ON HIRATA SEPARABLE GALOIS EXTENSIONS SATISFYING THE FUNDAMENTAL THEOREM

GEORGE SZETO and LIANYONG XUE

Department of Mathematics
Bradley University
Peoria, Illinois 61625
E-mail: szeto@bradley.edu and lxue@bradley.edu

Abstract

Let B be a Hirata separable and a Galois extension of B^G with Galois group G whose order is a unit in B. It is shown that there exists a one-to-one correspondence between the set of subgroups of G and the set of separable extensions A of B^G in B such that A is a direct summand of B as an A-bimodule and $V_B(A) = \oplus \sum_{g \in G(A)} J_g$ where $V_B(A)$ is the commutator subring of A in B, $J_g = \{b \in B \,|\, bx = g(x)b$ for each $x \in B\}$ for a $g \in G$, and $G(A) = \{g \in G \,|\, g(a) = a$ for all $a \in A\}$. Moreover, properties of $V_B(B^G)$ is also given when $B = B^G \cdot V_B(B^G)$.

1. Introduction

Let $F \subset K$ be a finite field Galois extension with Galois group G. It is well known that the fundamental theorem holds for $F \subset K$, that is, the map $\alpha : H \longrightarrow K^H$ for a subgroup H of G is a one-to-one correspondence between the set of subgroups of G and the set of separable subfields of K over F. In [1], S.U. Chase, D.K. Harrison, and A. Rosenberg extended this fact to finite indecomposable commutative ring Galois extensions (with no idempotents but 0 and 1). Recently, for a central Galois algebra B with Galois group G, in

---

2000 Mathematics Subject Classification: Primary 13B05, 16W20.
Key Words and phrases: Separable extensions, Hirata separable extensions, Azumaya algebras, Galois extensions, central Galois algebras.

[9] it was shown that there exists a one-to-one correspondence between the set of subgroups of G and the set of separable extensions A of B^G in B such that $V_B(A) = \oplus \sum_{g \in G(A)} J_g$ where $V_B(A)$ is the commutator subring of A in B, $J_g = \{b \in B \,|\, bx = g(x)b$ for each $x \in B\}$ for a $g \in G$, and $G(A) = \{g \in G \,|\, g(a) = a$ for all $a \in A\}$. The purpose of the present paper is to generalize the above result to a Hirata separable Galois extension. Let B be a Hirata separable and a Galois extension of B^G with Galois group G whose order is a unit in B. Assume that B^H is a separable extension of B^G for each subgroup H of G. We shall show that there exists a one-to-one correspondence between the set of subgroups of G and the set of separable subrings A containing B^G such that A is a direct summand of B as an A-bimodule and $V_B(A) = \oplus \sum_{g \in G(A)} J_g$. Thus a one-to-one correspondence is also derived between the set of subgroups of G and the set of separable subalgebras of $V_B(B^G)$ over C where C is the center of B.

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, $i = 1, 2, ..., m$ 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, $i = 1, 2, ..., m\}$ for some integer m such that $\sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g}$ for each $g \in G$ ([2]). 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 ([7],[8]) 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 of B^G if it is a Galois and a Hirata separable extension of B^G ([5]).

Throughout this paper, we assume that B is a Galois extension of B^G with Galois group G, C the center of B, $J_g = \{b \in B \,|\, bx = g(x)b$ for each $x \in B\}$ for a $g \in G$, and for a subring A of B, $G(A) = \{g \in G \,|\, g(a) = a$ for all $a \in A\}$ and $V_B(A)$ denotes the commutator subring of A in B.

3. Hirata Separable Galois Extensions

In this section, we shall generalize the following theorem from a central Galois algebra as given in [9] to a Hirata separable Galois extension: Let B be a central Galois algebra over C with Galois group G. Then B satisfies the fundamental theorem if and only if for any separable subalgebra A, $V_B(A) = \oplus \sum_{g \in G(A)} J_g$ where the fundamental theorem for B means that the map $H \longrightarrow B^H$ for a subgroup H of G is one-to-one correspondence between the set of subgroups of G and the set of separable algebras of B. Now, let B be a Hirata separable Galois extension of B^G with Galois group G whose order is a unit in B. Then B is called to satisfy the fundamental theorem if the map $H \longrightarrow B^H$ for a subgroup H of G is one-to-one correspondence between the set of subgroups of G and the set of separable extensions of B^G in B. Throughout this section, we assume that B is a Hirata separable Galois extension of B^G with Galois group G whose order is a unit in B and B^H is a separable extension of B^G for each subgroup H of G. We begin with a separable extension A of B^G in B such that $A = B^{G(A)}$.

Lemma 3.1. *For a separable extension A of B^G in B, if A is a direct summand of B as an A-bimodule and $V_B(A) = \oplus \sum_{g \in G(A)} J_g$, then $A = B^{G(A)}$.*

Proof. Since B is a Hirata separable extension of B^G and since A is a separable extension of B^G in B and a direct summand of B as an A-bimodule, $V_B(V_B(A)) = A$ ([6], Theorem 1). Moreover, B is a Galois extension of $B^{G(A)}$ with Galois group $G(A)$, so $V_B(B^{G(A)}) = \oplus \sum_{g \in G(A)} J_g$ ([4], Proposition 1). But by hypothesis, $V_B(A) = \oplus \sum_{g \in G(A)} J_g$, so $V_B(A) = V_B(B^{G(A)})$. Noting that the order of G is a unit in B, we have that the separable extension $B^{G(A)}$ of B^G is a direct summand of B as an $B^{G(A)}$-bimodule. Hence $V_B(V_B(B^{G(A)})) = B^{G(A)}$ ([6], Theorem 1). Therefore $A = B^{G(A)}$.

Lemma 3.2. *If B satisfies the fundamental theorem, then any separable extension A of B^G in B is a direct summand of B as an A-bimodule.*

Proof. Since B satisfies the fundamental theorem, $A = B^{G(A)}$. But the order of G is a unit in B, so is the order of $G(A)$. Hence B is a Galois extension of A such that A is a direct summand of B as an A-bimodule.

Next is a generalization of the fundamental theorem for a central Galois algebra as given in [9].

Theorem 3.3. *Let B be a Hirata separable Galois extension of B^G with Galois group G whose order is a unit in B such that B^H is a separable extension of B^G for each subgroup H of G. Then B satisfies the fundamental theorem if and only if for any separable extension A of B^G in B, A is a direct summand of B as an A-bimodule and $V_B(A) = \oplus \sum_{g \in G(A)} J_g$.*

Proof. By Lemma 3.2 and Proposition 1 in [4], the necessity is clear. For the sufficiency, we claim that the map $\alpha : H \longrightarrow B^H$ is a one-to-one correspondence between the set of subgroups of G and the set of separable extensions of B^G in B. By Lemma 3.1, α is onto, so it suffices to show that α is one-to-one. Let $\alpha(H) = \alpha(L)$ for some subgroups H and L of G. Then $B^H = B^L$. Let K be the subgroup of G generated by H and L. Then $B^K = B^H$ because $B^H = B^L$. Hence B is a Galois extension of B^H with Galois groups H and K. Thus $V_B(B^H) = V_B(B^K) = \oplus \sum_{g \in H} J_g = \oplus \sum_{g \in K} J_g$ ([4], Proposition 1). Since $H \subset K$, $\oplus \sum_{g \in K} J_g = (\oplus \sum_{g \in H} J_g) \oplus (\oplus \sum_{g \in H'} J_g)$ where $H' = \{g \,|\, g \in K$ but $g \notin H\}$. Noting that $\{J_g \,|\, g \in G\}$ are projective rank one C-modules ([5], Theorem 2), we conclude that H' is empty; and so $K = H$. Similarly, $K = L$. Therefore $H = L$, that is, α is one-to-one.

Remark. For a central Galois algebra B with Galois group G, it is known that the order of G is a unit in B ([4], Corollary 3). Then the order of H is also a unit in B for each subgroup H of G, and so B^H is a direct summand of B as a B^H-bimodule and a separable subalgebra of B by the proof of Theorem 3.8 on page 55 in [3]. Thus Theorem 3.3 is a generalization of Theorem 3.3 in [9] for a central Galois algebra.

4. The Commutator Subring

Let B be a Hirata separable Galois extension of B^G with Galois group G satisfying the fundamental theorem as given by Theorem 3.3. Since $B^G \cdot V_B(B^G)$ is a separable extension of B^G in B, $B^G \cdot V_B(B^G) = B^{G(B^G \cdot V_B(B^G))}$. Thus, by Theorem 6 in [5], B is a Hirata separable Galois extension of $B^G \cdot V_B(B^G)$ with Galois group $G(B^G \cdot V_B(B^G))$ and $V_B(B^G)$ is a central Galois algebra with Galois group $G/G(V_B(B^G))$. It can be shown that $B^G \cdot V_B(B^G)$ also satisfies the fundamental theorem. In this section, we study the class of B such that $B = B^G \cdot V_B(B^G)$. It will be shown that B satisfies the fundamental theorem if and only if each separable extension A of B^G in B is a direct summand of B as an A-bimodule and $V_B(B^G)$ is a central Galois algebra satisfying the fundamental theorem.

In this section, we assume that B is a Hirata separable Galois extension of B^G with Galois group G whose order is a unit in B. We denote $V_B(B^G)$ by Δ.

Lemma 4.1. *If $B = B^G \cdot \Delta$, then Δ is an Azumaya algebra over C^G.*

Proof. Since $B = B^G \cdot \Delta$, Δ is a Galois algebra over C^G with center C ([10], Theorem 3.3 and Lemma 3.1). Hence Δ is an Azumaya algebra over C. Moreover, since the order of G is a unit in B, B^G is a direct summand of B as a B^G-bimodule. Noting that B is a

Hirata separable extension of B^G, we have that $V_B(V_B(B^G)) = B^G$ ([6], Theorem 1); and so this implies that $C^G = C$. Thus Δ is an Azumaya algebra over C^G.

Theorem 4.2. *If $B = B^G \cdot \Delta$, then Δ is a central Galois algebra with Galois group induced by and isomorphic with G.*

Proof. Since $B = B^G \cdot \Delta$, Δ is a Galois algebra over C^G with Galois group induced by and isomorphic with G ([10], Theorem 3.3). But by Lemma 4.1, $C^G = C$ where C is the center of Δ, so Δ is a central Galois algebra with Galois group induced by and isomorphic with G.

Now we characterize B satisfying the fundamental theorem when $B = B^G \cdot \Delta$ in terms of Δ.

Lemma 4.3. *If B is a central Galois algebra with Galois group G satisfying the fundamental theorem, then for any separable subalgebra A of B, $A = \oplus \sum_{g \in G(A')} J_g$ where $A' = V_B(A)$.*

Proof. See Theorem 3.1 in [9].

Theorem 4.4. *Assume $B = B^G \cdot \Delta$. Then B satisfies the fundamental theorem if and only if any separable extension A of B^G in B is a direct summand of B as an A-bimodule, Δ is a central Galois algebra with Galois group induced by and isomorphic with G, and Δ satisfies the fundamental theorem.*

Proof. ($\Longrightarrow$) By Theorem 3.3, any separable extension A of B^G in B is a direct summand of B as an A-bimodule. Also by Theorem 4.2, Δ is a central Galois algebra over C^G $(= C)$ with Galois group induced by and isomorphic with G. Hence it suffices to show that Δ satisfies the fundamental theorem. In fact, let D be a separable subalgebra of Δ. Then B^GD is a separable extension of B^G in B. Since B satisfies the fundamental theorem, $B^GD = B^{G(B^GD)} = B^{G(D)} = (B^G \cdot \Delta)^{G(D)} \supset B^G\Delta^{G(D)} \supset B^GD$. Thus $B^GD = B^G\Delta^{G(D)}$; and so $V_B(B^GD) = V_B(B^G\Delta^{G(D)})$. Noting that $B = B^G \cdot \Delta$, we have that $V_\Delta(D) = V_\Delta(\Delta^{G(D)})$. Therefore $D = V_\Delta(V_\Delta(D)) = V_\Delta(V_\Delta(\Delta^{G(D)})) = \Delta^{G(D)}$ by the double centralizer property for the Azumaya algebra Δ ([3], Theorem 4.3 on page 57). Hence $\alpha' : H \longrightarrow \Delta^H$ for a subgroup H of G is onto from the set of subgroups of G and the set of separable subalgebras of Δ. To show that α' is one-to-one, let $\Delta^H = \Delta^L$ for some subgroups H and L of G. Using the similar argument as given in the proof of Theorem 3.3, let K be the subgroup of G generated by H and L. Then $\Delta^K = \Delta^H$. Hence Δ is a Galois extension of Δ^H with Galois groups H and K. Thus $V_\Delta(\Delta^H) = V_\Delta(\Delta^K) = \oplus\sum_{g\in H} J'_g = \oplus\sum_{g\in K} J'_g$ where $J'_g = \{b \in \Delta \,|\, bx = g(x)b \text{ for each } x \in \Delta\}$ for a $g \in G$ ([4], Proposition 1). Since Δ is a central Galois algebra with Galois group induced by and isomorphic with G, $\{J'_g \,|\, g \in G\}$ are projective rank one C-modules. Noting that $H \subset K$, we conclude that $K = H$. Similarly, $K = L$. Therefore $H = L$, that is, α' is one-to-one.

($\Longleftarrow$) By Theorem 3.3, it suffices to show that $V_B(A) = \oplus\sum_{g\in G(A)} J_g$ for any separable extension A of B^G in B. By hypothesis, A is a direct summand of B as an A-bimodule, so $V_B(A)$ is a separable subalgebra of Δ ([6], Theorem 1). But Δ is a central Galois algebra satisfying the fundamental theorem with Galois group induced by and isomorphic with G, so $V_B(A) = \oplus\sum_{g\in G(V_\Delta(V_B(A)))} J_g$ by Lemma 4.3. Since $B = B^G \cdot \Delta$, $G(V_\Delta(V_B(A))) = G(B^GV_\Delta(V_B(A))) = G(V_{B^G\Delta}(V_B(A))) = G(V_B(V_B(A))) = G(A)$. Thus $V_B(A) = \oplus\sum_{g\in G(A)} J_g$. Therefore B satisfies the fundamental theorem by Theorem 3.3.

We conclude the present paper with an expression of a separable extension of B^G in B satisfying the fundamental theorem as given in theorem 4.4.

Lemma 4.5. *If B satisfies the fundamental theorem, then for any separable extension A of B^G in B, $A \cap \Delta = \oplus\sum_{g\in G(A')} J_g$ where $A' = V_B(A)$.*

Proof. Since B satisfies the fundamental theorem and A is a separable extension of B^G in B, $A = B^{G(A)}$ such that A is a direct summand of B as an A-bimodule. Also B is a Hirata separable extension of B^G by hypothesis, so $V_B(A)$ is a separable subalgebra of Δ over C^G ([6], Theorem 1). Hence $B^G \cdot V_B(A)$ is a separable extension of B^G. Thus $B^G \cdot V_B(A) = B^{G(B^G \cdot V_B(A))} = B^{G(V_B(A))}$ by the fundamental theorem again. But then $V_B(B^G \cdot V_B(A)) = V_B(B^{G(V_B(A))})$. This implies that $\Delta \cap V_B(V_B(A)) = \oplus \sum_{g \in G(A')} J_g$ where $A' = V_B(A)$. Noting that $V_B(V_B(A)) = A$, we have that $A \cap \Delta = \oplus \sum_{g \in G(A')} J_g$.

Theorem 4.6. *Let B satisfy the fundamental theorem as given by Theorem 4.4. Then for any separable extension A of B^G in B, $A = B^G \cdot (A \cap \Delta)$.*

Proof. By Lemma 4.5, $A \cap \Delta = \oplus \sum_{g \in G(A')} J_g$ where $A' = V_B(A)$. Hence $V_\Delta(A \cap \Delta) = V_\Delta(\oplus \sum_{g \in G(A')} J_g) = V_\Delta(V_\Delta(A'))$, the last equation holds because Δ is a central Galois algebra satisfying the fundamental theorem by Theorem 4.4 and Proposition 1 in [4]. But then $V_\Delta(V_\Delta(A')) = A'$ ([3], Theorem 4.3 on page 57). Thus $V_B(A) = A' = V_\Delta(V_\Delta(A')) = V_\Delta(A \cap \Delta) = V_{B^G \cdot \Delta}(B^G \cdot (A \cap \Delta)) = V_B(B^G \cdot (A \cap \Delta))$. Therefore $A = B^G \cdot (A \cap \Delta)$ ([6], theorem 1).

Acknowledgement

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

References

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

[2] F.R. DeMeyer, Some Notes on the General Galois Theory of Rings, *Osaka J. Math.* **2** (1965), 117-127.

[3] F.R. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings,* Lecture Notes in Mathematics, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.

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

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

[6] K. Sugano, On Centralizers in Separable Extensions II, *Osaka J. Math.,* **8** (1971), 465-469.

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

[8] G. Szeto and L. Xue, The Galois Algebra with Galois Group which is the Automorphism Group. *Journal of Algebra* **293**(1) (2005), 312-318.

[9] G. Szeto and L. Xue, On Galois Algebras Satisfying the Fundamental Theorem, *Communications in Algebra*, to appear.

[10] L. Xue, On Characterizations of a Commutator Galois Extension, *JP Journal of Algebra and Number Theory,* **6**(3) (2006), 597-607.