On generating elements of ideals in skew polynomial rings

Shūichi Ikehata* Atsushi Nakajima†

*Okayama University
†Okayama University

ON GENERATING ELEMENTS OF IDEALS IN SKEW POLYNOMIAL RINGS

Dedicated to Professor Kazuo Kishimoto on his 60th birthday

SHŪICHI IKEHATA and ATSUSHI NAKAJIMA

Let $K$ be a field, $\rho : K \to K$ an automorphism of order $n$, and $F = K^\rho = \{ a \in K \mid \rho(a) = a \}$ the fixed subfield of $K$ by $\rho$. Let $R = K[X; \rho]$ be the skew polynomial ring in which the multiplication is given by $aX = X\rho(a)$ ($a \in K$). As is well known that for any two-sided ideal $J$ in $R$, there exist a non-negative integer $i$ and a monic polynomial $h(t)$ in $F[t]$ such that $J = X^ih(X^n)R = RX^ih(X^n)$ ([5]). Thus for any polynomial $f$ in $R$, we ought to get the above $i$ and $h(t)$ such that $RfR = X^ih(X^n)R = RX^ih(X^n)$. How can we get such a non-negative integer $i$ and a polynomial $h(t)$ in $F[t]$ from $f$ explicitly?

In this paper, we shall show a systematic method to get such a polynomial $h(t)$ in $F[t]$ from $f$ (section 1). In section 2, we consider the similar problem for the skew polynomial ring of derivation type.

1. Automorphism type. Let $K$ be a field, $\rho : K \to K$ an automorphism of order $n$, $F = K^\rho = \{ a \in K \mid \rho(a) = a \}$ the fixed subfield of $K$ by $\rho$ and $R = K[X; \rho]$ the skew polynomial ring of automorphism type. In this section, for any monic polynomial $f$ in $R$, we will find a non-negative integer $i$ and a monic polynomial $h(t)$ in $F[t]$ such that $I = RfR = X^ih(X^n)R = RX^ih(X^n)$.

Let $f = X^n + X^{n-1}a_{m-1} + \cdots + X^i a_i \ (a_i \neq 0)$ be a monic polynomial in $R$. Since

$$f = X^i(X^m + X^{m-i-1}a_{m-1} + \cdots + a_i) = X^ig,$$

where $g = X^m + X^{m-i-1}a_{m-1} + \cdots + a_i$, we have

$$I = RfR = RX^igR = X^igR.$$

Therefore in the following, we assume that

$$f = X^n + X^{n-1}a_{m-1} + \cdots + Xa_1 + a_0 \ (a_0 \neq 0) \quad \text{and} \quad I = RfR.$$

First we prove an elementary lemma which is useful in our study.

This research is partially supported by Grant-in-Aid for Scientific Research (C) (No. 01540051), Ministry of Education, Science and Culture.
Lemma 1.1.
(1) If $X^\nu$ is in $I$ for some $\nu \geq 1$, then $I = R$.
(2) $RX^k + I = R$ for all $k \geq 1$.
(3) If $X^\nu g$ is in $I$ for some $\nu \geq 1$ and $g$ in $R$, then $g$ is in $I$.

Proof. (1) If $X^\nu$ is in $I$ for some $\nu \geq 1$, then

$$X^{\nu-1}f = X^{\nu+\nu-1} + X^{\nu+\nu-2}a_{\nu-1} + \cdots + X^\nu a_1 + X^{\nu-1}a_0 \in I$$

and so $X^{\nu-1}a_0$ is in $I$. Since $a_0$ is non-zero, we have $X^{\nu-1}$ is in $I$. Repeating these processes, we have $X^0 = 1$ is in $I$, i.e., $I = R$.

(2) Since the ideal $RX^k + I$ contains $X^k$ and $f$ for any $k \geq 1$, we have $RX^k + I = R$ by the similar way as in (1).

(3) By (2), $R = RX^\nu + I$ for any $\nu \geq 1$ and so there exist $u$ in $R$ and $\nu$ in $I$ such that $1 = uX^\nu + \nu$. Thus $g = uX^\nu g + \nu g$ is in $I$.

Lemma 1.2.
(1) $R = K[X; \rho] = K[X^n] \oplus XK[X^n] \oplus \cdots \oplus X^{n-1}K[K^n]$ as $K[X^n]$-modules.

(2) For any two-sided ideal $J$ in $R$,

$$J = (K[X^n] \cap J) \oplus (XK[X^n] \cap J) \oplus \cdots \oplus (X^{n-1}K[X^n] \cap J)$$

That is, for any $y$ in $J$, if $y = y_0 + y_1 + \cdots + y_{n-1}$, where $y_i$ are in $X^iK[X^n]$, then $y_i$ are in $J$ for any $0 \leq i \leq n-1$.

Proof. (1) is clear because $X^na = aX^n$ for any $a$ in $K$.

(2) Since $K/F$ is a $(\rho)$-Galois extension, then by [2, Th. 1.3], there exists a Galois coordinate system $\{a_j, b_j\}$ in $K$ such that

$$\sum_j a_j b_j = 1 \quad \text{and} \quad \sum_j \rho(\langle a_j \rangle) b_j = 0 \quad (1 \leq i \leq n-1).$$

Thus $\sum_j (a_j - \rho(\langle a_j \rangle)) b_j = 1$ for any $1 \leq i \leq n-1$. If $y_i$ is in $X^iK[X^n]$, then $ay_j = y_i \rho\langle a \rangle$ for any $a$ in $K$. Hence we have

$$J \ni ya - ay = \sum_{i=1}^{n-1} y_i (a - \rho(\langle a \rangle)).$$

Replace $a$ by $a_j$ in the above equation, we get

$$\sum_j \sum_{i=1}^{n-1} y_j (a_j - \rho(\langle a_j \rangle)) b_j = \sum_{i=1}^{n-1} y_i \in J.$$

Therefore $y_0 = y - \sum_{i=1}^{n-1} y_i$ is in $J$. Repeating these processes, we have $y_i$. 

http://escholarship.lib.okayama-u.ac.jp/mjou/vol33/iss1/4
are in \( J \) for any \( 1 \leq i \leq n-1 \).

Now we have the main theorem in this section.

**Theorem 1.3.** For any monic polynomial
\[
f = X^n + X^{n-1}a_{n-1} + \cdots + Xa_1 + a_0 \quad (a_0 \neq 0)
\]
in \( R = K[X; \rho] \), we can explicitly get a monic polynomial \( h(t) \) with non-zero constant term in \( F[t] \) such that
\[
I = RfR = Rh(X^n) = h(X^n)R.
\]

**Proof.** We divide the proof into two cases.

Case I. Assume that \( f \) is in \( F[X] \). If we set
\[
f = f_0 + Xf_1 + \cdots + X^{n-1}f_{n-1} \quad (f_i \in F[X^n]),
\]
then by Lemmas 1.1 and 1.2, \( f_i \) are in \( I \) for any \( 0 \leq i \leq n-1 \). We define \( f_i^* \) as follows:

- If \( f_i = 0 \), then \( f_i^* = 0 \).
- If \( f_i \neq 0 \), then \( f_i^* = f_i a_i^{-1} \), where \( a_i \) is the coefficient of the highest degree in \( f_i \).

Then \( f_i^*R = Rf_i^* \) (\( 0 \leq i \leq n-1 \)) and
\[
I = Rf_0^* + Rf_1^* + \cdots + Rf_{n-1}^*.
\]
The greatest common divisor of \( f_0^*, f_1^*, \ldots, f_{n-1}^* \), except zero polynomials is of the form \( h(X^n) \) for some \( h(t) \) in \( F(t) \) and in this case \( I = Rh(X^n) = h(X^n)R \). Thus \( h(X^n) \) is the requested one.

Case II. Assume that \( f \) is not in \( F[X] \). Since \( K/F \) is a Galois extension, then by [2, Lemma 1.6], there exists an element \( c \) in \( K \) such that
\[
tr(c) = c + \rho(c) + \cdots + \rho^{n-1}(c) = 1.
\]

We define the map \( \tau : K[X; \rho] \to F[X] \) as follows.
\[
\tau \left( \sum_{k} X^k d_k \right) = \sum_{k} X^k tr(d_k).
\]

Then \( \sum_{i=0}^{n-1} X^i f_X X^{n-i} = X^n \tau(f_X) \) is in \( I \) and by \( tr(c) = 1 \), \( \tau(f_X) \) is a monic polynomial in \( F[X] \) of degree \( n \). If we set \( \tau(f_X) = X^n g_1 \), where \( g_1 \) is in \( F[X] \) and the constant term of \( g_1 \) is non-zero, then by Lemma 1.1(3), \( g_1 \) is in \( I \). Now we have
\[ f - \tau(fc) = f - X^s g_1 \]
\[ = X^m(a_{m_1} - \tau(a_{m_1}c)) + \cdots + X^m(a_{m_r} - \tau(a_{m_r}c)) \]
\[ = X^{m_r} q_1 u_1, \]

where \( m > m_1 > \cdots > m_r \geq 0, a_{m_1}, a_{m_2}, \ldots, a_{m_r} \in F, a_{m_j} - \tau(a_{m_j}c) \neq 0 \) \((1 \leq j \leq r), u_1 = a_{m_1} - \tau(a_{m_1}c)\) and \( q_1 \) is a monic polynomial in \( K[X] \) of degree \((m_1 - m_r) < m\) with non-zero constant term. Using by Lemma 1.1(3) again, \( q_1 \) is in \( I \) and

\[ I = RfR = Rg_1 R + Rq_1 R. \]

If \( q_1 \) is in \( F[X] \), then we take \( g_2 = q_1 \), and since \( g_1, g_2 \) are in \( F[X] \) with non-zero constant term, we have by the Case I, there exist \( h_1(X^n) \) and \( h_2(X^n) \) such that

\[ Rg_1 R = Rh_1(X^n) R h_1(X^n) R = Rh_2(X^n) R h_2(X^n) R. \]

Thus if we take the greatest common divisor \( h(t) \) in \( F[t] \) of \( h_1(t) \) and \( h_2(t) \) in \( F[t] \), we have \( I = h(X^n) R = Rh(X^n) \). If \( q_1 \) is not contained in \( F[X] \), then repeating the similar method as above, we can get a finite set of polynomials \( g_1, g_2, \ldots, g_s \) in \( F[X] \cap I \) such that \( \deg g_1 > \deg g_2 > \cdots > \deg g_s \), each \( g_i \) has non-zero constant term and

\[ I = Rg_1 R + Rg_2 R + \cdots + Rg_s R. \]

By Case I, there exist monic polynomials \( h_1(X^n) \) in \( F[X^n] \) such that \( Rg_1 R = h_1(X^n) R = Rh_1(X^n) \). Thus if we take the greatest common divisor \( h(t) \) of \( h_1 \), then \( h(t) \) is the requested one.

**Corollary 1.4.** Let \( f_1, f_2, \ldots, f_r \) be any polynomials in \( R = K[X; \rho] \) and \( I = Rf_1 R + Rf_2 R + \cdots + Rf_r R \). Then we can find a monic polynomial \( h(t) \) in \( F[t] \) and a non-negative integer \( s \) such that \( I = X^s h(X^n) R = RX^s h(X^n) \).

**Proof.** It follows from Theorem 1.3 that there exist monic polynomials \( h_1(t), h_2(t), \ldots, h_r(t) \) with non-zero constant terms in \( F[t] \) and non-negative integers \( s_1, s_2, \ldots, s_r \) such that \( Rf_i R = X^{s_i} h_i(X^n) R = RX^{s_i} h_i(X^n) (1 \leq i \leq r) \). Then by Lemma 1.1, \( X^{s_i} R + h_i(X^n) R = R \) for all \( 1 \leq i, j \leq r \). Noting this, we can easily verify that \( I = X^s h(X^n) R = RX^s h(X^n) \), where \( s = \min \{ s_1, s_2, \ldots, s_r \} \) and \( h(t) \) is the greatest common divisor of \( h_1(t), h_2(t), \ldots, h_r(t) \).

**Example 1.5.** Let \( K \) be the complex number field and let \( \rho : K \to K \) be the automorphism defined by \( \rho(a + bi) = a - bi \). Let \( f = X^3 + X^4 + X^3 + X^2 + \)
$X+1$ and $g = X^4 + X^4 + 2X^2 + X^2 + X + 1$ be the polynomials in $R = K[X; \rho]$. Since $f = X(X^4 + X^2 + 1) + (X^4 + X^2 + 1)$, then by the proof of Th. 1.3,

$$RfR = (X^4 + X^2 + 1)R = R(X^4 + X^2 + 1).$$

On the other hand, since $g = X(X^4 + 2X^2 + 1) + (X^4 + X^2 + 1)$ and $X^4 + 2X^2 + 1$ and $X^4 + X^2 + 1$ are in $RgR$, we have

$$X^2 = (X^4 + 2X^2 + 1) - (X^4 + X^2 + 1) \in RgR.$$ 

Thus by Lemma 1.1(1), $RgR = R$.

2. Derivation type. Let $K$ be a field, $D : K \to K$ a non-zero derivation, $F = \{a \in K \mid D(a) = 0 \}$, the constant subfield of $K$ by $D$. Let $R = K[X; D]$ be the skew polynomial ring of derivation type in which the multiplication is given by $aX = Xa + D(a) (a \in K)$. If $K$ is of characteristic zero, then it is well known that $R$ is a simple ring (e.g. [3, Theorem 7.28]). If $K$ is of characteristic $p > 0$ and $[K : F] = n < \infty$, then it is easy to see that $n = p^e$. Then the ideal structure of $R$ is well known. Indeed, for any nonzero ideal $J$ of $R$, there exists a monic polynomial $g$ in $R$ such that $J = gR = Rg$ (e.g. [1]). However, for any monic polynomial $f$ in $R$, it may not be easy work to find a monic polynomial $g$ in $R$ such that $RfR = gR = Rg$. The purpose of this section is to show a method to get $g$ from $f$. In [4], one of the authors studied $H$-separable polynomials in skew polynomial rings, and some results in there will be used in this section.

In the following, we assume that $K$ is of characteristic $p > 0$, $[K : F] = p^e$, $f = X^m + X^{m-1}a_{m-1} + \cdots + Xa_1 + a_0 \in R = K[X; D]$ and $I = RfR$.

Then by [6, p. 190, ex. 3], the minimal polynomial of $D$ as a linear transformation in $K$ over $F$ is a $p$-polynomial of the form

$$t^{pe} + t^{pe-1}a_e + \cdots + t^p a_1 + t \alpha_1 (a_i \in F)$$

and $\text{Hom}(\rho K, \rho K) = K[D]$ (the subring generated by $D$ and the left multiplications of elements in $K$). We put here

$$\phi = X^{pe} + X^{pe-1}a_e + \cdots + X^p a_1 + X \alpha_1 \in R.$$ 

Then $\phi$ is contained in the center of $R$ and it is an $H$-separable polynomial in $R$ by [4, Theorem 3.3]. It follows from [4, Theorem 3.4] that for any monic polynomial $g$ in $R$ with $gR = Rg$, there exists a monic polynomial $h(t)$ in $F[t]$ such that $g = h(\phi)$. Hence we shall get explicitly $h(t)$ in $F[t]$ such that $I = h(\phi)R = Rh(\phi)$. 

Produced by The Berkeley Electronic Press, 1991
First, we shall prove the following

**Lemma 2.1.**

1. \( R = K[X; D] = K[\phi] \oplus XK[\phi] \oplus \cdots \oplus X^{p^e-1}K[\phi] \) as \( K[\phi] \)-modules.

2. For any two-sided ideal \( J \) in \( R \),

\[
J = (K[\phi] \cap J) \oplus X(K[\phi] \cap J) \oplus \cdots \oplus X^{p^e-1}(K[\phi] \cap J).
\]

That is, for any \( y \) in \( J \), if \( y = y_0 + xy_1 + \cdots + X^{p^e-1}y_{p^e-1} \), where \( y_i \) are in \( K[\phi] \), then \( y_i \) are in \( J \) for any \( 0 \leq i \leq p^e-1 \).

**Proof.** (1) Since \( \phi \) is contained in the center of \( R \), the result is clear.

(2) Since \( [K: F] = p^e \) and \( \text{Hom}(rK, rK) = K[D] \), it follows from [4, Theorem 3.3] that there exist \( c_j, d_j \in K \) such that

\[
\sum_j D^{p^e-1}(c_j)d_j = 1, \quad \sum_j D^k(c_j)d_j = 0 \quad (0 \leq k \leq p^e-2).
\]

Since \( aX^k = \sum_{\nu=0}^k X^\nu \binom{k}{\nu} D^{k-\nu}(a) \) and \( ay_t = y_t a \ (a \in K) \), we have

\[
J \ni ay - ya = a\left(\sum_{k=0}^{p^e-1} X^k y_k\right) - ya
\]

\[
= \sum_{k=0}^{p^e-1} \left(\sum_{\nu=0}^k X^\nu \binom{k}{\nu} D^{k-\nu}(a) y_k\right) - ya
\]

\[
= \sum_{\nu=0}^{p^e-1} X^\nu \left(\sum_{k=\nu+1}^{p^e-1} \binom{k}{\nu} D^{k-\nu}(a) y_k\right) - \left(\sum_{\nu=0}^{p^e-1} X^\nu y_\nu\right) a
\]

\[
= \sum_{\nu=0}^{p^e-1} X^\nu \left(\sum_{k=\nu+1}^{p^e-1} \binom{k}{\nu} D^{k-\nu}(a) y_k\right)
\]

for any \( a \) in \( K \). Replace \( a \) by \( c_j \) in the above equation, we get

\[
\sum_j \sum_{\nu=0}^{p^e-1} X^\nu \left(\sum_{k=\nu+1}^{p^e-1} \binom{k}{\nu} D^{k-\nu}(c_j) d_j y_k\right) = y_{p^e-1}
\]

is in \( J \). Repeating these processes, we have \( y_i \) are in \( J \) for any \( 0 \leq i \leq p^e-1 \).

Now we shall state the theorem

**Theorem 2.2.** For any monic polynomial
ON GENERATING ELEMENTS OF IDEALS IN SKEW POLYNOMIAL RINGS

\[ f = X^m + X^{m-1}a_{m-1} + \cdots + Xa_1 + a_0 \]

in \( R = K[X; D] \), we can explicitly get a monic polynomial \( h(t) \) in \( F[t] \) such that

\[ I = RfR = Rh(\phi) = h(\phi)R. \]

Proof. We divide the proof into two cases.

Case I. Assume that \( f \) is in \( F[X] \). If we set \( f = f_0 + Xf_1 + \cdots + X^{p^e-1}f_{p^e-1} \) (\( f_i \in F[\phi] \)), then by Lemma 2.1, \( f_i \) are in \( I \) for any \( 0 \leq i \leq p^e-1 \). We define \( f_i^* \) as follows:

- If \( f_i = 0 \), then \( f_i^* = 0 \).
- If \( f_i \neq 0 \), then \( f_i^* = f_i b_i^{-1} \), where \( b_i \) is the coefficient of highest degree in \( f_i \).

Then \( f_i^* R = Rf_i^* (0 \leq i \leq p^e-1) \) and

\[ I = Rf_0^* + Rf_1^* + \cdots + Rf_{p^e-1}^*. \]

The greatest common divisor of \( f_0^*, f_1^*, \ldots, f_{p^e-1}^* \) except zero polynomials is of the form \( h(\phi) \) for some monic polynomial \( h(t) \) in \( F[t] \) and in this case \( I = Rh(\phi) = h(\phi)R \). Thus \( h(\phi) \) is the requested one.

Case II. Assume that \( f \) is not in \( F[X] \). Let \( tr : K \rightarrow K \) be the map defined by \( tr(a) = \sum_{i=0}^{p-1} a f_{i}^{1/p^e} D^{p^e-1-i}(a) (a \in K) \). Since \( t^{p^e} + t^{p^{e-1}}a_0 + \cdots + t^a \) is the minimal polynomial of \( D \) over \( F \), we have \( Dtr = 0 \) and there exists an element \( d \) in \( K \) such that \( tr(d) \neq 0 \). Hence \( tr(K) \) is contained in \( F \) and \( tr(c) = 1 \), where \( c = tr(d)^{-1}d \). We define a map \( \tau : K[X; D] \rightarrow F[X] \) as follows:

\[ \tau(\sum_k X^k d_k) = \sum_k X^k tr(d_k). \]

Since any ideal \( J \) in \( R \) is \( D \)-invariant, we know that \( J \) is also \( \tau \)-invariant. Hence \( \tau(fc) \) is a monic polynomial in \( F[X] \cap I \) of degree \( m \). We set here \( g_1 = \tau(fc) \). Then we have

\[ f - \tau(fc) = f - g_1 \]

\[ = X^{m_1}(a_{m_1} - \tau(a_{m_1}c)) + \cdots + X^{m_t}(a_{m_t} - \tau(a_{m_t}c)) \]

where \( m > m_1 > \cdots > m_r \geq 0, a_{m_1}, a_{m_2}, \ldots, a_{m_t} \in F, a_{m_j} - \tau(a_{m_j}c) \neq 0 (1 \leq j \leq r) \), \( u_i = a_{m_i} - \tau(a_{m_i}c) \) and \( q_1 \) is a monic polynomial in \( K[X] \cap I \) of degree \( m_1 < m \). Then we have

\[ I = RfR = Rg_1R + Rq_1R. \]

If \( q_1 \) is in \( F[X] \), then we take \( g_2 = q_1 \), and since \( g_1, g_2 \) are in \( F[X] \), we have by the Case I, there exist \( h_1(\phi) \) and \( h_2(\phi) \) such that

\[ Rg_1R = Rh_1(\phi)R = h_1(\phi)R \quad \text{and} \quad Rg_2R = Rh_2(\phi)R = h_2(\phi)R. \]
Thus we take the greatest common divisor \( h(t) \) of \( h_1(t) \) and \( h_2(t) \) in \( F[t] \), we have \( I = h(\phi)R = Rh(\phi) \). If \( q_1 \) is not contained in \( F[X] \), then repeating the similar method as above, we can get a finite set of polynomials \( g_1, g_2, \ldots, g_s \) in \( F[X] \cap I \) such that \( \deg g_1 > \deg g_2 > \cdots > \deg g_s \) and

\[
I = Rg_1R + Rg_2R + \cdots + Rg_sR.
\]

By Case I, there exist monic polynomials \( h_i(t) \) in \( F[t] \) such that \( Rg_iR = h_i(\phi)R = Rh_i(\phi) \). Thus if we take the greatest common divisor \( h(t) \) of \( h_1(t), h_2(t), \ldots, h_s(t) \), then \( h(t) \) is the requested one.

**Corollary 2.3.** Let \( f_1, f_2, \ldots, f_r \) be any polynomials in \( R = K[X; D] \) and \( I = Rf_1R + Rf_2R + \cdots + Rf_rR \). Then we can find a monic polynomial \( h(t) \) in \( F[t] \) such that \( I = h(\phi)R = Rh(\phi) \).

**Proof.** In fact, it follows from Theorem 2.2 that there exist \( h_i(t) \) in \( F[t] \) such that \( Rf_iR = h_i(\phi)R = Rh_i(\phi) \) \((1 \leq i \leq r) \). Then the greatest common divisor \( h(t) \) of \( h_1(t), h_2(t), \ldots, h_s(t) \) is the desired one.

We shall conclude our study with the following example.

**Example 2.4.** Let \( k \) be a field of odd prime characteristic \( p, K = k(y) \) the rational function field over \( k \), and

\[
D = \frac{d}{dy} \quad \text{a derivation of } K,
\]

and \( R = K[X; D] \). Then \( F = K^p = k(y^p) \). By Hochschild’s formula [6, p. 191 ex. 15], we have

\[
D^p = \left( \frac{d}{dy} \right)^p = y^p \left( \frac{d}{dy} \right)^p + \left( y \frac{d}{dy} \right)^{p-1} \frac{d}{dy} = y^p \frac{d}{dy} = D.
\]

Hence \( t^p - t \) is the minimal polynomial of \( D \) over \( F \).

Let \( f_1 = X^p - 2X^p + X, f_2 = X^p - 2X^p + 2X, \) and \( f_3 = X^p - X^p(y + 1) + Xy \) be in \( R \). Then we have \( f_1 = (X^p - X)^p - (X^p - X), f_2 = (X^p - X)^p - (X^p - X) + X, \) and \( f_3 = (X^p - X)^p - (X^p - X)y \). In virtue of Theorem 2.2, we can obtain \( Rf_1R = Rf_1 = f_1R, Rf_2R = R \) and \( Rf_3R = R(X^p - X) = (X^p - X)R \).

**References**

112.


DEPARTMENT OF MATHEMATICS
COLLEGE OF LIBERAL ARTS AND SCIENCES
OKAYAMA UNIVERSITY
2-1-1 TSUSHIMA-NAKA, OKAYAMA 700, JAPAN

(Received October 15, 1990)