J. Austral. Math. Soc. (*Series A*) 32 (1982), 165–170

ON SEPARABLE CYCLIC EXTENSIONS OF RINGS

GEORGE SZETO and YUEN-FAT WONG

(Received 27 November 1980; revised 19 February 1981)

Communicated by R. Lidl

Abstract

The quaternion algebra of degree 2 over a commutative ring as defined by S. Parimala and R. Sridharan is generalized to a separable cyclic extension $B[j]$ of degree n over a noncommutative ring B. A characterization of such an extension is given, and a relation between Azumaya algebras and Galois extensions for $B[j]$ is also obtained.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 16 A 16.

1. Introduction

Parimala and Sridharan (1977) studied a quaternion algebra $B[j]$ (a free ring extension of degree 2) over a commutative ring B with 1, where $j^2 = -1$, $\rho(a)j = ja$ for each a in B and ρ is an automorphism of B of order 2. One of the present authors (Szeto (1980)) generalized such a ring extension $B[j]$ from degree 2 to a cyclic extension of any degree n, and from a commutative ring B to a noncommutative ring B (Szeto and Wong (to appear)). It was shown that if B is a commutative Galois extension over A, the subring of B consisting of all elements fixed by ρ, then $B[j]$ is an Azumaya A-algebra (Szeto (1980), Theorem 3.2 and Lemma 3.4). In the present paper, for $B[j]$ over a not necessarily commutative ring B, we shall give a necessary and sufficient condition for the separability of $B[j]$ of degree n over B in terms of the elements of B, and generalize the above result to a noncommutative Galois extension B over A.

2. Preliminaries

Throughout, we assume that B is a ring with 1, ρ an automorphism of B of order n, $A(= B^{\rho})$, the subring of B consisting of all elements fixed by ρ, and $B[j]$ a free ring extension of B with basis $\{1, j, \ldots, j^{n-1}\}$ such that (1) $j^n = b$ for some unit b in A, and (2) $ja = \rho(a)j$ for each a in B. Now we recall some basic definitions as given by Auslander and Goldman (1960). Let T be a ring extension of a subring S with 1. Then T is called a separable extension over S if there exist elements u_i, v_i in T, $i = 1, \ldots, m$, for some integer m, such that $\sum u_i v_i = 1$, and for all a in T, $a(\sum u_i \otimes v_i) = (\sum u_i \otimes v_i)a$ in $T \otimes_S T$. Such an element $\sum u_i \otimes v_i$ is called a separable idempotent for T. If S is in the center of T, the separable extension T is called a separable S-algebra. Moreover, the separable S-algebra is called an Azumaya S-algebra if S is the center of T.

Let G be a finite automorphism group of a ring T and S the subring of the fixed elements under each element in $G(= T^G)$. Then T is called a Galois extension of S with Galois group G if there exist elements, u_i, v_i in T, $i = 1, \ldots, m$, for some integer m, such that $\sum u_i v_i = 1$ and $\sum u_i \sigma(v_i) = 0$ for each non-identity σ in G.

3. Separable extensions

In this section, we shall characterize the separability of $B[j]$ over B by describing the full set of separable idempotents for $B[j]$. We denote the set $\{c \text{ in } B: ac = c\rho^k(a) \text{ for each } a \text{ in } B\}$ by $B(\rho^k)$, for each $k = 1, \ldots, n-1$.

THEOREM 3.1. *The cyclic extension $B[j]$ is separable over B if and only if there exist a system of elements b_{pq} in B for $p, q = 0, 1, \ldots, n-1$ such that*

(1) $\rho(b_{pq}) = b_{p+1,q-1}$ *for* $p = 0, \ldots, n-2$ *and* $q = 1, \ldots, n-1$;
$b\rho(b_{n-1,q}) = b_{0,q-1}$ *for* $q > 0$;
$\rho(b_{p0}) = bb_{p+1,n-1}$ *for* $p < n-1$;
$\rho(b_{n-1,0}) = b_{0,n-1}$;

(2) b_{pq} *is in* $B(\rho^{p+q})$;

(3) $\Sigma\{b_{pq}: p + q = k \text{ and } 0 < k < n\} = -b\Sigma\{b_{pq}: p + q = k (\mathrm{mod}\, n) \text{ and } k > n\}$;
$b_{00} + b\Sigma\{b_{pq}: p + q = n\} = 1$.

PROOF. Let $B[j]$ be a separable extension over B with a separable idempotent $u = \Sigma\{b_{pq}(j^p \otimes j^q): p, q = 0, \ldots, n-1\}$. Then we have that (a) $ju = uj$, (b) $cu = uc$ for each c in B, and (c) $\Sigma\{b_{pq}j^{p+q}: p, q = 0, \ldots, n-1\} = 1$ b the

https://doi.org/10.1017/S1446788700024514 Published online by Cambridge University Press

definition of a separable idempotent for $B[j]$. Equation (a) implies that $\sum \rho(b_{pq})(j^{p+1} \otimes j^q) = \sum b_{pq}(j^p \otimes j^{q+1})$. Noting that $\{j^p \otimes j^q : p, q = 0, \ldots, n-1\}$ is a basis for $B[j] \otimes_B B[j]$, we have condition (1). Equation (b) gives $\sum cb_{pq}(j^p \otimes j^q) = \sum b_{pq}\rho^{p+q}(c)(j^p \otimes j^q)$, so $cb_{pq} = b_{pq}\rho^{p+q}(c)$ for each c in B. Hence b_{pq} is in $B(\rho^{p+q})$. In equation (c), since $j^n = b$, $(\sum_{p+q=k,k<n} b_{pq} + \sum_{p+q=k(\mathrm{mod}\ n),k>n} b_{pq}b)j^{p+q} = 1$ for $k = 0, \ldots, n-1$. Hence,

$$\sum_{0<p+q=k<n} b_{pq} = (-b)\left(\sum_{\substack{p+q=k(\mathrm{mod}\ n)\\ k>n}} b_{pq}\right) \quad \text{and} \quad b_{00} + b\left(\sum_{p+q=n} b_{pq}\right) = 1.$$

Conversely, equations (1), (2) and (3) imply (a), (b) and (c) by direct verifications. Thus $B[j]$ is separable over B.

By using conditions (1), (2) and (3) in Theorem 3.1, the set $\{b_{pq} : q \neq 0\}$ is determined by the set $\{b_{p0}\}$. Thus a system with less than n^2 elements b_{pq} can be made to determine a separable idempotent.

THEOREM 3.2. *The cyclic extension $B[j]$ over B is separable if and only if there exists a system of elements $\{b_{p0}$ in $B : p = 0, \ldots, n-1\}$ such that*

(1)′ *b_{p0} is in $B(\rho^p)$ for each p, and*

(2)′ $\sum_{p+q=k<n} \rho^{-q}(b_{p+q,0}) = -\sum_{p+q=k(\mathrm{mod}\ n),p+q>n} \rho^{-q}(b_{p+q-n,0})$ *for each k.*

PROOF. By Theorem 3.1, it suffices to show that conditions (1)′ and (2)′ are equivalent to (1), (2) and (3). First, let (1), (2) and (3) be true. Condition (1) implies that $b_{pq} = \rho^{-1}(b_{p+1,q-1}) = \rho^{-2}(b_{p+2,q-2}) = \cdots = \rho^{-q}(b_{p+q,0})$, where $p + q < n$. Also, for $p + q \geqslant n$, since $b\rho(b_{n-1,q}) = b_{0,q-1}$ and $\rho(b_{pq}) = b_{p+1,q-1}$ for $p = 0, \ldots, n-2$ by condition (1), $b_{pq} = \rho^{-(n-1-p)}(b_{n-1,q-(n-1-p)}) = b^{-1}\rho^{-n+p}(b_{0,q+p-n}) = b^{-1}\rho^{-n+p-q-p+n}(b_{q+p-n,0}) = b^{-1}\rho^{-q}(b_{p+q-n,0})$. Thus condition (3) becomes condition (2)′. Clearly, condition (2) implies condition (1)′.

Conversely, noting ρ is an automorphism of B, we can define $\{b_{pq} : p, q = 0, \ldots, n-1\}$ in terms of $\{b_{k0} : k = 0, \ldots, n-1\}$ such that $\rho(b_{pq}) = b_{p+1,q-1}$, for $p = 0, \ldots, n-2$ and $q = 1, \ldots, n-1$, $\rho(b_{n-1,0}) = b_{0,n-1}$, $b\rho(b_{n-1,q}) = b_{0,q-1}$, $\rho(b_{p0}) = bb_{p+1,n-1}$. Thus condition (1) holds. Next, let $p + q < n$. For any c in B, we have an element c' in B such that $c = \rho^{-q}(c')$. Hence $cb_{pq} = c\rho^{-q}(b_{p+q,0}) = \rho^{-q}(c')\rho^{-q}(b_{p+q,0}) = \rho^{-q}(c'b_{p+q,0}) = \rho^{-q}(b_{p+q,0})\rho^{p+q}(\rho^{-q}(c')) = b_{pq}\rho^{p+q}(c)$ by condition (1)′. Let $p + q \geqslant n$. For any c in B, we have $cb_{pq} = cb^{-1}\rho^{-q}(b_{p+q-n,0}) = \rho^{-q}(c')b^{-1}\rho^{-q}(b_{p+q-n,0}) = b^{-1}\rho^{-q}((b_{p+q-n,0})\rho^{p+q-n}(c')) = b^{-1}\rho^{-q}(b_{p+q-n,0})\rho^{p+q-n}(c) = b_{pq}\rho^{p+q}(c)$. Thus b_{pq} is in $B(\rho^{p+q})$. This proves condition (2). Condition (2)′ implies condition (3) by substituting the above b_{pq} defined by the b_{k0} in (2)′. Therefore, $\sum b_{pq}(j^p \otimes j^q)$ is a separable idempotent for $B[j]$.

It is interesting to note the location of the coefficients b_{pq} of a separable idempotent in a Cartesian plane: Let b_{pq} be located at the point (p, q) of a Cartesian plane, for $p, q = 0, \ldots, n-1$. Then join straight lines L_{pp} from $(0, p)$ to $(p, 0)$, L_p^p from $(p, n-1)$ to $(n-1, p)$ for $p = 0, \ldots, n-1$, and L_p^{p+1} from $(n-1, p+1)$ to $(0, p)$ for $p = 0, \ldots, n-2$. Then these directed lines L_{pp}, L_p^p and L_p^{p+1} indicate that $\rho(b_{pq}) = b_{p+1,q-1}$ for $p = 0, \ldots, n-2$ and $q = 1, \ldots, n-1$, $b\rho(b_{n-1,q}) = b_{0,q-1}$ for $q = 1, \ldots, n-1$, and $\rho(b_{p0}) = bb_{p+1,n-1}$ for $p = 0, \ldots, n-2$, respectively. Condition (3) in Theorem 3.1 means that the sum of elements b_{pq} along L_{pp} below the main diagonal $L_{n-1,n-1}$ for $p < n-1$ is equal to the product of $(-b)$ and the sum of elements b_{pq} along L_p^p above $L_{n-1,n-1}$. Moreover, condition (2) of Theorem 3.1 corresponds to the fact that b_{pq} is located at the point (p, q). Theorem 3.2 means that elements at the points $(p, 0)$ for $p = 0, \ldots, n-1$ are sufficient to determine a separable idempotent.

Next we have a necessary and sufficient condition for a separable extension $B[j]$ to be Azumaya over A. In $B[j]$, we denote the subalgebra generated by $\{a - \rho^i(a)\colon a \text{ in } B\}$ by A_i, $i = 1, \ldots, n-1$.

THEOREM 3.4. *Assume that B is separable over A and that n and b are units in A. Then $B[j]$ is an Azumaya A-algebra if and only if A_i is a faithful A-algebra for each i.*

PROOF. Since n and b are units in A, it is straightforward to verify that $(nb)^{-1}\sum_{p=1}^{n} j^p \otimes j^{n-p}$ is a separable idempotent for $B[j]$ over B. Hence $B[j]$ is a separable extension over B. But B is separable over A, so $B[j]$ is separable over A. Then, it suffices to show that the center of $B[j]$ is A if and only if A_i is a faithful A-algebra for each $i = 1, \ldots, n-1$. In fact, let $u = \sum a_i j^i$ be an element in the center. Then $ju = uj$, which implies that $\rho(a_i) = a_i$ for each i. Hence the a_i are in A. Moreover, since $cu = uc$ for each c in B, $a_i(c - \rho^i(c)) = 0$. By hypothesis, A_i is faithful over A, so $a_i = 0$. Thus $u = a_0$ in A. Since A is contained in the center by hypothesis, A is the center of $B[j]$.

Conversely, assume to the contrary that A_i is not faithful over A for some i. Then there exists an a_i in A such that $a_iA_i = 0$. Thus one can check that a_ij^i is in the center. This contradicts the fact that $B[j]$ is Azumaya over A. Therefore, A_i is faithful over A for each i.

In Szeto (1980), it was shown that if B is a commutative Galois extension over A with Galois group G of order n, then $B[j]$ is an Azumaya A-algebra. Now we want to generalize the above theorem to noncommutative Galois extensions. As for commutative Galois extensions (DeMeyer and Ingraham (1971), Proposition 1.2, 80), we have for the non-commutative case.

LEMMA 3.5. *If B is a Galois extension over a subring B' with Galois group G, then the left ideal generated by $\{a - \alpha(a)$: a in B and $\alpha \neq 1$ in $G\}$ is B.*

PROOF. Since B is Galois over B', there exist a_i, b_i in B, $i = 1, \ldots, k$ for some integer k, such that $\sum a_i b_i = 1$ and $\sum a_i \alpha(b_i) = 0$ for each $\alpha \neq 1$ in G. Hence $\sum a_i(b_i - \alpha(b_i)) = 1$. Thus the lemma is proved.

THEOREM 3.6. *Let B be a K-algebra and $B[j]$ a cyclic extension over B of degree n such that b and n are units in K. If B is a Galois extension over a subring B' with Galois group $G(= \{\rho\})$ of order n and if B' is Azumaya over K, then $B[j]$ is Azumaya over K.*

PROOF. Since B is Galois over B', it is a separable extension over B' by the proof of Theorem 1 in DeMeyer (1966). Also since B' is separable over K, $B[j]$ is separable over K by the transitivity property of separable extensions. Thus it suffices to show that the center of $B[j]$ is K. Let $x(= \sum a_i j^i)$ be in the center of $B[j]$. Then $jx = xj$. This implies that $\rho(a_i) = a_i$ for each $i \neq 0$. Hence the a_i are in B' for each $i \neq 0$. Moreover, $dx = xd$ for each d in B. This implies that $da_i = a_i \rho^i(d)$. In particular, this holds for each d in B', so $da_i = a_i d$. Thus the a_i are in the center of B' for each $i \neq 0$. That is, the a_i are in K. But then $a_i(d - \rho^i(d)) = 0$ for each d in B. By hypothesis, B is Galois over B', so $a_i = 0$ for each $i \neq 0$ by Lemma 3.5. thus $a = a_0$. Again, $a_0 d = da_0$ for all d in B, so a_0 is in K. On the other hand, K is contained in the center, so $B[j]$ is Azumaya over K.

In Theorem 3.6, if B is commutative, $B' = K$. Thus $B[j]$ is an Azumaya K-algebra. So, Theorem 3.6 generalizes the commutative case.

References

M. Auslander and O. Goldman (1960), 'The Brauer group of a commutative ring,' *Trans. Amer. Math. Soc.* **97**, 367–409.

S. U. Chase, D. K. Harrison and A. Rosenberg (1965), 'Galois theory and Galois cohomology of commutative rings,' *Mem. Amer. Math. Soc.* Soc. **52**.

Frank DeMeyer (1966), 'Galois theory in separable algebras over commutative rings,' *Illinois J. Math.* **2**, 287–295.

Frank DeMeyer and Edward Ingraham (1971), *Separable algebras over commutative rings*, Lecture notes in Mathematics 181 (Springer-Verlag, Berlin-Heidelberg-New York).

S. Parimala and R. Sridharan (1977), 'Projective modules over quaternion algebras,' *J. Pure Appl. Algebra*, **9**, 181–193.

G. Szeto (1980), 'A characterization of a cyclic Galois extensions of commutative rings,' *J. Pure Appl. Algebra*, **16**, 315–322.

G. Szeto and Y. F. Wong (to appear), 'On free quadratic extensions of rings'.

Department of Mathematics
Bradley University
Peoria, Illinois 61625
U.S.A.

Department of Mathematics
DePaul University
Chicago, Illinois 60637
U.S.A.