

# THE BOOLEAN ALGEBRA OF GALOIS ALGEBRAS

George Szeto and Lianyong Xue

Received 8 February 2002

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 each  $g \in G$ , and  $BJ_g = Be_g$  for a central idempotent  $e_g$ ,  $B_a$  the Boolean algebra generated by  $\{0, e_g \mid g \in G\}$ ,  $e$  a nonzero element in  $B_a$ , and  $H_e = \{g \in G \mid ee_g = e\}$ . Then, a monomial  $e$  is characterized, and the Galois extension  $Be$ , generated by  $e$  with Galois group  $H_e$ , is investigated.

2000 Mathematics Subject Classification: 16S35, 16W20.

**1. Introduction.** The Boolean algebra of central idempotents in a commutative Galois algebra plays an important role for the commutative Galois theory (see [1, 3, 6]). Let  $B$  be a Galois algebra with Galois group  $G$ ,  $C$  the center of  $B$ , and  $J_g = \{b \in B \mid bx = g(x)b \text{ for all } x \in B\}$  for each  $g \in G$ . In [2], it was shown that  $BJ_g = Be_g$  for some idempotent  $e_g$  of  $C$ . Let  $B_a$  be the Boolean algebra generated by  $\{0, e_g \mid g \in G\}$ . Then in [5], by using  $B_a$ , the following structure theorem for  $B$  was given. There exist  $\{e_i \in B_a \mid i = 1, 2, \dots, m \text{ for some integer } m\}$  and some subgroups  $H_i$  of  $G$  such that  $B = \oplus \sum_{i=1}^m Be_i \oplus Bf$  where  $f = 1 - \sum_{i=1}^m e_i$ ,  $Be_i$  is a central Galois algebra with Galois group  $H_i$  for each  $i = 1, 2, \dots, m$ , and  $Bf = Cf$  which is a Galois algebra with Galois group induced by and isomorphic with  $G$  in case  $1 \neq \sum_{i=1}^m e_i$ . In [4], let  $K$  be a subgroup of  $G$ . Then,  $K$  is called a nonzero subgroup of  $G$  if  $\prod_{k \in K} e_k \neq 0$  in  $B_a$ , and  $K$  is called a maximal nonzero subgroup of  $G$  if  $K \subset K'$ , where  $K'$  is a nonzero subgroup of  $G$  such that  $\prod_{k \in K} e_k = \prod_{k \in K'} e_k$ , then  $K = K'$ . We note that any nonzero subgroup is contained in a unique maximal nonzero subgroup of  $G$ . In [4], it was shown that there exists a one-to-one correspondence between the set of nonzero monomials in  $B_a$  and the set of maximal nonzero subgroups of  $G$ , and that, for a nonzero monomial  $e$  in  $B_a$  such that  $H_e \neq \{1\}$ ,  $Be$  is a central Galois algebra with Galois group  $H_e$  if and only if  $e$  is a minimal nonzero monomial in  $B_a$ . The purpose of the present paper is to characterize a monomial  $e$  in  $B_a$  in terms of the maximal nonzero subgroups of  $G$ . Then, the Galois extension  $Be$ , generated by a nonzero idempotent  $e$  and by a monomial  $e$  with Galois group  $H_e$ , is investigated, respectively. Let  $G(e) = \{g \in G \mid g(e) = e\}$  for each  $e \neq 0$  in  $B_a$ . We will show that (1)  $H_e$  is a normal subgroup of  $G(e)$ , and (2)  $Be$  is a Galois extension of  $(Be)^{H_e}$  with Galois group  $H_e$  and  $(Be)^{H_e}$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)/H_e$ . In particular, when  $e$  is a monomial,  $G(e) = N(H_e)$  (the normalizer

of  $H_e$ ), and when  $e$  is an atom (a minimal nonzero element) of  $B_a$ ,  $Be$  is a central Galois algebra over  $Ce$  with Galois group  $H_e$  and  $Ce$  is a commutative Galois algebra with Galois group  $G(e)/H_e$ . This generalizes and improves the result of the components of  $B$  in [5, Theorem 3.8] for a Galois algebra.

**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  $\{a_i, b_i \text{ in } B, i = 1, 2, \dots, m\}$  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  $C$ . In this paper, we 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 [2], it was shown that  $BJ_g = Be_g$  for some central idempotent  $e_g$  of  $B$ . We denote  $(B_a; +, \cdot)$ , the Boolean algebra generated by  $\{0, e_g \mid g \in G\}$ , where  $e \cdot e' = ee'$  and  $e + e' = e + e' - ee'$  for any  $e$  and  $e'$  in  $B_a$ . An order relation  $\leq$  is defined as usual, that is,  $e \leq e'$  in  $B_a$  if  $e \cdot e' = e$ . Throughout,  $e + e'$ , for  $e, e' \in B_a$ , means the sum in the Boolean algebra  $(B_a; +, \cdot)$ ,  $H_e = \{g \in G \mid e \leq e_g\}$  for an  $e \neq 0$  in  $B_a$ , and a monomial  $e$  in  $B_a$  is  $\prod_{g \in S} e_g \neq 0$  for some  $S \subset G$ .

**3. The Boolean algebra.** In this section, we will characterize a monomial  $e$  in  $B_a$  in terms of the maximal nonzero subgroups of  $G$ . We begin with several lemmas.

**LEMMA 3.1.** *Let  $\{e_i, f \mid i = 1, 2, \dots, m\}$  be given in [5, Theorem 3.8]. 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  $e = \sum_{i \in Z_e} e_i + f$ .*

**PROOF.** (1) By the proof of [5, Theorem 3.8], either  $e_i = \prod_{g \in H_i} e_g$ , where  $H_i$  is a maximum subset (subgroup) of  $G$  such that  $\prod_{g \in H_i} e_g \neq 0$ , or  $e_i = (1 - \sum_{j=1}^t e_j) \prod_{g \in H_i} e_g$  for some  $t < i$ , where  $H_i$  is a maximum subset (subgroup) of  $G$  such that  $(1 - \sum_{j=1}^t e_j) \prod_{g \in H_i} e_g \neq 0$ ; so, either  $e_i$  is a minimal element of  $B_a$  or  $e_i$  is a minimal element of  $(1 - \sum_{j=1}^t e_j)B_a$ . Noting that any minimal element in  $(1 - \sum_{j=1}^t e_j)B_a$  is also a minimal element in  $B_a$ , we conclude that each  $e_i$  is a minimal element in  $B_a$ . Next, we show that  $f$  is also a minimal element of  $B_a$  in case  $f \neq 0$ . In fact, by the proof of [5, Theorem 3.8],  $e_g f = 0$  for any  $g \neq 1$  in  $G$ ; so, for any  $e \in B_a$ ,  $ef = 0$  or  $ef = f$ . This implies that  $f$  is a minimal element of  $B_a$  in case  $f \neq 0$ . Moreover,  $\sum_{i=1}^m e_i + f = 1$ ; so,  $\{e_i, f \mid i = 1, 2, \dots, m\}$  is the set of all minimal elements of  $B_a$  in case  $f \neq 0$ .

(2) Since  $1 = \sum_{i=1}^m e_i + f$ , a sum of all minimal elements of  $B_a$ , the statement is immediate.  $\square$

**LEMMA 3.2.** *Let  $e$  be a nonzero element in  $B_a$ . Then,*

- (1) *there exists a monomial  $e'$  of  $B_a$  such that  $e \leq e'$  and  $H_e = H_{e'}$ ,*
- (2)  *$H_e$  is a maximal nonzero subgroup of  $G$ .*

**PROOF.** (1) For any nonzero element  $e$  in  $B_a$ , let  $e' = \prod_{g \in H_e} e_g$ . We claim that  $e \leq e'$  and  $H_e = H_{e'}$ . In fact, for any  $h \in H_e$ ,  $e \leq e_h$ ; so,  $e \leq \prod_{h \in H_e} e_h = e'$ . Moreover, for any  $h \in H_e$ ,  $e_h \geq \prod_{g \in H_e} e_g = e'$ ; so,  $h \in H_{e'}$ . Hence,  $H_e \subset H_{e'}$ . On the other hand, for any  $h \in H_{e'}$ ,  $e_h \geq e' = \prod_{g \in H_e} e_g \geq e$ ; so,  $h \in H_e$ . Thus,  $H_{e'} \subset H_e$ . Therefore,  $H_e = H_{e'}$ .

(2) By [4, Theorem 3.2],  $H_{e'}$  is a maximal nonzero subgroup of  $G$  for  $e'$  is a monomial. Hence,  $H_e (= H_{e'})$  is a maximal nonzero subgroup of  $G$ .  $\square$

Next is an expression of  $H_e$  for a nonzero  $e \in B_a$ .

**THEOREM 3.3.** *For any  $e \neq 0$  in  $B_a$ ,  $H_e = \cap_{i \in Z_e} H_{e_i}$  or  $H_1$ , where  $e = \sum_{i \in Z_e} e_i$  or  $e = \sum_{i \in Z_e} e_i + f$  as given in Lemma 3.1(2).*

**PROOF.** We first show that for  $e = e' + e''$  for some  $e', e'' \neq 0$  in  $B_a$ ,  $H_e = H_{e'} \cap H_{e''}$ . In fact, since  $e \geq e'$  and  $e \geq e''$ , we have  $H_e \subset H_{e'} \cap H_{e''}$ . Conversely, for any  $g \in H_{e'} \cap H_{e''}$ ,  $e_g \geq e'$  and  $e_g \geq e''$ ; so,  $e_g \geq e' + e'' = e$ . Hence,  $g \in H_e$ ; so,  $H_e = H_{e'} \cap H_{e''}$ . Therefore, by induction, if  $e = \sum_{i \in Z_e} e_i$ , then  $H_e = \cap_{i \in Z_e} H_{e_i}$ . Now, by Lemma 3.1, for any  $e \neq 0$  in  $B_a$ ,  $e = \sum_{i \in Z_e} e_i$  or  $e = \sum_{i \in Z_e} e_i + f$ . Similarly, if  $e = \sum_{i \in Z_e} e_i + f$ , then  $H_e = H_{(\sum_{i \in Z_e} e_i) + f} = (\cap_{i \in Z_e} H_{e_i}) \cap H_f$ . But, for  $g \in G$  such that  $e_g \neq 1$ ,  $e_g f = 0$ ; so,  $H_f = H_1$ . Therefore,  $H_e = (\cap_{i \in Z_e} H_{e_i}) \cap H_1 = H_1$  for  $H_1 \subset H_{e_i}$  for each  $i$ .  $\square$

We observe that there exist some  $e \neq 0$  such that  $H_e = \cap_{i \in Z_e} H_{e_i}$  and  $H_e \subset H_{e_j}$  for some  $j \notin Z_e$ , and that not all  $e \neq 0$  are monomials. Next, we identify which element  $e \neq 0$  in  $B_a$  is a monomial. Two characterizations are given. We begin with a definition.

**DEFINITION 3.4.** An  $e \neq 0$  in  $B_a$  is called a maximal  $G$ -element if  $H_e \neq H_1$  and, for any  $e' \in B_a$  such that  $e \leq e'$  and  $H_e = H_{e'}$ ,  $e = e'$ .

**LEMMA 3.5.** (1) *If  $e \neq 0$  such that  $ef = 0$ , then  $e = \sum_{i \in Z_e} e_i$ .*

(2) *If  $e$  is a monomial,  $e = \prod_{g \in S} e_g$  for some  $S \subset G$ , then  $e = 1$  or  $e = \sum_{i \in Z_e} e_i$ .*

**PROOF.** (1) By Lemma 3.1,  $e = \sum_{i \in Z_e} e_i$  or  $e = \sum_{i \in Z_e} e_i + f$ . If  $e \neq \sum_{i \in Z_e} e_i$ , then  $e = \sum_{i \in Z_e} e_i + f$  and  $f \neq 0$ . But then,  $f = (\sum_{i \in Z_e} e_i + f)f = ef = 0$ . This is a contradiction. Hence,  $e = \sum_{i \in Z_e} e_i$ .

(2) In case  $e = 1$ , we are done. In case  $e \neq 1$ . Since  $e_g f = 0$  for each  $g \in G$  such that  $e_g \neq 1$ ,  $ef = \prod_{g \in S} e_g f = 0$ . Thus, by (1),  $e = \sum_{i \in Z_e} e_i$ .  $\square$

**THEOREM 3.6.** *Keeping the notations of Lemma 3.1 for any  $e \neq 0, 1$  in  $B_a$ , the following statements are equivalent:*

- (1)  *$e = \prod_{g \in S} e_g$  for some  $S \subset G$ , a monomial in  $B_a$ ;*
- (2)  *$e$  is a maximal  $G$ -element in  $B_a$ ;*

(3)  $e = \sum_{i \in Z_e} e_i$  where  $\{e_i \mid i \in Z_e\}$  are all atoms such that  $H_e \subset H_{e_i}$  and  $H_e \neq H_1$ .

**PROOF.** (1) $\Rightarrow$ (2). Since  $e$  is a monomial and  $e \neq 1$ ,  $e = \prod_{g \in H_e} e_g$  where  $e_g \neq 1$  for some  $g \in H_e$ . Thus,  $H_e \neq H_1$ . Next, for any  $e'$  such that  $e \leq e'$  and  $H_e = H_{e'}$ ,

$$e \leq e' \leq \prod_{g \in H_{e'}} e_g = \prod_{g \in H_e} e_g = e. \quad (3.1)$$

Hence,  $e = e'$ . This implies that  $e$  is a maximal  $G$ -element in  $B_a$ .

(2) $\Rightarrow$ (1). Let  $e$  be a maximal  $G$ -element and  $e' = \prod_{g \in H_e} e_g$ . Then, by Lemma 3.2,  $e \leq e'$  and  $H_e = H_{e'}$ . But  $e$  is a maximal  $G$ -element; so,  $e = e'$  which is a monomial.

(1) $\Rightarrow$ (3). By Lemma 3.5,  $e = \sum_{i \in Z_e} e_i$ . Now, let  $e_j$  be an atom such that  $H_e \subset H_{e_j}$ . Then,  $e_j \leq \prod_{g \in H_{e_j}} e_g \leq \prod_{g \in H_e} e_g$ . But, by hypothesis,  $e$  is a monomial; so,  $e = \prod_{g \in H_e} e_g$ . Hence,  $e_j \leq e$ . This implies that  $e_j$  is a term in  $e$ . Thus,  $e = \sum_{i \in Z_e} e_i$  where  $\{e_i \mid i \in Z_e\}$  are all atoms such that  $H_e \subset H_{e_i}$ . Moreover, since  $e = \prod_{g \in S} e_g \neq 1$ , there exists  $g \in G$  such that  $e \leq e_g \neq 1$ . Thus,  $g \in H_e$  and  $g \notin H_1$ . Therefore,  $H_e \neq H_1$ .

(3) $\Rightarrow$ (1). Let  $e' = \prod_{g \in H_e} e_g$ . Then, by Lemma 3.2,  $e \leq e'$  and  $H_e = H_{e'}$ . Since  $H_e \neq H_1$ ,  $H_{e'} \neq H_1$ . Also, since  $e'$  is a monomial,  $e' = \sum_{j \in Z_{e'}} e_j$  by Lemma 3.5(2). Now, suppose that  $e \neq e'$ . Then, there is a  $j \in Z_{e'}$  but  $j \notin Z_e$ , that is,  $e_j$  is a term of  $e' = \sum_{j \in Z_{e'}} e_j$  but not a term of  $e = \sum_{i \in Z_e} e_i$ . But then,  $H_e = H_{e'} = \cap_{j \in Z_{e'}} H_{e_j} \subset H_{e_j}$  such that  $j \notin Z_e$ . This contradicts the hypothesis that  $e = \sum_{i \in Z_e} e_i$  where  $\{e_i \mid i \in Z_e\}$  are all atoms such that  $H_e \subset H_{e_i}$ . Thus,  $e = e'$  which is a monomial in  $B_a$ .  $\square$

**4. Galois extensions.** In [5], it was shown that  $Be$  is a central Galois algebra with Galois group  $H_e$  for any atom  $e \neq f$  of  $B_a$ . Also, for any  $e \neq 0$  in  $B_a$ ,  $Be$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)|_{Be} \cong G(e)$  where  $G(e) = \{g \in G \mid g(e) = e\}$  (see [5, Lemma 3.7]). In this section, we are going to show that, for any  $e \neq 0$  in  $B_a$  (not necessary an atom), (1)  $H_e$  is a normal subgroup of  $G(e)$ , and (2)  $Be$  is a Galois extension of  $(Be)^{H_e}$  with Galois group  $H_e$  and  $(Be)^{H_e}$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)/H_e$ . This generalizes and improves the result for  $Be$  when  $e$  is an atom of  $B_a$  as given in [5, Theorem 3.8]. In particular, for a monomial  $e$ ,  $G(e) = N(H_e)$ , the normalizer of  $H_e$  in  $G$ .

**LEMMA 4.1.** *Let  $e \neq 0$  in  $B_a$ . Then,  $H_e$  is a normal subgroup of  $G(e)$  where  $G(e) = \{g \in G \mid g(e) = e\}$ .*

**PROOF.** We first claim that  $H_e \subset G(e)$ . In fact, by Lemma 3.1, for any  $e \neq 0$  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  $e = \sum_{i \in Z_e} e_i + f$  where  $e_i$  are given in Lemma 3.1. Moreover, for each  $i$ ,

$e_i = \prod_{h \in H_{e_i}} e_h$  or  $e_i = (1 - \sum_{j=1}^t e_j) \prod_{g \in H_{e_i}} e_g$  for some  $t < i$ . Noting that  $g$  permutes the set  $\{e_i \mid i = 1, 2, \dots, t\}$  for each  $g \in G$  by the proof of [5, Theorem 3.8], we have, for each  $g \in G$ ,

$$g(e_i) = g\left(\prod_{h \in H_{e_i}} e_h\right) = \prod_{h \in H_{e_i}} e_{ghg^{-1}} \geq \prod_{h \in H_{e_i}} e_g e_h e_g^{-1} = e_g e_i e_g^{-1} \quad (4.1)$$

or

$$\begin{aligned} g(e_i) &= g\left(\left(1 - \sum_{j=1}^t e_j\right) \prod_{h \in H_{e_i}} e_h\right) = \left(1 - \sum_{j=1}^t e_j\right) \prod_{h \in H_{e_i}} e_{ghg^{-1}} \\ &\geq \left(1 - \sum_{j=1}^t e_j\right) \prod_{h \in H_{e_i}} e_g e_h e_g^{-1} \\ &= e_g \left(\left(1 - \sum_{j=1}^t e_j\right) \prod_{h \in H_{e_i}} e_h\right) e_g^{-1} = e_g e_i e_g^{-1}. \end{aligned} \quad (4.2)$$

Now, in case  $e = \sum_{i \in Z_e} e_i$ , for any  $h \in H_e$ ,

$$e = e_h e e_{h^{-1}} = \sum_{i \in Z_e} e_h e_i e_{h^{-1}} \leq \sum_{i \in Z_e} h(e_i) = h(e). \quad (4.3)$$

Thus,  $h(e) = e$  using Lemma 3.1(2). Noting that  $g$  permutes the set  $\{e_i \mid i = 1, 2, \dots, m\}$  for each  $g \in G$ , we have  $g(f) = f$  for each  $g \in G$ . Thus, we have  $h(e) = e$  for each  $h \in H_e$  in case  $e = \sum_{i \in Z_e} e_i + f$ . This proves that  $H_e \subset G(e)$ . Next, we show that  $H_e$  is a normal subgroup of  $G(e)$ . Since for each  $g \in G$ ,  $g(e_i)$  is also an atom,  $g(e) = e$  (i.e.,  $g \in G(e)$ ) implies that  $g$  permutes the set  $\{e_i \mid i \in Z_e\}$ . Therefore, for each  $i \in Z_e$ ,  $g(e_i) = e_j$  and  $gH_{e_i}g^{-1} = H_{e_j}$  for some  $j \in Z_e$ . But, by Theorem 3.3,  $H_e = \cap_{i \in Z_e} H_{e_i}$  (or  $H_e = H_1$  which is normal); so, for any  $g \in G(e)$ ,  $gH_e g^{-1} = g(\cap_{i \in Z_e} H_{e_i})g^{-1} = \cap_{i \in Z_e} gH_{e_i}g^{-1} = \cap_{j \in Z_e} H_{e_j} = H_e$ . Therefore,  $H_e$  is a normal subgroup of  $G(e)$ .  $\square$

**THEOREM 4.2.** *Let  $e$  be a nonzero element in  $B_a$ . Then,*

- (1)  *$Be$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)$ ,*
- (2)  *$Be$  is a Galois extension of  $(Be)^{H_e}$  with Galois group  $H_e$  and  $(Be)^{H_e}$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)/H_e$ .*

**PROOF.** (1) Since  $B$  is a Galois algebra with Galois group  $G$ ,  $B$  is a Galois extension with Galois group  $G(e)$ . But  $g(e) = e$  for each  $g \in G(e)$ ; so, by [5, Lemma 3.7],  $Be$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)$ .

(2) Clearly,  $Be$  is a Galois extension of  $(Be)^{H_e}$  with Galois group  $H_e$  by part (1). Next, we claim that  $|H_e|$ , the order of  $H_e$ , is a unit in  $Be$ . In fact, by [5, Theorem 3.8], for each atom  $e_i$  of  $B_a$ ,  $Be_i$  is a central Galois algebra over  $Ce_i$  with Galois group  $H_{e_i}$ ; so,  $|H_{e_i}|$ , the order of  $H_{e_i}$ , is a unit in  $Be_i$  (see [2, Corollary 3]). Hence,  $|H_e| (= |\cap H_{e_i}|)$  is a unit in  $Be$  if  $e = \sum_{i \in Z_e} e_i$ . If  $e = \sum_{i \in Z_e} e_i + f$  and  $f \neq 0$ , then  $H_e = H_1 = \{g \in G \mid g(e) = 1\} = \{g \in G \mid g(c) = c \text{ for each } c \in C\}$ . Hence, by

[2, Proposition 5],  $|H_e|$  is a unit in  $B$ . Thus,  $(Be)^{H_e}$  is a Galois extension of  $(Be)^{G(e)}$  with Galois group  $G(e)/H_e$  for  $H_e$  is a normal subgroup of  $G(e)$  by Lemma 4.1.  $\square$

Lemma 4.1 shows that, for any nonzero element  $e$  in  $B_a$ ,  $G(e)$  is contained in (not necessarily equal to) the normalizer  $N(H_e)$  of  $H_e$  in  $G$ . Next, we want to show that  $G(e) = N(H_e)$  when  $e$  is a monomial. Consequently, for any nonzero element  $e$  in  $B_a$ ,  $Be$  is embedded in a Galois extension  $Be'$  of  $(Be')^{H_e}$  with the same Galois group  $H_e$ , and  $(Be')^{H_e}$  is a Galois extension of  $(Be')^{G(e')}$  with Galois group  $G(e')/H_e$  such that  $G(e') = N(H_e)$  for some monomial  $e'$  in  $B_a$ .

**LEMMA 4.3.** *Let  $e$  be a nonzero element in  $B_a$ . Then, there exists a monomial  $e'$  in  $B_a$  such that  $e \leq e'$ ,  $H_e = H_{e'}$ , and  $N(H_e) = G(e')$  where  $G(e') = \{g \in G \mid g(e') = e'\}$  and  $N(H_e)$  is the normalizer of  $H_e$  in  $G$ .*

**PROOF.** By Lemma 3.2, there exists a monomial  $e'$  in  $B_a$  such that  $e \leq e'$  and  $H_e = H_{e'}$ ; so, it suffices to show that  $N(H_e) = G(e')$ . For any  $g \in N(H_e)$ ,  $g \in N(H_{e'})$ ; so, by Theorem 3.3,  $H_{e'} = gH_{e'}g^{-1} = g(\cap_{i \in \mathbb{Z}_{e'}} H_{e_i})g^{-1} = \cap_{i \in \mathbb{Z}_{e'}} gH_{e_i}g^{-1} = \cap_{i \in \mathbb{Z}_{e'}} H_{g(e_i)} = H_{\sum_{i \in \mathbb{Z}_{e'}} g(e_i)} = H_{g(e')}$ . Noting that  $e'$  is a monomial, we have  $g(e') = e'$  by Lemma 3.2, that is,  $g \in G(e')$ . This implies that  $N(H_e) \subset G(e')$ . Conversely,  $G(e') \subset N(H_{e'})$  by Lemma 4.1. But  $H_e = H_{e'}$ ; so,  $G(e') \subset N(H_e) = N(H_{e'})$ . Therefore,  $N(H_e) = G(e')$ .  $\square$

**THEOREM 4.4.** *Let  $e$  be a nonzero element in  $B_a$ . Then, there exists a monomial  $e'$  in  $B_a$  such that  $Be$  is embedded in  $Be'$ ,  $Be'$  is a Galois extension of  $(Be')^{H_e}$  with Galois group  $H_e$ , and  $(Be')^{H_e}$  is a Galois extension of  $(Be')^{N(H_e)}$  with Galois group  $N(H_e)/H_e$ .*

**PROOF.** By Lemma 4.3, there exists a monomial  $e'$  in  $B_a$  such that  $e \leq e'$ ,  $H_e$  is a normal subgroup of  $G(e')$ , and  $N(H_e) = G(e')$ . Hence,  $Be \subset Be'$ . But  $Be'$  is a Galois extension of  $(Be')^{H_{e'}}$  with Galois group  $H_{e'}$  and  $(Be')^{H_{e'}}$  is a Galois extension of  $(Be')^{G(e')}$  with Galois group  $G(e')/H_{e'}$  by Theorem 4.2; so, Theorem 4.4 holds.  $\square$

**ACKNOWLEDGMENTS.** This paper was written under the support of a Caterpillar Fellowship at Bradley University, and the authors would like to thank the Caterpillar Inc. for that support.

## REFERENCES

- [1] F. DeMeyer, *Separable polynomials over a commutative ring*, Rocky Mountain J. Math. **2** (1972), no. 2, 299–310.
- [2] T. Kanzaki, *On Galois algebra over a commutative ring*, Osaka J. Math. **2** (1965), 309–317.
- [3] G. Szeto, *A characterization of Azumaya algebras*, J. Pure Appl. Algebra **9** (1976/1977), no. 1, 65–71.
- [4] G. Szeto and L. Xue, *The Boolean algebra and central Galois algebras*, Int. J. Math. Math. Sci. **28** (2001), no. 4, 237–242.

- [5] ———, *The structure of Galois algebras*, J. Algebra **237** (2001), no. 1, 238–246.
- [6] O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents*, Nagoya Math. J. **35** (1969), 83–98.

George Szeto: Department of Mathematics, Bradley University, Peoria, IL 61625, USA  
E-mail address: [szeto@hilltop.bradley.edu](mailto:szeto@hilltop.bradley.edu)

Lianyong Xue: Department of Mathematics, Bradley University, Peoria, IL 61625, USA  
E-mail address: [lxue@hilltop.bradley.edu](mailto:lxue@hilltop.bradley.edu)



