Lecture 19 (13.1.)

Finally:

Proof of Thm 8.12

Existence of a factorization: Let $\mathcal{M}$ be the set of all ideals which do not have a factorization. Suppose, $\mathcal{M} \neq \emptyset$. Then by Zorn's Lemma, $\mathcal{M}$ has a maximal element I. Since $I \neq R$, it is contained in a maximal ideal P. Since $R \subseteq P^{-1}$, we get:

$$I \subseteq IP^{-1} \subseteq PP^{-1} \subseteq R.$$

By Lemma 8.14, $I \neq IP^{-1}$ and $P \neq PP^{-1}$. Since P is maximal and $PP^{-1} \subseteq R$ is an ideal, we must have $PP^{-1} = R$. Since $I \in \mathcal{M}$, it cannot be a prime ideal, so $I \subsetneq P$, hence $IP^{-1} \neq PP^{-1} = R$. Hence $I \subsetneq IP^{-1} \subsetneq R$. By maximality of I in $\mathcal{M}$, we thus have $IP^{-1} \notin \mathcal{M}$, so $IP^{-1} = P_1 \cdot \ldots \cdot P_r \Rightarrow I = IP^{-1}P = P_1 \cdot \ldots \cdot P_r \cdot P \Rightarrow I \notin \mathcal{M}$ ↯

Uniqueness of factorization: Let $I = P_1 \cdot \ldots \cdot P_r = Q_1 \cdot \ldots \cdot Q_s$ be two factorizations. Then $Q_1 \cdot \ldots \cdot Q_s \subseteq P_1$, so $Q_i \subseteq P_1$ for some i (by general fact in proof of Lemma 8.14). Wlog $i=1$. Since R is one-dimensional, $Q_1 = P_1$. Moreover, $P_1 \neq P_1P_1^{-1} \subseteq R$ by Lemma 8.14, so $P_1P_1^{-1} = R$ since P_1 is maximal. Multiplying the factorization by P_1^{-1} thus yields $P_2 \cdot \ldots \cdot P_r = Q_2 \cdot \ldots \cdot Q_s$. Inductively we deduce that $r=s$ and $Q_i = P_i$ $\forall i$ (after reordering appropriately).

□

Collecting equal prime ideals in a factorization, we see that any ideal I has a factorization $I = P_1^{v_1} \cdots P_r^{v_r}$ with unique r, prime ideals P_i, and $v_i > 0$.

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

$$P_1 := (3, 1+\sqrt{-5}) \qquad P_3 := (7, 3+\sqrt{-5})$$
$$P_2 := (3, 5+\sqrt{-5}) \qquad P_4 := (7, 4+\sqrt{-5})$$

Exercise: The P_i are prime ideals and

$$(3) = P_1P_2\,,\quad (7) = P_3P_4\,,\quad (1+2\sqrt{-5}) = P_2P_4,\quad (1-2\sqrt{-5}) = P_1P_3$$

$$\Rightarrow (21) = \begin{cases} (3)\cdot(7) = P_1P_2P_3P_4 \\ \\ (1+2\sqrt{-5})(1-2\sqrt{-5}) = P_2P_4P_1P_3 \end{cases} \text{ same ideal factorization!}$$

Thm 8.16

Every non-zero fractional ideal of R is invertible.

Proof:

If P is a non-zero prime ideal, then $P \neq PP^{-1} \subseteq R$ 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 $rI \subseteq R$ for some $r \neq 0$, hence (rI) is invertible. Have $(rI)^{-1} = r^{-1}I^{-1} \Rightarrow R = (rI)(rI)^{-1} = (rI)(r^{-1}I^{-1}) = II^{-1}$ $\Rightarrow I$ is invertible. $\square$

Corollary 8.17

Every fractional ideal I has a factorization $I = P_1^{\nu_1}\cdots P_r^{\nu_r}$ with unique r, prime ideals P_i, and $\nu_i \in \mathbb{Z}\setminus\{0\}$. $\square$

Corollary 8.18

I_R is the free abelian group with basis the non-zero prime ideals of R. $\square$

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) Cl_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 $(p) \subseteq P$. Since R is factorial, $p = \varepsilon \cdot \pi_1^{\nu_1} \cdots \pi_r^{\nu_r}$ for prime elements π_i and a unit ε. $\Rightarrow (p) = P_1^{\nu_1} \cdot \ldots \cdot P_r^{\nu_r} \subseteq P$ where $P_i := (\pi_i)$, a prime ideal $\Rightarrow P_i \subseteq P$ for some i (by general fact in proof of Lemma 8.14). $\Rightarrow P_i = P$ since R one-dimensional $\Rightarrow P$ principal.

$b \Rightarrow a$: Clear.

$b \Rightarrow c$: Let I be an invertible fractional ideal $\Rightarrow rI \subseteq R$ an ideal

$\Rightarrow rI = aR$ for some $a \in R$ since R PID

$\Rightarrow I = \frac{a}{r} R$ is principal.

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

$\Rightarrow$ is invertible by Thm 8.16

$\Rightarrow I \in \mathcal{I}_R$

Since Cl_R is trivial, $\mathcal{I}_R = \mathcal{P}_R \Rightarrow I = xR$ for some $x \in K$.

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

Hence, the Cl_R measures how far a Dedekind domain is from being a PID. Cl_R 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 L (special case of Dedekind domain). Here, the situation is much nicer: we will show that $Cl_L := Cl_R$ is <u>finite</u>!

This will follow from Minkowski 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 $[R : I] = |R/I|$ 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 $I = (X) \Rightarrow R/I \simeq \mathbb{Q}$.

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

Lemma 8.23

If $0 \neq a \in R$, then $|N_{L|\mathbb{Q}}(a)| = N((a))$.

Proof:

Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of R. Then $a\alpha_1, \dots, a\alpha_n$ is a $\mathbb{Z}$-basis of (a).

Write $a\alpha_i = \sum_j a_{ij}\alpha_j$ and let $A := (a_{ij})$. Then $\det(A) = N_{L|\mathbb{Q}}(a)$ by definition (see Def 2.28). Moreover, $|\det(A)| = [R:I]$. $\square$

Prop 8.24

The ideal norm is multiplicative: $N(IJ) = N(I)N(J)$.

Proof:

By ideal factorization (R is Dedekind), it suffices to show that if $I = P_1^{\nu_1} \cdots P_r^{\nu_r}$, then $N(I) = N(P_1)^{\nu_1} \cdots N(P_r)^{\nu_r}$.

By the Chinese Remainder Theorem we have

$$R/I \simeq \prod_{i=1}^{r} R/P_i^{\nu_i}.$$

It is thus sufficient to show the claim for $I = P^{\nu}$.

We have a chain

$$P \supseteq P^2 \supseteq \cdots$$

Note that $P^i \neq P^{i+1}$ by uniqueness of factorization.

Each quotient P^i/P^{i+1} is an R/P-vector space.

<u>Claim:</u> $\dim_{R/P} P^i/P^{i+1} = 1$ (general fact for Dedekind domains)

<u>Proof:</u> Let $x \in P^i \setminus P^{i+1}$. Let $J := (x) + P^{i+1}$. Then $P^{i+1} \subsetneq J \subseteq P^i$

$$\Rightarrow P = P^{-i}P^{i+1} \subsetneq P^{-i}J \Rightarrow P^{-i}J = R \text{ since } P \text{ maximal} \Rightarrow J = P^i$$

$\Rightarrow x$ spans P^i/P^{i+1}.

$\square$

So, $P^i/P^{i+1} \simeq R/P$ as R/P-vector spaces, hence

$$N(P^\nu) = [R : P^\nu] = [R:P][P:P^2]\cdots[P^{\nu-1}:P^\nu] = |R/P|^\nu = N(P)^\nu.$$

$\square$

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

$$N : I_R \longrightarrow \mathbb{R}_+^*$$