J. Austral. Math. Soc. (Series A) **34** (1983), 394–398

ON SEPARABLE NONCYCLIC EXTENSIONS OF RINGS

GEORGE SZETO and YUEN-FAT WONG

(Received 17 January 1982; revised 23 July 1982)

Communicated by R. Lidl

Abstract

The separable cyclic extension of rings is generalized to a separable noncyclic extension of rings: a crossed product with a factor set over a ring (not necessarily commutative). A representation of separable idempotents for a separable crossed product is obtained, and simplifications for some special factor sets are also given.

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

1. Introduction

Let R be a ring with 1 (not necessarily commutative), ρ an automorphism of order n of R for some integer n. The separability of the cyclic extension $R[i, \rho]$, has been intensively investigated (Parimula and Sridharan (1977), Nagahara and Kishimoto (1978), Szeto (1980), Szeto and Wong (1982)), where $ri = i(r)\rho$ for each r in R, $\{1, i, i^2, \ldots, i^{n-1}\}$ is a free basis of $R[i, \rho]$ over R, $i^n = b$ which is a unit in the center C of R and $(b)\rho = b$. The purpose of the present paper is to continue the above investigation to a noncyclic extension: a crossed product $\Delta(R, G)$, where G is a finite automorphism group (not necessarily cyclic) with factor set f: $G \times G \to U(C)$, the set of units of the center C of R. Our study includes cyclic extensions, crossed products over a commutative ring (DeMeyer and Ingraham (1971), Chapter 3), and crossed products with trivial factor set (Kanzaki (1964), Section 3).

https://doi.org/10.1017/S1446788700023818 Published online by Cambridge University Press

2. Preliminaries

Let R be a ring with 1, C the center of R, G $(= \{g_1, g_2, \ldots, g_n\colon g_1 =$ the identity of G for some integer $n\})$ an automorphism group of R, and $R^G = \{r$ in R such that $(r)g_i = r$ for each g_i in $G\}$. A *crossed product* $\Delta(R, G)$ with factor set $f\colon G \times G \to U(C)$, the set of units of C, is a free ring with a basis $\{U_i\colon i = 1, \ldots, n\}$ over R such that $rU_i = U_i((r)g_i)$ for each r in R, and $U_iU_j = U_k f(g_i, g_j)$, where $g_ig_j = g_k$ and $f(g_ig_j, g_m)(f(g_i, g_j))g_m = f(g_i, g_jg_m)f(g_j, g_m)$ for all g_i, g_j, g_m in G. We note that $\Delta(R, G)$ is associative if and only if the above equation holds. Let S be a subring with 1 of R. Then R is called a *separable extension* of S if there exist elements $\{a_i, b_i$ in R such that $i = 1, \ldots, m$ for some integer $m\}$, such that $t(\sum a_i \otimes b_i) = (\sum a_i \otimes b_i)t$ for each t in R and $\sum a_ib_i = 1$ where $\otimes$ is over S (Szeto and Wong (1982)). Such an element $\sum a_i \otimes b_i$ is called a *separable idempotent* for R over S. A ring R with 1 and with a finite automorphism group G is called a *Galois extension* over R^G if there exist elements $\{a_i, b_i$ in R: $i = 1, \ldots, m$ for some integer $m\}$ such that $\sum a_ib_i = 1$ and $\sum a_i((b_i)g_j) = 0$ whenever $g_j \neq g_1$ (DeMeyer (1965), (1966)). Since $(C)g_i = C$ for each i, G induces an automorphism group of C. The Kanzaki hypothesis (Kanzaki (1964), page 110) on R means that R is an Azumaya C-algebra (central separable) and C is Galois over C^G with Galois group induced by and isomorphic with G. Throughout, we assume that R is a ring with 1 and G an automorphism group of R.

3. Separability of crossed products

Under the Kanzaki hypothesis on R, we shall show a necessary and sufficient condition for $\Delta(R, G)$ being a separable extension over R. It is easy to see that $\Delta(R, G)$ has an identity U_1a^{-1} so that R is embedded in $\Delta(R, G)$, where $a = f(g_1, g_1)$. We begin with a representation of a separable idempotent for a separable crossed product $\Delta(R, G)$ over R.

THEOREM 1. *Under the Kanzaki hypothesis on R, the element x $(= \sum U_i \otimes U_jb_{ij}\colon i, j = 1, \ldots, n$ and b_{ij} are in $R)$ is a separable idempotent for $\Delta(R, G)$ if and only if*

(1) *$b_{ij} = 0$ whenever $g_j \neq g_i^{-1}$, and b_{ij} are in C,*

(2) *$b_{11'} = ((f(g_k, g_1))^{-1}g_1^{-1})f(g_i^{-1}, g_k)(b_{ii'}g_k)$, where $g_{1'} = g_1^{-1}$, $g_{i'} = g_i^{-1}$, and $g_i = g_kg_1$, and*

(3) *$a \cdot \sum_1 f(g_1, g_1^{-1})((f(g_k, g_1))^{-1}g_1^{-1})f(g_i^{-1}, g_k)(b_{ii'}g_k) = 1$, where $a = f(g_1, g_1)$ and $g_i = g_kg_1$.*

PROOF. Let x be a separable idempotent for $\Delta(R, G)$ over R. Since $bx = xb$ for each b in R, $\Sigma_{i,j} b(U_i \otimes b_j)b_{ij} = \Sigma_{i,j}(U_i \otimes U_j)b_{ij}b$. Hence $\Sigma_{i,j}(U_i \otimes U_j)(bg_ig_j)b_{ij} = \Sigma_{i,j}(U_i \otimes U_j)b_{ij}b$. In particular, taking b in C, we have that $(bg_ig_j)b_{ij} = b_{ij}b$, so $b_{ij}(b - (bg_ig_j)) = 0$. Hence b_{ij} is in the annihilator ideal I of the ideal J generated by $\{b - (bg_ig_j)$: b in $C\}$. By hypothesis, R is Azumaya over C, so $I = I_0R$ (DeMeyer and Ingraham (1971), Corollary 3.7, page 54) where $I_0 = I \cap C$. Noting that I_0 is the annihilator ideal of J in C, we have that $I_0 = \{0\}$ (DeMeyer and Ingraham (1971), Proposition 1.2, page 81) because C is Galois over C^G with Galois group induced by and isomorphic with G. This implies that $b_{ij} = 0$ whenever $g_j \neq g_i^{-1}$. Let $i' = j$ in case $g_j = g_i^{-1}$. Then $x = \Sigma_i(U_i \otimes U_{i'})b_{ii'}$. Thus we can write b_i for $b_{ii'}$ so that $x = \Sigma_i(U_i \otimes U_{i'})b_i$. Again, from the equation $bx = xb$ for each b in R, b_i are in C. Moreover, for each U_k, $U_kx = xU_k$, so $\Sigma_1(U_kU_1 \otimes U_{1'})b_1 = \Sigma_i U_i \otimes U_{i'}U_k(b_ig_k)$. Let $g_i^{-1}g_k = g_j$. Then $g_i = g_kg_j^{-1}$. Thus $U_{i'}U_k = U_jf(g_i^{-1}, g_k)$ and $U_i = U_kU_{j'}(f(g_k, g_j^{-1}))^{-1}$. This implies that

$$\sum_1 (U_kU_1 \otimes U_{1'})b_1 = \sum_i U_kU_{j'}\left(f\left(g_k, g_j^{-1}\right)\right)^{-1} \otimes U_j\left(g_i^{-1}, g_k\right)\left(b_ig_k\right)$$

$$= \sum_i \left(U_kU_{j'} \otimes U_j\right)\left(f\left(g_k, g_j^{-1}\right)\right)^{-1} g_jf\left(g_i^{-1}, g_k\right)\left(b_ig_k\right).$$

Let $U_j = U_{1'}$. Then, $g_j = g_1^{-1}$, $g_1 = g_j^{-1}$, $U_1 = U_{j'}$ and $U_{1'} = U_j$. Hence $U_kU_1 \otimes U_{1'} = U_kU_{j'} \otimes U_j$. Thus $b_1 = (f(g_k, g_1))^{-1}g_1^{-1}f(g_i^{-1}, g_k)(b_ig_k)$ for each 1, where $g_i = g_kg_1$. Furthermore, noting that $\Sigma_1 U_1f(g_1, g_{1'})b_1 = U_1a^{-1}$, we have that $a \cdot \Sigma_1 f(g_1, g_1^{-1})(f(g_k, g_1))^{-1}g_1^{-1}f(g_i^{-1}, g_k)(b_ig_k) = 1$. This proves the necessity. The sufficiency is immediate by reversing the above arguments.

From Theorem 1, the coefficients of x are in C and the factor set f: $G \times G \to U(C)$, so $\Delta(R, G)$ is separable over R if and only if $\Delta(C, G)$ is separable over C. Next, we study the separability of $\Delta(R, G)$ for some types of factor sets f. A factor set f is called *I-symmetric* if $f(g_i^{-1}, g_j) = f(g_j^{-1}, g_i)$ for all g_i, g_j in G. (f can be considered as a function on entries of a matrix with row index $\{1', \ldots, n'\}$ and column index $\{1, \ldots, n\}$ where $g_{i'} = g_i^{-1}$.) A factor set f is called a *scalar factor set* if $f(g_{i'}, g_i)$ is a constant for $i = 1, \ldots, n$. The following property of f is easy to verify:

LEMMA 2. *Let f be a factor set such that $f(g_1, g_1) = a$. Then $(af(g_i, g_{i'}))g_i = af(g_{i'}, g_i)$ for each i.*

THEOREM 3. *Assume that* $f: G \times G \to U(C^G)$ *such that* f *is I-symmetric and scalar. If* $\Delta(R, G)$ *is separable over* R, *then any separable idempotent* $x\ (= \Sigma_j(U_j \otimes U_{j'})b_j)$ *satisfies*

(1)′ $b_j = (b_1)g_j^{-1}$ *for some* b_1 *in* C *and for each* j, *and*

(2)′ $\Sigma_j(b_1)g_j^{-1} = a^{-2}$ *where* $a = f(g_1, g_1)$.

PROOF. Since $f(G \times G) \subset U(C^G)$, $af(g_j, g_j^{-1}) = af(g_j^{-1}, g_j)$ for each j by the lemma. Hence $f(g_j, g_j^{-1}) = f(g_j^{-1}, g_j) = a$ (for f is scalar). Since $f(g_i^{-1}, g_k)f(g_j^{-1}, g_k^{-1}) = f(g_j^{-1}g_k^{-1}, g_k)f(g_j^{-1}, g_k^{-1}) = f(g_j^{-1}, g_k^{-1}g_k)f(g_k^{-1}, g_k) = a^2$, $f(g_i^{-1}, g_k) = a^2(f(g_j^{-1}, g_k^{-1}))^{-1}$. But f is I-symmetric, so $f(g_j^{-1}, g_k^{-1}) = f(g_k, g_j)$. Then, conditions (2) and (3) in Theorem 1 imply that $b_j = (f(g_k, g_j))^{-2}a^2(b_i g_k)$ and $1 = a^4\Sigma_j(f(g_k, g_j))^{-2}(b_i g_k)$ where $g_i = g_k g_j$. Thus $1 = a^2\Sigma_j b_j$, and so $\Sigma_j b_j = a^{-2}$. Taking $i = 1$, we have that $g_k = g_j^{-1}$. Hence, $1 = a^4a^{-2}\Sigma_j(b_1 g_j^{-1}) = a^2\Sigma_j(b_1 g_j^{-1})$, so $\Sigma_j(b_1 g_j^{-1}) = a^{-2}$. Also, $b_j = a^{-2}a^2(b_1 g_j^{-1}) = b_1 g_j^{-1}$.

Condition (1)′ means that each coefficient b_j of x is determined by b_1, and condition (2)′ implies that the trace of b_1 is a^{-2}. It can be verified that the converse of Theorem 3 holds for any constant factor set f.

THEOREM 4. *If* $f: G \times G \to U(C^G)$ *is a constant, then the converse of Theorem* 3 *holds.*

Assume $nc = 1$ for some c in C. Then the trace of ca^{-2} is a^{-2}. Thus $\Delta(R, G)$ is a separable extension over R by Theorem 4. We conclude the paper with an example to demonstrate our results. Let $R[i, \rho]$ be a generalized quaternion algebra (Parimula and Sridharan (1977), Szeto (1980)), where $\{1, i\}$ is a basis for $R[i, \rho]$ over R, ρ an automorphism of R of order 2, $ri = i(r\rho)$ for each r in R and $i^2 = b$ in $U(C^\rho)$. We define $f: \langle\rho\rangle \times \langle\rho\rangle \to U(C)$ by $f(\rho^0, \rho) = f(\rho, \rho^0) = f(\rho^0, \rho^0) = 1$ and $f(\rho, \rho) = b$. Then it is easy to see that f is a factor set for the crossed product $\Delta(R, \langle\rho\rangle)$ with basis $U_0 = U_{\rho^0}$, $U_1 = U_\rho$ such that the identity is U_0 and that $R[i, \rho]$ is isomorphic with $\Delta(R, \langle\rho\rangle)$ with factor set f under α: $R[i, \rho] \to \Delta(R, \langle\rho\rangle)$ where $\alpha(x + iy) = U_0 x + U_1 y$ for x and y in R.

References

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

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

F. R. DeMeyer and E. Ingraham (1971), *Separable algebras over commutative rings* (Lecture Notes in Mathematics 181, Springer-Verlag, Berlin-Heidelberg-New York).

T. Kanzaki (1964), 'On commutor rings and Galois theory of separable algebras,' *Osaka J. Math.* **1**, 103–115.

T. Nagahara and K. Kishimoto (1978), 'On free cyclic extensions of rings,' *Math. J. Okayama Univ.*, 1–25.

S. Parimula 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 extension of commutative rings,' *J. Pure Appl. Algebra* **16**, 315–322.

G. Szeto and Y. F. Wong (1982), 'On separable cyclic extensions of rings,' *J. Austral. Math. Soc. Ser. A* **32**, 165–170.

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

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

https://doi.org/10.1017/S1446788700023818 Published online by Cambridge University Press