J. Austral. Math. Soc. (*Series A*) 38 (1985), 275–280

A CHARACTERIZATION OF SEPARABLE POLYNOMIALS OVER A SKEW POLYNOMIAL RING

GEORGE SZETO

(Received 28 April 1983; revised 30 November 1983)

Communicated by R. Lidl

Abstract

The characterization of a separable polynomial over an indecomposable commutative ring (with no idempotents but 0 and 1) in terms of the discriminant proved by G. J. Janusz is generalized to a skew polynomial ring $R[X, \rho]$ over a not necessarily commutative ring R where ρ is an automorphism of R with a finite order.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 16 A 05.

1. Introduction

Let R be a ring with 1, ρ an automorphism of R of order n for some integer n, and $R[X, \rho]$ a skew polynomial ring in an indeterminate X. A monic polynomial $f(X) = X^m - a_{m-1}X^{m-1} - \cdots - a_1X - a_0$ for some a_i in R and an integer m such that $Xf(X) = f(X)X$ is called a separable polynomial if the cyclic extension $R[x, \rho]$ ($\cong R[X, \rho]/(f(X))$) is a separable ring extension of R with a free basis $\{1, x, \ldots, x^{m-1}\}$ where $rx = x\rho(r)$ for each r in R, $x = X + (f(X))$ and $(f(X))$ is an ideal generated by $f(X)$. In the present paper, we assume that the order n of ρ is equal to the degree m of $f(X)$. When R is commutative and indecomposable with ρ equal to the identity automorphism, $f(X)$ is separable if and only if the discriminant (= the determinant of the matrix $[t_{i+1, j+1}]$ where $t_{i+1, j+1}$ = trace of x^ix^j for $i, j = 0, 1, \ldots, n-1$) is a unit in R (DeMeyer and Ingraham (1971), Theorem 4.4, page 111, or Janusz (1966)). Our purpose is to generalize this

https://doi.org/10.1017/S1446788700023132 Published online by Cambridge University Press

characterization to skew polynomial rings over a not necessarily commutative ring. Let B_k be the set $\{s \text{ in } R: rs = s\rho^{-k}(r) \text{ for each } r \text{ in } R\}$. We shall show that if $T(=[t_{i+1,j+1}])$ is invertible with the $(i+1, j+1)$th entry of T^{-1} in B_{i+j}, then $f(X)$ is separable, and that the converse holds in case R is finitely generated and projective over its center C.

The present paper was written during the author's sabbatical leave at the University of Chicago. The author wishes to thank Professor I. N. Herstein for his excellent lectures on Galois theory and Professor R. Swan on projective modules. The author would like to thank the referee for his valuable corrections and suggestions.

2. Preliminaries

Let R be a ring with 1 and S a subring with 1. Then R is called a separable extension over S if there exist elements a_i, b_i in R such that $\sum_{i=1}^{m} a_i b_i = 1$ for some integer m and $u(\sum a_i \otimes b_i) = (\sum a_i \otimes b_i)u$ for each u in R. Such an element $\sum a_i \otimes b_i$ is called a separable idempotent for R [DeMeyer and Ingraham (1971)], and $\{a_i, b_i\}$ is called a separable set for R. Throughout, we assume that $R[x, \rho]$ is a cyclic extension $(\cong R[X, \rho]/(f(X))$ where $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. We denote the ith projection map by π_i such that $\pi_i(u) = \pi_i(\sum_{k=0}^{n-1} r_k x^k) = r_i$ in R. Then $u = \sum_i \pi_i(u)x^i$. The trace t at u, $t(u) = \sum_i \pi_i(ux^i)$ [DeMeyer and Ingraham [1971], page 91]. It is easy to see that π_i and t are left R-module homomorphisms of $R[x, \rho]$.

3. A necessary condition

In this section, we shall show that if $R[x, \rho]$ is separable over R, then T $(=[t_{i+1,j+1}])$ has a left inverse with the $(i+1, j+1)$th entry in B_{i+j} for $i, j = 0, 1, \ldots, n-1$, and T is invertible in case R is finitely generated and projective over its center C.

PROPOSITION 3.1. *Let $R^\rho = \{r \text{ in } R \text{ such that } \rho(r) = r\}$. If $Xf(X) = f(X)X$ where $f(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0$, then a_i are in R^ρ.*

PROOF. Since $\{1, X, X^2, \ldots\}$ is free over R, the proposition is clear.

PROPOSITION 3.2. *The matrix T $(=[t_{i+1,j+1}]$, $i, j = 0, 1, \ldots, n-1)$ is a symmetric matrix over R^ρ.*

PROOF. Since $x^n = a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with a_i in R^ρ by Proposition 3.1, $t_{i+1,j+1} = t(x^ix^j) = t(x^jx^i) = \sum_{k=0}^{n-1} \pi_k(x^{i+j}x^k)$ are in R^ρ such that T is symmetric.

Now we obtain a "nice" separable set for the separable extension $R[x, \rho]$.

LEMMA 3.3. *If $R[x, \rho]$ is separable over R, then there exists a separable set $\{y_i, x^i: i = 0, 1, \ldots, n-1\}$, where y_i are in $R[x, \rho]$ such that $y_i = \sum_{k=0}^{n-1} d_{ik}x^k$ where d_{ik} is in B_{i+k}.*

PROOF. Since $R[x, \rho]$ is separable over R, there exists a separable set $\{x_i, z_i$ in $R[x, \rho]$: $i = 0, 1, \ldots, m$ for some integer $m\}$ such that $\sum_i x_iz_i = 1$ and $u(\sum x_i \otimes z_i) = (\sum x_i \otimes z_i)u$ for each u in $R[x, \rho]$. Let $x_i = \sum_{k=0}^{n-1} p_{ik}x^k$ and $z_i = \sum_{k=0}^{n-1} q_{ik}x^k$ for some p_{ik}, q_{ik} in R. Then $\sum x_i \otimes z_i = \sum_{i=0}^{m}(\sum_{k=0}^{n-1} p_{ik}x^k \otimes \sum_{s=0}^{n-1} q_{is}x^s) = \sum_s(\sum_k(\sum_i p_{ik}\rho^{-k}(q_{is}))x^k \otimes x^s)$. We let $d_{sk} = \sum_i p_{ik}\rho^{-k}(q_{is})$ and $y_s = \sum_{k=0}^{n-1} d_{sk}xk^k$. Then $\sum_{i=0}^{n-1} x_i \otimes z_i = \sum_{s=0}^{n-1} y_s \otimes x^s$. Thus $1 = \sum_i x_iz_i = \sum_s y_sx^s$, and $u(\sum_s y_s \otimes x^s) = u(\sum_i x_i \otimes z_i) = (\sum_i x_i \otimes z_i)u = (\sum_s y_s \otimes x^s)u$ for each u in $R[x, \rho]$. Taking $u = r$, we have that $r(\sum_s\sum_k d_{sk}x^k \otimes x^s) = (\sum_s\sum_k d_{sk}x^k \otimes x^s)r$; and so $rd_{sk} = d_{sk}\rho^{-s-k}(r)$ for each r in R. Thus d_{sk} is in B_{s+k}.

LEMMA 3.4. *If $R[x, \rho]$ is separable over R, then for each u in $R[x, \rho]$, $u = \sum y_it(x^iu)$.*

PROOF. The lemma is immediate by the proof of Theorem 2.1 in [DeMeyer and Ingraham (1971), page 92].

THEOREM 3.5. *If $R[x, \rho]$ is separable over R, then the matrix T has a left inverse A such that the $(i+1, j+1)$th entry of A is in B_{i+j}, $i, j = 0, 1, \ldots, n-1$.*

PROOF. Let $\{y_i, x^i\}$ be a separable set for $R[x, \rho]$ obtained in Lemma 3.3. Then, by Lemma 3.4, $x^j = \sum_{i=0}^{n-1} y_it(x^ix^j) = \sum_{i=0}^{n-1}(\sum_{k=0}^{n-1} d_{ik}x^k)t(x^ix^j) = \sum_i(\sum_k d_{ik}t(x^ix^j)x^k)$ (for $t(x^ix^j)$ are in R^ρ by Proposition 3.2). Hence $\pi_p(x^j) = \sum_i\sum_k d_{ik}t(x^ix^j)\pi_p(x^k)$ for each $j, p = 0, 1, \ldots, n-1$ (for $\pi_j(x^k) = \delta_{jk} = 1$ when $j = k$, or 0 when $j \neq k$). Thus $\delta_{pj} = \sum_i d_{ip}t(x^ix^j)$. Let $s_{pi} = d_{ip}$. Then $AT = I$, the identity matrix, where $A = [s_{p+1,i+1}]$, a matrix with the (p, i)th entry $s_{p+1,i+1}$.

LEMMA 3.6. *Let S be a ring with 1, and finitely generated and projective as a left module over a commutative subring K with 1. If $ab = 1$ for some a, b in S, then $ba = 1$.*

PROOF. We define a map f_b: ${}_KS \to {}_KS$ by $f_b(r) = rb$ for each r in S. Then it is easy to see that f_b is a left module homomorphism of S to S. Since $f_b(a) = ab = 1$,

https://doi.org/10.1017/S1446788700023132 Published online by Cambridge University Press

$f_b(ca) = cab = c$ for each c in S. Hence f_b is an onto map. But then the sequence $0 \to \ker(f_b) \to S \to S \to 0$ of left K-modules is exact. By hypothesis, S is finitely generated and projective as a left K-module, so $S \cong \ker(f_b) \oplus S$. Noting that $K_m \otimes_K S \cong K_m \otimes_K f_b(S)$ as free K_m-modules over the local ring K_m at each maximal ideal m of K, we have $K_m \otimes_K \ker(f_b) = 0_m$. Hence $\ker(f_b) = 0$. Thus f_b is a one-to-one map. Therefore, f_a is also a right inverse of f_b from the fact that $ab = 1$. Thus $ba = 1$.

THEOREM 3.7. *Let R be finitely generated and projective over its center C. If $R[x, \rho]$ is separable over R, then T is invertible such that the $(i + 1, j + 1)$th entry of T^{-1} is in B_{i+j} for $i, j = 0, 1, \ldots, n - 1$.*

PROOF. Since $\operatorname{Hom}_R(R[x, \rho], R[x, \rho])$ is a free module as a left R-module, it is finitely generated and projective over the commutative subring C. Thus the theorem is an immediate consequence of Theorem 3.5 and Lemma 3.6.

4. A sufficient condition

In this section, we are going to show a sufficient condition for the separability of $R[x, \rho]$. That is, if T is invertible such that the $(i + 1, j + 1)$th entry of T^{-1} is in B_{i+j} for $i, j = 0, 1, \ldots, n - 1$, then $R[x, \rho]$ is separable over R. We begin with some properties of the inverse of T when T is invertible.

LEMMA 4.1. *If T is invertible such that the $(i + 1, j + 1)$th entry of T^{-1} d_{ij} is in B_{i+j} for $i, j = 0, 1, \ldots, n - 1$, then (1) $t(y_i x^j) = t(x^j y_i) = \pi_i(x^j) = \delta_{ij}$, where $y_i = \sum_{k=0}^{n-1} d_{ik} x^k$, and (2) $d_{ij} = t(y_i y_j) = t(y_j y_i)$ in R^ρ (hence T^{-1} is symmetric).*

PROOF. Let $M = [m_{ij}]$ be a matrix over R. We denote the matrix with entries $\rho(m_{ij})$ by $\rho(M)$. Clearly, $\rho(TT^{-1}) = \rho(T^{-1}T) = \rho(T^{-1})\rho(T) = \rho(T)\rho(T^{-1}) = I$. Since T is over R^ρ by Proposition 3.1, $\rho(T^{-1})T = I = T\rho(T^{-1})$. Hence $\rho(T^{-1}) = T^{-1}$ by the uniquenss of T^{-1}. Thus T^{-1} is over R^ρ. Again, by Proposition 3.2, T is symmetric. Now let d_{ij} be the $(i + 1, j + 1)$th entry of T^{-1} and let $y_i = \sum_{k=0}^{n-1} d_{ik} x^k$. Since $T^{-1}T = I$, $\sum_k d_{ik} t(x^k x^j) = \delta_{ij}$. This implies that $t(\sum_k d_{ik} x^k x^j) = \delta_{ij}$; and so $t(y_i x^j) = \delta_{ij}$. Since d_{ik} are in R^ρ, $t(y_i x^j) = t(x^j y_i) = \pi_i(x^j)$, $i, j = 0, 1, \ldots, n - 1$. This proves part (1). But then $t(y_i y_j) = t(y_i \sum_k d_{jk} x^k) = t(\sum_k y_i d_{jk} x^k) = t(\sum_k y_i x^k d_{jk})$ (for d_{jk} are in R^ρ). This is equal to $\sum_k t(y_i x^k) d_{jk} = \sum_k \delta_{ik} d_{jk} = d_{ji}$ from the above result. Similarly, $t(y_j y_i) = t(\sum_k d_{jk} x^k y_i) = \sum_k d_{jk} t(x^k y_i) = \sum_k d_{jk} \delta_{ki} = d_{ji}$. Thus $t(y_i y_j) = t(y_j y_i)$. And, $t(y_i y_j) = t(y_j \sum_k d_{ik} x^k) = \sum_k t(y_j x^k) d_{ik} = \sum_k \delta_{jk} d_{ik} = d_{ij}$. Therefore, $t(y_i y_j) = t(y_j y_i) = d_{ij} = d_{ji}$ for all $i, j = 0, 1, \ldots, n - 1$. Thus part (2) holds.

LEMMA 4.2. *By keeping the hypotheses and notations of Lemma* 4.1 *and for each* $i, k = 0, 1, \ldots, n-1$, *we have that* (1) $\pi_i(u) = t(uy_i)$ *for all* u *in* $R[x, \rho]$, *and* (2) $t(y_k x^i y_i) = t(y_i x^i y_k)$ *and* $t(xy_k y_i) = t(xy_i y_k)$.

PROOF. (1) Let $u = \sum_{k=0}^{n-1} r_k x^k$ for some r_k in R. Then $\pi_i(u) = \sum_k r_k \pi_i(x^k) = \sum_k r_k t(x^k y_i)$ by Lemma 4.1–(1). Thus $\pi_i(u) = \sum_k t(r_k x^k y_i) = t(\sum_k r_k x^k y_i) = t(uy_i)$.

(2) Since $y_k = \sum_{j=0}^{n-1} d_{kj} x^j$ with d_{kj} in R^ρ, we have that $t(y_k x^i y_i) = t(\sum_j d_{kj} x^{j+i} y_i) = \sum_j d_{kj} t(x^{j+i} y_i) = \sum_j d_{kj} t(y_i x^{i+j})$. Similarly, $t(y_i x^i y_k) = t(\sum_j y_i d_{kj} x^{j+i}) = t(\sum_j y_i x^{j+i} d_{kj}) = \sum_j t(y_i x^{j+i}) d_{kj}$. We note that d_{kj} is in $(R^\rho \cap B_{k+j})$ and that a_i is in R^ρ for $i, j, k = 0, 1, \ldots, n-1$, so $a_i d_{kj} = d_{kj} \rho^{-k-j}(a_i) = d_{kj} a_i$ and $xy_i = y_i x$. Since $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $t(y_i x^{j+i})$ is a sum of some a_k's by using the linear property of t and the fact that $t(y_i x^j) = \delta_{ij}$ for $i, j = 0, 1, \ldots, n-1$ (Lemma 4.1–(1)). Hence $d_{kj} t(x^{j+i} y_i) = d_{kj} t(y_i x^{i+j}) = t(y_i x^{i+j}) d_{kj}$. Thus $t(y_k x^i y_i) = t(y_i x^i y_k)$. Also, since $xy_i = y_i x$ and $d_{kj} t(x^{j+1} y_i) = t(y_i x^{j+1}) d_{kj}$, we have that $t(xy_k y_i) = t(xy_i y_k)$.

THEOREM 4.3. *If the matrix* T *is invertible such that* $(i+1, j+1)$*th entry of* T^{-1} *is in* B_{i+j}, *then* $R[x, \rho]$ *is separable over* R, *where* $i, j = 0, 1, \ldots, n-1$.

PROOF. Keeping the notations of Lemmas 4.1, 4.2, we first show that, for an element u in $R[x, \rho]$, if $t(uy_i) = 0$ for each $i = 0, 1, \ldots, n-1$, then $u = 0$. In fact, $u = \sum_{i=0}^{n-1} \pi_i(u) x^i = \sum_i t(uy_i) x^i$ by Lemma 4.2–(1). Since $t(uy_i) = 0$ by hypothesis, $u = 0$. Next, we claim that $\sum y_i \otimes x^i$ is a separable idempotent for $R[x, \rho]$ by using the above result. Since $t((1 - \sum_{i=0}^{n-1} y_i x^i) y_k) = t(y_k) - t(\sum_i y_i x^i y_k) = \sum_i \pi_i(y_k x^i) - \sum_i t(y_i x^i y_k) = \sum_i t(y_k x^i y_i) - \sum_i t(y_i x^i y_k)$ by using Lemma 4.1–(1), that $\sum_i t(y_k x^i y_i) - \sum_i t(y_i x^i y_k) = 0$ by Lemma 4.2–(2) implies that $t((1 - \sum_{i=0}^{n-1} y_i x^i) y_k) = 0$ for each k. Thus $1 - \sum_i y_i x^i = 0$ by the above result. So, $\sum_i y_i x^i = 1$. We now claim that $w(\sum_i y_i \otimes x^i) = (\sum_i y_i \otimes x^i)wi$ for each w in $R[x, \rho]$. In case $w = x$, $x(\sum_i y_i \otimes x^i) = \sum_i xy_i \otimes x^i = \sum_i(\sum_k \pi_k(xy_i) x^k \otimes x^i) = \sum_i(\sum_k t(xy_i y_k) x^k \otimes x^i)$ by Lemma 4.1–(1). Since the coefficients of y_i, y_k and x^n are in R^ρ, so is $t(xy_i y_k)$ for each i and k; and so $t(xy_i y_k) x^k \otimes x^i = x^k t(xy_i y_k) \otimes x^i = x^k \otimes t(xy_i y_k) x^i$. Hence $x(\sum_i y_i \otimes x^i) = \sum_i(\sum_k x^k \otimes t(xy_i y_k) x^i) = \sum_k(x^k \otimes \sum_i t(xy_k y_i) x^i)$ by Lemma 4.2–(2). By Lemma 4.2–(1), this is equal to $\sum_k(x^k \otimes \sum_i \pi_i(xy_k) x^i) = \sum_k(x^k \otimes xy_k) = (\sum_k x^k \otimes y_k)x$ (for $xy_k = y_k x$). Thus, $x(\sum_i y_i \otimes x^i) = (\sum_i x^i \otimes y_i)x$. Also, we can see that the proof of this case holds for $w = 1$, so $\sum_i y_i \otimes x^i = \sum_i x^i \otimes y_i$. Thus $x(\sum_i y_i \otimes x^i) = (\sum_i y_i \otimes x^i)x$. Moreover, in case $w = r$ in R, $r(\sum_i y_i \otimes x^i) = \sum_i((\sum_k r d_{ik} x^k) \otimes x^i)$. Since d_{ik} is in B_{i+k}, this is equal to $\sum_i((\sum_k d_{ik} \rho^{-i-k}(r) x^k) \otimes x^i) = \sum_i((\sum_k d_{ik} x^k \rho^{-i}(r)) \otimes x^i) = \sum_i((\sum_k d_{ik} x^k) \otimes \rho^{-i}(r) x^i) = \sum_i((\sum_k d_{ik} x^k) \otimes x^i r) = \sum_i(y_i \otimes x^i)r$. Thus, from the above two cases, we conclude that $w(\Sigma_i y_i \otimes x^i) = (\Sigma_i y_i \otimes x^i)w$ for each w in $R[x, \rho]$. Therefore, $R[x, \rho]$ is separable over R.

COROLLARY 4.4. *Let R be a commutative ring with 1. Then $R[x, \rho]$ is separable over R if and only if the discriminant of $f(X)$ ($=$ the determinant of T) is a unit.*

PROOF. Since R is commutative with 1, d_{ij} is in B_{i+j}. Also, T^{-1} exists if T has a left inverse. Thus the corollary is immediate from Theorems 3.5 and 4.3.

References

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

G. J. Janusz (1966), 'Separable algebras over commutative rings', *Trans. Amer. Math. Soc.* **122**, 461–479.

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.

G. Szeto and Y. F. Wong (1981), 'On free quadratic extensions of rings', *Monatsch. Math.* **92**, 323–328.

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