Math. J. Okayama Univ. 33 (1991), 21 — 26

ON H-SEPARABLE POLYNOMIALS OF PRIME DEGREE

Dedicated to Professor Takasi Nagahara on his 60th birthday

SHÛICHI IKEHATA

In [3] and [4], the author has studied H-separable polynomials in skew polynomial rings. If the coefficient ring is commutative, the existence of H-separable polynomials in skew polynomial rings has been characterized in terms of Azumaya algebras and Galois extensions. However, if the coefficient ring is not commutative, we know few. In [8], we have studied on H-separable polynomials of degree 2 in skew polynomial rings of derivation type. In this paper, we shall study H-separable polynomials of prime degree in skew polynomial rings of automorphism type.

Throughout this paper, B will represent a ring with 1, and ρ an automorphism of B. Let $B[X;\rho]$ be the skew polynomial ring in which the multiplication is given by $bX = X\rho(b)$ $(b \in B)$. A monic polynomial f in $B[X;\rho]$ with $fB[X;\rho] = B[X;\rho]f$ is called a separable (resp. H-separable) polynomial if $B[X;\rho]/fB[X;\rho]$ is a separable (resp. H-separable) extension of B. As to terminologies used in this note, we follow [3].

In this note, we shall prove that $B[X;\rho]$ contains an H-separable polynomial of prime degree p if and only if the center Z of B is a Galois extension over Z^ρ with some conditions (Theorem 2). We shall also prove that if $f = X^p - u$ is a separable polynomial in $B[X;\rho]$ with prime degree p, and p is contained in the Jacobson radical of B, then f is an H-separable polynomial in $B[X;\rho]$ (Corollary 5).

We shall use the following conventions:

Z = the center of B.

$V_S(B)$ = the centralizer of B in S for a ring extension S/B.

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

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

First, we shall state the following

Lemma 1. *Assume that there exist a positive integer n and an invertible element u in B such that $\alpha u = u\rho^n(\alpha)$ $(\alpha \in B)$ and $\rho(u) = u$. Let l be a positive integer such that $(l, n) = 1$. If w is an element in B such that $\alpha w =$*

$w\rho^l(\alpha)$ (or $w\alpha = \rho^l(\alpha)w$) $(\alpha \in B)$, then $\rho^i(w)-\rho^j(w)$ are contained in the Jacobson radical $J(B)$ of B for all $i, j \geq 0$.

Proof. It is sufficient to prove $w-\rho(w)$ is contained in $J(B)$. Since $w^2 = w\rho^l(w)$, we have $w(w-\rho^l(w)) = 0$. Then, we obtain

$$\begin{aligned}(w-\rho^l(w))^3 &= (w-\rho^l(w))(w-\rho^l(w))(w-\rho^l(w))\\ &= (w-\rho^l(w))(-\rho^l(w))(w-\rho^l(w))\\ &= -w(w-\rho^l(w))(w-\rho^l(w))\\ &= 0.\end{aligned}$$

Hence $(w-\rho^l(w))B = B(w-\rho^l(w))$ is a nilpotent ideal of B, whence $w-\rho^l(w)$ is contained in $J(B)$. Since $(l, n) = 1$, we can easily see the assertion.

Now, we shall prove the following theorem which is a partial generalization of [3, Theorem 2.2].

Theorem 2. *Let p be a prime integer. Then, the following are equivalent:*

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

(b) *There exists an invertible element u in B such that $\alpha u = u\rho^p(\alpha)$ $(\alpha \in B)$, $\rho(u) = u$, and Z/Z^ρ is a G-Galois extension, where G is the group generated by $\rho|Z$ of order p.*

When this is the case, the set of all H-separable polynomials of degree ≥ 2 in $B[X;\rho]$ coincides with $\{X^p-uc \mid c$ is an invertible element in $Z^\rho\}$.

Proof. (b) $\Rightarrow$ (a). By [3, Proposition 1.4], X^p-u is an H-separable polynomial in $B[X;\rho]$.

(a) $\Rightarrow$ (b). By [4, Lemma 1], f is of the form X^p-u such that u is invertible in B, $\rho^p = (u^{-1})_l u_r$, and $\rho(u) = u$. By [3, Theorem 1.1], there exist $y_i = \sum_{k=0}^{p-1} X^k c_{i,k}$, $z_i = \sum_{k=0}^{p-1} X^k d_{i,k}$ in $B[X;\rho]$ such that $\alpha y_i = y_i\alpha$, $\rho^{p-1}(\alpha)z_i = z_i\alpha$ $(\alpha \in B)$ and $\sum_i y_i X^{p-1} z_i \equiv 1$, $\sum_i y_i X^k z_i \equiv 0 \pmod{fB[X;\rho]}$ $(0 \leq k \leq p-2)$. Then we have

(i) $\rho^k(\alpha)c_{i,k} = c_{i,k}\alpha$, $\rho^{p-1+k}(\alpha)d_{i,k} = d_{i,k}\alpha$ $(\alpha \in B)$ $(0 \leq k \leq p-1)$.

Now, we note that

$$1 \equiv \sum_i y_i X^{p-1} z_i = \sum_i \left(\sum_{r=0}^{p-1} X^r c_{i,r}\right) X^{p-1} \left(\sum_{s=0}^{p-1} X^s d_{i,s}\right)$$

$$= \sum_i \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} X^{p+r+s-1} \rho^{p+s-1}(c_{i,r}) d_{i,s}.$$

Since $X^p \equiv u \pmod{fB[X\,;\,\rho]}$ and $\rho^p = (u^{-1})_l u_r$, comparing the constant terms of both sides, we obtain

$$\begin{aligned} 1 &= \sum_i u\rho^p(c_{i,0}) d_{i,1} + \sum_i u\rho^{p-1}(c_{i,1}) d_{i,0} + \sum_i u^2 \sum_{j=2}^{p-1} \rho^{p+p-j}(c_{i,j}) d_{i,p-j+1} \\ &= \sum_i c_{i,0} u d_{i,1} + \sum_i u\rho^{p-1}(c_{i,1}) d_{i,0} + \sum_i \sum_{j=2}^{p-1} u\rho^{p-j}(c_{i,j}) u d_{i,p-j+1}. \end{aligned}$$

Next, we have

$$\begin{aligned} 0 &\equiv \sum_i y_i X^l z_i = \sum_i \sum_{r=0}^{p-1} (X^r c_{i,r}) X^l \Big(\sum_{s=0}^{p-1} X^s d_{i,s} \Big) \\ &= \sum_i \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} X^{l+r+s} \rho^{l+s}(c_{i,r}) d_{i,s}, \text{ for } 0 \le l \le p-2. \end{aligned}$$

Then, comparing the coefficients of the term X^{l+1} of both sides, we see that

$$0 = \sum_i \rho^{l+1}(c_{i,0}) d_{i,1} + \sum_i \rho^l(c_{i,1}) d_{i,0} + \sum_i \sum_{j=2}^{p-1} u\rho^{l+p-j+1}(c_{i,j}) d_{i,p-j+1}.$$

Therefore, we have

$$\begin{aligned} 1 = &\sum_i (c_{i,0} - \rho^{l+1}(c_{i,0})) u d_{i,1} + \sum_i (\rho^{p-1}(c_{i,1}) - \rho^l(c_{i,1})) u d_{i,0} \\ &+ \sum_i \sum_{j=2}^{p-1} u(\rho^{p-j}(c_{i,j}) - \rho^{l+p-j+1}(c_{i,j})) u d_{i,p-j+1}. \end{aligned}$$

Noting (i), it follows from Lemma 1 that the elements $\rho^{p-1}(c_{i,1}) - \rho^l(c_{i,1})$ and $\rho^{p-j}(c_{i,j}) - \rho^{l+p-j+1}(c_{i,j})$ $(2 \le j \le p-1)$ are contained in the Jacobson radical of B. Thus $\sum_i (c_{i,0} - \rho^{l+1}(c_{i,0})) u d_{i,1}$ is invertible in B, and so in Z $(0 \le l \le p-2)$. Since $\rho^p = (u^{-1})_l u_r$, the order of $\rho | Z$ coincides with p. Therefore, Z/Z^ρ is a $(\rho | Z)$-Galois extension by [1, Theorem 1.3 (f)]. The rest of the assertion follows from [4, Lemma 1 (3)] and [3, Proposition 1.4].

Now, we shall prove the following which is a partial generalization of [3, Theorem 2.2].

Corollary 3. *Let p be a prime number, and B an Azumaya Z-algebra. Let $f = X^p + X^{p-1} a_{p-1} + \cdots + a_0$ be in $B[X;\,\rho]$ with $fB[X;\,\rho] = B[X;\,\rho]f$,* *and* $S=B[X;\rho]/fB[X;\rho]$. *Then, f is an H-separable polynomial in* $B[X;\rho]$ *if and only if S is an Azumaya Z^{ρ}-algebra. When this is the case, there holds that Z/Z^{ρ} is a G-Galois extension, where G is the group generated by $\rho|Z$ of order p, and $f=X^{p}+a_0$. Moreover, the centralizer of B in S coincides with Z.*

Proof. Assume that S is an Azumaya Z^{ρ}-algebra. Since $S\supseteq B\supseteq Z^{\rho}$ and S_B is free, f is H-separable in $B[X;\rho]$ by [2, Theorem 1]. Then by [4, Lemma 1], $f=X^{p}+a_0$.

Conversely, we assume that f is an H-separable polynomial in $B[X;\rho]$. Since S/B is an H-separable extension and B is an Azumaya Z-algebra, it follows from [7, Theorem 1] that S is also Azumaya algebra over its center. Now, we shall prove $V_S(B)=Z$ and $V_S(S)=Z^{\rho}$. Put $x=X+fB[X;\rho]$ $\in S$. Then, for any $y=\sum_{i=0}^{p-1}x^{i}d_i$ in $V_S(B)$, we have $\rho^{i}(\alpha)d_i=d_i\alpha$ $(0\leq i\leq p-1,\ \alpha\in B)$. Hence, for all $\alpha\in Z$, we have $(\rho^{i}(\alpha)-\alpha)d_i=0$. Since Z/Z^{ρ} is a $(\rho|Z)$-Galois extension and the order of $\rho|Z$ is p (Theorem 2), it follows from [1, Theorem 1.3] that the ideal of Z generated by $\{\alpha-\rho^{i}(\alpha)\,|\,\alpha\in Z\}$ is equal to Z for $1\leq i\leq p-1$. Hence we have $d_i=0$ $(1\leq i\leq p-1)$, so $y=d_0\in V_B(B)=Z$, and $V_S(S)=Z^{\rho}$ is now clear.

In [6], Nagahara proved that if $f=X^2-Xa-b$ is a separable polynomial in $B[X;\rho]$ whose discriminant $\delta(f)=a^2+4b$ is contained in $J(B)$, then f is an H-separable polynomial in $B[X;\rho]$ ([6, Theorem 2]). In this case, the condition $\delta(f)\in J(B)$ implies $2\in J(B)$. In the prime power degree case, we shall prove the following

Theorem 4. *Let $f=X^{p^e}-u$ be a separable polynomial in $B[X;\rho]$. If p is a prime number, and p is contained in the Jacobson radical $J(B)$ of B, then f is an H-separable polynomial in $B[X;\rho]$.*

Proof. Since $fB[X;\rho]=B[X;\rho]f$, we have $\alpha u=u\rho^{p^e}(\alpha)$ $(\alpha\in B)$ and $\rho(u)=u$. In virtue of [5, Theorem 3.1], u is an invertible element in B and there exists an element c in Z such that

$$c+\rho(c)+\rho^{2}(c)+\cdots+\rho^{p^e-1}(c)=1.$$

Then, we have $(\rho|Z)^{p^e}=1_Z$. Let k be any integer such that $1\leq k\leq p^e-1$. If $(k,p^e)=p^i$ $(0\leq i\leq e-1)$, then $k=lp^i$, where $(l,p)=1$. We put here

$$d=c+\rho^{l}(c)+\rho^{2l}(c)+\cdots+\rho^{l(p^i-1)}(c)\ (\in Z).$$

Since $1 = \sum_{j=0}^{p^e-1} \rho^j(c) = \sum_{j=0}^{p^e-1} \rho^{tj}(c)$, we have

$$d+\rho^k(d)+\rho^{2k}(d)+\cdots+\rho^{k(p^{e-i}-1)}(d) = 1.$$

On the other hand, we obtain

$$\begin{aligned} 1-p^{e-i}\rho^k(d) &= d-\rho^k(d)+\sum_{s=2}^{p^{e-i}-1} \{\rho^{ks}(d)-\rho^k(d)\} \\ &= d-\rho^k(d)+\sum_{s=2}^{p^{e-i}-1}\sum_{j=1}^{s-1}\{(\rho^k)^{j-1}(d)-(\rho^k)^j(d)\}. \end{aligned}$$

Since $p \in J(B)$, $1-p^{e-i}\rho^k(d)$ is invertible in B, and so in Z. Therefore we see that the ideal of Z generated by $\{\alpha-\rho^k(\alpha) \mid \alpha \in Z\}$ coincides with Z and the order of $\rho \mid Z$ is equal to p^e. Hence by [1, Theorem 1.3], Z/Z^ρ is a $(\rho \mid Z)$-Galois extension. Thus, f is an H-separable polynomial in $B[X; \rho]$ by Theorem 2.

Corollary 5. *Let $f = X^p - u$ be a separable polynomial in $B[X; \rho]$. If p is a prime number and p is contained in the Jacobson radical $J(B)$ of B, then f is an H-separable polynomial in $B[X; \rho]$.*

We shall conclude our study with the following example which shows that in Theorem 4, if p is not prime power number, the assertion is not true.

Example. Let $B = \mathrm{GF}(3^3)$ and ρ the automorphism of B of order 3. Then B is a Galois extension over GF(3), and so, there exists an element α in B such that $\alpha+\rho(\alpha)+\rho^2(\alpha) = 1$. If we put $c = 2^{-1}\alpha$, then we obtain $c+\rho(c)+\cdots+\rho^5(c) = 1$. Therefore, by [5, Theorem 3.1], $f = X^6-1$ is a separable polynomial in $B[X; \rho]$ with $6 = 0$. Since the set of all H-separable polynomials in $B[X; \rho]$ is equal to $\{X^3-1, X^3-2\}$ ([3, Theorem 2.2]), f is not an H-separable polynomial in $B[X; \rho]$.

REFERENCES

[1] S. U. CHASE, D. K. HARRISON and A. ROSENBERG : Galois theory and Galois cohomology of commutative ring, Mem. Amer. Math. Soc. **52** (1965), 15–33.

[2] S. IKEHATA : Note on Azumaya algebras and H-separable extensions, Math. J. Okayama Univ. **23** (1981), 17–18.

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

[4] S. IKEHATA : Azumaya algebras and skew polynomial rings. II, Math. J. Okayama Univ. **26**

(1984), 49−57.
[5] Y. MIYASHITA : On a skew polynomial ring, J. Math. Soc. Japan **31** (1979), 317−330.
[6] T. NAGAHARA : Some *H*-separable polynomials of degree 2, Math. J. Okayama Univ. **26** (1984), 87−90.
[7] H. OKAMOTO : On projective *H*-separable extensions of Azumaya algebras, Results in Mathematics **14** (1988), 330−332.
[8] H. OKAMOTO and S. IKEHATA : On *H*-separable polynomials of degree 2, Math. J. Okayama Univ. 32 (1990), 53−59.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY
TSUSHIMA-NAKA, OKAYAMA-SHI, JAPAN 700

(*Received January 19, 1991*)