On Characterizations of a Center Galois Extension

by

George Szeto and Lianyong Xue

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 \( B \) is a center Galois extension of \( B^G \) (that is, \( C \) is a Galois algebra over \( C^G \) with Galois group \( G|_C \cong G \)) if and only if the ideal of \( B \) generated by \( \{ c - g(c) \mid c \in C \} \) is \( B \) for each \( g \neq 1 \) in \( G \). This generalizes the well known characterization of a commutative Galois extension \( C \) that \( C \) is a Galois extension of \( C^G \) with Galois group \( G \) if and only if the ideal generated by \( \{ c - g(c) \mid c \in C \} \) is \( C \) for each \( g \neq 1 \) in \( G \). Some more characterizations of a center Galois extension \( B \) are also given.

Key Words and Phrases. Galois extensions, Center Galois extensions, Central extensions, Galois central extensions, Azumaya algebras, Separable extensions, and \( H \)-separable extensions.

AMS 1991 Subject Classification Codes: 16S30; 16W20

1. Introduction. Let \( C \) be a commutative ring with 1, \( G \) a finite automorphism group of \( C \), and \( C^G \) the set of elements in \( C \) fixed under each element in \( G \). It is well known that a commutative Galois extension \( C \) is characterized in terms of the ideals generated by \( \{ c - g(c) \mid c \in C \} \) for \( g \neq 1 \) in \( G \), that is, \( C \) is a Galois extension with Galois group \( G \) if and only if the ideal generated by \( \{ c - g(c) \mid c \in C \} \) is \( C \) for each \( g \neq 1 \) in \( G \) ([3], Proposition 1.2, p.80). A natural generalization of a commutative Galois extension is the notion of a center Galois extension, that is, a noncommutative ring \( B \) with a finite automorphism group \( G \) and center \( C \) is called a center Galois extension of \( B^G \) with Galois group \( G \) if \( C \) is a Galois extension of \( C^G \) with Galois group \( G|_C \cong G \). S. Ikeda ([4],[5]) characterized a center Galois extension with a cyclic Galois group \( G \) of prime order in terms of a skew
polynomial ring. Then, the present authors generalized the Ikeda characterization to center Galois extensions with Galois group $G$ of any cyclic order ([7]) and to center Galois extensions with any finite Galois group $G$ ([8]). The purpose of the present paper is to generalize the above characterization of a commutative Galois extension to a center Galois extension. We shall show that $B$ is a center Galois extension of $B^G$ if and only if the ideal of $B$ generated by $\{e - g(c) \mid c \in C\}$ is $B$ for each $g \neq 1$ in $G$. A center Galois extension $B$ is also equivalent to each of the following statements: (i) $B$ is a Galois central extension of $B^G$, that is, $B = B^G C$ which is a $G$-Galois extension of $B^G$. (ii) $B$ is a Galois extension of $B^G$ with a Galois system $\{b_i \in B, a_i \in C, i = 1, 2, ..., m\}$ for some integer $m$, and (iii) the ideal of the subring $B^G C$ generated by $\{e - g(c) \mid c \in C\}$ is $B^G C$ for each $g \neq 1$ in $G$.

2. Definitions and Notations. Throughout this paper, $B$ will represent a ring with 1, $G = \{g_1 = 1, g_2, \cdots, g_n\}$ an automorphism group of $B$ of order $n$ for some integer $n$, $C$ the center of $B$, $B^G$ the set of elements in $B$ fixed under each element in $G$, and $B \ast G$ a skew group ring in which the multiplication is given by $gb = g(b)g$ for $b \in B$ and $g \in G$.

$B$ is called a $G$-Galois extension of $B^G$ if there exist elements $\{a_i, b_i \in B, i = 1, 2, ..., m\}$ for some integer $m$ such that $\sum_{i=1}^{m} a_i g(b_i) = \delta_{i,j}$. Such a set $\{a_i, b_i\}$ is called a $G$-Galois system for $B$. $B$ is called a center Galois extension of $B^G$ if $C$ is a Galois algebra over $C^G$ with Galois group $G|C \equiv G$. $B$ is called a central extension of $B^G$ if $B = B^G C$, and $B$ is called a Galois central extension of $B^G$ if $B = B^G C$ is a Galois extension of $B^G$ with Galois group $G$.

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 $\{a_i, b_i \in B, i = 1, 2, ..., m\}$ for some integer $m$ such that $\sum a_i b_i = 1$, and $\sum b_i \otimes b_i = \sum a_i \otimes b_i b$ for all $b$ in $B$ where $\otimes$ is over $A$. $B$ 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. $B$ is called centrally projective over $A$ if $B$ is a direct summand of a finite direct sum of $A$ as a $A$-bimodule.

3. The Characterizations. In this section, we denote $J_j^{(C)} = \{e - g_j(c) \mid c \in C\}$. We shall show that $B$ is a center Galois extension of $B^G$ if and only if $B = B J_j^{(C)}$,
the ideal of $B$ generated by $J_j^{(C)}$, for each $g_j \neq 1$ in $G$. Some more characterizations of a center Galois extension $B$ are also given. We begin with a lemma.

**Lemma 3.1.** If $B = BJ_j^{(C)}$ for each $g_j \neq 1$ in $G$ (that is, $j \neq 1$), then

1. $B$ is a Galois extension of $B^G$ with Galois group $G$ and a Galois system $\{b_i \in B; c_i \in C, i = 1, 2, \ldots, m\}$ for some integer $m$.
2. $B$ is centrally projective over $B^G$.
3. $B \ast G$ is $H$-separable over $B$.
4. $V_{B^G}(B) = C$.

**Proof.** (1) Since $B = BJ_j^{(C)}$ for each $j \neq 1$ in $G$, there exist $\{b_i^{(j)} \in B, c_i^{(j)} \in C, i = 1, 2, \ldots, m_j\}$ for some integer $m_j$, $j = 2, 3, \ldots, n$ such that $\sum_{i=1}^{m_j} b_i^{(j)} c_i^{(j)} - g_j(c_i^{(j)}) = 1$. Therefore, $\sum_{i=1}^{m_j} b_i^{(j)} c_i^{(j)} = 1 + \sum_{i=1}^{m_j} b_i^{(j)} g_j(c_i^{(j)})$. Let $b_i^{(j)} = -\sum_{i=1}^{m_j} b_i^{(j)} g_j(c_i^{(j)})$ and $c_i^{(j)} + 1 = 1$. Then $\sum_{i=1}^{m_j+1} b_i^{(j)} c_i^{(j)} = 1$ and $\sum_{i=1}^{m_j+1} b_i^{(j)} g_j(c_i^{(j)}) = 0$. Let $b_{i_2, i_3, \ldots, i_s} = b_i^{(2)} b_i^{(3)} \cdots b_i^{(n)}$ and $c_{i_2, i_3, \ldots, i_s} = c_i^{(2)} c_i^{(3)} \cdots c_i^{(n)}$ for $i_j = 1, 2, \ldots, m_j + 1$ and $j = 2, 3, \ldots, n$. Then

\[
\sum_{i_2=1}^{m_2+1} \sum_{i_3=1}^{m_3+1} \cdots \sum_{i_s=1}^{m_s+1} b_{i_2, i_3, \ldots, i_s} c_{i_2, i_3, \ldots, i_s}
\]

\[
= \sum_{i_2=1}^{m_2+1} \sum_{i_3=1}^{m_3+1} \cdots \sum_{i_s=1}^{m_s+1} b_{i_2}^{(2)} b_{i_3}^{(3)} \cdots b_{i_s}^{(n)} c_{i_2}^{(2)} c_{i_3}^{(3)} \cdots c_{i_s}^{(n)}
\]

\[
= \sum_{i_2=1}^{m_2+1} \sum_{i_3=1}^{m_3+1} \cdots \sum_{i_s=1}^{m_s+1} b_{i_2}^{(2)} c_{i_2}^{(3)} \cdots c_{i_s}^{(n)}
\]

\[
= 1
\]

and for each $j \neq 1$

\[
\sum_{i_2=1}^{m_2+1} \sum_{i_3=1}^{m_3+1} \cdots \sum_{i_s=1}^{m_s+1} b_{i_2, i_3, \ldots, i_s} g_j(c_{i_2, i_3, \ldots, i_s})
\]

\[
= \sum_{i_2=1}^{m_2+1} \sum_{i_3=1}^{m_3+1} \cdots \sum_{i_s=1}^{m_s+1} b_{i_2}^{(2)} c_{i_2}^{(3)} \cdots c_{i_s}^{(n)}
\]

\[
= \sum_{i_2=1}^{m_2+1} \sum_{i_3=1}^{m_3+1} \cdots \sum_{i_s=1}^{m_s+1} b_{i_2}^{(2)} c_{i_2}^{(3)} \cdots c_{i_s}^{(n)}
\]

3
Thus, \( b_{i_2,i_3,\ldots,i_n} \in B; c_{i_2,i_3,\ldots,i_n} \in C, i_j = 1, 2, \ldots, m_j + 1 \) and \( j = 2, 3, \ldots n \) is a Galois system for \( B \). This completes the proof of (1).

(2) By (1), \( B \) is a Galois extension of \( B^G \) with a Galois system \( \{ b_i \in B, c_i \in C, i = 1, 2, \ldots, m \} \) for some integer \( m \). Let \( f_i : B \rightarrow B^G \) given by \( f_i(b) = \sum_{j=1}^{m} g_j(c_i b) \) for all \( b \in B, i = 1, 2, \ldots, m \). Then, it is easy to check that \( f_i \) is a homomorphism as \( B^G \)-bimodule and \( b = \sum_{i=1}^{m} b_i c_i b = \sum_{i=1}^{m} b_i g_j(c_i) g_j(b) = \sum_{i=1}^{m} b_i \sum_{j=1}^{m} g_j(c_i b) = \sum_{i=1}^{m} b_i f_i(b) \) for all \( b \in B \). Hence \( \{ b_i, f_i, i = 1, 2, \ldots, m \} \) is a dual bases for \( B \) as \( B^G \)-bimodule, and so \( B \) is finitely generated and projective as \( B^G \)-bimodule. Therefore, \( B \) is a direct summand of a finite direct sum of \( B^G \) as a \( B^G \)-bimodule. Thus \( B \) is centrally projective over \( B^G \).

(3) By (1), \( B \) is a Galois extension of \( B^G \) with Galois group \( G \). Hence \( B \ast G \cong \text{Hom}_{B^G}(B, B) \) ([2], Theorem 1). By (2), \( B \) is centrally projective over \( B^G \). Thus, \( B \ast G \) (\( \cong \text{Hom}_{B^G}(B, B) \)) is \( H \)-separable over \( B \) ([6], Proposition 11).

(4) We first claim that \( V_{B^G}(C) = B \). Clearly, \( B \subseteq V_{B^G}(C) \). Let \( \sum_{j=1}^{n} b_j g_j \) in \( V_{B^G}(C) \) for some \( b_j \in B \). Then \( e(\sum_{j=1}^{n} b_j g_j) = (\sum_{j=1}^{n} b_j g_j) e \) for each \( e \) in \( C \), so \( eb_j = b_j g_j(e) \), that is, \( b_j(e - g_j(e)) = 0 \) for each \( g_j \in G \) and \( e \in C \). Since \( B = B J_1(C) \) for each \( g_j \neq 1 \), there exist \( b_j^{(j)} \in B \) and \( c_i^{(j)} \in C \), \( i = 1, 2, \ldots, m \) such that \( \sum_{i=1}^{m} b_j^{(j)} c_i^{(j)} = 0 \) for each \( g_j \). This implies that \( \sum_{j=1}^{n} b_j g_j = b_1 \in B \). Hence \( V_{B^G}(C) \subseteq B \), and so \( V_{B^G}(C) = B \). Therefore, \( V_{B^G}(B) \subseteq V_{B^G}(C) = B \). Thus \( V_{B^G}(B) = V_B(B) = C \).

We now show some characterizations of a center Galois extension \( B \).

**THEOREM 3.2.** The following statements are equivalent.

(1) \( B \) is a center Galois extension of \( B^G \).

(2) \( B = B J_{j}^{(C)} \) for each \( g_j \neq 1 \) in \( G \).

(3) \( B \) is a Galois extension of \( B^G \) with a Galois system \( \{ b_i \in B, c_i \in C, i = 1, 2, \ldots, m \} \) for some integer \( m \).
(4) $B$ is a Galois central extension of $B^G$.

(5) $B^G C = B^G C J_j^{(C)}$ for each $g_j \neq 1$ in $G$.

PROOF. (1) $\Rightarrow$ (2) By hypothesis, $C$ is a Galois extension of $C^G$ with Galois group $G|C \cong G$. Hence $C = C J_j^{(C)}$ for each $g_j \neq 1$ in $G$ ([3], Proposition 1.2, p.80). Thus, $B = B J_j^{(C)}$ for each $g_j \neq 1$ in $G$.

(2) $\Rightarrow$ (1) Since $B = B J_j^{(C)}$ for each $g_j \neq 1$ in $G$, $B \ast G$ is $H$-separable over $B$ by Lemma 3.1-(3) and $V_{B \ast G}(B) = C$ by Lemma 3.1-(4). Thus, $C$ is a Galois extension of $C^G$ with Galois group $G|C \cong G$ by ([1], Proposition 4).

(1) $\Rightarrow$ (3) This is Lemma 3.1-(1).

(3) $\Rightarrow$ (1) Since $B$ is a Galois extension of $B^G$ with a Galois system $\{b_i \in B, c_i \in C, i = 1, 2, \ldots, m\}$ for some integer $m$, we have $\sum_{i=1}^{m} b_i g_j (c_i) = \delta_{1,j}$. Hence $\sum_{i=1}^{m} b_i (c_i - g_j (c_i)) = 1$ for each $g_j \neq 1$ in $G$. So for every $b \in B$, $b = \sum_{i=1}^{m} b_i (c_i - g_j (c_i)) \in B J_j^{(C)}$. Therefore, $B = B J_j^{(C)}$ for each $g_j \neq 1$ in $G$. Thus, $B$ is a center Galois extension of $B^G$ by (2) $\Rightarrow$ (1).

(1) $\Rightarrow$ (4) Since $C$ is a Galois algebra with Galois group $G|C \cong G$, $B$ and $B^G C$ are Galois extensions of $B^G$ with Galois group $G|B \ast C \cong G$. Noting that $B^G C \subset B$, we have $B = B^G C$, that is, $B$ is a central extension of $B^G$. But $B$ is a Galois extension of $B^G$, so $B$ is a Galois central extension of $B^G$.

(4) $\Rightarrow$ (1) By hypothesis, $B = B^G C$ is a Galois extension of $B^G$. Hence there exists a Galois system $\{a_i; b_k \in B, i = 1, 2, \ldots, m\}$ for some integer $m$ such that $\sum_{i=1}^{m} a_i g_j (b_k) = \delta_{1,j}$ But $B = B^G C$, so $a_i = \sum_{k=1}^{m} b_k^{(a_i)} c_k^{(a_i)}$ and $b_k = \sum_{l=1}^{n_k} b_l^{(a_i)} c_l^{(a_i)}$ for some $b_k^{(a_i)}, c_k^{(a_i)}$ in $B^G$ and $a_i^{(a_i)}, c_i^{(a_i)}$ in $C$, $k = 1, 2, \ldots, n_k$, $i = 1, 2, \ldots, m$. Therefore,

$$
\delta_{1,j} = \sum_{i=1}^{m} a_i g_j (b_k) = \sum_{i=1}^{m} \sum_{k=1}^{n_k} b_k^{(a_i)} c_k^{(a_i)} g_j (b_k^{(a_i)} c_l^{(a_i)}) = \sum_{i=1}^{m} \sum_{k=1}^{n_k} b_k^{(a_i)} c_k^{(a_i)} \sum_{l=1}^{n_k} b_l^{(a_i)} c_l^{(a_i)} g_j (c_l^{(a_i)}) = \sum_{i=1}^{m} \sum_{k=1}^{n_k} b_k^{(a_i)} c_k^{(a_i)} \sum_{l=1}^{n_k} b_l^{(a_i)} c_l^{(a_i)} g_j (c_l^{(a_i)}).
$$

This shows that $\{b_k^{(a_i)}, c_k^{(a_i)} \in B; c_k^{(a_i)} = c_i^{(a_i)} \in C, k = 1, 2, \ldots, n_k, i = 1, 2, \ldots, m\}$ is a Galois system for $B$. Thus, $B$ is a center Galois extension of $B^G$ by (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (5) Since $B$ is a center Galois extension of $B^G$, $B = B J_j^{(C)}$ for each $g_j \neq 1$ in $G$ by (1) $\Rightarrow$ (2) and $B = B^G C$ by (1) $\Rightarrow$ (4). Thus, $B^G C = B^G C J_j^{(C)}$ for each $g_j \neq 1$ in $G$. 5
(5) $\implies$ (1) Since $B^G C = B^G C J_j^{(C)}$ for each $g_j \neq 1$ in $G$, $B = B J_j^{(C)}$ for each $g_j \neq 1$ in $G$. Thus, $B$ is a center Galois extension of $B^G$ by (2) $\implies$ (1).

The characterization of a commutative Galois extension $C$ in terms of the ideals generated by \{c - g(c) | c \in C\} for $g \neq 1$ in $G$ is an immediate consequence of Theorem 3.2.

**COROLLARY 3.3.** A commutative ring $C$ is a Galois extension of $C^G$ if and only if $C = C J_j^{(C)}$, the ideal generated by \{c - g_j(c) | c \in C\} is $C$ for each $g_j \neq 1$ in $G$.

**PROOF.** Let $B = C$ in Theorem 3.2. Then, the corollary is an immediate consequence of Theorem 3.2-(2).

By Theorem 3.2, we derive several characterizations of a Galois central extension $B$.

**COROLLARY 3.4.** If $B$ is a central extension of $B^G$ (that is, $B = B^G C$), then the following statements are equivalent.

1. $B$ is a Galois extension of $B^G$.
2. $B$ is a center Galois extension of $B^G$.
3. $B * G$ is H-separable over $B$.
4. $B = C J_j^{(B)}$ for each $g_j \neq 1$ in $G$.
5. $B = B J_j^{(B)}$ for each $g_j \neq 1$ in $G$.

**PROOF.** (1) $\iff$ (2) This is given by (1) $\iff$ (4) in Theorem 3.2.
3. $\implies$ (1) This is Lemma 3.1-(3).

Since $B = B^G C$ by hypothesis, it is easy to see that $J_j^{(B)} = B^G J_j^{(C)}$ for each $g_j$ in $G$. Thus, $B = C J_j^{(B)}$, $B = B J_j^{(B)}$, and $B = B J_j^{(C)}$ are equivalent. This implies that (2) $\iff$ (4) $\iff$ (5) by Theorem 3.2-(2).

We call a ring $B$ the DeMeyer-Kanzaki Galois extension of $B^G$ if $B$ is an Azumaya $C$-algebra and $B$ is a center Galois extension of $B^G$ (for more about the DeMeyer-Kanzaki
Galois extensions, see [2]). Clearly, the class of center Galois extensions is broader than the class of the DeMey er-Kanzaki Galois extensions. We conclude the present paper with two examples. (1) the DeMey er-Kanzaki Galois extension of $B^G$ and (2) a center Galois extension of $B^G$, but not the DeMey er-Kanzaki Galois extension of $B^G$.

**EXAMPLE 1.** Let $C$ be the field of complex numbers, that is, $C = R + R\sqrt{-1}$ where $R$ is the field of real numbers, $B = C[i, j, k]$ the quaternion algebra over $C$, and $G = \{1, g \mid g(c_1 + c_i + c_j + c_k) = g(c_1) + g(c_i)i + g(c_j)j + g(c_k)k \text{ for each } b = c_1 + c_i + c_j + c_k \in C[i, j, k] \}$ and $g(u + v\sqrt{-1}) = u - v\sqrt{-1}$ for each $c = u + v\sqrt{-1} \in C$. Then

(1) The center of $B$ is $C$.

(2) $B$ is an Azumaya $C$-algebra.

(3) $C$ is a Galois extension of $C^G$ with Galois group $G|_C \cong G$ and a Galois system

$$
\begin{align*}
\{a_1 = \frac{1}{\sqrt{2}}, a_2 = \frac{1}{\sqrt{2}}\sqrt{-1}, b_1 = \frac{1}{\sqrt{2}}, b_2 = -\frac{1}{\sqrt{2}}\sqrt{-1}\}.
\end{align*}
$$

(4) $B$ is the DeMey er-Kanzaki Galois extension of $B^G$ by (2) and (3).

(5) $B^G = R[i, j, k]$.

(6) $B = B^GC$, so $B$ is a central extension of $B^G$.

(7) $J^C_g = R\sqrt{-1}$.

(8) $B = B J^C_g$ since $1 = -\sqrt{-1}\sqrt{-1} \in B J^C_g$.

(9) $J^B_g = R\sqrt{-1} + R\sqrt{-1}i + R\sqrt{-1}j + R\sqrt{-1}k$.

(10) $B = C J^B_g$.

**EXAMPLE 2.** By replacing in Example 1 the field of complex numbers $C$ with the ring $C = Z \oplus Z$ where $Z$ is the ring of integers, $g(a, b) = (b, a)$ for all $(a, b) \in C$, and $G = \{1, g \mid g(c_1 + c_i + c_j + c_k) = g(c_1) + g(c_i)i + g(c_j)j + g(c_k)k \text{ for each } b = c_1 + c_i + c_j + c_k \in B = C[i, j, k] \}$. Then

(1) The center of $B$ is $C$.

(2) $C$ is a Galois extension of $C^G$ with Galois group $G|_C \cong G$ and a Galois system

$$
\begin{align*}
\{a_1 = (1, 0), a_2 = (0, 1); b_1 = (1, 0), b_2 = (0, 1)\}.
\end{align*}
$$

(3) $B$ is not an Azumaya $C$-algebra (for $\frac{1}{2} \notin C$), and so $B$ is not the DeMey er-Kanzaki Galois extension of $B^G$.

(4) $C^G = \{(a, a) \mid a \in Z\} = Z$

(5) $B^G = C^G[i, j, k]$.
(6) $B = B^G C$, so $B$ is a central extension of $B^G$.
(7) $J_g(C) = \{(a, -a) | a \in Z\} = Z(1, -1)$.
(8) $B = B J_g(C)$ since $1 = (1, 1) = (1, -1)(1, -1) \in B J_g(C)$.
(9) $J_g(B) = Z(1, -1) + Z(1, -1)i + Z(1, -1)j + Z(1, -1)k$.
(10) $B = C J_g(B)$.

References


George Szeto and Lianyong Xue
Department of Mathematics, Bradley University
Peoria, Illinois 61625 – U.S.A.
Email: szeto@bradley.bradley.edu and lxue@bradley.bradley.edu

8