1. Number Fields

A number field is a finite extension of \( \mathbb{Q} \). To be more precise, we’ll begin with some review of field extensions and algebraic elements.

**Definition 1.1.** A complex number \( \alpha \in \mathbb{C} \) is algebraic if there exists \( p(x) \in \mathbb{Q}[x] \) such that \( p(\alpha) = 0 \).

Any algebraic element \( \alpha \) defines an ideal \( I_\alpha = \{ p \in \mathbb{Q}[x] \mid p(\alpha) = 0 \} \). Since \( \mathbb{Q} \) is a field, \( \mathbb{Q}[x] \) is a PID and so \( I_\alpha = (p) \) for some \( p \in I_\alpha \) (which must be irreducible). The unique monic polynomial that generates \( I_\alpha \) is called the minimal polynomial for \( \alpha \), which we’ll denote \( p_{\min, \alpha} \). We call the degree of an algebraic number \( \text{deg}(\alpha) := \text{deg}(p_{\min, \alpha}) \).

**Proposition 1.2.** The following are equivalent:

1. \( \alpha \) is algebraic.
2. \( [\mathbb{Q}[\alpha] : \mathbb{Q}] < \infty \).
3. \( \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) \).

*Proof:*

(1 \( \Rightarrow \) 2): If \( \alpha \) is algebraic and \( d = \text{deg}(\alpha) \), then \( \mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/I_\alpha \) is a finite dimensional \( \mathbb{Q} \) vector space with basis \( \{1, \alpha, ..., \alpha^{d-1}\} \). Therefore \( [\mathbb{Q}[\alpha] : \mathbb{Q}] = d < \infty \).

(1 \( \Rightarrow \) 3): Since \( p_{\min, \alpha} \) is irreducible, \( I_\alpha \) is a maximal ideal and so \( \mathbb{Q}[\alpha] \) is a field. Since it contains \( \alpha \), \( \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) \).

(3 \( \Rightarrow \) 1): The element \( \frac{1}{\alpha} \in \mathbb{Q}(\alpha) \) is also contained in \( \mathbb{Q}[\alpha] \), so \( \frac{1}{\alpha} = q(\alpha) \) for \( q \in \mathbb{Q}[\alpha] \). Then \( \alpha q(\alpha) - 1 = 0 \). Thus \( \alpha \) satisfies the polynomial \( xq(x) - 1 \).

(2 \( \Rightarrow \) 1): \( \mathbb{Q}[\alpha] \) being a finite vector space over \( \mathbb{Q} \) means that the elements \( \{\alpha^i\} \) for \( i \) sufficiently large must be mutually dependent. This induces a polynomial relation in \( \alpha \) with \( \mathbb{Q} \) coefficients, hence \( \alpha \) is algebraic.

\( \Box \)

*Remark 1.3.* If \( \alpha, \beta \) are algebraic, then it is easy to check that \( \alpha + \beta, \alpha \beta, \) and \( \alpha/\beta \) (the latter only when \( \beta \neq 0 \)) are also algebraic. The algebraic elements of \( \mathbb{C} \) therefore form a subfield of \( \mathbb{C} \).

**Definition 1.4.** If \( F \) is a field containing \( \mathbb{Q} \) and \( [F : \mathbb{Q}] < \infty \), then \( F \) is called a number field of degree \( n = [F : \mathbb{Q}] \).

*Remark 1.5.* For any number field \( F \), the primitive element theorem guarantees us a (not necessarily unique) element \( \alpha \in F \) such that \( F = \mathbb{Q}(\alpha) \).

**Definition 1.6.** For a number field \( F \), an embedding of \( F \) into \( \mathbb{C} \) is a homomorphism \( \phi : F \to \mathbb{C} \). An embedding is called real if \( \text{im}(\phi) \subset \mathbb{R} \) and complex otherwise.

Given the finiteness of \( F \) as an extension, a natural question to ask about embeddings is how many there are. We know that, if \( \phi \) is a complex embedding, then so is its complex conjugate \( \overline{\phi} \). Thus the number of embeddings must be of the form \( r_1 + 2r_2 \), where \( r_1 \) is the number of real embeddings and \( 2r_2 \) is the number of complex embeddings.

**Corollary 1.7.** For a number field \( F \) of degree \( n \), there are exactly \( n \) distinct embeddings.

*Proof:*
Fix a primitive element $\alpha$, so that $F = \mathbb{Q}(\alpha)$. Any homomorphism $\phi : F \to \mathbb{C}$ is determined by the image of $\alpha$. Since $F \cong \phi(F) \cong \mathbb{Q}(\phi(\alpha)) \cong \mathbb{Q}[x]/(p_{\min,\phi(\alpha)})$ and $F \cong \mathbb{Q}[x]/(p_{\min,\alpha})$, the minimal polynomials of $\alpha$ and $\phi(\alpha)$ are the same. Therefore $\phi(\alpha)$ must be another root of $p_{\min,\alpha}$. Since it has no repeated roots, there are exactly $n$ choices of roots in $\mathbb{C}$.

\[ \square \]

1.1 Norm, Trace, and Discriminant

For $\alpha \in F$, consider the map $m_{\alpha} : F \to F$ given by $x \mapsto \alpha x$. This is a $\mathbb{Q}$ linear map, so it has a trace and a determinant. These are used to define the norm and trace of an element:

**Definition 1.8.** Given $\alpha \in F$, the **trace** of $\alpha$ is $\text{tr}(m_{\alpha})$ and is denoted $\text{tr}_{F/\mathbb{Q}}(\alpha)$. The **norm** of $\alpha$ is the determinant $\det(m_{\alpha})$ and is denoted $N_{F/\mathbb{Q}}(\alpha)$. We sometimes drop the “$F/\mathbb{Q}$" subscript when the number field is implicit.

**Remark 1.9.** Notice that basic properties of trace and determinant extend to the field norm and trace: $\text{tr}(\alpha + \beta) = \text{tr}(\alpha) + \text{tr}(\beta)$ and $N(\alpha \beta) = N(\alpha)N(\beta)$.

**Proposition 1.10.** Let $\deg(F) = n$, and $\{\phi_1, ..., \phi_n\}$ be the distinct embeddings of $F$. Then for any $\alpha \in F$:

\[
\text{tr}_{F/\mathbb{Q}}(\alpha) = \sum_{i} \phi_i(\alpha) \\
N_{F/\mathbb{Q}}(\alpha) = \prod_{i} \phi_i(\alpha)
\]

**Proof:**

Consider the field $\mathbb{Q}(\alpha) \subset F$ and the map $m_{\alpha} : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$. Since the minimal polynomial $p_{m_{\alpha}}$ of $m_{\alpha}$ is $p_{\min,\alpha}$, which has no multiple roots, $m_{\alpha}$ is diagonalizable. The number of eigenvalues of $m_{\alpha}$ is the degree $m = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Then, if $\{\alpha_j\}$ are the roots of $p_{\min,\alpha}$:

\[
\text{tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \sum_{j=1}^{m} \alpha_j
\]

Note that every embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$ can be extended to $e = \deg(F/\mathbb{Q}(\alpha))$ embeddings $F \to \mathbb{C}$. Then, by the same reasoning as above, we have:

\[
\text{tr}_{F/\mathbb{Q}}(\alpha) = \sum_{j=1}^{m} e\alpha_j
\]

But since the image of $\phi_i$ must be a root of $p_{\min,\alpha}$, we get:

\[
\text{tr}_{F/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \phi(\alpha)
\]

The same can be done to show that the product formula.

\[ \square \]

The trace as a map $F \to \mathbb{Q}$ induces a pairing:

\[
\langle - , - \rangle_F : F \times F \to \mathbb{Q} \quad (x,y) \mapsto \text{tr}_{F/\mathbb{Q}}(xy)
\]

We sometimes drop the $F$ subscript on the brackets unless it is necessary.
Exercise 1.11. Show that $\langle -, - \rangle_F$ is a nondegenerate bilinear pairing.

Definition 1.12. Given $n$ elements $\alpha_1, \ldots, \alpha_n \in F$, the discriminant $\text{disc}(\alpha_1, \ldots, \alpha_n)$ is defined to be the determinant of the matrix $\langle \alpha_i, \alpha_j \rangle$.

There are several observations about the discriminant that will be useful:

1. The discriminant can be evaluated using the embeddings $\phi_k$:
   \[
   \text{disc}(\alpha_1, \ldots, \alpha_n) = \det(tr(\alpha_i \alpha_j)) = \det((\phi_k(\alpha_j))^T \phi_k(\alpha_j)) = \det(\phi_k(\alpha_j))^2
   \]

2. If $(\beta_1, \ldots, \beta_n) = M(\alpha_1, \ldots, \alpha_n)$ for some matrix $M$, then:
   \[
   \text{disc}(\beta_1, \ldots, \beta_n) = \det(M)^2 \text{disc}(\alpha_1, \ldots, \alpha_n)
   \]
   This follows from the previous observation.

3. For $F = \mathbb{Q}(\alpha)$ of degree $d$, the discriminant of the power basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is:
   \[
   \text{disc}(1, \alpha, \ldots, \alpha^{d-1}) = \det \begin{pmatrix}
   1 & \phi_1(\alpha) & \cdots & \phi_1(\alpha)^{d-1} \\
   \vdots & \vdots & \ddots & \vdots \\
   1 & \phi_d(\alpha) & \cdots & \phi_d(\alpha)^{d-1}
   \end{pmatrix}^2
   = \prod_{i<j}(\phi_i(\alpha) - \phi_j(\alpha))^2
   = N_{F/\mathbb{Q}}(p'_{\text{min}, \alpha}(\alpha))
   \]
   where we used the Vandermonde determinant formula.

Proposition 1.13. For $F/\mathbb{Q}$ a degree $d$ number field and $B = \{\alpha_1, \ldots, \alpha_d\}$ be a collection of elements in $F$. Then $B$ forms a basis of $F/\mathbb{Q}$ if and only if $\text{disc}(\alpha_1, \ldots, \alpha_d) \neq 0$.

Proof:

One direction is straight-forward: if they don’t form a basis, there is a linear relation on the $\alpha_i$. This extends to a linear relation on the columns of $\phi_i(\alpha_j)$, hence making the discriminant zero by the first observation above. For the other direction, it suffices to prove that the discriminant is nonzero for one basis (and then use observation 2). We choose the power basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$, which has discriminant:

\[
\text{disc}(1, \alpha, \ldots, \alpha^{d-1}) = \prod_{i<j}(\phi_i(\alpha) - \phi_j(\alpha))^2
\]

This is nonzero because otherwise $\phi_i(\alpha) = \phi_j(\alpha)$ for $j \neq i$, which would imply that $\phi_i$ and $\phi_j$ sent $\alpha$ to the same thing. 

\[\square\]

As an application, we construct the total embedding of $F$ into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where $r_1$ is the number of real embeddings and $r_2$ is the number of pairs of complex embeddings. For each pair of complex embeddings $(\phi_r, \bar{\phi}_r)$, we chose one representative to define a map:

$$
\Phi : F \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\
\alpha \mapsto (\phi_1(\alpha), \ldots, \phi_{r_1}(\alpha), \phi_{r_1+1}(\alpha), \ldots, \phi_{r_1+r_2}(\alpha))
$$

This is non-canonical, since we made arbitrary choices of representatives. The question we will answer is: what does the image of $\Phi$ look like?
Example 1.14. Consider $F = \mathbb{Q}(\alpha)$ for $\alpha^3 = 2$. Then there are two complex embeddings and one real. If $\omega$ is a (primitive) cube root of unity, then one example of $\Phi$ would be:

$$\Phi(\alpha) = \left(\sqrt[3]{2}, \omega\sqrt[3]{2}\right)$$

Theorem 1.15. For a number field $F$ of degree $d$:

- $\Phi$ maps a basis of $F/\mathbb{Q}$ to an $\mathbb{R}$ basis of $\mathbb{R}^r \times \mathbb{C}^s$.
- $\Phi$ is injective.
- $\text{im}(\Phi)$ is dense.

Proof:

We identify $\mathbb{C}$ with $\mathbb{R}^2$ in the usual way. This induces a map $\tilde{\Phi} : F \to \mathbb{R}^d$.

1. If $\omega_1, ..., \omega_d$ is a basis of $F/\mathbb{Q}$, then by multilinearity of the determinant:

$$\det \begin{pmatrix} \tilde{\Phi}(\omega_1) \\ \vdots \\ \tilde{\Phi}(\omega_d) \end{pmatrix} = (2i)^{-r_2} \det(\phi_i(\omega_j)) \neq 0$$

Therefore $\{\tilde{\Phi}(\omega_i)\}$ form a basis of $\mathbb{R}^d$, and hence so do $\{\Phi(\omega_i)\}$.

2. Suppose $\Phi(\beta) = 0$. Extend $\beta$ to a basis $B$ of $F/\mathbb{Q}$. Then $\Phi(B)$ cannot be a basis because it has at most $d - 1$ linearly independent elements. This contradicts 1).

3. We have shown that $\Phi(F)$ contains a $\mathbb{R}^r \times \mathbb{C}^s$ over $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, so too must $\Phi(F)$ be dense in $\mathbb{R}^r \times \mathbb{C}^s$.

\[\square\]

1.2 Algebraic Integers

Definition 1.16. For a number field $F$, an element $\alpha \in F$ is an algebraic integer (also called integral) if $p_{\min,\alpha}$ has integer coefficients.

Proposition 1.17. Let $\alpha$ be an element of a number field $F$. The following are equivalent:

1. $\alpha$ is integral.
2. There exists a monic $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
3. $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$ module.
4. There exists a finitely generated, nonzero $\mathbb{Z}$ module $M \subset F$ such that $\alpha M \subset M$.

Proof:

(1 $\Rightarrow$ 2): Take $f(x)$ to be the minimal polynomial of $\alpha$.

(2 $\Rightarrow$ 1): Write $f(x) = p_{\min,\alpha}(x)q(x)$ for $q(x) \in \mathbb{Q}[x]$ monic. If $r = \deg(p_{\min,\alpha})$ and $p_{\min,\alpha} = \sum_{j=1}^{r} \beta_j x^j$ then the coefficients of the $r$ highest degree terms $f(x)$ are $\{\beta_1, ..., \beta_r\}$. These are integers by assumption, so in fact $p_{\min,\alpha} \in \mathbb{Z}[x]$.

(1 $\Rightarrow$ 3): A basis for $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(p_{\min,\alpha})$ is $\{1, \alpha, ..., \alpha^{r-1}\}$, so it is finitely generated.

(3 $\Rightarrow$ 4): Take $M = \mathbb{Z}[\alpha]$. 


(4 \Rightarrow 2): \text{Take } x_1, \ldots, x_n \text{ as as generators for } M. \text{ Then since } \alpha x_i \in M \text{ for all } i, \text{ we have a matrix relation:}

\begin{pmatrix}
\alpha x_1 \\
\vdots \\
\alpha x_n
\end{pmatrix} = N
\begin{pmatrix}
x_1 \\
\vdots \\
x_n
\end{pmatrix}

\text{for } N \text{ a matrix with integer coefficients. Then } \det(\alpha I_n - N) = 0, \text{ and so the polynomial } \det(xI_n - N) \in \mathbb{Z}[x] \text{ satisfies } \alpha.

\square

\textbf{Remark 1.18.} \text{If } \alpha \text{ and } \beta \text{ are algebraic integers, then } \mathbb{Z}[\alpha + \beta] \subset \mathbb{Z}[\alpha] \oplus \mathbb{Z}[\beta] \text{ must be finitely generated as a } \mathbb{Z} \text{ module because each of } \mathbb{Z}[\alpha], \mathbb{Z}[\beta] \text{ is. Therefore, by above, } \alpha + \beta \text{ is an algebraic integer. For similar reasons, } \alpha \beta \text{ is also an algebraic integer. This proves:}

\textbf{Corollary 1.19.} \text{The set of all algebraic integers in } F \text{ (denoted } O_F \text{) is a subring.}

\textbf{Theorem 1.20.} \text{For a degree number field } F \text{ of degree } d, \text{ the ring of integers } O_F \text{ is a free } \mathbb{Z} \text{ module of rank } d.

\textbf{Proof:} \text{Let } \alpha_1, \ldots, \alpha_n \text{ be a basis of } F/\mathbb{Q}. \text{ For each } \alpha_i, \text{ there exists an integer } m \text{ such that } m \alpha_i \text{ is integral (just take } m \text{ to be the lcm of the denominators of the coefficients of } p_{\min, \alpha_i}. \text{ Thus, we can assume } \{\alpha_i\} \text{ are integral. This directly means that the rank of } O_F \text{ is at least } d. \text{ Now define the map } \varphi : F \rightarrow \mathbb{Q}^d \text{ by:}

\varphi(\beta) = ((\alpha_1, \beta), (\alpha_2, \beta), \ldots, (\alpha_d, \beta))

\text{Note that, for } x, y \in O_F, (x, y) \in \mathbb{Z} \text{ because the trace of an algebraic integer is again an algebraic integers in } \mathbb{Q} \text{ (i.e. they are in } \mathbb{Z}). \text{ Therefore } \varphi \text{ sends } O_F \text{ to } \mathbb{Z}^d. \text{ Further, this is an injection because the } (-, -) \text{ is nondegenerate. Therefore the rank of } O_F \text{ is at most } d. \text{ Since it clearly has no torsion, it must be free of rank exactly } d.

\square

\textbf{Example 1.21.} \text{Let } F \text{ be a quadratic number field (degree 2). Then there is a squarefree integer } d \text{ such that } F = \mathbb{Q}(\sqrt{d}). \text{ It is a standard exercise to show that the ring of integers } O_F \text{ depends on } d \text{ mod 4 in the following way:}

O_F = \begin{cases} 
\mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \text{ mod } 4 \\
\mathbb{Z}[(1 + \sqrt{d})/2] & d \equiv 1 \text{ mod } 4
\end{cases}

\textbf{Remark 1.22.} \text{Suppose } \alpha = (\alpha_1, \ldots, \alpha_n) \text{ and } \beta = (\beta_1, \ldots, \beta_n) \text{ are two bases of } O_F. \text{ Then there is an integer matrix } M \text{ such that } \alpha = M \beta. \text{ Since both } M \text{ and } M^{-1} \text{ are integer matrices, } \det(M) \in \mathbb{Z}^\times = \{\pm 1\}. \text{ In particular, the discriminants } \text{disc}(\alpha_1, \ldots, \alpha_n) \text{ and } \text{disc}(\beta_1, \ldots, \beta_n) \text{ are equal and define an invariant of } O_F. \text{ This is known as the discriminant of the number field, denoted } \text{disc}_F.

\textbf{Lemma 1.23.} \text{Any set of elements } \{\beta_1, \ldots, \beta_d\} \text{ in } O_F \text{ with squarefree discriminant form a basis of } O_F.

\textbf{Proof:} \text{If } \{\beta_i\} \text{ is not a basis, then writing } \beta = M \alpha \text{ for a basis } \alpha = \{\alpha_i\} \text{ requires } \det(M) \not\in \mathbb{Z}^\times; \text{ in particular, } 
\text{disc}(\beta_1, \ldots, \beta_n) = \det(M)^2 \text{disc}(\alpha_1, \ldots, \alpha_n) \text{ is not squarefree.}

\square

\text{One should keep in mind that this is not an if and only if statement.}
2. Dedekind Rings

In this section, we will define Dedekind rings in order to give a theory of ideal factorization in $O_F$. Recall these equivalent definitions of a ring $R$ being Noetherian:

1. Every ideal $I \subset R$ is finitely generated.
2. Every nonempty collection of ideals in $R$ has a maximal element.
3. Every ascending chain of ideals $I_0 \subset I_1 \subset I_2 \subset \ldots$ eventually stabilizes.

**Exercise 2.1.** Show that these are equivalent.

An important fact about Noetherian rings is the Hilbert Basis Theorem:

**Proposition 2.2.** If $R$ is a Noetherian ring, then so is $R[x]$ (and hence so is $R[x_1, \ldots, x_n]$).

**Definition 2.3.** Suppose $R \subset S$ are rings. We say $\alpha \in S$ is integral over $R$ if there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$.

**Definition 2.4.** A domain $R$ is integrally closed if every $\alpha \in \text{Frac}(R)$ that is integral is in $R$ itself.

**Example 2.5.** $\mathbb{Z}[\sqrt{5}]$ is not integrally closed because $\frac{\sqrt{5}+1}{2} \in \mathbb{Q}(\sqrt{5})$ is integral over $\mathbb{Z}$ (and hence over $\mathbb{Z}[\sqrt{5}]$) but is not in $\mathbb{Z}[\sqrt{5}]$.

**Definition 2.6.** The Krull dimension of a commutative ring $R$ is the length of the longest chain of nested prime ideals $p_0 \subset p_1 \subset p_2 \subset \ldots \subset p_n$ (length is determined by the number of inclusions, not the number of primes).

**Example 2.7.** The Krull dimension of $\mathbb{Z}$ is 1 and the Krull dimension of $\mathbb{Z}[x_1, \ldots, x_n]$ is $n + 1$. More generally, the Krull dimension of $R[x]$ is one more than the Krull dimension of $R$.

**Definition 2.8.** A commutative ring $R$ is Dedekind if:

1. $R$ is a Noetherian domain.
2. $R$ is integrally closed.
3. The Krull dimension of $R$ is $\leq 1$ (i.e. non-zero primes are maximal).

**Proposition 2.9.** The ring of integers $O_F$ of a number field $F$ is a Dedekind ring.

**Proof:**

Since $O_F$ is finitely generated as a $\mathbb{Z}$ module, any submodule (ideal) is also finitely generated. To show that it is integrally closed, let $\alpha \in F$ be integral over $O_F$. Then $O_F[\alpha]$ is a finite $O_F$ module, and hence also a finite $\mathbb{Z}$ module. Therefore the submodule $\mathbb{Z}[\alpha]$ is also finitely generated, which is true if and only if $\alpha$ is integral over $\mathbb{Z}$.

Finally, let $p \subset O_F$ be nonzero. Then $O_F/p$ is an integral domain. We claim that $p$ contains a nonzero integer $m$; indeed, for any nonzero $\alpha \in p$, the degree 0 coefficient of $p_{\text{min}, \alpha}$ is in $p$. Thus $(m) \subset p$ and we have a ring surjection:

$$O_F/(m) \twoheadrightarrow O_F/p$$

We note that, if $d$ is the rank of $O_F$, then $O_F/(m) \cong (\mathbb{Z}/m\mathbb{Z})^\oplus d$. In particular, it is finite. Therefore $O_F/p$ is finite. Any finite integral domain is a field, so $p$ must be maximal. Therefore the Krull dimension is $1$. 

\qed
2.1 Fractional Ideals and Unique Factorization

**Definition 2.10.** For a Dedekind ring $R$, let $F$ denote the fraction field of $R$. A fractional ideal $I$ of $R$ is an additive subgroup of $F$ such that $\exists \alpha \in F^*$ such that $\alpha I$ is a nonzero ideal of $R$.

**Proposition 2.11.** The following are true for a Dedekind ring $R$ with $F = \text{Frac}(R)$:

1. Every nonzero ideal of $R$ is fractional.
2. Every fractional ideal that is contained in $R$ is an ideal of $R$.
3. If $I, J$ are fractional ideals, then $IJ = \{\sum \alpha_i \beta_i \mid \alpha_i \in I, \beta_i \in J\}$ is a fractional ideal.
4. $\alpha R$ is a fractional ideal of $R$ for any nonzero $\alpha$.
5. For all fractional ideals $I$, the set $I^{-1} = \{\alpha \in F \mid \alpha I \subset R\}$ is a fractional ideal of $R$.

**Proof:**

1. Clearly $1 \cdot I \subset R$.
2. Let $I \subset R$ be fractional. Then it is easy to check that $I$ is an additive subgroup of $R$, so we need only verify that $rI \subset I$ for any $r \in R$. Let $\alpha \in F^*$ be such that $\alpha I$ is an ideal of $R$. Then $r\alpha I \subset \alpha I$. For any $a \in I$, this inclusion means that there exists $b \in I$ such that $ra = b\alpha$, and therefore:

$$\alpha(ra - b) = 0 \Rightarrow ra - b = 0 \Rightarrow ra = b.$$ 

Therefore $ra \in I$, so $rI \subset I$.
3. If $\alpha, \beta$ are such that $\alpha I \subset R$ and $\beta J \subset R$, then clearly $\alpha \beta IJ \subset R$.
4. If $\alpha \neq 0$, then $\alpha R$ is an additive subgroup of $F$ and $\alpha \alpha^{-1} R \subset R$, so it is also a fractional ideal.
5. Exercise.

The main fact that we will use about Dedekind rings is that they admit prime factorization, just like in the integers. In fact, we can think of Dedekind rings as a generalization of the integers (just as $O_F$ was the generalization of integers as a subring $\mathbb{Q}$).

**Theorem 2.12.** Let $R$ be a Dedekind ring. Then the set $\mathcal{I}(R) = \{\text{fractional ideals } I \subset \text{Frac}(R)\}$ is abelian group under multiplication. Moreover, $\mathcal{I}(R) \cong \bigoplus_{\text{primes } \mathfrak{p}} \mathbb{Z}$. In other words, every fractional ideal factors uniquely into a finite product of powers of prime ideals.

To prove this, we will need three lemmata:

**Lemma 2.13.** For $R$ a Noetherian ring, every ideal $I \subset R$ contains a product of prime ideals.

**Proof:**

Define the set:

$$S = \{I \subset R \mid I \text{ does not contain a product of prime ideals}\}$$

Assume that $S$ is nonempty; then there is a maximal element $I_0$ of $S$. Since $I_0$ cannot be a prime ideal, there exists $r, s \in R$ such that $rs \in I_0$ but $r, s \notin I_0$. Then $(I_0, r)$ and $(I_0, s)$ are ideals containing $I_0$ properly. Since $I_0$ was maximal in $S$, then $(I_0, r)$ and $(I_0, s)$ both contain a product of prime ideals. Then $(I_0, r)(I_0, s)$ also contains a product of prime ideals. However, by construction of $r$ and $s$, $(I_0, r)(I_0, s) \subset I_0$, and so $I_0$ contains a product of primes. This is a contradiction, so $S = \emptyset$.

**Lemma 2.14.** Let $R \subset F$ be a Dedekind ring contained in a field. For $I \subset R$ a proper ideal, then $\exists \lambda \in F \setminus R$ such that $\lambda I \subset R$.

**Proof:**
Let \( p \) be a prime ideal containing \( I \) and fix a nonzero element \( a \in I \). Then by the previous Lemma, the ideal it generates contains a product of primes: \( p_1p_2\cdots p_n \subseteq (a) \). Further, we can take \( n \) to be the minimal such length. Then we have \( p_1p_2\cdots p_n \subseteq p \), which means \( p = p_i \) for some \( i \). Without loss of generality, let \( i = 1 \). Since \( n \) was minimal, \( p_2\cdots p_n \) is no longer a subset of \( (a) \), and so we may take \( b \in p_2\cdots p_n \setminus (a) \). Then \( b/a \in F \setminus R \). Further, any \( x \in I \) is also in \( p_1 = p \), so \( bx \in p_1p_2\cdots p_n \subseteq (a) \). Therefore \( bx/a \in R \) and \( 1/a I \subseteq R \).

\[ \square \]

**Lemma 2.15.** If \( I \) is a fractional ideal of \( R \), then \( II^{-1} = R \).

**Proof:**

By definition of \( I^{-1} \), the fractional ideal \( II^{-1} \) is contained in \( R \), so it must be an ideal of \( R \) (part 2. of Proposition 2.11). Assume that \( II^{-1} \neq R \); then by the previous Lemma, there exists some \( \lambda \in F \setminus R \) such that \( \lambda II^{-1} \subseteq R \). If we rewrite \( \lambda II^{-1} \) as \( I \cdot \lambda I^{-1} \), we see that:

\[ \lambda I^{-1} \subseteq I^{-1} \Rightarrow \lambda^n I^{-1} \subseteq I^{-1} \ \forall n \]

Now pick \( y \in I \) nonzero, and notice that \( \lambda^n y I^{-1} \subseteq y I^{-1} \subseteq R \). Fixing \( x \in I^{-1} \) nonzero, this says that \( \lambda^n xy \in R \) and therefore \( \lambda^n \in R x^{-1} y^{-1} \). This means that \( R[\lambda] \subseteq R x^{-1} y^{-1} \). Since \( R \) is Noetherian, we must conclude that \( R[\lambda] \) is a finitely generated submodule, which is true if and only if \( \lambda \) is integral. But \( \lambda \notin R \) by choice, and \( R \) is integrally closed. This is a contradiction.

\[ \square \]

The proof of Theorem 2.12 will follow from the next few claims.

**Claim 1:** Every nonzero prime ideal of \( R \) is a finite product of prime ideals.

**Proof:**

Let \( S = \{ J \subseteq R \mid J \text{ is not a product of primes} \} \) and assume it is nonempty. Then it has a maximal element \( I \). Since \( I \) is not prime, it is not maximal so \( I \subseteq p \) properly for some prime \( p \). Consider \( Ip^{-1} \subseteq pp^{-1} = R \). This is a proper ideal of \( R \). By Lemma 2.14, there exists some \( \lambda \in F \setminus R \) such that \( \lambda \in p^{-1} \). Therefore \( p^{-1} \not\subseteq R \), which makes \( I \) a strict subset of \( Ip^{-1} \). Since \( I \) was maximal in \( S \), we must be able to write \( Ip^{-1} = p_1\cdots p_n \) for \( p_i \) prime. However, that would mean \( I = pp_1\cdots p_n \), which is a contradiction. Therefore \( S \) is empty.

\[ \square \]

**Claim 2:** The expression of an ideal as a product of primes is unique (up to reordering).

**Proof:**

Suppose \( p_1\cdots p_r = q_1\cdots q_s \) are two expressions of \( I \) (we can assume \( s \geq r \)). Then \( q_1\cdots q_s \subseteq p_1 \). Assume \( q_i \neq p_1 \) for all \( i \). Then choose \( x_i \in q_i \) with \( x_i \notin p_1 \). Then the product \( x_1\cdots x_s \) is in \( q_1\cdots q_s \), and hence is in \( p_1 \). This is a contradiction because \( p_1 \) is prime, so we must have \( q_i = p_1 \) for some \( i \). Without loss of generality \( i = 1 \), so:

\[ p_1\cdots p_r = p_1q_2\cdots q_s \]

We can multiply both sides by \( p_1^{-1} \) to eliminate \( p_1 \) from the product. Repeating this, we end up with \( R = q_{s-r}\cdots q_s \). Since prime ideals are proper, so we must have \( r = s \). Further, each \( q_i \) was equal to some \( p_j \).

\[ \square \]

**Claim 3:** The previous two claims apply to all fractional ideals (except possibly with negative powers).

**Proof:**
If $I$ is fractional, then let $a, b \in R$ be such that $\frac{a}{b} I \subset R$. Then we can write:

$$\frac{a}{b} I = (a)(b)^{-1} I = p_1 \cdots p_n$$

uniquely. Rearranging:

$$I = p_1 \cdots p_n \cdot (a)^{-1}(b)$$

Further, we can also write $(a)$ and $(b)$ as a product of primes, which in turn expresses $I$ as a product of (possibly negative) powers of primes. We leave verifying uniqueness as an exercise.

The following useful fact comes as a corollary to unique factorization:

**Corollary 2.16.** For ideals $I \subset J$ ideals of a Dedekind ring $R$, there exists an ideal $J' \subset R$ such that $I = J J'$. 

**Proof:**

Write $J = p_1^{e_1} \cdots p_n^{e_n}$. Since $I \subset J$, we have $I \subset p_1$ and therefore $I p_1^{-e_1} \subset J p_1^{-e_1} = p_2^{e_2} \cdots p_n^{e_n}$. Repeating this until we exhaust prime factors of $J$, we get $IJ^{-1} \subset R$. Since it is contained in $R$, it is an ideal so we can set $J' = IJ^{-1}$. 

As an application, let’s briefly return to the case of $R = \mathcal{O}_F$ for a number field $F$. Fix a prime ideal $p \subset \mathcal{O}_F$ and consider the diagram:

$$
\begin{array}{ccc}
F & \subset & \mathcal{O}_F & \subset & p \\
| & | & | & | & | \\
Q & \subset & \mathbb{Z} & \subset & p \cap \mathbb{Z}
\end{array}
$$

The ideal $p \cap \mathbb{Z}$ has a generator which must be prime, so we can write $(p) = p \cap \mathbb{Z}$ for a prime $p \in \mathbb{Z}$. In this situation, we say that “$p$ lies above $p$.” It is not hard to show that $\mathcal{O}_F/p$ is a finite integral domain\(^1\), and contains a copy of $\mathbb{Z}/p\mathbb{Z}$. Therefore $\mathcal{O}_F/p \cong \mathbb{F}_{p^n}$ for some $n$. Moreover, since $p \in p$, we have $p\mathcal{O}_F \subset p$. Corollary 2.16 then says that there is some $J$ such that $Jp = p\mathcal{O}_F$. In particular, $p$ divides $p\mathcal{O}_F$. Since $p\mathcal{O}_F$ has only finitely many prime factors, it follows that there can only be finitely many primes $p$ lying over $p$.

### 2.2 The Ideal Class Group

For a Dedekind ring $R$, we now have a well-defined group structure on the set of fractional ideals $\mathcal{I}(R)$. We can then define the group homomorphism:

$$\varphi : F^* \to \mathcal{I}(R)$$

$$\alpha \mapsto (\alpha)$$

The kernel of $\varphi$ is the group of units $R^*$. The cokernel of $\varphi$ is $\mathcal{I}(R)/\text{im}(\varphi)$. This is the *ideal class group* of $R$, denoted $\text{Cl}(R)$. It is the group of fractional ideals modulo principal fractional ideals. Thus, for any Dedekind ring $R$, we have the exact sequence:

$$0 \to R^* \to F^* \to \mathcal{I}(R) \to \text{Cl}(R) \to 0$$

The first fact we would like to show is that $\text{Cl}(R)$ is finite for any $R$. To start, it is easy to characterize when it is trivial:

**Proposition 2.17.** Let $R$ be a Dedekind ring. Then the following are equivalent:

1. $\text{Cl}(R) = \{1\}$.

\(^1\)Hint: show that $p$ contains a prime number $p$, hence $|\mathcal{O}_F/p| \leq |\mathcal{O}_F/p| < \infty$
2. Every fractional ideal is principal.

3. \( R \) is a PID.

4. \( R \) is a UFD.

Proof:

(1 \( \iff \) 2) This is by definition of \( \text{Cl}(R) \).

(2 \( \Rightarrow \) 3 \( \Rightarrow \) 4) Exercise.

(4 \( \Rightarrow \) 2) It suffices to show that every prime ideal is principal. Let \( p \) be prime and fix \( x \in p \) nonzero. Since \( R \) is a UFD, we can write \( x = \alpha_1\alpha_2 \cdots \alpha_n \) for \( \alpha_i \) irreducible. Since \( p \) is prime, \( \alpha_i \in p \) for some \( i \). Therefore \( (\alpha_i) \subseteq p \); but since \( \alpha_i \) is irreducible, \( (\alpha_i) \) is prime. Therefore Krull dimension \( \leq 1 \) implies that \( p = (\alpha_i) \).

\[ \square \]

**Theorem 2.18.** Let \( F \) be a number field with ring of integers \( O_F \). Then \( \text{Cl}(O_F) \) is a finite group.

Our strategy for proving this will be to define a norm on fractional ideals and show that this norm is bounded on \( \text{Cl}(O_F) \). We can define the norm of an ideal using the following fact: every ideal \( I \subseteq O_F \) is a product of prime ideals and \( O_F/p \) is finite for any prime, so the ring \( O_F/I \) is finite.

**Definition 2.19.** Let \( I \subseteq O_F \) be an ideal. Then the norm of \( I \) is \( N_{F/Q}(I) := |O_F/I| \).

**Remark 2.20.** Recall that for any \( x \in O_F \), the determinant of the multiplication map \( m_x : O_F \to O_F \) defines the norm of \( x \). However, \( |\det(m_x)| = |\text{coker}(m_x)| = |O_F/mO_F| = N_{F/Q}(mO_F) \). Thus the norm of an element coincides with the norm of the ideal that it generates.

**Lemma 2.21.** Let \( I, J \) be ideals of \( O_F \). Then \( N(IJ) = N(I)N(J) \).

Proof:

Since we have ideal factorization, it suffices to prove this when \( I \) is prime. Notice that:

\[ N(IJ) = |O_F/IJ| = |O_F/J||J/IJ| \]

Therefore we must show \( |I/IJ| = |O_F/I| \). We showed earlier that \( O_F/I \) is a finite field, and hence \( J/IJ \) is a vector space over that field. Pick \( \alpha \in J \setminus IJ \), and consider the linear map \( m_\alpha : O_F/I \to J/IJ \) given by \( x \mapsto \alpha x \). This is an injection and \( \text{im}(m_\alpha) = \alpha O_F + IJ \). Since \( \alpha O_F \subseteq J \), by Lemma 2.16 there exists an ideal \( J' \) such that \( \alpha O_F = JJ' \). Further:

\[ JJ' + IJ = J \iff J' + I = O_F \]

\[ \iff I \nsubseteq J' \]

\[ \iff J' \not\subseteq I \]

If we suppose \( J' \subseteq I \), then \( \alpha O_F = J' \subseteq I J \) and hence \( \alpha \in IJ \). This is a contradiction, so \( J' \not\subseteq I \).

By above, this then means \( JJ' + IJ = J \). Therefore \( \text{im}(m_\alpha) = \alpha O_F + IJ = J \), which makes \( m_\alpha \) a surjection. We have thus demonstrated an isomorphism \( I/IJ \cong O_F/I \) as (finite) vector spaces, which gives us the desired result.

\[ \square \]

We can now use the multiplicativity of the norm to define norms of fractional ideals:

\[ 1 = N(I/-1) = N(I)N(I^{-1}) \Rightarrow N(I^{-1}) = \frac{1}{N(I)}. \]

In other words, if \( I = \prod_i p_i^{e_i} \), then:

\[ N(I) = \prod_i N(p_i)^{e_i} \]
Proposition 2.22. For every number field \( F/\mathbb{Q} \), there exists an integer \( G \) such that for every ideal \( I \) there exists \( \alpha \in I \) with \( N(\alpha) \leq GN(I) \).

Proof:
Let \( \alpha_1, \ldots, \alpha_d \) be a basis of \( O_F \) and consider the set:
\[
S_m = \left\{ \sum x_i \alpha_i \mid x_i \in \mathbb{Z}, 0 \leq x_i \leq m \right\} \subseteq O_F
\]
This has size \((m + 1)^d\). Choose \( m \) such that \( m^d \leq N(I) < (m + 1)^d \) and let \( \pi : O_F \to O_F/I \) be the natural projection. We have chosen \( m \) such that \( \pi(S_m) = O_F/I \), so there must exist \( s_1, s_2 \in S_m \) such that \( \pi(s_1) = \pi(s_2) \). Let \( \alpha = s_1 - s_2 \in I \). Since the coefficients of \( s_1 \) and \( s_2 \) were positive and less than \( m \), we can write:
\[
\alpha = \sum x_i \alpha_i
\]
for \( |x_i| < m \). Now for each \( i \) define:
\[
G_i = \sum_{j=1}^{d} |\sigma_i(\alpha_j)|
\]
where \( \{\sigma_j\} \) are the distinct embeddings \( F \hookrightarrow \mathbb{C} \). We note that:
\[
|\sigma_j(\alpha)| \leq \sum_{j=1}^{d} |x_i||\sigma_j(\alpha_i)| \leq G_j m
\]
Therefore:
\[
N(\alpha) = \left| \prod_{j} \sigma_j(\alpha) \right| \leq \left( \prod_{j} G_j \right) m^d
\]
Since \( N(I) \geq m^d \), this inequality becomes \( N(\alpha) \leq GN(I) \) as desired.

This bound is the necessary tool in proving that \( Cl(O_F) \) is finite.

Proof (of Theorem 2.18):
We will first show that every ideal class \( c \in Cl(O_F) \) has a representing ideal with norm less than \( G \), then we will show that the set of ideals with norm less than \( G \) is finite. From this, it will follow that \( Cl(O_F) \) is finite.

Given \( c \in Cl(O_F) \), let \( I \) be an ideal representative of \( c^{-1} \). Then, by Proposition 2.22 there exists \( \alpha \in I \) such that \( N(\alpha) \leq GN(I) \). If we consider the ideal \( \alpha O_F \subseteq I \), by Corollary 2.16 there exists \( J \) such that \( \alpha O_F = J \). Further, \( J \) is a representative of \( c \) and:
\[
N(J) = N(\alpha)N(I)^{-1} \leq GN(I)N(I)^{-1} = G
\]
Therefore every ideal class has a representative with norm bounded by \( G \).

Now consider the set:
\[
B = \{ I \subseteq O_F \mid N(I) \leq G \}
\]
If we write any element of this set as $I = \prod_{i=1}^{t} p_i^{e_i}$, we have:

$$N(I) = \prod_{i=1}^{t} N(p_i)^{e_i} \leq G$$

We showed at the end of Section 2.1 that $N(p_i) = p_i^{m_i}$, where $p_i$ lies over $p_i$ and $m_i \geq 1$. Since there are finitely many primes less than or equal to $G$ and finitely many primes lying over a given prime ideal, there can only be finitely many products shown above. Since ideal factorization is unique, it then follows that $B$ is a finite set.  

$\square$
3. Geometry of Numbers

While the preceding discussion could provide a bound on the size of $\text{Cl}(O_F)$, it would be very crude and wouldn’t be very sensitive to the structure of the number field $F$. Introducing the language of geometry and lattices will, among other things, give us a better picture of the class group and better bounds on its size. To start, here are a few characteristics of finitely generated abelian groups that we will use:

**Theorem 3.1.** Let $G$ be a free abelian group of rank $n$ and $H$ be a subgroup. Then:

1. $H$ is free of rank $m \leq n$.
2. There is a basis $e_1, \ldots, e_n$ of $G$ and a set of positive integers $a_1|a_2|\ldots|a_m$ such that $\{a_1e_1, \ldots, a_me_m\}$ is a basis of $H$.

Using this, one can show that if $A$ is a finitely generated abelian group, it is isomorphic to $\mathbb{Z}^{r_1} \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z}$ for some $r$ and $m_i$. In particular, $A$ is finite if and only if its rank is 0.

**Corollary 3.2.** For an $n \times n$ matrix $M$ with entries in $\mathbb{Z}$ acting on $G = \mathbb{Z}^n$ with image $H = M(G)$, we have:

1. $G/H$ is finite if and only if $\det(M) \neq 0$.
2. If $\det(M) \neq 0$, then $|\det(M)| = [G : H]$.

3.1 Lattices

Lattices discrete subgroups of the Euclidean plane. Here we will develop some of the necessary tools associated to lattices to prove two of Minkowski’s important theorems about lattices and number fields. One of these says that given a lattice, a convex symmetric body of a certain volume must intersect it somewhere. The other uses this fact to place a tighter bound than the one in Proposition 2.22.

**Definition 3.3.** For a real vector space $V$ of finite dimension, a subset $L \subset V$ is a lattice if there exists $e_1, \ldots, e_n \in L$ such that:

1. $L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$.
2. $e_1, \ldots, e_n$ is a basis of $V$ over $\mathbb{R}$.

**Remark 3.4.** Some sources relax the second condition, allowing for lattices whose rank is less than the dimension of $V$. However, these are clearly just full rank lattices in a subspace of $V$.

**Example 3.5.** The standard example of lattice is $\mathbb{Z}^n \subset \mathbb{R}^n$. So too is $M(\mathbb{Z}^n)$ for a matrix $M$ of full rank. In fact, these are all of the lattices in $\mathbb{R}^n$.

**Proposition 3.6.** For a number field $F$, the ring of integers $O_F$ is a lattice in $F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (where $r_1$ is the number of real embeddings of $F$ and $r_2$ is half the number of complex embeddings).

**Proof:** Since $O_F$ is free of rank $d = \text{deg}(F/\mathbb{Q})$, we can write $O_F = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_d$ for $\{e_i\}$ a basis of $F/\mathbb{Q}$. By Theorem 1.15, the map $\Phi : F \to F \otimes_{\mathbb{Q}} \mathbb{R}$ sends $\{e_i\}$ to a basis of $F \otimes_{\mathbb{Q}} \mathbb{R}$.

**Example 3.7.** For $d$ squarefree, the ring of integers of $\mathbb{Q}(\sqrt{d})$, which we characterized in Example 1.21, is a lattice in $\mathbb{R}^2$ (or $\mathbb{C}$). The two possibilities of this lattice are shown in Figure 3.1.
Definition 3.8. A subgroup $G \subset V$ of a vector space $V$ is discrete if $\forall x \in G$, there exists $\epsilon > 0$ such that $B_\epsilon(x) \cap G = x$. It is co-compact if $V/G$ is compact.

Proposition 3.9. For $V$ a finite dimensional vector space over $\mathbb{R}$, $L \subset V$ a subgroup, the following are equivalent:

1. $L$ is a lattice.
2. $L$ is a discrete subgroup and is co-compact.
3. $L$ generates $V$ over $\mathbb{R}$ (i.e. $V = L \otimes_{\mathbb{Z}} \mathbb{R}$) and for every bounded set $B \subset V$, the intersection $B \cap L$ is finite.

Proof:

(1 $\Rightarrow$ 2) Since $L = \mathbb{Z} e_1 + \ldots + \mathbb{Z} e_n$, we have a surjection:

$$\{ \sum x_i e_i \mid 0 \leq x_i < 1 \} \rightarrow V/L$$

Since the left is compact, the right must also be compact. 

FINISH

Corollary 3.10. If $I$ is a fractional ideal of a number field $F$, then $I$ is a lattice in $F \otimes \mathbb{R}$.

Proof:

There exists $\alpha \in F$ such that $\alpha I \subset O_F$, and we can assume $\alpha \in \mathbb{Z}^+$ (exercise). Let $m \in \mathbb{Z} \cap \alpha I$, which we have shown is nonempty in the proof of Proposition 2.9. Then we have:

$$\frac{m}{\alpha} O_F \subset I \subset \frac{1}{\alpha} O_F.$$ 

Since $O_F$ is a lattice, so is $qO_F$ for any $q \in \mathbb{Q}^*$. Therefore the $\frac{m}{\alpha} O_F$ and $\frac{1}{\alpha} O_F$ are both lattices. Then since $\frac{m}{\alpha}$ is co-compact, so is $I$. Additionally, since $\frac{1}{n} O_F$ is discrete, so is $I$. Therefore $I$ is a lattice.
Definition 3.11. The fundamental domain of a lattice \( L \subset V \) is:

\[
\mathcal{D}_L = \left\{ \sum x_i e_i \mid 0 \leq x_i < 1 \right\}
\]

where \( \{e_i\} \) are a basis of \( L \).

Notice that the fundamental domain depends on the choice of basis. What doesn’t depend on this choice, however, is the volume of the fundamental domain. This is known as the covolume of \( L \). More precisely, if \( \mu \) is a Haar measure on \( V \), then \( \text{covol}(L) = \mu(\mathcal{D}_L) \). It is not hard to show that this is independent of basis choice of \( L \), since the determinant of an integral change of basis matrix must be \( \pm 1 \) (see Remark 1.22). Since we will only ever use lattices in \( \mathbb{R}^n \), from here out the measure chosen is the Lebesgue measure.

Lemma 3.12. Let \( M \) be a matrix with \( \mathbb{R} \) coefficients and let \( L = M(\mathbb{Z}^n) \). Then:

1. \( L \) is a lattice if and only if \( \det(M) \neq 0 \).
2. If \( L \) is a lattice, then \( \text{covol}(L) = |\det(M)| \).

Proof:
1. \( L \) is a lattice if and only if \( M \) takes the standard basis to another basis of \( \mathbb{R}^n \), which is true if and only if \( \det(M) \neq 0 \).
2. Let \( \{e_i\} \) be the standard basis of \( \mathbb{Z}^n \). Since \( L = \mathbb{Z}M(e_1) + ... + \mathbb{Z}M(e_n) \), the fundamental domain of \( L \) is the image of the fundamental domain of \( \mathbb{Z}^n \). Its volume is exactly the area spanned by the columns of \( M \), which is the determinant. \( \square \)

Lemma 3.13. If \( S \subset \mathbb{R}^n \) and \( L \subset \mathbb{R}^n \) is a lattice such that \( \mu(S) > \text{covol}(L) \), then there exist \( s_1 \neq s_2 \in S \) such that \( s_1 - s_2 \in L \).

Proof:
Let \( \pi : \mathbb{R}^n \to \mathbb{R}^n/L \) be the projection map. The volume of \( \mathbb{R}^n/L \) as a set in \( \mathbb{R}^n \) is \( \text{covol}(L) \). Note that if \( \pi|_S \) was an injection, then it would be area preserving, and therefore \( \mu(\pi(S)) = \mu(S) > \text{covol}(L) \). But a set in \( \mathbb{R}^n/L \) cannot have volume more than \( \text{covol}(L) \), so \( \pi \) must not have been injective on \( S \). The result follows. \( \square \)

Definition 3.14. A set \( C \subset \mathbb{R}^n \) is symmetric (with respect to the origin) if \( x \in C \iff -x \in C \). It is convex if for all \( x, y \in C \), \( (t - 1)x + ty \in C \) for \( t \in [0, 1] \).

Theorem 3.15 (Minkowski). Let \( L \) be a lattice in \( \mathbb{R}^n \) and let \( C \subset \mathbb{R}^n \) be measurable which is convex and symmetric. Suppose also that \( \mu(C) > 2^n \text{covol}(L) \). Then \( C \) contains a nonzero element of \( L \). Moreover, if \( C \) is compact, then \( \mu(C) \geq 2^n \text{covol}(L) \) is sufficient.

Proof:
Let \( S = \frac{1}{2}C \), so that \( \mu(S) = 2^{-n}\mu(C) > \text{covol}(L) \). By Lemma 3.13, there exist \( s_1, s_2 \in S \) such that \( s_1 - s_2 \in L \). Therefore there are \( c_1, c_2 \in C \) such that \( \frac{1}{2}(c_1 - c_2) \in L \). Since \( C \) is symmetric, \( -c_2 \in C \), so by convexity we get \( \frac{1}{2}c_1 + \frac{1}{2}(-c_2) \in C \). Therefore \( \frac{1}{2}(c_1 - c_2) \in L \cap C \) and is nonzero.

In the case where \( C \) is compact, fix \( \epsilon > 0 \) and define:

\[
C_\epsilon = \bigcup_{x \in C} B_\epsilon(x).
\]

Since \( C \) is compact, we can refine this to a finite cover \( C_\epsilon = \bigcup_{i=1}^N B_\epsilon(x_i) \). Then \( \mu(C_\epsilon) \leq \mu(C) + \epsilon M \) for some \( M \), so we can apply the previous case to \( C_\epsilon \). Letting \( \epsilon \) be sufficiently small, we can ensure that the
lattice point we found is contained in $C$.  

\[ \square \]

3.2 Geometric bounds on the class group

This section we will state and prove the second Minkowski theorem, which is a stronger version of Proposition 2.22 with an explicit value of $G$, which depends on the lattice structure of $O_F$.

**Proposition 3.16.** Let $F$ be a number field, with $r_1$ the number of real embeddings and $r_2$ the number of complex embeddings. Let $\Phi : F \to F \otimes \mathbb{Q} \mathbb{R}$ be the map defined in Theorem 1.12. Then:

1. $\text{covol}(O_F) = 2^{-r_2} |\text{disc}_F|^{-1/2}$.

2. For $I$ a fractional ideal, $\text{covol}(I) = N(I) \text{covol}(O_F)$.

**Proof:**

We identify $\mathbb{C}$ with $\mathbb{R}^2$ in the usual way. Let $\{\omega_1, ..., \omega_n\}$ be a basis of $O_F$ and let $\phi_1, ..., \phi_n$ be the real embeddings of $F$ and let $\phi_{r_1+1}, ..., \phi_{r_1+r_2}$ be distinct, non-conjugate embeddings of $F$. Define the matrix:

$$ M = \begin{pmatrix}
\phi_1(\omega_1) & \cdots & \phi_{r_1}(\omega_1) & \text{Re}\phi_{r_1+1}(\omega_1) & \text{Im}\phi_{r_1+1}(\omega_1) & \cdots & \text{Im}\phi_{r_1+r_2}(\omega_1) \\
\vdots & & \vdots & \vdots & \vdots \\
\phi_1(\omega_n) & \cdots & \phi_{r_1}(\omega_n) & \text{Re}\phi_{r_1+1}(\omega_n) & \text{Im}\phi_{r_1+1}(\omega_n) & \cdots & \text{Im}\phi_{r_1+r_2}(\omega_n)
\end{pmatrix} $$

Notice that $M(\mathbb{Z}^n) = \Phi(O_F)$. Applying Lemma 3.12 we get $\text{covol}(O_F) = |\det(M)| = 2^{-r_2} |\det(\phi_1(\omega_1))| = 2^{-r_2} |\text{disc}_F|^{-1/2}$. The last equality came from observation 1 about the discriminant in Section 1.1.

Now let $I$ be a fractional ideal. Then there exists a nonzero integer $m$ such that $mI \subset O_F$. Since $O_F/mI$ is finite, $mI$ is a subgroup of $O_F$ whose rank is the same as that of $O_F$. Then there exists an $n$ by $n$ integer matrix $A$ such that $A \omega$ is a basis for $mI$ (here $\omega = (\omega_1, ..., \omega_n)$ is a basis for $O_F$). By Corollary 3.3, $|O_F : mI| = |\det(A)|$. However, we also know that $|O_F : mI| = N(mI) = m^n N(I)$. By Lemma 3.12, the covolume of $mI$ is $|\det(AM)|$, where $M$ is the same as above. Therefore:

$$ \text{covol}(mI) = |\det(AM)| = |\det(A)||\det(M)| = m^n N(I) \text{covol}(O_F) $$

On the other hand, multiplying the lattice $I$ by $m$ has the effect of pulling out a factor $m^n$ in its covolume, so $\text{covol}(mI) = m^n \text{covol}(I)$. Therefore we get $\text{covol}(I) = N(I) \text{covol}(O_F)$ as desired.  

\[ \square \]

**Lemma 3.17.** For $r_1, r_2 \in \mathbb{Z}^+$ and $R \geq 0$, define the set:

$$ W(r_1, r_2, R) = \left\{ (x_1, ..., x_{r_1}, y_1, ..., y_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum_{i}^{r_1} |x_i| + 2 \sum_{i}^{r_2} |y_i| \leq R \right\} $$

Letting $n = r_1 + 2r_2$, then the volume of this set is $\mu(W(r_1, r_2, R)) = \frac{2r_1}{n} \left( \frac{2}{\pi} \right)^{r_2} R^n$.

**Proof:**

We will induct on $n$. There are two base cases: $r_1 = 1, r_2 = 0$ and $r_1 = 0, r_2 = 1$. In the former case, $W(1, 0, R) = \{ x \in \mathbb{R} \mid |x| \leq R \}$ has volume $2R = \frac{2}{\pi} \left( \frac{2}{\pi} \right)^0 R^1$. In the latter case, $W(0, 1, R) = \{ y \in \mathbb{C} \mid 2|y| \leq R \}$ has volume $\pi(R/2)^2 = \frac{\pi^2}{4} \left( \frac{2}{\pi} \right)^1 R^2$.

There are two inductive steps. The first is fixing $r_2$ and sending $r_1 \to r_1 + 1$. We are assuming the
formula is true for $n - 1 = r_1 + 2r_2$. In this case the volume is:

$$|W(r_1 + 1, r_2, R)| = \int_{-R}^{R} W(r_1, r_2, R - |t|)dt$$

$$= \int_{-R}^{0} W(r_1, r_2, R + t)dt + \int_{0}^{R} W(r_1, r_2, R - t)dt$$

$$= 2^{r_1} \left( \frac{\pi}{2} \right)^{r_2} \frac{1}{(n-1)!} \left[ \int_{-R}^{0} (R + t)^{n-1}dt + \int_{0}^{R} (R - t)^{n-1}dt \right]$$

$$= 2^{r_1+1} \left( \frac{\pi}{2} \right)^{r_2} \frac{R^n}{n!}.$$

The second case is $r_2 \mapsto r_2 + 1$ fixing $r_1$. Then:

$$|W(r_1, r_2 + 1, R)| = \int_{0\leq |z| \leq R/2} W(r_1, r_2, R - 2|z|)dz$$

$$= 2^{r_1} \left( \frac{\pi}{2} \right)^{r_2} \int_{0}^{R/2} \int_{0}^{2\pi} t(R - 2t)^{n-1}d\theta dt$$

$$= 2^{r_1} \left( \frac{\pi}{2} \right)^{r_2} \cdot 2\pi \int_{0}^{R/2} t(R - 2t)^{n-2}dt$$

$$= 2^{r_1} \left( \frac{\pi}{2} \right)^{r_2+1} \frac{R^n}{(n-1)n}.$$

Therefore the formula also holds for $n$. □

**Theorem 3.18** (Minkowski). Let $F/\mathbb{Q}$ be a degree $n$ number field, $r_1$ and $r_2$ be the number of real and non-conjugate embeddings of $F$ into $\mathbb{C}$. Then every ideal $I$ of $O_F$ contains an element $x \in I$ such that:

$$N(x) \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{r_2} |\text{disc}_F|^{1/2} N(I)$$

**Proof:**

Recall from Proposition 3.16 that $\text{covol}(I) = 2^{-r_2} N(I) |\text{disc}_F|^{1/2}$. Let $X(R) := W(r_1, r_2, R)$, and choose $R$ such that:

$$\mu(X(R)) = \frac{2^{r_1}}{n!} \left( \frac{\pi}{2} \right)^{r_2} R^n = 2^n \text{covol}(I)$$

$$= 2^n 2^{-r_2} N(I) |\text{disc}_F|^{1/2} \quad (3.2.1)$$

Since $X(R)$ is symmetric, convex, and compact, by Theorem 3.15 there exists a nonzero $x \in I \cap X(R)$. By virtue of being in $X(R)$, this element satisfies:

$$\sum_{i}^{n} |\phi_i(x)| \leq R$$

Combining this with the inequality of geometric and arithmetic means, we have:

$$|N(x)| = \left| \prod_{i} \phi_i(x) \right| \leq \left( \frac{\sum_{i}^{n} |\phi_i(x)|}{n} \right)^n \leq \frac{R^n}{n^n}.$$
Using equation \ref{equation:3.2.2} we get the desired inequality:

\[ N(x) \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^{r/2} N(I) |\text{disc}_F|^{1/2} \]

We are slightly abusing notation and thinking of \( I \) as the lattice \( \Phi(I) \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \).

\[ \square \]

Remark 3.19. As \( n \) grows, the two constant terms in front of the discriminant decrease monotonically. As a result, this bound gets tighter as the degree of \( F/\mathbb{Q} \) increases.