COMMUTATIVE FROBENIUS ALGEBRAS GENERATED BY A SINGLE ELEMENT

By

Yoichi MIYASHITA

§ 0. Introduction.

Let R be a commutative with 1 ($\neq 0$), and $f(X)$ a monic polynomial over R. Let deg $f=n>0$. Then it is easily seen that $R[X]/(f(X))$ is a free R-module of rank n. On the other hand in his paper [8], G. J. Janusz proved that every strongly separable R-algebra (i. e., separable R-algebra which is R-finitely generated and projective) generated by a single element is of the form $R[X]/(f(X))$, where R has no proper idempotents, and $f(X)$ is a monic polynonial over R. The purpose of this note is to investigate the above in more general situation. Let R be a commutative ring with 1 ($\neq 0$), and $R[X]$ the polynomial ring in one indeterminate. Let $f(X)$ be a non-zero element of $R[X]$. $f(X)$ is said to be a *monic* polynomial over R, if the leading coefficient of $f(X)$ is 1. We consider 1 as a monic polynomial. If $f(X)$ is a monic polynimial over R such that $f(X)\neq 1$, then we call $f(X)$ a *proper monic* polynomial over R. If there are pairwise orthogonal non-zero idempotents e_i ($i=1, \cdots, r$) of R such that $\sum_i e_i=1$ and such that each $e_i \cdot f(X)$ is a monic polynomial over e_iR (i. e., the leading coefficient of $e_i \cdot f(X)$ is e_i), then we call $f(X)$ a *quasi-monic* (abbre., *q-monic*) polynomial over R. If $f(X)$ is a q-monic polynomial such that $f(X)\neq 1$, then we call $f(X)$ a *proper q-monic* polynomial. Then the first result is the following: Let R be a commutative ring with 1 ($\neq 0$), $\{I\}$ the set of all proper ideals I of $R[X]$ such that $R[X]/I$ is finitely generated and projective as an R-module, and $\{f(X)\}$ the set of all proper q-monic polynomials $f(X)$ over R. Then $f(X)\mapsto(f(X))$ is one-to-one mapping from $\{f(X)\}$ to $\{I\}$. If $[R[X]/((f(X))+\mathfrak{p}\cdot R[X]) : R/\mathfrak{p}]$ is constant for every maximal ideal $\mathfrak{p}$ of R, then $f(X)$ is monic (and conversely). This generalizes Janusz [8; Th. 2.9].

Our second result is the following: Let R be as above, and $f(X)$ a proper q-monic polynomial over R. Then $R[X]/(f(X))$ is a projective Frobenius extension (in the sense of Kasch [9]).

In case R is a field, this is found in N. Jacobson's paper [7].

In §3, we prove the uniqueness of factorizations into absolutely indecomposable (monic) polynomials of a monic polynomial over a indecomposable commutative ring. By making use of the first result, the proof is done. §4 is an appendix of this paper. The result is analogous to the one of §3. In this section only, we treat not necessary commutative algebras.

Throughout this paper, all rings are commutative rings with 1, except appendix §4, and ring homomorphisms carry the units into units. All modules are unitary.

§1. Let R be a commutative ring with 1 ($\neq 0$), and $f(X)$ a polynomial over R. If the leading coefficient of $f(X)$ is 1, we call $f(X)$ a *monic* polynomial over R. We consider 1 as a monic polynomial of degree 0. If $f(X)$ is a monic polynomial with $f(X)\neq 1$, then we call $f(X)$ a *proper monic* polynomial.

If there are pairwise orthogonal non-zero idempotents e_i ($i=1, \cdots, r$) of R such that $1=\sum_i e_i$ and such that each $e_i \cdot f(X)$ is monic over e_iR (i.e., the leading coefficient of $e_i \cdot f(X)$ is e_i), then we say that $f(X)$ is *q-monic* over R, with respect to $1=\sum e_i$. In this case, we can chose e_i ($i=1, \cdots, r$) such that $\deg e_1 f(X) > \deg e_2 \cdot f(X) > \cdots > \deg e_r \cdot f(X)$. Then $\deg e_1 \cdot f(X)$ is equal to $\deg f(X)$. $f(X)$ is monic over R if and only if $r=1$. If $\deg e_r f(X)=0$ and $r=1$, then $f(X)=1$, and conversely. If $f(X)$ is a q-monic polynomial such that $f(X)\neq 1$, then we call $f(X)$ a *proper q-monic* polynomial.

Proposition 1.1. *Let R be a commutative ring with* 1 ($\neq 0$).

(1) *Let $f(X)=a_nX^n+\cdots+a_0$ ($a_n\neq 0$) be a q-monic polynomial over R. Then the family of pairwise orthogonal non-zero idempotents e_i of R such that $1=\sum_{i=1,\cdots,r} e_i$ and such that $\deg e_1 \cdot f(X) > \cdots > \deg e_r \cdot f(X)$ are uniquely determined by $f(X)$, and each e_i is contained in the ring $Z[a_0, \cdots, a_n]$ (which denotes the subring of R generated by $1, a_0, \cdots, a_n$), where Z means the ring of integers. Therefore $f(X)$ is q-monic over $Z[a_0, \cdots, a_n]$.*

(2) *Let $f(X)$, $g(X)$, and $h(X)$ be polynomials over R such that $g(X)h(X) = f(X)$, and assume that $g(X)$ is q-monic with respect to $1=\sum u_j$ over R. Then $f(X)$ is q-monic if and only if so is $h(X)$.*

(3) *Let both $g(X)$ and $f(X)$ be q-monic over R. Then $R[X]/(f(X))$ is finitely generated and projective over R. If $g(X)R[X]=f(X)R[X]$ then $g(X)=f(X)$.*

(4) *Let S be an overring of R, and $f(X)$ a q-monic polynomial over R. If $f(X)g(X)\in R[X]$ for some $g(X)$ in $S[X]$, then $g(X)\in R[X]$. Therefore $f(X)S[X]\cap R[X]=f(X)R[X]$.*

Proof. (1) Let v_j ($j=1, \cdots, s$) be another family of pairwise orthogonal non-zero idempotents of R such that $1=\sum v_j$ and such that $\deg v_1\cdot f(X)>\cdots>\deg v_s\cdot f(X)$. Then $\deg e_1\cdot f(X)=\deg f(X)=\deg v_1\cdot f(X)$, and hence we have $a_n=v_1=e_1$. Therefore $(1-e_1)f(X)=(1-v_1)f(X)$. Put $(1-e_1)f(X)=g(X)$. Then $g(X)$ is a q-monic polynomial over $(1-e_1)R$ with respect to $1-e_1=\sum_{i\neq 1}e_s$ and $1-e_1=\sum_{j\neq 1}v_j$. By induction, we can complete the proof of the first half of (1). Noting that $a_n=e_1$, the latter half is also proved by induction. (2) Concerning "monic", the statement is obvious. Assume that $f(X)$ is q-monic with respect to $1=\sum e_i$ over R. If $e_iu_j\neq 0$, then $e_iu_jf=e_iu_jg\cdot e_iu_jh$, and e_iu_jf is monic over e_iu_jR. Therefore h is q-monic with respect to $1=\sum_{e_iu_j\neq 0}e_iu_j$. Similarly the converse can be proved. (3) If $f(X)$ and $g(X)$ are monic the proof is easily done. Let $f(X)$ and $g(X)$ be q-monic with respect to $1=\sum_{i=1,\cdots,r}e_i$ and $1=\sum_{j=1,\cdots,s}u_j$, respectively. And let $\deg e_1\cdot f(X)>\cdots>\deg e_r\cdot f(X)$ and $\deg u_1\cdot g(X)>\cdots>\deg u_s\cdot g(X)$. Evidently $R[X]/(f(X))\simeq\oplus_i e_i\cdot R[X]/(e_i\cdot f(X))$, $h+(f)\mapsto(e_1h+(e_1f),\cdots,e_rh+(e_rf))$, as R-algebras. Since each $e_i\cdot R[X]/(e_i\cdot f(X))$ is finitely generated and projective over e_iR, $R[X]/(f(X))$ is finitely generated and projective over R. If $\mathfrak{p}$ is a prime ideal of R, exact one e_{i_0} of e_i $(i=1,\cdots,r)$ is not in $\mathfrak{p}$. Then the $\mathfrak{p}$-rank of $R[X]/(f(X))$ is $\deg e_{i_0}f(X)$. Because, as $e_ie_{i_0}=0$ provided $i\neq i_0$, $A_{\mathfrak{p}}=(e_{i_0}A)$, and $(e_i\cdot R[X]/(e_i\cdot f(X)))_{\mathfrak{p}}=0$ $(i\neq i_0)$. Therefore the decomposition $R=\sum_i\oplus e_iR$ is the one induced by the continuous mapping $\mathfrak{p}\mapsto\mathfrak{p}$-rank of $R[X]/(f(X))$, from spec (R) to Z (discrete). Therefore $r=s$, and $e_i=u_i$ $(i=1,\cdots,r)$ (cf. [4], [5]). Since $e_if\cdot e_iR[X]=e_ig\cdot e_iR[X]$ for all i, we have $e_if=e_ig$ for all i, because e_if and e_ig are monic over e_iR. Hence $f=\sum e_if=\sum e_ig=g$. (4) It will be easily seen that if $f(x)$ is monic then the assersion is true. Assume that $f(X)$ is q-monic with respect to $1=\sum e_i$. Then each $e_i\cdot f(X)$ is monic over e_iR, and $e_if\cdot e_ig\in e_iR[X]$, and so e_ig is in $e_iR[X]$ for every i. Hence $g=\sum e_ig\in R[X]$.

Let R be a commutative ring with 1 $(\neq 0)$, and let P be a finitely generated and projective R-module. Then there exist uniquely pairwise orthogonal non-zero idempotents e_i $(i=1,\cdots,r)$ of R such that $1=\sum e_i$ and non-negativ integers $n_1>\cdots>n_r$ such that each e_iP is of constant $\mathfrak{p}$-rank n_i for all $\mathfrak{p}$ in space (e_iR) (orequivalently, for all $\mathfrak{p}\in$ spec (R) such that $\mathfrak{p}\not\ni e_i$). (Cf. [4], [5]). If ${}_RP$ is faithful then $n_r>0$, and conversely. These facts was already used in the proof of Prof. 1.1.

Theorem 1.2. (*cf.* [8; *Th.* 2.9], [3; *Lemma* 3]). *Let R be a commutative ring with* 1 $(\neq 0)$, *and let I be an ideal of the polynomial ring $R[X]$ in one indetermenate such that $R[X]/I$ is a finitely generated R-module. Put $S=R[X]/I$, and assume that there are pairwise orthogonal non-zero idempotents e_i $(i=1,\cdots,r)$ of R such that $1=\sum e_i$ and non-negative integers*

$n_1 > \cdots > n_r$ *such that, for each* i, $[e_iS/\mathfrak{p}\cdot e_iS : e_iR/\mathfrak{p}] = n_i$ *for all maximal ideal* $\mathfrak{p}$ *of* e_iR. *Then there is a q-monic polynomial* $f(X)$ *with respect to* $1 = \sum e_i$ *in* I *such that* $I/(f) \subseteq rad\,(R)\,(R[X]/(f))$ *and* $deg\ e_if = n_i$ $(i = 1, \cdots, r)$, *where* $rad\,(R)$ *denotes the Jacobson radical of* R. *In particular, if* S *is R-projective then* $I = (f)$.

Proof. We may assume that $R[X] \neq I$. First we assume that $r = 1$. We put $n_1 = n$. Then $n > 0$. For any $\mathfrak{p} \in \max(R)$, we denote by $\varphi_{\mathfrak{p}}$ the canonical homomorphism from $(R/\mathfrak{p})[X]$ $(\simeq R[X]/\mathfrak{p}\cdot R[X])$ to $R[X]/(\mathfrak{p}\cdot R[X] + I)$ $(\simeq S/\mathfrak{p}S)$. Then, as $[S/\mathfrak{p}S : R/\mathfrak{p}] = n$, there is a proper monic polynomial $f_{\mathfrak{p}}(X)$ in $R[X]$ of degree n which generates Ker $\varphi_{\mathfrak{p}}$ modulo $\mathfrak{p}$. Then it is evident that $(f_{\mathfrak{p}}) + \mathfrak{p}\cdot R[X] = I + \mathfrak{p}\cdot R[X]$. Put $U = \{h(X) \in R[X] \mid \deg h \leqslant n-1\}$. Then $U + (f_{\mathfrak{p}}) = R[X]$, and so $R[X] = U + (f_{\mathfrak{p}}) + \mathfrak{p}\cdot R[X] = U + I + \mathfrak{p}\cdot R[X]$ for every $\mathfrak{p} \in \max(R)$. Therefore $\mathfrak{p}(R[X]/(U+I)) = R[X]/(U+I)$. Since $R[X]/(U+I)$ is finitely generated, the last means that $R[X]/(U+I) = 0$, that is, $R[X] = U + I$. Let $X^n = u + f$, where $u \in U$, $f \in I$. Then $X^n - u = f \in I$, and the canonical epimorphism φ: $R[X]/(f) \to R[X]/I$ is defined. Since this epimorphism is an isomorphism modulo $\mathfrak{p}$ for every maximal ideal $\mathfrak{p}$ of R, we know that Ker $\varphi = I/(f) \subseteq \mathfrak{p}(R[X]/(f))$ for every $\mathfrak{p}$ in $\max(R)$. However, as $R[X]/(f)$ is a free R-module, we have $I/(f) \subseteq \mathrm{rad}\,(R)(R[X]/(f))$. Next we proceed to general case. Evidently $R[X]/I \simeq \oplus_i\ (e_iR[X]/e_iI)$, $g + I \mapsto (e_1g + e_1I, \cdots, e_rg + e_rI)$, as R-algebras. Then, for each i, there is a monic polynomial $f_i(X)$ over e_iR (i.e., the leading coefficient of f_i is e_i) such that $e_iI \ni f_i$, $e_iI/(f_i) \subseteq \mathrm{rad}\,(e_iR)\,(e_iR[X]/(f_i))$, and $\deg f_i = n_i$. Put $f = \sum f_i$. Then $f \in I$, $e_if = f_i$, and $I/(f) \subseteq \mathrm{rad}\,(R)\,(R[X]/(f))$, because $\mathrm{rad}\,(R) \supseteq \mathrm{rad}\,(e_iR)$ $(i = 1, \cdots, r)$. If S is R-projective then $I/(f)$ is an R-direct summand of $R[X]/(f)$. On the other hand $I/(f)$ is small, because $I/(f) \subseteq \mathrm{rad}\,(R)\,(R[X]/(f))$. Hence $I = (f)$.

Prom Prop. 1.1 and Th. 1.2, the next theorem follows easily.

Theorem 1.3. *Let* R *be a commutative ring with* 1 $(\neq 0)$, *and* I *the set of all proper ideals* I *of* $R[X]$ *such that* $R[X]/I$ *is finitely generated and projective as an R-module, and let* $\{f(X)\}$ *be the set of all proper q-monic polynomials* $f(X)$ *over* R. *Then the mapping* $f(X) \mapsto (f(X))$ *is a* 1–1 *mapping from* $\{f(X)\}$ *to* $\{I\}$.

§2. Let σ be a ring homomorphism from R to S, where R, S are commutative rings. Then S can be considered as an R-module by σ. S/R is called a Frobenius extension, if S is finitely generated and projective as an R-module, and $S \simeq \mathrm{Hom}\,(S_R, R_R)$ as S-modules (cf. Kasch [9]). If S/R is Frobenius, then there are R-hompmorphism h: $S \to R$ and r_i, $l_i \in S$ $(i = 1, \cdots, n)$ such that $x = \sum_i h(xr_i)l_i = \sum_i r_i \cdot h(l_ix)$ for all x in S, and conversely (cf. [10;

Cor. 1]). h is called a Frobenius homomorphism. In this case, S/R is a separable extension if and only if $\sum r_i l_i$ is a unit of S (cf. [6; Prop. 2.18]). These will be used in the proof of the next theorem.

Theorem 2.1. *Let R be a commutrtive ring with $1\ (\neq 0)$, and $f(X)$ a proper monic polynomial over R. Put $S=R[X]/(f)$. Then S/R is a free Frobenius extension. S/R is separable if and only if $(f)+(f')=R[X]$, where f' is the derivative of f.*

Proof. Let $f(X)=X^n-a_{n-1}X^{n-1}-\cdots-a_0$ $(a_i\in R)$. If $n=1$ then $S=R$. Therefore we may assume that $n\geqslant 2$. Then, as is easily seen, $S=R\cdot 1\oplus Ru+\cdots\oplus Ru^{n-1}$ (direct sum), where $u=X+(f(X))$. Therefore any x in S is uniquely written as $x=b_0+b_1u+\cdots+b_{n-1}u^{n-1}(b_i\in R)$. By H_i $(i=0,\cdots,n-1)$ we denote the mapping $x\mapsto b_i$. These are evidently R-homomorphisms from S to R. We put $H_{n-1}=H$. In the sequel we shall show that H is a Frobenius homomorphism. Evidently $H(x)=b_{n-1}$, and $xu=b_0u+b_1u^2+\cdots+b_{n-2}u^{n-1}+b_{n-1}(a_0+a_1u+\cdots+a_{n-1}u^{n-1})=b_{n-1}a_0+(b_0+b_{n-1}a_1)u+(b_1+b_{n-1}a_2)u^2+\cdots+(b_{n-3}+b_{n-1}a_{n-2})u^{n-2}+(b_{n-2}+b_{n-1}a_{n-1})u^{n-1}$. Hence $H(xu)=H_{n-1}(xu)=H_{n-2}(x)+H(x)a_{n-1}$, $H_{n-2}(xu)=H_{n-3}(x)+H(x)a_{n-2}$, $H_{n-3}(xu)=H_{n-4}(x)+H(x)a_{n-3},\cdots,H_2(xu)=H_1(x)+H(x)a_2$, $H_1(xu)=H_0(x)+H(x)a_1$, $H_0(xu)=H(x)a_0$. If we substitute xu for x in $H(xu)=H_{n-2}(x)+H(x)a_{n-1}$, then we get $H(xu^2)=H_{n-2}(xu)+H(xu)a_{n-1}=H_{n-3}(x)+H(x)a_{n-2}+H(xu)a_{n-1}$. Therefore $H(xu^3)=H_{n-3}(xu)+H(xu)a_{n-2}+H(xu^2)a_{n-1}=H_{n-4}(x)+H(x)a_{n-3}+H(xu)a_{n-2}+H(xu^2)a_{n-1}$. $H(xu^4)=H_{n-4}(xu)+H(xu)a_{n-3}+H(xu^2)a_{n-2}+H(xu^3)a_{n-1}=H_{n-5}(x)+H(x)a_{n-4}+H(xu)a_{n-3}+H(xu^2)a_{n-2}+H(xu^3)a_{n-1},\cdots$, $H(xu^{n-2})=H_1(x)+H(x)a_2+H(xu)a_3+H(xu^2)a_4+\cdots+H(xu^{n-3})a_{n-1}$, $H(xu^{n-1})=H_0(x)+H(x)a_1+H(xu)a_2+\cdots+H(xu^{n-2})a_{n-1}$. Thus we have the following:

$$
\begin{aligned}
b_{n-1}&=H(x)\\
b_{n-2}&=H(x(u-a_{n-1}))\\
b_{n-3}&=H(x(u^2-a_{n-1}u-a_{n-2}))\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
b_2&=H(x(u^{n-3}-a_{n-1}u^{n-4}-\cdots-a_3))\\
b_1&=H(x(u^{n-2}-a_{n-1}u^{n-3}-\cdots\qquad-a_2))\\
b_0&=H(x(u^{n-1}-a_{n-1}u^{n-2}-\cdots\qquad\quad-a_1)).
\end{aligned}
$$

We put $v_{n-1}=1$, $v_{n-2}=u-a_{n-1}$, $v_{n-3}=u^2-a_{n-1}u-a_{n-2},\cdots,v_0=u^{n-1}-a_{n-1}u^{n-2}-\cdots-a_1$. Then $x=\sum b_iu^i=\sum_{i=0,\cdots,n-1}H(xv_i)u^i$. Finally we shall prove that $\sum_i H(xv_i)u^i=\sum_i v_i\cdot H(u^ix)$. Now, $\sum_{i=0,\cdots,n-1}v_i\cdot H(u^ix)=H(u^{n-1}x)+\sum_{i=0,\cdots,n-2}v_i\cdot H(u^ix)=H(u^{n-1}x)+\sum_{i=0,\cdots,n-2}(u^{n-i-1}-\sum_{k=1,\cdots,n-i-1}a_{n-k}u^{n-i-1-k})H(u^ix)=\sum_{i=0,\cdots,n-1}u^{n-i-1}H(u^ix)-\sum_{i=0,\cdots,n-2}\sum_{k=1,\cdots,n-i-1}a_{n-k}u^{n-i-1-k}H(u^ix)$. On the other hand, $(x=)\sum_{i=0,\cdots,n-1}H(xv_i)u^i=H(x)u^{n-1}+\sum_{i=0,\cdots,n-2}H(xv_i)u^i=H(x)u^{n-1}$

$+\sum_{i=0,\cdots,n-2}H(xu^{n-i-1}-\sum_{k=1,\cdots,n-i-1}a_{n-k}xu^{n-i-1-k})u^i=\sum_{i=0,\cdots,n-1}H(xu^{n-i-1})u^i$ $-\sum_{i=0,\cdots,n-2}\sum_{k=1,\cdots,n-i-1}a_{n-k}H(xu^{n-i-1-k})u^i$. To be easily seen, first terms of two exuations are equal. Therefore it suffices to prove that $\sum_{i=0,\cdots,n-2}$ $\sum_{k=1,\cdots,n-i-1}a_{n-k}u^{n-i-1-k}H(u^ix)=\sum_{i=0,\cdots,n-2}\sum_{k=1,\cdots,n-i-1}a_{n-k}H(xu^{n-i-1-k})u^i$. But this is done by comparing the coefficients of a_{n-j} $(j=1,\cdots,n-1)$. To do this, we fix any j such that $1\leqslant j\leqslant n-1$. Then, if $i=0,1,\cdots,n-j-1$ then k can take j. Hence the coefficient of a_{n-j} of the first equation is $u^{n-1-j}H(x)+u^{n-2-j}H(ux)+u^{n-3-j}H(u^2x)+\cdots+u^{n-(n-j-1)-1-j}H(u^{n-j-1}x)$. Similarly the coefficient of a_{n-j} of the second equation is $H(xu^{n-1-j})+H(xu^{n-2-j})u$ $+H(xu^{n-3-j})u^2+\cdots+H(xu^{n-(n-j-1)-1-j})u^{n-j-1}$. To be easily seen, the both coefficients of a_{n-j} are equal. Hence, by [10; Cor. 1], S/R is a free Frobenius extension. We put $f'(X)=nX^{n-1}-(n-1)a_{n-1}X^{n-2}-\cdots-a_1$. Then, by direct computation, we have $f'(u)=\sum_{i=0,\cdots,n-1}v_iu^i$. Therefore S/R is separable if and only if $f'(u)$ is a unit of S, or equivalently, $(f(X))+(f'(X))=R[X]$. This completes the proof.

Remark 1. Since $\{u^i\,|\,i=0,\cdots,n-1\}$ is a free basis, we have $H(u^iv_j)=\delta_{ij}$ (Kronecker's delta), because $u^i=\sum_{j=0,\cdots,n-1}H(u^iv_j)u^j$.

Remark 2. Since $f'(u)=\sum_{i=0,\cdots,n-1}v_iu^i$, the trace homomorphism tr of an R-module S is $(x\rightarrow H(f'(u)x))$ $(x\in S)$, that is $tr=H\cdot f'(u)$. Hence $tr=0$ if and only if $f'(u)=0$, or equivalently, $f'(X)=0$. Since $(1,u,\cdots,u^{n-1})$ is a basis of ${}_RS$, $f'(u)$ is invertible in S if and only if $(f'(u),f'(u)u,\cdots,f'(u)u^{n-1})$ is a basis of ${}_RS$. Because, if $(f'(u),\cdots,f'(u)u^{n-1})$ is a basis, 1 is written as a linear combination of $f'(u)$, $f'(u)u,\cdots,f'(u)u^{n-1}$. Since $f'(u)u^i=\sum_jH(f'(u)u^iv_j)u^j=\sum_jv_jH(u^jf'(u)u^i)$, $(f'(u),\cdots,f'(u)u^{n-1})$ is a basis if and only if $\det(tr(u^iu^j))$ (or $\det(tr(u^iv_j))$) is invertible in R. This fact is found in Janusz [8]. Since $u^i=\sum_jv_jH(u^ju^i)$ $(i=0,\cdots,n-1)$, $(H(u^iu^j))$ is invertible in $(R)_n$ (the ring of $n\times n$ matrices over R), and $H(f'(u)u^iu^j)=H(\sum_kH(f'(u)u^iv_k)u^ku^j)$ $=\sum_kH(f'(u)u^iv_k)H(u^ku^j)$. Thus, in general, $\det(H(f'(u)u^iu^j))$ differs from $\det(H(f'(u)u^iv_j))$ by an invertible element $\det(H(u^iu^j))$ of R.

Corollary. *Let R be a commutative ring with* $1\ (\neq 0)$, *and $f(X)$ a proper q-monic polynomial over R. Then $R[X]/(f)$ is a projective Frobenius extension. $R[X]/(f)$ is separable over R if and only if $(f)+(f')=R[X]$, where f' is the derivative of f.*

Proof. There are pairwise orthogonal non-zero idempotents e_i of R such that $1=\sum_{i=1,\cdots,r}e_i$, $\deg e_1f>\cdots>\deg e_rf$, and each e_if is monic over e_iR. Then $R[X]/(f)\simeq\oplus_{i=1,\cdots,r}e_iR[X]/(e_if)$, $g+(f)\mapsto(e_1g+(e_1f),\cdots,e_rg+(e_rf))$, as R-algebras, and each $e_iR[X]/(e_if)$ is Frobenius over e_iR. As is easily seen, the direct sum of a finite number of Frobenius extensions is

Frobenius, and hence $R[X]/(f)$ is Frobenius over $R=e_1R\oplus\cdots\oplus e_rR$. Evidently $(e_if)'=e_if'$ $(i=1,\cdots,r)$, and $(f)+(f')=\oplus_{i=1,\cdots,r}((e_if)+(e_if'))$. And S/R is separable if and only if each $e_i\cdot R[X]/(e_if)$ is separable over e_iR. Hence we obtain the last assertion.

Let $f(X)$ be a proper q-monic polynomial over R. If $R[X]/(f)$ is a separable R-algebra, we call f a *separable* polynomial over R (Janusz [8]).

§3. Splitting ring of a monic polynomial.

In this section we consider the factorization of a monic polynomial.

Proposition 3.1. *Let $f(X)$ be a monic polynomial over R such that $f(X)\neq 1$. Theh there is a Frobenius extension A/R which contains $\alpha_1,\cdots,\alpha_n$ such that $f(X)=(X-\alpha_1)\cdots(X-\alpha_n)$ and $A=R[\alpha_1,\cdots,\alpha_n]\supseteq R$. If R is indecomposable then A/R can be chosen to be indecomposable.*

Proof. By Th. 2.1, there is a root α_1 of $f(X)$ such that $R[\alpha_1]/R$ is a Frobenius extension. Then, in $R[\alpha_1][X]$, $f(X)=(X-\alpha_1)f_1(X)$ for some $f_1(X)\in R[\alpha_1][X]$. If $f_1(X)\neq 1$, then there is a root α_2 of $f_1(X)$ such that $R[\alpha_1,\alpha_2]/R[\alpha_1]$ is a Frobenius extension. Continuing this process, we can find $\alpha_1,\cdots,\alpha_n$ such that $f(X)=(X-\alpha_1)\cdots(X-\alpha_n)$ and such that each $R[\alpha_1,\cdots,\alpha_{i+1}]/R[\alpha_1,\cdots,\alpha_i]$ is a Frobenius extension. Then, by the transitivity of "Frobenius extension", $R[\alpha_1,\cdots,\alpha_n]/R$ is a Frobenius extension (cf. [11], [10]). We put $A=R[\alpha_1,\cdots,\alpha_n]$. To prove the latter half, we take a primitive idempotent e in A. Then $R\simeq Re$ $(\subseteq Ae)$ (because ${}_RA$ is finitely generated, projective, and faithful, and R is indecomposable (cf. [4])), and $e\cdot f(X)=(eX-e\alpha_1)\cdots(eX-e\alpha_n)$ in $e\cdot A[X]$. Thus it suffices to prove that Ae/Re is a Frobenius extension. By [10; Cor. 1], there are $h:\ {}_RA\rightarrow{}_RR$, and r_j, $l_i\in A$ such that $x=\sum_i h(xr_i)l_i=\sum_i r_i\cdot h(l_ix)$ for all x in A. Then, for any x in Ae, $x=\sum_i h(xr_ie)e\cdot l_ie=\sum_i r_ie\cdot h(l_ie\cdot x)e$, and $(x\rightarrow h(x)e)(x\in Ae)$ is an Re-homomorphism from Ae to Re $(\simeq R)$. Therefore Ae/Re is a Frobenius extension with (eh, r_ie, l_ie), by [10; Cor. 1].

Proposion 3.2. *Let $g_i(X)$ $(i=1,\cdots,n)$ $(n\geqslant 2)$ be proper q-monic polynomials in $R[X]$. Put $f(X)=\coprod_i g_i(X)$. Then $f(X)$ is separable if and only if each $g_i(X)$ is separable, and $(g_i(X))+(g_j(X))=R[X]$ provided $i\neq j$.*

Proof. We may assume that $n=2$. Assume that $f(X)$ is separable. Then $(f)+(f')=R[X]$, and $f'=g_1'g_2+g_1g_2'$. Then $(g_1)+(g_1')\supseteq(f)+(f')=R[X]$, and so $(g_1)+(g_1')=R[X]$. Similarly we have $(g_1)+(g_2)=R[X]$. Conversely if $(g_i)+(g_i')=R[X]$ $(i=1, 2)$ and $(g_1)+(g_2)=R[X]$, then $(f')+(g_1)\supseteq(g_1'g_2)+(g_1)=R[X]$, and so $(f')+(g_1)=R[X]$. Similarly we have $(f')+(g_2)=R[X]$. Hence $(f')+(f)=R[X]$.

Proposition 3.3. *Let $R \subseteq S$ be an integral ring extension, and $f(X)$ a proper q-monic polynomial in $R[X]$. If $f(X)$ is separable in $S[X]$, then $f(X)$ is separable in $R[X]$.*

Rroof. By Prof. 1.1 (4), $S[X]/f(X)S[X]$ can be considered as an integral ring extension over $R[X]/f(X)R[X]$, canonically. And the separability of $f(X)$ in $S[X]$ implies that $f'(u)$ is a unit in $S[X]/f(X)S[X]$, where $u = X + f(X)R[X]$. Then $f'(u)$ is a unit in $R[X]/f(X)R[X]$, because $S[X]/f(X)S[X]$ is integral over $R[X]/f(X)R[X]$. Hence $f(X)$ is separable in $R[X]$, by Cor. to Th. 2.1.

Let $f(X)$ be a proper monic polynomial in $R[X]$, and assume that R has no proper idempotents. Let $R[X]/(f) = I_1/(f) \oplus \cdots \oplus I_r/(f)$ be a direct sum of proper ideals, where each I_i is an ideal of $R[X]$ which contains (f). Put $\sum_{i \neq j} I_i = F_j$ $(j = 1, \cdots, r)$. Then $R[X]/(f) = I_i/(f) \oplus F_i/(f)$, and $I_i = \cap_{j \neq i} F_j = \prod_{j \neq i} F_j$. By Th. 1.3, each F_i is generated by a proper monic polynomial f_i of $R[X]$, because $R[X]/F_i \simeq I_i/(f)$ is finitely generated and projective. Then $I_i = (\prod_{j \neq i} f_j)$, and $(f) = (\prod_j f_j)$. Hence $f = \prod_j f_j$, and $(f_i) + (f_j) = R[X]$ provided $i \neq j$. From this fact, we have the following

Proposition 3.4. (*cf.* [3; *Lemma* 3]). *Let R be an indecomposable ring, and $f(X)$ a proper monic polynomial in $R[X]$. Then $R[X]/(f(X))$ is indecomposable if and only if $f(X)$ has no factorization $f = gh$ of proper monic polynomials such that $(g) + (h) = R[X]$. In this case, we call $f(X)$ an indecomposable polynomial over R.*

Let $f(X)$ and $g(X)$ be proper monic polynomials in $R[X]$. If $(f) + (g) = R[X]$, we say that f and g are *comaximal* in $R[X]$. Then we have the following

Proposition 3.5. *Let R be an indecomposable ring, and let $f(X)$ be a proper monic polynomial over R. Then $f(X)$ is uniquely represented as a product of pairwise comaximal indecomposable polynomials over R.*

Proof. The uniqueness follows from the uniqueness of direct sum decomposition into indecomposable ideals.

Now we take a family of ring monomorphisms. Let $\mathfrak{S}$ be a class of ring monomorphisms σ: $B \to A$ such that both A and B are non-zero indecomposable rings. Further assume that $\mathfrak{S}$ satisfies the following conditions:

(1) Let σ: $B \to A$ be in $\mathfrak{S}$. If σ': $B' \to A'$ is isomorphic to σ, then σ' is in $\mathfrak{S}$, where "isomorphic" implies that there are ring isomorphisms α, β such that the following diagram is commutive:

$$\begin{array}{ccc} B & \xrightarrow{\sigma} & A \\ \beta \downarrow & & \downarrow \alpha \\ B' & \xrightarrow[\sigma']{} & A' \end{array}$$

(2) If $\mathfrak{E} \ni A/B,\ B/C$ then $A/C \in \mathfrak{E}$.

(3) If $\mathfrak{E} \ni A/B$ then $id_A,\ id_B \in \mathfrak{E}$.

(4) For any $A/B,\ T/B$ in $\mathfrak{E}$, there are $L/B \in \mathfrak{E}$ and ring monomorphisms $\rho: A/B \to L/B$ and $\tau: T/B \to L/B$ such that $L/\rho(A),\ L/\tau(T) \in \mathfrak{E}$.

$$\begin{array}{ccc} & L & \\ \diagup & & \diagdown \\ A & & T \\ \diagdown & & \diagup \\ & B & \end{array}$$

In the sequel, R denotes an indecomposable commutative ring such that $id_R \in \mathfrak{E}$.

Let $f(X)$ be a proper monic polynomial in $R[X]$. $f(X)$ is said to be $\mathfrak{E}$-absolutely indecomposable if $S[X]/(f(X))$ is an indecomposable ring for every S/R in $\mathfrak{E}$.

Proposition 3.6. *Let R be an indecomposable ring such that $id_R \in \mathfrak{E}$, and $f(X)$ a proper monic polynomial over R. Then there is an ring exension T/R in $\mathfrak{E}$ in which $f(X)$ is a product of pairwise comaxmal $\mathfrak{E}$-absolutely indecomposable polynomials. We call T/R an $\mathfrak{E}$-splitting ring of $f(X)$.*

Proof. This follows from the following fact: Let *T/R be in $\mathfrak{E}$, and let* $(R[X]/(f)) \otimes_R T = I_1 \oplus \cdots \oplus I_r$ be a direct sum of indecomposable ideals $\neq 0$. Then $r \leqslant \deg f(X)$.

Theorem 3.7. *Let R be an indecomposable ring such that $id_R \in \mathfrak{E}$, and $f(X)$ a monic polynomial over R. Let both T/R and U/R be $\mathfrak{E}$-splitting rings of $f(X)$. Let $f(X) = \prod_{i=1,\cdots,r} f_i(X)$ and $f(X) = \prod_{j=1,\cdots,s} g_j(X)$ be products of pairwise comaximal $\mathfrak{E}$-absolutely indecomposable polynomials in T/R and U/R, respectively. Let T_0 and U_0 be extension rings of R which are generated by all coefficients of f_i and all coefficients of g_j, respectively. Then $r=s$, and there is an R-algebra isomorphism φ from T_0/R to U_0/R such that $f_{\varepsilon(i)}^{\varphi} = g_i$ $(i=1, \cdots, r)$ for some permutation ε of $\{1, \cdots, r\}$.*

Proof. By condition (4), there are $L/R \in \mathfrak{E}$ and ring monomorphisms $\sigma: T/R \to L/R$ and $\tau: U/R \to L/R$ such that $L/\sigma(T),\ L/\tau(U) \in \mathfrak{E}$. Then f_i^{σ} $(i=1, \cdots, r)$ and g_j^{τ} $(j=1, \cdots, s)$ are indecomposable in $L[X]$, so that $r=s$ and $f_{\varepsilon(i)}^{\sigma} = g_i^{\tau}$ $(i=1, \cdots, r)$ for some permutation ε of $\{1, \cdots, r\}$, by Prop. 3.5. Then $f_{\varepsilon(i)}^{\sigma} = g_i^{\tau} \in (\sigma(T_0) \cap \tau(U_0))[X]$ $(i=1, \cdots, r)$. Hence $\sigma(T_0) = \tau(U_0)$ in L.

Here we present several examples of $\mathfrak{E}$. Let A, B be non-zero indecomposable commutative rings, and let $\sigma: B \to A$ be a ring monomorphism.

Example 1. A is finitely generated and projective (and faithful) as a B- module.

Proof. It suffices to prove (4). Let $A/B,\ T/B$ be in $\mathfrak{E}$, and let e be a primitive idempotent of $A\otimes_B T$. Then ${}_A A\otimes_B T$ and ${}_T A\otimes_B T$ are finitely generated and projective. Then $(A\otimes_B T)e$ is finitely generated, projective and faithful as an A-module, because A is indecomposable. Therefore $A\simeq Ae$, canonically. Similarly $(A\otimes_B T)e$ is finitely generated, projective, and faithful as a T-module, and $T\simeq Te$ canonically.

Example 2. A/B is a Frobenius extension.

Proof. Since "Frobenius extension" is transitive, it suffices to prove (4). Let A/B and T/B be in $\mathfrak{F}$, and take a primitive idempotent e of $A\otimes_B T$. Then $A\otimes_B T/A$ and $A\otimes_B T/T$ are Frobenius extension (cf. [10; Th. 3]). Then, by the same way with the proof of Prop. 3.1, we can see that both $(A\otimes_B T)e/Ae$ and $(A\otimes_B T)e/Te$ are in $\mathfrak{F}$.

Example 3. A/B is a strongly separable extension (in the sence of [8]). This is well known (cf. [8]).

§ 4. Appendix

In this section, we prove an analogous result for any (not necessary commutative) R-algebra. Let R be an indecomposable ring such that $id_R\in\mathfrak{F}$, and A an R-algebra such that ${}_R A$ is finitely generated, projective, and faithful. Then we call A an *$(R, \mathfrak{F})$-algebra.* If A has no proper central idempotents, then A is said to be *indecomposable.* If $A\otimes_R S$ is indecomposable for all S/R in $\mathfrak{F}$, A is said to be $\mathfrak{F}$-absolutely indecomposable. The next proposition is analogous to Prop. 3.6.

Proposition 4.1. *Let A be an $(R, \mathfrak{F})$-algebra. Then there is an S/R in $\mathfrak{F}$ such that an $(S, \mathfrak{F})$-algebra $A\otimes_R S$ is a direct sum of $\mathfrak{F}$-absolutely indecomposable S-algebra.*

We call S/R an $\mathfrak{F}$-splitting ring of A. Let $S_\lambda(\lambda\in\Lambda)$ be the set of all intermediate subrings of S/R such that $A_R\otimes S_\lambda$ contains all primitive central idempotents of $A\otimes_R S$. Then, since A_R is finitely generated and projective, $\cap_\lambda(A\otimes_R S_\lambda)=A\otimes_R(\cap_\lambda S_\lambda)$ in $A\otimes_R S$. Therefore there is the unique minimal member S_0 in $\{S_\lambda\,|\,\lambda\in\Lambda\}$. Let T/R be another $\mathfrak{F}$-splitting ring of A/R. Similarly we take an intermediate ring T_0/R of T/R.

Theorem 4.2. *S_0/R is isomorphic to T_0/R* as *R-algebras.*

Proof. By condition (4) there are L/R in $\mathfrak{F}$ and ring monomorphisms $\sigma\colon S/R\rightarrow L/R$ and $\tau\colon T/R\rightarrow L/R$ such that $L/\sigma(S)$, $L/\tau(T)\in\mathfrak{F}$. By identification we may consider S/R, T/R as R-subalgebras of L/R. Let $1=\sum_{i=1,\cdots,r}e_i$ and $1=\sum_{j=1,\cdots,s}u_j$ be sums of pairwise orthogonal primitive central idempotents in $A\otimes_R S$ and $A\otimes_R T$, respectively. Then, since $(A\otimes_R S)e_i$ is an $\mathfrak{F}$-absolutely indecomposable S-algebra, $(A\otimes_R S)e_i\otimes_S L$ is indecomposable.

Similarly $(A\otimes_R T)u_j\otimes_T L$ is indecomposable. Since $A\otimes_R L=\oplus_i ((A\otimes_R S)e_i \otimes_S L)=\oplus_j ((A\otimes_R T)u_j\otimes_T L)$, we have $r=s$ and $\{(A\otimes_R S)e_i\otimes_S L \mid i=1, \cdots, r\} = \{(A\otimes_R T)u_j\otimes_T L \mid j=1, \cdots, r\}$ in $A\otimes_R L$. Therefore we may assume that $e_i=f_i$ for all $i=1, \cdots, r$. Then $e_i=f_i\in(A\otimes_R S_0)\cap(A\otimes_R T_0)=A\otimes_R(S_0\cap T_0)$, and hence $S_0=T_0$. This completes the proof.

References

[1] M. AUSLANDER and D. BUCHSBAUM: On the ramification theory in Noethrian rings, Amer J. Math., 81 (1959), 749-765.

[2] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative ring, Trans. Amer. Math. Soc., 97 (1960), 367-409.

[3] G. AZUMAYA: On maximally central algebras, Nagoya Math. J., 2 (1951), 119-150.

[4] N. BOURBAKI: Algèbre commutative, Hermann, Paris, 1962.

[5] O. GOLDMAN: Determinants in projective modules, Nagoya Math. J., 18 (1961), 27-36.

[6] K. HIRATA and K. SUGANO: On semi-simple extensions and separable extensions over non-commutative rings, J. Math. Soc. Japan, 18 (1966), 360-373.

[7] N. JACOBSON: Generation of separable and central simple algebras, J. Math. Pures Appl., (9), 36 (1957), 217-227.

[8] G. L. JANUSZ: Separable algebras over a commutative ring, Trans. Amer. Math. Soc., 122 (1966), 461-479.

[9] F. KASCH: Projective Frobenius-Erweiterungen, Stzungsber Heidelberger Akad., 89-109 (1960/1961).

[10] T. ONODERA: Some studies on projective Frobenius extensions, J. Fac. Sci. Hokkaido Univ., Ser. I, 18 (1964), 89-107.

[11] B. PAREIGIS: Finige Bemerkungen uber Frobenius Erweiterungen, Math. Ann., 153 (1964), 1-13.

Department of Mathematics,
Tokyo University of Education

(Received Oct. 10, 1970)