##Week 3##

we already defined ideals

↳ additive subrings that are closed under scaling

Properties of ideals

- trivial, proper, improper
- generators: ⇝ finitely generated
  ⇝ principle

Example 1: R is any ring

trivial ideal: $I = \{0\}$

improper ideal: $I = R$

Proposition: Suppose I is an ideal in a ring with unity

then TFAE:

① I is improper, i.e. $I = R$

② I contains a unit, i.e. there is a unit $u \in I$ (with multiplicative inverse)

③ $1 \in I$

proof ① ⇒ ② $I = R \Rightarrow 1 \in I$ which is a unit

② ⇒ ③ Suppose you have a unit

then u has an inverse element $u^{-1} \in R$

I ideal $\Rightarrow 1 = \underset{R}{u^{-1}} \cdot \underset{I}{u} \in I$

③ → ① Suppose $1 \in I$, take any $r \in R$, then $r = r \cdot 1$

and $r \cdot 1 \in I$ because I ideal

$\Rightarrow I = R$

Corrolary 1 (Roy's sadness corrolary)

Suppose F is a field and $I \subseteq F$ is an ideal

then I is trivial or improper

Corrolary 2: Suppose F is a field

then every homomorphism $\phi: F \to R$ where R is (nontrivial) ring

is injective

proof: $Ker(\phi)$ is an ideal so it's either trivial (⇒ injective)

or $Ker(\phi) = F$ (b/c $\phi(1_F) = 1_R$) so can't happen

Generators for ideals:

Suppose R is a commutative ring (w/ 1)

Let $A \subseteq R$ be any subset

Then the ideal generated by A is the smallest ideal in R that contains A

Notational options:

1: (A)

2: $\langle A \rangle$

3: RA

Given an ideal $I \subseteq R$, we say:

- I is <u>generated</u> by A if $I = (A)$
- I is <u>finitely generated</u> if $I = (A)$ for some finite set A
- I is principle if $I = (\{a\}) = (a)$ for an element $a \in R$

<u>FACTS</u> ① $(A) = \bigcap_{\substack{I \subseteq R : \text{ideal} \\ A \subseteq I}} I$

② $(A) = \left\{ \sum_{\text{finite}} r_i a_i : r_i \in R, a_i \in A \right\}$

Example 2: In $\mathbb{Z}$, all ideals $I \subseteq \mathbb{Z}$ are of the form

$$I = (n) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

$\Rightarrow$ all ideals principle

Example 3: in $\mathbb{Z}[x]$

$(2) = \{2p(x) : p(x) \in \mathbb{Z}[x]\} = 2\mathbb{Z}[x]$

$(2, x) = \{2p(x) + xq(x) : q(x), p(x) \in \mathbb{Z}[x]\}$

Example 2 (cont.) $(2, 6) = \{2k + 6m : k, m \in \mathbb{Z}\} = \{2(k + 3m) : k, m \in \mathbb{Z}\}$

$= (2)$

claim $(2, x)$ is <u>not</u> a principle ideal ($\Rightarrow$ not every ideal in $\mathbb{Z}[x]$ is principle)

first check $(2, x) = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}$

$= \{f(x) \in \mathbb{Z}[x] : f(0) \text{ is even } (\Leftrightarrow f(x) \text{ has an even constant term})\}$

$(f(x) : c_0 + c_1 x + \dots + c_n x^n \text{ where } c_0 \text{ is even})$

quick consequence: $(2, x)$ is proper, $1 \notin (2, x)$

Now suppose $(2, x)$ is principle $(2, x) = (g(x))$

then ① $2 \in (2, x) = (g(x)) \Rightarrow 2 = p(x) g(x)$ for some $p(x)$

Using degree, this implies $p(x), g(x)$ are constant

$g(x) = \pm 1$ or $g(x) = \pm 2$

If $g(x) = \pm 1$ are units ($\text{so } (g(x)) = R$), so no $g(x) = \pm 2$

Then $x \in (2,x) = (g(x)) \Rightarrow x = p(x)g(x) = \underbrace{p(x)(2\mathbb{Z})}_{x \text{ coefficient even}}$

so not possible

$\Rightarrow (2,x)$ is not principle

Prime and Maximal ideals

Theorem: For an ideal $I \subseteq R$

properties of $I \leftrightarrow$ properties of R/I

Recall: For each ideal $I \subseteq R$ we have a "natural projection"

$$\pi : R \to R/I$$
$$r \mapsto r + I = \{r + i : i \in I\}$$

Remember: $a + I = b + I \iff a - b \in I$

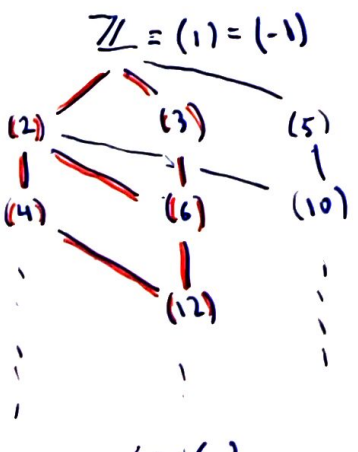
Example: ①

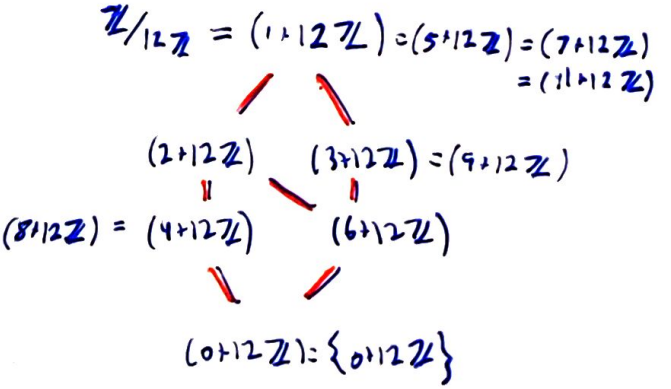
$I \subseteq R$ is proper $\iff R/I$ is nontrivial

Example ②: In $\mathbb{Z}$, look at ideal $(12) = 12\mathbb{Z}$

recall: all ideals in $\mathbb{Z}$ are principle; of the form (n) for $n \in \mathbb{Z}$

$2 \quad (m) \subseteq (n) \iff n$ divides m





FACT Lattice isomorphism theorem for rings

Given an ideal $I \subseteq R$

1. There is a bijection $\{\text{ideals } J \supseteq I \text{ in } R\} \leftrightarrow \{\text{ideals } \bar{J} \text{ in } R/I\}$

$$J \mapsto \pi(J) = \{j + I : j \in J\}$$
$$\pi^{-1}(\bar{J}) \longleftarrow \bar{J}$$

2. This is a bijection of "lattices" i.e. it respects inclusions, intersections

Maximal ideals

Def: A proper ideal $I \subseteq R$ is **maximal** if it's maximal among proper ideals (ordered by inclusion) i.e.

if J is an ideal with $I \subseteq J \subseteq R$ then either $J = I$ or $J = R$

in $\mathbb{Z}[x]$ Last time: $J = (2, x)$ is a proper ideal (no principle)

consider $I = (x) = \{x \cdot p(x) : p(x) \in \mathbb{Z}[x]\}$

Definitely $(x) \subseteq (2,x) \subsetneq \mathbb{Z}[x]$ but note $2 \in J = (2,x)$ but $2 \notin (x)$

$\Rightarrow (x) \subsetneq (2,x) \subsetneq \mathbb{Z}[x]$

$\mathbb{Z}[x]$

$(2,x)$

(x) not maximal

Theorem: A proper ideal $I \subseteq R$ is maximal

$\Updownarrow$

R/I is a field

proof: $I \subseteq R$ is maximal $\Leftrightarrow$ only ideals in R that contain I are I and R

$\Leftrightarrow$ lattice iso thm: the only ideals in the quotient ring are I/I = triv. and R/I

$\Updownarrow$

R/I is a field ■

Ex (3) (cont.) $(x) \subseteq \mathbb{Z}[x]$ is not maximal $\Leftrightarrow$ $\mathbb{Z}[x]/(x)$ is not a field

idea: try to involve first isomorphism theorem

I ideal $= (x) = \{x \cdot p(x) : p(x) \in \mathbb{Z}[x]\} = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$

$= \ker(ev_0)$

where $ev_0 : \mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(0)$ image? $\mathbb{Z}$

$\Rightarrow \mathbb{Z}[x]/(x) = \mathbb{Z}[x]/\ker(ev_0) \simeq \text{im}(ev_0) = \mathbb{Z}$ not a field ∴

Exercise: $\phi: \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$

$f(x) \mapsto f(0) + 2\mathbb{Z}$

claim: $\ker(\phi) = (2, x)$

$\text{im}(\phi) = \mathbb{Z}/2\mathbb{Z} \Rightarrow \frac{\mathbb{Z}[x]}{(2,x)} \cong \mathbb{Z}/2\mathbb{Z}$ field

so $(2, x)$ is maximal

but $\mathbb{Z}$ is an integral domain

Theorem: Suppose $I \subseteq R$ is a proper ideal

then I is prime

$\Updownarrow$

R/I is an integral domain

proof: R/I integral domain $\iff$ if $(a+I)(b+I) = 0$ then $a+I = 0+I$ or $b+I = 0+I$

$ab + I = 0 + I$

$\iff$ if $ab \in I$, then either $a \in I$ or $b \in I$

$\iff I$ is prime

Def: A proper ideal is prime if whenever $ab \in I$, then $a \in I$ or $b \in I$

Observations / facts:

① All maximal ideals are prime

② Every proper ideal is contained in a maximal ideal

(need: Zorn's lemma)

③ In $\mathbb{Z}$: all the prime ideals are maximal

Intuition for ideals: subspaces of a vector space

special case: principle ideals $(r) = \{cr : c \in R\}$

"span of r"

Claim: r is a unit when (r) is improper / $(r) = R$

($\Rightarrow$) r is a unit $\Rightarrow$ there is some element $v \in R$ s.t. $rv = 1$

so $1 = vr \in (r) \Rightarrow (r) = R$

($\Leftarrow$) Suppose $(r) = R$

then $1 \in (r) \Rightarrow 1 = cr$ for some $c \in R$

$\Rightarrow r$ is a unit

Ex: in $\mathbb{Z}$ (all ideals are principle)

$(6) = \{\dots, -6, 0, 6, \dots\}$

Claim: this is not a prime ideal

Proof: $2, 3 \notin (6)$ but $2 \cdot 3 = 6 \in (6)$

Proof: Look at $\mathbb{Z}/6\mathbb{Z}$ not a domain

b/c $\bar{2}, \bar{3} \neq 0$ but $\bar{2} \cdot \bar{3} = \bar{0}$

$(2) = \{\dots, -2, 0, 2, 4, \dots\} = 2\mathbb{Z}$

claim: (2) is a prime ideal

proof: Look at $\mathbb{Z}/2\mathbb{Z}$ is a field (so an integral domain)

$\Rightarrow (2)$ is maximal (thus prime)

proof: Suppose $ab \in (2)$ for some $a, b \in \mathbb{Z}$

so $2 \mid ab \Leftrightarrow ab = 2k$ for some $k \in \mathbb{Z}$

$\Rightarrow 2 \mid a$ or $2 \mid b$

$\Rightarrow a \in (2)$ or $b \in (2) \Rightarrow (2)$ is prime

note that in $\mathbb{Z}$ $(1) = \mathbb{Z}$ (neither max or prime)

$(0) = \{0\}$ (prime but not maximal)

$\mathbb{Z}/\{0\} \simeq \mathbb{Z}$ (int. domain but not a field)

Ex ③: $\mathbb{R}[x]$

$(2) = \{2f(x) : f(x) \in \mathbb{R}[x]\} \subseteq \mathbb{R}[x]$

$(x) = \{x f(x) : f(x) \in \mathbb{R}[x]\}$

$= \{g(x) \in \mathbb{R}[x] : g(x) = c_1 x + c_2 x^2 + \dots\}$

$= \{g(x) \in \mathbb{R}[x] : g(0) = 0\}$

Claim: x is a prime ideal

proof 1: Suppose $f(x) g(x) \in (x)$ for some $\mathbb{R}[x] \ni f(x), g(x)$

$\Rightarrow f(x) g(x) = x h(x)$ for some $h \in \mathbb{R}[x]$

$x = 0$: $f(0) \cdot g(0) = 0 \Rightarrow$ so $f(0) = 0$ or $g(0) = 0$

so $f \in (x)$ or $g \in (x)$

proof: $\mathbb{R}[x]/(x)$

find homo. $\phi : \mathbb{R}[x] \to S$

with $\ker(\phi) = (x)$

Week 2 pt 2

Let us $ev_0 : \mathbb{R}[x] \to \mathbb{R}$, $f(x) \mapsto f(0)$

then $K_e(ev_0) = (x)$

$im(ev_0) = \mathbb{R}$

so $\frac{\mathbb{R}[x]}{(x)} \simeq \mathbb{R}$ is a field

compare: $(x^2-1) \subseteq \mathbb{R}[x]$

claim: (x^2-1) is not a prime ideal

proof: $(x^2-1) = (x-1)(x+1) \in (x^2-1)$

and $(x-1), (x+1) \notin (x^2-1)$

proof: if $x+1 \in (x^2-1)$ then $x+1 = (x^2-1)f(x)$

$\Rightarrow \deg(x+1) = \deg(x^2-1) + \deg(f(x))$

contradiction!

proof: $ev_{1,-1} : \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$, $f(x) \mapsto (f(1), f(-1))$

check: $K_e(ev_{1,-1}) = (x^2-1)$

$im(ev_{1,-1}) = \mathbb{R} \times \mathbb{R}$

so $\frac{\mathbb{R}[x]}{(x^2-1)} \simeq \underbrace{\mathbb{R} \times \mathbb{R}}_{\text{not an integral domain}}$

$(1,0) \cdot (0,1) = (0,0)$ ∴ (Chinese remainder theorem)

proof: $\frac{\mathbb{R}[x]}{(x^2-1)} = \frac{\mathbb{R}[x]}{(x-1)(x+1)} = \frac{\mathbb{R}[x]}{(x-1)} \times \frac{\mathbb{R}[x]}{(x+1)} \simeq \mathbb{R}[x] \times \mathbb{R}[x]$

Ex (4) $\quad (4) \overset{J}{\subseteq} (2) \overset{I}{\subseteq} \mathbb{Z} \overset{R}{}$

$\mathbb{Z}$

$\ldots, \boxed{-4}, -3, \boxed{-2}, -1, \boxed{0}, 1, \boxed{2}, \ldots$

$2\mathbb{Z} = (2) = \{-4, -2, 0, 2, 4, \ldots\}$

$4\mathbb{Z} = (4) = \{-4, 0, 4, \ldots\}$

$\frac{4\mathbb{Z}}{4\mathbb{Z}}$

$\frac{2\mathbb{Z}}{4\mathbb{Z}}$

$\{C_0, C_2\}$

$\frac{\mathbb{Z}}{4\mathbb{Z}}$

$C_0 = \{\ldots, -4, 0, 4, \ldots\}$

$C_1 = \{\ldots, -3, 1, 5, \ldots\}$

$C_2 = \{\ldots, -2, 2, 6, \ldots\}$

$C_3 = \{\ldots, -1, 3, 7, \ldots\}$

$\frac{\mathbb{Z}/4\mathbb{Z}}{(2\mathbb{Z}/4\mathbb{Z})} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$

$D_0 = \{C_0, C_2\}$

$D_1 = \{C_1, C_3\}$

Better proof: $\frac{R/J}{I/J} \simeq \frac{R}{I}$ $\quad J \subseteq I \subseteq R$

Find hom. $\phi : R/J \to R/I$

with $\ker(\phi) = I/J$

$im(\phi) = R/I$

the $\phi(r+J) = r+I$ will work

why well defined?

Suppose $r+J = r'+J$

$r - r' \in J$ so $r - r' \in I$ because $J \subseteq I$

so $r+I = r'+I$