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 $\mathfrak{o} \bmod \mathfrak{p}$. 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 $f(x)\equiv g(x)^s \bmod \mathfrak{p}$ 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 $f_{i-1}(x)$.