A Note on Separable Polynomials of Derivation Type

Shūichi Ikehata

Department of Environmental and Mathematical Science
Faculty of Environmental Science and Technology
Okayama University, Tsushima, Okayama 700-8530, Japan
ikehata@ems.okayama-u.ac.jp

Abstract
Let $B$ be a ring with identity $1$, $Z$ the center of $B$, $D$ a derivation of $B$, and $B[X; D]$ the skew polynomial ring such that $\alpha X = X\alpha + D(\alpha)$ for each $\alpha \in B$. Assume that $B$ is of prime characteristic $p$ and $D|Z = 0$. Let $f = X^p - Xa - b \in B[X; D]$ such that $f B[X; D] = B[X; D]f$, where $e$ is any positive integer. Then we prove that $f$ is a separable polynomial in $B[X; D]$ if and only if $a$ is invertible in $B$.

Mathematics Subject Classification: 16S32, 16W25,

Keywords: separable polynomial, skew polynomial ring, derivation

1 Introduction
Throughout this paper, $B$ will represent a ring with identity element $1$, $Z$ the center of $B$, and $D$ a derivation of $B$. 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 $H$-separable if $A \otimes_B A$ is $A$-$A$-isomorphic to a direct summand of a finite direct sum of copies of $A$. As is well known, an $H$-separable extension is a separable extension. Let $f$ be a monic polynomial in $B[X; D]$ such that $f B[X; D] = B[X; D]f$. Then the residue ring $B[X; D]/f B[X; D]$ is a free ring extension of $B$. If $B[X; D]/f B[X; D]$ is a separable (resp.$H$-separable) extension of $B$, we call $f$ is a separable (resp.$H$-separable) polynomial in $B[X; D]$. These provide typical and essential examples of separable and $H$-separable extensions. K. Kishimoto, T. Nagahara, Y. Miyashita, G. Szeto, L. Xue, and the author studied extensively separable polynomials in skew polynomial rings (See References).
Moreover, by (1) and (2), we have $Z = D$, where $f$ is a monic polynomial in $B[X]$, where $B$ is a commutative ring. Then $f$ is a separable polynomial in $B[X]$ if and only if $f' + fB[X]$ is an invertible element in $B[X]/fB[X]$. The notion of separable polynomials was generalized to noncommutative cases, that is, skew polynomial ring cases.

In [3], we have proved the following result: Assume that $B$ is of prime characteristic $p$ and $D|Z = 0$. Let $f = X^p - Xa - b$ be in $B[X; D]$ such that $fB[X; D] = B[X; D]f$. Then $f$ is a separable polynomial in $B[X; D]$ if and only if $a$ is invertible in $B$. The purpose of this paper is to prove the result for $X^p = Xa - b$ for every positive integer $e$.

## 2 Main results

**Theorem 2.1** Assume that $B$ is of prime characteristic $p$ and $D|Z = 0$. Let $f = X^p - Xa - b$ be in $B[X; D]$ such that $fB[X; D] = B[X; D]f$, where $e$ is any positive integer. Then $f$ is a separable polynomial in $B[X; D]$ if and only if $a$ is invertible in $B$.

**Proof.** As was verified in [1, Corollary 1.7], the hypothesis $fB[X; D] = B[X; D]f$ is equivalent to the following:

$$D(a) = D(b) = 0, \ a \in Z \ and \ D^{p^e}(\alpha) - D(\alpha)a - b\alpha = 0 \ (\alpha \in B).$$

Assume that $f$ is a separable polynomial in $B[X; D]$. Then, it follows from [1, Theorem 4.1] that there exists an element $y = X^{p^e-1}d_{p^e-1} + X^{p^e-2}d_{p^e-2} + \cdots + Xd_1 + d_0$ in $B[X; D]$ such that $\alpha y = y\alpha \ (\alpha \in B)$ and $D^{p^e-1}(y) - ya = 1$, where $D(\Sigma_iX^ic_i) = \Sigma_iX^iD(c_i)$. Obviously, $\alpha y = y\alpha \ (\alpha \in B)$ implies $d_{p^e-1} \in Z$, and therefore $D(d_{p^e-1}) = 0$. By induction, we can easily see that

$$\alpha D^{k-1}(y) = D^{k-1}(y)\alpha \ (\alpha \in B). \quad (1)$$

and

$$D^k(d_{p^e-k}) = 0 \ (1 \leq k \leq p^e). \quad (2)$$

By (1) and (2), we have

$$D(\alpha)D^{p^e-2}(d_1) + \alpha D^{p^e-2}(d_0) = D^{p^e-2}(d_0)\alpha \ (\alpha \in B), \ D^{p^e-2}(d_1) \in Z. \quad (3)$$

Moreover, $D^{p^e-1}(y) - ya = 1$ implies

$$D^{p^e-1}(d_0) - d_0a = 1. \quad (4)$$

$$-d_1a = 0. \quad (5)$$
Putting $\alpha = D^{p^e-2}(d_0)$ in (3), we have

$$D^{p^e-1}(d_0)D^{p^e-2}(d_1) = 0. \quad (6)$$

Then, by (3), (4), (5), and (6), it follows that

$$D^{p^e-2}(d_0)\alpha - \alpha D^{p^e-2}(d_0) = D(\alpha)D^{p^e-2}(d_1)$$

$$= D(\alpha)\{D^{p^e-1}(d_0) - d_0a\}D^{p^e-2}(d_1)$$

$$= D(\alpha)\{D^{p^e-1}(d_0)D^{p^e-2}(d_1) - d_0D^{p^e-2}(ad_1)\}$$

$$= 0.$$

Hence, $D^{p^e-2}(d_0)$ is in $Z$, and therefore by (4), $1 = D^{p^e-1}(d_0) - ad_0 = -ad_0$, and so $a$ is invertible in $B$.

Conversely, assume that $a$ is invertible in $B$. Since $a$ is invertible in $Z$ by the earlier observation, there holds $D(a^{-1}) = 0$. Putting $y = -a^{-1}$, we have $D^{p^e-1}(y) - ya = 1$ and $\alpha y = y\alpha$ ($\alpha \in B$). Thus, $f$ is a separable polynomial in $B[X;D]$ by [1, Theorem 4.1].

Concerning an $H$-separable polynomial we already have the following equivalent condition as given in [2].

**Lemma 2.2** ([2, Lemma 1.5]) Let $f$ be a monic polynomial of degree $m$ in $B[X;D]$ such that $fB[X;D] = B[X;D]f$, and $I = fB[X;D]$. Then $f$ is an $H$-separable polynomial in $B[X;D]$ if and only if there exist elements $y_i, z_i \in B[X;D]$ with $\deg y_i < m$ and $\deg z_i < m$ such that $\alpha y_i = y_i\alpha$, $\alpha z_i = z_i\alpha$ ($\alpha \in B$) and

$$\sum_{i} D^{*m-1}(y_i)z_i \equiv 1 \pmod{I}, \quad \sum_{i} D^{*k}(y_i)z_i \equiv 0 \pmod{I} \quad (0 \leq k \leq m - 2).$$

As an immediate consequence of Theorem 2.1, we have the following theorem which is a generalization of [8, Theorem 3.3].

**Theorem 3.3** Assume that $B$ is of prime characteristic $p$ and $D|Z = 0$. Let $f = X^{p^e} - Xa - b$ be in $B[X;D]$ such that $fB[X;D] = B[X;D]f$. Then $f$ is not an $H$-separable polynomial in $B[X;D]$. In other words, there are no $H$-separable polynomials of the form $X^{p^e} - Xa - b$ in $B[X;D]$, for any positive integer $e$.

**Proof.** Assume that $f$ is an $H$-separable polynomial in $B[X;D]$. At first, we shall show the following:

Let $y = X^{p^e-1}d_{p^e-1} + X^{p^e-2}d_{p^e-2} + \cdots + Xd_1 + d_0 \in B[X;D]$ such that $\alpha y = y\alpha$ ($\alpha \in B$). Then $D^*(y) = 0$. 

Since $D|Z = 0$, as was verified in the proof of Theorem 2.1, we obtain
\[ D^k(d_p^e - k) = 0 \quad (1 \leq k \leq p^e). \]
Hence we have $D^{pe}(y) = 0$. Since $D^{pe}(y) - D^*(y)a = yb - by = 0$, we obtain $D^*(y)a = 0$. Since $f$ is an $H$-separable polynomial, $f$ is a separable polynomial in $B[X;D]$. By Theorem 2.1, $a$ is an invertible element in $B$, hence we conclude $D^*(y) = 0$.

Then by Lemma 2.2, there exist elements $y_i, z_i \in B[X;D]$ with $\deg y_i < m$ and $\deg z_i < m$ such that $\alpha y_i = y i \alpha$, $\alpha z_i = z_i \alpha$ ($\alpha \in B$) and
\[
\sum_i D^{*m-1}(y_i)z_i \equiv 1 \pmod{I}, \quad \sum_i D^*(y_i)z_i \equiv 0 \pmod{I} \quad (0 \leq k \leq m-2).
\]
However, by what we showed earlier, we see that $D^*(y_i) = 0$. Hence it is impossible that $\sum_i D^{x-1}(y_i)z_i \equiv 1 \pmod{I}$. This is a contradiction. Thus $f$ is not an $H$-separable polynomial.

Finally, we are interested in the following two questions.

**Question 1.** Assume that $B$ is of prime characteristic $p$ and $D|Z = 0$. Let $f = X^{pe} + X^{pe-1} \alpha_e + \cdots + X^e \alpha_2 + X \alpha_1 + \alpha_0$ be any $p$-polynomial in $B[X;D]$ such that $fB[X;D] = B[X;D]f$. Then is it true that $f$ is a separable polynomial in $B[X;D]$ if and only if $\alpha_1$ is invertible in $B$?

**Question 2.** Assume that $B$ is of prime characteristic $p$ and $D|Z = 0$. Then is it true that there are no $H$-separable polynomials in $B[X;D]$?

**Remark.** As was shown in [5, Theorem 2.2], if $B[X;D]$ contains an $H$-separable polynomial $f$ of degree $m \geq 2$, then $B$ is of prime characteristic $p$ and $f$ is a $p$-polynomial of the form $X^{pe} + X^{pe-1} \alpha_e + \cdots + X^e \alpha_2 + X \alpha_1 + \alpha_0$, where $m = p^e$. Hence in Question 2, we may restrict our attention to only $p$-polynomials.

**ACKNOWLEDGEMENTS.** This work was done while the author was visiting at the Mathematics Department of Bradley University in spring 2009. He expresses his gratitude to Professor George Szeto and Professor Larry Xue for many useful discussions and the hospitality of the Mathematics Department of Bradley University.

**References**


Received: March, 2009