Gulf Journal of Mathematics
Vol 1, Issue 2 (2013) 129-132

ON GALOIS MATRIX RINGS OF A RING

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

Abstract. Let R be a ring with 1, $M_n(R)$ the ring of $n \times n$-matrices over R for an integer n, and G an inner automorphism group of $M_n(R)$ of order n^2 induced by $\{U_i \in M_n(R), i = 1, \ldots, n^2\}$. Then the Galois matrix ring $M_n(R)$ over R with inner Galois group G is characterized in terms of $\{U_i\}$ and the trace of G.

1. Introduction and preliminaries

Let R be a ring with 1, and $M_n(R)$ the ring of $n \times n$-matrices over R for an integer n. It is well known that $M_n(R)$ is a Hirata extension of R, and an Azumaya R-algebra when R is commutative. In [7], it is shown that if 2 is invertible in R, then $M_2(R)$ is a Galois extension of R with an inner Galois group of order 4 by using the Sugano quaternions ([7, Theorem 4.4]). The purpose of the present paper is to study the Galois extension $M_n(R)$ of R with an inner Galois group G of order n^2 induced by $\{U_i \in M_n(R), i = 1, \ldots, n^2\}$. Equivalent conditions for such a Galois extension $M_n(R)$ of R are given in terms of $\{U_i\}$ and the trace of G.

Throughout the paper, let R be a ring with 1, C the center of R, D a subring of R with the same 1. As given in [1, 3, 5, 7], R is called a separable extension of D if the multiplication map: $R \otimes_D R \longrightarrow R$ splits as an R-bimodule homomorphism. In particular, if $D \subset C$, a separable extension R of D is called a separable D-algebra, and if $D = C$, a separable extension R of D is called an Azumaya C-algebra. If $R \otimes_D R$ is isomorphic to a direct summand of a finite direct sum of R as an R-bimodule, then R is called a Hirata separable extension of D. It is known that an Azumaya algebra is a Hirata separable extension. Let G be a finite automorphism group of R and $R^G = \{r \in R |\ g(r) = r\}$ for each $g \in G$. If there exist elements $\{a_i, b_i$ in R, $i = 1, 2, \ldots, m$ for some integer $m\}$ such that $\sum_{i=1}^{m} a_i g(b_i) = \delta_{1,g}$ for each $g \in G$, then R is called a Galois extension of R^G with Galois group G, and $\{a_i, b_i\}$ is called a G-Galois system for R. A Hirata separable Galois extension R of R^G is a Hirata separable extension and a Galois extension of R^G.

Date: Received: July 27, 2013; Accepted: Sep 15, 2013.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 13B05; Secondary 16S35.

Key words and phrases. Azumaya algebras, Galois extensions, Hirata separable extensions, Matrix rings, Inner automorphism groups.

A projective group ring RG_f of a finite group G over a ring R is a ring with a free basis $\{W_g\}$ for $g \in G$ over R such that $rW_g = W_g r$ for each $r \in R$ and $W_g W_h = W_{gh} f(g,h)$ for $g, h \in G$ where $f : G \times G \longrightarrow Units(C)$ is a factor set. The commutator subring of D in R is denoted by $V_R(D)$, that is, $V_R(D) = \{r \in R |\ rx = xr$ for all $x \in D\}$. It is known that if R is a Galois extension of R^G with Galois group G, then $V_R(R^G) = \oplus \sum_{g \in G} J_g$ where $J_g = \{r \in R |\ rx = g(x)r$ for each $x \in R\}$ ([6, Proposition 1]).

2. Galois Matrix Rings

By keeping the definitions and notations as given in section 2, a Galois matrix ring $M_n(R)$ over R with an inner Galois group of order n^2 induced by $\{U_i \in M_n(R)\}$ is characterized in terms of $\{U_i\}$ and the trace of G, where $G = \{g_i, i = 1, \ldots, n^2, g_i(r) = U_i r U_i^{-1}\}$ for each $r \in R$. Denote J_{g_i} by J_i. We begin with some properties of J_i.

Lemma 2.1. *Let $J_i^C = \{t \in M_n(C) | ty = g_i(y)t\}$ for each $y \in M_n(C)$. Then $J_i^C = J_i$ for each i.*

Proof. Let $r \in J_i$. Then $rx = g_i(x)r$ for each $x \in M_n(R)$. Since the commutator subring $V_{M_n(R)}(R)$ of R in $M_n(R)$ is $M_n(C), rx = xr$ for each $x \in R$ implies $J_i \subset J_i^C$. Similarly, $J_i^C \subset J_i$. Thus $J_i^C = J_i$ for each i.

Next we show equivalent conditions for a Galois matrix ring $M_n(R)$ of R with an inner Galois group G of order n^2 induced by $\{U_i \in M_n(R) | i = 1, \ldots, n^2\}$. □

Theorem 2.2. *By keeping the notations in this section, if $(M_n(R))^G = R$, then the following statements are equivalent:* (1) *$M_n(R)$ is a Galois extension of R with inner Galois group G;* (2) *$M_n(C)$ is a central Galois algebra over C with inner Galois group induced by and isomorphic with G;* (3) *$M_n(R) = \oplus \sum_i RU_i$ as R-modules (that is, $\{U_i, i = 1, \ldots, n^2\}$ are linearly independent over R);* (4) *n is invertible in C and $Tr(U_i) = 0$ for each $i \neq 1$ where g_1 is the identity of G and $Tr(x) = \sum_i g_i(x)$ for $x \in M_n(R)$.*

Proof (1) $\longrightarrow$ (2). Since $M_n(R)$ is a Galois extension of R with Galois group G, the commutator subring of R in $M_n(R), V_{M_n(R)}(R) = \oplus \sum_{i=1}^{n^2} J_i$ where $J_i = J_{g_i}$ ([6, Proposition 1]). On the other hand, $V_{M_n(R)}(R) = M_n(C)$, so $M_n(C) = \oplus \sum_{i=1}^{n^2} J_i$. By *Lemma* 2.1, $J_i = J_i^C$, so $M_n(C) = \oplus \sum_{i=1}^{n^2} J_i^C$. Moreover, it is easy to see that $G | M_n(C) \cong G$ and $(M_n(C))^G = C$. But $M_n(C)$ is also an Azumaya C-algebra, so $M_n(C)$ is a central Galois C-algebra with Galois group induced by and isomorphic with G (. [4, Theorem 1]).

(2) $\longrightarrow$ (3). Since $M_n(C)$ is a central Galois algebra over C with an inner Galois group induced by and isomorphic with $G, M_n(C) = CG_f,$, a projective group algebra of G over C with factor set $f : G \times G \longrightarrow Units\ of\ C$ where $f(g,h) = U_g U_h U_{gh}^{-1}$ for $g, h \in G$ ([1, Theorem 2]). Thus $M_n(C) = CG_f = \oplus \sum_{i=1}^{n^2} CU_i$. But then $M_n(R) \cong R \otimes_C M_n(C) = R \otimes_C (\oplus \sum_i CU_i) \cong \oplus \sum_i R \otimes_C CU_i \cong \oplus \sum_i RU_i$.

(3) $\longrightarrow$ (2). Since $M_n(R) = \oplus\sum_i RU_i, V_{M_n(R)}(R) = V_{\oplus\sum_i RU_i}(R)$. Hence $M_n(C) = \oplus\sum_i CU_i$. Let $f : G \times G \longrightarrow \oplus\sum_i CU_i$ by $f(g,h) = U_gU_hU_{gh}^{-1}$. We claim that $f(g,h)$ is invertible in C for all $g,h \in G$. In fact, for each $x \in \oplus\sum_i CU_i, x(U_gU_hU_{gh}^{-1}) = U_gg^{-1}(x)U_hU_{gh}^{-1} = U_gU_h(h^{-1}g^{-1}(x))U_{gh}^{-1} = U_gU_hU_{gh}^{-1}gh(h^{-1}g^{-1}(x)) = (U_gU_hU_{gh}^{-1})x$, so $(U_gU_hU_{gh}^{-1})$ is in the center of $M_n(C)$. Thus $f(g,h)$ is in C for all $g,h \in G$, and clearly, $f(g,h)$ is invertible in C. Similarly, we can show that $f(g,h)f(gh,k) = f(h,k)f(g,hk)$ for all $g,h,k \in G$. Thus the Azumaya C-algebra $M_n(C)$ is a projective group algebra of G over C. Therefore $M_n(C)$ is a central Galois algebra over C with inner Galois group induced by and isomorphic with G ([1, Theorem 3]).

(2) $\longrightarrow$ (4). Since $M_n(C)$ is a central Galois algebra over C with inner Galois group of order $n^2, M_n(C) = CG_f = \oplus\sum_{i=1}^{n^2} CU_i$ by (3) $\longrightarrow$ (2) and n^2 is invertible in C; and so n is invertible in C. Hence $\{U_i\}$ is a free basis for $M_n(C)$ over C. Noting that $Tr(U_i)$ is in C, we have $Tr(U_i) = \sum_j g_j(U_i) \in C$; that is, $\sum_j U_jU_iU_j^{-1} = \sum_k a_kU_k \in C$ for some units $a_k \in C$ and $g_jg_ig_j^{-1} = g_k \in G$. This implies that $Tr(U_i) = 0$ for each $i \neq 1$.

(4) $\longrightarrow$ (2). It suffices to show that $\{U_i, n^{-2}U_i^{-1} | i = 1, \ldots, n^2\}$ is a G-Galois system for $M_n(C)$. In fact, $\sum_i U_in^{-2}U_i^{-1} = 1$ and $\sum_i U_ig_k(n^{-2}U_i^{-1}) = n^{-2}\sum_i U_i(U_kU_i^{-1}U_k^{-1}) = n^{-2}Tr(U_k)U_k^{-1} = 0$ for each $k \neq 1$. Thus $M_n(C)$ is a central Galois algebra over C with Galois group induced by and isomorphic with G

3. APPLICATIONS

By keeping the notations of section 2, we shall apply *Theorem* 2.2 to obtain equivalent conditions for a Galois central simple algebra and for a Galois Azumaya algebra over a semilocal ring with no idempotents but 0 and 1. An example of a Galois $M_2(R)$ is given to demonstrate the result. We recall the well known Wedderburn theorem for a central simple algebra and the general Wedderburn theorem for an Azumaya algebra over a semilocal ring with idempotents but 0 and 1 due to F.R. DeMeyer in [2].

Proposition 3.1. (1) *Let A be a central simple algebra over C. Then $A = M_n(D)$ where D is a central division C-algebra and n is the dimension of A as a free D-module.* (2) *Let A be an Azumaya algebra over a semilocal ring C with no idempotents but* 0 *and* 1. *Then $A = M_n(E)$ where E is an Azumaya C-algebra such that $E/(ME)$ is a central division algebra over C/M for each maximal ideal M of C and n is the dimension of $A/(MA)$ as a free $E/(EM)$-module.*

Proof. Since A is a central simple algebra over $C, A = M_n(D)$ by the Wedderburn theorem. Moreover, it is well known that G is inner, and $A^G = D$ by hypothesis, so the equivalent conditions as given in *Theorem* 2.2 hold for the Galois extension $M_n(D)$ of D with Galois group G.

□

Theorem 3.2. *Let A be an Azumaya algebra over a semilocal ring C with no idempotents but 0 and 1, and G an automorphism group of A of order n^2 where $A = M_n(E)$ for some integer n and the Azumaya algebra E over C as given by the general Wedderburn theorem* ([2, Corollary 1]). Assume $A^G = E$. Then the equivalent conditions as given in *Theorem* 2.2 hold for a Galois extension A of E with Galois group G.

Proof. Since G is inner ([2]), the equivalent conditions given in *Theorem* 2.2 hold. □

We conclude the present paper with an example to demonstrate *Theorem* 2.2 for $n = 2$. Let R be a ring with 1 and 2 invertible in R. Let $G = \{g_1, g_2, g_3, g_4\}$ be an inner automorphism group of $M_2(R)$ induced respectively by

$$U_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; U_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \; U_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; U_4 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then $M_2(R)$ is a Galois extension of R with inner Galois group G ([7, Theorem 4.4]). Thus the equivalent conditions as given in *Theorem* 2.2 hold.

Acknowledgement.
This paper was done at Sun Yat-sen University, Guangzhou, 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. F.R. DeMeyer, Galois Theory in Separable Algebras over Commutativwe Rings, *Illinois J. Math.,* **10** 1966, 287-295.
2. F.R. DeMeyer, Projective Modules over Central Separable Algebras, *Canad. J. Math.,* **21** 1969, 39-43.
3. F.R. DeMeyer and E. Ingraham, Separable Algebras over Commutative Rings, **181**, Springer Verlag, Berlin, Heidelberg, New York, 1971.
4. M. Harada, Supplementary Results on Galois Extension, *Osaka J. Math.,* **2** 1965, 343-350.
5. S. Ikehata, Note on Azumaya Algebras and H-Separable Extensions, *Math. J. Okayama Univ.,* **23** 1981, 17-18.
6. T. Kanzaki, On Galois Algebra over a Commutative Ring, *Osaka J. Math.,* **2** 1965, 309-317.
7. A. Nelson and G. Szeto, When Is the Ring of 2x2 Matrices over a Ring Galois? *International J. Algebra,* **23** 2013, 17-18.
8. A. Rosenberg and D. Zelinsky, Automorphisms of Separable Algebras, *Pac. J. Math.,* **11** 1961, 1109-1117
9. K. Sugano, On a Special Type of Galois Extensions, *Hokkaido J. Math.,* **9** 1980, 123-128.

[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