Math. J. Okayama Univ. 25 (1983), 43—48

NOTE ON SKEW POLYNOMIALS

TAKASI NAGAHARA

Let B be an arbitrary ring with identity element 1, and $B[X;\rho]$ a skew polynomial ring $\sum_{i=0}^{\infty} X^iB$ whose multiplication is given by $aX = X\rho(a)$ $(a \in B)$ where ρ is an automorphism of B. A monic polynomial $f \in B[X;\rho]$ is called to be *separable* (resp. *Frobenius*) if $fB[X;\rho] = B[X;\rho]f$ and the factor ring $B[X;\rho]/fB[X;\rho]$ is separable (resp. Frobenius) over B. Such polynomials have been discussed in [2]—[11] from various angles.

The present study is more about separable (and Frobenius) polynomials in $B[X;\rho]$ which are closely associated with some results in [3], [4], [8] and [9].

We begin our study by stating the following lemma which contains the result of [9, Lemma 1].

Lemma 1. *Let* $f = X^n - \sum_{i=0}^{n-1} X^i a_i \in B[X;\rho]$ $(n \geq 2)$, *and* $fB[X;\rho] = B[X;\rho]f$. *Then*

(i) $a\rho^t(a_i) = \rho^t(a_i)\rho^{n-i}(a)$ $(0 \leq i \leq n-1$ *and* $a \in B)$ *for any integer* t.

(ii) $\rho^{n-1-i}(a_i) = a_i$ $(0 \leq i \leq n-1)$.

(iii) $\rho(a_i^s) = a_i^s$ $(0 \leq i \leq n-1)$ *for any integer* $s \geq 2$.

Proof. By [9, Lemma 1], it suffices to prove the assertion (iii). Now, by (1) and (ii), we have

$$a_i^2 = a_i\rho^{n-i}(a_i) = a_i\rho(a_i) = \rho(a_i)\rho^{n-i}(a_i) = \rho(a_i)\rho(a_i) = \rho(a_i^2)$$

where $0 \leq i \leq n-1$. Hence, for any positive integer m, we have that $a_i^{2m} = \rho(a_i^{2m})$, and

$$a_i^{2m+1} = a_i\rho(a_i)\rho(a_i)^{2m-1} = \rho(a_i)\rho(a_i)\rho(a_i)^{2m-1} = \rho(a_i)^{2m+1}$$

which implies our assertion.

Moreover, we can prove the next that contains the results of [8, Th. 1 (*b*)] and [11, pp. 10—11 (Remark)].

Lemma 2. *Let* $f = X^n - \sum_{i=0}^{n-1} X^i a_i$ $(n \geq 2)$ *be a separable polynomial in* $B[X;\rho]$. *Then*

$$\rho^{(n-1,i)}(a_i) = a_i \quad (0 \leq i \leq n-1)$$

where $(n-1, i)$ *is the greatest common divisor of* $n-1$ *and* i.

Proof. From the proof of [9, Lemma 1], it follows that

$$(1)\qquad a_i\rho(a_{n-1})-a_ia_{n-1}=a_{i-1}-\rho(a_{i-1})\quad(1\le i\le n-1)$$
$$a_0\rho(a_{n-1})=a_0a_{n-1},\text{ and }a_ia_{n-1}=a_{n-1}a_i\quad(0\le i\le n-1).$$

Hence by Lemma 1 (i), we have

$$(2)\quad a_i\rho(a_{n-1})=\rho(a_{n-1})\rho(a_i)=\rho(a_{n-1}a_i)=\rho(a_ia_{n-1})\quad(0\le i\le n-1).$$

By (1), this gives that

$$\rho(a_1a_{n-1})-a_1a_{n-1}=a_0-\rho(a_0).$$

Since $\rho^{n-1}(a_0)=a_0$ (Lemma 1 (ii)), it follows that

$$\begin{aligned}\rho^{n-1}(a_1a_{n-1})-a_1a_{n-1}&=\textstyle\sum_{s=0}^{n-2}(\rho^{s+1}(a_1a_{n-1})-\rho^s(a_1a_{n-1}))\\&=\textstyle\sum_{s=0}^{n-2}(\rho^s(a_0)-\rho^{s+1}(a_0))=0.\end{aligned}$$

Combining this with (2) and Lemma 1 (ii), we obtain

$$\begin{aligned}a_1a_{n-1}&=\rho^{n-1}(a_1a_{n-1})=\rho^{n-2}(\rho(a_1a_{n-1}))\\&=\rho^{n-2}(a_1\rho(a_{n-1}))=a_1\rho^{n-1}(a_{n-1}).\end{aligned}$$

Moreover, by (1), (2) and Lemma 1 (ii), we have

$$a_0a_{n-1}=a_0\rho(a_{n-1})=\rho(a_0a_{n-1})=\rho^{n-1}(a_0a_{n-1})=a_0\rho^{n-1}(a_{n-1}).$$

Since $Ba_0+Ba_1=B$ ([2, Lemma 1]), it follows that

$$(3)\qquad \rho^{n-1}(a_{n-1})=a_{n-1}.$$

Now, let $2\le r\le n-1$. Then, by (2), there holds that $\rho(a_ra_{n-1})=a_r\rho(a_{n-1})$. We assume here that

$$\rho(a_0a_{n-1})=\rho^t(a_r)\rho^{1-t(r-1)}(a_{n-1})$$

for some integer $t\ge 0$. Then, by Lemma 1 and (3), we have

$$\begin{aligned}\rho(a_ra_{n-1})&=\rho^t(a_r)\rho^{1-t(r-1)}(a_{n-1})=\rho^{1-t(r-1)}(a_{n-1})\rho^{t+1}(a_r)\\&=\rho^{t+1}(a_r)\rho^{1-t(r-1)+n-r}(a_{n-1})=\rho^{t+1}(a_r)\rho^{n-(t+1)(r-1)}(a_{n-1})\\&=\rho^{t+1}(a_r)\rho^{1-(t+1)(r-1)}(a_{n-1}).\end{aligned}$$

Hence, by induction method, we obtain that

$$\rho(a_ra_{n-1})=\rho^m(a_r)\rho^{1-m(r-1)}(a_{n-1})$$

for all integer $m\ge 0$. Taking $m=n-1$, it follows from Lemma 1 and (3) that

$$\begin{aligned}\rho(a_ra_{n-1})&=\rho^{n-1}(a_r)\rho^{1-(n-1)(r-1)}(a_{n-1})=\rho^{n-1}(a_r)\rho(a_{n-1})\\&=\rho^{1-(n-r)}(a_{n-1})\rho^{n-1}(a_r)=\rho^r(a_{n-1})\rho^{n-1-r+r}(a_r)\\&=\rho^r(a_{n-1})\rho^r(a_r)=\rho^r(a_{n-1}a_r)\end{aligned}$$

and hence $a_r a_{n-1} = \rho^{r-1}(a_r a_{n-1})$ (by (1)). Since

$$a_{r-1} - \rho(a_{r-1}) = \rho(a_r a_{n-1}) - a_r a_{n-1} \quad \text{(by (1) and (2))}$$

this gives

$$\begin{aligned} a_{r-1} - \rho^{r-1}(a_{r-1}) &= \sum_{s=0}^{r-2} (\rho^s(a_{r-1}) - \rho^{s+1}(a_{r-1})) \\ &= \sum_{s=0}^{r-2} (\rho^{s+1}(a_r a_{n-1}) - \rho^s(a_r a_{n-1})) = 0. \end{aligned}$$

Thus, we obtain $\rho^i(a_i) = a_i (1 \leq i \leq n-2)$. Moreover $\rho^i(a_i) = a_i$ for $i = 0$ and $n-1$ (by (3)). Since $\rho^{n-1-i}(a_i) = a_i$ for $i = 0, 1, \cdots, n-1$ (Lemma 1 (ii)), it follows that $\rho^{(n-1,i)}(a_i) = a_i (0 \leq i \leq n-1)$, completing the proof.

Now, for $g = \sum_{i=0}^{m} X^i b_i \in B[X;\rho]$, B_g denotes the subring of B which is generated by the subset

$$\{\rho^t(b_i) \mid 0 \leq i \leq m, \text{ and } t \text{ runs over all the integers}\} \cup \{1\}.$$

Clearly $B_g[X;\rho|B_g]$ is a subring of $B[X;\rho]$ containing g. Moreover, by $J(\rho^s)$ (resp. $B(\rho^s)$), we denote the fixed subring of ρ^s in B (resp. the subset of elements b in B such that $ab = b\rho^s(a)$ for all $a \in B$), where s is an integer. Evidently $B(\rho^0)$ is the center of B. Further, by ρ^*, we denote a ring automorphism of $B[X;\rho]$ defined by $\rho^*(\sum_i X^i a_i) = \sum_i X^i \rho(a_i)$ $(a_i \in B)$. Clearly, the fixed subring $J(\rho^{*s})$ of ρ^{*s} in $B[X;\rho]$ coincides with the subring $J(\rho^s)[X;\rho|J(\rho^s)]$. For a subring B_0 of B and for $f \in B[X;\rho]$, f is called to be separable (resp. Frobenius) over B_0 if $B_0 \ni 1$, $\rho(B_0) = B_0$, and f is a separable (resp. Frobenius) polynomial in $B_0[X;\rho|B_0]$.

If f is a separable polynomial in $B[X;\rho]$ of degree $n \geq 2$ then $B_f \subset J(\rho^{n-1})$ by virtue of Lemma 2. Hence by [5, Prop. 1.13], we readily obtain the following theorem which is one of our main results.

Theorem 3. *If f is a separable polynomial in $B[X;\rho]$ of degree $n \geq 2$, then f is Frobenius over B_f and over $J(\rho^{n-1})$.*

Next, we shall prove the following lemma which contains the result of [3, Prop. 3.2].

Lemma 4. *Assume that $B[X;\rho]$ contains a separable polynomial of degree $n \geq 2$. Then $J(\rho^{n(n-1)}) \supset B(\rho^s)$ for all integer s. Moreover, for $g \in B[X;\rho]$, if $ag = g\rho^s(a)$ $(a \in B)$ for some integer s, then g is contained in $J(\rho^{*n(n-1)})$.*

Proof. Let $f = X^n - \sum_{i=0}^{n-1} X^i a_i$ be a separable polynomial in $B[X;\rho]$ $(n \geq 2)$. In case $n = 2$, we have $\rho(a_0) = a_0$ (Lemma 2). Combining this

and the result of Lemma 1(iii), we see that $\rho(a_1^n) = a_1^n$ and $\rho(a_0^{n-1}) = a_0^{n-1}$ for $n \geq 2$. Now, let $c \in B(\rho^s)$ where s is an integer. Then

$$a_1^n c = c\rho^s(a_1^n) = ca_1^n \text{ and } a_0^{n-1}c = c\rho^s(a_0^{n-1}) = ca_0^{n-1}.$$

Since $\rho^{n(n-1)}(c) \in B(\rho^s)$ and $a_i \in B(\rho^{n-i})$ for $i = 0, 1$ (Lemma 1(i)), this gives

$$\rho^{n(n-1)}(c)a_1^n = a_1^n\rho^{n(n-1)}(c) = ca_1^n \text{ and}$$
$$\rho^{n(n-1)}(c)a_0^{n-1} = a_0^{n-1}\rho^{n(n-1)}(c) = ca_0^{n-1}.$$

Now by [2, Lemma 1], we have $a_1B + a_0B = B$ and whence $a_1^nB + a_0^{n-1}B = B$. Therefore, it follows that $\rho^{n(n-1)}(c) = c$. This proves $B(\rho^s) \subset J(\rho^{n(n-1)})$. As to the rest of our assertion, let $g = \sum_{i=0}^m X^i b_i \in B[X;\rho]$ and $ag = g\rho^s(a)$ $(a \in B)$ for some integer s. Then $\rho^i(a)b_i = b_i\rho^s(a)$, that is, $ab_i = b_i\rho^{s-i}(a)$ $(a \in B)$. Hence $b_i \in B(\rho^{s-i}) \subset J(\rho^{n(n-1)})$ $(0 \leq i \leq m)$. This implies $g \in J(\rho^{*n(n-1)})$, completing the proof.

Now, let $f = X^n - \sum_{i=0}^{n-1} X^i a_i$ be a separable polynomial in $B[X;\rho]$ $(n \geq 2)$, and $f_i = X^{n-i-1} - X^{n-i-2}a_{n-1} - \cdots - Xa_{i+2} - a_{i+1}$ $(0 \leq i \leq n-1)$. Then, by [4, Th. 1.8], there is an element y in $B[X;\rho]$ such that deg $y < n$, $\rho^{n-1}(a)y = ya$ $(a \in B)$, and $\sum_{i=0}^{n-1} f_i y X^i \equiv 1 \pmod{fB[X;\rho]}$. Then, by Lemma 4, the f_i and y are contained in $J(\rho^{*n(n-1)})$, and $\sum_{i=0}^{n-1} f_i y X^i \equiv 1 \pmod{fJ(\rho^{*n(n-1)})}$. Hence, again by [5, Th. 1.8], we obtain the following

Theorem 5. *Assume that $B[X;\rho]$ contains a separable polynomial of degree $n \geq 2$. Then, any separable polynomial in $B[X;\rho]$ is separable over $J(\rho^{n(n-1)})$.*

In virtue of Th. 5, we shall prove the following

Corollary 6. *Let f be a separable polynomial in $B[X;\rho]$ of degree $n \geq 2$, and assume that n is inversible in B. Then f is separable and Frobenius over $J(\rho^{n-1})$.*

Proof. By Th. 3, it suffices to prove that f is separable over $J(\rho^{n-1})$. Now, by Th. 5 and [5, Th. 1.8], there is an element y in $J(\rho^{*n(n-1)})$ such that deg $y < n$, $\rho^{n-1}(a)y = ya$ $(a \in J(\rho^{n(n-1)})$, and $\sum_{i=0}^{n-1} f_i y X^i \equiv 1 \pmod{fJ(\rho^{*n(n-1)})}$. Since $f \in J(\rho^{*n-1})$, the f_i are contained in $J(\rho^{*n-1})$. We set here $y_0 = n^{-1}\sum_{i=0}^{n-1} (\rho^{*n-1})^i(y)$. Then, we obtain

$$\sum_{i=0}^{n-1} f_i y_0 X^i = n^{-1}\sum_{i=0}^{n-1} (\rho^{*n-1})^i(\sum_{i=0}^{n-1} f_i y X^i) \equiv 1 \pmod{fJ(\rho^{*n-1})}$$

and $\rho^{n-1}(a)y_0 = y_0 a$ $(a \in J(\rho^{n-1}))$. Therefore, it follows from [5, Th. 1.8]

that f is separable over $J(\rho^{n-1})$, completing the proof.

Now, for a monic polynomial g in $B[X;\rho]$ with $gB[X;\rho] = B[X;\rho]g$ and $\rho^*(g) = g$, g will be called to be *s-separable* (or *$\tilde{\rho}$-separable*) over B if the discriminant of g (as an element of $B_g[X]$ in the sense of [6, p. 152]) is inversible in B, or equivalently, $gB[X;\rho]+g'B[X;\rho] = B[X;\rho]$ where g' is the derivative of g (cf. Lemma 1, [3, Th. 2.1], [4] and [6, Th. 2.1]). By [3, pp. 118—119], any s-separable polynomial is separable. The notion is useful to Galois theory of polynomials. If $g \in B[X;\rho]$ is s-separable then the factor ring $B[X;\rho]/gB[X;\rho]$ can be imbedded in a Galois extension of B which is a splitting ring of g. The converse holds for a monic $g \in B[X;\rho]$ with deg $g = 2$ and $gB[X;\rho] = B[X;\rho]g$ (cf. [6], [7], [8] and [10]). If $B = \mathrm{GF}(2^2)$ and ρ is an automorphism of B which is not identity, then $B[X;\rho]$ contains a separable polynomial of degree 2 which is ρ^*-invariant but is not s-separable (cf. [7, Remark 2.4]).

We shall now prove the following theorem which is a partial sharpening of the last result in [4, Th. 1.4].

Theorem 7. *Assume that $B[X;\rho]$ contains a separable polynomial of degree $n \geq 2$, and $n(n-1)$ is inversible in B. Then, any separable polynomial g in $B[X;\rho]$ with $\rho^*(g) = g$ is s-separable, and whence Frobenius.*

Proof. Let deg $g = m$. Then, by Th. 5 and [5, Th. 1.8], there is an element $y \in J(\rho^{*n(n-1)})$ such that $\sum_{i=0}^{m-1} g_i y X^i \equiv 1 \pmod{gJ(\rho^{*n(n-1)})}$. Clearly $g_i \in J(\rho^*)$ $(0 \leq i \leq n-1)$. We set here $y_0 = (n^2-n)^{-1}\sum_{i=1}^{n(n-1)} \rho^{*i}(y)$. Then $\sum_{i=0}^{m-1} g_i y_0 X^i \equiv 1 \pmod{gJ(\rho^{*n(n-1)})}$. Since $\rho^*(y_0) = y_0$, we have $\sum_{i=0}^{m-1} g_i y_0 X^i = (\sum_{i=0}^{m-1} g_i X^i) y_0 = g' y_0$. Therefore, it follows that $gB[X;\rho]+g'B[X;\rho] = B[X;\rho]$. This implies that g is s-separable in $B[X;\rho]$, completing the proof.

Now, an element a of B is said to be π-regular (resp. left π-regular) if there exists an element c in B and an integer $t > 0$ such that $a^t c a^t = a^t$ (resp. $ca^t = a^{t-1}$). If every element of B is π-regular then B will be called to be π-regular. Let B satisfy the descending chain condition on two-sided ideals, and z any element of the center Z of B. Then $Bz^t = Bz^{2t}$ for some integer $t > 0$ and $z^t = cz^{2t}$ for some $c \in Z$ (see, e.g., [1, Lemma 1]). Thus z is π-regular in Z. This implies that Z is a π-regular ring.

Finally, we shall prove the following theorem which is a generalization of [9, Th. 5].

Theorem 8. *Let the center of B be π-regular. Then, any separable polynomial in $B[X;\rho]$ is Frobenius.*

Proof. Let $f = X^n - \sum_{i=0}^{n-1} X^i a_i$ be a separable polynomial in $B[X;\rho]$ $(n \geq 2)$. Then, by [2, Lemma 1], there are elements d_0 and d_1 in B such that $1 = a_0d_0 + a_1d_1$ and the a_id_i are contained in the center Z of B. We set here

$$N(a_0b_0) = \prod_{i=1}^{n(n-1)} \rho^i(a_0d_0) = a_0b_0, \text{ and}$$
$$1 = \prod_{i=1}^{n(n-1)} \rho^i(a_0d_0 + a_1d_1) = a_0b_0 + a_1b_1$$

where $b_0, b_1 \in B$. Since a_0b_0 $(\in Z)$ is π-regular, there exists some integer $t > 0$ and an idempotent e_0 in Z such that $(a_0b_0)^tZ = (a_0b_0)^{t-1}Z = e_0Z$. Evidently $e_0a_0B = e_0B$. We put $e_1 = 1 - e_0$. Then, since $1 = (a_0b_0 + a_1b_1)^t = (a_0b_0)^t + a_1c_1$ for some $c_1 \in B$, we see that $B = e_0B + a_1B$, and so, $e_1B = e_1a_1B$. Hence $B = e_0B \oplus e_1B = e_0a_0B \oplus e_1a_1B$ (direct sum). This shows that e_0a_0 is inversible in e_0B and e_1a_1 is inversible in e_1B. Now, by Lemma 4, we have $\rho^{n(n-1)}(a_0d_0) = a_0d_0$, which implies that $\rho(a_0b_0) = a_0b_0$, and so, $\rho(e_i) = e_i$ $(i = 0, 1)$. Since f is separable over B, each e_if is separable in $R_i = e_iB[X;\rho|e_iB]$. Hence, by [2, Th. 1], each e_if is Frobenius in R_i. Noting

$$B[X;\rho]/fB[X;\rho] \simeq R_0/e_0fR_0 \oplus R_1/e_1fR_1$$

it follows that f is Frobenius. This completes the proof.

REFERENCES

[1] G. AZUMAYA: Strongly π-regular rings, J. Fac. Sci. Hokkaido Univ. Ser. I, 13 (1954), 34—39.

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

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

[4] S. IKEHATA: On separable polynomials and Frobenius polynomials in skew polynomial rings. II, Math. J. Okayama Univ. 25 (1983), 23—28.

[5] Y. MIYASHITA: On a skew polynomial ring, J. Math. Soc. Japan 31 (1979), 317—330.

[6] T. NAGAHARA: On separable polynomials over a commutative ring II, Math. J. Okayama Univ. 15 (1972), 149—162.

[7] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. 19 (1976), 65—95.

[8] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings II, Math. J. Okayama Univ. 21 (1979), 167—177.

[9] T. NAGAHARA: A note on separable polyomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ. 22 (1980), 73—76.

[10] T. NAGAHARA: On imbeddings of some separable extensions in Galois extensions, Sûrikaikaisekikenkyûsho Kôkyûroku 438 (1981), 29—30.

[11] T. NAGAHARA and K. KISHIMOTO: On free cyclic extensions of rings, Proc. 10 th Symp. Ring Theory (Shinshu Univ., Matsumoto, 1977), 1978, 1—25.

DEPARTMENT OF MATHEMATICS, OKAYAMA UNIVERSITY

(Received December 2, 1982)