A ring A is a (non-empty) set with two operations (addition, and multiplication).

Notation:

Addition $\longleftrightarrow$ $+$

Multiplication $\longleftrightarrow$ proximity or $\cdot$

$\Big\}\ A \times A \longrightarrow A$

Moreover:

- A is an abelian group with addition
- Multiplication is associative $((xy)z = x(yz))$
- Multiplication is distributive over addition:

$$\left.\begin{aligned} x(y+z) &= xy + xz. \\ (x+y)z &= xz + yz \end{aligned}\right\} \text{Distributivity}$$

In this course we will only consider rings s.t.

(a) Multiplication is commutative

(b) A multiplicative identity exists (denoted 1 or 1_A)

Notation: The additive identity denoted 0 ← zero element

The multiplicative identity is denoted 1.

We ALLOW $1 = 0$.

Check that if A is as above $(1=0)$, then $A=0$.

Such a ring is denoted 0.

The additive inverse of x is denoted $-x$.

Ring homomorphisms

Let A and B be rings. A <u>ring homomorphism from A to B</u> is a map

$$f : A \longrightarrow B$$

such that

$$\left.\begin{array}{ll} \text{(i)} & f(x+y) = f(x) + f(y) \\ \text{(ii)} & f(xy) = f(x) f(y) \end{array}\right\} x, y \in A$$

$$\text{(iii)} \quad f(1) = 1$$

An <u>ideal</u> I in a ring A is an additive subgroup of A such that if $x \in A$, $y \in I$, then $xy \in I$.

Examples:

(1) Let $A = \mathbb{Z}$, the ring of integers.
Let $I = (3) := \{3n \mid n \in \mathbb{Z}\}$.
Then I is an ideal (check)

(2) In fact, if A is any ring and $x \in A$ is an element then

$$(x) := \{xa \mid a \in A\}$$

is an ideal.
Such ideals are called principal ideals.

(3) Let $A = \mathbb{Z}[X]$, the ring of polynomials in a variable X with coefficients in $\mathbb{Z}$.

$$\mathbb{Z}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid a_i \in \mathbb{Z}\}$$

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

<u>Claim</u>: I is an ideal of A.

- Let $3p_1 + Xq_1$, $3p_2 + Xq_2$ be elements in I.

Then

$$(3p_1 + Xq_1) - (3p_2 + Xq_2)$$
$$= 3(p_1 - p_2) + X(q_1 - q_2) \in I.$$

So I is an additive subgroup of A.

- Let $y = I$ and $a \in A$.

Since $y \in I$, it must be of the form
$$y = 3p + Xq$$
Then $ya = 3(pa) + X(qa) \in I$.

Check that I is not a principal ideal.

(4) Let $f : A \longrightarrow B$ be a ring homomorphism.

Let $I = \{a \in A \mid f(a) = 0\} =: \ker(f)$.

Then I is an ideal. Indeed, being the kernel of an additive group homomorphism, I is an additive subgroup of A. Moreover, if $x \in I$ and $a \in A$, then
$$f(xa) = f(x)f(a) = 0 \cdot f(a) = 0.$$
Hence $xa \in \ker(f) = I$. //

Example 4 is typical. Every ideal arises as the kernel of a ring homomorphism. The broad steps are as follows:

Let $I \subseteq A$ be an ideal.

- Since I is a subgroup of an abelian group (viz. A) therefore I is normal, and the quotient group A/I makes sense.

- Easy to see A/I is abelian.

- A/I is a ring: Let $x+I$ and $y+I$ be two elements of A/I. Define

$$(x+I)(y+I) := xy + I.$$

This is well-defined. Suppose $x+I = x'+I$.
Recall this happens if and only if $x - x' \in I$.
Hence $(x-x')\cdot y \in I$. Complete this!

Check that $xy + I = x'y + I$, i.e.
check that $xy - x'y \in I$.

$$xy - x'y = (x-x')y$$

So $xy + I = x'y + I$.
By symmetry, if $y + I = y' + I$, then $xy + I = xy' + I$.
Finally combine these to give $xy + I = x'y' + I$.

- Check with the above multiplication A/I is a ring.

- Next check that the map

$$\pi : A \longrightarrow A/I$$
$$a \longmapsto a + I$$

is a ring homomorphism.

- Finally check that $I = \ker(\pi)$.

An isomorphism $f: A \longrightarrow B$ between rings A & B is a ring homomorphism which is one-to-one and onto.

Dictionary

injective $\longleftrightarrow$ one-to-one

surjective $\longleftrightarrow$ onto

bijective $\longleftrightarrow$ one-to-one and onto.

Recall: A ring homomorphism $f: A \longrightarrow B$ is injective if and only if $\ker(f) = 0$.

Prime ideals: Let A be a ring. An ideal $\mathfrak{p}$ of A is called prime (or a prime ideal) if

- $\mathfrak{p} \neq A$
- If $x, y \in A$ are such that $xy \in \mathfrak{p}$, then either x or y is in $\mathfrak{p}$.

Lemma: I is a prime ideal of a ring A if and only if A/I is an integral domain.

Proof: Clear (check).

Definition: Let A be a ring. An ideal $\mathfrak{m}$ in A is said to be a maximal ideal of A if

- $\mathfrak{M} \neq A$
- If I is an ideal containing $\mathfrak{M}$, then either $I = A$ or $I = \mathfrak{M}$.

Lemma: An ideal I of a ring A is maximal if and only if A/I is a field.

Proof: Recall that k is a field if $k \neq (0)$ and every non-zero element is a unit. Let I be be maximal, and $k = A/I$. Then, since $I \neq A$, $A/I \neq 0$, and since 0 is the only proper ideal of A/I (I being maximal), and hence if $x \neq 0$ in A/I, then x must be a unit, (otherwise the ideal generated by x is of the form J/I, $J \supseteq I$, violating maximality).

Conversely if A/I is a field, then the only proper ideal of A/I is 0, which means the only proper ideal of A/I is I/I. Thus if $J \supseteq I$ is an ideal in A, then $J = A$ or $J = I$.

Corollary: Maximal ideals are prime.