Algebra I Lecture 15: Properties of ideals

- New HW is up!
- Plug my topics course.

Example ~~Sum of ideals~~: $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, $d = \gcd(m,n)$. (Bezout)

Let R be a rng with $1 \neq 0$ throughout.

Def^n: $A \subseteq R$.

1). (A) = is the smallest ideal containing A (the ideal generated by A).

2). $RA = \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R, a_i \in A\}$ finite sums

$AR = \{a_1 r_1 + \dots + a_n r_n\}$.

ARR $RAR = \{r_1 a_1 r_1' + \dots + r_n a_n r_n'\}$.

A finitely generated ~~set~~ ideal is

$I = (\{a_1, \dots, a_n\})$; denoted $I = (a_1, \dots, a_n)$.

A principal ideal is one s.t. $I = (a)$, some $a \in \mathbb{Z}$.

Ex: The notation is like the gcd notation. In fact, in $\mathbb{Z}$, $(n,m) = (d)$ by the above.

~~The ideal $(2,x)$ in $\mathbb{Z}[x]$ is not principal~~

~~[polys with even constant term]~~

Any subset S is contained in R, so an ideal, so

$$(A) = \bigcap_{\substack{I \text{ ideal} \\ A \subseteq I}} I.$$

(1) and the intersection of ideals is an ideal

Left ideal gen. by A = intersection of left ideals containing A

RA is closed under $+$, mult. on left by any $r \in R$. I.e., it's a left ideal ($ra'a = (ra')a \in RA$)

If R has 1, $RA \supseteq A$.

And Conversely, any left ideal containing A is closed under ~~left mult. by R, $+$ in A~~ finite sum of ra $\Rightarrow RA \subseteq A$ $\Rightarrow$ left ideal gen. by A $= RA$.

Thus, $RAR = (A)$.

If R is commutative, $(A) = RA$.

If R is commutative, (a) = set of R-multiples of a.

Ex: $(2, x)$ in $\mathbb{Z}[x]$ is not principal.

$(2, x) = \{2p(x) + q(x)\cdot x \mid p, q \in \mathbb{Z}[x]\}$.

$= \{$polys with even constant terms$\}$ | pause here.

If $(2, x) = (a)$ (If it were principal), then $a = a(x)$

$2 \in (a) \Rightarrow \exists\, p$, ~~$2 =$~~ $p \cdot a = 2$

$\Rightarrow p, a$ are both constants. 2 prime

$\Rightarrow p \in \{\pm 1, \pm 2\}$. But $(\pm 1) = \mathbb{Z}[x]$, and $(2, x)$ is proper.

If $(\pm 2) = (2, x)$, then $x \in (\pm 2) \Rightarrow x = q \cdot (\pm 2)$ $*$

Clearly impossible.

Prop Lemma: R comm.

R a field $\Leftrightarrow$ $(0), (1)$ are the only ideals.

Pf: $\Leftarrow$: Let $x \in R \setminus \{0\}$, then $(x) = R \Rightarrow \exists\, y$ s.t. $xy = 1 \Rightarrow$ x a unit $\Rightarrow R^\times = R \setminus \{0\} \Rightarrow R$ is a field

$\Rightarrow$: R field $\Rightarrow$ every non-zero ideal has a unit $\Rightarrow$ is all of R.

~~Th~~ False for non-comm. rings?
$M_n(F)$ has only $0, M_n(F)$ as ideals,
but not a division ring (it's a simple ring)

Def An ideal M in R is maximal if $M \neq R$,
$\nexists$ ideal I with $M \subsetneq I \subsetneq R$.

Prop: In a ring with 1, every proper ideal
is contained in a maximal ideal.

Pf: (Zorn's Lemma): A non-empty poset in which
every chain has an upper bound has a maximal elt.

Poset: Set $S, \leq$ s.t.
$x \leq x$
$x \leq y, y \leq x \Rightarrow x = y$
$x \leq y, y \leq z \Rightarrow x \leq z$

Chain: Totally ordered set
($\forall x, y$, either $x \leq y$ or $y \leq x$)

Maximal elt: $m \in S$ s.t.
$m \leq x \Rightarrow m = x$.

P1: I proper ideal.
$S = \{$proper ideals containing $I\}$.

Then $S \neq \emptyset$, S is partially ordered by inclusion

If $\mathcal{C}$ is a chain, let $J = \bigcup_{A \in \mathcal{C}} A \supseteq I$
in S

Clm J is an ideal: $J \neq \emptyset$ as ~~$A, I \subseteq J$~~ $0 \in$ an ideal $\Rightarrow 0 \in J$.
If $a, b \in J$, say $a \in A$, $b \in B$, $A, B \in \mathcal{C}$,
either $A \subseteq B$ or $B \subseteq A$.
WLOG: $A \subseteq B \Rightarrow a, b \in A \Rightarrow a - b \in A \subseteq J$
Since each $A \in \mathcal{C}$ is closed under mult. by elts of R, so is J.

If T is not proper, then $1 \in T$.

But then $1 \in A$, some $A \in \mathcal{C}$.

Contradiction as each A is proper.

$\Rightarrow T \in S$

T is thus an upper bound for $\mathcal{C}$.

Zorn $\Rightarrow$ done. S has a max elt ☐

If R is commutative:

Prop: M maximal ideal $\Leftrightarrow R/M$ is a field.

($M \neq R$: no field of one elt!)

Pf: M maximal $\Leftrightarrow \nexists$ ideals I, $M \subsetneq I \subsetneq R$

By the Lattice Isom. Th^{m} for rings,

$$\{\text{ideals of } R \text{ containing } M\} \xleftrightarrow[\text{corr.}]{1\text{-}1} \{\text{ideals of } R/M\}$$

So M is maximal $\Leftrightarrow$ all ideals of R/M are $0, R/M$.

By prop. above, M maximal $\Leftrightarrow R/M$ a field.

Rmk: False for non-comm. rings.

e.g.: $(0) \subseteq M_n(F)$ is maximal.

R commutative:

Ideal P is prime if $P \neq R$ and

$ab \in P \Rightarrow a \in P$ or $b \in P$.

Euclid's Lemma in $\mathbb{Z}$: If p prime $\Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

i.e. $ab \in (p) \Rightarrow a \in (p)$ or $b \in (p)$.

(Stronger statement ...).

Prop: R comm. P prime $\iff R/P$ is an integral domain.

Pf: Translate Def^n of prime ideal on quotient level.

~~P prime $\iff P \neq R$ and~~

$r \in P \iff \bar{r} = 0$ in R/P, i.e.

Thus, P is prime $\iff \bar{R} \neq \bar{0}$ and $\overline{ab} = \bar{a}\bar{b} = \bar{0}$

$\Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

(no zero divisors)

$\iff \bar{R}$ is an integral domain

(HP)

In particular, R comm. & 1 is an integral domain $\iff 0$ is a prime ideal.

Cor: R comm $\Rightarrow$ Every maximal ideal of R is prime.

Pf: M maximal $\Rightarrow R/M$ a field $\Rightarrow R/M$ an integral domain $\Rightarrow M$ prime. ☐

Ex: In $\mathbb{Z}$, if p is prime, (p) is prime & maximal

In R, non-zero prime ideal $\iff$ maximal ideal.

Ex: $(x) \subseteq \mathbb{Z}[x]$

is prime as $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.] Recall...

$\mathbb{Z}$ is not a field $\Rightarrow$ (x) is not maximal.

The ideal 0 is prime, but not maximal.

Extra time:

Ex: Ideals of $\mathbb{Z}$ are $n\mathbb{Z}$

$n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow m \mid n$.

$n\mathbb{Z}$ max $\Leftrightarrow$ n prime

Thus $\mathbb{Z}/n\mathbb{Z}$ field $\Leftrightarrow$ n prime.

Ex: (p, x) maximal in $\mathbb{Z}[x]$.

$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}/p\mathbb{Z}$

$g(x) \mapsto g(0) \bmod p$.

$\ker(\varphi) = (p, x)$

Ex: $C = C^0([0,1] \to \mathbb{R})$ Cont. $\not\Rightarrow$.

$\mathrm{eval}_a : C \to \mathbb{R}$ hom. with kernel M_a.
$f \mapsto f(a)$

So $C/M_a \cong \mathbb{R}$

$\Rightarrow$ M_a is maximal

$= \{$ continuous $f : [0,1] \to \mathbb{R}, f(a) = 0\}$.

Converse: One can show every max. ideal of C is of the form M_a, some $a \in [0,1]$.