Lecture 18 (8.1.)

8. Ideal theory of rings of integers

Recall that the ring of integers in a number field is not necessarily factorial, e.g. the ring of integers in $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$ and

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

are two non-associate decompositions into irreducible elements.

Beautiful idea by Kummer: this defect is repaired when considering ideals instead of numbers and prime ideals instead of prime elements.

Note: "ideal" comes from "ideal number"!

Dedekind turned this into a powerful theory.

8.1 Fractional ideals

Ideals generalize numbers, fractional ideal generalize fractions of numbers.

Let R be a domain with fraction field K.

Def 8.1

A fractional ideal of R is an R-submodule I of K such that $rI \subseteq R$ for some non-zero $r \in R$.

Example 8.2

$\frac{1}{2}\mathbb{Z} \subset \mathbb{Q}$ is a fractional ideal.

Remark 8.3

Fractional ideals are not ideals in the usual sense (they are contained in K). Any ideal (in the usual sense) is obviously fractional; they are precisely the fractional ideals contained in R.

In the context of fractional ideals one sometimes says integral ideal to refer to ideals in the usual sense.

Lemma 8.4

Suppose that R is noetherian.
An R-submodule I of K is fractional iff it is finitely generated.
Any fractional ideal is of the form $\frac{1}{r}I$ for an ideal I.

Proof:
Suppose that I is fractional, so $rI \subseteq R$ for some $r \in R \Rightarrow rI$ an ideal in R.
Since R is noetherian, rI is finitely generated, so $rI = R\cdot\{x_1, \dots, x_n\}$.
Hence $I = R\cdot\{\frac{x_1}{r}, \dots, \frac{x_n}{r}\}$ is finitely generated. Moreover, $I = \frac{1}{r}\cdot R\{x_1, \dots, x_n\}$.
Conversely, suppose that I is finitely generated, so $I = R\cdot\{\frac{x_1}{r_1}, \dots, \frac{x_n}{r_n}\}$ with $x_i, r_i \in R$.
Taking $r := r_1 \cdot \dots \cdot r_n$, we get $rI \subseteq R \Rightarrow I$ is fractional. $\square$

Lemma 8.5

If I, J are fractional ideals, then so is

$$(I : J) := \{x \in K \mid xJ \subseteq I\}.$$

In particular,

$$I^{-1} := (R : I) = \{x \in K \mid xI \subseteq R\}$$

is fractional.

Proof:
First, suppose that $I, J \subseteq R$. Let $0 \neq r \in J$. If $x \in (I : J)$, then $xJ \subseteq I$
$\Rightarrow xr \in I \Rightarrow r(I : J) \subseteq R \Rightarrow (I : J)$ fractional.
n the general case let $r, s \in R$ be such that $rI \subseteq R$, $sJ \subseteq R$.
Then

$$(rsI : rsJ) = \{x \in K \mid xrsI \subseteq rsJ\} = \{x \in K \mid xI \subseteq J\} = (I : J)$$

Since $rsI, rsJ \subseteq R$, the above shows that $(rsI : rsJ) = (I : J)$ is fractional.

Def 8.6

A fractional ideal I is <u>invertible</u> if there is a fractional ideal J such that $IJ = R$.

Lemma 8.7

A fractional ideal I is invertible iff $I \cdot I^{-1} = R$.

Proof:

Suppose $IJ = R$. Then $yI \subseteq R \ \forall y \in J$, so $J \subseteq (R:I) = I^{-1}$.

$\Rightarrow R = IJ \subseteq I I^{-1} \subseteq R \Rightarrow I I^{-1} = R$.

$\square$

The set I_R of invertible fractional ideals is clearly an abelian group under multiplication, with identity element R.

Def 8.8

I_R is called the ideal group of R.

Lemma 8.9

Every non-zero principal fractional ideal $I = R \cdot x$, $x \in K$, is invertible with $I^{-1} = R \cdot x^{-1}$.

Proof:

Rx^{-1} is clearly a fractional ideal and $(Rx)(Rx^{-1}) = R$, so $(Rx)^{-1} = Rx^{-1}$.

$\square$

The non-zero principal fractional ideals form a subgroup P_R of I_R.

Def 8.10

The quotient $Cl_R := I_R / P_R$ is called the ideal class group of R and $h_R := |Cl_R|$ is called the class number of R.

So, $I = J$ in Cl_R iff IJ^{-1} is principal.

These are extremely important invariants of R.

Note that we have an exact sequence (im = ker in each position):

$$1 \longrightarrow R^* \longrightarrow K^* \longrightarrow I_R \longrightarrow Cl_R \longrightarrow 1$$

So, for the Kummer idea "elements ⇝ ideals", Cl_R measures how far away these two worlds are and R^* measures what we loose in this process.

To better understand Cl_R, we restrict to rings with a nice ideal theory.

8.2 Dedekind domains

From Corollary 3.32 and Thm 3.47 and Prop 5.21 we know that the ring $\mathcal{O}$ of integers in a number field L is of the following type.

Def 8.11

A Dedekind domain is an integral domain which is integrally closed, noetherian, and one-dimensional.
← every non-zero prime ideal is maximal

Note: A non-maximal order in a number field is not a Dedekind domain because it is not integrally closed.
We will show:

Thm 8.12

In a Dedekind domain R, every ideal I has a decomposition

$$I = P_1 \cdot \ldots \cdot P_r$$

into prime ideals P_i of R. This factorization is unique up to re-ordering of the factors. (Note: $0 = 0$ and R is the empty product).

The proof needs some preparation. Throughout, R is a Dedekind domain.

Lemma 8.13

For every non-zero ideal I of R there are non-zero prime ideals $P_1, \ldots, P_r$ such that $I \supseteq P_1 \cdot \ldots \cdot P_r$.

Proof:

Let $\mathcal{M}$ be the set of ideals I which do not have this property.
Suppose $\mathcal{M} \neq \emptyset$. Since R is noetherian, every chain in $\mathcal{M}$ becomes stationary and thus admits an upper bound. Hence, by Zorn's Lemma,

$\mathcal{M}$ contains a maximal element I. This cannot be a prime ideal since prime ideals obviously satisfy the claimed property. Hence, there are $b_1, b_2 \in R$ with $b_1 b_2 \in I$ but $b_1, b_2 \notin I$. Let $I_1 := (b_1) + I$ and $I_2 := (b_2) + I$. Then $I \subsetneq I_1, I_2$. Because of the maximality of I, we have $I_i \notin \mathcal{M}$, hence I_i contains a product of prime ideals. Since $I_1 I_2 \subseteq I$, also I contains a product of prime ideals, contradicting $I \in \mathcal{M}$. $\square$

Lemma 8.14

$IP^{-1} \neq I$ for any prime idea P and any non-zero ideal I.
(Note: we don't know (yet) if P is invertible, so cannot use $PP^{-1} = R$).

Proof:
If $P = 0$ then $P^{-1} = K$ and the claim holds, so can assume $P \neq 0$
We first show this for $I = R$, i.e. $P^{-1} \neq R$.
Let $0 \neq a \in P$. By Lemma 8.13 there are non-zero prime ideals $P_1, \ldots, P_r$ with

$P_1 \cdot \ldots \cdot P_r \subseteq (a) \subseteq P$. Let r be minimal with this property.

General fact: If a prime ideal P contains a product $I_1 \cdot \ldots \cdot I_r$ of ideals, then P contains one of the I_i.

Proof: Suppose $P \not\supseteq I_i$ $\forall i$. Then for each i there is $x_i \in I_i$, $x_i \notin P$.
Then $\prod x_i \in \prod I_i$ but $\prod x_i \notin P$ since P is prime. Hence $P \not\supseteq \prod I_i$. $\lightning$ $\square$

Hence, $P_i \subseteq P$ for some i, wlog $i = 1$. Since R is one-dimensional, $P_1 = P$ already.
Because of minimality of r, $P_2 \cdot \ldots \cdot P_r \not\subseteq (a)$. Hence, there is $b \in P_2 \cdot \ldots \cdot P_r$ with $b \notin (a)$, so $a^{-1} b \notin R$. On the other hand, $bP = bP_1 \in P_1 \cdot \ldots \cdot P_r \subseteq (a)$, so $a^{-1} b P \in R$, hence $a^{-1} b \in P^{-1}$. $\Rightarrow P^{-1} \neq R$.

Now, the general case. Let $I = R \cdot \{\alpha_1, \ldots, \alpha_n\}$. Suppose, $IP^{-1} = I$. Then for every $x \in P^{-1}$ we have

$$x \alpha_i = \sum_j a_{ij} \alpha_j \ , \quad a_{ij} \in R.$$

Hence, if $A := (x \delta_{ij} - a_{ij})$ and $\alpha := (\alpha_1, \ldots, \alpha_n)$, then $A \cdot \alpha^t = 0$.
Multiplication with the adjugate of A (see proof of Thm 2.27) yields

$$0 = \mathrm{adj}(A) \cdot A \cdot \alpha^t = \det(A)\alpha^t$$

$\Rightarrow \det(A)\alpha_i = 0 \;\forall i \Rightarrow \det(A) = 0$

$\Rightarrow$ x is a zero of $\det(X\delta_{ij} - a_{ij}) \in R[X] \Rightarrow x$ is integral over R

$\Rightarrow$ $x \in R$ since R is integrally closed.

$\Rightarrow P^{-1} \subseteq R$.

Since $P^{-1} \supseteq R$ by definition $\Rightarrow P^{-1} = R$ $\lightning$ to above. $\square$