

A Note on the Ring $I_{k/k}$ of Integers

by
 Dong-Uk Ko

Throughout this paper we assume that

Z = the ring of all integers, Q = the rational field
 C = the complex field,

Moreover, we assume that K and k are number fields such that $[k:k]=n$ and $[k:Q]=m$ and that I_k is the ring of integers of k . The purpose of this paper is to define the ring $I_{k/k}$ of integers of k/k (Definition 1) and to prove that ① $I_k = I_{k/k}$ (Theorem 3) ② $I_{k/k}$ is a Dedekind integral domain (corollary 6). As is well known I_k is a Dedekind integral domain and thus I_k has the unique factorization property with respect to prime ideals.
 (※)

Let k be an extension field of k with $[k:k]=n$. (Note that the complex field $C \supset K \supset k \supset Q$ and $(k:Q)=[k:k][k:Q]=mn$).

Definition 1. If $\alpha \in k$ satisfies

$$\alpha^r + \alpha_1 \alpha^{r-1} + \dots + \alpha_{r-1} \alpha + \alpha_r = 0 \quad (\alpha_i \in I_k, i=1, \dots, r)$$

then α is called an algebraic integer of k over k . $I_{k/k}$ denotes the set of all algebraic integers of k over k .

Definition 2. Let $k = k(\theta)$ and let $f(x) = X^n + \alpha_1 X^{n-1} + \dots + \alpha_{n-1} X + \alpha_n$ ($\alpha_i \in k$ and $i=1, n$) be a minimal polynomial of θ . Let us denote the conjugate elements of θ by

$$\theta = \theta^{(1)}, \theta^{(2)}, \dots, \theta^{(n)},$$

then $f(\theta^{(i)}) = 0$ for $i=1, \dots, n$. We put $K^{(i)} = k(\theta^{(i)})$ for $i=1, \dots, n$. Each $\alpha \in K$ has a unique representation

$$\alpha = \alpha_0 + \alpha_1 \theta + \dots + \alpha_{n-1} \theta^{n-1} \quad (\alpha_i \in k, i=0, \dots, n-1).$$

We define the algebraic conjugates of α by

$$\begin{aligned}\alpha &= \alpha^{(1)} = d_0 + d_1 \theta^{(1)} + \cdots + \alpha_{n-1} \theta^{(1)n-1} \\ \alpha^{(2)} &= \alpha_0 + \alpha_1 \theta^{(2)} + \cdots + \alpha_{n-1} \theta^{(2)n-1} \\ &\vdots \\ \alpha^{(n)} &= \alpha_0 + \alpha_1 \theta^{(n)} + \cdots + \alpha_{n-1} \theta^{(n)n-1}.\end{aligned}$$

(Note that if $\alpha \in k$ then $\alpha^i = \cdots = \alpha^{(n)} = \alpha$.) The norm $N_{k/k} \alpha$ and the trace $T_{k/k} \alpha$ of α are defined by

$$N_{k/k} \alpha = \alpha^{(1)} \cdots \alpha^{(n)}, \quad T_{k/k} \alpha = \alpha^{(1)} + \cdots + \alpha^{(n)},$$

respectively.

Theorem 1. We have the following properties about $I_{k/k}$.

- (i) $I_{k/k}$ is an integral domain.
- (ii) $\forall \alpha \in K \exists m (\neq 0) \in Z$ such that $m\alpha \in I_{k/k}$.
- (iii) $I_{k/k}$ is integrally closed, i.e., if $\alpha \in K$ satisfies $\alpha^r + \alpha_1 \alpha^{r-1} + \cdots + \alpha_{r-1} \alpha + \alpha_r = 0$ ($\alpha_i \in I_{k/k}$, $i=1, \dots, r$) then $\alpha \in I_{k/k}$.
- (iv) $I_{k/k} \cap k = I_k$
- (v) For $\alpha \in I_{k/k}$ $N_{k/k} \alpha, T_{k/k} \alpha \in I_k$

Furthermore, the algebraic conjugates $\alpha = \alpha^{(1)}, \dots, \alpha^{(n)}$ of α are also algebraic integers over k , i.e., $\alpha^{(i)}$ is an algebraic integer of $K^{(i)}$ over k for $i=1, \dots, n$ ($\alpha^{(i)} \in I_{k^{(i)}/k}$).

Proof (1): We shall prove that $\lambda \in I_{k/k} \leftrightarrow \exists \eta_1, \dots, \eta_n \in K$ such

that ① $\eta_i \eta_j \in I_k \eta_1 + \cdots + I_k \eta_n$ ($i, j=1, \dots, n$)

② $\lambda \in I_k \eta_1 + \cdots + I_k \eta_n$

Suppose $\lambda \in I_{k/k}$, then there exist $\alpha_i \in I_k$ such that

$$\lambda^r + \alpha_1 \lambda^{r-1} + \cdots + \alpha_{r-1} \lambda + \alpha_r = 0.$$

Thus, put $\lambda^{r-1} = \eta_1, \dots, \lambda = \eta_{r-1}$ and $1 = \eta_r$, then

$$\eta_i \eta_j = \lambda^{2r-(i+j)} = \begin{cases} \eta_{i+j-r} & \text{if } i+j > r \\ b_1 \eta_1 + \cdots + b_m \eta_r & \text{if } i+j \leq r \end{cases}$$

where b_i ($i=1, \dots, r$) $\in I_k$. That is, $\eta_i \eta_j \in I_k \eta_1 + \cdots + I_k \eta_r$. Next,

$$\lambda = \eta_{r-1} \implies \lambda \in I_k \eta_1 + \cdots + I_k \eta_n.$$

Conversely, suppose $\lambda \in I_k \eta_1 + \cdots + I_k \eta_n$. By our assumptions ① and ②

$$\lambda \eta_i = \sum_{j=1}^n c_{ij} \eta_j \quad (c_{ij} \in I_k).$$

Define the $N \times N$ -matrix $c = (\delta_{ij}\lambda - c_{ij})_{i,j=1 \dots N}$

$$\delta_{ij} = \begin{cases} 1, & i=j \\ 0, & i \neq j. \end{cases}$$

In this case:

$$C \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_N \end{pmatrix} = \begin{pmatrix} \lambda - C_{11} & -C_{12} & \cdots & -C_{1N} \\ -C_{21} & \lambda - C_{22} & \cdots & -C_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ -C_{N1} & -C_{N2} & \cdots & \lambda - C_{NN} \end{pmatrix} \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_N \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

If $\det C \neq 0$ then there exists the inverse C^{-1} and we have

$$\begin{pmatrix} \eta_1 \\ \vdots \\ \eta_N \end{pmatrix} = C^{-1} C \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_N \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

In consequence, $\eta_1 = \dots = \eta_N = 0$ and $\lambda = 0$. If $\det C = 0$ then λ is a root of the following equation

$$\begin{vmatrix} \lambda - C_{11} & \cdots & -C_{12} & \cdots & -C_{1N} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ -C_{N1} & \cdots & \lambda - C_{NN} & \cdots & -C_{NN} \end{vmatrix} = 0 \quad (C_{ij} \in I_k)$$

and thus $\lambda \in I_{k/k}$.

We shall prove (i) by using the above result. Take $\alpha, \beta \in I_{k/k}$, then

$$\begin{aligned} \alpha &\in I_k \eta_1 + \dots + I_k \eta_N, \quad \eta_i \eta_j \in I_k \eta_1 + \dots + I_k \eta_N \\ \beta &\in I_k \zeta_1 + \dots + I_k \zeta_M, \quad \zeta_i \zeta_j \in I_k \zeta_1 + \dots + I_k \zeta_M, \end{aligned}$$

where $\eta_i, \zeta_j \in K$ for $i=1, \dots, N$ and $j=1, \dots, M$. Since

$$\begin{aligned} \eta_i \eta_j &\in I_k \eta_1 + \dots + I_k \eta_N, \quad I_k \eta_1 + \dots + I_k \eta_N + I_k \zeta_1 + \dots + I_k \zeta_M + I_k \eta_1 \zeta_1 + \dots + I_k \eta_N \zeta_M \\ \zeta_i \zeta_j &\in I_k \zeta_1 + \dots + I_k \zeta_M \subset I_k \eta_1 + \dots + I_k \zeta_1 + \dots + I_k \eta_1 \zeta_1 + \dots + I_k \eta_N \zeta_M \\ (\eta_i \zeta_j)(\eta_k \zeta_l) &= (\eta_i \eta_k)(\zeta_j \zeta_l) \in I_k \eta_1 \zeta_1 + \dots + I_k \eta_N \zeta_M \\ &= C I_k \eta_1 + \dots + I_k \zeta_1 + \dots + I_k \eta_N \zeta_M \end{aligned}$$

and

$$\alpha \pm \beta, \alpha \beta \in I_k \eta_1 + \dots + I_k \eta_N + I_k \zeta_1 + \dots + I_k \zeta_M + I_k \eta_1 + \dots + I_k \eta_N \zeta_M$$

it follows that $\alpha \pm \beta, \alpha \beta \in I_{k/k}$. Thus $I_{k/k}$ is a commutative ring. It is clear that $I \in I_{k/k}$, and thus $I_{k/k}$ is an integral domain.

(ii): Let $X^r + \alpha_1 X^{r-1} + \dots + \alpha_{r-1} X + \alpha_r$ ($\alpha_i \in k$, $i=1, \dots, r$, $r \leq n$) be a minimal polynomial of $\alpha \in K$ over k . As in [2] there exist non-zero rational integers m_1, \dots, m_r such that

$$m_i \alpha_i, \dots, m_r \alpha_r \in I_k$$

Put $b_0 = m_1 m_r$ ($\in \mathbb{Z}$) then α is a root of

$$b_0 X^r + \beta_1 X^{r-1} + \dots + \beta_{r-1} X + \beta_r = 0. \quad (\beta_i \in I_k, i=1, \dots, r),$$

where $\beta_1 = b_0 \alpha_1, \dots$, and $\beta_r = b_0 \alpha_r$, $i, e.,$

$$b_0 \alpha^r + \beta_1 \alpha^{r-1} + \dots + \beta_{r-1} \alpha + \beta_r = 0.$$

Thus, we have

$$(b_0 \alpha)^r + \beta_1 b_0 (b_0 \alpha)^{r-1} + \dots + \beta_{r-1} b_0^{r-2} (b_0 \alpha) + b_0^{r-1} \beta_r = 0.$$

If we put $\beta_1 b_0 = \gamma_1, \dots$, $\beta_{r-1} b_0^{r-2} = \gamma_{r-1}$, $b_0^{r-1} \beta_r = \gamma_r$, then $b_0 \alpha$ is a root of

$$X^r + \gamma_1 X^{r-1} + \dots + \gamma_{r-1} X + \gamma_r = 0, \quad (\gamma_i \in I_k, i=1, \dots, r),$$

and thus $b_0 \alpha \in I_k$.

(iii) Suppose $\alpha \in K$ satisfies

$$\alpha^r + \alpha_1 \alpha^{r-1} + \dots + \alpha_{r-1} \alpha + \alpha_r = 0 \quad (\alpha_i \in I_{k/k}, i=1, \dots, r)$$

Since $\alpha_i \in I_{k/k}$ we have some positive rational integer N_i such that

$$\alpha_i^{N_i} = -(\beta_1 \alpha_i^{N_i-1} + \dots + \beta_{N_i-1} \alpha_i - \beta_{N_i}) \quad (\beta_i \in I_k, i=1, \dots, N_i)$$

Put $\alpha_i^{N_i-1} = \eta_{i1}, \dots$, $\alpha_i = \eta_{iN_i-1}$ and $1 = \eta_{iN_i}$, then

$$\begin{aligned} \eta_{i1} \eta_{ik} &\in I_k \eta_{i1} + \dots + I_k \eta_{iN_i} \\ \alpha_i &\in I_k \eta_{i1} + \dots + I_k \eta_{iN_i}, \quad (i=1, \dots, r). \end{aligned}$$

Let us put

$$\zeta_{1j_1 \dots j_r} = \alpha^l \eta_{1j_1} \dots \eta_{rj_r} \quad (l=0, 1, \dots, r-1, j_i=1, \dots, N_i, i=1, \dots, r)$$

then it follows that

$$\begin{aligned} \zeta_{1j_1 \dots j_r}, \zeta'_{1j'_1 \dots j'_r} &\in \sum I_k \zeta_{1j_1 \dots j_r} \\ \alpha &\in \sum I_k \zeta_{1j_1 \dots j_r}. \end{aligned}$$

That is, by (i) $\alpha \in I_{k/k}$.

(iv) Note that

$I_{k/k} \cap k =$ the set of all algebraic integers over k in k .

Since I_k is integrally closed in k (As in [2]) it follows that $I_{k/k} \cap k = I_k$.

(v): Let $\alpha = \alpha_0 + \alpha_1\theta + \dots + \alpha_{n-1}\theta^{n-1} \in I_{k/k}$ (see Definition 2), and let $X^r + \beta_1 X^{r-1} + \dots + \beta_{r-1}X + \beta_r$ ($\beta_i \in I_k$, $i=1, \dots, r$) be a minimal polynomial of α over k . Then

$$\alpha^r + \beta_1 \alpha^{r-1} + \dots + \beta_{r-1} \alpha + \beta_r = 0.$$

The algebraic conjugate $\alpha^{(i)} = \alpha_0 + \alpha_1 \theta^{(i)} + \dots + \alpha_{n-1} \theta^{(i)n-1}$ ($i=1, \dots, n$) of α satisfies the above equation, i.e.,

$$\alpha^{(i)r} + \beta_1 \alpha^{(i)r-1} + \dots + \beta_{r-1} \alpha^{(i)} + \beta_r = 0.$$

Thus $\alpha^{(i)}$ is algebraic integer over k ($\alpha^{(i)} \in I_{k/k}$).

On the other hand, $N_{k/k} \alpha = \alpha^{(1)} \dots \alpha^{(n)}$ and $T_{k/k} (\alpha^{(1)} + \dots + \alpha^{(n)})$ are symmetric functions of $\alpha^{(1)}, \dots$, and $\alpha^{(n)}$, and thus

$$N_{k/k} \alpha, T_{k/k} \alpha \in k.$$

Let L be an extension field of $K^{(1)}, \dots$, and $K^{(n)}$ such that $L \subset \mathbb{C}$ (the complex field). Then, $\alpha^{(1)}, \dots, \alpha^{(n)} \in I_{L/k}$, and also $N_{k/k} \alpha, T_{k/k} \alpha \in I_{L/k}$ by (i). Thus,

$$N_{k/k} \alpha, T_{k/k} \alpha \in I_{L/k} \cap k = I_k$$

by (iv). ///.

Theorem 2. When $[k:k] = n$ we have

$$I_{k/k} = I_k w_1 \oplus \dots \oplus I_k w_n \text{ (direct sum),}$$

where w_1, \dots , and w_n are elements of K . (We say that $\{w_1, \dots, w_n\}$ is a basis of $I_{k/k}$.)

Proof. As in Definition 2, we put $K = k(\theta) = k \oplus k\theta \oplus \dots \oplus k\theta^{n-1}$ ($\theta \in K$). By (ii) of Theorem 1. there exists a non-zero rational integer m such that $m\theta \in I_{k/k}$. Thus, we may assume that $\theta \in I_{k/k}$. Then we have a unique expression of $\alpha \in K$ such that

$$\alpha = \alpha_0 + \alpha_1 \theta + \dots + \alpha_{n-1} \theta^{n-1} \quad (\alpha_i \in k, i=0, 1, \dots, n-1).$$

Let

$$\begin{aligned} \alpha &= \alpha^{(1)} = \alpha_0 + \alpha_1 \theta^{(1)} + \dots + \alpha_{n-1} \theta^{(1)n-1} \\ &\vdots \\ \alpha^{(n)} &= \alpha_0 + \alpha_1 \theta^{(n)} + \dots + \alpha_{n-1} \theta^{(n)n-1} \end{aligned}$$

be the algebraic conjugate of α . We put

$$\Delta = \begin{vmatrix} 1 & \theta^{(1)} & \dots & \theta^{(1)n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta^{(n)} & \dots & \theta^{(n)n-1} \end{vmatrix} = \pi(\theta^{(1)} - \theta^{(j)})_{i < j}$$

and

$$\Delta^{(i+1)} = \begin{vmatrix} 1 & \theta^{(1)} & \dots & \theta^{(1)i-1} & \alpha^{(1)} & \theta^{(1)i+1} & \dots & \theta^{(1)n-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta^{(n)} & \dots & \theta^{(n)i-1} & \alpha^{(n)} & \theta^{(n)i+1} & \dots & \theta^{(n)n-1} \end{vmatrix}$$

then $\theta^{(i)} \neq \theta^{(j)}$ ($i \neq j$) $\implies \Delta \neq 0$ and $\alpha_i = \Delta^{(i+1)}/\Delta$. Since $\theta \in I_{k/k}$ and Δ^2 is a symmetric function of $\theta = \theta^{(1)} \dots \theta^{(n)}$, $\Delta^2 \in I_k$. In

$$\alpha_i = \frac{\Delta \Delta^{(i+1)}}{\Delta^2}$$

$\Delta^2 \in I_k$ and $\alpha_i \Delta^2 = \Delta \Delta^{(i+1)} \in k(\alpha_i \in k)$. If $\alpha \in I_{k/k}$, $\alpha_i \in I_k$.

Thus, $\alpha \in I_{k/k} \implies \Delta^2$, $\alpha_i \Delta^2 = \Delta \Delta^{(i+1)} \in I_k$. Therefore, when $\alpha \in I_{k/k}$ we have the following):

$$\begin{aligned} \alpha &= \alpha_0 + \alpha_1 \theta + \dots + \alpha_{n-1} \theta^{n-1} (\theta \in I_{k/k}, \alpha_i \in I_k, i=0, \dots, n-1) \\ &= \frac{\Delta \Delta^{(1)}}{\Delta^2} + \frac{\Delta \Delta^{(2)}}{\Delta^2} \theta + \dots + \frac{\Delta \Delta^{(n)}}{\Delta^2} \theta^{n-1} \\ &= \Delta \Delta^{(1)} \frac{1}{\Delta^2} + \Delta \Delta^{(2)} \frac{\theta}{\Delta^2} + \dots + \Delta \Delta^{(n)} \frac{\theta^{n-1}}{\Delta^2} \\ &\in I_k \frac{1}{\Delta^2} \oplus I_k \frac{\theta}{\Delta^2} \oplus \dots \oplus I_k \frac{\theta^{n-1}}{\Delta^2} \end{aligned}$$

In consequence

$$I_{k/k} \subseteq I_k \frac{1}{\Delta^2} \oplus I_k \frac{\theta}{\Delta^2} \oplus \dots \oplus I_k \frac{\theta^{n-1}}{\Delta^2} \quad (\text{direct sum})$$

Where the right hand side is a free I_k -module with a basis

$\left\{ \frac{1}{\Delta^2}, \frac{\theta}{\Delta^2}, \dots, \frac{\theta^{n-1}}{\Delta^2} \right\}$. Thus, $I_{k/k}$ is a I_k -submodule of a free I_k -module. It follows

that $I_{k/k}$ has a basis $\{w_1, \dots, w_n\}$ such that

$$I_{k/k} = I_k w_1 \oplus \dots \oplus I_k w_n$$

([10]). ///

Theorem 3. $I_{k/k} = I_k$.

Proof. It is clear that $I_k \subseteq I_{k/k}$ because that $Z \subseteq I_k$. Suppose $[K:k] = n$, $[k, Q] = m$ and

$$I_{k/k} = I_k w_1 \oplus \cdots \oplus I_k w_n \quad (w_i \in I_{k/k}, \quad i=1, \dots, n)$$

$$I_k = Z\zeta_1 \oplus \cdots \oplus Z\zeta_m \quad (\zeta_j \in I_k, \quad j=1, \dots, m).$$

Then, we have

$$I_{k/k} = Z\zeta_1 w_1 \oplus \cdots \oplus Z\zeta_m w_1 \oplus Z\zeta_1 w_2 \oplus \cdots \oplus Z\zeta_m w_n,$$

which is a direct sum because that $\zeta_1 w_1, \dots,$ and $\zeta_m w_n$ are linearly independent over Z .

Furthermore, since $I_k \subset I_{k/k}$

$$\zeta_1 w_1, \dots, \zeta_m w_n \in I_{k/k}.$$

Next, we want to prove that $w_i \ (i=1, \dots, n) \in I_k$. Let

$$g(X/k) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_{n-1} X + \alpha_n \ (\alpha_i \in I_k, \quad i=1, \dots, n)$$

be a minimal polynomial of $w_i \in I_{k/k}$.

Let us put

$$k^{(i)} = k, \dots, k^{(m)} \text{ as the conjugate fields of } k \text{ over } Q$$

$$g(X/k^{(j)}) = X^n + \alpha_1^{(j)} X^{n-1} + \cdots + \alpha_{n-1}^{(j)} X + \alpha_n^{(j)} \ (\alpha_i^{(j)} \in k^{(j)} \quad i=1, \dots, n).$$

Then a minimal polynomial of w_i over Q is

$$G(X) = g(X/k^{(1)}), \quad g(X/k^{(2)}) \cdots g(X/k^{(m)}).$$

Take a number field L such that $L \supset K^{(1)}, \dots, K^{(n)}$. Then $\alpha_i^{(j)} \in I_L$ for $i, j=1 \cdots n$ and each coefficient of $G(X)$ is in Q .

Since $Q \cap I_L = Z$ as in [2] we have each coefficient of

$$G(X) \in Z.$$

It is clear that $G(w_i) = 0$, and thus w_i is an element of I_k .

Therefore we have $\zeta_j w_i \in I_k$ for $i=1, \dots, m$ and $j=1, \dots, n$, because that $I_k \subset I_{k/k}$. In consequence, we have the following:

$$I_k = Z\zeta_1 w_1 \oplus Z\zeta_2 w_1 \oplus \cdots \oplus Z\zeta_m w_n$$

i.e., $I_k = I_{k/k}$. ///

Corollary, $I_{k/k}$ is a Dedekind integral domain.

Proof. By (*) above, since I_k is a Dedekind integral domain so is $I_{k/k}$ by Theorem 3. We have one other proof as follows.

We have two steps to do this.

Step I. Let us assume that

$$\begin{aligned} I_{k/k} &= I_k w_1 \oplus \cdots \oplus I_k w_n \\ I_k &= Z \zeta_1 \oplus \cdots \oplus Z \zeta_n. \end{aligned}$$

Then, as before,

$$I_k = Z \zeta_1 w_1 \oplus \cdots \oplus Z \zeta_n w_1 \oplus \cdots \oplus Z \zeta_n w_n.$$

Let Π be an ideal of $I_{k/k}$. Since Π is a I_k -submodule of the free I_k -module $I_{k/k}$ it has a basis $\{\alpha_1, \dots, \alpha_n\}$ such that

$$\Pi = I_k \alpha_1 \oplus \cdots \oplus I_k \alpha_n.$$

If we put

$$\Pi' = Z \zeta_1 \alpha_1 \oplus \cdots \oplus Z \zeta_n \alpha_1 \oplus Z \zeta_1 \alpha_2 \oplus \cdots \oplus Z \zeta_n \alpha_n,$$

then Π' is an ideal of I_k generated by $\{\zeta_1 \alpha_1, \dots, \zeta_n \alpha_n\}$. There exists a maximum matrix $A = (a_{ij})$ ($a_{ij} \in Z$) such that

$$\begin{pmatrix} \zeta_1 \alpha_1 \\ \vdots \\ \zeta_n \alpha_1 \\ \zeta_1 \alpha_2 \\ \vdots \\ \zeta_n \alpha_n \end{pmatrix} = A \begin{pmatrix} \zeta_1 w_1 \\ \vdots \\ \zeta_n w_1 \\ \zeta_1 w_2 \\ \vdots \\ \zeta_n w_n \end{pmatrix}$$

By a choice of $\{\zeta_1 \alpha_1, \dots, \zeta_n \alpha_n\}$ and $\{\zeta_1 w_1, \dots, \zeta_n w_n\}$ A can be denoted by

$$\det A = \begin{vmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_{mn} \end{vmatrix} \quad (e_i \in Z, i=1, 2, \dots, mn).$$

Therefore

$$N\Pi' = |\det A| = |e_1 \cdots e_{mn}|,$$

which called the norm of Π' . Thus, each element of I_k/Π' is uniquely represented by

$$a_1 \zeta_1 w_1 + \cdots + a_{mn} \zeta_n w_n,$$

where $0 \leq a_j < |e_j|$ for $j=1, 2, \dots, mn$. The number of elements in T_k/Π' is just $|e_1 \cdots e_{mn}| = |\det A|$. Put

$$\beta_1 = \sum_{i=1}^m a_i \zeta_i, \beta_2 = \sum_{i=1}^n a_{m+i} \zeta_i, \dots, \beta_n = \sum_{i=1}^m a_{mn-m+i} \zeta_i$$

then each element of $I_{k/k}/\Pi$ is represented by a unique form:

$$\beta_1 w_1 + \dots + \beta_n w_n.$$

Since I_k/Π^l is a finite set, so is $I_{k/k}/\Pi$.

Step II. (1) $I_{k/k}$ is integrally closed (iii) of Theorem 1.

(2) $I_{k/k}$ is a Noetherian ring.

Suppose a series of ideals $\Pi_1 \subset \Pi_2 \subset \dots$ in $I_{k/k}$. Then there corresponds a series of ideals $\Pi_1' \subset \Pi_2' \subset \dots$ in I_k .

By (*) above there exists a positive rational integer l such that $\Pi_l' = I_k$. Thus $\Pi_l = I_{k/k}$ and $I_{k/k}$ is Noetherian.

(3) For a prime ideal Π of $I_{k/k}$ the integral domain $I_{k/k}/\Pi$ is a finite set as above.

This implies that $I_{k/k}/\Pi$ is a field. Hence Π is a maximal ideal of $I_{k/k}$.

Summing up the above things, $I_{k/k}$ is a Dedekind integral domain. ///

References

1. K. Kawada: Number Theory Vol. I ~ III Euwananri Book Company (1976)
2. D. Ko: A study on the ring $I_{k/k}$ of integers and Fractional Ideals of k/k . Theses. Hangang Univ. (1985)
3. T. Takagi: Algebraic Number Theory, Euwananri Book company (1972)

Seoul Educational College,
Seoul (100), Korea.