Math. J. Okayama Univ. 22 (1980), 61–64

ON SEPARABLE POLYNOMIALS OF DEGREE 2 IN SKEW POLYNOMIAL RINGS III

Dedicated to Prof. Gorô. Azumaya on his 60th birthday

TAKASI NAGAHARA

Throughout this paper, B will mean a (non-commutative) ring with identity element 1 which has an automorphism ρ and a derivation D so that $\rho D=D\rho$ and $D(ab)=D(a)\rho(b)+aD(b)$ $(a,\ b\in B)$. By $B[X;\rho,\ D]$, we denote the ring of all polynomials $\sum_i X^i b_i$ $(b_i\in B)$ with an indeterminate X whose multiplication is given by $bX=X\rho(b)+D(b)$ $(b\in B)$. For a monic polynomial $f\in B[X;\rho,\ D]$, if $fB[X;\rho,\ D]=B[X;\rho,\ D]f$ and the factor ring $B[X;\rho,\ D]/fB[X;\rho,\ D]$ is separable (resp. Galois (resp. Frobenius)) over B then f will be called to be separable (resp. Galois (resp. Frobenius)). Moreover, by $B[X;\rho,\ D]_2$, we denote the subset of $B[X;\rho,\ D]$ of all polynomials $f=X^2-Xa-b$ with $fB[X;\rho,\ D]=B[X;\rho,\ D]f$.

The purpose of this note is to study separable polynomials in $B[X;\rho,\ D]_2$ under the condition $2^nB=2^{n+1}B$ for some integer $n\geq 0$ (Ths. 2 and 3). Obviously, this condition is fulfilled if B satisfies the descending chain condition on two-sided ideals.

As to notations and terminologies used here we follow the previous one [4].

Now, let α be an element in B such that $\rho(\alpha)=\alpha$, $D(\alpha)=0$, $\alpha B=B\alpha$, and $\alpha^nB=\alpha^{n+1}B$ for some integer $n\geq 0$. Then the annihilator $\mathrm{Ann}(\alpha^n)$ of α^n in B is a two-sided ideal of B. Since $\alpha^nB=\alpha^{2n}B$ and $\mathrm{Ann}(\alpha^n)=\mathrm{Ann}(\alpha^{2n})$, it follows that $B=\alpha^nB\oplus\mathrm{Ann}(\alpha^n)$ (direct sum). Here we write $1=e_1+e_2$ where $e_1\in\alpha^nB$ and $e_2\in\mathrm{Ann}(\alpha^n)$. Then the e_i are central idempotents of B which are orthogonal. Moreover $e_1B=\alpha^nB$ and $e_2B=\mathrm{Ann}(\alpha^n)$. Since $\rho(\alpha^nB)=\alpha^nB$ and $D(\alpha^nB)\subset\alpha^nB$, we have $\rho(e_1)=e_1$ and $D(e_1)=0$. This shows that $\rho(e_2)=e_2$ and $D(e_2)=0$. Hence $\rho(e_2B)=e_2B$ and $D(e_2B)\subset e_2B$. Thus, if $B\supsetneq\alpha^nB\supsetneq\{0\}$ then we have that for $f\in B[X;\rho,\ D]$,

$$e_if\in e_iB[X;\ \rho|e_iB,\ D|e_iB]\quad(i=1,2)$$

where $\rho|e_iB$ and $D|e_iB$ are restrictions of ρ and D to e_iB respectively. In this paper, we denote e_i by $e_i(\alpha)$ $(i=1,\ 2)$.

First, we shall prove the following

Lemma 1. *Let α be an element in B such that $\rho(\alpha)=\alpha$, $D(\alpha)=0$, $\alpha B=B\alpha$, and $B \supsetneq \alpha^n B=\alpha^{n+1}B \supsetneq \{0\}$ for some integer $n \geq 0$.*

(i) *For $f \in B[X;\ \rho,\ D]$, f is separable (resp. Frobenius) if and only if each $e_i(\alpha)f$ is separable (resp. Frobenius) in $e_i(\alpha)B[X;\ \rho|e_i(\alpha)B,\ D|e_i(\alpha)B]$.*

(ii) *For $f \in B[X;\ \rho,\ D]$ of degree 2, f is Galois if and only if each $e_i(\alpha)f$ is Galois in $e_i(\alpha)B[X;\ \rho|e_i(\alpha)B, D|e_i(\alpha)B]$.*

Proof. We set $B_i=e_i(\alpha)B$, $f_i=e_i(\alpha)f$, and

$$A_i = B_i[X;\ \rho|B_i,\ D|B_i]/f_iB_i[X;\ \rho|B_i,\ D|B_i]$$

where $i=1, 2$. Then we have a B-ring isomorphism

$$B[X;\ \rho,\ D]/fB[X;\ \rho,\ D] \simeq A_1 \oplus A_2$$

From this, the assertion (i) will be easily seen. To see (ii), we assume that each f_i is Galois in $B_i[X;\ \rho|B_i,\ D|B_i]_2$, that is, each A_i is a $\mathfrak{G}_i$-Galois extension of B_i. By [3, Lemma 1. 2], the $\mathfrak{G}_i$ are of order 2. We set here $\mathfrak{G}_i=\{1, \sigma_i\}$ $(i=1, 2)$. Then, there exist elements $r_{ij},\ s_{ij} \in B_i$ $(i=1, 2;\ j=1, \cdots, m)$ such that $\sum_j r_{ij}s_{ij}=e_i(2)$ and $\sum_j r_{ij}\sigma_i(s_{ij})=0$ $(i=1, 2)$. Now let σ be the map of $A_1 \oplus A_2$ into itself defined by $a_1+a_2 \to \sigma_1(a_1)+\sigma_2(a_2)$ $(a_i \in A_i)$. Obviously, σ is an automorphism of order 2, and the fixed subring of σ in $A_1 \oplus A_2$ coincides with $B_1+B_2=B$. Moreover, we have that

$$\sum_j (r_{1j}+r_{2j})(s_{1j}+s_{2j})=1 \quad \text{and} \quad \sum_j (r_{1j}+r_{2j})\sigma(s_{1j}+s_{2j})=0.$$

This shows that $A_1 \oplus A_2$ is Galois over B. Thus f is Galois. The converse is obvious, completing the proof.

Now, we shall prove the following theorem which is a partial generalization of the result of [4, Th. 16].

Theorem 2. *Assume that $2^nB=2^{n+1}B$ for some integer $n \geq 0$ and $B[X;\ \rho,\ D]_2$ contains an element $g=X^2-Xu-v$ so that $B=uB+2B$ and $D(u) \in 2^nB$. Then, for $f=X^2-Xa-b \in B[X;\ \rho,\ D]_2$, f is separable if and only if f is Galois; and in this case, there holds that $B=aB+2B$ and $D(a) \in 2^nB$.*

Proof. Let $f=X^2-Xa-b \in B[X;\ \rho, D]_2$. As is well known, if f is Galois then it is separable. To see the converse, we assume that f is separable. We shall here distinguish three cases.

Case I. $2^nB=B$. In this case, 2 is inversible in B. Hence by

[4, Th. 7], f is Galois.

Case II. $2^nB = \{0\}$. By the assumption, we have that $2^n = 0$ and $B = uB + 2B = Bu + 2B$ (by [4, (i)]). Hence, by [4. Lemma 10], u and $\delta(g) = u^2 + 4v$ are inversible in B. Moreover $D(u) = 0$. Since $u^2 - u\rho(u) = 2D(u)$ ([4, (i)]), this implies that $\rho(u) = u$. Therefore, by [4, Th. 16], we obtain that f is Galois, $B = aB + 2B$, and $D(a) = 0$.

Case III. $B \supsetneq 2^nB \supsetneq \{0\}$. By Lemma 1, each $e_i(2)f$ is separable in $e_i(2)B[X; \rho | e_i(2)B, D | e_i(2)B]$. Since $2^n e_1(2)B = e_1(2)B$, it follows from the result of Case I that $e_1(2)f$ is Galois. Moreover, we have $2^n e_2(2)B = \{0\}$. Hence by the result of Case II, $e_2(2)f$ is Galois, $e_2(2)B = (e_2(2)a)e_2(2)B + 2e_2(2)B$, and $e_2(2)D(a) = 0$. Therefore, it follows from Lemma 1 that f is Galois. Moreover, one will easily see that $aB + 2B = (e_1(2) + e_2(2))(aB + 2B) = B$, and $D(a) \in e_1(2)B = 2^nB$. This completes the proof.

Next, we shall deal with separable polynomials in $B[X; \rho] (D = 0)$, and prove the following theorem which contains the result of [2, Cor. to Th. 3. 5].

Theorem 3. *Assume that* $2^nB = 2^{n+1}B$ *for some integer* $n \geq 0$. *Then, any separable polynomial in* $B[X; \rho]_2$ *is Frobenius.*

Proof. Let $f = X^2 - Xa - b$ be a separable polynomial in $B[X; \rho]_2$. Then, by [4, Th. 1] and [3, (2, 0)], we have $\rho(a) = a$, $\rho(b) = b$, $aB = Ba$, and $bB = Bb$. We shall here distinguish three cases.

Case I. $2^nB = B$. In this case, 2 is inversible in B. Hence, by [3, Th. 2. 7], f is Galois, and so, f is Frobenius.

Case II. $2^nB = \{0\}$. By [3, (2, x, xv, xvii], there exist elements b_1 and b_2 in B such that

$$1 = b(b_1 + \rho(b_1)) - ab_2, \quad b_1a = \rho(b_1)a, \quad \text{and}$$
$$uv = vu \text{ for each pair } u, v \in \{a, b, b_1, \rho(b_1), b_2\}.$$

Then we have that

$$1 = b^n(b_1 + \rho(b_1))^n + ac, \qquad ac = ca$$

for some element c in B, and whence

$$a = b^n(b_1 + \rho(b_1))^n a + aca = b^n(b_1 + \rho(b_1))^{n-1}2b_1a + a^2c$$
$$= 2^n b^n a b_1^n + a^2c = a^2c.$$

Thus, we obtain that $aB \subset a^2B \subset aB$, that is, $aB = a^2B$. By Lemma 1, each $e_i(a)f$ is separable in $e_i(a)B[X; \rho | e_i(a)B]$. Since $e_1(a)a$ is

inversible in $e_1(a)B$, $e_1(a)f$ is Frobenius by the result of [1, Th. 1(a)]. Moreover, we have $e_2(a) = e_2(a)\,(b(b_1 + \rho(b_1)) - ab_2) = e_2(a)b(b_1 + \rho(b_1))$. This implies that $e_2(a)b$ is inversible in $e_2(a)B$. Hence by [1, Th. 1(b)], $e_2(a)f$ is Frobenius. Therefore, it follows from Lemma 1 that f is Frobenius.

Case III. $B \supsetneqq 2^nB \supsetneqq \{0\}$. By Lemma 1, each $e_i(2)f$ is separable in $e_i(2)B[X;\ \rho|e_i(2)B]$. Since $2^ne_1(2)B = e_1(2)B$, $e_1(2)f$ is Frobenius by the result of Case I. Moreover, we have $(e_2(a)2)^n = 0$. Hence $e_2(2)f$ is Frobenius by the result of Case II. Thus, f is Frobenius by Lemma 1. This completes the proof.

We shall conclude our study with the following corollary which is an easy consequence of Th. 3.

Corollary 4. *If the subring of B generated by 1 is finite then any separable polynomial in $B[X;\ \rho]_2$ is Frobenius.*

REFERENCES

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

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

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

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

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received October 17, 1979*)