The Group Idempotents in a Partial Galois Extension

Xiao-Long Jiang\(^1\) and George Szeto\(^2\)*

Abstract. Let \((R, \alpha_G)\) be a partial Galois extension with a partial action \(\alpha_G\) of a finite group \(G\), \(B\) the Boolean ring generated by \(\{1_g | g \in G\}\) where \(1_g\) is the central idempotent associated with \(g \in G\). Let \(e \neq 0 \in B\) and \(G(e) = \{g \in G | e1_g \neq 0\}\). We call \(e\) a group idempotent if \(G(e)\) is a subgroup of \(G\). It is shown that if \(e\) is a group idempotent, then \((Re, \alpha_{G(e)})\) is a partial Galois extension induced by \(e\). Thus the set of these partial Galois extensions in \((R, \alpha_G)\) is computed, and a structure theorem for \((R, \alpha_G)\) is obtained.

1. Introduction and Preliminaries

Galois theory for rings has been intensively investigated in [1, 3, 4, 7], and recently generalized to partial Galois extensions for rings due to many applications of a partial action of a group on a ring ([2, 5, 6, 7, 8, 9]). In [8], let \(B(R)\) be the Boolean semigroup generated by \(\{1_g | g \in G\}\) under the multiplication of \(R\) where \(1_g\) is the central idempotent associated with \(g \in G\), \(e \in B(R)\), and \(G(e) = \{g \in G | e1_g \neq 0\}\). It is shown that if \(e\) is a minimal element in \(B(R)\) and invariant under the partial action \(\alpha_g\) for each \(g \in G\), then \(G(e)\) is a group such that \(Re\) is a Galois extension of \((Re)^{G(e)}\) with Galois group \(G(e)\) (see Proposition 6 in [8]). The group \(G(e)\) plays an important role for the structure of a partial Galois extension \((R, \alpha_G)\) as given by Theorem 3.8 in [8]. In the present paper, let \((R, \alpha_G)\) be a partial Galois extension with a partial action \(\alpha_G\) and \(B\) the Boolean ring generated by \(\{1_g | g \in G\}\). For any non-zero element \(e \in B\), we call \(e\) a group idempotent if \(G(e)\) is a subgroup of \(G\). We shall show some properties of a group idempotent and that if \(e\) is a group idempotent, then \((Re, \alpha_{G(e)})\) is a partial Galois extension in \((R, \alpha_G)\) such that \(G(e)\) is the group \(K \subset G\) maximal with \((Re, \alpha_K)\) as a partial Galois extension. Thus the set of these partial Galois extensions induced by an idempotent in \((R, \alpha_G)\) is computed and a structure theorem of \((R, \alpha_G)\) is obtained.

Let \(R\) be a ring with 1 and \(G\) a finite group with identity \(1_G\). As defined in [5], \((R, \alpha_G)\) is a ring with a partial action \(\alpha_G\) if \(\alpha_g : D_{g^{-1}} \rightarrow D_g\) is a ring isomorphism where \(D_{g^{-1}}\) and \(D_g\) are ideals of \(R\) for all \(g \in G\) such that (1) \(D_{1_G} = R\) where

\[\text{Date:} \text{Received: Aug 25, 2014; Accepted: Oct 29, 2014}\]

* Corresponding author.

2010 Mathematics Subject Classification. Primary 13B05; Secondary 16W22.

Key words and phrases. Partial Galois extension, Boolean ring, Central idempotent.
$\alpha_{1_G}$ is the identity automorphism of $R$; (2) $\alpha_g(D_g^{-1} \cap D_h) = D_g \cap D_{gh}$ for all $g,h \in G$; (3) $(\alpha_g \alpha_h)(r) = \alpha_{gh}(r)$ for every $r \in (D_{h^{-1}} \cap D_{(gh)^{-1}})$. Assume that $D_g = R1_g$ where $1_g$ is a central idempotent in $R$ for each $g \in G$. Denote $\{r \in R|\alpha_g(r1_g^{-1}) = r1_g\}$ for all $g \in G$ by $R^G_g$. Then $(R, \alpha_G)$ is called a partial Galois extension of $R^G_g$ if there exist $\{x_i; y_i \in R|i = 1, \ldots, n\}$ for some integer $n$ such that $\sum_{i=1}^{n} x_i \alpha_g(y_i1_g^{-1}) = \delta_{g1}1_R$ for $g \in G$, where $\{x_i; y_i\}$ is called a partial Galois system for $R$. We shall employ the following identity $\alpha_g(1_h1_g^{-1}) = 1_{gh}1_g$ for all $g, h \in G$ ([5], page 79).

2. Group Idempotents

By keeping the notations in section 2, $(R, \alpha_G)$ denotes a partial Galois extension. Let $B$ be the Boolean ring generated by $\{g|g \in G\}$ with the usual partial order $e \leq f$ when $e = fe$. Since $G$ is finite, $B$ is finite with minimal elements $\{E_i|i = 1, \ldots, m\}$ for some integer $m$ denoted by $M$. Recall that for an $e \neq 0 \in B, G(e) = \{g \in G|e1_g \neq 0\}$ and $e$ is called a group idempotent if $G(e)$ is a subgroup of $G$. By the canonical form of an element $e \in B, e = \prod_{i \in I_e} E_i$ where $I_e \subset \{1, \ldots, m\}$. In this section, we shall show some properties of $M$.

**Lemma 2.1.** Let $M = \{E_i|i = 1, \ldots, m\}$ be the set of minimal elements in $B$. Then $E_i = \prod_{g \in G} 1_g \neq 0$ with a maximal number of factors $1_g$.

*Proof.* For any $e \neq 0 \in B, e$ is a sum of products of $1_g$ for some $g \in G$ and a product of $1_g$ in the sum is less than $e$, so $E_i = \prod_{g \in G} 1_g \neq 0$ with a maximal number of factors $1_g$.

The following is a characterization of a group idempotent in $M$.

**Lemma 2.2.** For any $E \in M, E$ is a group idempotent if and only if $E \in R^{\alpha_G(e)}$.

*Proof.* See Proposition 6 in [8].

**Theorem 2.3.** (1) Let $e \neq 0 \in R^{\alpha_G(e)}$. If $e1_g1_h \neq 0$ for all $g, h \in G(e)$, then $G(e)$ is a subgroup of $G$. (2) For any $e \neq 0 \in B, e \in M$ if and only if $\prod_{g \in G} 1_g \neq 0$ with a maximal number of factors $1_g$ for all $g \in G(e)$.

*Proof.* (1) Let $g \in G(e)$. Since $\alpha_g(e1_g^{-1}) = e1_g \neq 0, g^{-1} \in G(e)$. Also for any $g, h \in G(e), \alpha_g(e1_h1_g^{-1}) = \alpha_g(e1_h1_g^{-1}) = \alpha_g(e1_g^{-1})\alpha_g(1_h1_g^{-1}) = (e1_g)(1_{gh}1_g) = e1_{gh}1_g \neq 0$. By hypothesis, $e1_h1_g^{-1} \neq 0$, so $e1_{gh} \neq 0$; and so $gh \in G(e)$. Thus $G(e)$ is a group. (2) Since for any minimal element $E$ of $B, E = \prod_{g \in G} 1_g \neq 0$ with a maximal number of factors $1_g$ for $g \in G$ by Lemma 2.1, $E = \prod_{g \in G} 1_g \neq 0$ for all $g \in G(e)$. Thus For any $e \neq 0 \in B, e \in M$ if and only if $\prod_{g \in G} 1_g \neq 0$ with a maximal number of factors $1_g$ for all $g \in G(e)$.

Next we show that $G(e)$ can be computed from $G(E_i)$ where $e = \sum_{i \in I} E_i$ for some $I \subset \{1, \ldots, m\}$.
Theorem 2.4. Let $e \in B, e = \sum_{i \in I} E_i$ where $I \subset \{1, \ldots, m\}$. Then, $G(e)$ is a group if and only if $\bigcup_{i \in I} G(E_i)$ is a group.

Proof. It suffices to show that $G(e) = \bigcup_{i \in I} G(E_i)$. In fact, for any $g \in G(e), e I_g \neq 0$, so $(\sum_{i \in I} E_i) I_g \neq 0$. Hence $E_i I_g \neq 0$ for some $i \in I$. Thus $g \in G(E_i)$; and so $G(e) \subset \bigcup_{i \in I} G(E_i)$. Conversely, for any $g \in \bigcup_{i \in I} G(E_i), g \in G(E_i)$ for some $i \in I$, so $E_i I_g \neq 0$. But $G(e) = \sum_{i \in I} G(E_i)$ and $E_i E_j = E_i \delta_{ij}$ for $i, j \in I$, so $e I_g \neq 0$. Thus $g \in G(e)$. This completes the proof.

Recall that $M = \{E_1, \ldots, E_m\}$ is the set of minimal elements in $B$. We want to show that any $\alpha_h$ for an $h^{-1} \in G(E_i)$ maps $E_i$ in $M$ to an element in $M$.

Theorem 2.5. Let $E \in M$ and $h^{-1} \in G(E)$, then $\alpha_h(E h^{-1}) \in M$.

Proof. By Lemma 2.1, $E = \prod_{g \in G} 1_g \neq 0$ with a maximal number of factors $1_g$, so for any $h^{-1} \in G(E), 1_h^{-1}$ is a factor of $E$. Hence $E h^{-1} = E \neq 0$; and so $\alpha_h(E h^{-1}) = \alpha_h(\prod_{g \in G(E)} 1_g 1_h^{-1}) = (\prod_{g \in G(E)} 1_g 1_h^{-1}) \neq 0$. We claim that $(\prod_{g \in G(E)} 1_g 1_h^{-1}) 1_g 1_h$ is in $M$. It suffices to show that for any $q \notin hG(E), (\prod_{g \in G(E)} 1_g 1_h^{-1}) = 0$. Applying $\alpha_h^{-1}$ to $(\prod_{g \in G(E)} 1_g 1_h^{-1}) q 1_h 1_h^{-1}$, we have $\alpha_h^{-1}(\prod_{g \in G(E)} 1_g 1_h^{-1}) q 1_h 1_h^{-1} = E 1_h^{-1} 1_h^{-1} q = E 1_h^{-1} q$. But $q \notin hG(E), \text{ so } h^{-1} q \notin G(E)$. Thus $E 1_h^{-1} q = 0$. Noting that $\alpha_h^{-1}$ is an isomorphism, we conclude that $(\prod_{g \in G(E)} 1_g 1_h^{-1}) q = 0$; that is, $\alpha_h(E h^{-1})$ is in $M$. This completes the proof.

3. Partial Galois Extensions

Keeping the notations and definitions in section 2, we shall show that any group idempotent $e$ induces a partial Galois extension $(R e, \alpha_G(e))$. Thus we can show that the map $e \rightarrow (R e, \alpha_G(e))$ is a one-to-one correspondence between the set of group idempotents and the set of the partial Galois extensions induced by a group idempotent with a partial action of a subgroup of $G$ maximal for the partial Galois extension $R e$. Also we obtain a structure theorem for $(R, \alpha_G)$ as a direct sum of these partial Galois extensions.

Theorem 3.1. Let $e$ be a group idempotent. Then $e \in R^G$ and $(R e, \alpha_G(e))$ is a partial Galois extension such that $G(e)$ is the subgroup $K$ of $G$ maximal for the partial Galois extension $(R e, \alpha_K)$.

Proof. Let $e = \sum_{i \in I} E_i$ for some $I \subset \{1, \ldots, m\}$. Then $G(e) = \bigcup_{i \in I} G(E_i)$ by Theorem 2.4. For any $h \in G(e)$, since $G(e)$ is a group, $h^{-1}$ is in $G(e)$. Hence there exists an $i \in I$ such that $E_i I_{h^{-1}} \neq 0$. By Theorem 2.5, $\alpha_h(E_i 1_{h^{-1}}) = (\prod_{g \in G(E_i)} 1_g 1_h^{-1}) E_i 1_h$. Noting that $\{hg, hI \in G(E_i)\} \subset G(e)$ such that $(\prod_{g \in G(E_i)} 1_g 1_h^{-1}) E_i 1_h \neq 0$, we have that the minimal idempotent $(\prod_{g \in G(E_i)} 1_g 1_h)$ is a term of $e$. Moreover, for each $i \in I$ such that $E_i 1_{h^{-1}} = 0, \alpha_h(E_i 1_{h^{-1}}) = 0$. Thus $\alpha_h(e 1_{h^{-1}}) = \alpha_h(\sum_{i \in I} (E_i 1_{h^{-1}})) = \sum_{i \in I} \alpha_h(E_i 1_{h^{-1}}) = e 1_h$; and so $e$ is in $R^G$. By hypothesis,
\((R, \alpha_G)\) is a partial Galois extension, so there exist \(\{x_i; y_i \in R | i = 1, \ldots, n\}\) for some integer \(n\) such that \(\sum_i x_i \alpha_G(y_i 1_R) = \delta_1 1_R\). Thus \(\sum_i e \sum_i x_i \alpha_G(y_i 1_R^{-1}) = e \sum_i x_i \alpha_G(y_i 1_R^{-1}) = e \delta_1 1_R\) for each \(g \in G(e)\). This implies that \((Re, \alpha_{G(e)})\) is a partial Galois extension. Moreover, let \((Re, \alpha_K)\) be a partial Galois extension with a partial action of a subgroup \(K\). Then \(e1_k \neq 0\) for each \(k \in K\). Thus \(K \subseteq G(e)\); and so \(G(e)\) is the subgroup \(K\) of \(G\) maximal for the partial Galois extension \((Re, \alpha_K)\).

**Corollary 3.2.** Let \(\lambda : e \rightarrow (Re, \alpha_{G(e)})\) for a group idempotent \(e \in B\). Then \(\lambda\) is a one-to-one correspondence between the set of group idempotents in \(B\) and the set of partial Galois extensions as given in Theorem 3.1.

**Proof.** This is an immediate consequence of Theorem 3.1.

Recall that for any non-zero \(e \in B\), \(e = \sum_{i \in I_e} E_i\) where \(E_i \in M\) and \(I_e \subset \{1, \ldots, m\}\). We shall give an equivalent condition for \((R, \alpha_G)\) as a direct sum of the partial Galois extensions as given in Theorem 3.1.

**Lemma 3.3.** Let \(e, f \in B\) be distinct group idempotents such that \(e = \sum_{i \in I_e} E_i\) and \(f = \sum_{j \in I_f} E_j\). Then, \(ef = 0\) if and only if \(G(E_i) \neq G(E_j)\) for any \(i \in I_e\) and \(j \in I_f\).

**Proof.** Noting that \(E_i\) and \(E_j\) are minimal elements in \(B\), we have that \(E_i = E_j\) if and only if \(G(E_i) = G(E_j)\). Also \(E_i E_j = 0\) for different \(E_i\) and \(E_j\), so \(ef = 0\) if and only if \(E_i E_j = 0\) for any \(i \in I_e\) and \(j \in I_f\). This is equivalent to \(G(E_i) \neq G(E_j)\) for any \(i \in I_e\) and \(j \in I_f\).

**Theorem 3.4.** Let \((R, \alpha_G)\) be a partial Galois extension. Then, \((R, \alpha_G) = \oplus \sum_{i=1}^k (Re_i, \alpha_{G(e_i)})\) a direct sum of partial Galois extensions as given in Theorem 3.1 if and only if \(G(E_s) \neq G(E_t)\) for any \(s \in I_{e_i}\) and \(t \in I_{e_j}\) for any \(i \neq j\) where \(\{e_i, | i = 1, \ldots, k\}\) for some integer \(k\) are group idempotents summing to \(1_R\).

**Proof.** \((\rightarrow)\). Since \((R, \alpha_G)\) is a direct sum of partial Galois extensions as given in Theorem 3.1, \(e_i e_j = 0\) for any \(i \neq j\). Thus \(G(E_s) \neq G(E_t)\) for any \(s \in I_{e_i}\) and \(t \in I_{e_j}\) for any \(i \neq j\) by Lemma 3.3 and \(\{e_i, | i = 1, \ldots, k\}\) for some integer \(k\) are group idempotents summing to \(1_R\).

\((\leftarrow)\). By hypothesis, \(\{e_i, | i = 1, \ldots, k\}\) for some integer \(k\) are group idempotents, so \((Re_i, \alpha_{G(e_i)})\) is a partial Galois extension for each \(i\) as given in Theorem 3.1. Moreover, \(G(E_s) \neq G(E_t)\) for each \(i\) as given in Theorem 3.1. Thus the proof is complete.
Remark To compute the Boolean ring $B$ generated by $\{1_g | g \in G\}$, it suffices to compute the set of all minimal elements $\{E_i | i = 1, \ldots, m\}$ by the canonical form of an element in $B$. Then $G(e)$ can be computed from $G(E_i)$ by Theorem 2.4. Thus the set of all group idempotents can be computed also by Theorem 2.4.

We conclude the present paper with an example to demonstrate the computation.

Example Let $(R, \alpha_G)$ be the partial Galois extension as given by Example 6.3 in [5]: $R = \sum_{i=1}^6 Ae_i$ where $A$ is a commutative Galois algebra with Galois cyclic group $G$ with a generator $g$ of order 6, and $\{e_i | i = 1, \ldots, 6\}$ are orthogonal non-zero idempotents summing to $1_R$. The partial action $\alpha_G$ on $R$ is defined by: $\alpha_G : A(e^{6-i}) \to A(e^i)$ for each $i$. Then every non-identity element $e_i$ is a minimal element in $B$ so that $M = \{1_g^61_g, 1_g^61_g^2, 1_g^61_g^3, 1_g^61_g^4, 1_g^61_g^5\}$. Thus there are three proper group idempotents: $E_1 = \{1_g^61_g + 1_g^61_g^2, E_2 = 1_g^61_g^2 + 1_g^61_g^4, E_3 = 1_g^61_g^3\}$; and so there are three proper partial Galois extensions of $(R, \alpha_G)$ by Theorem 3.1.

Acknowledgement
This paper was done at Sun Yat-sen University, Guangzhou, China in Summer, 2014 when the second author visited the Mathematics Department of Sun Yat-sen University, and supported by a Research Excellence Award at Bradley University. The second author would like to thank Sun Yat-sen University for her hospitality and the award.

References

1 Department of Mathematics, Sun Yat-Sen University, Guangzhou, 510275 P.R. China
E-mail address: mcsjxl@mail.sysu.edu.cn
2 Department of Mathematics, Bradley University, Peoria, Illinois 61625 U.S.A.
E-mail address: szeto@fsmail.bradley.edu