Math. J. Okayama Univ. 25 (1983), 23—28

ON SEPARABLE POLYNOMIALS AND FROBENIUS POLYNOMIALS IN SKEW POLYNOMIAL RINGS. II

SHÛICHI IKEHATA

Throughout this paper, B will mean a ring with 1, ρ an automorphism of B, and D a ρ-derivation of B (i.e. an additive endomorphism such that $D(ab)=D(a)\rho(b)+aD(b)\,(a,\ b\in B)$). Let $R=B[X;\rho,D]$ be the skew polynomial ring in which the multiplication is given by $aX=X\rho(a)+D(a)$ $(a\in B)$. In particular, we set $B[X;\rho]=B[X;\rho,0]$, $B[X;D]=B[X;1,D]$, and as usual, $B[X]=B[X;1,0]$. By $R_{(0)}$, we denote the set of all monic polynomials g in R with $gR=Rg$. A polynomial g in $R_{(0)}$ is called to be separable if R/gR is a separable extension of B. Let f be a polynomial in $B[X;\rho]_{(0)}$ (resp. $B[X;D]_{(0)}$) whose coefficients are ρ-invariant. As was shown in [3], if the derivative f' of f is invertible in R modulo fR, then f is separable in R. In this case, f is called a $\tilde{\rho}$-separable (resp. $\tilde{D}$-separable) polynomial. Such polynomials are applicable to Galois theory of skew polynomials.

In this paper, we shall give some sufficient conditions for a separable polynomial to be $\tilde{\rho}$-separable (resp. $\tilde{D}$-separable). The study contains some generalizations of the results of [3].

We shall use the following conventions:

Z = the center of B, $C(A)$ = the center of a ring of A.

$B^{\rho}=\{a\in B\mid \rho(a)=a\}$, $B^{D}=\{a\in B\mid D(a)=0\}$.

u_r = the right multiplication effected by $u\in B$.

I_u = the inner derivation effected by $u\in B$; $I_u(a)=au-ua$.

ρ^* : $B[X;\rho]\to B[X;\rho]$ is the ring automorphism defined by $\rho^*(\sum_i X^i d_i)=\sum_i X^i\rho(d_i)$.

D^* : $B[X;D]\to B[X;D]$ is the inner derivation defined by $D^*(\sum_i X^i d_i)=\sum_i X^i D(d_i)$.

1. $\tilde{\rho}$-separable polynomials. In this section, we assume that $R=B[X;\rho]$ and f is in $R_{(0)}\cap B^{\rho}[X]$ of degree m. First, we shall define the discriminant of f. As was shown in [3, Remark 1.3], f is in $C(B^{\rho})[X]$. The $C(B^{\rho})$-module $C(B^{\rho})[X]/fC(B^{\rho})[X]$ has a free basis $\{1, x, \cdots, x^{m-1}\}$ where $x=X+fC(B^{\rho})[X]$. Let π_i be the projection of $C(B^{\rho})[X]/fC(B^{\rho})[X]$ on to the coefficients of x^i. The trace map t is defined by $t(z)=\sum_{i=0}^{m-1}\pi_i(zx^i)$ $(z\in C(B^{\rho})[X]/fC(B^{\rho})[X])$. Then the discriminant $\delta(f)$ is defined by

$\delta(f)=\det\|t(x^k x^l)\|$ $(0\leqq k, l\leqq m-1)$. By [4, Theorem 2.1] and [3, Theorem 2.1], we see that f is $\tilde{\rho}$-separable if and only if $\delta(f)$ is invertible in B.

Now, we shall begin our study with the following

Lemma 1.1. *$a\delta(f)=\delta(f)\rho^{m(m-1)}(a)$ for all $a\in B$.*

Proof. For $k\geqq 0$, we set $x^k=x^{m-1}b_{m-1}+x^{m-2}b_{m-2}+\cdots+xb_1+b_0$ $(b_i\in C(B^\rho))$. Then, we have $X^k\equiv X^{m-1}b_{m-1}+\cdots+Xb_1+b_0$ (mod fR). Since $aX^k=X^k\rho^k(a)$ $(a\in B)$, it follows that $ab_i=b_i\rho^{k-i}(a)$ and so, $a\pi_i(x^k)=\pi_i(x^k)\rho^{k-i}(a)$ $(0\leqq i\leqq m-1)$. Since $t(x^\nu)=\sum_{i=0}^{m-1}\pi_i(x^{i+\nu})$, we obtain $at(x^\nu)=t(x^\nu)\rho^\nu(a)$. Then the assertion is now easy.

In the rest of this section, we assume that $f=X^m+X^{m-1}a_{m-1}+\cdots+Xa_1+a_0$ is a separable plynomial. Then by [3, Theorem A], there exists $y\in R$ with deg $y<m$ such that $\rho^{m-1}(a)y=ya$ $(a\in B)$ and $\sum_{j=0}^{m-1}Y_jyX^j\equiv 1$ (mod fR), where $Y_j=X^{m-j-1}+X^{m-j-2}a_{m-1}+\cdots+Xa_{j+2}+a_{j+1}$. Under this situation, we shall prove the following

Lemma 1.2. *Assume that $u\in B^\rho$ and $au=u\rho^n(a)$ (or $\rho^n(a)u=ua$) $(a\in B)$ with a positive integer n. Then*

$$f'(\textstyle\sum_{k=0}^{n-1}\rho^{*k}(y)u)=(\sum_{k=0}^{n-1}\rho^{*k}(y)u)f'\equiv nu \pmod{fR}.$$

Proof. Since $u\in B^\rho$ and $au=u\rho^n(a)$, we have $uy=yu$ and $yu=u\rho^{*n}(y)=\rho^{*n}(y)u$. Hence $\rho^*(\sum_{k=0}^{n-1}\rho^{*k}(y)u)=\sum_{k=0}^{n-1}\rho^{*k}(y)u$. Since $Y_j\in C(B^\rho)[X]$ ([3, Lemma 1.2]) and $f'=\sum_{j=0}^{m-1}Y_jX^j$, it follows that

$$\begin{aligned}nu&\equiv\textstyle\sum_{j=0}^{m-1}Y_j(\sum_{k=0}^{n-1}\rho^{*k}(y)u)X^j\\&=f'(\textstyle\sum_{k=0}^{n-1}\rho^{*k}(y)u)=(\sum_{k=0}^{n-1}\rho^{*k}(y)u)f' \pmod{fR}.\end{aligned}$$

This completes the proof.

Corollary 1.3.

$$(f'\textstyle\sum_{i=0}^{m-i-1}\rho^{*k}(y))a_i=(\sum_{i=0}^{m-i-1}\rho^{*k}(y)f')a_i\equiv(m-i)a_i \pmod{fR},$$

for $0\leqq i\leqq m-1$.

Proof. Since $f\in R_{(0)}\cap B^\rho[X]$, we have $aa_i=a_i\rho^{m-i}(a)$ $(a\in B)$ and $\rho(a_i)=a_i$ by [3, Lemma 1.3 a)].

Now, we shall prove the following theorem which contains a generalization of [3, Theorem 2.2] and a partially generalization of [5, Theorem 2.7].

Theorem 1.4. *Let* $f = X^m + X^{m-1}a_{m-1} + \cdots + Xa_1 + a_0$ *be in* $R_{(0)} \cap B^\rho[X]$. *Assume that* f *is separable. If there holds one of the following conditions* (1)—(6), *then* f *is* $\tilde{\rho}$*-separable*:

(1) *There exists a regular element* u *in* B *and a positive integer* n *such that* $au = u\rho^n(a)$ (*or* $ua = \rho^n(a)u$) ($a \in B$), *and* n *is invertible in* B.

(2) $m(m-1)$ *is invertible in* B.

(3) *Both* a_0 *and* a_1 *are regular elements* (i.e., *non-zero divisors*) *in* B.

(4) a_{m-1} *is a regular element in* B.

(5) $\rho \mid Z = 1_Z$ *and* $m-1$ *is invertible in* B.

(5′) $\rho \mid Z = 1_Z$ *and* m *is in the Jacobson radical* rad(B) *of* B.

(6) $\rho \mid Z = 1_Z$ *and* a_1 *is in* rad(B).

Moreover, if (2) *is satisfied then every separable polynomial in* $R_{(0)} \cap B^\rho[X]$ *is* $\tilde{\rho}$*-separable.*

Proof. Case (1). Since $au = u\rho^n(a)$ ($a \in B$), we have $\rho^n(u) = u$ and $a\rho^\nu(u) = \rho^\nu(u)\rho^n(a)$. We set here $v = u\rho(u) \cdots \rho^{n-1}(u)$. Then $\rho(v) = v$. Since v is regular in B, so is in R/fR. Hence by Lemma 1.2, f' is invertible in R modulo fR. Thus, f is $\tilde{\rho}$-separable.

Cases (2) and (3). By [1, Lemma 1], there exist $\alpha, \beta \in B$ such that $a_0\alpha + a_1\beta = 1$. By Corollary 1.3, there exist $z_1, z_2 \in R$ such that $ma_0 \equiv f'z_1a_0$ and $(m-1)a_1 \equiv f'z_2a_1$ (mod fR). Therefore, if both a_0 and a_1 are regular elements in B, f' is invertible in R modulo fR. Next, we assume that $m(m-1)$ is invertible in B. Then f' is invertible in R modulo fR since

$$m(m-1) \equiv f'((m-1)z_1a_0\alpha + mz_2a_1\beta) \pmod{fR}.$$

Moreover, $\delta(f)$ is invertible in B and $a\delta(f) = \delta(f)\rho^{m(m-1)}(a)$ ($a \in B$) by Lemma 1.1. Therefore, every separable polynomial in $R_{(0)} \cap B^\rho[X]$ is $\tilde{\rho}$-separable by case (1).

Case (4). It is obvious by Corollary 1.3.

Cases (5), (5′) and (6). Obviously, (5′) implies (5).
We put here $y = X^{m-1}c_{m-1} + \cdots + Xc_1 + c_0$. Then we have

$$\begin{aligned}\textstyle\sum_{j=0}^{m-1} Y_j y X^j &= \textstyle\sum_{j=0}^{m-1} Y_j X^j \rho^{*j}(y) \\ &= \textstyle\sum_{j=0}^{m-1}(\sum_{\nu=j}^{m-1} X^\nu a_{\nu+1})\rho^{*j}(y) \\ &= a_1 y + \textstyle\sum_{\nu=1}^{m-1}\sum_{j=0}^{\nu}\sum_{\mu=0}^{m-1} X^{\nu+\mu}a_{\nu+1}\rho^j(c_\mu).\end{aligned}$$

Comparing the constant terms modulo fR of the both sides, we have

$$1 = a_1c_0 + \textstyle\sum_{\nu=1}^{m-1}\sum_{\mu=0}^{m-1}\sum_{j=0}^{\nu} b_{\nu+\mu}a_{\nu+1}\rho^j(c_\mu),$$

where b_k is the constant term of X^k modulo fR and $a_m = 1$. It is obvious that $ab_{\nu+\mu} = b_{\nu+\mu}\rho^{\nu+\mu}(a)$, $aa_{\nu+1} = a_{\nu+1}\rho^{m-\nu-1}(a)$ and $\rho^{m-1+\mu}(a)c_\mu = c_\mu a$

($a \in B$). Hence $b_{\nu+\mu}a_{\nu+1}\rho^j(c_\mu) \in Z$. Since $b_{\nu+\mu}, a_{\nu+1} \in B^\rho$ and $\rho \mid Z = 1_Z$, we have $b_{\nu+\mu}a_{\nu+1}\rho^j(c_\mu) = b_{\nu+\mu}a_{\nu+1}c_\mu$. Then we obtain

$$1 = a_1c_0 + \sum_{\nu=1}^{m-1}\sum_{\mu=0}^{m-1}(\nu+1)b_{\nu+\mu}a_{\nu+1}c_\mu.$$

Moreover, one will easily see that $b_{\nu+\mu} = 0$ ($\nu+\mu \leqq m-1$) and $b_{\nu+\mu} \in a_0B$ ($\nu+\mu \geqq m$). Since $(\nu+1)a_0a_{\nu+1} = ma_0a_{\nu+1} - (m-(\nu+1))a_{\nu+1}a_0$, it follows from Corollary 1.3 that there exists $z \in R$ such that $1 \equiv a_1c_0 + f'z$ (mod fR). Now, if a_1 is in rad(B) then f' is invertible in R modulo fR. Next, if $m-1$ is invertible in B, then $m-1 \equiv (m-1)a_1c_0 + (m-1)f'z$ (mod fR), and whence, f' is invertible in R modulo fR by Corollary 1.3 again. This completes the proof.

As an immediate consequence of Theorem 1.4, we have the following

Corollary 1.5. *Assume that B is an algebra over a field of characteristic zero. Then, every separable polynomial which is in $R_{(0)} \cap B^\rho[X]$ is $\tilde{\rho}$-separable.*

Corresponding to [2, Theorem], we have the following

Corollary 1.6. *Assume that B is of prime characteristic $p > 0$ and $\rho \mid Z = 1_Z$. Then a monic polynomial $g = X^p + Xb_1 + b_0$ in $R_{(0)}$ is separable if and only if b_1 is invertible in B.*

Proof. First, we consider the case $p = 2$. Then we have $\rho(b_0) = b_0$ by [3, Lemma 1.3]. Hence, if g is separable then it is in $B^\rho[X]$ by [3, Proposition 3.1]. Moreover, if b_1 is invertible in B, then $b_1 = b_1^{-1}b_1^2 = b_1^{-1}b_1\rho(b_1) = \rho(b_1)$, and so $g \in B^\rho[X]$. Thus, the assertion follows from Theorem 1.4 and [3, Theorem 2.1]. Next, we consider the case $p > 2$. Then we have $g \in B^\rho[X]$ by [3, Remark 1.4]. Hence the assertion follows from Theorem 1.4 and [3, Theorem 2.1].

2. $\tilde{D}$-separable polynomials. In this section, we assume that $R = B[X;D]$. The following theorem is a sharpening of [3, Theorems 2.7 and 4.4].

Theorem 2.1. *If there holds one of the following conditions* (1) *and* (2), *then every separable polynomial in $B[X;D]_{(0)}$ is $\tilde{D}$-separable.*

(1) $(b_n)_rD^n + (b_{n-1})_rD^{n-1} + \cdots + (b_1)_rD = I_{b_0}$ *with some* $b_i \in B^D$ ($0 \leqq i \leqq n$) *where b_1 is invertible in B.*

(2) *$B[X;D]_{(0)}$ contains at least one $\tilde{D}$-separable polynomial.*

Proof. Let f be a separable polynomial of degree m. Then by [3, Theorem A] there exists $y \in R$ with deg $y < m$ such that $ay = ya$ $(a \in B)$ and $\sum_{j=0}^{m-1} Y_j y X^j \equiv 1 \pmod{fR}$, where $Y_j = X^{m-j-1} + X^{m-j-2}a_{m-1} + \cdots + Xa_{j+2} + a_{j+1}$.

Case (1). Since $b_i \in B^D$ $(0 \leqq i \leqq n)$, we have $(b_n)_r D^{*n} + \cdots + (b_1)_r D^* = I^*_{b_0}$. Hence

$$0 = yb_0 - b_0 y = \sum_{i=1}^{n} D^{*i}(y) b_i = D^*(\sum_{i=1}^{n} D^{*i-1}(y) b_i).$$

We put here $u = \sum_{i=1}^{n} D^{*i-1}(y) b_i$. Then $Xu = uX$ and $Y_j u = u Y_j$ ([3, Lemma 1.2]). Therefore, noting $\sum_{j=0}^{m-1} Y_j D^*(y) X^j \equiv 0 \pmod{fR}$, we have

$$\begin{aligned} b_1 &\equiv \sum_{j=0}^{m-1} Y_j (\sum_{i=1}^{n} D^{*i-1}(y) b_i) X^j \\ &\equiv \sum_{j=0}^{m-1} Y_j u X^j = f'u \doteq uf' \pmod{fR}. \end{aligned}$$

Thus, f' is invertible.

Case (2). Let $g = X^n + X^{n-1}d_{n-1} + \cdots + Xd_1 + d_0$ be $\tilde{D}$-separable polynomial in R. Then by [3, Theorem 2.1], g' is invertible in $C(B^D)[X]$ modulo $gC(B^D)[X]$. Therefore, there exists an element $h = \sum_{i=0}^{n-1} X^i c_i$ in $C(B^D)[X]$ such that $g'h \equiv 1 \pmod{gC(B^D)[X]}$. Comparing the constant terms modulo $gC(B^D)[X]$ of the both sides, we have

$$1 \equiv \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} (k+1) h_{k+i} d_{k+1} c_i,$$

where $h_\nu \in C(B^D)$ is the constant term of X^ν modulo $gC(B^D)[X]$. Now, by [3, Lemma 1.6], we have

$$d_k a - a d_k = \sum_{\nu=k+1}^{n} \binom{\nu}{k} D^{\nu-k}(a) d_\nu \ (a \in B) \text{ and } d_\nu \in B^D.$$

We set here $v = \sum_{\nu=k+1}^{n} \binom{\nu}{k} D^{*\nu-k-1}(y) d_\nu$. Then, by making use of the same methods as in the proof of (1), we see that $Xv = vX$ and $Y_j v = v Y_j$. Therefore, we obtain

$$\begin{aligned} (k+1) d_{k+1} &\equiv \sum_{j=0}^{m-1} Y_j (\sum_{\nu=k+1}^{n} \binom{\nu}{k} D^{*\nu-k-1}(y) d_\nu) X^j \\ &\equiv f'v \equiv vf' \pmod{fR}. \end{aligned}$$

Since $1 = \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} (k+1) d_{k+1} h_{k+i} c_i$, we conclude that f' is invertible in R modulo fR. This completes the proof.

REFERENCES

[1] S. IKEHATA: On a theorem of Y. Miyashita, Math. J. Okayama Univ. 21 (1979), 49—52.

[2] S. IKEHATA: A note on separable polynomials in skew polynomial rings of derivation type, Math. J. Okayama Univ. 22 (1980), 59—60.

[3] S. IKEHATA: On separable polynomials and Frobenius polynomials in skew polynomial rings, Math. J. Okayama Univ. 22 (1980), 115—129.

[4] T. NAGAHARA: On separable polynomials over a commutative rings II, Math. J. Okayama Univ. 15 (1972), 149—162.
[5] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. 19 (1976), 65—95.
[6] T. NAGAHARA: A note on separable polynomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ. 22 (1980), 73—76.

DEPERTMENT OF MATHEATICS
OKAYAMA UNIVERSITY

(*Received November 11, 1982*)