THE BOOLEAN ALGEBRA AND CENTRAL 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

ABSTRACT. Let B be a Galois algebra with Galois group G, $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$ for a $g \in G$, and $BJ_g = Be_g$ for a central idempotent e_g. Then a relation is given between the set of elements in the Boolean algebra $(B_a, \leq)$ generated by $\{0, e_g \mid g \in G\}$ and a set of subgroups of G, and a central Galois algebra Be with a Galois subgroup of G is characterized for an $e \in B_a$.

Keywords and phrases. Galois algebras, central Galois algebras, and Boolean algebras.

2000 Mathematics Subject Classification. Primary 16S35, 16W20

1. Introduction. Galois theory of rings have been intensively studied ([1], [3], [4], [5], [6], [7]). Let B be a Galois algebra with Galois group G and $J_g = \{b \in B \mid bx = g(x)b$ for all $x \in B\}$ for each $g \in G$. In [4], it was shown that $BJ_g = Be_g$ for some central idempotent e_g of B. Let B_a be the Boolean algebra generated by $\{0, e_g \mid g \in G\}$. In [7], the following structure theorem for B was given: There exist $\{e_i \in B_a \mid i = 1, 2, ..., m$ for some integer $m\}$ and some subgroups H_i of G such that $B = \oplus \sum_{i=1}^{m} Be_i \oplus B(1 - \sum_{i=1}^{m} e_i)$ where Be_i is a central Galois algebra with Galois group H_i for each $i = 1, 2, ..., m$ and $B(1 - \sum_{i=1}^{m} e_i) = C(1 - \sum_{i=1}^{m} e_i)$ which is a commutative Galois algebra with Galois group induced by and isomorphic with G in case $1 \neq \sum_{i=1}^{m} e_i$ where C is the center of B. We observe that (1) $e_i = \Pi_{h \in H_i} e_h$ which is a non-zero monomial in B_a for a maximal subset

H_i of G, (2) H_i is a subgroup of G, and (3) Be_i is a central Galois algebra with Galois group H_i. In the present paper, we shall discuss a general case: what kind of elements e in B_a and subgroups H_e give a central Galois algebra Be with Galois group H_e? We shall show that (1) for any non-zero monomial $e = \Pi_{g \in S} e_g$ of B_a for some subset S of G, let $H_e = \{g \in G \,|\, e \leq e_g$, that is, $ee_g = e\}$; then H_e is a subgroup of G, (2) when $H_e \neq \{1\}$, Be is a central Galois algebra with Galois group H_e if and only if e is a non-zero minimal element in B_a (that is, Be is one of the component of B as given in Theorem 3.8 in [7]), (3) for a non-zero monomial $e = \Pi_{g \in S} e_g$ of B_a for some subset S of G, let $T_e = \{g \in G \,|\, e = e_g\}$; then T_e is a subgroup of G if and only if $e = 1$, and (4) let $H_1 = \{g \in G \,|\, e_g = 1\}$. Then $e_g = 0$ for each $g \notin H_1$ if and only if B is either a central Galois algebra with Galois group H_1 or a commutative Galois algebra with Galois group G. Thus, $\{Be \,|\, e$ is a non-zero minimal element in $B_a\}$ are the only central Galois algebras with Galois group H_e arising from non-zero monomials e in B_a, and when $B_a = \{0, 1\}$, B is a central Galois algebra with Galois group H_1 and the center C is a commutative Galois algebra with Galois group G/H_1. This fact generalizes the F. R. DeMeyer theorem for a Galois algebra with an indecomposable center C ([1, Theorem 1]).

2. Definitions and Notations. Let B be a ring with 1, C the center of B, G an automorphism group of B of order n for some integer n, 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, $i = 1, 2, ..., m\}$ 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 $J_g = \{b \in B \,|\, bx = g(x)b$ for all $x \in B\}$ and $J_g^{(A)} = \{b \in A \,|\, bx = g(x)b$ for all $x \in A\}$ for each $g \in G$ where $A \subset B$. In [4], it was shown

that $BJ_g = Be_g$ for some central idempotent e_g of B. We denote B_a the Boolean algebra generated by $\{0, e_g \,|\, g \in G; \leq\}$ where $e \leq e'$ if $ee' = e$.

3. The monomials and subgroups. Let e be a non-zero monomial of B_a, $e = \Pi_{g \in S} e_g$ for a subset S of G. We have two subsets of G, $H_e = \{g \in G \,|\, e \leq e_g\}$ and $T_e = \{g \in G \,|\, e = e_g\}$. We are going to show that H_e is a subgroup of G, and that T_e is a subgroup of G if and only if $e = 1$. Let K be a subgroup of G. Then K is called a non-zero subgroup of G if $\Pi_{k \in K} e_k \neq 0$, and K is called a maximal non-zero subgroup of G if $K \subset K'$ where K' is a non-zero subgroup of G such that $\Pi_{k \in K} e_k = \Pi_{k \in K'} e_k$, then $K = K'$. We note that each non-zero subgroup is contained in a unique maximal non-zero subgroup of G. We shall show that there exists a ono-to-one correspondence between the following three sets: (1) the set of non-zero monomials in B_a, (2) the set of maximal non-zero subgroups of G, and (3) the set of Galois extensions in B generated by a non-zero monomial e with a maximal Galois subgroup of G.

Lemma 3.1. *Let e be a non-zero monomial in B_a and $H_e = \{g \in G \,|\, e \leq e_g\}$. Then H_e is a subgroup of G.*

Proof. For any $g, h \in H_e$, $e \leq e_g$ and $e \leq e_h$. Hence $e \leq e_g e_h$. But $J_g J_h \subset J_{gh}$, so $BJ_g J_h \subset BJ_{gh}$. Therefore $Be_g e_h \subset Be_{gh}$. Thus $e_g e_h \leq e_{gh}$; and so $e \leq e_g e_h \leq e_{gh}$. This implies that $gh \in H_e$. Noting that G is finite, we conclude that H_e is a subgroup of G.

Theorem 3.2. *There exists a ono-to-one correspondence between the set of non-zero monomials in B_a and the set of maximal non-zero subgroups of G.*

Proof. Define $f : e \longrightarrow H_e$ for a non-zero monomial e in B_a where H_e is given in Lemma 3.1. By Lemma 3.1, H_e is a subgroup of G. Also, by the definition of H_e, it is easy to see that H_e is a maximal non-zero subgroup of G. Thus f is well defined.

Next we show that f is one-to-one. Let e and e' be two non-zero monomials in B_a such that $f(e) = f(e')$, that is, $H_e = H_{e'}$. Then $e = \Pi_{h \in H_e} e_h = \Pi_{h \in H_{e'}} e_h = e'$. Thus f is one-to-one. Moreover, let K be a maximal non-zero subgroup of G. Then $e = \Pi_{k \in K} e_k \neq 0$ and $K = \{g \in G \,|\, e \leq e_g\}$ by the definition of a maximal non-zero subgroup of G. Thus $f(e) = K$. Therefore f is a bijection.

Let $N(H_e)$ be the normalizer of H_e in G for a non-zero monomial e in B_a. We next show that Be is a Galois extension with a maximal Galois subgroup $G(e)$ where $G(e) = \{g \in G \,|\, g(e) = e\}$, and $G(e) = N(H_e)$. Consequently, we can establish a one-to-one correspondence between the set of maximal non-zero subgroups of G and the set of Galois extensions in B generated by a non-zero monomial e with a maximal Galois subgroup of $N(H_e)$.

Lemma 3.3. *For a non-zero monomial e in B_a, let $G(e) = \{g \in G \,|\, g(e) = e\}$. Then, (1) $G(e) = N(H_e)$ where $N(H_e)$ is the normalizer of H_e in G, and (2) Be is a Galois extension with a maximal Galois subgroup of $G(e)|_{Be} \cong G(e)$.*

Proof. (1) For any $g \in N(H_e)$, since $Be = B\Pi_{h \in H_e} e_h = B\Pi_{h \in H_e} J_h$, $g(Be) = g(B\Pi_{h \in H_e} J_h) = B\Pi_{h \in H_e} J_{ghg^{-1}} = B\Pi_{h \in gH_e g^{-1}} J_h = B\Pi_{h \in H_e} J_h = Be$ (for $gHg^{-1} = H$). Hence $g(e) = e$; and so $g \in G(e)$. Conversely, for any $g \in G(e)$,

$$Be = g(Be) = g(B\Pi_{h \in H_e} e_h) = g(B\Pi_{h \in H_e} J_h) = B\Pi_{h \in H_e} J_{ghg^{-1}} = B\Pi_{h \in H_e} e_{ghg^{-1}}.$$

Thus $e = \Pi_{h \in H_e} e_{ghg^{-1}}$. Therefore $e \leq e_{ghg^{-1}}$; and so $e_{ghg^{-1}} \in H_e$ for each $h \in H_e$. This implies that $g \in N(H_e)$.

(2) Since B is a Galois algebra with Galois group G and $e \in C^{G(e)}$, Be is a Galois extension with a maximal Galois subgroup of $G(e)|_{Be} \cong G(e)$ (see the proof of Lemma 3.7 in [7]). Moreover, let $g \in G$ but $g \notin G(e)$. Then $g(e) \neq e$. Thus g is not an automorphism of Be; and so $G(e)$ is the maximal Galois group contained in G for Be.

THEOREM 3.4. *There exists a one-to-one correspondence between the set of maximal non-zero subgroups of G and the set of Galois extensions in B generated by a non-zero monomial e with a maximal Galois subgroup $G(e)|_{Be} \cong G(e)$ such that $G(e) = N(H_e)$.*

PROOF. Let $\alpha : e \longrightarrow Be$ for each non-zero monomial e in B_a. Then, by Lemma 3.3, Be is a Galois extension in B generated by e with a maximal Galois subgroup $G(e)|_{Be} \cong G(e)$ such that $G(e) = N(H_e)$. Clearly, α is a bijection from the set of non-zero monomials in B_a to the set of Galois extensions Be for a non-zero monomial e in B_a with a maximal Galois subgroup $G(e)|_{Be} \cong G(e)$ which is $N(H_e)$. Thus Theorem 3.4 is an immediate consequence of Theorem 3.2.

In the following, we show that the set $T_e = \{g \in G \,|\, e = e_g\}$ for a non-zero monomial e in B_a is not a subgroup of G unless $e = 1$.

THEOREM 3.5. *Let e be a non-zero monomial in B_a and $T_e = \{g \in G \,|\, e = e_g\}$. Then T_e is a subgroup of G if and only if $e = 1$.*

PROOF. Assume T_e is a subgroup of G. Then $1 \in T_e$; and so $e = e_1 = 1$. Conversely, assume $e = 1$. Then $T_e = T_1 = \{g \in G \,|\, 1 = e_g\}$. But the condition that $1 = e_g$ is equivalent to that $1 \leq e_g$, so $T_e = T_1 = H_1$ where H_1 is given in Lemma 3.1. Hence by Lemma 3.1, T_e is a subgroup of G.

4. Central Galois algebras. In section 3, Lemma 3.1 proves that for a non-zero monomial $e \in B_a$, H_e $(= \{g \in G \,|\, e \leq e_g\})$ is a subgroup of G. In [7], it was shown that if H is a maximal subset of G such that $\Pi_{h \in H} J_h \neq \{0\}$, then H is a subgroup of G. We shall show that the maximal subset H is exactly H_e for a minimal non-zero monomial $e \in B_a$. Thus Be is a central Galois algebra with Galois group H_e ([7, Theorem 3.6]). Next is

a characterization of the central Galois algebra Be with Galois group H_e for a non-zero monomial $e \in B_a$.

THEOREM 4.1. *Let e be a non-zero monomial in B_a such that $H_e \neq \{1\}$. The following statements are equivalent:*

(1) Be is a central Galois algebra with Galois group H_e.

(2) $eJ_g = \{0\}$ for each $g \notin H_e$.

(3) e is a minimal non-zero monomial in B_a.

PROOF. (1) $\Longrightarrow$ (2). Since B is a Galois algebra over a commutative ring R with Galois group G, $B = \oplus \sum_{g \in G} J_g$ ([4, Theorem 1]). Hence

$$Be = \oplus \sum_{g \in G} eJ_g = (\oplus \sum_{h \in H_e} eJ_h) \oplus (\oplus \sum_{g \notin H_e} eJ_g).$$

By hypothesis, Be is a central Galois algebra with Galois group H_e, so $Be = \oplus \sum_{h \in H_e} J_h^{(Be)}$. But by Lemma 3.3 in [7], $J_h^{(Be)} = eJ_h$ for each $h \in H_e$; and so $Be = \oplus \sum_{h \in H_e} eJ_h$. Thus $\oplus \sum_{g \notin H_e} eJ_g = \{0\}$, that is, $eJ_g = \{0\}$ for each $g \notin H_e$.

(2) $\Longrightarrow$ (1). Since $Be = \oplus \sum_{g \in G} eJ_g = (\oplus \sum_{h \in H_e} eJ_h) \oplus (\oplus \sum_{g \notin H_e} eJ_g)$ and $eJ_g = \{0\}$ for each $g \notin H_e$, $Be = \oplus \sum_{h \in H_e} eJ_h$. By Lemma 3.3 in [7] again, $J_h^{(Be)} = eJ_h$ for each $h \in H_e$. Hence $Be = \oplus \sum_{h \in H_e} J_h^{(Be)}$, where $J_h^{(Be)} J_{h^{-1}}^{(Be)} = (eJ_h)(eJ_{h^{-1}}) = eJ_h J_{h^{-1}} = eC$ which is the center of Be. Moreover, B is a Galois R-algebra, so it is a separable R-algebra. Thus, Be is a separable algebra over Re ([2, Proposition 1.11, page 46]). Therefore, Be is a central Galois algebra over Ce ([3, Theorem 1]).

(3) $\Longrightarrow$ (2). Since e is a minimal non-zero monomial in B_a, for each $g \in G$, either $e \leq e_g$ or $ee_g = 0$. Since $e \leq e_g$ for each $g \in H_e$, we have that $ee_g = 0$ for each $g \notin H_e$. Therefore $BeJ_g = Bee_g = \{0\}$; and so $eJ_g = \{0\}$ for each $g \notin H_e$.

(2) $\Longrightarrow$ (3). Suppose e is not a minimal non-zero monomial in B_a. Then there exists a $g \in G$ such that $0 < ee_g < e$. By the definition of H_e, $e = \Pi_{h \in H_e} e_h$; and so $ee_h = e$ for

each $h \in H_e$. Hence $g \notin H_e$. Therefore $BeJ_g = Bee_g \neq \{0\}$. This implies that $eJ_g \neq \{0\}$ for some $g \notin H_e$. This contradicts to hypothesis (2). Thus statement (3) holds.

When e is a minimal non-zero monomial in B_a, Theorem 4.1 shows that Be is a central Galois algebra with Galois group H_e. Hence the order of H_e is a unit in Be ([4, Corollary 3]). Moreover, by Lemma 3.3, Be is a Galois extension with Galois group $G(e)$ which is $N(H_e)$, so we have a structure of Be.

THEOREM 4.2. *For a minimal non-zero monomial e in B_a, Be is a central Galois algebra with Galois group H_e and Ce is a commutative Galois algebra with Galois group $G(e)/H_e$.*

PROOF. Since e is a minimal non-zero monomial in B_a, Be is a central Galois algebra with Galois group H_e by Theorem 4.1. Hence $|H_e|$, the order of H_e, is a unit in Ce. Moreover, by Lemma 3.3, Be is a Galois extension with Galois group $G(e)$ which is $N(H_e)$, so H_e is a normal subgroup of $G(e)$. Let $\{a_i, b_i \mid i = 1, 2, ..., m\}$ be a $G(e)$-Galois system for Be. Then, $\sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g} e$ for each $g \in G(e)$. Let $x_i = \frac{1}{|H_e|} \sum_{h \in H_e} h(a_i)$ and $y_i = \sum_{h \in H_e} h(b_i)$. Then, x_i and y_i are invariant under each element in H_e. Hence $x_i, y_i \in Ce$ since $(Be)^{H_e} = Ce$. It is straightforward to verify that $\{x_i, y_i\}$ is a $G(e)/H_e$-Galois system for Ce.

Theorem 4.1 characterizes a central Galois algebra Be for a minimal non-zero monomial $e \in B_a$. Next we want to characterize a central Galois algebra $B1$ for the maximal monomial 1 in B_a.

THEOREM 4.3. *Let $H_1 = \{h \in G \mid e_h = 1\}$. Then $e_g = 0$ for each $g \notin H_1$ if and only if B is either a central Galois algebra with Galois group H_1 or a commutative Galois algebra with Galois group G.*

Proof. ($\Longrightarrow$) Case 1: $H_1 \neq \{1\}$. Since $e_g = 0$ for each $g \notin H_1$, $J_g = \{0\}$ for each $g \notin H_1$. Hence, by (2) $\Longrightarrow$ (1) in Theorem 4.1, B $(= B1)$ is a central Galois algebra with Galois group H_1. Case 2: $H_1 = \{1\}$. By hypothesis, $e_g = 0$ for each $g \neq 1$ in G, so $B = \oplus \sum_{g \in G} J_g = J_1 = C$. Thus B is a commutative Galois algebra with Galois group G.

($\Longleftarrow$) Assume B is a central Galois algebra with Galois group H_1. Then $H_1 \neq \{1\}$. Hence, by (1) $\Longrightarrow$ (2) in Theorem 4.1, $J_g = 1J_g = \{0\}$ for each $g \notin H_1$. Thus $e_g = 0$ for each $g \notin H_1$. Next, assume B is a commutative Galois algebra with Galois group G. Then $J_g = \{0\}$ for each $g \neq 1$ in G ([3, Proposition 2]). Hence $e_g = 0$ for each $g \neq 1$ in G. Therefore $H_1 = \{1\}$ and $e_g = 0$ for each $g \notin H_1$.

As a consequence of Theorem 4.3, the F. R. DeMeyer theorem ([1, Theorem 1]) for central Galois algebras with a connected center is generalized.

Corollary 4.4. *Let B be a Galois algebra with Galois group G. If $B_a = \{0, 1\}$, then B is a central Galois algebra with Galois group H_1 and C is a commutative Galois algebra with Galois group G/H_1.*

Proof. Since $B_a = \{0, 1\}$, $e_g = 0$ for each $g \notin H_1$; and so the corollary holds.

We conclude the present paper with an example of a Galois algebra B such that $B_a = \{0, 1\}$, but its center C is not indecomposable.

Example 4.5. Let $R[i, j, k]$ be the quaternion algebra over the real field R, $B = R[i, j, k] \oplus R[i, j, k]$, and $G = \{1, g_i, g_j, g_k, g, gg_i, gg_j, gg_k\}$ where $g_i(a_1, a_2) = (ia_1i^{-1}, ia_2i^{-1})$, $g_j(a_1, a_2) = (ja_1j^{-1}, ja_2j^{-1})$, $g_k(a_1, a_2) = (ka_1k^{-1}, ka_2k^{-1})$, and $g(a_1, a_2) = (a_2, a_1)$ for all (a_1, a_2) in B. Then,

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

$-\frac{1}{4}(i,0)$, $b_3 = -\frac{1}{4}(j,0)$, $b_4 = -\frac{1}{4}(k,0)$, $b_5 = \frac{1}{4}(0,1)$, $b_6 = -\frac{1}{4}(0,i)$, $b_7 = -\frac{1}{4}(0,j)$, $b_8 = -\frac{1}{4}(0,k)\}$.

(2) $B^G = \{(r,r) \mid r \in R\} \cong R$.

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

(4) $J_1 = C = R \oplus R$, $J_{g_i} = (Ri) \oplus (Ri)$, $J_{g_j} = (Rj) \oplus (Rj)$, $J_{g_k} = (Rk) \oplus (Rk)$, and $J_g = J_{gg_i} = J_{gg_j} = J_{gg_k} = \{0\}$.

(5) $BJ_1 = BJ_{g_i} = BJ_{g_j} = BJ_{g_k} = B1$ and $BJ_g = BJ_{gg_i} = BJ_{gg_j} = BJ_{gg_k} = \{0\}$. Hence $e_1 = e_{g_i} = e_{g_j} = e_{g_k} = 1$ and $e_g = e_{gg_i} = e_{gg_j} = e_{gg_k} = 0$. Thus $B_a = \{0,1\}$.

(6) $H_1 = \{1, g_i, g_j, g_k\}$ and B is a central Galois algebra with Galois group H_1.

(7) $C = R \oplus R$ which is a commutative Galois algebra with Galois group $G/H_1 \cong \{1, g\}$.

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] F.R. DeMeyer, *Galois Theory in Separable Algebras over Commutative Rings,* Illinois J. Math., **10**(1966), 287-295.

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

[3] M. Harada, *Supplementary Results on Galois Extension,* Osaka J. Math., **2**(1965), 343-350.

[4] T. Kanzaki, *On Galois Algebra Over A Commutative Ring,* Osaka J. Math., **2**(1965), 309-317.

[5] G. Szeto and L. Xue, *On three types of Galois extensions of rings,* Southeast Asian Bulletin of Mathematics, **23**(1999) 731-736.

[6] G. Szeto and L. Xue, *On Characterizations of a Center Galois Extension,* International Journal of Mathematics and Mathematical Sciences, Vol. 23, No. **11**(2000), 753-758.

[7] G. Szeto and L. Xue, *The Structure of Galois Algebras,* Journal of Algebra, Vol. 237, No. **1**(2001), 238-246.