THE GALOIS EXTENSIONS INDUCED BY IDEMPOTENTS
IN A GALOIS ALGEBRA

GEORGE SZETO and LIANYONG XUE

Received 7 June 2001

2000 Mathematics Subject Classification: 16S35, 16W20.

1. Introduction. The Boolean algebra of idempotents for commutative Galois algebras plays an important role (see [1, 3, 6]). Let $B$ be a Galois algebra with Galois group $G$ and $J_B = \{ b \in B \mid bx = g(x)b \text{ for all } x \in B \}$ for each $g \in G$, $e_B$ the central idempotent such that $BJ_B = Be_B$, and $e_K = \sum_{g \in K} e_g$ for a subgroup $K$ of $G$. Then $Be_K$ is a Galois extension with the 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 $B(1-e_G)$.

Let $B$ be a Galois algebra with Galois group $G$, $J_B = \{ b \in B \mid bx = g(x)b \text{ for all } x \in B \}$ for each $g \in G$, $e_B$ the central idempotent such that $BJ_B = Be_B$, and $e_K = \sum_{g \in K} e_g$ for a subgroup $K$ of $G$. Then $Be_K$ is a Galois extension with the 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 $B(1-e_G)$.
2. Definitions and notation. 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 $G$. We call $B$ a Galois extension of $B^G$ with Galois group $G$ if there exist elements \( \{a_i, b_i \in B, \ i = 1, 2, \ldots, m \} \) for some integer $m$ such that $\sum_{i=1}^m a_i g(b_i) = \delta_{1, g}$ for each $g \in G$. We call $B$ a Galois algebra over $B^G$ if $B$ is a Galois extension of $B^G$ which is contained in $C$ and $B$ 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 [2], it was shown that $BJ_g = Be_g$ for some central idempotent $e_g$ of $B$. We denote by $\langle B_a; +, \cdot \rangle$ 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 $\langle B_a; +, \cdot \rangle$ and a monomial $e$ in $B_a$ is $\prod_{g \in S} e_g \neq 0$ for some $S \subset G$.

3. Galois extensions generated by idempotents. Let $K$ be a subgroup of $G$. The idempotent $\sum_{g \in K, e_g = 1} e_g \in B_a$ is called the group idempotent of $K$ denoted by $e_K$. Let $G(e) = \{ g \in G \mid g(e) = e \}$ for $e \in B_a$. Then we will show that $K \subset G(e_K)$ and $e_K$ generates a Galois extension $Be_K$ 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 $Be_K$ 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 $Bg(e_h) = g(Be_h) = g(BJ_h) = Bg(J_h) = BJ_{gh^{-1}} = Be_{gh^{-1}}$. Thus $g(e_h) = e_{gh^{-1}}$.

(2) It is clear by (1). \( \square \)

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

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

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

\[
g(e_K) = g\left(\sum_{k \in K, e_k = 1} e_k\right) = \sum_{k \in K, e_k = 1} g(e_k) = \sum_{k \in K, e_k = 1} e_{kg^{-1}} = \sum_{gk^{-1} \in \sum_{g \in K, e_g = 1} k^{-1}} e_{gk^{-1}} = e_{gKg^{-1}}.
\]

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

(2) We first claim that for any $e \neq 0$ in $B_a$, $Be$ 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 \( \sum_{i=1}^{m} (a_i e) g(b_i e) = e \delta_{1,g} \) for each \( g \in G(e) \). Therefore, \( \{a_i e, b_i e \in B_e, i = 1, 2, \ldots, m\} \) is a \( G(e) \)-Galois system for \( B_e \) 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 \( g \mid B_e \neq 1 \) whenever \( g \neq 1 \) in \( G(e) \). Thus, \( B_e \) 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.** The extension \( B \) is a Galois extension with Galois group \( G(e) \) for a central idempotent \( e \) of \( B \) if and only if \( B = B_e \oplus B(1 - e) \) such that \( B_e \) 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 \( B = B_e \oplus B(1 - e) \) such that \( B_e \) 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 \( G(e) \), \( B = B_e \oplus B(1 - e) \) such that \( B_e \) 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 \( \{a_j^{(i)}; b_j^{(i)} \in B_e \mid j = 1, 2, \ldots, n_i\} \) be a \( G(e) \)-Galois system for \( B_e \) and let \( \{a_j^{(2)}; b_j^{(2)} \in B(1 - e) \mid j = 1, 2, \ldots, n_2\} \) be a \( G(e) \)-Galois system for \( B(1 - e) \). Then we claim that \( \{a_j^{(i)}; b_j^{(i)} \mid j = 1, 2, \ldots, n_i, \ i = 1, 2\} \) is a \( G(e) \)-Galois system for \( B \). In fact, \( \sum_{i=1}^{2} \sum_{j=1}^{n_i} a_j^{(i)} b_j^{(i)} = e + (1 - e) = 1 \). Moreover, for each \( g \neq 1 \) in \( G(e) \)—noting that \( g \neq 1 \) in \( G(e) \) if and only if \( g \mid B_e \neq 1 \) and \( g \mid B(1 - e) \neq 1 \) by hypothesis—we have that \( \sum_{j=1}^{n_i} a_j^{(i)} g(b_j^{(i)}) = 0, \ i = 1, 2, \) so \( \sum_{j=1}^{n_i} a_j^{(i)} g(b_j^{(i)}) = 0 \). Therefore \( \{a_j^{(i)}; b_j^{(i)} \mid j = 1, 2, \ldots, n_i, \ i = 1, 2\} \) is a \( G(e) \)-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 \( (B_e)^{G(e)} \subset C_e \) 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 \( B = B_e \oplus B(1 - e) \) such that \( B_e \) and \( B(1 - e) \) are Galois algebras with Galois group induced by and isomorphic with \( G(e) \).

**Corollary 3.4.** An algebra \( B \) is a Galois algebra with Galois group \( G \) if and only if \( B = B_G \oplus B(1 - e_G) \) such that \( B_G \) 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 \( S(K) = \{H \mid H \text{ is a subgroup of } G \text{ and } e_H = e_K \} \) and \( \alpha : S(K) \rightarrow e_K \). It is easy to see that \( \alpha \) is a bijection from \( \{S(K) | K \text{ is a subgroup of } G\} \) to the set of group idempotents in \( B_a \).

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

**Lemma 3.5.** Let \( K \) be a subgroup of \( G \), then for a \( g \in G \), \( g \in G(e_K) \) if and only if \( gKg^{-1} \subset S(K) \).
Proof. Suppose \( g \in G(e_K) \), then
\[
e_K = g(e_K) = g \left( \sum_{k \in K, e_k \neq 1} e_k \right) = \sum_{k \in K, e_k \neq 1} g(e_k) = \sum_{k \in K, e_k \neq 1} e_{gkg^{-1}} = e_{gKg^{-1}}.
\]
(3.2)
Thus \( gKg^{-1} \in S(K) \). On the other hand, suppose \( gKg^{-1} \in S(K) \). Then
\[
g(e_K) = g \left( \sum_{k \in K, e_k \neq 1} e_k \right) = \sum_{k \in K, e_k \neq 1} g(e_k) = \sum_{k \in K, e_k \neq 1} e_{gkg^{-1}} = e_{gKg^{-1}} = e_K.
\]
(3.3)
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 \( N(K) \subset G(e_K) \). 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 that the order of \( G \) is a unit in \( B \). If \( S(K) \) contains exactly one conjugate of the subgroup \( K \), then \( Be_K \) is a Galois extension 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 \( G(e_K)/K \).

Proof. By Theorem 3.2(2), \( Be_K \) is a Galois extension with Galois group \( G(e_K) \). Hence \( Be_K \) is a Galois extension of \( (Be_K)^K \) 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 \( Be_K \). 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 \( (Be_K)^K \) is a Galois extension of \( (Be_K)^{G(e_K)} \) 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 \( G \) (i.e., \( G \) is abelian) of an order invertible in \( B \), then for any subgroup \( K \) of \( G, Be_K \) is a Galois extension 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 \( \{e_i | i = 1, 2, \ldots, m\} \) 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.
THE GALOIS EXTENSIONS INDUCED BY IDEMPOTENTS ...

\textbf{Theorem 3.9.} Let $B$ be a Galois algebra with Galois group $G$. Then $B = B_G \oplus B(1-e_G)$ such that $B_G = \bigoplus_{i=1}^{m} B_{ei}$ where each $B_{ei}$ 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 [5, Theorem 3.8].

\textbf{Proof.} Since $e_i = \prod_{h \in H_i} e_h$ where $H_i$ is the maximal subset (subgroup) of $G$ such that $\prod_{h \in H_i} e_h \neq \{0\}$ or $e_i = (1 - \sum_{j=1}^{t} e_j) \prod_{h \in H_i} e_h$ where $H_i$ is the maximal subset (subgroup) of $G$ for some $t < i$ such that $(1 - \sum_{j=1}^{t} e_j) \prod_{h \in H_i} e_h \neq \{0\}$ (see [5, Theorem 3.8]), we have that $e_i(\sum_{g \in G, eg \neq 1} e_g) = e_i$ for each $i$. Thus $\sum_{i=1}^{m} e_i \leq \sum_{g \in G, eg \neq 1} e_g$. Noting that $e_g(1 - \sum_{i=1}^{m} e_i) = 0$ for each $g \neq 1$ in $G$ (see [5, Theorem 3.8]), we have that $(\sum_{g \in G, eg \neq 1} e_g)(1 - \sum_{i=1}^{m} e_i) = 0$, that is, $(\sum_{g \in G, eg \neq 1} e_g)(\sum_{i=1}^{m} e_i) = \sum_{g \in G, eg \neq 1} e_g$. Hence $\sum_{g \in G, eg \neq 1} e_g \leq \sum_{i=1}^{m} e_i$. Thus $\sum_{g \in G, eg \neq 1} e_g = \sum_{i=1}^{m} e_i$, that is, $e_G = \sum_{i=1}^{m} e_i$. But then by [5, Theorem 3.8], $B = \bigoplus_{i=1}^{m} B_{ei} \oplus B(1 - \sum_{i=1}^{m} e_i) = B_G \oplus B(1 - e_G)$ 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 $B_G = \bigoplus_{i=1}^{m} B_{ei}$ such that each $B_{ei}$ 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 $B_a$.

\textbf{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 $e_S = \sum_{i \in Z_S} e_i$.

\textbf{Proof.} Since $C = \bigoplus_{i=1}^{m} C e_i \oplus C f$ (see [5, Theorem 3.8]), $e_S = \sum_{i=1}^{m} c_i e_i + c f$ for some $c_i, c \in C$. It can be checked 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 $e_S = \sum_{i \in Z_S} e_i + c f$. Moreover, since $e_g f = 0$ for each $g \neq 1$ in $G$ (see [5, Theorem 3.8]), we have that $0 = e_S f = (\sum_{i \in Z_S} e_i + c f) f = c f$. Hence $e_S = \sum_{i \in Z_S} e_i$. The uniqueness of $Z_S$ is clear.

Next is a description of the components $B_{ek}$ and $B(1 - e_k)$ for a subgroup $K$ of $G$ as given in Theorem 3.2.

\textbf{Corollary 4.2.} For any subgroup $K$ of $G$, $B = B_{K} \oplus B(1 - e_k)$ such that $B_{k} = \sum_{i \in Z_K} B_{ei}$ 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 $G(e_k)$.

\textbf{Proof.} It is an immediate consequence of Theorems 3.2(2) and 4.1. \hfill \Box

In [4], let $K$ be a subgroup of $G$. Then $K$ is called a nonzero subgroup of $G$ if $\prod_{k \in K} e_k \neq 0$, 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 $K = K'$. 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 (see [4, Theorem 3.2]). Also, any maximal nonzero
subgroup $K = H_e = \{ g \in G \mid e \leq e_g \}$ where $e = \prod_{k \in K} e_k$ and $H_e$ is a normal subgroup of $G(e)$ (see [4, Lemma 3.3]). Next is a characterization of a monomial idempotent $e_S (= \sum_{g \in S, e_g \neq 1} e_g)$ for a subset of $G$.

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

**Proof.** ($\Rightarrow$) By [4, Theorem 3.2], $e \rightarrow H_e$ is a one-to-one correspondence between the set of monomials in $B_a$ and the set of maximal nonzero subgroups of $G$. Noting that $e = \prod_{g \in H_e} e_g$ when $e$ is a monomial, we have for any monomials $e$ and $e'$, $H_e \subset H_e'$ implies that $e \geq e'$. Thus, $e_j \leq e_S$ whenever $H_{e_S} \subset H_{e_j}$ for an atom $e_j$ because $e_S$ is a monomial by hypothesis.

($\Leftarrow$) By Theorem 4.1, $e_S = \sum_{e_i \in Z S} e_i$ where $Z_S = \{ e_i \mid e_i \leq e_S \}$. Let $e = \prod_{g \in H_{e_S}} e_g$. Then $e_S \leq e$ and $H_{e_S} = H_e$. Suppose $e_S \neq e$. Then $e_S = \sum_{e_i \in Z_S} e_i < e = \sum e_j$ where $\sum_{e_i \in Z_S} e_i$ is a direct summand of $\sum e_j$ by Theorem 4.1. It is easy to check that $H_{e_S} = \cap_{e_i \in Z_S} H_{e_i} = H_e = \cap H_{e_j}$. Therefore there exists some $e_j \notin Z_S$, that is, $e_j \notin e_S$ such that $H_{e_S} \subset H_{e_j}$. 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**


George Szeto: Department of Mathematics, Bradley University, Peoria, IL 61625, USA

E-mail address: szeto@hilltop.bradley.edu

Lianyong Xue: Department of Mathematics, Bradley University, Peoria, IL 61625, USA

E-mail address: lxue@hilltop.bradley.edu