46. *Construction of Integral Basis. IV*

By Kōsaku OKUTSU
Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1982)

Let $\mathfrak{o}$ be a principal ideal domain, and k its quotient field. Let $f(x)$ be a monic irreducible separable polynomial of degree n in $\mathfrak{o}[x]$, and θ one of the roots of $f(x)$ in an algebraic closure $\bar{k}$ of k. In our preceding notes, we have given a formula for the integral basis of $K=k(\theta)$, i.e. an $\mathfrak{o}$-basis of integral closure $\mathfrak{o}_K$ of $\mathfrak{o}$ in K, for the case where $\mathfrak{o}$ is a complete discrete valuation ring. Now, using these results, we shall give a similar formula for the general (global) case.

§ 1. Let $\{\mathfrak{p}_\lambda\}_{\lambda\in\Lambda}$ be the set of all maximal ideals of $\mathfrak{o}$, $\pi_\lambda\in\mathfrak{o}$ a generator of $\mathfrak{p}_\lambda$, k_λ a completion of k with respect to $\mathfrak{p}_\lambda$, and $\mathfrak{o}_\lambda$ its ring of integers. (Fixing an embedding of k in k_λ, we assume that k is a subfield of k_λ.) Let $\bar{k}_\lambda$ be the algebraic closure of k_λ. We denote by $|\ |_\lambda$ a fixed valuation of $\bar{k}_\lambda$ which is an extension of the valuation corresponding to $\mathfrak{p}_\lambda$. Let $f(x)=\prod_{i=1}^{s} f_{\lambda,i}(x)$ be a factorization of $f(x)$ in $k_\lambda[x]$, where $f_{\lambda,i}(x)$ is a monic irreducible polynomial in $\mathfrak{o}_\lambda[x]$ of degree $n_{\lambda,i}$. Let $\theta_{\lambda,i}$ be one of the roots of $f_{\lambda,i}(x)$ in $\bar{k}_\lambda$. We define a k-isomorphism $\iota_{\lambda,i}$ from $K=k(\theta)$ into $\bar{k}_\lambda$ by putting $\iota_{\lambda,i}(\theta)=\theta_{\lambda,i}$. For each $\lambda\in\Lambda$ we define a real valued function $\|\ \|_\lambda$ on K as follows. $\|\alpha\|_\lambda=\sup_{i=1,\dots,s}|\iota_{\lambda,i}(\alpha)|_\lambda$ $(\alpha\in K)$. For a polynomial $h(x)=a_0x^m+\cdots+a_m$ in $\mathfrak{o}[x]$, we put $|h(x)|_\lambda=\sup_{j=0,\dots,m}|a_j|_\lambda$.

We have following Proposition 1, and Definition in generalization of what we have seen in Part I.

Proposition 1. *For each $\lambda\in\Lambda$ and any positive integer $m<n$, there exists a monic polynomial $g_{\lambda,m}(x)$ of degree m in $\mathfrak{o}[x]$ with the following property:*

For any polynomial $G(x)$ of degree m in $\mathfrak{o}[x]$, we have

$$\|g_{\lambda,m}(\theta)\|_\lambda\le\|G(\theta)_\lambda\|/|G(x)|_\lambda.$$

Definition. We will call a monic polynomial $g_{\lambda,m}(x)$ with the property in the above proposition a *devisor polynomial* of degree m of $f(x)$ for $\mathfrak{p}_\lambda$. We put $\mu_{\lambda,m}=\min_{i=1,\dots,s}\operatorname{ord}_{\pi_\lambda\mathfrak{o}_\lambda}(g_{\lambda,m}(\theta_{\lambda,i}))$, and $\nu_{\lambda,m}=[\mu_{\lambda,m}]$. $\nu_{\lambda,m}$ will be called the *integrality index* of degree m of θ for $\mathfrak{p}_\lambda$.

Proposition 2. *Let $g_{\lambda,m}(x)$, $\nu_{\lambda,m}$ be a divisor polynomial, and the integrality index of degree m of θ for $\mathfrak{p}_\lambda$. We put*

$$R_\lambda=\sum_{m=0}^{n-1}\mathfrak{o}\frac{g_{\lambda,m}(\theta)}{\pi_\lambda^{\nu_{\lambda,m}}}.$$

Then R_λ coincides with the subring $\{x\in\mathfrak{o}_K\mid\pi_\lambda^l\cdot x\in\mathfrak{o}[\theta]$ for some positive *integer* $l\}$ *of* $\mathfrak{o}_K$, *and any maximal ideal of* R_λ *containing* $\mathfrak{p}_\lambda$ *is invertible in* R_λ.

Proposition 3. *If any prime divisor of* $\mathfrak{p}_\lambda\mathfrak{o}[\theta]$ *is invertible in* $\mathfrak{o}[\theta]$, *we have* $\nu_{\lambda,m}=0$ *for* $m=0, \cdots, n-1$.

Let Λ_0 be the subset of Λ such that $\lambda \in \Lambda_0$ means the following: There exists some maximal ideal $\mathfrak{P}$ of $\mathfrak{o}[\theta]$ containing π_λ which is not invertible in $\mathfrak{o}[\theta]$. If $\mathfrak{p}_\lambda\mathfrak{o}[\theta]$ is prime to the conductor $(\mathfrak{o}[\theta]:\mathfrak{o}_K)$ of $\mathfrak{o}[\theta]$, every prime divisor of $\mathfrak{p}_\lambda\mathfrak{o}[\theta]$ is invertible in $\mathfrak{o}[\theta]$. As the discriminant $D(f)$ of $f(x)$ is contained in $(\mathfrak{o}[\theta]:\mathfrak{o}_K)$, we have $\mathfrak{p}_\lambda \ni D(f)$ for any $\lambda \in \Lambda_0$. Thus Λ_0 is a finite set.

Theorem 1. *Let* $g_m(x)$ *be a monic polynomial of degree* m *in* $\mathfrak{o}[x]$ *satisfying* $g_m(x)\equiv g_{\lambda,m}(x) \pmod{\pi_\lambda^{\nu_{\lambda,m}+1}}$ *for any* $\lambda \in \Lambda$, *where* $g_{\lambda,m}(x)$ *is a divisor polynomial, and* $\nu_{\lambda,m}$ *is the integrality index of degree* m *for* $\mathfrak{p}_\lambda$ *of* θ. *Then we have*

$$\mathfrak{o}_K=\sum_{m=0}^{n-1} \mathfrak{o}\frac{g_m(\theta)}{\prod_{\lambda\in\Lambda_0}\pi_\lambda^{\nu_{\lambda,m}}}.$$

Remark. The product $\prod_\lambda$ in the above theorem may be taken over the prime ideals $\mathfrak{p}_\lambda$ containing the discriminant of $f(x)$.

§2. Now we show how divisor polynomials $g_{\lambda,m}(x)$ for $\mathfrak{p}_\lambda$ can be constructed from primitive divisor polynomials of the irreducible factors of $f(x)$ in $k_\lambda[x]$. Let $f(x)=\prod_{i=1}^{s} f_{\lambda,i}(x)$ be an irreducible factorization of $f(x)$ in $\mathfrak{o}_\lambda[x]$. We fix now λ, and write $f_i(x)$ for $f_{\lambda,i}(x)$. Let θ_i be a root of $f_i(x)$ in $\bar{k}_\lambda$, and n_i the degree of $f_i(x)$ $(i=1, \cdots, s)$. Let $f_{i,j}(x)$ be a j-th primitive divisor polynomial of $f_i(x)$ $(1\leq j\leq r_i$, where r_i is the depth of $f_i(x))$, and $f_{i,0}(x)=f_i(x)$. We put $S_{i,j}=\{k\in\{1, 2, \cdots, s\}\,|\,|f_{i,j}(\theta_k)|_\lambda \geq |f_{i,j}(\theta_i)|_\lambda\}$. It is easy to see that $S_{i,j}\supsetneqq S_{i',j'}$ implies $m_j(\theta_i, k_\lambda) < m_{j'}(\theta_{i'}, k_\lambda)$ (where $m_j(\theta_i, k_\lambda)$ is the degree of $f_{i,j}(x)$ as in Part II). Furthermore $S_{i,j}\cap S_{i',j'}\neq\emptyset$ implies $S_{i,j}\subset S_{i',j'}$ or $S_{i',j'}\subset S_{i,j}$. Thus when $m_j(\theta_i, k_\lambda)=m_{j'}(\theta_{i'}, k_\lambda)$ and $S_{i,j}\cap S_{i',j'}\neq\emptyset$, we have $S_{i,j}=S_{i',j'}$. Now introduce an equivalence relation $\sim$ in the set $\{(i,j)\,|\,1\leq i\leq s, 0\leq j\leq r_i\}$ in defining $(i,j)\sim(i',j')\Leftrightarrow S_{i,j}=S_{i',j'}$ and $m_j(\theta_i, k_\lambda)=m_{j'}(\theta_{i'}, k_\lambda)$. We denote by $\mathfrak{S}$ a complete set of representatives of the equivalence classes given by this $\sim$. Then we have

Theorem 2. *For any integer* m $(0\leq m<n)$, *there exist some integers* $q_{i,j}\geq 0$ $((i,j)\in\mathfrak{S})$ *satisfying*

$$\sum_{(i,j)\in\mathfrak{S}} q_{i,j}m_j(\theta_i, k_\lambda)=m, \quad \textit{and} \quad \sup_{k=1,\cdots,s}\Big|\prod_{(i,j)\in\mathfrak{S}} f_{i,j}(\theta_k)^{q_{i,j}}\Big|_\lambda=\|g_{\lambda,m}(\theta)\|_\lambda$$

where $g_{\lambda,m}(x)$ *is a divisor polynomial of degree* m *of* θ *for* $\mathfrak{p}_\lambda$.

A divisor polynomial $g_{\lambda,m}(x)$ is therefore obtained from $f_{\lambda,i}(x)$ as follows. Let $q_{i,j}\in\{0,1,\cdots,m\}$ $((i,j)\in\mathfrak{S})$ be a solution of $\sum_{(i,j)\in\mathfrak{S}} q_{i,j}m_j(\theta_i, k_\lambda)=m$. For this solution W, consider the value

$$\sup_{k=1,\cdots,s}\Big|\prod_{(i,j)\in\mathfrak{S}} f_{i,j}(\theta_k)^{q_{i,j}}\Big|_\lambda$$

which we denote with v_W. As there are only a finite number of such solutions W, there is a minimum value v_{W_0} of these values, and the corresponding solution $W_0=\{q^0_{i,j}((i,j)\in\mathfrak{S})\}$. Let $g(x)$ be a monic polynomial of degree m in $\mathfrak{o}[x]$ satisfying

$$|g(x)-\prod_{(i,j)\in\mathfrak{S}} f_{i,j}(x)^{q^0_{i,j}}|_\lambda \leq \sup_{k=1,\cdots,s} |\prod_{(i,j)\in\mathfrak{S}} f_{i,j}(\theta_k)|_\lambda.$$

Then $g(x)$ is the divisor polynomial of degree m for $\mathfrak{p}_\lambda$ of θ.

Reference

[1] K. Okutsu: Construction of Integral Basis. I; II; III. Proc. Japan Acad., **58**A, 47–49; 87–89; 117–119 (1982).