

On a Generalization of the DeMeyer Theorem for Galois Algebras

George Szeto and Lianyong Xue

Department of Mathematics, Bradley University
Peoria, Illinois 61625 – U.S.A.

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

1 Introduction

Let B be a Galois algebra over a commutative ring R with Galois group G , C the center of B , and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. In [1], it was shown that if C contains no idempotents but 0 and 1, then B is a central Galois algebra with Galois group K and C is a commutative Galois algebra with Galois group G/K ([1], Theorem 1). When C admits more idempotents such that $J_g = \{0\}$ for each $g \notin K$ where $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$ for each $g \in G$, the above conclusion also holds for B ([3]). Moreover, another sufficient condition was given for a central Galois algebra B with Galois group G : if $B = \bigoplus_{g \in G} J_g$, B is a separable R -algebra, and $J_g J_{g^{-1}} = C$ for each $g \in G$, then B is a central Galois algebra with Galois group G ([2], Theorem 1). Recently, using the Boolean algebra B_a generated by $\{0, e_g \mid g \in G\}$ where $B J_g = B e_g$, the following structure theorem of B was shown in [5]: There exist idempotents $\{e_i \mid i = 1, 2, \dots, m \text{ for some integer } m\}$ in B_a such that $B = \bigoplus_{i=1}^m B e_i \oplus B f$ where $B e_i$ is a central Galois algebra with Galois group $H_i (= \{h \in G \mid e_h e_i = e_i\})$ for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m e_i$, and $B f = C f$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G in case $1 \neq \sum_{i=1}^m e_i$. The purpose of the present paper is to show that the above decomposition is unique, that is, if there exist idempotents $\{e'_i \mid i = 1, 2, \dots, m' \text{ for some integer } m'\}$ in B_a such that $B = \bigoplus_{i=1}^{m'} B e'_i \oplus B f'$ where $B e'_i$ is a central Galois algebra with Galois group $H_i (= \{h \in G \mid e_h e'_i = e'_i\})$ for each $i = 1, 2, \dots, m'$, $f' = 1 - \sum_{i=1}^{m'} e'_i$, and $B f' = C f'$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G , then $m = m'$ and $\{e_i \mid i = 1, 2, \dots, m\} = \{e'_i \mid i = 1, 2, \dots, m'\}$. Moreover, we shall show that these e_i are the only idempotents in B_a such that $B e_i$ are central Galois algebras with Galois groups $H_i (= \{h \in G \mid e_h e_i = e_i\})$, that is, if $B e$ is a central Galois algebra with Galois group $H_e (= \{h \in G \mid e_h e = e\})$ for an idempotent e in B_a , then $e = e_i$ for some $1 \leq i \leq m$. Also, f is the only idempotent in B_a such that $B f$ is a commutative Galois algebra with Galois group induced by and isomorphic with G , that is, if $B e$ is a

commutative Galois algebra for an idempotent e in B_a with Galois group induced by and isomorphic with G , then $e = f$. Our results generalize the DeMeyer theorem for Galois algebras ([1], Theorem 1), and the characterization of a central Galois algebra shown by Kanzaki ([3], Proposition 3).

2 Definitions and Notations

Let B be a ring with 1, C the center of B , G a finite automorphism group of B , and B^G the set of elements in B fixed under each element in G . 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 $g \in G$. 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 extension if B is a Galois extension of C . Throughout this paper, we will assume that B is a Galois algebra with Galois group G . Let $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$. In [3], it was shown that $BJ_g = Be_g$ for some central idempotent e_g of B . We denote $(B_a; \dot{+}, \cdot)$ the Boolean algebra generated by $\{0, e_g \mid g \in G\}$ where $e \cdot e' = ee'$ and $e \dot{+} e' = e + e' - ee'$ for any e and e' in B_a . In [5], it was shown that there exist idempotents $\{e_i \mid i = 1, 2, \dots, m$ for some integer $m\}$ in B_a and some subgroups H_i of G such that $B = \oplus \sum_{i=1}^m Be_i \oplus Bf$ where Be_i is a central Galois algebra with Galois group H_i for each $i = 1, 2, \dots, m$, $f = 1 - \sum_{i=1}^m e_i$, and $Bf = Cf$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G in case $1 \neq \sum_{i=1}^m e_i$ ([5], Theorem 3.8). Throughout, $(B_a; +, \cdot)$ denotes the Boolean algebra generated by $\{0, e_g \mid g \in G\}$, $\{e_i, f \mid i = 1, 2, \dots, m\}$ are as given in Theorem 3.8 in [5], and $H_e = \{g \in G \mid e \leq e_g\}$ for each $e \in B_a$.

3 Galois Extensions Generated by an Idempotent

In this section, keeping the notations in section 2, we shall show that the decomposition in Theorem 3.8 in [5] is unique and that $\{e_i \mid i = 1, 2, \dots, m\}$ are the only idempotents in B_a such that Be_i are central Galois algebras with Galois groups H_{e_i} . Also, f is the only idempotent in B_a such that Bf is a commutative Galois algebra with Galois group induced by and isomorphic with G .

Lemma 3.1. *Let $\{e_i, f \mid i = 1, 2, \dots, m\}$ and the subgroups $\{H_i \mid i = 1, 2, \dots, m\}$ of G be given in Theorem 3.8 in [5]. Then*

- (1) $\{e_i, f \mid i = 1, 2, \dots, m\}$ is the set of all minimal elements of B_a in case $f \neq 0$,
(2) for each $e \neq 0$ in B_a , there exists a unique subset Z_e of the set $\{1, 2, \dots, m\}$ such that
 $e = \sum_{i \in Z_e} e_i$ or $e = \sum_{i \in Z_e} e_i + f$,
(3) $H_i = H_{e_i}$ for each $i = 1, 2, \dots, m$, and
(4) the subgroups $\{H_i \mid i = 1, 2, \dots, m\}$ are different subgroups of G .

Proof. For (1) and (2), see Lemma 3.1 in [7].

(3) By the definition of H_i ([5], Theorem 3.8), H_i is a maximum subset of G such that $e_i = \prod_{g \in H_i} e_g \neq 0$ or a maximum subset of G such that $e_i = (1 - \sum_{j=1}^t e_j) \prod_{g \in H_i} e_g \neq 0$ for some $t < i$. Hence for each $g \in G$, we have that $e_i e_g = e_i$ if and only if $g \in H_i$. Therefore $H_i = H_{e_i}$ for each $i = 1, 2, \dots, m$.

(4) For any $1 \leq i < i' \leq m$, by the definition of H_i ([5], Theorem 3.8), either (i) $H_{i'} = gH_i g^{-1}$ for some $g \notin N(H_i)$, the normalizer of H_i in G or (ii) $e_{i'} = (1 - \sum_{j=1}^{t'} e_j) \prod_{g \in H_{i'}} e_g$ for some $i \leq t' < i'$. In case (i), $H_{i'}$ is different from H_i . In case (ii), if $H_{i'} = H_i$, then $e_{i'} = (1 - \sum_{j=1}^{t'} e_j) \prod_{g \in H_{i'}} e_g = (1 - \sum_{j=1}^{t'} e_j) \prod_{g \in H_i} e_g = (1 - \sum_{j=1}^{t'} e_j) (1 - \sum_{j=1}^t e_j) \prod_{g \in H_i} e_g = (1 - \sum_{j=1}^{t'} e_j) e_i = 0$ for $t < i \leq t'$. This is a contradiction. Hence $H_{i'} \neq H_i$. This completes the proof.

Lemma 3.2. For any $e, e' \neq 0$ in B_a , $H_{e+e'} = H_e \cap H_{e'}$.

Proof. By Theorem 3.3 in [7], it is immediate.

Theorem 3.3. Let $e \neq 0$ in B_a . Then

- (1) Be is a central Galois algebra with Galois group H_e if and only if $e = e_i$ for some $1 \leq i \leq m$.
(2) Be is a commutative Galois algebra with Galois group induced by and isomorphic with G if and only if $e = f$.

Proof. (1) (\implies) Since Be is a central Galois algebra over Ce with Galois group H_e , $Be = \bigoplus_{h \in H_e} J_h^{(Be)}$ where $J_h^{(Be)} = \{b \in Be \mid bx = h(x)b \text{ for all } x \in Be\}$ for each $h \in H_e$ ([3], Theorem 1). By Lemma 3.3 in [5], $J_h^{(Be)} = eJ_h$ for each $h \in H_e$, so $Be = \bigoplus_{g \in H_e} eJ_g$. Since B is a Galois algebra over R with Galois group G , $B = \bigoplus_{g \in G} J_g$. Hence $Be = \bigoplus_{g \in G} eJ_g = (\bigoplus_{h \in H_e} eJ_h) \oplus (\bigoplus_{g \notin H_e} eJ_g)$. Thus $eJ_g = \{0\}$, that is,

$$(*) \quad ee_g = 0 \text{ for each } g \notin H_e.$$

Now assume that $e \neq e_i$ for $i = 1, 2, \dots, m$. Then by Lemma 3.1, $e = \sum_{i \in Z_e} e_i$ with $|Z_e| \geq 2$ or $e = \sum_{i \in Z_e} e_i + f$ and $f \neq 0$. In case $e = \sum_{i \in Z_e} e_i$ with $|Z_e| \geq 2$, by Lemma 3.2, $H_e = \cap_{i \in Z_e} H_{e_i}$. By Lemma 3.1 again, $H_i = H_{e_i}$ for each $i = 1, 2, \dots, m$ and the subgroups $\{H_i \mid i = 1, 2, \dots, m\}$ are different subgroups of G , so there exists an $i \in Z_e$ such that $H_e \subset H_{e_i}$ but $H_e \neq H_{e_i}$. Thus there exists an $g \in H_{e_i}$ but $g \notin H_e$. For such an g , we have that $e_i e_g = e_i \neq 0$ since $g \in H_{e_i}$. Also, noting that $e_i \leq e$, we have that $e_i e_g = e_i e e_g = 0$ since $g \notin H_e$ by the earlier result (*). This is a contradiction. In case $e = \sum_{i \in Z_e} e_i + f$ and $f \neq 0$, $Be = \oplus \sum_{i \in Z_e} Be_i \oplus Bf$ where $Bf = Cf$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G . Thus Cf is a commutative Galois algebra over $(Cf)^{H_e}$ with Galois group induced by and isomorphic with H_e ; and so $H_e|_{Cf} \neq \{1\}$. Therefore $(Be)^{H_e} \neq Ce$. This contradicts to that Be is a central Galois algebra over Ce with Galois group H_e . Consequently, $e = e_i$ for some $1 \leq i \leq m$.

(\Leftarrow) It is a consequence of Theorem 3.8 in [5] and Lemma 3.1.

(2) (\Rightarrow) By Lemma 3.1, $e = \sum_{i \in Z_e} e_i$ or $e = \sum_{i \in Z_e} e_i + f$ and $f \neq 0$. If $e = \sum_{i \in Z_e} e_i$, then $Be = \oplus \sum_{i \in Z_e} Be_i$ where Be_i is a central Galois algebra with Galois group H_i ; and so Be is not commutative, a contradiction. Hence $e = \sum_{i \in Z_e} e_i + f$ and $f \neq 0$. If Z_e is not empty, then Be is not commutative, a contradiction again. Thus $e = f$.

(\Leftarrow) This is given by Theorem 3.8 in [5].

Theorem 3.4. *Let $\{e_i \mid i = 1, 2, \dots, m\}$ be given in Theorem 3.8 in [5]. If there exist idempotents $\{e'_i \mid i = 1, 2, \dots, m'\}$ for some integer m' in B_a such that $B = \oplus \sum_{i=1}^{m'} Be'_i \oplus Bf'$ where Be'_i is a central Galois algebra with Galois group $H_{e'_i}$ for each $i = 1, 2, \dots, m'$, $f' = 1 - \sum_{i=1}^{m'} e'_i$, and $Bf' = Cf'$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G , then $m = m'$ and $\{e_i \mid i = 1, 2, \dots, m\} = \{e'_i \mid i = 1, 2, \dots, m'\}$.*

Proof. It is an immediate consequence of Lemma 3.1 and Theorem 3.3.

Theorem 3.5. *Let B be a Galois algebra with Galois group G , C the center of B , and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. Then*

(1) $K = H_1$ where $H_1 = \{g \in G \mid 1 \leq e_g\} = \{g \in G \mid e_g = 1\}$.

(2) B is a central Galois algebra with Galois group K and C is a commutative Galois

algebra with Galois group G/K if and only if $B_a = \{0, 1\}$.

Proof. (1) For any $g \in H_1$, $BJ_g = Be_g = B$. But $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$, so for any $b \in J_g$, $b(g(c) - c) = 0$ for all $c \in C$. Therefore $B(g(c) - c) = BJ_g(g(c) - c) = \{0\}$. Thus $g(c) = c$ for all $c \in C$; and so $H_1 \subset K$. Conversely, for any $g \in K$, g is an Azumaya algebra automorphism of B over C , so $BJ_g = B$ ([4], Proposition 4). Hence $e_g = 1$. Thus $g \in H_1$. This implies that $K = H_1$.

(2) (\Leftarrow) Since $B_a = \{0, 1\}$, 1 is the minimal element of B_a . Therefore, by Theorem 3.3, B is a central Galois algebra with Galois group H_1 . But by (1), $K = H_1$, so B is a central Galois algebra with Galois group K . Moreover, the order of K is a unit in B ([3], Corollary 3), so C is a commutative Galois algebra with Galois group G/K .

(\Rightarrow) By hypothesis, B is a central Galois algebra with Galois group K . But by (1), $K = H_1$, so B is a central Galois algebra over C with Galois group H_1 . Hence 1 is the minimal element of B_a by Theorem 3.3. Thus $B_a = \{0, 1\}$.

Theorem 3.5 is a generalization of the DeMeyer theorem for Galois algebras, and the characterization of a central Galois algebra shown by Kanzaki is also derived.

Corollary 3.6. ([1], Theorem 1) *Let B be a Galois algebra with Galois group G , C the center of B , and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. If C contains no idempotents but 0 and 1, then B is a central Galois algebra with Galois group K and C is a commutative Galois algebra with Galois group G/K .*

Proof. Since C contains no idempotents but 0 and 1, $B_a = \{0, 1\}$. Hence by Theorem 3.5, B is a central Galois algebra with Galois group K and C is a commutative Galois algebra with Galois group G/K .

Corollary 3.7. ([3], Proposition 3) *Let B be a Galois algebra with Galois group G , C the center of B , and $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$. Then B is a central Galois algebra with Galois group K and C is a commutative Galois algebra with Galois group G/K if and only if $J_g = \{0\}$ for each $g \notin K$.*

Proof. (\Leftarrow) Since $J_g = \{0\}$ for each $g \notin K$, $e_g = 0$ for each $g \notin K$. But by Theorem 3.5-(1), $e_g = 1$ for each $g \in K$, so $B_a = \{0, 1\}$. Thus by Theorem 3.5-(2), B is a central

Galois algebra with Galois group K and C is a commutative Galois algebra with Galois group G/K .

(\implies) Since B is a central Galois algebra with Galois group $K (= H_1)$, 1 is the minimal element of B_a by Theorem 3.3. Hence $B_a = \{0, 1\}$. Therefore $e_g = \{0\}$ for each $g \notin K$, that is, $J_g = \{0\}$ for each $g \notin K$.

Remark: Let $G(e) = \{g \in G \mid g(e) = e\}$ for each $e \neq 0$ in B_a and $\{e_i \mid i = 1, 2, \dots, m\}$ be given in Theorem 3.8 in [5]. Then it can be shown that H_{e_i} is a normal subgroup of $G(e_i)$ and Ce_i is a commutative Galois algebra with Galois group $G(e_i)/H_{e_i}$ for each $i = 1, 2, \dots, m$.

References

- [1] F. DeMeyer. Galois theory in separable algebras over commutative rings, *Illinois J. Math.*, 10: 287-295, 1966.
- [2] M. Harada, Supplementary results on Galois extension, *Osaka J. Math.*, 2: 343-350, 1965
- [3] T. Kanzaki. On Galois algebra over a commutative ring. *Osaka J. Math.*, 2: 309-317, 1965.
- [4] A. Rosenberg and D. Zelinsky, Automorphisms of separable algebras, *Pacific J. Math.*, 11: 1109-1117, 1961
- [5] G. Szeto and L. Xue. The structure of Galois algebras. *Journal of Algebra*, Vol. 237, No. 1: 238-246, 2001.
- [6] G. Szeto and L. Xue. The Boolean algebra and central Galois algebras, *International Journal of Mathematics and Mathematical Sciences*, Vol. 28, No. 4(2001), 237-242.
- [7] G. Szeto and L. Xue. The Boolean algebra of Galois algebras, *International Journal of Mathematics and Mathematical Sciences*, (to appear).