

Some Notes on the Structure of Galois Algebras

George Szeto and Lianyong Xue

Department of Mathematics, Bradley University

Peoria, Illinois 61625 – U.S.A.

Email: szeto@bradley.edu and lxue@bradley.edu

Abstract

Let B be a Galois algebra over a commutative ring R with Galois group G . Then B is a direct sum of Galois algebras such that each direct summand is a composition of a central Galois algebra and a commutative Galois algebra. A sufficient condition is also given under which B is commutative.

1. Introduction

Let B be a Galois algebra with Galois group G over a commutative ring R with no idempotents but 0 and 1, C the center of B , and $K = \{g \in G \mid g(c) = c \text{ for each } c \in C\}$. Then in [2] it was shown that B is a central Galois algebra with Galois group K and C is a commutative Galois algebra over R with Galois group G/K . The purpose of the present paper is to generalize this theorem to any Galois algebra by using the structure theorem for Galois algebras ([5], Theorem 3.8). We shall give a further description of the structure of a Galois algebra, and derive a sufficient condition for a Galois algebra being commutative. 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

Throughout this paper, B will represent a ring with 1, G a finite automorphism group of B , C the center of B , and B^G the set of elements in B fixed under each element in G .

A ring B is called a Galois extension of B^G with Galois group G if there exist elements $\{a_i, b_i$ in B , $i = 1, 2, \dots, n\}$ for some integer n such that $\sum_{i=1}^n a_i g(b_i) = \delta_{1,g}$ for each $g \in G$, a Galois algebra over R if B is a Galois extension of R which is contained in C , and a central Galois extension if B is a Galois extension over its center C .

3. Galois Algebras

Throughout, let B be a Galois algebra with Galois group G over a commutative ring R , C the center of B , and $B^G = \{b \in B \mid g(b) = b \text{ for each } g \in G\}$. It was shown that if R contains no idempotents but 0 and 1, then B is a central Galois algebra with Galois group $K (= \{g \in G \mid g(c) = c \text{ for each } c \in C\})$ and C is a commutative Galois algebra over R with Galois group G/K ([2], Theorem 1). We shall generalize this theorem for any Galois algebra by using the structure theorem for B ([5], Theorem 3.8).

Lemma 3.1. ([5], Theorem 3.8) *Let B be a Galois algebra over R with Galois group G . Then there are orthogonal idempotents $\{e_i \mid i = 1, 2, \dots, m$ for some integer $m\}$ in C and subgroups H_i of G such that Be_i is a central Galois algebra with Galois group H_i for each $i = 1, 2, \dots, m$ and $B = \bigoplus_{i=1}^m Be_i$ or $B = (\bigoplus_{i=1}^m Be_i) \oplus Ce$ where $e = 1 - \sum_{i=1}^m e_i$ and $Ce = Be$ is a commutative Galois algebra with Galois group $G|_{Ce} \cong G$.*

Next lemma describes the direct summand Be_i of B for $i = 1, 2, \dots, m$ in Lemma 3.1.

Lemma 3.2. *By keeping the notations as given in Lemma 3.1, let $G(e_i) = \{g \in G \mid g(e_i) = e_i\}$ and $K_i = \{g \in G(e_i) \mid g(ce_i) = ce_i \text{ for each } c \in C\}$, then Be_i is a Galois algebra over Re_i with Galois group $G(e_i)$ and K_i is a normal subgroup of $G(e_i)$ for each $i = 1, 2, \dots, m$.*

Proof. Since B is a Galois algebra with Galois group G , it is a Galois extension with Galois group $G(e_i)$ and Be_i is a Galois extension of $(Be_i)^{G(e_i)}$ with Galois group

$G(e_i)|_{Be_i} \cong G(e_i)$ ([5], Lemma 3.7). Moreover, by Lemma 3.1 in [6], let B_a be the Boolean algebra generated by $\{0, e_g \mid g \in G\}$, then each e_i is a minimal element in B_a such that $e_i = \Pi e_g$ for some $e_g \in B_a$. This implies that for each $h \in G$, $h(e_i)$ ($= h(\Pi e_g) = \Pi e_{hgh^{-1}}$) is also a minimal element in B_a . Thus, for each $g \in G$, $g(e_i) = e_i$ or $g(e_i) \cdot e_i = 0$. But then $(Be_i)^{G(e_i)} = B^G e_i$ by the proof of Lemma 9 in [4]; and so $(Be_i)^{G(e_i)} = Re_i$. Therefore Be_i is a Galois algebra over Re_i with Galois group $G(e_i)$. Also it is clear that K_i is a normal subgroup of $G(e_i)$ for each $i = 1, 2, \dots, m$.

Theorem 3.3. *By keeping the notations of Lemma 3.1 and Lemma 3.2, let $G(e_i) = \{g \in G \mid g(e_i) = e_i\}$, then Be_i is a central Galois algebra over Ce_i with Galois group K_i and Ce_i is a commutative Galois algebra over Re_i with Galois group $G(e_i)/K_i$ for each $i = 1, 2, \dots, m$.*

Proof. By Lemma 3.2, Be_i is a Galois algebra over Re_i with Galois group $G(e_i)$ and K_i is a normal subgroup of $G(e_i)$ for each $i = 1, 2, \dots, m$. Hence Be_i is a Galois extension of $(Be_i)^{K_i}$ with Galois group K_i . By Lemma 3.1, Be_i is a central Galois algebra over Ce_i with Galois group H_i , so $(Be_i)^{H_i} = Ce_i$. It is clear that $H_i \subset K_i$, so $Ce_i \subset (Be_i)^{K_i} \subset (Be_i)^{H_i} = Ce_i$. Thus $(Be_i)^{K_i} = (Be_i)^{H_i} = Ce_i$; and so Be_i is a central Galois algebra over Ce_i with Galois group K_i and Ce_i is a commutative Galois algebra over Re_i with Galois group $G(e_i)/K_i$ for each $i = 1, 2, \dots, m$.

Corollary 3.4. *By keeping the notations of Theorem 3.3, $H_i = K_i$.*

Proof. By Lemma 3.1 and Theorem 3.3, Be_i is a central Galois algebra over Ce_i with Galois groups H_i and K_i respectively, and $H_i \subset K_i$. Let $J_g = \{b \in Be_i \mid bx = g(x)b \text{ for all } x \in Be_i\}$. Then $J_g \neq \{0\}$ for each $g \in K_i$ such that $Be_i = \bigoplus_{h \in H_i} J_h = \bigoplus_{g \in K_i} J_g$ ([3], Theorem 1). Noting that $H_i \subset K_i$, we conclude that $H_i = K_i$.

Corollary 3.5. *By keeping the notations of Theorem 3.3, if $G(e_i)$ is cyclic for each $i = 1, 2, \dots, m$, then B is commutative.*

Proof. By Theorem 3.3, Be_i is a Galois algebra over Re_i with Galois group $G(e_i)$, so Be_i is commutative whenever $G(e_i)$ is cyclic ([1], Theorem 11) for each i . Thus $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ is commutative.

Corollary 3.6. *By keeping the notations of Theorem 3.3, if G is an Abelian group such that $J_{g_i} \cdot J_{g_j} = \{0\}$ for all non-identity $g_i \neq g_j \in G$ where $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$, then B is commutative.*

Proof. Since $BJ_{g_i} = Be_{g_i}$ ([3], Proposition 2 and Lemma 2) and $J_{g_i} \cdot J_{g_j} = \{0\}$ for all non-identity $g_i \neq g_j \in G$, $e_{g_i} \cdot e_{g_j} = 0$ for all non-identity $g_i \neq g_j$ in G . Hence e_{g_i} and e_{g_j} are different minimal elements in B_a in case $e_{g_i} \neq 0$ and $e_{g_j} \neq 0$. Thus each e_i in $\{e_i \mid i = 1, 2, \dots, m\}$ as given in Lemma 3.1 is e_{g_i} for some $g_i \neq 1$ in G , and $H_i = \{g \in G \mid e_g e_{g_i} = e_{g_i}\} = \{1, g_i\}$ which is a cyclic group; and so each Be_i is commutative ([1], Theorem 11). Therefore $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ is commutative.

Remarks: (1) Theorem 3.3 covers the case of B in which R contains no idempotents but 0 and 1 where $e_i = 1$ for each i .

(2) By Theorem 3.3, if $J_g = \{0\}$ for each $g \neq 1$, then $B = \sum_{g \in G} J_g = J_1 = C$ ([3], Theorem 1); and so B is commutative.

4. Galois Algebras with a Transitive Galois Group

In this section, we will show that a Galois algebra with a Galois group G is a direct sum of Galois algebras with Galois group induced by and isomorphic with G . Then a structure theorem for a Galois algebra with a transitive Galois group is obtained and an element in the Galois group G is characterized. Let $I = \{e_i \mid i = 1, 2, \dots, m \text{ for some integer}$

$m\}$ as given in Lemma 3.1. Then, by Lemma 3.1 in [6], each e_i is a minimal element in B_a , the Boolean algebra generated by $\{0, e_g \mid g \in G\}$, and each element $g \in G$ permutes I . Hence $I = \cup_{j=1}^k O_j$ where $\{O_j\}$ are the orbits of I under the G -action. We call G a transitive Galois group if I has one orbit under the G -action. We note that if G is a transitive Galois group, then for any $e_i, e_j \in I$, there exists a $g \in G$ such that $g(e_i) = e_j$. Let $E_j = \sum_{e_i \in O_j} e_i$. Then $g(E_j) = E_j$ for each $g \in G$, and $B = \oplus \sum_{j=1}^k BE_j \oplus Ce$.

Theorem 4.1. *$B = \oplus \sum_{j=1}^k BE_j \oplus Ce$ such that BE_j is a Galois algebra over RE_j with transitive Galois group $G|_{BE_j} \cong G$ for each $j = 1, 2, \dots, k$.*

Proof. Since O_j is an orbit of I under the action of G , G is transitive on O_j . Also since $g(E_j) = E_j$ for each $g \in G$, $G(E_j) = G$ where $G(E_j) = \{g \in G \mid g(E_j) = E_j\}$. Thus BE_j is a Galois algebra over RE_j with Galois group $G|_{BE_j} \cong G$ ([5], Lemma 3.7) for each $j = 1, 2, \dots, k$.

Theorem 4.1 implies that the study of a Galois algebra is reduced to the study of Galois algebras BE_j with transitive Galois group $G|_{BE_j} \cong G$ and a commutative Galois algebra Be , so we study a Galois algebra with a transitive Galois group for the rest of the section.

We begin with a structure theorem for B .

Theorem 4.2. *Let B be a Galois algebra with a transitive Galois group G and $I = \{e_i \mid i = 1, 2, \dots, m\}$ as given in Lemma 3.1. Then*

- (1) $Be_i \cong Be_j$ for any $i, j = 1, 2, \dots, m$,
- (2) Be_i is a Galois algebra over Re_i with Galois group $G(e_i)$,
- (3) for $i, j = 1, 2, \dots, m$, $G(e_i)$ and $G(e_j)$ are conjugate subgroups of G , that is, there exists a $g \in G$ such that $G(e_j) = gG(e_i)g^{-1}$, and

(4) let $P(Be_i, Be_j)$ be the set of isomorphisms from Be_i to Be_j induced by G ; then

$$gG(e_i) = P(Be_i, Be_j) \text{ for any } g \in G \text{ such that } g(e_i) = e_j.$$

Proof. (1) Since G is transitive on I , there exists a $g \in G$ such that $g(e_i) = e_j$. Hence $g : Be_i \rightarrow Be_j$ is an isomorphism as rings because g is an automorphism of B .

(2) This is a consequence of Lemma 3.2.

(3) Since $g(e_i) = e_j$, $gG(e_i)g^{-1} \subset G(e_j)$. Thus the order of $G(e_i) \leq$ the order of $G(e_j)$. Similarly $g^{-1}G(e_j)g \subset G(e_i)$. Thus $G(e_j) \subset gG(e_i)g^{-1}$, and so $G(e_j) = gG(e_i)g^{-1}$.

(4) Since $g^{-1}P(Be_i, Be_j) \subset G(e_i)$, $P(Be_i, Be_j) \subset gG(e_i)$. Also $gG(e_i) \subset P(Be_i, Be_j)$, so $gG(e_i) = P(Be_i, Be_j)$ for any $g \in G$ such that $g(e_i) = e_j$.

As given by Corollary 3.5, we have a sufficient condition under which B is commutative.

Corollary 4.3. *If $G(e_i)$ is cyclic for some $i = 1, 2, \dots, m$, then B is commutative.*

Proof. By Theorem 4.2, $B = (\oplus \sum_{i=1}^m Be_i) \oplus Ce$ such that $Be_i \cong Be_j$ for any $i, j = 1, 2, \dots, m$. By hypothesis, Be_i is a Galois algebra with cyclic Galois group $G(e_i)$, so Be_i is commutative ([1], Theorem 11). Thus B is commutative.

Let $\text{Aut}(B)$ be the automorphism group of B , $\text{Aut}_I(B) = \{\alpha \in \text{Aut}(B) \mid \alpha \text{ permutes } I\}$. Then $\text{Aut}_I(B)$ is a subgroup of $\text{Aut}(B)$, and $G \subset \text{Aut}_I(B)$. Let $g \in G$. Then for each $e_i \in I$, either $g(e_i) = e_i$ or $g(e_i) = e_j \neq e_i$ for some $e_j \in I$. Hence $G = S_1 \cup S_2$ where $S_1 = \{g \in G \mid g(e_i) = e_i \text{ for some } e_i \in I\}$ and $S_2 = \{g \in G \mid g(e_i) \neq e_i \text{ for each } i = 1, 2, \dots, m\}$.

Theorem 4.4. (1) *For any $g \in S_1$ such that $g|_{Be_i} =$ identity on Be_i for some $i = 1, 2, \dots, m$, then g is the identity of G (hence $G(e_i)|_{Be_i} \cong G(e_i)$), and (2) *For any $g \in S_2$, $J_g = \{0\}$, that is, $e_g = 0$.**

Proof. (1) Since B is a Galois algebra with Galois group G , there exists a G -Galois system for B $\{a_j, b_j$ in B , $j = 1, 2, \dots, n\}$ for some integer n such that $\sum_{j=1}^n a_j g(b_j) = \delta_{1,g}$ for each $g \in G$. Hence $\sum_{j=1}^n (a_j e_i) g(b_j e_i) = e_i \delta_{1,g}$ for each $g \in G(e_i)$. Thus $e_i = \sum_{j=1}^n (a_j e_i) (g(b_j e_i) - b_j e_i)$ for each $g \neq 1$ in $G(e_i)$. But $e_i \neq 0$, so $g|_{Be_i} \neq 1$ whenever $g \neq 1$ in $G(e_i)$. Therefore, that $g|_{Be_i} = \text{identity on } Be_i$ implies that g is the identity of G .

(2) For any $g \in S_2$, Assume $J_g \neq \{0\}$. Since $BJ_g = Be_g$ ([3], Proposition 2 and Lemma 2), $e_g \neq 0$. Let $e_i = \Pi e_h$ for some $e_h = e_g$. Then $e_g e_i = e_i$, and so $g \in H_i$ by the definition of H_i ([5], theorem 3.8). Thus $g(e_i) = e_i$, a contradiction. Therefore $J_g = \{0\}$.

Next is a description of S_1 .

Corollary 4.5. *Let $S_1 = \{g \in G \mid g(e_i) = e_i \text{ for some } e_i \in I\}$. Then $S_1 = \cup_{i=1}^m G(e_i)$.*

Proof. Let $g \in G(e_i)$. Then $g(e_i) = e_i$; and so $g \in S_1$. Thus $\cup_{i=1}^m G(e_i) \subset S_1$. On the other hand, if $g \in S_1$, then $g(e_i) = e_i$ for some $e_i \in I$; and so $g \in G(e_i)$. Hence $S_1 \subset \cup_{i=1}^m G(e_i)$. Thus $S_1 = \cup_{i=1}^m G(e_i)$.

Corollary 4.6. *If $e_g \cdot e_h \neq 0$ for all $g, h \in S_1$. Then $B = Be_1 \oplus Ce$ such that Be_1 is a central Galois algebra with Galois group H_1 (that is, $m = 1$) as given in Lemma 3.1.*

Proof. For any $g, h \in S_1$, $e_g \cdot e_h \neq 0$ by hypothesis, so $e_g \cdot e_h = e_g \cdot e_{gh} \neq 0$ ([3], Proposition 2). Hence $e_{gh} \neq 0$. Thus $gh \in S_1$ by Theorem 4.4; and so S_1 is a subgroup of G , and $e_1 = \Pi_{g \in S_1} e_g \neq 0$. Therefore $S_1 \subset H_1$ by the definition of H_1 . But $S_1 = \cup_{i=1}^m G(e_i)$ by Corollary 4.5, so $H_1 = H_2 = \dots = H_m = S_1$. Thus $B = Be_1 \oplus Ce$ such that Be_1 is a central Galois algebra with Galois group H_1 by Lemma 3.1.

We conclude the present paper with two examples: (1) a Galois algebra B over R with Galois group G such that B is not a central Galois algebra over C with Galois group

$K (= \{g \in G \mid g(c) = c \text{ for all } c \in C\})$, and (2) a noncommutative Galois extension with a cyclic Galois group.

EXAMPLE 1. Let $R[i, j, k]$ be the real quaternion algebra over R , D the field of complex numbers, $B = R[i, j, k] \oplus (D \otimes_R D)$, and $G = \{1, g_i, g_j, g_k\}$ where $g_i(a, d_1 \otimes d_2) = (iai^{-1}, \bar{d}_1 \otimes d_2)$, $g_j(a, d_1 \otimes d_2) = (jaj^{-1}, d_1 \otimes \bar{d}_2)$, and $g_k(a, d_1 \otimes d_2) = (kak^{-1}, \bar{d}_1 \otimes \bar{d}_2)$ for all $(a, d_1 \otimes d_2)$ in B , where \bar{d} is the conjugate of the complex number d . Then,

(1) B is a Galois extension with a G -Galois system: $\{a_1 = (1, 0), a_2 = (i, 0), a_3 = (j, 0), a_4 = (k, 0), a_5 = (0, 1 \otimes 1), a_6 = (0, \sqrt{-1} \otimes 1), a_7 = (0, 1 \otimes \sqrt{-1}), a_8 = (0, \sqrt{-1} \otimes \sqrt{-1})\}$; $b_1 = \frac{1}{4}(1, 0), b_2 = -\frac{1}{4}(i, 0), b_3 = -\frac{1}{4}(j, 0), b_4 = -\frac{1}{4}(k, 0), b_5 = \frac{1}{4}(0, 1 \otimes 1), b_6 = -\frac{1}{4}(0, \sqrt{-1} \otimes 1), b_7 = -\frac{1}{4}(0, 1 \otimes \sqrt{-1}), b_8 = \frac{1}{4}(0, \sqrt{-1} \otimes \sqrt{-1})\}$.

(2) $B^G = R \oplus (R \otimes R) \cong R \oplus R$.

(3) By (1) and (2) B is a Galois algebra over $R \oplus R$ with Galois group G .

(4) $C = R \oplus (D \otimes_R D)$.

(5) By (3) and (4) B is not a central Galois algebra with Galois group G .

(6) $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\} = \{1\}$, and so B is not a central Galois algebra with Galois group K .

EXAMPLE 2. Let $B = M_2(R) \oplus M_2(R)$, a direct sum of matrix rings of order 2 over reals R , and $G = \langle \alpha \rangle$ where $\alpha(x, y) = (y, x)$ for all $(x, y) \in B$. Then B is a noncommutative Galois extension with Galois group G of order 2.

REFERENCES

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

- [2] F.R. DeMeyer, Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.*, **10** (1966), 287-295.
- [3] T. Kanzaki, On Galois Algebra over a Commutative Ring, *Osaka J. Math.*, **2**(1965), 309-317.
- [4] K. Kishimoto and T. Nagahara, On G -extensions of a semi-connected ring. *Math. J. Okayama Univ.* **32** (1990), 25-42.
- [5] G. Szeto and L. Xue, The Structure of Galois Algebras, *Journal of Algebra*, **237**(1)(2001), 238-246.
- [6] G. Szeto and L. Xue, The Boolean Algebra of Galois Algebras, *International Journal of Mathematics and Mathematical Sciences*, **2003**(11) (2003), 673-679.