J. Math. Soc. Japan
Vol. 31, No. 2, 1979

On a skew polynomial ring

By Yôichi MIYASHITA

(Received Oct. 7, 1977)

§ 0. Introduction.

If K is a commutative ring, and A is a commutative Frobenius K-algebra generated by a single element, then there exists a quasi-monic polynomial $f(X)$ such that $K[X]/(f(X))$ is K-algebra isomorphic to A, and conversely ([6]). In the preceding paper [8], as a generalization of this result, we have studied non-singular bilinear maps which come from a (*)-positively filtered ring $R=\bigcup_{i\geq 0}R_i$ over a not necessarily commutative ring K. In the present paper we study the case when R_1/K is isomorphic to K as right K-module (or equivalently, as left K-module). In this case, $R=\bigcup_{i\geq 0}R_i$ is a skew polynomial ring $K[X;\rho, D]=K\oplus XK\oplus X^2K\oplus\cdots$, which is defined by an automorphism ρ of K, a ρ-derivation D of K, and $aX=X\rho(a)+D(a)$ $(a\in K)$. Therefore some arguments proceed as in the case when R is a polynomial ring over a commutative ring, and more explicit descriptions may be obtained. Proposition 1.4 and Theorem 1.8 in this paper correspond to [6; Proposition 2.1], and Theorem 1.10 is analogous to [6; Proposition 3.2]. Further, Theorem 1.3 is a concrete description of [8; Theorem 12], and Theorem 1.9 corresponds to [5; Proposition 2.4]. However, the characterization of a separable polynomial (Theorem 1.8) is not enough. Because it is not easy to check that condition in practice. In fact, a monic polynomial $f(X)$ over a commutative ring is separable if and only if its discriminant (i.e. the resultant of $f(X)$ and $f'(X)$) is invertible, by virtue of the local criterion for a separable algebra. But, in our situation, we don't have a corresponding result. Consequently, in § 2 and § 3, we give several examples of separable polynomials. Further, concerning a separable polynomial, we have an open problem: Is a separable polynomial always Frobenius (i.e. its residue class ring is Frobenius over K)? Some arguments on this problem are done in § 3 (Theorem 3.4 and Theorem 3.5). It is easy to find a monic polynomial f such that $Rf=fR$ and R/Rf is not Frobenius over K. But we don't know as yet a separable polynomial which is not Frobenius. Finally, needless to say, the condition $Rf=fR$ for a monic polynomial f is not an easy one (Lemma 1.14 and Lemma 2.1). Concerning this, if K is an indecomposable commutative ring, every non-zero K-R-submodule I of R such that R/I is finitely generated and pro-

jective as left K-module is expressed as $I=fR$ with a monic polynomial f such that $Kf=fK$ (, and conversely) ([7]). If we assume that K is a two sided simple ring, then every non-zero K-R-submodule of R is expressed as the above, too. Because every gr_iR is a simple K-bimodule, and $R_{m-1}\oplus fR=R$ for any monic polynomial f of degree m. It will be worthy to find another condition about this problem.

§1.

Throughout this paper, all rings are associative, but not necessarily commutative. Every ring has the identity 1, which is preserved by homomorphisms, inherited by subrings and acts as the identity operator on modules. Let ${}_AP_{A'}$ be a left A-, right A'-module. If $P_{A'}$ is finitely generated, projective, and generator, and $\mathrm{Hom}(P_{A'}, P_{A'})$ (the ring of all right A'-endomorphisms of P) $\simeq A$ under the mapping induced by ${}_AP$, we call ${}_AP_{A'}$ an invertible module. It is well known that this is right-left symmetric. Here we recall the definition of a (*)-positively filtered ring, which is defined in [8].

Let $R\supseteqq K$ be rings, and $R_0=K\subseteqq R_1\subseteqq R_2\subseteqq\cdots$ an ascending sequence of additive subgroups such that $R=\bigcup_i R_i$ and $R_iR_j\subseteqq R_{i+j}$ for all $i, j\geqq 0$. Then we call $R=\bigcup R_i$ a positively filtered ring over K. If, further, $R=\bigcup R_i$ satisfies the following condition (*) we call $R=\bigcup R_i$ a (*)-positively filtered ring over K:

(*) Each R_i/R_{i-1} $(i\geqq 1)$ is an invertible K-bimodule, and $(R_i/R_{i-1})\otimes_K(R_j/R_{j-1})$ $\simeq R_{i+j}/R_{i+j-1}$ by the canonical mapping $(x_i+R_{i-1})\otimes(x_j+R_{j-1})\mapsto x_ix_j+R_{i+j-1}$ $(x_i\in R_i,\ x_j\in R_j)$, for all $i, j\geqq 1$.

We denote this ring by $K[R_1]$, and put $R_i=0$, if $i<0$. For any $i\geqq 0$, we put $gr_iR=R_i/R_{i-1}$, which is an invertible K-bimodule. By induction we can see that $R_i=R_1\cdots R_1$ (i-times)$=R_1^i$. Since gr_iR_K is projective, $R_i=R_{i-1}\oplus P_i$ for some right K-submodule P_i of R_i. Similarly $R_i=R_{i-1}\oplus Q_i$ for some left K-submodule Q_i of R_i. We call P_i (resp. Q_i) a monic right (resp. left) K-submodule of degree i. If P_i is a K-bisubmodule, P_i is called a monic K-bisubmodule of degree i. Note that $P_i\simeq gr_iR$ as K-bimodules, in this case.

Now we assume that $gr_1R_K\simeq K_K$, and $X+K\mapsto 1$ under this right K-isomorphism, where $X\in R_1$. Then $R_1=K\oplus XK$, and $Xa=0$ $(a\in K)$ implies $a=0$. For any $a\in K$, aX is written as $aX=a'+Xa''$ $(a', a''\in K)$. Since ${}_Kgr_1R_K$ is invertible, we know that $gr_1R=K(X+K)$ and $a(X+K)=0$ $(a\in K)$ implies $a=0$. Therefore $R_1=K\oplus KX$, and so the mapping $\rho: a\mapsto a''$ is an automorphism of K. Further it is easily seen that the mapping $D: a\mapsto a'$ is a ρ-derivation from K to K (i.e. $D(ab)=D(a)\rho(b)+aD(b)$ $(a, b\in K)$). Thus $aX=X\rho(a)+D(a)$ $(a\in K)$. Then the condition (*) implies that $gr_1R\otimes_K\cdots\otimes_K gr_1R$ (i-times) $\simeq gr_iR$, $(X+K)\otimes\cdots\otimes(X+K)\mapsto X^i+R_{i-1}$, and $X^ia=0$ implies $a=0$. Hence $R_i=R_{i-1}\oplus X^iK$ for all $i\geqq 1$. Similarly $R_i=R_{i-1}\oplus KX^i$. Therefore $R=K\oplus XK\oplus X^2K\oplus\cdots=K\oplus KX\oplus KX^2\oplus\cdots$. Thus $R=K[X;\rho, D]$, where $aX=X\rho(a)+D(a)$ $(a\in K)$. Note

that $aX^i \equiv X^i\rho^i(a) \pmod{R_{i-1}}$ for all $a \in K$. Conversely, an automorphism ρ and a ρ-derivation D of K determine an extension ring $R=K[X;\rho, D]$ of K, which is defined by $aX=X\rho(a)+D(a)$ (cf. [**1**]). If we put $R_i=K\oplus XK\oplus\cdots\oplus X^iK$, we can easily see that $R=\cup_i R_i$ is a (*)-positively filtered ring over K such that $R_1/K_K \cong K_K$, by the mapping $Xa+K \mapsto a$ $(a\in K)$.

In the remainder of this paper we assume that $R=K[X;\rho, D]$ and $R_i=K\oplus XK\oplus\cdots\oplus X^iK$ $(i\geqq 0)$. Let g be a monic polynomial of degree n. Then $R_n=R_{n-1}\oplus gK=R_{n-1}\oplus Kg$. Conversely, if P_n is a monic right K-submodule of degree n then $g\equiv X^n \pmod{R_{n-1}}$ for some $g\in P_n$. Then $R_n=R_{n-1}\oplus gK$, and so $gK=P_n$, because $gK\subseteqq P_n$. If P_n is a monic K-bisubmodule, then $P_n=Kg$, so that $P_n=Kg=gK$. In this case, as is easily seen, $ag=g\rho^n(a)$ for all $a\in K$. Hence $P_n \cong gr_nR$, $g \mapsto X^n+R_{n-1}$, as K-bimodules.

In the following we fix a monic polynomial $f=X^m+X^{m-1}a_{m-1}+\cdots+a_0$ $(m\geqq 1)$, and put $a_m=1$. As in [**6**], we put

$$
\begin{aligned}
&Y_{m-1}=1\\
&Y_{m-2}=X+a_{m-1}\\
&Y_{m-3}=X^2+Xa_{m-1}+a_{m-2}\\
&\cdots\cdots\cdots\\
&Y_i=X^{m-i-1}+X^{m-i-2}a_{m-1}+\cdots+a_{i+1}\\
&\cdots\cdots\cdots\\
&Y_0=X^{m-1}+X^{m-2}a_{m-1}+\cdots\cdots\cdots\cdots+a_1.
\end{aligned}
$$

$f^*=X^m+a_{m-1}^*X^{m-1}+\cdots+a_0^*$ $(a_m^*=1)$ is defined by $a_i^*X^{m-1}\equiv X^{m-1}a_i \pmod{R_{m-2}}$ $(i=0, 1, \cdots, m-1)$ (i.e. $\rho^{m-1}(a_i^*)=a_i$). Further we put

$$
\begin{aligned}
&Y_{m-1}^*=1\\
&Y_{m-2}^*=X+a_{m-1}^*\\
&Y_{m-3}^*=X^2+a_{m-1}^*X+a_{m-2}^*\\
&\cdots\cdots\cdots\\
&Y_i^*=X^{m-i-1}+a_{m-1}^*X^{m-i-2}+\cdots+a_{i+1}^*\\
&\cdots\cdots\cdots\\
&Y_0^*=X^{m-1}+a_{m-1}^*X^{m-2}+\cdots\cdots\cdots\cdots+a_1^*.
\end{aligned}
$$

M, M^*, M_1, and M_1^* are defined by $M=R_{m-2}\oplus R_{m-1}f$, $M^*=R_{m-2}\oplus f^*R_{m-1}$, $M_1=R_{m-2}\oplus Rf$, and $M_1^*=R_{m-2}\oplus f^*R$. We begin with the following

LEMMA 1.1. (1) $X^iY_j\equiv\delta_{ij}X^{m-1} \pmod{M_1}$ $(0\leqq i, j\leqq m-1)$, *where* δ_{ij} *is Kronecker's delta.*

(2) $Y_j^*X^i\equiv\delta_{ij}X^{m-1} \pmod{M_1^*}$ $(0\leqq i, j\leqq m-1)$. (Cf. [**9**; Remark 1.1].)

PROOF. (1) $X^iY_i=X^i(X^{m-i-1}+X^{m-i-2}a_{m-1}+\cdots+a_{i+1})=X^{m-1}+X^{m-2}a_{m-1}+\cdots+X^ia_{i+1}\equiv X^{m-1} \pmod{M_1}$. If $j<i$ then it is evident that $X^jY_i\equiv 0 \pmod{M_1}$. If

$m-1\geqq j\geqq i+1$ then $X^jY_i=X^{j-i-1}X^{i+1}Y_i=X^{j-i-1}(X^m+X^{m-1}a_{m-1}+\cdots+X^{i+1}a_{i+1})\equiv X^{j-i-1}(-X^ia_i-\cdots-a_0)\equiv 0 \pmod{M_1}$. Similarly we can prove (2).

LEMMA 1.2. $Y_j^*f\equiv f^*Y_j \pmod{R_{m-2}}$ $(j=0, \cdots, m-1)$.

PROOF. $Y_j^*f\equiv Y_j^*(X^m+X^{m-1}a_{m-1}+\cdots+X^ja_j)\equiv Y_j^*X^{j+1}(X^{m-j-1}+X^{m-j-2}a_{m-1}+\cdots+a_{j+1})+X^{m-1}a_j\equiv Y_j^*X^{j+1}Y_j+X^{m-1}a_j \pmod{R_{m-2}}$. Similarly we have $f^*Y_j\equiv Y_j^*X^{j+1}Y_j+a_j^*X^{m-1} \pmod{R_{m-2}}$. But, by definition, $a_j^*X^{m-1}\equiv X^{m-1}a_j \pmod{R_{m-2}}$. Hence $Y_j^*f\equiv f^*Y_j \pmod{R_{m-2}}$ $(j=0, 1, \cdots, m-1)$.

Now, assume that $Kf=fK$ (monic K-bisubmodule). Note that $R_{m-1}=Y_{m-1}K\oplus Y_{m-2}K\oplus\cdots\oplus Y_0K=Y_{m-1}^*K\oplus Y_{m-2}^*K\oplus\cdots\oplus Y_0^*K$. By definition, $M=R_{m-2}\oplus R_{m-1}f$. On the other hand $M^*=R_{m-2}\oplus f^*R_{m-1}=R_{m-2}+f^*Y_{m-1}K+\cdots+f^*Y_0K=R_{m-2}+Y_{m-1}^*fK+\cdots+Y_0^*fK$, by virtue of Lemma 1.2. But, since $fK=Kf$, we have $M^*=R_{m-2}+Y_{m-1}^*Kf+\cdots+Y_0^*Kf=R_{m-2}+R_{m-1}f=M$. Hence $M=M^*$ (if $fK=Kf$). Then, as $R=R_{m-1}+Rf$, we have $f^*R=f^*(R_{m-1}+Rf)\subseteqq R_{m-2}+Rf=M_1$, and so $M_1^*\subseteqq M_1$. Symmetrically $M_1\subseteqq M_1^*$. Thus $M_1=M_1^*$.

Next we shall prove that if $yR_{m-1}\subseteqq M$ $(y\in R_{m-1})$ then $y=0$. Since $y\in R_{m-1}\cap M=R_{m-2}$, we have $yR_1\subseteqq R_{m-1}\cap M=R_{m-2}$. Hence $y\in R_{m-3}$. Then $yR_2\subseteqq R_{m-1}\cap M=R_{m-2}$, $\cdots$. Eventually $y\in K$, and so $yR_{m-1}\subseteqq R_{m-1}\cap M=R_{m-2}$, and hence $y=0$, as desired. Now, $Kf^*KR_{m-1}\subseteqq M$, because $M=M^*$ is a K-bisubmodule. Hence $Kf^*K\cap R_{m-1}=0$ by the preceding argument, and so $R_{m-1}\oplus Kf^*K=R_m$. Therefore $Kf^*K=f^*K=Kf^*$. Lastly, let $z\in R$ and $zR_{m-1}\subseteqq M_1$ $(=M_1^*)$. Let $z\equiv z_0 \pmod{f^*R}$, where $z_0\in R_{m-1}$. Then $z_0R_{m-1}\subseteqq R_{2m-1}\cap M_1\subseteqq R_{m-2}+R_{m-1}f=M$. Hence $z_0=0$. Thus $z\in f^*R$. Further, assume that $z\in R_m$. Then $z\in f^*R\cap R_m=f^*K$. Hence $f^*R=\{z\in R\mid zR\subseteqq M_1\}=\{z\in R\mid zR_{m-1}\subseteqq M_1\}$, and $f^*K=\{z\in R_m\mid zR_{m-1}\subseteqq M\}$. Similarly $Rf=\{z\in R\mid Rz\subseteqq M_1\}=\{z\in R\mid R_{m-1}z\subseteqq M_1\}$, and $Kf=\{z\in R_m\mid R_{m-1}z\subseteqq M\}$. Thus we obtain the following

THEOREM 1.3. *Let $f=X^m+X^{m-1}a_{m-1}+\cdots+a_0$ $(m\geqq 1)$, and assume that $Kf=fK$. Then there exists a monic polynomial f^* of degree m such that $R_{m-2}\oplus f^*R_{m-1}=R_{m-2}\oplus R_{m-1}f$ $(=M)$. Such a f^* is uniquely determined by f. In fact, $f^*=X^m+a_{m-1}^*X^{m-1}+\cdots+a_0^*$, where $a_i^*X^{m-1}\equiv X^{m-1}a_i \pmod{R_{m-2}}$ $(i=0, \cdots, m-1)$ (i.e. $\rho^{m-1}(a_i^*)=a_i$), and there holds $Kf^*=f^*K$.*

The latter half of the above is a concrete description of $(fK)^*$ for a monic K-bisubmodule fK in the case that $R_1/K_K\cong K_K$ (cf. [8; Theorem 12]).

In what follows, we assume $fK=Kf$. Let F be the bilinear map from $(R/f^*R)\times(R/Rf)$ to R/M_1 defined by $F(y+f^*R, z+Rf)=yz+M_1$ $(y, z\in R)$, where $M_1=R_{m-2}\oplus Rf=R_{m-2}\oplus f^*R$. Then $F(a(y+f^*R), r(z+Rf)b)=aF((y+f^*R)r, z+Rf)b$ $(a, b\in K, y, z, r\in R)$. In this sense we say that F is a (K, R, K)-bilinear map. Since $R=R_{m-1}\oplus Rf$, we have $R/M_1\cong R_{m-1}/R_{m-2}=K(X^{m-1}+R_{m-2})=(X^{m-1}+R_{m-2})K$. X^i+f^*R $(i=0, 1, \cdots, m-1)$ is a basis for ${}_KR/f^*R$, and Y_j+Rf $(j=0, 1, \cdots, m-1)$ is a basis for R/Rf_K, and then Lemma 1.1 implies that F is a non-singular (K, R, K)-bilinear map, that is, ${}_KR/f^*R_R\cong {}_K\mathrm{Hom}(R/Rf_K, R/M_{1K})_R$

(the module of all right K-homomorphisms from R/Rf to R/M_1) and ${}_RR/Rf_K \cong {}_R\mathrm{Hom}({}_KR/f^*R, {}_KR/M_1)_K$ under the maps induced by F. These facts are proved in [8], in more general form.

Let π be the right K-isomorphism from R/M_1 to K such that $\pi(X^{m-1}a+M_1)=a$ $(a\in K)$. Let π^* be the left K-isomorphism from R/M_1 to K such that $\pi^*(aX^{m-1}+M_1)=a$ $(a\in K)$. Then, for any $a\in K$, $aX^{m-1}+M_1=X^{m-1}\rho^{m-1}(a)+M_1$, and so $\pi(aX^{m-1}+M_1)=\pi(X^{m-1}\rho^{m-1}(a)+M_1)=\rho^{m-1}(a)=\rho^{m-1}\pi^*(aX^{m-1}+M_1)$.

PROPOSITION 1.4. *For any y in R there hold $y\equiv\sum_j \pi^*(yY_j+M_1)X^j\equiv\sum_j \pi^*(yX^j+M_1)Y_j^*$ (mod f^*R) and $y\equiv\sum_j Y_j\pi(X^jy+M_1)\equiv\sum_j X^j\pi(Y_j^*y+M_1)$ (mod Rf), where $j=0, 1, \cdots, m-1$.*

PROOF. Let $y\equiv\sum_{i=0,\cdots,m-1} d_i'X^i$ (mod f^*R). Then, $yY_j+M_1=\sum_i d_i'X^iY_j+M_1=d_j'X^{m-1}+M_1$, by Lemma 1.1. Hence $\pi^*(yY_j+M_1)=d_j'$ $(j=0, \cdots, m-1)$. Thus $y\equiv\sum_j \pi^*(yY_j+M_1)X^j$ (mod f^*R). Next, let $y\equiv\sum_{i=0,\cdots,m-1} Y_id_i''$ (mod Rf). Then, $X^jy+M_1=\sum_i X^jY_id_i''+M_1=X^{m-1}d_i''+M_1$, by Lemma 1.1. Hence $y\equiv\sum_j Y_j\pi(X^jy+M_1)$ (mod Rf). The remainder is similarly proved.

PROPOSITION 1.5. *Let f be a monic polynomial of degree m $(\geqq 1)$ such that $Kf=fK$, and let f^* be the monic polynomial as in Theorm* 1.3. *Then $\{y\in R\mid yR\subseteqq Rf\}=\{y\in R\mid Ry\subseteqq f^*R\}$, that is, the bound of ${}_RR/Rf$ is equal to the bound of R/f^*R_R.*

PROOF. For y in R, $(R/f^*R)y=0$ and $\mathrm{Hom}(R/Rf_K, R/M_{1K})y=0$ are equivalent since ${}_KR/f^*R_R \cong {}_K\mathrm{Hom}(R/Rf_K, R/M_{1K})_R$. But, the latter is equivalent to $y(R/Rf)=0$, by Proposition 1.4.

In the sequel we denote the bound of ${}_RR/Rf$ by I. If $fR=Rf$ then $I=fR=Rf$, and $f=f^*$.

REMARK. Since $R=R_{m-1}\oplus Rf$, $I=\{y\in R\mid yR_{m-1}\subseteqq Rf\}$.

Let ${}_TV$, ${}_TW$ be left T-modules over a ring T. If ${}_TV$ is isomorphic to a direct summand of ${}_TW^n$ (direct sum of n copies of ${}_TW$) for some n, then we write ${}_TV|{}_TW$. Then it is easily seen that ${}_TV|{}_TW$ if and only if there are $\sigma_1, \cdots, \sigma_n$ in $\mathrm{Hom}({}_TV, {}_TW)$ and $\tau_1, \cdots, \tau_n$ in $\mathrm{Hom}({}_TW, {}_TV)$ such that $\sum_i \tau_i\sigma_i(v)=v$ for all $v\in V$. Let $\sigma: U\to T$ be a ring homomorphism. Then, by σ, T is considered as a U-bimodule, and we obtain a T-bimodule ${}_TT\otimes_UT_T$. If ${}_TT_T|{}_TT\otimes_UT_T$ then σ (abbre. T/U) is said to be a separable extension. As is well known, this is equivalent to that the canonical map $T\otimes_UT\to T$, $t\otimes t'\mapsto tt'$ splits as a T-T-homomorphism, or equivalently, there is an element $\sum t_i\otimes t_i'$ in $T\otimes_UT$ such that $\sum_i t_it_i'=1$ and $\sum_i tt_i\otimes t_i'=\sum_i t_i\otimes t_i't$ for all $t\in T$. If ${}_TT\otimes_UT_T|{}_TT_T$, σ is called an H-separable extension. It is known that an H-separable extension is a separable extension (K. Hirata).

LEMMA 1.6. *Any R-R-homomorphism ν: ${}_R(R/I)\otimes_K(R/f^*R)_R\to {}_RR/I_R$ is written as $\nu((y+I)\otimes(z+f^*R))=yrz+I$ $(y, z\in R)$ with an element r of R such that $rf^*\in I$ and $ra\equiv ar$ (mod I) for all $a\in K$.*

PROOF. This is evident from the sequence of isomorphisms $\mathrm{Hom}({}_R(R/I)\otimes_K(R/f^*R)_R, {}_RR/I_R)\cong \mathrm{Hom}({}_KR/f^*R_R, {}_K\mathrm{Hom}({}_RR/I, {}_RR/I)_R)\cong \mathrm{Hom}({}_KR/f^*R_R, {}_KR/I_R)$.

LEMMA 1.7. *Any R-R-homomorphism $\mu: {}_RR/I_R\to {}_R(R/I)\otimes_K(R/f^*R)_R$ is written as $\mu(y+I)=\sum_{j=0,\cdots,m-1}(yY_jr+I)\otimes(X^j+f^*R)$ $(y\in R)$ with an element r of R such that $fr\in I$ and $\rho^{m-1}(a)r\equiv ra \pmod I$ for all $a\in K$.*

PROOF. Put $u=X^{m-1}+M_1\in R/M_1$. Then $R/M_1=uK$, and $ua=0$ $(a\in K)$ implies $a=0$. And, $bu=u\rho^{m-1}(b)$ for all $b\in K$. The bilinear map F induces an isomorphism ${}_KR/f^*R_R\cong {}_K\mathrm{Hom}(R/Rf_K, uK_K)_R$, and so ${}_R(R/I)\otimes_K(R/f^*R)_R\cong {}_R(R/I)\otimes_K\mathrm{Hom}(R/Rf_K, uK_K)_R$. Since R/Rf_K is finitely generated and projective, ${}_R(R/I)\otimes_K\mathrm{Hom}(R/Rf_K, uK_K)_R\cong {}_R\mathrm{Hom}(R/Rf_K, (R/I)\otimes_K uK_K)_R$, $(y+I)\otimes\gamma\mapsto(z+Rf\to(y+I)\otimes\gamma(z+Rf))$. Therefore $(\sharp)$: $\mathrm{Hom}({}_RR/I_R, {}_R(R/I)\otimes_K(R/f^*R)_R)\cong \mathrm{Hom}({}_RR/I_R, {}_R\mathrm{Hom}(R/Rf_K, (R/I)\otimes_K uK_K)_R)\overset{\alpha}{\cong}\mathrm{Hom}({}_RR/Rf_K, {}_R(R/I)\otimes_K uK_K)$, where $\alpha(*)=*(1+I)$. Let r be an element of R such that $fr\in I$. Then the mapping $(z+Rf\to(zr+I)\otimes u)$ is in $\mathrm{Hom}({}_RR/Rf_K, {}_R(R/I)\otimes_K uK_K)$ if and only if $\rho^{m-1}(a)r\equiv ra \pmod I$ for all $a\in K$. Then $(zr+I)\otimes u=(\sum_j Y_j\pi(X^jz+M_1)r+I)\otimes u=(\sum_j Y_jr\pi^*(X^jz+M_1)+I)\otimes u=\sum_j(Y_jr+I)\otimes(X^{m-1}\pi(X^jz+M_1)+M_1)=\sum_j(Y_jr+I)\otimes(\sum_i X^jY_i\pi(X^iz+M_1)+M_1)$ (Lemma 1.1) $=\sum_j(Y_jr+I)\otimes(X^jz+M_1)$ (Proposition 1.4). Finally, under the above sequence $(\sharp)$ of isomorphisms, $(y+I\to\sum_j(yY_jr+I)\otimes(X^j+f^*R))$ corresponds to $(z+Rf\to\sum_j(Y_jr+I)\otimes(X^jz+M_1)=(zr+I)\otimes u)$. This proves the lemma.

By Lemma 1.7 (and Lemma 1.6), we obtain the following

THEOREM 1.8. *Assume that $Rf=fR=I$. Then R/I is separable over K if and only if there is an element y in R such that $\sum_{j=0,\cdots,m-1}Y_jyX^j\equiv 1 \pmod I$ and $\rho^{m-1}(a)y\equiv ya \pmod I$ for all $a\in K$.*

REMARK. It is easily seen that $\sum_j X^jrY_j^*\equiv\sum_j Y_jrX^j \pmod I$, if $\rho^{m-1}(a)r\equiv ra \pmod I$ for all $a\in K$.

Note that if $\rho=id$ and $D=0$ then $\sum_{j=0,\cdots,m-1}X^jY_j$ is the derivative of f.

THEOREM 1.9. *Assume that $Rf=fR=I$. Then R/I is H-separable over K if and only if there are y_i, z_i $(i=1,\cdots,s)$ in R_{m-1} such that $ay_i=y_ia$, $\rho^{m-1}(a)z_i=z_ia$ for all $a\in K$ and $\sum_i y_iyz_i\equiv\pi^*(y+M_1) \pmod I$ for all $y\in R$.* (Cf. [**5**; Proposition 2.4].)

PROOF. By Lemmas 1.6 and 1.7, R/I is H-separable over K if and only if there are y_i, z_i $(i=1,\cdots,s)$ in R_{m-1} such that $ay_i=y_ia$, $\rho^{m-1}(a)z_i=z_ia$ for all $a\in K$, and $\sum_{i,j}(y_iyY_jz_i+I)\otimes(X^j+I)=(1+I)\otimes(y+I)$ for all $y\in R$. But $(1+I)\otimes(y+I)=\sum_j(1+I)\otimes(\pi^*(yY_j+M_1)X^j+I)=\sum_j(\pi^*(yY_j+M_1)+I)\otimes(X^j+I)$. Therefore the last condition is equivalent to that $\sum_i y_iyY_jz_i\equiv\pi^*(yY_j+M_1) \pmod I$ $(j=0,\cdots,m-1)$ for all $y\in R$. Since $\sum_j RY_j=RR_{m-1}=R$, this is equivalent to that $\sum_i y_iyz_i\equiv\pi^*(y+M_1) \pmod I$ for all $y\in R$. This completes the proof.

Let f be a monic polynomial such that $Rf=fR$. If R/Rf is separable over

K, f is called a separable polynomial.

THEOREM 1.10. *Let f, g be monic polynomials such that $Rf=fR$, $Rg=gR$, $\deg f=m$ ($\geqq 1$), and $\deg g=n$ ($\geqq 1$). Then the following are equivalent.*

(i) *fg is a separable polynomial.*

(ii) *f and g are separable polynomials, and $Rf+Rg=R$.*

To prove this we need two lemmas.

LEMMA 1.11. *Let f, g be monic polynomials such that $Rf=fR$ and $Rg=gR$. If $Rf+Rg=R$ then $fg=gf$.*

PROOF. There is a monic polynomial f_1 such that $fg=gf_1$, because $fg\in Rg=gR$. Then $Rf_1=(Rf+Rg)f_1=Rff_1+Rgf_1=Rff_1+Rfg\subseteq Rf$. Therefore $Rf_1\subseteq Rf$. But $\deg f=\deg f_1$. Hence $f_1=f$. Thus $fg=gf$.

LEMMA 1.12. *Let T_1, T_2 be separable extensions over K. Then $T=T_1\oplus T_2$ (direct sum of rings) is a separable extension over K, too.*

PROOF. There is an element $\sum_i t_{1i}\otimes t_{1i}^*$ in $T_1\otimes_K T_1$ such that $\sum_i t_{1i}t_{1i}^*=1$ and $\sum_i t_1t_{1i}\otimes t_{1i}^*=\sum_i t_{1i}\otimes t_{1i}^*t_1$ ($\in T_1\otimes_K T_1$) for all $t_1\in T_1$. Similarly there is an element $\sum_j t_{2j}\otimes t_{2j}^*$ in $T_2\otimes_K T_2$ such that $\sum_j t_{2j}t_{2j}^*=1$ and $\sum_j t_2t_{2j}\otimes t_{2j}^*=\sum_j t_{2j}\otimes t_{2j}^*t_2$ ($\in T_2\otimes_K T_2$) for all $t_2\in T_2$. Put $v=\sum_i(t_{1i}, 0)\otimes(t_{1i}^*, 0)+\sum_j(0, t_{2j})\otimes(0, t_{2j}^*)$ ($\in T\otimes_K T_T$). Then $tv=vt$ ($\in {}_TT\otimes_K T_T$) for all $t\in T$. Further, under the mapping $T\otimes_K T\to T$, $t\otimes t'\mapsto tt'$, v corresponds to $(\sum_i t_{1i}t_{1i}^*, \sum_j t_{2j}t_{2j}^*)=(1_{T_1}, 1_{T_2})$. Hence T is a separable extension over K.

PROOF OF THEOREM 1.10. (i) $\Rightarrow$ (ii). For any $y=\sum_i X^id_i$ we put $\beta(y)=\sum_{i\geq 1}X^{i-1}d_i$. Then β is a right K-homomorphism. Note that $\beta^i(f)=Y_{i-1}$ ($i=1, \cdots, m$). Let us calculate $\beta^i(fg)$ ($i=1, 2, \cdots$). We put $f=\sum_{i\geq 0}X^ia_i$, where $a_m=1$ and $a_i=0$ for all $i>m$. $\beta(fg)=\beta(\sum_{i\geq 0}X^ia_ig)=\sum_{i\geq 1}X^{i-1}a_ig+\beta(a_0g)=\beta(f)g+\beta(g)\rho^n(a_0)$, because $a_0g=g\rho^n(a_0)$. Then $\beta^2(fg)=\beta^2(f)g+\beta(g)\rho^n(a_1)+\beta^2(g)\rho^n(a_0)$. Inductively we can prove that $\beta^i(fg)=\beta^i(f)g+\beta(g)\rho^n(a_{i-1})+\beta^2(g)\rho^n(a_{i-2})+\cdots+\beta^i(g)\rho^n(a_0)$. Let y be any element of R such that $ya=\rho^{m+n-1}(a)y$ for all $a\in K$. Then $\sum_{i=1,\cdots,m+n}\beta^i(fg)yX^{i-1}=\sum_{i=1,\cdots,m+n}\beta^i(f)gyX^{i-1}+\sum_{i=1,\cdots,m+n}\sum_{j=1,\cdots,i}\beta^j(g)\rho^n(a_{i-j})yX^{i-1}=\sum_{i=1,\cdots,m+n}\beta^i(f)gyX^{i-1}+\sum_{j=1,\cdots,m+n}\beta^j(g)(\sum_{i=j,\cdots,m+n}y\rho^{1-m}(a_{i-j})X^{i-j})X^{j-1}=\sum_{i=1,\cdots,m}\beta^i(f)gyX^{i-1}+\sum_{j=1,\cdots,n}\beta^j(g)yf^*X^{j-1}$, because $\beta^i(f)=0$ ($i>m$) and $\beta^j(g)=0$ ($j>n$). Further, for any $a\in K$, $\rho^{m-1}(a)gy\equiv g\rho^{m+n-1}(a)y\equiv gya$ (mod Rf) and $\rho^{n-1}(a)yf\equiv y\rho^{-m}(a)f\equiv yfa$ (mod Rg), where $f=f^*$, Now, assume that $\sum_i\beta^i(fg)yX^{i-1}\equiv 1$ (mod Rfg). Then $\sum_i\beta^i(f)gyX^{i-1}\equiv 1$ (mod $Rf(=Rf^*)$), and $\rho^{m-1}(a)gy\equiv gya$ (mod Rf) for all $a\in K$. Hence f is separable. Similarly we can prove that g is separable. Further, since $Rf+Rg\ni 1$, we have $Rf+Rg=R$. (ii) $\Rightarrow$ (i). By Lemma 1.11, we know that $fg=gf$, so that $Rf\cap Rg=Rfg=Rgf$. Then $R/(Rf\cap Rg)\simeq(R/Rf)\oplus(R/Rg)$ canonically, by Chinese remainder theorem. Hence, by Lemma 1.12, R/Rfg is a separable extension of K.

When $Rf=fR=I$, we know that $R/I\simeq\mathrm{Hom}(R/I_K, R/M_{1K})$ as K-R/I-bimodules. Then, noting that ${}_KR/M_{1K}$ ($\simeq {}_Kgr_{m-1}R_K$) is invertible, we obtain

$(gr_{m-1}R)^{-1}\otimes_K(R/I)\cong \mathrm{Hom}(R/I_K, K_K)$ as K-R/I-bimodules. Therefore R/I is Frobenius over K (i.e. $R/I\cong \mathrm{Hom}(R/I_K, K_K)$ as K-R/I-bimodules) if and only if $(gr_{m-1}R)^{-1}\otimes_K(R/I)\cong R/I$ as K-R/I-bimodules. But, as is well known, the latter is equivalent to that ρ^{m-1} can be extended to an inner automorphism of R/I. Thus we have the following

PROPOSITION 1.13. *Assume that $Rf=fR=I$. Then R/I is Frobenius over K if and only if there is an element r in R such that $r+I$ is invertible in R/I and $\rho^{m-1}(a)r\equiv ra \pmod I$ for all $a\in K$.*

From the preceding argument, if R/I is Frobenius over K, then $gr_{m-1}R\otimes_K R_{m-1}\cong R_{m-1}$ as K-bimodules, because $R/I\cong R_{m-1}$ as K-bimodules. In particular, if $D=0$ then $gr_{m-1}R\oplus\cdots\oplus gr_{2(m-1)}R\to gr_0R\oplus\cdots\oplus gr_{m-1}R$ as K-bimodules. For instance, let K be a field, $D=0$, and ρ an automorphism of K with order $\rho\geqq m$ $(\geqq 2)$. Then R/I is not a Frobenius extension over K, because each ${}_Kgr_iR_K$ is simple, and $gr_{2(m-1)}R$ is not isomorphic to gr_jR for all $j=0,\cdots, m-1$, as K-bimodules.

The following is a special case.

COROLLARY. *Assume that $fR=Rf=I$, and that ${}_RR/I_K$ is a simple module. Then if R/I is separable over K then R/I is Frobenius over K.*

PROOF. By Theorem 1.8, there is an element r in R such that $\rho^{m-1}(a)r\equiv ra \pmod I$ for all $a\in K$, and $\sum_j Y_jrX^j\equiv 1 \pmod I$. Then, since $(Rr+I)/I$ is a non zero R-K-submodule of R/I, we have $(Rr+I)/I=R/I$, and hence $\eta: R/I\to R/I$, $x+I\mapsto xr+I$ is a left R-epimorphism. And the kernel of this epimorphism is an R-K-submodule, and so $\mathrm{Ker}\ \eta=0$. Thus η is a left R-isomorphism. Hence $r+I$ is invertible. Therefore R/I is Frobenius over K, by Proposition 1.13.

Here we state a problem. Assume that f is a separable polynomial. Is the extension ring R/fR of K always Frobenius over K. Some arguments about this problem will be done in § 3.

We end this section with the following

LEMMA 1.14. *Let $y=X^r+X^{r-1}d_{r-1}+\cdots+d_0$ $(r\geqq 1)$. Then $Ry=yR$ if and only if $ay=y\rho^r(a)$ for all $a\in K$ and $Xy=y(X+d_{r-1}-\rho(d_{r-1}))$.*

PROOF. Since $R=R_{r-1}\oplus Ry=R_{r-1}\oplus yR$, $Ry\subseteqq yR$ implies that $Ry=yR$. Thus the "if" part is evident. Assume $Ry=yR$. Then $Ky=yK$. Therefore, for any $a\in K$, there exists an element a' in K such that $ay=ya'$, and then we have $a'=\rho^r(a)$. Further there is an element d in K such that $Xy=y(X+d)$. Then, comparing the coefficients of X^r, we have $d=d_{r-1}-\rho(d_{r-1})$.

§ 2. Free quadratic extensions.

Let $A\supseteqq K$ be rings. If A/K is an invertible K-bimodule, we call A a quadratic extension of K. In particular, if $A/K_K\cong K_K$ (or equivalently, ${}_KA/K\cong {}_KK$), A is

called a free quadratic extension of K. Assume that $A \simeq R_1$ as K-bimodule. Then A has the form $K[X; \rho, D]/J$, where g is a monic polynomial of degree 2 such that $Rg=gR=J$.

By Lemma 1.14, we can easily see the following

LEMMA 2.1. *Let $g=X^2-Xa-b$ be a monic polynomial of $K[X; \rho, D]$. Then the following conditions are equivalent.*

(i) $Rg=gR$.

(ii) (α) *For any c of K, $a\rho^2(c)+D\rho(c)+\rho D(c)=\rho(c)a$, and $b\rho^2(c)+D^2(c)-D(c)a=cb$,* ($\beta$) $b-\rho(b)=D(a)-a(a-\rho(a))$, *and* $D(b)=b(a-\rho(a))$.

In the sequel of this section, we assume that $g=X^2-Xa-b$ and $Rg=gR=J$, and put $X+J=x$. Then $x^2=xa+b$, and $cx=x\rho(c)+D(c)$ for all $c\in K$. In case $\rho=id_K$, we have $x^2a+xb=x^3=(xa+b)x=x^2a+x(D(a)+b)+D(b)$ which implies $D(a)=D(b)=0$.

LEMMA 2.2. *The following conditions are equivalent.*

(i) *g is a separable polynomial.*

(ii) *There is an element y in R_1 such that $\rho(c)y=yc$ for all c in K, and $yX+(X-a)y\equiv 1 \pmod{J}$.*

(iii) *There are u, v in K such that $\rho^2(c)u=uc$, $v\rho^{-1}(c)=D(c)u+cv$ for all c in K, $a(u+\rho(u))+v+\rho(v)-\rho(a)u+D(u)=0$, and $b(u+\rho(u))-v\rho^{-1}(a)+D(v)=1$.*

PROOF. (i) $\Leftrightarrow$ (ii) follows from Theorem 1.8. Put $y=Xu+v$. Then we can easily see that (ii) $\Leftrightarrow$ (iii).

If R/J is G-Galois over K (cf. [4]) then $(G:e)=2$ by Nagahara [**10**; Lemma 1.2].

THEOREM 2.3. *The following conditions are equivalent.*

(i) *R/J is Galois over K.*

(ii) *There is an element s in K such that* (α) $4b+s^2-2D(s)$ (*or* $4b+s\rho(s)$) *is invertible in K (or, $2x-s$ is invertible in R/J),* (β) $s+\rho(s)=2a$, $s^2-D(s)=sa$, *and* $cs-s\rho(c)=2D(c)$ *for all $c\in K$.*

PROOF. (i) $\Rightarrow$ (ii). Let $G=\{1, \tau\}$ be a Galois group of a Galois extension R/J of K, where $\tau\neq id$, and $\tau^2=id$. Put $s=x+\tau(x)$. Then $s\in K$, and $\tau(x)=s-x$. Since $cx=x\rho(c)+D(c)$ for all $c\in K$, and $x^2=xa+b$, we have $c\tau(x)=\tau(x)\rho(c)+D(c)$ for all $c\in K$, and $\tau(x)^2=\tau(x)a+b$. Then the former implies that $cs-s\rho(c)=2D(c)$ for all $c\in K$, and the latter implies that $2a=s+\rho(s)$ and $s^2-D(s)=sa$. By [**10**; Lemma 1.2], $2x-s$ is invertible in R/J, or equivalently, $(2x-s)^2=4b+s\rho(s)=4b+s^2-2D(s)$ is invertible in K. (ii) $\Rightarrow$ (i). We put $Y=s-X$. By (β), $cY=Y\rho(c)+D(c)$ for all c in K, and so the mapping $\varphi: X\mapsto Y$ induces a K-automorphism of R. Then, by (β), we know $\varphi(g)=g$. Hence φ induces a K-automorphism τ of R/J such that $\tau(x)=s-x$. Let c_0+xc_1 be an element of R/J such that $\tau(c_0+xc_1)=c_0+xc_1$. Then, $sc_1=0$, and $2c_1=0$. Then $(4b+s^2-2D(s))c_1=0$. But $4b+s^2-2D(s)$ is invertible. Hence $c_1=0$. Finally, as in the proof of [**10**; Lemma 1.5],

$(s-2x)^{-1}(s-x)\tau(1)+(s-2x)^{-1}\tau(-x)=0$, and $(s-2x)^{-1}(s-x)\cdot 1+(s-2x)^{-1}(-x)=1$. Thus R/J is $\{1, \tau\}$-Galois over K. This proves the theorem.

REMARK. If $2\cdot 1$ is invertible in K, the condition $s^2-D(s)=sa$ follows from two conditions $s+\rho(s)=2a$ and $cs-s\rho(c)=2D(c)$ for all c in K.

From the proof of Theorem 2.3, if an element s of K satisfies (ii) (β) of Theorem 2.3, then $\tau: x\mapsto s-x$ induces a K-automorphism of R/J. Therefore we have the following

COROLLARY 1. *The following conditions are equivalent.*

(i) *The mapping $\tau: x\mapsto a-x$ induces a K-automorphism of R/J, and R/J is $\{1, \tau\}$-Galois over K.*

(ii) (α) *$4b+a^2$ is invertible in K,* (β) *$\rho(a)=a$, $D(a)=0$, and $ca-a\rho(c)=2D(c)$ for all $c\in K$.*

In the above, if we assume $\rho D=D\rho$, then the condition that $ca-a\rho(c)=2D(c)$ for all $c\in K$ is superfluous, by Lemma 2.1. Noting this fact we have

COROLLARY 2. *Assume that $\rho=id_K$, and that $2\cdot 1$ is invertible in K. Then R/J is Galois over K if and only if $4b+a^2$ is invertible in K. (Cf. Nagahara* [**10**; *Theorem* 3.4].)

Finally, let us improve a theorem which is found in Nagahara [**10**; Theorem 2.5 and Theorem 2.7].

THEOREM 2.4. *Assume that $D=0$. Then the following conditions are equivalent.*

(i) *R/J is Galois over K.*

(ii) *R/J is separable over K, and $2K+aK=K$.*

(iii) *R/J is separable over K, and $c\equiv\rho(c) \pmod{2K}$ for any c of the center of K.*

(iv) *$2x-a$ is invertible in R/J and $\rho(a)=a$.*

(v) *$4b+a^2$ is invertible in K, and $\rho(a)=a$.*

PROOF. Since $Rg=gR$, we know that $b-\rho(b)=-a(a-\rho(a))$, $b(a-\rho(a))=0$, and $ca=a\rho(c)$, $cb=b\rho^2(c)$ for all $c\in K$, by Lemma 2.1. Then $a(a-\rho(a))=a^2-a^2=0$, and so $b=\rho(b)$. Assume that g is separable. Then, by Lemma 2.2, there are u, v in K such that $\rho^2(c)u=uc$, $\rho(c)v=vc$ for all c in K, and $a(u+\rho(u))+v+\rho(v)-\rho(a)u=0$, $b(u+\rho(u))-av=1$. Then $1=\rho^{-2}(u)b+\rho^{-1}(u)b-\rho^{-1}(v)a$. Since $b(a-\rho(a))=0$ and $a(a-\rho(a))=0$, we know $1\cdot(a-\rho(a))=0$, that is, $a=\rho(a)$. Then, by Nagahara [**10**; Lemma 2.2], we have $4\cdot 1_K\in(4b+a^2)K$. Hence $(4b+a^2)K=4bK+a^2K=4K+a^2K$. Assume (i). Then, by [**4**; Proposition 1.3], R/J is separable over K, and so $\rho(a)=a$, $\rho(b)=b$. Then, by [**10**; Theorem 2.5], $4b+a^2$ is invertible in K. Hence $2K+aK=K$. Thus (i) $\Rightarrow$ (ii). Conversely, assume (ii). Then, $4K+a^2K=K$, and so $4b+a^2$ is invertible in K, by the preceding argument. Then, by [**10**; Theorem 2.5], R/J is Galois over K. Let c be in the center of K. Then $ca=a\rho(c)=\rho(c)a$, and so $c\equiv\rho(c) \pmod{2K}$, because $a+2K$ is invertible in $K/2K$.

Thus (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii). Finally we assume (iii). Then, since bu lies in the center of K, $bu\equiv\rho(bu)\equiv b\rho(u)$ (mod $2K$). Put $b\rho(u)=bu+2d$. Then $1=b(u+\rho(u))-av$ $=2bu+2d-av$. Thus $2K+aK=K$. Hence (iii) $\Rightarrow$ (ii). (i) $\Leftrightarrow$ (iv) $\Leftrightarrow$ (v) follow from [**10**; Theorem 2.5].

§ 3. Examples.

THEOREM 3.1. *Assume that $D=0$, and let $f=X^m-b$ ($m\geqq 2$) be in $R=K[X;\rho]$. Then the following conditions are equivalent:*

(i) *f is a separable polynomial.*

(ii) (α) *$\rho(b)=b$, and $cb=b\rho^m(c)$ for all $c\in K$,* (β) *b is invertible in K, and $d+\rho(d)+\cdots+\rho^{m-1}(d)=1$ for some d of the center of K.*

PROOF. (i) $\Rightarrow$ (ii). $Kf=fK$ implies that $cb=b\rho^m(c)$ for all $c\in K$. And, $Xf=fX$ (Lemma 1.14) yields $\rho(b)=b$. Let y be as in Theorem 1.8. Then, since $X^{m-1}y$ $+X^{m-2}yX+\cdots+yX^{m-1}=X^{m-1}(y+\rho(y)+\cdots+\rho^{m-1}(y))=(\rho^{-(m-1)}(y)+\rho^{-(m-2)}(y)+$ $\cdots+y)X^{m-1}$, $X+I$ is invertible in R/I, where $I=fR=Rf$. Then $X^m+I=b+I$ is invertible in R/I. Since ${}_KK$ and K_K are direct summands of ${}_KR/I$ and R/I_K respectively, it is easily seen that b is invertible in K. Then, by [**5**; Corollary to Theorem 2.11], $d+\rho(d)+\cdots+\rho^{m-1}(d)=1$ for some d of the center of K. (ii) $\Rightarrow$ (i). This follows also from [**5**; Corollary to Theorem 2.11].

Let B be a ring, and put $K=B\oplus B$. Let ρ be the transposition (i.e. $\rho(x_1, x_2)$ $=(x_2, x_1)$). Put $d=(1_B, 0)$. Then d lies in the center of K, and $d+\rho(d)=(1_B, 1_B)$ $=1$. Thus $f=X^2-1$ is separable in $K[X;\rho]$. Put $y=Xd$. Then y satisfies the condition in Theorem 1.8. But $y+I$ is not invertible.

THEOREM 3.2. *Let p be a prime number, and assume that $p1_K=0$ and $\rho=id_K$. Then, for $f=X^p-Xa-b\in R=K[X;D]$, the following conditions are equivalent.*

(i) *f is a separable polynomial.*

(ii) (α) *$D(a)=D(b)=0$, $D^p(c)-D(c)a=cb-bc$ for all $c\in K$, and a lies in the center of K,* (β) *there is an element y in R_{p-1} such that $D^{p-1}(y)-ya=1$ and $cy=yc$ for all c of K, where $D(h)=hX-Xh$ for any $h\in R$.*

To prove this we need the following

LEMMA 3.3. (1) *Let p be a prime number, and let $0\leqq j<p-1$. Then* $\sum_{i=0,\cdots,p-1-j}\binom{i+j}{i}\equiv 0$ (mod p). (2) *Assume that $p1_K=0$. Then, for any $y\in R=K[X;D]$, $X^{p-1}y+X^{p-2}yX+\cdots+yX^{p-1}=D^{p-1}(y)$.*

PROOF. (1) Let F_p be the prime field of characteristic p, and we take the polynomial ring $F_p[t]$. Then, in $F_p[t]$, $\sum_{i=0,\cdots,p-1-j}t(1+t)^{i+j}=t(1+t)^j\sum_{i=0,\cdots,p-1-j}$ $(1+t)^i=-(1+t)^j+1+t^p$. On the other hand, the coefficient of t^{j+1} in $\sum_{i=0,\cdots,p-1-j}$ $t(1+t)^{i+j}$ is $\sum_{i=0,\cdots,p-1-j}\binom{i+j}{i}1_K$. Thus $\sum_{i=0,\cdots,p-1-j}\binom{i+j}{i}\equiv 0$ (mod p). (2) For any $h=\sum_i X^ic_i$ in R, we put $D(h)=hX-Xh=\sum_i X^iD(c_i)$. Then, by induction, we can

see that $hX^r=\sum_{i=0,\cdots,r} X^i\binom{r}{i}D^{r-i}(h)$ for all $r\geqq 0$. Then, $\sum_{r=0,\cdots,p-1} X^{p-1-r}yX^r$ $=\sum_{r=0,\cdots,p-1}(\sum_{i=0,\cdots,r} X^{p-1-r+i}\binom{r}{i}D^{r-i}(y))=\sum_{j=0,\cdots,p-1}(\sum_{i=0,\cdots,p-1-j} X^{p-1-j}\binom{i+j}{i}$ $D^j(y))=D^{p-1}(y)$, as desired.

PROOF OF THEOREM 3.2. By Lemma 1.14, $fR=Rf$ if and only if $Xf=fX$ and $cf=fc$ for all c of K. On the other hand, $p1_K=0$ implies that $cX^p=X^pc+D^p(c)$ for all $c\in K$ (cf. the proof of Lemma 3.3). Therefore, as is easily seen, $fR=Rf$ if and only if (ii) (α) holds. Now, assume that f is separable. Let $y\in R_{p-1}$ be as in Theorem 1.8. Then, by Lemma 3.3, $X^{p-1}y+X^{p-2}yX+\cdots+yX^{p-1}$ $=D^{p-1}(y)$, and so $D^{p-1}(y)-ya=1$. Thus (i) $\Rightarrow$ (ii). Now it is evident that (ii) $\Rightarrow$ (i).

Here we state some particular cases of Theorem 3.2.

First, let $f=X^p-X-b$. Then $fR=Rf$ implies that f is separable, because we can take $1=y$ (cf. Kishimoto [2]).

When $D^{p-1}=0$, (β) is equivalent to that a is invertible in the center of K.

$f=X^p$ is separable if and only if $D^p=0$ and there exists y in R_{p-1} such that $D^{p-1}(y)=1$ and $cy=yc$ for all $c\in K$. For instance, let L be a field of characteristic $p\,(>0)$, and $K=L[t]$. Then X^p is separable in $K[X;D]$, where D is the usual derivation.

A monic polynomial f is called Frobenius, if $Rf=fR=I$ and R/I is Frobenius over K. For any ring A, we denote the Jacobson radical of A by $\mathrm{rad}(A)$.

THEOREM 3.4. *Let f be a separable polynomial of degree m ($\geqq 2$).*

(1) *If $D=0$ and $\mathrm{rad}(K)$ is a maximal ideal of K, then f is Frobenius.*

(2) *If ${}_KK_K$ is simple and there exists $y\in R_1$ as in Theorem 1.8, then f is Frobenius.*

PROOF. (1) Let y be as in Theorem 1.8. Put $\mathfrak{p}=\mathrm{rad}(K)$ and $y=\sum_{j=0,\cdots,m-1} X^jd_j$. Then, $\rho^{m-1}(c)d_0=d_0c$ for all $c\in K$. Therefore, if $d_0\notin\mathfrak{p}$ then d_0 is invertible in K, and hence f is Frobenius, by Proposition 1.13. On the other hand, if $d_0\in\mathfrak{p}$, then $X+I+\mathfrak{p}R$ is invertible in $R/(I+\mathfrak{p}R)$ (cf. Theorem 1.8 and its Remark), where $\mathfrak{p}R=R\mathfrak{p}$. Then, since ${}_KR/I$ and R/I_K are finitely generated, $X+I$ is invertible in R/I by Nakayama's Lemma. Therefore $X^{m-1}+I$ is invertible, and hence f is Frobenius, by Proposition 1.13. (2) Let y be as in Theorem 1.8, and put $y=Xu+v$. If $u=0$ then $(y=)$ v is invertible in K. Thus f is Frobenius, by Proposition 1.13. Assume $u\neq 0$. Then, for any $c\in K$, $\rho^m(c)u=uc$, and $\rho^{m-1}(c)v$ $+D\rho^{m-1}(c)u=vc$. The former implies that u is invertible, because ${}_KK_K$ is simple. Then the latter implies that $D(c)=vu^{-1}\rho(c)-cvu^{-1}$ for all c of K, that is, D is inner. Thus this case is reduced to the one when $D=0$ (cf. [1]). Then, (2) follows from (1).

COROLLARY. *Let f be a separable polynomial of degree 2, and assume that ${}_KK_K$ is simple. Then f is Frobenius.*

Let e be a central idempotent of K. Then $D(e)=D(e^2)=D(e)\rho(e)+eD(e)$. Therefore, if $\rho(e)=e$ then $D(e)\in eK$, and so $D(e)=0$. Then, for any a in K, $D(ae)=D(a)e$, and e lies in the center of R. Consequently, a monic polynomial f is separable (resp. Frobenius) if and only if ef and $(1-e)f$ are separable (resp. Frobenius) over eK and $(1-e)K$, respectively. Assume that K is a direct sum of (two sided) indecomposable ideals I_i $(i=1, \cdots, r)$, and let $1=\sum_{i=1,\cdots,r} e_i$ $(e_i\in I_i)$. Then ρ induces a permutation of $\{e_1, \cdots, e_r\}$, and hence it suffices to treat the case $\rho(e_1)=e_2, \cdots, \rho(e_{r-1})=e_r, \rho(e_r)=e_1$. Further, assume that $D=0$. Let f be a separable polynomial of degree 2, and let $y=Xu+v$ be as in Theorem 1.8. First we assume $r=2$. Then $\rho(c)v=vc$ for all $c\in K$, and so $\rho(e_1)v=ve_1=e_1v$. Hence $v=0$, because $e_1+\rho(e_1)=1$. Then the assumption for y yields that $X+I$ is invertible in R/I, where $I=fR=Rf$. Hence f is Frobenius, by Proposition 1.13. Next we eliminate the condition $r=2$. By Lemma 2.1, $ca=a\rho(c)$ and $cb=b\rho^2(c)$ for all $c\in K$. Further, by Lemma 2.2, $b(u+\rho(u))-av=1$. Hence $\rho^2(c)=c$ for all c in the center of K, and so $\rho^2(e_i)=e_i$ $(i=1, \cdots, r)$. Thus this case is reduced to the one when $r\leqq 2$. Then, by Theorem 3.4 (1), we have the following

THEOREM 3.5. *Let $D=0$, and f a separable polynomial of degree 2. Assume that K is a direct sum of rings I_i $(i=1, \cdots, r)$, and that each* rad(I_i) *is a maximal ideal of I_i. Then f is Frobenius.*

If K is a commutative artinean ring, then K is a direct sum of local rings. Thus we have the following

COROLLARY. *Let $D=0$, and f a separable polynomial of degree 2. If K is a commutative artinean ring, then f is Frobenius.*

References

[1] P.M. Cohn, Free rings and their relations, Academic Press, 1971.

[2] K. Kishimoto, On abelian extensions of rings I, Math. J. Okayama Univ., 14 (1970), 159-174.

[3] K. Kishimoto, On abelian extensions of rings II, Math. J. Okayama Univ., 15 (1971), 57-70.

[4] Y. Miyashita, Finite outer Galois theory of non commutative rings, J. Fac. Sci. Hokkaido Univ., Ser. I, 19 (1966), 114-134.

[5] Y. Miyashita, On Galois extensions and crossed products, J. Fac. Sci. Hokkaido Univ., Ser. I, 21 (1970), 97-121.

[6] Y. Miyashita, Commutative Frobenius algebras generated by a single element, J. Fac. Sci., Hokkaido Univ., Ser. I, 21 (1971), 166-176.

[7] Y. Miyashita, Note on an ideal of a positively filtered ring over a commutative ring, Math. J. Okayama Univ., 19 (1976), 61-63.

[8] Y. Miyashita, Non-singular bilinear maps which come from some positively filtered rings, J. Math. Soc. Japan, 30 (1978), 7-14.

[9] T. Nagahara, On separable polynomials over a commutative ring III, Math. J. Okayama Univ., 16 (1974), 189-197.

[10] T. Nagahara, On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ., 19 (1976), 65-95.

Yôichi MIYASHITA
Department of Mathematics
University of Tsukuba
Sakuramura, Ibaraki, 300-31
Japan