Math 3032 Lecture 12 (March 2, 2021)

OH today 12-2 pm

Next week: no lecture. optional review assignment

in addition a usual assigned

Today: prime and maximal ideals

Let R is a commutative + unital ring.

An ideal $A \subseteq R$ is an additive subgp s.t.

if $r \in R$ and $a \in A$ then $ra \in A$. "absorbing"

Raison d'être: R/A is a ring.

What is R/A qualitatively?

E.g.: $\mathbb{Z} \times \mathbb{Z} = R$ not an integral domain } qualitatively
i.e. has zero divisors. } poor

$(m,0)\cdot(0,n) = (0,0) \quad \forall m,n \in \mathbb{Z}.$

Ideal $\mathbb{Z} \times \{0\} = \{(m,0) \in R, \quad m \in \mathbb{Z}\}.$

$\cap$

R

$[(a,b)] = [(0,b)]$

$[(\cancel{a,0}) + (0,b)]$

$R/_{\mathbb{Z}\times\{0\}} \cong \mathbb{Z}$ ↑ is a domain. qualitatively improved.

$\mathbb{Z} \times 3\mathbb{Z} = \{(m,3n), \quad m,n \in \mathbb{Z}\}. \Rightarrow$ ~~$(m,0) \to 0$~~ in quotient

~~$(0,3) \to 0$~~ in quotient

$R/_{\mathbb{Z}\times 3\mathbb{Z}} \cong \mathbb{Z}_3$. field. even better than a domain.

$[(a,b)] = [(0, b \bmod 3)]$

Quotients don't always improve things:

$$\mathbb{Z}/8\mathbb{Z} \simeq \mathbb{Z}_8$$

↪ not a domain

even though $\mathbb{Z}$ was.

Question: When is R/I . domain ?
. field

E.g.: When $R = \mathbb{Z}$, then $I = (n) = n\mathbb{Z}$

R/I is a field if n is nonzero prime

domain if n is zero or prime. ← prime.

Defn: An element $p \in R$ is **prime** if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

E.g.: 0 is prime iff R is integral domain.

Pf: $0 \mid r \iff r = 0$ (i.e. $r = 0 \cdot s$.)

So "0 is prime" $\iff$ if $ab = 0$ then $a = 0$ or $b = 0$.

$r \in R \rightsquigarrow$ principal ideal $(r) = \{\text{multiples of } r\}$.

$p \mid ab \iff ab \in (p)$.

Defn: An ideal $I \subseteq R$ is **prime** if

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

Prop: An ideal I in a com unital ring R is prime iff R/I is an int. domain.

Pf: R/I is a domain $\iff$

$([a][b] = 0 \Rightarrow [a] = 0$ or $[b] = 0)$

$\|$

$[ab]$ (classes in R/I).

$[r]$ is zero in R/I iff $r \in I$.

$ab \in I$ $\qquad$ $a \in I$ or $b \in I$.

So the prop. just follows from definition unpacking.

What about if we want R/I to be a field?

[trivial ring $\{0\}$ is not a field.
in a field, $1 \neq 0$.]

R/I is a field exactly when it has no proper ideals.

If R/I not a field, then take some proper ideal $J \subseteq R/I$ $\xleftarrow{[r] \leftarrow r}$ R

Look at $\widetilde{J} \subseteq R$ defined as $r \in \widetilde{J}$ iff $[r] \in J$.

- it's an ideal. Pf: to be an ideal, you must be closed under $+$ and absorbing.

if $r_1, r_2 \in \widetilde{J}$ is $r_1 + r_2 \in \widetilde{J}$?

Yes because $[r_1 + r_2] = [r_1] + [r_2]$. and
$\uparrow$ $\uparrow$ J closed.
J J

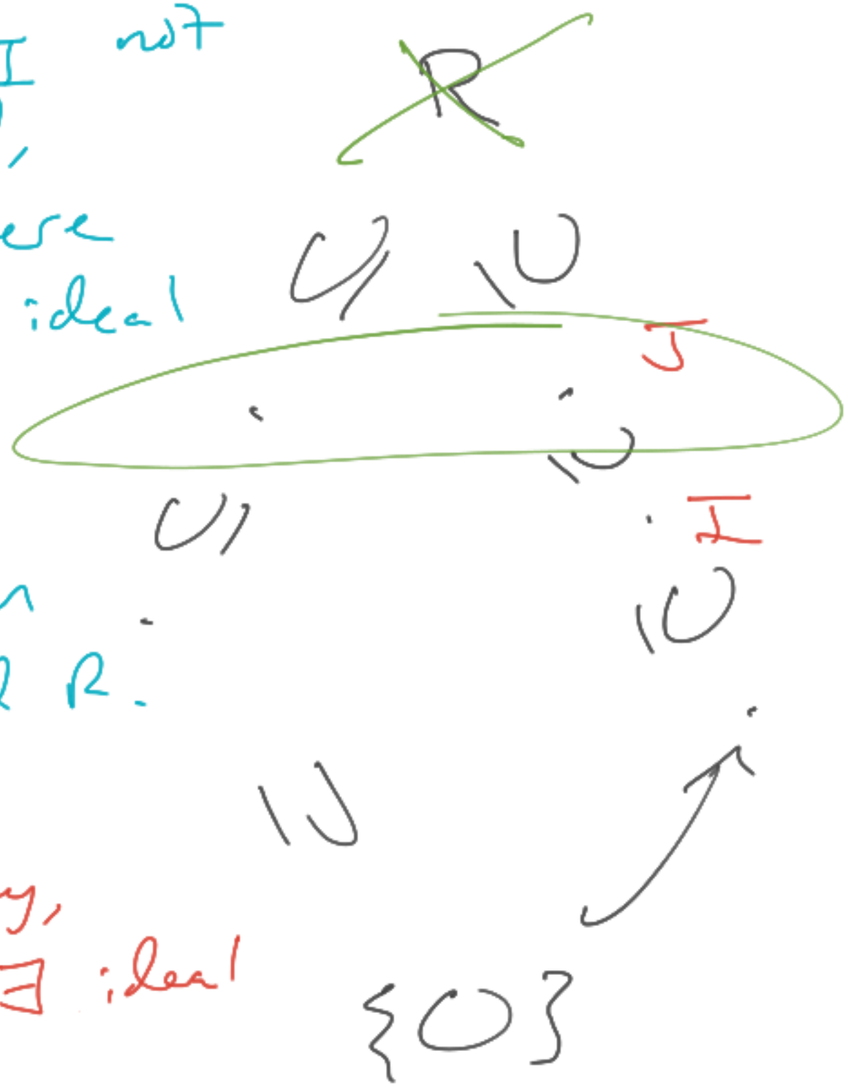
is $\widetilde{J}$ absorbing? Yes: if $r_1 \in \widetilde{J}$ and $r_2 \in R$.

then $[r_1 r_2] = [r_1] \cdot [r_2] \in J$ because J
$\uparrow$ $\uparrow$ is an ideal.
J R/I

$J \neq 0 \subseteq R/I$, $\widetilde{J} \neq I$

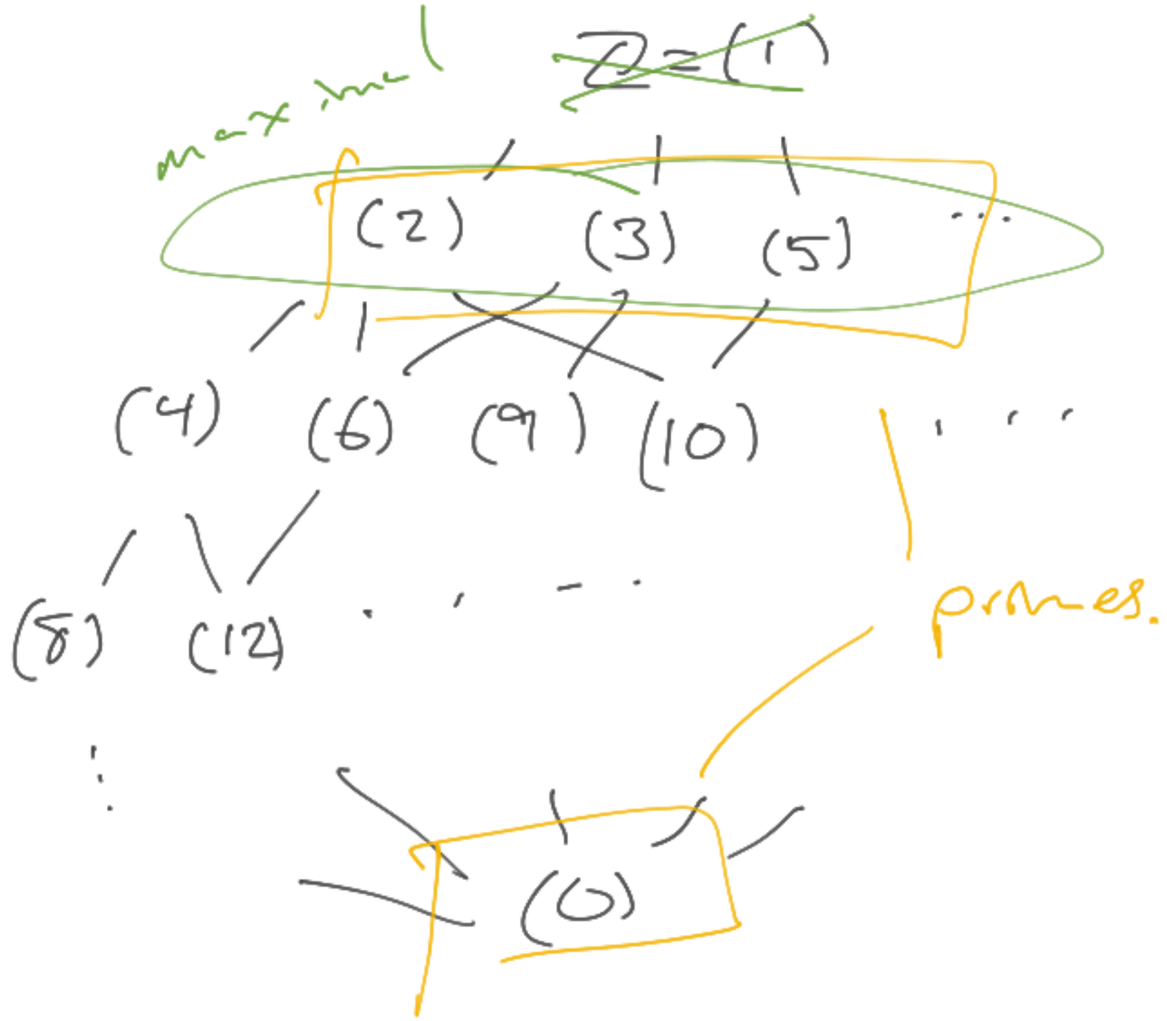
$J \neq R/I$, $\widetilde{J} \neq R$

If R/I not a field, then there is an ideal in R strictly between I and R.



Conversely, suppose $\exists$ ideal J strictly between I and R.

$[J] = \{[j] \text{ where } j \in J\} \subseteq R/I$.



Claim: this is proper ideal in R/I.

Defn: An ideal $I \subsetneq R$ is **maximal**
if it is not R itself,
and there are no ideals strictly between I and R.

Summary of the discussion on the last few slides:

Prop: R/I is a field iff I is maximal.

Cor: maximal ideals are prime

because fields are domains.
but prime ideals not always maximal.

In $\mathbb{Z}$, every ideal is principal.] PID

also in $\mathbb{Z}_n$. → because we know all additive subgps, and they are all cyclic.

↳ not PID unless n prime.

both PIR

not in $\mathbb{Z}[x]$

$\mathbb{Z}[x]/I \cong \mathbb{Z}_3$ so this I is maximal.

↳ $\{ a_0 + a_1 x + \dots + a_n x^n \text{ s.t. } a_0 \in 3\mathbb{Z} \} = I$

$(1) \neq I$

$3, x$

not principal.

if were principal, then there would be some $f(x) \in \mathbb{Z}[x]$ s.t.

$I = (f)$ i.e. $3, x$ are multiples of f.

the only poly that divides both $3 \& x$ is 1.

Defn: A principal ideal domain is a ring where every ideal is principal.

and ring is integral domain.

Thm: If $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a PID.

This pf works anywhere that we have long div.

Pf: We showed it was a domain weeks ago.

Let $I \subseteq \mathbb{F}[x]$ be an ideal. If $I = (0)$, done. Otherwise,

Pick $g \in I$ of minimal degree. Claim: $I = (g)$.

$\neq 0$

Indeed: if $f \in I$, wts that $g \mid f$.

Use (existence of) long division: $\exists\, q, r \in \mathbb{F}[x]$

s.t. $f = qg + r$ and $\deg r < \deg g$.

I $\quad$ I since $g \in I$ $\quad$ so $r \in I$ because I is an additive gp.

I is absorbing, but $\deg r < \deg g$ minimal, so $r = 0$. $\square$

How common is it that all nonzero primes are maximal?

If R is a PID then yes.

Defn: $p \in R$ is irreducible if (p not a unit and) for any factorization $p = fg$, f or g is a unit.

Thm: If R is a PID then $p \in R$ is irred iff (p) is maximal iff (p) is prime and nonzero.

irred: "p is irred" — A

(p) is maximal — B

(p) is prime and nonzero — C

Pf: $B \Rightarrow C$ already done.

C ⇒ A Suppose (p) is prime and $p = fg$.

Since (p) is prime, f or $g \in (p)$.

Suppose $f \in (p)$. Then $f = gp$ for some $g \in R$.

So $p = ggp$. Since R is a domain, $p \neq 0$,

so $1 = gg$ so g, g are units.

A ⇒ B Suppose p is irred. and $I \supseteq (p)$ is an ideal.

Since R is a PID, $I = (f)$ for some $f \in R$.

but $p \in (p) \subseteq I = (f)$, so $p = fg$ for some g.

So either f or g is a unit since p irred.

if f is a unit, then

$$I = (f) \subseteq R.$$

ψ

$$r = (rf^{-1}) \cdot f \quad \text{for any } r \in R.$$

if g is a unit, then $(f) = (g)$. $\square$.

Defn: A ring R is a unique factorization domain (UFD) if every elt factors uniquely into irred factors.

uniquely ↑ caveats: up to reorder and mult. by units.

E.g.: In $\mathbb{Z}$, -6.

$$-6 = (-2)\cdot 3 = 3\cdot(-2)$$
$$= 2\cdot(-3) = (-3)\cdot 2.$$

$\pm 2, \pm 3$ are irred.

2 and -2 are the same up to units.

$(2) = (-2)$ as ideals.

Prop: R is a UFD iff if $p \in R$ is irred and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Defn: A ring R is a unique factorization domain (UFD) if every elt factors uniquely into irred factors.

Prop: R is a UFD iff

if $p \in R$ is irred then p is prime.

- **Why?** Suppose you factor

$$r = p_1 \cdots p_m = q_1 \cdots q_n$$

p_i, q_j's are all irred

Then p_1 must divide some q_i. Up to reordering, $p_1 \mid q_1$. This forces q_1, p_1 the same up to units.

So $p_2 \cdots p_m = \text{unit} \cdot q_2 \cdots q_n$. Repeat.

F a field $\Rightarrow$ $F[x]$ has long division.

Long division $\Rightarrow$ PID.

PID $\Rightarrow$ UFD.

Summary: for any field, $F[x]$ has unique factorization.