

Lecture 3

Recall: poset of ideals
prime + max ideals

$R/\underline{I}$ int domain $\iff \underline{I}$ prime
field $\iff \underline{I}$ max

Examples K field $K[x_1, \dots, x_n]$

What are some primes?

What are some maximal ideals?

• Principal ideals ($\neq$) prime?

Suppose $h_1 h_2 = g f$ h_1, h_2 not multiples
of $f \Rightarrow f$ must factor by UF.

Recall exercise not all ideals are principal!
 $(x_1, x_2) = \{f x_1 + g x_2\}$

When not principal difficult to say
Algebraic geometry!

- What are maximal ideals?
Find surjective maps to fields!

ex

$$\phi_{a_1, \dots, a_n} : K[x_1, \dots, x_n] \rightarrow K$$

$\text{Ker } \phi_{a_1, \dots, a_n}$ is maximal!

$$= (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$$

Another example: $\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$

$$\begin{aligned} 1 &\mapsto 1 \\ x &\mapsto i \end{aligned}$$

$$\text{Ker } \phi = (x^2 + 1) \quad \frac{\mathbb{R}[x]}{(x^2 + 1)} \cong \mathbb{C} \Rightarrow \frac{\mathbb{R}[x]}{(x^2 + 1)} \text{ maximal.}$$

Def A ring is local if it has a unique maximal ideal (i.e. fields)

R/M is the "residue field"

Example All fields are local rings
 0 is unique max ideal.

Proposition i) If R is a ring and M ideal

i) if $\forall x \in R \setminus M$ is a unit in R then R is local and M it's unique maximal ideal.

ii) If M is maximal s.t. every elt of $R \setminus M$ is a unit then R is local.

Proof i) Any ideal $I \neq (1)$ consists of non units so every ideal is contained in M
 $\Rightarrow M$ max and R local $\square$.

ii) Let $x \in A - M$, since M is maximal
Ideal $(x) \not\subseteq M = \langle x, M \rangle = (1) \Rightarrow$
 $xy + m = 1$ for $y \in R, m \in M$.

$\Rightarrow xy \in 1 + M$ which by assumption
means xy is a unit. Claim follows
by i $\square$.

Examples 1) $I = (p^k) \subseteq \mathbb{Z}$ p prime

in $\mathbb{Z} : (p^k) \subseteq (p^{k-1}) \subseteq \dots \subseteq (p) \subseteq (1)$
no other ideals between (p^k) and (1) .

Correspondence under quotients $\Rightarrow$.

$$(0 + \underline{I}) \subseteq (p^{k-1} + \underline{I}) \subseteq \dots \subseteq (p + \underline{I})$$

only ideals in $\mathbb{Z}/I$.

$\Rightarrow (p+I)$ is unique max ideal $\mathbb{Z}_{(p)}$
is local.

2) $K[x]$ not local. Many max ideals
 $K[x]/(x^2)$ has unique max ideal $(x+I)$

in fact only ideals are $0 \subseteq (x+I) \subseteq (1)$

elements of $K[x]/(x^2) = \{a+bx\}$ with $x^2=0$.

units are $K \subseteq K[x]/(x^2)$ $K = R \setminus (x)$.

3) Power series ring $K[[x]]$. K field

$$f = a_0 + a_1x + \dots + a_nx^n + \dots$$

Who are the units? If $a_0 \neq 0 \exists g$
s.t. $gf = 1$.

Units $K[[x]] = K[[x]] \setminus (x) \Rightarrow (x)$ maximal
and $K[[x]]$ is local.

4) Ring of rational functions.

$$R(x) = \left\{ \frac{f}{g} \mid f, g \text{ polynomials}, g \neq 0 \right\} / \sim.$$

Consider $R \subseteq R(x)$ subring for which $g(0) \neq 0$. (functions which can be evaluated at 0).

Who are the units (?)

$$\left(\frac{f}{g} \right)^{-1} = \frac{g}{f} \quad \text{must have } f(0) \neq 0 \text{ to be in } R.$$

$\Rightarrow f \in R[x]$ not in max ideal (x) .

R is local and $M = \left\{ \frac{f}{g} \mid \frac{f(0)}{g(0)} = 0 \right\}$.

$R \setminus M = \text{units.}$

$$\phi_0 : R \longrightarrow R$$
$$\frac{f}{g} \longmapsto \frac{f(0)}{g(0)}$$

evaluation at 0.
is surjective with
kernel M .

Operations on Ideals

Recall I, J ideals in R . $\Rightarrow$

$I \cap J, I + J$ are ideals.

$I \cap J$ biggest ideal contained in both I, J .

$I + J$ smallest ideal containing both I, J .

These operations work over any arbitrary set of ideals of R :

$\bigcap_{I \in A} I$ ideal $A \subseteq \mathcal{I}(R)$

$\sum_{I \in A} I := \left\{ \sum_{\text{finite sums}} x_I \mid x_I \in I \right\}.$

Def. I ideal is finitely generated
if $I = \underbrace{(a_1) + (a_2) + \dots + (a_n)}_{\parallel (a_1, a_2, \dots, a_n)} \quad a_i \in R.$

Example. $(x, y) \subset \mathbb{Q}[x, y].$

$$(x, y) = \{ f \mid f(0, 0) = 0 \}.$$

meaning no constant term.

Solve exercise: (x, y) not principal

Lemma For any i, j

$$(a_1, \dots, a_n) = (a_1, \dots, a_{i-1}, a_i + b a_j, a_{i+1}, \dots, a_n)$$

Proof Short exercise.

Example 1) $R = \mathbb{Z}$.

$$n > m$$

$$n = k_1 m + r_1$$

$$m = k_2 r_1 + r_2$$

$$r_1 = k_3 r_2 + r_3$$

$\vdots$ Euclidean
algorithm

$$(n, m) = (n - k_1 m, m)$$

$$= (m, r_1).$$

$$= (r_1, r_2)$$

$$= (\gcd(n, m))$$

$$n, m \text{ coprime int} \iff (n, m) = 1.$$

2) $R = \mathbb{Q}[x]$. division algorithm

$$(f, g) = (\gcd(f, g)).$$

$\mathbb{Q}[x]$ is a principal ideal domain
iff no common factor

$$(f, g) = (f) + (g) = (1).$$

no common solutions to $f=0, g=0$.
over $\mathbb{Q}$ or $\mathbb{C}$.

Ideal product

$$I \cdot J = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J \right\}$$

note this may not be equal to

$$\{ a \cdot b \mid a \in I, b \in J \}$$

Not an ideal in general!

Example. Principal ideals behave nicely!

$$(a_1 \dots a_k) = (a_1) \cdot (a_2) \cdot \dots \cdot (a_k).$$

$$a_1 \dots a_k \in (a_1) \dots (a_k).$$

$$\begin{aligned} \text{Converse: } (a_1) \cdot \dots \cdot (a_k) &= \left\{ \sum_{i=1}^n b_{i1} a_1 \dots b_{ik} a_k \right\} \\ &= \left\{ \sum_{i=1}^n b_{i1} \dots b_{ik} a_1 \dots a_k \right\} = \left\{ \left(\sum_{i=1}^n b_{i1} \dots b_{ik} \right) a_1 \dots a_k \right\} \\ &\subseteq (a_1 \dots a_k). \quad \square \end{aligned}$$

Example $S = \{ a \cdot b \mid a \in I, b \in J \}$ is not an ideal in general.

Need non-principal ideals!

$$\mathbb{R}[x, y] \supseteq (x, y) = I = J.$$

$$x^2, y^2 \in S \quad \text{but} \quad x^2 + y^2 \notin S.$$

since it does not factor.

Notice $\forall I_1, \dots, I_k$

$$I_1 \cdot \dots \cdot I_k \subseteq I_1 \cap \dots \cap I_k. \quad \text{since}$$

$$I_1 \cdot \dots \cdot I_k \subseteq R \cdot I_i = I_i \quad (\text{ideal})$$

Three ideal operations $\cap, +, \cdot$.

$(\mathcal{I}(R), +, \cdot)$ forms a semi-ring.
(both $+$, $\cdot$ are commutative)

$$(1) \cdot \underline{I} = \underline{I} \quad \text{mult identity}$$

$$(0) + \underline{I} = \underline{I} \quad \text{additive identity.}$$

$$\underline{I} + (\underline{J} + \underline{K}) = (\underline{I} + \underline{J}) + \underline{K} \quad \text{associative}$$

$$\underline{I} \cdot (\underline{J} \cdot \underline{K}) = (\underline{I} \cdot \underline{J}) \cdot \underline{K}$$

$$(0) \cdot \underline{I} = (0) \quad \text{annihilation}$$

$$\underline{I}(\underline{J} + \underline{K}) = \underline{I}\underline{J} + \underline{I}\underline{K} \quad \text{distributivity}$$

$$\underline{I} + \underline{I} = \underline{I} \quad + \text{ is } \underline{\text{idempotent}}.$$

⚠ union of ideals is not an ideal

$(2), (3) \subseteq \mathbb{Z} \quad (2) \cup (3) \text{ not ideal.}$

Def I, J are coprime if $I + J = (1)$

I, J coprime $\iff \exists a \in I, b \in J$ s.t.
 $a + b = 1$.

Proposition I, J coprime then

$$I \cap J = I \cdot J.$$

Proof Always have $I \cdot J \subseteq I \cap J$. since
 $I \cdot J \subseteq I$ and $I \cdot J \subseteq J$.

Other direction: Since $I + J = (1) \exists -$
 $a \in I, b \in J$ s.t. $a + b = 1 \Rightarrow$

$$x = x \cdot 1 = x(a + b) = xa + xb.$$

Since $x \in I \cap J$ $xa \in I \cdot J$ $xb \in I \cdot J$

$\Rightarrow x \in I \cdot J$ (closed under addition)
 $\square$.

Example. In $\mathbb{Z}$ $(n) (m)$ coprime

$\Leftrightarrow n, m$ coprime integers.

coprime $\Rightarrow \text{lcm}(n, m) = nm$

$$(n)(m) = (\text{lcm}(n, m)) = (nm) \\ = (n) \cap (m).$$