数理解析研究所講究録
第 438 巻 1981 年 15-22

ON SEPARABLE POLYNOMIALS IN SKEW POLYNOMIAL RINGS

Shuichi IKEHATA

Department of Mathematics, Okayama University

Throughout this paper, B will mean a ring with 1, ρ an automorphism of B, D a ρ-derivation of B (i.e. an additive endomorphsim such that $D(ab) = D(a)\rho(b) + aD(b)$ for all $a, b \in B$). 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 $B[X;\rho] = B[X;\rho,0]$ and $B[X;D] = B[X;1,D]$. 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. $B[X;D]_{(0)}$) such that the coefficients are fixed by ρ. As was shown in [3], if f', the derivative 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. 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 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 $u \in B$;

$I_u(a) = au - ua$.

$\rho^*: B[X;\rho] \to B[X;\rho]$ 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. In this section, we assume that $R = B[X;\rho]$ and f is in $R_{(0)} \cap B^\rho[X]$ with $\deg f = m$. First, we shall define the discrimnant of f. As was shown in [3, Remark 1.3], f is in $C(B^\rho)[X]$. The free $C(B^\rho)$-module $C(B^\rho)[X]/fC(B^\rho)[X]$ has a basis $\{1, x, \ldots, x^{m-1}\}$, where $x = X + fC(B^\rho)[X]$. Let π_i be theprojection 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 $\delta(f)$ of 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], f is $\tilde{\rho}$-separable if and only if $\delta(f)$ is invertible in B.

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

Proof. For $k \geqq 0$, we put $x^k = x^{m-1}b_{m-1} + x^{m-2}b_{m-2} + \ldots + db_1 + b_0$ $(b_i \in C(B^\rho))$. Then, we have $X^k \equiv X^{m-1}b_{m-1} + \ldots + Xb_1 + b_0 \pmod{fR}$. Since $aX^k =$

$X^k\rho^k(a)$ $(a \in B)$, we have $ab_i = b_i\rho^{k-i}(a)$ 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 $f = X^m + X^{m-1}a_{m-1} + \dots + Xa_1 + a_0$ is a separable polynomial. 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 $\sum_{j=0}^{m-1} Y_j y X^j \equiv 1 \pmod{fR}$, where $Y_j = X^{m-j-1} + X^{m-j-2}a_{m-1} + \dots + Xa_{j+2} + a_{j+1}$. Under the above hypothesis and notations, we shall prove the floowing Lemma.

Lemma 1.2. Assume that $au = u\rho^n(a)$ (or $\rho^n(a)u = ua$) $(a \in B)$ with an element $u \in B$ and a positive iteger n. Then $f'(\sum_{k=0}^{n-1} \rho*^k(y)u) = (\sum_{k=0}^{n-1}\rho*^k(y)uf') \equiv nu \pmod{fR}$.

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

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

Corollary 1.3. $(f'\sum_{i=0}^{m-i-1} \rho*^k(y))a_i = (\sum_{i=0}^{m-i-1}\rho*^k(y)f')a_i \equiv (m-i)a_i \pmod{fR}$, for $0 \leqq i \leqq m-1$.

Proof. Since $f \in R_{(0)} \cap B^{\rho}[X]$, we have $aa_i = a_i \rho^{m-1}(a)$ $(a \in B)$ 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 $f = X^m + X^{m-1}a_{m-1} + \ldots Xa_1 + a_0$ be in $R_{(0)} \cap B^{\rho}[X]$. Assume that f is separable. If there holds one 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 which is invertible in B such that $au = u\rho^n(a)$ (or $ua = \rho^n(a)u$) $(a \in B)$.

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

(3) Both a_0 and a_1 are regular elements in B.

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

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

(5') $\rho | Z = 1_Z$ and m is in rad B, the Jacobson radical of B.

(6) $\rho | Z = 1_Z$ 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). Let $v = u\rho(u)\ldots\rho^{n-1}(u)$. Since $au = u\rho^n(a)$ $(a \in B)$ and $\rho^n(u) = u$, we have $a\rho^{\nu}(u) = \rho^{\nu}(u)\rho^n(a)$ and $\rho(v) = v$. Since v is regular element 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.

Case (2) and (3). By [1, Lemma 1], there exist α, $\beta \in B$ 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 mdodulo fR. Next, if $m(m-1)$ is invertible in B, then f' is invertible in R mdoulo fR since

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

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

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

Case (5),(5') and (6). Obviously, (5') implies (5). We put here $y = X^{m-1}c_{m-1} + \ldots + Xc_1 + c_0$. 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.

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

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

It is easily verfied that $b_{\nu+\mu} = 0$ $(\nu+\mu \leqq m-1)$ and $b_{\nu+\mu} \in a_0B$ $(\nu+\mu \leqq m)$. 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 $1 \equiv a_1c_0 + f''z \pmod{fR}$.

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 $m - 1 \equiv (m-1)a_1c_0 + (m-1)f'z \pmod{fR}$. Thus, f' is invertible in R modulo fR by Corollary 1.3 again. This completes the proof.

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

Corollary 1.5. Assume that B is an algebra over a field of characterisric 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 $\rho | Z = 1_Z$. 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 consdier the case $p = 2$. Then by [3, Lemma 1.3], $gR = Rg$ implies $\rho(b_0) = b_0$. Hence, if g is separable then it is in $B^{\rho}[X]$ by [3, Propostion 3.1]. Since $ab_1 = b_1\rho(a)$ $(a \ B)$, we have $b_1{}^2 = b_1\rho(b_1)$. Hence, if b_1 is invertible in B, then $b_1 = \rho(b_1)$, and so $g \in B^{\rho}[X]$. Thus, the assertion follows from Theorem 1.4. Next, we consider the case $p > 2$. Then by [3, Remark 1.4], $gR = Rg$ implies g $B^{\rho}[X]$. Thus, the assertion follows from Theorem 1.4.

2. 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. Assume that $(b_n)_r D^n + (b_{n-1})_r D^{n-1} + \ldots + (b_1)_r D = I_{b_0}$ with some $b_i \in B^D$. If b_1 is invertible in B, then every separable polynomial in R is $\tilde{D}$-separable.

Proof. Let $f = X^m + X^{m-1}a_{m-1} + \ldots + Xa_1 + a_0$ be separable in R. Then by [3, Theorem A] there exists $y \in R$ with $\deg y < m$ such that $ay = ya$ $(a \in B)$ and $\sum_{j=0}^{m-1} Y_j y X^j \equiv 1 \pmod{fR}$. Since $b_i \in B^D$, we have

$(b_n)_r D^{*n} + (b_{n-1})_r D^{*n-1} + \ldots + (b_1)_r D^* = I_{b_0}{}^*$.

Then

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

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

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

Thus, f is $\tilde{D}$-separable by [3, Theorem 2.1].

References

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

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

[3] ________ : 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 ring III, Math. J. Okayama Univ., 15(1972), 149 - 162.

[5] ________ : On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ., 19(1976), 65 - 95.

[6] ________ : A note on separable polynomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ., 22(1980), 73 - 76.