PORTUGALIAE MATHEMATICA
Vol. 56 Fasc. 3 – 1999

NOTES ON GALOIS EXTENSIONS WITH INNER GALOIS GROUPS

X.-L. Jiang and G. Szeto

Abstract: Let S be a ring with 1, C the center of S, G a finite inner automorphism group of S of order n for some integer n invertible in S where $G=\{g_1,g_2,...,g_n\}$ and $g_i(s)=U_i\,s\,U_i^{-1}$ for some U_i in S and all s in S, and R the subring of all elements fixed under each element in G. Then, S is a G-Galois extension of R which is an Azumaya C-algebra with a Galois system $\{n^{-1}U_i,\,U_i^{-1}\}$ if and only if S is a projective group ring RG_f for some factor set f which is an H-separable extension of R and R is a separable C-algebra. Moreover, some correspondence relations are given between certain sets of separable subalgebras of such an S.

1 – Introduction

Let S be a ring with 1, G a finite automorphism group of S, $G=\{_1,g_2,...,g_n\}$ for some integer n and R the subring of the elements fixed under each element in G. R. Alfaro and G. Szeto ([1] and [2]) studied the G-Galois extension S of R which is an Azumaya algebra. Let G be an inner automorphism group with $g_i(s)=U_i\,s\,U_i^{-1}$ for some U_i and all s in S and assume n is a unit in S. When R is commutative, F.R. DeMeyer [5] showed that S is a central Galois R-algebra if and only if S is an Azumaya projective group R-algebra, where a projective group algebra RG_f is an R-algebra with a basis $\{U_i\,/\,i=1,...,n\}$, $r\,U_i=U_i\,r$ for all r in R and $U_i\,U_j=f(g_i,g_j)\,U_k$ where $g_i\,g_j=g_k$ and $f\colon\ G\times G\to U(R)$ (the units of R) is a factor set. When R is not commutative, S.L. Jiang [8], D.X. Deng and G. Szeto [6] studied the G-Galois extension of R with Galois system

Received: September 10, 1997; *Revised*: November 18, 1997.
AMS Mathematics Subject Classification: 16S30, 16W20.
Keywords and Phrases: Galois extensions, Projective group rings, Azumaya algebras, H-separable extensions.

$\{n^{-1}U_i,\, U_i^{-1}\}$. The purpose of the present paper is to characterize such an S in terms of H-separable extensions when R is an Azumaya algebra over C where C is the center of S and two correspondence theorems are also shown between certain sets of separable subalgebras of S.

2 – Preliminaries

Throughout, we assume n is a unit in S and keep the notations as given above. A ring extension A over a subring B is called a separable extension if there exist elements $\{a_i, b_i\}$ in A, $i = 1, 2, ..., m$, for some integer m such that $\sum a_i\, b_i = 1$ and $\sum a\, a_i \otimes b_i = \sum a_i \otimes b_i\, a$ for all a in A where $\otimes$ is over B. A separable extension of its center is called an Azumaya algebra. If $A \otimes A$ is isomorphic with a direct summand of a finite direct sum of A as an A-bimodule where $\otimes$ is over B, then A is called an H-separable extension of B. It is known that an H-separable extension is a separable extension and that an Azumaya algebra is an H-separable extension. Let S be a ring with a finite automorphism group G as given above. Then S is called a G-Galois extension of R if there exist elements $\{c_i, d_i\}$ in S, $i = 1, 2, ..., k$, for some integer k such that $R = S^G = \{r \,\mathrm{in}\, S \,/\, g(r) = r$ for all $g \,\mathrm{in}\, G\}$, and $\sum c_i\, g(d_i) = 0$ for each $g \neq 1$ in G and $\sum c_i\, d_i = 1$. We call $\{c_i, d_i\}$ a G-Galois system for S. A projective group ring RG_f is defined in the same way as a projective group algebra of a group G over a ring R. Let B be a subring of a ring A, $V_A(B)$ denotes the commutator subring of B in A.

3 – Characterizations of Galois extensions

In this section, we shall give characterizations of a G-Galois extension S of R with Galois system $\{n^{-1}U_i,\, U_i^{-1}\}$, and of a G-Galois extension S of R which is an Azumaya algebra over the center C of S.

Theorem 3.1. *By keeping the notations of Section 2, the following statements are equivalent:*

(**1**) *S is a G-Galois extension of R with Galois system $\{n^{-1}U_i,\, U_i^{-1}\}$.*

(**2**) *$S = RG_f$.*

(**3**) *$\{U_i\}$ are linearly independent over R.*

(**4**) *$\{g_i\, R_i\}$ are linearly independent in* $\mathrm{Hom}(S, S)$ *over R, where $R_i(s) = sU_i$ for each i and all s in S.*

Proof: $(\mathbf{1})\to(\mathbf{2})$. The proof of $RG_f \subset S$ is given on pp. 289–290 in [5] with G-Galois system $\{n^{-1}U_j, U_j^{-1}\}$. That is, we first claim that $\{U_i\}$ are linearly independent over R. Let $\sum r_i U_i = 0$ for some r_i in R. Then for each g_k in G,

$$\begin{aligned} 0 &= \sum n^{-1} U_j \left(\sum r_i U_i\right) \left(g_k^{-1}(U_j^{-1})\right) \\ &= \sum n^{-1} U_j \left(\sum r_i g_i \left(g_k^{-1}(U_j^{-1})\right) U_i\right) \\ &= \sum r_i \left(\sum n^{-1} U_j \left(g_i g_k^{-1}(U_j^{-1})\right)\right) U_i \\ &= r_k U_k \end{aligned}$$

(for $\{n^{-1}U_j, U_j^{-1}\}$ is a G-Galois system). Thus $r_k = 0$ and so $\{U_i\}$ are linearly independent over R. Next, we define $f\colon G\times G \to U(R)$ by $f(g_i, g_j) = U_i U_j U_k^{-1}$, where $g_i g_j = g_k$. Then it is straightforward to verify that f is a factor set such that $RG_f = \sum R U_i \subset S$. For $S \subset RG_f$, we first claim that RG_f is a G'-Galois extension of R with Galois group G' induced by and isomorphic with G. Clearly, RG_f is invariant under G. Let $g_i = g_j$ acting on RG_f. Then $g_i(U_k) = g_j(U_k)$, $U_i U_k U_i^{-1} = U_j U_k U_j^{-1}$ for all $k = 1, ..., n$. Hence $(U_i^{-1} U_j) U_k = U_k (U_i^{-1} U_j)$. Thus $U_i^{-1} U_j$ is in R, $U_j = U_i t$ for some t in R. But $\{U_i\}$ are R-linearly independent in RG_f, so $i = j$. This implies that $G' \cong G$. Next, since $\{n^{-1}U_i, U_i^{-1}\}$ is a G-Galois system contained in RG_f, RG_f is a G'-Galois extension of R with $G' \cong G$. Moreover, since S is also a G-Galois extension of R, $S = RG_f$.

$(\mathbf{2})\to(\mathbf{1})$. The proof is given by Theorem 3 in [5] to show that $\{n^{-1}U_i, U_i^{-1}\}$ is a G-Galois system for S over R. $(\mathbf{2})\to(\mathbf{3})$ is clear. $(\mathbf{3})\to(\mathbf{1})$ is immediate because that $\{U_i\}$ are linearly independent over R implies that $S = RG_f$. $(\mathbf{4})\to(\mathbf{3})$. Let $\sum r_i U_i = 0$ for some r_i in R. Then $\sum r_i (U_i s U_i^{-1}) U_i = 0$ for all s in S, $\sum r_i g_i(s) U_i = 0$, that is, $\sum r_i g_i(sU_i) = 0$, or, $\sum r_i g_i R_i(s) = 0$. Hence $\sum r_i (g_i R_i) = 0$ in $\mathrm{Hom}(S, S)$. This $r_i = 0$ for each i by (4). $(\mathbf{3})\to(\mathbf{4})$ is immediate by reversing each step of (4)→(3). ∎

Let S be a G-Galois extension of R with Galois system $\{n^{-1}U_i, U_i^{-1}\}$ as given in Theorem 3.1. When S is also an Azumaya algebra over its center C, we shall characterize such an S in terms of H-separable extensions. We note that $C \subset R$ for G is inner.

Theorem 3.2. *The following statements are equivalent:*

($\mathbf{1}$) *$S = RG_f$ and S is an Azumaya C-algebra.*

($\mathbf{2}$) *$S = RG_f$, S is an H-separable extension of R and R is a separable C-algebra.*

(**3**) *S is a G-Galois extension of R with Galois system $\{n^{-1}U_i,\, U_i^{-1}\}$ and R is an Azumaya C-algebra.*

Proof: (**1**)→(**2**). Since RG_f is an Azumaya C-algebra and RG_f is a free R-module of rank n, RG_f is an H-separable extension of R ([7], Theorem 1). Also, noting that R is an R-direct summand of RG_f and that RG_f is separable over C, we have that R is a separable C-algebra ([4], the proof on p. 120).

(**2**)→(**1**). By the transitivity of separable extensions, RG_f is a separable C-algebra. Since $RG_f = S$, RG_f is an Azumaya C-algebra.

(**1**)→(**3**). Let $\Delta = V_S(R)$ the commutator subring of R in S. Then $RG_f = R\,\Delta$ (for $\{U_i\} \subset \Delta$). Since R is an R-direct summand of RG_f and RG_f is a free R-module of rank n, R is a separable C-algebra ([4], the proof on p. 120). Also, $S = RG_f$ so S is a G-Galois extension of R with Galois system $\{n^{-1}U_i,\, U_i^{-1}\}$ by Theorem 3.1. Noting that RG_f is an Azumaya C-algebra by hypothesis, R is an Azumaya C-algebra ([3], Theorem 4.4, p. 58).

(**3**)→(**1**). By the transitivity of separable extensions and Theorem 3.1, $RG_f = S$ and is an Azumaya C-algebra. ∎

Next we derive a structure theorem for the skew group ring of G over RG_f as given in Theorem 3.2.

Theorem 3.3. *Let S with center C be given in Theorem 3.2 and denote the skew group ring of G over S by S^*G. Then $S^*G \cong M_n(R)$, the matrix ring of order n over R.*

Proof: Let $\Delta = V_S(R)$ where $S = RG_f$ by Theorem 3.2. Then $\Delta = \sum CU_i$ by a direct computation. But Δ is a C-algebra, so $U_i\,U_j = f(g_i, g_j)\,U_k$ is in Δ where $g_i\,g_j = g_k$ in G. Hence $f : G \times G \to U(C)$ (= units of C). Thus $S = RG_f \cong R \otimes CG_f$ where CG_f is a projective group algebra over C, where $\otimes$ is over C. Therefore,

$$\begin{aligned} S^*G &\cong \mathrm{Hom}_R(R \otimes CG_f,\, R \otimes CG_f) \\ &\cong R \otimes \mathrm{Hom}_C(CG_f, CG_f) \\ &\cong R \otimes M_n(C) \\ &\cong M_n(R)\,. \;\blacksquare \end{aligned}$$

4 – Correspondences of separable subalgebras

In this section, we shall give two correspondence theorems for an Azumaya projective group ring as given in Theorem 3.2. Let RG_f be an Azumaya algebra over its center C, $\mathcal{C} = \{$separable C-subalgebras of RG_f contained in $R\}$ and $\mathcal{D} = \{$separable C-subalgebras of RG_f containing $CG_f\}$. We shall show that $\mathcal{C}$ and $\mathcal{D}$ are in a one-to-one correspondence. We begin with a lemma for a separable subalgebra of an Azumaya algebra.

Lemma 4.1. *Let A be an Azumaya algebra over its center C and T a separable subalgebra of A. Then*

(**1**) *T and $V_A(T)$ (the commutator subring of T in A) are Azumaya algebras over the same center D,*

(**2**) *$T \cap V_A(T) = D$.*

Proof: (**1**) By the commutant theorem for Azumaya algebras ([3], Theorem 4.3), $V_A(T)$ is a separable subalgebra of A and $V_A(V_A(T)) = T$. Let D be the center of T. Then $D \subset V_A(T)$ and $D \subset T = V_A(V_A(T))$. Hence $D \subset$ the center of $V_A(T)$. Conversely, the center of $V_A(T) \subset V_A(V_A(T)) = T$, so the center of $V_A(T) \subset D$. Thus (1) holds.

(**2**) $D \subset T \cap V_A(T)$ is clear. Conversely, for any d in $T \cap V_A(T)$, d is in T and in $V_A(T)$, so d is in D because $T = V_A(V_A(T))$ again. ∎

Lemma 4.2.

(**1**) *Let B be a separable subalgebra of RG_f containing R. Then $B \cap (CG_f)$ is a separable subalgebra contained in CG_f.*

(**2**) *Let E be a separable subalgebra of RG_f containing CG_f. Then $E \cap R$ is a separable subalgebra contained in R.*

Proof: Let S be RG_f and T be CG_f.

(**1**) Let $A = V_S(B)$. Then A is a separable subalgebra contained in T. Since T is an Azumaya C-algebra, $V_T(A)$ and $V_S(A)$ $(= B)$ are separable subalgebras such that $V_T(A) = B \cap T$. Hence $B \cap T$ is a separable subalgebra contained in T.

Part (2) is similar. ∎

Theorem 4.3. *The map $\alpha\colon \mathcal{C} \to \mathcal{D}$ by $B \to B(CG_f)$ for any B in $\mathcal{C}$ is bijective with the inverse map $\beta\colon A \to A \cap R$ for any A in $\mathcal{D}$.*

Proof: Let S be RG_f and T be CG_f. Since B is a separable subalgebra contained in R and T is an Azumaya subalgebra of the Azumaya algebra S, $\alpha(B) = BT$ is in $\mathcal{D}$. But R is a C-direct summand of S, so $\beta\alpha(B) = BT \cap R = B$. This implies that α is an injection. Next, let E be a separable subalgebra containing T. Then $V_S(E) \subset R$ (for $T \subset E$ and $V_S(T) = R$). Hence $V_S(E) = V_R(E)$. Denote $V_R(E)$ by F. Since E is a separable subalgebra of the Azumaya algebra S, F is also a separable subalgebra contained in R by Lemma 4.1; and so E, F $(= V_S(E))$ and $V_R(F)$ are Azumaya algebras over the same center D by Lemma 4.1 again. $V_R(F) \subset V_S(F) = V_S(V_S(E)) = E$ as Azumaya algebras over D and T is an Azumaya C-algebra contained in E, so $V_R(F)\,T$ is an Azumaya D-subalgebra of E. Thus $E \cong V_R(F)\,T \otimes V_E(V_R(F)\,T)$ by the commutant theorem for Azumaya algebras where $\otimes$ is over D ([3], Theorem 4.3). Noting that $V_R(F) = V_R(V_S(E)) = R \cap V_S(V_S(E)) = R \cap E$ and that $V_E(V_R(F)\,T) = E \cap (V_S(V_R(F)\,T)) = E \cap V_R(V_R(F)) = E \cap F$ (for $V_S(T) = R$), we have that $E \cong (R \cap E)\,T \otimes (E \cap F) \cong (R \cap E)\,(E \cap F)\,T$ by the multiplication map ([3], Theorem 4.3). Since $E \cap F \subset E \cap R$, $E = (E \cap R)\,T$. Since $E \cap R = V_R(F)$ is in $\mathcal{C}$ by Lemma 4.2, α is a surjective with the inverse map β. Therefore $\mathcal{C}$ and $\mathcal{D}$ are in a one-to-one correspondence. ∎

In the following, we want to establish a one-to-one correspondence between the set of separable subalgebras containing R and the set of separable subalgebras contained in CG_f. Let $\mathcal{C}' = \{$separable C-subalgebras of RG_f containing $R\}$ and $\mathcal{D}' = \{$separable C-subalgebras of RG_f contained in $CG_f\}$. Then we have

Theorem 4.4. *Let RG_f be an Azumaya C-algebra as given in Theorem 3.3. Then $\mathcal{C}'$ and $\mathcal{D}'$ are in a one-to-one correspondence under $\alpha\colon B \to B \cap CG_f$ with the inverse map $\beta\colon E \to RE$ for any B in $\mathcal{C}'$ and E in $\mathcal{D}'$.*

Proof: Let S be RG_f and T be CG_f. At first, we note that α is well defined by Lemma 4.2 and $\alpha\beta(E) = RE \cap T = E$ for any E in $\mathcal{C}'$, so β is an injection. Next we claim that $B = R(B \cap T)$ for any B in $\mathcal{C}'$. In fact, since $R \subset B$ is a separable C-subalgebra of S, $V_S(B) \subset T$ is a separable subalgebra with the same center as B by Lemma 4.1. Let the center of B be D and $V_S(B)$ be F. T is an Azumaya C-algebra, so $V_S(F)$ is a separable subalgebra with the same center D as F by Lemma 4.1 again. But R and T are Azumaya C-algebras, so $RV_T(F) \subset R(V_S(F)) = B$ as Azumaya subalgebras over D. Thus $B \cong R(V_T(F)) \otimes V_B(R(V_T(F)))$, where $\otimes$ is over D. Moreover, $V_T(F) = T \cap V_S(F) = T \cap V_S(V_S(B)) = T \cap B$, and $V_B(R(V_T(F))) = T \cap V_B(V_T(F)) = T \cap B \cap V_S(V_T(F)) = B \cap V_T(V_T(F)) = B \cap F = D$ by Lemma 4.1. Thus

$B \cong R(V_T(F)) \otimes D \cong R(V_T(F)) = R(T \cap B)$. Noting that $T \cap B$ is in $\mathcal{D}'$, we conclude that α is surjective. ∎

We close the paper with three examples:

(**1**) S is a G-Galois extension of R such that $S = RG_f$, $C \subset R$, and R is an Azumaya C-algebra,

(**2**) S is a G-Galois extension of R such that $S = RG_f$, $C \subset R$, but R is not an Azumaya C-algebra,

(**3**) S is a G-Galois extension of R but $\{n^{-1}U_i,\, U_i^{-1}\}$ is not a G-Galois system.

Example 1. Let R be a 2 by 2 matrix algebra over the rational field Q, $S = R[i,j,k]$, the quaternion ring over R, and $G = \{1, g_i, g_j, g_k\}$ where $g_i(s) = i\,s\,i^{-1}$, $g_j(s) = j\,s\,j^{-1}$, and $g_k(s) = k\,s\,k^{-1}$ for all s in S. Then

(**1**) $S^G = R$.

(**2**) S is a G-Galois extension of R with a G-Galois system $\{4^{-1}, 4^{-1}i, 4^{-1}j, 4^{-1}k;\ 1, i^{-1}, j^{-1}, k^{-1}\}$. Hence $S = RG_f$.

(**3**) The center C of $S = Q \subset R$.

(**4**) R is an Azumaya C-algebra.

Thus S satisfies the hypotheses of Theorem 3.2.

Example 2. Let R and S be given in Example 1, $G = \{1, g_i\}$. Then

(**1**) $S^G = R[i]$.

(**2**) S is a G-Galois extension of $R[i]$ with a G-Galois system $\{2^{-1}, 2^{-1}i;\ 1, i^{-1}\}$. Hence $S = S^G\, G_f$.

(**3**) The center of $S^G = Q[i] \neq Q = C$, so S^G is not an Azumaya C-algebra.

Thus S satisfies the hypotheses of Theorem 3.1 but not Theorem 3.2.

Example 3. Let S be a 2 by 2 matrix algebra over the rational field Q, $G = \{1, g\}$, $g(s) = U\,s\,U^{-1}$ where $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ for all s in S. Then S is a G-Galois extension of S^G with a G-Galois system, $\left\{\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\right\}$; but $\left\{2^{-1}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, 2^{-1}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix};\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1}\right\}$ is not a G-Galois system. Thus $S \neq S^G\, G_f$ by Theorem 3.1.

ACKNOWLEDGEMENT – This paper was revised under the suggestions of the referee. The author would like to thank him for his suggestions.

REFERENCES

[1] Alfaro, R. and Szeto, G. – Skew group rings which are Azumaya, *Comm. in Algebra,* 23(6) (1995), 2255–2261.

[2] Alfaro, R. and Szeto, G. – On Galois extensions of an Azumaya algebra, *Comm. in Algebra,* 25(6) (1997), 1873–1882.

[3] DeMeyer, F.R. and Ingraham, E. – *Separable Algebras over Commutative Rings*, Vol. 181, Springer Verlag, Berlin, Heidelberg, New York, 1771.

[4] DeMeyer, F.R. – Some notes on the general Galois theory, *Osaka J. Math.,* 2 (1965), 117–127.

[5] DeMeyer, F.R. – Galois theory in separable algebras over commutative rings, *Illinois J. Math.,* 10 (1966), 287–295.

[6] Deng, X.D. and Szeto, G. – On a class of free Galois extensions, *Portugaliae Math.,* 51 (1994), 103–108.

[7] Ikehata, S. – Note on Azumaya algebras and H-separable extensions, *Math. J. Okayama Univ.,* 23 (1981), 17–18.

[8] Jiang, X.L. – A Galois theorem for projective group rings, *Math. J. Ann.,* 17A(6) (1966), 737–744.

[9] Sugano, K. – On a special type of Galois extensions, *Hokkaido Math. J.,* 9 (1980), 23–128.

Xiao-Long Jiang,
Mathematics Department, Zhongshan University,
510275 Guangzhou – P. R. CHINA

and

George Szeto,
Mathematics Department, Bradley University,
Peoria, Illinois, 61625 – U.S.A.