Two stories:

- where does the complicated framework of modern comm. algebra come from?
- What are the logical basics of this language?

Last time:

R/I field $\iff$ I maximal,

R/I domain $\iff$ I prime.

Today: Principal Ideal Domains.

$$\mathbb{Z} \text{ vs. } \mathbb{F}[x]$$
$$\mathbb{Q} \text{ vs. } \mathbb{F}(x)$$
$$\mathbb{Q}[\alpha] \text{ vs. } \mathbb{F}(x)[f(x)]$$

Say ring R is Euclidean if $\exists$ size function $\delta : R \setminus 0 \to \mathbb{N}$, s.t.

$\forall\, a, b \in R, b \neq 0, \exists\, q, r \in R$, s.t.

$$\begin{cases} a = qb + r, \\ r = 0 \text{ or } \delta(r) < \delta(b). \end{cases}$$

Examples: $\delta : \mathbb{Z} \setminus 0 \to \mathbb{N}$

$a \mapsto |a|$

$\delta : \mathbb{F}[x] \setminus 0 \to \mathbb{N}$

$f(x) \mapsto \deg(f)$. ///

Euclidean $\Rightarrow$ PIR:

Any ideal $I \subseteq R$ has the form $I = mR = \{ma : a \in R\}$ for some element $m \in R$.

Proof: If $I = 0 = 0R$, done.

Otherwise let $m \in I \setminus 0$ have minimal size. Note $m \in I \Rightarrow mR \subseteq I$.

Conversely, I claim $I \subseteq mR$.

For any $a \in I$, divide by m to get

$$\begin{cases} a = qm + r, \\ r = 0 \text{ or } \delta(r) < \delta(m). \end{cases}$$

We must have $r=0$, otherwise

$$r = a - qm \in I \setminus 0$$

contradicts minimality of m. ///

Remark: This m is not unique.

Corollary: GCD exist in Euclidean rings. Indeed, given $a, b \in R$ we have $aR + bR = \{ar + bs : r, s \in R\}$ is an ideal, hence $aR + bR = dR$ for some $d \in R$, called <u>a</u> greatest common divisor. Meaning:

- $d \mid a$ & $d \mid b$.
- $e \mid a$ & $e \mid b \Rightarrow e \mid d$.

Proof: Define "$m \mid n$" $\Leftrightarrow$ "$n \in mR$."

Since $a \in aR \subseteq aR + bR = dR$
$\quad\quad b \in bR \subseteq aR + bR = dR$

we have $d \mid a$ & $d \mid b$.

And if $e|a$ & $e|b$, then $a, b \in eR$, and hence

$$d \in dR = aR + bR \subseteq eR.$$

i.e. $e|d$. ///

Translate Prime & Maximal ideals into language of PIRs.

Prime ideals in PIR:

Ideal $pR \subseteq R$ is prime iff

$$\boxed{p \nmid a \;\&\; p \nmid b \implies p \nmid ab}$$

for all a, b. Indeed,

$$p \nmid a \iff a \notin pR \iff a \in R \setminus pR. \quad ///$$

In this case we say

$$\underset{\text{prime ideal}}{pR \subseteq R} \equiv \underset{\text{element.}}{p \in R \text{ prime}} \quad (p \neq 0)$$

Max ideals in PIR can be complicated, so now we restrict to PIDs (i.e. PIRs that are also domains)

Remark: In a domain we have

$$aR = bR \iff a = ub \text{ for unit } u \in R.$$

"$a \sim b$"

"a, b are associates"

Indeed, if $a \sim b$ then $a = ub$ implies $a \in bR$ hence $aR \subseteq bR$. and $b = u^{-1}a \Rightarrow b \in aR \Rightarrow bR \subseteq aR$.

Conversely, if $aR = bR$ then have $b = ak$ & $a = bl$ some $k, l \in R$

$$a = bl$$
$$a = akl$$
$$a(1-kl) = 0 \qquad a \neq 0$$
$$1 - kl = 0$$
$$1 = kl,$$

hence $a \sim b$. ///

Max ideals in PID.

$mR \leq R$ maximal $\Longleftrightarrow$

($a | m \implies a \sim m$ or $a \sim 1$.)

Say $m \in R$ is an "irreducible element."

Idea: Irreducible element has "no nontrivial divisors."

Proof: $mR \leq R$ maximal and $a | m$ then $mR \leq aR \leq R$ implies

$mR = aR$ or $aR = R = 1R$
$(m \sim a)$ $\quad$ $(a \sim 1)$.

a is a unit.

Conversely let $m \in R$ irreducible and consider $mR \subseteq aR \subseteq R$. This implies $a | m$. By irred. of m, this implies $a \sim m$ (i.e. $mR = aR$) or $a \sim 1$ (i.e. $aR = R$). ///

Observe:

- $p \nmid a$ & $p \nmid b \implies p \nmid ab$
- $a \mid m \implies a \sim m$ or $a \sim 1$

Both famous properties of prime integers, i.e., they coincide in $\mathbb{Z}$.

Euclid's Lemma (Prop VII.30)

Irreducible $\Leftrightarrow$ Prime in a PID.

This result has confused me a few times. Both directions are easy & both directions are hard.

Remark: There are too many definitions in comm. algebra. But "PID" is one of the good definitions.