<table>
<thead>
<tr>
<th>Title</th>
<th>On Separable Polynomials and Skew Polynomial Rings (Skew Polynomial Rings, Group Rings and Related Topics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>IKEHATA, SHUICHI</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (1981), 438: 15-22</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1981-09</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/102786">http://hdl.handle.net/2433/102786</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
ON SEPARABLE POLYNOMIALS IN SKEW POLYNOMIAL RINGS

Shuichi IKEHATA

Department of Mathematics, Okayama University

Throughout this paper, $B$ will mean a ring with 1, $\rho$ an automorphism of $B$, $D$ a $\rho$-derivation of $B$ (i.e. an additive endomorphism 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 $\rho$. 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 $\bar{\rho}$-separable (resp. $\bar{D}$-separable) polynomial. In this paper, we shall give some sufficient conditions for a separable polynomial to be $\bar{\rho}$-separable (resp. $\bar{D}$-separable). The study contains some generalizations of the results of [3].

We shall use the following conventions:

$Z = \text{the center of } B$, $C(A) = \text{the center of a ring } A$. 

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

\( u^*_x \) is the right multiplication effected by \( u \in B \).

\( I_u \) is the inner derivation effected by \( u \in B \);

\( I_u(a) = au - ua \).

\( \rho^* : B[X; \rho] + B[X; \rho] \) is the ring automorphism defined by \( \rho^*(\sum_i x^i d_i) = \sum_i x^i f(d_i) \).

\( D^* : B[X; D] \to B[X; D] \) 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 \( R(0) \wedge B^0[X] \) with \( \deg f = m \). First, we shall define the discriminant of \( f \). As was shown in [3, Remark 1.3], \( f \) is in \( C(B^0)[X] \). The free \( C(B^0) \)-module \( C(B^0)[X]/fC(B^0)[X] \) has a basis \( \{ 1, x, \ldots, x^{m-1} \} \), where \( x = X + fC(B^0)[X] \). Let \( \pi_i \) be the projection on to the coefficients of \( x^i \). The trace map \( \tau \) is defined by \( \tau(z) = \sum_{i=0}^{m-1} \pi_i(zx^i) (z \in C(B^0)[X]/fC(B^0)[X]) \). Then the discriminant \( \delta(f) \) of \( f \) is defined by \( \delta(f) = \det|\tau(x^k x^l)| \) \( (0 \leq k, l \leq m - 1) \).

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 \( k \geq 0 \), we put \( x^k = x^{m-1} b_{m-1} + x^{m-2} b_{m-2} + \ldots + db_1 + b_0 \) \( (b_i \in C(B^f)) \). Then, we have \( x^k \equiv x^{m-1} b_{m-1} + \ldots + X b_1 + b_0 \pmod{fr} \). Since \( ax^k = \ldots \)
\[ X^k \rho^k(a) \ (a \in B), \text{ we have } ab_i = b_i \rho^{k-i}(a) \text{ and so,} \]
\[ a \pi_i(x^k) = \pi_i(x^k) \rho^{k-i}(a) \ (0 \leq i \leq m-1). \]
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 \( f = x^m + x^{m-1}a_{m-1} + \ldots + Xa_1 + a_0 \) is a separable polynomial.

Then by [3, Theorem A], there exists \( y \in \mathbb{R} \) with \( \deg y < m \) such that \( \rho^{m-1}(a)y = ya \ (a \in B) \) and \( \sum_{j=0}^{m-1} Y_j X^j \equiv 1 \pmod{f \mathbb{R}} \), where \( Y_j = x^{m-j-1} + x^{m-j-2}a_{m-1} + \ldots + Xa_{j+2} + a_{j+1} \). 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 integer \( n \). Then \( f'(\sum_{k=0}^{n-1} \rho^k(y)u) = (\sum_{k=0}^{n-1} \rho^k(y)uf') \equiv nu \pmod{f \mathbb{R}} \).

**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 \( \rho^k(\sum_{k=0}^{n-1} \rho^k(y)u) = \sum_{k=0}^{n-1} \rho^k(y)u \). Then, noting \( Y_j \in C(B^\rho)[X] \) ([3, Lemma 1.2]) and \( f' = \sum_{j=0}^{m-1} Y_j x^j \), we obtain

\[ nu \equiv \sum_{j=0}^{m-1} Y_j (\sum_{k=0}^{n-1} \rho^k(y)u)x^j \]
\[ = f'(\sum_{k=0}^{n-1} \rho^k(y)u) = (\sum_{k=0}^{n-1} \rho^k(y)u)f' \pmod{f \mathbb{R}}. \]

**Corollary 1.3.** \( (f'\sum_{i=0}^{m-1} \rho^i(y)a_i = (\sum_{i=0}^{m-1} \rho^i(y)f')a_i \equiv (m-i)a_i \pmod{f \mathbb{R}}, \) for \( 0 \leq i \leq m-1. \)
Proof. Since $f \in R(0) \cap B^0[X]$, we have $a \in a_i^m - 1 (a \in B)$ 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 $R(0) \cap B^0[X]$. Assume that $f$ is separable. If there holds one the following conditions (1) - (6), then $f$ is $\overline{\rho}$-separable.

(1) There exists a regular element $u$ in $B$ and a positive integer $n$ which is invertible in $B$ such that $au = u^0(a)$ (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) $\rho|\mathbb{Z} = 1_{\mathbb{Z}}$ and $m - 1$ is invertible in $B$.

(5') $\rho|\mathbb{Z} = 1_{\mathbb{Z}}$ and $m$ is in $\text{rad} B$, the Jacobson radical of $B$.

(6) $\rho|\mathbb{Z} = 1_{\mathbb{Z}}$ and $a_1$ is in $\text{rad} B$.

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

Proof. Case (1). Let $v = u^0(u)\ldots\rho^{n-1}(u)$. Since $au = u^n(a)$ $(a \in B)$ and $\rho^n(u) = u$, we have $a^\overline{\nu}(u) = \rho^\overline{\nu}(u)\rho^n(a)$ 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 \( \overline{\delta} \)-separable.

Case (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 \( m a_0 \equiv f' z_1 a_0 \) and \( (m-1)a_1 \equiv f' z_2 a_1 \) (mod \( fR \)). Therefore, if both \( a_0 \) and \( a_1 \) are regular elements in \( B \), \( f' \) is invertible in \( R \) modulo \( fR \). Next, if \( m(m-1) \) is invertible in \( B \), then \( f' \) is invertible in \( R \) modulo \( fR \) since

\[
(m(m-1) \equiv f'(m-1)z_1 a_0 + mz_2 a_1 \beta \pmod{fR}).
\]

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

\[
_{j=0}^{m-1} y_j x^j = \sum_{j=0}^{m-1} y_j x^j \rho^{-j}(y) = \sum_{j=0}^{m-1} \rho^{m-1} v \rho^{-j}(y)
\]

\[
= a_1 y + \sum_{v=1}^{m-1} \rho^{-j}(c_\mu).
\]

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

\[
1 = a_1 c_0 + \sum_{v=1}^{m-1} \sum_{\mu=0}^{v} b_{\nu+1} a_{\nu+1} \rho^{-j}(c_\mu),
\]

where \( b_\nu \) is the constant term of \( x^\nu \) modulo \( fR \).
Since \( ab_{\nu+\mu} = b_{\nu+\mu} \rho^{\nu+\mu}(a) \), \( a_{\nu+1} = a_{\nu+1} \rho^{m-\nu-1}(a) \)
and \( \rho^{m-\nu-1}(a)c_{\mu} = c_{\mu}a \), we have \( b_{\nu+\mu}a_{\nu+1} \rho^{\nu+\mu}(c_{\mu}) \in \mathbb{Z} \).
Since \( b_{\nu+\mu}, a_{\nu+1} \in B^0 \) and \( \rho|Z = 1 \), we have
\[ b_{\nu+\mu}a_{\nu+1} \rho^{\nu+\mu}(c_{\mu}) = b_{\nu+\mu}a_{\nu+1}c_{\mu}. \]
Then we obtain
\[ l = a_1c_0 + \lambda_{\nu=1} \mu_{\nu=1}^{m-\nu-1} b_{\nu+\mu}a_{\nu+1}c_{\mu}. \]
It is easily verified that \( b_{\nu+\mu} = 0 \), \( (\nu+\mu) \leq m-1 \), and
\( b_{\nu+\mu} \in a_0B \), \( (\nu+\mu) \leq m \). 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 \( z \in \mathbb{R} \) such that \( l \equiv a_1c_0 + f'z \) (mod \( f \mathbb{R} \)).
Now, if \( a_1 \) is in \( \text{rad } B \), then \( f' \) is invertible
in \( R \) modulo \( f \mathbb{R} \).
Next, if \( m-1 \) is invertible in \( B \), then
\( m-1 \equiv (m-1)a_1c_0 + (m-1)f'z \) (mod \( f \mathbb{R} \)). Thus, \( f' \) is
invertible in \( R \) modulo \( f \mathbb{R} \) 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 \( R(0) \otimes B^0[X] \) is \( \tilde{\rho} \)-
separable.

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

**Corollary 1.6.** Assume that \( B \) is of prime char-
acteristic $p > 0$ and $\rho | Z = 1_Z$. Then a monic polynomial $g = X^p + X b_1 + b_0$ in $R(0)$ is separable if and only if $b_1$ is invertible in $B$.

Proof. First, we consider the case $p = 2$. Then by [3, Lemma 1.3], $g R = R g$ implies $\rho(b_0) = b_0$. Hence, if $g$ is separable then it is in $B^0[X]$ by [3, Proposition 3.1]. Since $a b_1 = b_1 \rho(a) (a \in B)$, 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 $g \in B^0[X]$. Thus, the assertion follows from Theorem 1.4. Next, we consider the case $p > 2$. Then by [3, Remark 1.4], $g R = R g$ implies $g \in B^0[X]$. 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 $(b_n)_D^n + (b_{n-1})_D^{n-1} + \ldots + (b_1)_D = I_{b_0}$ with some $b_1 \in B^D$. If $b_1$ is invertible in $B$, then every separable polynomial in $R$ is $\tilde{D}$-separable.

Proof. Let $f = X^m + X^{m-1} a_{m-1} + \ldots + X a_1 + a_0$ 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 $\sum_{j=0}^{m-1} y^j x^j \equiv 1 \pmod{fr}$. Since $b_1 \in B^D$, we have
\[(b_n)_r D^n + (b_{n-1})_r D^{n-1} + \ldots + (b_1)_r D^* = I_{b_0^*}.\]

Then
\[0 = y b_0 - b_0 y = \sum_{i=1}^{n} D^*_i (y) b_i = D^* (\sum_{i=1}^{n} D^*_{i-1} (y) b_i).\]

We put here \(u = \sum_{i=1}^{n} D^*_{i-1} (y) b_i.\) Then \(X u = u X\) and
\[Y_j u = u Y_j \quad ([3,\text{ Lemma }1.2]).\]

Therefore, we have
\[b_1 \equiv \sum_{j=0}^{m-1} Y_j (\sum_{i=1}^{n} D^*_{i-1} (y) b_i) X^j \equiv \sum_{j=0}^{m-1} Y_j u X^j = f' u = uf' \quad \text{(mod } f R).\]

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

References


