

On Galois Groups of a Semiconnected Galois Extension

George Szeto and Lianyong Xue

Department of Mathematics, Bradley University

Peoria, Illinois 61625 – U.S.A.

Email: szeto@bradley.edu and lxue@bradley.edu

Abstract

Let B be a semiconnected Galois extension (that is, B contains only finitely many central idempotents) with Galois group G , and G' the fat group of G . Then an equivalent condition is given under which a subgroup of G' is a Galois group for B . A semiconnected Galois extension B with a cyclic permutation Galois group G is constructed, and all cyclic Galois subgroups of G' are computed.

Key Words and phrases. Galois extensions, semiconnected Galois extensions, fat groups of Galois groups.

2000 Mathematics Subject Classification. Primary 16S35, 16W20.

1. Introduction. The Galois theory for semiconnected rings was investigated in [4] and [9], where a ring is called semiconnected if it contains only finitely many central idempotents. Let B be a semiconnected Galois extension of B^G with Galois group G . Then $B = \sum_{i=1}^m B e_i$, where e_i are minimal central idempotents of B for some integer m , and the fundamental theorem states that there exists a one-to-one correspondence between the set of fat groups of subgroups of G and the set of certain subextensions in B ([9], Theorem, [4], Theorem 13 and Theorem 15) where the fat group K' of a subgroup K of G is $\{\alpha \in \text{Aut}_{B^G}(B) \mid \text{for each } i = 1, 2, \dots, m, \alpha|_{B e_i} = k_i|_{B e_i} \text{ for some } k_i \in K\}$ ([9]). A Galois extension of B^G with Galois group G such that $G = \text{Aut}_{B^G}(B)$ are characterized ([7],[8]). Thus there are many Galois extensions of rings B whose Galois group $G \neq \text{Aut}_{B^G}(B)$. Let

B be a semiconnected Galois extension of B^G with Galois group G . In the present paper, we are interested in what kind of fat groups K' of subgroups K of G are Galois group for B ; that is, B is a Galois extension of $B^{K'}$ with Galois group K' . Moreover, it is known that a Galois group G of a semiconnected Galois extension is a semidirect product of $G(e_i)$ and P_m where $G(e_i) = \{g \in G \mid g(e_i) = e_i\}$ for each $i = 1, 2, \dots, m$, and P_m the symmetric group on the set $\{e_i \mid i = 1, 2, \dots, m\}$ ([4], [9]). We are interested in two cases: (i) $P_m = \langle 1 \rangle$ and (ii) $G(e_1) = \langle 1 \rangle$. Case (1) was studied in [4]. It was shown that $Be_i \cong Be_1$ and Be_i is a Galois extension of $(Be_i)^{G(e_i)}$ with Galois group $G(e_i)$ which is isomorphic with G for each $i = 1, 2, \dots, m$. For case (ii), we shall give an equivalent condition for a cyclic subgroup of the fat group G' of G being a Galois group for B . This provides examples of Galois extensions of noncommutative rings with cyclic Galois groups by comparing the case that any Galois algebra with cyclic Galois group is commutative ([1], Theorem 11, [3], Theorem 4).

2. Definitions and Notations. Let B be a ring with 1, G a finite automorphism group of B , and B^G the set of elements in B fixed under each element in G . Then B is called a Galois extension of B^G with Galois group G if there exist elements $\{a_i, b_i$ in B , $i = 1, 2, \dots, k\}$ for some integer k such that $\sum_{i=1}^k a_i g(b_i) = \delta_{1,g}$ for each $g \in G$. We call B semiconnected if it contains only finitely many central idempotents.

Throughout this paper, the ring B is a semiconnected Galois extension of B^G with Galois group G , C the center of B with finite number of idempotents, $I (= \{e_i \mid i = 1, 2, \dots, m$ for some integer $m\})$ the set of minimal central idempotents of B , $G(e_i) = \{g \in G \mid g(e_i) = e_i\}$ for each $e_i \in I$, and $\{a_i, b_i \in B$, $i = 1, 2, \dots, k\}$ a Galois system for B . The fat group of G is denoted by G' , that is, $G' = \{\alpha \in \text{Aut}(B)$ such that for each $i = 1, 2, \dots, m$, $\alpha|_{Be_i} = g_i|_{Be_i}$ for some $g_i \in G\}$. In particular, we call an $\alpha \in G'$ a Galois element for B if $\sum_{i=1}^k a_i \alpha(b_i) = \delta_{1,\alpha}$, and a subgroup K of G' is called a Galois group for B if each element in K is a Galois element for B .

3. Galois Groups. Keeping the notations as given in section 2, we shall give an equivalent condition for a subgroup K' of G' under which K' is a Galois group for B . Let $\alpha \in G'$ and $\{O_i(\alpha) \mid i = 1, 2, \dots, n(\alpha)\}$ the set of orbits of I under the α -action. Then $I = \cup_{i=1}^{n(\alpha)} O_i(\alpha)$. Denote $\sum_{e_j \in O_i(\alpha)} e_j$ by E_i . Then $B = \oplus \sum_{i=1}^m B e_i = \oplus \sum_{i=1}^{n(\alpha)} B E_i$ and $\alpha(E_i) = E_i$ for each $i = 1, 2, \dots, n(\alpha)$. As given in section 2, $G(e) = \{g \in G \mid g(e) = e\}$ for each central idempotent e of B . We first show that the fat group G' of G is not a Galois group for B when $m > 1$.

PROPOSITION 3.1. *If e is a nonzero central idempotent of B , then $G(e) \cong G(e)|_{Be}$.*

PROOF. Let $g \in G(e)$ such that $g|_{Be} = \text{identity}$. Then $g(be) = be$ for all $b \in B$. Assume $g \neq 1$ in G . Then $\sum_{i=1}^k a_i g(b_i) = 0$ where $\{a_i, b_i \in B \mid i = 1, 2, \dots, k\}$ is a Galois system for B . Since $g(e) = e$, $\sum_{i=1}^k (a_i e) g(b_i e) = 0$; and so $\sum_{i=1}^k (a_i e)(b_i e) = 0$. But $\sum_{i=1}^k a_i b_i = 1$, so $\sum_{i=1}^k (a_i e) g(b_i e) = e \neq 0$. This is a contradiction. Thus $G(e) \cong G(e)|_{Be}$.

THEOREM 3.2. *If $I (= \{e_i \mid i = 1, 2, \dots, m\})$ has more than one element (that is, $m > 1$), then G' is not a Galois group.*

PROOF. Since $m > 1$, $B = \oplus \sum_{i=1}^m B e_i$ has more than one direct summands. Let $\alpha \in G'$ such that $\alpha|_{Be_1} = \text{identity}$, and $\alpha|_{Be_i} \neq \text{identity}$ for some $i \neq 1$. Since G contains an identity and a nonidentity element, such an α exists in G' . Since $\alpha \neq 1$, it suffices to show that $\sum_{p=1}^k a_p \alpha(b_p) \neq 0$. In fact, since $\alpha|_{Be_1} = \text{identity}$, α permutes the set $\{e_2, e_3, \dots, e_m\}$. Hence $\sum_{p=1}^k a_p \alpha(\sum_{i=2}^m b_p e_i) \in \sum_{i=2}^m B e_i$. Thus

$$\begin{aligned} \sum_{p=1}^k a_p \alpha(b_p) &= \sum_{p=1}^k a_p \alpha\left(\sum_{i=1}^m b_p e_i\right) = \sum_{p=1}^k a_p \alpha(b_p e_1) + \sum_{p=1}^k a_p \alpha\left(\sum_{i=2}^m b_p e_i\right) \\ &= \sum_{p=1}^k a_p b_p e_1 + \sum_{p=1}^k a_p \alpha\left(\sum_{i=2}^m b_p e_i\right) = e_1 + b \neq 0 \end{aligned}$$

where $b = \sum_{p=1}^k a_p \alpha(\sum_{i=2}^m b_p e_i) \in \sum_{i=2}^m B e_i$. This proves that α is not a Galois element for B .

As defined in section 2, an element $\alpha \in G'$ is called a Galois element for B if $\sum_{i=1}^k a_i \alpha(b_i) = \delta_{1,\alpha}$. Now we give a characterization of a Galois element for B .

LEMMA 3.3. *By keeping the notations of Theorem 3.2, for any $\alpha \in G'$, α is a Galois element for B if and only if $\alpha = 1$ or $\alpha|_{BE_i} \neq \text{identity}$ for each $i = 1, 2, \dots, n(\alpha)$, where $E_i = \sum e_j$, $e_j \in O_i(\alpha)$, the i th orbit of I under the α -action.*

PROOF. (\Leftarrow) Let $\alpha \in G'$ such that $\alpha = 1$ or $\alpha|_{BE_i} \neq \text{identity}$ for each $i = 1, 2, \dots, n(\alpha)$. We claim that $\sum_{p=1}^k a_p \alpha(b_p) = \delta_{1,\alpha}$. In case $\alpha = 1$, $\sum_{p=1}^k a_p \alpha(b_p) = \sum_{p=1}^k a_p b_p = 1 = \delta_{1,\alpha}$. In case $\alpha|_{BE_i} \neq \text{identity}$ for each $i = 1, 2, \dots, n(\alpha)$. We claim that $\sum_{p=1}^k a_p \alpha(b_p) = 0$. For each $i = 1, 2, \dots, n(\alpha)$, $E_i = \sum_{e_l \in O_i} e_l$ where O_i is an orbit of I under the α -action. We claim that $\alpha|_{Be_l} \neq \text{identity}$ for each $e_l \in O_i$. In fact, assume that $\alpha|_{Be_l} = \text{identity}$ for some $e_l \in O_i$. Then $O_i = \{e_l\}$ with only one element e_l ; and so $\alpha|_{BE_i} = \alpha|_{Be_l} = \text{identity}$. This contradicts with the hypothesis that $\alpha|_{BE_i} \neq \text{identity}$. Hence $\alpha|_{Be_l} \neq \text{identity}$ for each $e_l \in O_i$. Next, since $\alpha \in G'$, there exists a $g_l \in G$ such that $\alpha|_{Be_l} = g_l|_{Be_l} \neq \text{identity}$ for each $e_l \in O_i$. Hence

$$\begin{aligned} E_i \left(\sum_{p=1}^k a_p \alpha(b_p) \right) &= \sum_{p=1}^k a_p \alpha(b_p E_i) = \sum_{e_l \in O_i} \sum_{p=1}^k a_p \alpha(b_p e_l) \\ &= \sum_{e_l \in O_i} \sum_{p=1}^k a_p g_l(b_p e_l) = \sum_{e_l \in O_i} \left(\sum_{p=1}^k a_p g_l(b_p) \right) g_l(e_l) = 0. \end{aligned}$$

Thus $\sum_{p=1}^k a_p \alpha(b_p) = \sum_{i=1}^{n(\alpha)} (E_i \sum_{p=1}^k a_p \alpha(b_p)) = 0$. We conclude that α is a Galois element for B .

(\Rightarrow) Since α is a Galois element for B , $\sum_{p=1}^k a_p \alpha(b_p) = \delta_{1,\alpha}$. If $\alpha = 1$, we are done. If $\alpha \neq 1$, then $\alpha|_{BE_i} \neq \text{identity}$ for some $i = 1, 2, \dots, n(\alpha)$ (for $B = \bigoplus_{i=1}^{n(\alpha)} BE_i$). We claim that $\alpha|_{BE_i} \neq \text{identity}$ for each $i = 1, 2, \dots, n(\alpha)$. In fact, at first, by the argument as given in the above proof of the sufficiency, that $\alpha|_{BE_i} \neq \text{identity}$ for some $i = 1, 2, \dots, n(\alpha)$ implies that

$$E_i \left(\sum_{p=1}^k a_p \alpha(b_p) \right) = 0. \quad (*)$$

Then, assuming $\alpha|_{BE_j} = \text{identity}$ for some $j = 1, 2, \dots, n(\alpha)$, we have that

$$E_j \left(\sum_{p=1}^k a_p \alpha(b_p) \right) = \sum_{p=1}^k a_p \alpha(b_p E_j) = \sum_{p=1}^k a_p b_p E_j = E_j. \quad (**)$$

Hence

$$0 = \delta_{1,\alpha} = \sum_{p=1}^k a_p \alpha(b_p) = \sum_{i=1}^{n(\alpha)} (E_i \sum_{p=1}^k a_p \alpha(b_p)) = \sum_{j \in J} E_j \neq 0$$

where $J = \{j \mid \alpha \text{ restricted on } BE_j \text{ is identity}\}$ by (*) and (**). This is a contradiction.

Thus $\alpha|_{BE_i} \neq \text{identity}$ for each $i = 1, 2, \dots, n(\alpha)$. This completes the proof.

By Lemma 3.3, we have an equivalent condition for a subgroup K' of G' being a Galois group for B .

THEOREM 3.4. *Let K' be a subgroup of G' . Then K' is a Galois group for B if and only if each element α in K' is either $\alpha = 1$ or $\alpha|_{BE_i} \neq \text{identity}$ for each $i = 1, 2, \dots, n(\alpha)$.*

4. Cyclic Galois Groups. It was known that a Galois algebra with cyclic Galois group is commutative ([1], Theorem 11, [3], Theorem 4). In this section, keeping the notations as given in section 3, we shall construct a semiconnected Galois extension B (not necessarily commutative) with a cyclic permutation Galois group $G \subset P_m$ where P_m is the permutation group on m symbols, and compute all cyclic Galois groups in G' for B as an application of Theorem 3.4.

LEMMA 4.1. *If $\beta \in P_m$ is a product of disjoint cycles of same length, then β^i is also a product of disjoint cycles of same length for each $i = 1, 2, \dots, m$.*

PROOF. In fact, if the order of β is s , then the order of β^i is s/d where d is the greatest common divisor of s and i .

THEOREM 4.2. *Let A be a ring with no central idempotents but 0 and 1, $B = A^m$, a direct sum of m -copies of A with multiplication and addition componentwise, and $G = \langle \alpha \rangle$, a cyclic automorphism group generated by the permutation $\alpha(x_1, x_2, x_3, \dots, x_m) = (x_m, x_1, x_2, \dots, x_{m-1})$ for $(x_1, x_2, \dots, x_m) \in B$. Then (1) B is a semiconnected Galois extension with Galois group G , and (2) for a cyclic subgroup $\langle \beta \rangle$ of G' for some $\beta \in G'$, $\langle \beta \rangle$ is a Galois group for B if and only if β is a product of disjoint cycles of same length t for some divisor t of m for $t > 1$.*

PROOF. (1) Let $a_i = b_i = (0, 0, \dots, 0, 1, 0, \dots, 0, 0)$ with 1 at the i th component and 0 elsewhere for $i = 1, 2, \dots, m$. Then $\sum_{i=1}^m a_i b_i = (1, 1, \dots, 1) =$ the identity of B , and $\sum_{i=1}^m a_i \alpha^t(b_i) = (0, 0, \dots, 0) =$ the zero of B for $t = 1, 2, \dots, m - 1$. Since $G = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$, $\{a_i, b_i \mid i = 1, 2, \dots, m\}$ is a Galois system for B . Thus B is a Galois extension with Galois group G with minimal central idempotents $\{a_i \mid i = 1, 2, \dots, m\}$.

(2) Since $G = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$, G is a transitive Galois group on the set of minimal central idempotents $I (= \{e_i \mid i = 1, 2, \dots, m\})$ where $e_i = a_i$ for $i = 1, 2, \dots, m$. Hence $B = \bigoplus \sum_{i=1}^m B e_i = A^m$ and $G' = P_m$, the permutation group on m symbols. Thus $\langle \beta \rangle \subset P_m$; and so $\langle \beta \rangle$ is a Galois group for B if and only if β is a product of disjoint cycles of same length t for some divisor t of m by Theorem 3.4 and Lemma 4.1.

COROLLARY 4.3. *Let $B = A^m$ with a cyclic automorphism group $\langle \alpha \rangle$ as given in Theorem 4.2. If β in P_m is a Galois element for B , then so is β^i for each $i = 1, 2, \dots, m$, that is, $\langle \beta \rangle$ is a Galois group for B .*

PROOF. This is an immediate consequence of Lemma 4.1 and Theorem 4.2.

COROLLARY 4.4. *Let B be given in Theorem 4.2. Then there are*

$$\sum_{\substack{t \mid m \\ t > 1}} \frac{m!}{(t \cdot \phi(t))^{m/t} \cdot (m/t)!}$$

number of cyclic Galois groups in G' for B where $\phi(t) =$ the number of $i = 1, 2, \dots, t$ which is relatively prime to t .

PROOF. By Theorem 4.2, for each $\beta \in P_m$, $\langle \beta \rangle$ is a Galois group for B if and only if β is a product of disjoint cycles of same length $t > 1$ for some divisor t of m . Hence the number of cyclic Galois groups in G' is equal to the number of the cyclic subgroups $\langle \beta \rangle$ such that β is a product of disjoint cycles of same length $t > 1$ for some divisor t of m . For each divisor $t > 1$ of m , there are $\frac{m!}{(t!)^{m/t}} \cdot \frac{1}{(m/t)!}$ different partitions of $\{1, 2, \dots, m\}$ into $\frac{m}{t}$ parts of t elements each. For each part of t elements, $(t-1)!$ cyclic permutations of order t can be formed, so each generates a cyclic group of order t . Noting that each cyclic group of order t has $\phi(t)$ different generators, we conclude that for each partition we can form $\left(\frac{(t-1)!}{\phi(t)}\right)^{m/t}$ number of distinct cyclic subgroups of order t . Hence for each divisor t of m such that $t > 1$, there are

$$\frac{m!}{(t!)^{m/t}} \cdot \left(\frac{(t-1)!}{\phi(t)}\right)^{m/t} \cdot \frac{1}{(m/t)!} = \frac{m!}{(t \cdot \phi(t))^{m/t} \cdot (m/t)!}$$

distinct cyclic Galois subgroups of order t for B . Thus

$$\sum_{\substack{t|m \\ t>1}} \frac{m!}{(t \cdot \phi(t))^{m/t} \cdot (m/t)!}$$

is the total number of cyclic Galois groups in G' for B .

We conclude the present paper with a semiconnected Galois extension with a cyclic permutation Galois group to demonstrate our results.

EXAMPLE 4.5. Let $B = A^4$ be as given in Theorem 4.2 where A is a ring with no central idempotents but 0 and 1 (for example, $A = M_2(R)$, the matrix ring of order 2 over the real field R), and $G = \langle \alpha \rangle$ where $\alpha(a_1, a_2, a_3, a_4) = (a_4, a_1, a_2, a_3)$ for $(a_1, a_2, a_3, a_4) \in B$. Then

(1) $B = \sum_{i=1}^4 B e_i$ is a semiconnected Galois extension with a cyclic automorphism group $\langle \alpha \rangle \subset G'$ ($= P_4$).

(2) There are $\frac{4!}{(2 \cdot \phi(2))^{4/2} \cdot (4/2)!} + \frac{4!}{(4 \cdot \phi(4))^{4/4} \cdot (4/4)!} = 3 + 3 = 6$ different cyclic Galois groups in G' ($= P_4$) for B .

(3) In G' , there are noncyclic Galois groups in G' for B . Let $H = \{1, \alpha = (12)(34), \beta = (13)(24), \alpha\beta = (14)(23)\} \subset G'$. Then H is a Galois group for B by Theorem 4.2.

Next example shows that Galois elements do not necessarily generate a Galois group.

EXAMPLE 4.6. Let $B = A^6$ be as given in Theorem 4.2 with a cyclic automorphism group $\langle (123456) \rangle \subset G'$ ($= P_6$). Let $\alpha = (12)(34)(56)$, $\beta = (123)(456)$, and $H = \langle \alpha, \beta \rangle$. Then α and β are Galois elements such that $\alpha\beta = (1)(2463)(6)$. Thus $\alpha\beta$ is not a Galois element by Theorem 4.2; and so H is not a Galois group for B .

ACKNOWLEDGEMENT. This paper was written under the support of a Caterpillar Fellowship at Bradley University. The authors would like to thank Caterpillar Inc. for the support.

REFERENCES

- [1] F.R. DeMeyer, *Some Notes on the General Galois Theory of Rings*, Osaka J. Math., **2** (1965), 117-127.
- [2] F.R. DeMeyer and E. Ingraham, *Separable Algebras over Commutative Rings*, Lecture Notes in Mathematics, Volume 181, Springer Verlag, Berlin, Heidelberg, New York, 1971.
- [3] T. Kanzaki, *On Galois Algebra Over A Commutative Ring*, Osaka J. Math., **2** (1965), 309-317.
- [4] K. Kishimoto and T. Nagahara, *On G -extensions of a semi-connected ring*, Math. J. Okayama Univ. **32** (1990), 25-42.

- [5] G. Szeto and L. Xue, *The structure of Galois algebras*, Journal of Algebra, **237** (2001), no. 1, 238-246.
- [6] G. Szeto and L. Xue, *The Boolean Algebra of Galois Algebras*, International Journal of Mathematics and Mathematical Sciences, **11** (2003), 673-679.
- [7] G. Szeto and L. Xue, *The Galois Algebra with Galois Group which is the Automorphism Group*, Journal of Algebra, to appear.
- [8] G. Szeto and L. Xue, *On Galois Extensions with Automorphism Group as Galois Group*, Contemporary Mathematics, Proceeding of "Conference on Algebra and Its Applications", Ohio University, March 22-25, 2005. to appear.
- [9] O. Villamayor and D. Zelinsky, *Galois theory for rings with finitely many idempotents*, Nagoya Math. J. **27**(1966), 721-731.