International Journal of Algebra, Vol. 6, 2012, no. 5, 219 - 225

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 $\alpha : H \longrightarrow B^H$ 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 α 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 noncommutative. 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 $\alpha : H \longrightarrow B^H$ is one-to-one. This implies that α 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 α 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 $\{a_i, b_i \in B \mid \sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g}$ 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 $A \otimes_D A \longrightarrow A$ 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, $J_g = \{b \in B \mid bx = g(x)b$ for each $x \in B\}$ for $g \in G$. For a subgroup H of G, let $\mathcal{S}_H = \{g \in H \mid J_g \neq \{0\}\}$ and $\mathcal{T}_H = \{g \in H \mid J_g = \{0\}\}$. We shall give a set $\mathcal{F}$ with a maximal number of subgroups such that the Galois map α is one-to-one on $\mathcal{F}$. We begin with two important properties of C-modules $\{J_g \mid g \in \mathcal{S}_G\}$.

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 $V_B(B^G) = \oplus \sum_{g\in G} J_g$.*

Lemma 3.2 *Let $D \subset \mathcal{S}_G$ and $\beta : D \longrightarrow \oplus \sum_{g\in D} J_g$. Then β is one-to-one from the set of subsets D of $\mathcal{S}_G$ to the set $\{\oplus \sum_{g\in D} J_g \mid D \subset \mathcal{S}_G\}$.*

Proof. By Lemma 3.2 in [9], β is one-to-one on the set $\{D = \{g\} \mid g \in \mathcal{S}_G\}$. Next, let D, $E \subset \mathcal{S}_G$ such that $\beta(D) = \beta(E)$. Then $\oplus \sum_{d\in D} J_d = \oplus \sum_{e\in E} J_e$. Assume there exists some $d \in D$ but not in E. Then $J_d \cap \oplus \sum_{e\in E} J_e = \{0\}$.

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

Next we give a collection of sets $\mathcal{F}$ with a maximal number of subgroups of G such that α 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 $\mathcal{S}_{H'} \neq \mathcal{S}_{H''}$ for $H' \neq H'' \in \mathcal{F}$. Then α 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, $\oplus \sum_{h \in \mathcal{S}_{H'}} J_h = \oplus \sum_{h \in \mathcal{S}_{H''}} J_h$ by Lemma 3.1 because B is a Galois extension of $B^{H'}$ $(= B^{H''})$ with Galois groups H' and H''. Thus $\mathcal{S}_{H'} = \mathcal{S}_{H''}$ by Lemma 3.2. But then $H' = H''$ by the definition of $\mathcal{F}$. This shows that α 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 $D \subset \mathcal{S}_G$, $< D >$ the subgroup generated by the elements in D, and $\mathcal{F}_0 = \{< D > | D \subset \mathcal{S}_G\}$. Then (1) $\mathcal{F}_0 = \{< \mathcal{S}_H > | H$ is a subgroup of $G\}$, (2) $\mathcal{F}_0$ is a set with a maximal number of subgroups of G such that $\mathcal{S}_{<D>} \neq \mathcal{S}_{<E>}$ for $< D > \neq < E >$ where $D, E \subset \mathcal{S}_G$, (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 $\mathcal{S}_H \subset \mathcal{S}_G$, $< \mathcal{S}_H > \in \mathcal{F}_0$. Conversely, for any $< D > \in \mathcal{F}_0$, $\mathcal{S}_{<D>} \subset < D >$, so $< \mathcal{S}_{<D>} > = < D >$. Noting that $< D >$ is a subgroup of G, we have $\mathcal{F}_0 \subset \{< \mathcal{S}_H > | H$ is a subgroup of $G\}$. Thus statement (1) holds.

(2) Since $D \subset \mathcal{S}_{<D>} \subset < D >$, $< \mathcal{S}_{<D>} > = < D >$ for any $D \subset \mathcal{S}_G$. Hence $\mathcal{S}_{<D>} \neq \mathcal{S}_{<E>}$ 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 $\mathcal{S}_H \subset \mathcal{S}_G$ for any subgroup H, $H \notin \mathcal{F}_0$ unless $H = < \mathcal{S}_H >$. 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 $\mathcal{S}_H \neq \mathcal{S}_L$ for $H \neq L \in \mathcal{F}$. We define a map $f : \mathcal{F} \longrightarrow \mathcal{F}_0$ by $f(H) = < \mathcal{S}_H >$. We claim that f is one-to-one and onto. In fact, let $f(H) = f(L)$ for $H, L \in \mathcal{F}$; then $< \mathcal{S}_H > = < \mathcal{S}_L >$. Thus $\mathcal{S}_{<\mathcal{S}_H>} = \mathcal{S}_{<\mathcal{S}_L>}$. Since $\mathcal{S}_H = \mathcal{S}_{<\mathcal{S}_H>}$ and $\mathcal{S}_L = \mathcal{S}_{<\mathcal{S}_L>}$, $\mathcal{S}_H = \mathcal{S}_L$. 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 $\mathcal{C} = \{D | D \subset \mathcal{S}_G\}$ and $\mathcal{D} = \{H | H$ is a subgroup of $G\}$. Define a relation $\sim$ on $\mathcal{C}$ by $D \sim E$ if $< D >=< E >$ for $D, E \in \mathcal{C}$, and $\approx$ on $\mathcal{D}$ by $H \approx L$ if $\mathcal{S}_H = \mathcal{S}_L$. Then it is clear that both $\sim$ and $\approx$ are equivalent relations. Denote the equivalent class of D by $[D]$ for $D \in \mathcal{C}$, and the equivalent class of H by $\overline{H}$ for $H \in \mathcal{D}$. Then $\mathcal{C} = \cup_{D \subset \mathcal{S}_G}[D]$ and $\mathcal{D} = \cup\overline{H}$ for $H \in \mathcal{D}$. We count the number of $\mathcal{F}$ as given in Theorem 3.3.

Theorem 3.5 *(1) $|\mathcal{F}_0| =$ the number of $\{[D] | D \subset \mathcal{S}_G\}$ and (2) Let $|\overline{H}|$ be the number of subgroups in $\overline{H}$ for a subgroup H. Then the number of $\mathcal{F}$ as given in Theorem 3.3 $= \Pi_{<D>\in\mathcal{F}_0}|\overline{< D >}|$, a product of $|\overline{< D >}|$ for $< D >\in \mathcal{F}_0$.*

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

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

4 The Double Centralizer Property

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

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

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

Corollary 4.3 *Assume B satisfies the double centralizer property for $\{B^H | H$ is a subgroup of $G\}$. Then α is one-to-one if and only if $\mathcal{S}_H \neq \mathcal{S}_L$ 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 $\widetilde{H}$ the equivalent class of H. The following results are immediate.

Theorem 5.1 *Let H be a proper subgroup of G and $|\widetilde{H}|$ the number of subgroups in $\widetilde{H}$. Then $|\widetilde{H}| = 1$ 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 $K =< \mathcal{S}_K >$ 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 $\mathcal{S}_K = \mathcal{S}_H$. By hypothesis, $K =< \mathcal{S}_K >$ and $H =< \mathcal{S}_H >$, so $K = H$.

Also as defined in section 3, two subgroups $H \approx L$ if $\mathcal{S}_H = \mathcal{S}_L$. 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 $H =< \mathcal{S}_H >$.*

Proof. Let L be a Galois group for B of B^H. Then $B^L = B^H$; and so $\mathcal{S}_L = \mathcal{S}_H$ by Lemma 3.1 and Lemma 3.2. Hence $H \approx L$. By hypothesis, $|\overline{H}| = 1$, so $L = H$. Moreover, since $\mathcal{S}_{<\mathcal{S}_H>} = \mathcal{S}_H$, $< \mathcal{S}_H > \approx H$. Thus $< \mathcal{S}_H >= H$ because $|\overline{H}| = 1$ again.

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

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 $G =< \mathcal{S}_G >$, $G' =< \mathcal{S}_{G'} >$, and $< \mathcal{S}_G, \mathcal{S}_{G'} >$ is a Galois group for B of B^G where $< \mathcal{S}_G, \mathcal{S}_{G'} >$ is the group generated by the elements in $\mathcal{S}_G$ and $\mathcal{S}_{G'}$, then $G = G'$.*

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

[1] S.U. Chase, D.K. Harrison, A. Rosenberg, "Galois Theory and Galois Cohomology of Commutative Rings", Memoirs Amer. Math. Soc. No. 52, 1965.

[2] F.R. DeMeyer, Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.*, **10** (1966), 287-295.

[3] F.R. DeMeyer, E. Ingraham, "Separable algebras over commutative rings", Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.

[4] M. Dokuchaev, M. Ferrero, A. Paques, Partial Action and Galois Theory, *Journal of Pure and Applied Algebra,* **208** (2007), 77-87.

[5] T. Kanzaki, On Galois Algebra Over a Commutative Ring, *Osaka J. Math.*, **2** (1965), 309-317.

[6] K. Sugano, On a Special Type of Galois Extensions, *Hokkaido J. Math.,* **9** (1980) 123-128.

[7] G. Szeto, L. Xue, The Structure of Galois Algebras, *Journal of Algebra,* **237**(1) (2001), 238-246.

[8] G. Szeto, L. Xue, On Galois Algebras Satisfying the Fundamental Theorem, *Communications in Algebra*, **35**(12) (2007), 3979 - 3985.

[9] G. Szeto, L. Xue, On Galois Extensions with an Inner Galois Group, *Recent developments in algebra and related areas*, 239-245, Adv. Lect. Math. (ALM), 8, Int. Press, Somerville, MA, 2009.

[10] G. Szeto, L. Xue, On Galois Extensions with a One-to-one Galois Map, *International Journal of Algebra*, **5**(17) (2011), 801 - 807

[11] O. E. Villamayor, D. Zelinsky, Galois Theory for Rings with Finitely Many Idempotents, *Nagoya Math. J.*, **27** (1966), 721-731.

[12] O. E. Villamayor, D. Zelinsky, Galois Theory with Infinitely Many Idempotents. *Nagoya Math. J.*, **35** (1969), 83-98.

Received: August, 2011