Lecture 19 (13.1)

Finally:

Proof of Thm 8.12

Existence of a factorization: Let \( I \) be the set of all ideals which do not have a factorization. Suppose, \( \emptyset \neq I \). Then by Zorn’s Lemma, \( I \) has a maximal element \( I \). Since \( I \neq \emptyset \), it is contained in a maximal ideal \( P \). Since \( R = \mathbb{P} \), we get:

\[ I \subseteq I P^{-1} \cap P P^{-1} \subseteq R. \]

By Lemma 8.14, \( I \neq I P^{-1} \) and \( P \neq P P^{-1} \). Since \( P \) is maximal and \( P P^{-1} \subseteq R \) is an ideal, we must have \( P P^{-1} = R \). Since \( I \neq \emptyset \), it cannot be a prime ideal, so \( I \neq P \), hence \( I P^{-1} \neq P P^{-1} \). Hence \( I \neq I P^{-1} \subseteq R \). By maximality of \( I \) in \( \emptyset \), we thus have \( I P^{-1} \subseteq \emptyset \), so \( I P^{-1} = P_1 \ldots P_r \Rightarrow I = I P^{-1} P = P_1 \ldots P_r P = \mathbb{P} \).

Uniqueness of factorization: Let \( I = P_1 \ldots P_r = Q_1 \ldots Q_s \) be two factorizations.

Then \( Q_1 \ldots Q_s \subseteq P_r \), so \( Q_i = P_j \) for some \( i \) (by general fact in proof of lemma 8.14), \( \deg P_j = 1 \). Since \( R \) is one-dimensional, \( Q_1 = P_1 \). Moreover, \( P_1 \neq P_1 P_2^{-1} \subseteq R \) by Lemma 8.14, so \( P_1 P_2^{-1} = R \) since \( P_1 \) is maximal. Multiplying the factorization by \( P_1 \) thus yields \( P_2 \ldots P_r = Q_2 \ldots Q_s \). Inductively we deduce that \( r = s \) and \( Q_i = P_i \) \( \forall i \) (after reordering appropriately).

\[ \square \]

Collecting equal prime ideals in a factorization, we see that any ideal \( I \) has a factorization \( I = P_1^{u_1} \ldots P_r^{u_r} \) with unique \( r \) prime ideals \( P_i \), and \( u_i > 0 \).

Example 8.15

Recall that in \( \mathbb{Z} [\sqrt{-5}] \subset \mathbb{Q} (\sqrt{-5}) \) we have:

\[ 21 = 3 \cdot 7 = (1 + 2 \sqrt{-5})(1 - 2 \sqrt{-5}) \]

Let:

\[
\begin{align*}
P_1 & := (3, 1 + \sqrt{-5}) & P_3 & := (7, 3 + \sqrt{-5}) \\
P_2 & := (3, 5 + \sqrt{-5}) & P_4 & := (7, 4 + \sqrt{-5})
\end{align*}
\]
Exercise: The $P_i$ are prime ideals and 
\[(3) = P_1^2, \quad (7) = P_2^3 P_4, \quad (1 + 2\sqrt{-5}) = P_2 P_4, \quad (1 - 2\sqrt{-5}) = P_1 P_3 \]

\[\Rightarrow (21) = \begin{cases} 
(3) (7) = P_1^2 P_2 P_3 P_4 \\
(1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = P_2 P_4 P_5 
\end{cases} \text{ same ideal factorization!} \]

**Theorem 8.16**
Every non-zero fractional ideal of $R$ is invertible.

**Proof:**
If $P$ is a non-zero prime ideal, then $P \neq PP^{-1} = R$ by Lemma 8.14, so $PP^{-1} = R$ since $P$ is maximal. Hence, $P$ is invertible. Then, by Thm 8.12, every non-zero ideal is invertible. If $I$ is fractional, then $rI \in R$ for some $r \neq 0$, hence $(rI)^{-1}$ is invertible. Have $(rI)^{-1} = r^{-1} I^{-1} \Rightarrow R = (rI)(rI)^{-1} = (rI)(r^{-1} I^{-1}) = I I^{-1} \Rightarrow I$ is invertible. \(\square\)

**Corollary 8.17**
Every fractional ideal $I$ has a factorization $I = P_1^{r_1} \cdots P_r^{r_r}$ with unique $r_i$ prime ideals $P_i$, and $r_i \in \mathbb{Z} \setminus \{0\}.$ \(\square\)

**Corollary 8.18**
$I_R$ is the free abelian group with basis the non-zero prime ideals of $R$.

**Remark 8.19**
Dedekind domains are precisely the integral domains in which every non-zero fractional ideal is invertible.

**Lemma 8.20**
The following are equivalent (R a Dedekind domain):
a) $R$ is factorial  
b) $R$ is a PID  
c) $C R$ is trivial (i.e. $I_R = P_R$)
Proof:

(a) $\Rightarrow$ (b): By factorization, it is sufficient to show that every prime ideal is principal.

Let $P \neq 0$ be a prime ideal. Choose $0 \neq p \in P$. Then $(p) = P$. Since $R$ is factorial, $P = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_i^{e_i}$ for prime elements $\mathcal{P}_i$ and a unit $e_i \Rightarrow (\mathcal{P}_i^{e_i}) = \mathcal{P}_i^{e_i} \subseteq P$. Let $\mathcal{P}_i = (\mathcal{P}_i)$, a prime ideal $\Rightarrow \mathcal{P}_i \subseteq P$ for some $i$ (by general fact in proof of Lemma 8.14), $\Rightarrow \mathcal{P}_i = P$ since $R$ one-dimensional $\Rightarrow P$ principal.

(b) $\Rightarrow$ (a): Clear.

(b) $\Rightarrow$ (c): Let $I$ be an invertible fractional ideal $\Rightarrow I \subseteq R$ a principal ideal $\Rightarrow I = aR$ for some $a \in R$ since $R$ PID $\Rightarrow I = \frac{a}{I}R$ is principal.

(c) $\Rightarrow$ (b): Let $I \subseteq R$ be a non-zero ideal

$\Rightarrow$ is invertible by Thm 8.16 $\Rightarrow I = I_R$

Since CLR is trivial, $I_R = P_R = I = xR$ for some $x \in K$.

Since $I \subseteq R$ $\Rightarrow x \in R \Rightarrow I$ principal.

Hence, the CLR measures how far a Dedekind domain is from being a PD. CLR can be arbitrarily complicated; every abelian group is the class group of some Dedekind domain!

8.3 Finiteness of the class group

Throughout, $R$ is the ring of integers in a number field $K$ (special case of Dedekind domain).

Here, the situation is much nicer: we will show that $\text{Cl}_K = \text{CLR}$ is finite!

This will follow from Minkowski's theory.

Another important ingredient is the ideal norm: recall from Lemma 5.23 that a non-zero ideal $I \subseteq R$ is a free $\mathbb{Z}$-module of the same dimension as $R$, hence $|I \cap R| = |R/I|_\mathbb{Z}$ is finite.
**Def 8.21**

\[ N(I) := [R : I] \]

is called the (ideal) norm of \( I \).

**Remark 8.22**

For a general Dedekind domain \( R \) it is not true that \( R/I \) is finite: take e.g. \( R = \mathbb{Q}[x] \) (a PID) and \( I = (x) \Rightarrow R/I \cong \mathbb{Q} \).

The terminology "norm" is justified by the following property.

**Lemma 8.23**

If \( O \supseteq a \in R \), then \( \left| N_{L|Q}(a) \right| = N(a) \).

**Proof:**

Let \( a_1, \ldots, a_n \) be a \( \mathbb{Z} \)-basis of \( R \). Then \( a_1 a_1, \ldots, a_n a_n \) is a \( \mathbb{Z} \)-basis of \( (a) \).

Write \( a a_i = \sum_j a_{ij} a_j \) and let \( A := (a_{ij}) \). Then \( \det(A) = N_{L|Q}(a) \)

by definition (see Def 2.28). Moreover, \( \left| \det(A) \right| = [R : I] \). \( \square \)

**Prop 8.24**

The ideal norm is multiplicative: \( N(\mathfrak{I} \mathfrak{J}) = N(\mathfrak{I}) N(\mathfrak{J}) \).

**Proof:**

By ideal factorization (\( R \) is Dedekind), it suffices to show that if \( \mathfrak{I} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n} \), then \( N(I) = N(\mathfrak{P}_1)^{\alpha_1} \cdots N(\mathfrak{P}_n)^{\alpha_n} \).

By the Chinese Remainder Theorem we have

\[ R/I \cong \prod_{i=1}^n R/\mathfrak{P}_i^{\alpha_i} \]

It is thus sufficient to show the claim for \( I = \mathfrak{P}^\mu \).

We have a chain

\[ \mathfrak{P} \supseteq \mathfrak{P}^2 \supseteq \cdots \]

Note that \( \mathfrak{P}^{\mu+1} = \mathfrak{P}^\mu \) by uniqueness of factorization.

Each quotient \( \mathfrak{P}^{\mu}/\mathfrak{P}^{\mu+1} \) is an \( R/\mathfrak{P} \)-vector space.
Claim: \( \dim_{R/p} \mathbb{P}^i/p^i \mathbb{H} = 1 \) (general fact for Dedekind domains)

Proof: Let \( x \in p^i / p^i \mathbb{H} \). Let \( \mathfrak{J} := (x) + p^i \mathbb{H} \). Then \( p^i \mathbb{H} \subset \mathfrak{J} \subset p^i \mathbb{H} \).

\[ \Rightarrow \mathfrak{J} = \mathbb{P}^i \mathbb{H} \Rightarrow \mathbb{P}^i \mathbb{J} = R \text{ since } \mathbb{P} \text{ maximal} \Rightarrow \mathfrak{J} = p^i \mathbb{H} \]

\( \Rightarrow x \text{ spans } p^i / p^i \mathbb{H} \).

So, \( p^i / p^i \mathbb{H} \cong R/p \) as \( R/p \)-vector spaces, hence

\[ N(p^i) = [R : p^i] = [R : \mathbb{P}] [\mathbb{P} : p^i] \cdots [p^i : p^i] = |R/p|^\mathfrak{P} = N(p)^\omega. \]

Multiplicativity allows us to extend the ideal norm to a group morphism

\[ N : \mathbb{I}_R \to \mathbb{R}_+^* \]