24. *Construction of Integral Basis. II*

By Kōsaku OKUTSU
Department of Mathematics, Gakushuin University

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

Let $\mathfrak{o}$ be a complete discrete valuation ring with the maximal ideal $\mathfrak{p}$, k its quotient field, $\bar{k}$ an algebraic closure of k, and k_s the separable closure of k in $\bar{k}$. Let θ be an element of k_s which is integral over $\mathfrak{o}$. In Part I, we have defined divisor polynomials and integrality indexes of θ, by means of which we have given an integral basis of $k(\theta)$ explicitly.

In this part, we shall define primitive divisor polynomials of θ, with which the divisor polynomials of θ will be expressed explicitly. We denote by $|\ \ |$ a fixed valuation of $\bar{k}$, extending the valuation of k. Let $f(x)$ be the minimal polynomial of θ over k, and assume that the degree of n of $f(x)$ is greater than 1.

§1. We define a finite sequence $\{\lambda_i(\theta, k)\}_{i=1,2,\dots,r}$ of real numbers and a finite sequence $\{m_i(\theta, k)\}_{i=0,1,2,\dots,r}$ of natural numbers inductively as follows.

Definition 1. We put $m_0(\theta, k)=n$, $\lambda_i(\theta, k)=\min\{|\theta-\beta| \mid \beta\in\bar{k}$ such that $[k(\beta):k]<m_{i-1}(\theta, k)\}$, and $m_i(\theta, k)=\min\{[k(\gamma):k] \mid \gamma\in\bar{k}$ such that $|\theta-\gamma|=\lambda_i(\theta, k)\}$. We have clearly $\lambda_i(\theta, k)<\lambda_{i+1}(\theta, k)$ and $m_i(\theta, k)>m_{i+1}(\theta, k)$, and there exists some integer r such that $m_r(\theta, k)=1$. r is said to be the *depth* of $f(x)$ or of θ over k.

$\lambda_i(\theta, k)$ and $m_i(\theta, k)$ do not depend upon the choice of a root θ of $f(x)$.

Proposition 1. *There exists an element α_i of k_s satisfying $|\theta-\alpha_i|=\lambda_i(\theta, k)$, and $[k(\alpha_i):k]=m_i(\theta, k)$ $(i=1, \cdots, r)$.*

Definition 2. We call the minimal polynomial of α_i over k an *i-th primitive divisor polynomial* of θ or of $f(x)$ over k.

Proposition 2. *An i-th primitive divisor polynomial of $f(x)$ over k is a divisor polynomial of $f(x)$ of degree $m_i(\theta, k)$ over k.*

Proposition 3. *We assume that the depth r of $f(x)$ is greater than* 1. *Then for any integer i $(1<i\leq r)$, an i-th primitive divisor polynomial of $f(x)$ over k is a first primitive divisor polynomial over k of an (i–1)-th primitive divisor polynomial of $f(x)$ over k.*

Now we assume that an element θ of k_s is not contained in k. Let α, η be two elements of k_s such that $|\theta-\eta|=\lambda_1(\theta, k)$, and $|\theta-\alpha|=\lambda_1(\theta, k)$, $[k(\alpha):k]=m_1(\theta, k)$. For any Galois extension F of k, we denote by $G(F/k)$ the Galois group of F over k. Suppose that F contains $k(\theta, \alpha, \eta)$.

We put $H=\{\sigma \in G(F/k) \mid |\theta-\theta^{\sigma}| \leq \lambda_1(\theta, k)\}$, then H is obviously a subgroups of $G(F/k)$. Let L be the subfield of F fixed by H. It is easy to see that L does not depend upon the choice of F. The notations α, η, L will keep these meanings throughout this section.

Proposition 4. *Let T be the maximal tamely ramified subextension of $k(\alpha)$ over k. Then we have*

$$T \subset L \subset k(\theta) \cap k(\eta).$$

Proposition 5. *For any element $\beta \neq 0$ of $k(\alpha)$, there exist elements $\gamma \in k(\theta)$, $\delta \in k(\eta)$ such that*

$$|\beta-\gamma|<|\beta|, \quad \textit{and} \quad |\beta-\delta|<|\beta|.$$

For any finite extension k' over k, we denote by $e(k'/k)$, $f(k'/k)$ the ramification index and the residue class degree of the extension k'/k, respectively.

The next proposition follows from Propositions 4 and 5.

Proposition 6. *We have*

$$e(k(\alpha)/k) \mid e(k(\theta)/k), \qquad f(k(\alpha)/k) \mid f(k(\theta)/k)$$

and

$$e(k(\alpha)/k) \mid e(k(\eta)/k), \qquad f(k(\alpha)/k) \mid f(k(\eta)/k).$$

Corollary 1. *Assume that the depth r of $f(x)$ is greater than 1. Then for any i $(1 \leq i \leq r)$ we have*

$$m_i(\theta, k) \mid m_{i-1}(\theta, k).$$

Corollary 2. *If $k(\theta)$ is tamely ramified over k, we have $L=k(\alpha)$.*

Remark. As we will see later, $k(\alpha)$ is not necessarily contained by $k(\theta)$, when $k(\theta)$ is not tamely ramified over k.

The following proposition is useful in numerical applications.

Proposition 7. *Let $f_i(x)$ be an i-th primitive divisor polynomial of $f(x)$ $(1 \leq i \leq r$,* where r is the depth of $f(x)$), *and let l_i be the natural number such that $l_i-1<\mathrm{ord}_{\mathfrak{y}}(f_i(\theta)) \leq l_i$. Then $f_i(x)$ is irreducible* mod $\mathfrak{y}^{l_i}$ *in* $\mathfrak{o}[x]$.

§ 2. The following theorem shows how we can construct divisor polynomials of $f(x)$ by means of the primitive divisor polynomials of $f(x)$.

Theorem 1. *Let r be the depth of $f(x)$, and $f_i(x)$ an i-th primitive divisor polynomial of $f(x)$ $(i=1, \cdots, r)$. For any integer m such that $1 \leq m<n$, we define uniquely a finite sequence $q_1(m), \cdots, q_r(m)$ of integers by the following conditions.*

$$m=\sum_{i=1}^{r} q_i(m) m_i(\theta, k), \quad \textit{and} \quad 0 \leq q_i(m)<\frac{m_{i-1}(\theta, k)}{m_i(\theta, k)}, \quad (i=1, \cdots, r).$$

Then $\prod_{i=1}^{r} f_i(x)^{q_i(m)}$ is a divisor polynomial of degree m of $f(x)$ over k.

Corollary. *Let $g_m(x)$ be a divisor polynomial of degree m of $f(x)$ over k. Put $\kappa_i=\mathrm{ord}_{\mathfrak{y}}(f_i(\theta))$ $(1 \leq i \leq r)$ and $\mu_m=\mathrm{ord}_{\mathfrak{y}}(g_m(\theta))$ $(1 \leq m<n)$. Then we have*

$$\sum_{m=1}^{n-1} \mu_m = \frac{n}{2} \sum_{i=1}^{r} \left(\frac{m_{i-1}(\theta, k)}{m_i(\theta, k)} - 1 \right) \cdot \kappa_i .$$

By this corollary and Theorem 3 in Part I, we have the following.

Proposition 8. *Let $D(1, \theta, \cdots, \theta^{n-1})$ be the discriminant of $\mathfrak{o}[\theta]$ over $\mathfrak{o}$ and $D(k(\theta)/k)$ the discriminant of $\mathfrak{o}_{k(\theta)}$ over $\mathfrak{o}$. Then we have*

$$\mathrm{ord}_{\mathfrak{P}} (D(k(\theta)/k)) = f \cdot (e-1) - n \sum_{i=1}^{r} \left(\frac{m_{i-1}(\theta, k)}{m_i(\theta, k)} - 1 \right) \cdot \kappa_i + \mathrm{ord}_{\mathfrak{P}} (D(1, \theta, \cdots, \theta^{n-1})).$$

In Part III, we will give an explicit construction of the primitive divisor polynomials from the given polynomial $f(x)$.

Reference

[1] K. Okutsu: Construction of integral basis. I. Proc. Japan Acad., **58A**, 47–49 (1982).