Gulf Journal of Mathematics
Vol 2, Issue 3 (2014) 26-29

ON GALOIS MATRIX EXTENSIONS OF HIGH ORDER

XIAOLONG JIANG[1] AND GEORGE SZETO[2*]

Abstract. Let R be a commutative ring with 1 and A a central R-Galois algebra with an inner Galois group G of order n for some integer n. Let $M_m(R)$ be the ring of $m \times m$-matrices over R for an integer m. Then $M_m(R)$ is also a central Galois R-algebra with an inner Galois group for each $m = n^{(2^i)}$ where i is a non-negative integer. In particular, 2 is invertible in R if and only if $M_m(R)$ is a central Galois R-algebra with an inner Galois group for each $m = 2^{(2^i)}$ where i is a non-negative integer.

1. Introduction and preliminaries

Let $S \subset T$ be rings with the same identity. As given in ([1], [2], [3], and [4]), the ring extension T/S is called a separable extension if the multiplication map $T \otimes_S T \longrightarrow T$ splits as T-bimodules, and a separable extension of its center is called an Azumaya algebra over its center. Let G be a finite automorphism group of T. Then T is called a Galois extension of S if there exists $\{a_i, b_i \in T | i = 1, \cdots, k\}$ for some integer k such that $\sum_i a_i g(b_i) = \delta_{1,g}$ and $T^G = S$ where $T^G = \{t \in T | g(t) = t \text{ for each } g \in G\}$, and a Galois extension T of S is a central Galois S-algebra if S is the center of T. The set of elements $\{a_i, b_i \in T\}$ is called a G-Galois system for the Galois extension T of S. Throughout the paper, let R be a commutative ring with 1, $M_n(R)$ the matrix ring over R of order n for an integer n. Let G be a finite group of order m for an integer m. As defined in [3], RG_f is called a projective group algebra of G over R if RG_f has an R-basis $\{U_i | i = 1, \cdots, m\}$ such that $rU_i = U_i r$ for all $r \in R$ and for each i, and $U_i U_j = U_k f(g_i, g_j)$ where $g_i g_j = g_k \in G$ and $f : G \times G \longrightarrow U(R)$ (= the set of units of R) is a factor set.

Galois theory for fields has been generalized to Galois theory for rings ([1], [2], [3], and [4]). Central Galois algebras play an important role in Galois cohomology theory and algebraic geometry. In [3], a structure theorem for a central Galois algebra with an inner Galois group is given. Let A be an R- central Galois algebra with an inner Galois group G of order n induced by the elements $\{U_i | i = 1, 2, \cdots, n \text{ for some integer } n\}$. Then $A = RG_f$ which is a projective group algebra of G over R ([3, Theorem 6]). Conversely, any Azumaya projective

Date: Received: Dec 21, 2013; Accepted: Apr 1, 2014.
* Corresponding author.
2010 *Mathematics Subject Classification.* Primary 13B05; Secondary 16S35.
Key words and phrases. Central Galois Algebras, Matrix Rings, Projective Group Algebras, Inner Galois Groups.

group algebra RG_f over R is a central Galois R-algebra with an inner Galois group induced by the elements of the basis of RG_f ([2, Theorem 3]). We note that the endomorphism ring of RG_f is a matrix ring over R and the equivalent conditions for a Galois matrix ring as given by *Theorem* 2.3 in ([5]). The purpose of the present paper is to obtain many Galois matrix algebras $M_m(R)$ of order m for an integer m by using the above structure theorem of a central Galois algebra with an inner Galois group. Then the result implies the following equivalent condition for a Galois R-algebra $M_2(R)$ with an inner Galois group: 2 is invertible in R if and only if $M_m(R)$ is a Galois R-algebra with an inner Galois group for each $m = 2^{(2^i)}$ where $i \geq 0$. Thus when $n = 2$, we obtain an equivalent condition for the Galois matrix R-algebra $M_2(R)$ with an inner Galois group better than the one as given by *Theorem* 2.3 in [5].

2. Galois Matrix Rings

In this section, we shall show that the endomorphism ring of a central Galois algebra with an inner Galois group is also a central Galois algebra with an inner Galois group. Thus we have many central Galois matrix algebras of order higher than 2, and obtain an equivalent condition for a Galois matrix algebra of order 2 with an inner Galois group better than the one as given by *Theorem* 2.3 in [5]. We begin with some properties of a central Galois algebra.

Lemma 2.1. *If A and B are central Galois algebras over R with Galois groups G and H respectively, then $A \otimes_R B$ is a central Galois algebra over R with Galois group $G \otimes H$.*

Proof. Since A and B are Galois algebras over R with Galois groups G and H respectively, A contains a G-Galois system $\{a_i, b_i | i = 1, \cdots, n$ for some integer $n\}$ and B contains an H-Galois system $\{c_j, d_j | j = 1, \cdots, m$ for some integer $m\}$ such that $\sum_i a_i g(b_i) = \delta_{1,g}$ and $\sum_j c_j h(d_j) = \delta_{1,h}$. Then $\sum_{i,j}(a_i \otimes c_j)((g \otimes h)(b_i \otimes d_j)) = \sum_{i,j}(a_i \otimes c_j)(g(b_i) \otimes h(d_j)) = \sum_{i,j} a_i g(b_i) \otimes c_j h(d_j) = \delta_{1,g\otimes h}$. Thus $A \otimes_R B$ contains a $G \otimes H$-Galois system, $\{a_i \otimes c_j, b_i \otimes d_j\}$; and so $A \otimes_R B$ is a Galois extension of $(A \otimes_R B)^{G\otimes H}$. Next we compute $(A \otimes_R B)^{G\otimes H}$. Clearly, $B \cong R \otimes_R B \subset (A \otimes_R B)^{G\otimes 1}$. Conversely, let $\sum_i x_i \otimes y_i \in (A \otimes_R B)^{G\otimes 1}$. Then $(g\otimes 1)(\sum_i x_i \otimes y_i) = \sum_i g(x_i) \otimes y_i = \sum_i x_i \otimes y_i$ for each $g \in G$. Let k be the order of G and $tr(\ ) = \sum_g g(\ )$. Then $k(\sum_i x_i \otimes y_i) = \sum_i tr(x_i) \otimes y_i = \sum_i 1 \otimes tr(x_i) y_i \in R \otimes_R B$. Since A is a central Galois R-algebra with Galois group G, the order of G is invertible in R. Thus $\sum_i x_i \otimes y_i \in R \otimes_R B$; and so $B \cong R \otimes_R B = (A \otimes_R B)^{G\otimes 1}$. Therefore $(A \otimes_R B)^{G\otimes H} = ((A \otimes_R B)^{G\otimes 1})^{1\otimes H} \subset (R \otimes_R B)^{1\otimes H} \subset R \otimes_R R \cong R$ similarly. Consequently, $(A \otimes_R B)^{G\otimes H} = R$. Moreover, By hypothesis, A and B are central Galois R-algebras, so $A \otimes_R B$ is an Azumaya R-algebras; and so the center of $A \otimes_R B$ is R. Thus $A \otimes_R B$ is a central Galois R-algebra with Galois group $G \otimes H$.

□

Lemma 2.2. *If A is a central Galois R-algebra with Galois group G, then the opposite algebra A^o of A is also a central Galois R-algebra with Galois group G^o where G^o is the opposite group of G.*

Proof. Let $\{a_i, b_i | i =, \cdots, n\}$ for some integer n be a G-Galois system for A. It is straightforward to verify that $\{b_i, a_i | i = 1, \cdots, n\}$ is a Galois G^o-system for A^o. □

.

Corollary 2.3. *Let A be a central Galois R-algebra with Galois group G. Then $A \otimes_R A^o$ is a central Galois R-algebra with Galois group $G \otimes G^o$.*

Proof. This is an immediate consequence of *Lemma* 3.1 and *Lemma* 3.2. □

Applying *Corollary* 2.3 to a central Galois algebra with an inner Galois group G, we obtain many matrix Galois R-algebras of order higher than 2.

Lemma 2.4. *Let A be a central Galois R-algebra with an inner Galois group G induced by the elements $\{U_i \in A | i = 1, \cdots, n$ for some integer $n\}$. Then $M_n(R)$ is a central Galois R-algebra with an inner Galois group of order n^2.*

Proof. Since A is a central Galois R algebra with an inner Galois group G induced by the elements $\{U_i \in A | i = 1, \cdots, n$ for some integer $n\}$, by the structure theorem ([3, Theorem 6]) $A = RG_f$, an Azumaya projective group algebra of G over R with an R-basis $\{U_i \in A | i = 1, \cdots, n$ for some integer $n\}$. Hence $Hom_R(A, A) \cong M_n(R)$, a matrix algebra over R of order n. Noting that A is an Azumaya R-algebra, we have $Hom_R(A, A) \cong A \otimes_R A^o$ ([4, Theorem 3.4]). By *Corollary* 2.3, $A \otimes_R A^o$ is a central Galois R-algebra with Galois group $G \otimes G^o$, so $M_n(R)$ is a central Galois R-algebra with Galois group isomorphic with $G \otimes G^o$. Since G is inner, so is G^o. Thus $G \otimes G^o$ is inner of order n^2. □

Next we obtain many central Galois matrix algebras of order higher than 2.

Theorem 2.5. *Let A be a central Galois R-algebra with an inner Galois group G of order n for some integer n. Then $M_m(R)$ where $m = n^{2^i}$ is a central Galois R-algebra with an inner Galois group of order $n^{2^{i+1}}$ for each $i \geq 0$.*

Proof. By *Lemma* 2.4, $M_n(R)$ is a central Galois R-algebra with an inner Galois group of order n^2, so $M_{(n^2)}(R)$ is a central Galois R-algebra with an inner Galois group of order n^{2^2} by *Lemma* 2.4 again. Then by induction, the theorem holds. □

In [5], a central Galois matrix R-algebra $M_n(R)$ of order n with an inner Galois group G induced by $\{U_i \in M_n(R) | i = 1, \cdots, n^2\}$ for an integer n is characterized in terms of n and the trace of G. For $n = 2$, the conditions of 2 invertible in R and the zero trace of U_i for each $i \neq 0$ are redundent.

Theorem 2.6. *$M_2(R)$ is a central Galois R-algebra with an inner Galois group if and only if 2 is invertible in R. If 2 is invertible in R, then $M_{(2^{2^i})}(R)$ is a central Galois algebra R-algebra with an inner Galois group for each $i \geq 0$.*

Proof. By *Theorem* 2.3 in [6], if 2 is invertible in R, $M_2(R)$ is a central Galois R-algebra with an inner Galois group. Conversely, since $M_2(R)$ is a central Galois R-algebra of rank 4 over R, it is well known that the order of the Galois group is 4 which is invertible in R. Thus 2 is invertible in R. Moreover, the last statement is a consequence of *Theorem* 2.5.

□

Acknowledgement.
The major part of the present paper was done at Sun Yat-Sen University, Guangzhou, P.R. China in Summer, 2013 when the second author visited the Mathematics Department of Sun Yat-Sen University. The second author would like to thank Sun Yat-Sen University for her hospitality.

References

1. R. Alfaro and G. Szeto, On Galois extensions of an Azumaya algebra, *Comm. Algebra,* **25** 1997, 1873-1882.
2. F.R. DeMeyer, Galois Theory in Separable Algebras over Commutative Rings, *Illinois J. Math.,* **10** 1966, 287-295.
3. F.R. DeMeyer, Some notes on the general Galois theory of rings, *Osaka J. Math.,* **2** 1965, 117-127.
4. F.R. DeMeyer and E. Ingraham, Separable Algebras over Commutative Rings, **181**, Springer Verlag, Berlin, Heidelberg, New York, 1971.
5. X.L. Jiang and G. Szeto, On Galois Matrix Rings of a Ring, *Gulf J. Math.,* **1** 2013, 1-4.
6. A. Nelson and G. Szeto, When Is the Ring of 2x2 Matrices over a Ring Galois? *International J. Algebra,* **7** 2013, 439-444.

[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