Ring Homomorphisms: Given two rings R, S, a function $\phi: R \to S$ is called a ring homomorphism if

① ϕ is a Group homomorphism.
$(\phi(a+b) = \phi(a) + \phi(b) \ \forall a, b \in R)$

② ϕ respects multiplication
$$\phi(ab) = \phi(a)\phi(b).$$

Note: If R is a ring with 1, $\phi(R)$ must be also,

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$$
$$\phi(b) = \phi(1 \cdot b) = \phi(1)\phi(b). \ \forall b \in R.$$

sim. $\phi(b) = \phi(b \cdot 1) = \phi(b)\phi(1)$ $\Rightarrow \phi(1)$ is the unit for the image $\phi(R)$.

An left ideal I of a Ring R is a subring such that $ab \in I \ \forall a \in R, b \in I$.

right ideal
two-sided ideal
similar.

for commutative rings, left ideals are two-sided (i.e. all ideals are two-sided).

Constructing ideals: given $S = \{a_1, \dots, a_n\} \subseteq R$, the ideal generated by S

$$= I(S) = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n : r \in R\}.$$

You can check that this forms an ideal.

factor ring / quotient ring :

Given Ring R (comm. with 1) and an ideal I,

R/I is the quotient ring, defined as

$$R/I = \{x + I : x \in R\}.$$

This does form a ring : It's definitely a group under $+$, because I is a subgroup of an abelian group.

$\forall x, y \in R$

$$(x+I)(y+I) = xy + Iy + xI + I^2$$

$$= xy + \underbrace{\underbrace{(y+x)I}_{\in I} + \underbrace{I^2}_{\in I,\ = I \text{ if } R \text{ has } 1.}}_{I}$$

$$= xy + I \in R/I.$$

We can check the other properties. ✓

Integral Domains : commutative rings with 1 with no zero divisors.

(eg: $\mathbb{Z}$, $\mathbb{Z}_p$ (p prime), $\mathbb{Z}[x]$ (polynomials with coefficients in $\mathbb{Z}$.), $\mathbb{Z}_p[x]$, $\mathbb{R}[x]$, $\mathbb{R}$, $\mathbb{Z}[i]$

$$(a+bi)(c+di) = 0$$

$$\Rightarrow |a+bi|\,|c+di| = 0$$

$$\sqrt{a^2+b^2}\,\sqrt{c^2+d^2} = 0$$

$$\Rightarrow a = b = 0 \text{ or } c = d = 0.$$

$\Rightarrow \mathbb{Z}[i]$ is an integral domain.

Not an integral domain but comm ring w/ 1:

$\mathbb{Z}_{10}$ $\quad 2 \cdot 5 = 0$

$\mathbb{Z} \times \mathbb{Z}$ $\quad (1,0)(0,5) = (0,0)$

If R is an integral domain, we can form the **field of quotients** $Q(R) = R \times (R \setminus \{0\}) / \sim$ with these additions and multiplications

(thinking secretly)

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{ax}{bx} = \frac{a}{b}$$

$$(a,b) + (c,d) = (ad+bc, bd)$$
$$(a,b)(c,d) = (ac, bd)$$

show well-defined

equivalence relation: $(ax, bx) \sim (a,b)$ if $x \neq 0$, $x \in R$.

Then $(1,1)$ is the unity

$(0,1)$ is the zero

every nonzero element is invertible!

The integral domain is inside $Q(R)$ as $(R, 1)$

$$Q(\mathbb{Z}) = \mathbb{Q}, \quad Q(\mathbb{Q}) \cong \mathbb{Q}.$$

Kinds of Ideals:

Prime Ideals: An ideal I of a c. ring with 1 is an ideal I s.t.

If $a \cdot b \in I$, then $a \in I$ or $b \in I$.

(eg In $\mathbb{Z}$, $m\mathbb{Z}$ is an ideal, but it's not a prime ideal unless m is prime. $a \cdot b \in I \Leftrightarrow a \cdot b = mk$

if this is prime $m | a$ or $m | b$.)

But eg $m = 6$

$4 \cdot 9 = 6 \cdot 6$

neither $6|4$ false

$6|9$ false.

A <u>maximal ideal</u> ~~Is~~ is an ideal I in R s.t. there does not exist a proper Ideal J $J \subsetneq R$ s.t. $I \subsetneq J \subsetneq R$..

A <u>principal ideal</u>. is an ideal generated by a single element.

eg In every c. ring with 1, $\langle 0 \rangle = \{0\}$ is a principle ideal,

Fix $a \in R$, $\langle a \rangle$ is principal.

ex. $\langle x \rangle$ in $\mathbb{R}[x]$ is principal.

also prime –

$\langle x \rangle = \{a_1 x + a_2 x^2 + \dots a_k x^k : k \geq 1, a_j \in \mathbb{R}\}$

if $a(x)b(x) \in \langle x \rangle$,

$\Rightarrow a(x) \in \langle x \rangle$ or $b(x) \in \langle x \rangle$,

$\langle 3, x \rangle$ is an ideal in $\mathbb{Z}[x]$.

$\rightarrow$ Not principal.