Mathematical Journal of Okayama University

Volume 40, *Issue* 1 1998 *Article* 9

JANUARY 1998

Purely Inseparable Ring Extensions and H-Separable Polynomials

Shûichi Ikehata*

*Okayama University

Math. J. Okayama Univ. 40 (1998), 55-63 [2000]

PURELY INSEPARABLE RING EXTENSIONS AND H-SEPARABLE POLYNOMIALS

SHÛICHI IKEHATA

1. Introduction

Purely inseparable ring extensions of exponent one has been studied by S. Yuan ([17], [18]), and G. Georgantas ([2]). In the theory, derivations play a role analogous to that of automorphisms in the theory of cyclic Galois extensions. H-separable polynomials in skew polynomial rings has been studied in [6, 7, 8, 9, 10, 13, 15, 16]. If the coefficient ring is commutative, the existence of H-separable polynomials has been characterized in terms of Azumaya algebras and purely inseparable extensions ([6]). However, if the coefficient ring is non-commutative, we have only results without satisfaction. Concerning skew polynomial rings of derivation type, in [15] we studied H-separable polynomials of degree 2.
The purpose of this paper is to give some generalizations and sharpening of the results in [6] and [15]. Our first main result is the following: If the skew polynomial ring of derivation type $B[X;D]$ contains an H-separable polynomial f of degree $m \geq 2$, then necessarily B is of prime characteristic p, and f is a p-polynomial of the form $\sum_{j=0}^{e} X^{p^j} b_{j+1} + b_0$ $(m = p^e)$, and the center of $B[X;D]$ coincides with $Z^D[f]$, where Z is the center of B, and $Z^D = \{a \in Z | D(a) = 0\}$ (See Theorem 2.2). By using a purely inseparable extension and an H-separable polynomial, we shall give a construction theorem: Let B be an Azumaya Z-algebra, and Z a purely inseparable extension of exponent one over a ring A. Then there exists an Azumaya A-algebra S such that B can be embedded as the centralizer of Z in S (See Theorem 2.4). This theorem was proved for central simple algebras by K. Hoechsmann ([3]). As an application, the present study contains a sharpening of a result of K. A. Knus, M. Ojanguren and D. J. Saltman [12, Theorem 6.3] and some related results of G. Georgantas [2, Theorems 1,2].
Throughout this paper, B will represent a ring with 1, D a derivation of B. We denote by $B[X;D]$ the skew polynomial ring defined by $aX = Xa + D(a)$ $(a \in B)$. By $B[X;D]_{(0)}$, we denote the set of all monic polynomials g in $B[X;D]$ such that $gB[X;D] = B[X;D]g$. A ring extension T/S is called a *separable* extension, if the T-T-homomorphism of $T \otimes_S T$ onto T defined by $a \otimes b \to ab$ splits, and T/S is called an *H-separable* extension, if $T \otimes_S T$ is T-T-isomorphic to a direct summand of a finite direct

---

1991 *Mathematics Subject Classification.* 16W25, 16S36.

Key words and phrases. Derivation, Skew polynomial rings, H-separable extensions, Purely inseparable extensions of exponent one.

Mathematical Journal of Okayama University, Vol. 40 [1998], Iss. 1, Art. 9

sum of copies of T. As is well known every H-separable extension is a separable extension. A polynomial g in $B[X;D]_{(0)}$ is called *separable* (resp. *H-separable*) if $B[X;D]/gB[X;D]$ is a *separable* (resp. *H-separable*) extension of B. A ring extension B/A of commutative rings is called a *purely inseparable extension of exponent one with* δ, if ${}_AB$ is a finitely generated projective module of finite rank and $\mathrm{Hom}({}_AB, {}_AB) = B[\delta]$, where δ is a derivation of B and $A = \{a \in B | \delta(a) = 0\}$. ([17], [18])
In this paper, we shall use the following conventions.
Z = the center of B.
$V_B(A)$ = the centralizer of A in B for a ring extension B/A.
u_ℓ (resp.u_r) = the left (resp. right) multipliction effected by $u \in B$.
$B^D = \{a \in B | D(a) = 0\}$, where D is a derivation of B.
$D|A$ = the restriction of D to a suburing A of B.
I_u = the inner derivation effected by u, that is, $I_u = u_\ell - u_r$.
$D^*: B[X;D] \to B[X;D]$ is the derivation defined by $D^*(\sum_i X^i d_i) = \sum_i X^i D(d_i)$.

2. H-SEPARABLE POLYNIMIALS.

First, we shall state the following lemma which is a generalization of [15, Lemma 2] and corresponds to [7, Lemma 1].

Lemma 2.1. *Let* $f = X^m + X^{m-1}a_{m-1} + \cdots + Xa_1 + a_0$ *be in* $B[X;D]_{(0)}$ *and* $m \geq 2$. *If* f *is an H-separable polynomial in* $B[X;D]$, *then there holds the following:*
(1) If $\sum_{j=0}^{m-1} (\beta_j)_\ell D^j = I_u$ $(\beta_j \in B, u \in B^D)$, *then* $\beta_j = 0$ $(0 \leq j \leq m-1)$ *and* $u \in Z^D$.
(2) If $\sum_{j=0}^{m-1} (\beta_j)_r D^j = I_u$ $(\beta_j \in B, u \in B^D)$, *then* $\beta_j = 0$ $(0 \leq j \leq m-1)$ *and* $u \in Z^D$.

Proof. (1) Assume that $\sum_{j=0}^{m-1} \beta_j D^j(a) = ua - au$ $(a \in B)$. Then

$$\sum_{j=0}^{m-1} D(\beta_j)D^j(a) + \sum_{j=0}^{m-1} \beta_j D^j(D(a)) = uD(a) - D(a)u.$$

Hence we have $\sum_{j=0}^{m-1} D(\beta_j)_\ell D^j = 0$. An easy induction shows that

$$\sum_{j=0}^{m-1} D^\nu(\beta_j)_\ell D^j = 0 \ (\nu \geq 1) \ and \ \sum_{j=0}^{m-1} (\beta_j)_\ell D^j = I_u.$$

Then for all $h = \sum_{k=0}^{r} X^k d_k \in B[X;D]$, we have

$$\begin{aligned}
\sum_{j=0}^{m-1} \beta_j D^{*j}(h) &= \sum_{j=0}^{m-1} \beta_j (\sum_{k=0}^{r} X^k D^j(d_k)) \\
&= \sum_{j=0}^{m-1} \sum_{k=0}^{r} (\sum_{\nu=0}^{k} X^\nu \binom{k}{\nu} D^{k-\nu}(\beta_j) D^j(d_k)) \\
&= \sum_{k=0}^{r} \sum_{\nu=0}^{k} X^\nu \binom{k}{\nu} (\sum_{j=0}^{m-1} D^{k-\nu}(\beta_j) D^j(d_k)) \\
&= \sum_{\nu=0}^{r} X^\nu \sum_{k=\nu}^{r} \binom{k}{\nu} (\sum_{j=0}^{m-1} D^{k-\nu}(\beta_j) D^j(d_k)) \\
&= \sum_{\nu=0}^{r} X^\nu (\sum_{k=\nu+1}^{r} \binom{k}{\nu} \sum_{j=0}^{m-1} D^{k-\nu}(\beta_j) D^j(d_k)) \\
&\quad + \sum_{\nu=0}^{r} X^\nu (\sum_{j=0}^{m-1} \beta_j D^j(d_\nu)) \\
&= \sum_{\nu=0}^{r} X^\nu (I_u(d_\nu)) = I_u^*(h).
\end{aligned}$$

Since f is an H-separable polynomial in $B[X;D]$, it follows from [6, Lemma 1.5] that there exist $y_i, z_i \in B[X;D]$ with $\deg y_i < m$ and $\deg z_i < m$ such that $ay_i = y_i a, az_i = z_i a$ $(a \in B)$. and

$$\sum_i D^{*m-1}(y_i) z_i \equiv 1, \sum_i D^{*k}(y_i) z_i \equiv 0 \ (\mathrm{mod} f B[X;D]) \ (0 \leq k \leq m-2).$$

Then we have

$$\beta_{m-1} = \sum_{j=0}^{m-1} \sum_i \beta_j D^{*j}(y_i) z_i \equiv 0 \ (\mathrm{mod} f B[X;D]).$$

This implies $\beta_{m-1} = 0$ and $\sum_{j=0}^{m-2} \beta_j D^{*j} = I_u^*$. Since $\sum_{j=0}^{m-2} \beta_j D^{*j+1} = I_u^* D^* = D^* I_u^*$ and $uy_i = y_i u$, we have

$$\begin{aligned}
\beta_{m-2} &= \sum_{j=0}^{m-2} \sum_i \beta_j D^{*j+1}(y_i) z_i \\
&= \sum_i D^*(I_u^*(y_i)) z_i \equiv 0 \ (\mathrm{mod} f B[X;D]).
\end{aligned}$$

Repeating this procedure, we conclude that $\beta_j = 0$ $(0 \leq k \leq m-2)$, and $u \in Z$. Similarly, we can prove (2). □

The following is a sharpening of [15, Corollary 3], and a partial generalization of [6, Theorem 3.1]. We realize that the existence of an H-separable polynomial is very strong condition.

Theorem 2.2. *If $B[X;D]$ contains an H-separable polynomial f of degree $m \geq 2$, then we have the following:*
(1) B is of prime characteristic p and f is a p-polynomial of the form

$$\sum_{j=0}^{e} X^{p^j} b_{j+1} + b_0 \ (m = p^e),\ \ b_{j+1} \in Z^D \ (0 \leq j \leq e) \text{ and } b_0 \in B^D.$$

(2) The center of $B[X;D]$ coincides with $Z^D[f]$, that is, $V_{B[X;D]}(B[X;D]) = Z^D[f]$.
(3) Every H-separable polynomial in $B[X;D]$ is of the form $f + c_0$, where c_0 is an element in Z^D.

Proof. (1) Let $f = X^m + X^{m-1}a_{m-1} + \cdots + Xa_1 + a_0$. By [4, Lemma 1.6], we have

$$a_i a = \sum_{j=i}^{m} \binom{j}{i} D^{j-i}(a) a_j \ (a \in B,\ 0 \leq j \leq m-1)$$

and

$$a_i \in B^D \ (0 \leq i \leq m-1).$$

Hence by Lemma 2.1, we obtain

$$\binom{m}{i} = 0 \ (1 \leq i \leq m-1) \text{ and } \binom{j}{i} a_j = 0 \ (1 \leq i < j \leq m-1).$$

Then by the same arguments in the proof of [6, Theorem 3.1], we see that B is of prime characteristic p, and f is a p-polynomial of the form $\sum_{j=0}^{e} X^{p^j} b_{j+1} + b_0$ $(m = p^e)$. Since $af = fa$, and $aX^{p^j} = X^{p^j}a + D^{p^j}(a)$ $(a \in B)$, we have $b_{j+1} \in Z^D$ $(0 \leq j \leq e)$.
(2) Since $Xf = fX$ and $af = fa$ $(a \in B)$, we see that f is contained in the center of $B[X;D]$. Next, assume $g \in V_{B[X;D]}(B[X;D])$. Then since f is monic and of degree p^e, there exist $h, r \in B[X;D]$ such that $g = hf + r$ and $\deg r < p^e$. Noting that $g, f \in V_{B[X;D]}(B[X;D])$, we obtain $(ah - ha)f = ra - ar$ for all $a \in B$, and $(Xh - hX)f = rX - Xr$. Since $\deg f = p^e > \deg(ra - ar), \deg(rX - Xr)$, it follows that $ra = ar$, $ah = ha$, $rX = Xr$, and $Xh = hX$. Hence $r, h \in V_{B[X;D]}(B[X;D])$. We put here $r = \sum_{j=0}^{p^e-1} X^j d_j$ $(d_j \in B^D)$. Since $ra = ar$, we have $\sum_{j=0}^{p^e-1} D^j(a) d_j = d_0 a$ $(a \in B)$, that is, $\sum_{j=1}^{p^e-1} (d_j)_r D^j = I_{d_0}$. Then by Lemma 2.1, we have $d_j = 0$ $(1 \leq k \leq p^e - 1)$. Hence we obtain $r = d_0 \in Z^D$. Replacing g by h, we repeat the same method. Then we see that there exist $h_1 \in V_{B[X;D]}(B[X;D])$ and $d_1 \in Z^D$ such that $h = h_1 f + d_1$. Repeating this, we see that g is contained in $Z^D[f]$.

(3) Let g be any H-separable polynomial of degree n in $B[X;D]$. Then by Lemma 2.1 and [4, Lemma 1.6], we see that $n = p^e$, and $g = f + c_0$, for some $c_0 \in Z^D$. □

Corresponding to [6, Proposition 1.4], we have the following

Proposition 2.3. *Let B be a ring with its center Z, D a derivation of B, and $\delta = D|Z$. Assume that Z/Z^δ is a purely inseparable extension of exponent one with δ, Z is a projective module over Z^δ of rank p^e, and δ satisfies the minimal polynomial $t^{p^e} + t^{p^{e-1}}\alpha_e + \cdots + t^p\alpha_2 + t\alpha_1 (\alpha_i \in Z^\delta)$. If there exists an element u in B^D such that $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = I_u$, then there hold the following:*
(1) $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u$ is an H-separable polynomial in $B[X;D]$.
(2) $V_{B[X;D]}(B) = Z[f]$, and $V_{B[X;D]}(B[X;D]) = Z^\delta[f]$.
(3) $B[X;D]_{(0)} = \{\ h(f) \mid h(t)$ is a monic polynomial in $Z^\delta[f]\}$.
(4) $\{\ g \in B[X;D] \mid g$ is an H-separable polynomial in $B[X;D]\} = \{\ f + z \mid z \in Z^\delta\}$.

Proof. (1) Since $\alpha_i \in B^D$ $(1 \le i \le e)$ and $aX^{p^j} = X^{p^j}a + D^{p^j}(a)$ $(a \in B, 1 \le j \le e)$, we have $Xf = fX$ and $af = fa$, and hence f is contained in the center of $B[X;D]$ and so in $B[X;D]_{(0)}$. Since Z/Z^δ is a purely inseparable extension of exponent one with δ, it follows from [6, Theorem 3.3(d)] that there exist $x_i, y_i \in Z$ such that

$$\sum_i \delta^{p^e-1}(x_i)y_i = 1 \text{ and } \sum_i \delta^k(x_i)y_i = 0 \ (0 \le k \le p^e - 2).$$

Thus f is H-separable in $B[X;D]$ by [6, Lemma 1.5].
(2) Let $g \in V_{B[X;D]}(B)$. Then since f is monic and of degree p^e, there exist $h, r \in B[X;D]$ such that $g = hf + r$ and $\deg r < p^e$. Noting that $g, f \in V_{B[X;D]}(B)$, we obtain $(ah - ha)f = ra - ar$ for all $a \in B$. Since $\deg f = p^e > \deg(ra - ar)$, it follows that $ra = ar$, and $ah = ha$. Hence $r, h \in V_{B[X;D]}(B)$. We put here $r = \sum_{j=0}^{p^e-1} X^j d_j$ $(d_j \in B)$. Since $ra = ar$, we have $\sum_{j=0}^{p^e-1} D^j(a)d_j = d_0 a$ $(a \in B)$. Then since $\sum_i \delta^{p^e-1}(x_i)y_i = 1$ and $\sum_i \delta^k(x_i)y_i = 0$ $(0 \le k \le p^e - 2)$, we obtain

$$d_k = \sum_{j=0}^{p^e-1}\sum_i D^{j+p^e-1-k}(x_i)y_i d_j - d_0 \sum_i D^{p^e-1-k}(x_i)y_i = 0$$

for all $1 \le k \le p^e - 1$. Hence we have $r = d_0 \in Z$. Replacing g by h, we repeat the same argument. Then we see that there exist $h_1 \in V_{B[X;D]}(B)$ and $d_1 \in Z$ such that $h = h_1 f + d_1$. Repeating this, we obtain g is contained in $Z[f]$. By Theorem 2.2 (2), we already know $V_{B[X;D]}(B[X;D]) = Z^\delta[f]$. This completes the proof of (2).
(3) If g is monic, then $c_s = 1$. Thus we obtain the assertion.

(4) It is clear that $f+z$ is contained in $B[X;D]_{(0)}$ for any $z \in Z^{\delta}$. We already have elements $x_i, y_i \in Z$ such that

$$\sum_i \delta^{p^e-1}(x_i)y_i = 1 \text{ and } \sum_i \delta^k(x_i)y_i = 0 \ (0 \le k \le p^e-2).$$

Hence, it follows from [6, Lemma 1.5] that $f+z$ is an H-separable polynomial in $B[X;D]$. □

The following theorem corresponds to [7, Theorem 2] which treats to the case whose coefficient ring is an Azumaya algebra.

Theorem 2.4. *Let B be an Azumaya Z-algebra, D a derivation of B, and $\delta = D|Z$. Assume that Z/Z^{δ} is a purely inseparable extension of exponent one with δ, and δ satisfies the minimal polynomial $t^{p^e} + t^{p^{e-1}}\alpha_e + \cdots + t^p\alpha_2 + t\alpha_1 (\alpha_i \in Z^{\delta})$. If there exists an element u in B^D such that $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = I_u$, then there hold the following:*
(1) $B[X;D]$ is an Azumaya $Z^{\delta}[f]$-algebra, where $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u$.
(2) For any $z \in Z^{\delta}$, we put $S_z = B[X;D]/(f+z)B[X;D]$. Then S_z is an Azumaya Z^{δ}-algebra with $V_{S_z}(Z) = B$ and $V_{S_z}(B) = Z$.

Proof. (1) By Proposition 2.3.(2), the center of $B[X;D]$ coincides with $Z^{\delta}[f]$. Let

$$\hat{D} : B[f] \to B[f] \text{ be the derivation defined by } \hat{D}(\sum_i f^i d_i) = \sum_i f^i D(d_i).$$

We put here

$$h = Y^{p^e} + Y^{p^{e-1}}\alpha_e + \cdots + Y^p\alpha_2 + Y\alpha_1 - u - f \in B[f][Y;\hat{D}],$$

where Y is an indeterminate and $\beta Y = Y\beta + \hat{D}(\beta)$ $(\beta \in B[f])$. Then h is in the center of $B[f][Y;\hat{D}]$. Since Z/Z^{δ} is a purely inseparable extension of exponent one with δ, it is obvious that $Z[f]/Z^{\delta}[f]$ is also a purely inseparable extension of exponent one with $\hat{D}|Z[f]$. We see that $\hat{D}^{p^e} + \alpha_e\hat{D}^{p^{e-1}} + \cdots + \alpha_2\hat{D}^p + \alpha_1\hat{D} = I_u$. Hence by Proposition 2.3, h is an H-separable polynomial in $B[f][Y;\hat{D}]$. Let $\phi : B[f][Y;\hat{D}] \to B[X;D]$ be the mapping defined by $\phi(\sum_i Y^i\beta_i) = \sum_i X^i\beta_i$ $(\beta_i \in B[f])$. Since $\beta Y = Y\beta + \hat{D}(\beta)$ $(\beta \in B[f])$, ϕ is $B[f]$-ring epimorphism. Now we shall show that

$$\ker\phi = hB[f][Y;\hat{D}].$$

Obviously, $h \in \ker\phi$. Let $g \in \ker\phi$. Then there exists $q, r \in B[f][Y;\hat{D}]$ such that $g = qh + r, \deg r < \deg h = p^e$. We denote $r = \sum_{k=0}^{p^e-1} Y^k\beta_k, \beta_k \in B[f]$. Then $\phi(g) = \phi(r) = \sum_{k=0}^{p^e-1} X^k\beta_k = 0$. Suppose there exists k such that $\beta_k \neq 0$. Let $\beta_k = f^{n_k}c_k +$ (lower terms), $c_k \neq 0$. We consider the largest suffix s such that n_s is the largest number. Then the highest degree term in $\sum_{k=0}^{p^e-1} X^k\beta_k$ equals to $X^{n_s p^e + s}c_s \neq 0$, which is a contradiction. Hence we have $r = 0$, and so, $\ker\phi = hB[f][Y;\hat{D}]$. Thus we have a $B[f]$-ring isomorphim

$$B[f][Y;\hat{D}]/hB[f][Y;\hat{D}] \cong B[X;D].$$

Hence $B[X;D]$ is an H- separable extension over $B[f]$. Since B is an Azumaya Z-algebra, $B[f]$ is also Azumaya over $Z[f]$. Then it follows from [14, Theorem 1] that $B[X;D]$ is an Azumaya algebra.
(2) Considering the canonical epimorphism $B[X;D] \to S_z = B[X;D]/(f + z)B[X;D]$ defined by $X \to X + (f+z)B[X;D]$, we see that S_z is Azumaya Z^δ-algebra. Then by Proposition 2.3 (2), we have $V_{S_z}(B) = Z$. Finally, $V_{S_z}(Z) = B$ follows from [16, Proposition 3.2]. □

As a special case of Theorem 2.4, we have the following which relates to a theorem of G. Georgantas [2, Theorem 1].

Corollary 2.5. *Let B be a commutative ring, D a derivation of B, and $A = B^D$. Assume that B/A is a purely inseparable extension of exponent one with D, and D satisfies the minimal polynomial $t^{p^e} + t^{p^{e-1}}\alpha_e + \cdots + t^p\alpha_2 + t\alpha_1 (\alpha_i \in A)$. Then there holds the following:*
(1) $B[X;D]$ is an Azumaya $A[f]$-algebra, and $V_{B[X;D]}(B[f]) = B[f]$, where $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1$.
(2) For any $a \in A, S_a = B[X;D]/(f+a)B[X;D]$ is an Azumaya A-algebra with $V_{S_a}(B) = B$.

In the Theorem 2.4, if α_1 is an invertible element in Z^δ, then necessarily we can take an element $u \in B^D$ such that $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = I_u$. Precisely, we have

Proposition 2.6. *Let B be an Azumaya Z-algebra, D a derivation of B, and $\delta = D|Z$. Assume that Z/Z^δ is a purely inseparable extension of exponent one with δ, and δ satisfies the minimal polynomial $t^{p^e} + t^{p^{e-1}}\alpha_e + \cdots + t^p\alpha_2 + t\alpha_1 (\alpha_i \in Z^\delta)$. If α_1 is an invertible element in Z^δ, then there exists an element $u \in B^D$ such that $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = I_u$.*

Proof. Since B is separable over Z and the derivation $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D$ equals to zero on the center Z, it is an inner derivarion of B. Hence there is an element $w \in B$ such that $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = I_w$. Since $\alpha_i \in Z^\delta$, we have $DI_w = I_w D$. Hence $D(w) \in Z$. By $I_w(w) = 0$, we see that

$$D^{p^e-1}(w) + \alpha_e D^{p^{e-1}-1}(w) + \cdots + \alpha_2 D^{p-1}(w) + \alpha_1 w \in B^D.$$

Hence $\alpha_1 w \in Z + B^D$. Then since α_1 is invertibe in Z^δ, we can take an element u in B^D such that $I_w = I_u$. □

The following is a generalization of [12, Theorem 6.3] and correspond to [2, Theorem 2].

Mathematical Journal of Okayama University, Vol. 40 [1998], Iss. 1, Art. 9

Theorem 2.7. *Let A be a commutative ring. Suppose E is an Azumaya A-algebra and suppose E contains a commutative subalgebra Z such that ${}_ZE$ is a projective module, Z/A is a purely inseparable extension of exponent one with δ, ${}_AZ$ is a projective module of rank p^e, and δ satisfies a minimal polynomial $t^{p^e}+t^{p^{e-1}}\alpha_e+\cdots+t^p\alpha_2+t\alpha_1(\alpha_i \in A)$. We put $B = V_E(Z)$. Then there exists a derivation D of B which is an extension of δ, and an element u in B^D such that E is B-ring isomorphic to $B[X;D]/(X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u)B[X;D]$.*

Proof. By [12, Theorem 4.1], B is an Azumaya Z-algebra. By [12, Theorem 6.1], δ extends to a derivation Δ of E. Since $\delta(Z) \subset Z$, we have $\Delta(B) \subset B$. Since E is a separable A-algebra, and Δ is an A-derivation, Δ is an inner derivation of E. Hence there is $v \in E$ such that $\Delta(c) = cv - vc$ $(c \in E)$. Then we have $cv^{p^j} = v^{p^j}c + \Delta^{p^j}(c)$ $(j \geq 0)$. Hence $c(v^{p^e} + v^{p^{e-1}}\alpha_e + \cdots + v^p\alpha_2 + v\alpha_1) - (v^{p^e} + v^{p^{e-1}}\alpha_e + \cdots + v^p\alpha_2 + v\alpha_1)c = (\Delta^{p^e} + \alpha_e\Delta^{p^{e-1}} + \cdots + \alpha_2\Delta^p + \alpha_1\Delta)(c)$. That is, $\Delta^{p^e} + \alpha_e\Delta^{p^{e-1}} + \cdots + \alpha_2\Delta^p + \alpha_1\Delta = I_u$, where $u = v^{p^e} + v^{p^{e-1}}\alpha_e + \cdots + v^p\alpha_2 + v\alpha_1$. Since $(\Delta^{p^e} + \alpha_e\Delta^{p^{e-1}} + \cdots + \alpha_2\Delta^p + \alpha_1\Delta)|Z = \delta^{p^e} + \alpha_e\delta^{p^{e-1}} + \cdots + \alpha_2\delta^p + \alpha_1\delta = 0$, it follows that u is contained in $V_E(Z) = B$. We denote here E', the subalgebra of E generared by B and v, and put $D = \Delta|B$. Since $D(u) = \Delta(u) = uv - vu = 0$, the polynomial $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u$ is contained in $B[X;D]_{(0)}$. Then there is a B-ring epimorphism

$$\phi : B[X;D]/fB[X;D] \to E'$$

defined by $\phi(X) = v$. By Theorem 2.4, $B[X;D]/fB[X;D]$ is an Azumaya A-algebra. Then since ϕ is B-ring epimorphism, we have that ϕ is an isomorphism. Hence E' is an Azumaya A-algebra. Since $V_E(E') \subset V_E(B) = Z, V_E(E')$ is commutative. By the double centralizer theorem [1, Theorem 4.3, p.57], we have $V_E(E') = A$ and $E' = E$. □

References

[1] F. DeMeyer and F. Ingraham: Separable algebras over a commutative ring, Lecture Notes in Math. **181**, Springer, Berlin, 1971.

[2] G. Georgantas: Inseparable Galois cohomology, J. Algebra **38** (1976), 368–379.

[3] K. Hoechsmann: Simple algebras and derivations, Trans. Amer. Math. Soc. **180** (1963),1–12.

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

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

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

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

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

[9] S. Ikehata and G. Szeto: On H-separable polynomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ. **34** (1992), 49–55.
[10] S. Ikehata and G. Szeto: On H-skew polynomial rings and Galois extensions, Rings, extensions, and cohomology (Evanston, IL, 1993), 113–121, Lecture Notes in Pure and Appl. Math., **159**, Dekker, New York, 1994.
[11] R. Irving: Prime ideals of Ore extensions over commutative rings. II, J. Algebra **58** (1979), 399–423.
[12] K. A. Knus, M. Ojanguren and D. J. Saltman: On Brauer groups in characteristic p, Lecture Notes in Mathematics **549**, Springer, Berlin 1976, 25–49.
[13] Y. Miyashita: On a skew polynomial ring, J. Math. Soc. Japan **31** (1979), 317–330.
[14] H. Okamoto: On projective H-separable extensions of Azumaya algebras, Results in Mathematics **14** (1988), 330–332.
[15] H. Okamoto and S. Ikehata: On H-separable polynomials of degree 2, Math. J. Okayama Univ. **32** (1990), 53–59.
[16] S. Szeto and L. Xue: On the Ikehata theorem for H-separable skew polynomial rings, Math. J. Okayama Univ., **40** (1998), 27–32.
[17] S. Yuan: On logarithmic derivatives, Bull. Soc. Math. France, **96** (1968), 41–52.
[18] S. Yuan: Inseparable Galois theory of exponent one, Trans. Amer. Math. Soc. **149** (1970), 163–170.

SHÛICHI IKEHATA
DEPARTMENT OF MATHEMATICAL SCIENCE
FACULTY OF ENVIRONMENTAL SCIENCE AND TECHNOLOGY
OKAYAMA UNIVERSITY
TSUSHIMA, OKAYAMA 700-8530, JAPAN

(Received May 12, 1999)
(Revised June 4, 1999)