Math. J. Okayama Univ. 23 (1981), 19—32

AZUMAYA ALGEBRAS AND SKEW POLYNOMIAL RINGS

SHÛICHI IKEHATA

Throughout the present paper, every ring has identity 1, its subring contains 1, and every module over a ring is unital. A ring homomorphism means such one sending 1 to 1. In what follows, B will represent a ring, ρ an automorphism of B, D a ρ-derivation of B (i. e. an additive endomorphism of B such that $D(ab)=D(a)\rho(b)+aD(b)$ for all a, $b\in B$). Let $R=B[X;\rho,D]$ be the skew polynomial ring in which the multiplication is given by $aX=X\rho(a)+D(a)$ $(a\in B)$. In particular, we set $B[X;\rho]=B[X;\rho,0]$, $B[X;D]=B[X;1,D]$. By $R_{(0)}$, we denote the set of all monic polynomials g in R with $gR=Rg$.

A ring extension B/A is called to be separable if the B-B-homomorphism of $B\otimes_A B$ onto B defined by $a\otimes b\to ab$ splits, and B/A is called to be H-separable if $B\otimes_A B$ is B-B-isomorphic to a direct summand of a finite direct sum of copies of B. As is well known, an H-separable extension is separable. A polynomial g in $R_{(0)}$ is called to be separable (resp. H-separable) if R/gR is a separable (resp. H-separable) extension of B. Moreover, a ring extension B/A is called to be G-Galois if there exists a finite group G of automorphisms of B such that $A=B^G$ (the fixed ring of G in B) and $\sum_i x_i\sigma(y_i)=\delta_{1,\sigma}$ $(\sigma\in G)$ for some finite x_i, $y_i\in B$.

We shall use the following conventions.

$C(B)=$ the center of B.

$V_B(A)=$ the centralizer of A in B for a ring extension B/A.

$U(B)=$ the set of all invertible elements in B.

u_l (resp. u_r) $=$ the left (resp. right) multiplication effected by $u\in B$, $B_l=\{u_l\,|\,u\in B\}$.

$B^\rho=\{a\in B\,|\,\rho(a)=a\}$, $B^D=\{a\in B\,|\,D(a)=0\}$.

$\rho^*: B[X;\rho]\to B[X;\rho]$ is the ring automorphism defined by $\rho^*(\sum_i X^i d_i)=\sum_i X^i\rho(d_i)$.

$D^*: B[X;D]\to B[X;D]$ is the inner derivation defined by $D^*(\sum_i X^i d_i)=\sum_i X^i D(d_i)$.

For several years, separable polynomials in skew polynomial rings are extensively studied by Kishimoto [8, 9], Nagahara [12, 13, 14, 15, 16], Miyashita [11], and by the author [4, 5, 6].

The main results of this paper are the following: Let B be a com-

mutative ring. For $f\in R_{(0)}=B[X;\rho]_{(0)}$ and $A=B^{\rho}$, R/fR is an Azumaya A-algebra if and only if $\deg f=$ the order of ρ, B/A is a G-Galois extension with $G=\langle\rho\rangle$ (cyclic group generated by ρ), and f is of the form X^m+a_0 with $a_0\in U(A)$. Moreover, for $R_{(0)}=B[X;D]_{(0)}$ and $A=B^D$, $R_{(0)}$ contains a polynomial f of degree m such that R/fR is an Azumaya A-algebra if and only if ${}_AB$ is a finitely generated projective module of rank m and Hom $({}_AB, {}_AB)$ coincides with the subring generated by B_l and D; when this is so and $m\geqq 2$, B is of prime characteristic p, f is of the form $\sum X^q a_q+a_0$ (q runs over powers $1, p, p^2, \cdots, p^r=m$), and $\mathrm{Hom}({}_AB, {}_AB)$ is B-ring isomorphic to $R/(f-a_0)R$. Further, for $f\in R_{(0)}$, R/fR is an Azumaya A-algebra if and only if f is H-separable in R. The present study contains also some sharpenings of G. Szeto [18, 19], G. Szeto and Y. F. Wong [20], and the result of S. Yuan [21, Theorem 2. 4] (§§2, 3).

In our study, H-separable polynomials in skew polynomial rings play important rôles. Therefore, §1 is devoted to giving preliminary results concerning H-separable polynomials.

1. *H*-separable polynomials. Throughout this section, let $f=X^m+X^{m-1}a_{m-1}+\cdots+Xa_1+a_0$ be in $B[X;\rho,D]$. First, we state the following which is easily obtained from the result of Miyashita [11, Theorem 1. 9], and plays an important rôle in our study.

Theorem 1.1. *Let f be in $R_{(0)}=B[X;\rho,D]_{(0)}$, and $I=fR$. If f is an H-separable polynomial in R, then there exist y_i, $z_i\in R$ with* $\deg y_i<m$ *and* $\deg z_i<m$ *such that $ay_i=y_ia$, $\rho^{m-1}(a)z_i=z_ia$ $(a\in B)$ and $\sum_i y_iX^{m-1}z_i\equiv 1$ (mod I), $\sum_i y_iX^kz_i\equiv 0$ $(0\leqq k\leqq m-2)$, and conversely.*

By virtue of Theorem 1. 1, wa shall prove the following

Proposition 1.2. *Let f be in $R_{(0)}=B[X;\rho]_{(0)}$. If f is H-separable in R, then $a_0\in U(B)$, $\rho^m=(a_0^{-1})_l(a_0)_r$, $f\in C(B^{\rho})[X]$ and is Frobenius in R.*

Proof. By Theorem 1. 1, $1\equiv\sum_i y_iX^{m-1}z_i\equiv X^{m-1}\sum_i\rho^{*m-1}(y_i)z_i\equiv\sum_i y_i\rho^{*-(m-1)}(z_i)X^{m-1}$ (mod fR). We put here $x=X+fR$. Then, x is invertible in R/fR. Hence there exist $d_j\in B$ $(0\leqq j\leqq m-1)$ such that

$$x(x^{m-1}d_{m-1}+\cdots+xd_1+d_0)=(x^{m-1}d_{m-1}+\cdots+xd_1+d_0)x=1.$$

Noting $x^m=-x^{m-1}a_{m-1}-\cdots-xa_1-a_0$, we have

$$\begin{aligned}1&=-(x^{m-1}a_{m-1}+\cdots+a_0)d_{m-1}+x^{m-1}d_{m-2}+\cdots+xd_0\\&=-(x^{m-1}a_{m-1}+\cdots+a_0)\rho(d_{m-1})+x^{m-1}\rho(d_{m-2})+\cdots+x\rho(d_0).\end{aligned}$$

Since $\{1, x, \cdots, x^{m-1}\}$ is a free basis of R/fR_B, it follows that $-a_0 d_{m-1} = -a_0\rho(d_{m-1})=1$. Moreover, $aa_0=a_0\rho^m(a)$ $(a\in B)$ by [6, Lemma 1.3 a)]. Hence $a_0\in U(B)$, $\rho^m=(a_0^{-1})_l(a_0)_r$, $\rho(d_{m-1})=d_{m-1}$, and therefore, $\rho(a_0)=a_0$. Thus, f is in $C(B^\rho)[X]$ by [6, Proposition 3.1]. The last assertion follows immediately from [4, Theorem 1(a)].

Lemma 1.3. *Let f be in $R_{(0)}=B[X;\rho]_{(0)}$. If f is H-separable in R, then* $1, \rho, \rho^2, \cdots, \rho^{m-1}$ $(\in {}_B\mathrm{Hom}(B_{B^\rho}, B_{B^\rho}))$ *are linearly independent over B.*

Proof. Assume that $\sum_{j=0}^{m-1}\beta_j\rho^j=0$ $(\beta_j\in B)$. Then, it is easily verified that $\sum_{j=0}^{m-1}\rho^\nu(\beta_j)\rho^j=0$ $(\nu\geqq 0)$. Hence we have $\sum_{j=0}^{m-1}\beta_j\rho^{*j}=0$. By Theorem 1.1, there exist y_i, $z_i\in R$ with deg $y_i<m$ and deg $z_i<m$ such that $ay_i=y_ia$, $\rho^{m-1}(a)z_i=z_ia$ $(a\in B)$ and $X^{m-1}\sum_i\rho^{*m-1}(y_i)z_i\equiv 1$, $X^k\sum_i\rho^{*k}(y_i)z_i\equiv 0$ $(\mathrm{mod}\, fR)$ $(0\leqq k\leqq m-2)$. Then, we have

$$\begin{aligned}\rho^{-(m-1)}(\beta_{m-1}) &\equiv \textstyle\sum_{j=0}^{m-1}\rho^{-(m-1)}(\beta_j)X^{m-1}\sum_i\rho^{*j}(y_i)z_i\\ &= X^{m-1}\textstyle\sum_{j=0}^{m-1}\beta_j\sum_i\rho^{*j}(y_i)z_i\\ &= X^{m-1}\textstyle\sum_i(\sum_{j=0}^{m-1}\beta_j\rho^{*j}(y_i))z_i\equiv 0 \ (\mathrm{mod}\ fR).\end{aligned}$$

This implies $\beta_{m-1}=0$, and $\sum_{j=0}^{m-2}\beta_j\rho^{*j}=0$. Since $\sum_{j=0}^{m-2}\beta_j\rho^{*j+1}=0$, we have $\beta_{m-2}=0$ again. Repeating this, we concludet hat $\beta_j=0$ $(0\leqq j\leqq m-1)$.

Proposition 1.4. *Let $g=X^n+b_0$ be in $R_{(0)}=B[X;\rho]_{(0)}$. Assume that the order of the cyclic group G generated by $\rho|C(B)$ is n, and $C(B)/C(B)^G$ is a G-Galois extension. If b_0 is invertible in B, then g is H-separable in R.*

Proof. Since $C(B)/C(B)^G$ is G-Galois, there exist α_i, $\beta_i\in C(B)$ such that $\sum_i\alpha_i\beta_i=1$ and $\sum_i\rho^k(\alpha_i)\beta_i=0$ $(1\leqq k\leqq n-1)$. We put here $y_i=\alpha_i$ and $z_i=-Xb_0^{-1}\beta_i$. Obviously, $ay_i=y_ia$ and $\rho^{n-1}(a)z_i=z_ia$ $(a\in B)$. Since $X^n\equiv -b_0$ $(\mathrm{mod}\ gR)$, it follows that $\sum_i y_iX^{n-1}z_i\equiv 1$ $(\mathrm{mod}\ gR)$ and $\sum_i y_iX^kz_i\equiv 0$ $(\mathrm{mod}\ gR)$ $(0\leqq k\leqq n-2)$. Thus, g is H-separable by Theorem 1.1.

Now, in case $R=B[X;D]$, the result of Theorem 1.1 takes the place of the next

Lemma 1.5. *Let f be in $R_{(0)}=B[X;D]_{(0)}$, and $I=fR$. If f is H-separable in R, then there exist y_i, $z_i\in R$ with* deg $y_i<m$ *and* deg $z_i<m$ *such that $ay_i=y_ia$, $az_i=z_ia$ $(a\in B)$ and $\sum_i D^{*m-1}(y_i)z_i\equiv 1$ $(\mathrm{mod}\ I)$, $\sum_i D^{*k}(y_i)z_i\equiv 0$ $(\mathrm{mod}\ I)$ $(0\leqq k\leqq m-2)$, and conversely.*

Proof. Let f be H-separable, and $\{y_i, z_i\}$ as in Theorem 1.1. Then, for $0\leqq k\leqq m-2$,

$$0\equiv\sum_i y_i X^k z_i=\sum_{j=1}^k \binom{k}{j} X^j \sum_i D^{*k-j}(y_i)z_i+\sum_i D^{*k}(y_i)z_i \pmod I.$$

Since, $\sum_i y_i z_i\equiv 0$, by induction method we see that $\sum_i D^{*k}(y_i)z_i\equiv 0$ $(0\leqq k\leqq m-2)$ and $\sum_i D^{*m-1}(y_i)z_i\equiv 1 \pmod I$. The converse is obvious.

Corresponding to Lemma 1. 3, we have the following

Lemma 1.6. *Let f be in $R_{(0)}=B[X;D]_{(0)}$. If f is H-separable in R, then* 1, D, D^2, $\cdots$, D^{m-1} $(\in {}_B\mathrm{Hom}(B_{B^D}, B_{B^D}))$ *are linearly independent over B.*

Proof. Assume that $\sum_{j=0}^{m-1}\beta_j D^j=0$ $(\beta_j\in B)$. Then, for all $a\in B$, $0=D(\sum_{j=0}^{m-1}\beta_j D^j(a))=\sum_{j=0}^{m-1}D(\beta_j)D^j(a)+\sum_{j=0}^{m-1}\beta_j D^j(D(a))$. Hence we have $\sum_{j=0}^{m-1}D(\beta_j)D^j=0$. An easy induction shows that $\sum_{j=0}^{m-1}D^\nu(\beta_j)D^j=0\,(\nu\geqq 0)$. Then, for all $h=\sum_{k=0}^r X^k d_k\in R$, we have

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

Hence, for $\{y_i, z_i\}$ as in Lemma 1. 5, we obtain

$$\beta_{m-1}=\sum_{j=0}^{m-1}\sum_i\beta_j D^{*j}(y_i)z_i\equiv 0 \pmod{fR}.$$

This implies $\beta_{m-1}=0$, and $\sum_{j=0}^{m-2}\beta_j D^{*j}=0$. Since $\sum_{j=0}^{m-2}\beta_j D^{*j+1}=0$, we have $\beta_{m-2}=0$ again. Repeating this, we conclude that $\beta_j=0\,(0\leqq j\leqq m-1)$.

2. Azumaya algebras induced by $B[X;\rho]$. Throughout this section, B will mean a commutative ring, ρ an automorphism of B, G the cyclic group generated by ρ, $A=B^G=B^\rho$, and $R=B[X;\rho]$.

First, we shall prove the following which is one of our main results.

Theorem 2.1. *Let $f=X^m+X^{m-1}a_{m-1}+\cdots+a_0$ be in $R_{(0)}$, and $S=R/fR$. Then, f is H-separable in R if and only if S is an Azumaya A-algebra. When this is the case, there holds that B/A is G-Galois, the order of G is m, $f=X^m+a_0$, $a_0\in U(A)$.*

Proof. Assume that S is an Azumaya A-algebra. Since $S\supseteqq B\supseteqq A$ and S_B is free, f is H-separable in R by [7, Theorem 1]. To see the converse, we assume that f is H-separable in R. Then, by Proposition 1. 2 and Lemma 1. 3, we see that $a_0\in U(A)$ and the order of ρ is m. Since $Rf=fR$, we have $aa_i=a_i\rho^{m-i}(a)$ $(a\in B,\ 0\leqq i\leqq m-1)$ by [6, Lemma 1. 3

a)]. Hence by Lemma 1. 3, we obtain $a_j=0$ $(1\leqq i\leqq m-1)$, and so $f=X^m+a_0$. Now, we shall prove that B/A is a G-Galois extension. We set $x=X+fR\in S$. Then, for $y=\sum_{i=0}^{m-1}x^i d_i\in V_S(B)$, we have $\rho^i(a)d_i=d_i a$ $(0\leqq i\leqq m-1,\ a\in B)$, and whence $d_i=0$ $(1\leqq i\leqq m-1)$. Thus we obtain $V_S(B)=B$. Moreover, if $z=\sum_{i=0}^{m-1}x^i c_i\in S$ and $\rho^{m-1}(a)z=za$ for all $a\in B$ then we see that $z=xc_1$. Hence by Theorem 1. 1, there exist α_i, $\beta_i\in B$ such that $\sum_i \alpha_i x^{m-1}x\beta_i=1$ and $\sum_i \alpha_i x^k x\beta_i=0$ $(0\leqq k\leqq m-2)$. Since $x^m=-a_0$, we have

$$1=\sum_i \alpha_i(-a_0\beta_i),\ \ 0=x^{k+1}\sum_i \rho^{k+1}(\alpha_i)\beta_i \quad (0\leqq k\leqq m-2)$$

and whence $0=\sum_i \rho^{k+1}(\alpha_i)(-a_0\beta_i)$. This implies that B/A is G-Galois. Since S/B and B/A are separable, S/A is separable. Recalling $V_S(B)=B$, it follows that $V_S(S)=A$, and B is an Azumaya A-algebra.

Next, we shall prove the following theorem which contains a sharpening of the results of G. Szeto [18, Lemma 3. 1 and Theorem 3. 2] and [19, Lemma 2. 1 and Theorem 2. 2].

Theorem 2.2. *The following conditions are equivalent*:

(a) *B/A is a G-Galois extension with G of order m.*

(b) *$R_{(0)}$ contains an H-separable polynomial of degree m.*

(c) *$R_{(0)}$ contains a polynomial f of degree m such that R/fR is an Azumaya A-algebra.*

(d) $\{g\in R\,|\,g$ *is H-separable*$\}=\{X^m+a\,|\,a\in U(A)\}$.

When this is the case, for every $a\in U(A)$, B is a maximal commutative A-subalgebra of $R/(X^m+a)R$, $(R/(X^m+a)R)\otimes_A B\cong B\otimes_A(R/(X^m+a)R)\cong M_m(B)$, and moreover, if $m\in U(A)$ then $A[X]/(X^m+a)A[X]$ is a separable splitting ring for $R/(X^m+a)R$.

Proof. By Theorem 2. 1 and Proposition 1. 4, we have (c)$\Longleftrightarrow$(b)$\Longleftrightarrow$(a). Moreover, (d)$\Longrightarrow$(b) is obvious. Next, we assume (a), (b) and (c). If $g\in R_{(0)}$ is H-separable then $g\in\{X^m+a\,|\,a\in U(A)\}$ by Theorem 2. 1. Conversely, if $a\in U(A)$ then X^m+a is H-separable by Proposition 1. 4. Thus, we obtain (d). Now, let $f=X^m+a$ be H-separable in R. From the proof of the preceeding theorem, we see that B is a maximal commutative A-subalgebra of R/fR. If $m\in U(A)$ then f is separable in $A[X]$ by [6, Theorem 2. 2]. Moreover, $A[X]/fA[X]$ may be considered as an A-subalgebra of R/fR. Clearly, this is a maximal commutative A-subalgebra of R/fR. By the above remarks, the rest of the assertions will be easily seen ([2, Theorem 2. 5. 5], [3, Proposition 3. 1]).

The following corollaries are also sharpenings of [20, Theorems 3. 5,

3. 6], [19, Theorem 3. 5] and [18, Theorem 2. 5].

Corollary 2.3. *Let f be in $A[X]\cap B[X;\rho]_{(0)}$. If $(A[X]/fA[X])\otimes_A(R/fR)$ is an Azumaya $A[X]/fA[X]$-algebra, then the order of ρ is equal to* $\deg f$ *and B/A is a G-Galois extension.*

Proof. Since A is a direct summand of $A[X]/fA[X]$, it follows from [2, Corollary 2. 1. 10] that R/fR is an Azumaya A-algebra. Thus, B/A is G-Galois by Theorem 2. 2.

Corollary 2.4. *Assume that the order of $\rho=m\in U(A)$. Let X^m+a be in $B[X;\rho]_{(0)}$. If $B\otimes_A(R/(X^m+a)R)$ is an Azumaya B-algebra then B/A is a G-Galois extension.*

Proof. Since $m\in U(A)$, A is a direct summand of B. Hence by [2, Corollary 2. 1. 10], $R/(X^m+a)R$ is an Azumaya A-algebra. Thus, B/A is G-Galois by Theorem 2. 2.

Throughout the rest of this section, we assume that R contains an H-separable polynomial of degree $m\geqq 2$.

First, we shall prove the following

Lemma 2.5. $R_{(0)}=\{X^s g(X^m)\,|\,g(t)\in A[t]_{(0)},\ s\geqq 0\}$.

Proof. Obviously, $X^s g(X^m)$ $(g(t)\in A[t]_{(0)},\ s\geqq 0)$ are contained in $R_{(0)}$. Let $f\in R_{(0)}$. Then, we may write $f=X^s(X^n+X^{n-1}a_{n-1}+\cdots+Xa_1+a_0)$ $(a_0\neq 0)$, and $n=qm+r$ $(0\leqq r<m)$. Then, noting f, $X^s\in R_{(0)}$, one will easily see that $X^n+X^{n-1}a_{n-1}+\cdots+Xa_1+a_0\in R_{(0)}$. Hence by [6, Lemma 1. 3], we have $aa_0=a_0\rho^n(a)=a_0\rho^r(a)$ and $aa^i=a_i\rho^{n-i}(a)$ $(a\in B)$. Since 1, $\rho,\cdots,\rho^{m-1}$ are linearly independent over B (Lemma 1. 3), it follows that $r=0$, and $a_i=0$ for i which is not a multiple of m. Moreover, since $a_{n-1}=0$, we have $a_i\in A$ for all i ([6, Remark 1. 4]). Thus, we obtain $X^n+X^{n-1}a_{n-1}+\cdots+Xa_1+a_0=g(X^m)$ for some $g(t)\in A[t]_{(0)}$.

Lemma 2.6. *Let $g(t)\in A[t]_{(0)}$, and $s>0$ an integer.*

(a) *X^s is separable in R if and only if $s=1$.*

(b) *$g(X^m)$ is separable in R if and only if $g(t)$ is separable in $A[t]$ and the constant term of $g(t)$ is in $U(A)$.*

Proof. (a). If X^s is separable in R then $s=1$ by [4, Lemma 1]. The converse is obvious. (b). We set $S=R/g(X^m)R$, $x=X+g(X^m)R$, and $u=X^m+g(X^m)R$. Moreover, let $g(t)$ be of degree k. Then $B[u]=$

$u^{k-1}B+\cdots+uB+B$, and $S=\sum_{i=0}^{m-1}\sum_{j=0}^{k-1}x^iu^jB$. Since $\{x^i\,|\,0\leqq i\leqq km-1\}$ is linearly independent over B, so is $\{x^iu^j\,|\,0\leqq i\leqq m-1,\ 0\leqq j\leqq k-1\}$. Let $\hat{\rho}: B[u]\to B[u]$ be the automorphism defined by $\hat{\rho}(\sum_i u^ib_i)=\sum_i u^i\rho(b_i)$, and set $h=Y^m-u\in B[u][Y;\hat{\rho}]=R'$, where Y is an indeterminate. Then it follows that $h\in R'_{(0)}$, and S is $B[u]$-ring isomorphic to R'/hR'. Moreover, $B[u]^{\hat{\rho}}=A[u]\cong A[t]/g(t)A[t]$, and $B[u]=A[u]\otimes_A B$ is $\langle\hat{\rho}\rangle$-Galois over $A[u]$ (Theorem 2. 2). Now, assume that $g(X^m)$ is separable in R. Then, by [4, Lemma 1], the constant term of $g(X^m)$ is in $U(A)$. This implies that $x^m=u\in U(A[u])$. Hence, by Theorem 2. 2, S is an Azumaya $A[u]$-algebra. Since S/B and B/A are separable, it follows from [2, Theorem 2. 3. 8] that $A[u]/A$ is separable, and whence $g(t)$ is separable in $A[t]$. Conversely, assume that $g(t)$ is separable in $A[t]$ and the constant term of $g(t)$ is in $U(A)$. Then $u\in U(A[u])$. Hence, by Theorem 2. 2, S is an Azumaya $A[u]$-algebra. Since $A[u]/A$ is separable, it follows that S/B is separable, and whence $g(X^m)$ is separable in R.

Now, we are in the position to prove the following

Theorem 2.7. *For $f\in R_{(0)}$, the following conditions are equivalent:*

(a) *f is separable in R.*

(b) *$f=g(X^m)$ or $Xg(X^m)$ for some $g(t)$ of $A[t]_{(0)}$ such that $g(t)$ is separable in $A[t]$ and the constant term of $g(t)$ is in $U(A)$.*

(c) *R/fR is a separable A-algebra.*

Proof. Assume (a). Since $f\in R_{(0)}$, it follows from Lemma 2. 5 that $f=X^sg(X^m)$ for some $g(t)\in A[t]_{(0)}$ and $s\geqq 0$. By [11, Theorem 1. 10], X^s $(s\geqq 1)$ and $g(X^m)$ are separable in R. Hence by Lemma 2. 6, we obtain (b). The implication (b) $\Longrightarrow$ (a) follows immediately from the results of Lemma 2. 6 and [11, Theorem 1. 10]. Moreover, (c) $\Longrightarrow$ (a) is obvious. Assume (b). Then $R/fR=R/g(X^m)R$ or $R/XR\oplus R/g(X^m)R$ $(=B\oplus R/g(X^m)R)$. Hence, (c) will be immediate from the proof of Lemma 2. 6.

In the rest of this section, we shall use the following conventions: $N_\rho(c)=\rho^{m-1}(c)\rho^{m-2}(c)\cdots\rho(c)c$ $(c\in B)$, $N_\rho(U(B))=\{N_\rho(c)\,|\,c\in U(B)\}$, $B_a=R/(X^m-a)R$ $(a\in U(A))$, $\Omega_\rho(B)=\{B_a\,|\,a\in U(A)\}$, $P_\rho(B)=\{\langle B_a\rangle\,|\,a\in U(A)\}$, where $\langle B_a\rangle$ is the B-ring isomorphism class of B_a in $\Omega_\rho(B)$. By Theorem 2. 2, we have $\Omega_\rho(B)=\{R/fR\,|\,f$ is H-separable in $R\}$. Under this situation, we shall prove the following

Lemma 2.8. *For a, $b\in U(A)$, B_a and B_b are B-ring isomorphic if and only if $ab^{-1}\in N_\rho(U(B))$.*

Proof. We set $x=X+(X^m-a)R\in B_a$ and $y=X+(X^m-b)R\in B_b$. First, we assume that there exists a B-ring isomorphism ϕ of B_a onto B_b, and set $\phi(x)=\sum_{i=0}^{m-1}y^i a_i$. Then, for $c\in B$, $c\phi(x)=\phi(cx)=\phi(x\rho(c))=\phi(x)\rho(c)$, and this implies $\rho^i(c)a_i=a_i\rho(c)$ $(0\leqq i\leqq m-1)$. Since 1, $\rho, \cdots, \rho^{m-1}$ are linearly independent over B, it follows that $\phi(x)=ya_1$, $(ya_1)^m=a$, and so $bN_\rho(a_1)=a$. Thus, we obtain $b^{-1}a\in N_\rho(U(B))$. The converse will be easily seen.

In virtue of Lemma 2. 8, we obtain the following

Proposition 2.9. *$P_\rho(B)$ forms an abelian group under the composition $\langle B_r\rangle * \langle B_s\rangle=\langle B_{rs}\rangle$ with the identity $\langle B_1\rangle$, which is isomorphic to the factor group $U(A)/N_\rho(U(B))$.*

Remark. 2.10. Since B_1 is considered as the trivial crossed product of B with G, B_1 is B-ring isomorphic to $\mathrm{Hom}({}_AB, {}_AB)$. Hence B_a is B-ring isomorphic to $\mathrm{Hom}({}_AB, {}_AB)$ if and only if $a\in N_\rho(U(B))$.

3. Azumaya algebras induced by $B[X; D]$. Throughout this section, B will mean a commutative ring, D a derivation of B, $A=B^D$, and $R=B[X; D]$.

First, we shall prove the following

Theorem 3.1. *Let $f\in R_{(0)}$, $\deg f=m$, and $S=R/fR$. Then the following conditions are equivalent:*

(a) *f is H-separable in R.*

(b) *S is an Azumaya A-algebra.*

(c) *There exist y_i, $z_i\in B$ such that $\sum_i D^{m-1}(y_i)z_i=1$* and $\sum_i D^k(y_i)z_i=0$ $(0\leqq k\leqq m-2)$.

When this is the case, there holds that if $m\geqq 2$, then B is of prime characteristic p, and f is a p-polynomial of the form $\sum_{j=0}^{r}X^{p^j}b_{j-1}+b_0$ $(p^r=m)$.

Proof. (c) $\Longrightarrow$ (a). It is immediate from Lemma 1. 5.

(b) $\Longrightarrow$ (a). Since $S\supseteqq B\supseteqq A$ and S_B is free, f is H-separable in R by [7, Theorem 1].

(a) $\Longrightarrow$ (b), (c). We set $x=X+fR$ $(\in S)$, and $\sum_{j=0}^{m-1}x^j d_j\in V_S(B)$ $(d_j\in B)$. Then, for each $b\in B$, we have $b(\sum_{j=0}^{m-1}x^j d_j)=(\sum_{j=0}^{m-1}x^j d_j)b$, which implies $D^{m-1}(b)d_{m-1}+\cdots+D(b)d_1+bd_0=d_0b$. By Lemma 1. 6, 1, $D, \cdots, D^{m-1}$ are linearly independent over B. Hence $d_{m-1}=\cdots=d_1=0$. Thus, we obtain $V_S(B)=B$, and $V_S(S)=V_B(x)=A$. This implies (c). Moreover, by [17, Lemma 1 (3)], ${}_AB$ is f. g. projective, $B\otimes_A S\cong S\otimes_A B\cong M_m(B)$.

Since A is a direct summand of B, it follows from [2, Corollary 2. 1. 10] that S is an Azumaya A-algebra. Thus, we obtain (b). Now, by Lemma 1. 6 and [6, Lemma 1. 6], we have

$$\binom{m}{i} 1_B=0 \quad (1_B=1\in B,\ 1\leqq i\leqq m-1)$$
$$\binom{j}{i} a_j=0 \quad (1\leqq i<j\leqq m-1).$$

Then

$$m1_B=\binom{m}{m-1} 1_B=0,\ ja_j=\binom{j}{j-1} a_j=0 \quad (2\leqq j\leqq m-1).$$

Let $p_1, \cdots, p_n$ be all the prime divisors of m and $m=q_1\cdots q_n$ where for each k, q_k is some power of p_k. Suppose $n>1$. Then, as is well known, we have

$$(\binom{m}{q_k},\ q_k)=1 \quad (1\leqq k\leqq n)$$

whence

$$((\binom{m}{q_1}, \cdots, \binom{m}{q_n}),\ m)=1$$

where $(x, y, \cdots, z)$ means the greatest common divisor of integers $x, y, \cdots, z$. From this, one will easily see that $1_B=0$, which is a contradiction. Hence we obtain $n=1$, and so $m=p^e$ $(p_1=p)$. Moreover, we have

$$(\binom{m}{p^{e-1}},\ m)=p \text{ and so } p1_B=0.$$

Hence B is of characteristic p. Since $ja_j=0$ $(2\leqq j\leqq m-1)$, $a_j=0$ for $j\geqq 2$ with $(j,\ p)=1$. If $1<p^t<j=p^t r<m$ and $(r,\ p)=1$ then

$$(\binom{j}{p^t},\ p)=1 \text{ and so } a_j=0.$$

This proves the last assertion.

Lemma 3.2. *Assume that R contains an H-separable polynomial f of degree m. Then there hold the following:*

(a) $V_R(B)=B[f]$, *and* $V_R(R)=A[f]$.

(b) $R_{(0)}=\{g\in A[f] \mid g \text{ is monic}\}$.

(c) $\{g\in R \mid g \text{ is H-separable}\}=\{f+a \mid a\in A\}$.

Proof. Let $g\in V_R(B)$. Then, since f is monic and of degree m, there exist $h,\ r\in R$ such that $g=hf+r$ and $\deg r<m$. Now, let b be an arbitraly element of B. Noting that $g,\ f\in V_R(B)$, we obtain $(bh-hb)f=rb-br$. Since $\deg f=m>\deg (rb-br)$, it follows that $rb=br$, and

$bh=hb$. Hence $h\in V_R(B)$. Moreover, since $1, D, \cdots, D^{m-1}$ are linearly independent over B (Lemma 1. 6), we have $r\in B$. By those above, we can easily verify that there exist $c_i\in B$ such that $g=f^k c_k+f^{k-1}c_{k-1}+\cdots+fc_1+c_0$. Next, let $g\in V_R(R)$. Then, since $Xg=gX$ and $Xf=fX$, we have $f^k D(c_k)+\cdots+D(c_0)=0$. Hence $D(c_i)=0$, and $c_i\in A$ $(0\leqq i\leqq k)$. If g is monic then $c_k=1$. Thus, we obtain (a) and (b) (cf. [6, Lemma 1. 6]). The assertion (c) is a direct consequence of (a), (b) and Theorem 3. 1.

Now, we shall prove the following which is one of our main results containing S. Yuan [21, Theorem 2. 4].

Theorem 3.3. *The following are equivalent*:

(a) ${}_AB$ *is a finitely generated projective module of rank* m *and* $\mathrm{Hom}({}_AB, {}_AB)=B[D]$ *(the subring generated by* B_l *and* D*).*

(b) R *contains an H-separable polynomial* f *of degree* m.

(c) $R_{(0)}$ *contains a polynomial* f *of degree* m *such that* R/fR *is an Azumaya A-algebra.*

(d) $R_{(0)}$ *contains a polynomial* f *of degree* m, *and there exist* y_i, $z_i\in B$ *such that* $\sum_i D^{m-1}(y_i)z_i=1$ *and* $\sum_i D^k(y_i)z_i=0$ $(0\leqq k\leqq m-2)$.

When this is the case, for any H-separable polynomial $f=\sum_{i=0}^m X^i a_i$, *there hold the following*:

(1) $\sum_{i=1}^m a_i D^i=0$, $\mathrm{Hom}({}_AB, {}_AB)$ *is B-ring isomorphic to* $R/(f-a_0)R$, *and either* $f=X+a_0$ *or* f *is a p-polynomial.*

(2) B *is a maximal commutative A-subalgebra of* R/fR *with* $B\otimes_A(R/fR)\cong(R/fR)\otimes_A B\cong M_m(B)$.

Proof. (b) $\Longleftrightarrow$ (c) $\Longleftrightarrow$ (d). These equivalences have been proved in Theorem 3. 1.

(c), (d) $\Longrightarrow$ (a). Since $fR=Rf$, we have $D^m+a_{m-1}D^{m-1}+\cdots+a_1D=0$ and $a_i\in A$ by [6, Lemma 1. 6], where $f=X^m+X^{m-1}a_{m-1}+\cdots+Xa_1+a_0$. Then the map $f_i: B\to B$ defined by $f_i(b)=\sum_{j=0}^{m-1}a_{j+1}D^j(by_i)$ $(a_m=1)$ is in $\mathrm{Hom}({}_AB, {}_AA)$, since $D(f_i(b))=0$. According to (d), we have

$$\begin{aligned}\sum_i f_i(b)z_i&=\sum_i\left(\sum_{j=0}^{m-1}a_{j+1}D^j(by_i)\right)z_i\\&=\sum_i\sum_{j=0}^{m-1}a_{j+1}\left(\sum_{\nu=0}^{j}\binom{j}{\nu}D^{j-\nu}(b)D^\nu(y_i)\right)z_i\\&=\sum_{j=0}^{m-1}a_{j+1}\sum_{\nu=0}^{j}\binom{j}{\nu}D^{j-\nu}(b)\left(\sum_i D^\nu(y_i)z_i\right)\\&=a_m b\sum_i D^{m-1}(y_i)z_i=b\quad(b\in B).\end{aligned}$$

Hence, ${}_AB$ is f. g. projective. On the other hand,

$$f_i(b)=\sum_{j=0}^{m-1} a_{j+1} D^j(by_i)=\sum_{j=0}^{m-1} a_{j+1}(\sum_{\nu=0}^{j} \binom{j}{\nu} D^{j-\nu}(y_i)D^{\nu}(b)).$$

This implies that $f_i \in \sum_{k=0}^{m-1} BD^k$, and so, for each $\phi \in \mathrm{Hom}({}_AB, {}_AB)$, $\phi = \sum_i \phi(z_i) f_i \in \sum_{k=0}^{m-1} BD^k$. Since 1, $D, \cdots, D^{m-1}$ are linearly independent over B (Lemma 1.6), we obtain $\mathrm{Hom}({}_AB, {}_AB) = B \oplus BD \oplus \cdots \oplus BD^{m-1}$. Now, we shall show that ${}_AB$ is of rank m. For a prime ideal P of A, C will mean the localization of A by P. Then

$$\mathrm{rank}_C(\mathrm{Hom}({}_CC \otimes_A B, {}_CC \otimes_A B)) = \mathrm{rank}_C(C \otimes_A \mathrm{Hom}({}_AB, {}_AB)).$$

This means $(\mathrm{rank}_C C \otimes_A B)^2 = (\mathrm{rank}_C C \otimes_A B)m$. Hence $\mathrm{rank}_C C \otimes_A B = m$. Thus, we obtain $\mathrm{rank}_A B = m$.

(a) $\Longrightarrow$ (c). Since $Db_l = b_l D + D(b)_l$ $(b \in B)$, the map $\psi : R \to \mathrm{Hom}({}_AB, {}_AB) = B[D]$ defined by $\psi(\sum_i X^i d_i) = \sum_i (-D)^i (d_i)_l$ is a B-ring epimorphism. Then we have $R/Ker\ \psi \cong \mathrm{Hom}({}_AB, {}_AB)$. Since ${}_AB$ is projective of rank m, $\mathrm{Hom}({}_AB, {}_AB)$ is an Azumaya A-algebra of rank m^2. Hence $R/Ker\ \psi$ is a projective B-module of rank m (cf. [1]). Then by [10, Theorem 3], there exists a polynomial g in $R_{(0)}$ such that $Ker\ \psi = gR$. Now, it is obvious that the degree of g is m. This implies (c). Moreover, g is H-separable in R by the implication (c) $\Longrightarrow$ (d). We write here $g = \sum_{i=0}^{m} X^i b_i$. Noting that $g \in Ker\ \psi$, we have $\sum_{i=0}^{m} (-D)^i (b_i)_l = 0$. Since $b_i \in A$, it follows that

$$b_0 = \sum_{i=0}^{m} (-D)^i (b_i) = (\sum_{i=0}^{m} (-D)^i (b_i)_l)(1) = 0.$$

Hence by Lemma 3.2, we obtain $g = f -$(the constant term of f) for any H-separable polynomial f in R. The other assertions follow immediately from the result of Theorem 3.1 and its proof.

Now, by virtue of Lemma 3.2 and Theorem 3.3, we can prove the following which contains some characterizations of separable (H-separable) polynomials in R.

Theorem 3.4. *Assume that R contains an H-separable polynomial f. Let ψ: $A[t] \to R$ be defined by $\psi(g_0(t)) = g_0(f)$.*

(a) *ψ induces a one-to-one correspondence between $A[t]_{(0)}$ and $R_{(0)}$.*

(b) *For $g_0 \in A[t]_{(0)}$, g_0 is separable in $A[t]$ if and only if $R/\psi(g_0)R$ is a separable A-algebra, and moreover, $\psi(g_0)$ is H-separable in R if and only if* $\deg g_0 = 1$.

Proof. Obviously, ψ induces an injective mapping of $A[t]_{(0)}$ into $R_{(0)}$. Moreover, we have $\psi(A[t]_{(0)}) = R_{(0)}$ by Lemma 3.2. This implies (a). Now, let g_0 be an element of $A[t]_{(0)}$ of degree k. We set $g = \psi(g_0)$, $S = R/gR$, $x = X + gR$, and $u = f + gR$. Then $B[u] = u^{k-1}B + \cdots + uB + B$, $xv -$

$vx \in B[u]$ ($v \in B[u]$), and $S = \sum_{i=0}^{m-1} \sum_{j=0}^{k-1} x^i u^j B$ for $m = \deg f$. Since $\{x^i \mid 0 \leqq i \leqq km-1\}$ is linearly independent over B, so is $\{x^i u^j \mid 0 \leqq i \leqq m-1, 0 \leqq j \leqq k-1\}$ and $\{w \in B[u] \mid xw = wx\} = u^{k-1}A + \cdots + uA + A = A[u]$. Let $\hat{D}$: $B[u] \to B[u]$ be the derivation defined by $D(v) = vx - xv$, and set $h = f(Y) - u \in B[u][Y; \hat{D}] = R'$, where Y is an indeterminate. Then, it follows that $h \in R'_{(0)}$, and S is $B[u]$-ring isomorphic to R'/hR'. Since $B[u]^{\hat{D}} = A[u]$ and h is H-separable in R' (Theorem 3. 1), S is an Azumaya $A[u]$-algebra (Theorem 3. 3). Now, assume that g_0 is separable in $A[t]$. Then, since $A[u] \cong A[t]/g_0 A[t]$, S is separable over A. Conversely, if S is separable over A then $A[u]$ is separable over A ([2, Theorem 2. 3. 8]), and so g_0 is separable in $A[t]$. The other assertion is immediate by Lemma 3. 2.

Throughout the rest of this section, we assume that R contains an H-separable polynomial of degree $\geqq 2$. Then, by Theorem 3. 1 and Lemma 3. 2, B is of prime characteristic p and R contains an H-separable polynomial $\sum_{j=0}^{e} X^{p^j} b_{j+1}$, which will be represented by f. For any $b \in B$, we set $\Delta_0(b) = 1$ and $\Delta_i(b) = D(\Delta_{i-1}(b)) + \Delta_{i-1}(b)b$ ($i \geqq 1$). Then, an easy induction shows that

$$(X+b)^n = \sum_{i=0}^{n} X^i \binom{n}{i} \Delta_{n-i}(b)$$

whence

$$(X+b)^{p^j} = X^{p^j} + \Delta_{p^j}(b) \qquad (j \geqq 0).$$

Since $c(X+b) = (X+b)c + D(c)$ ($c \in B$), it is easy to see that Δ_{p^j} is an additive endomorphism of B. Let θ_b: $R \to R$ be the map defined by $\theta_b(\sum_i X^i d_i) = \sum_i (X+b)^i d_i$. Then, θ_b is a B-ring isomorphism of R. Hence $\theta_b(f)$ is contained in $R_{(0)}$, and so $\theta_b(f) \in A[X]$ by [6, Lemma 1. 6]. Since $\theta_b(f) = \sum_{j=0}^{e} (X+b)^{p^j} b_{j+1} = \sum_{j=0}^{e} X^{p^j} b_{j+1} + \sum_{j=0}^{e} \Delta_{p^j}(b) b_{j+1} = f + \sum_{j=0}^{e} \Delta_{p^j}(b) b_{j+1}$, we have $\sum_{j=0}^{e} \Delta_{p^j}(b) b_{j+1} \in A$. Hence the map δ: $B \to A$ defined by $\delta(b) = \sum_{j=0}^{e} \Delta_{p^j}(b) b_{j+1}$ is an additive homomorphism.

Now, for any $a \in A$, we put $B_a = R/(f+a)R$. Further we put $\Omega_D(B) = \{B_a \mid a \in A\}$, and $P_D(B) = \{\langle B_a \rangle \mid a \in A\}$, where $\langle B_a \rangle$ is the B-ring isomorphism class of B_a in $\Omega_D(B)$. Under this situation, we shall prove the following

Lemma 3.5. *Let B_a, B_c be in $\Omega_D(B)$. Then, B_a and B_c are B-ring isomorphic if and only if $a - c \in \delta(B)$.*

Proof. We set $x=X+(f+a)R\in B_a$, $y=X+(f+c)\in B_c$, and assume that there exists a B-ring isomorphism ϕ of B_a onto B_c with $\phi(x)=\sum_{j=0}^{p^e-1}y^jd_j$ $(d_j\in B)$. Since $bx=xb+D(b)$ $(b\in B)$, this implies $b(\sum_{j=0}^{p^e-1}y^jd_j)=(\sum_{j=0}^{p^e-1}y^jd_j)b+D(b)$. Comparing the constant terms of the both sides, we obtain $\sum_{j=0}^{p^e-1}d_jD^j=D$. Since $1, D, \cdots, D^{p^e-1}$ are linearly independent over B, it follows that $d_1=1$, $d_j=0$ $(2\leqq j\leqq p^e-1)$, and so $\phi(x)=y+d_0$. Hence $-a=\phi(f(x))=f(y+d_0)=f(y)+\delta(d_0)$. Thus, we obtain $a-c\in\delta(B)$. The converse is obvious.

In virtue of Lemma 3. 5, we obtain the following

Proposition 3.6. *$P_D(B)$ forms an abelian group under the composition $\langle B_a\rangle*\langle B_c\rangle=\langle B_{a+c}\rangle$ with the identity $\langle B_0\rangle$, which is isomorphic to the (additive) factor group $A/\delta(B)$.*

Remark 3.7. By theorem 3. 3, we see that $\mathrm{Hom}({}_AB, {}_AB)$ is B-ring isomorphic to B_a if and only if $\langle B_a\rangle$ is the identity of $P_D(B)$. Moreover, if b_1 is invertible in A (that is, *f is $\tilde{D}$*-separable in R in the sense of [6]) then, for each $a\in A$, $A[X]/fA[X]$ is a separable splitting ring for the Azumaya A-algebra B_a.

REFERENCES

[1] N. BOURBAKI: Éléments de Mathématique, Algébre Commutative, Chaps. 1—2, Hermann, Paris, 1961.

[2] F. DEMEYER and E. INGRAHAM: Separable Algebras over a Commutative Ring, Lecture Notes in Math. **181**, Springer, Berlin, 1971.

[3] K. HIRATA: Separable extensions and centralizers of rings, Nagoya Math. J. **35** (1969), 31—45.

[4] S. IKEHATA: On a theorem of Y. Miyashita, Math. J. Okayama Univ. **21** (1979), 49—52.

[5] S. IKEHATA: A note on separable polynomials in skew polynomial rngs of derivation type, Math. J. Okayama Univ. **22** (1980), 59—60.

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

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

[8] K. KISHIMOTO: A classification of free quadratic extensions of rings, Math. J. Okayama Univ. **18** (1976), 139—148.

[9] K. KISHIMOTO: A classification of free extensions of rings of automorphism type and derivation type, Math. J. Okayama Univ. **19** (1977), 163—169.

[10] Y. MIYASHITA: Note on an ideal of a positively filtered ring over a commutative ring, Math. J. Okayama Univ. **19** (1976), 61—63.

[11] Y. MIYASHITA: On a skew polynomial ring, J. Math. Soc. Japan **31** (1979), 317—330.

[12] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. **19** (1976), 65—95.

[13] T. NAGAHARA: Supplements to the previous paper "On separable polynomials of degree 2 in skew polynomial rings", Math. J. Okayama Univ. **19** (1977), 159—161.

[14] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings II, Math. J. Okayama Univ. **21** (1979), 166—177.

[15] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings III, Math. J. Okayama Univ. **22** (1980), 61—64.

[16] T. NAGAHARA: A note on separable polynomials in skew polynomial rings of automorphism type, Math. J. Okayama Univ. **22** (1980), 73—76.

[17] T. NAKAMOTO: On QF-extensions in an H-separable extension, Proc. Japan Acad. **50** (1974), 440—443.

[18] G. SZETO: On Galois extensions over commutative rings, Proceedings of the 1978 Antwerp Conference, Lecture Notes Pure Appl. Math. **51**, Marcel Dekker, New York-Basel, 1979.

[19] G. SZETO: A characterization of a cyclic Galois extension of commutative rings, J. Pure Appl. Algebra **16** (1980), 315—322.

[20] G. SZETO and Y. F. WONG: On quaternion algebras over a commutative ring, Math. Japonica **25** (1980), 55—59.

[21] S. YUAN: On logalithmic derivatives, Bull. Soc. Math. France **96** (1968), 41—52.

DEPERTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received June 17, 1980*)