

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	Basic Definitions	5
4.2	Cyclotomic Fields	9
4.3	Class Number	9
4.4	Unique Factorisation	12
4.5	Computation of the Class Group	17
4.6	Fermat's Theorems	23
5	Notes	25
5.1	Fermat's Last Equation for the Cubic	26

1 Introduction

- adding ideals, coprime (sums to entire ring)

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 $\lambda g, \lambda^{-1}h \in \mathbb{Z}[t]$.
- 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)

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

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 $\{x_1, \dots, x_n\}$. Suppose (a_{ij}) is a square matrix with integer entries. Let

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

Then the elements $\{y_1, \dots, y_n\}$ 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 $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_n\}$ 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 $\sigma_i : K \rightarrow \mathbb{C}$ be the n embeddings. We call $\sigma_i(\alpha)$ the **K -conjugates** of α .

We define the **trace** to be $\text{Tr}_{K|\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$ and the **norm** $\text{Norm}_{K|\mathbb{Q}}(\alpha) = N_{K|\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$. 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 β_1, \dots, β_n are the n roots of m_β in \mathbb{C} , then one can choose embeddings $\sigma_i : \beta \rightarrow \beta_i$.
- $\text{Norm}_{K|\mathbb{Q}}(\gamma\delta) = \text{Norm}_{K|\mathbb{Q}}(\gamma)\text{Norm}_{K|\mathbb{Q}}(\delta)$
- $\text{Norm}_{K|\mathbb{Q}}(\gamma) = 0$ if and only if $\gamma = 0$.
- $\text{Norm}_{K|\mathbb{Q}}(q) = q^n$ for $q \in \mathbb{Q}$.
- If $K = \mathbb{Q}(\alpha)$ and $m_\alpha(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0$, then we have $\text{Norm}_{K|\mathbb{Q}}(\alpha) = (-1)^n c_0$ and $\text{Norm}_{K|\mathbb{Q}}(\alpha) = -c_{n-1}$. 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. \square

Definition 2.0.3. Let $w = \{w_1, \dots, w_n\}$ 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. $\Delta(w)^2 = \det(\text{Tr}_{K|\mathbb{Q}}(w_i w_j))$ and consequently $\Delta(w)^2 \in \mathbb{Q}$.

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

$$\begin{aligned} \Delta(w)^2 &= \det(A)^2 = \det(A^T A) = \det\left(\sum_k \sigma_k(w_i) \sigma_k(w_j)\right) \\ &= \det\left(\sum_k \sigma_k(w_i w_j)\right) = \det(\text{Tr}_{K|\mathbb{Q}}(w_i w_j)) \end{aligned}$$

\square

Lemma 2.0.5. If $v = \{v_1, \dots, v_n\}$ is a basis for $K|\mathbb{Q}$ and $w = \{w_1, \dots, w_n\} \subseteq K$ 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. \square

Lemma 2.0.6. If $K = \mathbb{Q}(\alpha)$ and $v = \{1, \alpha, \dots, \alpha^{n-1}\}$, 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 $\alpha_1, \dots, \alpha_n$. 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. $\Delta(w_1, \dots, w_n) \neq 0$ if and only if w_1, \dots, w_n is a basis for $K|\mathbb{Q}$.

Proof. Suppose $K = \mathbb{Q}(\alpha)$ and let $v = \{1, \alpha, \dots, \alpha^{n-1}\}$. 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 $\beta_1, \dots, \beta_n \in R$ such that

1. $\alpha = \beta_1 \cdots \beta_n$
2. If $\alpha = \gamma_1 \cdots \gamma_m$ 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 irreducibility shows they are associates. We can inductively show factorisation is unique. □

4 Ring of Integers

4.1 Basic Definitions

Definition 4.1.1. 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 4.1.2. 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 4.1.3 (\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 $\text{Tr}_{K|\mathbb{Q}}(\alpha) = 2a$ and $\text{Norm}_{K|\mathbb{Q}}(\alpha) = a^2 - db^2$. 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 $A^2 \equiv dB^2 \pmod{4}$.

Now a case split,

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

Thus, we have

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

Lemma 4.1.4. $\alpha \in K$ 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 $M = \langle 1, \alpha, \dots, \alpha^{d-1} \rangle$, 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, \dots, 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 $\alpha \in \mathcal{O}_K$. \square

Theorem 4.1.5. *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 4.1.4, 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 4.1.4 that $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. \square

Remark 4.1.6. 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 4.1.7. *If $\alpha \in \mathcal{O}_K$, then $\text{Tr}_{K|\mathbb{Q}}(\alpha), \text{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. Let $\alpha \in \mathcal{O}_K$. Then all the $K|\mathbb{Q}$ conjugates $\alpha_1, \dots, \alpha_n$ belong to the splitting field of the minimal polynomial, \mathcal{O}_L . Now, $\text{Tr}_{K|\mathbb{Q}}(\alpha) \in \mathcal{O}_L$ and $\text{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathcal{O}_L$ by Theorem 4.1.5. Now the trace and norm are both in \mathbb{Q} , and $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$. \square

Definition 4.1.8. $\alpha \in \mathcal{O}_K$ is a **unit** if $\alpha^{-1} \in \mathcal{O}_K$.

Lemma 4.1.9. *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 $\text{Norm}_{K|\mathbb{Q}}(\alpha) = \pm 1$
2. If α and β are associates in \mathcal{O}_K , then $\text{Norm}_{K|\mathbb{Q}}(\alpha) = \pm \text{Norm}_{K|\mathbb{Q}}(\beta)$
3. If $\text{Norm}_{K|\mathbb{Q}}(\alpha)$ 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,

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

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

Conversely, if $\text{Norm}_{K|\mathbb{Q}}(\alpha) = \pm 1$, let $\alpha_1, \dots, \alpha_n$ be the $K|\mathbb{Q}$ conjugates with $\alpha = \alpha_1$. Then, $\alpha_1 \dots \alpha_n = \pm 1$, such that $\alpha(\alpha_2 \dots \alpha_n) = \pm 1$. Hence, $\alpha^{-1} = \pm(\alpha_2 \dots \alpha_n)$, which is in \mathcal{O}_L (the splitting field of the minimal polynomial) by Theorem 4.1.5. 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

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

by (i)

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

Remark 4.1.10. 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 4.1.9 (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 4.1.11. $w_1, \dots, w_n \in \mathcal{O}_K$ 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, \dots, w_n is a \mathbb{Z} -basis for \mathcal{O}_K . We sometimes call this set the integral basis for K .

Example 4.1.12. 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

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

Remark 4.1.13. Let $v = \{v_1, \dots, v_n\}$ and $w = \{w_1, \dots, w_n\}$ be any two \mathbb{Q} -bases of K . Define $M = \langle v_1, \dots, v_n \rangle_{\mathbb{Z}}$ and $N = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$ be the \mathbb{Z} -submodules of K . Suppose that $v, w \subseteq \mathcal{O}_K$. Then $\Delta(v)^2$ and $\Delta(w)^2$ both lie in \mathbb{Z} , as $\Delta(v)^2 = \det(\text{Tr}_{K|\mathbb{Q}}(v_i v_j))$.

Suppose now that $N \subseteq M$. Then we can find $c_{ij} \in \mathbb{Z}$ such that $w_i = \sum_{j=1}^n c_{ij} v_j$. Define $C = (c_{ij})$.

By Theorem 1.0.7, we have

$$|\det(C)| = [M : N] = \#M/N =: m$$

as additive groups. By Lemma 2.0.5, we have

$$\Delta(w)^2 = (\det(C))^2 \Delta(v)^2 = m^2 \Delta(v)^2$$

If $M = N$, then by Lemma 1.0.6, C is unimodular, thus $\Delta(w)^2 = \Delta(v)^2$.

Definition 4.1.14. Let M be any subset of \mathcal{O}_K which has a \mathbb{Z} -basis. Define $\Delta(M)^2 := \Delta(w)^2$ for any \mathbb{Z} -basis w of M .

From the previous remark, if $N \subseteq M$, then $\Delta(N)^2 = m^2 \Delta(M)^2$, so we have that $\Delta(M)^2 | \Delta(N)^2$.

Theorem 4.1.15 (Integral Basis Theorem). *The ring \mathcal{O}_K has an integral basis.*

Proof. Let $v = \{v_1, \dots, v_n\}$ be any \mathbb{Q} -basis for K . Multiplying v_i by a sufficiently large number, we can suppose $v \subseteq \mathcal{O}_K$.

Let $M = \langle v_1, \dots, v_n \rangle_{\mathbb{Z}}$. Then $\Delta(M)^2 \neq 0$ and in \mathbb{Z} as $\{v_1, \dots, v_n\}$ are \mathbb{Q} -linearly independent. Choose the basis v such that $|\Delta(M)^2|$ is minimal.

We claim that $M = \mathcal{O}_K$, and hence that $\{v_1, \dots, v_n\}$ is an integral basis. Suppose for a contradiction there is some $\alpha \in \mathcal{O}_K$ such that $\alpha \notin M$. Then $\alpha = \sum_{j=1}^n c_j v_j$ with $c_j \in \mathbb{Q}$. Then for any j and $m \in \mathbb{Z}$, $\alpha + m v_j \in \mathcal{O}_K$, but $\alpha + m v_j \notin M$. By adding suitable \mathbb{Z} -multiples of v_j to α , we may assume $|c_j| \leq 1/2$. Since $\alpha \notin M$, there exists j such that $c_j \neq 0$. Choose such j .

Let w be a new \mathbb{Q} -basis obtained from v by replacing v_j by α . We have $w \subseteq \mathcal{O}_K$. The change of basis matrix

$$C = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots \\ c_1 & \cdots & c_j & \cdots & c_n \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

has determinant c_j . Thus

$$|\Delta(w)^2| = c_j^2 |\Delta(v)^2| < |\Delta(v)^2|$$

contradicting the minimality of $|\Delta(v)^2|$. Hence, such an α does not exist, giving $M = \mathcal{O}_K$. \square

Proposition 4.1.16. *Let $w = \{w_1, \dots, w_n\}$ be any \mathbb{Q} -basis for K such that $w \subseteq \mathcal{O}_K$. Let $M = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$ and let $M \neq \mathcal{O}_K$. Then there exists a prime p such that $p^2 \mid \det(M)^2$ and $c_1, \dots, c_n \in \mathbb{Z}$ not all divisible by p such that*

$$\frac{1}{p}(c_1 w_1 + \cdots + c_n w_n) \in \mathcal{O}_K$$

Proof. Let $m = [\mathcal{O}_K : M] > 1$ such that $|\Delta(M)^2| = m^2 |\Delta(\mathcal{O}_K)^2|$. Since $m > 1$, there is a prime p dividing m , such that $p^2 \mid \Delta(M)^2$. As $m = \#\mathcal{O}_K/M$, by Cauchy's Theorem on finite groups, \mathcal{O}_K/M has an element of order p . Let $\alpha + M$ be such element. Then $\alpha = \sum d_j w_j$ with $d_j \in \mathbb{Q}$. By construction, $p\alpha \in M$ so that $pd_j \in \mathbb{Z}$. Thus, we can take $\alpha = 1/p \sum_j (pd_j) w_j \in \mathcal{O}_K$. \square

Remark 4.1.17. The above shows a general method to find the integral basis for \mathcal{O}_K , where $[K : \mathbb{Q}] = n$.

- Let $w = \{w_1, \dots, w_n\}$ be any \mathbb{Q} -basis for K such that $w \subseteq \mathcal{O}_K$. Calculate $\Delta(w)^2$. Taking $M = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$, we know $M \subseteq \mathcal{O}_K$.
- If $[\mathcal{O}_K : M] = m$, then we know $|\Delta(M)^2| = m^2 |\Delta(\mathcal{O}_K)^2|$. If $\Delta(M)^2$ is squarefree, then $m = 1$, giving $\mathcal{O}_K = M$. Else, we can find a prime p such that $p^2 \mid \Delta(M)^2$ and $c_i \in \mathbb{Z}$ not all divisible by p such that $1/p \sum c_i w_i \in \mathcal{O}_K$.
- Thus if $\Delta(M)^2$ is not squarefree, then for each prime p such that $p^2 \mid \Delta(M)^2$, take $\alpha \in \mathcal{O}_K$ of the form $1/p \sum c_i w_i$ where p does not divide all c_j and $c_j \in \mathbb{Z}$. Suppose p does not divide c_j for $j = k$. Multiplying through by $r \in \mathbb{Z}$ such that $rc_k \equiv 1 \pmod{p}$, we may without loss of generality suppose that $c_k \equiv 1 \pmod{p}$. Subtracting integer multiples of w_i , we may further suppose that $0 \leq c_i < p$ for all i , giving $c_k = 1$. Replacing w_k with the new α , we get another basis, spanning a \mathbb{Z} -module M' . The change of basis matrix has determinant $c_k/p = 1/p$, and in particular $\Delta(M')^2 = \frac{1}{p^2} \Delta(M)^2$.
- Repeating the process with M' instead of M , if no such α exists (this requires finite checking as we only need to look for $0 \leq c_i < p$), then p cannot divide m . Eventually we reach a basis where none of the available primes divide m such that $m = 1$, giving the integral basis.

Example 4.1.18. Let $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Start with \mathbb{Q} -basis $\{1, \sqrt{d}\}$. Then we clearly have $\{1, \sqrt{d}\} \subseteq \mathcal{O}_K$ and

$$\Delta(\{1, \sqrt{d}\})^2 = \begin{vmatrix} 1 & -\sqrt{d} \\ 1 & +\sqrt{d} \end{vmatrix}^2 = 4d$$

As d is squarefree the only prime p such that $p^2 | \Delta(\{1, \sqrt{d}\})^2$ is $p = 2$.

We have two cases,

- $d \equiv 1 \pmod{4}$. We find $\frac{1}{2}(1 + \sqrt{d}) \in \mathcal{O}_K$. In this case we find

$$\Delta(\{1, \frac{1}{2}(1 + \sqrt{d})\})^2 = \frac{1}{2^2}4d = d$$

and so we are done.

- $d \not\equiv 1 \pmod{4}$. Then we see that $\frac{1}{2}(1 + \sqrt{d}) \notin \mathcal{O}_K$ as the minimal polynomial is not in $\mathbb{Z}[x]$. The other cases to check are $\frac{1}{2}$, $\frac{1}{2}\sqrt{d}$, neither are in \mathcal{O}_K . No such α was found, so 2 does not divide the index $m = [\mathcal{O}_K : \langle 1, \sqrt{d} \rangle_{\mathbb{Z}}]$. This shows $\{1, \sqrt{d}\}$ is an integral basis.

Definition 4.1.19. 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 4.1.20. 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. \square

4.2 Cyclotomic Fields

Take the cyclotomic extension $\mathbb{Q}(\mu_p)$ for a prime p . Let ζ be a primitive p -th root. Let f be the minimal polynomial of ζ .

4.3 Class Number

Definition 4.3.1. 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 4.3.2. 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, $I \sim K$. \square

Definition 4.3.3. 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 4.3.4. 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 $I \sim \mathcal{O}_K$. \square

Lemma 4.3.5. *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 annihilated by some monic polynomial in $\mathbb{Z}[x]$, so write $\alpha^d + a_{d-1}\alpha^{d-1} + \dots + a_0 = 0$. We can choose one such that $a_0 \neq 0$. In particular, $a_0 = -\alpha(a_1 + \dots + \alpha^{d-1}) \in I \cap \mathbb{Z}$. \square

Lemma 4.3.6. *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 $w = \{w_1, \dots, w_n\}$ 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, $\#\mathcal{O}_K/(a) = a^n < \infty$. \square

Definition 4.3.7. *The norm of I is defined as $N(I) := \#\mathcal{O}_K/I$.*

Proposition 4.3.8. *Let $\sigma : K \rightarrow K$ be an automorphism. Then $I = (\alpha_1, \dots, \alpha_n)$ and $I^\sigma = (\alpha_1^\sigma, \dots, \alpha_n^\sigma) = (\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ have an induced isomorphism. In particular, they have the same norm.*

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

Proposition 4.3.9. *If $I = (a)$, then $N(I) = |\text{Norm}_{K|\mathbb{Q}}(\alpha)|$.*

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

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

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,

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

\square

Lemma 4.3.10 (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 $w \in \mathcal{O}_K$ and $1 \leq t \leq M$, $t \in \mathbb{Z}$ with*

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

Proof. Let $\{w_1, \dots, w_n\}$ 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 $w_i^{(1)}, \dots, w_i^{(n)}$ 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

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

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, \dots, w_n .

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

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

By construction, $\phi(\{\gamma\})$ lies in the n -dimensional unit cube, $B := \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid 0 \leq x_i < 1\}$. 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,

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

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

Remark 4.3.11. If $M = 1$ in the above lemma, then we for any $\gamma \in K$, we can find a $w \in \mathcal{O}_K$ with $|\text{Norm}_{K|\mathbb{Q}}(\gamma - w)| < 1$. Then, given any $\alpha, \beta \in \mathcal{O}_K$, let $\gamma = \alpha/\beta$. Thus, we have a $w \in \mathcal{O}_K$ such that

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

In particular, by multiplicativity of the Norm, $|\text{Norm}_{K|\mathbb{Q}}(\alpha - \beta w)| < |\text{Norm}_{K|\mathbb{Q}}(\beta)|$. 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 4.3.12. *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 $|\text{Norm}(\beta)|$ 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 $|\text{Norm}(t(\alpha/\beta) - w)| < 1$. By construction, $t\alpha - \beta w \in I$ with $|\text{Norm}(t\alpha - \beta w)| < |\text{Norm}(\beta)|$. This contradicts the minimality of $|\text{Norm}(\beta)|$ unless $t\alpha - \beta w = 0$. 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. \square

4.4 Unique Factorisation

Lemma 4.4.1. *If $I, J \subseteq \mathcal{O}_K$ are ideals with I nonzero with $JI = I$ then $J = \mathcal{O}_K$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ 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 product of 1's in the identity. Thus, $1 \in J$, giving $J = (1) = \mathcal{O}_K$. \square

Lemma 4.4.2. *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 4.1.4. \square

Lemma 4.4.3. *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 4.4.2, $\beta/w \in \mathcal{O}_K$, 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 4.4.1, $w^{-1}J = \mathcal{O}_K$, giving $J = (w)$. \square

Proposition 4.4.4. *For any nonzero ideal $I \subseteq \mathcal{O}_K$, there exists a k such that $1 \leq k \leq h_K$ and I^k is principal.*

Proof. Among the $h_K + 1$ ideals $\{I^i \mid 1 \leq i \leq h_K + 1\}$, some two must be equivalent. Suppose $I^i \sim I^j$ with $j > i$. Thus $(\alpha)I^i = (\beta)I^j$ for some $\alpha, \beta \in \mathcal{O}_K$. Let $k = j - i$ and $J = I^k$. Then, $(\alpha)I^i = (\beta)I^i J \subseteq (\beta)I^i$ such that $\{\alpha/\beta\}I^i \subseteq I^i$. By Lemma 4.4.2, we have $\alpha/\beta \in \mathcal{O}_K$. Also, $(\alpha/\beta)I^i = JI^i$, so by Lemma 4.4.3, $(\alpha/\beta) = J$. Thus $J = I^k$ is principal. \square

Proposition 4.4.5. *The ideal classes form a group C_K . It is called the class group of K and its order is the class number h_K .*

Proof. Given two ideal classes $[I], [J]$, define the product by $[I] \cdot [J] := [IJ]$. This is clearly well-defined. The element $[O_K]$ acts as an identity, and associativity is derived from the ring structure of \mathcal{O}_K . Given $[I] \in C_K$, as I^k is principal for some I , $[I^{k-1}]$ clearly gives an inverse. \square

Lemma 4.4.6 (Cancellation Lemma). *Let $A, B, C \subseteq \mathcal{O}_K$ be nonzero ideals with $AB = AC$. Then $B = C$.*

Proof. Let k be such that $A^k = (\alpha)$ is principal. Multiplying by A^{k-1} , we get $(\alpha)B = (\alpha)C$, so $B = C$. \square

Definition 4.4.7. Let $A, B \subseteq \mathcal{O}_K$ be nonzero ideals. Write $B|A$ if there exists an ideal $C \subseteq \mathcal{O}_K$ such that $A = BC$.

Proposition 4.4.8. Let A, B be nonzero ideals in \mathcal{O}_K . Then $B \supseteq A$ if and only if there exists an ideal C such that $A = BC$ (equivalently, $B|A$).

Proof. Let $k \geq 1$ be such that $B^k = (\beta)$ is principal. If $B \supseteq A$, then we have $B^{k-1}A \subseteq B^k = (\beta)$. Let $C := \{1/\beta\}B^{k-1}A$ such that $C \subseteq \mathcal{O}_K$ is an ideal. Then, $BC = B\{1/\beta\}B^{k-1}A = A$.

Conversely, if $B|A$ then $A = BC'$ for some C' . Immediately, $BC' \subseteq B$ as B is an ideal. Thus $A \subseteq B$. \square

Lemma 4.4.9. Let A, B be nonzero ideals and P be a prime ideal of \mathcal{O}_K such that $P|AB$. Then either $P|A$ or $P|B$.

Proof. Suppose that $P|AB$ and that P does not divide A . We have $P \supseteq AB$ but $P \not\supseteq A$, so we can find a $\alpha \in A$ with $\alpha \notin P$. On the other hand, for any $\beta \in B$, we have $\alpha\beta \in P$. As P is a prime ideal, given $\alpha\beta \in P$, one of α or β belongs to P . Thus $\beta \in P$. This gives $P \supseteq B$, thus $P|B$. \square

Remark 4.4.10. Nonzero prime ideals in \mathcal{O}_K are maximal. This follows from the fact that if P is a nonzero prime ideal of \mathcal{O}_K , then \mathcal{O}_K/P is a finite integral domain, thus a field.

Theorem 4.4.11 (Unique Factorisation Theorem for ideals of \mathcal{O}_K). Let A be any nonzero proper ideal of \mathcal{O}_K . Then there exist prime ideals P_1, \dots, P_r such that $A = P_1 \cdots P_r$. The factorisation is unique up to the order of factors.

Proof. Suppose that there is some nonzero proper ideal A that has no prime factorisation. Let A be such an ideal with $N(A)$ minimal. There exists a maximal (thus prime) ideal P_1 containing A . In particular, we can find an ideal C with $A = P_1C$.

If $A = C$, then $P_1C = C$, which gives $P_1 = \mathcal{O}_K$, a contradiction. Thus $A \subsetneq C$. By the definition of Norm, we have $N(A) = N(C)[C : A] > N(C)$. By the minimality assumption, we can factor C into prime ideals $C = P_2 \cdots P_r$ (or trivially if $C = \mathcal{O}_K$). Then, $A = P_1 \cdots P_r$, a contradiction. Hence every nonzero proper ideal has a prime factorisation.

Suppose now that $A = P_1 \cdots P_r = Q_1 \cdots Q_s$. We know that $P_1|Q_1 \cdots Q_s$. Take k minimal such that $P_1|Q_1 \cdots Q_k$. If $k = 1$, $P_1|Q_1$, and if $k > 1$, $P_1|(Q_1 \cdots Q_{k-1})Q_k$, but P_1 does not divide $(Q_1 \cdots Q_{k-1})$, thus $P_1|Q_k$. We therefore have $P_1|Q_k$. As Q_k is maximal, $P_1 = Q_k$. Without loss of generality, take $k = 1$, and inductively repeat by applying the Cancellation Lemma.

In the end we get $\mathcal{O}_K = Q'_1 \cdots Q'_t$ unless $r = s$, but only one side clearly contains the identity. \square

Remark 4.4.12. Prime ideals that appear in A are those which contain A . We don't have to worry about associates as for any unit u , $(u)I = I$. If \mathcal{O}_K is a PID, this is a direct proof that it is a UFD.

Remark 4.4.13. Note that ideals A, B in \mathcal{O}_K are coprime if and only if there is no shared maximal ideal P . In other words, they have no prime factor in common.

By observing the factorisation and applying the cancellation lemma, if A, B are coprime, we have

- $A|BC$, then $A|C$
- $A|I$ and $B|I$ implies $AB|I$

Lemma 4.4.14. If A and B are coprime, then $AB = A \cap B$.

Proof. Clearly, $AB \subseteq A \cap B$, thus $A \cap B | AB$. On the other hand, $A | A \cap B$ and $B | A \cap B$, by coprimality and unique factorisation, we have $AB | A \cap B$. \square

Lemma 4.4.15. *If A, B are nonzero coprime ideals, then $N(AB) = N(A)N(B)$.*

Proof. By the Chinese Remainder Theorem, we have

$$\mathcal{O}_K/(A \cap B) \simeq \mathcal{O}_K/A \oplus \mathcal{O}_K/B$$

when A, B are coprime. By the previous lemma, we have $A \cap B = AB$. By considering the cardinality on both sides, the proof follows. \square

Lemma 4.4.16. *If P is a nonzero prime ideal of \mathcal{O}_K and $i \geq 0$, $\#P^i/P^{i+1} = \#\mathcal{O}_K/P$.*

Proof. We have $P^{i+1} \subseteq P^i$, but by the Cancellation Lemma, cannot have equality. Thus we can choose a $\pi \in P^i$ such that $\pi \notin P^{i+1}$. Then, $P^i \supseteq (\pi)$. Let $(\pi) = P^i B$, then we have that P does not divide B .

Define a homomorphism on additive groups by

$$\begin{aligned} \theta : \mathcal{O}_K &\rightarrow P^i/P^{i+1} \\ \alpha &\mapsto \alpha\bar{\pi} \end{aligned}$$

by the map which multiplies α by π then reduces modulo P^{i+1} . Now we also have

$$\begin{aligned} \theta(\alpha) = 0 &\iff \alpha\pi \in P^{i+1} \iff (\alpha\pi) \subseteq P^{i+1} \iff (\alpha)P^i B \subseteq P^{i+1} \\ &\iff P^{i+1} | (\alpha)P^i B \iff P | B(\alpha) \iff P | (\alpha) \end{aligned}$$

Thus, $\ker(\theta) = P$.

Thus by the first isomorphism theorem, it suffices to show that θ is surjective. Now

$$(\pi) + P^{i+1} = P^i B + P^{i+1} = P^i$$

as $B + P = \mathcal{O}_K$. Thus, given any $\beta + P^{i+1} \in P^i/P^{i+1}$, there exists $\alpha \in \mathcal{O}_K$ and $\gamma \in P^{i+1}$ such that $\alpha\pi + \gamma = \beta$. Then $\theta(\alpha) = \beta + P^{i+1}$. \square

Corollary 4.4.17. *If P is a nonzero prime ideal and $e \geq 1$, then $N(P^e) = N(P)^e$.*

Proof. Taking \mathcal{O}_K and P^i as additive groups, we have

$$N(P^e) = \#\mathcal{O}_K/P^e = \#\mathcal{O}_K/P \cdot \#P/P^2 \cdots \#P^{e-1}/P^e = (\#\mathcal{O}_K/P)^e = N(P)^e$$

where the second equality comes from the third isomorphism theorem used telecopically (or noting that $0 \rightarrow P^{i-1}/P^i \rightarrow \mathcal{O}_K/P^i \rightarrow \mathcal{O}_K/P^{i-1} \rightarrow 0$ is a short exact sequence). \square

Corollary 4.4.18. *If $A = \prod_i P_i^{e_i}$, then $N(A) = \prod N(P_i)^{e_i}$, where P_i are distinct nonzero prime ideals*

Proof. Using the proof above and Lemma 4.4.15. \square

Corollary 4.4.19. *If A, B are nonzero ideals, then $N(AB) = N(A)N(B)$*

Proof. A consequence of Unique Factorisation and the previous corollary. \square

Remark 4.4.20. If $N(I) = p$ for a rational prime, then I is automatically prime as \mathcal{O}_K/I is a finite ring with p elements. Alternatively, consider the factorisation of I and note that any nontrivial prime ideal has norm at least 2.

On the other hand, if P is prime, it is maximal, thus \mathcal{O}_K/P is a finite field with p^k elements for some prime p and integer k .

Alternatively, let K be a number field of degree $[K : \mathbb{Q}] = n$. Let P be a nonzero prime ideal of \mathcal{O}_K . Then $P \cap \mathbb{Z}$ is a prime ideal of \mathbb{Z} , so it is of the form $p\mathbb{Z}$ for some rational p . Thus $P \supseteq p\mathcal{O}_K = (p)$. We say that P **lies above** p . Suppose that

$$(p) = P_1^{e_1} \cdots P_r^{e_r}$$

where P_i are distinct prime ideals in \mathcal{O}_K . Then they are all prime ideals lying above the rational prime p . Taking norms,

$$p^n = N(P_1)^{e_1} \cdots N(P_r)^{e_r}$$

such that $N(P_i) = p^{f_i}$ with $\sum_{i=1}^r e_i f_i = n$. As P must be one of the P_i , we see that $N(P)$ is a power of p .

Definition 4.4.21. The integer e_i is called the **ramification index** of P_i . If $e_i > 1$, we say that P_i is **ramified**. If some $e_i > 1$, we say that p **ramifies** in K . The integer f_i is called the **degree** of P_i .

Note here that $p^{f_i} = \#\mathcal{O}_K/P_i$ and that \mathcal{O}_K/P_i is isomorphic to the finite field with p^{f_i} elements.

Example 4.4.22. Considering $\mathbb{Z}[\sqrt{-5}]$, we have

$$(6) = (2)(3) = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

Let $P_1 = (2, 1 + \sqrt{-5})$, $P_2 = (2, 1 - \sqrt{-5})$, $Q_1 = (3, 1 + \sqrt{-5})$, $Q_2 = (3, 1 - \sqrt{-5})$. Now,

$$(2) = (4, 6) \subseteq P_1 P_2 \subseteq (2, 6) = (2)$$

Thus $P_1 P_2 = (2)$. We have $N((2)) = \text{Norm}(2) = 4$, thus $N(P_1)N(P_2) = 4$. Also, $a \equiv b \pmod{2}$ when $a + b\sqrt{-5} \in P_i$, giving $P_i \neq \mathcal{O}_K$. Thus $N(P_1) = N(P_2) = 2$.

By similar calculation, we have $(3) = (9, 6) \subseteq Q_1 Q_2 \subseteq (3, 6) = (3)$, such that $Q_1 Q_2 = (3)$, with $N(Q_1) = N(Q_2) = 3$. As these are prime, we see that P_1, P_2, Q_1, Q_2 are prime ideals.

Now, $P_1, Q_1 \supseteq (1 + \sqrt{-5})$ and $P_2, Q_2 \supseteq (1 - \sqrt{-5})$, so contains once of each, comparing norms gives $P_1 Q_1 = (1 + \sqrt{-5})$ and $P_2 Q_2 = (1 - \sqrt{-5})$.

Thus,

$$(2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = P_1 P_2 Q_1 Q_2 = P_1 Q_1 P_2 Q_2$$

giving unique factorisation, although the factorisation into irreducibles are different.

Theorem 4.4.23 (Dedekind). Suppose that $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$ with a minimal polynomial $m(x) \in \mathbb{Z}[x]$ with degree n . If p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and $\bar{m}(x) := m(x) \pmod{p} \in \mathbb{F}_p[x]$ factorises as

$$\bar{m}(x) = \prod_{i=1}^r \bar{g}_i(x)^{e_i}$$

with \bar{g}_i distinct and irreducible, then

- $P_i = (p, g_i(\alpha))$ is a prime ideal of \mathcal{O}_K (where $g_i(x)$ is any polynomial such that $g_i(x) \equiv \bar{g}_i(x) \pmod{p}$)

- P_i are distinct
- The degree of P_i is the degree of \bar{g}_i
- $(p) = \prod_{i=1}^r P_i^{e_i}$

Proof. Suppose that p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Consider the natural map $\mathbb{Z}[\alpha] \rightarrow \mathcal{O}_K/p\mathcal{O}_K$. An element γ of the kernel must have the form $p\beta$ for $\beta \in \mathcal{O}_K$. As p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, we must have $\beta \in \mathbb{Z}[\alpha]$. Thus the kernel is precisely $p\mathbb{Z}[\alpha]$, which induces an injection $\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$. This must be an isomorphism of rings as both sides have order p^n .

Now consider the ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ taking $g(x)$ to $g(\alpha) + p\mathbb{Z}[\alpha]$. This has kernel

$$\{g(x) \mid g(x) = m(x)h(x) + pj(x)\} = (p, m(x))$$

giving

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, m(x))$$

Finally, consider the homomorphism from $\mathbb{Z}[x]$ to $\mathbb{F}_p[x]/(\bar{m}(x))$ sending $g(x)$ to $\bar{g}(x) + (\bar{m}(x))$. The kernel of this map is

$$\{g(x) \mid \bar{m}(x) \mid \bar{g}(x)\} = \{g(x) = m(x)h(x) + pj(x)\} = (p, m(x))$$

Thus $\mathbb{Z}[x]/(p, m(x)) \simeq \mathbb{F}_p[x]/(\bar{m}(x))$, and composing maps, we get

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, m(x)) \simeq \mathbb{F}_p[x]/(\bar{m}(x))$$

There is a bijective correspondence between prime ideals of \mathcal{O}_K containing (p) and the prime ideals of $\mathcal{O}_K/p\mathcal{O}_K$, and these have a correspondence to prime ideals of $\mathbb{F}_p[x]/(\bar{m}(x))$. However, these prime ideals are generated by irreducible factors $\bar{g}_i(x)$ of $\bar{m}(x)$. Tracing back with correspondence, these correspond to $P_i = (p, g_i(\alpha))$ in \mathcal{O}_K . This shows (i) and (ii). Also, the isomorphism shows $N(P_i) = \#\mathbb{F}_p[x]/(\bar{g}_i(x))$, which shows (iii).

Finally, we have

$$\prod_{i=1}^r P_i^{e_i} = \prod_{i=1}^r (p, g_i(\alpha))^{e_i} \subseteq \prod_{i=1}^r (p, g_i(\alpha)^{e_i}) \subseteq (p, \prod_{i=1}^r g_i(\alpha)^{e_i}) = (p)$$

On the other hand, $p^{f_i} = N(P_i) = p^{\deg(g_i)}$, such that

$$N\left(\prod_{i=1}^r P_i^{e_i}\right) = p^{\sum_{i=1}^r e_i f_i} = p^{\sum_{i=1}^r e_i \deg(g_i)} = p^n$$

On the other hand, $N((p)) = p^n$, so $(p) = \prod_{i=1}^r P_i^{e_i}$. □

Corollary 4.4.24. *If p ramifies, then $p \mid \Delta(\mathbb{Z}[\alpha])^2$.*

Proof. Note that if $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then $p \mid \Delta(\mathbb{Z}[\alpha])^2$, so we may suppose that p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then by Dedekind, if p ramifies with a factor P^2 , then $\bar{m}(x)$ has a multiple irreducible factor $\bar{g}(x)$ over \mathbb{F}_p , for which $g(\alpha) \in (p, g(\alpha)) = P$. We then have that $m(x) = g(x)^2 h(x) + pk(x)$ such that

$$m'(x) = g(x)(2g'(x)h(x) + g(x)h'(x)) + pk'(x) = g(x)j(x) + pl(x)$$

say. Thus $m'(\alpha) = g(\alpha)j(\alpha) + p\beta$ with $\beta \in \mathcal{O}_K$. It follows that

$$\text{Norm}_{K|\mathbb{Q}}(m'(\alpha)) = \prod_{\sigma} \sigma(m'(\alpha)) = \prod_{\sigma} \sigma(g(\alpha)j(\alpha)) + p\gamma$$

for some algebraic integer γ . In particular,

$$\text{Norm}_{K|\mathbb{Q}}(m'(\alpha)) = \text{Norm}_{K|\mathbb{Q}}(g(\alpha))\text{Norm}_{K|\mathbb{Q}}(j(\alpha)) + p\gamma$$

and as $P|(g(\alpha))$, we have $p|\text{Norm}_{K|\mathbb{Q}}(g(\alpha))$. Now this also gives that $\gamma \in \mathbb{Z}$. Thus $p|\text{Norm}_{K|\mathbb{Q}}(m'(\alpha))$, and now the result follows as $\Delta^2(\mathbb{Z}[\alpha]) = \pm \text{Norm}_{K|\mathbb{Q}}(m'(\alpha))$. \square

Example 4.4.25. Let $K = \mathbb{Q}(\sqrt{-5})$ such that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $\Delta(\mathbb{Z}[\sqrt{-5}])^2 = 4(-5) = -20$. The possible ramified primes are 2 and 5. We have $m(x) = x^2 + 5$ and

- $x^2 + 5 \equiv (x + 1)^2 \pmod{2}$, such that $(2) = (2, \sqrt{-5} + 1)^2$
- $x^2 + 5 \equiv x^2 \pmod{5}$, such that $(5, \sqrt{-5})^2 = (\sqrt{-5})^2$.

For all primes we have $\sum_{i=1}^r e_i f_i = 2$, so $r \leq 2$. Thus either $r = 1, e_1 = 2, f_1 = 1$ (ramified case), $r = 1, e_1 = 1, f_1 = 2$ (inert case), $r = 2, e_1 = e_2 = 1, f_1 = f_2 = 1$ (splitting case). We extend this notion to general algebraic number fields, saying that p is **inert** if (p) is prime in \mathcal{O}_K , and that p splits otherwise.

We have considered $p = 2, 5$, so consider $p \neq 2, 5$.

- $\left(\frac{-5}{p} = -1\right)$. Then $x^2 + 5$ is irreducible modulo p , and

$$(p) = P := (p, \sqrt{-5}^2 + 5) = (p)$$

is inert.

- $\left(\frac{-5}{p} = 1\right)$, then $x^2 + 5 \equiv (x - a)(x + a) \pmod{p}$, where $a \not\equiv -a \pmod{p}$. Thus, $(p) = P_1 P_2$, where $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$.

4.5 Computation of the Class Group

Definition 4.5.1. Let $\{v_1, \dots, v_n\}$ be any basis for \mathbb{R}^n . Let $L = \{\sum_{i=1}^n a_i v_i \mid a_i \in \mathbb{Z}\}$ be the lattice generated by v_i . This is an additive subgroup of \mathbb{R}^n . Let $D = \{\sum_{i=1}^n a_i v_i \mid a_i \in [0, 1)\}$. We call D the **fundamental domain** for L .

Note that any $v \in \mathbb{R}^n$ can be expressed uniquely as $v = u + w$ with $u \in L$ and $w \in D$.

Definition 4.5.2. If $v_i = \sum_{j=1}^n a_{ij} e_j$ where $\{e_1, \dots, e_n\}$ is the standard basis for \mathbb{R}^n , we define

$$\text{Vol}(D) := |\det(a_{ij})|$$

we also sometimes denote this $\text{Vol}(L)$.

Note that $\text{Vol}(D)^2 = \det(v_i \cdot v_j)$, being the determinant of the matrix $(a_{ij})(a_{ij})^T$. $\text{Vol}(D)$ is independent of the choice of \mathbb{Z} -basis for L , as the change of basis for this is a unitary matrix with determinant ± 1 .

Lemma 4.5.3 (Blichfeldt). Let L be a lattice in \mathbb{R}^n , and let S be a bounded measurable subset of \mathbb{R}^n such that $\text{Vol}(S) > \text{Vol}(L)$. Then there exist $x, y \in S$ with $x \neq y$ such that $x - y \in L$.

Proof. OoSN. Lemma 8.1 of ANT. Slight measure theory bits. \square

Definition 4.5.4. We say that $S \subseteq \mathbb{R}^n$ is **convex** if

$$x, y \in S, 0 \leq \lambda < 1 \implies \lambda x + (1 - \lambda)y \in S$$

We say that S is **symmetric** (about the origin), if

$$x \in S \implies -x \in S$$

Theorem 4.5.5 (Minkowski's Convex Body Theorem). *Let L be a lattice in \mathbb{R}^n . Let S be a bounded measurable subset of \mathbb{R}^n which is convex and symmetric. If $\text{Vol}(S) > 2^n \text{Vol}(L)$ then there exists $v \in L - \{0\}$ with $v \in S$.*

Proof. OoSN. Theorem 8.3 of ANT. Need to clear what 'measurable' is first... \square

Remark 4.5.6. If S is closed (thus compact), it is enough to have $\text{Vol}(S) \geq 2^n \text{Vol}(L)$.

Example 4.5.7. If $p \equiv 1 \pmod{4}$, then there exists $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$. We first note from $(\frac{-1}{p}) = 1$ that there is an s with $s^2 \equiv -1 \pmod{p}$. If $p = x^2 + y^2$, then this equals $0 \pmod{p}$, so $(x/y)^2 \equiv -1 \pmod{p}$. In particular, $x \equiv \pm sy \pmod{p}$. Note,

$$x \equiv sy \pmod{p} \iff x = sy + pz \text{ with } z \in \mathbb{Z} \iff (x, y) = y(s, 1) + z(p, 0)$$

In particular, $\{(s, 1), (p, 0)\}$ is a basis for L (solutions) in \mathbb{R}^2 with

$$\text{Vol}(L) = \left| \det \begin{pmatrix} s & p \\ 1 & 0 \end{pmatrix} \right| = p$$

Let C be the disc $x^2 + y^2 < 2p$ with radius $\sqrt{2p}$. C is convex and symmetric about the origin, and we also have

$$\text{Vol}(C) = \pi(\sqrt{2p})^2 = 2\pi p > 2^2 p = 2^2 \text{Vol}(L)$$

Thus, by Minkowski's Theorem, there exists a nonzero $v \in L$ such that $v \in C$. Suppose that $v = (x, y)$. As $v \in L$ we have $x \equiv sy \pmod{p}$, thus $x^2 + y^2 \equiv 0 \pmod{p}$. On the other hand, $v \in C$ implies that $x^2 + y^2 < 2p$, so we have $x^2 + y^2 = 0$ or p . As v is nonzero, this gives a solution $x^2 + y^2 = p$.

Definition 4.5.8. Let $[K : \mathbb{Q}] := n = r + 2s$ where r is the number of real embeddings $\sigma_1, \dots, \sigma_r : K \rightarrow \mathbb{R}$ and s is the number of pairs of complex embeddings $\sigma_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \dots, \bar{\sigma}_{r+s} : K \rightarrow \mathbb{C}$.

Let $\sigma : K \rightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n$ defined as

$$\sigma(x) := (\sigma_1(x), \dots, \sigma_r(x), \Re(\sigma_{r+1}(x)), \Im(\sigma_{r+1}(x)), \dots, \Re(\sigma_{r+s}(x)), \Im(\sigma_{r+s}(x)))$$

Now let \mathcal{O}_K be the ring of integers of K and let $\{v_1, \dots, v_n\}$ be an integral basis for \mathcal{O}_K . Write A for the matrix whose i th row is $\sigma(v_i)$. By elementary column operations,

$$(-2i)^s \det(A) = \det(\sigma_j(v_i)) = \pm \sqrt{|\Delta^2(K)|} \neq 0$$

where the $(-2i)$ factor comes from the change of basis matrix from $(\Re(z), \Im(z))$ to (z, \bar{z}) . In particular $\det(A) \neq 0$ and $\sigma(\mathcal{O}_K)$ is a lattice in \mathbb{R}^n with volume $\sqrt{|\Delta^2(K)|}/2^s$.

If I is an ideal of \mathcal{O}_K with basis $w = \{w_1, \dots, w_n\}$, then $w_i = \sum_j c_{ij} v_j$, and

$$N(I) = [\mathcal{O}_K : I] = \det(c_{ij})$$

by Theorem 1.0.7. Also, by Lemma 2.0.5, we have $\Delta^2(w) = \det^2(c_{ij}) \Delta^2(v)$, so $\Delta^2(w) = N(I)^2 \Delta^2(v)$, giving

$$\text{Vol}(\sigma(I)) = \frac{\sqrt{|\Delta^2(w)|}}{2^s} = \frac{N(I) \sqrt{|\Delta^2(v)|^2}}{2^s}$$

Lemma 4.5.9. For $t > 0$, let

$$R_t := \{(x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s\} \mid \sum_{i=1}^r |x_i| + 2 \sum_{i=1}^s |z_i| \leq t$$

Then

- R_t is a compact, symmetric, and convex subset of \mathbb{R}^n
- $\text{Vol}(R_t) = 2^r t^n (\pi/2)^s / n!$

Proof. OoSN. See Lang, ANT, page 116. □

Theorem 4.5.10. Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then there exists a nonzero $\alpha \in I$ with

$$|\text{Norm}_{K|\mathbb{Q}}(\alpha)| \leq c_K(N(I))$$

where

$$c_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta^2(K)|}$$

is the **Minkowski's constant** for K .

Proof. Choose $t \in \mathbb{R}$ such that $\pi^s t^n / n! = 4^s \sqrt{|\Delta^2(K)|} N(I)$. Then,

$$\text{Vol}(R_t) = \frac{2^r t^n (\pi/2)^s}{n!} = \frac{2^n \sqrt{|\Delta^2(K)|} N(I)}{2^s} = 2^n \text{Vol}(\sigma(I))$$

By Minkowski's Theorem, there exists a nonzero $\alpha \in I$ such that $\sigma(\alpha) \in R_t$. In particular,

$$\sum_{i=1}^r |\sigma_i(\alpha)| + 2 \sum_{i=r+1}^s \sqrt{\Re(\sigma_i(\alpha)^2) + \Im(\sigma_i(\alpha))^2} \leq t$$

In particular, $\sum_{i=1}^n |\sigma_i(\alpha)| \leq t$, so by AM-GM inequality we get

$$\left(\prod_{i=1}^n |\sigma_i(\alpha)|\right)^{\frac{1}{n}} \leq \frac{1}{n} \left(\sum_{i=1}^n |\sigma_i(\alpha)|\right) \leq \frac{t}{n}$$

giving $|\text{Norm}_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{t}{n}\right)^n = c_K(N(I))$. □

Theorem 4.5.11. Any class ideal $c \in C_K$ contains an ideal J such that $N(J) \leq c_K$, that is

$$N(J) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta^2(K)|}$$

Proof. Let I be any ideal in the inverse class c^{-1} . As we know there exists a nonzero $\alpha \in I$ such that $|\text{Norm}_{K|\mathbb{Q}}(\alpha)| \leq c_K N(I)$. As $(\alpha) \subseteq I$, we have $I|(\alpha)$, we have an ideal J such that $IJ = (\alpha)$. Thus $[J] = c$ and $J \in c$. Taking Norms,

$$N(I)N(J) = N(IJ) = |\text{Norm}_{K|\mathbb{Q}}(\alpha)| \leq c_K N(I)$$

giving $N(J) \leq c_K$. □

Remark 4.5.12. For a nonzero ideal $J \subseteq \mathcal{O}_K$, we have $N(J) = \#\mathcal{O}_K/J$ so that $N(J)(x+J) \in J$ for any $x \in \mathcal{O}_K$ by Langrange's Theorem, viewing \mathcal{O}_K/J as an additive group. Taking $x = 1$, we see that $N(J) \in J$. Thus $J \supseteq (N(J))$ and that $J|(N(J))$. Thus, every class c contains an ideal J such that J has an element $m \in J \cap \mathbb{N}$ with $m \leq c_K$ ($m = N(J)$).

Corollary 4.5.13. *If $K \neq \mathbb{Q}$, then $|\Delta^2(K)| > 1$*

Proof. As $N(J) \geq 1$ for any ideal $J \subseteq \mathcal{O}_K$, we have

$$1 \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta^2(K)|} \leq \left(\frac{4}{\pi}\right)^n \frac{n!}{n^n} \sqrt{|\Delta^2(K)|}$$

Define $b_n := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$. It suffices to show that $b_n > 1$ for all $n \geq 2$. Now,

$$\frac{b_{n+1}}{b_n} = \frac{\pi}{4} \left(1 + \frac{1}{n}\right)^n = \frac{\pi}{4} \left(1 + n\frac{1}{n} + \dots\right) \geq \frac{\pi}{2} > 1$$

Thus $b_n > 1$ for all $n \geq 2$. □

Let c be any ideal class. Then there exists some $J \in c$ such that $N(J) \leq c_K$. Writing J as a product of prime ideals, we have $J = P_1 \dots P_s$. By multiplicativity of the norm, we have $N(P_i) \leq c_K$ for each i . Moreover, as $c = [J] = [P_1 \dots P_s] = [P_1] \dots [P_s]$, c is in the group generated by ideal classes of prime ideals of norm at most c_K . Thus the class group itself is generated by classes of prime ideals in \mathcal{O}_K of norm at most c_K .

To find a suitable set of generators, note that prime ideals of norm at most c_K are factors of ideals (p) where $p \leq c_K$. By Dedekind, p factorises into prime ideals to get a complete set of generators.

To determine the class group, it remains to find any relations satisfied by the classes of these prime ideals. Relations can be obtained by the prime factorisation of ideals (p) , noting (p) is principal, and others can be obtained by factoring principal ideals (α) generated by elements $\alpha \in \mathcal{O}_K$ of smaller norm.

To then show that these relations is complete, one needs to show that appropriate combinations of these generators are not principal. For complex quadratic fields, we can see that I is non-principal by checking all $\alpha \in \mathcal{O}_K$ such that $\text{Norm}_{K|\mathbb{Q}}(\alpha) = N(I)$ and checking whether $I = (\alpha)$. If K is complex quadratic there are only finitely many possible α to check (by explicitly considering the norm).

Example 4.5.14. Let $K = \mathbb{Q}(\sqrt{-5})$ such that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. As \mathcal{O}_K is not a PID (as it is not a UFD), so $h_K > 1$. Also, $n = 2, s = 1, r = 0$, and $\Delta^2(K) = -20$, so

$$c_K = \frac{2!}{2^2} \left(\frac{4}{\pi}\right) \sqrt{20} = \frac{4\sqrt{5}}{\pi} < 3$$

Thus every ideal class contains an ideal of norm at most 2, and that C_K is generated by classes of prime ideals of norm at most 2.

Now, $(2) = P_2^2$, where $P_2 = (2, 1 + \sqrt{-5})$, with $N(P_2) = 2$, so $[P_2]$ generates C_K . Now as $[P_2]^2 = [(2)] = [\mathcal{O}_K]$, C_K is cyclic of order 2 and thus $h_K = 2$.

Example 4.5.15. Taking $K = \mathbb{Q}(\sqrt{-6})$ for $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ with $n = 2, r = 0, s = 1$ and $\Delta^2(K) = -24$, we have

$$c_K = \frac{2!}{2^2} \left(\frac{4}{\pi}\right) \sqrt{24} = \frac{4\sqrt{6}}{\pi} \approx 3.1$$

The ideal class group C_K is generated by classes of prime ideals P such that $N(P) \leq c_K$, meaning that $N(P) = 2$ or 3 .

By Dedekind, $(2) = P_2^2$ where $P_2 := (2, \sqrt{-6})$ and $(3) = P_3^2$ with $P_3 = (3, \sqrt{-6})$. We have $N(P_2) = 2$ and $N(P_3) = 3$. Thus C_K is generated by $[P_2]$ and $[P_3]$. Neither of these are principal as no $(x + y\sqrt{-6})$ can have norm 2 or 3. Now,

$$\sqrt{-6} = \sqrt{-6} \cdot 3 + 2 \cdot \sqrt{-6} \in P_2 P_3$$

And $\text{Norm}_{K|\mathbb{Q}}(\sqrt{-6}) = 6$, giving $(\sqrt{-6}) = P_2 P_3$. It follows that $[P_2][P_3] = [\mathcal{O}_K]$, again showing that C_K must be cyclic of order 2, generated by $[P_2]$ and $h_K = 2$.

Example 4.5.16. We find all integer solutions of the equation $y^2 + 54 = x^3$. Let $x, y \in \mathbb{Z}$ be a solution. If y is even, $x^3 \equiv 2 \pmod{4}$, which is impossible. If $3|y$, then $3|x$, and setting $x = 3x_1, y = 3y_1$, we get $y_1^2 + 6 = 3x_1^3$. Thus $3|y_1$, and writing $y_1 = 3y_2$, we get $3y_2^2 + 2 = x_1^3$. However, $3y_2^2 + 2 \equiv 2 \text{ or } 5 \pmod{9}$, whereas $x_1^3 \equiv 0, 1 \text{ or } 8 \pmod{9}$. This contradiction shows y is coprime to 3.

In particular, $\gcd(y, 6) = 1$, and thus $\gcd(x, 6) = 1$. We now use the ideal factorization $(y + 3\sqrt{-6})(y - 3\sqrt{-6}) = (x)^3$. We claim the factors on the left are coprime. If a prime ideal divides both factors, then $6\sqrt{-6} = \{y + 3\sqrt{-6}\} - \{y - 3\sqrt{-6}\} \in P$, so $P|(6\sqrt{-6}) = P_2^3 P_3^3$. Thus P is either P_2 or P_3 . On the other hand, as $P|(y + 3\sqrt{-6})$ implies that $P|(x)^3$, taking norms gives $N(P)|x^6$, which is impossible as $\gcd(x, 6) = 1$. Thus these are coprime ideals of \mathcal{O}_K , and by unique factorisation of ideals, we have

$$(y + 3\sqrt{-6}) = I^3$$

for some ideal I . As I^3 is principal we know $[I^3] = [\mathcal{O}_K]$, and as $h_K = 2$, $[I]^2 = [\mathcal{O}_K]$ (by Langrange), giving $[I] = [\mathcal{O}_K]$. As I is principal, we have $I = (\alpha)$ for some $\alpha \in \mathcal{O}_K$.

It follows that $(y + 3\sqrt{-6}) = (\alpha)^3 = (\alpha)^3$, giving $y + 3\sqrt{-6} = u\alpha^3$ for some unit u . Units in \mathcal{O}_K are ± 1 , so for both of these we have $u = u^3$. Thus,

$$y + 3\sqrt{-6} = \{u\alpha\}^3 = \{a + b\sqrt{-6}\}^3$$

by equating coefficients and solving gives $3 = b(3a^2 - 6b^2)$ thus $1 = b(a^2 - 2b^2)$. Thus $b = -1$ and $a^2 = 1$, giving $y = a^3 - 18b^2a = a(a^2 - 18b^2) = \pm 17$. With these y the only possible x is 7, giving solutions $x = 7, y = \pm 17$.

Example 4.5.17. Let $K = \mathbb{Q}(\sqrt{-163})$ such that $\mathcal{O}_K = \mathbb{Z}(\frac{1}{2}(1 + \sqrt{-163}))$. Then,

$$c_K = \frac{2}{\pi}\sqrt{163} \approx 8.13 < 9$$

Thus the class group C_K is generated by classes of prime ideals dividing $(2), (3), (5), (7)$. Note that the minimal polynomial of the generator is $x^2 - x + 41$. Modulo 2, this is $x^2 + x + 1$, which is irreducible. In particular, the only prime above 2 is (2) , which is principal (we are using the fact $\mathcal{O}_K \simeq \mathbb{Z}[x]/(x^2 - x + 41)$ and the third isomorphism here). For $p = 3, 5, 7$, we use Dedekind and note that all polynomials $x^2 + 163 \pmod{p}$ is irreducible thus (p) is inert. Thus the only relevant prime ideals are principal. In particular, C_K is trivial and $h_K = 1$. Thus \mathcal{O}_K is a UFD.

Example 4.5.18. The fact $h_K = 1$ for $K = \mathbb{Q}(\sqrt{-163})$ implies that $n^2 + n + 41$ is prime for $0 \leq n \leq 39$.

Suppose for a contradiction that $n^2 + n + 41$ is not prime for some $n < 40$. Now $n^2 + n + 41 < 41^2$ and so $n^2 + n + 41$ must have a prime factor $q < 41$.

Now,

$$q|n^2 + n + 41 = \left\{ n + \frac{1}{2}(1 + \sqrt{-163}) \right\} \left\{ n + \frac{1}{2}(1 - \sqrt{-163}) \right\}$$

However q does not divide either factor in \mathcal{O}_K and so q cannot be prime in \mathcal{O}_K . As we are in a UFD, it follows that q cannot be irreducible. Thus $q = \alpha\beta$ where $\text{Norm}_{K|\mathbb{Q}}(\alpha) = \text{Norm}_{K|\mathbb{Q}}(\beta) = q$. If

$$\alpha = x + y \frac{1 + \sqrt{-163}}{2}$$

then

$$q = \text{Norm}_{K|\mathbb{Q}}(\alpha) = \left(x + \frac{y}{2}\right)^2 + 163 \left(\frac{y}{2}\right)^2$$

As q is not square we have $y \neq 0$, giving $q \geq 163/4 > 40$, which gives a contradiction.

Remark 4.5.19. With similar logic,

- $n^2 + n + 17$ is prime for $0 \leq n \leq 15$ with $\mathbb{Q}(\sqrt{-67})$.
- $n^2 + n + 11$ is prime for $0 \leq n \leq 9$ with $\mathbb{Q}(\sqrt{-43})$
- $n^2 + n + 5$ is prime for $0 \leq n \leq 3$ with $\mathbb{Q}(\sqrt{-19})$
- $n^2 + n + 3$ is prime for $0 \leq n \leq 1$ with $\mathbb{Q}(\sqrt{-11})$

Example 4.5.20. Taking $K = \mathbb{Q}(\sqrt{-29})$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-29}]$ and $\Delta^2(K) = -116$. We have $n = 2$ and $s = 1$, so

$$c_K = \left(\frac{2}{\pi}\right) \sqrt{116} \approx 6.9 < 7$$

C_K is thus generated by classes of prime ideals dividing (2), (3) and (5). To factor these, by Dedekind,

- $x^2 + 29 \equiv (x + 1)^2 \pmod{2}$, so $(2) = P_2^2$ where $P_2 := (2, \sqrt{-29} + 1)$ of norm 2.
- $x^2 + 29 \equiv x^2 - 1 \equiv (x + 1)(x - 1) \pmod{3}$, so $(3) = P_3 P'_3$, where $P_3 := (3, \sqrt{-29} + 1)$ and $P'_3 := (3, \sqrt{-29} - 1)$ are distinct prime ideals of norm 3.
- $x^2 + 29 \equiv x^2 - 1 \equiv (x + 1)(x - 1) \pmod{5}$, so $(5) = P_5 P'_5$ with $P_5 := (5, \sqrt{-29} + 1)$ and $P'_5 := (5, \sqrt{-29} - 1)$ are distinct prime ideals of norm 5.

In particular, $[P]^2 = [P_3][P'_3] = [P_5][P'_5] = [\mathcal{O}_K]$. Thus C_K is generated by $[P_2], [P_3], [P_5]$. Considering $\text{Norm}_{K|\mathbb{Q}}(x + y\sqrt{-29}) = x^2 + 29y^2$, there are no elements in \mathcal{O}_K with norms $\pm 2, \pm 3, \pm 5$, meaning P_2, P_3, P_5 are not principal, and $[P_2]$ must have order 2.

The only element $\alpha \in \mathcal{O}_K$ of norm ± 9 is ± 3 . Thus if $P_3^2 = (\alpha)$, then we have $P_3^2 = (3) = P_3 P'_3$, which implies $P_3 = P'_3$, a contradiction. Thus the order of $[P_3]$ is at least 3. We also cannot have order 3 as there are no solutions to $x^2 + 29y^2 = \pm 27$.

Considering $[P_5]$, note that $3^2 + 29 \times 2^2 = 125$, so that $N(3 + 2(\sqrt{-29})) = 5^3$. Thus, $(3 + 2\sqrt{-29})$ must be one of $P_5^3, P_5^2 P'_5, P_5 P_5'^2, P_5'^3$. However, $3 + 2\sqrt{-29} \in P_5$, giving $3 + 2\sqrt{-29} \notin P_5'$. Thus P_5 does not divide this, giving $(3 + 2\sqrt{-29}) = P_5^3$, and taking conjugates shows $(3 - 2\sqrt{-29}) = P_5'^3$. Thus $[P_5]$ has order dividing 3. As P_5 is not principal, the order of P_5 is exactly 3.

Finally,

$$(30) = (2)(3)(5) = (1 + \sqrt{-29})(1 - \sqrt{-29})$$

And from $(2)(3)(5) = P_2^2 P_3 P_3' P_5 P_5'$, we can deduce that $(1 \pm \sqrt{-29})$ must be of the form $P_2 P_3^* P_5^*$, and in either case, $[P_3]$ is in the group generated by $[P_2]$ and $[P_5]$. Thus, C_K is an abelian group generated by an element of order 2 and an element order 3. This gives a cyclic group of order 6. We can use the arguemtn above to explicitly find that $(2 + 5\sqrt{-29}) = P_3^6$ and $(2 - 5\sqrt{-29}) = P_3'^6$.

Example 4.5.21. Let $K = \mathbb{Q}(\sqrt{-37})$. Given that $h_K = 2$, we show that there are no integral solutions of the equation $y^2 = x^3 + 37$.

Suppose that $x, y \in \mathbb{Z}$ such that $y^2 + 37 = x^3$. Then as ideals we have

$$(y + \sqrt{-37})(y - \sqrt{-37}) = (x)^3$$

We claim these two are coprime ideals. Suppose that a prime ideal P divides both. Then $y \pm \sqrt{-37} \in P$, so that the difference $2\sqrt{-37} \in P$. Thus $P|(2\sqrt{-37})$ and since P is prime we conclude that $P|(2)$ or $P|(\sqrt{-37})$. As $\mathcal{O}_K = \mathbb{Z}[\sqrt{-37}]$, we factor (2) and (37) using the decomposition of $x^2 + 37$ modulo p . We have

- $x^2 + 37 \equiv (x + 1)^2 \pmod{2}$, giving $(2) = P_2^2$ where $P_2 := (2, 1 + \sqrt{-37})$
- $x^2 + 37 \equiv x^2 \pmod{37}$, so $(37) = (37, \sqrt{-37})^2 = P_{37}^2$, where $P_{37} := (\sqrt{-37})$ is a prime of norm 37.

It follows that if P is a common factor of $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$, then $P = P_2$ or $P = P_{37}$. In either case, as $P|(y + \sqrt{-37})$, we have $P|(x)^3$, taking norms we get $2|x^6$ or $37|x^6$ respectively. Thus either $2|x$ or $37|x$.

If $37|x$, then from our original equation we have $37|y$. Thus 37^2 divides $x^3 - y^2 = 37$, a contradiction. If $2|x$, we have $8|x^3$, but then $y^2 + 1 \equiv 0 \pmod{4}$, a contradiction.

Thus $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$ are coprime ideals. Their products is a cube, thus by unique factorisation of ideals we have

$$(y + \sqrt{-37}) = I^3$$

for some ideal I . As I^3 is principal, the order of $[I]$ in C_K divides 3. As $h_K = 2$, I must be principal. Thus,

$$(y + \sqrt{-37}) = (a + b\sqrt{-37})^3$$

for some $a, b \in \mathbb{Z}$. In particular, $y + \sqrt{-37} = u(a + b\sqrt{-37})^3$ for some unit $u \in \mathcal{O}_K$. As the only such units are ± 1 , we have $u = \pm 1$, so we may replacing a, b by $-a, -b$ if appropriate, we may assume that $u = 1$. Expanding, we get $y = a(a^2 - 111b^2)$ and $1 = b(3a^2 - 37b^2)$. The second equation implies that $b = \pm 1$ and $3a^2 - 37 = \pm 1$. No such a exists.

4.6 Fermat's Theorems

Definition 4.6.1. Let p be prime and $m \in \mathbb{Z}$. m is a **quadratic residue** mod p if there exists a $x \in \mathbb{Z}$ such that $m \equiv x^2 \pmod{p}$. Otherwise, m is a **quadratic non-residue** mod p .

Lemma 4.6.2. For any prime $p \neq 2$, define $\psi : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ by $x \mapsto x^2$. This is a 2-to-1 map. In particular, exactly half of $\{1, \dots, p-1\}$ are quadratic residues mod p , and half are quadratic non-residues mod p .

Proof. Follows by observing the kernel and also noting that $\psi(x) = \psi(p-x)$. □

Definition 4.6.3. For a prime p and $p \nmid m$, define the **Legendre symbol** by

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & \text{if } m \text{ is a quadratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

When $p|m$, define $\left(\frac{m}{p}\right) = 0$.

Lemma 4.6.4. Let p be an odd prime and $p \nmid m, n, m_1, m_2$. Then,

- If $m_1 \equiv m_2 \pmod{p}$, then $\left(\frac{m_1}{p}\right) = \left(\frac{m_2}{p}\right)$
- $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right)$
- $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$ or $p = 2$. $\left(\frac{-1}{p}\right) = -1 \iff p \equiv 3 \pmod{4}$.
- $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}$. $\left(\frac{2}{p}\right) = -1 \iff p \equiv \pm 3 \pmod{8}$.

Theorem 4.6.5 (Gauss's Law of Quadratic Reciprocity). Let $p \neq 2, q \neq 2$ be distinct primes. If either $p \equiv 1$ or $q \equiv 1 \pmod{4}$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. If both $p \equiv 3$ and $q \equiv 3 \pmod{4}$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Theorem 4.6.6. If p is prime and $p \equiv 1 \pmod{4}$, then there exists $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ and this decomposition is unique.

Proof. Assume that $p \equiv 1 \pmod{4}$. Then we have $(-1)^{(p-1)/2} = 1$, so there exists some $r \in \mathbb{Z}$ such that $p|1 + r^2$. Extending to $\mathbb{Z}[i]$, we have $p|(1 + ri)(1 - ri)$. If p is irreducible in $\mathbb{Z}[i]$, then $p|(1 + ri)$ or $p|(1 - ri)$, as any irreducible is prime. However, p cannot divide $1 + ri$ for example, as $\frac{1}{p} + \frac{r}{p}i \notin \mathcal{O}_K$. Thus we can write $p = (a + bi)(c + di)$ neither units. Taking norms,

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

As \mathbb{Z} is a UFD and neither $a + bi$ or $c + di$ has norm ± 1 , we have $p = a^2 + b^2 = (a + bi)(a - bi)$. This shows existence. If $a + bi = \alpha\beta \in \mathbb{Z}[i]$, taking norms gives

$$p = \text{Norm}(\alpha)\text{Norm}(\beta)$$

Thus α or β must be a unit. Hence $a + bi$ is irreducible in $\mathbb{Z}[i]$ and similarly for $a - bi$. Hence $p = (a + bi)(a - bi)$ is the unique factorisation of p into irreducibles. If $p = e^2 + f^2 = (e + fi)(e - fi)$, then $e + fi$ is an associate of $a + bi$ or $a - bi$, and in any case $\{a^2, b^2\} = \{e^2, f^2\}$. \square

Theorem 4.6.7. The only integer solutions of $y^2 + 2 = x^3$ are $x = 3, y = \pm 5$

Proof. If y were even then x is also even, giving $8|y^2 + 2$ which is impossible since $4|y^2$. Thus y is odd. We can decompose $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. Suppose that there is an irreducible element α which divides both $y + \sqrt{-2}$ and $y - \sqrt{-2}$. Then α divides the difference $2\sqrt{-2} = \sqrt{-2}^3$. However, $\sqrt{-2}$ is irreducible since its norm is 2, which is prime in \mathbb{Z} . Hence we must have $\alpha = \pm\sqrt{-2}$. Now,

$$\alpha|y + \sqrt{-2} \implies \sqrt{-2}|y \implies 2|y^2$$

which is a contradiction as y is odd. Hence $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime. Unique factorisation of $\mathbb{Z}[\sqrt{-2}]$ implies that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are associates of cubes. As the only units are ± 1 , they are indeed both cubes. Now,

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3$$

solving gives $(a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}$. Thus $b(3a^2 - 2b^2) = 1$. Giving $b = \pm 1$ and $a = \pm 1$. Substituting these combinations, we get $y = \pm 5$, thus $x = 3$. \square

5 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 - i min poly irreducible has no repeated roots - i 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 \mathcal{O}_K are generated by n elements as they are submodules of \mathbb{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,

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

Remark 5.0.1. Note first that every ideal in \mathcal{O}_K can be written with at most 2 generators. (Proof. prime ideals height c over a noetherian ring can be generated by c elements, and the height of any maximal ideal in \mathcal{O}_K is 2) Thus, write (α, β) for the ideal $(\alpha) + (\beta)$. Then the product

$$(\alpha, \beta)(\gamma, \delta) = \left\{ \sum_{i=1}^n \mu_i \nu_i \mid \mu_i \in (\alpha, \beta), \nu_i \in (\gamma, \delta) \right\}$$

clearly contains $\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta$. On the other hand, $\mu_i \nu_i$ is of the shape $(\alpha a + \beta b)(\gamma c + \delta d) \in (\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta)$. Thus,

$$(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta)$$

Reducing generators explicitly can be done using ad-hoc methods (usually just expanding and double inclusion).

5.1 Fermat's Last Equation for the Cubic

We prove in this subsection that $x^3 + y^3 = z^3$ has no nontrivial solutions in \mathbb{Z} . We work in $K = \mathbb{Q}(\sqrt{-3})$, and we write

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

such that $\mathcal{O}_K = \mathbb{Z}[\omega]$ for the rest of this subsection.

Lemma 5.1.1. *We have the following:*

- $\omega^3 = 1$. The units of \mathcal{O}_K are $\pm 1, \pm \omega, \pm \omega^2$.
- The ring \mathcal{O}_K is a UFD.
- The element $\lambda := \sqrt{-3}$ is prime with norm 3. Moreover we have $\lambda = \omega(1-\omega) = (-\omega^2)(1-\omega^2)$.

Proof. Note that to find the units, we look for $\text{Norm}_{K|\mathbb{Q}}(a + b\omega) = a^2 - ab + b^2 = \pm 1$. The set of solutions that satisfy this gives exactly the above units. To show \mathcal{O}_K is a UFD, it suffices to show that $\mathbb{Q}(\sqrt{-3})$ has class number 1. This is actually immediate as we have

$$c_K = \left(\frac{2}{\pi}\right) \sqrt{3} \approx 1.103 < 2$$

Thus every ideal class contains a prime ideal whose norm is at most 1, and in particular every ideal class contains a principal ideal, thus actually simply has class number 1. The last case follows by a simple check. \square

Lemma 5.1.2. *If $\alpha \in \mathbb{Z}[\omega]$ and λ does not divide α , then $\alpha^3 = \pm 1 \pmod{\lambda^4}$.*