Math. J. Okayama Univ. **41** (1999), 63–69

PURELY INSEPARABLE RING EXTENSIONS AND AZUMAYA ALGEBRAS

Dedicated to Professor Takasi Nagahara on his 70th birthday

SHÛICHI IKEHATA

Throughout this paper, B will mean a ring with prime characteristic p, 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 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 $A = \{a \in B \mid \delta(a) = 0\}$. (cf. [2], [10], [11])

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) multiplication effected by $u \in B$.

$B^D = \{a \in B \mid D(a) = 0\}$, where D is a derivation of B.

$D|A$ = the restriction of D to a subring A of B.

$\mathrm{Der}_A(B)$ = the set of all A-derivations of B.

I_u = the inner derivation effected by u, that is, $I_u = u_\ell - u_r$.

In the previous paper [7], we have studied purely inseparable extensions of exponent one and H-separable polynomials in the skew polynomial rings of derivation type over non commutative rings. In particular we considered Azumaya algebras whose centers are purely inseparable extensions

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

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

of exponent one over their constant rings. Then we constructed new Azumaya algebras. In this paper, some results in [7] will be generalized and sharpened. For example, in [7] we have proved the following: *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 $B[X; D]$ is an Azumaya $Z^{\delta}[f]$ -algebra, where $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u$.* ([7, Theoren 2.4]). Since B is separable over Z, it is clear that $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = I_u$ for some u in B. It is important that u is contained in B^D, which is assumed in the above. However, necessarily we can take such u in B^D (Theorem 2). Moreover, we have more results when we can take $I_u = 0$ (Theorem 5).

First, we shall state the following lemma which is immediate by [4 , Theorem 4.1].

Lemma 1. *Let Z be a commutative ring of prime characteristic p. Let $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0$ $(\alpha_i \in Z^{\delta})$ be in $Z[X;\delta]_{(0)}$. Then f is a separable polynomial in $Z[X;\delta]$ if and only if there exists an element c in Z such that*

$$\delta^{p^e-1}(c) + \alpha_e \delta^{p^{e-1}-1}(c) + \cdots + \alpha_2\delta^{p-1}(c) + \alpha_1 c = 1.$$

Now, we are in a position to prove the following theorem which is a sharpenning of [7, Theorem 2.4, Proposition 2.6] and a generalization of [3, Theorem4.1].

Theorem 2. *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, Z is a projective module over Z^{δ} of rank p^e, and δ satisfies the minimal polynomial*

$$t^{p^e} + t^{p^{e-1}}\alpha_e + \cdots + t^p\alpha_2 + t\alpha_1 (\alpha_i \in Z^{\delta}).$$

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 $D(w) \in Z$. Since Z/Z^{δ} is a purely inseparable extension of exponent one with

δ, $X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1$ is an H-separable polynomial in $Z[X;\delta]$ ([5, Theorem 3.3]), so it is separable polynomial in $Z[X;\delta]$. Then by Lemma 1, there exists an element c in Z such that

$$\delta^{p^e-1}(c) + \alpha_e\delta^{p^{e-1}-1}(c) + \cdots + \alpha_2\delta^{p-1}(c) + \alpha_1 c = 1.$$

By Leibniz' formula, we obtain

$$\begin{aligned} D^{p^j-1}(cw) &= \sum_{\nu=0}^{p^j-1}\binom{p^j-1}{\nu}D^{p^j-1-\nu}(c)D^\nu(w) \\ &= \delta^{p^j-1}(c)w + \sum_{\nu=1}^{p^j-1}\binom{p^j-1}{\nu}\delta^{p^j-1-\nu}(c)D^\nu(w) \quad (j \geq 1). \end{aligned}$$

Since $\sum_{\nu=1}^{p^j-1}\binom{p^j-1}{\nu}\delta^{p^j-1-\nu}(c)D^\nu(w) \in Z$, we see that

$$D^{p^j-1}(cw) = \delta^{p^j-1}(c)w + (\text{some element in } Z) \text{ for all } \ j \geq 1.$$

Hence we have

$$\begin{aligned} w &= (\sum_{j=0}^{e}\alpha_{j+1}\delta^{p^j-1}(c))w \\ &= \sum_{j=0}^{e}\alpha_{j+1}(D^{p^j-1}(cw)) + (\text{some element in } Z). \end{aligned}$$

Since

$$D(\sum_{j=0}^{e}\alpha_{j+1}(D^{p^j-1}(cw))) = \sum_{j=0}^{e}\alpha_{j+1}D^{p^j}(cw) = I_w(cw) = 0,$$

we have $w \in B^D + Z$. Then $w = u + z$, for some $u \in B^D$ and $z \in Z$, and so $I_w = I_u$. □

It is well known that if B is an Azumaya Z-algebra, then every derivation on Z can be extended to a derivation of B (M. A. Knus [8]). Hence in Theorem 2, such D always exists. In the proof of Theorem 2, we used only the separability of $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 \in Z[X;\delta]$. Hence by [4, Theorem 4.1] we have the following

Corollary 3. *Assume that* $X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0$ *is a separable polynomial in* $Z[X;\delta]$. *Let* B *be an Azumaya* Z*-algebra. Then there exists a derivation* D *of* B *which is an extention of* δ *and an element* u *in* B^D *such that* $X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 + \alpha_0 - u$ *is a separable polynomial in* $B[X;D]$.

Under the same situation of Theorem 2, we already have the following ([7, Proposition 2.3 and Theorem 2.4])

(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) $B[X; D]$ *is an Azumaya* $Z^\delta[f]$*-algebra,* $V_{B[X;D]}(B) = Z[f]$*, and* $V_{B[X;D]}(Z) = B[f]$.
(3) $B[X; D]_{(0)} = \{\ h(f) \mid h(t)$ *is a monic polynomial in* $Z^\delta[t]\}$.
(4) $\{\ g \in B[X; D] \mid g$ *is an* H*-separable polynomial in* $B[X; D]\} = \{\ f + z \mid z \in Z^\delta\}$.

Moreover, we have the following which is a generalization of [5, Theorem 3.4]

Proposition 4. *Let* $\psi : Z^\delta[t]_{(0)} \to B[X; D]_{(0)}$ *be defined by* $\psi(g_0(t)) = g_0(f)$.
(1) ψ *indeuces a one-to-one correspondence between* $Z^\delta[t]_{(0)}$ *and* $B[X; D]_{(0)}$.
(2) For $g_0(t) \in Z^\delta[t]_{(0)}$, $g_0(t)$ *is a separable polynomial in* $Z^\delta[t]$ *if and only if* $B[X; D]/g_0(f)B[X; D]$ *is a separable* Z^δ*-algebra. Moreover, the center of* $B[X; D]/g_0(f)B[X; D]$ *is isomorphic to* $Z^\delta[t]/g_0(t)Z^\delta[t]$.

Proof. (1) is clear from the statement (3) under Corollary 3.
(2) Since $B[X; D]$ is an Azumaya $Z^\delta[f]$-algebra, the center of $B[X; D]/g_0(f)B[X; D]$ is $(Z^\delta[f] + g_0(f)B[X; D])/g_0(f)B[X; D]$, which is isomorphic to $Z^\delta[t]/g_0(t)Z^\delta[t]$. Then the assertion is immediate by [1, Theorem 2.3.8]. □

In Theorem 2, if $V_B(B^D) = Z$, then obviously $I_u = 0$. Conversely, if $I_u = 0$, that is, $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = 0$, then we have $V_B(B^D) = Z$. This will be proved in the following theorem.

Theorem 5. *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* $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = 0$*, then there hold the following:*
(1) $B = B^D Z = B^D \otimes_{Z^\delta} Z$, ${}_{B^D}B$ *is a finitely generated projective module.*
(2) B^D *is an Azumaya* Z^δ*-algebra, and* $V_B(B^D) = Z$.
(3) $\mathrm{Hom}({}_{B^D}B_{B^D}, {}_{B^D}B_{B^D}) = Z[D] = Z \oplus ZD \oplus ZD^2 \oplus \cdots \oplus ZD^{p^e-1}$.
(4) $\mathrm{Der}_{B^D}(B) = ZD \oplus ZD^p \oplus \cdots \oplus ZD^{p^{e-1}}$. *In particular,* $\mathrm{Der}_{Z^\delta}(Z) = Z\delta \oplus Z\delta^p \oplus \cdots \oplus Z\delta^{p^{e-1}}$.

(5) $B[X;D]$ and $Z[X;\delta]$ are Azumaya $Z^{\delta}[f]$-algebras and $B[X;D]=Z[X;\delta] \otimes_{Z^{\delta}} B^D = Z[X;\delta] \otimes_{Z^{\delta}[f]} B^D[f]$, where $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1$.

Proof. We define the map $\tau : B \to B$ by

$$\tau(b) = \sum_{j=0}^{e} \alpha_{j+1} D^{p^j - 1}(b).$$

Since $D^{p^e} + \alpha_e D^{p^{e-1}} + \cdots + \alpha_2 D^p + \alpha_1 D = 0$, τ is a $B^D - B^D$-map, and the image is contained in B^D. Since Z/Z^{δ} is a purely inseparable extension of exponent one with δ, it follows from [5, Theorem 3.3(d)] that there exist $x_i, y_i \in Z$ such that

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

We define the map $\varphi_i : B \to B^D$ by $\varphi_i = \tau(x_i)_r$. Then we have

$$\begin{aligned}
\sum_i \varphi_i(b)y_i &= \sum_i \tau(bx_i)y_i \\
&= \sum_i \sum_{j=0}^{e} \alpha_{j+1} D^{p^j-1}(bx_i)y_i \\
&= \sum_i \sum_{j=0}^{e} \alpha_{j+1} \sum_{\nu=0}^{p^j-1} \binom{p^j-1}{\nu} D^{p^j-1-\nu}(b)\delta^{\nu}(x_i)y_i \\
&= \sum_{j=0}^{e} \alpha_{j+1} \sum_{\nu=0}^{p^j-1} \binom{p^j-1}{\nu} D^{p^j-1-\nu}(b)(\sum_i \delta^{\nu}(x_i)y_i) \\
&= b. \quad (b \in B)
\end{aligned}$$

This shows that $B = B^D Z$, and ${}_{B^D}B$ is a finitely generated projective module. Since $B \cong B^D \otimes_{Z^{\delta}} Z$ is an Azumaya Z-algebra and Z^{δ} is a direct summand of Z, B^D is an Azumaya Z^{δ}-algebra by [1, Corollary 1.1.10]. $B = B^D Z$ implies $V_B(B^D) = Z$. This complets the proof of (1) and (2).
(3) Let φ be in $\mathrm{Hom}({}_{B^D}B_{B^D}, {}_{B^D}B_{B^D})$. Then we have

$$\varphi(b) = \sum_i \tau(bx_i)\varphi(y_i). \quad (b \in B)$$

Since $V_B(B^D) = Z$, it is easy to see $\varphi(Z) \subset Z$. Hence we obtain

$$\begin{aligned}\varphi(b) &= \sum_i \varphi(y_i)\tau(bx_i)\\ &= \sum_i \varphi(y_i)\sum_{j=0}^{e}\alpha_{j+1}\sum_{\nu=0}^{p^j-1}\binom{p^j-1}{\nu}\delta^{p^j-1-\nu}(x_i)D^\nu(b).\end{aligned}$$

This implies that $\varphi \in \sum_{\nu=0}^{p^j-1} ZD^\nu$. Since $f = X^{p^e} + X^{p^{e-1}}\alpha_e + \cdots + X^p\alpha_2 + X\alpha_1 - u$ is an H-separable polynomial in $B[X;D]$, $1, D, D^2, \cdots, D^{p^e-1}$ are linearly independent over Z ([7, Lemma 2.1]). Thus we have $\mathrm{Hom}({}_{B^D}B_{B^D}, {}_{B^D}B_{B^D}) = Z[D] = Z \oplus ZD \oplus ZD^2 \oplus \cdots \oplus ZD^{p^e-1}$.
(4) Let Δ be any derivation in $\mathrm{Der}_{B^D}(B)$. By (3), we have $\Delta = \sum_{k=1}^{p^e-1} z_kD^k$ ($z_k \in Z$). (Note that Δ has no constant term). For any $a, b \in B$, we obtain

$$\begin{aligned}\Delta(ab) &= \sum_{k=1}^{p^e-1} z_k(\sum_{\nu=0}^{k}\binom{k}{\nu}D^{k-\nu}(a)D^\nu(b))\\ &= \sum_{\nu=0}^{p^e-1}(\sum_{k=\nu}^{p^e-1}\binom{k}{\nu}z_kD^{k-\nu}(a))D^\nu(b).\end{aligned}$$

On the other hand

$$\Delta(a)b + a\Delta(b) = (\sum_{k=1}^{p^e-1} z_kD^k(a))b + \sum_{\nu=1}^{p^e-1} az_\nu D^\nu(b).$$

Since $1, D, D^2, \cdots, D^{p^e-1}$ are linearly independent over B ([7, Lemma 2.1]), we obtain

$$az_\nu = \sum_{k=\nu}^{p^e-1}\binom{k}{\nu}z_kD^{k-\nu}(a) \ (a \in B, 1 \leq \nu \leq p^e-1),$$

and hence,

$$\sum_{k=\nu+1}^{p^e-1}\binom{k}{\nu}z_kD^{k-\nu} = 0.$$

Since $1, D, D^2, \cdots, D^{p^e-1}$ are linearly independent over B again, we have

$$\binom{k}{\nu}z_k = 0 \quad (1 \leq \nu < k \leq p^e-1).$$

Then by the same arguments in the proof of [5, Theorem 3.1], we see that Δ is in $ZD \oplus ZD^p \oplus \cdots \oplus ZD^{p^{e-1}}$. This completes the proof of (4).

(5) is immediate by [1, Theorem 2.4.3]. $\square$

Under the same situation of Theorem 5 we have the following

Corollary 6. *Let Δ be an another derivation of B which is an extension of δ. If $B^{\Delta} = B^{D}$, then $\Delta = D$.*

Proof. By Theorem 5(4), $\Delta = \sum_{j=0}^{e-1} z_j D^{p^j}$ $(z_j \in Z)$. Since $\Delta|Z = D|Z = \delta$, we have $\delta = \sum_{j=0}^{e-1} z_j \delta^{p^j}$, and so $z_0 = 1$ and $z_j = 0$ $(1 \leq j \leq e-1)$. $\square$

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

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

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

[8] K. A. Knus: Sur le theoreme de Skolem-Noether et sur les derivation des algebres d'Azumaya, C. R. Acad. Sci. Paris Ser. A-B **270**, (1970) A637–A639.

[9] 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.

[10] S. Yuan: On logarithmic derivatives, Bull. Soc. Math. France, **96** (1968), 41–52.

[11] 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
e-mail address: ikehata@ems.okayama-u.ac.up

(*Received May 30, 2000*)