32. *Construction of Integral Basis. III*

By Kōsaku OKUTSU
Department of Mathematics, Gakushuin University

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

Let $\mathfrak{o}$ be a complete discrete valuation ring with the maximal ideal $\mathfrak{p}=\pi\mathfrak{o}$, k its quotient field, $f(x)$ a monic irreducible separable polynomial in $\mathfrak{o}[x]$ with degree n and θ a root of $f(x)$ in an algebraic closure $\bar{k}$ of k. In Part II, we have defined *primitive divisor polynomials* (p.d.p.) $f_1(x), f_2(x), \cdots, f_r(x)$ of θ, by means of which we have given an integral basis of $K=k(\theta)$ explicitly. We have denoted the degree of $f_i(x)$ by $m_i(\theta, k)$ $(i=1, \cdots, r)$. As we consider $\mathfrak{o}$, k, $f(x)$, and θ as fixed in this part, we shall write simply m_i for $m_i(\theta, k)$. We know $m_r=1$, $m_0=n$, and $m_i \mid m_{i-1}$ $(i=1, \cdots, r)$.

Now we shall give a construction of these p.d.p. $f_i(x)$, $i=1, \cdots, r$.

We begin with "last p.d.p." $f_r(x)$ of degree 1, and proceed retrogressively: We shall obtain $f_{i-1}(x)$ from $f_r(x), f_{r-1}(x), \cdots, f_i(x)$. $f_r(x)$ can be obtained as follows.

We fix a complete set of representatives V of $\mathfrak{o}$ mod $\mathfrak{p}$. By Hensel's lemma there exists a unique polynomial $g(x)$ in $\mathfrak{o}[x]$ with coefficients in V which is irreducible mod $\mathfrak{p}$ and $f(x)\equiv g(x)^s$ mod $\mathfrak{p}$ where $s=\deg f/\deg h$. $g(x)$ will be called the *irreducible component of* $f(x)$ mod $\mathfrak{p}$. If its degree is greater than 1, then any monic polynomial with degree 1, for example x, is a last p.d.p. If $g(x)$ is linear, put $g(x)=x-c_0$ $(c_0\in V)$. It is clear that $\mathrm{ord}_{\mathfrak{p}}(\theta-c_0)=(\mathrm{ord}_{\mathfrak{p}}(f(c_0)))/n$. When $n\nmid \mathrm{ord}_{\mathfrak{p}}(f(c_0))$, $x-c_0$ is a last p.d.p. When $n\mid \mathrm{ord}_{\mathfrak{p}}(f(c_0))$, put $F_0(x)=f(x)$, $t_1=(\mathrm{ord}_{\mathfrak{p}}(F_0(c_0)))/n$, and $F_1(x)=\sum_{i=0}^{n}((F_0^{(i)}(c_0))/i!\,\pi^{t_1(n-i)})x^i$. Then $F_1(x)$ is shown to be a monic polynomial in $\mathfrak{o}[x]$.

Let $g_1(x)$ be the irreducible component of $F_1(x)$ mod $\mathfrak{p}$. If $\deg g_1(x)>1$, then $x-c_0$ is a last p.d.p. If $g_1(x)$ is linear and equal to $x-c_1$ then consider $(\mathrm{ord}_{\mathfrak{p}}(F_1(c_1)))/n=t_2$. If $t_2\notin N$, then $x-(c_0+c_1\pi^{t_1})$ is a last p.d.p. If $t_2\in N$, then we define $F_2(x)$ from $F_1(x)$ just as we have defined $F_1(x)$ from $F_0(x)$. We may obtain a last p.d.p. of the form $x-(c_0+c_1\pi^{t_1}+c_2\pi^{t_1+t_2})$, or we should continue further in the same way. This procedure ends after a finite number of steps.

Let α_i be a root of $f_i(x)$ in $\bar{k}$ and let e_i, f_i be the ramification index, the residue class degree of the extension $k(\alpha_i)$ over k $(i=0, 1, \cdots, r)$. We fix i $(1<i\leq r)$, and assume that $f_i(x), f_{i+1}(x), \cdots, f_r(x)$ are already obtained. Then the following propositions give e_{i-1}, f_{i-1}, and finally the theorem will determine $f_{i-1}(x)$.

Proposition 1. *We put* $l_i/t_i=\mathrm{ord}_\mathfrak{p}(f_i(\theta))$ *where* l_i, t_i *are natural numbers such that* $(l_i, t_i)=1$ *for* $i=1, \cdots, r-1$, *and for* $i=r$ *when* $\mathrm{ord}_\mathfrak{p}(f_r(\theta))>0$. *If* $\mathrm{ord}_\mathfrak{p}(f_r(\theta))=0$, *we put* $l_r=0$, $t_r=1$. *Then* e_{i-1} *coincides with the least common multiple of* $t_i, t_{i+1}, \cdots, t_r$ $(1\leq i\leq r)$.

Now let m be any integer such that $1\leq m<n$. We put $H_{i,m}(x)=f_i(x)^l \sum_{j=i+1}^{r} f_j(x)^{q_j(m)}$ where $l=[m/m_i]$, and $g_j(m)$ $(j=1, \cdots, r)$ are integers defined in Theorem 1 of Part II, satisfying $0\leq q_i(m)<m_{j-1}/m_j$ $(j=1, \cdots, r)$ and $m=\sum_{j=1}^{r} q_j(m)m_j$. Then the degree of $H_{i,m}(x)$ is equal to m.

Proposition 2. *The notations being as above, we put* $\mu_{i,m}=\mathrm{ord}_\mathfrak{p}(H_{i,m}(\theta))$, *and* $S_0^i=\{m(0\leq m<n)\mid \mu_{i,m}=[\mu_{i,m}]\}$ $(1\leq i\leq r)$. *Then the residue class degree* f_{i-1} *of the extension* $k(\alpha_{i-1})$ *over* k *is equal to the dimension of the vector space over* $\mathfrak{o}/\mathfrak{p}$ *generated by the set* $\{(H_{i,m}(\theta)/\pi^{[\mu_{i,m}]}) \bmod \mathfrak{P}\mid m\in S_0^i\}$ *where* $\mathfrak{P}$ *is the maximal ideal of* $\mathfrak{o}_K$. (An algorithm can be given to compute this dimension from $f(x)$.)

We put $S_t^i=\{m\in\{0,1,\cdots,n-1\}\mid \mu_{i,m}-[\mu_{i,m}]=t/e_{i-1}\}$ $(t=0,1,\cdots, e_{i-1}-1)$. Then we have $S_t^i\neq\phi$ for any i $(1\leq i\leq r)$, and t $(0\leq t<e_{i-1})$, and we have $\{0,1,\cdots,n-1\}=S_0^i\cup S_1^i\cup\cdots\cup S_{e_{i-1}-1}^i$ (direct sum). Now we will define a sequence $\{F_{i-1,j}(x)\}_{j=0,1,\ldots}$ of monic polynomials with degree m_{i-1} as follows. We put $F_{i-1,0}(x)=f_i(x)^{d_i}$ where $d_i=m_{i-1}/m_i$, and put $\Lambda_{i-1,0}=\mathrm{ord}_\mathfrak{p}(F_{i-1,0}(\theta))$. Assume $F_{i-1,j-1}(x)$ has been defined. Then we put $\Lambda_{i-1,j-1}=\mathrm{ord}_\mathfrak{p}(F_{i-1,j-1}(\theta))$. For any m $(1\leq m<m_{i-1})$, let $H_{i,m}(x)=\prod_{k=i}^{r} f_k(x)^{q_k(m)}$ and $\mu_{i,m}=\mathrm{ord}_\mathfrak{p}(H_{i,m}(\theta))$ as above. First we assume that next two conditions (i), (ii) are satisfied.

(i) $\Lambda_{i-1,j-1}-[\Lambda_{i-1,j-1}]=\dfrac{t}{e_{i-1}}$ for some $t\in N$ $(0\leq t<e_{i-1})$.

(ii) $\left(\dfrac{H_{i,m_0}(\theta)}{\pi^{[\mu_{i,m_0}]}}\right)^{-1}\left(\dfrac{F_{i-1,j-1}(\theta)}{\pi^{[\Lambda_{i-1,j-1}]}}\right) \bmod \mathfrak{P}$ is contained in the vector space over $\mathfrak{o}/\mathfrak{p}$ generated by the set

$$\left\{\left(\frac{H_{i,m_0}(\theta)}{\pi^{[\mu_{i,m_0}]}}\right)^{-1}\left(\frac{H_{i,m}(\theta)}{\pi^{[\mu_{i,m}]}}\right) \bmod \mathfrak{P}\mid m\in S_t^i \text{ and } 0\leq m<m_{i-1}\right\}$$

where m_0 is some element of S_t^i such that $0\leq m_0<m_{i-1}$.
In this case we define

$$F_{i-1,j}(x)=F_{i-1,j-1}(x)-\sum_{\substack{m\in S_t^i\\ 0\leq m<m_{i-1}}} a_m\pi^{[\Lambda_{i-1,j-1}]-[\mu_{i,m}]}H_{i,m}(x)$$

where a_m $(m\in S_t^i, 0\leq m<m_{i-1})$ are elements of $V(\subset\mathfrak{o})$ which are uniquely determined by the condition:

$$\left(\frac{H_{i,m_0}(\theta)}{\pi^{[\mu_{i,m_0}]}}\right)^{-1}\left(\frac{F_{i-1,j-1}(\theta)}{\pi^{[\Lambda_{i-1,j-1}]}}\right)\equiv \sum_{\substack{m\in S_t^i\\ 0\leq m<m_{i-1}}} a_m\left(\frac{H_{i,m_0}(\theta)}{\pi^{[\mu_{i,m_0}]}}\right)^{-1}\left(\frac{H_{i,m}(\theta)}{\pi^{[\mu_{i,m}]}}\right) \pmod{\mathfrak{P}}.$$

When one of the above conditions (i), (ii) is not satisfied, we put $F_{i-1,j}(x)=F_{i-1,j-1}(x)$.

Theorem 1. *The notations being as above, there exists some natural number s such that* $F_{i-1,s}(x)=F_{i-1,s+1}(x)$. *For this s,* $F_{i-1,s}(x)$ *is an* $(i-1)$*-th primitive divisor polynomial of* θ *over* k.

In Part IV we will give an explicit formula for an integral basis when $\mathfrak{o}$ is a principal ideal domain.

Reference

[1] K. Okutsu: Construction of integral basis I; II. Proc. Japan Acad., **58**A, 47–49; 87–89 (1982).