Algebraic Number Theory Notes

Alexandre Daoud

May 2, 2016

1 Introduction

Definition 1.1. Let K be a finite degree algebraic field extension of $\mathbb{Q}$. Then K is said to be a **number field**.

Example 1.2. Let $f(X) \in \mathbb{C}[X]$ be a monic irreducible polynomial. If $\alpha \in \mathbb{C}$ is a root of $f(X)$ then $\mathbb{Q}(\alpha)$ is a number field. To see this, consider the following ring homomorphism

$$\begin{aligned} \varphi : \mathbb{Q}[X] &\to \mathbb{Q}[\alpha] \\ X &\mapsto \alpha \end{aligned}$$

Then $\ker \varphi = (f)$ and thus $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha]$. Now $\mathbb{Q}[X]$ is a PID and (f) is maximal since f is irreducible. Hence $\mathbb{Q}[X]/(f)$ is a field and we may write $\mathbb{Q}[X]/(f) \cong \mathbb{Q}(\alpha)$. Finally, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f$ since $\mathbb{Q}(\alpha)$ has a $\mathbb{Q}$-basis of $\{ 1, \alpha, \alpha^2, \ldots, \alpha^{\deg f - 1} \}$.

Example 1.3. Let $\alpha = \sqrt{2}$. Then α satisfies the monic irreducible polynomial $X^2 - 2$ over $\mathbb{Q}$. Hence $\mathbb{Q}(\sqrt{2})$ is a number field.

Example 1.4. Let $f(X) = X^3 - 2 \in \mathbb{Q}[X]$. Then f has roots $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \omega\sqrt[3]{2}, \alpha_3 = \omega^2\sqrt[3]{2}$ where ω is the primitive cube root of unity. Then

$$\mathbb{Q}(\alpha_i) \cong \mathbb{Q}[X]/(f)$$

are all number fields but $\mathbb{Q}[\alpha_1], \mathbb{Q}[\alpha_2], \mathbb{Q}[\alpha_3]$ are all distinct subfields of $\mathbb{Q}$.

Definition 1.5. An **algebraic number** is any element of a number field.

Definition 1.6. Let K be a number field. If $\alpha \in K$ satisfies a monic polynomial over $\mathbb{Z}$ then α is said to be an **algebraic integer**. The set of all algebraic integers of K is denoted $\mathcal{O}_K$.

Proposition 1.7. *Let K be a number field. Then α is an algebraic integer of K if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.*

Proof. Suppose that the minimal polynomial of α has integer coefficients. Then, by definition, α is an algebraic integer.

Conversely, suppose that α is an algebraic integer. Then α is a root of a monic polynomial with integer coefficients, say $f(X)$. Let $g(X)$ be its minimal polynomial. Then $g(X)|f(X)$. Then there exists a monic polynomial $h(X) \in \mathbb{Q}[X]$ such that $g(X)h(X) = f(X)$. We need to show that $g(X)$ also has integer coefficients. Suppose that it doesn't. Then there exists a prime number which divides the denominator of one of the coefficients of g. Let u be the least integer such that $p^u g(X)$ has no coefficients whose denominators are divisible by p. Similarly, let v be the same for $h(X)$. Then

$$p^u g(X) p^v h(X) = p^{u+v} g(X) h(X) \equiv 0 \pmod{p} \in \mathbb{F}_p[X]$$

This is a contradiction since $p^u g(X)$ and $p^v h(X)$ are non-zero polynomials whose product is 0 but $\mathbb{F}_p(X)$ has no zero divisors. □

Corollary 1.8. *The algebraic integers of $\mathbb{Q}$ are exactly $\mathbb{Z}$.*

Proof. Let $a/b \in \mathbb{Q}$. Then its minimal polynomial over $\mathbb{Q}$ is $X - a/b$. Now, the previous proposition implies that a/b is an algebraic integer if and only if $b = 1$. □

Theorem 1.9. *Let K be a number field. Then $\alpha \in K$ is an algebraic integer if and only if $Z[\alpha]$ is finitely generated.*

Proof. Suppose that α is an algebraic integer. Let $f(X)$ be its minimal polynomial of degree n. Then by Proposition 1.7, $f(X)$ is monic with integer coefficients. Now any α^u can be written as a $\mathbb{Z}$-linear combination of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for all $u \geq n$. Hence

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^{n-1}$$

whence $\mathbb{Z}[\alpha]$ is finitely generated.

Conversely, suppose that $\mathbb{Z}[\alpha]$ is finitely generated. Let $a_i, \ldots, a_n$ be generators for $\mathbb{Z}[\alpha]$. Then there exists polynomials $f_i(X) \in \mathbb{Z}[X]$ such that $a_i = f_i(\alpha)$ for all $1 \leq i \leq n$. Fix some natural number $N > \deg f_i$ for all i. Then we may write

$$\alpha^N = \sum_{i=1}^{n} b_i a_i$$

for some $b_i \in \mathbb{Z}$. That is to say

$$\alpha^N - \sum_{i=1}^{n} b_i f_i(\alpha) = 0$$

Taking

$$f(X) = X^N - \sum_{i=1}^{n} b_i f_i(X)$$

we may see that α is an algebraic integer. □

Corollary 1.10. *Let K be a number field. Then $\mathcal{O}_K$ is a ring.*

Proof. Let $\alpha, \beta \in \mathcal{O}_K$. Then the previous theorem implies that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated whence $\mathbb{Z}[\alpha, \beta]$ is finitely generated. $\mathbb{Z}[\alpha, \beta]$ is a ring and thus $\alpha \pm \beta$ and $\alpha\beta$ are in $\mathbb{Z}[\alpha, \beta]$. $\mathbb{Z}[\alpha \pm \beta]$ and $\mathbb{Z}[\alpha\beta]$ are subgroups of $\mathbb{Z}[\alpha, \beta]$ and are hence finitely generated. By the opposite implication of the previous theorem, we see that $\alpha \pm \beta$ and $\alpha\beta$ are in $\mathcal{O}_K$. □

Theorem 1.11. *Let $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer d. Then*

$$\mathcal{O}_K = \begin{cases} \{\, a + b\sqrt{d} \mid a, b \in \mathbb{Z} \,\} & \text{if } d \not\equiv 1 \pmod{4} \\ \left\{\, a + b\left(\frac{1+\sqrt{d}}{2}\right) \,\middle|\, a, b \in \mathbb{Z} \,\right\} & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

Proof. Suppose $\alpha \in K$ is an algebraic integer. Then $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$ and satisfies some monic irreducible polynomial $f(X)$ over $\mathbb{Z}$. The conjugate of α is $a - b\sqrt{d}$ and thus its minimal polynomial is

$$f(X) = X^2 + (2a)X + (a^2 - b^2 d)$$

Necessarily, $2a, a^2 - b^2 d \in \mathbb{Z}$. This implies that either $a \in \mathbb{Z}$ or $a = A/2$ for some odd integer $A \in \mathbb{Z}$. In the first case, we must then have that $b^2 d \in \mathbb{Z}$. Since d is square-free, this implies that $b \in \mathbb{Z}$. Hence at the very least, the algebraic integers contain $\{\, a + b\sqrt{d} \mid a, b \in \mathbb{Z} \,\}$.

In the second case we have

$$\frac{A^2}{4} - b^2 d \in \mathbb{Z} \tag{1}$$

Multiplying through by 4 we see that $A^2 - 4b^2 d \in 4\mathbb{Z}$. We must therefore have that $4b^2 d \in \mathbb{Z}$. Since d is square-free, this implies that $2b \in \mathbb{Z}$, say $2b = B$. Equation 1 implies that $b \notin \mathbb{Z}$ so B is an odd integer. Then

$$A^2 - B^2 d \equiv 0 \pmod{4}$$

with A and B both odd integers. But any odd integer is congruent to 1 modulo 4 so

$$1 - d \equiv 0 \pmod{4}$$

Now this is only possible if $d \equiv 1 \pmod{4}$ and the result follows. □

2 Norms, Traces and Discriminants

Definition 2.1. let L/K be a finite extension of number fields. Given $\alpha \in L$, consider the K-linear map

$$\begin{aligned} \mu_\alpha : L &\to L \\ x &\mapsto \alpha x \end{aligned}$$

We define the **norm** of α, denoted $\mathrm{N}_{L/K}(\alpha)$ to be the determinant of the matrix of μ_α. Furthermore, we define the **trace** of α, denoted $\mathrm{Tr}_{L/K}(\alpha)$, to be the trace of the matrix of μ_α. Finally, we define the **characteristic polynomial** of α, denoted $\chi_{L/K}(\alpha)(X)$, to be the characteristic polynomial of the matrix of μ_α.

Example 2.2. Let $K = \mathbb{Q}(2)$. Let $\alpha \in \mathbb{Q}(2)$ and fix the $\mathbb{Q}$-basis of K, $\{\, 1, \sqrt{2} \,\}$. To calculate the norm and trace of α, it suffices to examine the effect of α on the basis elements. We can write $\alpha = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Then multiplication by α sends 1 to $a + b\sqrt{2}$ and sends $\sqrt{2}$ to $a\sqrt{2} + 2b$. The matrix of μ_α in the chosen basis is thus

$$M = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$$

Hence $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \det M = a^2 - 2b^2$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}\ M = 2a$. We now calculate the characteristic polynomial of α :

$$\begin{aligned} \chi_{L/K}(\alpha)(X) &= \det(XI - M) \\ &= \begin{vmatrix} X - a & b \\ 2b & X - a \end{vmatrix} \\ &= (X - a)^2 - 2b^2 \\ &= X^2 - 2aX + a^2 - 2b^2 \end{aligned}$$

We see that the coefficient of X is minus the trace of α and its constant term is the norm of alpha.

Lemma 2.3. *Let K be a number field and $f(X) \in K[X]$ an irreducible polynomial. Then $f(X)$ cannot have a multiple root in an algebraic closure of K.*

Proof. Let $\overline{K}$ be an algebraic closure of K. Suppose that $f(X)$ has a multiple root in $\overline{K}$, say α. We may write $f(X) = (X-\alpha)^m g(X)$ for some $m \geq 2$ and $g(X) \in \overline{K}[X]$. Calculating the formal derivative of $f(X)$ we have

$$f'(X) = m(X-\alpha)^{m-1}g(X) + (X-\alpha)^m g'(X)$$

Hence $f'(X)$ and $f(X)$ have the factor $(X-\alpha)^{m-1}$ in common in $\overline{K}[X]$. This implies that α is a root of both $f(X)$ and $f'(X)$ meaning the minimal polynomial of α over K divides both $f(X)$ and $f'(X)$. But $f(X)$ was assumed to be irreducible so that common factor must be $f(X)$ itself. Now, $\deg f'(X) < \deg f(X)$ meaning $f'(X)$ is identically zero but this is not possible since K has characteristic 0. □

Theorem 2.4. *Let K be a number field and $\overline{K}$ an algebraic closure of K. If L/K is a finite extension of degree n then there exist n distinct K-embeddings of L into $\overline{K}$.*

Proof. We shall prove the theorem by induction on $[L : K]$. First suppose that $L = K(\alpha)$ for some $\alpha \in \overline{K}$. Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Then $f(X)$ has degree n and, by Lemma 2.3, it has n distinct roots in $\overline{K}$, say $\alpha = \alpha_1, \ldots, \alpha_n$. We thus have n distinct K-embeddings given by

$$\begin{aligned} \sigma_i : L &\to \overline{K} \\ \alpha &\mapsto \alpha_i \end{aligned}$$

Now suppose that $m < n$ and that for any degree m extension of K, say F, there exist m-distinct K-embeddings of F into $\overline{K}$. Let L/K be an extension of degree n and suppose that $\alpha \in L$. We have that $K \subseteq K(\alpha) \subseteq L$. Let $q = [K(\alpha) : K]$. From the previous paragraph, we know that there exists q distinct embeddings of $K(\alpha)$ into K. Since $K(\alpha)$ is isomorphic to $K(\sigma_i(\alpha))$ for all K-embeddings $\sigma_i : K(\alpha) \to \overline{K}$, there exists an extension of σ_i to an isomorphism τ_i such that the following diagram commutes

$$\begin{tikzcd}
L \arrow[r, "\tau_i"] & L_i \\
K(\alpha) \arrow[u] \arrow[r, "\sigma_i|_{K(\alpha)}"] & K(\sigma_i(\alpha)) \arrow[u] \\
K \arrow[u] \arrow[ur]
\end{tikzcd}$$

By the tower law we have $[L : K(\alpha)] = [L : K(\sigma_i(\alpha))] = n/q$. Therefore, by the induction hypothesis, there exist n/q distinct $K(\sigma_i(\alpha))-$embeddings of L_i into $\overline{K}$, say θ_{ij} for $1 \leq j \leq n/q$. Then $\theta_{ij} \circ \tau_i$ for $i = 1, \ldots, q$ and $j = 1, \ldots, n/q$ give n distinct K-embeddings of L into $\overline{K}$. □

Corollary 2.5. *Let K be a number field of degree n. Then there exist n distinct $\mathbb{Q}$-embeddings of K into $\mathbb{C}$.*

Definition 2.6. Let L/K be an extension of number fields of degree n. Let $\alpha \in L$ and let $\sigma_1, \ldots, \sigma_n$ be distinct K-embeddings of L into an algebraic closure of K, say $\overline{K}$. Then $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are the **conjugates** of α.

Proposition 2.7. *Let L/K be an extension of number fields and $\overline{K}$ an algebraic closure of K. Let $\sigma_1, \ldots, \sigma_n$ be the distinct K-embeddings of L into $\overline{K}$. Then for all $\alpha \in L$ we have*

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Proof. Let $f(X)$ be the minimal polynomial of α over K and let m be its degree. Let $\chi_{K(\alpha)/K}(\alpha)$ be the characteristic polynomial of α. We first claim that $f(X) = \chi_{K(\alpha)/K}(\alpha)(X)$. Both polynomials are monic by their definition and the degree of $\chi_{K(\alpha)/K}(\alpha)$ is also m. Let μ_α be the linear map given by multiplication of α. By the Cayley-Hamilton theorem, we have that $\chi_{K(\alpha)/K}(\mu_\alpha) = 0$. It is easy to see that $\chi_{K(\alpha)/K}(\alpha)(\mu_\alpha) = \mu_{\chi_{K(\alpha)/K}}(\alpha)$. Hence α is a root of $\chi_{K(\alpha)/K}(X)$. This implies that $f(X)|\chi_{K(\alpha)/K}(X)$. But these polynomials have the same degree and are both monic so we must have that $f(X) = \chi_{K(\alpha)/K}(X)$.

We now construct the matrix of μ_α in a K-basis of L. Let $\{ 1, \ldots, \alpha^{m-1} \}$ be a K-basis of $K(\alpha)$. If k is the degree of $L/K(\alpha)$ then let $\{ \beta_1, \ldots, \beta_k \}$ be a $K(\alpha)$-basis of L. Then $\{ \alpha^i \beta_j \}$ for $0 \leq i \leq m$ and $1 \leq j \leq k$ is a K-basis of L. Then the matrix of μ_α can be written as

$$\mu_\alpha = \underbrace{\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ 0 & 0 & \vdots & 0 \\ 0 & 0 & \cdots & B \end{pmatrix}}_{k \text{ times}}, \quad B = \begin{pmatrix} 0 & 0 & \cdots & a_0 \\ 1 & 0 & \cdots & a_1 \\ 0 & 1 & \ddots & a_2 \\ \vdots & \cdots & \cdots & \vdots \\ 0 & \cdots & \cdots & a_{m-1} \end{pmatrix}$$

wehre a_i are the coefficients of the minimal polynomial of α. It then follows that

$$\mathrm{N}_{L/K}(\alpha) = \mathrm{N}_{K(\alpha)/K}(\alpha)^k \tag{2}$$
$$\mathrm{Tr}_{L/K}(\alpha) = k\,\mathrm{Tr}_{K(\alpha)/K}(\alpha) \tag{3}$$
$$\chi_{L/K}(\alpha)(X) = \chi_{K(\alpha)/K}(\alpha)(X)^k = f(X)^k \tag{4}$$

Hence

$$\begin{aligned} f(X) &= (X - \alpha_1) \ldots (X - \alpha_m) \\ &= X^m - \left(\sum_{i=1}^{m} \alpha_i \right) X^{m-1} + \cdots \pm \prod_{i=1}^{m} \alpha_i \\ &= X^m - \mathrm{Tr}_{K(\alpha)/K}(\alpha) X^{m-1} + \cdots + \pm \mathrm{N}_{K(\alpha)/K}(\alpha) \end{aligned}$$

This, together with the previous equations, gives us

$$\mathrm{N}_{L/K}(\alpha) = \left(\prod_{i=1}^{m} \alpha_i \right)^k$$
$$\mathrm{Tr}_{L/K}(\alpha) = k \sum_{i=1}^{m} \alpha_i$$

Now, $f(X)$ has m distinct roots in $\overline{K}$ and this determines the m distinct K-embeddings of $K(\alpha)$ into $\overline{K}$. By Theorem 2.4, there are k ways in which we can extend these to K-

embeddings of L. Hence

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$
$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

□

Example 2.8. Consider the number field extensions $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(i, \sqrt{2})$. There are four embeddings of $\mathbb{Q}(i, \sqrt{2})$ into $\mathbb{C}$ given by

$$\sigma_1 : i \mapsto i, \sqrt{2} \mapsto \sqrt{2}$$
$$\sigma_2 : i \mapsto -i, \sqrt{2} \mapsto \sqrt{2}$$
$$\sigma_3 : i \mapsto i, \sqrt{2} \mapsto -\sqrt{2}$$
$$\sigma_4 : i \mapsto -i, \sqrt{2} \mapsto -\sqrt{2}$$

We have that

$$\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) = \sigma_1(a+ib)\sigma_2(a+ib) = a^2+b^2$$

$$\mathrm{N}_{\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}}(a+ib) = \sigma_1(a+ib)\sigma_2(a+ib)\sigma_3(a+ib)\sigma_4(a+ib) = (a^2+b^2)^2$$

Corollary 2.9. *Let K be a number field and $\alpha \in K$ an algebraic integer. Then the norm and trace of α are rational integers.*

Proof. By the proof of the theorem, the characteristic polynomyial of α is a power of the minimal polynomial and thus has rational integer coefficients. □

Corollary 2.10. *Let K be a number field and $\alpha \in \mathcal{O}_K$. Then the norm of α is equal to ± 1 if and only if α is a unit in $\mathcal{O}_K$.*

Proof. First suppose that the norm of α is equal to ± 1. Let $f(X) = \sum_{i=0}^{n} a_i X^i$ be its minimal polynomial over K. Then $f(X)$ has constant term ± 1. We claim that $1/\alpha$ is a root of the polynomial $1 + a_{n-1}X + \cdots \pm X^n$. We have that

$$g(X) = X^n(X^{-n} + a_{n-1}X^{-1} + \cdots \pm 1) = X^n f(1/X)$$

Hence $g(1/\alpha) = (1/\alpha)^n f(\alpha) = 0$. Clearly, $g(X) \in \mathbb{Z}[X]$. If the coefficient of the leading term is 1 then we are done, if not then $-g(X)$ is also a monic polynomial with rational integer coefficients with $1/\alpha$ as a root and thus α is a unit in $\mathcal{O}_K$.

Conversely, suppose that α is a unit in $\mathcal{O}_K$. Since α is a unit, we have that $1/\alpha \in \mathcal{O}_K$. Then

$$1 = \mathrm{N}_{K/\mathbb{Q}}(1) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\,\mathrm{N}_{K/\mathbb{Q}}(1/\alpha)$$

By the previous corollary, we know that both $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{N}_{K/\mathbb{Q}}(1/\alpha)$ are elements of $\mathbb{Z}$ so we must have that $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$. □

Lemma 2.11. *Let K be a number field. Then $\mathbb{Q}\mathcal{O}_K = K$.*

Proof. It is trivial from the definition of K that $\mathbb{Q}\mathcal{O}_K \in K$.
Conversely, suppose that $\alpha \in K$. We claim that there exists a $d \in \mathbb{Z}$ such that $\alpha d \in \mathcal{O}_K$. Indeed, let $f(X)$ be the minimal polynomial of α over $\mathbb{Q}$. Let d be the least common multiple of the denominators of the coefficients of $f(X)$. Then

$$g(X) = d^{\deg f} f(X/d)$$

is a monic polynomial with coefficients in $\mathbb{Z}$ and αd as a root. Hence $\alpha d \in \mathcal{O}_K$ $\square$

Theorem 2.12. *Let K be a number field. Then $\mathcal{O}_K$ is a free Abelian group of rank $n = [K : \mathbb{Q}]$.*

Proof. Fix a $\mathbb{Q}$-basis of K, say $\{ \alpha_1, \dots, \alpha_n \}$. By Lemma 2.11, each α_i gives rise to an algebraic integer β_i. Furthermore, it is easy to see that the set $\{ \beta_1, \dots, \beta_n \}$ is still $\mathbb{Q}$-linearly independent and spans K. Hence any $x \in \mathcal{O}_K$ can be written in the form

$$x = \sum_{i=1}^{n} c_i \beta_i$$

for some $c_i \in \mathbb{Q}$. We claim that the denominators of the c_i are bounded for all $x \in \mathcal{O}_K$ and $c_i \in \mathbb{Q}$. Suppose the contrary. Then there exists a sequence $\{ x_j \}_{j \geq 1}$ where

$$x_j = \sum_{i=1}^{n} c_{ij} \beta_i$$

for some $c_{ij} \in \mathbb{Q}$ such that the greatest denominator of the c_{ij} tends to infinity as $j \to \infty$.

Now let $\sigma_1, \dots, \sigma_n$ be the distinct $\mathbb{Q}$-embeddings of K into an algebraic closure of K, say $\overline{K}$. Then

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}}(x_j) &= \prod_{m=1}^{n} \sigma_m(x_j) \\
&= \prod_{m=1}^{n} \sigma_m \left(\sum_{i=1}^{n} c_{ij} \beta_i \right) \\
&= \prod_{m=1}^{n} \sum_{i=1}^{n} c_{ij} \sigma_m(\beta_i)
\end{aligned}$$

Now, $\mathrm{N}_{K/\mathbb{Q}}(x_{ij})$ is necessarily an integer and the right hand side is a homogeneous polynomial in the c_{ij} with fixed coefficients. Hence we must have that the denominators are bounded, say by some constant B. We then have that

$$\mathcal{O}_K \subseteq \frac{1}{B} \bigoplus_{i=1}^{n} \mathbb{Z}\beta_i$$

The right hand side of this inclusion is a free Abelian group which means $\mathcal{O}_K$ must be a free Abelian group. Since $\mathcal{O}_K$ contains a set of n linearly independent elements, it must have rank n. $\square$

Definition 2.13. Let L/K be an extension of number fields and $S = \{ x_1, \dots, x_n \} \subseteq L$. We define the **discriminant** of S to be

$$\Delta_{L/K}(S) = \det \mathrm{Tr}_{L/K}(x_i x_j)$$

Proposition 2.14. *Let L/K be an extension of number fields and let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases for this extension. Suppose that $C = (c_{ij})$ is the change of basis matrix from the β-basis to the α-basis. Then*

$$\Delta_{L/K}(\alpha_1, \ldots, \alpha_n) = \det(C)^2 \Delta_{L/K}(\beta, \ldots, \beta_n)$$

Proof. We have that

$$\alpha_i \alpha_k = \sum_{j=1}^{n} \sum_{l=1}^{n} c_{ij} c_{kl} \beta_j \beta_l$$

Passing to the trace yields

$$\operatorname{Tr}_{L/K}(\alpha_i \alpha_k) = \sum_{j=1}^{n} \sum_{l=1}^{n} c_{ij} c_{kl} \operatorname{Tr}_{L/K}(\beta_j \beta_l)$$

Let $A = (\operatorname{Tr}_{L/K}(\alpha_i \alpha_j))$ and $B = \operatorname{Tr}_{L/K}(\beta_i \beta_j)$. Then the above calculations imply that $A = CBC^t$. The proposition then follows by passing to the determinant. □

Proposition 2.15. *Let L/K be an extension of number fields and let $\sigma_1, \ldots, \sigma_n$ be the distinct K-embeddings of L into an algebraic closure of K, say $\overline{K}$. If $S = \{ x_1, \ldots, x_n \} \subseteq L$ then*

$$\Delta_{L/K}(S) = [\det \sigma_i(x_j)]^2$$

Proof. By Proposition 2.7, we have

$$\operatorname{Tr}_{L/K}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i) \sigma_k(x_j)$$

If A is the matrix whose $(ij)^{th}$ entry is $\sigma_i(x_j)$ then $(\operatorname{Tr}_{L/K}(x_i x_j)) = AA^t$. The proposition then follows by passing to the determinant in the previous equation. □

Proposition 2.16. *Let L/K be an extension of number fields and let $S = \{ \alpha_1, \ldots, \alpha_n \} \subseteq L$. If $\Delta_{L/K}(S) \neq 0$ then S is linearly independent. Conversely, if $S = \{ \alpha_1, \ldots, \alpha_n \}$ is a K-basis for L then $\Delta_{L/K}(S) \neq 0$.*

Proof. First suppose that $S = \{ \alpha_1, \ldots, \alpha_n \}$ are linearly dependent. Then there exists $a_1, \ldots, a_n \in K$, not all zero, such that

$$0 = \sum_{i=1}^{n} a_i \alpha_i$$

Hence for any $1 \leq j \leq n$ we have

$$0 = \operatorname{Tr}_{L/K}(\alpha_j \sum_{i=1}^{n} a_i \alpha_i) = \sum_{i=1}^{n} a_i \operatorname{Tr}_{L/K}(\alpha_i \alpha_j)$$

Writing this as a matrix equation yields

$$(\operatorname{Tr}_{L/K}(\alpha_i \alpha_j)) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0$$

Which implies that $\Delta_{L/K}(S) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) = 0$.

Conversely, suppose that $S = \{ \alpha_1, \dots, \alpha_n \}$ is a K-basis for L and that $\Delta_{L/K}(S) = 0$. Then there exists $a_1, \dots, a_n \in K$ such that for all $1 \leq j \leq n$ we have $\sum_{i=1}^n a_i \mathrm{Tr}_{L/K}(\alpha_i\alpha_j) = 0$. Now set $\alpha = \sum_{i=1}^n a_i\alpha_i$. α is clearly non-zero since the α_i are a K-basis for L and the a_i are not all zero. Now let $\beta \in L$. We may write $\beta = \sum_{i=1}^n b_i\alpha_i$ for some $b_i \in K$. Then

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\beta\alpha) &= \mathrm{Tr}_{L/K}(\alpha \sum_{i=1}^n b_i\alpha_i) \\
&= \sum_{i=1}^n b_i \mathrm{Tr}_{L/K}(\alpha\alpha_i) \\
&= \sum_{i=1}^n b_i \mathrm{Tr}_{L/K}(\sum_{j=1}^n a_j\alpha_j\alpha_i) \\
&= \sum_{i=1}^n \sum_{j=1}^n b_i a_j \mathrm{Tr}_{L/K}(\alpha_j\alpha_i) = 0
\end{aligned}$$

In particular, we may take $\beta = \alpha^{-1}$. Then $\mathrm{Tr}_{L/K}(\beta\alpha) = \mathrm{Tr}_{L/K}(1) = 0$. This is a contradiction to the fact that the characteristic of K is zero. We must therefore have that $\Delta_{L/K}(S) \neq 0$. □

Proposition 2.17. *Let K be a number field and suppose that $L = K(\alpha)$ for some algebraic number α. Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Let $S = \{ 1, \alpha, \alpha^2, \dots, \alpha^{n-1} \}$ be the power K-basis for L. If $\alpha = \alpha_1, \dots, \alpha_n$ are the roots of $f(X)$ in an algebraic closure of K then*

$$\Delta_{L/K}(S) = \operatorname{disc} f(X) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Proof. Let $\sigma_1, \dots, \sigma_n$ be the distinct K-embeddings of L into an algebraic closure of K where $\sigma_i(\alpha) = \alpha_i$. Then for all $0 \leq j \leq n-1$ we have $\sigma_i(\alpha^j) = \alpha_i^j$. Proposition 2.7 then implies that

$$\Delta_{L/K}(S) = \left[\det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix} \right]^2$$

This matrix on the right hand side is the Vandermonde matrix whose determinant is given by $\prod_{i<j} \alpha_j - \alpha_i$. The square of this is exactly the discriminant of $f(X)$. □

Corollary 2.18. *Let K be a number field and $L = K(\alpha)$ for some algebraic number α. Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Let $S = \{ 1, \alpha, \alpha^2, \dots, \alpha^{n-1} \}$ be the power K-basis for L. Then*

$$\Delta_{L/K}(S) = (-1)^{\binom{n}{2}} \mathrm{N}_{L/K}(f'(\alpha))$$

Proof. Let $\alpha = \alpha_1, \dots, \alpha_n$ be the roots of $f(X)$ in an algebraic closure of K. Then

$$\Delta_{L/K}(S) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j)$$

Now, $f(X) = (X - x_1) \dots (X - \alpha_n)$ and thus $f'(X) = \sum_{k=1}^{n} \prod_{j \neq k} (X - \alpha_j)$. If we substitute α_i for X in $f'(X)$, only the $k = i$ term remains and we get $f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$. Hence

$$\Delta_{L/K}(S) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$$

Furthermore, if $\sigma_1, \dots, \sigma_n$ are the distinct K-embeddings of L into an algebraic closure of K, we have $f'(\alpha_i) = f'(\sigma_i(\alpha)) = \sigma_i(f'(\alpha))$. We thus obtain

$$\Delta_{L/K}(S) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} \sigma_i(f'(\alpha)) = (-1)^{\binom{n}{2}} \mathrm{N}_{L/K}(f'(\alpha))$$

□

Definition 2.19. Let K be an extension of number fields. Suppose that $\{ \alpha_1, \dots, \alpha_n \} \subseteq K$ is a $\mathbb{Q}$-basis for K. Then such a basis is an **integral basis** if

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

Remark. Theorem 2.12 guarantees the existence of an integral basis for any number field.

Lemma 2.20. *Let K be a number field. Then the discriminant of any integral basis of K is invariant under a change of basis to any other integral basis.*

Proof. Let $S = \{ \alpha_1, \dots, \alpha_n \}$ and $T = \{ \beta_1, \dots, \beta_n \}$ be integral bases for K. By Proposition 2.14, we have

$$\Delta_{K/\mathbb{Q}}(S) = \det(C)^2 \Delta_{K/\mathbb{Q}}(T)$$

where C is the change of basis matrix that sends the β-basis to the α-basis. Now, we must have that $\det C$ is a unit in $\mathbb{Z}$ meaning it is equal to ± 1. This proves the lemma. □

Definition 2.21. Let K be a number field. We define the **discriminant** of K, denoted Δ_K, to be the discriminant of any integral basis of K.

Theorem 2.22 (Stickelberger's Theorem)**.** *Let K be a number field. Then Δ_K is congruent to 0 or 1 modulo 4.*

Proof. Let $S = \{ \alpha_1, \dots, \alpha_n \}$ be an integral basis for K. Let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of K into an algebraic closure of $\mathbb{Q}$. Then

$$\Delta_K = \Delta_{L/K}(S) = [\det(\sigma_i(\alpha_j))]^2 = \left[\sum_{\pi \in S_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}) \right]^2$$

We may split the sum up into even and odd permutations as follows

$$P = \sum_{\substack{\pi \in S_n \\ \operatorname{sgn}(\pi)=1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}), \quad N = \sum_{\substack{\pi \in S_n \\ \operatorname{sgn}(\pi)=-1}} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)})$$

Now let L be a Galois extension of K. Then given any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, we have that σ permutes the embeddings σ_i. Hence we must have one of the following: $\sigma(P) = P, \sigma(N) = N$ or $\sigma(P) = N, \sigma(N) = P$. In both cases, we see that σ fixes both $P + N$ and PN. By Galois Theory, this implies that $P + N$ and PN are both rational numbers. Furthermore, it is easy to see that P and N are rational integers since the α_i are algebraic integers. Finally,

$$\Delta_K = (P - N)^2 = (P + N)^2 - 4PN$$

So we must have that $\Delta_K \equiv 0, 1 \pmod 4$. □

3 Ideal Factorisation

In this section, by integral domain, we shall mean an integral domain that is not a field.

Lemma 3.1. *Let R be a ring and $I \lhd R$ a prime ideal. Suppose that $J_1, \ldots, J_n \lhd R$ such that $J_1 \ldots J_N \subseteq I$. Then there exists at least one $1 \leq i \leq n$ such that $J_i \subseteq I$.*

Proof. Let $j = \sum_{k=1}^{m} j_{1k} \ldots j_{nk} \in J_1 \ldots J_n$ where $j_{ik} \in J_i$. By hypothesis, we have that $j \in I$. By the definition of an ideal, we have that $j_{1k} \ldots j_{nk} \in I$ for all $1 \leq k \leq m$. By the definition of a prime ideal, we must have that at least one of the $j_{ik} \in I$. But j_{ik} is an arbitrary element of J_i and thus $J_i \in I$. □

Lemma 3.2. *Let R be a Noetherian integral domain and $I \lhd R$ a non-zero ideal. Then I contains a product of non-zero prime ideals.*

Proof. Let S be the set of all non-zero ideals of R that do not contain a product of prime ideals. Since R is Noetherian, S contains a maximal element, say I. By definition, I is not prime so there must exist some $x, y \in R \backslash I$ such that $xy \in I$. Then $(x) + I$ and $(y) + I$ are not in S by the maximality of I. They thus each contain a product of prime ideals. Now, since R is an integral domain, we have that $((x) + I)((y) + I)$ is nonzero. But this ideal product is contained in I which implies that I contains a product of prime ideals - a contradiction. □

Definition 3.3. Let R be an integral domain and K its field of fractions. We define a **fractional ideal** of R to be an R-submodule of K, say M, such that $dM \subseteq A$ for some $d \in A \backslash \{ 0 \}$. Equivalently, any fractional ideal is given by

$$\frac{1}{d} I = \{ x \in K \mid dx \in I \}$$

where $I \lhd R$ is an ideal.

Remark. Henceforth, we shall refer to ordinary ideals as **integral ideals** to distinguish them from fractional ideals.

Lemma 3.4. *Let R be Noetherian. Then the fractional ideals of R are the finitely generated R-submodules of K.*

Proof. First suppose that M is a fractional ideal. Then we may write $M = 1/dI$ for some integral ideal I. Since R is Noetherian, I is finitely generated. Then M is a finitely generated R-submodule of K.

Conversely, suppose that M is a finitely generated R-submodule of K. Them $M = \langle m_1, \ldots, m_n \rangle$ for some $m_1, \ldots, m_n \in M$. Now each $m_i = 1/r_i$ for some $r_i \in R$. So we have

$$\left(\prod_{i=1}^{n} r_i \right) M \subseteq R$$

which is exactly what it means for M to be a fractional ideal of R. □

Definition 3.5. let R be a ring, L its field of fractions and M and N be fractional ideals of R. Then we define the following fractional ideals:

$$MN = \left\{ \sum_{i=1}^{k} m_i n_i \;\middle|\; m_i \in M, n_i \in N, k \in \mathbb{N} \right\}$$
$$M' = \{ x \in K \mid xM \subseteq R \}$$

Definition 3.6. Let R be an integral domain. We say that R is a **Dedekind domain** if it is Noetherian, integrally closed and every non-zero prime ideal is maximal.

Lemma 3.7. *Let R be a unique factorisation domain. Then R is integrally closed in its field of fractions K.*

Proof. Let $\alpha \in K$ be integral over R. Then α satisfies a monic polynomial

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with each $a_i \in R$. Since R is a UFD, we may write $\alpha = c/d$ with $\gcd(c,d) \in R^\times$. We then have that

$$\left(\frac{c}{d}\right)^n + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + \cdots + a_0$$

Multiplying through by d^n we have

$$c^n + dz = 0$$

for some $z \in R$. It follows that $d | c^n$. Now, if d is not a unit then $\gcd(c,d) \notin R^\times$ so we must have that d is a unit. But then $\alpha = cd^{-1} \in R$. □

Proposition 3.8. *Let R be a principal ideal domain. Then R is a Dedekind domain.*

Proof. Clearly, any PID is necessarily Noetherian. Furthermore Lemma 3.7 implies that R is integrally closed since any PID is necessarily a UFD. Finally, by a theorem of elementary ring theory, every prime ideal in a PID is maximal. Hence R is a Dedekind domain. □

Proposition 3.9. *Let R be a Dedekind domain with field of fractions K. If $\mathfrak{p}$ is a non-zero prime ideal of R then*

1. $\mathfrak{p}' \neq R$
2. $\mathfrak{p}\mathfrak{p}' \neq \mathfrak{p}$
3. $\mathfrak{p}\mathfrak{p}' = R$

Proof.

<u>Part 1:</u> Let $a \in \mathfrak{p}\backslash\{0\}$. By Lemma 3.2 we can write

$$(a) \supseteq \mathfrak{q}_1 \ldots \mathfrak{q}_n$$

for some non-zero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ and n minimal. Then by Lemma 3.1 we have that, up to renumbering, $\mathfrak{q}_1 \subseteq \mathfrak{p}$. But $\mathfrak{q}_1$ is a non-zero prime ideal and is thus maximal by hypothesis. We must then have that $\mathfrak{q}_1 = \mathfrak{p}$. Now denote $\mathfrak{b} = \mathfrak{q}_2 \ldots \mathfrak{q}_n$. Then

$$\mathfrak{p}\mathfrak{b} \subseteq (a) \subseteq \mathfrak{p}$$

Furthermore, $\mathfrak{b} \not\subseteq (a)$ by minimality of n. Hence we may choose $b \in \mathfrak{b}$ such that $b \notin (a)$. Then $b\mathfrak{p} \subseteq (a)$ whence $ba^{-1}\mathfrak{p} \subseteq R$. Hence $ba^{-1} \in \mathfrak{p}'$ but $ba^{-1} \notin R$.

<u>Part 2:</u> Suppose that $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$. Fix an $x \in \mathfrak{p}'$. Then $x^n\mathfrak{p} \subseteq \mathfrak{p}$ for all $n \in \mathbb{N}$. This implies that $R[x]$ is a fractional ideal of R. By Lemma 3.4, we know that $R[x]$ is a finitely generated R-submodule of $K = \mathrm{Frac}(R)$. Hence, x is integral over R. But R is integrally closed so we must have that $x \in R$. This implies that $\mathfrak{p}' \subseteq R$. But $\mathfrak{p}$ is an integral ideal of R so $R \subseteq \mathfrak{p}'$. Hence $R = \mathfrak{p}'$ but this contradicts Part 1.

<u>Part 3:</u> Since $\mathfrak{p}$ is an integral ideal of R, we have that $R \subseteq \mathfrak{p}'$. This implies that $\mathfrak{p} = \mathfrak{p}R \subseteq \mathfrak{p}\mathfrak{p}'$. Now, $\mathfrak{p}$ is necessarily maximum so we must have that either $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$ or $\mathfrak{p}\mathfrak{p}' = R$. The former is a contradiction to Part 2 so the latter necessarily holds.

□

Theorem 3.10. *Let R be a Dedekind domain and $I \lhd R$ a non-zero proper ideal. Then there exists distinct non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ of R and natural numbers $e_1, \dots, e_n$ all greater than or equal to 1 satisfying*

$$I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$$

The above decomposition is unique. Furthermore, we express R as the empty product.

Proof. Denote by S the set of all ideals in R that cannot be expressed as a product of prime ideals. Suppose that S is non-empty. Since R is Noetherian, there exists a maximal element of S, say $\mathfrak{b}$. By hypothesis, $\mathfrak{b} \neq R$ so there exists a maximal prime ideal $\mathfrak{p}$ such that $\mathfrak{b} \subseteq \mathfrak{p}$. By Proposition 3.9 we have $\mathfrak{b}\mathfrak{p}' \subseteq \mathfrak{p}\mathfrak{p}' = R$. Therefore, $\mathfrak{b}\mathfrak{p}'$ is an integral ideal of R. By definition, we have that $R \subseteq \mathfrak{p}'$. From this we see that $\mathfrak{b} \subseteq \mathfrak{b}\mathfrak{p}'$. Now, the same proof as for Part 2 of Proposition 3.9 implies that $\mathfrak{b} \neq \mathfrak{b}\mathfrak{p}'$ whence $\mathfrak{b}\mathfrak{p}' \notin S$. Then $\mathfrak{b}\mathfrak{p}'$ admits a factorisation into prime ideals

$$\mathfrak{b}\mathfrak{p}' = \mathfrak{q}_1 \dots \mathfrak{q}_n$$

where each $\mathfrak{q}_i$ is a non-zero prime ideal of R. Multiplying both sides by $\mathfrak{p}$ yields

$$\mathfrak{b} = \mathfrak{p}\mathfrak{q}_1 \dots \mathfrak{q}_n$$

which implies that $\mathfrak{b} \notin S$. This is a contradiction so we must have that S is empty. Thus all non-zero ideals of R admit a factorisation into prime ideals.

To prove uniqueness let $I \lhd R$ be a non-zero proper ideal and suppose that

$$I = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_m^{\alpha_m} = \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_n^{\beta_n}$$

where the $\mathfrak{p}_i$ and the $\mathfrak{q}_i$ are all non-zero prime ideals. We have that $\mathfrak{p}_1 R = \mathfrak{p}_1$. From this we see that $\mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_n^{\beta_n} = \mathfrak{p}_1{}^{\alpha_1} \dots \mathfrak{p}_m^{\alpha_m} \subseteq \mathfrak{p}_1$. By Lemma 3.1, there exists a $1 \leq j \leq n$ such that $\mathfrak{p}_1 \subseteq \mathfrak{q}_j$. But all non-zero prime ideals are maximal in R so we have that $\mathfrak{p}_1 = \mathfrak{q}_j$ and $\alpha_1 = \beta_j$. After possibly reordering, we see that

$$\mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_m^{\alpha_m} = \mathfrak{q}_2^{\beta_2} \dots \mathfrak{q}_n^{\beta_n}$$

Continuing by induction, we conclude that the factorisations must be the same with $n = m$. □

Given a number field K, $\mathcal{O}_K$ is not necessarily a UFD. Indeed, if $K = \mathbb{Q}(\sqrt{-5})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and we have that

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

are two factorisations of 6 whose factors are pairwise non-associate (they do not differ multiplicatively by a unit) irreducible elements. However, we do have unique factorisation of non-zero ideals into prime ideals in $\mathcal{O}_K$.

Proposition 3.11. *Let K be a number field. Then $\mathcal{O}_K$ is Noetherian.*

Proof. By Theorem 2.12, $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module. Since $\mathbb{Z}$ is Noetherian, each $\mathbb{Z}$-submodule of $\mathcal{O}_K$ is also finitely generated. In particular, any integral ideal of $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of $\mathcal{O}_K$ so the integral ideals are finitely generated. Hence $\mathcal{O}_K$ is Noetherian. □

Proposition 3.12. *Let K be a number field of degree n. Let $\mathfrak{a} \lhd \mathcal{O}_K$ be a non-zero ideal. Then $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Proof. We first prove that $\mathfrak{a} \cap \mathbb{Z} \neq \{ 0 \}$ and is non-empty. To this end, let $\alpha \in \mathfrak{a}$. Let $f(X) = X^m + \cdots + a_0 \in \mathbb{Z}[X]$ be its minimal polynomial. Clearly, $a_0 \neq 0$ since otherwise, $f(X)$ would be reducible. We then have that

$$a_0 = -(\alpha^m + \cdots + a_1\alpha) \in \mathfrak{a} \cap \mathbb{Z}$$

Now choose a non-zero $d \in \mathfrak{a} \cap \mathbb{Z}$. By an isomorphism theorem, we have

$$\frac{\mathcal{O}_K/(d)}{\mathfrak{a}/(d)} \cong \mathcal{O}_K/\mathfrak{a}$$

Now, Theorem 2.12 implies that $\mathcal{O}_K \cong \mathbb{Z}^n$ and thus $\mathcal{O}_K/(d) \cong (\mathbb{Z}/(d))^n$ which is finite. Hence $\mathcal{O}_K/\mathfrak{a}$ is finite. □

Corollary 3.13. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Proposition 3.11 implies that $\mathcal{O}_K$ is Noetherian. $\mathcal{O}_K$ is integrally closed by definition so it remains to show that every non-zero prime ideal is maximal in $\mathcal{O}_K$. To this end, let $\mathfrak{p} \lhd \mathcal{O}_K$ be a non-zero prime ideal. Then the quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain. But any finite integral domain is necessarily a field and thus $\mathfrak{p}$ must be maximal. □

Definition 3.14. Let K be a number field and $\mathfrak{a} \lhd \mathcal{O}_K$. We define the **norm** of $\mathfrak{a}$ to be

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$$

Proposition 3.15. *Let K be a number field and $\mathfrak{a} \lhd \mathcal{O}_K$ a non-zero ideal. Let $\alpha_1, \dots, \alpha_n$ be an integral basis for K and $\beta_1, \dots, \beta_n$ a $\mathbb{Z}$-basis for $\mathfrak{a}$. If T is the matrix such that*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = T \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Then $N(\mathfrak{a}) = |\det T|$.

Proof. By the structure theorem for finitely generated modules over a Euclidean domain, we can write $\beta_i = a_i\alpha_i$ for all $1 \leq i \leq n$ and some $a_i \in \mathbb{Z}$. Then the diagonal of T consists of the a_i and the rest of the entries are zero. We have that

$$\begin{aligned} |\mathcal{O}_K/\mathfrak{a}| &= |(\mathbb{Z}/(\alpha_1) \oplus \cdots \oplus \mathbb{Z}/(\alpha_n))/(\mathbb{Z}/(a_1\alpha_1) \oplus \cdots \oplus \mathbb{Z}/(a_n\alpha_n))| \\ &= |\mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)| \\ &= |a_1 \dots a_n| \\ &= |\det T| \end{aligned}$$

□

Corollary 3.16. *Let K be a number field of degree n and $\alpha_1, \dots, \alpha_n$ generators for some ideal $I \lhd \mathcal{O}_K$ as a $\mathbb{Z}$-module. Then*

$$\Delta_{K/\mathbb{Q}}(\{ \alpha_1, \dots, \alpha_n \}) = N(I)^2 \Delta_K$$

Proof. This follows directly from Proposition 2.14 and Proposition 3.15. □

Proposition 3.17. *Let K be a number field of degree n and $(a) \lhd \mathcal{O}_K$ a principal ideal for some non-zero generator $a \in \mathcal{O}_K$. Then*

$$N((a)) = |\,\mathrm{N}_{K/\mathbb{Q}}(a)|$$

Remark. The above norm is multiplicative. The proof of this fact is omitted.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for K. Let $\beta_i = \alpha x_i$. Then

$$\begin{aligned}\Delta_{K/\mathbb{Q}}(\{\,\beta_1, \ldots, \beta_n\,\}) &= \det(\sigma_i(\alpha x_i))^2 \\ &= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^2 \Delta_K \\ &= (\mathrm{N}_{K/\mathbb{Q}}(\alpha))^2 \Delta_K\end{aligned}$$

The proposition then follows by comparing to the result in Corollary 3.16. □

Example 3.18. Let d be a square-free integer satisfying $d \equiv 0 \pmod 3$ and $d \not\equiv \pm 1 \pmod 9$. Let $K = \mathbb{Q}(d^{1/3})$. We claim that $\mathcal{O}_K = \mathbb{Z}[d^{1/3}]$. Let $\theta = d^{1/3}$. The minimal polynomial of θ over $\mathbb{Q}$ is $f(X) = X^3 - d$. Since $\mathrm{disc}(f(x)) = -27d^2$ we have

$$-27d^2 = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 \Delta_K$$

where Δ_K is the discriminant of the number field K[1]. So the only primes dividing the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ are either 3 or a divisor of d. Let p be such a prime. Recall that the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ represents the number of elements in the quotient group $\mathcal{O}_K/\mathbb{Z}[\theta]$. Hence if p is the number of elements of $\mathcal{O}_K/\mathbb{Z}[\theta]$ then there must exist an element $y \neq 0 + \mathbb{Z}[\theta]$ such that $py = 0 + \mathbb{Z}[\theta]$. This is equivalent to there existing non-zero $x \in \mathbb{Z}[\theta]$ such that $x/p \in \mathcal{O}_K$ but $x/p \notin \mathbb{Z}[\theta]$.

Let

$$z = \frac{x}{p} = \frac{A + B\theta + C\theta^2}{p}$$

be such an element of $\mathcal{O}_K$ for some $A, B, C \in \mathbb{Z}$. If ω is a primitive cube root of unity then the other conjugates of $z = z_1$ are given by

$$\begin{aligned}z_2 &= \frac{A + B\omega\theta + C\omega^2\theta^2}{p} \\ z_3 &= \frac{A + B\omega^2\theta + C\omega\theta^2}{p}\end{aligned}$$

We can then calculate the coefficients e_i of the minimal polynomial of z in terms of symmetric polynomials:

$$\begin{aligned}e_0 &= \frac{A^3 + dB^3 + d^2C^3 - 3ABCd}{p^3} \\ e_1 &= \frac{3A^2 - 3BCd}{p^2} \\ e_2 &= \frac{3A}{p}\end{aligned}$$

[1]the discriminant of a cubic polynomial of the form $X^3 + aX + b$ is given by $-4a^3 - 27b^2$

where we have used the fact that $1+\omega+\omega^2=0$. Now since $z \in \mathcal{O}_K$, we must have that $e_1, e_2, e_3 \in \mathbb{Z}$. First assume that $p \neq 3$. Then since $e_2 \in \mathbb{Z}$, we must have that $p|A$. We can add integer multiples of $1, \theta, \theta^2$ to A, B, C without changing the fact that the $e_i \in \mathbb{Z}$. Hence without loss of generality, we may assume that $0 \leq A \leq B \leq Cp-1$. It then follows that $A = 0$. Since $e_1 \in \mathbb{Z}$, we have that $p^2|BCd$. But d is square free so we must have that $p|BC$. If $B = 0$ then, since $e_0 \in \mathbb{Z}$ we have $p^3|d^2C^3$. This implies that $p|C^3$ whence $C = 0$. Conversely, if $C = 0$ then $p^3|dB^3$ whence $B = 0$. Hence in the case $p \neq 3$ we have that $z = 0$ and thus $x = 0$. But this a contradiction.

Hence assume $p = 3$. We may assume, without loss of generality, that $A, B, C = 0$ or ± 1. If $A = 0$ then $3|BCd$. But d is not divisible by 3 so $3|BC$ so either $B = 0$ or $C = 0$. Suppose that $B = 0$. Then $27|d^2C^3$ whence $3|C$ and so $C = 0$. Similarly, if $C = 0$ then $B = 0$. This is again a contradiction.

So, finally, assume that $A = \pm 1$. Without loss of generality, suppose that $A = 1$. Then $BCd \equiv 1 \pmod 3$ and $27|(1 + B^3d + C^3d^2 - 3BCd)$. So $B, C \neq 0$. We have four cases:

$\underline{B = C = 1}$: In this case we have $27|(1 + d + d^2 - 3d)$ and so $(d-1)^2 \equiv 0 \pmod{27}$. But then $d - 1 \equiv 0 \pmod 9$ which is a contradiction to the assumption that $d \not\equiv 1 \pmod 9$.

$\underline{B = 1, C = -1}$: In this case we have $27|(1 + d - d^2 + 3d)$ and so $d^2 - 4d - 1 \equiv 0 \pmod 3$. But $d \equiv 1, 2 \pmod 3$ which is a contradiction.

$\underline{B = -1, C = 1}$: In this case we have $27|(1 - d + d^2 + 3d)$ which is a contradiction to the assumption $d \not\equiv 1 \pmod 9$.

$\underline{B = -1, C = -1}$: In this case we have $27|(1 - d - d^2 - 3d)$ which is again a contradiction modulo 3.

We see that in all cases, there does not exist a prime dividing $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ and so $\mathcal{O}_K = \mathbb{Z}[\theta]$ as required.

Lemma 3.19. *Let K be a number field and I a non-zero fractional ideal of $\mathcal{O}_K$. Then $II' = \mathcal{O}_K$.*

Proof. First suppose that I is an integral ideal. If $I = \mathcal{O}_K$ then, clearly, $I' = \mathcal{O}_K$ and we are done. Hence assume that I is a proper ideal of $\mathcal{O}_K$. Then we can write

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

for some non-zero prime ideals $\mathfrak{p}_i \triangleleft \mathcal{O}_K$. By Proposition 3.9 we know that $\mathfrak{p}_i\mathfrak{p}_i' = \mathcal{O}_K$. We then have that

$$\begin{aligned} x \in I' \iff x \in xI \subseteq \mathcal{O}_K &\iff (x)\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathcal{O}_K \\ &\iff (x)\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1' \\ &\vdots \\ &\iff (x) \subseteq \mathfrak{p}_1' \cdots \mathfrak{p}_r' \\ &\iff x \in \mathfrak{p}_1' \cdots \mathfrak{p}_r' \end{aligned}$$

It then follows that $II' = \mathcal{O}_K$ and we are done for the case where I is a non-zero integral ideal.

Now suppose that I is a non-zero fractional ideal. Then we may write $I = (1/d)J$ for some non-zero integral ideal J. From the previous case, we know that J has an inverse, say J^{-1}. It then follows that $I^{-1} = dJ^{-1}$ is an inverse for I. Indeed, $II^{-1} = (1/d)JdJ^{-1} = \mathcal{O}_K$. □

Henceforth, given any fractional ideal I, we shall write I' as I^{-1}.

Corollary 3.20. *Let K be a number field. Denote by J_K the set of all non-zero fractional ideals of $\mathcal{O}_K$. Then J_K is an abelian group under multiplication of ideals.*

Definition 3.21. Let K be a number field and let P_K be the (normal) subgroup of I_K containing all principal fractional ideals of $\mathcal{O}_K$. Then we define the group $\mathrm{Cl}(\mathcal{O}_K) = I_K/P_K$ to be the **ideal class group** of K. We call the cardinality of I_K/P_K the **class number** of K and we denote it by h_K.

We will soon prove that the class group is finite.

Proposition 3.22. *Let R be a Dedekind domain. Then R is a unique factorisation domain if and only if it is a principal ideal domain.*

Proof. We know from elementary ring theory that any PID is necessarily a UFD.

Conversely, assume that R is a UFD. We first claim that all prime ideals of R are principal. To this end, let $\mathfrak{p} \triangleleft R$ be a prime ideal. If $\mathfrak{p}$ is the zero ideal then it is clearly principal so we may assume that $\mathfrak{p}$ is non-zero. Let $x \in \mathfrak{p}$ be non-zero. Since R is a UFD, we can write x as a product of primes $x = p_1 \cdots p_r$ for some $p_i \in R$. Now $\mathfrak{p}$ is prime which implies that at least one of the $p_i \in \mathfrak{p}$. Let $p = p_i$. Since R is Dedekind, the ideal $(p) \triangleleft R$ is maximal which means we must have $\mathfrak{p} = (p)$. This proves the claim.

Now let $I \triangleleft R$ be an arbitrary ideal of R. Given $x \in I$, let $l(x)$ denote the number of primes in the prime decomposition of x. Choose $x \in I$ such that $l(x)$ is minimal. We claim that x is a generator of I. Indeed, suppose that $y \in I$ such that x does not divide y. Let z be the greatest common divisor of x and y. Clearly, $l(z) < l(x)$. We may write $x = za$ and $y = zb$ for some coprime a, b. We now claim that $(a, b) = R$. Indeed, consider the collection

$$\{\, J \triangleleft R \mid J \subseteq (a, b) \,\}$$

Since R is Noetherian, this collection of ideals contains a maximal element, say $\mathfrak{m}$. Since any maximal ideal is a prime ideal, there must exist a prime $p \in R$ such that $\mathfrak{m} = (p) \subseteq (a, b)$. But then p divides both a and b which contradicts the fact that they are coprime. Hence $R = (a, b)$. Thus $1 \in (a, b)$ and there exist elements $x_0, y_0 \in R$ such that $x_0 a + y_0 b = 1$. This implies that $z = x_0 x + y_0 y$, contradicting the fact that $l(z) < l(x)$. We must therefore have that x divides all $y \in I$ and we are done. □

Proposition 3.23. *Let K be a number field. Then $\mathcal{O}_K$ is a principal ideal domain if and only if* $\mathrm{Cl}(\mathcal{O}_K) = \{\, 0 \,\}$.

Proof. Suppose that $\mathcal{O}_K$ is a principal ideal domain and let I be a fractional ideal of $\mathcal{O}_K$. Then we can write $I = (1/d)J$ for some $d \in \mathcal{O}_K$ and integral ideal $J \triangleleft \mathcal{O}_K$. Since $\mathcal{O}_K$ is a PID we have that $J = (a)$ for some $a \in \mathcal{O}_K$. Then $J = (a/d)$ and is thus principal.

Conversely, suppose that $\mathrm{Cl}(\mathcal{O}_K) = \{\, 0 \,\}$. Then every fractional ideal of $\mathcal{O}_K$ is principal. In particular, every integral ideal of $\mathcal{O}_K$ is principal and we are done. □

It follows that, given a number field K, $\mathcal{O}_K$ is a unique factorisation domain if and only if it is a principal ideal domain. This is in turn equivalent to the ideal class group being trivial. We thus see that the class group is a measure of the failure of a ring of integers to be a unique factorisation domain.

Theorem 3.24 (Dedekind's Theorem)**.** *Let K be a number field and suppose that $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Suppose furthermore that there exists a prime p that does not divide*

$[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. *Let* $f(X)$ *be the minimal polynomial of* α *over* $\mathbb{Q}$ *and let* $\overline{f}(X) \in \mathbb{F}_p[X]$ *be its reduction modulo* p. *Suppose that*

$$\overline{f} = g_1^{e_1} \cdots g_r^{e_r}$$

is the factorisation of $\overline{f}$ *into irreducibles in* $\mathbb{F}_p[X]$. *For each* $1 \leq i \leq r$, *let* h_i *be such that*

1. $h_i \equiv g_i \pmod{p}$
2. $\mathfrak{p}_i = (p, h_i(\alpha))\mathcal{O}_K$

Then

1. $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *are the distinct prime ideals of* $\mathcal{O}_K$ *that contain* p
2. $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ *is the prime ideal factorisation in* $\mathcal{O}_K$
3. $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p] = \deg(g_i)$

Example 3.25. Consider $K = \mathbb{Q}(\sqrt{-5})$. Since $-5 \equiv 3 \pmod{4}$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then neither 2 nor 3 divide $[\mathcal{O}_K : \mathbb{Z}[\sqrt{-5}]$ so we can apply Dedekind's Theorem to investigate how $2\mathcal{O}_K$ and $3\mathcal{O}_K$ factorise. $X^2 + 5$ is the minimal polynomial of $\sqrt{-5}$ over $\mathbb{Q}$. We first consider $p = 2$. We have

$$\begin{aligned} X^2 + 5 &\equiv X^2 + 1 \pmod{2} \\ &= (X+1)^2 \end{aligned}$$

Writing $\mathfrak{p} = (2, 1 + \sqrt{-5})\mathcal{O}_K$ it follows that $2\mathcal{O}_K = \mathfrak{p}^2$. Now for $p = 3$ we have

$$X^2 + 5 \equiv X^2 + 2 \pmod{3} \qquad = (X+1)(X-1)$$

Writing $\mathfrak{q} = (3, 1 + \sqrt{-5})\mathcal{O}_K$ and $\overline{\mathfrak{q}} = (3, 1 - \sqrt{-5})\mathcal{O}_K$ we have that $3\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}}$.

Now, by Dedekind's Theorem, we have that $N(\mathfrak{p}) = 2$ and $N(\mathfrak{q}) = N(\overline{\mathfrak{q}})$. Indeed, in the $p = 2$ case for example, we have $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_2] = \deg(X+1) = 1$. It then follows that $\mathfrak{p}, \mathfrak{q}, \overline{\mathfrak{q}}$ are all distinct prime ideals. We have the following calculation for the norm of $(1 + \sqrt{-5})\mathcal{O}_K$:

$$N((1 + \sqrt{-5})) = |\,\mathrm{N}_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(1 + \sqrt{5})| = 6$$

Furthermore, $N(\mathfrak{p}\mathfrak{q}) = N(\mathfrak{p})N(\mathfrak{q})$. Observe that

$$1 + \sqrt{-5} = 3(1 + \sqrt{-5}) - 2(1 + \sqrt{-5}) \in \mathfrak{p}\mathfrak{q}$$

It then follows that $(1+\sqrt{-5})\mathcal{O}_K \subseteq \mathfrak{p}\mathfrak{q}$. But these two ideals have the same norm so we must have that $(1+\sqrt{-5})\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$. By a similar argumentation, we have that $(1-\sqrt{-5})\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{q}}$.

We therefore have that the non-unique factorisation of elements of $\mathcal{O}_K$

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

becomes a unique factorisation of ideals of $\mathcal{O}_K$

$$\mathfrak{p}^2\mathfrak{q}\overline{\mathfrak{q}} = 6\mathcal{O}_K = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}\overline{\mathfrak{q}})$$

4 Valuation Rings and Localisation

Definition 4.1. Let R be an integral domain and $K = \mathrm{Frac}(R)$. A **valuation** of R (or K) is a map

$$v : \mathbb{K} \setminus \{ 0 \} \to \mathbb{Z}$$

such that, for all $a, b \in K$,

1. $v(ab) = v(a) + v(b)$
2. $v(a + b) \geq v(a) + v(b)$ with equality if and only if $v(a) \neq v(b)$

Example 4.2. Let $R = \mathbb{Z}$ and fix a prime p in R. If $a/b \in \mathbb{Q}$ is non-zero we can always write $a/b = p^\alpha c/d$ for some c, d coprime to p. We define the **p-adic valuation** to be

$$v_p(a/b) = \alpha$$

It is readily verified that this is a valuation of $\mathbb{Z}$.

Proposition 4.3. *Let K be a field and v a non-trivial valuation of K. Then*

1. *The set given by*

$$\mathcal{O}_v = \{ x \in K \setminus \{ 0 \} \mid v(x) \geq 0 \} \cup \{ 0 \}$$

is a ring called the ***valuation ring*** *of K.*

2. $\mathrm{Frac}(\mathcal{O}_K) = K$.
3. *$\mathcal{O}_v$ is a local ring[2] with maximal ideal*

$$\mathfrak{m}_v = \{ x \in K \setminus \{ 0 \} \mid v(x) > 0 \} \cup \{ 0 \}$$

4. *$\mathfrak{m}_v$ is a principal ideal whose generator is any element whose valuation is minimal - such a generator is called a* ***uniformiser*** *for $\mathcal{O}_v$.*
5. *Every non-zero ideal $I \lhd \mathcal{O}_v$ is a power of $\mathfrak{m}$. In particular, $\mathcal{O}_v$ is a principal ideal domain.*
6. *$\mathcal{O}_v$ is a Euclidean domain with Euclidean function v.*

Proof.

Part 1: We first show that $\mathcal{O}_v$ contains the identities. It clearly contains 0 by definition. We have $v(1) = v(1 \cdot 1) = v(1) + v(1) = 2v(1)$ so necessarily $v(1) = 0$ and thus $1 \in \mathcal{O}_v$. Furthermore, $v(-1) + v(-1) = v(-1 \cdot -1) = v(1) = 0$ so also $v(-1) = 0$ and so $-1 \in \mathcal{O}_v$ - this guarantees the existence of additive inverses.

[2] recall that a local ring is one that has a unique maximal ideal (sometimes the Noetherian property is also required but we shall be explicit when this is the case)

Now suppose $a, b \in \mathcal{O}_v$. Then $v(ab) = v(a) + v(b) \geq 0$ so $ab \in \mathcal{O}_v$. Finally, $v(a-b) \geq v(a) + v(-b) = v(a) + v(-1) + v(b) \geq 0$ so $a - b \in \mathcal{O}_v$. Hence $\mathcal{O}_v$ is a ring.

Part 2: It suffices to prove that for any $x \in K$ then either $x \in \mathcal{O}_K$ or $x^{-1} \in \mathcal{O}_K$. But this is clear since either $v(x) \geq 0$ or $v(x) < 0$. Indeed, in the latter case we have $v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$ and so $v(x^{-1}) = -v(x)$ whence $v(x^{-1}) \geq 0$.

Part 3: It is clear that $\mathfrak{m}_v$ is an ideal of $\mathcal{O}_v$. To show that it is the unique maximal ideal, it suffices to show that any element in $\mathcal{O}_v \backslash \mathfrak{m}_v$ is a unit. Let x be such an element. Then $v(x) = 0$. We have $v(x^{-1}) = -v(x)$ and thus $v(x^{-1}) = 0$ whence $x^{-1} \in \mathcal{O}_v \backslash \mathfrak{m}_v$ as required.

Part 4: Let $x \in \mathfrak{m}_v$ be of minimal valuation. We claim that $\mathfrak{m}_v = (x)$. Indeed, let $y \in \mathfrak{m}_v$. We need to show that $y = rx$ for some $r \in \mathcal{O}_v$. This is equivalent to showing that $yx^{-1} = r$ for some $r \in \mathcal{O}_v$. We have that

$$v(yx^{-1}) = v(y) + v(x^{-1}) = v(y) - v(x)$$

Now, by assumption, $v(y) \geq v(x)$ and so $v(y) - v(x) \geq 0$ which means that $yx^{-1} \in \mathcal{O}_v$ as required.

Part 5: Let π be a uniformiser for $\mathcal{O}_v$. Since v is a group homomorphism between $K^\times$ and $\mathbb{Z}$, it follows that $\mathrm{im}(v) = v(\pi)\mathbb{Z}$. Hence $v(\pi)$ divides $v(r)$ for all $r \in \mathcal{O}_z$. Let $r \in \mathfrak{m}_v$ be non-zero. Then $v(r) = v(\pi)k$ for some positive $k \in \mathbb{Z}$. It follows that $v(\pi^{-k}r) = kv(\pi) + v(r) = 0$. Hence $\pi^{-k}r$ is a unit of $\mathcal{O}_K$ and thus $r = \pi^k u$ for some unit $u \in \mathcal{O}_v$.

Now let $I \lhd \mathcal{O}_v$ be a non-zero ideal. By a similar argument for $\mathfrak{m}_v$, there exists an $r_0 \in I$ such that $I = (r_0)$. But we can always write $r_0 = \pi^k u$ for some integer k and unit $u \in \mathcal{O}_K$. Hence $I = (r_0) = (\pi^k u) = (\pi^k) = (\pi)^k = \mathfrak{m}_v^k$. It then follows that $\mathcal{O}_v$ is a principal ideal domain.

Part 6: We claim that $N : \mathcal{O}_v \to \mathbb{Z}_{\geq 0}$ given by $N(0) = 0$ and $N(r) = v(r)$ for non-zero $r \in \mathcal{O}_v$ is a Euclidean function for $\mathcal{O}_v$.

We need to show that for all non-zero $a, b \in \mathcal{O}_v$, there exists $q, r \in \mathcal{O}_v$ such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

Suppose first that $v(a) \geq v(b)$. Then $v(a/b) = v(a) - v(b) \geq 0$ so $q = a/b \in \mathcal{O}_v$ and $r = 0$. Now suppose that $v(a) < v(b)$. In this case, we can just let $q = 0$ and $r = a$.

□

Example 4.4. Consider the p-adic valuation v_p on $\mathbb{Q}$ as defined before. Then

$$\mathcal{O}_{v_p} = \left\{ p^n \frac{a}{b} \;\middle|\; n \geq 0, a, b \in \mathbb{Z} \text{ and } a, b \text{ coprime to } p \right\}$$

Example 4.5. Let K be a nunber field and fix a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$. Let $f \in K^\times$. Then we can write

$$(f) = P_1^{e_1} \cdots P_r^{e^r}$$

for some prime ideals $P_i \lhd \mathcal{O}_K$ and integers e_i. We can define the $\mathfrak{p}$-adic valuation of f to be the power of $\mathfrak{p}$ in the prime ideal factorisation of (f).

Definition 4.6. Let R be a ring and $S \subseteq R$ a subset. We say that S is **multiplicative** if $1 \in S$ and $s, t \in S$ implies that $st \in S$.

Example 4.7. If R is an integral domain then $R \backslash \{ 0 \}$ is a multiplicative subset of R.

Example 4.8. If R is an integral domain and $P \lhd R$ is a prime ideal then $S = R \backslash P$ is a multiplicative subset of R.

Definition 4.9. Let R be a ring and $S \subseteq R$ a multiplicative subset. Define an equivalence relation on $S \times R$ where $(s, r) \sim (s', a')$ if and only if there exists $s'' \in S$ such that $s''(as' - a's) = 0$. We define the **localisation** (or **ring of fractions**)of R with respect to S, denoted $S^{-1}R$ to be the set of all equivalence classes of this relation. We denote the equivalence class of (s, a) by a/s. This set forms a ring with addition given by

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss}$$

and multiplication given by

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

$1/1$ is the multiplicative identity and $0/1$ is the additive identity.

Example 4.10. Let R be an integral domain and $S = \{ 0 \}$ the multiplcative subset of R consisting of only zero. Then $S^{-1}R = \mathrm{Frac}(R)$

Example 4.11. Let R be an integral domain and $r \in R$. Consider the set $S = \{ 1, r, r^2, \ldots \}$. Then S is a multiplicative subset of R and $S^{-1}R$ is called the localisation of R at the element r.

Example 4.12. Let R be an integral domain and $\mathfrak{p} \lhd R$ a prime ideal. Then $S = R \backslash \mathfrak{p}$ is multiplicative and $S^{-1}R$ is called the localisation of R at the prime ideal $\mathfrak{p}$. This is sometimes denoted $R_{\mathfrak{p}}$.

Here we give a survey of some interesting results pertaining to DVRs and localisation.

Proposition 4.13. *Let R be a ring and $S \subseteq R$ a multiplicative subset. If $I \lhd R$ is an ideal then $S^{-1}I = \{ a/s \mid a \in I, s \in S \}$ is an ideal of $S^{-1}R$.*

Proposition 4.14. *Let R be a ring and $S \subseteq R$ a multiplicative subset. Then there is a one-to-one correspondence between the prime ideals $Q \lhd R$ that are disjoint from S and the prime ideals of $S^{-1}R$ given by $Q \mapsto S^{-1}Q$.*

Example 4.15. Let R be an integral domain and $\mathfrak{p}$ a prime ideal. Let $R_{\mathfrak{p}}$ be the corresponding localisation. Then there is a one-to-one correspondence between the prime ideals Q such that $Q \subseteq \mathfrak{p}$ and the prime ideals of $R_{\mathfrak{p}}$.

Theorem 4.16. *Let R be an integrally closed Noetherian local integral domain that is not a field. Let $\mathfrak{m} \lhd R$ be its unique maximal ideal. Then R is a discrete valuation ring.*

Corollary 4.17. *Let R be a Noetherian integral domain in which every non-zero prime ideal is maximal. Then R is a Dedekind domain if and only if every localisation of R is a discrete valuation ring.*

Lemma 4.18. *Let R be a Noetherian integral domain. Then R is integrally closed if and only if every localisation of R is integrally closed.*

Proposition 4.19. *let R be a Dedekind domain and $I \lhd R$ a non-zero ideal. Let $I = P_1^{e_1} \cdots P_r^{e_r}$ be its unique factorisation into prime ideals. Then*

$$R/I \cong (R/P_1^{e_1}) \oplus \cdots \oplus (R/P_r^{e_r})$$

Furthermore, $R/P^i \cong R_P/(PR_p)^i$ is a discrete valuation ring.

5 Geometry of Numbers

Definition 5.1. Let V be an n-dimensional vector space over $\mathbb{R}$. We say that a subset $X \subseteq V$ is **compact** if it is both closed and bounded.

Definition 5.2. Let V be an n-dimensional vector space over $\mathbb{R}$. Let $\Lambda \subseteq V$ be a subgroup. We say that V is **discrete** if for every compact subset $X \subseteq V$ we have $|X \cap \Lambda| < \infty$.

Theorem 5.3. *Let V be an n-dimensional vector space over $\mathbb{R}$. Let $\Lambda \subseteq V$ be a subgroup. Then the following are equivalent:*

1. *Λ is discrete*
2. *Λ is a finitely generated $\mathbb{Z}$-module and some generating set is linearly independent over $\mathbb{R}$.*
3. *Λ is a finitely generated $\mathbb{Z}$-module and every $\mathbb{Z}$-basis of Λ is linearly independent over $\mathbb{R}$.*

Proof. We shall prove the theorem in the order (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).

(1) $\implies$ (2): Assume that Λ is discrete. Let $e_1, \ldots, e_r \in \Lambda$ be linearly independent over $\mathbb{R}$ with r maximal. Since V is n-dimensional, we have $r \leq n$. Let

$$P = \left\{ \sum_{i=1}^{r} a_i e_i \;\middle|\; a_i \in [0,1] \right\}$$

be the parallelotope generated by the e_i. Cleary, P is closed and bounded and is thus compact. Since Λ is discrete, $P \cap \Lambda$ is finite.

Fix some $x \in \Lambda$. Since r is maximal, there exist some $b_i \in \mathbb{R}$ such that $x = \sum_{i=1}^{r} b_i e_i$. Given any real number $c \in \mathbb{R}$, we can always write $c = [c] + \{c\}$ where $[c]$ is its integral part and $\{c\}$ is its fractional part. It follows that for all i we have $b_i = [b_i] + a_i$ where $a_i = \{b_i\} \in [0,1)$. Write $\lambda = \sum_{i=1}^{r} [b_i] e_i$ and $p = \sum_{i=1}^{r} a_i e_i$ so that $x = \lambda + p$. Since Λ is a group, we have that $\lambda \in \Lambda$. Furthermore, it is clear that $p \in P$. Now, $p = x - \lambda \in \Lambda$ and so $p \in P \cap \Lambda$. It thus follows that Λ is finitely generated as a $\mathbb{Z}$-module by $\{ e_1, \ldots, e_r \} \cup (P \cap \Lambda) = P \cap \lambda$.

Now let $m = |P \cap \Lambda|$. Let $j \in \mathbb{Z}$ and define $x_j = jx - \sum_{i=1}^{r} [jb_i] e_i$. Clearly, $x_j \in \Lambda$. Also, $x_j = \sum_{i=1}^{r} (jb_i - [jb_i]) e_i$ and so $x_j \in P$. It thus follows that $x_j \in \Lambda \cap P$. By the pigeonhole principle, we must have that $x_j = x_k$ for some $j \neq k$ and both j, k between 1 and $m+1$. This means that jb_i and kb_i have the same fractional part. Hence

$$(j-k) b_i = [jbi] - [kb_i] \in \mathbb{Z}$$

Hence $b_i = B_i / m!$ for some $B_i \in \mathbb{Z}$. Indeed, $1 \leq j - k \leq m$ so $j - k$ must divide $m!$. We may thus write

$$x = \sum_{i=1}^{r} b_i e_i = \sum_{i=1}^{r} \frac{B_i}{m!} e_i$$

whence Λ is a finitely generated $\mathbb{Z}$-submodule of the $\mathbb{Z}$-module, say M, generated by the $e_i / m!$.

By the structure theorem for finitely generated modules over a Euclidean domain, there exist a $\mathbb{Z}$-basis $\{ g_1, \ldots, g_r \}$ for M and integers $n_1, \ldots, n_r$ such that $n_1 g_1, \ldots, n_r g_r$ is a $\mathbb{Z}$-basis for Λ (after possibly removing the $n_i g_i$ that are zero). Now, the change of basis matrix between the $e_i/m!$ and the g_i is invertible and, since the e_i are linearly independent over $\mathbb{R}$, we must have that the g_i are linearly independent over $\mathbb{R}$ whence the $n_i g_i$ are linearly independent over $\mathbb{R}$.

(2) $\implies$ (3): Assume that Λ is a finitely generated $\mathbb{Z}$-module and that some generating set is linearly independent over $\mathbb{R}$. Let $g_1, \ldots, g_r$ be such a linearly independent generating set. Trivially, the g_i are linearly independent over $\mathbb{Z}$ and so form a $\mathbb{Z}$-basis for Λ.

Let $h_1, \ldots, h_s$ be another $\mathbb{Z}$-basis for Λ. Clearly we must have that $r = s$. We can then write

$$g_i = \sum_{j=1}^{r} m_{ij} h_j$$

for some $m_{ij} \in \mathbb{Z}$. This then implies that the h_i must be linearly independent over $\mathbb{R}$.

(3) $\implies$ (1): Suppose that Λ is a finitely generated $\mathbb{Z}$-module and every $\mathbb{Z}$-basis of Λ is linearly independent over $\mathbb{R}$. Let $e_1, \ldots, e_r$ be a $\mathbb{Z}$-basis for Λ. By assumption, the e_i are linearly independent over $\mathbb{R}$ so we may extend the e_i to a $\mathbb{R}$ basis of V, say $e_1, \ldots, e_n$. Let $f_1, \ldots, f_n$ denote the standard basis of V. Then there is a linear map

$$\begin{aligned} L : V &\to V \\ e_i &\mapsto f_i \end{aligned}$$

This is clearly continuous with continuous inverse and is thus a homeomorphism of ths standard topology on V. L thus preserves compactness. If $X \subseteq V$ is compact then $L(X) \subseteq V$ is compact aand there must exist a ball $B \subseteq V$ centered at 0 which contains $L(X)$ and is closed and bounded. Let such a ball have radius R. It is easy to see that $L(\Lambda) \cap B$ is finite. Indeed, $L(\Lambda)$ is the $\mathbb{Z}$-span of $f_1, \ldots, f_r$ and thus

$$L(\Lambda) \cap B = \left\{ \sum_{i=1}^{r} m_i f_i \;\middle|\; m_i \in \mathbb{Z}, \sum_{i=1}^{r} m_i^2 \leq R^2 \right\}$$

But there are only finitely many such integer vectors so $L(\Lambda) \cap B$ must be finite. Applying the inverse of L we see that $\Lambda \cap L^{-1}(B)$ is finite. Now, $X \subseteq L^{-1}(B)$ so $\Lambda \cap X$ is finite. Since X was an arbitrary compact subset of V, Λ must be discrete.

$\square$

Definition 5.4. Let V be an n-dimensional vector space over $\mathbb{R}$ and $\Lambda \subseteq V$ a subgroup. We say that Λ is a **lattice** if it is discrete and has rank n.

Definition 5.5. Let V be an n-dimensional vector space over $\mathbb{R}$ and $\Lambda \subseteq V$ a lattice. If $e_1, \ldots, e_n$ is a $\mathbb{Z}$-basis for Λ, we define the **e-parallelotope**[3] of Λ to be the set

$$E = \left\{ \sum_{i=1}^{n} a_i e_i \;\middle|\; a_i \in [0, 1] \right\}$$

Its volume, denoted vol(E) is given by the absolute value of the determinant of the matrix whose columns are the e_i.

Lemma 5.6. *Let V be an n-dimensional vector space over $\mathbb{R}$ and $\Lambda \subseteq V$ a lattice. Let $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ be two $\mathbb{Z}$-bases for Λ. Then the volume of the e-parallelotope is equal to the volume of the f-parallelotope.*

[3] note: this is not conventional notation!

Proof. Dnote by E and F the e-parallelotope and f-parallelotope respectively. We may write $f_j = \sum_{k=1}^{n} n_{jk} e_k$ for some integers n_{jk}. Let $N = (n_{jk})$ be the matrix whose entries are the n_{jk}. It follows that

$$\mathrm{vol}(F) = |\det(N)| \, \mathrm{vol}(E)$$

Clearly, N^{-1} has $\mathbb{Z}$ entries so $\det(N)$ is a unit in $\mathbb{Z}$ (i.e ± 1). Hence $\mathrm{vol}(F) = \mathrm{vol}(E)$. □

Definition 5.7. Let V be an n-dimensional vector space over $\mathbb{R}$ and $\Lambda \subseteq V$ a lattice. We define the **covolume** of Λ, denoted $\mathrm{covol}(\Lambda)$, to be the volume of the parallelotope given by any $\mathbb{Z}$-basis of Λ.

Definition 5.8. Let V be a finite dimensional vector space over $\mathbb{R}$ and $S \subseteq V$ a subset. We say that S is **convex** if for all $x, y \in S$ we have $tx + (1-t)y \in S$ for all $t \in [0,1]$[4].

Theorem 5.9 (Minkowski's Convex Body Theorem)**.** *Let V be an n-dimensional vector space over $\mathbb{R}$, $\Lambda \subseteq V$ a lattice and $S \subseteq V$ a measurable[5] subset. Then*

1. *If $\mathrm{vol}(S) > \mathrm{covol}(\Lambda)$ then there exists $x, y \in S$ such that $0 \neq x - y \in \Lambda$.*
2. *If $\mathrm{vol}(S) > 2^n \, \mathrm{covol}(\Lambda)$ and S is symmetric[6] and convex then there exists a non-zero point in $S \cap \Lambda$.*
3. *If $\mathrm{vol}(S) \geq 2^n \, \mathrm{covol}(\Lambda)$ and S is symmetric, convex and compact then there exists a non-zero point in $S \cap \Lambda$.*

Proof.

Part 1: Fix a $\mathbb{Z}$-basis of Λ and let P be the parallelotope defined by it. We can think of Λ as acting on V by translation. Then P is a fundamental domain for this action. In other words, $V = \bigcup_{\lambda \in \Lambda} P_\lambda$ where $P_\lambda = \lambda + P$[7]. Observe that $P_\lambda \cap P_\mu$ is non-zero at most along some subset of the boundaries of P_λ and P_μ. Furthemore, set $S_\lambda = \lambda + S$. We then have that

$$S = \bigcup_{\lambda \in \Lambda} (P_\lambda \cap S) \implies \mathrm{vol}(S) = \sum_{\lambda \in \Lambda} \mathrm{vol}(P_\lambda \cap S)$$

Through a translation, we have that $P_\lambda \cap S \cong P \cap S_{-\lambda}$ and so $\mathrm{vol}(S) = \sum_{\lambda \in \Lambda} \mathrm{vol}(P \cap S_{-\lambda})$. Now assume that all the subsets $P \cap S_{-\lambda}$ are disjoint. Then they are disjoint subsets of P whence $\sum_{\lambda \in \Lambda} \mathrm{vol}(P \cap S_{-\lambda}) \leq \mathrm{vol}(P)$. But, by assumption, $\mathrm{vol}(S) > \mathrm{vol}(P)$ which is a contradiction. Hence there exists $\lambda, \mu \in \Lambda$ with $\lambda \neq \mu$ such that

$$\begin{aligned} \varnothing &\neq (P \cap S_{-\lambda}) \cap (P \cap S_{-\mu}) \\ &= P \cap (S_{-\lambda} \cap S_{-\mu}) \end{aligned}$$

In particular, $S_{-\lambda} \cap S_{-\mu} \neq \varnothing$ so there exists $x, y \in S$ such that $x - \lambda = y - \mu$. Then $x - y = \lambda - \mu \in \Lambda$ and $x \neq y$.

Part 2: Let $S' = (1/2)S$. Then $\mathrm{vol}(S') = 2^{-n} \, \mathrm{vol}(S) > \mathrm{covol}(\Lambda)$. Hence by Part 1, there exists, $y, z \in S'$ such that $0 \neq y - z \in \Lambda$. Then $2x, 2z \in S$ so $-2z \in S$ by symmetry. Let $x = y - z$. Then

$$x = y - z = \frac{1}{2}(2y - 2z) = \frac{1}{2}(2y) + \frac{1}{2}(-2z)$$

[4]geometrically, this means that, given any two points in S, the line joining them is fully contained in S
[5]interpret this is any subset of V that has an intuitive volume
[6]$x \in S \implies -x \in S$
[7]consider $\Lambda = \mathbb{Z}^2 \subseteq \mathbb{R}^2$ with the e_i the standard basis

Since S is convex, it follows that $x \in S$.

Part 3: Let $S_m = (1 + 1/m)S$ for all positive integers m. By Part 2, there exists an $x_m \in \Lambda \cup S_m$. Note that the sequence $\{ x_m \} \subseteq \Lambda \cap S_1$. But Λ is a lattice and, in particular, is discrete. S_1 is clearly compact so $\Lambda \cap S_1$ is finite. Hence $x_m = x$ for infinitely many m. Then $x \in \cap_m S_m$. But each S_m is compact whence $x \in \cap_m S_m = S$ and we are done.

□

We shall use these results to show that the class group of a number field is finite. Let K be a number field of degree n. Recall that there exist n distinct embeddings of K into an algebraic closure of $\mathbb{C}$. It is not hard to see that $n = r + 2s$ where r is the number of real embeddings and $2s$ is the number of complex embeddings.

Definition 5.10. Let K be a number field of degree n and let $\sigma_1, \dots, \sigma_n$ be the distinct embeddings of K into an algebraic closure of $\mathbb{Q}$. We can label them so that $\sigma_1, \dots, \sigma_r, \dots, \sigma_s, \dots, \sigma_{2s}$ is the list of embeddings where r is the number of real embeddings and s is the number of complex conjugate pairs of embeddings. Furthermore, choose the ordering of these embeddings such that, for $r \le j \le r_s$, σ_{j+s} is the complex conjugate of σ_j. Note that we can identify $\mathbb{C}$ with $\mathbb{R}^2$ via the mapping $z \mapsto (\operatorname{Re} z, \operatorname{Im} z)$. We define the **canonical embedding** of K to be the mapping $K \to \mathbb{R}^n$ given by

$$(\sigma_1, \dots, \sigma_r, \operatorname{Re} \sigma_{r+1}, \operatorname{Im} \sigma_{r+1}, \dots, \operatorname{Re} \sigma_{r+s}, \operatorname{Im} \sigma_{r+s})$$

Lemma 5.11. *Let V be an n-dimensional vector space over $\mathbb{R}$ and $\Lambda \subseteq V$ a lattice. Suppose that $M \subseteq \Lambda$ is a subgroup of index m. Then M is a lattice and* $\operatorname{covol}(M) = m \operatorname{covol}(\Lambda)$.

Proof. By the stucture theorem for finitely generated modules over a Euclidean domain, there exists a $\mathbb{Z}$-basis $e_1, \dots, e_n$ for Λ and integers $r_1, \dots, r_n$ such that $r_1 e_1, \dots, r_n e_n$ is a $\mathbb{Z}$-basis for M. Let $X \subseteq V$ be compact. Then $M \cap X \subseteq \Lambda \cap X$. But the latter is finite so M must be discrete and is thus a lattice.

Let $[e_1, \dots, e_n]$ denote the matrix with columns given by the e_i. Then

$$\operatorname{covol}(M) = |\det[r_1 e_1, \dots, r_n e_n]| = |r_1 \cdots r_n| \det[e_1, \dots, e_n] = \prod_{i=1}^{n} r_i \operatorname{covol}(\Lambda)$$

It is easy to see that $m = \prod_{i=1}^{n} r_i$. Indeed, m is the order of the quotient group Λ/M. But this is isomorphic to $\mathbb{Z}/(r_1) \oplus \cdots \oplus \mathbb{Z}/(r_n)$ which has $r_1 \cdots r_n$ elements. □

Proposition 5.12. *Let K be a number of degree n and discriminant Δ_K. Let $\sigma_1, \dots, \sigma_n$ be the n distinct emebddings of K into an algebraic closure of $\mathbb{Q}$ such that $n = r + 2s$ and let σ denote the canonical embedding of K into $\mathbb{R}^n$. Furthermore, let $I \triangleleft \mathcal{O}_K$ be an integral ideal. Then*

1. *$\sigma(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ and* $\operatorname{covol}(\sigma(\mathcal{O}_K)) = 2^{-s}|\Delta_K|^{1/2}$.
2. *$\sigma(I)$ is a lattice in $\mathbb{R}^n$ and* $\operatorname{covol}(\sigma(I)) = N(I)2^{-s}|\Delta_K|^{1/2}$.

Proof. Part 1: Let $x_1, \dots, x_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\operatorname{covol}(\sigma(\mathcal{O}_K))$ is given by the absolute value of

$$\begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_r(x_1) & \operatorname{Re} \sigma_{r+1}(x_1) & \operatorname{Im} \sigma_{r+1}(x_1) & \cdots & \operatorname{Re} \sigma_{r+2s}(x_1) & \operatorname{Im} \sigma_{r+2s}(x_1) \\ \sigma_1(x_2) & \cdots & \sigma_r(x_2) & \operatorname{Re} \sigma_{r+1}(x_2) & \operatorname{Im} \sigma_{r+1}(x_2) & \cdots & \operatorname{Re} \sigma_{r+2s}(x_2) & \operatorname{Im} \sigma_{r+2s}(x_2) \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \sigma_1(x_n) & \cdots & \sigma_r(x_n) & \operatorname{Re} \sigma_{r+1}(x_n) & \operatorname{Im} \sigma_{r+1}(x_n) & \cdots & \operatorname{Re} \sigma_{r+s}(x_n) & \operatorname{Im} \sigma_{r+s}(x_n) \end{vmatrix}$$

Omitting writing everything except the σ_{r+1} columns, we have

$$\pm\operatorname{covol}(\sigma(\mathcal{O}_K)) = \begin{vmatrix} \cdots & \frac{1}{2}(\sigma_{r+1}(x_1)+\sigma_{r+s+1}(x_1)) & \frac{1}{2i}(\sigma_{r+1}(x_1)-\sigma_{r+s+1}(x_1)) & \cdots \\ \cdots & \vdots & \vdots & \cdots \\ \cdots & \frac{1}{2}(\sigma_{r+1}(x_n)+\sigma_{r+s+1}(x_n)) & \frac{1}{2i}(\sigma_{r+1}(x_n)-\sigma_{r+s+1}(x_n)) & \cdots \end{vmatrix}$$
$$= \left(\frac{1}{2}\right)^s\left(\frac{1}{2i}\right)^s \begin{vmatrix} \cdots & \sigma_{r+1}(x_1)+\sigma_{r+s+1}(x_1) & \sigma_{r+1}(x_1)-\sigma_{r+s+1}(x_1) & \cdots \\ \cdots & \vdots & \vdots & \cdots \\ \cdots & \sigma_{r+1}(x_n)+\sigma_{r+s+1}(x_n) & \sigma_{r+1}(x_n)-\sigma_{r+s+1}(x_n) & \cdots \end{vmatrix}$$

Adding the column with the differences to the column with the sums gives

$$\pm\operatorname{covol}(\sigma(\mathcal{O}_K)) = \left(\frac{1}{2}\right)^s\left(\frac{1}{2i}\right)^s \begin{vmatrix} \cdots & 2\sigma_{r+1}(x_1) & \sigma_{r+1}(x_1)-\sigma_{r+s+1}(x_1) & \cdots \\ \cdots & \vdots & \vdots & \cdots \\ \cdots & 2\sigma_{r+1}(x_n) & \sigma_{r+1}(x_n)-\sigma_{r+s+1}(x_n) & \cdots \end{vmatrix}$$
$$= \left(\frac{1}{2i}\right)^s \begin{vmatrix} \cdots & \sigma_{r+1}(x_1) & \sigma_{r+1}(x_1)-\sigma_{r+s+1}(x_1) & \cdots \\ \cdots & \vdots & \vdots & \cdots \\ \cdots & \sigma_{r+1}(x_n) & \sigma_{r+1}(x_n)-\sigma_{r+s+1}(x_n) & \cdots \end{vmatrix}$$

Subtracting the column whose entries have a single term from the column with the differences gives

$$\pm\operatorname{covol}(\sigma(\mathcal{O}_K)) = \left(\frac{1}{2i}\right)^s \begin{vmatrix} \cdots & \sigma_{r+1}(x_1) & -\sigma_{r+s+1}(x_1) & \cdots \\ \cdots & \vdots & \vdots & \cdots \\ \cdots & \sigma_{r+1}(x_n) & -\sigma_{r+s+1}(x_n) & \cdots \end{vmatrix}$$
$$= (-1)^s\left(\frac{1}{2i}\right)^s \begin{vmatrix} \cdots & \sigma_{r+1}(x_1) & \sigma_{r+s+1}(x_1) & \cdots \\ \cdots & \vdots & \vdots & \cdots \\ \cdots & \sigma_{r+1}(x_n) & \sigma_{r+s+1}(x_n) & \cdots \end{vmatrix}$$

But recall from Proposition 2.15 that such a determinant is the square root of $|\Delta_K|$. Thus

$$\operatorname{covol}(\sigma(\mathcal{O}_K)) = \left|(-1)^s\left(\frac{1}{2i}\right)^s|\Delta_K|^{1/2}\right| = 2^{-s}|\Delta_K|^{1/2}$$

Part 2: Recall that an integral ideal $I \triangleleft \mathcal{O}_K$ has index $N(I)$ in $\mathcal{O}_K$. Hence by Lemma 5.11, $\sigma(I)$ is a lattice. Furthermore,

$$\operatorname{covol}(\sigma(I)) = N(I)\operatorname{covol}(\sigma(\mathcal{O}_K)) = N(I)2^{-s}|\Delta_K|^{1/2}$$

□

Definition 5.13. Let K be a number field of degree n such that $n = r + 2s$ where r is the number of real embeddings and s is the number of complex conjugate pairs of complex embeddings of K into an algebraic closure of $\mathbb{Q}$. We define the **Minkowski constant** c_K of K to be

$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}|\Delta_K|^{1/2}$$

where Δ_K is the discriminant of K.

Lemma 5.14. *Let $t > 0 \in \mathbb{R}$ and consider the set*

$$B(r,s)_t = \left\{ (y,z) \in \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \sum_i |y_i| + 2\sum_i |z_i| \le t \right\}$$

Then

$$\mathrm{vol}(B(r,s)_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$$

Proof. We shall prove the lemma by induction on r and s. First suppose that $r = 1$ and $s = 0$. Then $B(1,0)_t = [-t,t]$. The lemma clearly holds in this case. Next suppose that $r = 0$ and $s = 1$. Then $B(0,1)_t$ is the disc of radius $t/2$ in the complex plane and the lemma also holds in this case.

Now assume that the formula holds for $B(r,s)_t$. We shall prove that it holds for $B(r+1,s)_t$.

$B(r+1,s)_t$ is the region of $\mathbb{R} \times \mathbb{R}^r \times \mathbb{C}^s$ defined by

$$|y| + \sum_i |y_i| + 2\sum_i |z_i| \le t$$

for some $y \in \mathbb{R}$. This is equivalent to

$$\sum_i |y_i| + 2\sum_i |z_i| \le t - |y|$$

For $|y| > t$, B_t is empty so we have

$$\begin{aligned}
\mathrm{vol}(B(r+1,s)_t) &= \int_{-t}^{t} B(r,s)_{t-|y|}\, dy \\
&= 2\int_0^t 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-y)^n}{n!}\, dy \\
&= 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{1}{n!} \int_0^t (t-y)^n\, dy \\
&= 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{1}{n!} \int_0^t \left[\frac{1}{n+1}(t-y)^n\right]_0^t \\
&= 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{t^n}{(n+1)!}
\end{aligned}$$

as desired.

We now prove that that the formula holds for $B(r,s+1)_t$. This is the region of $\mathbb{R}^r \times \mathbb{C}^s \times \mathbb{C}$ defined by

$$\sum_i |y_i| + 2\sum_i z_i + 2|z| \le t$$

for some $z \in \mathbb{C}$. This is equivalent to

$$\sum_i |y_i| + 2\sum_i z_i \le t - 2|z|$$

and hence $B(r,s+1)_t$ is empty when $|z| \ge t/2$. We thus have

$$\mathrm{vol}(B(r,s+1)_t) = \int_{|z| \le t/2} B(r,s)_{t-2|z|}\, d\sigma$$

where $d\sigma$ is the infinitesimal area element of $\mathbb{C}$. Swapping to polar coordinates, we have $z = \rho\exp(i\theta)$ and $d\sigma = d\rho d\theta$. Hence

$$\begin{aligned}\operatorname{vol}(B(r, s+1)_t) &= \int_{\rho=0}^{t/2}\int_{\theta=0}^{2\pi} \rho 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-2\rho)^n}{n!}\, d\rho d\theta \\ &= 2^r \left(\frac{\pi}{2}\right)^s \frac{2\pi}{n!}\int_{\rho=0}^{t/2} \rho(t-2\rho)^n \, d\rho\end{aligned}$$

Applying integration by parts yields

$$\int_{\rho=0}^{t/2} \rho(t-2\rho)^n \, d\rho = \frac{t^{n+2}}{4(n+1)(n+2)}$$

and we are done. □

Proposition 5.15 (Minkowski bound)**.** *Let K be a number field of degree n such that $n = r + 2s$ where r is the number of real embeddings and s is the number of complex conjugate pairs of complex embeddings of K into an algebraic closure of $\mathbb{Q}$. If $I \triangleleft \mathcal{O}_K$ is an integral ideal then there exists non-zero $x \in I$ such that*

$$|\operatorname{N}_{K/\mathbb{Q}}(x)| \leq c_K N(I)$$

where c_K is the Minkowski constant of K.

Proof. Let $t > 0 \in \mathbb{R}$ and let

$$B(r,s)_t = \left\{ (y,z) \in \mathbb{R}^r \times \mathbb{C}^s \;\middle|\; \sum_i |y_i| + 2\sum_i |z_i| \leq t \right\}$$

Clearly, $B(r,s)_t$ is compact and symmetric. We first claim that it is also convex. To this end, let $(a,b),(c,d) \in B(r,s)_t$. We need to show that $m_1(a,b) + m_2(c,d) \in B(r,s)_t$ for all $m_1 \geq 0$, $m_2 \leq 1$ such that $m_1 + m_2 = 1$. We have

$$m_1(a,b) + m_2(c,d) = (m_1 a + m_2 c, m_1 b + m_2 d)$$

and so

$$\begin{aligned}\sum_i |m_1 a_i + m_2 c_i| + 2\sum_i |m_1 b_i + m_2 d_i| &= \sum_i |m_1 a_i + m_2 c_i| + 2\sum_i |m_1 b_i + m_2 d_i| \\ &\leq \sum_i m_1|a_i| + m_2|c_i| + 2\sum_i m_1|b_i| + m_2|d_i| \\ &= m_1\left(\sum_i |a_i| + 2\sum_i |b_i\right) + m_2\left(\sum_i |c_i| + 2\sum_i |d_i|\right) \\ &\leq m_1 t + m_2 t = t\end{aligned}$$

and so $B(r,s)_t$ is convex.

Now choose t such that $\operatorname{vol}(B(r,s)_t) = 2^n \operatorname{covol}(\sigma(I))$. Then

$$2^r\left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} = 2^n N(I) 2^{-s}|\Delta_K|^{1/2}$$

Rearranging and using the fact that $n = r + 2s$ we have

$$t^n = \left(\frac{4}{\pi}\right)^s n! |\Delta_K|^{1/2} N(I)$$

Now by Minkowski's Convex Body Theorem, there exists non-zero $x \in I$ such that $\sigma(x) = (y_1, \ldots, y_r, z_1, z_s) \in B(r, s)_t$. Note that

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{i=1}^{r} y_i \prod_{j=1}^{s} z_j \overline{z_j}$$

By the arithmetic mean-geometric mean inequality we have

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)|^{1/n} \leq \frac{1}{n}\left(\sum_i |y_i| + 2\sum_j |z_j|\right)$$

By the choice of t we then have that

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| \leq \frac{t^n}{n^n} = c_K N(I)$$

as desired. □

Corollary 5.16. *Let K be a number field of degree $n = r + 2s$. Then every element of $\mathrm{Cl}(\mathcal{O}_K)$ has an integral ideal representative $J \lhd \mathcal{O}_K$ such that $N(J) \leq c_K$.*

Proof. Given any equivalence class in $\mathrm{Cl}(\mathcal{O}_K)$, choose a fractional ideal, say M. Given any non-zero $y \in M$ we have $y\mathcal{O}_K \subseteq M$ and so $yM^{-1} \subseteq \mathcal{O}_K$. Observe that $[yM^{-1}] = [M^{-1}]$ as multiplying by an element of K won't affect the principality of the fractional ideal M^{-1}. We thus may assume, without loss of generality, that M^{-1} is an integral ideal. By Proposition 5.15, we may choose a non-zero $x \in M^{-1}$ such that

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| \leq c_K N(M^{-1})$$

Multiplying through by $N(M)$ we get

$$|N(xM)| \leq c_K$$

Clearly, xM is in the same equivalence class as M and $xM \subseteq M^{-1}M \subseteq \mathcal{O}_K$ and is thus integral as required. □

Lemma 5.17. *Let R be a Dedekind domain and $I_1, I_2 \lhd R$ integral ideals. Then I_1 divides I_2 if and only if $I_2 \subseteq I_1$.*

Proof. Let $\mathfrak{p} \lhd \mathcal{O}_K$ be prime. Let $n_P(I)$ denote the exponent of $\mathfrak{p}$ in the prime factorisation of $\mathfrak{p}$. Then I_1 divides I_2 if and only if $n_\mathfrak{p}(I_1) \leq n_\mathfrak{p}(I_2)$ for all prime ideals $\mathfrak{p}$. Now we have $I_2 \subseteq I_1$ if and only if $I_2 I_1^{-1} \subseteq \mathcal{O}_K$. But this is equivalent to $n_\mathfrak{p}(I_2) - n_\mathfrak{p}(I_1) \geq 0$ and we are done. □

Corollary 5.18. *Let K be a number field. Then $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

Proof. By the existence of the Minkowski bound, it suffices to show that, given any positive integer M, there exist only finitely many integral ideals whose norm is M.

We first claim that any integral ideal with norm M necessarily contains M. To this end, let $I \lhd \mathcal{O}_K$ be an integral ideal such that $N(I) = M$. Then, by definition, we have $|\mathcal{O}_K/I| = M$. But it is easy to see that the characteristic of a finite ring must divide its order. Hence we must have that $M \equiv 0 \pmod{I}$ and thus $M \in I$.

Now, if $M \in I$ then $(M) \subseteq I$. By Lemma 5.17, I divides (M). But, by unique factorisation, (M) has only finitely many divisors. It thus follows that there can exist only finitely many ideals containing M and thus there can only exist finitely many ideals with norm M. □

Remark. This result doesn't necessarily hold for general Dedekind domains. Indeed, a counter example is the complex algebraic curves of positive genus.

Example 5.19. Consider the number field $K = \mathbb{Q}(\sqrt{-13})$. $-13 \equiv 3 \pmod 4$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$. It follows that $\Delta_K = -4 \cdot 13$. Now, the degree of K over $\mathbb{Q}$ is $n = 2$ and there are clearly only complex embeddings so $s = 1$. We may thus calculate a bound on the Minkowski constant:

$$c_k = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}(2\sqrt{13}) = \frac{4\sqrt{13}}{\pi} < \frac{4\sqrt{13}}{3} = \frac{2\sqrt{52}}{3} < \frac{2\cdot 7.5}{3} = 5$$

Hence every equivalence class in $\mathcal{O}_K$ contains an integral ideal representative I satisfying $N(I) \leq 4$. Since every integral ideal admits a unique factorisation into prime ideals, this means that the class group is generated by classes of prime ideals $[\mathfrak{p}]$ such that $N(\mathfrak{p}) \leq 4$.

We now factorise the ideals generated by the rational primes less than or equal to 4 (i.e 2 and 3) using Dedekind's Theorem. First note that $[\mathcal{O}_K : \mathbb{Z}[\sqrt{-13}] = 1$ and so we may apply Dedekind's Theorem to 2 and 3. The minimal polynomial of $\sqrt{-13}$ over $\mathbb{Q}$ is X^2+13. Considering this modulo 2 we have

$$\begin{aligned} X^2 + 13 &\equiv X^2 + 1 \pmod 2 \\ &= (X+1)^2 \end{aligned}$$

and so $p\mathcal{O}_K = \mathfrak{p}^2$ where $\mathfrak{p} = (2, 1+\sqrt{-13})\mathcal{O}_K$ and $N(\mathfrak{p}) = 2$.

Considering the minimal polynomial modulo 3 we have

$$X^2 + 13 \equiv X^2 + 1 \pmod 3$$

But this polynomial is irreducible in $\mathbb{F}_3[X]$ so $3\mathcal{O}_K$ is prime and has norm 9.

It follows that the class group is generated by the class $[\mathfrak{p}]$. Note that since $\mathfrak{p}^2 = 2\mathcal{O}_K$ which is principal, $[\mathfrak{p}]$ must have order either 1 or 2.

Suppose that the order of $[\mathfrak{p}]$ is order 1. Then we would be able to write $\mathfrak{p} = (x + y\sqrt{-13})\mathcal{O}_K$ for some $x, y \in \mathbb{Z}$. Passing to the norms we have $2 = |\,\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{-13})| = x^2 + 13y^2$. But this equation clearly has no solutions in integers so $[\mathfrak{p}]$ must have order 2. Therefore, $\mathrm{Cl}(\mathcal{O}_K) = \mathbb{F}_2$.

We can use this to find solutions to the equation $y^2 = x^3 - 13$ in $\mathbb{Z}$. Indeed, suppose that (x, y) is a solution to this equation. First assume that x is even. Then $y^2 \equiv 3 \pmod 4$ which is a contradiction. Hence x must be odd. Furthermore, x and y are coprime. Indeed, we may rewrite the equation as $y^2 - x^3 = -13$ to see that the only possible prime dividing both y and x is 13. But then 13^2 would divide the left hand side of the original equation and not the right hand side. Thus x and y are coprime.

We now factor the equation in $\mathcal{O}_K$ to get

$$(y+\sqrt{-13})(y-\sqrt{-13}) = x^3$$

Suppose that a prime ideal $\mathfrak{p}$ divides both ideals $(y+\sqrt{-13})\mathcal{O}_K$ and $(y-\sqrt{-13})\mathcal{O}_K$. Then $\mathfrak{p}$ divides $(x)^3$ and, in particular, (x). But x is odd so $\mathfrak{p}$ cannot divide $2\mathcal{O}_K$. Observe also that $\mathfrak{p}$ divides $2y\mathcal{O}_K$ whence $\mathfrak{p}$ divides $y\mathcal{O}_K$. But this is a contradiction to the fact that x and y are coprime so there cannot exist a prime ideal dividing both $(y+\sqrt{-13})\mathcal{O}_K$ and $(y-\sqrt{-13})\mathcal{O}_K$. Hence by unique factorisation of ideals, there exists ideals $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_K$ such that

$$(y+\sqrt{-13})\mathcal{O}_K = \mathfrak{a}^3, \quad (y-\sqrt{-13})\mathcal{O}_K = \mathfrak{b}^3$$

Now $\mathrm{Cl}(\mathcal{O}_K) = \mathbb{F}_2$ and so $[\mathfrak{a}]^3 = [\mathfrak{b}]^3 = 1$ whence $\mathfrak{a}$ and $\mathfrak{b}$ are principal. In particular,

$$(y+\sqrt{-13})\mathcal{O}_K = (a+b\sqrt{-13})^3\mathcal{O}_K$$

for some $a, b \in \mathbb{Z}$. Hence, $y+\sqrt{-13} = (a+b\sqrt{-13})^3 u$ for some unit $u \in \mathcal{O}_K^\times$. Recall that a unit in $\mathcal{O}_K$ must have norm ± 1. Suppose that $c+d\sqrt{-13}$ is a unit for some $c, d \in \mathbb{Z}$. Then $c^2+13d^2 = 1$. This is only possible if $c = \pm 1$ and $d = 0$. Hence the only units in $\mathcal{O}_K$ are ± 1. Hence

$$y+\sqrt{-13} = (a+b\sqrt{-13})^3$$

Expanding the right hand side out (with the binomial theorem or otherwise) gives

$$y+\sqrt{-13} = a^3 + 3a^2b\sqrt{-13} - 3\cdot 13ab^2 - 13b^3\sqrt{-13}$$

Comparing coefficients of $\sqrt{-13}$ yields

$$1 = 3a^2b - 13b^3 = b(3a^2-13b^2)$$

whence $b = \pm 1$. If $b = 1$ then $1 = 3a^2 - 13$ which is not possible. Hence $b = -1$ which gives $1 = -3a^2 + 13$ whence $a = \pm 2$. This then gives

$$y = a^3 - 39ab^2 = \pm 8 \mp 78$$

and thus $y = \pm 70$. Substituting ths into the original equation gives $70^2 = x^3 - 13$. Simplifying gives us $x^3 = 4913$. Note[8] that $4913 = 17^3$ and so $x = 17$. Thus, the complete list of solutions to $y^2 = x^3 - 13$ is $(17, \pm 70)$.

Example 5.20. Consider the number field $\mathbb{Q}(\sqrt{19})$. Then $19 \equiv 3 \pmod 4$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{19}]$. We thus have that $\Delta_K = 4\cdot 19$. Note that the degree of the number field is 2 with only one real embedding. We can thus calculate the Minkowski constant

$$c_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}|\Delta_K|^{1/2} = \frac{2!}{2^2}\cdot 2\sqrt{19} = \sqrt{19} < 5$$

Hence $\mathrm{Cl}(\mathcal{O}_K)$ is generated by classes of prime ideals of norm at most 4. We now factorise the ideals generated by the rational primes up to 4, namely $2\mathcal{O}_K$ and $3\mathcal{O}_K$. The minimal polynomial of $\sqrt{19}$ over $\mathbb{Q}$ is $X^2 - 19$. Considering this modulo 2 we have

$$\begin{aligned} X^2 - 19 &\equiv X^2 + 1 \pmod 2 \\ &= (X+1)(X+1) \end{aligned}$$

[8] Oh God, don't expect me to do this in the exam *flashbacks from elementary number theory*

and so $2\mathcal{O}_K = \mathfrak{p}^2$ where $\mathfrak{p} = (2, 1+\sqrt{19})\mathcal{O}_K$ is prime. Furthermore, $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_2] = 1$ and so $N(\mathfrak{p}) = 2$.

Now consider the minimal polynomial modulo 3:

$$\begin{aligned} X^2 - 19 &\equiv X^2 + 2 \pmod 3 \\ &= (X+1)(X-1) \end{aligned}$$

and so $3\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are prime and $N(\mathfrak{q}_1) = N(\mathfrak{q}_2) = 3$. We claim that both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are principal. By Dedekind's Theorem, we can write $\mathfrak{q}_1 = (3, 1+\sqrt{19})\mathcal{O}_K$. To show that $\mathfrak{q}_1$ is principal, it suffices to show that it contains a principal ideal whose norm equals that of $\mathfrak{q}_1$. It is easy to see that $4+\sqrt{19} \in \mathfrak{q}_1$. Then $N((4+\sqrt{19})\mathcal{O}_K) = |\operatorname{N}_{K/\mathbb{Q}}(4+\sqrt{19})| = |4^2 - \sqrt{19}^2| = 3$ as desired. Hence $\mathfrak{q}_1$ is principal. A similar argument shows that $\mathfrak{q}_2$ is also principal. Hence $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $[\mathfrak{p}]$. Now, $[\mathfrak{p}]$ must have order either 1 or 2 since $\mathfrak{p}^2$ is principal. Suppose that $\mathfrak{p}$ has order 1. This is equivalent to $\mathfrak{p}$ being principal. We claim that $\mathfrak{p}\mathfrak{q}_i$ is principal for some i. Since $\mathfrak{q}_i$ is principal, this will imply that $\mathfrak{p}$ is principal. It is easy to see[9] that $5-\sqrt{19} \in \mathfrak{p}\mathfrak{q}_1$. So

$$N(\mathfrak{p}\mathfrak{q}_1) = N(\mathfrak{p})N(\mathfrak{q}_1) = 2 \cdot 3 = 6 = |\operatorname{N}_{K/\mathbb{Q}}(5-\sqrt{19})| = N((5-\sqrt{19})\mathcal{O}_K)$$

and so $\mathfrak{p}\mathfrak{q}_1 = (5-\sqrt{19})\mathcal{O}_K$ whence the product is principal. Hence $\mathfrak{p}$ is principal. This means that $[\mathfrak{p}]$ has order 1 in $\mathrm{Cl}(\mathcal{O}_K)$ whence the class group is trivial. Thus $\mathcal{O}_K$ is a principal ideal domain and, in particular, a unique factorisation domain.

Theorem 5.21 (Hermite-Minkowski)**.** *Let K be a number field of degree $n \geq 2$ such that $n = r + 2s$. Then*

$$|\Delta_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$$

Proof. Let $[I] \in \mathrm{Cl}(\mathcal{O}_K)$ be an ideal class. By Corollary 5.16, there exists an integral representative of $[I]$, say I, such that $N(I) \leq c_K$. But $1 \leq N(I)$ so $c_K \geq 1$. This implies that

$$|\Delta_K|^{1/2} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}$$

and so

$$|\Delta_K| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{n^{2n}}{n!^2}$$

Since $\pi/4 < 1$ and $n \geq 2s$ we have

$$|\Delta_K| \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{n!^2} =: a_n$$

Now,

$$a_2 = \frac{\pi^2}{4} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)$$

[9] the product contains 6 and it also contains $-(1+\sqrt{19})$

Using the binomial theorem, we obtain the estimate

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} > \frac{\pi}{4}\left(1+\frac{2n}{n}\right) = \frac{3\pi}{4}$$

And so

$$a_n > a_2\left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

□

Theorem 5.22 (Hermite)**.** *Let $n \geq 1$ be a natural number. Then there are only finitely many number fields K such that $|\Delta_K| \leq n$.*

Proof. Let K be a number field and fix a natural number $N \in \mathbb{N}$. Suppose that $|\Delta_K| = N$. By the Hermite-Minkowski Thereom, there exists an upper bound on the degree of $n = r+2s$, depending only on N. Hence we may assume that N and n are both fixed natural numbers. We need to show that there are only finitely many number fields K such that $|\Delta_K| = N$ and $[K:\mathbb{Q}] = n$.

Let $\Lambda = \sigma(\mathcal{O}_K)$ be the lattice equal to the image of the canonical embedding σ in $\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$. By Proposition 5.12, $\operatorname{covol}(\sigma(\mathcal{O}_K)) = 2^{-s}|\Delta_K|^{1/2}$.

Consider the set M of elements $(y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^n$ satisfying

1. if $r > 0$ then

$$|y_1| \leq \frac{2^{r+3s-1}}{\pi^s}N^{1/2}, \quad |y_i| \leq \frac{1}{2} \text{ for } i \neq 1, \quad |z_i| \leq \frac{1}{2}$$

2. if $r = 0$ then

$$|\operatorname{Im}(z_1)| \leq \frac{2^{r+3s-2}}{\pi^{s-1}}N^{1/2}, \quad |\operatorname{Re}(z_1)| \leq \frac{1}{4} \quad , |z_i| \leq \frac{1}{2} \text{ for } i \neq 1$$

It is easy to see that M is compact and symmetric. With a little bit of geometric intuition, we see that M is convex[10] and $\operatorname{vol}(M) = 2^{r+s}N^{1/2} = 2^n \operatorname{covol}(\Lambda)$. Appealing to Minkowski's Convex Body Theorem, there exists a non-zero $x \in \mathcal{O}_K$ such that $\sigma(x) \in M$. We see that the conjugates of x are all bounded above by a constant depending only on N. Since x is an algebraic integer, the coefficients of its minimal polynomial are integers. Since such coefficients are the elementary symmetric polynomials in the conjugates of x, they must all be bounded above by a constant depending only on N. Thus there are only finitely many choices for such coefficients. If we can show that $K = \mathbb{Q}(\alpha)$ then we are done.

Suppose that $r > 0$. Then

$$|\operatorname{N}_{K/\mathbb{Q}}(x)| = \left|\prod_{i=1}^{n} \sigma_j(x)\right| \leq |\sigma_1(x)|2^{-(n-1)}$$

Recall that $|\operatorname{N}_{K/\mathbb{Q}}(x)|$ is an integer. It then follows that $|\sigma_1(x)| > 1$. Let τ be the restriction of σ_1 to $\mathbb{Q}(x)$. Recall that there are exactly $[K:\mathbb{Q}(x)]$ extensions of τ to an embedding of K into $\mathbb{C}$. Label such an extension $\overline{\tau}$. Then

$$|\overline{\tau}(x)| = |\sigma_1(x)| > 1$$

[10]in the $r > 0$ we have a product of intervals and discs, in the $r = 0$ case, we have a product of a rectangle with discs

But there is only one such embedding σ_i satisfying this property and thus $[K : \mathbb{Q}(x)] = 1$ whence $K = \mathbb{Q}(x)$.

Now suppose that $r = 0$. Then a similar argument shows that $|\sigma_1(x)| = |\overline{\sigma}_1(x)|$. Thus $\sigma_j(x) \neq \sigma_1(x)$ unless $\sigma_j(x) = \overline{\sigma}_1(x)$. We need to rule out this case in order for the previous argument to follow through. Assume that $\sigma_1(x) = \overline{\sigma}_1(x)$. Then $\sigma_1(x)$ is real and so $\mathrm{Im}(\sigma_1(x)) = 0$. Then

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| = \left|\prod_{i=1}^{n} \sigma_i(x)\right| = |\sigma_1(x)| \left|\prod_{i=2}^{n} \sigma_i(x)\right| \leq \frac{1}{4} \cdot \left(\frac{1}{2}\right)^{n-1}$$

Now the norm must be non-zero and integer but this is a contradiction. Hence $\sigma_1(x)$ is not real and $\sigma_1(x) \neq \overline{\sigma}_1(x)$. The argument for the previous case then applies in this situation and $K = \mathbb{Q}(x)$. □

6 Ramification Theory

Definition 6.1. Let K be a number field and p a prime number. Suppose that $p\mathcal{O}_K$ admits the unique factorisation

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

We say that p **ramifies** in K if $e_i \geq 2$ for some $1 \leq i \leq r$.

Theorem 6.2. *Let K be a nunber field with discriminant Δ_K and p a prime number. Then p ramifies in K if and only if p divides Δ_K.*

Proof. Let $x_1, \ldots, x_n$ be an integral basis for $\mathcal{O}_K$. Recall that

$$\Delta_K = \det T_{ij}$$

where T_{ij} is the matrix corresponding to the linear map

$$T : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}$$
$$T(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(x, y)$$

evaluated at the basis $x_1, \ldots, x_n$. We may 'reduce' this mapping modulo p to obtain a mapping

$$\overline{T} : \mathcal{O}_K/p\mathcal{O}_K \times \mathcal{O}_K/p\mathcal{O}_K \mapsto \mathbb{Z}/p\mathbb{Z}$$

If $\overline{x_i} \equiv x_i \pmod{p\mathcal{O}_K}$ then $\overline{T}$ is given by the matrix $\overline{T}_{ij} = \mathrm{Tr}_{K/\mathbb{Q}}(\overline{x_i x_j})$.[11]

Then p divides Δ_K if and only if p divides $\det(T_{ij})$ if and only if $\det(\overline{T}_{ij}) = 0$. Hence if suffices to show that p ramifies in K if and only if $\det(\overline{T}_{ij}) = 0$.

Suppose $p\mathcal{O}_K$ admits the unique factorisation

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

By Dedekind's Theorem[12], we have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[t]/(h_1^{e_1}) \oplus \cdots \oplus \mathbb{F}_p[t]/(h_r^{e_r})$$

[11] here we are abusing notation slightly, our trace is understood to be a linear map $\mathcal{O}_K/p\mathcal{O}_K \to \mathbb{Z}/p\mathbb{Z}$.

[12] needs clarification: isn't Dedekind's only applicable when there exists a power basis for the ring of integers?

where $h_1, \ldots, h_r \in \mathbb{F}_p[t]$ are distinct irreducible polynomials. We thus see that p ramifies in K if and only if at least one of the factors in the above decomposition is not a field. Then

$$\overline{T} = \begin{pmatrix} \overline{T}_1 & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & \overline{T}_r \end{pmatrix}$$

where $\overline{T}_i$ is the trace pairing

$$T_i : \mathbb{F}_p[t]/(h_i^{e_i}) \times \mathbb{F}_p[t]/(h_i^{e_i}) \to \mathbb{F}_p$$

Now suppose, without loss of generality, that $e_1 \geq 2$ and all other $e_i = 1$. It suffices to prove that $\det(T_i) = 0$ and $\det(T_i) \neq 0$ for all $i \neq 1$.

For the first case, note that $\mathbb{F}_p[t]/(h_i)$ is a finite field. Label it k with $[k : \mathbb{F}_p] = \deg h_i = n$. Recall that any finite field is perfect and thus $k/\mathbb{F}_p$ is a finite separable extension. By the primitive element theorem, there exists an $x \in k$ such that $k = \mathbb{F}_p(x)$. Then $1, x, \ldots, x^{n-1}$ is an $\mathbb{F}_p$-basis for k. The lm-entry for T_i is then given by

$$\mathrm{Tr}_{k/\mathbb{F}_p}(x^{l+m-2}) = \sum_q x_q^{l+m-2}$$

where the x_q are the conjugates of x. Then

$$T_i = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ \vdots & \cdots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{pmatrix}$$

This is a Vandermonde matrix with determinant $\det T_i = \prod_{r<s}(x_r - x_s)$. Recall that the conjugates of x are exactly the other elements of the basis. Hence $x_r \neq x_s$ for all $r < s$ and thus the determinant is non-zero. This proves the first case.

For the second case, choose $y \in (h_1) \pmod{(h_1)^{e_1}}$ such that $y \neq 0$. We may extend y to an $\mathbb{F}_p$-basis of $\mathbb{F}_p[t]/(h_i^{e_1})$.[13] Note that $y^{e_1} = 0$ so every xy is nilpotent. So the trace of xy is equal to 0 for all x. hence in $\overline{T}_1$, there is a row of zeroes which is the same as $\det T_i = 0$ and we are done. $\square$

Corollary 6.3. *Let K be a number field. Then there are only finitely many primes that ramify in K. In particular, at least one prime ramifies in K.*

Proof. Let Δ_K be the discriminant of K. The primes that ramify in K are exactly the prime divisors of Δ_K. By the Hermite-Minkowski Theorem, we have $|\Delta_K| > 1$. From this we conclude two things. $\Delta_K \neq 0$ which means only finitely many primes can ramify in K. Secondly, Δ_K must have at least one prime divisor and thus at least one prime ramifies in K. $\square$

7 Units of $\mathcal{O}_K$

Let K be a number field. We denote the multiplicative group of units of K as U_K.

[13] it is indeed a vector space, we do not need to worry that it is not a field.

Lemma 7.1. *Let K be a number field and $\mu \in \mathcal{O}_K$ a root of unity. Then μ is a unit. In particular, the set of all roots of unity in $\mathcal{O}_K$ is a subgroup of U_K, which we denote μ_K.*

Proof. Let μ be a root of unity. Then $\mu^n = 1$ for some $n \in \mathbb{N}$. Hence μ is a root of the polynomial $X^n - 1$ which is monic with integer coefficients. Thus $\mu \in \mathcal{O}_K$.

1 is clearly a root of unity itself. Let μ, ν be two roots of unity. Then there exists, $m, n \in \mathbb{N}$ such that $\mu^m = 1$ and $\nu^n = 1$. Then $(\mu\nu)^{mn} = 1$ and so mn is a root of unity. Furthermore, given any root of unity μ such that $\mu^n = 1$, we have $\mu^{-n} = 1^{-1}$ and so $(\mu^{-1})^n = 1$ whence the inverse of μ is a root of unity. Hence the set of all roots of unity in U_K is a subgroup. □

Lemma 7.2. *Let K be a field and $G \subseteq K^\times$ a finite subgroup. Then K is cyclic and consists of roots of unity.*

Proof. Let n be the least common multiple of the orders of all elements of G. Then $x^n = 1$ for all $x \in G$. Since the polynomial $X^n - 1$ has at most n distinct roots in K, we have that $|G| \leq n$. Now at least one element of G must have order equal to n so $1, x, \ldots, x^{n-1}$ are n distinct elements in G so $|G| = n$ and is generated by x. □

Theorem 7.3 (Dirichlet's Unit Theorem)**.** *Let K be a number field of degree $n = r + 2s$. Then*

$$U_K \cong \mu_K \oplus \mathbb{Z}^{r+s-1}$$

and μ_K is cyclic.

Proof. Consider the logarithmic mapping

$$L : \mathcal{O}_K \backslash \{ 0 \} \to \mathbb{R}^{r+s}$$

Defined by

$$L(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_r(x)|, \ldots, 2\log|\sigma_{r+1}(x)|, \ldots, 2\log|\sigma_{r+s}(x)|)$$

First observe that the restriction of L to U_K is a homomorphism between the multiplicative group of $\mathcal{O}_K$ and the additive group of $\mathbb{R}^{r+s}$. By an abuse of notation, we will also call this restriction L. Furthermore, the image of U_K is contained in the hyperplane $W \subseteq \mathbb{R}$ given by

$$\sum_{i=1}^{r} x_i + \sum_{i=1}^{s} y_j = 0$$

Indeed, every $x \in U_K$ satisfies $\mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1$ so

$$1 = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \left(\prod_{i=1}^{s} |\sigma_i(x)| \right)^2$$

Passing to the logarithm on both sides shows that $L(x)$ is contained in W.

We first claim that for all compact subsets $B \subseteq W$, $B' = L^{-1}(B)$ is finite. Since B is bounded there exists an $a \in \mathbb{R}$ such that $a > 1$ and

$$\frac{1}{a} \leq |\sigma_i(x)| \leq a$$

for all $x \in B'$ and for all $i = 1, \ldots, r+s$. Hence the coefficients of the characteristic polynomial of x are bounded since they are exactly the elementary symmetric polynomials in the $\sigma_i(x)$. Furthermore, these coefficients are necessarily integers since $x \in \mathcal{O}_K$. Hence, given B, there are only finitely many possible characteristic polynomials meaning there are only finitely many possible x.

We next claim that $L(U_K)$ is discrete and $\ker L$ is finite. To prove this claim, we must first show that $L(U_K) \cap B$ is finite for every compact subset $B \subseteq W$. We know that $L^{-1}(B)$ is finite so $L(U_K) \cap B = L(L^{-1}(B))$ is also finite as desired. Furthermore, $\ker L = L^{-1}(\{0\})$. Now, $\{0\}$ is compact and contained is a subset of W so $\ker L$ is finite.

By Theorem 5.3, $L(U_K)$ is a finitely generated $\mathbb{Z}$-module of rank at most $m \leq r+s-1$.

We can summarise this in the following short exact sequence:

$$0 \longrightarrow \ker L \longrightarrow U_K \longrightarrow L(U_K) \longrightarrow 0$$

so that $U_K / \ker L \cong L(U_K) \cong \mathbb{Z}^m$ for some $m \leq r+s-1$.

We now claim that $\ker L = \mu_K$ and is cyclic. It is easy to see that $\ker L$ is the set of all elements of U_K that have finite order. Indeed, since $\ker L$ is finite, any $x \in H$ must have finite order. Conversely, suppose that $x \in U_K \backslash \ker L$ has finite order. Then $L(x) \neq 0$. But x has finite order so there exists a non-zero natural number m such that $x^m = 1$ and $0 = L(1) = L(x^m) = mL(x) \neq 0$ which is a contradiction. It then easily follows that $\ker L = \mu_K$. Furthermore, Lemma 7.2 guarantees that this group is infact cyclic.

We thus see that $U_K \cong \mu_K \oplus \mathbb{Z}^m$ for some $m \leq r+s-1$. To finally prove the theorem, we need to show that $m = r+s-1$. We shall only prove this in the real quadratic case where $r = 2$ and $s = 0$. In this case, we need to prove that there exists a non-trivial unit.

Let Δ_K be the discriminant of K and σ the canonical embedding of K. Set $a = |\Delta_K|^{1/2}$. For all $l_1 > 0$, let l_2 be such that $l_1 l_2 = a$. Consider the box

$$B_l = \{ (y_1, y_2) \in \mathbb{R}^2 \mid |y_i| \leq l_i \}$$

Then B_l is clearly symmetric, convex and compact with volume given by $\mathrm{vol}(B_l) = 4 l_1 l_2 = 4a = 2^n \operatorname{covol}(\sigma(\mathcal{O}_K))$. By Minkowski's Convex Body Theorem, there exists a non-zero $x \in B_l \cap \sigma(\mathcal{O}_K)$. In other words, there exists a non-zero $x \in \mathcal{O}_K$ such that $|\sigma_1(x)| \leq l_1$ and $|\sigma_2(x)| \leq l_2$. Observe that

$$|\operatorname{N}_{K/\mathbb{Q}}(x)| = |\sigma_1(x)\sigma_2(x)| \leq l_1 l_2 = a$$

Now let $l_1 \to 0^+$. Then there exist infinitely many $x_1, x_2, \dots \in \mathcal{O}_K$ such that $|\sigma_1(x_k)| \to 0$. Hence it is clear that there are infinitely many distinct x_k satisfying $|\operatorname{N}_{K/\mathbb{Q}}(x_k)| \leq a$. Recall that $x_k \in \mathcal{O}_K$ is an algebraic integer so the norm must be a rational integer. Hence there are only finitely many choices for such a norm. Now recall that $N((x)) = |\operatorname{N}_{K/\mathbb{Q}}(x)|$. Thus there are only finitely many choices for $N((x_k))$. We must therefore have that $(x_k) = (x_l)$ for some distinct x_k and x_l. But this is equivalent to x_k/x_l being a unit and we are done. $\square$