ON SEPARABLE POLYNOMIALS IN SKEW POLYNOMIAL RINGS

SATOSHI YAMANAKA

Abstract. Let B be a ring with identity element 1 of prime characteristic p, D a derivation of B, and $B[X;D]$ the skew polynomial ring in which the multiplication is given by $\alpha X = X\alpha + D(\alpha)$ for any $\alpha \in B$. We consider a condition for $X^p - Xa - b \in B[X;D]$ to be a Galois polynomial.

1. Introduction

This is based on a joint work with S. Ikehata [17].

In [12, 13, 14], T. Nagahara has studied separable and Galois polynomials of degree 2 in skew polynomial rings. He got several interesting results. The pourpose of this paper is to give a generalization of Nagahara's result for polynomials of degree 2 to general prime degree p.

Throughout this paper, B will mean a ring with identity element 1 and D a derivation of B, that is, D is an additive endomorphism of B such that $D(\alpha\beta) = D(\alpha)\beta + \alpha D(\beta)$ for any $\alpha,\ \beta \in B$. We assume that B is of prime characteristic p. Let $B[X;D]$ be the skew polynomial ring in which the multiplication is given by $\alpha X = X\alpha + D(\alpha)$ $(\alpha \in B)$.

A ring extension A/B is called separable if the A-A-homomorphism of $A \otimes_B A$ onto A defined by $a \otimes b \to ab$ splits, and A/B is called Hirata separable if $A \otimes_B A$ is A-A-isomorphic to a direct summand of a finite direct sum of copies of A. It is well known that a Hirata separable extension is a separable extension.

Let f be a monic polynomial in $B[X;D]$ such that $fB[X;D] = B[X;D]f$, then the residue ring $B[X;D]/fB[X;D]$ is a free ring extension of B. If $B[X;D]/fB[X;D]$ is a *separable* (resp. *Hirata separable*) extension of B, then f is called a *separable* (resp. *Hirata separable*) polynomial in $B[X;D]$. These provide typical and essential examples of separable and Hirata separable extensions. K. Kishimoto, T. Nagahara, Y. Miyashita, G. Szeto, L. Xue, and S. Ikehata studied extensively separable polynomials in skew polynomial rings. In [11], Y. Miyashita gave characterizations of separable and Hirata separable polynomials of general degree by the theory of (*)-positively filtered rings. He gave a method to study polynomials of general degree in skew polynomial rings. Then in [1, 2, 3, 4], Ikehata studied separable polynomials and Hirata separable plolynomials in skew polynomial rings by making use of Miyashita's method. Recently, the author and Ikehata gave an alternative proof of Miyashita's theorem in [16].

A ring extension A/B is called a G-Galois extension, provided that there exists a finite group of G of automorphisms of A such that $B = A^G$ (the fix ring of G in A) and $\sum_i x_i\sigma(y_i) = \delta_{1,\sigma}$ for some finite number of elements $x_i,\ y_i \in A$. We call $\{x_i,\ y_i\}$ a G-Galois coordinate system for A/B. It is well known that a G-Galois extension is a separable

The detailed version of this paper will be submitted for publication elsewhere.

extension. Let f be a monic polynomial in $B[X;D]$ such that $fB[X;D] = B[X;D]f$, then f is called a Galois polynomial in $B[X;D]$ if $B[X;D]/fB[X;D]$ is a G-Galois extension over B for some finite group G.

We shall use the following conventions:

Z = the center of B.

$U(Z)$ = the set of all invertible elements in Z.

$B^D = \{\alpha \in B \mid D(\alpha) = 0\}$, $Z^D = \{\alpha \in Z \mid D(\alpha) = 0\}$.

$B[X;D]_{(0)}$ = the set of all monic polynomials g in $B[X;D]$ such that $gB[X;D] = B[X;D]g$.

2. Galois polynomials in $B[X;D]$

In [12, 13, 14], T. Nagahara has studied separable and Galois polynomials of degree 2 in skew polynomial rings. He proved the following

Proposition 1. ([12, Theorem 3.7]) *Assume $2 = 0$, and let $f = X^2 - Xa - b$ be in $B[X;D]_{(0)}$. Then f is a Galois polynomial in $B[X;D]$ if and only if there exists an element s in $U(Z)$ such that $D(s) + as = 1$.*

The purpose of this paper is to generalize the above result to the general prime degree.

We shall state some basic results which were already known. The following is easily verified by a direct computation.

Lemma 2. ([1, Corollary 1.7]) *Let $f = X^p - Xa - b$ be in $B[X;D]$. Then f is in $B[X;D]_{(0)}$, that is, $fB[X;D] = B[X;D]f$, if and only if*

(1) $a \in Z^D$, and $b \in B^D$.

(2) $D^p(\alpha) - D(\alpha)a = \alpha b - b\alpha \quad (\alpha \in B)$.

Concerning Galois polynomials, the following Kishimoto's result is fundamental.

Lemma 3. ([9, Theorem 1.1 and Corollary 1.7], [6, Lemma 2.3]) *Let $f = X^p - X - b$ be in $B[X;D]_{(0)}$. Then f is a Galois polynomial over B.*

Proof. For convenience, we outline the proof. Let $A = B[X;D]/fB[X;D]$ and $x = X + fB[X;D]$. The mapping $\sigma : A \to A$ defined by $\sigma(\sum_i x^i d_i) = \sum_i (x+1)^i d_i$ is a B-automorphism of A of order p. Let $G =< \sigma >$. It is easy to see that $A^G = B$. We put here

$$a_j = j^{-1}\sigma^j(x) \quad \text{and} \quad b_j = (-j^{-1})x \quad (1 \leq j \leq p-1).$$

Then the expansions of

$$\Pi_{j=1}^{p-1}(a_j + b_j) = 1 \quad \text{and} \quad \Pi_{j=1}^{p-1}(a_j + \sigma^k(b_j)) = 0 \quad (1 \leq j \leq p-1)$$

enable us to see the existence of a G-Galois coordinate system for A/B. Thus, A is a G-Galois extension over B.

In general, if we consider a polynomial $f = X^p - Xa - b \in B[X;D]_{(0)}$ and $a \neq 1$, it is not easy to check whether f is a Galois polynomial or not.

Now, we shall generalize Nagahara's theorem to general prime degree p case. In what follows we fix the following.

Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$. We put here $A = B[X;D]/fB[X;D]$ and $x = X + fB[X;D]$.

First we shall state the following lemma.

Lemma 4.

$$D^{p-1}(s^{p-1}) = -s^{-1}(sD)^{p-1}(s) \text{ for any element } s \text{ in } U(Z).$$

Then we can prove the following theorem which is a generalization of Nagahara's theorem ([12, Theorem 3.7]).

Theorem 5. *Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$. If f is a Galois polynomial in $B[X;D]$ with a Galois group $G =< \sigma_s >$ of order p, where $\sigma_s(x) = x + s^{-1}$ with an element $s \in U(Z)$, then $s^{-1}(sD)^{p-1}(s) + s^{p-1}a = 1$. Conversely, if there exists an element $s \in U(Z)$ such that $s^{-1}(sD)^{p-1}(s) + s^{p-1}a = 1$ then f is a Galois polynomial in $B[X;D]$ with a Galois group $G =< \sigma_s >$ of order p, where $\sigma_s(x) = x + s^{-1}$.*

The proofs of Lemma 4 and Theorem 5 are written in the detailed version of this paper which will be submitted for publication elsewhere. Theorem 5 is proved by making use of the following two formulas : For any $s \in Z$,

$$(X + s)^p = X^p + s^p + D^{p-1}(s), \quad \text{and}$$

$$(sD)^p = s^p D^p + (sD)^{p-1}(s)D \quad \text{(the Hochschild's formula)}.$$

Remark. In [12], T. Nagahara proved that if $f = X^2 - Xa - b$ is a Galois polynomial in $B[X;D]$, then necessarily the order of the Galois group is 2. However, in general case we do not prove yet that if $f = X^p - Xa - b$ is a Galois polynomial in $B[X;D]$, then the order of the Galois group is p.

In virtue of Lemma 4, we obtain the following corollary as a direct consequence of Theorem 5.

Corollary 6. *Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$. If there exists an element $y \in Z$ such that $D^{p-1}(y) - ya = 1$ and $y = -s^{p-1}$ for some element $s \in U(Z)$, then f is a Galois polynomial in $B[X;D]$ with a Galois group $G =< \sigma_s >$ of oreder p, where $\sigma_s(x) = x + s^{-1}$. Conversely, if f is a Galois polynomial in $B[X;D]$ with a Galois group $G =< \sigma_s >$ of order p, where $\sigma_s(x) = x + s^{-1}$ with an element $s \in U(Z)$, then $D^{p-1}(y) - ya = 1$ and $y = -s^{p-1}$.*

Corollary 7. *Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$. If there exists an invertible element $u \in Z^D$ such that $u^{p-1} = a$, then f is a Galois polynomial in $B[X;D]$ with a Galois group $G =< \sigma_{u^{-1}} >$, where $\sigma_{u^{-1}}(x) = x + u$.*

Finally we shall state the following theorem which is proved in [17].

Theorem 8. *Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$. If there exists an element $z \in Z$ such that $D(z)$ is invertible in Z, then f is a Hirata separable polynomial in $B[X;D]$. In addition, if z is an invertible element in Z, then, f is a Galois polynomial in $B[X;D]$ with a Galois group $G =< \tau >$, where $\tau(x) = x + D(z)z^{-1}$.*

Lastly, as a direct consequence of Theorem 8, we obtain the following

Corollary 9. *If B is a simple ring and $D|Z \neq 0$, then $f = X^p - Xa - b$ in $B[X;D]_{(0)}$ is always a Hirata separable and Galois polynomial in $B[X;D]$.*

Corollary 10. *If B is a field and $D \neq 0$, then $f = X^p - Xa - b$ in $B[X;D]_{(0)}$ is always a Hirata separable and Galois polynomial in $B[X;D]$.*

References

[1] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings, *Math. J. Okayama Univ.,* **22** (1980), 115–129.

[2] S. Ikehata, Azumaya algebras and skew polynomial rings, *Math, J. Okayama Univ.,* **23** (1981), 19–32.

[3] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings. II, *Math. J. Okayama Univ.,* **25** (1983), 23–28.

[4] S. Ikehata, Azumaya algebras and skew polynomial rings II, *Math, J. Okayama Univ.,* **26** (1984), 49–57.

[5] S. Ikehata, Purely inseparable ring extensions and H-separable polynomials, *Math. J. Okayama Univ.,* **40** (1998), 55–63.

[6] S. Ikehata, On H-separable and Galois polynomials of degree p in skew polynomial rings, *Int. Math. Forum* **3** (2008), 1581–1586.

[7] S. Ikehata, A note on separable polynomials of derivation type, *Int. J. Algebra* **3** (2009), no. 14, 707–711.

[8] N. Jacobson, Lecture in abstract algebra. Vol III: Theory of fields and Galois theory, *D. Van Nostrand Co., Inc.,* (1964)

[9] K. Kishimoto, On abelian extensions of rings. I, *Math. J. Okayama Univ.,* **14** (1970), 159–174.

[10] K. Kishimoto, On abelian extensions of rings. II, *Math. J. Okayama Univ.,* **15** (1971), 57–70.

[11] Y. Miyashita, On a skew polynomial ring, *J. Math. Soc. Japan,* **31** (1979), no. 2, 317–330.

[12] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings, *Math. J. Okayama Univ.,* **19** (1976), 65–95.

[13] T. Nagahara, A note on separable polynomials in skew polynomial rings of atutomorphism type, *Math. J. Okayama Univ.,* **22** (1980), 73–76.

[14] T. Nagahara, Some H-separable polynomials of degree 2, *Math. J. Okayama Univ.,* **26** (1984), 87–90.

[15] G. Szeto and L. Xue, On the Ikehata theorem for H-separable skew polynomial rings, *Math. J. Okayama Univ.,* **40** (1998), 27–32.

[16] S. Yamanaka and S. Ikehata, An alternative proof of Miyashita' s theorem in a skew polynomial ring, *Int. J. Algebra* **6** (2012), 1011–1023.
[17] S. Yamanaka and S. Ikehata, On Galois polynomials of degree p in skew polynomial rings of derivation type, Submitted.

Department of Mathematics
Graduate School of Natural Science and Technology
Okayama University
Okayama 700-8530 JAPAN
E-mail address: s_yamanaka@math.okayama-u.ac.jp