INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY. CABLE: CENTRATOM TRIESTE

SMR.637/32

ADVANCED WORKSHOP ON ARITHMETIC ALGEBRAIC GEOMETRY

(31 August - 11 September 1992)

Classical Algebraic Number Theory (1)
Ring of Integers, Norm, Trace and Discriminant

M. Bilhan
Department of Mathematics
Middle East Technical University
Inonu Bulvari
06531 Ankara
Turkey

Ring of Integers, Norm, Trace and Discriminant

M. Bilhan
METU, Department of Mathematics,
06531 - Ankara - Turkey

Some Definitions

An algebraic number field (or a number field) is a finite extension K of the field $\mathbb{Q}$ of rational numbers.

Let α be a complex number. α is said to be an algebraic number if it is algebraic over $\mathbb{Q}$, ie if $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some integer $n \geq 1$ and rational numbers $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. α is said to be an algebraic integer if it is integral over $\mathbb{Z}$, ie if $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $n \geq 1$ and $a_0, \ldots, a_{n-1}$ integers ($\in \mathbb{Z}$).

Other characterizations of algebraic integers:

Lemma 1. For a complex number α, the following are equivalent:

(i) α is integral over $\mathbb{Z}$,

(ii) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module,

(iii) There is a subring B of $\mathbb{C}$ containing $\mathbb{Z}$ and α, such that B is a finitely generated $\mathbb{Z}$-module,

(iv) α is algebraic over $\mathbb{Q}$, with minimal polynomial $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$.

Pf. For the equivalences (i)⇔(ii)⇔(iii) see, for example, [13], Chap. II. Later, we shall prove that (i)⇒(iv).

The Ring of Integers of a Number Field

Let K be a number field and define the set

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ integral over } \mathbb{Z}\}.$$

Theorem 1. $\mathcal{O}_K$ is a subring of K containing $\mathbb{Z}$. The field of fractions of $\mathcal{O}_K$ is K. More precisely:
(*) $\forall \alpha \in K, \exists \beta \in \mathcal{O}_K, \exists c \in \mathbb{Z}$ such that $\alpha = \frac{\beta}{c}$.
Moreover $\mathcal{O}_K$ is integrally closed (ie any element of K which is integral over $\mathcal{O}_K$ belongs to $\mathcal{O}_K$).

Definition. $\mathcal{O}_K$ is called the ring of integers of K. Any element of $\mathcal{O}_K$ is called an integer of K.

Pf of Tm 1. Using the equivalent characterizations given by Lemma 1:

$$\alpha, \beta \in \mathcal{O}_K \overset{\text{(by ii)}}{\Rightarrow} \mathbb{Z}[\alpha] = \sum_{\text{finite}} \mathbb{Z}\alpha_i, \quad \mathbb{Z}[\beta] = \sum_{\text{finite}} \mathbb{Z}\beta_j$$

$$\Rightarrow \mathbb{Z}[\alpha,\beta] = \sum_i \sum_j \mathbb{Z}\alpha_i\beta_j \quad \left(\text{finitely generated } \mathbb{Z}\text{-modules}\right)$$

Since $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta \in \mathbb{Z}[\alpha,\beta]$ we conclude (by Lemma 1 (iii)) that $\mathcal{O}_K$ is a subring of K.

To prove (*): Let $\alpha \in K$. Then α is algebraic over $\mathbb{Q}$, so $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$. Let c be the least common multiple of the denominators of $a_0, \ldots, a_{n-1}$. Multiplying the above equation by c^n we see that $c\alpha$ [illegible]

To prove that $\mathcal{O}_K$ is integrally closed, let $\alpha \in K$ be integral over $\mathcal{O}_K$, ie $\alpha^m + b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0 = 0$ for some $b_0, b_1, \ldots, b_{m-1} \in \mathcal{O}_K$. Then see again [13], Chap. II to prove that α is integral over $\mathbb{Z}$, ie $\alpha \in \mathcal{O}_K$.

Norm and Trace

Let L/K be a finite extension of number fields. For $\alpha \in L$, consider the map $m_\alpha : L \longrightarrow L$ defined by $m_\alpha(\beta) = \alpha\beta$ for any $\beta \in L$ (multiplication by α). m_α is a K-linear operator of L. Let $\Delta_{m_\alpha} = \det(xI_L - m_\alpha)$ be the characteristic polynomial of m_α. Then for $n = [L:K]$,

$$\Delta_{m_\alpha} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$
$$= \prod_{i=1}^{n} (x - \alpha_i) \quad (\text{where } \alpha_i \in \mathbb{C}\ i = 1, \ldots, n)$$

Def. The trace of α wrt L/K, denoted $\mathrm{Tr}_{L/K}(\alpha)$ is defined to be the trace of the linear operator m_α and the norm of α wrt L/K, denoted $N_{L/K}(\alpha)$ is defined to be the determinant of m_α.

ie $$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha) = -a_{n-1} = \sum_{i=1}^{n} \alpha_i$$
$$N_{L/K}(\alpha) = \det(m_\alpha) = (-1)^n a_0 = \prod_{i=1}^{n} \alpha_i$$

So $\mathrm{Tr}_{L/K} : L \longrightarrow K$ is an additive homomorphism

and N [illegible] $: L^* \longrightarrow K^*$ is a multiplicative "

Since Δ_{m_α} is a polynomial with coefficients in K, it is invariant under each K-embedding $\sigma_i : L \hookrightarrow \mathbb{C}$ and $\sigma_i(\alpha) = \alpha_i$ for some $i=1,\dots,n$.

Denoting by $\sigma_1,\dots,\sigma_n$ all K-embeddings of L, we get

$$Tr_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad , N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) .$$

Remarks.

1. $Tr_{L/K}(c) = nc$ and $N_{L/K}(c) = c^n$ if $c \in K$.

2. If $\alpha \in \mathcal{O}_L$, then for any $i=1,\dots,n$ $\sigma_i(\alpha)$ is integral over $\mathbb{Z}$, so $\sigma_i(\alpha) \in \mathcal{O}_L$. So for $\alpha \in \mathcal{O}_L$:

$$Tr_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \in \mathcal{O}_L \cap K = \mathcal{O}_K \text{ and}$$

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathcal{O}_L \cap K = \mathcal{O}_K .$$

3. Suppose $\alpha \in \mathcal{O}_K$. Then all conjugates of α are in $\mathcal{O}_K$. Since the coefficients of $Irr(\alpha,\mathbb{Q})$ can be expressed in symmetric polynomials of these conjugates, these coefficients lie in $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. This proves that (i)⇒(iv) in Lemma 1.

Theorem 2. If K is a number field of degree $n = [K:\mathbb{Q}]$, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof: Using the property (*) in Theorem 1, one can choose an algebraic integer as a primitive element of K, ie $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis of K over $\mathbb{Q}$ and $\mathbb{Z}[\alpha]$ is a free $\mathbb{Z}$-module of rank n contained in $\mathcal{O}_K$.

Now, we need two lemmas to finish the proof.

Lemma 2. Let M be a sub-$\mathbb{Z}$-module of a number ring K. Define the complementary set of M by

$$M^* = \{ \beta \in K \mid Tr_{K/\mathbb{Q}}(\beta M) \subset \mathbb{Z} \} .$$

Obviously M^* is a sub-$\mathbb{Z}$-module of K.

(a) If $M = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_r$, then $M^* = \mathbb{Z}\alpha_1^* \oplus \cdots \oplus \mathbb{Z}\alpha_r^*$ where $\{\alpha_1^*,\dots,\alpha_r^*\}$ is the dual basis wrt $Tr_{K/\mathbb{Q}}$, ie $Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j^*) = \delta_{ij}$ $\forall (i,j)$.

In particular, if M is free of rank r, so is M^*.

(b) If M_1 and M_2 are two sub-$\mathbb{Z}$-modules of M, then $M_1 \subset M_2 \Rightarrow M_2^* \subset M_1^*$.

The proof is left as exercise.

The next lemma is the main theorem on finitely generated $\mathbb{Z}$-modules:

Lemma 3. Let M be a free $\mathbb{Z}$-module of rank n and M' be a sub-$\mathbb{Z}$-module of M. Then M' is a free $\mathbb{Z}$-module of rank $q \le n$ and there is a basis $\{\omega_1,\dots,\omega_n\}$ of M and there are positive integers $c_1,\dots,c_q$ such that $c_i | c_{i+1}$ for each $i=1,\dots,q-1$ and $\{c_1\omega_1,\dots,c_q\omega_q\}$ is a basis of M'.

Now we may complete the proof of Theorem 2:

$\mathbb{Z}[\alpha] \subset \mathcal{O}_K \subset \mathcal{O}_K^*$ and $\mathcal{O}_K^* \subset \mathbb{Z}[\alpha]^*$ (by Lemma 2)

Since $\mathbb{Z}[\alpha]$ is free of rank n, so is $\mathbb{Z}[\alpha]^*$ (by

Lemma 2). But $\mathbb{Z}[\alpha] \subset \mathcal{O}_K \subset \mathbb{Z}[\alpha]^*$, so we conclude by Lemma 3, that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Definition. A basis $\{\alpha_1, \dots, \alpha_n\}$ of $\mathcal{O}_K$ as a free $\mathbb{Z}$-module is called an integral basis of K.

Absolute Norm of an Ideal

Definition. Let $\mathfrak{n}$ be an ideal of $\mathcal{O}_K$ for a number field K. The absolute norm (or norm) of $\mathfrak{n}$ is $N(\mathfrak{n}) = \left|\mathcal{O}_K/\mathfrak{n}\right|$.

Proposition 1. If $\alpha \in \mathcal{O}_K$, then $N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.

Proof: $\alpha\mathcal{O}_K \subset \mathcal{O}_K$ and $\mathcal{O}_K \cong \alpha\mathcal{O}_K$ as $\mathbb{Z}$-modules. Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, $\alpha\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. By Lemma 3, there exist a basis $\{\omega_1, \dots, \omega_n\}$ of $\mathcal{O}_K$ and positive integers $c_1, \dots, c_n$ s.t. $c_i | c_{i+1}$ and $\{c_1\omega_1, \dots, c_n\omega_n\}$ is a basis of $\alpha\mathcal{O}_K$. Then

$$\mathcal{O}_K/\alpha\mathcal{O}_K \cong \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n \Big/ \mathbb{Z}c_1\omega_1 \oplus \cdots \oplus \mathbb{Z}c_n\omega_n$$

$$\cong \mathbb{Z}/(c_1) \oplus \cdots \oplus \mathbb{Z}/(c_n)$$

$$\Rightarrow N(\alpha\mathcal{O}_K) = c_1 \cdots c_n .$$

Let $\varphi : \mathcal{O}_K \longrightarrow \alpha\mathcal{O}_K$ be the $\mathbb{Z}$-linear map defined by $\varphi(\omega_i) = c_i\omega_i$ $(\forall i)$. Then φ is an isomorphism. Let $\psi : \alpha\mathcal{O}_K \longrightarrow \alpha\mathcal{O}_K$ be the $\mathbb{Z}$-linear map defined by $\psi(c_i\omega_i) = \alpha\omega_i$ $(i = 1, \dots, n)$. Then ψ is an automorphism of the $\mathbb{Z}$-module $\alpha\mathcal{O}_K$. So $\det\psi = \pm 1$. But $m_\alpha = \psi \circ \varphi$. So

$$N_{K/\mathbb{Q}}(\alpha) = \det m_\alpha = \pm \det\varphi = \pm c_1 \cdots c_n$$

This proves the result.

Corollary. The norm of any ideal of $\mathcal{O}_K$ is finite.

Proof: Take $\mathfrak{n} \subset \mathcal{O}_K$ an ideal and let $\alpha \in \mathfrak{n}$.

$$\alpha\mathcal{O}_K \subset \mathfrak{n} \Rightarrow N(\mathfrak{n}) = \left|\mathcal{O}_K/\mathfrak{n}\right| \leq \left|\mathcal{O}_K/\alpha\mathcal{O}_K\right| = |N_{K/\mathbb{Q}}(\alpha)|$$

Discriminant

Let L/K be a finite extension of number fields of degree $[L:K] = n$. The discriminant of a subset $\{\alpha_1, \dots, \alpha_n\}$ of L is defined by

$$D(\alpha_1, \dots, \alpha_n) = \det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{i,j}$$

Proposition 2. Let $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ and $\mathcal{B}' = \{\beta_1, \dots, \beta_n\}$ be two bases of L over K. If A is the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$, then

$$D(\beta_1, \dots, \beta_n) = (\det A)^2 D(\alpha_1, \dots, \alpha_n) .$$

Pf : $\left(\mathrm{Tr}(\beta_i\beta_j)\right)_{i,j} = A \left(\mathrm{Tr}(\alpha_i\alpha_j)\right)_{i,j} A^t$

$\Rightarrow$ result.

Definition. The discriminant (or absolute discriminant) d_K of a number field K is defined to be the discriminant of any integral basis $\{\alpha_1,\dots,\alpha_n\}$ of K.

ie $d_K = D(\alpha_1,\dots,\alpha_n) = \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{i,j}$.

Remark. The definition of the absolute discriminant d_K is independent from the choice of the integral basis. Because the change of basis matrix A from an integral basis to another integral basis must have determinant equal to ± 1.

Proposition 3. Let L/K be a finite extension of number fields of degree $[L:K]=n$ and let $\sigma_1,\dots,\sigma_n : L \hookrightarrow \mathbb{C}$ be the distinct K-embeddings of L. Then
$D(\alpha_1,\dots,\alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0$.

Proof: $\mathrm{Tr}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$

This is the (i,j)-entry of the matrix MM^t

where $M = \left(\sigma_k(\alpha_i)\right)_{i,k}$. So $D(\alpha_1,\dots,\alpha_n) = (\det M)^2$.

To prove : $\det M \neq 0$.

Suppose $\det M = 0$. Then there exist $a_1,\dots,a_n$ complex numbers, not all zero, such that $\sum_{i=1}^{n} a_i \sigma_k(\alpha_j) = 0 \quad \forall j=1,\dots,n$. This implies that $\sum_{i=1}^{n} a_i \sigma_i = 0$ and contradicts the linear independence of $\sigma_1,\dots,\sigma_n$ over $\mathbb{C}$.

Remark. If $L=K(\alpha)$, then $\{1,\alpha,\dots,\alpha^{n-1}\}$ is a basis of L over K. Let f be the minimal polynomial of α over K. Then the roots of f are the conjugates of α, ie $\sigma_i(\alpha) = \alpha_i$ $(i=1,\dots,n)$ with the notations of Proposition 3. Then

$$D(1,\alpha,\dots,\alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2 = \det(\alpha_i^j)^2$$
$$= \prod_{i\neq j} (\alpha_i - \alpha_j) \quad \left(\text{Vandermonde determinant}\right)$$
$$\neq 0$$

This result also proves that the discriminant of any basis of L over K is nonzero (combining with Proposition 2), ie another proof for the last part of Proposition 3.

Dedekind Domains

Definition. A Dedekind domain is an integral domain such that
(i) Every ideal is finitely generated (ie D is Noetherian),
(ii) Every nonzero prime ideal of D is a maximal ideal (ie D has Krull dimension 1),
(iii) D is integrally closed (ie every element of the field of fractions of D which is integral over D belongs to D).

Remark: (i) $\Leftrightarrow$ every increasing sequence of ideals of D is stationnary
$\Leftrightarrow$ every nonempty set of ideals of D has a maximal element.

Examples. 1. Every field is trivially a Dedekind domain. From now on, we shall consider the Dedekind domains which are not a field.
2. Any principal ideal domain is a Dedekind domain.

Remark. A unique factorization domain is not necessarily a Dedekind domain. For example $\mathbb{Z}[x,y]$ is not a Dedekind domain.

The next theorem furnishes the most important example for our purpose.

Theorem 3. For every number field K, the ring of integers $\mathcal{O}_K$ is a Dedekind domain.

Proof: By Theorem 2, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n=[K:\mathbb{Q}]$.
(i) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. By Lemma 3, $\mathfrak{a}$ is a free sub-$\mathbb{Z}$-module of $\mathcal{O}_K$ of finite rank. So $\mathfrak{a}$ is finitely generated as an ideal.
(ii) Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. By Corollary of Proposition 1, $|\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p}) < \infty$. Being a finite integral domain, $\mathcal{O}_K/\mathfrak{p}$ is a field. Hence $\mathfrak{p}$ is a maximal ideal.
(iii) By Theorem 1, $\mathcal{O}_K$ is integrally closed.
Thus we proved that $\mathcal{O}_K$ is a Dedekind domain.

Fractional Ideals of a Dedekind Domain

Let D be a Dedekind domain with field of fractions K.

Def. A fractional ideal $\mathfrak{a}$ of D is a D-submodule of K such that $d\mathfrak{a} \subset D$ for some $0 \neq d \in D$.

Remark 1. Every ideal $\mathfrak{a} \subset D$ is a fractional ideal, called integral ideal if there may be confusion.

Remark 2. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional ideals of D. Then

$\mathfrak{a}+\mathfrak{b} = \{\alpha+\beta \mid \alpha\in\mathfrak{a}, \beta\in\mathfrak{b}\}$, $\mathfrak{a}\cap\mathfrak{b}$ and $\mathfrak{a}\mathfrak{b} = \{\sum_{\text{finite}} \alpha_i\beta_i \mid \alpha_i\in\mathfrak{a}, \beta_i\in\mathfrak{b}\}$ are fractional ideals of D.

Remark 3. The nonzero fractional ideals of D constitute a commutative monoid for multiplication. We shall see that they form an abelian group.

Proposition 4. Let D be a Dedekind domain which is not a field. For any maximal ideal $\mathfrak{m}$ of D there is a fractional ideal $\mathfrak{m}'$ of D such that $\mathfrak{m}\mathfrak{m}' = D$ ($\mathfrak{m}'$ is called the inverse of $\mathfrak{m}$ and denoted by $\mathfrak{m}' = \mathfrak{m}^{-1}$).

Sketch of the proof: Let K = field of fractions of D. $\mathfrak{m}' = \{\alpha\in K \mid \alpha\mathfrak{m}\subset D\}$ is the required ideal (for details of the proof, see [13], Chap. on Dedekind domains).

Theorem 4. Let D be a Dedekind domain and let P be the set of nonzero prime ideals of D.
i) Any nonzero fractional ideal $\mathfrak{a}$ of D can be written uniquely in the form

$$\mathfrak{a} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})} \quad \text{with } n_{\mathfrak{p}}(\mathfrak{a})\in\mathbb{Z}, \text{ almost all zero}$$

ii) The nonzero fractional ideals of D form a free abelian group generated by P.

Pf: (b) is an obvious consequence of (a). It suffices then to prove (a). For any fractional ideal $\mathfrak{a}$, $d\mathfrak{a}$ is an integral ideal for some $0\neq d\in D$. So it is enough to prove (a) for integral ideals of D.

Let Φ be the set of nonzero integral ideals of D which are not a finite product of prime ideals. Our aim is to prove that Φ is empty. Suppose $\Phi\neq\emptyset$. Since D is Noetherian, Φ contains a maximal element $\mathfrak{b}$. Necessarily $\mathfrak{b}\neq D$ and $\mathfrak{b}$ is not a maximal ideal in D. So $\mathfrak{b}\subsetneq\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of D. Let $\mathfrak{m}'$ be the fractional ideal such that $\mathfrak{m}\mathfrak{m}' = D$ (by Proposition 4).

$$\mathfrak{b}\subsetneq\mathfrak{m} \Rightarrow \mathfrak{b}\mathfrak{m}'\subsetneq\mathfrak{m}\mathfrak{m}' = D.$$

But $D\subsetneq\mathfrak{m}' \Rightarrow \mathfrak{b} = \mathfrak{b}D \subsetneq \mathfrak{b}\mathfrak{m}'$.

So $\mathfrak{b}\subsetneq\mathfrak{b}\mathfrak{m}'\subsetneq D$.

So $\mathfrak{b}\mathfrak{m}'$ is an integral ideal $\neq 0$ containing $\mathfrak{b}$ strictly. So $\mathfrak{b}\mathfrak{m}'\notin\Phi$. So $\mathfrak{b}\mathfrak{m}' = \mathfrak{p}_1\cdots\mathfrak{p}_s$ for some $\mathfrak{p}_1,\dots,\mathfrak{p}_s\in P$. But this implies that $\mathfrak{b} = \mathfrak{m}\mathfrak{p}_1\cdots\mathfrak{p}_s$, which is a contradiction. This proves the "existence part" of (a).

For the uniqueness : Suppose

$$\prod \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})} = \prod \mathfrak{p}^{n'_{\mathfrak{p}}(\mathfrak{a})}$$ for some integers

$n_{\mathfrak{p}}(\mathfrak{a})$, $n'_{\mathfrak{p}}(\mathfrak{a})$ almost all equal to 0.

$$\Rightarrow \prod \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a}) - n'_{\mathfrak{p}}(\mathfrak{a})} = D .$$

If all $n_{\mathfrak{p}}(\mathfrak{a}) - n'_{\mathfrak{p}}(\mathfrak{a})$ are not 0, separating positive and negative exponents, we get an expression of the form

$$\mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r} = \mathfrak{a}_1^{h_1} \cdots \mathfrak{a}_t^{h_t}$$

for some nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{a}_1, \ldots, \mathfrak{a}_t$ two by two distinct, with $k_1, \ldots, k_r, h_1, \ldots, h_t > 0$ integers.

$\Rightarrow \mathfrak{p}_1 \supset \mathfrak{a}_1^{h_1} \cdots \mathfrak{a}_t^{h_t}$, $\mathfrak{p}_1$ prime ideal

$\Rightarrow \mathfrak{p}_1$ contains at least one of the factors, say $\mathfrak{p}_1 \supset \mathfrak{a}_1$.

But in the Dedekind domain all prime ideals which are nonzero are maximal. So we get $\mathfrak{p}_1 = \mathfrak{a}_1$, which is a contradiction.

Thus the Theorem 4 is proved.

Class Group of a Dedekind Domain D

The nonzero fractional ideals of D form a group $\mathcal{J}(D)$. The nonzero principal fractional ideals αD with $\alpha \in K^*$ (K = field of fractions of D) form a subgroup $\mathcal{H}(D) = \{\alpha D \mid \alpha \in K^*\}$.

Definition. The group $Cl(D) = \mathcal{J}(D) / \mathcal{H}(D)$ is called the class group of D.

Remarks:

1. D is a PID $\Leftrightarrow Cl(D) = \{1\}$
2. In case of a Dedekind domain D :
   D is a PID $\Leftrightarrow$ D is a UFD.
3. For any number field K, the class group $Cl(\mathcal{O}_K)$ is finite, its order h_K is called the class number of K. This important theorem of Algebraic Number Theory will be proved by Kenku (see also [13], the Charter concerning the class group and units).

Properties of the Exponents $n_{\mathfrak{p}}(\mathfrak{a})$:

Let D be a Dedekind domain, with field of fractions $K \neq D$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two

nonzero fractional ideals of D. Then, with the notations of Theorem 4:

(i) $n_p(\mathfrak{a}\mathfrak{b}) = n_p(\mathfrak{a}) + n_p(\mathfrak{b}) \quad \forall p \in P$

(ii) $\mathfrak{b} \subset D \Leftrightarrow n_p(\mathfrak{b}) \geq 0 \quad \forall p \in P$

(iii) $\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow \mathfrak{a}\mathfrak{b}^{-1} \subset D \overset{(\text{def})}{\Leftrightarrow} \mathfrak{b} \mid \mathfrak{a}$

$\Leftrightarrow n_p(\mathfrak{b}) \leq n_p(\mathfrak{a}) \quad \forall p \in P$

(iv) $n_p(\mathfrak{a}+\mathfrak{b}) = \mathrm{Inf}\left(n_p(\mathfrak{a}), n_p(\mathfrak{b})\right) \quad \forall p \in P$

For division introduced in (iii):

$\mathfrak{a}+\mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b})$.

(v) $n_p(\mathfrak{a}\cap\mathfrak{b}) = \mathrm{Sup}\left(n_p(\mathfrak{a}), n_p(\mathfrak{b})\right)$

For division in (iii):

$\mathfrak{a}\cap\mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$.

Some Textbooks on Algebraic Number Theory

[1] Z.I. Borevich and I.R. Shafarevich, Number Theory, Academic Press, 1966.

[2] J.W.S. Cassels, Local Fields, Cambridge University Press, 1986.

[3] J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, 1967.

[4] J.S. Chahal, Topics in Number Theory, Plenum Press.

[5] H. Cohn, A Classical Invitation to Algebraic Numbers, Springer.

[6] H. Hasse, Zahlentheorie, Akademie Verlag Berlin, 1949 (reimpressed by Springer).

[7] H. Hasse, Vorlesungen über Zahlentheorie, Springer Grundlehren 59 (2d ed. 1964).

[8] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig, 1923 (reimpressed by Chelsea).

[9] G.J. Janusz, Algebraic Number Fields, Academic Press, 1973.

[10] S. Lang, Algebraic Number Theory, Addison Wesley, 1970.

[11] D.A. Marcus, Number Fields, Springer, 1977.

[12] P. Ribenboim, Algebraic Numbers, Wiley-Interscience, 1972

[13] P. Samuel, Théorie Algébrique des Nombres, Hermann, 1967.

[14] J.P. Serre, Corps Locaux, Hermann, 1968.

[15] N. Schappacher, Notes on Algebraic Number Theory, Isfahan Workshop on Geometry and Algebra, May 1992 (manuscript).

[16] E. Weiss, Algebraic Number Theory, McGraw Hill, 1963

[17] A. Weil, Basic Number Theory, Springer