  $B$  is an Azumaya Galois extension of  $B^{1 \otimes H} (\cong M_2(C))$  with Galois group  $1 \otimes H$  and  $B$  is also a Hirata separable Galois extension of  $B^{1 \otimes H}$ .

**Example 2.**

Let  $A, C, R$ , and  $G$  be as given in Example 1 and  $B = M_2(R) \otimes_R A$ . Then  $B$  is an Azumaya Galois extension of  $B^{1 \otimes G} (\cong M_2(R))$  with Galois group  $1 \otimes G$  where  $B$  is not a Hirata separable extension of  $B^{1 \otimes G}$  because  $B$  is not an Azumaya algebra over  $R$ .

**Example 3.**

Let  $C$  be the complex field,  $R$  the real field, and  $G = \{1, \alpha\}$  where  $\alpha(c) = \bar{c}$  for each  $c \in C$ . Then  $C$  is a Galois algebra over  $R$  with Galois group  $G$ . Let  $B = C * G$  the skew group ring of  $G$  over  $C$ . Then  $B$  is a Galois extension of  $B^{\bar{G}}$  with Galois group  $\bar{G}$  where  $\bar{G}$  is the inner automorphism group of  $B$  induced by the elements in  $G$ . Since  $\bar{G}$  is inner,  $B$  is a Hirata Galois extension of  $B^{\bar{G}}$  with Galois group  $\bar{G}$  ([9], Corollary 3). Also  $B^{\bar{G}} = R * G$ ,

a commutative separable algebra over  $R$ , so  $B^{\overline{G}}$  is not an Azumaya algebra over  $R$ . Thus  $B$  is not an Azumaya Galois extension of  $B^{\overline{G}}$ .

### Acknowledgement

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

### References

- [1] R. Alfaro and G. Szeto, Skew Group Rings which are Azumaya, *Comm. in Algebra*, 23(6)(1995), 2255-2261.
- [2] R. Alfaro and G. Szeto, On Galois Extensions of an Azumaya Algebra, *Comm. in Algebra*, 25(6)(1997), 1873-1882.
- [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 Commutator Rings and Galois Theory of Separable Algebras, *Osaka J. Math.*, 1 (1964), 103-115.
- [7] T. Kanzaki, On Galois algebra over a commutative ring, *Osaka J. Math.*, 2(1965), 309-317.
- [8] M. Ouyang, Azumaya Extensions and Galois Correspondence, *Algebra Colloquium*, 7:1 (2000), 43-57.
- [9] K. Sugano, On a Special Type of Galois Extensions, *Hokkaido J. Math.*, 9(1980), 123-128.