

On Galois Algebras 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 Galois algebra over a commutative ring R with Galois group G such that B^H is a separable subalgebra of B for each subgroup H of G . Then it is shown that B satisfies the fundamental theorem if and only if B is one of the following three types: (1) B is an indecomposable commutative Galois algebra, (2) $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B , and (3) B is an indecomposable Galois algebra such that for each separable subalgebra A , $V_B(A) = \bigoplus_{g \in G(A)} J_g$, and the centers of A and $B^{G(A)}$ are the same where $V_B(A)$ is the commutator subring of A in B , $J_g = \{b \in B \mid bx = g(x)b \text{ for each } x \in B\}$ for a $g \in G$, and $G(A) = \{g \in G \mid g(a) = a \text{ for all } a \in A\}$.

Key Words and Phrases. Separable extensions, Azumaya algebras, Galois extensions, Galois algebras, central Galois algebras.

2000 Mathematics Subject Classification. Primary 13B05, 16W20.

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 $\alpha : H \rightarrow K^H$ 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). In [5], for a noncommutative Galois extension B of B^G with Galois group G , let H be a subgroup of G , then it was shown that $V_B(B^H) = \bigoplus_{g \in H} J_g$ where $V_B(B^H)$ is the commutator subring of B^H in B and $J_g = \{b \in B \mid bx = g(x)b \text{ for each } x \in B\}$ for a $g \in G$. We note that the set $\{J_g \mid g \in G\}$ plays an important role for noncommutative Galois extensions ([5],[7],[8]). In the present paper, we shall characterize a Galois algebra $B \supset B^G$ with Galois group G which satisfies the fundamental theorem in terms of $\{J_g \mid g \in G\}$. At first, we show the following result for a central Galois algebra: Let B be a central Galois algebra with Galois group G . Then, B satisfies the fundamental theorem if and only if for each separable subalgebra A , $V_B(A) = \bigoplus_{g \in G(A)} J_g$ where $J_g = \{b \in B \mid bx = g(x)b \text{ for each } x \in B\}$, $V_B(A)$ the commutator subring of A in B , and $G(A) = \{g \in G \mid g(a) = a \text{ for all } a \in A\}$. Next we obtain a structure of a Galois algebra B satisfying the fundamental theorem, that is, B is an indecomposable central Galois algebra over its center C with Galois group K where $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$ and C is an indecomposable commutative Galois algebra over $C^G (= B^G)$ with Galois group G/K . Then assume that B^H is a separable subalgebra of B for each subgroup H of G , using this structure for B , we shall show that a Galois algebra B satisfies the fundamental theorem if and only if B is one of the following three types: (1) B is an indecomposable commutative Galois algebra, (2) $B = Re \oplus R(1-e)$ where e and $1-e$ are minimal central idempotents in B , and (3) B is an indecomposable Galois algebra such that for each separable subalgebra A , $V_B(A) = \bigoplus_{g \in G(A)} J_g$, and the centers of A and $B^{G(A)}$ are the same.

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.

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 , $i = 1, 2, \dots, m$ 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 , $i = 1, 2, \dots, m\}$ 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 ([8]). A ring B is called indecomposable if it contains no central idempotents but 0 and 1.

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

3. Central Galois Algebras

In this section, let B be a central Galois algebra over its center C with Galois group G , A a separable subalgebra of B , and $A' = V_B(A)$. We shall show a characterization of B satisfying the fundamental theorem in terms of $\{J_g \mid g \in G\}$. We begin with some properties of a central Galois algebra satisfying the fundamental theorem.

Theorem 3.1. *Let B be a central Galois algebra over C with Galois group G . If B satisfies the fundamental theorem, then for any separable subalgebra A , $V_B(A) = \bigoplus_{g \in G(A)} J_g$ and $A = \bigoplus_{g \in G(A')} J_g$.*

Proof. Since A is a separable subalgebra of B which satisfies the fundamental theorem, $A = B^{G(A)}$. Hence B is a Galois extension of A ($= B^{G(A)}$) with Galois group $G(A)$. Thus $V_B(A) = V_B(B^{G(A)}) = \bigoplus_{g \in G(A)} J_g$ ([5], Proposition 1). Moreover, noting that B is an Azumaya algebra, we have that A' ($= V_B(A)$) is a separable subalgebra of B such

that $V_B(A') = V_B(V_B(A)) = A$ by the double centralizer property for Azumaya algebras ([4], Theorem 4.3, page 57). By hypothesis, $A' = B^{G(A')}$, so B is a Galois extension of A' with Galois group $G(A')$. This implies that $V_B(A') = \bigoplus_{g \in G(A')} J_g$. Therefore $A = V_B(A') = \bigoplus_{g \in G(A')} J_g$.

Next is the converse of Theorem 3.1. We need a fact for the ideal group $\{J_g \mid g \in G\}$ as given by Rosenberg and Zelinsky ([6]).

Lemma 3.2. *Let A be a central Galois algebra with Galois group G . Then $\{J_g \mid g \in G\}$ is a group with $J_g J_h = J_{gh}$ for $g, h \in G$ and isomorphic with G by $g \mapsto J_g$ for $g \in G$.*

Proof. Since A is a central Galois algebra with Galois group G , A is an Azumaya algebra with the finite automorphism group G . Hence $J_g J_h = J_{gh}$ for $g, h \in G$ ([6], Lemma 5) and J_g is a finitely generated and projective rank one C -module ([6], page 1112). Moreover, since A is a central Galois algebra with Galois group G again, $A = \bigoplus_{g \in G} J_g$ ([5], Theorem 1) such that J_g is a rank one C -module for each $g \in G$. Thus $g \mapsto J_g$ for $g \in G$ is a group isomorphism between G and $\{J_g \mid g \in G\}$.

Theorem 3.3. *Let B be a central Galois algebra with Galois group G . If for any separable subalgebra A of B , $V_B(A) = \bigoplus_{g \in G(A)} J_g$, then B satisfies the fundamental theorem.*

Proof. Since B is a central Galois algebra with Galois group G , $|G|$, the order of G , is a unit in B ([5], Corollary 3). Hence, for any subgroup H of G , $|H|$ is a unit in B . Thus B^H is a separable subalgebra of B . Therefore the map $\alpha : H \rightarrow B^H$ is well defined from the set of subgroups of G and the set of separable subalgebras of B . Next, let A be a separable subalgebra of B . Then $A' (= V_B(A))$ is also a separable subalgebra of B such that $V_B(A') = V_B(V_B(A)) = A$ by the double centralizer property for Azumaya algebras

([4], Theorem 4.3, page 57). By hypothesis, $V_B(A) = \oplus \sum_{g \in G(A)} J_g$. On the other hand, B is a Galois extension of $B^{G(A)}$ with Galois group $G(A)$, so $V_B(B^{G(A)}) = \oplus \sum_{g \in G(A)} J_g$ ([5], Proposition 1). Thus $V_B(A) = \oplus \sum_{g \in G(A)} J_g = V_B(B^{G(A)})$. Moreover, since $G(A)$ is a subgroup of G , $|G(A)|$ is a unit in B . Thus $B^{G(A)}$ is a separable subalgebra of the Azumaya algebra B . Therefore

$$A = V_B(V_B(A)) = V_B(V_B(B^{G(A)})) = B^{G(A)}.$$

This implies that the map $\alpha : H \rightarrow B^H$ is onto from the set of subgroups of G to the set of separable subalgebras of B . Next we claim that α is one-to-one. In fact, let $\alpha(H) = \alpha(L)$ for some subgroups H and L of G . Then $B^H = B^L$. Since B is a Galois extension of B^H with Galois group H , $V_B(B^H) = \oplus \sum_{g \in H} J_g$ ([5], Proposition 1). Similarly, $V_B(B^L) = \oplus \sum_{g \in L} J_g$. Thus $\oplus \sum_{g \in H} J_g = V_B(B^H) = V_B(B^L) = \oplus \sum_{g \in L} J_g$. Since B is a central Galois algebra with Galois group G , $B = \oplus \sum_{g \in G} J_g$ such that $J_g \neq \{0\}$ for each $g \in G$. But $H, L \subset G$, so $\oplus \sum_{g \in H} J_g = \oplus \sum_{g \in L} J_g \subset B = \oplus \sum_{g \in G} J_g$. This implies that $H = L$ by Lemma 3.2; and so α is one-to-one.

By combining Theorem 3.1 and Theorem 3.3, a characterization is obtained.

Theorem 3.4. *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 , $V_B(A) = \oplus \sum_{g \in G(A)} J_g$.*

4. Galois Algebras

In this section, we shall generalize the characterization of a central Galois algebra satisfying the fundamental theorem as given in section 3 to a Galois algebra not necessarily central. We begin with an expression and some properties of a Galois algebra satisfying the fundamental theorem. The following lemma is useful.

Lemma 4.1. *Let B be a Galois algebra over R with Galois group G and $\lambda \in \text{Aut}_R(B)$. If e is a nontrivial central idempotent in B such that $\lambda|_{Be}$ is an identity and $\lambda|_{B(1-e)}$ is not an identity, then $\lambda \notin G$.*

Proof. See Lemma 4.1 in [9].

Theorem 4.2. *Let B be a Galois algebra over a commutative ring R with Galois group G . If B satisfies the fundamental theorem, then either B is indecomposable or $B = Re \oplus R(1-e)$ where e and $1-e$ are minimal central idempotents in B .*

Proof. We first claim that R is indecomposable. Suppose there exists a nontrivial central idempotent e in R . Then $B = Be \oplus B(1-e)$. Since B is separable over R , Be and $B(1-e)$ are separable algebras over Re and $R(1-e)$, respectively; and so $Be \oplus R(1-e)$ and $Re \oplus B(1-e)$ are proper separable subalgebras of B . Hence $G(Be \oplus R(1-e))$ and $G(Re \oplus B(1-e))$ are proper subgroups of G by the fundamental theorem for B . But $G(Be \oplus R(1-e))|_{Be} = \langle 1 \rangle = G(Re \oplus B(1-e))|_{B(1-e)}$, so $G(Be \oplus R(1-e)) = \langle 1 \rangle = G(Re \oplus B(1-e))$ by Lemma 4.1. Hence $Be \oplus R(1-e) = B = Re \oplus B(1-e)$ by the fundamental theorem for B again. Thus $B = Re \oplus R(1-e) = R$, a contradiction. This implies that R is indecomposable. Next, we claim that either B is indecomposable or $B = Re \oplus R(1-e)$ where e and $1-e$ are minimal central idempotents in B . In case B is indecomposable, we are done. In case B is decomposable, there exists a nontrivial central idempotent e in B . Then $B = Be \oplus B(1-e)$ such that $e \neq 0 \neq 1-e$. By the previous argument, we have that $Be \oplus R(1-e) = B = Re \oplus B(1-e)$; and so $B = Re \oplus R(1-e)$. Since B is a Galois algebra over R with Galois group G , B is a finitely generated R -module where R is indecomposable. Hence B contains only finitely many minimal central idempotents $\{e_i \mid i = 1, 2, \dots, m\}$ for some integer m . Thus $B = \bigoplus_{i=1}^m Be_i$. Now we want to show that $m \leq 2$. Assume $m > 2$. Then $B = Be_1 \oplus Be_2 \oplus B(1-e_1-e_2)$ where e_1, e_2 , and $1-e_1-e_2$ are orthogonal central idempotents. Considering the proper separable subalgebra

$B(e_1 + e_2) \oplus B(1 - e_1 - e_2)$ of B , we have that $G(B(e_1 + e_2) \oplus B(1 - e_1 - e_2))|_{B(e_1 + e_2)} = \langle 1 \rangle$; and so $G(B(e_1 + e_2) \oplus B(1 - e_1 - e_2)) = \langle 1 \rangle$ by Lemma 4.1 again. But $G(B) = \langle 1 \rangle$, so $B = B(e_1 + e_2) \oplus B(1 - e_1 - e_2)$ which is a proper separable subalgebra of B , a contradiction. Therefore $m \leq 2$. This implies that $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B .

We can obtain a partial converse theorem of Theorem 4.2.

Theorem 4.3. *Let B be a Galois algebra over R with Galois group G . If $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B over R , then B satisfies the fundamental theorem and $|G|=2$.*

Proof. Let $g \neq 1$ in G . Then $g(e) = 1 - e$ and $g(1 - e) = e$ because e and $1 - e$ are minimal central idempotents. Thus $|G|=2$. On the other hand, since B does not have proper separable subalgebras, the fundamental theorem holds for B .

To show another partial converse of Theorem 4.2, it suffices to discuss the case in which B is indecomposable. We note that for an indecomposable Galois algebra B with Galois group G , B is a central Galois algebra with Galois group K and C is a commutative Galois algebra with Galois group G/K ([3], Theorem 1).

Next we want to generalize the characterization for a central Galois algebra as given in Theorem 3.4 to a Galois algebra not necessarily central.

Theorem 4.4. *Let B be a Galois algebra over a commutative ring R with Galois group G . If B satisfies the fundamental theorem, then for any separable subalgebra A ,*

$$V_B(A) = \bigoplus \sum_{g \in G(A)} J_g.$$

Proof. By hypothesis $A = B^{G(A)}$, so B is a Galois extension of A with Galois group $G(A)$. Thus $V_B(A) = V_B(B^{G(A)}) = \bigoplus \sum_{g \in G(A)} J_g$ ([5], Proposition 1).

To show the converse of Theorem 4.4 for an indecomposable Galois algebra B with Galois group G , We first show that the map $\alpha : H \rightarrow B^H$ is one-to-one for a subgroup H of G .

Lemma 4.5. *Let B be an indecomposable Galois algebra with Galois group G . Then $J_g \neq \{0\}$ for $g \in K$ and $J_g = \{0\}$ for $g \notin K$.*

Proof. By Theorem 1 in [3], B is a central Galois algebra over C with Galois group K , so $J_g \neq \{0\}$ for $g \in K$ and $J_g = \{0\}$ for $g \notin K$ ([5], Proposition 3).

Lemma 4.6. *Let B be an indecomposable Galois algebra with Galois group G . Then the map $\alpha : H \rightarrow B^H$ is one-to-one for a subgroup H of G .*

Proof. Let H and L be subgroups of G such that $\alpha(H) = \alpha(L)$. Then $B^H = B^L$. Hence $V_B(B^H) = V_B(B^L)$. Since B is a Galois extension of $B^H (= B^L)$ with Galois group H and L , respectively, we have that $\bigoplus \sum_{g \in H} J_g = V_B(B^H) = V_B(B^L) = \bigoplus \sum_{g \in L} J_g$. By Lemma 4.5, $J_g \neq \{0\}$ for $g \in K$ and $J_g = \{0\}$ for $g \notin K$. Hence $\bigoplus \sum_{g \in H \cap K} J_g = \bigoplus \sum_{g \in L \cap K} J_g$; and so $H \cap K = L \cap K$. Next we consider subgroups H and $G(B^H)$. Clearly, $H \subset G(B^H)$ and $B^H = B^{G(B^H)}$, so $\alpha(B^H) = \alpha(B^{G(B^H)})$. But then $H \cap K = G(B^H) \cap K$ by the above argument. Also we have that $(B^H)^K = (B^{G(B^H)})^K$; and so $B^{HK} = B^{G(B^H)K}$, that is, $C^{HK} = C^{G(B^H)K}$. Thus by the fundamental theorem for indecomposable commutative Galois extension C over C^G with Galois group G/K , $HK/K = G(B^H)K/K$. Therefore $H/(H \cap K) \cong HK/K = G(B^H)K/K \cong G(B^H)/(G(B^H) \cap K) = G(B^H)/(H \cap K)$. Noting that $H \subset G(B^H)$, we conclude that $H = G(B^H)$. Similarly, $L = G(B^L)$; and so $H = G(B^H) = G(B^L) = L$. This implies that α is one-to-one.

The following is a characterization of a Galois algebra satisfying the fundamental theorem as a generalization of Theorem 3.4.

Theorem 4.7. *Let B be a Galois algebra over R with Galois group G and C the center of B . Assume that B^H is a separable subalgebra of B for each subgroup H of G . Then B satisfies the fundamental theorem if and only if B is one of the following three types: (1) B is an indecomposable commutative Galois algebra, (2) $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B , and (3) B is an indecomposable Galois algebra such that for each separable subalgebra A , $V_B(A) = \bigoplus_{g \in G(A)} J_g$, and the centers of A and $B^{G(A)}$ are the same.*

Proof. (\implies) Assume that B satisfies the fundamental theorem. Then by Theorem 4.2, either B is indecomposable or $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B . In case B is indecomposable, either B is an indecomposable commutative Galois algebra or B is an indecomposable noncommutative Galois algebra. If B is an indecomposable noncommutative Galois algebra, $V_B(A) = \bigoplus_{g \in G(A)} J_g$ for any separable subalgebra A by Theorem 4.4. Also since $A = B^{G(A)}$, it is clear that the center of A = the center of $B^{G(A)}$.

(\impliedby) In case B is indecomposable commutative, the sufficiency is given by Theorem 2.3 in [1]. In case $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B , we are done by Theorem 4.3. In case B is indecomposable such that for any separable subalgebra A , $V_B(A) = \bigoplus_{g \in G(A)} J_g$ and the centers of A and $B^{G(A)}$ are the same, then the map $\alpha : H \longrightarrow B^H$ is one-to-one from the set of subgroups of G to the set of invariant separable subalgebras B^H of B by Lemma 4.6. Hence it suffices to show that α is onto, that is, for any separable subalgebra A of B , $A = B^{G(A)} = \alpha(G(A))$. By hypothesis, $V_B(A) = \bigoplus_{g \in G(A)} J_g$. But B is a Galois extension of $B^{G(A)}$ with Galois group $G(A)$, so $V_B(B^{G(A)}) = \bigoplus_{g \in G(A)} J_g$ ([5], Proposition 1). Hence $V_B(A) = V_B(B^{G(A)})$. Thus

$V_B(AC) = V_B(A) = V_B(B^{G(A)}) = V_B(B^{G(A)}C)$. But B is a Galois algebra over R , so it is separable over R . Hence C is separable over R . Thus AC and $B^{G(A)}C$ are subalgebras of the Azumaya algebra B . Hence $AC = B^{G(A)}C$ by the double centralizer property for Azumaya algebras ([4], Theorem 4.3, page 57). Let Z be the center of AC and Z_0 be the center of A . By hypothesis, the center of $A =$ the center of $B^{G(A)}$, so Z_0 is also the center of $B^{G(A)}$. It is clear that $Z_0 \subset Z$. Thus $A \otimes_{Z_0} Z \cong AC = B^{G(A)}C \cong B^{G(A)} \otimes_{Z_0} Z$. Noting that $A \subset B^{G(A)}$, we conclude that $A = B^{G(A)}$. This completes the proof.

Remark 1. For an indecomposable Galois algebra B with Galois group G , B^H is always a separable subalgebra over R for a subgroup H of G such that $H \supset K$ or $H \subset K$, so the hypothesis that B^H is a separable subalgebra over R for any subgroup H of G can be restated only for any H not comparable with K .

Remark 2. Let B be a Galois algebra over R with Galois group G . It can be shown that for a subgroup H of G , if B^H is a direct summand of B as a B^H -bimodule, then B^H is a separable subalgebra of B .

Remark 3. By Theorem 4.6 in [9], it was shown that for a Galois algebra B over R with Galois group G which is the automorphism group $\text{Aut}_R(B)$ either B is commutative with no idempotents but 0 and 1, or $B = Re \oplus R(1 - e)$ where e and $1 - e$ are minimal central idempotents in B . Thus B satisfies the fundamental theorem by Theorem 4.7.

References

- [1] Chase, S.U., Harrison, D.K., Rosenberg, A. (1965). Galois Theory and Galois Cohomology of Commutative Rings. *Memoirs Amer. Math. Soc.*, No. 52.
- [2] DeMeyer, F.R. Some Notes on the General Galois Theory of Rings. *Osaka J. Math.* 2:117-127, 1965

- [3] DeMeyer, F.R. Galois Theory in Separable Algebras over Commutative Rings. *Illinois J. Math.* 10:287-295, 1966.
- [4] DeMeyer, F.R., Ingraham, E. (1971). Separable algebras over commutative rings. *Springer Verlag, Berlin, Heidelberg, New York*, Volume 181.
- [5] Kanzaki, T. On Galois Algebra Over A Commutative Ring. *Osaka J. Math.* 2:309-317, 1965.
- [6] Rosenberg, A., Zelinsky, D. Automorphisms of Separable Algebras. *Pacific J. Math.* 11:1109-1117, 1961.
- [7] Sugano, K. On a Special Type of Galois Extensions. *Hokkaido J. Math.* 9:123-128, 1980.
- [8] Szeto, G., Xue, L. The structure of Galois algebras. *Journal of Algebra* 237(1):238-246, 2001.
- [9] G. Szeto, G., Xue, L. The Galois Algebra with Galois Group which is the Automorphism Group. *Journal of Algebra* 293(1):312-318, 2005.