3 lectures ago, introduced prime ideals
let's say more about them.

R = comm. ring.

Def. An ideal $P \subsetneq R$ is prime
if $ab \in P$ implies $a \in P$ or $b \in P$

Def an element $p \in R$
is prime iff the ideal $\langle p \rangle$ is prime.

equiv: p is not a unit
and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

(p sat. the conclusion of Euclid's lemma.)

non-zero? not a zero-divisor?

Def an element $r \in R$ is irreducible
if r is not a unit and
$r = ab$ implies a is a unit
or b is a unit

equiv: r is reducible if can write $r = a \cdot b$
where a, b are not units.

Prop If R is an integral domain and
p is prime then p is irreducible.
a non-zero

Pf: Suppose $p = a \cdot b$. Then $p \mid ab$,
so $p \mid a$ or $p \mid b$

if $p|a$, write $a = cp$

then $p = a \cdot b = c \cdot p \cdot b$

so $p(1 - c \cdot b) = 0$

so either $p = 0$ or $1 - cb = 0$

so $cb = 1$

so b is a unit. ☐

Prop R is an integral domain iff 0 is prime.

Pf Observe that $0|r$ iff $r = 0 \cdot$ (something) iff $r = 0$.

Now R is an int. domain
iff $ab = 0$ implies $a = 0$ or $b = 0$
iff $0|ab$ implies $0|a$ or $0|b$
iff 0 is prime. ☐

Prop. An ideal $P \subset R$ is prime iff R/P is an integral domain.

Proof: R/P is an integral domain means:
$\forall\, a, b \in R/P$, if $ab = \bar{0}$ then $a = \bar{0}$ or $b = \bar{0}$

write $a = \bar{r}$ and $b = \bar{s}$ for some $r, s \in R$

equiv: $\forall\, r, s \in R$, if $\bar{r}\bar{s} = \bar{0}$ then $\bar{r} = \bar{0}$ or $\bar{s} = \bar{0}$

equiv: $\forall\, r, s \in R$, if $rs \in P$ then $r \in P$ or $s \in P$ ☐

Example: studied $P = \langle 3, 1-\sqrt{-5} \rangle \subset R = \mathbb{Z}[\sqrt{-5}]$

had $\varphi: \mathbb{Z}[\sqrt{-5}] \twoheadrightarrow \mathbb{Z}_3$ surj. hom.
with $\ker \varphi = P$

by 1st iso thm, $R/P \cong \mathbb{Z}_3$

$\mathbb{Z}_3$ is an int. domain so P is prime.

seen: in an int. domain, prime (and nonzero) implies irreducible.

Thm: if R admits a division algorithm,
e.g. $R = \mathbb{Z}$ or $\mathbb{Q}[x]$ or $\mathbb{Z}[i]$,

then irreducible $\Rightarrow$ prime.

Pf: read the pf of Euclid's lemma. □

But in $\mathbb{Z}[\sqrt{-5}]$, seen that $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible
but they're not prime.

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

another example: $3 \cdot 3 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$

$2+\sqrt{-5}$ is irred. because if $2+\sqrt{-5} = z \cdot w$

then $9 = |z|^2 \cdot |w|^2$ so either $|z|^2 = 1 \rightsquigarrow z = \pm 1$
$|w|^2 = 1 \rightsquigarrow w = \pm 1$
or $|z|^2 = |w|^2 = 3$ $\rightsquigarrow$ impossible.

Also seen: in a ring w/ a division alg, every ideal is principal.

given $I \subset R$, $\exists\, a \in R$ s.t. $I = \langle a \rangle$
(the Euclidean algor.)

Project: | In an int. domain where every ideal is principal (a principal ideal domain PID)

irreducible implies prime.

In $R = \mathbb{Z}[\sqrt{-7}]$, 3 is not prime.

so $R/\langle 3 \rangle$ should not be an int. domain.

what is it?

let $J = \langle 3, 1+\sqrt{-5} \rangle$ $K = \langle 3, 1-\sqrt{-5} \rangle$

know: $R/J \cong \mathbb{Z}_3$ $R/K \cong \mathbb{Z}_3$

$J \cdot K = \langle 3 \rangle$ $J + K = \langle 1 \rangle$

bec. $1+\sqrt{-5} + 1-\sqrt{-5} = 2$
and $3 - 2 = 1$.

if $J+K = \langle 1 \rangle$ then $J \cap K = J \cdot K$

Final version of the Chinese Remainder Thm:

if R is a comm. ring

and $J, K \subset R$ are ideals with

$J + K = \langle 1 \rangle$

then $R/J \cdot K \cong R/J \times R/K$

example: ① above, $R/\langle 3 \rangle = \mathbb{Z}_3 \times \mathbb{Z}_3$ (not an int. domain!)

② $R = \mathbb{Z}$, $J = \langle 2 \rangle$ $K = \langle 3 \rangle$

$\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$

③ $R = \mathbb{Q}[x]$ $J = \langle x-5 \rangle$ $K = \langle x-6 \rangle$ $J + K = \langle 1 \rangle$

$\mathbb{Q}[x]/\langle x^2 - 11x + 30 \rangle \cong \mathbb{Q}[x]/\langle x-5 \rangle \times \mathbb{Q}[x]/\langle x-6 \rangle$

$\cong \mathbb{Q} \times \mathbb{Q}$

Proof: Consider the map $R \xrightarrow{\varphi} R/J \times R/K$

defined by $\varphi(r) = (\bar{r}, \bar{r})$ (in R/J! in R/K!)

check: φ is a hom.

$\ker \varphi$? $\varphi(r) = (\bar{0}, \bar{0})$

iff $r \in J$ and $r \in K$

iff $r \in J \cap K$.

$J + K = \langle 1 \rangle$, so $J \cap K = J \cdot K$.

next I claim that φ is surjective.

let $\bar{a} \in R/J$, $\bar{b} \in R/K$. $a, b \in R$

because $J+K = \langle 1 \rangle$, we can write

$1 = j + k$ for $j \in J$, $k \in K$.

then $a = aj + ak$, so $\bar{a} = \overline{ak}$ in R/J

and $b = bj + bk$, so $\bar{b} = \overline{bj}$ in R/K

let $r = ak + bj$

then in R/J we have $\bar{r} = \overline{ak} = \bar{a}$

and in R/K, $\bar{r} = \overline{bj} = \bar{b}$

so $\varphi(\bar{r}) = (\bar{a}, \bar{b}) \in R/J \times R/K$.

Now by 1st iso thm,

$R/\ker\varphi \cong \operatorname{im}\varphi$

$R/J\cdot K \cong R/J \times R/K$ as desired. ∎