Math. J. Okayama Univ. 32 (1990), 53–59

ON H-SEPARABLE POLYNOMIALS OF DEGREE 2

HIROAKI OKAMOTO and SHÛICHI IKEHATA

Throughout the present paper, B will represent a ring with 1, and D a derivation of B. Let $B[X; D]$ be the skew polynomial ring in which the multiplication is given by $bX = Xb + D(b)$ $(b \in B)$. A monic polynomial f in $B[X; D]$ with $fB[X; D] = B[X; D]f$ is called a separable (resp. H-separable) polynomial if $B[X; D]/fB[X; D]$ is a separable (resp. H-separable) extension of B. (By the way, it is well known that every H-separable extension is separable.)

In [1], one of the present authors has studied H-separable polynomials in skew polynomial rings. If the coefficient ring B is commutative, the existence of H-separable polynomials in $B[X; D]$ have been characterized in terms of Azumaya algebras and purely inseparable extensions ([1, Theorems 3.1 and 3.3]). However, in case B is not commutative, we know few. In the present paper, we study on H-separable polynomials of degree 2 in $B[X; D]$ together with separable polynomials of degree 2 whose discriminants are contained in the Jacobson radical $J(B)$ of B.

We shall use the following conventions:

Z = the center of B.

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

$I_u = u_r - u_l$ = the inner derivation of B effected by $u \in B$.

$B[X; D]_{(2)}$ = the set of all monic polynomials g of degree 2 in $B[X; D]$ with $gB[X; D] = B[X; D]g$.

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

D^*: $B[X; D] \to B[X; D]$ be the inner derivation of $B[X; D]$ effected by X, namely $D^*(\sum_i X^i d_i) = \sum_i X^i D(d_i)$.

First, we state the next lemma without proof.

Lemma 1 ([3, p. 82, (3, i)]). *Let $f = X^2 - Xa - b$ be in $B[X; D]$. Then f is in $B[X; D]_{(2)}$ if and only if*

(i) $2D = I_a$,

(ii) $D^2 - a_r D = I_b$, *and*

(iii) $a, b \in B^D$.

Lemma 2. *Suppose that $B[X; D]_{(2)}$ contains an H-separable polynomial f. Let $b_1, b_2 \in B$ and $u \in B^D$.*

(1) *If $(b_1)_l D+(b_2)_l = I_u$, then $b_1 = b_2 = 0$ and $u \in Z$.*

(2) *If $(b_1)_r D+(b_2)_r = I_u$, then $b_1 = b_2 = 0$ and $u \in Z$.*

Proof. (1) As is easily seen, $(D(b_1))_l D+(D(b_2))_l+|(b_1)_l D+(b_2)_l|D = (b_1)_l D^2+(D(b_1))_l D+(b_2)_l D+(D(b_2))_l = D|(b_1)_l D+(b_2)_l| = DI_u = I_u D$, whence $(D(b_1))_l D+(D(b_2))_l = 0$ follows; an easy induction shows that $(D^t(b_1))_l D+(D^t(b_2))_l = 0\ (t \geq 1)$. Then for any $h = \sum_{k=0}^{r} X^k d_k \in B[X; D]$, we see that

$$\begin{aligned} b_1 D^*(h)+b_2 h &= b_1 \sum_{k=0}^{r} X^k D(d_k)+b_2 \sum_{k=0}^{r} X^k d_k \\ &= \sum_{k=0}^{r} \sum_{j=0}^{k} X^j \binom{k}{j} D^{k-j}(b_1) D(d_k) \\ &\quad + \sum_{k=0}^{r} \sum_{j=0}^{k} X^j \binom{k}{j} D^{k-j}(b_2) d_k \\ &= \sum_{k=0}^{r} \sum_{j=0}^{k} X^j \binom{k}{j} (D^{k-j}(b_1) D(d_k)+D^{k-j}(b_2) d_k) \\ &= \sum_{k=0}^{r} X^k (b_1 D(d_k)+b_2 d_k) = \sum_{k=0}^{r} X^k I_u(d_k) = I_u^*(h). \end{aligned}$$

Since f is H-separable, [1, Lemma 1.5] shows that there exist $y_i, z_i \in B[X; D]$ with $\deg y_i \leq 1$, $\deg z_i \leq 1$ such that $\alpha y_i = y_i \alpha$, $\alpha z_i = z_i \alpha$ for all $\alpha \in B$ and $\sum_i D^*(y_i) z_i \equiv 1$, $\sum_i y_i z_i \equiv 0 \pmod{fB[X; D]}$. Hence, $b_1 \sum_i D^*(y_i) z_i + b_2 \sum_i y_i z_i = \sum_i (b_1 D^*(y_i)+b_2 y_i) z_i = \sum_i I_u^*(y_i) z_i = 0$, whence we obtain

$$b_1 \equiv b_1 \sum_i D^*(y_i) z_i + b_2 \sum_i y_i z_i \equiv 0 \pmod{fB[X; D]}.$$

This implies that $b_1 = 0$, and $(b_2)_l = I_u^*$ (in $B[X; D]$). Since $(b_2)_l D^* = I_u^* D^* = D^* I_u^*$, we have $b_2 \equiv b_2 \sum_i D^*(y_i) z_i = \sum_i b_2 D^*(y_i) z_i = \sum_i D^* I_u^*(y_i) z_i \equiv 0 \pmod{fB[X; D]}$, whence $b_2 = 0$ follows. Since $I_u^* = 0$, we get eventually $u \in Z$. Similarly, we can prove (2).

Corollary 3. *If $B[X; D]$ contains an H-separable polynomial $f = X^2 - Xa - b$, then $2 = 0$, that is, B is an algebra over* GF(2).

Proof. By Lemma 1, $2D = I_a$ and $a \in B^D$. Hence, by Lemma 2, we have $2 = 0$.

Next we shall prove

Lemma 4. *If $B[X; D]$ contains an H-separable polynomial $f = X^2 - Xa - b$, then there exists a finite system $\{u_i, v_i, c_i, d_i\}$ of elements in B such that*

(iv) $$c_i, u_i \in Z,$$

(v) $$(c_i)_r D = -I_{d_i}, (u_i)_r D = -I_{v_i},$$

(vi) $$\sum_i (D(c_i)v_i + D(d_i)u_i) = 0,$$

(vii) $$\sum_i v_i D(d_i) = 1,$$

(viii) $$\sum_i (c_i v_i + d_i u_i) = 0, \text{ and}$$

(ix) $$\sum_i v_i d_i = 0.$$

Conversely, if there exists such a system $\{u_i, v_i, c_i, d_i\}$, then each polynomial in $B[X; D]_{(2)}$ is H-separable.

Proof. Choose $\{y_i, z_i\}$ as in [1, Lemma 1.5], and write $y_i = Xc_i + d_i$, $z_i = Xu_i + v_i$ ($c_i, d_i, u_i, v_i \in B$). Then, since $\alpha y_i = y_i \alpha$, $\alpha z_i = z_i \alpha$ for all $\alpha \in B$, we readily obtain (iv) and (v). Since $\sum_i D^*(y_i) z_i \equiv 1$ and $\sum_i y_i z_i \equiv 0 \pmod{fB[X; D]}$, we obtain

(a) $$\sum_i (aD(c_i)u_i + D^2(c_i)u_i + D(c_i)v_i + D(d_i)u_i) = 0,$$

(b) $$\sum_i (bD(c_i)u_i + D^2(d_i)u_i + D(d_i)v_i) = 1,$$

(c) $$\sum_i (ac_i u_i + D(c_i)u_i + c_i v_i + d_i u_i) = 0,$$

(d) $$\sum_i (bc_i u_i + D(d_i)u_i + d_i v_i) = 0.$$

By (ii), (iv) and (v), $D(c_i)u_i = -I_{v_i}(c_i) = 0$, $D^2(c_i)u_i = D(c_i)au_i + I_b(c_i)u_i = D(c_i)u_i a = 0$, $D(d_i)v_i = I_{v_i}(D(d_i)) + v_i D(d_i) = -D^2(d_i)u_i + v_i D(d_i)$ and $D(d_i)u_i + d_i v_i = -I_{v_i}(d_i) + d_i v_i = v_i d_i$. Hence, by (a), (b), (c) and (d), we obtain (vi), (vii) and

(e) $$\sum_i (ac_i u_i + c_i v_i + d_i u_i) = 0,$$

(f) $$\sum_i (bc_i u_i + v_i d_i) = 0.$$

By (iv), (v), (vi) and (vii), we see that

$$\sum_k c_k u_k = \sum_i v_i D(d_i) \sum_k c_k u_k = \sum_{i,k} v_i D(d_i) c_k u_k$$

$$
\begin{aligned}
&= -\sum_{i,k} v_i I_{d_k}(d_i) u_k = \sum_{i,k} v_i I_{d_i}(d_k) u_k \\
&= -\sum_{i,k} v_i D(d_k) c_i u_k = -\sum_i v_i c_i \sum_k D(d_k) u_k \\
&= \sum_i v_i c_i \sum_k D(c_k) v_k = \sum_{i,k} v_i c_i D(c_k) v_k \\
&= -\sum_{i,k} v_i I_{d_i}(c_k) v_k = 0.
\end{aligned}
$$

Hence, (e) and (f) imply (viii) and (ix).

Conversely, suppose that there exist elements c_i, d_i, u_i, v_i in B satisfying (iv)-(ix). Put $y_i = Xc_i + d_i$ and $z_i = Xu_i + v_i$. Then, the above computation and [1, Lemma 1.5] enable us to see that every polynomial in $B[X; D]_{(2)}$ is H-separable.

As an immediate consequence of Lemma 4 (putting $u_i = c_i = 0$), we have the following

Corollary 5. *If there exists a system* $\{d_i, v_i\}$ *of elements in* Z *such that*

(viii) $$\sum_i v_i D(d_i) = 1, \text{ and}$$

(iv) $$\sum_i v_i d_i = 0,$$

then each polynomial in $B[X; D]_{(2)}$ *is* H*-separable.*

Corollary 6. *If the ideal of* Z *generated by* $D(Z)$ *coincides with* Z, *then each polynomial in* $B[X; D]_{(2)}$ *is* H*-separable.*

Proof. By assumption, there exists a system $\{v_i, d_i\}_{i=1}^n$ of elements in Z such that $\sum_{i=1}^n v_i D(d_i) = 1$. We set here $v_{n+1} = -\sum_{i=1}^n v_i d_i$ and $d_{n+1} = 1$. Then, we have $\sum_{i=1}^{n+1} v_i D(d_i) = \sum_{i=1}^n v_i D(d_i) + v_{n+1} D(d_{n+1}) = 1$, and $\sum_{i=1}^{n+1} v_i d_i = \sum_{i=1}^n v_i d_i + v_{n+1} d_{n+1} = 0$. Thus the assertion follows from Corollary 5.

Corollary 7. *If* $D(Z)$ *contains an invertible element, then each polynomial in* $B[X; D]_{(2)}$ *is* H*-separable.*

Now, we consider the following conditions:

(C_1) B is a commutative ring.

(C_2) The ideal of Z generated by $D(Z)$ contains a non zero divisor.

(C_3) Z is a semiprime ring.

We shall prove the following theorem, which is the first main results of this paper.

Theorem 8. *Assume that there holds one of the conditions* (C_1)-(C_3). *Then the following are equivalent:*

(a) $B[X; D]$ *contains an H-separable polynomial* f *of degree* 2.

(b) $B[X; D]_{(2)}$ *is non-empty,* Z *is a projective* Z^D*-module of rank* 2 *and* $\mathrm{Hom}_{Z^D}(Z, Z) = Z[D \mid Z]$, *that is,* Z/Z^D *is a purely inseparable Galois extension of exponent* 1 *in the sense of S. Yuan* [6].

(c) $B[X; D]_{(2)}$ *is non-empty, and there exist* $v_i, d_i \in Z$ *such that* $\sum_i v_i D(d_i) = 1$ *and* $\sum_i v_i d_i = 0$.

When this is the case, every polynomial in $B[X; D]_{(2)}$ *is H-separable, and* $f-g \in Z^D$ *for each* $f, g \in B[X; D]_{(2)}$.

Proof. Careful scrutiny of the proof of [1, Theorem 3.3] shows that (b) and (c) are equivalent without assuming (C_1)-(C_3), and (c) $\Rightarrow$ (a) by Corollary 5. It remains therefore to prove (a) $\Rightarrow$ (c). In virtue of [1, Theorem 3.3], the case of (C_1) is obvious. Let $\{u_i, v_i, c_i, d_i\}$ be a finite system of elements of B as in Lemma 4. In case (C_2) holds, (v) shows that $c_i = u_i = 0$, and therefore $\{d_i, v_i\}$ is a system of elements of Z, and (c) is satisfied. Now, suppose (C_3). By (v) and (vii), we have

$$c_k^2 = \sum_i v_i D(d_i) c_k^2 = -\sum_i v_i I_{d_k}(d_i) c_k = \sum_i v_i I_{d_i}(d_k) c_k$$
$$= -\sum_i v_i c_i D(d_k) c_k = \sum_i v_i c_i I_{d_k}(d_k) = 0,$$

whence $c_k = 0$. Similarly, we can show $u_k = 0$. Thus, we obtain (c).

Now, let $f = X^2 - Xa - b$ be an H-separable polynomial in $B[X; D]$. For any $g = X^2 - Xu - v \in B[X; D]_{(2)}$, we have $D^2 - u_r D = I_v$ and $v \in B^D$ (Lemma 1). Since $D^2 - a_r D = I_b$ and $b \in B^D$, we have $(u-a)_r D = I_{b-v}$ and $b - v \in B^D$. Then, by Lemma 2, we have $u = a$ and $v - b \in Z^D$. The rest of the assertion is clear by Lemma 4.

Let ρ be an automorphism of B, and $B[X; \rho]$ the skew polynomial ring in which the multiplication is defined by $aX = X\rho(a)$ $(a \in B)$. We define a separable (resp. H-separable) polynomial in $B[X; \rho]$ in the same way as in the case of $B[X; D]$. In [4], Nagahara has studied separable polynomials of degree 2 in $B[X; \rho]$ whose discriminants are in the Jacobson radical $J(B)$ of B. Now, we shall prove the following theorem for $B[X; D]$, which corresponds to the results of Nagahara [4, Theorems 1 and 2].

Theorem 9. *Let* $f = X^2 - Xa - b \in B[X; D]$.

(1) *Then the following are equivalent:*

(a) *f is separable in $B[X; D]$ and $\delta(f) = a^2+4b \in J(B)$.*
(b) *f is H-separable in $B[X; D]$ and $a \in J(B)$.*
When this is the case, $D(Z)$ contains an invertible element.
(2) *If $D(Z)$ contains an invertible element,* (a), (b) *are equivalent to*
(c) *f is in $B[X; D]_{(2)}$ and $a \in J(B)$.*

Proof. (1) (a) $\Rightarrow$ (b). In virtue of [2, Theorem 1.8] there exists $y = Xc+d \in B[X; D]$ such that $\alpha y = y\alpha$ ($\alpha \in B$) and $(X-a)(Xc+d)+(Xc+d)X \equiv 1 \pmod{fB[X; D]}$. By a brief computation, we obtain

$$
\begin{aligned}
&(\text{x}) && c \in Z,\\
&(\text{xi}) && c_r D = -I_d,\\
&(\text{xii}) && D(d)+2bc-ad = 1,\\
&(\text{xiii}) && D(c)+ac+2d = 0.
\end{aligned}
$$

Then, we see that

$$
\begin{aligned}
D(d)D(c) &= D(D(d)c)-D^2(d)c\\
&= -D^2(d)c && \text{(by (xi))}\\
&= -\{D(d)a+I_b(a)\}c && \text{(by (ii))}\\
&= -D(d)ac = -D(d)ca = 0 && \text{(by (iii), (x), (xi))}
\end{aligned}
$$

Hence

$$
\begin{aligned}
\delta(f)(c+dD(c)) &= (a^2+4b)(c+dD(c))\\
&= a^2c+4bc+a^2dD(c)+4bdD(c)\\
&= a\{-D(c)-2d\}+2\{1+ad-D(d)\}\\
&\quad +a\{D(d)+2bc-1\}D(c)\\
&\qquad\qquad \text{(by (i), (x), (xii), (xiii))}\\
&= -2aD(c)-2D(d)+aD(d)D(c)+2abcD(c)+2\\
&= 2 && \text{(by (i), (x), (xi))}
\end{aligned}
$$

Furthermore

$$
\begin{aligned}
\delta(f)(2c) &= \delta(f)(2c+2dD(c)) = 2\delta(f)(c+dD(c)) = 4.\\
\delta(f)(1-2bc) &= \delta(f)-\delta(f)(2c)b = a^2+4b-4b = a^2.
\end{aligned}
$$

Then, noting that $\delta(f) \in J(B)$, we see that $2,\ a^2 \in J(B)$. By (i), $Ba \subseteq aB+2B$. Hence it follows that $(BaB)^2 = BaBaB \subseteq Ba(aB+2B)B \subseteq Ba^2B+2B \subseteq J(B)$. Thus $BaB \subseteq J(B)$, and so $a \in J(B)$. Then we see that $D(d) = 1-(2bc-ad)$ is invertible in B by (xii). Since $D(d)c = 0$, we obtain $c = 0$, and so $d \in Z$. Then f is H-separable by Corollary 7.

(b) $\Rightarrow$ (a). By Corollary 3, we have $2 = 0$. Consequently, $\delta(f) = a^2 + 4b = a^2 \in J(B)$.

(2) This is clear by the proof of (1) (and Corollary 7).

In virtue of Theorems 8 and 9, we have the following which contains [3, Corollary 3.13].

Corollary 10. *If $B[X; D]$ contains a separable polynomial f of degree 2 with $\delta(f) = a^2+4b \in J(B)$, then $B[X; D]_{(2)} = \{f+z \mid z \in Z^D\} = \{g \in B[X; D] \mid g$ is a separable polynomial of degree $2\} = \{g \in B[X; D] \mid g$ is an H-separable polynomial of degree $2\}$.*

Combining Theorem 9 and [1, Theorem 3.1], we have the following which corresponds to [5, Theorem 2.1].

Corollary 11. *Suppose that B is a commutative ring. Let $f = X^2 - Xa - b \in B[X; D]_{(2)}$. Then f is a separable polynomial with $\delta(f) = a^2+4b \in J(B)$ if and only if $B[X; D]/fB[X; D]$ is an Azumaya B^D-algebra with $a \in J(B)$.*

REFERENCES

[1] S. IKEHATA : Azumaya algebras and skew polynomial rings, Math. J. Okayama Univ. 23 (1981), 19–32.

[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, M. J. Okayama Univ 19 (1976), 65–95.

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

[5] T. NAGAHARA : A note on imbeddings of non-commutative separable extensions in Galois extensions, Houston J. Math. 12 (1986), 411–417.

[6] S. YUAN : Inseparable Galois theory of exponent one, Trans. Amer. Math. Soc. 149 (1970), 163–170.

DEPARTMENT OF MATHEMATICS

OKAYAMA UNIVERSITY

TSUSHIMA-NAKA, OKAYAMA-SHI, JAPAN 700

(Received January 11, 1990)