The Science Reports of the Kanazawa University, Vol. II, No. 1, pp. 15—21, March, 1953.

# On the canonical basis of ideals

By Yoshikazu EDA

(Received, June 6, 1952)

1. We wish to give the canonical basis of ideals of an algebraic number field and its applications.

$P$, $I$, $K$ and $\mathfrak{o}$ denote the rational number field, the integral domain of $P$, algebraic number field over $P$ with degree $n$ and the integral domain of $K$, respectively. Elements of $P$ and $K$ are shown by little Latin letters, $p$ being a rational prime, and Greek letters. Germann letters denote ideals or vectors.

Suppose that the basis of $\mathfrak{o}$ are known and are written as following [3] (numbers in square brackets refer to the references at the end of this note):

$$\mathfrak{o}=[\omega_1,\ \omega_2,\ \cdots\cdots,\ \omega_n],$$

where, we put

$$\omega_i\omega_j=\sum_{k=1}^{n} r_{ij}^{k}\,\omega_k,\quad r_{ij}^{k}\in I,\quad i,j,\ k=1,\ 2,\ \cdots\cdots,\ n.$$

$\mathfrak{r}_k^m$ denotes a column vector $(r_{mk}^1,\ \cdots\cdots,\ r_{m,k}^n)$ and $R$ is an $(n,\ n^2)$ rectangular matrix:

$$R=\begin{bmatrix} \mathfrak{r}_1^1 & \mathfrak{r}_1^2 & \cdots\cdots\cdots & \mathfrak{r}_1^n \\ \cdots\cdots\cdots & & & \\ \mathfrak{r}_n^1 & \mathfrak{r}_n^2 & \cdots\cdots\cdots & \mathfrak{r}_n^n \end{bmatrix}.$$

The irreducible equation defining the field K is

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots\cdots+a_1x+a_0=0.$$

It is well-known that we may assume the basis of an Ideal $\mathfrak{a}$ in K the following type [1]:

$$(1)\qquad \begin{cases} a_1=a_1^1\,\omega_1 \\ a_2=a_2^1\,\omega_1+a_2^2\,\omega_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_n=a_n^1\,\omega_1+a_n^2\,\omega_2+\cdots\cdots+a_n^n\,\omega_n \end{cases}$$

$$a_j^i\in I,\quad a_i^i>0,\quad i,\ j=1,\ 2,\ \cdots\cdots,\ n$$

and

$$N\mathfrak{a}=a_{12\cdots n},$$

where $N\mathfrak{a}$ denote the norm of $\mathfrak{a}$ and

$$a_{l\cdots m}=\prod_{i=l}^{m} a_i^i \qquad (l\geqq m).$$

We may write this equation in the next form :

(2) $$\mathfrak{a}=A\mathfrak{o}$$

where $\mathfrak{a}=(a_1, \cdots\cdots, a_2)$ and $\mathfrak{o}=(\omega_1, \cdots\cdots, \omega_n)$ is a column vector and $A$ is a triangular matrix :

$$A=\begin{bmatrix} a_1^1 & & O \\ a_2^1 & a_2^2 & \\ \vdots & \vdots & \ddots \\ a_n^1 & a_n^2, & \cdots\cdots a_n^n \end{bmatrix}$$

$$a_j^i=0 \ (i>j), \quad a_i^i>0, \quad i, j=1, 2, \cdots\cdots, n.$$

Our aim is studying this matrix $A$.

## 2.

**Lemma 1.** *There are matrices* $T_i$ $(i=1. 2, \cdots\cdots, n)$, *such that*

$$\sum_{k=1}^{i} a_i^k \ \mathfrak{x}_k^i = \mathfrak{t}_{ij} A$$

*where* $\mathfrak{t}_{ij}$ *is a law vector* $(t_{ij}^1, t_{ij}^2, \cdots\cdots, t_{ij}^n)$, $t_{ij}^k, \in\mathfrak{o}$, $i, j, k=1, 2, 3, \cdots\cdots, n$, *and*

$$T_i=[t_{ij}^k]=\begin{bmatrix} t_{i1}^1 \cdots\cdots\cdots\cdots & t_{i1}^n \\ \cdots\cdots\cdots\cdots & \\ t_{in}^n \cdots\cdots\cdots\cdots & t_{in}^n \end{bmatrix}$$

Proof. From our relations

$$a_i\omega_j\in\mathfrak{a}, \qquad i, j=1, 2, \cdots\cdots, n$$

there are numbers $t_{ij}^k\in I$, $\quad i, j, k=1, 2, \cdots\cdots, n$, such that

$$a_i\,\omega_j=\sum_{l=1}^{n} t_{ij}^l\, a_l, \qquad t_{ij}^l\in I$$

then we obtain from (1)

$$a_i\omega_j=(\sum_{k=1}^{i} a_i^k\,\omega_k)\omega_j=\sum_{i=1}^{i} a_i^k \sum_{m=1}^{n} r_{kj}^m\,\omega_m=\sum_{m=1}^{n}(\sum_{k=1}^{i} a_i^k\, r_{kj}^m)\omega_m,$$

and from (2)

$$\sum_{l=1}^{n} t_{ij}^l\, a_l=\sum_{l=1}^{n} t_{ij}^l\,(\sum_{m=1}^{j} a_l^m\,\omega_m)=\sum_{m=1}^{j}(\sum_{l=1}^{n} t_{ij}^l\, a_l^m)\,\omega_m$$

$$=\sum_{m=1}^{n}(\sum_{l=m}^{n} t_{ij}^l\, a_l^m)\,\omega_m$$

and so,

$$\sum_{k=1}^{i} a_i^k r_{kj}^m = \sum_{l=m}^{n} t_{ij}^l a_l^m, \qquad i, j, m = 1, 2, \cdots, n$$

**Lemma 2.**

$$\Delta_{kj}^{m-1} = a_{m\cdots n} r_{kj}^{m-1} - a_{m\cdots(l-1)} \sum_{l=m}^{n} a_l^{m-1} \Delta_{kj}^l,$$

*where*

$$\Delta_{kj}^m = \begin{bmatrix} r_{kj}^m & r_{kj}^{m+1} & \cdots & r_{kj}^n \\ a_{m+1}^m & a_{m+1}^{m+1} & 0 & 0 \\ \vdots & \vdots & \ddots & \\ a_n^m & a_n^{m+1} & \cdots & a_n^n \end{bmatrix},$$

*and*

$$\Delta_{kj}^n = r_{kj}^n.$$

Proof.

$$\Delta_{kj}^{m-1} = a_{m\cdots n} r_{kj}^{m-1} + \sum_{l=m}^{n} (-1)^{l-m+1} a_l^{m-1} D_l,$$

where

$$D_l = \begin{vmatrix} r_{kj}^m & \cdots & r_{kj}^n \\ a_m^m & & 0 \\ \vdots & \ddots & \vdots \\ a_{l-1}^m & a_{l-1}^{l-1} & 0 \\ a_{l+1}^m & a_{l+1}^l & a_{l-1}^{l+1} \\ \vdots & \vdots & \vdots \\ a_n^m & a_n^l & a_n^{l+1} \end{vmatrix}$$

$$= (-1)^{l-m} \begin{vmatrix} a_m^m & & 0 \\ \vdots & \ddots & \vdots \\ a_{l-1}^m & a_{l-1}^{l-1} & 0 \\ r_{kj}^m & r_{kj}^l & r_{kj}^n \\ a_{l+1}^m & a_{l+1}^l & a_{l+1}^{l+1} \\ \vdots & \vdots & \vdots \\ a_n^m & a_n^l & a_n^{l+1} \end{vmatrix}$$

$$=(-1)^{l-m}\, a_{m\cdots(l-1)}\, \Delta^{l}_{kj},$$

(Laplace's expansion theorem), thus our lemma follows.

## 3.

**Theorem.** *Basis of Ideal* $\mathfrak{a}$ *in our field* $K$ *is given by the following conditions*;

$$\mathfrak{a}=[\alpha_1, \cdots\cdots, \alpha_n]$$

$$\mathfrak{a}=A\mathfrak{o} \qquad (A \text{ is given by } (3)).$$

$$N\mathfrak{a}=a_{1\cdots\cdots n}$$

$$\sum_{k=1}^{i} a^{k}_{i}\, \Delta^{m}_{kj} \equiv 0 \mod a_{m\cdots n},$$

$$i,\ j,\ k=1,\ 2,\ \cdots\cdots,\ n.$$

*We wish to call this basis canonical.*

Proof. Our result is proved by induction using above Lemmas. If $m=n$, then from our Lemma 1, we take $n$-th component of a vector $v^{m}_{k}$, i. e.

$$a^{n}_{n}\, t^{n}_{ij}=\sum_{k=1}^{i} a^{k}_{i}\, r^{n}_{kj}=\sum_{k=1}^{i} a^{n}_{i}\, \Delta^{n}_{kj}.$$

Suppose that our proposition is true for all $m'$, $m\leqq m'\leqq n$, then from Lemma 1,

$$\sum_{l=m-1}^{n} a^{m-1}_{l}\, t^{l}_{ij}=\sum_{k=1}^{i} a^{k}_{i}\, r^{m-1}_{kj}$$

and so

$$a^{m-1}_{m-1}\, t^{m-1}_{ij}=\sum_{k=1}^{i} a^{k}_{i}\, r^{m-1}_{kj}-\sum_{l=m}^{n} a^{m-1}_{l}\, t^{l}_{ij}.$$

and

$$a_{m-1,m\cdots n}\, t^{m-1}_{ij}=a_{m\cdots n}\sum_{k=1}^{i} a^{k}_{i}\, r^{m-1}_{kj}-a_{m\cdots(l-1)}\sum_{l=m}^{n} a^{m-1}_{l}\, a_{l\cdots m}\, t^{l}_{ij}$$

$$=\sum_{k=1}^{i} a^{k}_{i}\,(a_{m\cdots n}\, r^{m-1}_{kj}-a_{m\cdots(l-1)}\sum_{l=m}^{n} a^{m-1}_{l}\, \Delta^{l}_{kj})$$

$$=\sum_{k=1}^{i} a^{k}_{i}\, \Delta^{m-1}_{kj}.$$

thus, our theorem is established.

Especially, if we put $\omega_1=1$, then

$$r^{k}_{1i}=r^{k}_{i1}=\begin{cases}1 & k=i,\\ 0 & k\neq i.\end{cases}$$

**Corollary.** 1. $i=1$,

$$a_{m\cdots n}\, t^{m}_{1j}=(-1)^{j-m}\, a^{1}_{1}\, D^{m}_{j}$$

*where*

$$D_j^m=(-1)^{j-m}\Delta_{1j}^m=\begin{vmatrix} a_{m+1}^m & a_{m+1}^{m+1} & 0 & \cdots & 0 \\ \vdots & \vdots & & & 0 \\ & & & & a_{j-1}^{j-1} \\ a_j^m & a_{j+1}^m & \cdots & & a_j^{j-1} \end{vmatrix}$$

*From this relation, we deduce the relations*

$$a_m^m \mid a_1^1, \qquad m=1, 2, \cdots\cdots, n.$$

$i=2$,

$$a_{m\cdots n}t_{2j}^m=(-1)^{m-j}\, a_2^1 D_j^m+a_2^2\,\Delta_{2j}^m$$

$i=3$,

$$a_{m\cdots n}t_{3j}^m=(-1)^{m-j}\, a_3^1 D_j^m+a_3^2\,\Delta_{2j}^m+a_3^3\,\Delta_{3j}^m,$$

*etc.*

*From these relations, we get*

$$a_2^2 \mid a_2^1, \quad a_2^2 \mid a_1^1.$$

These relations are well known in the quadratic number field.

**Corollary 2.** *If $N\mathfrak{a}=a$ is quadratfrei, then its basis have the following type*:

$$\mathfrak{a}=[a,\ a_2+\omega_2,\ \cdots\cdots,\ a_n+\omega_n].$$

**Corollary 3.** *We can put the basis of prime ideal $\mathfrak{p}$ with grade $f$ the following type*:

$$\mathfrak{p}=\begin{bmatrix} p & & f_1 & & & & 0 \\ & p & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & p & f_2 & \\ & & & & & p & \\ a_j^i & & 0 & & a_j^i & 0 & \end{bmatrix}\mathfrak{o}$$

where,

$$N\mathfrak{p}=p^f,\quad f=\sum f_i$$

**4.** Prime factorization of $p$ in cubic fields. Prime factorization of $p$ is made to depend upon prime factorization of $f(x)$ mod $p$, and many results in connection with this problem in general algebraic number field are known by Dedekind [1], Ore, and others. In cubic fields, this problem is performed in detail by Wilson [4]. Now, we give only the canonical form being given by our method.

$f$ denote the grade of primideal.

$f=1$ :

$$\mathfrak{p}=\begin{bmatrix} p & 0 & 0 \\ -t & 1 & 0 \\ -s & 0 & 1 \end{bmatrix}\mathfrak{o}, \qquad \text{where } f(t)\equiv g(t)\equiv 0 \bmod p \text{ and } |t|,\ |s|<p.$$

$f=2$ :

(i)

$$\mathfrak{p}=\begin{bmatrix} p & 0 & 0 \\ 0 & p & 0 \\ -t & -s & 1 \end{bmatrix}\mathfrak{o},$$

(ii)

$$\mathfrak{p}=\begin{bmatrix} p & 0 & 0 \\ -t & 1 & 0 \\ s & 0 & p \end{bmatrix}\mathfrak{o},$$

$f=3$ :

$$\mathfrak{p}=\begin{bmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{bmatrix}\mathfrak{o}.$$

where $\mathfrak{o}=[1, \omega_1, \omega_2]$, and $\omega_1$, $\omega_2$ are defined by its defining function $f(x)$, and $g(x)$.

When $f=2$, we must remark that, from our theorem ($n=3$, $m=2$, $i=3$, $j=2$ or 3), giving

$$R'=\begin{bmatrix} r_{22}^1 & r_{22}^2 & r_{22}^3 \\ r_{23}^1 & r_{23}^2 & r_{23}^3 \\ r_{33}^1 & r_{33}^2 & r_{33}^3 \end{bmatrix},$$

we get

$$(4)\quad \begin{cases} -t-s(r_{22}^2+sr_{22}^3)+r_{32}^2+sr_{32}^3\equiv 0 & \bmod p \\ -ts-s(r_{23}^2+sr_{23}^3)+r_{33}^2+sr_{33}^3\equiv 0 & \bmod p. \end{cases}$$

$f=2$ (ii) is reduced to $f=2$ (i) from $p\mid s$ (Theorem).

**Example.** (Dedekind [2]).

$$f(x)=x^3-x^2-2x-8,$$
$$\mathfrak{o}=[1, \alpha, \beta],$$

where

$$f(\alpha)=0,$$
$$\beta=\frac{1}{2}\alpha(\alpha-1)-1,$$

and

$$R'=\begin{bmatrix} 2 & 1 & 2 \\ 4 & 0 & 0 \\ -2 & 2 & -1 \end{bmatrix},$$

we can easily deduce the prime factorization of 2, i. e.,

$$2=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$

where

$$\mathfrak{p}_1=[2,\ \alpha,\ \beta],$$
$$\mathfrak{p}_2=[2,\ \alpha,\ \beta+1],$$
$$\mathfrak{p}_3=[2,\ \alpha+1,\ \beta+1]$$

and of cause

$$N\mathfrak{p}_1=N\mathfrak{p}_2=N\mathfrak{p}_3=2.$$

Now, from our above relations (4),

$$F(s)\equiv 2s^3+s^2-s+2\equiv 0 \mod p$$

$F(s)$ is irreducible mod $p$ except $p=2$ and 5, and so for $p=5$, we obtain

$$F(s)\equiv(s-2)(2s^2-1) \mod 5$$

where $2s^2-1$ is irreducible mod 5. Thus we get in our cubic field only one 2 grad primeideal $\mathfrak{p}$ :

$$\mathfrak{p}=[5,\ -2\alpha+\beta],$$

and in this case

$$5=\mathfrak{p}\mathfrak{p}',$$

where

$$\mathfrak{p}'=[5,\ \alpha-1,\ \beta+1]=[5,\ \alpha-1].$$

Department of Mathematics
Kanazawa University.

**References.**

[1] R. Dedekind : Uber die Anzahl der Ideal Klassen in den verschiedenen Ordnungen eines endlichen Körpers, 1877. Gesammelte Mathematische Werke I, 1930.

[2] R. Dedekind : Uber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der hoheren Kongruenzen, 1878. Werke, I. 1930.

[3] N. R. Wilson : Integers and basis of a number field. Transaction of the American Mathematical Society. Vol. 29, 1927.

[4] N. R. Wilson : On finding Ideals. Annals of Mathematics. Vol. 30, 1929.