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 $|h(x)|=\sup_{i=0,\cdots,m}|a_i|$. 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 $h(x)$

$\sum_{m=0}^{d} r_m g_m(x)$. As $|h(\theta)|/|h(x)| \geq |g_d(\theta)|$, we have $|h(\theta)| \geq |r_d g_d(\theta)|$. Then $|h(\theta)/\pi^l| \leq 1$ implies $|(r_d/\pi^{l-\nu_d})\cdot(g_d(\theta)/\pi^{\nu_d})| \leq 1$. Put $t=\mathrm{ord}_\mathfrak{p}(r_d/\pi^{l-\nu_d})$. Now assume t is negative. As t is an integer, we have $t \leq -1$. Then $0 \leq \mathrm{ord}_\mathfrak{p}(g_d(\theta)/\pi^{\nu_d}) < 1$ implies $\mathrm{ord}_\mathfrak{p}((r_d/\pi^{l-\nu_d})\cdot(g_d(\theta)/\pi^{\nu_d})) < 0$ in contradiction with $r_d g_d(\theta)/\pi^l \in \mathfrak{o}_K$. Thus we have $r_d/\pi^{l-\nu_d} \in \mathfrak{o}$, and so $(\sum_{m=0}^{d-1} r_m g_m(\theta))/\pi^l \in \mathfrak{o}_K$. Repeating this argument, we obtain $r_m/\pi^{l-\nu_m} \in \mathfrak{o}$ for $m=0, \cdots, d-1$. Thus $\alpha \in \sum_{m=0}^{n-1} \mathfrak{o}(g_m(\theta)/\pi^{\nu_m})$. This proves the theorem.

§2. Denote the maximal ideal of $\mathfrak{o}_K$ with $\mathfrak{P}$, the residue class degree and the ramification index of $\mathfrak{P}$ over k with f, e, respectively. We shall show that f, e can be obtained from the knowledge of $\nu_1, \cdots, \nu_{n-1}$.

Put $S_m = \{t \mid 0 \leq t \leq n-1,\ \mu_t - [\mu_t] = \mu_m - [\mu_m]\}$ for any m with $0 \leq m \leq n-1$, and $\{0, 1, \cdots, n-1\} = S_{m_0} \cup S_{m_1} \cup \cdots \cup S_{m_l}$ (direct sum), and assume $\mu_{m_i} - [\mu_{m_i}] < \mu_{m_j} - [\mu_{m_j}]$ for any pair i, j with $0 \leq i < j \leq l$. Then we have,

Proposition 2. *For any m and $t \in S_m$, $(g_t(\theta)/\pi^{\nu_t})((g_m(\theta)/\pi^{\nu_m})^{-1})$ is an element of $\mathfrak{o}_K$ and $\{(g_t(\theta)/\pi^{\nu_t})((g_m(\theta)/\pi^{\nu_m})^{-1}) \bmod \mathfrak{P} \mid t \in S_m\}$ are linearly independent over $\mathfrak{o}/\mathfrak{p}$.*

Proposition 3. *For any j with $1 \leq j \leq l$*

$$\frac{g_{m_j}(\theta)}{\pi^{\nu_{m_j}}}\mathfrak{o}_K = \sum_{i=0}^{j-1} \sum_{t \in S_{m_i}} \mathfrak{o}\frac{g_t(\theta)}{\pi^{\nu_t - 1}} + \sum_{i=j}^{l} \sum_{t \in S_{m_i}} \mathfrak{o}\frac{g_t(\theta)}{\pi^{\nu_t}}.$$

We omit the proof of these propositions, which will be published elsewhere. The next theorem follows them easily.

Theorem 2. (i) *The number $l+1$ of distinct S_{m_i}'s is equal to e.*
(ii) *For any $i=0, 1, \cdots, e-1$, the number of elements of S_{m_i} is f.*
(iii) $\mu_{m_i} - [\mu_{m_i}] = i/e$ $(i=0, 1, \cdots, e-1)$.

Proof. From Propositions 3 follows

$$\mathfrak{o}_K = \sum_{i=0}^{j-1} \sum_{t \in S_{m_j}} \mathfrak{o}\pi \cdot \left(\frac{g_{m_j}(\theta)}{\pi^{\nu_{m_j}}}\right)^{-1} \frac{g_t(\theta)}{\pi^{\nu_t}} + \sum_{i=j}^{l} \sum_{t \in S_{m_i}} \mathfrak{o}\left(\frac{g_{m_i}(\theta)}{\pi^{\nu_{m_j}}}\right)^{-1} \cdot \frac{g_t(\theta)}{\pi^{\nu_t}}$$

for any j with $1 \leq j \leq l$. So it follows from Proposition 2 that

$$\left\{\left(\frac{g_{m_j}(\theta)}{\pi^{\nu_{m_j}}}\right)^{-1} \frac{g_t(\theta)}{\pi^{\nu_t}} \bmod \mathfrak{P} \mid t \in S_{m_j}\right\}$$

is a base of the vector space $\mathfrak{o}_K/\mathfrak{P}$ over $\mathfrak{o}/\mathfrak{p}$. Thus the number of elements of S_{m_j} should be equal to f. As $n = e \cdot f$, we have $l = e-1$. And as $0 \leq \mu_{m_i} - [\mu_{m_i}] < 1$, $e(\mu_{m_i} - [\mu_{m_i}])$ is a natural number, and as $\mu_{m_i} - [\mu_{m_i}] \neq \mu_{m_j} - [\mu_{m_j}]$ for any pair $i \neq j$, we obtain $\mu_{m_i} - [\mu_{m_i}] = i/e$. This proves the theorem.

On the discriminant of $\mathfrak{o}_K$, we obtain the following.

Theorem 3. *Let $D(1, \theta, \cdots, \theta^{n-1})$ be the discrimiant of $\mathfrak{o}[\theta]$ and $D_{K/k}$ the discriminant of $\mathfrak{o}_K$ over k. Then*

$$D_{K/k} = \pi^{-2(\sum_{m=1}^{n-1} \nu_m)} D(1, \theta, \cdots, \theta^{n-1}).$$
$$= \pi^{f\cdot(e-1) - 2\sum_{m=1}^{n-1} \mu_m} D(1, \theta, \cdots, \theta^{n-1}).$$

In Part II, we will give an explicit construction of the divisor polynomial $f(x)$.

References

[1] Berwick, W. E. H.: Integral basis. Cambridge Tracts in Mathematics and Mathematical Physics, 22 (1927).

[2] Zassenhaus, Hans: Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung, Funktionalanalysis, Approximationstheorie. Numerische Mathematik (Oberwolfach, 1965), pp. 90–103, Birkhäuser, Basel (1967).