On Galois Extensions Satisfying
the Fundamental Theorem

George Szeto

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

Lianyong Xue

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

Abstract

Let B be a Galois extension of B^G with Galois group G. It is shown that B satisfies the fundamental theorem if and only if B is either indecomposable satisfying the fundamental theorem, or $B = B^G e \oplus B^G(1-e)$ where e and $1-e$ are minimal central idempotents in B, and G has order 2.

1 Introduction

In [1], it was shown that the fundamental theorem holds for any indecomposable commutative Galois extension (with no idempotents but 0 and 1). Recently, in [5], a Galois algebra B over a commutative ring R with Galois group G satisfying the fundamental theorem is characterized; that is, 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 indecomposable noncommutative such that $A = \oplus \sum_{g \in G(A')} J_g$ and the centers of A and

$B^{G(A)}$ are the same for each separable subalgebra A, where $A' = V_B(A)$, the commutator subalgebra of A in B, $G(A') = \{g \in G \,|\, g(a) = a \text{ for all } a \in A'\}$, and $J_g = \{b \in B \,|\, bx = g(x)b \text{ for each } x \in B\}$ ([5], Theorem 4.7). The purpose of the present paper is to generalize the above characterization to any Galois extension, not necessary a Galois algebra. We shall show that, for any Galois extension B of B^G with Galois group G, B satisfies the fundamental theorem if and only if B is one of the following two types: (1) B is indecomposable satisfying the fundamental theorem, or (2) $B = B^G e \oplus B^G(1-e)$ where e and $1 - e$ are minimal central idempotents in B, and G has order 2.

2   Definitions and Notations

Let B be a ring with 1, G a finite automorphism group 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 Galois extension of B^G with Galois group G if there exist elements $\{a_i, b_i \text{ in } B, i = 1, 2, ..., m\}$ 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 the center of B ([3]). We call B a separable extension of A if there exist $\{a_i, b_i \text{ in } B, i = 1, 2, ..., m$ 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. A ring B is called indecomposable if it contains no central idempotents but 0 and 1. We call B satisfying the fundamental theorem if $\alpha : H \longrightarrow B^H$ for a subgroup H of G is a one-to-one correspondence between the set of subgroups of G and the set of separable subextensions of B^G in B.

Throughout this paper, we assume that B is a Galois extension of B^G with Galois group G.

3   The Fundamental Theorem

In this section, keeping all the definitions and notations in section 2, we shall show some properties of B satisfying the fundamental theorem, leading to the characterization: B satisfies the fundamental theorem if and only if B is one of the following two types: (1) B is indecomposable satisfying the fundamental theorem, or (2) $B = B^G e \oplus B^G(1-e)$ where e and $1 - e$ are minimal central idempotents in B, and G has order 2.

We begin with a lemma that will play an important role.

Lemma 3.1 *Let e be a nonzero central idempotent in B. If $g|_{Be}$ is an identity for a $g \in G$, then $g = $ identity in G.*

Proof. See Lemma 4.1 in [4].

Lemma 3.2 *If B satisfies the fundamental theorem, then for any nonzero central idempotent e in B, $Be = B^G e$.*

Proof. Let e be a nonzero central idempotent in B. Then $B^G e \oplus B(1-e)$ is a separable extension of B^G such that $G(B^G e \oplus B(1-e))|_{B(1-e)}$ is identity. Hence $G(B^G e \oplus B(1-e)) = \{1\}$ by Lemma 3.1. Since B satisfies the fundamental theorem, $B = B^G e \oplus B(1-e)$. Thus $Be = B^G e$.

Next we investigate the number of central idempotents in B^G and B respectively.

Lemma 3.3 *If B satisfies the fundamental theorem, then B^G is indecomposable.*

Proof. Let e be a nontrivial central idempotent in B^G. Then e and $1-e$ are nonzero central idempotents in B. Thus $Be = B^G e$ and $B(1-e) = B^G(1-e)$ by Lemma 3.2, and so $B = Be \oplus B(1-e) = B^G e \oplus B^G(1-e) = B^G$. This is a contradiction. Therefore B^G is indecomposable.

Lemma 3.4 *If B satisfies the fundamental theorem, then B has only finitely many minimal central idempotents.*

Proof. Let I be the set of minimal central idempotents in B, $e \in I$, and O_e the G-orbit of e; that is, $O_e = \{g(e) \,|\, g \in G\}$. Then O_e contains at most n elements where n is the order of G and $\sum_{e' \in O_e} e'$ is an idempotent in B^G. But B^G is indecomposable by Lemma 3.3, so $\sum_{e' \in O_e} e' = 1$. This implies that $O_e = I$, and so I is a finite set.

Corollary 3.5 *If B satisfies the fundamental theorem, then the G-action on the set of minimal central idempotents in B is transitive.*

Lemma 3.6 *If B satisfies the fundamental theorem, then B has at most two minimal central idempotents.*

Proof. By Lemma 3.4, B has finitely many minimal central idempotents. Let $I = \{e_1, e_2, \cdots, e_m\}$ for some integer m be the set of minimal central idempotents in B. Then $B = \oplus \sum_{i=1}^m Be_i = \oplus \sum_{i=1}^m B^G e_i$ by Lemma 3.2. In case $m = 1$; we are done. In case $m > 1$; we first show that $B^G(e_1 + e_2)$ is a proper subring of $B^G e_1 \oplus B^G e_2$. In fact, it is clear that $B^G(e_1 + e_2) \subset B^G e_1 \oplus B^G e_2$. Assume $e_1 \in B^G(e_1 + e_2)$. Then $e_1 = r(e_1 + e_2)$ for some $r \in B^G$. Hence $e_1 = e_1^2 = e_1 \cdot r(e_1 + e_2) = re_1$. Thus $(1-r)e_1 = 0$. By Corollary 3.5, the G-action on I is transitive, so for each e_i, $i = 2, 3, \cdots, m$, there exists some $g_i \in G$ such that $g_i(e_1) = e_i$. Thus $(1-r)e_i = 0$ for each $i = 1, 2, 3, \cdots, m$. Noting that $\{e_1, e_2, \cdots, e_m\}$ are all the minimal central idempotents in B, we

have that $1-r = 0$; and so $r = 1$. But then $e_1 = r(e_1+e_2) = e_1+e_2$. Therefore $e_2 = 0$, a contradiction. This implies that $e_1 \notin B^G(e_1+e_2)$; and so $B^G(e_1+e_2)$ is a proper subring of $B^G e_1 \oplus B^G e_2$. Next we claim that $m \leq 2$. Assume $m > 2$. Then $B = Be_1 \oplus Be_2 \oplus B(1 - e_1 - e_2) = B^G e_1 \oplus B^G e_2 \oplus B^G(1 - e_1 - e_2)$ by Lemma 3.2 where $1 - e_1 - e_2 \neq 0$. Considering the proper separable extension $B^G(e_1+e_2) \oplus B(1-e_1-e_2)$ of B^G in B, we have that $G(B^G(e_1+e_2) \oplus B(1-e_1-e_2))|_{B(1-e_1-e_2)} = \{1\}$; and so $G(B^G(e_1+e_2) \oplus B(1-e_1-e_2)) = \{1\}$ by Lemma 3.1. But $G(B) = \{1\}$, so $B = B^G(e_1+e_2) \oplus B(1-e_1-e_2)$. Since $B^G(e_1+e_2)$ is a proper subring of $B^G e_1 \oplus B^G e_2$, $B \neq B^G(e_1+e_2) \oplus B(1-e_1-e_2)$, a contradiction. Thus $m \leq 2$. This completes the proof.

Next we show the main theorem.

Theorem 3.7 *Let B be a Galois extension of B^G with Galois group G. Then B satisfies the fundamental theorem if and only if either $B = B^G e \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B and $G = \{1, g\}$ such that $g(e) = 1-e$, or B is indecomposable satisfying the fundamental theorem.*

Proof. ($\Longrightarrow$) In case B is indecomposable satisfying the fundamental theorem, we are done. In case B is decomposable; then by Lemma 3.6, $m = 1$ or 2. When $m = 1$, $B = Be_1 = B^G e_1 = B^G$, this is impossible. Thus $m = 2$; and so $B = B^G e_1 \oplus B^G e_2$. Then for any $g \neq 1$ in G, $g(e_1) = e_2 = 1 - e_1$. Therefore $G = \{1, g\}$.

($\Longleftarrow$) It suffices to show the case in which $B = B^G e \oplus B^G(1 - e)$ where e and $1 - e$ are minimal central idempotents in B and $G = \{1, g\}$ such that $g(e) = 1-e$. In fact, there are exactly two trivial separable extensions over B^G in B: B^G and B corresponding to exactly two trivial subgroups of G: $\{1, g\}$ and $\{1\}$.

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] G. Szeto and L. Xue, The structure of Galois algebras, *Journal of Algebra,* **237**(1) (2001), 238 - 246.

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

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

Received: November 29, 2006