Recall An ideal M in a ring R is maximal iff $M \subseteq I \subseteq R \Rightarrow (M = I \text{ or } I = R)$

An ideal P in a ring R is prime iff $ab \in P \Rightarrow (a \in P \text{ or } b \in P)$

We proved: For a commutative ring R

$I \subseteq R$ is maximal $\Leftrightarrow$ R/I is a field

$I \subseteq R$ is prime $\Leftrightarrow$ R/I is an integral domain.

Hence • maximal ideals are prime.

Also : There are prime ideals that are not maximal

(eg $\langle x \rangle \subseteq \mathbb{Z}[x]$)

Example $\langle 2, x \rangle \subseteq \mathbb{Z}[x]$ is a maximal ideal

Proof We argue that $\mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{Z}_2$.

Consider $\varphi : \mathbb{Z} \to \mathbb{Z}[x]/\langle 2, x\rangle$, $\varphi(k) = k + \langle 2, x\rangle$

Given $(a_0 + a_1 x + \cdots a_n x^n) + \langle 2, x\rangle \in \mathbb{Z}[x]/\langle 2, x\rangle$,

$a_1 x + \cdots + a_n x^n \in \langle x \rangle \subseteq \langle 2, x\rangle$.

$\Rightarrow (a_0 + a_1 x + \cdots + a_n x^n) + \langle 2, x\rangle = a_0 + \langle 2, x \rangle = \varphi(a_0)$

$\Rightarrow \varphi$ is onto

$\ker \varphi = \{a \in \mathbb{Z} \mid a + \langle 2, x\rangle = \langle 2, x \rangle\}$

Now $\forall a \in \mathbb{Z}$, $a \in \langle 2, x\rangle \Rightarrow \exists c_0, \ldots c_m, b_0 \ldots b_k \in \mathbb{Z}$ so that

$a = 2 \cdot (c_0 + c_1 x^1 + \cdots + c_m x^m) + x \cdot (b_0 + \cdots b_k x^k)$

$= 2c_0 +$ higher order terms

$\Leftrightarrow$ $a = 2c_0$ for some $c_0 \in \mathbb{Z}$ and h.o.t. $= 0$

Thus $\ker \varphi = 2\mathbb{Z}$.

1^{st} isomorphism theorem $\Rightarrow$ $\mathbb{Z}/2 \xrightarrow{\overline{\varphi}} \mathbb{Z}[x]/\langle 2, x\rangle$

$\overline{\varphi}(k + 2\mathbb{Z}) = k + \langle 2, x \rangle$

is an isomorphism.

Since $\mathbb{Z}_2$ is a field, so is $\mathbb{Z}[x]/\langle 2, x\rangle$

$\Rightarrow \langle 2, x \rangle \subseteq \mathbb{Z}[x]$ is maximal.

Recall In a commutative ring R an ideal $I \subseteq R$ is principal iff $I = aR = \langle a \rangle$ for some $a \in R$.

Definition An integral domain is a principal ideal domain (PID) iff every ideal is principal.

Ex $\mathbb{Z}$, $F[x]$ (where F is a field) are PID's.
$\mathbb{Z}[x]$ is not a PID: $\langle 2, x \rangle = \langle 2 \rangle + \langle x \rangle$ is not principal

PID's are nice rings. It would be useful to have a criterion for an integral domain to be a PID.

Definition An integral domain R has a division algorithm if there is a function $\delta : R \setminus \{0\} \to \mathbb{N}$ called the division function or a norm so that $\forall\, a, b \in R$, $b \neq 0$ $\exists\, q, r \in R$ with

1) $a = qb + r$
2) $r = 0$ or $\delta(r) < \delta(b)$ (Note $\delta(0)$ is not defined)

Note $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$. In particular $0 \in \mathbb{N}$!

Ex 1) $R = \mathbb{Z}$ $\delta(a) = |a|$ for all $a \in \mathbb{Z} \setminus \{0\}$.
2) $R = F[x]$, F a field. $\delta(p) = \deg p$

Claim $R = \mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ has a division algorithm

Proof Recall: if $z \in \mathbb{C}$, $z = a + ib$, $a, b \in \mathbb{R}$. Then $\bar{z} = a - ib$ and $|z|^2 = z\bar{z} = a^2 + b^2$.
Moreover, $\forall\, z, w \in \mathbb{C}$ $\overline{zw} = \bar{z} \cdot \bar{w}$. Hence
$$|zw|^2 = zw\,\overline{zw} = zw\,\bar{z}\,\bar{w} = z\bar{z}\,w\bar{w} = |z|^2 |w|^2.$$

Define $\delta : \mathbb{Z}[i] \to \mathbb{N}$ by $\delta(\alpha + i\beta) := |\alpha + i\beta|^2 = \alpha^2 + \beta^2$

Then $\forall u, v \in \mathbb{Z}[i]$, $\delta(uv) = |uv|^2 = |u|^2 |v|^2 = \delta(u)\delta(v)$.

We now argue: $\forall a, b \in \mathbb{Z}[i]$, $b \neq 0$ $\exists q, r \in \mathbb{Z}[i]$ so that

$$a = qb + r \quad \text{and} \quad \delta(r) < \delta(b)$$

"Recall" Given $x \in \mathbb{R}$ $\exists n \in \mathbb{Z}$ s.t. $x \in [n, n+1]$

Then $\min(x - n, n+1-x) \leq 1/2$

$\Rightarrow$ $\forall x \in \mathbb{R}$ $\exists m \in \mathbb{Z}$ s.t. $|x - m| \leq 1/2$

Now given $z = x + iy \in \mathbb{C}$ $\exists m, n \in \mathbb{Z}$ s.t. $|x-m| \leq 1/2$, $|y-n| \leq 1/2$.

And then

$$|(x+iy) - (m+in)|^2 = |(x-m) + i(y-n)|^2 \leq |x-m|^2 + |y-n|^2 \leq \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}$$

Therefore:

$$\boxed{\forall z \in \mathbb{C} \;\; \exists q \in \mathbb{Z}[i] \;\; \text{s.t.} \;\; |z - q|^2 \leq 1/2}$$

$$\Rightarrow \boxed{\forall a, b \in \mathbb{Z}[i], \; b \neq 0, \;\; \exists q \in \mathbb{Z}[i] \;\; \text{s.t.} \;\; \left|\tfrac{a}{b} - q\right| \leq 1/2}$$

Let $r = a - qb$. Then

$$|r|^2 = |a - qb|^2 = \left|b\left(\tfrac{a}{b} - q\right)\right|^2 = |b|^2 \left|\tfrac{a}{b} - q\right|^2 \leq \tfrac{1}{2}|b|^2 < |b|^2$$

i.e. $\delta(r) < \delta(b)$

Integral domains with the division algorithm are also called $\boxed{\text{Euclidean domains}}$

<u>Theorem 27.1</u> Any Euclidean domain R is a PID

i.e. any ideal in R is principal.

<u>Proof</u> Let $\delta : R \setminus \{0\} \to \mathbb{N}$ be the division function, $I \subset R$ an ideal.

If $I = 0$ (the zero ideal) then $I = \langle 0 \rangle$, so principal.

Suppose $I \neq 0$.

Consider $S = \{ \delta(x) \mid x \in I \text{ and } x \neq 0 \}$.

By well-ordering principle $\exists\, b \in I$ s.t. $\delta(b) = \min S$; this $b \neq 0$.

Given $a \in I$ $\exists\, q, r \in R$ s.t. $a = qb + r$ and

either $r = 0$ or $\delta(r) < \delta(b)$

Since $a, b \in I$ and I is an ideal, $r = a - qb \in I$.

Since $\delta(b) = \min S$, r has to be 0.

(If $r \neq 0$, $\delta(r) < \delta(b) = \min S$, contradiction). $\square$

Ex. $\mathbb{Z}[i]$ is a PID.

<u>Definition</u> Let R be a commutative ring.

$x \in R$ is <u>irreducible</u> iff $x \neq 0$, x is not a unit and $x = ab$
$\Rightarrow a$ is a unit or b is a unit.

$p \in R$ is <u>prime</u> iff $\langle p \rangle$ is a prime ideal;

(By this definition $0 \in R$ is prime since $\langle 0 \rangle$ is a prime ideal)

<u>Lemma 27.2</u> Let R be a commutative ring, $p \in R$. Then

$\langle p \rangle$ is a prime ideal (and p is prime) iff

p is not a unit and $(p \mid ab \Rightarrow p \mid a$ or $p \mid b)$

<u>Proof</u> Recall that $x \in (p) \Leftrightarrow x = qp$ for some $q \in R \Leftrightarrow p \mid x$.

Also $\langle p \rangle \neq R \Leftrightarrow p$ is <u>not</u> a unit.

Now $\langle p \rangle$ is prime $\Leftrightarrow \langle p \rangle \neq R$ and $(ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle)$

Hence $\langle p \rangle$ is prime $\Leftrightarrow$ p is not a unit and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

<u>Lemma 27.3</u> In an integral domain R nonzero primes are irreducibles.

<u>Proof</u> Suppose $p \in R$ is prime, $p \neq 0$ and $p = ab$ for some $a, b \in R$.

Then $p \mid a$ or $p \mid b$. Say $p \mid a$. Then $a = qp$ for some q. $\Rightarrow p = qpb$

$\Rightarrow 0 = p(1 - qb)$. Since R is an integral domain and $p \neq 0$

$1 - qb = 0$. $\Rightarrow b$ is a unit.

Similarly if $p \mid b$, a is a unit. $\Big\} \Rightarrow p$ is irreducible.