Notes on Algebraic Number Theory

Apiros3

First Version : Apr 15, 2025
Last Update : Jan 29, 2025

Contents

1 Introduction **2**

2 Definitions **2**

3 Specific Domains **4**

3.1 Unique Factorization Domain 4

4 Ring of Integers **5**

4.1 Fermat's Theorems 7

5 Ideals **7**

5.1 Unique Factorization of Ideals 7

5.1.1 Class Number 8

5.1.2 Ideal Classes as Groups 10

6 Notes **11**

1 Introduction

Some background lemmas :

- Gauss's Lemma (irreducible in $\mathbb{Z}[t]$ implies irreducible in $\mathbb{Q}[t]$), content function to show there exists $\lambda \neq 0$ such that λg, $\lambda^{-1}h \in \mathbb{Z}[t]$.
- Eisenstein

Definition 1.0.1. *A **number field** or **algebraic number field** is a finite extension K of $\mathbb{Q}$. The index $[K : \mathbb{Q}]$ is the **degree** of the number field.*

Theorem 1.0.2. *If K is a number field, then $K = \mathbb{Q}(\theta)$ for some algebraic number $\theta \in K$.*

Theorem 1.0.3. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct monomorphisms (embeddings)*

$$\sigma_i : K \to \mathbb{C}$$

The elements $\sigma_i(\theta)$ are the distinct zeros in $\mathbb{C}$ of the minimal polynomial m_θ of θ over $\mathbb{Q}$.

Definition 1.0.4. *If $\sigma_i(K) \subseteq \mathbb{R}$, then σ_i is called a **real embedding**, otherwise it is called a **complex embedding**.*

Definition 1.0.5. *A square matrix over $\mathbb{Z}$ is called **unimodular** if it has determinant ± 1.*

Note that A is unimodular if and only if A^{-1} has coefficients in $\mathbb{Z}$. (Proof sketch, by considering what EROs transform A into an identity.)

Lemma 1.0.6. *Let G be a free abelian group of rank n with $\mathbb{Z}$-basis $\{x_1, \ldots, x_n\}$. Suppose (a_{ij}) is a square matrix with integer entries. Let*

$$y_i = \sum_j a_{ij} x_j$$

Then the elements $\{y_1, \ldots, y_n\}$ form a $\mathbb{Z}$-basis for G if and only if (a_{ij}) is unimodular.

Proof. TODO!! □

Theorem 1.0.7. *Let G be a free abelian group of rank n, and H be a subgroup. Then G/H is finite if and only if H has rank n. Moreover, if G and H have $\mathbb{Z}$-basis $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ with $y_i = \sum_j a_{ij} x_j$, we have*

$$\#G/H = |\det(a_{ij})|$$

Proof. TODO!!! □

2 Definitions

Definition 2.0.1. *Let $K|\mathbb{Q}$ be an algebraic number field of degree n, and let $\alpha \in K$. Let $\sigma_i : K \to \mathbb{C}$ be the n embeddings. We call $\sigma_i(\alpha)$ the K**-conjugates** of α.*

*We define the **trace** to be $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ and the **norm** $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = N_{K|\mathbb{Q}}(\alpha) = N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$. When $K = \mathbb{Q}(\alpha)$, we call these the **absolute conjugates, trace,** and **norm**.*

Proposition 2.0.2. *We record the following properties :*

- *For any $K = \mathbb{Q}(\beta)$, suppose that β has minimal polynomial $m_\beta(X)$. If $\beta_1, \ldots, \beta_n$ are the n roots of m_β in $\mathbb{C}$, then one can choose embeddings $\sigma_i : \beta \to \beta_i$.*
- $\mathrm{Norm}_{K|\mathbb{Q}}(\gamma\delta) = \mathrm{Norm}_{K|\mathbb{Q}}(\gamma)\mathrm{Norm}_{K|\mathbb{Q}}(\delta)$
- $\mathrm{Norm}_{K|\mathbb{Q}}(\gamma) = 0$ *if and only if* $\gamma = 0$.
- $\mathrm{Norm}_{K|\mathbb{Q}}(q) = q^n$ *for* $q \in \mathbb{Q}$.
- *If $K = \mathbb{Q}(\alpha)$ and $m_\alpha(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$, then we have $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = (-1)^n c_0$ and $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = -c_{n-1}$. In particular, the norm and trace are both in $\mathbb{Q}$. Generally speaking, for any $K = \mathbb{Q}(\beta)$, $\alpha \in K$, the norm and trace of α are symmetric functions of the conjugates of $\sigma_i(\alpha)$, thus in $\mathbb{Q}$.*

Proof. Immediate. The last line follows as a consequence of the Fundamental Theorem on the theory of symmetric functions. □

Definition 2.0.3. *Let $w = \{w_1, \ldots, w_n\}$ be a n-tuple of elements of K, where $n = [K : \mathbb{Q}]$.*

- *The **determinant** is* $\Delta(w) := \det(\sigma_i(w_j))$
- *The **discriminant** of w is* $\Delta(w)^2$

Lemma 2.0.4. $\Delta(w)^2 = \det(\mathrm{Tr}_{K|\mathbb{Q}}(w_i w_j))$ *and consequently* $\Delta(w)^2 \in \mathbb{Q}$.

Proof. Let $A = (\sigma_i(w_j))$. Then,

$$\Delta(w)^2 = \det(A)^2 = \det(A^T A) = \det\left(\sum_k \sigma_k(w_i)\sigma_k(w_j)\right)$$

$$= \det\left(\sum_k \sigma_k(w_i w_j)\right) = \det(\mathrm{Tr}_{K|\mathbb{Q}}(w_i w_j))$$

□

Lemma 2.0.5. *If $v = \{v_1, \ldots, v_n\}$ is a basis for $K|\mathbb{Q}$ and $w = \{w_1, \ldots, w_n\} \subseteq K$ with $w_i = \sum_j c_{ij} v_j$ and $c_{ij} \in \mathbb{Q}$, then*

$$\Delta(w) = \det(C)\Delta(v)$$

Proof. Write $A_v = (\sigma_i(v_j))$ and $A_w = (\sigma_i(w_j))$ such that $\Delta(v) = \det(A_v)$ and $\Delta(w) = \det(A_w)$. Now,

$$A_w = (\sigma_i(w_j)) = \left(\sigma_i\left(\sum_k c_{jk} v_k\right)\right) = \left(\sum_k c_{jk}\sigma_i(v_k)\right) = A_v C^T$$

The proof thus follows by taking det on both sides. □

Lemma 2.0.6. *If $K = \mathbb{Q}(\alpha)$ and $v = \{1, \alpha, \ldots, \alpha^{n-1}\}$, then*

$$\Delta(v)^2 = \prod_{i<j}(\alpha_j - \alpha_i)^2$$

where α_i are the conjugates of α.

Proof. Note first that

$$\Delta(v) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}$$

which is the so-called van der Monde determinant. We note that this is a polynomial of degree $n(n-1)/2$ in $\alpha_1, \ldots, \alpha_n$. As it vanishes when we set $\alpha_i = \alpha_j$, the polynomial is divisible by $\alpha_i - \alpha_j$ for all $i < j$. There are $n(n-1)/2$ such factors. By observing the diagonal, the coefficient of $\alpha_2\alpha_3^2 \cdots \alpha_n^{n-1}$ is 1, so we must have

$$\Delta(v) = \prod_{i<j} (\alpha_j - \alpha_i)$$

□

Corollary 2.0.7. $\Delta(w_1, \ldots, w_n) \neq 0$ *if and only if* $w_1, \ldots, w_n$ *is a basis for* $K|\mathbb{Q}$*.*

Proof. Suppose $K = \mathbb{Q}(\alpha)$ and let $v = \{1, \alpha, \ldots, \alpha^{n-1}\}$. Noting the previous lemma, as α_i are distinct, we must have $\Delta(v) \neq 0$.

By Lemma 2.0.5, using C as a change of basis, $\Delta(w) \neq 0$ for any other basis w of $K|\mathbb{Q}$. If w is not a basis, then $\det(C) = 0$, giving $\Delta(w) = 0$. □

3 Specific Domains

3.1 Unique Factorization Domain

Definition 3.1.1. *R is a* ***unique factorisation domain*** *if R is an integral domain, and for all nonzero and nonunit $\alpha \in R$, there exists irreducible $\beta_1, \ldots, \beta_n \in R$ such that*

1. $\alpha = \beta_1, \ldots, \beta_n$
2. *If $\alpha = \gamma_1, \ldots, \gamma_m$ with irreducible γ_i, then $m = n$ and there exists a permutation σ such that β_i and $\gamma_{\sigma(i)}$ are conjugates.*

Proposition 3.1.2. *Suppose that R is an integral domain in which factorisation into irreducibles is possible. Then the following are equivalent*

1. *Factorization is unique*
2. *Irreducible elements are prime*

Proof. Sketch. If the factorisation is unique and we have an irreducible p such that $p|xy$, $pc = xy$, by unique factorisation p is a factor of x or y.

If irreducible elements are prime, for any factorisation $\prod x_i$ and $\prod y_i$, taking x_i divides some y_j by primality, and by irreduciblity shows they are associates. We can inductively show factorisation is unique. □

4 Ring of Integers

Definition 4.0.1. *We say that $\alpha \in K$ is an **algebraic integer** if there exists a monic $g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$. We define $\mathcal{O}_K$ as the set of all algebraic integers in $\mathcal{O}$.*

Proposition 4.0.2. *Some basic properties :*

- *Suppose $\alpha \in K$. Then $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial is in $\mathbb{Z}[x]$ by Gauss's lemma.*
- *Pick any $\alpha \in K$ such that there is a monic polynomial $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0 \in \mathbb{Q}[x]$. Picking an n, we have*

  $$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \cdots + n^d a_0 = 0$$

  thus, picking an n to clear the denominators of all a_i, we get $n\alpha \in \mathcal{O}_K$.
- *The minimal polynomial of $r \in \mathbb{Q}$ is $x - r$ which is in $\mathbb{Z}[x]$ if and only if $r \in \mathbb{Z}$. Thus if $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$. Generally, $\mathbb{Z} \subseteq \mathcal{O}_K$.*

Proof. Immediate. □

Example 4.0.3 ($\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$)**.** Without loss of generality, we assume that $d \neq 1$ and is square-free. First note that $[K : \mathbb{Q}] = 2$, and K has a $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$.

Taking any $a, b \in \mathbb{Q}$, $\alpha = a + b\sqrt{d} \in K$. Noting $\sigma_1(\alpha) = a + b\sqrt{d}$ and $\sigma_2(\alpha) = a - b\sqrt{d}$, we have $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = 2a$ and $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = a^2 - db^2$. Given $b \neq 0$, we have $m_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$. Thus $\alpha \in \mathcal{O}_K$ if and only if $2a, a^2 - db^2 \in \mathbb{Z}$. Suppose that $\alpha \in \mathcal{O}_K$. Then $(2a)^2 - d(2b)^2 \in \mathbb{Z}$, giving $d(2b)^2 \in \mathbb{Z}$. Writing $2b = u/v$, we have $du^2v^{-2} \in \mathbb{Z}$, such that $v^2 | du^2$. As d is square free, we have $v|u$, giving $2b \in \mathbb{Z}$. Write $2a = A$ and $2b = B$ with $A, B \in \mathbb{Z}$. Then we have $A^2 \equiv dB^2 \mod 4$.

Now a case split,

- $d \equiv 2$ or $3 \mod 4$. Then we must have A, B both even, giving $a, b \in \mathbb{Z}$
- $d \equiv 1 \mod 4$. Then $A \equiv B \mod 2$, so a, b are both in $\mathbb{Z}$ or both in $\mathbb{Z} + 1/2$.
- $d \equiv 0 \mod 4$ does not occur as d is square free

Thus, we have

$$\mathcal{O}_K = \begin{cases} \langle 1, \sqrt{d} \rangle = \{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\} & d \equiv 2, 3 \mod 4 \\ \langle 1, \frac{1+\sqrt{d}}{2} \rangle = \{m + n\frac{1+\sqrt{d}}{2} \mid m, n \in \mathbb{Z}\} & d \equiv 1 \mod 4 \end{cases}$$

Lemma 4.0.4. *$\alpha \in K$ is an algebraic integer if and only if there exists a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq K$ such that $\alpha M \subseteq M$.*

Proof. Suppose that $\alpha \in \mathcal{O}_K$ such that $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$ with $a_i \in \mathbb{Z}$. Taking $M = \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$, we have $\alpha M \subseteq M$.

Conversely, suppose $M \subseteq K$ is a non-zero finitely generated $\mathbb{Z}$-module such that $\alpha M \subseteq M$. Take $w_1, \ldots, w_s$ to be a generating set for M, and write

$$\alpha w_i = \sum_j c_{ij} w_j$$

with $c_{ij} \in \mathbb{Z}$. Taking $C = (c_{ij})$, we have

$$(\alpha I - C)\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

such that α satisfies $\det(xI - C)$, a monic polynomial with integer coefficients. Thus $\alpha \in \mathcal{O}_K$. □

Theorem 4.0.5. *Let K be an algebraic number field. If $\alpha, \beta \in \mathcal{O}_K$, then $\alpha + \beta$, $\alpha\beta \in \mathcal{O}_K$.*

Proof. Suppose $\alpha, \beta \in \mathcal{O}_K$. By Lemma 4.0.4, we have finitely generated $\mathbb{Z}$-modules M, N such that $\alpha M \subseteq M$ and $\beta N \subseteq N$.

Now, MN is finitely generated, and

$$(\alpha + \beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN$$

It follows again from Lemma 4.0.4 that $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. □

Remark 4.0.6. The above also follows as a direct consequence from the fact given any A that is a subring of B, elements of B that are integral over A form a subring.

Corollary 4.0.7. *If $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha), \mathrm{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. Let $\alpha \in \mathcal{O}_K$. Then all the $K|\mathbb{Q}$ conjugates $\alpha_1, \ldots, \alpha_n$ belong to the splitting field of the minimal polynomial, $\mathcal{O}_L$. Now, $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) \in \mathcal{O}_L$ and $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathcal{O}_L$ by Theorem 4.0.5. Now the trace and norm are both in $\mathbb{Q}$, and $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$. □

Definition 4.0.8. *$\alpha \in \mathcal{O}_K$ is a **unit** if $\alpha^{-1} \in \mathcal{O}_K$.*

Lemma 4.0.9. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and let $\alpha, \beta \in \mathcal{O}_K$. Then,*

1. *α is a unit in $\mathcal{O}_K$ if and only if $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \pm 1$*
2. *If α and β are associates in $\mathcal{O}_K$, then $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \pm\mathrm{Norm}_{K|\mathbb{Q}}(\beta)$*
3. *If $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)$ is a rational prime (primes in $\mathbb{Z}$), then α is irreducible in $\mathcal{O}_K$.*

Proof. (i) Suppose that α is a unit. Then,

$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\mathrm{Norm}_{K|\mathbb{Q}}(\alpha^{-1}) = \mathrm{Norm}_{K|\mathbb{Q}}(\alpha\alpha^{-1}) = \mathrm{Norm}_{K|\mathbb{Q}}(1) = 1$$

which is a product of elements in $\mathbb{Z}$, so both are ± 1.

Conversely, if $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \pm 1$, let $\alpha_1, \ldots, \alpha_n$ be the $K|\mathbb{Q}$ conjugates with $\alpha = \alpha_1$. Then, $\alpha_1 \ldots \alpha_n = \pm 1$, such that $\alpha(\alpha_2 \ldots \alpha_n) = \pm 1$. Hence, $\alpha^{-1} = \pm(\alpha_2 \ldots \alpha_n)$, which is in $\mathcal{O}_L$ (the splitting field of the minimal polynomial) by Theorem 4.0.5. As K is a field, α^{-1} lies in K, giving $\alpha^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K$.

(ii) We have $\alpha = u\beta$ for some unit u, so

$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \mathrm{Norm}_{K|\mathbb{Q}}(u)\mathrm{Norm}_{K|\mathbb{Q}}(\beta) = \pm\mathrm{Norm}_{K|\mathbb{Q}}(\beta)$$

by (i)

(iii) Let $\alpha = \gamma\delta$. Then $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = p = \mathrm{Norm}_{K|\mathbb{Q}}(\gamma)\mathrm{Norm}_{K|\mathbb{Q}}(\delta)$ for some prime $p \in \mathbb{Z}$. The result again follows from (i) □

Remark 4.0.10. The converse for (*ii*) and (*iii*) are false. Take $K = \mathbb{Q}(\sqrt{-5})$, where the ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

Note first we have a factorisation $6 = 2 \cdot 3 = (1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$ in $\mathcal{O}_K$. Now, $\text{Norm}_{K|\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2$, so the norm in our factors are $4, 9, 6, 6$ respectively. If any of these elements are not irreducible, we should be able to find $\alpha = \beta\gamma$ such that the norm of β, γ lie in ± 2 or ± 3. Clearly, no such solutions exist. By Lemma 4.0.9 (*ii*), we see this factorisation is not unique.

Note that the norm for $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are equal but are not associates (only units are ± 1) Also, we have clearly exhibited an α that is irreducible with non-prime norm.

Definition 4.0.11. *$w_1, \ldots, w_n \in \mathcal{O}_K$ is said to be an* ***integral basis*** *for $\mathcal{O}_K$ if $\mathcal{O}_K = \{\sum_j c_j w_j \mid c_j \in \mathbb{Z}\}$.*

Equivalently, $w_1, \ldots, w_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$. We sometimes call this set the integral basis for K.

Example 4.0.12. Taking $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer such that $[K : \mathbb{Q}] = 2$, $\mathcal{O}_K$ has integral basis

$$\begin{cases} \{1, \sqrt{d}\} & d \equiv 2, 3 \text{ mod } 4 \\ \{1, \frac{1+\sqrt{d}}{2}\} & d \equiv 1 \text{ mod } 4 \end{cases}$$

4.1 Fermat's Theorems

Theorem 4.1.1. *If p is prime and $p \equiv 1$ mod 4, then there exists $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ and this decomposition is unique.*

Proof. □

Theorem 4.1.2. *The only integer solutions of $y^2 + 2 = x^3$ are $x = 3, y = \pm 5$*

Proof. □

Theorem 4.1.3. *If prime $p \equiv 1$ or 3 mod 8, then $p = x^2 + 2y^2$ uniquely.*

Proof. □

Theorem 4.1.4. *If prime $p \equiv 1$ mod 3 then $p = x^2 + 3y^2$.*

5 Ideals

5.1 Unique Factorization of Ideals

Definition 5.1.1. *Let K, L be fields with $K \subseteq L$. Let I be an ideal of $\mathcal{O}_K$. Then $I \cdot \mathcal{O}_L$ is defined to be the ideal of $\mathcal{O}_L$ generated by the products of the form $i\ell$ such that $i \in I$ and $\ell \in \mathcal{O}_L$.*

Proposition 5.1.2. *Given ideals I, J of $\mathcal{O}_K$, a principal ideal $(a) = a\mathcal{O}_K$ of $\mathcal{O}_K$,*

1. *$(IJ) \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)(J \cdot \mathcal{O}_L)$*
2. *$I^n \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)^n$*
3. *$(a) \cdot \mathcal{O}_L = a\mathcal{O}_L$ (principal ideals are generated by the same element)*

Proof. The first is simply an expansion of both sides, then double inclusion. The second follows by induction using the first statement. The third statement is straightforward from definitions. □

5.1.1 Class Number

Definition 5.1.3. *Let I and J be non-zero ideals of $\mathcal{O}_K$. Then we write $I \sim J$ if there exist $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ such that $I(\alpha) = J(\beta)$.*

Proposition 5.1.4. *The relation $\sim$ gives an equivalence relation.*

Proof. Reflexivity and symmetry are immediate. For transitivity, if we have $I(\alpha) = J(\beta)$ and $J(\gamma) = K(\delta)$, we see that

$$I(\alpha\gamma) = I(\alpha)(\gamma) = J(\beta)(\gamma) = J(\gamma)(\beta) = K(\delta)(\beta) = K(\delta\gamma)$$

In particular, $I \sim K$. □

Definition 5.1.5. *The equivalence classes in $\mathcal{O}_K$ under $\sim$ are called **ideal classes**. We write C_K to denote the set of ideal classes. The cardinality $h_K = |C_k|$ is the **class number** of K.*

Proposition 5.1.6. *We have $h_K = 1$ if and only if $\mathcal{O}_K$ is a PID.*

Proof. ($\Rightarrow$) Suppose that $h_K = 1$. Then for all proper ideals I in $\mathcal{O}_K$, there exists $\alpha, \beta \in \mathcal{O}_K$ such that

$$I(\alpha) = \mathcal{O}_K(\beta)$$

The right side is (β). As $\beta \in (\beta)$, we have $\beta = i\alpha$ for some $i \in I$. Thus, $\beta/\alpha \in I$. We claim that $(\beta/\alpha) = I$. Clearly, $(\beta/\alpha) \subseteq I$. Given $a \in I$, we have $a\alpha \in I(\alpha) = (\beta)$, so $a\alpha = r\beta$ for some $r \in \mathcal{O}_K$, giving $a = r\beta/\alpha$. Thus $\alpha \in (\beta/\alpha)$ and $I \subseteq (\beta/\alpha)$.

($\Leftarrow$) Suppose that $\mathcal{O}_K$ is a PID. Then for any nonzero $I \subseteq \mathcal{O}_K$, there exists an $\alpha \in \mathcal{O}_K$ such that $I = (\alpha)$. In particular, $I(1) = \mathcal{O}_K(\alpha)$, so $I \sim \mathcal{O}_K$. □

Lemma 5.1.7. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then $I \cap \mathbb{Z} \neq \{0\}$.*

Proof. Choose any nonzero $\alpha \in I$. α is annihalated by some monic polynomial in $\mathbb{Z}[x]$, so write $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$. We can choose one such that $a_0 \neq 0$. In particular, $a_0 = -\alpha(a_1 + \cdots + \alpha^{d-1}) \in I \cap \mathbb{Z}$. □

Lemma 5.1.8. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then $\mathcal{O}_K/I$ is a finite ring.*

Proof. Choose any nonzero $a \in I \cap \mathbb{Z}$. We have $(a) \subseteq I \subseteq \mathcal{O}_K$. The map from $\mathcal{O}_K/(a)$ to $\mathcal{O}_K/I$ that takes $\alpha + (a)$ to $\alpha + I$ is well-defined and onto. Thus it suffices to show that $\mathcal{O}_K/(a)$ is finite.

Let $w = \{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. Then $\mathcal{O}_K/(a)$ is isomorphic as an additive group to $(\mathbb{Z}/a\mathbb{Z})^n$, where $n = [K : \mathbb{Q}]$. In particular, $\#\mathcal{O}_K/(a) = a^n < \infty$. □

Definition 5.1.9. *The norm of I is defined as $N(I) := \#\mathcal{O}_K/I$.*

Proposition 5.1.10. *Let $\sigma : K \to K$ be an automorphism. Then $I = (\alpha_1, \ldots, \alpha_n)$ and $I^\sigma = (\alpha_1^\sigma, \ldots, \alpha_n^\sigma) = (\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ have an induced isomorphism. In particular, they have the same norm.*

Proof. The map is given by $x + I \to \sigma(x) + I^\sigma$. This is surjective as σ is surjective, and injective as every element of I^σ comes from I. □

Proposition 5.1.11. *If $I = (a)$, then $N(I) = |\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)|$.*

Proof. Let $w = \{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. Then αw is a $\mathbb{Z}$ basis for $I = (\alpha)$. By definition,

$$\Delta(\alpha w) = \det(\sigma_i(\alpha w_j)) = \det(\sigma_i(\alpha)\sigma_i(w_j)) = \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right) \Delta(w) = \mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\Delta(w)$$

Now I is an additive subgroup of $\mathcal{O}_K$ with index $N(I)$. Thus if $\alpha w_i = \sum c_{ij} w_j$ with $c_{ij} \in \mathbb{Z}$, then we have $N(I) = |\det(c_{ij})|$ by Theorem 1.0.7.

By Lemma 2.0.5, we have $\Delta(\alpha w) = \det(c_{ij})\Delta(w)$. In particular,

$$N(I) = |\Delta(\alpha w)/\Delta(w)| = |\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)|$$

□

Lemma 5.1.12 (Hurwitz)**.** *Let K be a number field with $[K : \mathbb{Q}] = n$. Then there exists a positive integer M depending only on the choice of integral basis for $\mathcal{O}_K$ such that for any $\gamma \in K$, there exists a $w \in \mathcal{O}_K$ wand $1 \leq t \leq M$, $t \in \mathbb{Z}$ iwth*

$$|\mathrm{Norm}_{K|\mathbb{Q}}(t\gamma - w)| < 1$$

Proof. Let $\{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. For any $\gamma \in K$, write

$$\gamma = \sum_{i=1}^{n} \gamma_i w_i$$

with $\gamma_i \in \mathbb{Q}$. Let $\gamma_i = a_i + b_i$ with $a_i \in \mathbb{Z}$ and $0 \leq b_i < 1$. As quick notation, write $[\gamma] = \sum_{i=1}^{n} a_i w_i$ and $\{\gamma\} = \sum_{i=1}^{n} b_i w_i$. Thus $\gamma = [\gamma] + \{\gamma\}$ and $[\gamma] \in \mathcal{O}_K$ for all $\gamma \in K$.

Let $w_i^{(1)}, \ldots, w_i^{(n)}$ be the $K|\mathbb{Q}$ conjugates of w_i and set

$$C := \prod_{j=1}^{n} \left(\sum_{i=1}^{n} |w_i^{(j)}| \right)$$

Then, if $\gamma = \sum_{i=1}^{n} \gamma_i w_i$ and $\mu := \max_{1 \leq i \leq n} |\gamma_i|$, we have

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\gamma)| = |\prod_{j=1}^{n} \left(\sum_{i=1}^{n} \gamma_i w_i^{(j)} \right)| \leq \prod_{j=1}^{n} \left(\sum_{i=1}^{n} \mu |w_i^{(j)}| \right) = C\mu^n$$

Choose m to be the first integer after $C^{1/n}$ and let $M = m^n$ such that M only depends on the choice of $w_1, \ldots, w_n$.

Define a linear map $\phi : K \to \mathbb{R}^n$ by

$$\phi\left(\sum_{i=1}^{n} \gamma_i w_i \right) = (\gamma_1, \ldots, \gamma_n)$$

By construction, $\phi(\{\gamma\})$ lies in the n-dimensional unit cube, $B := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \leq x_i < 1\}$. Partitioning B into m^n subcubes inside $1/m$ and consider the points $\phi(\{k\gamma\})$ for $0 \leq k \leq m^n$. There are $m^n + 1$ such points inside m^n subcubes, so there is some subcube with two points. Picking these k, say h, l with $h > l$ and taking $t = h - l$, we have $1 \leq t \leq m^n = M$.

By construction $t\gamma = w + \delta$ where $w := [h\gamma] - [l\gamma] \in \mathcal{O}_K$ and $\delta := \{h\gamma\} - \{l\gamma\}$ such that

$$\phi(\delta) \in [-1/m, 1/m]^n$$

By the inequality established previously,

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\delta)| \leq C(1/m)^n < 1$$

as $m > C^{1/n}$. Now, as $\delta = t\gamma - w$, the lemma follows. □

Remark 5.1.13. If $M = 1$ in the above lemma, then we for any $\gamma \in K$, we can find a $w \in \mathcal{O}_K$ with $|\mathrm{Norm}_{K|\mathbb{Q}}(\gamma - w)| < 1$. Then, given any $\alpha, \beta \in \mathcal{O}_K$, let $\gamma = \alpha/\beta$. Thus, we have a $w \in \mathcal{O}_K$ such that

$$|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha/\beta - w)| = |\mathrm{Norm}_{K|\mathbb{Q}}((\alpha - \beta w)/\beta)| < 1$$

In particular, by multiplicativity of the Norm, $|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha - \beta w)| < |\mathrm{Norm}_{K|\mathbb{Q}}(\beta)|$. Thus, we can write $\alpha = \beta w + (\alpha - \beta w)$ such that the remainder has strictly smaller Norm. Thus $\mathcal{O}_K$ is a Euclidian domain (hence a PID, hence class number 1).

Theorem 5.1.14. *The class number $h_K = \#C_k$ is finite*

Proof. Let I be a nonzero ideal of $\mathcal{O}_K$. Choose $0 \neq \beta \in I$ such that $|\mathrm{Norm}(\beta)|$ is minimal, and let M be as in Hurwitz's Lemma. Applying Hurwitz with $\gamma := \alpha/\beta$, there is some t in the range $1 \leq t \leq M$ and $w \in \mathcal{O}_K$ such that $|\mathrm{Norm}(t(\alpha/\beta) - w)| < 1$. By construction, $t\alpha - \beta w \in I$ with $|\mathrm{Norm}(t\alpha - \beta w)| < |\mathrm{Norm}(\beta)|$. This contradicts the minimality of $|\mathrm{Norm}(\beta)|$ unless $t\alpha - w\beta = 0$. In particular, $t\alpha \in (\beta)$. Although t is based on α, as it lies between 1 and M, we know that $M!\alpha \in (\beta)$. As α was arbitrary,

$$(M!)I \subseteq (\beta)$$

Now let $J := \{1/\beta \times M! \times \alpha \mid \alpha \in I\}$. Then J is an ideal in $\mathcal{O}_K$, using the subset equation we established previously. Also, $(\beta)J = (M!)I$, so $I \sim J$. Also by construction, $\mathcal{O}_K \supseteq J \supseteq (M!)$. As we know $\mathcal{O}_K/(M!)$ is finite, there are only finitely many choices of J. Hence I is equivalent to one of finitely many ideals, and in particular there are finitely many equivalence classes. □

5.1.2 Ideal Classes as Groups

Lemma 5.1.15. *If $I, J \subseteq \mathcal{O}_K$ are ideals with I nonzero with $JI = I$ then $J = \mathcal{O}_K$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$ basis for I. As $I = JI$, we can find $b_{ij} \in J$ such that $\alpha_i = \sum_{j=1}^n b_{ij}\alpha_j$. Hence $\det(b_{ij} - \delta_{ij}) = 0$, and expanding this determinant, every term lies in J apart from the prodct of 1's in the identity. Thus, $1 \in J$, giving $J = (1) = \mathcal{O}_K$. □

Lemma 5.1.16. *If I is a nonzero ideal of $\mathcal{O}_K$ and $w \in K$ with $wI \subseteq I$, then $w \in \mathcal{O}_K$.*

Proof. Take $M = I$ with Lemma 4.0.4. □

Lemma 5.1.17. *If I, J are nonzero ideals in $\mathcal{O}_K$ and $w \in \mathcal{O}_K$ is such that $(w)I = JI$, then $(w) = J$.*

Proof. Choose any $\beta \in J$. Then we have $(w)I \supseteq (\beta)I$, such that $\{\beta/w\}I \subseteq I$. By Lemma 5.1.16, $\beta/w \in \mathcal{O}_K$, thus $\beta \in (w)$. As β was arbitrary, we see that $J \subseteq (w)$.

Thus $w^{-1}J$ is an ideal in $\mathcal{O}_K$. From assumption, we have $I = (w^{-1}J)I$, so by Lemma 5.1.15, $w^{-1}J = \mathcal{O}_K$, giving $J = (w)$. □

6 Notes

In Lemma 2.0.5, we note the transpose is due to the fact that we order elements in the det on elements to be placed by row, whereas the change of basis works column-wise.

characteristic 0, separable -> min poly irreducible has no repeated roots -> has degree many embeddings

The $\mathbb{Z}$ basis for $\mathcal{O}_K$ generates K as a $\mathbb{Q}$ basis, as for any algebraic α, there is some $n\alpha \in \mathcal{O}_K$.

Ideals inside Ok are generated by n elements as they are submodules of Z^n

If $\mathcal{O}_K$ has integral basis $w_1, \dots, w_n$, then we can view

$$\mathcal{O}_K \simeq \bigoplus_{i=1}^{n} \mathbb{Z} w_i$$

as an isomorphism of abelian groups. Also, $n := [K : \mathbb{Q}]$. Given any principal ideal (a) in $\mathcal{O}_K$, we have

$$(a) = a\mathcal{O}_K \simeq \bigoplus_{i=1}^{n} a\mathbb{Z} w_i$$

because $aw_1, \dots, aw_n$ is an integral basis for (a). In particular,

$$O_K/(a) \simeq \bigoplus_{i=1}^{n} \mathbb{Z} w_i / \bigoplus_{i=1}^{n} a\mathbb{Z} w_i = \bigoplus_{i=1}^{n} (\mathbb{Z}/a\mathbb{Z}) w_i \simeq (\mathbb{Z}/a\mathbb{Z})^n$$