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 $[k(\alpha_i):k]=m_i(\theta, k)$ $(i=1,\dots,r)$.*

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 $k(\theta, \alpha, \eta)$.