A note on twisted polynomial rings

Dedicated to Professor Yoshie Katsurada on her sixtieth birthday

By Tadashige OKADA and Ryô SAITÔ

§ 1. Introduction

Throughout this paper, we assume that every ring has an identity 1, every module over a ring is unitary and a ring extension A/B has the same identity. Let R be a commutative ring. An R-algebra Λ is called separable if Λ is left $\Lambda^e=\Lambda\otimes_R\Lambda^0$-projective where Λ^0 is an opposite ring of Λ. An R-algebra Λ which is finitely generated and projective as an R-module is called a symmetric R-algebra if Λ is isomorphic to $\mathrm{Hom}_R(\Lambda, R)$ as a left Λ^e-module ([1], [3]).

Let S be a commutative ring which is a finite Abel extension of R with Galois group $G=<\sigma_1>\times\cdots\times<\sigma_l>$ (direct product of cyclic groups) such that the order of $\sigma_i=n_i$. We consider a twisted polynomial ring of l-variables $B=S[X_1,\cdots,X_l;\ \sigma_1,\cdots,\sigma_l]$. That is, $B=\{\sum_{p_1,\cdots,p_l} X_1^{p_1}\cdots X_l^{p_l}a_{p_1,\cdots,p_l}|a_{p_1,\cdots,p_l}\in S\}$; and B has the following arithmetics; for any $a\in S$, $aX_i=X_ia^{\sigma_i}$ and $X_iX_j=X_jX_i$.

For a $f(X_1,\cdots,X_l)=F(X_1^{n_1},\cdots,X_l^{n_l})\in R[X_1,\cdots,X_l]$, we have $f(X_1,\cdots,X_l)B=Bf(X_1,\cdots,X_l)$. Let $f_i(X_i)=F_i(X_i^{n_i})\in R[X_i]$ $(i=1,\cdots,l)$ be monic polynomials. Put $I=\sum_{i=1}^{l}Bf_i(X_i)$, $A=B/I$ and $u_i=X_i+I\in A$. Then we have a following theorem.

THEOREM 2. *If $f_i(0)=F_i(0)$ is a unit of R $(i=1,\cdots,l)$, then*

$$A=\sum_{0\leqq\alpha_j\leqq n_j-1}\oplus u_1^{\alpha_1}\cdots u_l^{\alpha_l}S[u_1^{n_1},\cdots,u_l^{n_l}]$$

$$=\Delta(C_{\sigma_1^{\alpha_1}\cdots\sigma_l^{\alpha_l},\ \sigma_1^{\beta_1}\cdots\sigma_l^{\beta_l}},\ S[u_1^{n_1},\cdots,u_l^{n_l}],\ G=\langle\sigma_1\rangle\times\cdots\times\langle\sigma_l\rangle)$$

(crossed product where the factor set is defined by the following way. $C_{\sigma_1^{\alpha_1}\cdots\sigma_l^{\alpha_l},\sigma_1^{\beta_1}\cdots\sigma_l^{\beta_l}}=\prod_{i=1}^{l}u_i^{\nu_i}$ *where*

$$\nu_i=\begin{cases} n_i & \text{if}\ \ \alpha_i+\beta_i\geqq n_i \\ 0 & \text{if}\ \ \alpha_i+\beta_i\leqq n_i-1). \end{cases}$$

$$=\Delta(u_1^{n_1},\ S_1[u_1^{n_1},\cdots,u_l^{n_l}],\ \langle\sigma_1\rangle)\otimes_{R[u_1^{n_1},\cdots,u_l^{n_l}]}\cdots\cdots\otimes\Delta(u_l^{n_l},\ S_l[u_1^{n_1},\cdots,u_l^{n_l}],\ \langle\sigma_l\rangle)$$

(*tensor product of cyclic crossed products where* $S_i[u_1^{n_1},\cdots,u_l^{n_l}] = S[u_1^{n_1},\cdots,u_l^{n_l}]^{G_i} = \{x\in S[u_1^{n_1},\cdots,u_l^{n_l}] \mid x^{\omega}=x$ *for all* $\omega\in G_i\}$ *and* $G_i=\langle\sigma_1\rangle\times\cdots\times\langle\sigma_{i-1}\rangle\times\langle\sigma_{i+1}\rangle\times\cdots\times\langle\sigma_l\rangle$).

The authors extend their hearty thanks to Professor Y. Miyashita for his kind suggestion and encouragement.

§ 2. The proos of Theorem 2 and some results

We use notations which is written in § 1. In the case that $l=1$, we denote $B=S[X;\sigma]=\{\sum_p X^p a_p \mid a_p\in S\}$ etc.

PROPOSITION 1. *In the case that* $l=1$, *for a monic polynomial* $f(X)=\sum X^p a_p\in B$, *the followings are equivalent.*

(1) $f(X)B=Bf(X)$.
If a $a_p\neq 0$, *it is a non zero divisor in* S *and* $a_0\neq 0$.

(2) $f(X)=F(X^n)\in R[X]$.
If a $a_p\neq 0$, *it is a non zero divisor in* S *and* $a_0\neq 0$.

PROOF.

(2) $\Longrightarrow$ (1) trivial.

(1) $\Longrightarrow$ (2) By the condition that $Bf(X)=f(X)B$, for any $\alpha\in S$, there exists $\beta\in S$ such that $\alpha f=f\beta$. That is, $\sum X^p\alpha^{\sigma^p}a_p=\alpha\sum X^p a_p=\sum X^p a_p\beta$ So, $\alpha^{\sigma^p}a_p=a_p\beta$. By the condition that $a_0\neq 0$ and that this is a non zero divisor, $\alpha=\beta$. For a p such that $a_p\neq 0$, $\alpha^{\sigma^p}=\beta=\alpha$. So, $\sigma^p=1$ and $n|p$ (i.e. n divides p). This denotes that $f(X)=F(X^n)$. By the condition that $Bf(X)=f(X)B$, there exists $\alpha\in S$ such that $Xf(X)=f(X)(X+\alpha)$. That *is*, $\sum_t X^{nt+1}a_{nt}=\sum_t X^{nt+1}a_{nt}^{\sigma}+\sum_t X^{nt}a_{nt}\alpha$. *So*, $a_{nt}\alpha=0$ for all t, and by the fact that $a_0\neq 0$, $\alpha=0$. This denotes that $a_{nt}^{\sigma}=a_{nt}$. That is, $f(X)=F(X^n)\in R[X]$. Q.E.D.

Let $f_i(X_i)=F_i(X_i^{n_i})\in R[X_i]$ $(i=1,\cdots,l)$ be monic polynomials. Put $I=\sum_{i=1}^{l}Bf_i(X_i)$, $A=B/I$ and $u_i=X_i+I\in A$. If $\deg F_i(X_i)=m_i$, $\deg f_i(X_i)=n_i m_i$. Here, $\deg f_i(X_i)$ $(i=1,\cdots,l)$ is the degree of $f_i(X_i)$. Then, we have $A=\sum_{0\leq p_j\leq n_j m_j-1}\oplus u_1^{p_1}\cdots u_l^{p_l}S$.

The PROOF of THEOREM 2 see (§ 1). As $f_i(0)$ is a unit of R, $f_i(X_i)B+X_iB=B$ and $Bf_i(X_i)+BX_i=B$, each u_i is a unit of A. $S[u_1^{n_1},\cdots,u_l^{n_l}]$ is a free S-module of rank $\prod_{i=1}^{l}m_i$, $R[u_1^{n_1},\cdots,u_l^{n_l}]$ is a free R-module rank $\prod_{i=1}^{l}m_i$ *and* $S[u_1^{n_1},\cdots,u_l^{n_l}]=R[u_1^{n_1},\cdots,u_l^{n_l}]\otimes_R S$. By ordinary computations, we have

$A = \sum_{0 \leq p_j \leq n_j m_j - 1} \oplus u_1^{p_1} \cdots u_l^{p_l} S = \sum_{0 \leq \alpha_j \leq n_j - 1} \oplus u_1^{\alpha_1} \cdots u_l^{\alpha_l} S[u_1^{n_1}, \cdots, u_l^{n_l}]$. By our assumptions, for any $a \in S$, $au_i = u_i a^{\sigma_i}$. As $S[u_1^{n_1}, \cdots, u_l^{n_l}]$ is a G-Galois extension of $R[u_1^{n_1}, \cdots, u_l^{n_l}]$, $\sum_{0 \leq \alpha_j \leq n_j - 1} \oplus u_1^{\alpha_1} \cdots u_l^{\alpha_l} S[u_1^{n_1} \cdots u_l^{n_l}]$ is a crossed product. As the factor set, we take $\{C_{\sigma_1^{\alpha_1} \cdots \sigma_l^{\alpha_l}, \sigma_1^{\beta_1} \cdots \sigma_l^{\beta_l}} = \prod_{i=1}^{l} u_i^{\nu_i}$ where $\nu_i = n_i$ if $\alpha_i + \beta_i \geqq n_i$ and $\nu_i = 0$ *if* $\alpha_i + \beta_i \leqq n_i - 1\}$. The fact that A can be written $\Delta(u_1^{n_1}, S_1[u_1^{n_1}, \cdots, u_l^{n_l}], \langle\sigma_1\rangle) \otimes_{R[u_1^{n_1}, \cdots, u_l^{n_l}]} \cdots \cdots \otimes \Delta(u_l^{n_l}, S_l[u_1^{n_1}, \cdots, u_l^{n_l}], \langle\sigma_l\rangle)$ (*tensor* product of cyclic crossed products where $S_i[u_1^{n_1}, \cdots, u_l^{n_l}] = S[u_1^{n_1}, \cdots, u_l^{n_l}]^{G_i} = \{x \in S[u_1^{n_1}, \cdots, u_l^{n_l}] \mid x^{\omega} = x$ *for all* $\omega \in G_i\}$ *and* $G_i = \langle\sigma_1\rangle \times \cdots \times \langle\sigma_{i-1}\rangle \times \langle\sigma_{i+1}\rangle \times \cdots \times \langle\sigma_l\rangle$.) is a result of general Galois theory of commutative rings ([2]). Q.E.D.

COROLLARY 3. *In Theorem 2, furthermore we assume that* $f_i(X_i) = X_i^{n_i} - a_i$ *(i.e.* $F_i(X_i) = X_i - a_i$*) and* a_i *is a unit of* R $(i = 1, \cdots, l)$, *we have*

$$A = \Delta(a_1, S_1, \langle\sigma_1\rangle) \underset{R}{\otimes} \cdots \underset{R}{\otimes} \Delta(a_l, S_l, \langle\sigma_l\rangle) \quad \textit{where} \quad S_i = S^{G_i}.$$

PROOF. In this case, $u_i^{n_i} = a_i \in R$. So, this follows immediately from THEOREM 2.

PROPOSITION 4. *Under the same assumptions as in* THEOREM 2, *A is a symmetric R-algebra.*

PROOF. As $R[u_i^{n_i}]$ is a free R-module of rank m_i $(i = 1, \cdots, l)$, $R[u_1^{n_1}, \cdots, u_l^{n_l}] \cong R[u_1^{n_1}] \underset{R}{\otimes} \cdots \underset{R}{\otimes} R[u_l^{n_l}]$. $R[u_i^{n_i}] \cong R[X_i]/F_i(X_i)R[X_i]$ is a free symmetric R-algebra ([6] THEOREM 2.1). So, $R[u_1^{n_1}, \cdots, u_l^{n_l}]$ is also a symmetric R-algebra ([3]). As A is a central separable $R[u_1^{n_1}, \cdots, u_l^{n_l}]$-algebra, by [4] THEOREM 4.2, A is a symmetric $R[u_1^{n_1}, \cdots, u_l^{n_l}]$-algebra. So, A is a symmetric R-algebra. Q.E.D.

LEMMA. 5. *Let R be a commutative ring and* $R[X_1, \cdots, X_l]$ *be a polynomial ring of l-variables* ($l \geqq 1$, *not twisted*). *Let* $\mathfrak{A}$ *be a proper ideal of* $R[X_1, \cdots, X_l]$ *such that* $\mathfrak{A} = \sum_{i=1}^{l} f_i(X_1, \cdots, X_l) R[X_1, \cdots, X_l]$ $(f_i(X_1, \cdots, X_l) \in R[X_1, \cdots, X_l], (i = 1, \cdots, l))$. *We put* $S = R[X_1, \cdots, X_l]/\mathfrak{A}$, *and assume that S is a finitely generated R-module. Then S is a separable R-algebra if and only if*

$$\left(det\left(\frac{\partial f_i}{\partial X_j}\right)_{1 \leq i, j \leq l}\right) + \mathfrak{A} = R[X_1, \cdots, X_l].$$

PROOF. This is easily seen.

COROLLARY 6. *In* LEMMA 5, *moreover we assume that* f_i $(i = 1, \cdots, l)$ *is a monic polynomial of* $R[X_i]$. *Then S is separable R-algebra if and* *only if each* $f_i=f_i(X_i)$ *is a separable polynomial of* $R[X_i]$ *in the sence of* [5] $(i=1,\cdots,l)$.

PROOF. only if part; By LEMMA 5,

$$\left(det\left(\frac{\partial f_i}{\partial X_j}\right)_{1\leq i,\, j\leq l}\right)+\mathfrak{A}=R[X_1,\cdots,X_l]. \quad \text{So,}$$

$$\left(\frac{df_1}{dX_1}\cdots\frac{df_l}{dX_l}\right)+\mathfrak{A}=R[X_1,\cdots,X_l]. \quad \text{Especially,}$$

$$\left(\frac{df_i}{dX_i}\right)+\mathfrak{A}=R[X_1,\cdots,X_l] \text{ and } \left(\frac{df_i}{dX_i}\right)+(f_i(X_i))=R[X_i] \ (i=1,\cdots,l).$$

So, by LEMMA 5, each $f_i(X_i)$ is a separable polynomial $(i=1,\cdots,l)$. if part; By LEMMA 5 $\left(\frac{df_i}{dX_i}\right)+(f_i(X_i))=R[X_i]$ for each i $(i=1,\cdots,l)$. So, $\left(\frac{df_1}{dX_1}\cdots\frac{df_l}{dX_l}\right)+\sum_{i=1}^{l}f_i(X_i)R[X_1,\cdots,X_l]=R[X_1,\cdots,X_l]$. By LEMMA 5, S is a separable R-algebra. Q.E.D.

PROPOSITION 7. *Under the same assumptions as in* THEOREM 2, *the followings are equivalent.*

(1) *Each* $F_i(X_i)$ *is a separable polynomial of* $R[X_i]$ $(i=1,\cdots,l)$.

(2) *A is a separable R-algebra.*

PROOF. (1)$\Longrightarrow$(2). It is sufficient if we prove that $R[u_1^{n_1},\cdots,u_l^{n_l}]$ is a separable R-algebra. But this is similarly proved as PROPOSITION 4.

(2)$\Longrightarrow$(1). By our assumptipns, $R[u_1^{n_1},\cdots,u_l^{n_l}]$ is a separable R-algebra. But as $R[u_1^{n_1},\cdots,u_l^{n_l}]\cong R[X_1,\cdots,X_l]/\sum_{i=1}^{l}F_i(X_i)R[X_1,\cdots,X_l]$, by COROLLARY 6, each $F_i(X_i)$ is a separable polynomial of $R[X_i]$ $(i=1,\cdots,l)$. Q.E.D.

Department of Mathematics, Hokkaido University

References

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

[2] S. U. CHASE, D. K. HARRISON and A. ROSENBERG: Galois theory and Galois cohomology of commutative rings; Mem. Amer. Math. Soc. 52 (1965), 15-33.

[3] S. EILENBERG and T. NAKAYAMA: On the dimension of modules and algebras II; Nagoya Math. J. 9 (1955), 1-16).

[4] S. ENDO and Y. WATANABE: On separable algebras over a commutative ring; Osaka J. Math. 4 (1967), 233-242.

[5] G. J. JANUSZ: Separable algebras over commutative rings; Trans. Amer. Math. Soc. 122 (1966), 461-479.

[6] Y. MIYASHITA: Commutative Frobenius algebras generated by a single element; J. Fac. Sci. Hokkaido Univ. XXI (1971), 166–176.

(Received February 29, 1972)