9. Decomposition of ideals in Dedekind domains

Recall: a ring R is a Dedekind domain if 1) R is Noetherian int. domain, int. closed in its field of fract.

2) $\forall$ non-zero prime ideal in R is maximal.

Examples: $K[x]$, $\mathcal{O}_K$

We assume that R is a Dedekind domain with field of fractions K.

Def A fractional ideal is a finitely generated R-submodule of K.

Rem 1) $x_1, \dots, x_l \in K$. Then

$I = \{ \sum a_i x_i \mid a_i \in R \} \subset K$

a fract. ideal.

2) if $I \subset R$ is a fract. ideal then I is an ordinary ideal.

3) Assume $I = (x_1, \dots, x_l)$. Write

$x_i = z_i / w_i$ $z_i, w_i \in R$, let $w = \prod_i w_i$

then $w \cdot x_i \in R \Rightarrow w \cdot I \subset R$ an ideal. This means: $\forall$ fractional idea I $\exists$ an idea $J \subset R$ and $w \in R$ s.t. $I = \frac{1}{w} \cdot J$

Operations on fract. ideals

1) multiplication: I_1, I_2 - fract. ideals

$I_1 \cdot I_2$ = submodule of K generated by xy $\forall x \in I_1, y \in I_2$

If $I_1 = (x_1, \dots, x_n), I_2 = (y_1 \dots y_m)$

then $I_1 \cdot I_2 = (x_i y_j)_{\substack{i=1..n \\ j=1..m}}$

– fin. gen.

Note: $R \cdot I = I \Rightarrow R$ is neutral w.r.t. multiplication

2) inverse: assume $I \neq (0)$

define $I^{-1} = \{x \in K \mid xI \subset R\}$

this is an R-submodule of K:

$x_1, x_2 \in I^{-1}$, $a \in R$

$(x_1 + x_2) I = x_1 I + x_2 I \subset R$

$\Rightarrow x_1 + x_2 \in I^{-1}$

$(a x_1) \cdot I = a(x_1 I) \subset R$

$\Rightarrow a x_1 \in I^{-1}$

Why is I^{-1} fin. gen?

let $0 \neq y \in I$ then $y \cdot I^{-1} \subset R$

is an ideal $\Rightarrow$

$$y \cdot I^{-1} = (x_1, \ldots, x_n) \qquad x_i \in R$$

$\Rightarrow I^{-1} = \left(\frac{x_1}{y}, \ldots, \frac{x_n}{y}\right)$

$\Rightarrow I^{-1}$ is a fract. ideal.

<u>Def</u> Let $\mathcal{Y}(R)$ be the set of non-zero fract. ideals of R.

<u>Thm 9.1</u> $\mathcal{Y}(R)$ with multiplication and invers defined above is an abelian group.

<u>Lemma</u> Let $(0) \neq I \subset R$ be an ideal. Then $\exists$ non-zero prime ideals $p_i \subset R$, $i = 1 \ldots n$, s.t. $\prod_{i=1}^{n} p_i \subset I$

Proof $\mathcal{C}$ = the set of all non-zero ideals in R that do not satisfy the assertion of the Lemma.

If $\mathcal{C} \neq \emptyset$, then $\exists\ I \subset \mathcal{C}$ that is maximal in $\mathcal{C}$ (see the previous lecture)

I is not prime $\Rightarrow \exists\ x_1, x_2 \in R \setminus I$

$x_1 \cdot x_2 \in I$. Define $I_1 = (I, x_1)$

$I_2 = (I, x_2)$

$I \subsetneq I_1$, $I \subsetneq I_2$

$\Rightarrow I_1, I_2 \notin \mathcal{C} \Rightarrow \exists\ p_i, q_j \subset R$

prime ideals: $\prod_i p_i \subset I_1$

$\prod_j q_j \subset I_2$

$$I_1 \cdot I_2 = (I^2, x_1 \cdot I, x_2 \cdot I, \underbrace{x_1 \cdot x_2}_{\substack{\cap \\ I}}) \subset I$$

$$\Rightarrow \prod_i p_i \times \prod_j q_j \subset I$$

– contradicts the def. of $\mathcal{C}$

$\Rightarrow \mathcal{C} = \emptyset$

$\square$

Proof of thm. 9.1 mult. of fractional ideals is associative and commut (exercise)

R is the neutral element. We only need to check that any fract. ideal $I \in \mathcal{J}(R)$ is invertible: $I^{-1} \cdot I = R$

Step 1 Let $(0) \neq \mathfrak{p} \subset R$ prime ideal (in part., $\mathfrak{p}$ is maximal).

Need to show: $\mathfrak{p}^{-1} \cdot \mathfrak{p} = R$

Note: $\mathfrak{p} \subset R$ $\quad \mathfrak{p}^{-1} = \{x \in K \mid x \cdot \mathfrak{p} \subset R\}$

$\Rightarrow R \subset \mathfrak{p}^{-1}$; also $\mathfrak{p}^{-1} \cdot \mathfrak{p} \subset R$

Multiply $R \subset \mathfrak{p}^{-1}$ by $\mathfrak{p}$:

$$\mathfrak{p} \subset \mathfrak{p}^{-1} \cdot \mathfrak{p} \subset R$$

$\mathfrak{p}$ is maximal $\Rightarrow$ either $\mathfrak{p}^{-1} \cdot \mathfrak{p} = R$

or $\mathfrak{p} = \mathfrak{p}^{-1} \cdot \mathfrak{p}$

We need to exclude the case

$\mathfrak{p} = \mathfrak{p}^{-1} \cdot \mathfrak{p}$.

Choose $0 \neq b \in \mathfrak{p}$. Using the Lemma above find prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, s.t. $(0) \neq \mathfrak{p}_i$; $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subset (b) \subset \mathfrak{p}$ and n minimal possible.

One of $\mathfrak{p}_i \subset \mathfrak{p}$. Otherwise

$\exists\, a_i \in \mathfrak{p}_i \setminus \mathfrak{p} \quad \forall i = 1 \dots n$

$\prod a_i \in \prod \mathfrak{p}_i \subset \mathfrak{p}$ – impossible,

because $\mathfrak{p}$ is prime.

We may assume: $\mathfrak{p}_1 \subset \mathfrak{p} \Rightarrow \mathfrak{p}_1 = \mathfrak{p}$

By minimality of n $\quad \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n \not\subset (b)$

$\Rightarrow \exists\, a \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n \; : \; a \notin (b)$

Then $\underset{\substack{\parallel \\ a \cdot \mathfrak{p}}}{a \cdot \mathfrak{p}_1} \subset (b)$

$\Rightarrow \delta = a/b \in \mathfrak{p}^{-1}$ but $\delta \notin R$

By assumption $\delta \cdot \mathfrak{p} \subset \mathfrak{p}$

If $\mathfrak{p} = (x_1 \dots x_n)$ then

$\delta \cdot x_i = \sum a_{ij} x_j \qquad a_{ij} \in R$

Let $A = (a_{ij})$

$\det(A - \delta \cdot Id)$ annihilates x_i

(see Lemma in lecture 4)

K has no zero-divisors $\Rightarrow \det(A - \delta Id) = 0$

$\Rightarrow$ get an equation of integral depend.

for $\delta \Rightarrow \delta$ is int / R, but R is a Dedekind domain, so int. closed in $K \Rightarrow \delta \in R$ — contradiction.

<u>Step 2</u> Let $(0) \neq I \subset R$ an ideal

Need: $I^{-1} \cdot I = R$

$\mathcal{C}$ = set of non-zero ideals in R, s.t. $I^{-1} \cdot I \neq R$

If $\mathcal{C} \neq \emptyset$, then $\exists$ a maximal element $I \in \mathcal{C}$.

I is not prime by Step 1.

$\Rightarrow \exists\, \mathfrak{p} \neq (0)$ prime: $I \subset \mathfrak{p}$

as above: $R \subset \mathfrak{p}^{-1}$ multiply by I

$\Rightarrow \quad I \subset \mathfrak{p}^{-1} I \subset R$

An argument as in step 1 shows that $I \neq \mathfrak{p}^{-1} I \Rightarrow$ by maximality

$\mathfrak{p}^{-1} I \notin \mathcal{C}$

$\Rightarrow (\mathfrak{p}^{-1} I)^{-1} \cdot (\mathfrak{p}^{-1} I) = R$

$\Rightarrow (\mathfrak{p}^{-1} I)^{-1} \cdot \mathfrak{p}^{-1} \subset I^{-1}$

and $\quad R \subset I^{-1} I \subset R$

$\Rightarrow \quad I^{-1} \cdot I = R$

<u>Step 3</u> Let I be a fract. ideal

$\Rightarrow \exists x \in R, \quad J \subset R$ ideal, s.t.

$$I = \frac{1}{x} \cdot J$$

then $\quad I^{-1} = x \cdot J^{-1}$

$$\Rightarrow I \cdot I^{-1} = \frac{1}{x} \cdot J \cdot x \cdot J^{-1} = J \cdot J^{-1} \underset{\text{by Step 2}}{=} R$$

$\square$

<u>Thm. 9.2</u> Let R be a Dedekind domain. Any non-zero ideal $I \subset R$ can be represented as a product

$$I = p_1 \cdot \ldots \cdot p_n$$

where p_i are non-zero prime ideals; this expression is unique up to reordering of the factors.

<u>Proof</u> Let $\mathcal{C}$ = set of all non-zero ideals that are not products of primes. If $\mathcal{C} \neq \emptyset \Rightarrow \exists$ maximal $I \in \mathcal{C}$

I is not prime $\Rightarrow \exists$ a prime p

$$I \subset p \Rightarrow p^{-1} I \subset R$$

$\Rightarrow p^{-1} I$ is an ideal

as in the previous proof:

$I \neq p^{-1} I$ (otherwise multiply by $I^{-1} \Rightarrow R = p^{-1} \Rightarrow p = R$ contradict.)

So $I \subsetneq p^{-1} I \Rightarrow \exists\, p_1 \dots p_n$:

$$p^{-1} I = p_1 \cdot \ldots \cdot p_n$$

by maximality of I

$\Rightarrow I = p \cdot p_1 \cdot \ldots \cdot p_n$ — contradicts the def. of $\mathcal{C}$ $\Rightarrow \mathcal{C} = \emptyset$

$\Rightarrow$ all ideals are products of primes

Uniqueness.

Assume $I = p_1 \cdot \ldots \cdot p_m = \tilde{p}_1 \cdot \ldots \cdot \tilde{p}_n$ $(*)$

if $m = 0 \Rightarrow I = R \Rightarrow n = 0$

Check that p_1 is one of $\tilde{p}_i$

assume not; then $\exists\, a_i \in \tilde{p}_i \setminus p_1 \ \forall i$

$\Rightarrow \prod_{i=1}^{n} a_i \in I \setminus p_1$, because p_1 prime

— contradiction

$\Rightarrow \exists\ \tilde{p}_j = p_1$

Multiply both sides of (*)

by p_1^{-1}, go on by induction $\square$

<u>Thm. 9.2'</u> R- Dedekind domain. Any fract. ideal in $I \subset R$ can be written as

$$I = \prod p_i \Big/ \prod q_j$$

for some prime p_i and q_j, $\overset{\forall i,j}{p_i \neq q_j}$.

Uniqueness up to reordering the factors.

<u>Proof</u> exercise (deduce from thm 9.2) $\square$

<u>Thm 9.3.</u> (Chinese remainder thm.)

R is arbitrary ring, $I_i \subset R$ $i = 1 \dots n$ ideals, s.t. $\forall i \neq j$ $I_i + I_j = R$

Then

$$R \Big/ \prod_{i=1}^{n} I_i \simeq \prod_{i=1}^{n} R/I_i$$

isomorphic as rings.

Proof Step 1: the case $n=2$

Need: $R/_{I_1 I_2} \cong R/_{I_1} \times R/_{I_2}$

Consider the morph. of rings

$$\varphi: R \longrightarrow R/_{I_1} \times R/_{I_2}$$
$$x \longmapsto (x \bmod I_1,\ x \bmod I_2)$$

$\ker(\varphi) = \{x \in R \mid x \in I_1 \text{ and } x \in I_2\}$

$= I_1 \cap I_2 \supset I_1 \cdot I_2$

Note: $I_1 + I_2 = R \Rightarrow \exists\, a \in I_1,\ b \in I_2$

s.t. $a + b = 1$

$x \in I_1 \cap I_2 \Rightarrow x = x(a+b)$

$$= \underbrace{x \cdot a}_{\substack{\cap \\ I_1 \cdot I_2}} + \underbrace{x \cdot b}_{\substack{\cap \\ I_1 \cdot I_2}} \in I_1 \cdot I_2$$

$\Rightarrow \ker(\varphi) = I_1 \cdot I_2$.

Surjectivity of φ:

let $(x \bmod I_1,\ y \bmod I_2) \in R/_{I_1} \times R/_{I_2}$

$x, y \in R$. Let $z = bx + ay$

a, b as above; $\varphi(z) = ?$

$$z = (1-a)x + ay = x + a(y-x)$$
$$\equiv x \pmod{I_1}$$

analogously: $z \equiv y \pmod{I_2}$

$$\Rightarrow \varphi(z) = (x \bmod I_1,\ y \bmod I_2)$$

<u>Step 2</u> Induction on n:

Enough to prove:

$$R \Big/ \prod_{i=1}^{n} I_i \cong R/I_1 \times R \Big/ \prod_{i=2}^{n} I_i$$

This follows from the case $n=2$, if we show that $I_1 + \prod_{i=2}^{n} I_i = R$

Let $a_i + b_i = 1$, $a_i \in I_1$, $b_i \in I_i$, $i = 2 \ldots n$

Take $\prod_{i=2}^{n} (a_i + b_i) = 1$

$$\underbrace{(\ldots\ldots)}_{\in I_1} + \underbrace{b_2 \cdot \ldots \cdot b_n}_{\in \prod_{i=2}^{n} I_i} \overset{\shortparallel}{}$$

$\square$