International Mathematical Forum, 3, 2008, no. 32, 1581 - 1586

# On $H$-Separable and Galois Polynomials of Degree $p$ in Skew Polynomial Rings

**Shûichi 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

*In memory of Professor Kozo Sugano*

**Abstract**

Let $B$ be a ring with identity 1, $D$ a derivation of $B$, and $B[X;D]$ the skew polynomial ring such that $\alpha X = X\alpha + D(\alpha)$ for each $\alpha \in B$. Then conditions are given for $X^p - Xa - b \in B[X;D]$ to be an $H$-separable and Galois polynomial where $p$ is a prime integer.

**Mathematics Subject Classification:** 16S30, 16W20

**Keywords:** $H$-separable polynomial, skew polynomial ring, Galois extension.

## 1 Introduction

Throughout this paper, $B$ will mean a ring with identity element 1 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. The notion of $H$-separable extensions was introduced by K. Hirata as a generalization of Azumaya algebras. An Azumaya $C$-algebra means a separable extension over its center $C$. K. Sugano had studied consistently $H$-separable extensions. 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.*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, and the author studied extensively separable polynomials in skew polynomial rings (See References). In [2, 5], the author gave a characterization of $H$-separable polynomials in skew polynomial rings. If the coefficient ring $B$ is not commutative, the condition is complicated and not easy to check. As was shown in [5], if $B[X;D]$ contains an $H$-separable polynomial of degree $\geq 2$, then $B$ is necessarily of a prime characteristic $p$. Therefore in the following, we assume that $B$ is of a prime characteristic $p$. In [12], G. Szeto and L. Xue succeeded to give a nice characterization of a polynomial $X^n - u$ to be $H$-separable in skew polynomial rings of automorphism type. However, considering skew polynomial rings of derivation type, the situation is not parallel. So the purpose of this paper is to give some intelligible conditions for a polynomial $f = X^p - Xa - b$ in $B[X;D]$ to be $H$-separable and Galois. For $p = 2$, some interesting work was done in [9, 10, 11]. The following is the main result (Theorem 3.3): Let $f = X^p - Xa - b$ be in $B[X;D]$ such that $fB[X;D] = B[X;D]f$. If there exists an element $z \in Z$, the center of $B$, such that $D(z)$ is invertible in $Z$, then $f$ is an $H$-separable polynomial in $B[X;D]$. In addition, if $z$ is an invertible element in $Z$, then, $f$ is a Galois polynomial in $B[X;D]$.

Moreover, a ring extension $A/B$ is called $G$-Galois, if there exist a finite group $G$ of automorphisms of $A$ such that $B = A^G$ (the fix ring of $G$ in $A$) and $\sum_i x_i\sigma(y_i) = \delta_{1,\sigma}$ ($\sigma \in G$) for some finite number of elements $x_i, y_i \in A$. We call $\{x_i, y_i\}$ a $G$-Galois coordinate system for $A/B$. As is well known, a $G$-Galois 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 $f$ is called a Galois polynomial in $B[X;D]$ if the residue ring $B[X;D]/fB[X;D]$ is a $G$-Galois extension over $B$ for some finite group $G$. We shall show that some $H$-separable polynomials are Galois polynomials.

We shall use the following conventions:

$Z$ = the center of $B$.

$u_r$ (resp. $u_\ell$) = the right (resp. left) multiplication in $B$ by $u \in B$.

$I_u = u_r - u_\ell$ = the inner derivation of $B$ by $u \in B$.

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

$$gB[X;D] = B[X;D]g.$$

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

$D^* : B[X;D] \to B[X;D]$ be the inner derivation of $B[X;D]$ by $X$,

namely $D^*(\Sigma_i X^i d_i) = \Sigma_i X^i D(d_i)$.

# 2 Preliminary results

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

**Lemma 2.1** (*[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. *$D^p - a_r D = I_b$.*

The following is a characterization of an $H$-separable polynomial.

**Lemma 2.2** (*[2, Lemma 1.5]*) *Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$, and $I = fB[X;D]$. Then $f$ is an $H$-separable polynomial over $B$ if and only if there exist $y_i, z_i \in B[X;D]$ with $\deg y_i < p$ and $\deg z_i < p$ such that $\alpha y_i = y_i \alpha$, $\alpha z_i = z_i \alpha$ $(\alpha \in B)$ and*

$$\sum_i D^{*p-1}(y_i)z_i = 1 \pmod{\mathrm{I}} \quad \sum_i D^{*k}(y_i)z_i \equiv 0 \pmod{\mathrm{I}} \ (0 \le k \le p-2).$$

The above characterization of an $H$-separable polynomial is not easy to check. So, in the next section, we shall give some intelligible sufficient conditons for a polynomial $f$ to be $H$-separable.

Concerning Galois polynomials, the following lemma is important.

**Lemma 2.3** (*[7, Theorem 1.1 and Corollary 1.1]*) *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 $S = B[X;D]/fB[X;D]$ and $x = X + fB[X;D] \in S$. The mapping $\sigma : S \to S$ defined by $\sigma(\sum_i x^i d_i) = \sum_i (x+1)^i d_i$ is a $B$-automorphism of $S$ of order $p$. Let $G =< \sigma >$. It is easy to see that $S^G = B$. We put here

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

Then the expansions of

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

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

# 3 Main results

To show the main theorem (Theorem 3.3), we first prove the following lemma which is a special case of our main theorem.

**Lemma 3.1** *Let $f = X^p - Xa - b$ be in $B[X;D]_{(0)}$. If there exists an element $z \in Z$ such that $D(z) = 1$, then $f = X^p - b$, that is, $a = 0$, and $f$ is an $H$-separable polynomial in $B[X;D]$. In addition, if $z$ is an invertible element in $Z$, then, $f$ is a Galois polynomial in $B[X;D]$.*

*Proof.* By Lemma 2.1.(2), we have

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

We put $\alpha = z$ in the above. Then since $D(z) = 1$, we have $a = 0$. For $0 \leq i \leq p-1$, we put $x_i = -z^i, y_i = z^{p-i-1}$. Then we can easily see

$$\sum_{i=0}^{p-1} D^{p-1}(x_i)y_i = 1 \quad \text{and} \quad \sum_{i=0}^{p-1} D^k(x_i)y_i = 0 \quad (0 \leq k \leq p-2).$$

Therefore $f = X^p - b$ is an $H$-separable polynomial in $B[X;D]$ by Lemma 2.2.

Next, we assume $z$ is an invertible element in $Z$. We consider the derivation $\Delta = z_\ell D = zD$ of $B$. Then since $D(z) = 1$, we have $\Delta(z) = z$. Hence by the well known Hochschild's formula, we have

$$\Delta^p = (zD)^p = z^pD^p + (zD)^{p-1}(z)D = z^pD^p + zD = z^pI_b + \Delta = \Delta + I_{z^pb}.$$

We set here $Y = zX$. Then

$$\alpha Y = Y\alpha + \Delta(\alpha) \quad (\alpha \in B).$$

So, we see that $B[X;D] = B[Y;\Delta]$ and $Y^p = (zX)^p = (Xz+1)^p = (Xz)^p + 1 = X^pz^p + Xz + 1$. Hence $Y^p - Y = (X^pz^p + Xz + 1) - (Xz + 1) = X^pz^p = (f+b)z^p = fz^p + bz^p$. It follows from Lemma 2.3 that $g = Y^p - Y - bz^p = fz^p$ is a Galois polynomial in $B[Y;\Delta]$. Noting $B[X;D] = B[Y;\Delta]$ and $fB[X;D] = B[X;D]f = gB[Y;\Delta] = B[Y;\Delta]g$, we see that $f$ is also a Galois polynomial in $B[X;D]$.

The following is an immediate consequence of Lemma 3.1.

**Corollary 3.2** *Let $f = X^p - b$ be in $B[X;D]_{(0)}$. If there exists an element $z \in Z$ such that $D(z) = 1$, then $f$ is an $H$-separable polynomial in $B[X;D]$. In addition, if $z$ is an invertible element in $Z$, then, $f$ is a Galois polynomial in $B[X;D]$.*

Now we prove the main theorem.

**Theorem 3.3** *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 an $H$-separable polynomial in $B[X;D]$. In addition, if $z$ is an invertible element in $Z$, then, $f$ is a Galois polynomial in $B[X;D]$.*

*Proof.* Assume that $cD(z) = 1$ for some $c \in Z$. We put $\Delta = cD$. Then $\Delta(z) = 1$, and

$$\begin{aligned}\Delta^p = (cD)^p &= c^p D^p + (cD)^{p-1}(c)D \\ &= c^p(aD + I_b) + \Delta^{p-1}(c)D \\ &= (c^{p-1}a + \Delta^{p-1}(c)c^{-1})\Delta + I_{c^p b}.\end{aligned}$$

Since $\Delta(z) = 1$, we have $c^{p-1}a + \Delta^{p-1}(c)c^{-1} = 0$, and so $\Delta^p = I_{bc^p}$, $bc^p \in B^\Delta$. We set $Y = cX$. Then

$$\alpha Y = Y\alpha + \Delta(\alpha) \ \text{ and } \ \alpha Y^p = Y^p\alpha + \Delta^p(\alpha) \ \ (\alpha \in B).$$

So, we see that $B[X;D] = B[Y;\Delta]$ and $Y^p - bc^p = c^p f$. Hence by the previous Corollary 3.2, $Y^p - bc^p$ is an $H$-separable and Galois polynomial in $B[Y;\Delta]$, and so $f$ is also an $H$-separable and Galois polynomial in $B[X;D]$.

The following corollaries are immediate consequences of Theorem 3.3.

**Corollary 3.4** *If $B$ is a simple ring and $D|Z \neq 0$, then $f = X^p - Xa - b$ in $B[X;D]_{(0)}$ is always an $H$-separable and Galois polynomial in $B[X;D]$.*

**Corollary 3.5** *If $B$ is a field and $D \neq 0$, then $f = X^p - Xa - b$ in $B[X;D]_{(0)}$ is always an $H$-separable and Galois polynomial in $B[X;D]$.*

We shall conclude our study with the following example.

**Example 3.6** *Let $k$ be a field of a prime characteristic $p$ and $B = k[t]$, the polynomial ring. Let $D = \frac{d}{dt}$, then $D^p = 0$, $D(t) = 1$ and $B^D = k[t^p]$. Then for any $u \in k[t^p]$, $f = X^p - u$ is an $H$-separable and Galois polynomial in $B[X;D]$. Next, Let $\Delta = t\frac{d}{dt}$, then $\Delta^p - \Delta = 0, \Delta(t) = t$ and $B^\Delta = k[t^p]$. Then for any $u \in k[t^p]$, $g = Y^p - Y - u$ is a Galois polynomial in $B[Y;\Delta]$. However, since the ideal generated by $\Delta^{p-1}(B)$ does not equal to $B$, it follows from [2, Theorem 3.1] that $g$ is not an $H$-separable polynomial in $B[Y;\Delta]$.*

**ACKNOWLEDGEMENTS.** This work was done while the author was visiting at the Mathematics Department of Bradley University in spring 2008. 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

[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, A note on separable polynomials in skew polynomial rings of derivation type, *Math. J. Okayama Univ.,* **22** 1980, 59–60.

[4] S. Ikehata, On H-separable polynomials of prime degree, *Math. J. Okayama Univ.,* **33** 1991, 21–26.

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

[6] S. Ikehata, Purely inseparable ring extensions and Azumaya algebras, *Math. J. Okayama Univ.,* **41** 1999, 63–69.

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

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

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

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

[11] H. Okamoto and S. Ikehata, On H-separable polynomials of degree 2, *Math. J. Okayama Univ.,* **32** 1990, 53–59.

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

**Received: March 18, 2008**