PORTUGALIAE MATHEMATICA
Vol. 51 Fasc. 1 – 1994

ON A CLASS OF FREE GALOIS EXTENSIONS

X.D. Deng and G. Szeto

Abstract: Let RG_f be a projective group algebra over a commutative ring R, where G is a finite group and f is a factor set. If RG_f is a central Galois R-algebra with inner Galois group G' induced by the basis of RG_f, then there exists a one-to-one correspondence between the set of subgroups H' of G' such that RH_f is Galois with a free basis induced by H' and the set of Azumaya subalgebras B over R such that $RG = B(G(B))_f$, where $G(B) = \{\alpha \in G \mid \alpha(b) = b\}$ for any b in B and $B(G(B))_f$ is a projective group ring over B.

1 – Introduction

Let RG_f $(= \sum RU_\alpha,\ \alpha \text{ in } G)$ be a projective group algebra with a free basis $\{U_\alpha \mid \alpha \text{ in } G\}$ over a commutative ring R where G is a finite group and f is a factor set: $G \times G \to U(R)$ which is the set of units of R. In [1] and [2], F.R. DeMeyer proved that RG_f is a central Galois R-algebra if and only if it is an Azumaya R-algebra, where the Galois group G' is inner induced by $\{U_\alpha\}$. If the coefficient ring R is noncommutative, then we call RG_f a projective group ring over R. Let RG_f be a central Galois R-algebra with inner Galois group G'. The purpose of the present paper is to show a fundamental theorem for RG_f. It will be shown that there exists a one-to-one correspondence between the set of subgroups H' of G' such that RG_f is a free Galois extension with basis $\{U_\alpha \mid \alpha \text{ in } H\}$ over $(RG_f)^{H'}$ and the set of Azumaya subalgebras B such that $RG_f = B(G(B))_f$ where $G(B) = \{\alpha \text{ in } G' \mid \alpha(b) = b \text{ for each } b \text{ in } B\}$ and $B(G(B))_f$ is a projective group ring over B where f on a subgroup is the restriction of f on G. In this case, $B = (RG_f)^{G(B)'}$ and $(RG_f)^{H'}$ is also an Azumaya subalgebra.

Received: September 6, 1991; *Revised*: May 22, 1992.
AMS Classification numbers: 16S35, 16W20.
Keywords and Phrases: Projective group rings and algebras, Azumaya algebras, Central Galois algebras, Galois extensions.

2 – Definitions and notations

Throughout, we assume that all rings have an identity 1. A ring A is called a ring extension over a subring B if A and B have the same identity. For the definitions of separable extensions and algebras and Azumaya algebras, we refer to [1], [3] and [8]. Let A be a ring extension over B, G a finite automorphism group of A of order n for some integer n. Then A is called a Galois extension over B with Galois group G if $B = A^G$ $(= \{a \text{ in } A \mid \alpha(a) = a \text{ for each } \alpha \text{ in } G\})$ and there exist $\{a_i, b_i \text{ in } A \mid i = 1, ..., m \text{ for some integer } m\}$ such that $\sum_i a_i \alpha(b_i) = \delta_{1\alpha}$ (the Kronecker δ) for α in G. Such a set $\{a_i, b_i\}$ is called a Galois coordinate system for A. Let R be a ring with center C, $U(C)$ the set of units of C, and G a finite group. Then $f\colon G \to U(C)$ is called a factor set if $f(\alpha\beta,v)\, f(\alpha,\beta) = f(\alpha,\beta v)\, f(\beta,v)$ for all α, β, v in G, and RG_f $(= \sum RU_\alpha$, α in $G)$ is called a projective group ring over R if $\{U_\alpha\}$ are free over R, $rU_\alpha = U_\alpha r$ for each r in R and α in G, and $U_\alpha U_\beta = U_{\alpha\beta}\, f(\alpha,\beta)$ for all α, β in G. RG_f is called a projective group algebra when R is commutative (see [1] and [2]).

3 – Main results

In the following, we assume that A $(= RG_f)$ is a central Galois algebra over a commutative ring R with inner Galois group G', where G is a finite group of order n for some integer n, f is a factor set and G' is the inner automorphism group of A induced by $\{U_\alpha\}$; that is, $\alpha'(a) = U_\alpha\, a U_\alpha^{-1}$ for each a in A and α in G. We recall that RG_f is Galois over R with inner Galois group G' if and only if RG_f is an Azumaya R-algebra ([1], Theorems 1 and 2).

Theorem 1. *Let A $(= RG_f)$ be a central Galois R-algebra with inner Galois group G' and H' a subgroup of G'. Then, A is a free Galois extension with a free basis $\{U_\alpha \mid \alpha \text{ in } H\}$ over $A^{H'}$ with Galois group H' if and only if RH_f $(= \sum RU_\alpha$, α in $H)$ is an Azumaya R-algebra.*

Proof: Let RH_f be an Azumaya R-algebra. Then it is a central Galois R-algebra ([1], Theorem 3). Let $\{a_i, b_i \text{ in } RH_f \mid i = 1, ..., m \text{ for some integer } m\}$ be a Galois coordinate system. Then, for each b in $A^{H'}$ and α in H, $\alpha'(b) = b$, so $U_\alpha\, bU_\alpha^{-1} = b$. Hence $U_\alpha b = bU_\alpha$ for each α in H. Thus $bx = xb$ for each x in RH_f. Now we claim that $\{U_\alpha \mid \alpha \text{ in } H\}$ are free over $A^{H'}$. Let $\sum t_\alpha U_\alpha = 0$ for α in H and t_α in $A^{H'}$. Then for any α in H,

$$0 = \sum_i a_i \Big(\sum t_\alpha U_\alpha\Big)\, \beta'^{-1}(b_i) = \sum_\alpha t_\alpha \Big(\sum_i a_i\, \alpha'\, \beta'^{-1}(b_i)\Big) U_\alpha = t_\beta\, U_\beta \ .$$

Since U_β is a unit, $t_\beta = 0$ for each β in H. Thus $(A^{H'})H_f$ is a projective group ring over $A^{H'}$ in A. Moreover, $(A^{H'})H_f \supset RH_f$, so $(A^{H'})H_f$ is Galois over $A^{H'}$ with inner Galois group H' (for RH_f is Galois over R with inner Galois group H'). But A is also Galois over $A^{H'}$ with inner Galois group H', so $A = (A^{H'})H_f$. This proves the sufficiency. For the necessity, let A be a free Galois extension over $A^{H'}$ with a basis $\{U_\alpha \mid \alpha \text{ in } H\}$. Then $A = (A^{H'})H_f$. Denote $A^{H'}$ by B and let C be the center of B. Then $A = BH_f$, a projective group ring over B. Clearly, $A = BH_f = B \otimes CH_f$. Since A has center R, it is easy to see that $R = C$. Moreover, since A is Azumaya C-algebra, both B and CH_f are Azumaya C-algebras ([3], Chapter 4, Theorem 4.4). Thus RH_f is an Azumaya R-algebra. ∎

By the proof of the necessity of the above theorem, we have

Corollary 2. *By keeping the notations and hypotheses of Theorem 1, if A is a free Galois extension with a basis $\{U_\alpha \mid \alpha \text{ in } H\}$ over $A^{H'}$ with Galois group H', then $A^{H'}$ is an Azumaya R-algebra such that $A = (A^{H'})H_f$.* ∎

Next, we want to show the converse. Let B be an Azumaya subalgebra of A, $G(B) = \{\alpha \text{ in } G \mid \alpha'(b) = b \text{ for each } b \text{ in } B\}$. Then $B(G(B))$ $(= \sum BU_\alpha$, α in $G(B))$ is a subalgebra of A such that $bU_\alpha = U_\alpha b$ for each α in $G(B)$ and b in B.

Theorem 3. *Let B be an Azumaya subalgebra of A. Then, $B(G(B))$ is an Azumaya R-algebra if and only if $R(G(B))_f$ is Galois over R with inner Galois group $(G(B))'$.*

Proof: Let $R(G(B))_f$ be Galois over R with inner Galois group $(G(B))'$. Then it is an Azumaya R-algebra. Since $bU_\alpha = U_\alpha b$ for each b in B and α in $G(B)$, $\{U_\alpha \mid \alpha \text{ in } G(B)\}$ are free over B as proved in Theorem 1. Hence $B(G(B)) = B(G(B))_f$, a projective group ring over B. Since $B(G(B))_f = B \otimes R(G(B))_f$, $B(G(B))_f$ is an Azumaya R-algebra (for B and $R(G(B))_f$ are so) ([3], Chapter 2, Proposition 3.3). Conversely, let $B(G(B))$ be an Azumaya R-algebra. Since $bU_\alpha = U_\alpha b$ for each b in B and α in $G(B)$, the center of $R(G(B))_f$ is contained in R. Hence the center of $R(G(B))_f$ is R. On the other hand, A $(= RG_f)$ is a separable R-algebra if and only if the order of G is a unit ([1], Lemma 1). Hence the order of $G(B)$ is a unit. Thus $R(G(B))_f$ is a separable R-algebra. But then $R(G(B))_f$ is Galois over R with inner Galois group $(G(B))'$. ∎

We note that the Azumaya subalgebra $B(G(B))_f$ in the above theorem may not be A. We are going to show that there exists a bigger Azumaya subalgebra $D \supset B$ such that $A = D(G(B))_f$ and $G(D) = G(B)$.

Theorem 4. *Let A and B be given as in Theorem 3 such that $B(G(B))$ is an Azumaya subalgebra of A. Then there exists a unique Azumaya subalgebra D containing B such that $A = D(G(B))_f$ and $G(D) = G(B)$.*

Proof: By Theorem 3, $B(G(B)) = B(G(B))_f$, a projective group ring over B. Since B and $B(G(B))_f$ are Azumaya subalgebras of A, there exists an Azumaya subalgebra D' of A such that $A \cong B(G(B))_f \otimes D' \cong B \otimes R(G(B))_f \otimes D'$ as Azumaya R-algebras ([3], Chapter 2, Theorem 4.3). Let $D = B \otimes D'$. Then $A \cong D \otimes R(G(B))_f$ where D and $R(G(B))_f$ are commutant Azumaya subalgebras in A. Hence, by $A(G(B))'$ Theorem 3, $A \cong D \otimes R(G(D))_f$; and so $R(G(D))_f = R(G(B))_f$ ([3], Chapter 2, Theorem 4.3). Thus $G(D) = G(B)$. Also, by Theorem 1, $A \cong A^{(G(D))'} \otimes R(G(D))_f$, so $D = A^{(G(D))'} = A^{(G(B))'}$ by the commutant theorem again. Thus $A = D(G(B))_f$. Moreover, let D'' be another subalgebra of A such that $A = D''(G(B))_f$; then clearly $D'' = D$. ∎

By Theorems 2 and 4, we have a one-to-one correspondence theorem for central Galois algebras with an inner Galois group.

Theorem 5. *Let A $(= RG_f)$ be a central Galois R-algebra with inner Galois group G'. Then there exists a one-to-one correspondence between the set S of subgroups H' of G' such that A is a free Galois extension of $A^{H'}$ with a basis $\{U_\alpha \mid \alpha \text{ in } H\}$ and the set T of Azumaya subalgebras B of A such that $A = B(G(B))_f$.*

Proof: For a subgroup H' of G' in S, A is a free Galois extension of $A^{H'}$ with a basis $\{U_\alpha \mid \alpha \text{ in } H\}$, so Theorem 1 implies that $A^{H'}$ is an Azumaya subalgebra of A such that $A = A^{H'}H_f$. Then $A^{H'}$ is in T. Then the map $\phi\colon H' \to A^{H'}$ is defined. On the other hand, let B be an Azumaya subalgebra of A in T. Then $A = B(G(B))_f$. Hence, by Theorem 1, $B = A^{G(B)'}$. Thus $(G(B))'$ is a subgroup of G' such that A is a free Galois extension over B $(= A^{G(B)'})$ with a basis $\{U_\alpha \mid \alpha \text{ in } G(B)\}$. This implies that $(G(B))'$ is in S; and so the map $\psi\colon B \to (G(B))'$ is defined. Moreover, since $A = A^{H'}H_f = A^{H'}(G(A^{H'}))_f$, $H = G(A^{H'})$. Thus $H' = (G(A^{H'}))' = \psi\phi(H')$; and so $\psi\phi = 1$. Also, $A = B(G(B))_f = A^{(G(B))'}(G(B))_f$, so $B = A^{(G(B))'} = \phi\psi(B)$. Thus $\phi\psi = 1$. Therefore the correspondence is one-to-one. ∎

We note that there exist subgroups H' of G' not belonging to the correspondence as given in Theorem 5. For example, the ordinary real quaternion algebra RG_f where $G = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8 and R is the real field. Then RG_f is an Azumaya R-algebra but $R\langle i\rangle_f$, $R\langle j\rangle_f$ and $R\langle k\rangle_f$ are not Azumaya algebras over R. Thus the subgroups $\langle i\rangle'$, $\langle j\rangle'$ and $\langle k\rangle'$ do not belong to the correspondence. We conclude the paper with a theorem suggested by the referee. The theorem identifies which subgroups of G' belong to the correspondence as given in Theorem 5.

Theorem 6. *Let G be a finite Abelian group of exponent m, and assume R contains no more than m distinct m^{th} roots of 1. If RG_f and RH_f are R-Azumaya algebras for a subgroup H of G, then there exists a subgroup K of G such that $G = H \times K$ where RK_f is an Azumaya R-algebra and the commutator subalgebra of RH_f in RG_f.*

Proof: From the proof of Theorem 4 in [1] (p. 292), the map $\psi\colon G \times G \to U(R)$ by $\psi(\alpha,\beta) = f(\alpha,\beta)(f(\beta,\alpha))^{-1}$ is a nonsingular skew pairing because RG_f is an Azumaya R-algebra. Also, since R contains no more than m distinct m^{th} roots of 1 by hypothesis, the map $\alpha \to \psi(\alpha,\_)$ for α in G is an isomorphism from G to $\mathrm{Hom}(G,U(R))$. Similarly, since RH_f is an Azumaya R-algebra, the map $\alpha \to \psi(\alpha,\_)$ for α in H is an isomorphism from H to $\mathrm{Hom}(H,U(R))$. Moreover, the map $\alpha \to \psi(\alpha,\_)$ for any α in G defines a homomorphism from G onto $\mathrm{Hom}(H,U(R))$ with kernel K. We then have that $G/K \cong \mathrm{Hom}(H,U(R))$ where $K = \{\alpha \text{ in } G \,|\, \psi(\alpha,\beta) = 1 \text{ for any } \beta \text{ in } H\}$. Next, we claim that $K \cap H = \{e\}$, the identity of G, and $G = HK$. In fact, let α be an element in $H \cap K$. Then $\psi(\alpha,\beta) = 1$ for any β in H. Hence $f(\alpha,\beta) = f(\beta,\alpha)$ for any β in H; and so U_α is in the center of RH_f. Thus $\alpha = e$ (for RH_f has center R). Noting that $\mathrm{Hom}(H,U(R)) \cong H$, we conclude that $G = KH$. But then $G = H \times K$. Therefore, $RG_f \cong RH_f \otimes RK_f$ as Azumaya R-algebras where RK_f is an Azumaya R-algebra and the commutator subalgebra of RH_f in RG_f as noted in [1] (p. 203). ∎

ACKNOWLEDGEMENTS – This work was done while the second author held an Amoco fellowship at Bradley University and visited Zhongshan University, P.R. China and Okayama University, Japan. The author would like to thank Professors S. Ikehata and A. Nakajima for their helpful discussions. Also this paper was revised under the suggestions of the referee. The authors would like to thank the referee for his valuable suggestions.

REFERENCES

[1] DeMeyer, F.R. – Galois theory in separable algebras over commutative rings, *Illinois J. Math.*, 2 (1966), 287–295.

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

[3] DeMeyer, F.R. and Ingraham, E. – *Separable algebras over commutative rings*, Lecture Notes Math., 181, Berlin, Heidelberg, New York, Springer, 1971.

[4] DeMeyer, F.R. and Janusz, G.J. – Group rings which are Azumaya algebras, *Trans. Amer. Math. Soc.*, 279 (1983), 389–395.

[**5**] Deng, X.D. and Szeto, G. – *On projective group rings*, to appear.

[**6**] Kreimer, H.F. and Cook, P.M. – Galois theory and normal bases, *J. Algebra*, 43 (1976), 115–121.

[**7**] Szeto, G. – A characterization of a cyclic Galois extension of commutative rings, *J. Pure and Applied Alg.*, 16 (1980), 315–322.

[**8**] Szeto, G. – On separable abelian extensions of rings, *Internat. J. Math. and Math. Sci.*, 4 (1982), 779–784.

X.D. Deng,
Mathematics Department, Zhongshan University,
Guangzhou – PEOPLE'S REPUBLIC OF CHINA

and

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