TOKYO J. MATH.
VOL. 11, NO. 2, 1988

A Note on Ideal Bases

Fuminori KAWAMOTO

Gakushuin University

§ 1. Construction of ideal bases.

In Okutsu [2], integral bases of finite separable extensions of quotient fields of Dedekind domains were obtained in terms of "divisor polynomials" introduced there. The purpose of this note is to generalize this result to ideal bases. In § 2, we shall give an example which illustrates this result.

Let $\mathfrak{o}$ be a Dedekind domain with the quotient field k and $f(x)$ a monic irreducible separable polynomial of degree n in $\mathfrak{o}[x]$. Let θ be one of the roots of $f(x)$ in an algebraic closure $\bar{k}$ of k. Let $K=k(\theta)$ and assume that $\mathfrak{A}$ is a fixed non-zero ideal of K throughout this section. Let $\{\mathfrak{p}_\lambda\}_{\lambda\in\Lambda}$ be the set of all prime ideals of $\mathfrak{o}$, k_λ a completion of k with respect to $\mathfrak{p}_\lambda$, and $\mathfrak{o}_\lambda$ its valuation ring. Fixing an embedding of k in k_λ, we assume that k is a subfield of k_λ. Let $\bar{k}_\lambda$ be an algebraic closure of k_λ. We denote by $\varphi_\lambda(\ )$ (or $\varphi_{\mathfrak{p}_\lambda}(\ )$) the exponential valuation on $\bar{k}_\lambda$ which is the unique extension of the $\mathfrak{p}_\lambda$-adic valuation of k. For each $\lambda\in\Lambda$, let $f(x)=\prod_{i=1}^{s_\lambda} f_{\lambda,i}(x)$ be a factorization of $f(x)$ in $k_\lambda[x]$, where $f_{\lambda,i}(x)$ is a monic irreducible polynomial in $\mathfrak{o}_\lambda[x]$. For simplicity, we will write s for s_λ in some cases. Let $\theta_{\lambda,i}$ be one of the roots of $f_{\lambda,i}(x)$ in $\bar{k}_\lambda$. We define a k-isomorphism $\iota_{\lambda,i}$ from $K=k(\theta)$ into $\bar{k}_\lambda$ by putting $\iota_{\lambda,i}(\theta)=\theta_{\lambda,i}$. Let $\iota_{\lambda,i}(\mathfrak{A})=\mathfrak{A}\mathfrak{o}_{k_\lambda(\theta_{\lambda,i})}$ which is an ideal of $k_\lambda(\theta_{\lambda,i})$ where $\mathfrak{o}_{k_\lambda(\theta_{\lambda,i})}$ is the valuation ring of $k_\lambda(\theta_{\lambda,i})$. For each $\lambda\in\Lambda$, we define a rational-valued and ∞-valued function $\Phi_\lambda(\ )$ on K as follows:

$$\Phi_\lambda(\alpha)=\min_{1\le i\le s_\lambda}\{\varphi_\lambda(\iota_{\lambda,i}(\alpha))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))\} \qquad (\alpha\in K)\ .$$

Then we note that α is an element of $\mathfrak{A}$ if and only if $\Phi_\lambda(\alpha)\geqq 0$ for any $\lambda\in\Lambda$. For a polynomial $g(x)=a_0x^m+\cdots+a_m$ in $\mathfrak{o}[x]$, we put

$$\varphi_\lambda(g(x))=\min_{0\le j\le m}\varphi_\lambda(a_j)\ .$$

PROPOSITION 1. *For each $\lambda\in\Lambda$ and any positive integer m ($<n$), there*

Received August 18, 1987

exists a monic polynomial $g_{\lambda,m}(x)$ *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*

$$\Phi_\lambda(g_{\lambda,m}(\theta))\geqq\Phi_\lambda(g(\theta))-\varphi_\lambda(g(x))\ .$$

PROOF. Let $\lambda\in\Lambda$ and $1\leqq m<n$ be fixed. Let $a\in\mathfrak{o}$ such that $\varphi_\lambda(a)=\varphi_\lambda(g(x))$. Then $g(x)/a$ is the polynomial in $\mathfrak{o}_\lambda[x]$ and consider the factorization of it into irreducible factors. $g(x)/a$ may be decomposed in $\mathfrak{o}_\lambda[x]$ as $H(x)G(x)$, where $H(x)$ is a monic polynomial in $\mathfrak{o}_\lambda[x]$, and $G(x)$ is a polynomial in $\mathfrak{o}_\lambda[x]$ without integral roots. Since $G(0)$ is a unit of $\mathfrak{o}_\lambda$, $\varphi_\lambda(\theta_{\lambda,i})\geqq 0$ implies $\varphi_\lambda(G(\theta_{\lambda,i}))=0$ for any i $(1\leqq i\leqq s)$. Consequently we have $\varphi_\lambda(M(\theta_{\lambda,i}))\geqq\varphi_\lambda(G(\theta_{\lambda,i}))$ for any monic polynomial $M(x)$ in $\mathfrak{o}_\lambda[x]$ such that $\deg M(x)=\deg G(x)$ and for all i. Thus

$$\Phi_\lambda(H(\theta)M(\theta))\geqq\Phi_\lambda(H(\theta)G(\theta))=\Phi_\lambda(g(\theta))-\varphi_\lambda(g(x))\ ,$$

where $H(x)M(x)$ is a monic polynomial of degree m in $\mathfrak{o}_\lambda[x]$. Since $m<n$ and $f(x)$ is separable, we have $\Phi_\lambda(H(\theta)M(\theta))<\infty$. So we may assume that $H(\theta_{\lambda,i})M(\theta_{\lambda,i})$ is non-zero if $1\leqq i\leqq r$, and is zero if $r<i\leqq s$. Let c be a positive integer such that

$$c>\varphi_\lambda(H(\theta_{\lambda,i})M(\theta_{\lambda,i}))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))+\max_{1\leqq u\leqq s}\varphi_\lambda(\iota_{\lambda,u}(\mathfrak{A}))$$

for any i $(1\leqq i\leqq r)$. Let $h(x)$ be a monic polynomial of degree m in $\mathfrak{o}[x]$ satisfying $h(x)\equiv H(x)M(x) \bmod \mathfrak{p}_\lambda^c$. Then we have $\varphi_\lambda(h(\theta_{\lambda,i})-H(\theta_{\lambda,i})M(\theta_{\lambda,i}))\geqq c$ $(1\leqq i\leqq s)$. Therefore if $1\leqq i\leqq r$, by the definition of c, we have $\varphi_\lambda(h(\theta_{\lambda,i}))=\varphi_\lambda(H(\theta_{\lambda,i})M(\theta_{\lambda,i}))$, so that

$$\varphi_\lambda(h(\theta_{\lambda,i}))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))=\varphi_\lambda(H(\theta_{\lambda,i})M(\theta_{\lambda,i}))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))\ .$$

If $r<j\leqq s$,

$$\begin{aligned}\varphi_\lambda(h(\theta_{\lambda,j}))-\varphi_\lambda(\iota_{\lambda,j}(\mathfrak{A}))&\geqq c-\varphi_\lambda(\iota_{\lambda,j}(\mathfrak{A}))\\&>\varphi_\lambda(H(\theta_{\lambda,i})M(\theta_{\lambda,i}))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))\end{aligned}$$

for any i $(1\leqq i\leqq r)$. Hence

$$\Phi_\lambda(h(\theta))=\Phi_\lambda(H(\theta)M(\theta))\ .$$

So we have to show that the set of rational numbers $\{\Phi_\lambda(h(\theta))\mid h(x)$ is a monic polynomial of degree m in $\mathfrak{o}[x]\}$ has the maximum value. It follows from the facts that $\varphi_\lambda(\ )$ is a discrete valuation and $\Phi_\lambda(h(\theta))<\infty$ by the same reason as above. This proves our proposition.

DEFINITION. We will call a monic polynomial $g_{\lambda,m}(x)$ with the property in Proposition 1 a *divisor polynomial* of degree m of θ and $\mathfrak{A}$ for $\mathfrak{p}_\lambda$. We put $\mu_{\lambda,m}=\Phi_\lambda(g_{\lambda,m}(\theta))$ and $\nu_{\lambda,m}=[\mu_{\lambda,m}]$, where $[x]$ is the greatest integer $\leqq x$ as usual. $\nu_{\lambda,m}$ will be called the *integrality index* of degree m of θ and $\mathfrak{A}$ for $\mathfrak{p}_\lambda$ (it follows from the above proof that $\mu_{\lambda,m}$ and $\nu_{\lambda,m}$ do not depend on the choice of $g_{\lambda,m}(x)$).

PROPOSITION 2. *We put* $\Lambda_0=\{\lambda\in\Lambda \mid \mathfrak{p}_\lambda$ *is a prime divisor of* $d(f)$ *or* $N_{K/k}\mathfrak{A}\}$, *where* $d(f)=(-1)^{n(n-1)/2}N_{K/k}(f'(\theta))$ *and* $f'(x)$ *denotes the derivative of* $f(x)$. *If* $\lambda\notin\Lambda_0$, *then we have* $\Phi_\lambda(g(\theta))=0$ *for any* m $(1\leqq m<n)$ *and for any monic polynomial* $g(x)$ *of degree* m *in* $\mathfrak{o}[x]$. *In particular,* $\mu_{\lambda,m}=\nu_{\lambda,m}=0$.

PROOF. For any i $(1\leqq i\leqq s)$, we put $u_i=\max\{\varphi_\lambda(\theta_{\lambda,i}-\theta_{\lambda,i}{}^\sigma) \mid \sigma: k_\lambda$-isomorphism on $\bar{k}_\lambda$ such that $\theta_{\lambda,i}{}^\sigma\neq\theta_{\lambda,i}\}$, and $v_i=\max\{\varphi_\lambda(\theta_{\lambda,i}-\theta_{\lambda,i'}{}^\sigma) \mid 1\leqq i'\leqq s$ and $i'\neq i$, $\sigma: k_\lambda$-isomorphism on $\bar{k}_\lambda\}$. Then there is some i_0 $(1\leqq i_0\leqq s)$ such that $\varphi_\lambda(g(\theta_{\lambda,i_0}))\leqq\max\{mu_{i_0}, mv_{i_0}\}$. Though this fact is shown in Okutsu [2], its proof will be recalled here for the sake of completeness. Let $g(x)=\prod_{j=1}^{t}g_j(x)$ be an irreducible decomposition in $\mathfrak{o}_\lambda[x]$ and γ_j a root of $g_j(x)$ in $\bar{k}_\lambda$. For any i $(1\leqq i\leqq s)$ and any j $(1\leqq j\leqq t)$, we put $w_{i,j}=\max\{\varphi_\lambda(\theta_{\lambda,i}-\gamma_j{}^\sigma) \mid \sigma: k_\lambda$-isomorphism on $\bar{k}_\lambda\}$. Now, for any i $(1\leqq i\leqq s)$, we assume that there is some $j(i)$ $(1\leqq j(i)\leqq t)$ such that $w_{i,j(i)}>\max\{u_i, v_i\}$. Put $w_{i,j(i)}=\varphi_\lambda(\theta_{\lambda,i}-\gamma_{j(i)}{}^\sigma)$. Since $w_{i,j(i)}>u_i$ and $\theta_{\lambda,i}$ is separable over $k_\lambda(\gamma_{j(i)}{}^\sigma)$, by Krasner's lemma (cf. [1]), we have $k_\lambda(\theta_{\lambda,i})\subset k_\lambda(\gamma_{j(i)}{}^\sigma)$, so that $\deg f_{\lambda,i}(x)\leqq\deg g_{j(i)}(x)$. On the other hand, if $j(i)=j(i')$, then we have $i=i'$ for the following reason. Put $w_{i',j(i')}=\varphi_\lambda(\theta_{\lambda,i'}-\gamma_{j(i')}{}^{\sigma'})$ and assume $v_i\leqq v_{i'}$. Then $\varphi_\lambda(\theta_{\lambda,i}-\theta_{\lambda,i'}{}^{\sigma\sigma'^{-1}})=\varphi_\lambda(\theta_{\lambda,i}{}^{\sigma^{-1}}-\theta_{\lambda,i'}{}^{\sigma'^{-1}})\geqq\min\{w_{i,j(i)}, w_{i',j(i')}\}>v_i$. So we have $i=i'$ by the definition of v_i. Consequently

$$n=\deg f(x)\leqq\sum_{i=1}^{s}\deg g_{j(i)}(x)\leqq\deg g(x)=m\ .$$

This is impossible. Hence there is some i_0 $(1\leqq i_0\leqq s)$ such that $w_{i_0,j}\leqq\max\{u_{i_0}, v_{i_0}\}$ for any j $(1\leqq j\leqq t)$. Thus we get $\varphi_\lambda(g(\theta_{\lambda,i_0}))\leqq\max\{mu_{i_0}, mv_{i_0}\}$. Therefore

$$\begin{aligned}\Phi_\lambda(g(\theta))&\leqq\varphi_\lambda(g(\theta_{\lambda,i_0}))-\varphi_\lambda(\iota_{\lambda,i_0}(\mathfrak{A}))\\&\leqq\max\{mu_{i_0}, mv_{i_0}\}-\min_{1\leqq t\leqq s}\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))\ .\end{aligned}$$

Hence

$$(*)\qquad \Phi_\lambda(g(\theta))\leqq\max_{1\leqq i\leqq s}\{mu_i, mv_i\}-\min_{1\leqq i\leqq s}\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))$$

for any monic polynomial $g(x)$ of degree m in $\mathfrak{o}[x]$. Then our hypothesis yields $u_i=v_i=0$ and $\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))=0$ for any i $(1\leqq i\leqq s)$. So we have $\Phi_\lambda(g(\theta))=0$ by $(*)$ and the definition of $\Phi_\lambda(\ )$. The proof is completed.

THEOREM 1. *The notations being as above, for any positive integer m $(<n)$, let $g_m(x)$ be a monic polynomial of degree m in $\mathfrak{o}[x]$ satisfying $g_m(x)\equiv g_{\lambda,m}(x) \bmod \mathfrak{p}_\lambda^{[\mu_{\lambda,m}+\alpha_\lambda]+1}$ for any $\lambda\in\Lambda_0$, where we put $\alpha_\lambda=\max_{1\leqq i\leqq s_\lambda}\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))$ for any $\lambda\in\Lambda$. Then we have*

$$\mathfrak{A}=\mathfrak{b}_0\oplus\bigoplus_{m=1}^{n-1}\mathfrak{b}_m^{-1}g_m(\theta)$$

where we put $\mathfrak{b}_0=\mathfrak{A}\cap k$ and $\mathfrak{b}_m=\prod_{\lambda\in\Lambda}\mathfrak{p}_\lambda^{\nu_{\lambda,m}}$.

REMARK 1. We can write $\mathfrak{b}_0=\prod_{\lambda\in\Lambda}\mathfrak{p}_\lambda^{e_\lambda}$, where e_λ is the least integer $\geqq\alpha_\lambda$.

PROOF OF THEOREM 1. By Proposition 2, $g_m(x)$ is a divisor polynomial of degree m for $\mathfrak{p}_\lambda$ for any $\lambda\notin\Lambda_0$. We shall show that $g_m(x)$ is also a divisor polynomial of degree m for $\mathfrak{p}_\lambda$ for any $\lambda\in\Lambda_0$. By the definition of $g_m(x)$, we have $\varphi_\lambda(g_m(\theta_{\lambda,i})-g_{\lambda,m}(\theta_{\lambda,i}))\geqq[\mu_{\lambda,m}+\alpha_\lambda]+1>\mu_{\lambda,m}+\alpha_\lambda$ for any i $(1\leqq i\leqq s)$. Consequently for any i

$$\begin{aligned}&\varphi_\lambda(g_m(\theta_{\lambda,i}))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))\\&\quad\geqq\min\{\varphi_\lambda(g_{\lambda,m}(\theta_{\lambda,i})),\ \mu_{\lambda,m}+\alpha_\lambda\}-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A}))\\&\quad\geqq\min\{\varphi_\lambda(g_{\lambda,m}(\theta_{\lambda,i}))-\varphi_\lambda(\iota_{\lambda,i}(\mathfrak{A})),\ \mu_{\lambda,m}\}\\&\quad=\mu_{\lambda,m}\ .\end{aligned}$$

Therefore we have $\Phi_\lambda(g_m(\theta))\geqq\Phi_\lambda(g_{\lambda,m}(\theta))$. As $g_{\lambda,m}(x)$ is a divisor polynomial, we have $\Phi_\lambda(g_m(\theta))=\Phi_\lambda(g_{\lambda,m}(\theta))$ and $g_m(x)$ is a divisor polynomial of degree m for $\mathfrak{p}_\lambda$ for any $\lambda\in\Lambda_0$. Consequently $\Phi_\lambda(\mathfrak{b}_m^{-1}g_m(\theta))=\Phi_\lambda(g_m(\theta))-\nu_{\lambda,m}\geqq0$ for any $\lambda\in\Lambda$, so that $\mathfrak{b}_m^{-1}g_m(\theta)\subset\mathfrak{A}$ $(1\leqq m<n)$. Conversely, let α be an element of $\mathfrak{A}$. Then there are an element c of $\mathfrak{o}$ and a polynomial $h(x)$ in $\mathfrak{o}[x]$ such that $\alpha=h(\theta)/c$ and $\deg h(x)<n$. Since $g_m(x)$ $(1\leqq m<n)$ are monic polynomials of degree m, we can write $h(x)=\sum_{m=0}^{t}a_mg_m(x)$ with some elements a_m's of $\mathfrak{o}$, where we put $g_0(x)=1$ and $t=\deg h(x)$. For any $\lambda\in\Lambda$, $\mu_{\lambda,t}\geqq\Phi_\lambda(h(\theta))-\varphi_\lambda(h(x))\geqq\Phi_\lambda(h(\theta))-\varphi_\lambda(a_t)$. Therefore $\varphi_\lambda(a_t/c)+\mu_{\lambda,t}\geqq\Phi_\lambda(\alpha)\geqq0$ by $\alpha\in\mathfrak{A}$, so $\varphi_\lambda(a_t/c)\geqq-\nu_{\lambda,t}$ for any $\lambda\in\Lambda$. Hence we have $a_t/c\in\mathfrak{b}_t^{-1}$. Repeating this process, we have $a_m/c\in\mathfrak{b}_m^{-1}$ for any m $(1\leqq m\leqq t)$. Then we have $a_0/c\in\mathfrak{b}_0$. Furthermore $\{g_m(\theta)\}_{m=0,\cdots,n-1}$ is linearly independent over k, because $g_m(x)$ is a polynomial of degree m. This proves our theorem.

REMARK 2. For some m $(1\leqq m<n)$ and $\lambda\in\Lambda_0$, assume that $\Phi_\lambda(h(\theta))\geqq\nu_{\lambda,m}$

for any monic polynomial $h(x)$ of degree m in $\mathfrak{o}[x]$ (for example, if $\alpha_\lambda=0$ and $\nu_{\lambda,m}=0$ for some m and $\lambda\in\Lambda_0$, we have $\Phi_\lambda(h(\theta))\geqq 0=\nu_{\lambda,m}$ for any $h(x)$). Then it is easy to see from the first part of above proof that we do not have to solve the simultaneous congruences as in Theorem 1 for these m and λ.

§ 2. An example.

In this section, we will use the same notations as in the previous section. Let $\boldsymbol{Z}$, $\boldsymbol{Z}_p$, $\boldsymbol{Q}$, and $\boldsymbol{Q}_p$ denote the ring of rational integers, the ring of p-adic integers, the field of rational numbers, and the field of p-adic numbers respectively where p is a prime. Let l be an odd prime and $K=\boldsymbol{Q}(\zeta)$ where ζ is a fixed primitive l-th root of unity. Let $f(x)=x^{l-1}+\cdots+x+1$ and $1\leqq m\leqq l-2$. We note that l is the only prime divisor of $d(f)$ and $\varphi_l(\zeta^i-\zeta^j)=1/(l-1)$ $(i\neq j)$. Suppose that n is a rational integer. Since $f(x+1)$ is of Eisenstein type for l, $f(x)$ is irreducible in $\boldsymbol{Z}_l[x]$. We define a $\boldsymbol{Q}$-isomorphism ι from K into $\bar{\boldsymbol{Q}}_l$ by putting $\iota(\zeta)=\zeta$. Let $\mathfrak{l}=\{\alpha\in\mathfrak{o}_K \mid \varphi_l(\iota(\alpha))>0\}$, where $\mathfrak{o}_K$ is the ring of integers in K. $\mathfrak{l}$ is a unique prime ideal lying above l in K, generated by $\zeta-1$. By $(*)$, we have $\varphi_l(g(\zeta))-\varphi_l(\iota(\mathfrak{l}^n))\leqq(m-n)/(l-1)=\varphi_l((\zeta-1)^m)-\varphi_l(\iota(\mathfrak{l}^n))$ for any monic polynomial $g(x)$ of degree m in $\boldsymbol{Z}[x]$. Consequently $(x-1)^m$ and $[(m-n)/(l-1)]$ are a divisor polynomial and the integrality index of degree m of ζ and $\mathfrak{l}^n$ for l. Hence we have by Theorem 1

$$\mathfrak{l}^n=\bigoplus_{m=0}^{l-2}\boldsymbol{Z}l^{-[(m-n)/(l-1)]}(\zeta-1)^m\ .$$

Suppose that p is a prime number such that $p\equiv 1 \bmod l$. Then since ζ is an element of $\boldsymbol{Z}_p$, $f(x)=\prod_{i=1}^{l-1}(x-\zeta^i)$ is the irreducible decomposition in $\boldsymbol{Z}_p[x]$. For each i $(1\leqq i\leqq l-1)$, we define a $\boldsymbol{Q}$-isomorphism ι_i from K into $\bar{\boldsymbol{Q}}_p$ by putting $\iota_i(\zeta)=\zeta^i$. Let $\mathfrak{p}_i=\{\alpha\in\mathfrak{o}_K \mid \varphi_p(\iota_i(\alpha))>0\}$. Then $\mathfrak{p}_1,\cdots,\mathfrak{p}_{l-1}$ are all prime ideals lying above p in K. Suppose that n is a positive integer and let $1\leqq i\leqq l-1$. Then there exists an element a_i of $\boldsymbol{Z}$ satisfying $a_i\equiv\zeta^i \bmod p^n\boldsymbol{Z}_p$. Consequently $\varphi_p(a_i-\zeta^i)\geqq n$ and since $\varphi_p(\zeta^i-\zeta^j)=0$, $\varphi_p(a_i-\zeta^j)=0$ $(j\neq i)$. By $(*)$, we have

$$\begin{aligned}&\min_{1\leqq j\leqq l-1}\{\varphi_p(g(\zeta^j))-\varphi_p(\iota_j(\mathfrak{p}_i^n))\}\\ &\quad\leqq 0=\min_{1\leqq j\leqq l-1}\{\varphi_p((\zeta^j-a_i)^m)-\varphi_p(\iota_j(\mathfrak{p}_i^n))\}\end{aligned}$$

for any monic polynomial $g(x)$ of degree m in $\boldsymbol{Z}[x]$. Hence $(x-a_i)^m$ and 0 are a divisor polynomial and the integrality index of degree m of ζ

and $\mathfrak{p}_i^n$ for p. Furthermore $(x-1)^m$ and $[m/(l-1)]=0$ are a divisor polynomial and the integrality index of degree m of ζ and $\mathfrak{p}_i^n$ for l. Since $\varphi_l(\iota(\mathfrak{p}_i^n))=0$ and $[m/(l-1)]=0$, by Theorem 1 and Remark 2, we have

$$\mathfrak{p}_i^n = \boldsymbol{Z}p^n \oplus \bigoplus_{m=1}^{l-2} \boldsymbol{Z}(\zeta-a_i)^m \qquad (1\leqq i\leqq l-1)\,.$$

For each $i\,(1\leqq i\leqq l-1)$, we define a $\boldsymbol{Q}$-automorphism σ_i of K by putting $\sigma_i(\zeta)=\zeta^i$. Then $\mathfrak{p}_1^{\sigma_i^{-1}}=\mathfrak{p}_i$. For any $s\,(2\leqq s\leqq l)$, we put $\mathfrak{A}_s=\prod_{i=1}^{l-1}\mathfrak{p}_1^{[is/l]\sigma_i^{-1}}=\prod_{i=1}^{l-1}\mathfrak{p}_i^{[is/l]}$. Let $(x/\mathfrak{p}_1)_l$ denote the l-th power residue symbol mod $\mathfrak{p}_1$ in K and put $\chi(x)=(x/\mathfrak{p}_1)_l^{-1}$. Let $J(\chi,\chi^j)=-\sum_x \chi(x)\chi^j(1-x)$ and $\tau(\mathfrak{p}_1)=-\sum_x \chi(x)\zeta_p^x$, where x runs through all representatives of $\mathfrak{o}_K$ mod $\mathfrak{p}_1$ and ζ_p is a primitive p-th root of unity. $\mathfrak{A}_s\,(2\leqq s\leqq l-1)$ is a principal ideal of K, generated by $\prod_{j=1}^{s-1}J(\chi,\chi^j)$ and $\mathfrak{A}_l$ is a principal ideal of K, generated by $\tau(\mathfrak{p}_1)^l$. We shall look for an ideal basis of $\mathfrak{A}_s$. Let $g(x)$ be a monic polynomial of degree m in $\boldsymbol{Z}[x]$. This may be decomposed as $g(x)\equiv\prod_{i=1}^{l-1}(x-\zeta^i)^{e_i}h(x) \bmod p\boldsymbol{Z}_p$, where e_i is a non-negative integer, $h(x)$ is a monic polynomial in $\boldsymbol{Z}_p[x]$ and $\varphi_p(h(\zeta^i))=0$ for any $i\,(1\leqq i\leqq l-1)$. Since $m<l-1$ and $\sum_{i=1}^{l-1}e_i+\deg h(x)=m$, there is some i_0 with $e_{i_0}=0$. Then $\varphi_p(g(\zeta^{i_0}))=0$. Therefore

$$\min_{1\leqq i\leqq l-1}\{\varphi_p(g(\zeta^i))-\varphi_p(\iota_i(\mathfrak{A}_s))\} = \min_{i_0\leqq i\leqq l-1}\{\varphi_p(g(\zeta^i))-\varphi_p(\iota_i(\mathfrak{A}_s))\}\leqq -\left[\frac{i_0 s}{l}\right].$$

If i_0 is the largest integer with $e_{i_0}=0$, $i_0\geqq l-1-m$. Hence we have

$$\min_{1\leqq i\leqq l-1}\{\varphi_p(g(\zeta^i))-\varphi_p(\iota_i(\mathfrak{A}_s))\}\leqq -\left[\frac{(l-1-m)s}{l}\right]$$

for any monic polynomial $g(x)$ of degree m in $\boldsymbol{Z}[x]$. For any $j\,(1\leqq j\leqq l-2)$, there exists an element a_j of $\boldsymbol{Z}$ such that $a_j\equiv\zeta^{l-j} \bmod p^{[(l-1-j)s/l]+1}\boldsymbol{Z}_p$ (note that if $s=l$, we can put $a_j\equiv\zeta^{l-j} \bmod p^{l-1-j}$, and if $a\equiv\zeta^{-1} \bmod p^{[(l-2)s/l]+1}$ with $a\in\boldsymbol{Z}$, we may put $a_j=a^j$). Let $g_m(x)=\prod_{j=1}^{m}(x-a_j)\,(1\leqq m\leqq l-2)$. Since $\varphi_p(a_j-\zeta^{l-j})>0$, $\varphi_p(a_j-\zeta^i)=0\,(1\leqq i\neq l-j\leqq l-1)$. Consequently

$$\varphi_p(g_m(\zeta^i))=\sum_{j=1}^{m}\varphi_p(\zeta^i-a_j)=\begin{cases}\varphi_p(\zeta^i-a_{l-i})\geqq\left[\dfrac{(i-1)s}{l}\right]+1 & (l-1-m<i\leqq l-1)\\ 0 & (1\leqq i\leqq l-1-m)\end{cases}$$

and

$$\varphi_p(g_m(\zeta^i))-\varphi_p(\iota_i(\mathfrak{A}_s))\begin{cases}\geqq 0 & (l-1-m<i\leqq l-1)\\ =-\left[\dfrac{is}{l}\right] & (1\leqq i\leqq l-1-m)\,.\end{cases}$$

Therefore

$$\min_{1\leqq i\leqq l-1}\{\varphi_p(g_m(\zeta^i))-\varphi_p(\iota_i(\mathfrak{A}_s))\}=-\left[\frac{(l-1-m)s}{l}\right].$$

Hence $g_m(x)$ and $-[(l-1-m)s/l]$ are a divisor polynomial and the integrality index of degree m of ζ and $\mathfrak{A}_s$ for p. Furthermore $(x-1)^m$ and $[m/(l-1)]=0$ are a divisor polynomial and the integrality index of degree m of ζ and $\mathfrak{A}_s$ for l, so, by Theorem 1 and Remark 2, we have

$$\mathfrak{A}_s=\boldsymbol{Z}p^{s-1}\oplus\bigoplus_{m=1}^{l-2}\boldsymbol{Z}p^{[(l-1-m)s/l]}g_m(\zeta)\qquad(2\leqq s\leqq l)\ .$$

ACKNOWLEDGEMENT. The author thanks K. Okutsu for his kind advice.

References

[1] S. LANG, *Algebraic Number Theory*, Addison-Wesley, 1970.
[2] K. OKUTSU, On extensions of Dedekind domains, to appear in Arch. Math.
[3] K. OKUTSU, Construction of integral basis I-IV, Proc. Japan Acad. Ser. A, **58** (1982), 47-49; 87-89; 117-119; 167-169.

Present Address:
DEPARTMENT OF MATHEMATICS, GAKUSHUIN UNIVERSITY
MEJIRO, TOSHIMA-KU, TOKYO 171, JAPAN.