Math. J. Okayama Univ. 22 (1980), 115—129

ON SEPARABLE POLYNOMIALS AND FROBENIUS POLYNOMIALS IN SKEW POLYNOMIAL RINGS

Dedicated to Professor Gorô Azumaya on his 60th birthday

SHÛICHI IKEHATA

In [3] and [4], K. Kishimoto studied some special separable polynomials in skew polynomial rings, and in [7], T. Nagahara made a thorough investigation of separable polynomials of degree 2. More recently, Y. Miyashita [6] studied systematically separable polynomials and Frobenius polynomials.

In the present paper, we intend to make further progress on the study in this direction, and generalize or sharpen some results obtained in [6], [7] and [9].

Throughout the present paper, K will represent a ring with 1, ρ an automorphism of K, and D a ρ-derivation of K (i. e. an additive endomorphism of K such that $D(ab) = D(a)\rho(b) + aD(b)$ for all $a, b \in K$). Let $R = K[X; \rho, D]$ be the skew polynomial ring in which the multiplication is given by $aX = X\rho(a) + D(a)$ $(a \in K)$. In particular, we set $K[X; \rho] = K[X; \rho, 0]$, $K[X; D] = K[X; 1, D]$ (and $K[X] = K[X; 1, 0]$). By $R_{(0)}$ we denote the set of all monic polynomials g in R with $Rg = gR$. A ring extension A/B is called a separable extension if the A-A-homomorphism of $A \otimes_B A$ onto A defined by $a \otimes b \to ab$ splits, and A/B is called a Frobenius extension if A_B is finitely generated (*f. g.*) projective and A is B-A-isomorphic to $\mathrm{Hom}(A_B, B_B)$. A polynomial g in $R_{(0)}$ is called a separable (resp. Frobenius) polynomial if R/Rg is a separable (resp. Frobenius) extension of K.

We use the following convensions:

$Z =$ the center of K.

$C(A) =$ the center of a ring A.

$u_l =$ the left multiplication by $u \in K$, and $u_r =$ the right multiplication by u.

$I_{u,\rho} =$ the inner ρ-derivation effected by $u \in K$; $I_{u,\rho}(a) = au - u\rho(a)$ $(a \in K)$.

$I_u = I_{u,1} = u_r - u_l$, and $D_\rho = I_{-1,\rho} = \rho - 1$.

$K^\rho = \{a \in K \mid \rho(a) = a\}$, $K^D = \{a \in K \mid D(a) = 0\}$, and $K^{\rho,D} = K^\rho \cap K^D$.

$f = X^m + X^{m-1}a_{m-1} + \cdots + Xa_1 + a_0$ $(\in R)$, and

$Y_0 = X^{m-1} + X^{m-2}a_{m-1} + \cdots + Xa_2 + a_1$

$Y_1 = X^{m-2} + X^{m-3}a_{m-1} + \cdots + a_2$

....

$Y_{m-2} = X + a_{m-1}$

$Y_{m-1} = 1$.

We borrow heavily of Miyashita [6] at various points. Among other things, the following proved in [6, Theorem 1.8 and Proposition 1.13] play essential rôles in our study:

Theorem A. *Let f be in $R_{(0)}$, and $I = Rf$. If f is separable then there exists $y \in R$ with* deg $y < m$ *such that* $\sum_{j=0}^{m-1} Y_j y X^j \equiv 1$ (mod I) and $\rho^{m-1}(a)y = ya$ *for all $a \in K$, and conversely. In particular, f in $K[X]$ is separable if and only if the derivative f' of f is invertible in $K[X]$ modulo I.* (Note that $f' = \sum_{j=0}^{m-1} Y_j X^j$.)

Theorem B. *Let f be in $R_{(0)}$, and $I = Rf$. If f is Frobenius then there exists $r \in R$ with* deg $r < m$ *such that r is invertible in R modulo I and $\rho^{m-1}(a)r = ra$ (or $r\rho^{m-1}(a) = ar$) for all $a \in K$, and conversely. In particular, f in $K[X; D]_{(0)}$ is always Frobenius.* (We can take 1 as r.)

In §1, we consider the condition $Rf = fR$. The results obtained in this section will play fundametal rôles in our subsequent study. In §2, we assume that $\rho D = D\rho$, and introduce the notion of $(\tilde{\rho}, \tilde{D})$-separability, which is closely related to derivatives. The characterizations of $(\tilde{\rho}, \tilde{D})$-separable polynomials will be given. §3 contains several remarks on separable polynomials in $K[X; \rho]$ and $K[X; D]$, in particular, [7, Theorems 2.19 and 3.5] will be generalized. In §4, K will be assumed to be of prime characteristic p, and R will be $K[X; D]$. A criterion for a p-polynomial in $R_{(0)}$ to be separable is given. In case D is Z-linear ($D|Z = 0$), this enables us to see that if R contains at least one $(\tilde{1}, \tilde{D})$-separable p-poynomial then every separable p-polynolmial in R is $(\tilde{1}, \tilde{D})$-separable. In §5, we define a QF-polynomial and show that every separable polynomial in $K[X; \rho]$ is a QF-polynomial. Finally, in §6, we show that the question raised by Miyashita in [6] has an affirmative answer for some special cases.

1. Polynomials in $R_{(0)}$.

First, we state the following

Lemma 1.1. *If f is in $R_{(0)}$, then $af = f\rho^m(a)$ ($a \in K$) and $Xf = f(X - D_\rho(a_{m-1}))$, and conversely.*

Proof. Assume that $Rf = fR$. Since f is monic, for every $a \in K$ there exists $b \in K$ such that $af = fb$. Comparing the leading coefficients of the both sides, we obtain $b = \rho^m(a)$. Similarly, there exists $c \in K$

such that $Xf = f(X-c)$. Comparing the coefficients of X^m in the both sides, we have $c = D_\rho(a_{m-1})$.

Lemma 1. 2. *Assume that* $\rho D = D\rho$. *Then* $Kf = fK$ (*i. e.* $af = f\rho^m(a)$ $(a \in K)$) *if and only if*

a) $a_i\rho^m(a) = \sum_{j=i}^m \binom{j}{i} \rho^i D^{j-i}(a)a_j \, (a \in K,\ 0 \leqq i \leqq m-1)$.

In particular, if f *is in* $K^{\rho,D}[X]$ and $Kf = fK$, *then* f, f' *are in* $C(K^{\rho,D})[X]$.

Proof. Obviously, $Kf = fK$ if and only if $af = f\rho^m(a)$ $(a \in K)$. By an easy induction, we obtain $aX^j = \sum_{i=0}^j X^i \binom{j}{i} \rho^i D^{j-i}(a)$ $(a \in K,\ j \geqq 0)$. Hence,

$$af = \sum_{j=0}^m \Big(\sum_{i=0}^j X^i \binom{j}{i} \rho^i D^{j-i}(a)\Big) a_j = \sum_{i=0}^m X^i \Big(\sum_{j=i}^m \binom{j}{i} \rho^i D^{j-i}(a)\, a_j\Big)$$

and

$$f\rho^m(a) = \sum_{i=0}^m X^i a_i \rho^m(a).$$

From those above, we readily see that $Kf = fK$ is equivalent to a).

Next, we shall prove the latter part. For any $a \in K$, we have

$$\begin{aligned} af' &= \sum_{j=1}^m j\Big(\sum_{i=0}^{j-1} X^i \binom{j-1}{i} \rho^j D^{j-1-i}(a)a_j\Big) \\ &= \sum_{j=1}^m \sum_{i=1}^j X^{i-1} i \binom{j}{i} \rho^{i-1} D^{j-i}(a)a_j \\ &= \sum_{i=1}^m \sum_{j=i}^m X^{i-1} i \binom{j}{i} \rho^{i-1} D^{j-i}(a)a_j \\ &= \sum_{i=1}^m X^{i-1} i \Big(\sum_{j=i}^m \binom{j}{i} \rho^{i-1} D^{j-i}(a)\, a_j\Big). \end{aligned}$$

Since $\sum_{j=i}^m \binom{j}{i} \rho^{i-1} D^{j-i}(a)a_j = a_i \rho^{m-1}(a)$ by a), we obtain $af' = f'\rho^{m-1}(a)$. In case $R = K[X;\ \rho]$, Lemma 1. 1 can be stated more explicitly as follows:

Lemma 1.3. *Let* f *be in* $R = K[X;\ \rho]$. *Then* f *is in* $R_{(0)}$ *if and only if*

a) $aa_i = a_i\rho^{m-i}(a)$ $(a \in K,\ 0 \leqq i \leqq m-1)$,

b) $D_\rho(a_i) = a_{i+1}D_\rho(a_{m-1})$ $(0 \leqq i \leqq m-2)$,

c) $a_0 D_\rho(a_{m-1}) = 0$.

In particular, $R(X + a_0) = (X + a_0)R$ *if and only if* $aa_0 = a_0\rho(a)\,(a \in K)$.

Proof. Comparing the coefficients, we can easily see that $af = f\rho^m(a)$ implies a) and $Xf = f(X - D_\rho(a_{m-1}))$ does b) and c), and conversely.

Remark 1.4. Let f be in $K[X;\ \rho]_{(0)}$. Then, by Lemma 1.3, there holds $aD_\rho(a_{m-1}) = D_\rho(a_{m-1})\rho(a)$ $(a \in K)$, and if $D_\rho(a_{m-1}) = 0$ then f is in $C(K^\rho)\,[X]$,

Corollary 1.5. *Let K be a semiprime ring, and $R = K[X;\ \rho]$. If f is in $R_{(0)}$ then $D_\rho(a_{m-1}) = 0$, and hence $f \in C(K^\rho)\,[X]$.*

Proof. By Lemma 1.3, $a_{m-1}a_{m-1} = a_{m-1}\rho(a_{m-1})$ and $a_{m-1}\rho(a_{m-1}) = \rho(a_{m-1})\rho(a_{m-1})$, i. e. $a_{m-1}D_\rho(a_{m-1}) = 0 = D_\rho(a_{m-1})\,\rho(a_{m-1})$.
Hence $D_\rho(a_{m-1})^3 = D_\rho(a_{m-1})\rho(a_{m-1})D_\rho(a_{m-1}) - D_\rho(a_{m-1})a_{m-1}D_\rho(a_{m-1}) = 0$. Since K is semiprime and $KD_\rho(a_{m-1}) = D_\rho(a_{m-1})K$, we obtain $D_\rho(a_{m-1}) = 0$.

Finally, we consider the case $R = K[X;\ D]$.

Lemma 1. 6. *Let f be in $R = K[X;\ D]$. Then $Rf = fR$ if and only if*

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

b) $a_i \in K^D$ $(0 \leqq i \leqq m-1)$.

When this the case, f is in $C(K^D)\,[X]$.

Proof. By Lemma 1. 1, $Rf = fR$ if and only if $af = fa$ $(a \in K)$ and $Xf = fX$. Obviously, $Xf = fX$ is equivalent to b). The equivalence of $af = fa\ (a \in K)$ and a) has been proved in Lemma 1. 2.

Corollary 1.7. *Assume that K is of prime characteristic p. Let f be in $R = K[X;\ D]$ and of the form $\sum_{i=0}^{e} X^{p^i}b_{i+1} + b_0$. Then $Rf = fR$ if and only if*

a) $\sum_{i=0}^{e} D^{p^i}(a)b_{i+1} + ab_0 - b_0 a = 0\ (a \in K)$ *and* $b_{i+1} \in Z\,(0 \leqq i \leqq e)$,

b) $b_i \in K^D\ (0 \leqq i \leqq e+1)$.

2. $(\tilde{\rho}, \widetilde{D})$-separable polynomials. Throughout this section, we assume that $\rho D = D\rho$. Let $R = K[X;\ \rho,\ D]$, and consider the mappings $\rho^* : R \rightarrow R$ and $D^* : R \rightarrow R$ defined by $\rho^*(\sum_i X^i d_i) = \sum_i X^i \rho(d_i)$ and $D^*(\sum_i X_i{}^i d_i) = \sum_i X^i D(d_i)$, respectively. As is easily seen, ρ^* is a ring automorphism of R, and D^* is the inner ρ^*-derivation of R effected by X; $D^*(h) = hX - X\rho^*(h)\ (h \in R)$. Obviously ρ^* and D^* are extensions of ρ and D, respectively. Henceforth, our interest will be restricted to such f that $f \in K[X;\ \rho,\ D]_{(0)} \cap K^{\rho,D}[X]$ $(\subseteqq C(K^{\rho,D})\,[X]$ by Lemmas 1.1 and 1.2). Then the ideal $I = Rf$ is both ρ^*-invariant $(\rho^*(I) = I)$ and D^*-invariant $(D^*(I) \subseteqq I)$. Thus, ρ^* induces naturally an automorphism $\tilde{\rho}$ of R/I, and D^* does an inner $\tilde{\rho}$-derivation $\widetilde{D}$ of R/I. Needless to say, $\tilde{\rho}$ and $\widetilde{D}$ are regarded as extensions of ρ and D, respectively. Now, accorcing to $f \in K^{\rho,D}[X]$, we obtain $\rho^*(Y_j) = Y_j$, $D^*(Y_j) = 0$, and $f' = \sum_{j=0}^{m-1} Y_j X^j = \sum_{j=0}^{m-1} X^j Y_j$. Next, we consider the following mappings:

$$\begin{aligned} \mu:\ & {}_{R/I}R/I \otimes_K R/I_{R/I} \to {}_{R/I}R/I_{R/I} \\ & x \otimes y \to xy; \\ \xi:\ & R/I \otimes_K R/I \to R/I \otimes_K R/I \\ & x \otimes y \to \widetilde{D}(x) \otimes \tilde{\rho}(y) + x \otimes D(y); \\ \eta:\ & R/I \otimes_K R/I \to R/I \otimes_K R/I \\ & x \otimes y \to \tilde{\rho}(x) \otimes \tilde{\rho}(y) - x \otimes y. \end{aligned}$$

Then, it is easy to see that ξ and η are (well-defined) additive homomorphisms. If there exists an R/I-R/I-homomorphism ν: $R/I \to R/I \otimes_K R/I$ such that $\mu\nu = 1$, $\xi\nu = \nu\widetilde{D}$ and $\eta\nu = \nu(\tilde{\rho} - 1)$, then f is called a $(\tilde{\rho}, \widetilde{D})$-separable polynomial in R. A $(\tilde{\rho}, \tilde{0})$-separable polynomial in $K[X; \rho]$ and a $(\tilde{1}, \widetilde{D})$-separable polynomial in $K[X; D]$ will be called a $\tilde{\rho}$-separable polynomial and a $\widetilde{D}$-separable polynomial, respectively. Obviously, every $(\tilde{\rho}, \widetilde{D})$-separable polynomial is a separable polynomial.

We are now in a position to state our first main theorem.

Theorem 2.1. *Let f be in $K[X; \rho, D]_{(0)} \cap K^{\rho,D}[X]$, and $I = Rf$. Then the following are equivalent:*

a) *f is $(\tilde{\rho}, \widetilde{D})$-separable in R.*

b) *There exists $y \in K^{\rho,D}[x]$ with* deg $y < m$ *such that $\sum_{j=0}^{m-1} Y_j y X^j \equiv 1 \pmod{I}$ and $\rho^{m-1}(a)y = ya$ for all $a \in K$.*

c) *f' is invertibie in R modulo I.*

d) *f is separable in $K^{\rho,D}[X]$.*

e) *f is separable in $C(K^{\rho,D})[X]$.*

Proof. Recall that d) (resp. e)) is equivalent to the condition that f' is invertible in $K^{\rho,D}[X]$ (resp. $C(K^{\rho,D})[X]$) modulo $K^{\rho,D}[X]f$ (resp. $C(K^{\rho,D})[X]f$) (see Theorem A).

a)$\Longrightarrow$b). Let ν: ${}_{R/I}R/I_{R/I} \to {}_{R/I}R/I \otimes_K R/I_{R/I}$ be such that $\mu\nu = 1$, $\xi\nu = \nu\widetilde{D}$ and $\eta\nu = \nu(\tilde{\rho} - 1)$. Then, by [6, Lemma 1.7], there exists $y \in R$ with deg $y < m$ such that $\rho^{m-1}(a)y = ya (a \in K)$ and $\nu(z + I) = \sum_{j=0}^{m-1} (zY_j y + I) \otimes (X^j + I) (z \in R)$. Since $\rho^*(Y_j) = Y_j$, we have

$$\begin{aligned} 0 &= \nu(\tilde{\rho} - 1)(1 + I) = \eta\nu(1 + I) \\ &= \eta\{\textstyle\sum_{j=0}^{m-1} (Y_j y + I) \otimes (X^j + I)\} \\ &= \textstyle\sum_{j=0}^{m-1} (Y_j \rho^*(y) + I) \otimes (X^j + I) - \sum_{j=0}^{m-1} (Y_j y + I) \otimes (X^j + I) \\ &= \textstyle\sum_{j=0}^{m-1} (Y_j(\rho^*(y) - y) + I) \otimes (X^j + I). \end{aligned}$$

Since $\{X^j + I \mid j = 0, \cdots, m-1\}$ is a free basis of ${}_KR/I$, we see that $\rho^*(y) - y = Y_{m-1}(\rho^*(y) - y) \in I$. Since $\deg(\rho^*(y) - y) \leqq \deg\ y < m$, we obtain $\rho^*(y) = y$. Next, since $D^*(Y_j) = 0$, we have

$$\begin{aligned} 0 &= \nu\widetilde{D}(1 + I) = \xi\nu(1 + I) \\ &= \xi\{\textstyle\sum_{j=0}^{m-1}(Y_jy + I) \otimes (X^j + I)\} \\ &= \textstyle\sum_{j=0}^{m-1}(D^*(Y_jy) + I) \otimes (X^j + I) \\ &= \textstyle\sum_{j=0}^{m-1}(Y_jD^*(y) + I) \otimes (X^j + I). \end{aligned}$$

By the same reason as above, we see that $D^*(y) = Y_{m-1}D^*(y) \in I$. This together with $\deg D^*(y) \leqq \deg\ y < m$ implies $D^*(y) = 0$. Thus we conclude $y \in K^{\rho,D}[X]$.

b) $\Longrightarrow$ c). Since $y \in K^{\rho,D}[X]$ and $Y_j \in C(K^{\rho,D})[X]$ (Lemma 1.2), we have $Xy = yX$ and $Y_jy = yY_j$. Since $f' = \sum_j Y_jX^j$, $\sum_{j=0}^{m-1} Y_jyX^j \equiv 1$ (mod I) implies therefore $f'y = yf' \equiv 1$ (mod I).

c) $\Longrightarrow$ e). Since $f' + I$ is invertible in R/I and $f' \in C(K^{\rho,D})[X]$, it follows that $f' + I$ is invertible in $(C(K^{\rho,D})[X] + I)/I \cong C(K^{\rho,D})[X]/C(K^{\rho,D})[X]f$. Hence f' is invertible in $C(K^{\rho,D})[X]$ modnlo $C(K^{\rho,D})[X]f$. Thus, f is separable in $C(K^{\rho,D})[X]$.

e) $\Longrightarrow$ d) $\Longrightarrow$ c) are obvious.

e) $\Longrightarrow$ a). There exists $y \in C(K^{\rho,D})[X]$ such that $f'y \equiv 1$ (mod $C(K^{\rho,D})[X]f$) and $\deg y < m$. As was shown in the proof of Lemma 1.2, $af' = f'\rho^{m-1}(a)$ $(a \in K)$. Hence, $f'(\rho^{m-1}(a)y - ya) = af'y - f'ya \equiv 0$ (mod I). Since f' is invertible modnlo I much more and $\deg(\rho^{m-1}(a)y - ya) < m$, it follows then $\rho^{m-1}(a)y = ya$ $(a \in K)$. Now, according to the proof of [6, Lemma 1.7], we can prove that $\sum_{j=0}^{m-1}(Y_jy + I) \otimes (X^j + I)$ commntes with every element of R/I. Consider the R/I-R/I-homomorphism $\nu: R/I \to R/I \otimes_K R/I$ defined by $\nu(z + I) = \sum_{j=0}^{m-1}(zY_j + I) \otimes (X^j + I)$. Obviously, $\sum_{j=0}^{m-1} Y_jyX^j = f'y \equiv 1$ (mod I) implies $\mu\nu = 1$. Moreover, we have

$$\begin{aligned} \eta\nu(z + I) &= \eta\{\textstyle\sum_{j=0}^{m-1}(zY_jy + I) \otimes (X^j + I)\} \\ &= \textstyle\sum_{j=0}^{m-1}(\rho^*(z)Y_jy + I) \otimes (X^j + I) - \sum_{j=0}^{m-1}(zY_jy + I) \otimes (X^j + I) \\ &= \textstyle\sum_{j=0}^{m-1}\{(\rho^*(z) - z)Y_jy + I\} \otimes (X_j + I) \\ &= \nu(\tilde{\rho} - 1)(z + I) \end{aligned}$$

and

$$\begin{aligned} \xi\nu(z + I) &= \xi\{\textstyle\sum_{j=0}^{m-1}(zY_jy + I) \otimes (X^j + I)\} \\ &= \textstyle\sum_{j=0}^{m-1}\{D^*(z)Y_jy + I\} \otimes (X^j + I) \\ &= \nu\widetilde{D}(z + I). \end{aligned}$$

This completes the proof.

If f is $(\tilde{\rho}, \tilde{D})$-seprable, then by Theorem 2.1 we can teke f' as r in Theorem B, so that f is a Frobenins polynomial.

Theorem 2. 2. *Let f be in $K[X; \rho]_{(0)} \cap K^{\rho}[X]$. Assume that $\rho^n = u_l u_r^{-1}$ with a unit u of K and a positive integer n that is a unit in K. If f is separable then it is $\tilde{\rho}$-separable.*

Proof. Let $v = \rho^{n-1}(u)\rho^{n-2}(u)\cdots\rho(u)u$. Since $ua = \rho^n(a)u$ $(a \in K)$ and $\rho^n(u) = u$, we have $\rho^{\nu}(u)a = \rho^n(a)\rho^{\nu}(u)$ and $\rho^{\nu}(u)u = u\rho^{\nu}(u)$. Hence, $va = \rho^{n^2}(a)v$ and $\rho(v) = u\rho^{n-1}(u)\cdots\rho(u) = v$. By Theorem A, there exists $y \in R$ with deg $y < m$ snch that $\rho^{m-1}(a)y = ya$ $(a \in K)$ and $\sum_j Y_j y X^j \equiv 1$ (mod I). We put here $g = n^{-2}\sum_{\nu=0}^{n^2-1}\rho^{*\nu}(y)$. Since $\rho(v) = v$, $\rho^{n^2}(a) = vav^{-1}$ and $\rho^{m-1}(a)y = ya$, we obtain $\rho^{*n^2}(y) = vyv^{-1} = yvv^{-1} = y$. This proves $\rho^*(g) = g$, and so, $g \in K^{\rho}[X]$. Since f', $Y_j \in C(K^{\rho})$ $[X]$ (Lemma 1.2), we see that

$$\begin{aligned} 1 &\equiv n^{-2}\textstyle\sum_{j=0}^{m-1} Y_j\{\sum_{\nu=0}^{n^2-1}\rho^{*\nu}(y)\} X^j \\ &= \textstyle\sum_{j=0}^{m-1} Y_j g X^j = g(\sum_{j=0}^{m-1} Y_j X^j) = gf' = f'g \pmod{I}. \end{aligned}$$

Thus, f is $\tilde{\rho}$-separable by Theorem 2. 1.

Corollary 2. 3. *Let f be in $K[X; \rho]_{(0)}$. Assume that $\rho = u_l u_r^{-1}$ with a unit u of K. If f is separable, then it is $\tilde{\rho}$-separable.*

Proof. By Lemma 1. 3a), $ua_{m-1} = a_{m-1}\rho(u) = a_{m-1}u$, and therefore $D_{\rho}(a_{m-1}) = 0$. Then, f is in $K^{\rho}[X]$ by Remark 1. 4, and hence $\tilde{\rho}$-separable by Theorem 2. 2.

Let K be a (two-sided) simple ring, and f a separable polynomial in $K[X; \rho]$. Then f is in $C(K^{\rho})$ $[X]$ by Corollary 1. 5. By Lemma 1. 2a), we have $aa_i = a_i\rho^{m-i}(a)$ $(a \in K)$. Hence, if $a_j \neq 0$ for some j, then ρ^{m-j} is necessarily an inner automorphism. On the other hand, if $a_i = 0$ for all i then $f = X$ by [1, Lemma 1]. Now, the following two corollaries are obvious by Theorem 2. 2.

Corollary 2. 3. *Let K be a simple ring of characteristic zero. If f is a separable polynomial in $K[X; \rho]$, then it is $\tilde{\rho}$-separable.*

Corollary 2. 5. *Let K be a simple ring of characteristic $p > 0$, and f a separable polynomial with deg $f > 1$ in $K[X; \rho]$. Let n be the minimal positive integer such that ρ^n is inner. If $(p, n) = 1$, then every separable polynomial in $K[X; \rho]$ is $\tilde{\rho}$-separable.*

Remark 2.6. (c.f. [7, Remark 2.4]). Let ρ be the generator of the Galois group of $GF(4)/GF(2)$. Let $f = X^2 + 1 \in GF(4)[X; \rho]$. Since $z + \rho(z) = 1$ with some z, f is separable by [7, Lemma 2.3]. But, f' being zero, f is not $\tilde{\rho}$-separable.

Next, we consider the case $R = K[X; D]$.

Theorem 2.7. *Let $R = K[X; D]$. If $D = I_u$, then every separable polynomial in R is $\tilde{D}$-separarable.*

Proof. Assume that f is a separable polynomial in R. Then $f \in K^D[X]$ by Lemma 1.6. Now, putting $Y = X - u$, we see that $R = K[Y]$ and $f = \sum_{i=0}^{m} (Y + u)^i a_i$ is in $K[Y]_{(0)}$. Moreover, the derivative f_Y' of f with respect to Y equals $\sum_{i=0}^{m}((Y + u)^i a_i)_Y' = \sum_{i=1}^{m} i(Y+u)^{i-1} a_i = f'$. Since f_Y' is invertible modulo Rf by Theorem A, f is $\tilde{D}$-separable by Theorem 2.1.

Corollary 2.8. *Let $R = K[X; D]$. If f is separable in R and m is invertible in K, then f is $\tilde{D}$-separable.*

Proof. By Lemma 1.6 a), we have $a_{m-1}a = aa_{m-1} + mD(a)$. Since m is invertible in K, D is an inner derivation, and f is $\tilde{D}$-separable by Theorem 2.7.

3. Some remarks on $K[X; \rho]$ and $K[X; D]$. If f is separable in $K[X; \rho]$, then by [1, Lemma 1] there exist d, $c_0 \in K$ such that $a_1 c_0 - a_0 d = 1$. By making use of this fact, we shall prove the following two propositions.

Proposition 3.1. (cf. [9, Theorem 1 (b)]). *Let f be separable in $K[X; \rho]$. If $\rho(a_0) = a_0$ then $\rho(a_{m-1}) = a_{m-1}$, and so $f \in C(K^\rho)[X]$.*

Proof. By Remark 1.4 and Lemma 1.3, we have $D_\rho(a_{m-1}) = (a_1 c_0 - a_0 d) D_\rho(a_{m-1}) = a_1 D_\rho(a_{m-1})(c_0) - a_0 D_\rho(a_{m-1}) \rho(d) = 0$.

Proposition 3.2. *Let f be separable in $K[X; \rho]$. Then $(\rho|Z)^{m(m-1)} = 1_Z$.*

Proof. Let c be an arbitrary element of Z. Then, by Lemma 1.3 a), $(\rho^\nu - \rho^{\nu+m})(c)a_0 = a_0\rho^{\nu+m}(c) - \rho^{\nu+m}(c)a_0 = 0$, and so $(1 - \rho^{(m-1)m})(c)a_0 = \{(1 - \rho^m) + \cdots + (\rho^{m(m-2)} - \rho^{m(m-1)})\}(c)a_0 = 0$. Similarly, $(1 - \rho^{m(m-1)})(c)a_1 = 0$. Hence, $(1 - \rho^{(m-1)m})(c) = (1 - \rho^{(m-1)m})(c)(a_1 c_0 - a_0 d) = 0$.

Now, we assume that $\rho=u_l u_r^{-1}$ with some unit u in K. Then, it is easy to see that $K[X;\rho]=K[Y]$, where $Y=Xu$. If f is in $K[X;\rho]_{(0)}$ then, as was shown in the proof of Corollary 2. 3, it is in $K^{\rho}[X]$, i. e. $ua_i=a_iu$. Hence $f=\sum_{i=0}^{m}(Yu^{-1})^i a_i=hu^{-m}$, where $h=\sum_{i=0}^{m}Y^iu^{m-i}a_i$. As is easily seen, h is in $K[Y]_{(0)}=Z[Y]_{(0)}$. Taking those above into mind, we shall generalize [7, Theorem 2. 19] as follows:

Theorem 3. 3. *Let $\rho=u_l u_r^{-1}$ with a unit u in K, and let $\psi: K[X;\rho]\to K[X]$ be defined by $\psi(\sum_{i=0}^{n}X^id_i)=\sum_{i=0}^{n}X^iu^{n-i}d_i$.*

(a) *ψ induces a one-to-one correspondence between $K[X;\rho]_{(0)}$ and $Z[X]_{(0)}$.*

(b) *Let g be in $K[X;\rho]_{(0)}$. Then g is separable if and only if so is $\psi(g)$.*

(c) *Let g be in $K[X;\rho]_{(0)}$. Then $K[X;\rho]/gK[X;\rho]$ is K-ring isomorphicto $K\otimes_Z(Z[X]/\psi(g)Z[X])$.*

(d) *Let g_1, g_2 be in $K[X;\rho]_{(0)}$. Then $K[X;\rho]/g_1K[X;\rho]$ is K-ring isomorphic to $K[X;\rho]/g_2K[X;\rho]$ if and only if $Z[X]/\psi(g_1)Z[X]$ is Z-ring isomorphic to $Z[X]/\psi(g_2)Z[X]$.*

Proof. Obviously, ψ induces an injective mapping of $K[X;\rho]_{(0)}$ into $K[X]_{(0)}=Z[X]_{(0)}$. Given $\sum_{i=0}^{n}X^ib_i$ in $Z[X]_{(0)}$, $\sum_{i=0}^{n}X^iu^{i-n}b_i$ is in $K[X;\rho]_{(0)}$ and its image by ψ is $\sum_{i=0}^{n}X^ib_i$. Thus, ψ maps $K[X;\rho]_{(0)}$ onto $Z[X]_{(0)}$. The mapping Ψ: $K[X;\rho]\to K[X]$ defined by $\psi(\sum_iX^id_i)=\sum_iX^iu^{-i}d_i$ is easily seen to be a K-ring isomorphism. Since for any $g\in K[X;\rho]_{(0)}$ of degree n we have $\Psi(g)=\psi(g)u^{-n}$, Ψ induces naturally a K-ring isomorphism $\bar{\Psi}$: $K[X;\rho]/gK[X;\rho]\cong K[X]/\psi(g)K[X]$. Therefore, g is separable in $K[X;\rho]$ if and only if so is $\psi(g)$ in $K[X]$. By Theorem 2. 1, $\psi(g)$ is separable in $K[X]$ if and only if so it is in $Z[X]$. As a combination of those above, we obtain (b). Moreover, the K-ring isomorphism $K[X]\psi(g)K[X]\cong K\otimes_Z(Z[X]/\psi(g)Z[X])$ together with $\bar{\Psi}$ implies (c). Finally, we shall prove (d). If $K[X;\rho]/g_1K[X;\rho]\cong K[X;\rho]/g_2K[X;\rho]$ (K-ring isomorphism), then we have the following K-isomorphisms:

$$\begin{aligned}K[X]/\psi(g_1)K[X]&\cong K[X;\rho]/g_1K[X;\rho]\\&\cong K[X;\rho]/g_2K[X;\rho]\cong K[X]/\psi(g_2)K[X].\end{aligned}$$

As is easily verified, the center of $K[X]/\psi(g_k)K[X]$ is Z-ring isomorphic to $Z[X]/\psi(g_k)Z[X]$. Hence we have a Z-ring isomorphism $Z[X]/\psi(g_1)Z[X]\cong Z[X]/\psi(g_2)Z[X]$. The converse is obvious by (c).

Corresponding to Theorem 3. 3, we shall generalize [7, Theorem 3. 5] as follows:

Theorem 3.4. *Let $D=I_u$, and let $\phi: K[X;\ D]\rightarrow K[X]$ be defined by $\phi(\sum_{i=0}^{n} X^i d_i) = \sum_{i=0}^{n}(X+u)^i d_i$.*

(a) *ϕ induces a one-to-one correspondence between $K[X;\ D]_{(0)}$ and $Z[X]_{(0)}$.*

(b) *Let g be in $K[X;\ D]_{(0)}$. Then g is separable if and only if so is $\phi(g)$.*

(c) *Let g be in $K[X;\ D]_{(0)}$. Then $K[X;\ D]/gK[X;\ D]$ is K-ring isomorphic to $K\otimes_Z(Z[X]/\phi(g)Z[X])$.*

(d) *Let g_1, g_2 be in $K[X;\ D]_{(0)}$. Then $K[X;\ D]/g_1K[X;\ D]$ is K-ring isomorphic to $K[X;\ D]/g_2K[X;\ D]$ if and only if $Z[X]/\phi(g_1)Z[X]$ is Z-ring isomorphic to $Z[X]/\phi(g_2)Z[X]$.*

Proof. From the proof of Theorem 2.7, it is easy to see that ϕ is a K-ring isomorphism and induces a one-to-one correspondence between $K[X;\ D]_{(0)}$ and $Z[X]_{(0)}$. Since ϕ induces naturally a K-ring isomorphism $\bar{\phi}$: $K[X;\ D]/gK[X;\ D]\cong K[X]/\phi(g)K[X]$, g is separable in $K[X;\ D]$ if and only if so is $\phi(g)$ in $K[X]$. By Theorem 2.1, $\phi(g)$ is separable in $K[X]$ if and only if so it is in $Z[X]$. Combining those above, we obtain (b). Moreover, the K-ring isomorphism $K[X]/\phi(g)K[X]\cong K\otimes_Z(Z[X]/\phi(g)Z[X])$ together with $\bar{\phi}$ implies (c). Finally, we shall prove (d). If $K[X;\ D]/g_1K[X;\ D]\cong K[X;\ D]/g_2K[X;\ D]$ (K-ring isomorphism), then we have the following K-ring isomorphisms:

$$\begin{aligned} K[X]/\phi(g_1)K[X] &\cong K[X;\ D]/g_1K[X;\ D] \\ &\cong K[X;\ D]/g_2K[X;\ D]\cong K[X]/\phi(g_2)K[X]. \end{aligned}$$

As is easily verified, the center of $K[X]\phi(g_k)K[X]$ is Z-ring isomorphic to $Z[X]/\phi(g^k)Z[X]$. Hence, $Z[X]/\phi(g_1)Z[X]$ is Z-ring isomorphic to $Z[X]/\phi(g_2)Z[X]$. The converse is obvious by (c).

4. p-polynomials in $K[X;D]$. Throughout this section, we assume that K is of prime characteristic p and $R=K[X;\ D]$. We assume further that f is a p-polynomial and of the form $\sum_{i=0}^{e} X^{p^i}b_{i+1}+b_0$.

First, we shall prove the following which is a generalization of [6, Theorem 3.2]:

Theorem 4.1. *Let f be in $R_{(0)}$. Then f is separable if and only if there exists $y\in R$ with deg $y<p^e$ such that $ay=ya$ $(a\in K)$* and $\sum_{i=0}^{e} D^{*p^i-1}(y)b_{i+1}+1=0$.

Proof. By an easy induction, we have

$$D^{*\nu}(g)=\sum_{j=0}^{\nu}\binom{\nu}{j}(-1)^{\nu-j}X^{\nu-j}gX^j \qquad (g\in R,\ \nu\geqq 0).$$

Since $\binom{p^k-1}{j}(-1)^{p^k-j-1}\equiv 1 \pmod{p^k}$, there holds $D^{*p^k-1}(g)=\sum_{j=0}^{p^k-1}X^{p^k-j-1}gX^j$. Assume that f is separable. Then, by Theorem A, there eyists $y\in R$ with $deg\, y<p^e$ such that $ay=ya\ (a\in K)$ and $\sum_{j=0}^{p^e-1}Y_jyX^j\equiv 1 \pmod{Rf}$. Noting that $b_{i+1}\in K^D$ (Lemma 1. 6 b)), we obtain

$$\begin{aligned}\sum_{i=0}^{e}D^{*p^i-1}(-y)b_{i+1}+1&=-\sum_{j=0}^{p^e-1}X^{p^e-j-1}yX^j-\sum_{j=0}^{p^{e-1}}X^{p^{e-1}-j-1}b_eyX^j\\&\quad-\cdots-\sum_{j=0}^{p-1}X^{p-j-1}b_2yX^j-b_1y+1\\&=-\sum_{j=0}^{p^e-1}Y_jyX^j+1\equiv 0 \pmod{Rf}.\end{aligned}$$

Since the degree of the left side of the above is smaller than p^e, we conclude $\sum_{i=0}^{e}D^{*p^i-1}(-y)b_{i+1}+1=0$. Reversing the above arguments, we can prove the converse.

Corollary 4.2. ([6. Theorem 3. 2]) *Let* $f=X^p+Xb_1+b_0$ be in $R_{(0)}$. *Then f is separable if and only if there exists $y\in R$ with $deg\, y<p$ such that $ay=ya\ (a\in K)$ and $D^{*p-1}(y)+yb_1+1=0$.*

Remark 4. 3. If f is in $R_{(0)}$, then $f\in K^D[X]$ (Lemma 1. 6 b)) and $f'=b_1$. Hence, by Theorem 2. 1, we see that f is $\tilde{D}$-separable if and only if b_1 is invertible in K (cf. [2, Theorem]).

Now, we shall prove the main theorem of this section.

Theorem 4. 4. *Assume that D is Z-linear (i. e. $D|Z=0$). If $R=K[X;D]$ contains a $\tilde{D}$-separable p-polynomial, then every sepasable p-polynomial f in R is $\tilde{D}$-separable.*

Proof. By Theorem 4. 1, there exists $y=X^{p^e-1}d_{p^e-1}+\cdots+Xd_1+d_0\in R$ such that $ay=ya\ (a\in K)$ *and* $\sum_{i=0}^{e}D^{*p^i-1}(y)b_{i+1}+1=0$. An easy induction shows that $aD^{*^k}(y)=D^{*^k}(y)a\ (a\in K,\ k\geqq 0)$. Now, assume that $D^{*i-1}(y)=X^{p^e-i}D^{i-1}(d_{p^e-i})+\cdots+D^{i-1}(d_0)$ for some $i\geqq 1$. Since $aD^{*^{i-1}}(y)=D^{*^{i-1}}(y)a$, we see that $D^{i-1}(d_{p^e-1})$ is in Z, and therefore $D^i(d_{p^e-1})=0$, proving that $D^{*^i}(y)=X^{p^e-i-1}D^i(d_{p^e-i-1})+\cdots+D^i(d_0)$. Thus, we obtain eventually $D^{*p^e}(y)=0$.

Now, let $g=\sum_{j=0}^{n}X^{p^j}c_{j+1}+c_0$ be a $\tilde{D}$-separable p-polynomial in R, where $c_0\in K^D$ and $c_1,\cdots,c_{n+1}\in Z\cap K^D$ (Corollary 1. 7). Then, by Theorem 2. 1, $g'=c_1$ is a unit of K, and hence of Z. Since $\sum_{j=1}^{n}(c_{j+1})_rD^{p^j}+(c_1)_rD+I_{c_0}=0$ by Corollary 1. 7, we have then $D=$

$-\sum_{j=1}^{n}(c_1^{-1}c_{j+1})_r D^{p^j} - I_{c_1^{-1}c_0}$. Since $c_1^{-1}c_0 \in K^D$ and $ay = ya\ (a \in K)$, it follows $I^*_{c_1^{-1}c_0}(y) = 0$. Hence, $D^*(y) = \{-\sum_{j=1}^{n}(c_1^{-1}c_{j+1})_r D^{*p^j}\}(y)$ $= \{-\sum_{j=1}^{n}(c_1^{-1}c_{j+1})_r(-\sum_{k=1}^{n}(c_1^{-1}c_{k+1})_r D^{*p^k})^{p^j}\}(y)$. Combining this with $c_1^{-1}c_{j+1} \in K^D \cap Z$ and $D^{*p^e}(y) = 0$, we can easily see that $D^*(y) = 0$, and so $yb_1 + 1 = \sum_{i=0}^{e} D^{*p^t-1}(y)b_{i+1} + 1 = 0$, i. e. $d_1 b_1 = -1$. Thus, b_1 is invertible, and f is $\widetilde{D}$-separable by Theorem 2. 1.

5. QF-polynomials. In this section, we return back to the general case $R = K[X; \rho, D]$. Let A, B be rings, and ${}_AM_B$, ${}_AN_B$ A-B-bimodules. If ${}_AM_B$ is isomorphic to a direct summand of ${}_AN_B^n$ (the direct sum of n copies of ${}_AN_B$) for some n, then we write ${}_AM_B \mid {}_AN_B$. As is well-known, ${}_AM_B \mid {}_AN_B$ if and only if $\sum_i \psi_i\phi_i = 1_M$ for some $\phi_1, \cdots, \phi_n \in \mathrm{Hom}({}_AM_B, {}_AN_B)$ and $\psi_1, \cdots, \psi_n \in \mathrm{Hom}({}_AN_B, {}_AM_B)$.

Let f be in $R_{(0)}$, and $I = Rf$. If R/I is a right QF-extension over K (R/I_K is f. g. projective and ${}_KR/I_{R/I} \mid {}_K\mathrm{Hom}(R/I_K, K_K)_{R/I}$), then f is called a right QF-polynomial in R. A left QF-polynomial is defined by symmetrically, and a right and left QF-polynomial is called a QF-polynomial. Needless to say, every Frobenius polynomial is a QF-polynomial.

First, we prove the following

Theorem 5. 1. *Let f be in$R_{(0)}$, and $I = Rf$. If f is a right (resp. left) QF-polynomial, then there exist r_i, $s_i \in R$ with* deg $r_i < m$ *and* deg $s_i < m$ *such that $ar_i = r_i\rho^{m-1}(a)$, $s_ia = \rho^{m-1}(a)s_i$ $(a \in K)$ and $\sum_i s_ir_i \equiv 1$ (resp. $\sum_i r_is_i \equiv 1$)* (mod I), *and conversely.*

Proof. As is shown in [6, pp. 323-324], ${}_K\mathrm{Hom}(R/I_K, K_K)_{R/I} \cong {}_KKv \otimes {}_KR/I_{R/I}$ with a left K-free element $v \in R$ such that $va = \rho^{m-1}(a)v$ $(a \in K)$. Hence, f is right QF if and only if ${}_KR/I_{R/I} \mid {}_KKv \otimes {}_KR/I_{R/I}$. For any $\phi \in \mathrm{Hom}({}_KR/I_{R/I}, {}_KKv \otimes {}_KR/I_{R/I})$, We can easily find an $r \in R$ with $\phi(1+I) = v \otimes (r+I)$ such that deg $r < m$ and $ar = r\rho^{m-1}(a)(a \in K)$. Conversely, for such r the mapping ϕ: $R/I \to Kv \otimes {}_KR/I$ defined by $\phi(x+I) = v \otimes (rx+I)$ is a K-R/I-homomorphism. Similarly, for any $\psi \in \mathrm{Hom}({}_KKv \otimes {}_KR/I_{R/I}, {}_KR/I_{R/I})$, we can find an $s \in R$ with $\psi(v \otimes (1+I)) = s + I$ such that deg $s < m$ and $sa = \rho^{m-1}(a)s$ $(a \in R)$; conversely for such s the mapping $\psi: Kv \otimes {}_KR/I \to R/I$ defined by $\psi(v \otimes (x+I)) = sx + I$ is a K-R/I-homomorphism. Thus, the assertion concerning a right QF-polynomial is now immediate. Symmetrically, we can prove that concerning a left QF-polynomial.

Example. Let K be a field with an automorphism ρ of order 2, and

$R=K[X;\rho]$. Now, let $r=Xc_1+c_0$ and $s=Xd_1+d_0$ be such that $ar=r\rho(a)$ and $sa=\rho(a)s$ $(a\in K)$. Then, by $\rho\neq 1$ we see that $c_0=d_0=0$, and therefore $rs=X^2\rho(c_1)d_1$. In view of Theorem 5. 1, this implies that X^2 cannot be a right (left) QF-polynomial.

We conclude this section with the following

Theorem 5. 2. *Let* $R=K[X;\rho]$. *Then every separable polynomial* f *in* R *is a QF-polynomial.*

Proof. By Lemma 1. 3, $aX^{k-j-1}a_k = X^{k-j-1}\rho^{k-j-1}(a)a_k = X^{k-j-1}a_k\rho^{m-j-1}(a)$ $(a\in K)$. Hence, $aY_jX^j=Y_j\rho^{m-j-1}(a)X^j=Y_jX^j\rho^{m-1}(a)$ *and* $aX^jY_j=X^j\rho^j(a)Y_j=X^jY_j\rho^{m-1}(a)$. According to Theorem A, there exists $y\in R$ with deg $y<m$ such that $\rho^{m-1}(a)y=ya$ $(a\in K)$ and $\sum_{j=1}^{m-1}Y_jyX^j\equiv 1$ (mod I). Obviously, $\rho^{m-1}(a)\rho^{*\nu}(y)=\rho^{*\nu}(y)a$. Since $\sum_jY_jyX^j=\sum_jX^jyY_j$ by [6, Remark, p. 322], we have then

$$\sum_jY_jX^j\rho^{*j}(y)=\sum_jY_jyX^j\equiv 1 \pmod{I},$$
$$\sum_j\rho^{*-j}(y)X^jY_j=\sum_jX^jyY_j\equiv 1 \pmod{I}.$$

Thus, f is a QF-polynomial by Theorem 5. 1.

6. Frobenius polynomials. In [6], Miyashita posed the following question: Is any separable polynomial Frobenius? Some arguments concerning the question have been done in [6], [1], [10] and [11]. We shall prove first the following :

Theorem 6.1. *Let* $R=K[X;\rho]$. *Assume that* Z *is an integral domain and* $\rho|Z\neq 1_Z$. *Then every separable polynomial* f *in* R *is Frobenius.*

Proof. By [1, Lemma 1], there exist d, $c_0\in K$ such that $a_1c_0-a_0d=1$ and $a_1c_0\in Z$. Choose a $c\in Z$ such that $\rho(c)\neq c$. Then $\rho^m(c)\neq c$ or $\rho^{m-1}(c)\neq c$. Since $(c-\rho^m(c))\,a_0d=0$ and $(c-\rho^{m-1}(c))a_1c_0=0$ by Lemma 1. 3, we obtain $a_0d=0$ or $a_1c_0=0$, i. e. $a_1c_0=1$ or $a_0d=1$. Then, either a_1 or a_0 is invertible in K. Hence f is Frobenius by [1, Theorem 1].

Corollary 6. 2. *Let* K *be a prime ring, and* $R=K[X;\rho]$. *If* $\rho|Z\neq 1_Z$, *then every separable polynomial in* R *isFrobenius.*

Corollary 6. 3. *If* K *is a commutative integral domain, then every separable polynomial in* $K[X;\rho]$ *is Frobenius.*

Proposition 6.4. *Assume that K is a simple ring and f is a separabie polynomial in $R = K[X; \rho, D]$.*

(a) *If $\rho | Z \neq 1_Z$ then f is Frobenius.*

(b) *If $\rho | Z = 1_Z$ and $[K: Z] < \infty$, then f is Frobenius.*

Proof. (a) By [12, Lemme 3], $D = I_{u,\rho}$ with some $u \in K$. Then, it is easy to see that $R = K[\mathrm{Y}; \rho]$, where $Y = X - u$. Hence, f is Frobenius by Theorem 6. 1.

(b) By Noether-Skolem theorem, $\rho = u_l u_r^{-1}$ with some unit u in K. Then, in Theorem B, we can take u^{m-1} as r, and therefore f is Frobenius.

Now, we shall prove the following that is a slight generalization of [6, Theorem 3. 4 (2)]:

Theorem 6.5. *Assume that K is a simple ring. Let f be a separable polynomial in $R = K[X; \rho, D]$, and let $y = X^n c_n + X^{n-1} c_{n-1} + \cdots + c_0$ $(c_n \neq 0)$ be as in Theorem A. If $n = 0$ or $(m, n) = 1$, then f is Frobenius.*

Proof. If $n = 0$, then $\rho^{m-1}(a) c_0 = c_0 a$ $(a \in K)$. Since K is simple, c_0 has to be a unit, and therefore f is Frobenius by Theorem B. Henceforth, we assume that $(m, n) = 1$, and choose positive integers r, s such that $mr - ns = 1$. As is easily verified, $\delta_\nu = \sum_{i=0}^{\nu} \rho^i D \rho^{-i}$ is a ρ-derivation and

$$D = \sum_{k=0}^{r-1} \rho^{km} \delta_{m-1} \rho^{-km} - \rho \left(\sum_{l=0}^{s-1} \rho^{ln} \delta_{n-1} \rho^{-ln}\right) \rho^{-1}.$$

By Lemma 1. 1, $af = f\rho^m(a)$ $(a \in K)$. Comparing the coefficients of X^{m-1} in the both sides, we obtain

$$\delta_{m-1}(\rho^{m-1}(a)) + \rho^{m-1}(a) a_{m-1} = a_{m-1} \rho^m(a).$$

This means that δ_{m-1} is an inner ρ-deivation. Next, $\rho^{m-1}(a) y = ya$ implies $\rho^{m+n-1}(a) c_n = c_n a$ and $\delta_{n-1}(\rho^{m+n-2}(a)) c_n + \rho^{m+n-2}(a) c_{n-1} = c_{n-1} a$. Recalling that $c_n \neq 0$ and K is simple, we see that c_n is a unit. Hence,

$$\begin{aligned} \delta_{n-1}(\rho^{m+n-2}(a)) &= c_{n-1} a c_n^{-1} - \rho^{m+n-2}(a) c_{n-1} c_n^{-1} \\ &= c_{n-1} c_n^{-1} \rho^{m+n-1}(a) - \rho^{m+n-2}(a) c_{n-1} c_n^{-1}, \end{aligned}$$

which means that δ_{n-1} is an inner ρ-derivation. Since both $\rho^i \delta_{m-1} \rho^{-i}$ and $\rho^i \delta_{n-1} \rho^{-i}$ are inner ρ-derivations, D is so. Hence, f is Frobenius by [1, Corollary 1].

Corollary 6.6. *If K is a simple ring, then every separable poly-*

nomial of prime degree in $K[X; \rho, D]$ is Frobenius.

Corollary 6.7. *Assume that K is a simple ring of characteristic zero and $\rho D = D\rho$. Then every separable polynomial in $K[X; \rho, D]$ is Frobenius.*

Proof. Let f be a separable polynomial in $K[X; \rho, D]$. Obviously, $D = m^{-1}\sum_{i=0}^{m-1}\rho^i D\rho^{-i} = m^{-1}\delta_{m-1}$. As was shown in the proof of Theorem 6.5, δ_{m-1} is an inner ρ-derivation. Hence, D is also an inner ρ-derivation, and so f is Frobenius by [1, Corollary 1].

REFERENCES

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

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

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

[4] K. KISHIMOTO: A classification of free extensions of rings of automorphism type and derivation type, Math. J. Okayama Univ. **18** (1977), 163—169.

[5] Y. MIYASHITA: Commutative Frobenius algebras generated by a single element, J. Fac. Sci. Hokkaido Univ., Ser. I, **21** (1971), 166—176.

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

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

[8] 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.

[9] T. NAGAHARA: On separable polynomials of degree 2 in skew polynomial rings II, Math. J. Okayama Univ. **21**(1979), 167—177.

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

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

[12] E. WEXLER-KREINDLER: Propriétés de transfert des extensions d'Ore, Lecture Notes in Math. **641**, Springer-Verlag, Berlin, 1978, 235—251.

DEPERTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received November 17, 1979*)