On Central Galois Algebras of a Galois Algebra

George Szeto and **Lianyong Xue**

Department of Mathematics, Bradley University
Peoria, Illinois 61625, USA
Email: szeto@hilltop.bradley.edu lxue@hilltop.bradley.edu

Abstract. Let B be a Galois algebra over R with Galois group G, C the center of B, $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ for each $g \in G$, e_g an idempotent in C such that $BJ_g = e_gB$, $K_g = \{g \in G \,|\, g(e_gc) = e_gc$ for each $e_gc \in e_gC\}$, and $B_g = \sum_{k\in K_g} e_gJ_k$. Then characterizations are given for B_g being a central Galois algebra with Galois group K_g. Consequently, the results of DeMeyer and Kansaki on central Galois algebras are generalized respectively.

2000 Mathematics Subject Classification: 16S35, 16W20

1 Introduction

Let B be a Galois algebra over a commutative ring R with Galois group G, C the center of B, and $K = \{g \in G \,|\, g(c) = c$ for each $c \in C\}$. A natural question is whether B is a central Galois algebra with Galois group K. The answer is affirmative if R contains no idempotents but 0 and 1 ([2], Theorem 1). For any R, a central Galois algebra with Galois group K was characterized in terms of $\{J_g \,|\, g \in G\}$ where $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ ([5], Proposition 3). We note that for an $g \in G$, $BJ_g = e_gB$ for some central idempotent e_g in C ([5]). Let $K_g = \{g \in G \,|\, g(e_gc) = e_gc$ for each $e_gc \in e_gC\}$ and $B_g = \sum_{k\in K_g} e_gJ_k$. Then K_g is a subgroup of G and B_g is invariant under K_g. The purpose of the present paper is to characterize a central Galois algebra B_g with Galois group K_g in terms of the Azumaya Galois extension $(e_gB)^L$ with Galois group K_g/L where $L = \{k \in K_g \,|\, k(a) = a$ for all $a \in B_g\}$, and the Azumaya Galois extension is in the sense of [1]. Consequently, our results derive a characterization of the central Galois algebra B_1 $(= \sum_{h\in K} J_h)$ with Galois group K $(= K_1)$, and the central Galois algebra B in which $e_g = 0$ or 1 for any $g \in G$, respectively; and so the results of DeMeyer and Kansaki on central Galois algebras are generalized respectively.

2 Basic Definitions and Notations

Throughout, let B be a Galois algebra over a commutative ring R with Galois group G, C the center of B, $K = \{g \in G \,|\, g(c) = c$ for each $c \in C\}$, $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ for each $g \in G$, e_g a central idempotent in C such that $BJ_g = e_gB$ ([5]), $G(e_g) = \{g \in G \,|\, g(e_g) = e_g\}$, $K_g = \{g \in G \,|\, g(e_gc) = e_gc$ for each $e_gc \in e_gC\}$, $B_g = \sum_{h \in K_g} e_gJ_h$ for each $g \in G$, and $J_g^{(A)} = \{a \in A \,|\, ax = g(x)a$ for all $x \in A\}$ for a subring A of B. We keep the definitions of a Galois extension, a Galois algebra, a central Galois algebra, a separable extension, and an Azumaya algebra as defined in ([6]). An Azumaya Galois extension A with Galois group G is a Galois extension A of A^G which is a C^G-Azumaya algebra where C the center of A ([1]).

3 Central Galois Algebras B_g

Keeping the definitions and notations in section 2, let $K_g = \{g \in G \,|\, g(e_gc) = e_gc$ for each $e_gc \in e_gC\}$ and $B_g = \sum_{h \in K_g} e_gJ_h$ for each $g \in G$. Noting that K_g is an Azumaya automorphism group of e_gB, we have that $(e_gJ_{k_1})(e_gJ_{k_1}) = e_gJ_{k_1k_2}$ for any $k_1, k_2 \in K_g$, and so B_g is a subring of e_gB and invariant under K_g. We shall characterize the central Galois algebra B_g with Galois group $\overline{K_g}$ $(= K_g/L)$ where $L = \{k \in K_g \,|\, k(a) = a$ for all $a \in B_g\}$ in terms of the Azumaya Galois extension $(e_gB)^L$ with Galois group $\overline{K_g}$, and derive some consequences when $e_g = 1$ and $e_g = 0$ or 1 for any $g \in G$, respectively. We begin with some properties of K_g, B_g, and $(e_gB)^{K_g}$.

Lemma 3.1. *The order of K_g is a unit in e_gC.*

Proof. Since B is a Galois algebra over R with Galois group G, there exists a $c \in C$ such that $\mathrm{Tr}_G(c) = 1$ by Proposition 5 in [5] on page 314. Clearly, $G(e_g)$ $(= \{g \in G \,|\, g(e_g) = e_g\})$ is a subgroup of G, and K_g is a subgroup of $G(e_g)$. Let $\{G(e_g)h_i \,|\, h_i \in G,\, i = 1, 2, \cdots, n$ for some integer $n\}$ be the set of the right cosets of $G(e_g)$ in G and $d = \sum_{i=1}^n h_i(c)$. Then $\mathrm{Tr}_{G(e_g)}(d) = \sum_{g \in G(e_g)} g(d) = \sum_{g \in G(e_g)} \sum_{i=1}^n gh_i(c) = \mathrm{Tr}_G(c) = 1$. Noting that

$g(e_g) = e_g$ for each $g \in G(e_g)$, we have that $\mathrm{Tr}_{G(e_g)}(e_g d) = e_g$. Next, let $\{g_i K_g \,|\, g_i \in G(e_g),\, i = 1, 2, \cdots, m$ for some integer $m\}$ be the set of the left cosets of K_g in $G(e_g)$. Noting that $e_g C \subset (e_g B)^{K_g}$ by the definition of K_g, we have that $e_g = \mathrm{Tr}_{G(e_g)}(e_g d) = \sum_{i=1}^{m} \sum_{k \in K_g} g_i k(e_g d) = |K_g| \sum_{i=1}^{m} g_i(e_g d)$ where $|K_g|$ is the order of K_g. But e_g is the identity of $e_g C$, so $|K_g|$ is a unit in $e_g C$.

Lemma 3.2. *$(e_g B)^{K_g}$ is a separable algebra over $e_g R$.*

Proof. Since B is a Galois algebra over R with Galois group G, B is a separable algebra over R. Hence $e_g B$ is a separable algebra over $e_g R$ ([3], Proposition 1.11, page 46). Since B is a Galois algebra over R with Galois group G again, $e_g B$ is a Galois extension of $(e_g B)^{K_g}$ with Galois group K_g because $e_g \in C^{K_g}$ ([6], Lemma 3.7). Hence $e_g B$ is a finitely generated and projective left (or right) module over $(e_g B)^{K_g}$. Moreover, by Lemma 3.1, the order of K_g is a unit in $e_g C$, so $(e_g B)^{K_g}$ is a direct summand of $e_g B$ as a bimodule over $(e_g B)^{K_g}$. Thus $(e_g B)^{K_g}$ is a separable algebra over $e_g R$ by the proof of Theorem 3.8 on page 55 in [3] for Be_g is a separable algebra over $e_g R$.

Lemma 3.3. *Let Z be the center of B_g. Then B_g and $(e_g B)^{K_g}$ are Azumaya algebras over Z such that $B_g = V_{e_g B}((e_g B)^{K_g})$ and $V_{e_g B}(B_g) = (e_g B)^{K_g}$.*

Proof. Since B is a Galois algebra over R with Galois group G, $e_g B$ is a Galois extension of $(e_g B)^{K_g}$. Hence $V_{e_g B}((e_g B)^{K_g}) = \oplus \sum_{k \in K_g} J_k^{(e_g B)}$. But, by Lemma 3.3 in [6], $J_k^{(Be_g)} = e_g J_k$ for each $k \in K_g$, so $V_{e_g B}((e_g B)^{K_g}) = \oplus \sum_{k \in K_g} e_g J_k = B_g$. By Lemma 3.2, $(e_g B)^{K_g}$ is a separable algebra over $e_g R$, so $(e_g B)^{K_g}$ is a separable subalgebra of the Azumaya algebra $e_g B$ over $e_g C$. Thus B_g $(= V_{e_g B}((e_g B)^{K_g}))$ is a separable subalgebra of $e_g B$ over $e_g C$, and $V_{e_g B}(B_g) = (e_g B)^{K_g}$ by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). This implies that B_g and $(e_g B)^{K_g}$ are Azumaya algebras over the same center Z.

Lemma 3.4. *Let $L = \{k \in K_g \mid k(a) = a$ for all $a \in B_g\}$. Then*

(1) the order of L is a unit in e_gB and

(2) $(e_gB)^L$ is a Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$ $(= K_g/L)$.

Proof. (1) By Lemma 3.1, the order of K_g is a unit in e_gB. But L is a subgroup of K_g, so the order of L is a unit in e_gB.

(2) Since B is a Galois algebra with Galois group G, e_gB is a Galois extension of $(e_gB)^{G(e_g)}$ with Galois group $G(e_g)$ ([6], Lemma 3.7). Noting that $L \subset K_g \subset G(e_g)$ as normal subgroups, we have that $(e_gB)^L$ is a Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$.

Lemma 3.5. *Let A be an Azumaya Galois extension of A^G with Galois group G. Then $A = A^G \cdot V_A(A^G) \cong A^G \otimes_{C^G} V_A(A^G)$ where C is the center of A.*

Proof. Since A is an Azumaya Galois extension of A^G with Galois group G, A^G is an Azumaya C^G-algebra by definition and the skew group ring $A * G$ is an Azumaya C^G-algebra by Theorem 1 in [1]. Hence $A * G$ is an Azumaya C^G-algebra containing an Azumaya subalgebra A^G. Thus $A * G = A^G \cdot V_{A*G}(A^G) \cong A^G \otimes_{C^G} V_{A*G}(A^G)$ as Azumaya C^G-algebras by the commutator theorem for Azumaya algebras ([3], Theorem 4.3, page 57). Since $V_{A*G}(A^G) = V_A(A^G) * G$, $A * G \cong (A^G \otimes_{C^G} V_A(A^G)) * G$. This implies that $A \cong A^G \otimes_{C^G} V_A(A^G) \cong A^G \cdot V_A(A^G)$, and so $A = A^G \cdot V_A(A^G)$.

Next we show the main theorem.

Theorem 3.6. *Let $e_g \neq 0$ for an $g \in G$. Then the following are equivalent:*

(1) B_g is a central Galois algebra over Z with Galois group $\overline{K_g}$.

(2) $(e_gB)^L = (B_g)(e_gB)^{K_g}$.

(3) $(e_gB)^L$ is an Azumaya Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$.

Proof. (1) $\Longrightarrow$ (2) Since B_g is a central Galois algebra over Z with Galois group $\overline{K_g}$, $B_g \otimes_Z (e_gB)^{K_g}$ is a Galois extension of $Z \otimes_Z (e_gB)^{K_g}$ with Galois group $\overline{K_g} \otimes 1$. But

$B_g \otimes_Z (e_gB)^{K_g}$ is an Azumaya Z-algebra by Lemma 3.3, so $B_g \otimes_Z (e_gB)^{K_g} \cong (B_g)(e_gB)^{K_g}$ ([3], Theorem 4.4, page 58). Hence $(B_g)(e_gB)^{K_g}$ is a Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$ ($\cong \overline{K_g} \otimes 1$). Noting that $B_g \subset (e_gB)^L$ and $(e_gB)^{K_g} \subset (e_gB)^L$, we have that $(B_g)(e_gB)^{K_g} \subset (e_gB)^L$ which are Galois extensions of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$. Thus $(e_gB)^L = (B_g)(e_gB)^{K_g}$.

(2) $\Longrightarrow$ (3) By Lemma 3.4, $(e_gB)^L$ is a Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$. By Lemma 3.3, B_g and $(e_gB)^{K_g}$ are Azumaya algebras over Z, so $(e_gB)^L = (B_g)(e_gB)^{K_g} \cong B_g \otimes_Z (e_gB)^{K_g}$ which is an Azumaya algebra over Z. Noting that $Z^{K_g} = Z$, we conclude that $(e_gB)^L$ is an Azumaya Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$.

(3) $\Longrightarrow$ (2) By hypothesis, $(e_gB)^L$ is an Azumaya Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$, so $(e_gB)^L = ((e_gB)^L)^{K_g} \cdot V_{(e_gB)^L}(((e_gB)^L)^{K_g})$ by Lemma 3.5. Since $((e_gB)^L)^{K_g} = (e_gB)^{K_g}$ for L is a subgroup of K_g, it suffices to show that $V_{(e_gB)^L}((e_gB)^{K_g}) = B_g$. In fact, since $B_g = V_{e_gB}((e_gB)^{K_g})$ by Lemma 3.3, and $B_g \subset (e_gB)^L \subset e_gB$, we have that $B_g = V_{B_g}((e_gB)^{K_g}) \subset V_{(e_gB)^L}((e_gB)^{K_g}) \subset V_{e_gB}((e_gB)^{K_g}) = B_g$. Thus $V_{(e_gB)^L}((e_gB)^{K_g}) = B_g$.

(2) $\Longrightarrow$ (1) By Lemma 3.3, $(B_g)(e_gB)^{K_g} \cong B_g \otimes_Z (e_gB)^{K_g}$ as Azumaya Z-algebras such that $B_g = V_{(e_gB)^L}((e_gB)^{K_g}) = \oplus \sum_{\overline{k} \in \overline{K_g}} J_{\overline{k}}^{((e_gB)^L)}$. By hypothesis, $(e_gB)^L = (B_g)(e_gB)^{K_g}$ which is an Azumaya Galois extension of $(e_gB)^{K_g}$ with Galois group $\overline{K_g}$, so it can be check that $J_{\overline{k}}^{((e_gB)^L)} = J_{\overline{k}}^{(B_g)}$ for each $\overline{k} \in \overline{K_g}$. Hence $B_g = \oplus \sum_{\overline{k} \in \overline{K_g}} J_{\overline{k}}^{(B_g)}$. Noting that $Z^{\overline{K_g}} = Z$ and that B_g is an Azumaya Z-algebra, we conclude that $J_{\overline{k}}^{(B_g)} J_{\overline{k}^{-1}}^{(B_g)} = Z$ for all $\overline{k} \in \overline{K_g}$. Thus B_g is a central Galois algebra with Galois group $\overline{K_g}$ ([4], Theorem 1).

When $e_g = 1$, Theorem 3.6 derives a characterization of the central Galois algebra B_1 ($= \sum_{h \in K} J_h$) with Galois group K ($= K_1$), and the central Galois algebra B in which $e_g = 0$ or 1 for any $g \in G$, respectively. We recall that $K = \{g \in G \,|\, g(c) = c$ for each

$c \in C\}$.

Corollary 3.7. *Let* $B_K = \sum_{h\in K} J_h$ *and* $L = \{k \in K \mid k(a) = a$ *for all* $a \in B_K\}$. *Then* B_K *is a central Galois algebra with Galois group* K *if and only if* $B^L = B_K B^K$ *which is an Azumaya Galois extension of* B^K *with Galois group* K/L.

Proof. It is easy to check that $K_1 = K$ and $B_1 = B_K$, so the corollary is the case $e_g = 1$ of Theorem 3.6.

Corollary 3.8. B *is a central Galois algebra with Galois group* K *if and only if* $e_g = 1$ *or 0 for each* $g \in G$.

Proof. ($\Longrightarrow$) Since B is a central Galois algebra with Galois group K, $B = \oplus\sum_{h\in K} J_h$. But B is a Galois algebra with Galois group G, so $B = \oplus\sum_{g\in G} J_g$. Thus $\oplus\sum_{g\notin K} J_g = \{0\}$. Therefore $J_g = \{0\}$, that is, $e_g = 0$ for each $g \notin K$. Noting that $K = K_1$, we have that $e_g = 1$ or 0 for each $g \in G$.

($\Longleftarrow$) Since B is a Galois algebra with Galois group G, $B = \oplus\sum_{g\in G} J_g$. But $e_g = 1$ or 0 for each $g \in G$ by hypothesis, so $B = \sum_{h\in K_1} J_h = \sum_{h\in K} J_h = B_1 = B_K$ where B_K is defined in Corollary 3.7. Hence B $(= B_K)$ is a central Galois algebra with Galois group K by Corollary 3.7 because $B^L = B = B_K B^K$.

Corollary 3.9 ([2], Theorem 1) *If* C *contains no idempotents but 0 and 1, then* B *is a central Galois algebra with Galois group* K.

Proof. Since C contains no idempotents but 0 and 1, $e_g = 1$ or 0 for each $g \in G$. Hence by Corollary 3.8, B is a central Galois algebra with Galois group K.

Corollary 3.10. ([5], Proposition 3) B *is a central Galois algebra with Galois group* K *if and only if* $J_g = \{0\}$ *for each* $g \notin K$.

Proof. By noting that $K_1 = K$ and that $J_g = \{0\}$ if and only if $e_g = 0$, the corollary is an immediate consequence of Corollary 3.8.

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

References

[1] R. Alfaro and G. Szeto, On Galois extensions of an Azumaya algebra. *Comm. in Algebra,* 25(6): 1873-1882, 1997.

[2] F. R. DeMeyer, Galois theory in separable algebras over commutative rings, *Illinois J. Math.,* 10: 287-295, 1966.

[3] F. R. DeMeyer and E. Ingraham, Separable algebras over commutative rings, Volume 181. Springer Verlag, Berlin, Heidelberg, New York, 1971.

[4] M. Harada, Supplementary results on Galois extension, *Osaka J. Math.,* 2: 343-350, 1965

[5] T. Kanzaki, On Galois algebra over a commutative ring. *Osaka J. Math.,* 2: 309-317, 1965.

[6] G. Szeto and L. Xue, The structure of Galois algebras. *Journal of Algebra,* Vol. 237, No. 1: 238-246, 2001.