Last time: R = (commutative) ring with 1

An ideal $I \subseteq R$ is prime iff $\forall a, b \in R$
$ab \in I \Rightarrow (a \in I \text{ or } b \in I)$

An ideal $M \subseteq R$ is maximal if $\forall$ ideal I with
$M \subseteq I \subseteq R$ either $M = I$ or $I = R$

R is an integral domain $\Leftrightarrow \forall a \in R, a \neq 0$
$ab = 0$ for some $b \in R \Rightarrow b = 0$

(Equivalently $ab = ac \Rightarrow b = c$. $\forall b, c \in R$)

We proved: (i) $I \subseteq R$ is prime $\Leftrightarrow$ R/I is an integral domain
(ii) $M \subseteq R$ is maximal $\Leftrightarrow$ R/M is a field.

(i) + (ii) $\Rightarrow$ any maximal ideal is prime

Not all prime ideals are maximal

Finite integral domains are fields

Lemma 32.1 If R is an integral domain then so is $R[x]$.

Proof Enough to show:
If $f(x), g(x) \in R[x]$ and $f, g \neq 0$, then $fg \neq 0$.

Suppose $f(x), g(x) \neq 0$.

Then $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ for some n, $a_0 \ldots a_n$, $a_n \neq 0$

$g(x) = b_0 + b_1 x + \cdots + b_m x^m$ for some m, $b_0 \ldots b_m$, $b_m \neq 0$

Then $g(x)f(x) = a_m b_n x^{n+m} +$ lower order terms

Moreover, since R is an integral domain, $a_m, b_n \neq 0$

$a_m b_n \neq 0 \Rightarrow g(x)f(x) \neq 0$.

$\therefore R[x]$ is an integral domain.

Question Suppose F is a field, $I \subseteq F[x]$ an ideal

Then $I = \langle f \rangle := f F[x]$ for some $f \in F[x]$.

What condition on f guarantees that $\langle f \rangle$ is maximal?

Remark 32.2 For any commutative ring R, $a, b \in R$

$\langle a \rangle \subseteq \langle b \rangle \iff a \in \langle b \rangle \iff a = bq$ for some $q \in R$

$\iff$ "$b \mid a$."

Lemma 32.3 Let R be an integral domain, $a, b \in R$

$\langle a \rangle = \langle b \rangle \iff a = ub$ for some unit $u \in R$

Proof ($\Rightarrow$) $\langle a \rangle = \langle b \rangle \Rightarrow$ $a \mid b$ and $b \mid a$

$\Rightarrow$ $b = au$, $a = bv$ for some $u, v \in R$

$\Rightarrow$ $a = auv$ —//—

$\Rightarrow$ $1 = uv$ [integral domains have cancellation laws]

$\Rightarrow$ u, v are units

Conversely if $a = ub$ where u is a unit,

Then $b = u^{-1}a$.

$a = ub \Rightarrow b \in \langle a \rangle \Rightarrow \langle b \rangle \subseteq \langle a \rangle$

$b = u^{-1}a \Rightarrow a \in \langle b \rangle \Rightarrow \langle a \rangle \subseteq \langle b \rangle$

$\Rightarrow \langle a \rangle = \langle b \rangle$.

Definition Let R be an integral domain. $0 \neq a \in R$ is <u>irreducible</u> if

1) a is not a unit
2) $a = bc \Rightarrow$ b is a unit or c is a unit.

Ex $R = \mathbb{Z}$, $a \in \mathbb{Z}$, $a > 0$ is irreducible

$\Rightarrow$ a is a prime number.

Ex $x^2 + 1 \in \mathbb{R}[x]$ is irreducible

Reason For any field F, $u \in F[x]$ is a unit $\Rightarrow$

$\exists v \in F[x]$ s.t. $u \cdot v = 1 \Rightarrow 0 = \deg(uv) = \deg u + \deg v$

$\Rightarrow \deg u = 0 \Rightarrow u$ is a nonzero constant polynomial

If $x^2 + 1 = f(x)g(x)$ for some $f, g \in \mathbb{R}[x]$

Then $2 = \deg f + \deg g$. If $\deg f = 1$, $f(x) = ax+b$ for some $a, b \in \mathbb{R}$. $\Rightarrow r = -b/a$ is a root of $f(x)$ $\Rightarrow r^2+1 = f(r)g(r) = 0 \cdot g(r) = 0$. $\exists r \in \mathbb{R}$ s.t. $r^2 = -1$ which is impossible. $\Rightarrow \deg f = 0$ or $\deg f = 2$. If $\deg f = 0$, f is a unit. If $\deg f = 2$, $\deg g = 0 \Rightarrow$ g is a unit.

We will show: for any field F, if $p(x) \in F[x]$ is irreducible then $\langle p \rangle := p(x)F[x]$ is maximal. $\Rightarrow$ $F[x]/\langle p \rangle$ is a field.

—

Definition (Goodman 6.5.9) A principal ideal domain (PID) is an integral domain R so that every ideal I in R is principal: $\exists a \in R$ so that $I = \langle a \rangle$.

Examples · $\mathbb{Z}$ is a PID

· For any field F, $F[x]$ is a PID

Not all integral domains are PID.

Ex $\mathbb{R}[x]$ is an integral domain. By 32.1, the ring $\mathbb{R}[x,y] = (\mathbb{R}[x])[y]$ = polynomial in 2 variables with real coefficients is a PID.

The ideal $I = \langle x \rangle + \langle y \rangle$ is not principal: $\nexists\, p(x,y) \in \mathbb{R}[x,y]$ so that

$$x = p(x,y)\,q(x,y)$$
$$y = p(x,y)\,q'(x,y)$$

for some $q, q' \in \mathbb{R}[x,y]$.

PID's have many nice properties.

Definition (Goodman 6.5.5) Let R be an integral domain, $p \in R$ is **prime** if $p \neq 0$, p is not a unit and

$$p \mid (ab) \Rightarrow p \mid a \text{ or } p \mid b.$$

Lemma 32.4 (Goodman, 6.5.18) Let R be an integral domain, $p \in R$, $p \neq 0$, p not a unit. Then

(a) $\langle p \rangle$ is maximal $\Rightarrow$ $\langle p \rangle$ is prime $\Rightarrow$ p prime $\Rightarrow$ p irreducible

(b) if R is a PID then p irreducible $\Rightarrow$ $\langle p \rangle$ is maximal.

Proof (a). We've seen that any maximal ideal is prime.

- Suppose $\langle p \rangle$ is prime and $p \mid (ab)$. Then $ab = qp$ for some $q \in R$. $\Rightarrow ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ (hence $p \mid a$) or $b \in \langle p \rangle$ (and then $p \mid b$).
- Suppose p is prime and $p = ab$. Since p is prime, $p \mid a$ or $p \mid b$. Say $p \mid a$. Then $a = qp$ for some $q \in R$.

  $\Rightarrow p = ab = pqb$. Since R is an integral domain, we can cancel p's. $\Rightarrow 1 = qb$. $\Rightarrow b$ is a unit.

(b) Suppose p is irreducible and $\langle p \rangle \subseteq J \subseteq R$.

Since R is a PID, $J = \langle a \rangle$ for some $a \in R$. $\langle p \rangle \subset \langle a \rangle$ $\Rightarrow p \neq ab$ for some $b \in R$ (see Remark 32.2)

Since p is irreducible, either b is a unit (and then $J = \langle a \rangle = \langle p \rangle$ by 32.3) or a is a unit (and then $J = \langle a \rangle = R$).