On the Injective Galois Map

Xiaolong Jiang

Department of Mathematics
Zhongshan University
Guangzhou, 510257, P.R. China
mcsjxl@mail.sysu.edu.cn

George Szeto

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

Abstract

Let \( B \) be a Galois extension of \( B^G \) with Galois group \( G \), and \( \alpha : H \rightarrow B^H \) the Galois map from the set of subgroups of \( G \) to the set of subextensions of \( B^G \). Then a sufficient condition on a set with a maximal number of subgroups is given under which \( \alpha \) is one-to-one on the set. Moreover, the collection of such sets of subgroups is computed, and thus we can determine which Galois group \( H \) is unique for the Galois extension \( B \) over \( B^H \).

Mathematics Subject Classification: 16S35, 16W20

Keywords: Galois extensions, Separable extensions, Azumaya algebras, Galois map.

1 Introduction

The Galois theory for rings has been intensively investigated ([1], [2], [3], [4], [6], [7], [8]). The fundamental theorem was generalized from Galois extensions for fields to commutative rings and to commutative partial Galois extensions ([1], [3], [7], [9], [10]). Let \( B \) be a ring Galois extension of \( B^G \) with Galois group \( G \), \( C \) is the center of \( B \), \( J_g = \{ b \in B \mid bx = g(x)b \text{ for each } x \in B \} \) for \( g \in G \), and \( V_B(B^G) \) the commutator subring of \( B^G \) in \( B \). Then \( V_B(B^G) = \oplus \sum_{g \in G} J_g \) ([5], Proposition 1). We note that \( J_g = \{0\} \) for each \( g \neq 1 \in G \) when \( B \)
is commutative. But \( J_g \) may not be \( \{0\} \) for a \( g \neq 1 \in G \) when \( B \) is non-commutative. Recently, it was shown ([9], Theorem 3.4) that if \( B \) is a Galois extension of \( B^G \) with Galois group \( G \) such that \( J_g \neq \{0\} \) for each \( g \in G \), then the Galois map \( \alpha : H \rightarrow B^H \) is one-to-one. This implies that \( \alpha \) is one-to-one for all central Galois algebras ([2]) and Hirata separable Galois extensions ([6]). Observing that \( J_g = \{0\} \) for some \( g \in G \) for a Galois extension, we shall give a collection of sets \( \mathcal{F} \) of subgroups such that each \( \mathcal{F} \) is a set of maximal number of subgroups satisfying some condition on which \( \alpha \) is one-to-one. This generalizes the above result as given in [9] to a Galois extension with some \( J_g = \{0\} \). Also, our result leads to a sufficient condition for the uniqueness of Galois group for a Galois extension.

2 Preliminaries

Throughout this paper, we call \( B \) a Galois extension of \( B^G \) with Galois group \( G \) if \( B \) is a ring with 1 and \( G \) a finite automorphism group of \( B \) such that there exist \( \{a_i, b_i \in B \mid \sum_{i=1}^{m} a_i g(b_i) = \delta_{1g} \text{ for some integer } m\} \) where \( B^G \) is the set of elements in \( B \) fixed under each element in \( G \). Let \( A \) be a ring extension of \( D \). Then \( A \) is called a separable extension of \( D \) if the multiplication map \( A \otimes_D A \rightarrow A \) splits as an \( A \)-bimodule homomorphism, and \( A \) is an Azumaya algebra over \( C \) if \( A \) is a separable extension of its center \( C \). For more about Galois extensions, separable extensions, and Azumaya algebras, see [3].

3 The Injective Galois Map

In this section, let \( B \) be a Galois extension of \( B^G \) with Galois group \( G \), \( C \) is the center of \( B \), \( J_g = \{b \in B \mid bx = g(x)b \text{ for each } x \in B\} \) for each \( g \in G \). For a subgroup \( H \) of \( G \), let \( S_H = \{g \in H \mid J_g \neq \{0\}\} \) and \( T_H = \{g \in H \mid J_g = \{0\}\} \). We shall give a set \( \mathcal{F} \) with a maximal number of subgroups such that the Galois map \( \alpha \) is one-to-one on \( \mathcal{F} \). We begin with two important properties of \( C \)-modules \( \{J_g \mid g \in S_G\} \).

Lemma 3.1 ([5], Proposition 1) Let \( B \) be a Galois extension of \( B^G \) with Galois group \( G \) and \( V_B(B^G) \) the commutator subring of \( B^G \) in \( B \). Then \( V_B(B^G) = \bigoplus_{g \in G} J_g \).

Lemma 3.2 Let \( D \subset S_G \) and \( \beta : D \rightarrow \bigoplus_{g \in D} J_g \). Then \( \beta \) is one-to-one from the set of subsets \( D \) of \( S_G \) to the set \( \{\bigoplus_{g \in D} J_g \mid D \subset S_G\} \).

Proof. By Lemma 3.2 in [9], \( \beta \) is one-to-one on the set \( \{D = \{g\} \mid g \in S_G\} \). Next, let \( D, E \subset S_G \) such that \( \beta(D) = \beta(E) \). Then \( \bigoplus_{d \in D} J_d = \bigoplus_{e \in E} J_e \). Assume there exists some \( d \in D \) but not in \( E \). Then \( J_d \cap \bigoplus_{e \in E} J_e = \{0\} \).
Thus statement (1) holds.

Hence $J_d \not\subset \sum_{e \in E} J_e$; and so $\sum_{d \in D} J_d \neq \sum_{e \in E} J_e$. This contradiction implies that $D \subset E$. Similarly $E \subset D$. Thus $D = E$. Therefore $\beta$ is one-to-one.

Next we give a collection of sets $\mathcal{F}$ with a maximal number of subgroups of $G$ such that $\alpha$ is one-to-one on $\mathcal{F}$.

**Theorem 3.3** Let $\mathcal{F}$ be a set with a maximal number of subgroups of $G$ such that $S_{H'} \neq S_{H''}$ for $H' \neq H'' \in \mathcal{F}$. Then $\alpha$ is one-to-one on $\mathcal{F}$.

**Proof.** Let $H'$ and $H'' \in \mathcal{F}$ such that $\alpha(H') = \alpha(H'')$. Then $B^{H'} = B^{H''}$. Hence $V_B(B^{H'}) = V_B(B^{H''})$; that is, $\sum_{h \in S_{H'}} J_h = \sum_{h \in S_{H''}} J_h$ by Lemma 3.1 because $B$ is a Galois extension of $B^{H'} (= B^{H''})$ with Galois groups $H'$ and $H''$. Thus $S_{H'} = S_{H''}$ by Lemma 3.2. But then $H' = H''$ by the definition of $\mathcal{F}$. This shows that $\alpha$ is one-to-one on $\mathcal{F}$.

The following is a set of minimal subgroups as given in Theorem 3.3.

**Theorem 3.4** Let $D \subset S_G$, $<D>$ the subgroup generated by the elements in $D$, and $\mathcal{F}_0 = \{<D>|D \subset S_G\}$. Then (1) $\mathcal{F}_0 = \{<S_H>|H \text{ is a subgroup of } G\}$, (2) $\mathcal{F}_0$ is a set with a maximal number of subgroups of $G$ such that $S_{<D>} \neq S_{<E>}$ for $<D> \neq <E>$ where $D, E \subset S_G$. (that is, $\mathcal{F}_0$ is one of $\mathcal{F}$ with a maximal number of subgroups of $G$ as given in Theorem 3.3), and (3) Let $|\mathcal{F}|$ be the number of subgroups in $\mathcal{F}$. Then $|\mathcal{F}_0| = |\mathcal{F}|$.

**Proof.** (1) For each subgroup $H$, since $S_H \subset S_G$, $<S_H> \in \mathcal{F}_0$. Conversely, for any $<D> \in \mathcal{F}_0$, $S_{<D>} \subset <D>$, so $<S_{<D>}> = <D>$. Noting that $<D>$ is a subgroup of $G$, we have $\mathcal{F}_0 \subset \{<S_H>|H \text{ is a subgroup of } G\}$. Thus statement (1) holds.

(2) Since $D \subset S_{<D>}$, $<S_{<D>}> = <D>$ for any $D \subset S_G$. Hence $S_{<D>} \neq S_{<E>}$ for $<D> \neq <E>$. It remains to show that $\mathcal{F}_0$ has a maximal number of subgroups of $G$ satisfying the above property. Since $S_H \subset S_G$ for any subgroup $H$, $H \notin \mathcal{F}_0$ unless $H = <S_H>$. Thus $\mathcal{F}_0$ is one of $\mathcal{F}$ as given in Theorem 3.3.

(3) Let $\mathcal{F}$ be a set with a maximal number of subgroups of $G$ such that $S_H \neq S_L$ for $H \neq L \in \mathcal{F}$. We define a map $f : \mathcal{F} \rightarrow \mathcal{F}_0$ by $f(H) = <S_H>$. We claim that $f$ is one-to-one and onto. In fact, let $f(H) = f(L)$ for $H, L \in \mathcal{F}$; then $<S_H> = <S_L>$. Thus $S_{<S_H>} = S_{<S_L>}$. Since $S_H = S_{<S_H>}$ and $S_L = S_{<S_L>}$, $S_H = S_L$. But then $H = L$ by the definition of $\mathcal{F}$. Also by part (1), $f$ is onto. Therefore $|\mathcal{F}_0| = |\mathcal{F}|$.

By Theorem 3.4, we shall compute the number of $\mathcal{F}$ as given in Theorem 3.3. Let $\mathcal{C} = \{D|D \subset S_G\}$ and $\mathcal{D} = \{H|H \text{ is a subgroup of } G\}$. Define a
relation \sim \text{ on } \mathcal{C} by \, D \sim E \text{ if } < D > = < E > \text{ for } D, E \in \mathcal{C}, \text{ and } \approx \text{ on } \mathcal{D} \text{ by } H \approx L \text{ if } S_H = S_L. \text{ Then it is clear that both } \sim \text{ and } \approx \text{ are equivalent relations. Denote the equivalent class of } D \text{ by } [D] \text{ for } D \in \mathcal{C}, \text{ and the equivalent class of } H \text{ by } \mathcal{H} \text{ for } H \in \mathcal{D}. \text{ Then } \mathcal{C} = \cup_{D \in \mathcal{S}_G} [D] \text{ and } \mathcal{D} = \mathcal{H} \text{ for } H \in \mathcal{D}. \text{ We count the number of } \mathcal{F} \text{ as given in Theorem 3.3.}

\textbf{Theorem 3.5} (1) \, |\mathcal{F}_0| = \text{ the number of } \{|[D]| [D] \subset S_G\} \text{ and (2) Let } |\mathcal{H}| \text{ be the number of subgroups in } \mathcal{H} \text{ for a subgroup } H. \text{ Then the number of } \mathcal{F} \text{ as given in Theorem 3.3} = \prod_{<D> \in \mathcal{F}_0} <D>, \text{ a product of } |<D>| \text{ for } <D> \in \mathcal{F}_0.

\textbf{Proof.} (1) \text{ Since } \mathcal{F}_0 = \{< D > | D \subset S_G\} \text{ and } < D > = < E > \text{ implies } D \sim E, \, |\mathcal{F}_0| = \text{ the number of } \{|[D]| [D] \subset S_G\}.

(2) \text{ By Theorem 3.4-(3), } f : \mathcal{F} \longrightarrow \mathcal{F}_0 \text{ by } f(H) = < S_H > \text{ for a subgroup } H \in \mathcal{F} \text{ is a one-to-one correspondence. Since there are } |< S_H >| \text{ subgroups in } < S_H >, \text{ the number of } \mathcal{F} \text{ as given in Theorem 3.3} = \prod_{H \in \mathcal{D}} |< S_H >| \text{ where } H \in \mathcal{D} \text{ are representatives of } \{\mathcal{H}\}. \text{ But } \{< S_H > | H \in \mathcal{D}\} = \mathcal{F}_0 \text{ by Theorem 3.4-(1), so the number of } \mathcal{F} \text{ as given in Theorem 3.3} = \prod_{<D> \in \mathcal{F}_0} |<D>|, \text{ a product of } |<D>| \text{ for } <D> \in \mathcal{F}_0.

\section{4 The Double Centralizer Property}

In Theorem 3.3, we give a set \mathcal{F} with a maximal number of subgroups of \textit{G} such that the Galois map \alpha : H \longrightarrow B^H \text{ is one-to-one for } H \in \mathcal{F}. \text{ In this section, we shall show that if the Galois extension } B \text{ of } B^G \text{ with Galois group } G \text{ satisfies the double centralizer property on the set } \{B^H | H \text{ is a subgroup of } G\}, \text{ then any set } \mathcal{S} \text{ of subgroups on which } \alpha \text{ is one-to-one is contained in some } \mathcal{F}, \text{ where we call } B \text{ satisfying the double centralizer property on } \{B^H | H \text{ is a subgroup of } G\} \text{ if } V_B(V_B(B^H)) = B^H \text{ for each subgroup } H.

\textbf{Theorem 4.1} \text{ Assume } B \text{ satisfies the double centralizer property for } \{B^H | H \text{ is a subgroup of } G\}. \text{ Let } \mathcal{S} \text{ be a set of subgroups of } G \text{ such that } \alpha \text{ is one-to-one on } \mathcal{S}. \text{ Then } \mathcal{S} \subset \mathcal{F} \text{ for some } \mathcal{F} \text{ as given in Theorem 3.3.}

\textbf{Proof.} \text{ We first claim that for subgroups } K \text{ and } L \text{ of } G, \alpha(K) = \alpha(L) \text{ if and only if } S_K = S_L. \text{ In fact, } \alpha(K) = \alpha(L) \text{ implies } S_K = S_L \text{ by the argument in the proof of Theorem 3.3. Conversely, let } S_K = S_L. \text{ Then } \oplus_{k \in K} J_k = \oplus_{l \in L} J_l. \text{ Hence } V_B(B^K) = V_B(B^L) \text{ by Lemma 3.1. Taking the commutators both sides, we have } B^K = B^L \text{ because } B \text{ satisfies the double centralizer property for } \{B^H | H \text{ is a subgroup of } G\}. \text{ Thus } \alpha(K) = B^K = B^L = \alpha(L). \text{ Next, for } K, L \in \mathcal{S} \text{ such that } S_K = S_L, \alpha(K) = \alpha(L) \text{ by the above result. Since } \alpha \text{ is one-to-one on } \mathcal{S} \text{ by hypothesis, } K = L. \text{ This implies that } \mathcal{S} \text{ is a set with subgroups } H', H'' \text{ such that } S_{H'} \neq S_{H''} \text{ if } H' \neq H'' \text{. Thus } \mathcal{S} \text{ is contained}
in some $\mathcal{F}$ with a maximal number of subgroups such that $S_{H'} \neq S_{H''}$ for $H' \neq H'' \in \mathcal{F}$ as given in Theorem 3.3.

The following results are immediate from Theorem 4.1.

**Corollary 4.2** Assume $B$ satisfies the double centralizer property for $\{B^H | H \text{ is a subgroup of } G\}$. Then the collection of the sets $\mathcal{F}$ of subgroups as given in Theorem 3.3 is the full collection of the sets each with a maximal number of subgroups on which $\alpha$ is one-to-one.

**Corollary 4.3** Assume $B$ satisfies the double centralizer property for $\{B^H | H \text{ is a subgroup of } G\}$. Then $\alpha$ is one-to-one if and only if $S_H \neq S_L$ for subgroups $H \neq L$ of $G$.

**Remark 4.4** The sufficiency holds for any Galois extension $B$ by Theorem 3.3, so it does not need the double centralizer property for $B$.

5 The Uniqueness of a Galois Group

Let $B$ be a Galois extension of $B^G$ with Galois group $G$ and $H$ a proper subgroup of $G$. It is clear that $B$ is a Galois extension of $B^H$ with Galois group $H$. In this section, we shall discuss which Galois group $H$ is unique for the Galois extension $B$ over $B^H$. We define $H \simeq L$ if $\alpha(H) = \alpha(L)$ for subgroups $H$ and $L$ of $G$. It is clear that $\simeq$ is an equivalent relation. We denote $\tilde{H}$ the equivalent class of $H$. The following results are immediate.

**Theorem 5.1** Let $H$ be a proper subgroup of $G$ and $|\tilde{H}|$ the number of subgroups in $\tilde{H}$. Then $|\tilde{H}| = 1$ if and only if $H$ is unique for the Galois extension $B$ over $B^H$.

**Theorem 5.2** Let $H$ be a proper subgroup of $G$. If $K = < S_K >$ for each $K \simeq H$, then $H$ is unique for the Galois extension $B$ over $B^H$.

*Proof.* Let $K$ be a Galois group for $B$ of $B^H$. Then $B^K = B^H$; and so $K \simeq H$ and $S_K = S_H$. By hypothesis, $K = < S_K >$ and $H = < S_H >$, so $K = H$.

Also as defined in section 3, two subgroups $H \approx L$ if $S_H = S_L$. Let $|\overline{H}|$ be the number of subgroups in $\overline{H}$. We give more subgroups each being a unique Galois group for a Galois extension $B$.

**Theorem 5.3** Let $H$ be a proper subgroup of $G$. If $|\overline{H}| = 1$, then $H$ is unique for the Galois extension $B$ over $B^H$ and $H = < S_H >$. 
Proof. Let $L$ be a Galois group for $B$ of $B^H$. Then $B^L = B^H$; and so $S_L = S_H$ by Lemma 3.1 and Lemma 3.2. Hence $H \approx L$. By hypothesis, $|\overline{H}| = 1$, so $L = H$. Moreover, since $S_{<S_H>} = S_H$, $< S_H > \approx H$. Thus $< S_H > = H$ because $|\overline{H}| = 1$ again.

We note that if $B$ satisfies the double centralizer property for $\{B^K | K \text{ is a subgroup of } G\}$, then the relations $\approx$ and $\simeq$ are the same. Then the following corollary is immediate.

**Corollary 5.4** Assume $B$ satisfies the double centralizer property for $\{B^K | K \text{ is a subgroup of } G\}$. Then $H$ is a unique Galois group for the Galois extension $B$ over $B^H$ if and only if $|H| = 1$.

We conclude the present paper with a Galois extension $B$ of $B^G$ with the unique Galois group $G$.

**Theorem 5.5** Let $G$ and $G'$ be Galois groups for $B$ of $B^G$. If $G = < S_G >$, $G' = < S_{G'} >$, and $< S_G, S_{G'} >$ is a Galois group for $B$ of $B^G$ where $< S_G, S_{G'} >$ is the group generated by the elements in $S_G$ and $S_{G'}$, then $G = G'$.

**Proof.** Since $G$ and $G'$ are Galois groups for $B$ of $B^G$, $B^G = B'^G$. Since $G = < S_G >$, $G' = < S_{G'} >$, and $< S_G, S_{G'} >$ is a Galois group for $B$ of $B^G$, $V_B(B^G) = V_B(B'^G) = V_B(B^{<S_G,S_{G'}>}) = \oplus \sum_{g \in S_G} J_g = \oplus \sum_{g \in S_{G'}} J'_g = \oplus \sum_{g \in S_{<S_G,S_{G'}>}} J_p$ by Lemma 3.1. Noting that $S_G \cup S_{G'} \subset S_{<S_G,S_{G'}>}$, we have that $S_G = S_{G'}$ by Lemma 3.2. By hypothesis, $G = < S_G >$, $G' = < S_{G'} >$, so $G = G'$.

**ACKNOWLEDGEMENTS.** This paper was written during a visit of the second author to the Mathematics Department of Zhongshan University, China in Summer 2011. The second author would like to thank Zhongshan University for the hospitality.

**References**


Received: August, 2011