13. Construction of Integral Basis. I

By Kōsaku OKUTSU
Department of Mathematics, Gakushuin University

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

Let $f(x)$ be a monic irreducible separable polynomial of degree n in $\mathfrak{o}[x]$, where $\mathfrak{o}$ is a principal ideal domain. Let k be the quotient field of $\mathfrak{o}$, and θ one of the roots of $f(x)$ in an algebraic closure of $\bar{k}$ of k. The purpose of this series of papers is to give an explicit formula for an $\mathfrak{o}$-basis of the integral closure $\mathfrak{o}_k$ of $\mathfrak{o}$ in $K=k(\theta)$. We begin with considering the "local case".

§ 1. Throughout this section, let $\mathfrak{o}$ be a discrete valuation ring with maximal ideal $\mathfrak{p}$, k its quotient field, and assume that k is complete under the valuation induced by $\mathfrak{p}$. Let π be a generator of $\mathfrak{p}$. We denote by $|\ \ |$ a fixed valuation on the algebraic closure $\bar{k}$ of k, which is an extension of the valuation corresponding to $\mathfrak{p}$. Let $f(x)$ be a monic irreducible separable polynomial in $\mathfrak{o}[x]$ of degree n, and θ one of the roots of $f(x)$ in $\bar{k}$. For a polynomial $h(x)=a_0x^m+\cdots+a_m$ in $\mathfrak{o}[x]$, we put $|h(x)|=\sup_{i=0,\dots,m}|a_i|$. Then we have the following

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

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

$$|g_m(\theta)|\leq\frac{|g(\theta)|}{|g(x)|}.$$

Definition. We will call any monic polynomial $g_m(x)$ with the property in the Proposition 1 a *divisor polynomial* of degree m of θ, or of $f(x)$. We put $\mu_m=\mathrm{ord}_{\mathfrak{p}}(g_m(\theta))$, and $\nu_m=[\mu_m]$, where $[\ \ ]$ is the Gauss symbol. ν_m will be called the *integrality index* of degree m of θ, or of $f(x)$. ($g_m(x)$ is not uniquely determined by θ and m, but it is clear that ν_m does not depend on the choice of $g_m(x)$.)

Theorem 1. *We denote by $\mathfrak{o}_k$ the valuation ring in $K=k(\theta)$. Let $g_m(x)$, ν_m be a divisor polynomial and the integrality index of degree m of θ $(m=1,2,\cdots,n-1)$, and put $g_0(x)=1$, $\nu_0=0$. Then we have $\mathfrak{o}_K=\sum_{m=0}^{n-1}\mathfrak{o}((g_m(\theta))/\pi^{\nu_m})$.*

Proof. For any $m=0,1,\cdots,n-1$ we have $|(g_m(\theta))/\pi^{\nu_m}|\leq 1$, so that $\sum_{m=0}^{n-1}\mathfrak{o}((g_m(\theta))/\pi^{\nu_m})\subset\mathfrak{o}_K$. As $\mathfrak{o}_K\subset\mathfrak{o}[\theta]/\pi^l$ for some positive integer l, there exists, for any element α of $\mathfrak{o}_K$, some polynomial $h(x)$ in $\mathfrak{o}[x]$ such that $\alpha=h(\theta)/\pi^l$, where the degree d of $h(x)$ is less than n. As $g_m(x)$ is monic, we can find $d+1$ elements $r_0,\cdots,r_d$ of $\mathfrak{o}$ such that $h(x)$