

The Galois Algebra with Galois Group which is the Automorphism Group

George Szeto and Lianyong Xue

Department of Mathematics

Bradley University

Peoria, Illinois 61625

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

ABSTRACT

Let B be a Galois algebra over a commutative ring R with Galois group G . Then it is shown that $G = \text{Aut}_R(B)$ if and only if B is commutative with no idempotents but 0 and 1, or $B \cong R \oplus R$ where R contains no idempotents but 0 and 1.

1. INTRODUCTION

It is well known that the Galois group of a Galois extension of a field is the automorphism group of the field, and S. U. Chase, D. K. Harrison, and A. Rosenberg proved this fact for a commutative Galois extension with no idempotents but 0 and 1 ([3], Theorem 3.5). We are interested in the converse problem: let B be a Galois algebra over a commutative ring R with Galois group G . If $G = \text{Aut}_R(B)$, is B a commutative ring with no idempotents but 0 and 1? The present paper will show that $G = \text{Aut}_R(B)$ if and only if either B is commutative with no idempotents but 0 and 1, or $B \cong R \oplus R$ where R contains no idempotents but 0 and 1. We shall employ the general Wedderburn Theorem for an Azumaya algebra over a local ring as given by F. R. DeMeyer ([6], Corollary 1) to calculate the inner automorphism group of a central Galois algebra. Then the problem is reduced to the problem for a Galois algebra B with at most four central idempotents. But then B

is either a composition of a central Galois algebra and a commutative Galois algebra with no idempotents but 0 and 1 ([5], Theorem 1), or commutative with exactly two minimal central idempotents. This will lead to the conclusion.

This paper was revised under the suggestions of the referee. The authors would like to thank the referee for the valuable suggestions. Also this work was done under the support of a Caterpillar Fellowship at Bradley University. We 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 .

Let A be a subring of a ring 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. 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 , $i = 1, 2, \dots, m\}$ for some integer m such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. Such a set $\{a_i, b_i\}$ is called a G -Galois system for B . A ring B is called a Galois algebra over R if B is a Galois extension of R and R is contained in C , and B is called a central Galois algebra if B is a Galois extension of C . The characteristic of a ring C is denoted by $\text{Char}(C)$.

3. THE INNER AUTOMORPHISM GROUP

Let B be a central Galois algebra over its center C with Galois group G . We shall show that the rank of B over C is defined and equal to k^2 where $k^2 = |G|$, the order of G , for some integer k (for the rank of a projective module, see [7], page 27). Then by using the general Wedderburn Theorem for Azumaya algebras over a local ring as given by F. R. DeMeyer ([6], Corollary 1), we show that the order of the inner automorphism group

of B is greater than $|G|$ when either $|G| > 2$, or $|G| = 2$ and $\text{Char}(C) \neq 2$. We begin with the general Wedderburn Theorem.

PROPOSITION A. (F. R. DeMeyer, [6], Corollary 1) *Let A be an Azumaya algebra over a semi-local ring C with no idempotents but 0 and 1. Then $A \cong M_n(D)$, a matrix ring of order n for some integer n over an Azumaya algebra D with no idempotents but 0 and 1 in the same class of A in the Brauer group of C .*

LEMMA 3.1. *Let B be a Galois algebra over a commutative ring R with Galois group G . Then the rank of B over R is defined and $\text{rank}_R(B) = |G|$.*

Proof. Since B is a Galois algebra over R with Galois group G , the skew group ring $B * G \cong \text{Hom}_R(B, B)$. Hence for each prime ideal p of R , $R_p \otimes_R (B * G) \cong R_p \otimes_R \text{Hom}_R(B, B)$, that is, $B_p * G \cong \text{Hom}_{R_p}(B_p, B_p)$. Thus $\text{rank}_{R_p}(B_p) \cdot |G| = (\text{rank}_{R_p}(B_p))^2$; and so $|G| = \text{rank}_{R_p}(B_p)$ for each p . Therefore $\text{rank}_R(B) = |G|$.

LEMMA 3.2. *If B is a central Galois algebra over its center C with Galois group G , then $|G| = k^2$ for some integer k .*

Proof. By Lemma 3.1, $\text{rank}_C(B) = |G|$, so B is an Azumaya algebra of rank $|G|$ over C . Hence for any prime ideal p of C , $C_p \otimes_C B \cong M_n(D)$, a matrix ring of order n for some integer n over an indecomposable Azumaya C_p -algebra D by Proposition A. Noting that $\text{rank}_{C_p}(D) = \text{rank}_{C_p/pC_p}(D/pD) = d^2$ for some integer d , we have that $\text{rank}_{C_p}(C_p \otimes_C B) = (nd)^2$; and so $|G| = \text{rank}_C(B) = (nd)^2 = k^2$ where $k = nd$.

For a central Galois algebra over C with Galois group G of order greater than 2, we want to show that the order of the inner automorphism group of B , $|\text{Inn}(B)| > |G|$. We first work on $\text{Inn}(B)$ for a matrix ring B .

LEMMA 3.3. *Let $B = M_n(R)$, a matrix ring of order n for some integer n over a commutative ring R . Let α_A and $\alpha_{A'}$ be inner automorphisms of B induced by invertible matrices A and A' , respectively. If $\alpha_A = \alpha_{A'}$, then $A = rA'$ for some $r \in R$.*

Proof. Since $\alpha_A = \alpha_{A'}$, $AEA^{-1} = A'E(A')^{-1}$ for each $E \in B$. Hence $(A')^{-1}AE = E(A')^{-1}A$ for each $E \in B$. Thus $(A')^{-1}A$ is in the center of B . Therefore $(A')^{-1}A = rI$ for some $r \in R$ where I is the identity matrix of B ; and so $A = rA'$.

LEMMA 3.4. *Let $B = M_n(R)$ as given in Lemma 3.3 and let $\text{Inn}(B)$ denote the inner automorphism group of B . If either $n > 2$, or $n = 2$ and $\text{Char}(R) \neq 2$, then $|\text{Inn}(B)| > n^2$.*

Proof. Let $\mathcal{S} = \{I + D \mid I \text{ is the identity matrix of } B \text{ and } D \text{ is a strictly upper triangular matrix with 1 as nonzero entries}\}$. Then for any $r \in R$ and any two distinct upper triangular matrices D and D' , $I + D$ is an invertible matrix and $I + D \neq r(I + D')$. Hence $\alpha_{(I+D)} \neq \alpha_{(I+D')}$ by Lemma 3.3. Similarly, let $\mathcal{T} = \{I + E \mid E \text{ is a strictly lower triangular matrix with 1 as nonzero entries}\}$. Then $I + E \neq r(I + E')$ for any $E \neq E'$ as given in \mathcal{T} and $r \in R$. Hence $\alpha_{(I+E)} \neq \alpha_{(I+E')}$ by Lemma 3.3. Thus $|\text{Inn}(B)| \geq |\mathcal{S}| + |\mathcal{T}| = 2 \cdot |\mathcal{T}| = 2 \cdot (2^{\frac{n(n-1)}{2}} - 1) > n^2$ for all $n > 2$. For $n = 2$ and $1 \neq -1$, $I, I + D, I - D, I + E$, and $I - E$ are 5 invertible elements in B which induce 5 distinct inner automorphisms of B . Therefore $|\text{Inn}(B)| \geq 5 > 4 = n^2$.

THEOREM 3.5. *Let A be an Azumaya algebra over its center C of rank k^2 for some integer k . If either $k > 2$, or $k = 2$ and $\text{Char}(C) \neq 2$, then $|\text{Inn}(A)| > k^2$.*

Proof. Let J be the Jacobson radical of A , then $A/JA \cong \bigoplus_{i=1}^t A_i$ for some integer t where A_i is a central simple algebra over a field F_i for each i . By hypothesis, $\text{rank}_C(A) = k^2$, so $A_i = M_{k_i}(D_i)$, a matrix ring of order k_i over a central division algebra D_i for some integer k_i such that $k_i^2 \dim_{F_i}(D_i) = k^2$ for each i . Since $\dim_{F_i}(D_i) = m_i^2$ for some integer m_i , $k_i^2 \dim_{F_i}(D_i) = \dim_{F_i}(A_i) = (k_i m_i)^2 = k^2$. We claim that $|\text{Inn}(A_i)| > (k_i m_i)^2 = k^2$ for

each i . In fact, there are more than k_i^2 invertible matrices $\{E_j\}$ over D_i inducing distinct inner automorphisms by Lemma 3.4 and there are m_i^2 linearly independent invertible elements $\{d_t\}$ in D_i over F_i , so there are more than $(k_i m_i)^2$ invertible elements $\{E_j d_t\}$ in A_i which induce more than $(k_i m_i)^2$ distinct inner automorphisms of A_i . Thus $|\text{Inn}(A_i)| > (k_i m_i)^2 = k^2$. Therefore $|\text{Inn}(A)| > \prod_{i=1}^t (k_i m_i)^2 = k^{2t} \geq k^2$.

Next is our first main result for a central Galois algebra derived from Azumaya algebras.

THEOREM 3.6. *Let B be a central Galois algebra of rank k^2 with Galois group G . If either $k > 2$, or $k = 2$ and $\text{Char}(C) \neq 2$, then $|\text{Inn}(B)| > |G|$.*

Proof. Since B is a central Galois algebra with Galois group G , B is an Azumaya algebra such that $\text{rank}_C(B) = |G| = k^2$ for some integer k by Lemma 3.1 and Lemma 3.2. Thus $|\text{Inn}(B)| > k^2 = |G|$ by Theorem 3.5.

4. THE GALOIS GROUP

In this section, we shall show the main theorem for a Galois algebra B over R with Galois group G ; that is, $G = \text{Aut}_R(B)$ if and only if either B is commutative with no idempotents but 0 and 1, or $B \cong R \oplus R$ where R contains no idempotents but 0 and 1. We need two results, the first one is the structure of a Galois algebra with no idempotents but 0 and 1 proved by F. R. DeMeyer ([5], Theorem 1) and the second one is the existence of an automorphism of a Galois algebra which is not in the Galois group.

PROPOSITION B. (F. R. DeMeyer, [5], Theorem 1) *Let B be a Galois algebra with no idempotents but 0 and 1 over R with Galois group G and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$ where C is the center of B . Then B is a central Galois algebra with Galois group K and C is a commutative Galois algebra over R with Galois group G/K .*

LEMMA 4.1. *Let B be a Galois algebra over R with Galois group G and $\lambda \in \text{Aut}_R(B)$. If $e \neq 0$ is a central idempotent in B such that $\lambda|_{Be}$ is identity and $\lambda|_{B(1-e)}$ is not identity, then $\lambda \notin G$.*

Proof. Since B is a Galois algebra over R , B has a G -Galois system $\{a_i, b_i$ in B , $i = 1, 2, \dots, m\}$ for some integer m such that $\sum_{i=1}^m a_i b_i = 1$ and $\sum_{i=1}^m a_i g(b_i) = 0$ for each $g \neq 1$ in G . Assume $\lambda \in G$. Then $\sum_{i=1}^m a_i \lambda(b_i) = 0$ because $\lambda \neq 1$ in G . Hence $0 = 0 \cdot e = \sum_{i=1}^m a_i \lambda(b_i) e = \sum_{i=1}^m a_i \lambda(b_i e) = \sum_{i=1}^m a_i (b_i e) = e$. This is a contradiction; and so $\lambda \notin G$.

LEMMA 4.2. *Let B be a Galois algebra over R with Galois group G . If $G = \text{Aut}_R(B)$, then R contains no idempotents but 0 and 1.*

Proof. Assume $e^2 = e \in R$ and $e \neq 0, 1$. Then $B = Be \oplus B(1-e)$, $G(Be) = Be$, and $G(B(1-e)) = B(1-e)$. Hence for each $g \neq 1$ in G , $g|_{Be} \neq 1$ or $g|_{B(1-e)} \neq 1$. Without loss of generality, assume $g|_{B(1-e)} \neq 1$. Therefore $\lambda = 1 \oplus g|_{B(1-e)} \in \text{Aut}_R(B)$ but $\lambda \notin G$ by Lemma 4.1. Thus $|\text{Aut}_R(B)| > |G|$. This is a contradiction; and so R contains no idempotents but 0 and 1.

LEMMA 4.3. *Let B be a Galois algebra over R with Galois group G . If $G = \text{Aut}_R(B)$ and $|G| > 2$, then B is a Galois algebra with no central idempotents but 0 and 1.*

Proof. By Lemma 4.2, R contains no idempotents but 0 and 1. Next we claim that B contains no central idempotents but 0 and 1. Since B is a Galois algebra over R with Galois group G , B is a finitely generated R -module. Hence C contains only finitely many minimal idempotents $\{e_i \mid i = 1, 2, \dots, q\}$ for some integer q . If $q = 1$, then B is a Galois algebra with no central idempotents but 0 and 1. Next we show that $q > 1$ leads to a contradiction. Assume that $q > 1$. Since $\{e_i \mid i = 1, 2, \dots, q\}$ are the minimal idempotents in C , g permutes $\{e_i\}$ for each $g \in G$. Let $g \neq 1$ in G and $g(e_1) = e_j$ for some j . Then

$g(Be_1) = Be_j$. There are 4 cases. Case 1: $j = 1$ and $g|_{Be_1} = 1$; we have that $g|_{B(1-e_1)} \neq 1$ since $g \neq 1$ in G . But then by Lemma 4.1, $g \notin G$. This is a contradiction. Case 2: $j = 1$ and $g|_{Be_1} \neq 1$; we have an automorphism $\lambda \in \text{Aut}_R(B)$ such that $\lambda|_{Be_1} = g|_{Be_1}$ and $\lambda|_{Be_i} = 1$ for $i \neq 1$. Thus $\lambda \in \text{Aut}_R(B)$ but $\lambda \notin G$ by Lemma 4.1. Therefore $\text{Aut}_R(B) \neq G$, a contradiction again. Case 3: $j \neq 1$ and $q > 2$; we have an automorphism $\lambda \in \text{Aut}_R(B)$ such that $\lambda|_{Be_1} = g|_{Be_1}$, $\lambda|_{Be_j} = g^{-1}|_{Be_j}$ and $\lambda|_{Be_i} = 1$ for $i \neq 1, j$. Thus $\lambda \in \text{Aut}_R(B)$ but $\lambda \notin G$ by Lemma 4.1. Therefore $\text{Aut}_R(B) \neq G$. This contradiction leads to $q = 1$ or 2 . Case 4: $j \neq 1$ and $q = 2$; then $g(e_1) = e_2$. Since $|G| > 2$, there exists a $g' \neq 1, g$ in G such that $g'(e_1) = e_1$ or $g'(e_1) = e_2$. Noting that $g'(e_1) = e_1$ is either Case 1 or Case 2, we can assume that $g'(e_1) = e_2$. But then $(g^{-1}g')(e_1) = e_1$ and $g^{-1}g' \neq 1$ in G . This is either Case 1 or Case 2 which leads to a contradiction. Hence $q = 1$, and so B is a Galois algebra with no central idempotents but 0 and 1.

Next we show the structure of B when $G = \text{Aut}_R(B)$ for either $|G| > 2$ or $|G| = 2$ respectively.

THEOREM 4.4. *Let B be a Galois algebra over R with Galois group G . If $G = \text{Aut}_R(B)$ and $|G| > 2$, then B is a commutative Galois algebra with no idempotents but 0 and 1.*

Proof. Since $G = \text{Aut}_R(B)$ and $|G| > 2$, by Lemma 4.3, B is a Galois algebra with no central idempotents but 0 and 1. Hence by Proposition B, B is a central Galois algebra with Galois group K where $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$, and C is a commutative Galois algebra over R with Galois group G/K . But then $|K| = k^2$ for some integer k by Lemma 3.2. Since $G = \text{Aut}_R(B)$, $K = \text{Aut}_C(B)$. We have three cases: Case 1: either $k > 2$ or $k = 2$ and $\text{Char}(C) \neq 2$; then $|\text{Aut}_C(B)| \geq |\text{Inn}(A)| > k^2 = |K|$ by Theorem 3.6. This contradicts to $K = \text{Aut}_C(B)$. Case 2: $k = 2$ and $\text{Char}(C) = 2$; then $|K| = 2^2 = 4$, and so B is a central Galois algebra with Galois group K of order 4. Thus 4 is a unit in C ([8], Corollary 3). This is impossible because $\text{Char}(C) = 2$ by hypothesis in this case.

Consequently, We are left with only case 3: $k = 1$, that is, $K = \{1\}$, so $B = C$ which is a commutative Galois algebra with no idempotents but 0 and 1.

THEOREM 4.5. *Let B be a Galois algebra over R with Galois group G . If $G = \text{Aut}_R(B)$ and $|G| = 2$, then either B is a commutative Galois algebra with no idempotents but 0 and 1, or $B \cong R \oplus R$ where R contains no idempotents but 0 and 1.*

Proof. Since $|G| = 2$, G is a cyclic group. Hence B is commutative ([4], Theorem 11). By hypothesis, B is a Galois algebra over R with Galois group G and $G = \text{Aut}_R(B)$. Hence R contains no idempotents but 0 and 1 by Lemma 4.2. But then by Corollary 12(ii) in [9], either B contains no idempotents but 0 and 1, or $B \cong R \oplus R$. Thus either B is a commutative Galois algebra with no idempotents but 0 and 1, or $B \cong R \oplus R$ where R contains no idempotents but 0 and 1.

THEOREM 4.6. *Let B be a Galois algebra over R with Galois group G . Then $G = \text{Aut}_R(B)$ if and only if either B is commutative with no idempotents but 0 and 1, or $B \cong R \oplus R$ where R contains no idempotents but 0 and 1.*

Proof. (\implies) is consequences of Theorem 4.4 and Theorem 4.5.

(\impliedby) If B is commutative with no idempotents but 0 and 1, then $G = \text{Aut}_R(B)$ ([3], Theorem 3.5). Next, assume $B \cong R \oplus R$ where R contains no idempotents but 0 and 1. Then B contains only two minimal idempotents, $e_1 = (1, 0)$ and $e_2 = (0, 1) = 1 - e_1$. Hence for any $\alpha \neq 1$ in $\text{Aut}_R(B)$, $\alpha(e_1) = e_2$ and $\alpha(e_2) = e_1$. Thus $\text{Aut}_R(B) = \{1, \alpha \mid \alpha(ae_1 + be_2) = ae_2 + be_1 \text{ for each } ae_1 + be_2 \in B\}$; and so $G = \text{Aut}_R(B)$.

Theorem 4.6 can be applied to a Galois Azumaya extension as studied in [1] and [2]. A ring B is called a Galois Azumaya extension of B^G with Galois group G if B is a Galois extension of B^G with Galois group G and B^G is an Azumaya C^G -algebra (see [1] and [2]). A ring B is called a DeMeyer-Kanzaki Galois extension of B^G with Galois group G if B is

an Azumaya algebra over C and C is a Galois algebra over C^G with Galois group induced by and isomorphic with G (see [4],[8]).

COROLLARY 4.7. *Let B be a Galois Azumaya extension of B^G with Galois group G . Then $G = \text{Aut}_{B^G}(B)$ if and only if either B is a DeMeyer-Kanzaki Galois extension with no central idempotents but 0 and 1, or $B \cong B^G \oplus B^G$ which is a Galois extension of B^G with Galois group G of order 2 where $G = \{1, g\}$ such that $g(be) = b(1 - e)$ and $g(b(1 - e)) = be$ for each $b \in B^G$, and $e = 1 \oplus 0$ is a minimal central idempotent of B .*

Proof. (\implies) Since B is a Galois Azumaya extension of B^G with Galois group G , $B = B^G \cdot V_B(B^G) \cong B^G \otimes_{C^G} V_B(B^G)$ such that $V_B(B^G)$ is Galois algebra over C^G with Galois group $G|_{V_B(B)} \cong G$ ([1], Theorem 2). By hypothesis, $G = \text{Aut}_{B^G}(B)$, so $G|_{V_B(B)} = \text{Aut}_{C^G}(V_B(B^G))$. Thus by Theorem 4.6, either $V_B(B^G)$ is commutative with no idempotents but 0 and 1, or $V_B(B^G) \cong C^G \oplus C^G$ where C^G contains no idempotents but 0 and 1. Noting that $B = B^G \cdot V_B(B^G)$ implies that the center of $V_B(B^G)$ is C , we conclude that either B is a DeMeyer-Kanzaki Galois extension with no central idempotents but 0 and 1, or $B \cong B^G \oplus B^G$ where B^G contains no central idempotents but 0 and 1; and so B contains only two minimal central idempotents, $e = 1 \oplus 0$ and $1 - e$. Thus for a $g \neq 1$ in G , $g(e) = 1 - e$ and $g(1 - e) = e$. Therefore $G = \{1, g\}$ is of order 2 such that $g(be) = b(1 - e)$ and $g(b(1 - e)) = be$ for each $b \in B^G$.

(\impliedby) If B is a DeMeyer-Kanzaki Galois extension with no central idempotents but 0 and 1, then C is a commutative Galois algebra with Galois group $G|_C \cong G$ with no idempotents but 0 and 1. Hence $G \cong G|_C = \text{Aut}_{C^G}(C)$ ([3], Theorem 3.5). But $B = B^G \cdot C \cong B^G \otimes_{C^G} C$ ([4], Lemma 2), so $G \cong G|_C = \text{Aut}_{C^G}(C) \cong \text{Aut}_{B^G}(B)$. Next, assume $B = B^G \oplus B^G$ which is a Galois extension of B^G with Galois group G of order 2 where $G = \{1, g\}$ such that $g(be) = b(1 - e)$ and $g(b(1 - e)) = be$ for each $b \in B^G$, and $e = 1 \oplus 0$ is a minimal central idempotent of B . Since any non identity element in $\text{Aut}_{B^G}(B)$ permutes $\{e, 1 - e\}$ and $B = B^G \oplus B^G$, $\text{Aut}_{B^G}(B) = \{1, g\} = G$.

REFERENCES

- [1] R. Alfaro and G. Szeto, Skew Group Rings which are Azumaya, *Comm. in Algebra* **23**, No. 6 (1995), 2255-2261.
- [2] R. Alfaro and G. Szeto, On Galois Extensions of an Azumaya Algebra, *Comm. in Algebra* **25**, No. 6 (1997), 1873-1882.
- [3] S.U. Chase, D.K. Harrison, A. Rosenberg, "Galois Theory and Galois Cohomology of Commutative Rings", *Memoirs Amer. Math. Soc.* No. 52, 1965.
- [4] F.R. DeMeyer, Some Notes on the General Galois Theory of Rings, *Osaka J. Math.* **2** (1965), 117-127.
- [5] F.R. DeMeyer, Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.* **10** (1966), 287-295.
- [6] F.R. DeMeyer, Projective Modules over Central Separable Algebras, *Canadian J. Math.* **21** (1969), 117-127.
- [7] F.R. DeMeyer and E. Ingraham, "Separable algebras over commutative rings", Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.
- [8] T. Kanzaki, On Galois Algebra Over A Commutative Ring, *Osaka J. Math.* **2** (1965), 309-317.
- [9] K. Kishimoto and T. Nagahara, On G -extensions of a semi-connected ring. *Math. J. Okayama Univ.* **32** (1990), 25-42.