61. *Integral Basis of the Field* $Q(\sqrt[n]{a})$

By Kōsaku OKUTSU
Department of Mathematics, Gakushuin University

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

In application of the theory exposed in our preceding notes [1], we give here explicitly an integral basis of the field $\boldsymbol{Q}(\sqrt[n]{a})$, where $n, a \in \boldsymbol{Z}$, $n \geq 2$, $(n, a)=1$. Some facts about the Newton diagram which are needed, will be first explained.

1. Newton diagram and irreducible factors of a polynomial. Let k be a complete discrete valuation field with exponential valuation v. For a monic polynomial $f(x)=x^n+a_1x+\cdots+a_n$ in $k[x]$, we define the *Newton diagram* of $f(x)$ as follows (cf. [2]). Put $m_i=v(a_i)$ $(i=1, \cdots, n)$. We define inductively a sequence $(i_0, i_1, \cdots, i_t)$ which is a subset of $\{0, 1, \cdots, n\}$, and a sequence of rational numbers $(\kappa_1, \cdots, \kappa_t)$ as follows. Put $i_0=0$. Assuming i_s is already defined, we put

$$\kappa_{s+1}=\min\{(m_h-m_{i_s})/(h-i_s) \mid i_s<h\leq n\}$$

$$i_{s+1}=\max\{h \mid i_s<h\leq n \text{ and } (m_h-m_{i_s})/(h-i_s)=\kappa_{s+1}\}.$$

Then we have clearly $0=i_0<i_1<\cdots<i_t=n$, and $\kappa_1<\kappa_2<\cdots<\kappa_t$. We put $j_s=m_{i_s}$ $(s=1, \cdots, t)$.

Let P_0 be the point $(0, 0)$ and P_s the point (i_s, j_s) in the Cartesian plane $(s=1, \cdots, t)$. The broken line consisting of t segments $P_{s-1}P_s$ $(s=1, \cdots, t)$ will be called the *Newton diagram* of $f(x)$, denoted N_f, the number t the *order* of N_f, and $(i_1, i_2, \cdots, i_t; \kappa_1, \cdots, \kappa_t)$ the *index* of N_f. Obviously N_f is "convex downward", all points (i, m_i) $(i=0, 1, \cdots, n)$ are lying "upper than" N_f, and N_f is the extremal curve with these properties in a well understood sense. It is clear that the order of the Newton diagram of a monic irreducible polynomial is one.

Lemma 1. *Let $f(x)$ be a monic polynomial in $k[x]$ whose Newton diagram N_f has the index $(i_1, \cdots, i_t; \kappa_1, \cdots, \kappa_t)$, and $g(x)$ be a monic polynomial in $k[x]$ with the Newton diagram N_g with order one and the index $(l; \bar{\kappa})$. Then the order and the index of the Newton diagram N_{fg} of the product of $f(x)$ and $g(x)$ are obtained as follows.*

i) *When $\bar{\kappa}<\kappa_1$, N_{fg} has the order $t+1$ and the index $(l, i_1+l, i_2+l, \cdots, i_t+l; \bar{\kappa}, \kappa_1, \cdots, \kappa_t)$.*

ii) *When $\bar{\kappa}=\kappa_s$ for some s $(1\leq s\leq t)$, N_{fg} has the order t and the index $(i_1, \cdots, i_{s-1}, i_s+l, \cdots, i_t+l; \kappa_1, \cdots, \kappa_t)$.*

iii) *When $\kappa_s<\bar{\kappa}<\kappa_{s+1}$ for some s $(1\leq s\leq t)$, N_{fg} has the order $t+1$, and the index $(i_1, \cdots, i_s, i_s+l, \cdots, i_t+l; \kappa_1, \cdots, \kappa_s, \bar{\kappa}, \kappa_{s+1}, \cdots, \kappa_t)$.*

iv) *When $\kappa_t<\bar{\kappa}$, N_{fg} has the order $t+1$, and the index $(i_1, \cdots, i_t,$*

$i_t+l\,;\kappa_1,\cdots,\kappa_t,\bar{\kappa})$.

From this Lemma 1, we have immediately the following

Proposition 1. *Let $f(x)$ be a monic polynomial in $k[x]$ whose Newton diagram N_f has the index $(i_1,\cdots,i_t\,;\kappa_1,\cdots,\kappa_t)$. Then $f(x)$ is a product of t monic polynomials $f_1,\cdots,f_t$ in $k[x]$ with order* 1, *the index of the Newton diagram N_{f_s} being $(i_s-i_{s-1}\,;\kappa_s)$.*

Corollary. *If $f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in k[x]$ has the Newton diagram N_f of order* 1 *and $v(a_n)$ is relatively prime to n, then $f(x)$ is irreducible. Especially $f(x)$ is irreducible if $f(x)$ is of Eisenstein type,* i.e. *if $v(a_i)\geq 1$ $(1\leq i\leq n)$ and $v(a_n)=1$.*

2. Decomposition of $x^{p^m}-a$ over $\boldsymbol{Q}_p$. Let p be a prime, m a natural number, and $a\in Z$, $(a,p)=1$. By means of the following lemma, which is easy to prove, we can obtain irreducible factors of $x^{p^m}-a$ in $\boldsymbol{Q}_p[x]$.

Lemma 2. *For any natural number $i<p^m$, we have*

$$\mathrm{ord}_p({}_{p^m}C_i)=m-\mathrm{ord}_p(i).$$

To decompose $f(x)=x^{p^m}-a$ in irreducible factors, we observe $f(x)=F(x-a)$ where $F(x)=\sum_{i=1}^{p^m}{}_{p^m}C_i a^{p^m-i}x^i+a^{p^m}-a$. Put $F_0(x)=F(x)-(a^{p^m}-a)$. The index $(i_1,i_2,\cdots\,;\kappa_1,\kappa_2,\cdots)$ of N_{F_0} is $(p^m-p^{m-1},p^m-p^{m-2},\cdots,p^m-1,p^m\,;1/\varphi(p^m),\cdots,1/\varphi(p),\infty)$ where φ is the Euler function.

Now we calculate the index of N_F and obtain the irreducible factors of $F(x)$. We put $r=\mathrm{ord}_p(a^{p^{m-1}}-1)$.

(i) If $r/p^m<\kappa_1$, we have $r=1$. In this case the index of N_F is $(p^m\,;1/p^m)$, and $F(x)$ is an Eisenstein polynomial. So $F(x)$ is irreducible.

(ii) If $\kappa_s\leq(r-\mathrm{ord}_p({}_{p^m}C_{i_s}))/(p^m-i_s)<\kappa_{s+1}$ for some $s<t$, we have $s=r-1>0$. When p is an odd prime,

$$\kappa_s<\frac{1}{p^{m-s}}=\frac{r-\mathrm{ord}_p({}_{p^m}C_{i_s})}{p^m-i_s}.$$

So the index of N_F is $(p^m-p^{m-1},\cdots,p^m-p^{m-r+1},p^m\,;1/\varphi(p^m),\cdots,1/\varphi(p^{m-r+2}),1/p^{m-r+1})$ and each corresponding factor is Eisenstein type. When $p=2$, $\kappa_s=1/2^{m-s}=(r-\mathrm{ord}_2({}_{p^m}C_{i_s}))/(2^m-i_s)$. So the index of N_F is $(2^{m-1},\cdots,2^m-2^{m-r+2},2^m\,;1/2^{m-1},\cdots,1/2^{m-r+2},1/2^{m-r+1})$. The first $r-2$ factors are of Eisenstein type. The last factor is not of Eisenstein type, but we can show that it is also irreducible.

(iii) If $\kappa_m\leq(r-\mathrm{ord}_p({}_{p^m}C_{i_s}))/(p^m-i_m)$, then $r>m$. In this case the index of N_F is $(p^m-p^{m-1},\cdots,p^m-1,p^m\,;1/\varphi(p^m),\cdots,1/\varphi(p),r-m)$, and $F(x)$ is a product of m Eisenstein polynomials and a polynomial of degree 1.

3. Integral Basis of $\boldsymbol{Q}(\sqrt[n]{a})$. Let, n,a be two rational integers such that $n\geq 2$, and $(n,a)=1$. We assume that $f(x)=x^n-a$ is irreducible in $Z[x]$. We shall calculate the integral basis of the field $Q(\sqrt[n]{a})$.

Now let p be a prime such that $m=\mathrm{ord}_p(n)$ is positive. Let us fix p for a while. Put $l=n/p^m$. By Hensel's lemma we have the irreducible decomposition $x^l-a=\prod_{j=1}^{v}H_j(x)$ in $Q_p[x]$ where $H_j(x)$ is irreducible modulo p, and $H_j(x) \bmod p$ and $H_k(x) \bmod p$ are prime to each other for any $k\neq j$. On the other hand, by the results of above section, we have the irreducible decomposition $(x+a)^{p^m}-a=\prod_{i=1}^{u}G_i(x)$ in $Q_p[x]$, where $r=\mathrm{ord}_p(a^{p^{m-1}}-1)$, $u=\min\{r, m+1\}$ when p is an odd prime, and $u=\min\{r-1, m+1\}$ when $p=2$.

Proposition 2. *The notations being the same as above, let $F_{ij}(x)$ be the greatest common divisor of $G_i(x^l-a)$ and $H_j(x^{p^m})$. In case $p\neq 2$, or $p=2$ and $r>m+1$, $F_{ij}(x)$ is an irreducible polynomial in $Q_p[x]$ with degree $\varphi(p^{m-i+1})\cdot\deg H_j(x)$ when $i<u$, and $p^{m-u+1}\cdot\deg H_j(x)$ when $i=u$. In case $p=2$ and $r\leq m+1$, $F_{ij}(x)$ is irreducible in $Q_2[x]$, and has the degree $\varphi(2^{m-i+1})\cdot\deg H_j(x)$ for $i\leq r-2$. As for $F_{r-1,j}(x)$ of degree $2^{m-r+1}\cdot\deg H_j(x)$, it is irreducible or decomposed into two irreducible factors of the same degree according as the following (a) or (b) takes place. Let γ be any root of $F_{r-1,j}(x)$, $\mathfrak{o}$ be the valuation ring of $Q_2(\gamma)$, and $\mathfrak{P}$ the maximal ideal of $\mathfrak{o}$. Let $\bar{\gamma}$ be the class of γ mod $\mathfrak{P}$. $\bar{\gamma}$ may be considered as an element of the algebraic closure of the prime field $Z/2Z$, and $Z/2Z(\bar{\gamma})$ is a subfield of the residue field $\mathfrak{o}/\mathfrak{P}$. Now it is shown that $H_j(\gamma)^{2m-r}/2\in\mathfrak{o}$ and (a) means $H_j(\gamma)^{2m-r}/2 \bmod \mathfrak{P}\notin Z/2Z(\bar{\gamma})$, and (b) means $H_j(\gamma)^{2m-r}/2 \bmod \mathfrak{P}\in Z/2Z(\bar{\gamma})$. If $l>1$, $H_j(x)$ and x are a first and a second (and last) primitive divisor polynomials of any irreducible factor of $F_{i,j}(x)$ for $1\leq i\leq r-1$. If $l=1$, we have $v=1$ and $H_1(x)=x-a$ is a first (and last) primitive divisor polynomial.*

Now let q be a prime such that $t=\mathrm{ord}_q(a)$ is positive, which we consider as fixed for a while. Put $a_0=a/q^t$, $s=(n, t)$, $n_0=n/s$, $t_0=t/s$. Then by Hensel's lemma we have the irreducible decomposition $x^s-a_0=\prod_{i=1}^{m}\Psi_i(x)$ where $\Psi_i(x)$ is a monic polynomial in $Q_q[x]$ such that $\Psi_i(x) \bmod q$ is irreducible in $Z/qZ[x]$, and $\Psi_j(x)\not\equiv\Psi_i(x) \bmod q$ for any $j\neq i$.

Proposition 3. *The notations being as above, put $\Phi_j(x)=q^{t_0\deg\Psi_j}\Psi_j(x^{n_0}/q^{t_0})$. Then $\Phi_j(x)$ is a monic irreducible polynomial in $Z_q[x]$, and so $x^n-a=\prod_{i=1}^{m}\Phi_j(x)$ is an irreducible decomposition in $Q_q[x]$. Moreover x is a first (and last) primitive divisor polynomial of $\Phi_j(x)$ in $Q_q[x]$ $(j=1,\cdots,m)$.*

In virtue of our Theorems 1, 2 in [1]-IV and above Propositions 2, 3 we obtain finally:

Theorem. *Let n, a be two rational integers such that $n\geq 2$, $(n, a)=1$, and suppose $f(x)=x^n-a$ is irreducible in $Z[x]$. Let $\sqrt[n]{a}$ be one of the root of $f(x)$ in C. Let $n=\prod_{i=1}^{k}p_i^{s_i}$, $a=\prod_{j=1}^{l}q_j^{t_j}$ where p_i $(i=1,\cdots,k)$, q_j $(j=1,\cdots,l)$ are distinct primes. Put $n_i=n/p_i^{s_i}$*

$(i=1, \cdots, k)$. *Now put* $g_0(x)=1$, *and for any* $m \in \{1, 2, \cdots, n\}$, *denote by* $g_m(x)$ *a monic polynomial in* $\boldsymbol{Z}[x]$ *satisfying*

$$g_m(x) \equiv (x^{n_i}-a)^{[m/n_i]} x^{m-n_i[m/n_i]} \bmod p_i^{[[m/n_i]\gamma_i]+1} \qquad (i=1, \cdots, k)$$

where

$$\gamma_i = \begin{cases} \dfrac{1}{p_i^{s_i}} & \textit{when } \mathrm{ord}_{p_i}(a^{p_i^{s_i}-1}-1)=1, \\ \dfrac{1}{\varphi(p_i^{s_i})} & \textit{when } \mathrm{ord}_{p_i}(a_i^{p^{s_i-1}}-1)>1. \end{cases}$$

Then

$$\left\{ \frac{g_m(a)}{\prod_{i=1}^{k} p_i^{[[m/n_i]\gamma_i]} \prod_{j=1}^{l} q_j^{[tm_j/n]}} \,\middle|\, m=0, 1, \cdots, n-1 \right\}$$

is an integral basis of $\boldsymbol{Q}(\sqrt[n]{a})$.

Remark. Let $n=p$, $a=p^t \prod_{j=1}^{v} q_j^{t_j}$ where $p, q_1, \cdots, q_v$ are distinct primes, and $t, t_1, \cdots, t_v$ are rational integers such that $0 \leq t < p$, $1 \leq t_j < p$ $(j=1, \cdots, v)$. By the similar method as above we have the following.

Put

$$\gamma = \begin{cases} t/p & \text{when } r=0 \\ 1/p & \text{when } r=1 \\ 1/(p-1) & \text{when } r \geq 2 \end{cases}$$

where $r=\mathrm{ord}_p(a^{p-1}-1)$.

Then $\{(\theta-a)^m / p^{[m\gamma]} \prod_{j=1}^{v} q_j^{[mt_j/p]} \mid m=0, 1, \cdots, p-1\}$ is an integral basis of $\boldsymbol{Q}(\sqrt[n]{a})$.

References

[1] K. Okutsu: Construction of integral basis. I–IV. Proc. Japan Acad., **58A**, 47–49; 87–89; 117–119; 167–169 (1982).

[2] N. Koblitz: p-adic Numbers, p-adic Analysis, and Zeta Functions. Springer (1977).