7. Ideals and Dedekind domains

Reminder about ideals R – a ring, $R \neq 0$

Def 1) An additive subgroup $I \subset R$ is called an ideal, if $\forall x \in R, y \in I$ $xy \in I$ (shorter $R \cdot I \subset I$)

if $I \neq R$, then R/I is a ring.

2) An ideal $\mathfrak{p} \subset R$ is prime, if $\mathfrak{p} \neq R$ and $R/\mathfrak{p}$ is an integral domain.

3) A prime ideal $\mathfrak{m} \subset R$ is maximal, if $\forall$ ideal $I \subset R$ $\mathfrak{m} \subsetneq I \Rightarrow I = R$

Notation $x_1 \ldots x_n \in R$

$$(x_1, \ldots, x_n) = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in R \right\} \text{ – an ideal in } R.$$

Remarks 1) (0) is prime $\Leftrightarrow$ R is an integral dom.

2) $(x) = R \Leftrightarrow x \in R^{\times}$

3) a prime ideal $\mathfrak{m} \subset R$ is maximal $\Leftrightarrow$ $R/\mathfrak{m}$ is a field.

4) if $I \subsetneq R$ an ideal, then

$\exists$ a maximal ideal $\mathfrak{m} \subset R$, s.t.
$I \subset \mathfrak{m}$

(to prove this use Zorn's lemma)

<u>Operations on ideals</u> $I_1, I_2 \subset R$ ideals

1) $I_1 + I_2 = \{x + y \mid x \in I_1, y \in I_2\}$
is an ideal in R.

2) $I_1 \cap I_2$ = set-theoretic intersection
an ideal in R

3) $I_1 \cdot I_2$ = ideal generated by all
$x \cdot y$ for $x \in I_1$, $y \in I_2$

Note: $I_1 \cdot I_2 \subset I_1 \cap I_2$ (in general $\neq$)

Let $\varphi: R \longrightarrow S$ a morphism of rings

$I \subset R$, $J \subset S$ ideals

4) extension $I \cdot S$ = the ideal in S
generated by $\varphi(I)$

5) restriction $\varphi^{-1}(J)$ – an ideal in R
if φ is injective, we write
$R \cap J$ for $\varphi^{-1}(J)$

Note: $\mathfrak{p} \subset S$ is a prime ideal.
Then $\varphi^{-1}(\mathfrak{p})$ is prime

Proof $\varphi(1_R) = 1_S \notin \mathfrak{p} \Rightarrow 1_R \notin \varphi^{-1}(\mathfrak{p})$
$\Rightarrow \varphi^{-1}(\mathfrak{p}) \neq R$

$$R/\varphi^{-1}(\mathfrak{p}) \hookrightarrow S/\mathfrak{p}$$ an embedding

$S/\mathfrak{p}$ an int. dom. $\Rightarrow R/\varphi^{-1}(\mathfrak{p})$ also an int. domain $\square$

Examples 1) $R = K$ a field. Only (0) and K are ideals; (0) is maximal

2) $R = K[X]$ all ideals are principal
$I = (f)$ is prime $\Leftrightarrow$ either $f = 0$ or f is irreducible.
(f) is maximal $\Leftrightarrow$ f is irred

3) $R = K[X, Y]$ not PID:
$\underset{\text{maximal ideal}}{\mathfrak{m}} = (X, Y)$ $\quad R/\mathfrak{m} = K$

If $K = \overline{K}$, then any maximal ideal is of the form $(X-a, Y-b)$

for some $a, b \in K$

(Hilbert's Nullstellensatz)

There are more prime ideals in R

e.g. $\underset{\text{prime, not maximal}}{\mathfrak{p}=(f)}$ $f \in K[x,y]$ irreducible

4) $R = \mathcal{O}_K$, K - a number field

not all ideals are principal

$e_1, \dots, e_n$ — basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module.

Assume $\mathfrak{a} \subset \mathcal{O}_K$ an ideal, $\mathfrak{a} \neq (0)$, $\mathfrak{a} \neq \mathcal{O}_K$

$\mathfrak{a}$ is a subgroup of $\mathbb{Z}^n$

$\Rightarrow \mathfrak{a} \simeq \mathbb{Z}^m$ for some $m \leq n$

for $\underset{\neq 0}{a} \in \mathfrak{a}$ $\quad a e_1, \dots, a e_n \in \mathfrak{a}$

$a e_1, \dots, a e_n$ also form a basis of $K/\mathbb{Q}$

($x \in K$ $\quad \frac{x}{a} = \sum_{i=1}^n \alpha_i e_i$, $\quad \alpha_i \in \mathbb{Q}$,

then $\quad x = \sum_{i=1}^n \alpha_i (a e_i)$)

$\Rightarrow m = n$

$\Rightarrow \mathfrak{a}$ is a sublattice in $\mathcal{O}_K$

$\Rightarrow \mathcal{O}_K/\mathfrak{a}$ is finite

($\mathfrak{a} \simeq \mathbb{Z}^n \hookrightarrow \mathcal{O}_K \simeq \mathbb{Z}^n$ inclusion is of finite index)

Also note: $\mathbb{Z} \cap \mathfrak{a} \neq (0)$

Let $\underset{\neq (0)}{\mathfrak{p}} \subset \mathcal{O}_K$ be a prime ideal

Then $\mathfrak{p} \cap \mathbb{Z} = (p)$ a prime ideal in $\mathbb{Z}$

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathcal{O}_K \\ \cup & & \cup \\ \mathfrak{p}\cap\mathbb{Z} = (p) & \hookrightarrow & \mathfrak{p} \end{array} \quad \overset{\text{take quotients}}{\Longrightarrow} \quad \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \hookrightarrow & \mathcal{O}_K/\mathfrak{p} \\ \| & & \\ \mathbb{F}_p & & \end{array}$$

<u>Prop 7.1</u> If $\underset{\neq (0)}{\mathfrak{p}}$ is a prime ideal in $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$, for $q = p^m$, $(p) = \mathfrak{p} \cap \mathbb{Z}$

<u>Proof</u> $\mathcal{O}_K/\mathfrak{p}$ is a finite ring without zero-divisors $\Rightarrow$ it is a field

$0 \neq x \in \mathcal{O}_K/\mathfrak{p}$. Mult by x

defines a map $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$

This map is injective:

if $y_1, y_2 \in \mathcal{O}_K/\mathfrak{p}$, s.t.

$xy_1 = xy_2 \Rightarrow x\cdot(y_1 - y_2) = 0$

$\Rightarrow y_1 - y_2 = 0$

Injetive self-map of a finite set is surjective $\Rightarrow \exists\, y \in \mathcal{O}_K/\mathfrak{p}$, s.t.

$x\cdot y = 1 \Rightarrow x$ is inve~~rt~~ible

We have an emb. $\mathbb{F}_p \hookrightarrow \mathcal{O}_K/\mathfrak{p}$

$\Rightarrow \operatorname{char}(\mathcal{O}_K/\mathfrak{p}) = p$ $\square$

<u>Corollary</u> If $(0) \neq \mathfrak{p}$ a prime ideal in $\mathcal{O}_K$, then $\mathfrak{p}$ is maximal.

<u>Remark</u> R – a ring. The set of prime ideals in R is called the spectrum of R, denoted $\operatorname{Spec} R$

$\operatorname{Spec} R$ carries Zariski topology defined as follows:

Let $I \subset R$ arbitrary ideal

Define $V(I) = \{ p \in \operatorname{Spec} R \mid I \subset p \}$

to be the closed sets

One checks: $V((0)) = \operatorname{Spec} R$

$$V(R) = \emptyset$$

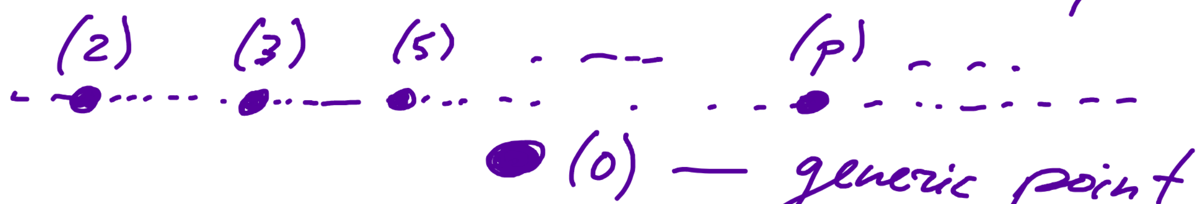
$$V(I_1 \cdot I_2) = V(I_1) \cup V(I_2)$$

$$V\Big(\sum_j I_j\Big) = \bigcap_j V(I_j)$$ for arbitrary family of ideals $\{I_j\}_j$

$\Rightarrow$ we get a topology on $\operatorname{Spec} R$.

<u>E.g.</u> $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), \ldots (p) \ldots\}$

(0) is not maximal, (p) is maximal for $p \neq 0$ prime



$V((p)) = \{(p)\} \Rightarrow (p)$ is a closed point of $\operatorname{Spec} \mathbb{Z}$

$\operatorname{Spec} \mathbb{Z}$ is the "arithmetic line"

<u>Analogy:</u> $\operatorname{Spec} \mathbb{C}[X]$

max. ideals are $(X - a)$ $a \in \mathbb{C}$

the only prime ideal that is not maximal is (0)

Also, analogous picture for $\operatorname{Spec} \mathcal{O}_K$ with K – arbitrary number field

Def 1) A ring R is Noetherian, if any ideal in R is finitely generated

2) An integral domain R is called a Dedekind domain, if:

a) R is Noetherian and integr. closed in its field of fractions

b) Every non-zero prime ideal in R is maximal.

Prop 7.2 $\mathcal{O}_K$ is a Dedekind dom.

Proof $\mathcal{O}_K$ is the int. closure of $\mathbb{Z}$ in K $\Rightarrow$ it is int. closed in K (corollary from Prop. 5.3)

$\mathcal{O}_K$ is Noetherian: $\mathfrak{a} \subset \mathcal{O}_K$ ideal,

$\mathfrak{a} \simeq \mathbb{Z}^n \Rightarrow$ fin. gen. even as an abelian group $\Rightarrow \mathfrak{a}$ is fin. gen as an ideal.

Any $(0) \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ is maximal (corollary from Prop. 7.1.) $\square$