Prop Assume R is commutative. P is a prime ideal iff R/P is an integral domain.

Pf: "translate definition of prime ideal into language of quotients"

Prop: Every maximal ideal is a prime ideal (R commutative)

Pf: Maximal $\Rightarrow R/M$ is a field & integral

R commutative

Integral domain is a ring with no zero div (except 0).

Euclidean domain is an I.D. with a division algorithm that is $\forall a, b \in R$ s.t. $b \neq 0$ there is a norm on $N: R \to \mathbb{Z}^+$ with $a = qb + r$ and $r = 0$ OR $N(r) < N(b)$

q is called quotient r is called remainder

Examples: Fields are E.D. $N(a) = 0$

$\mathbb{Z}$ is a E.D. with $N(a) = |a|$

$F[x]$ where F is a Field is E.D. $N(p(x)) =$ degree of $p(x)$

$\mathbb{Z}[x]$ is not a E.D.

Need to do examples:

$\mathbb{Z}_2[x]/(1+x+x^2)$ on Sage

$\mathbb{R}[x]/(1+x^2) \cong \mathbb{C}$

Euclidean algorithm -

Example $\gcd(18, 30)$

$30 = 1 \cdot 18 + 12$

$18 = 1 \cdot 12 + 6$

$12 = 2 \cdot 6$ so 6 is the $\gcd(18,30)$

$6 = 18 - 1 \cdot 12$
$12 = 30 - 18$
$\Rightarrow 6 = -1 \cdot 30 + 2 \cdot 18$

So $6 \in (18,30) = (6)$

Now generalize this to Euclidean Domain

this shows that every E.D. is a P.I.D.

Examples: $\mathbb{R}[x]$ is a E.D.

x^3+1 and x^2+2x+1 show $(x^3+1, x^2+2x+1) =$

$x^3+1 = x(x^2+2x+1) - 2x^2 - x + 1$

$x^2+2x+1 = -\frac{1}{2}(-2x^2 - x + 1) + \frac{3}{2}x + \frac{3}{2}$

$-2x^2 - x + 1$

There are integral domains that are not E.D. eg. $\mathbb{Z}[x]$

Gave example to compute $\gcd(2, x)$

$P \subseteq R$ is a prime ideal if $1 \notin P$ (i.e. $P \neq R$ and if $ab \in P$ then either $a \in P$ or $b \in P$

Thm R commutative with 1

(1) $I \subseteq R$ is max $\Rightarrow$ I is PRIME

(2) I is max $\Leftrightarrow$ R/I is a field

(3) I is prime $\Leftrightarrow$ R/I is an I.D.

Pf: (2) we showed last time

(1) I is MAX $\Rightarrow$ R/I is a field
$\Rightarrow$ R/I is I.D. $\Rightarrow$ I is PRIME

if we show (3) but as I mentioned this foll
by translating notion of prime ideal into lan
of quotients.

$rs \in I \Leftrightarrow (r+I)(s+I) = I$

$\Rightarrow$ $r \in I$ OR $s \in I \Rightarrow r+I = I$ OR $s+I = I$

Fact If R is P.I.D. then

I PRIME $\iff$ I MAX

Just need to show "$\Rightarrow$"

Assume $I=(p) \subseteq (m)$ maximal $\subsetneq R$

then $p=rm \Rightarrow m \in (p)$ OR $r \in (p)$

if $m \in (p)$ then $(m)=(p)$
if $r \in (p)$ then $r=ps$ and $p=psm$ and $sm=$
so m is a unit and then $(m)=R$ (not poss

Fact R is a field $\iff$ $R[x]$ is a P.I.D.

we discussed "$\Rightarrow$" as an example since

R field $\Rightarrow R[x]$ is E.D. $\Rightarrow R[x]$ is P.I.D.

"$\Leftarrow$" because (x) is prime $\Rightarrow$
(x) is MAX $\Rightarrow$
$R[x]/(x) \cong R$ is Field

An element $r \in R$ is irreducible if $r=ab \Rightarrow$ a or uni

$p \in R$ is prime if (p) is PRIME

irreducible and prime are not same

EXAMPLE $R = \mathbb{Z}[i\sqrt{5}]$

$\gamma = 2 + i\sqrt{5}$ is an irreducible element

$\gamma(2 - i\sqrt{5}) = 9$ so $9 \in (\gamma)$ but $9 = 3 \cdot 3$ and $3 \notin (\gamma)$

In an I.D. p PRIME $\Rightarrow$ p irred.

$p = ab \Rightarrow a \in (p)$, $a = rp \Rightarrow p = prb \Rightarrow b$ unit
(since either $a \in (p)$ or $b \in (p)$)

In a P.I.D. p PRIME $\Leftrightarrow$ p irred.

"$\Leftarrow$" if r is irred (want to show (r) is p

(r) is contained in some maximal ideal (m)

$\Rightarrow r = ma$ with m not a unit (otherwise therefore a unit and $(r) = (m)$

(r) is maximal & we know maxim are PRIME.