2/19
Weds
Week 5

8.2 – Principal ideal domains

Def: An integral domain R is called a principal ideal domain (PID) if every ideal of R is principal.

[That is, every ideal is of the form $(a) = \{ar \mid r \in R\}$]

Last time: If R is a Euclidean domain, then R is a PID.

Ex: $\mathbb{Z}$ is a PID.

Ex: $F[x]$ where F is a field is a Euclidean domain, so its a PID.

Ex: $\mathbb{Z}[x]$ is not a PID.

$\mathbb{Z}[x]$ is an integral domain but not every ideal is principal.

Let

$$(2,x) = \{ 2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x] \}$$

$(2,x) = (2) + (x)$ ⟷ This is an example of this:
R is a ring, I, J are ideals of R.
You can make the ideal
$I + J = \{ i + j \mid i \in I, j \in J \}$

Ex: Let F be a field. Then F is an integral domain and its only ideals are

$\{0\} = (0)$ and $F = (1)$.

So F is a PID.

We will show that $(2,x)$ is not principal.

Note that any polynomial in $(2,x)$ has even constant term.

So, $(2,x) \neq \mathbb{Z}[x]$.

In $(2,x)$:

$2(x^2+1) + x(x^3+5x-2)$

$= x^4+7x^2-2x+2$

↑ even constant term

Suppose $(2,x) = (a(x))$ where $a(x) \in \mathbb{Z}[x]$.

We will show this leads to a contradiction and hence $(2,x)$ is not principal and $\mathbb{Z}[x]$ is not PID.

$(a(x)) = \{a(x)p(x) \mid p(x) \in \mathbb{Z}[x]\}$

Since $2 = 2 \cdot 1 + x \cdot 0 \in (2,x)$.

So, $2 \in (a(x))$ and hence $2 = a(x)p(x)$ where $p(x) \in \mathbb{Z}[x]$.

Since $\mathbb{Z}$ is an integral domain, and our polys live in $\mathbb{Z}[x]$ we have

$0 = \deg(2) = \deg(a(x)p(x)) = \deg(a(x)) + \deg(p(x))$

($\mathbb{Z}$ is an integral domain)

Since $\deg(a(x)) \geq 0$ and $\deg(p(x)) \geq 0$,
we have $\deg(a(x)) = \deg(p(x)) = 0$.

So, $a(x)$ and $p(x)$ are constants in $\mathbb{Z}$
and $a(x)p(x) = 2$.

So, $a(x), p(x) \in \{\pm 1, \pm 2\}$

case 1:
If $a(x) = \pm 1$, then $a(x)$ is a unit
and so $(2,x) = (a(x)) = (\pm 1) = \mathbb{Z}[x]$.
This contradicts the fact that $(a(x)) \neq \mathbb{Z}[x]$.

case 2:
If $a(x) = \pm 2$, then $(2,x) = (a(x)) = (\pm 2) = (2)$
But here $x = 2 \cdot 0 + x \cdot 1 \in (2,x)$
but $x \notin (2)$. ← $x \neq 2f(x)$ for any $f(x) \in \mathbb{Z}[x]$

Contradiction.

So in either case we get a contradiction.
Thus, $(2,x)$ is not principal and $\mathbb{Z}[x]$ is not a PID.

Recall: Let R be a commutative ring with $1 \neq 0$. Then every maximal ideal of R is a prime ideal of R

We can get an "almost-converse" in a PID.

Prop: Let R be a PID. Let I be a prime ideal of R with $I \neq \{0\}$. Then I is maximal

Ex: $\mathbb{Z}$ is a PID

maximal ideals of $\mathbb{Z}$	prime ideals of $\mathbb{Z}$
$p\mathbb{Z}$, p is prime	$p\mathbb{Z}$, p is prime
	$\{0\}$

Proof: Let $I \neq \{0\}$ be a prime ideal of a PID R. Since I is prime, $I \neq R$.

Since R is a PID, $I = (p)$ where $p \in R$.

Let's show I is maximal.

Suppose $J = (m)$ is another ideal of R with

$$I \subseteq J \subseteq R$$

that is $(p) \subseteq (m) \subseteq R$.

We wa
$(p)=$
Since (
we
So, $p =$
Thus
Since (
either

We want to show either
$(p)=(m)$ or $(m)=R$.

Since $(p)\subseteq(m)$ and $p=p\cdot 1\in(p)$,
we know $p\in(m)$.

So, $p=mk$ where $k\in R$.

Thus $mk\in(p)$.

Since (p) is a prime ideal,
either $m\in(p)$ or $k\in(p)$.

Case 1: Suppose $m\in(p)$.

Then $m=pl$ where $l\in R$.

This implies that $(m)\subseteq(p)$.

Why? If $mq\in(m)$ where $q\in R$,
then $mq=plq\in(p)$.

So, $(p)\subseteq(m)$ and $(m)\subseteq(p)$.

Thus, in this case $(p)=(m)$.

Case 2: Suppose $k\in(p)$.

So, $k=pt$ where $t\in R$.

Then $p=mk=mpt$.

So, $p-pmt=0$.

Then, $p(1-mt)=0$

Since R is a PID, R is
an integral domain so
either $p=0$ or $1-mt=0$.

We know $p\neq 0$ since
$\{0\}\neq I=(p)$.

So, $1-mt=0$.

Thus, $1=mt$.

Hence m is a unit.

Then, $(m)=R$.

If an ideal
contains a
unit its the
whole ring

Therefore, $I=(p)$ is maximal. ▨

8.3 - UFD's

Def: Let R be an integral domain.

(1) Let $r \in R$ where $r \neq 0$ and r is not a unit.
We say that r is <u>irreducible</u> in R
if whenever $r = ab$, with $a, b \in R$,
then at least one of a or b is a unit
in R.

② Let $p \in R$ with $p \neq 0$ and p is not a unit.
We say that p is <u>prime</u> in R if (p) is a prime ideal.

Recall:

(p) prime $\Leftrightarrow$ If $ab \in (p)$, then either $a \in (p)$ or $b \in (p)$
If $ab = pk$, then either $a = p\ell$ or $b = pt$

Generalizing this idea $\rightarrow$ If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

③ Two elements $a, b \in R$ are called <u>associates</u> if $a = bu$ where u is a unit in R.

<u>Ex:</u> $R = \mathbb{Z}$

x is irreducible iff x is prime
[We will prove this for PID's]

5 and -5 are associates

$$5 = (-5)\underbrace{(-1)}_{\text{unit}}$$