The Galois extensions induced by idempotents in a Galois Algebra

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 each \( g \in G \), \( e_g \) the central idempotent such that \( BJ_g = Be_g \) and \( e_K = \sum_{g \in K} e_g \) for a subgroup \( K \) of \( G \). Then \( Be_K \) is a Galois extension with Galois group \( G(e_K) = \{ g \in G \mid g(e_K) = e_K \} \) containing \( K \) and the normalizer \( N(K) \) of \( K \) in \( G \). An equivalence condition is also given for \( G(e_K) = N(K) \), and \( Be_G \) is shown to be a direct sum of all \( Be_i \) generated by a minimal idempotent \( e_i \). Moreover, a characterization for a Galois extension \( B \) is shown in terms of the Galois extension \( Be_G \) and \( B(1-e_G) \).

Key Words and Phrases. Galois extensions, Galois algebras, central Galois algebras, and Boolean algebras.

2000 Mathematics Subject Classification. Primary 16S35, 16W20

1. Introduction. The Boolean algebra of idempotents for commutative Galois algebras plays an important role ([1], [2], and [3]). Let \( B \) be a Galois algebra with Galois group \( G \) and \( J_g = \{ b \in B \mid bx = g(x)b \ \text{for all} \ x \in B \} \) for each \( g \in G \). Then, in [4], it was shown that the ideal \( BJ_g = Be_g \) for some central idempotent \( e_g \). By using the Boolean algebra of central idempotents \( \{ e_g \} \) in the Galois algebra \( B \), the following structure theorem of \( B \) was shown: There exist some subgroups \( H_i \) of \( G \) and minimal idempotents of \( \{ e_i \mid i = 1, 2, \ldots, m \} \), such that \( B = \oplus_{i=1}^{m} Be_i \oplus B(1-\sum_{i=1}^{m} e_i) \) where \( Be_i \) is a central Galois algebra with Galois group \( H_i \) for each \( i = 1, 2, \ldots, m \) and \( B(1-\sum_{i=1}^{m} e_i) \) is \( C(1-\sum_{i=1}^{m} e_i) \), 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 \( B \). Let \((B_a; +, \cdot)\)
be 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 \( B_a \). In the present paper, we shall study the Galois extension \( B_eK \) where \( eK = \sum_{g \in K} e_g \in B_a \) for a subgroup \( K \) of \( G \). Let \( G(e) = \{g \in G \mid g(e) = e\} \) for a central idempotent \( e \). Then it will be shown that \( K \subset N(K) \subset G(eK) \) and \( B_eK \) is a Galois extension with Galois group \( G(eK) \) where \( N(K) \) is the normalizer of \( K \) in \( G \).

A necessary and sufficient condition for \( G(eK) = N(K) \) is also given so that \( B_eK \) is a Galois extension of \( (B_eK)^K \) with Galois group \( K \) and \( (B_eK)^K \) is a Galois extension of \( (B_eK)^{G(eK)} \) with Galois group \( G(eK)/K \). Let \( S(K) = \{H \mid H \text{ is a subgroup of } G \text{ and } e_H = e_K\} \). Then the map \( S(K) \rightarrow e_K \) from \( \{S(K) \mid K \text{ is a subgroup of } G\} \) to \( B_a \) is one-to-one. In particular, when \( K = G \), we derive an expression for \( B, B = B_{eG} \oplus B(1 - e_G) \) such that \( B_{eG} = \oplus \sum_{i=1}^{m} B_{e_i} \), a direct sum of central Galois algebra with Galois subgroup \( H_i \) and \( B(1 - e_G) = B(1 - \sum_{i=1}^{m} e_i) = C(1 - e_G) \) which is a commutative Galois algebra with Galois group induced by and isomorphic with \( G \). Moreover, a characterization for a Galois extension \( B \) is shown in terms of the Galois extension \( B_{eG} \) and \( B(1 - e_G) \).

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 \( \{a_i, b_i \mid i = 1, 2, \ldots, m\} \) 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 [4], it was shown that \( BJ_g = B_{e_g} \) 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 \( B_a \). Throughout, \( e + e' \) for \( e, e' \in B_a \) means the sum in the Boolean algebra \( (B_a; +, \cdot) \) and a monomial \( e \) in \( B_a \) is \( \Pi_{g \in S} e_g \neq 0 \) for some \( S \subset G \).
3. Galois Extensions Generated by Idempotents. Let $K$ be a subgroup of $G$. The idempotent $\sum_{g \in K} e_g \in B_a$ is called the group idempotent of $K$ denoted by $e_K$. Let $G(e) = \{g \in G | g(e) = e\}$ for $e \in B_a$. Then we shall show that $K \subseteq G(e_K)$ and $e_K$ generates a Galois extension $B e_K$ with Galois group $G(e_K)$. A necessary and sufficient condition for $G(e_K) = N(K)$ is also given where $N(K)$ is the normalizer of $K$ in $G$. Thus some consequences for the Galois extension $B e_K$ can be derived when $K$ is a normal subgroup of $G$ or $K = G$.

**Lemma 3.1.** For any $g, h \in G$,

1. $g(e_h) = e_{gh^{-1}}$.
2. $e_h = 1$ if and only if $e_{gh^{-1}} = 1$.

**Proof.** (1) It is easy to check that $g(j_h) = j_{gh^{-1}}$, so $B g(e_h) = g(B e_h) = g(B j_h) = B g(j_h) = B j_{gh^{-1}} = B e_{gh^{-1}}$. Thus $g(e_h) = e_{gh^{-1}}$.

(2) It is clear by (1).

**Theorem 3.2.** Let $K$ be a subgroup of $G$, $e_K = \sum_{g \in K, g \neq 1} e_g$, and $G(e_K) = \{g \in G | g(e_K) = e_K\}$. Then

1. $K$ is a subgroup of $G(e_K)$ and
2. $B = B e_K \oplus B(1 - e_K)$ such that $B e_K$ and $B(1 - e_K)$ are Galois extensions with Galois group induced by and isomorphic with $G(e_K)$.

**Proof.** (1) For any $g \in K$, by Lemma 3.1,

$$g(e_K) = g\left(\sum_{k \in K, k \neq 1} e_k\right) = \sum_{k \in K} g(e_k) = \sum_{k \in K, k \neq 1} e_{gk^{-1}} = \sum_{g \neq 1} e_{gk^{-1}} = e_{gK^{-1}}.$$ 

Since $g \in K$, $gK^{-1} = K$. Hence $g(e_K) = e_K$, and so $g \in G(e_K)$.

(2) We first claim that for any $e \neq 0$ in $B_a$, $B e$ is a Galois extension with Galois group induced by and isomorphic with $G(e)$. In fact, since $B$ is a Galois extension with Galois
group $G$, there exists a $G$-Galois system for $B$ \{a_i, b_i \in B, \ i = 1, 2, \ldots, m\} for some integer
$m$ such that $\sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. Hence $\sum_{i=1}^{m} (a_i e) g(b_i e) = \delta_{1,g}$ for each
g $\in G(e)$. Therefore, \{a_i e, b_i e \in Be, \ i = 1, 2, \ldots, m\} is a $G(e)$-Galois system for $Be$ and
$e = \sum_{i=1}^{m} (a_i e) (b_i e - g(b_i e))$ for each $g \neq 1$ in $G(e)$. But $e \neq 0$, so $g|_{Be} \neq 1$ whenever $g \neq 1$
in $G(e)$. Thus, $Be$ is a Galois extension with Galois group induced by and isomorphic with
$G(e)$. Statement (2) is a particular case when $e = e_K$ and $e = 1 - e_K$ respectively.

The proof of Theorem 3.2-(2) suggests an equivalence condition for a Galois extension
$B$.

**THEOREM 3.3.** $B$ is a Galois extension with Galois group $G(e)$ for a central
idempotent $e$ of $B$ if and only if $B = Be \oplus B(1 - e)$ such that $Be$ and $B(1 - e)$ are Galois
extensions with Galois group induced by and isomorphic with $G(e)$. In particular, $B$ is
a Galois algebra with Galois group $G(e)$ for a central idempotent $e$ of $B$ if and only if
$B = Be \oplus B(1 - e)$ such that $Be$ and $B(1 - e)$ are Galois algebras with Galois group
induced by and isomorphic with $G(e)$.

**PROOF.** ($\Rightarrow$) Since $B$ is a Galois extension with Galois group $G(e)$, $B = Be \oplus
B(1 - e)$ such that $Be$ and $B(1 - e)$ are Galois extensions with Galois group induced by
and isomorphic with $G(e)$ by the proof of Theorem 3.2-(2).

($\Leftarrow$) Let \{a_j^{(1)}, b_j^{(1)} \in Be \mid j = 1, 2, \ldots, n_1\} be an $G(e)$-Galois system for $Be$ and
\{a_j^{(2)}, b_j^{(2)} \in B(1 - e) \mid j = 1, 2, \ldots, n_2\} an $G(e)$-Galois system for $B(1 - e)$.
Then we claim that \{a_j^{(0)}, b_j^{(0)} \mid j = 1, 2, \ldots, n_i, i = 1, 2\} is an $G(e)$-Galois system for $B$. In fact,
$\sum_{i=1}^{n_1} \sum_{j=1}^{n_i} a_j^{(i)} b_j^{(i)} = e + (1 - e) = 1$. Moreover, for each $g \neq 1$ in $G(e)$, noting that
g $\neq 1$ in $G(e)$ if and only if $g|_{Be} \neq 1$ and $g|_{B(1 - e)} \neq 1$ by hypothesis, we have that
$\sum_{j=1}^{n_i} a_j^{(i)} g(b_j^{(i)}) = 0$, $i = 1, 2$, so $\sum_{i=1}^{n_2} \sum_{j=1}^{n_i} a_j^{(i)} b_j^{(i)} = 0$. Therefore \{a_j^{(i)}, b_j^{(i)} \mid j = 1, 2, \ldots, n_i, i = 1, 2\} is an $G(e)$-Galois system for $B$, and so $B$ is a Galois extension with
Galois group $G(e)$.
Next, it is clear that $B^{G(e)} \subset C$ if and only if $(Be)^{G(e)} \subset Ce$ and $(B(1-e))^{G(e)} \subset C(1-e)$, so by the above argument, $B$ is a Galois algebra with Galois group $G(e)$ for a central idempotent $e$ of $B$ if and only if $B = Be \oplus B(1-e)$ such that $Be$ and $B(1-e)$ are Galois algebras with Galois group induced by and isomorphic with $G(e)$.

**COROLLARY 3.4.** $B$ is a Galois algebra with Galois group $G$ if and only if $B = Be_G \oplus B(1-e_G)$ such that $Be_G$ and $B(1-e_G)$ are Galois algebras with Galois group induced by and isomorphic with $G$.

**PROOF.** By Theorem 3.2-(1), $G(e_G) = G$, so the corollary is immediate by Theorem 3.3.

Now let $S(K) = \{ H \mid H$ is a subgroup of $G$ and $e_H = e_K \}$ and $\alpha : S(K) \to e_K$. It is easy to see that $\alpha$ is a bijection from $\{ S(K) \mid K$ is a subgroup of $G \}$ to the set of group idempotents in $B$.

We are interested in an equivalence condition for $K$ such that $G(e_K) = N(K)$. We need a lemma.

**LEMMA 3.5.** Let $K$ be a subgroup of $G$. Then for an $g \in G$, $g \in G(e_K)$ if and only if $gKg^{-1} \in S(K)$.

**PROOF.** Suppose $g \in G(e_K)$. Then

$$e_K = g(e_K) = g \left( \sum_{k \in K, e_k \neq 1} e_k \right) = \sum_{k \in K} g(e_k) = \sum_{k \in K} e_{gkg^{-1}} = \sum_{gkg^{-1} \in gKg^{-1} \neq 1} e_{gkg^{-1}} = e_{gKg^{-1}}.$$  

Thus $gKg^{-1} \in S(K)$. On the other hand, suppose $gKg^{-1} \in S(K)$. Then

$$g(e_K) = g \left( \sum_{k \in K, e_k \neq 1} e_k \right) = \sum_{k \in K} g(e_k) = \sum_{k \in K} e_{gkg^{-1}} = \sum_{gkg^{-1} \in gKg^{-1} \neq 1} e_{gkg^{-1}} = e_{gKg^{-1}} = e_K.$$
Thus $g \in G(e_K)$.

**THEOREM 3.6.** $G(e_K) = N(K)$ if and only if $S(K)$ contains exactly one conjugate of the subgroup $K$.

**PROOF.** ($\Rightarrow$) For any $g \in G$ such that $gKg^{-1} \in S(K)$, $g \in G(e_K)$ by Lemma 3.5. But $G(e_K) = N(K)$ by hypothesis, so $g \in N(K)$. Hence $gKg^{-1} = K$. Thus $S(K)$ contains exactly one conjugate of the subgroup $K$.

($\Leftarrow$) For any $g \in N(K)$, $gKg^{-1} = K$, so $gKg^{-1} \in S(K)$. Hence $g \in G(e_K)$ by Lemma 3.5. Thus $N(K) \subseteq G(e_K)$. Conversely, for each $g \in G(e_K)$, $gKg^{-1} \in S(K)$ by Lemma 3.5, so $gKg^{-1} = K$ by hypothesis. Thus $g \in N(K)$. This implies that $G(e_K) = N(K)$.

**COROLLARY 3.7.** Assume the order of $G$ is a unit in $B$. If $S(K)$ contains exactly one conjugate of the subgroup $K$, then $B e_K$ is a Galois extension of $(B e_K)^K$ with Galois group $K$ and $(B e_K)^K$ is a Galois extension of $(B e_K)^{G(e_K)}$ with Galois group $G(e_K)/K$.

**PROOF.** By Theorem 3.2-(2), $B e_K$ is a Galois extension with Galois group $G(e_K)$. Hence $B e_K$ is a Galois extension of $(B e_K)^K$ with Galois group $K$ for $K$ is a subgroup of $G(e_K)$ by Theorem 3.2-(1). Moreover, by hypothesis, the order of $G$ is a unit in $B$, so the order of $K$ is a unit in $B e_K$. Since $S(K)$ contains exactly one conjugate of the subgroup $K$, $K$ is a normal subgroup of $G(e_K)$ by Theorem 3.6. Thus $(B e_K)^K$ is a Galois extension of $(B e_K)^{G(e_K)}$ with Galois group $G(e_K)/K$.

Next are some consequences for an abelian group $G$ or $K = G$.

**COROLLARY 3.8.** If $B$ is an abelian extension with Galois group $G$ (that is, $G$ is abelian) of an order invertible in $B$, then for any subgroup $K$ of $G$, $B e_K$ is a Galois ex-
tension of \((Be_K)^K\) with Galois group \(K\) and \((Be_K)^K\) is a Galois extension of \((Be_K)^{G(e_K)}\) with Galois group \(G(e_K)/K\).

When \(K = G\), we derive an expression for \(B\) by using the set \(\{e_i \mid i = 1, 2, \ldots, m\}\) of minimal idempotents in \(B_a\). This gives detail descriptions of the components \(Be_G\) and \(B(1 - e_G)\) as given in Corollary 3.4.

**THEOREM 3.9.** Let \(B\) be a Galois algebra with Galois group \(G\). Then \(B = Be_G \oplus B(1 - e_G)\) such that \(Be_G = \oplus \sum_{i=1}^{m} Be_i\) where each \(Be_i\) is a central Galois algebra with Galois group \(H_i\) for some subgroup \(H_i\) of \(G\) and \(B(1 - e_G) = C(1 - e_G)\) which is a commutative Galois algebra with Galois group induced by and isomorphic with \(G\) in case \(e_G \neq 1\) where \(\{e_i \mid i = 1, 2, \ldots, m\}\) are given in Theorem 3.8 in [5].

**PROOF.** Since \(e_i = \Pi_{h \in H_i} e_h\) where \(H_i\) is the maximal subset (subgroup) of \(G\) such that \(\Pi_{h \in H_i} e_h \neq 0\) or \(e_i = (1 - \sum_{j=1}^{t} e_j) \Pi_{h \in H_i} e_h\) where \(H_t\) is the maximal subset (subgroup) of \(G\) for some \(t < i\) such that \((1 - \sum_{j=1}^{t} e_j) \Pi_{h \in H_i} e_h \neq 0\) ([5], Theorem 3.8), we have that \(e_i(\sum_{g \in G} e_g) = e_i\) for each \(i\). Thus \(\sum_{i=1}^{m} e_i \leq \sum_{g \in G} e_g\). Noting that \(e_g(1 - \sum_{i=1}^{m} e_i) = 0\) for each \(g \neq 1\) in \(G\) ([5], Theorem 3.8), we have that \((\sum_{g \in G} e_g)(1 - \sum_{i=1}^{m} e_i) = 0\), that is, \((\sum_{g \in G} e_g)(\sum_{i=1}^{m} e_i) = \sum_{g \in G} e_g\). Hence \(\sum_{g \in G} e_g \leq \sum_{i=1}^{m} e_i\). Thus \(\sum_{g \in G} e_g = \sum_{i=1}^{m} e_i\), that is, \(e_G = \sum_{i=1}^{m} e_i\). But then by Theorem 3.8 in [5], \(B = \oplus \sum_{i=1}^{m} Be_i \oplus B(1 - \sum_{i=1}^{m} e_i) = Be_G \oplus B(1 - e_G)\) such that \(B(1 - e_G) = C(1 - e_G)\) which is a commutative Galois algebra with Galois group induced by and isomorphic with \(G\), and \(Be_G = \oplus \sum_{i=1}^{m} Be_i\) such that each \(Be_i\) is a central Galois algebra with Galois group \(H_i\) for some subgroup \(H_i\) of \(G\) where \(\{e_i \mid i = 1, 2, \ldots, m\}\) are minimal idempotents of \(B_a\).
4. A Relationship between Idempotents. In this section, we shall show a relationship between the set of idempotents \( \{e_g \mid g \in G \} \) and the set of minimal elements in \( B_a \), and give an equivalence condition for a monomial idempotent \( e_S = (\sum_{g \in S} e_g) \) where \( S \) is a subset of \( G \), and a monomial \( e \) in \( B_a \) is \( \Pi_{g \in S} e_g \neq 0 \) for some \( S \subset G \).

**Theorem 4.1.** Let \( S \) be a subset of \( G \). Then there exists a unique subset \( Z_S \) of the set \( \{1, 2, \ldots, m\} \) such that \( e_S = \sum_{i \in Z_S} e_i \).

**Proof.** Since \( C = \oplus \sum_{i=1}^{m} C e_i \oplus C f \) ([5], Theorem 3.8), \( e_S = \sum_{i=1}^{m} c_i e_i + cf \) for some \( c_i, c \in C \). It can be check that \( e_i \) are minimal elements of \( B_a \), so \( e_S e_i = e_i \) or \( e_S e_i = 0 \). Let \( Z_S = \{i \mid e_S e_i = e_i\} \). Then for each \( i \in Z_S \), \( e_i = e_S e_i = c_i e_i \), and for each \( i \notin Z_S \), \( 0 = e_S e_i = c_i e_i \). Hence \( e_S = \sum_{i \in Z_S} e_i + cf \). Moreover, since \( e_g f = 0 \) for each \( g \neq 1 \) in \( G \) ([5], Theorem 3.8), we have that \( 0 = e_S f = (\sum_{i \in Z_S} e_i + cf) f = cf \). Hence \( e_S = \sum_{i \in Z_S} e_i \). The uniqueness of \( Z_S \) is clear.

Next is a description of the components \( B e_K \) and \( B(1 - e_K) \) for a subgroup of \( K \) of \( G \) as given in Theorem 3.2.

**Corollary 4.2.** For any subgroup \( K \) of \( G \), \( B = B e_K \oplus B(1 - e_K) \) such that \( B e_K = \sum_{i \in Z_K} B e_i \) and \( B(1 - e_K) = B(1 - \sum_{i \in Z_K} e_i) \) which are Galois extensions with Galois group induced by and isomorphic with \( G(e_K) \).

**Proof.** It is an immediate consequence of Theorem 3.2-(2) and Theorem 4.1.
is a non-zero subgroup of $G$ such that $\Pi_{k \in K} e_k = \Pi_{k \in K} e_k$, then $K = K'$. It was shown that the set of monomials in $B_a$ and the set of maximal nonzero subgroups of $G$ are in a one-to-one correspondence ([6], Theorem 3.3). Also, any maximal nonzero subgroup $K = H_e = \{ g \in G \mid e \preceq e_g \}$ where $e = \Pi_{k \in K} e_k$ and $H_e$ is a normal subgroup of $G(e)$ ([6], Lemma 4.1). Next is a characterization of a monomial idempotent $e_S = \sum_{e \neq 1} e_g$ for a subset of $G$.

**THEOREM 4.3.** Let $S$ be a subset of $G$ such that $e_S = \sum_{g \in S} e_g \neq 0, 1$. Then $e_S$ is a monomial if and only if $e_j \leq e_S$ whenever $H_{e_S} \subseteq H_{e_j}$ for an atom $e_j$.

**PROOF.** $(\Rightarrow)$ By Theorem 3.3 in [6], $e \mapsto H_e$ is a one-to-one correspondence between the set of monomials in $B_a$ and the set of maximal non-zero subgroups of $G$. Noting that $e = \Pi_{g \in H_e} e_g$ when $e$ is a monomial, we have that for any monomials $e$ and $e'$, $H_e \subseteq H_{e'}$ implies that $e \geq e'$. Thus, $e_j \leq e_S$ whenever $H_{e_S} \subseteq H_{e_j}$ for an atom $e_j$ because $e_S$ is a monomial by hypothesis.

$(\Leftarrow)$ By Theorem 4.1, $e_S = \sum_{e \in Z_S} e_i$ where $Z_S = \{ e_i \mid e_i \leq e_S \}$. By Theorem 3.3-(1) in [6], there exists a monomial $e$ of $B_a$ such that $e_S \subseteq e$ and $H_{e_S} = H_e$. Suppose $e_S \neq e$. Then $e_S = \sum_{e \in Z_S} e_i < e = \sum e_j$ where $\sum_{e_i \in Z_S} e_i$ is a direct summand of $\sum e_j$ by Theorem 4.1. But by Theorem 3.4 in [6], $H_{e_S} = \cap_{e \in Z_S} H_{e_i} = H_e = \cap H_{e_j}$. Therefore there exists some $e_j \not\in Z_S$, that is, $e_j \not\in e_S$ such that $H_{e_S} \subseteq H_{e_j}$. This is a contradiction. Thus $e_S = e$ which is a monomial.

**ACKNOWLEDGEMENTS**

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


