Last time:

- In a UFD, gcds always exist.
- Defined the ideal generated by $a_1, \dots, a_m \in R$

$$\langle a_1, \dots, a_m \rangle = \{ x_1 a_1 + x_2 a_2 + \dots + x_m a_m \mid x_i \in R \}$$

Example: Take $R = \mathbb{Z}[x]$.

What is $\langle x+2, x+3 \rangle$?

$$\langle x+2, x+3 \rangle = \{ p(x)\cdot(x+2) + q(x)\cdot(x+3) \mid p, q \in \mathbb{Z}[x] \}$$

Note that $1 \in \langle x+2, x+3 \rangle$ because

$$1 = (-1)\cdot(x+2) + (1)(x+3).$$

Since $1 \in \langle x+2, x+3 \rangle$ and $\langle x+2, x+3 \rangle$ is an ideal (closed under multiplication by any $r \in R$) then $\langle x+2, x+3 \rangle = \mathbb{Z}[x]$.

In other words

$$\langle x+2, x+3 \rangle = \underbrace{\langle 1 \rangle = R}$$

true in any ring.

- A principal ideal is an ideal generated by 1

- A principal ideal is an ideal generated by 1 element.
- A principal ideal domain (PID) is an integral domain where every ideal is principal.

Example: $R = \mathbb{Z}$

What is $\langle -10, 25 \rangle$?

$$\langle -10, 25 \rangle = \{ x_1 \cdot (-10) + x_2 \cdot 25 \mid x_1, x_2 \in \mathbb{Z} \}$$

$$= \langle 5 \rangle = \langle -5 \rangle.$$

Proposition: Let R be a domain.

(a) • If $\langle a, b \rangle = \langle d \rangle$ then d is a gcd of a and b.

(b) • If R is an integral domain then $\langle a \rangle = \langle b \rangle \iff a, b$ are associates.

Proof: (a) Suppose $a, b \in R$ and $\langle a, b \rangle = \langle d \rangle$

We have that $a \in \langle a, b \rangle$ and $b \in \langle a, b \rangle$,

so $a \in \langle d \rangle$ and $b \in \langle d \rangle$, which shows that a and b are multiples of d, so d is a common divisor of a, b.

Now, suppose c is another common divisor of a, b.

As $d \in \langle d \rangle = \langle a, b \rangle$ then $d = \underbrace{x_1 \cdot a}_{c \text{ divides this}} + \underbrace{x_2 \cdot b}_{c \text{ divides this}}$

for some $x_1, x_2 \in R$

$\Rightarrow c$ divides d.

(b) If $\langle a \rangle = \langle b \rangle$ then $a \mid b$ and $b \mid a$. In an integral domain, this means that a, b are associates. ∎

Question: • What is $\langle 0 \rangle$?

$\langle 0 \rangle = \{0\}$.

• What is $\langle \text{unit} \rangle$?

$\langle \text{unit} \rangle = \langle 1 \rangle = R$.

because associates

Recall –

Corollary: In a principal ideal domain R any two elements a, b have a gcd d. Furthermore you can write $d = x_1 a + x_2 \cdot b$.

Proof: Take $a, b \in R$. The ideal $\langle a, b \rangle$ must be principal, say $\langle a, b \rangle = \langle d \rangle$.

That means that d is a g.c.d of a, b, and $d \in \langle d \rangle = \langle a, b \rangle$ so

$$d = x_1 a + x_2 b.$$

Proposition: Let R is a PID and let p be an irreducible element. Then if $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof: Suppose p is irreducible, and $p \mid a \cdot b$. If $p \mid a$ we are done, so suppose $p \nmid a$. As we are in a PID, there is a gcd of p and a, call it d.

gcd of p and a, call it d.

Since p is irreducible, its only divisors are units and associates of p. Associates of p are not divisors of a, so the only common divisors of p and a are the units, thus d is a unit. As we are in a PID, we can write

$$d = x_1 \cdot a + x_2 \cdot p$$

Multiplying by d^{-1}, we get

$$1 = d^{-1} x_1 a + d^{-1} x_2 p.$$

Multiplying by b we get

$$b = d^{-1} x_1 \cdot a \cdot b + b \cdot d^{-1} \cdot x_2 \cdot p$$

p divides this — p divides this

This implies that $p \mid b$. ∎

Corollary: If R is a PID and p

Corollary: If R is a PID and p is irreducible then

$$p \mid a_1 \cdot a_2 \cdots a_n \implies p \mid a_1 \text{ or } p \mid a_2 \text{ or } \cdots \; p \mid a_n.$$

"

Theorem: Every principal ideal domain is a unique factorsation domain.

Idea of the proof:

Suppose R is a PID. Let a be a non-zero non-unit element in R. If a is irreducible then $a = a$ is a factorsation into irreducibles. If a is not irreducible then $a = a_1 \cdot a_2$ with a_1, a_2 non zero, non units.

If a_1, a_2 are irreducible, this is a factorsation of a as a product of irreducibles.

If one of a_1, a_2 is not, you can decompose it as a product of two other elements. We can continue doing this.

Since R is a PID then this process has to stop at some point (see section 7.9 of the textbook for this). When this stops, we have

$$a = \underbrace{a_1 \cdot a_2 \cdot \dots \cdot a_n}_{\text{factorisation into irreducibles.}}$$

To show that this factorisation is unique (up to reordering and up to associates), suppose you have two factorisations into irreducible elements:

$$a = \underbrace{a_1 \cdot a_2 \cdot \dots \cdot a_n}_{\text{irreducible elements.}} = \underbrace{b_1 \cdot b_2 \dots b_m}_{\text{irreducible elements.}}$$

Since $a_1 \mid a = b_1 \cdot b_2 \dots b_m$ and a_1 is irreducible then $a_1 \mid b_i$ for some factor b_i. Since b_i is irreducible, its only divisors are

units and associates of b_i. So because a_1 is not a unit, a_1 is an associate of b_i, say $a_1 = u \cdot b_i$ (unit)

$$a = u \cdot \cancel{b_i} \cdot a_2 a_3 \cdots a_n = b_1 \cdot b_2 \cdots \cancel{b_i} \cdots b_m$$

$$(ua_2)\, a_3 \cdots a_n = b_1 b_2 \cdots \cancel{b_i} \cdots b_m$$

Continue this process to show that every a_i is associate to a b_j, and the two factorisations are the same up to reordering and associates. ∎

Picture.