ON AZUMAYA INVARIANT SUBRINGS OF A GALOIS EXTENSION

Lianyong Xue
Department of Mathematics
Bradley University
Peoria, Illinois 61625, USA
lxue@bradley.edu

Abstract

Let $B$ be a ring with 1, $C$ the center of $B$, $G$ a finite automorphism group of $B$, and $B^G$ the set of elements in $B$ fixed under each element in $G$. Then it is shown that if $B$ is a commutator Galois extension with Galois group $G$, then $B$ is an Azumaya $C$-algebra if and only if $B^G$ is an Azumaya $C^G$-algebra. This generalizes F. DeMeyer’s result for center Galois extensions. A Galois $H$-separable extension of an Azumaya algebra is also characterized.

1. Introduction

Let $B$ be a Galois extension of $B^G$ with Galois group $G$ and $C$ the center of $B$. In ([1], [2]), the class of Galois extensions $B$ with Galois group $G$ such that $B^G$ is an Azumaya $C^G$-algebra (that is, $B$ is an Azumaya Galois extension with Galois group $G$) was studied. It can be shown that for a Galois extension $B$ with Galois group $G$, $B^G$ is an Azumaya $C^G$-algebra implies that $B$ is an Azumaya $C$-algebra. In [4], DeMeyer showed that, if $C$ is a Galois extension with Galois group $G|_C \cong G$ (that is, $B$ is a center Galois extension

AMS 2000 Subject Classification Codes: 16S35, 16W20
Key Words and Phrases: Galois extensions, Center Galois extensions, Commutator Galois extensions, Azumaya algebras, $H$-separable extensions.
with Galois group $G$), then $B$ is an Azumaya $C$-algebra if and only if $B^G$ is an Azumaya $C^G$-algebra ([4], Lemma 2). Noting that an Azumaya Galois extension is not necessarily a center Galois extension, in the present paper, we are interested in a more general problem: Is it true that $B$ is an Azumaya $C$-algebra if and only if $B^G$ is an Azumaya $C^G$-algebra for a Galois extension $B$ with Galois group $G$? We first prove this affirmatively when $V_B(B^G)$, the commutator subring of $B^G$ in $B$, is a Galois extension with Galois group $G|V_B(B^G) \equiv G$ (that is, $B$ is a commutator Galois extension with Galois group $G$). Since $C \subseteq V_B(B^G)$, our result generalizes the above DeMeyr result for center Galois extensions.

Then, we construct an example of a Galois $H$-separable extension $B$ ([6]) such that $B$ is an Azumaya $C$-algebra, but $B^G$ is not an Azumaya $C^G$-algebra. Moreover, several equivalent conditions are given for a Galois $H$-separable extension $B$ under which $B$ is an Azumaya $C$-algebra implies that so is $B^G$ over $C^G$.

2 Basic Definitions and Notations

Throughout this paper, $B$ will represent a ring with 1, $C$ the center of $B$, $G$ a finite automorphism group of $B$, $B^G$ the set of elements in $B$ fixed under each element in $G$, $B*G$ the skew group ring of $G$ over $B$, that is, $B*G$ is the free left $B$-module in which the multiplication is given by $gb = g(b)g$ for $b \in B$ and $g \in G$, and $\overline{G}$ the inner automorphism group of $B*G$ induced by $G$, that is, $\overline{g}(x) = g x g^{-1}$ for each $x \in B*G$ and $g \in G$. We note that $\overline{G}$ restricted to $B$ is $G$.

Let $A$ be a subring of a ring $B$ with the same identity 1. We denote $V_B(A)$ the commutator subring of $A$ in $B$. We call $B$ a separable extension of $A$ if there exist $\{a_i, b_i \in B, i = 1, 2, \ldots, k \}$ for some integer $k$ such that $\sum a_i b_i = 1$, and $\sum b a_i \otimes b_i = \sum a_i \otimes b b$ for all $b \in B$ where $\otimes$ is over $A$. An Azumaya algebra is a separable extension of its center. A ring $B$ is called a $H$-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. 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 $g \in G$ ([4]). Such a set \( \{a_i, b_i\} \) is called a $G$-Galois system for $B$. A Galois extension $B$ of $B^G$ is called a Galois algebra over $B^G$ if $B^G$ is contained in $C$ ([4],[9]). We called $B$ a center Galois extension with Galois group $G$ if $C$ is a Galois algebra over $C^G$ with Galois group $G|_{C^G} \cong G$ ([7],[8]), and a commutator Galois extension of $B^G$ with Galois group $G$ if $V_B(B^G)$ is a Galois extension of $(V_B(B^G))^G$ with Galois group $G|_{V_B(B^G)} \cong G$ ([10]). A Galois extension $B$ of $B^G$ with Galois group $G$ is called an Azumaya Galois extension if $B^G$ is an Azumaya $C^G$-algebra ([1],[2]). As studied in [6], $B$ is called a Galois $H$-separable extension of $B^G$ if it is a Galois and an $H$-separable extension of $B^G$.

3. Main Results

**Theorem 3.1.** Let $B$ be a commutator Galois extension of $B^G$ with Galois group $G$. Then $B$ is an Azumaya $C$-algebra if and only if $B^G$ is an Azumaya $C^G$-algebra.

**Proof.** ($\Rightarrow$) Since $B$ is a commutator Galois extension of $B^G$ with Galois group $G$, $V_B(B^G)$ is a Galois extension of $(V_B(B^G))^G$ with Galois group $G|_{V_B(B^G)} \cong G$. Noting that $V_B(B^G) \subseteq B^G \cdot V_B(B^G) \subseteq B$, we have that both $B^G \cdot V_B(B^G)$ and $B$ are Galois extensions of $B^G$ with Galois group $G|_{B^G \cdot V_B(B^G)} \cong G$. Thus $B = B^G \cdot V_B(B^G)$. Clearly, $C \subseteq V_B(B^G)$, so $B = B^G \cdot V_B(B^G) = B^G C \cdot V_B(B^G)$ such that $B^G C$ and $V_B(B^G)$ are $C$-subalgebras of the Azumaya $C$-algebra $B$. Hence, they are Azumaya $C$-algebras by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). But then the center of $B^G$ is $C^G$ (for the center of $B^G C$ is $C$). Thus, $(V_B(B^G))^G = (V_B(B^G))^G = C^G$. Therefore, $V_B(B^G)$ is a Galois algebra over $C^G$. This implies that there exists an element $c \in C$ such that $Tr_G(c) = 1$ ([5], proof of Proposition 5, page 314). Next we claim that the skew group ring $B \ast G$ is a separable extension over $B$. In fact, let $a_i = g_i$ and $b_i = c g_i^{-1}$ in $B \ast G$ for $i = 1, 2, \ldots, n$ where $G = \{g_1, g_2, \ldots, g_n\}$ for some integer $n$ and $c \in C$ such that $Tr_G(c) = 1$. Then $\sum a_i b_i = \sum g_i (c g_i^{-1}) = \sum g_i (c) = Tr_G(c) = 1$, and for all $b$ in $B$ and $g \in G$,
Therefore, \( \{ a_i = g_i; b_i = cg_i^{-1} \} \) is a separable system of \( B \ast G \) over \( B \). Thus the skew group ring \( B \ast G \) is a separable extension over \( B \). By hypothesis, \( B \) is an Azumaya \( C \)-algebra, so \( B \ast G \) is a separable \( C \)-algebra by the transitivity of separable extensions.

Since \( V_B(B^G) \) is a Galois algebra over \( C^G \) again, \( V_B(B^G) \) is finitely generated, projective, and separable over \( C^G \). But \( V_B(B^G) \) is an Azumaya \( C \)-algebra, so \( C \) is a separable \( C^G \)-algebra ([3], Theorem 3.8, page 55). Thus \( B \ast G \) is a separable \( C^G \)-algebra by the transitivity of separable extensions again. But \( B^G \equiv \text{Hom}_{B^G}(B, B) \equiv V_{\text{Hom}_{C^G}(B, B)}(B \ast G) \) where \( B \) is a progenerator \( C^G \)-module, so \( \text{Hom}_{C^G}(B, B) \) is an Azumaya \( C^G \)-algebra ([3], Proposition 4.1, page 56) containing a separable subalgebra \( B \ast G \). Thus, the commutator subalgebra \( B^G \) is also a separable \( C^G \)-algebra ([3], Theorem 4.3, page 57). Therefore \( B^G \) is an Azumaya \( C^G \)-algebra.

(\( \Leftarrow \Rightarrow \)) Since \( B \) is a Galois extension of \( B^G \), \( B \) is a separable extension of \( B^G \). By hypothesis, \( B^G \) is an Azumaya \( C^G \)-algebra, so \( B \) is a separable \( C^G \)-algebra by transitivity of separable extensions. Thus, \( B \) is an Azumaya \( C \)-algebra ([3], Theorem 3.8, page 55).

If \( B \) is a center Galois extension of \( B^G \), then \( C \) is a Galois algebra over \( C^G \) with Galois group \( G|_C \equiv G \) by the definition of a center Galois extension. But \( C \subset V_B(B^G) \), so \( V_B(B^G) \) is a Galois extension of \( V_B(B^G)^G \) with Galois group \( G|_{V_B(B^G)^G} \equiv G \) with the same Galois system as \( C \). Hence the DeMeyer's result ([4], Lemma 2) is an immediate consequence of Theorem 3.1.
Corollary 3.2. ([4], Lemma 2) Let $B$ be a center Galois extension of $B^G$ with Galois group $G$. Then $B$ is an Azumaya $C$-algebra if and only if $B^G$ is an Azumaya $C^G$-algebra.

For a general Galois extension $B$ of $B^G$ with Galois group $G$, the necessity of Theorem 3.1 is not true. A counter example can be constructed by using the following theorem.

Theorem 3.3. Let $A$ be an Azumaya Galois extension of $A^G$ with Galois group $G$ of order $n$ invertible in $A$ and $E$ the center of $A$. Then

1. $A * G$ is a Galois $H$-separable extension of $(A * G)^G$ with inner Galois group $G$, and

Proof. (1) Since $A$ is a Galois extension of $A^G$ with Galois group $G$, $A * G$ is a Galois extension of $(A * G)^G$ with an inner Galois group $G$ with the same Galois system for $A$. Thus $A * G$ is an $H$-separable extension of $(A * G)^G$ because $G$ is inner ([6], Corollary 3).

(2) Since $A$ is an Azumaya Galois extension of $A^G$ with Galois group $G$ by hypothesis, $A * G$ is an Azumaya $E^G$-algebra ([2], Theorem 1). Since $n$ is invertible in $A$, $E^G G$ is a separable $E^G$-subalgebra of the Azumaya $E^G$-algebra $A * G$. Hence $(A * G)^G = V_{A * G}(E^G G)$ is also a separable $E^G$-subalgebra of $A * G$ by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). Moreover, since $(A * G)^G$ and $E^G G$ are commutator separable subalgebras of the Azumaya $E^G$-algebra $A * G$, they have the same center. But the center of the group algebra $E^G G$ is not $E^G$, so $(A * G)^G$ is not an Azumaya $E^G$-algebra.

Theorem 3.3-(2) shows that for a Galois $H$-separable extension $B (= A * G)$ of $B^G$, $B$ is an Azumaya $C$-algebra does not necessarily implies that $B^G$ is an Azumaya $C^G$-algebra. Next, we give some equivalent conditions for $B^G$ being an Azumaya $C^G$-algebra.

Theorem 3.4. Let $B$ be a Galois $H$-separable extension of $B^G$ with Galois group $G$ of order $n$ invertible in $B$. If $B$ is an Azumaya $C$-algebra, then the following are equivalent:
(1) $B^G$ is an Azumaya $C^G$-algebra.

(2) The center of $B^G$ is $C^G$.

(3) The center of $V_B(B^G)$ is $C$.

(4) $B = B^G \cdot V_B(B^G)$.

**Proof.** (1) $\implies$ (2) It is clear.

(2) $\implies$ (3) Since $B$ is a Galois $H$-separable extension of $B^G$ with Galois group $G$, $V_B(V_B(B^G)) = B^G$ ([6], Proposition 4-(1)). This implies that $B^G$ and $V_B(B^G)$ have the same center. Thus, the center of $V_B(B^G)$ is $C^G$. But, clearly, $C$ is contained in the center of $V_B(B^G)$, so $C = C^G$.

(3) $\implies$ (1) Since $B^G$ and $V_B(B^G)$ have the same center, $C$ is also the center of $B^G$. Hence $C = C^G$. Since $B$ is a Galois $H$-separable extension and $n^{-1} \in B$, $V_B(B^G)$ is a separable $C$-algebra ([6], Proposition 4-(3), (i)$\iff$(iii)); and so $V_B(B^G)$ is an Azumaya $C$-algebra. But $B$ is an Azumaya $C$-algebra, so $B^G (= V_B(V_B(B^G)))$ is also an Azumaya $C$-algebra ([3], Theorem 4.3, page 57).

(3) $\implies$ (4) Since $B$ is a Galois $H$-separable extension of $B^G$ with Galois group $G$, $V_B(B^G) = \oplus_{g \in G} J_g$ where $J_g = \{ b \in B \mid xb = bg(x) \text{ for all } x \in B \}$ for each $g \in G$ (in particular, $J_1 = C$) ([5], Proposition 1). But, by hypothesis, $C$ is the center of $V_B(B^G)$, so $J_g$ is not contained in the center of $V_B(B^G)$ for each $g \neq 1$ in $G$. Therefore, $g|_{V_B(B^G)}$ is not an identity for each $g \neq 1$ in $G$ ([6], Proposition 5), that is, $L = \{ g \in G \mid g|_{V_B(B^G)} \text{ is an identity} \} = \{ 1 \}$. Thus, $\oplus_{g \in L} J_g = J_1 = C$, the center of $V_B(B^G)$, so $B = B^G \cdot V_B(B^G)$ ([6], Proposition 6-(3), (i)$\iff$(ii)).

(4) $\implies$ (3) Since $B^G$ and $V_B(B^G)$ have the same center, the center of $V_B(B^G)$ is also the same as the center of $B^G \cdot V_B(B^G)$. By hypothesis, $B = B^G \cdot V_B(B^G)$, so the center of $V_B(B^G)$ is $C$. 

6
The following theorem gives an equivalent condition under which a commutator Galois extension is a center Galois extension.

**Theorem 3.5.** Let $B$ be a commutator Galois extension with Galois group $G$. Then $B$ is a center Galois extension of $B^G$ if and only if $V_B(B^G)$ is commutative.

**Proof.** ($\Rightarrow$) Since $B$ is a center Galois extension of $B^G$, $C$ is a Galois algebra over $C^G$ with Galois group $G|C \cong G$. Hence $B$ and $B^G C$ are Galois extension of $B^G$ with the same Galois system for $C$. Thus, $B = B^G C$, and so $V_B(B^G) = V_B(B^G C) = V_B(B) = C$, a commutative ring.

($\Leftarrow$) Since $V_B(B^G)$ is a Galois extension of $(V_B(B^G))^G$ with Galois group $G|V_B(B^G) \cong G$, $B$ and $B^G \cdot V_B(B^G)$ are Galois extensions of $B^G$ with the same Galois system for $V_B(B^G)$. Thus, $B = B^G \cdot V_B(B^G)$. By hypothesis, $V_B(B^G)$ is a commutative ring, so $V_B(B^G) = V_B(B^G \cdot V_B(B^G)) = V_B(B) = C$. Therefore, $B$ is a center Galois extension of $B^G$.

We conclude this paper with two examples to demonstrate our results in Theorem 3.1 and Theorem 3.3, and to illustrate that a commutator Galois extension is not necessarily a center Galois extension.

**Example 1.** Let $A = Q[i, j, k]$ be the quaternion algebra over the rational field $Q$, $B = M_2(Q) \otimes_Q A$ where $M_2(Q)$ is the matrix ring of order 2 over the rational field $Q$, and $G = \{1 \otimes_Q 1, 1 \otimes_Q g_i, 1 \otimes_Q g_j, 1 \otimes_Q g_k\}$ where $g_i(x) = ixi^{-1}$, $g_j(x) = jxj^{-1}$, and $g_k(x) = kxk^{-1}$ for all $x$ in $Q[i, j, k]$. Then

1. $B^G = M_2(Q) \otimes_Q Q \cong M_2(Q)$.
2. The center $C$ of $B$ is $Q \otimes_Q Q \cong Q$.
3. $B$ is a Galois extension of $B^G$ with Galois group $G$ with a Galois system.
\{1 \otimes 1, 1 \otimes i, 1 \otimes j, 1 \otimes k; \frac{1}{4} \otimes 1, -\frac{1}{4} \otimes i, -\frac{1}{4} \otimes j, -\frac{1}{4} \otimes k\}.

(4) \( V_B(B^G) = Q \otimes Q \cong A \), and so \( V_B(B^G) \) is a Galois extension with Galois group \( G_{V_B(B^G)} \cong G \) with the same Galois system given in (3) and \( V_B(B^G) \neq C \).

(5) \( B \) is an Azumaya \( C \)-algebra.

(6) \( B^G \) is an Azumaya \( C^G \)-algebra.

(7) \( V_B(B^G) \) is not commutative.

(8) \( B \) is not a center Galois extension of \( B^G \) with Galois group \( G \) by Theorem 3.5.

Example 2. Let \( A = M_2(C) \) be the matrix ring of order 2 over the field of complex numbers \( C \) and \( G = \{1, g\} \) with \( g((c_{ij})) = (\overline{c_{ij}}) \) where \( \overline{c_{ij}} \) is the conjugate of \( c_{ij} \) in \( C \).

Then,

(1) \( A \) is a Galois extension of \( A^G \) with Galois group \( G \) with a Galois system \( \{a_1 = I, a_2 = iI; b_1 = \frac{1}{2}I, b_2 = -\frac{1}{2}I\} \), that is, \( a_1b_1 + a_2b_2 = I \) and \( a_1g(b_1) + a_2g(b_2) = 0 \), where \( I \) is the identity of \( M_2(C) \), \( 0 \) is the zero matrix in \( M_2(C) \), and \( i \) is the complex unit.

(2) \( A^G = M_2(R) \), the matrix ring of order 2 over the field of real numbers \( R \).

(3) The center of \( A \) is \( C \).

(4) \( C^G = R \).

(5) \( A^G \) is an Azumaya \( R \)-algebra.

(6) By (1) and (5), \( A \) is an Azumaya Galois extension of \( A^G \).

(7) By Theorem 3.3, \( A \ast G \) is a Galois \( H \)-separable extension of \( (A \ast G)^G \) with inner Galois group \( \overline{G} \).

(8) \( A \ast G \) is an Azumaya \( R \)-algebra.

(9) \( (A \ast G)^G \) (\( = M_2(R) \oplus M_2(R)g \)) has center \( R \oplus Rg \), so \( (A \ast G)^G \) is not an Azumaya \( R \)-algebra.
Acknowledgement. The author would like to thank Professor George Szeto for many useful suggestions and discussions. 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


