Last time • Proved division algorithm for $F[x]$, F a field.
• Proved that if $p(x) \in F[x]$ and $ev_\alpha(p) = 0$, then $(x-\alpha) \mid p$
• Proved that $F[x]/\langle p \rangle = \{ r + \langle p \rangle \mid r \in F[x], \deg r < \deg p \}$

Something that I should have defined earlier:

Definition Let R_1, R_2 be two rings. Their product $R_1 \times R_2$ is the abelian group $R_1 \times R_2$ with multiplication defined coordinate-wise:
$(a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot a_2, b_1 b_2)$
Then $R_1 \times R_2$ is a ring.

Remarks 1) The operations on $R_1 \times R_2$ are defined so that the two projections
$\pi_1 : R_1 \times R_2 \to R_1$, $\pi_1(a,b) = a$
and $\pi_2 : R_1 \times R_2 \to R_2$, $\pi_2(a,b) = b$
are ring homomorphisms.
2) $(a,0) \cdot (0,b) = (a \cdot 0, 0 \cdot b) = (0,0)$, so $R_1 \times R_2$ has zero divisors. In particular $R_1 \times R_2$ is never a field.

Definition Let R be a ring and $M \subseteq R$ an ideal. M is maximal if (1) $M \neq R$ and (2) for any ideal $I \subseteq R$ with $M \subseteq I \subseteq R$ either $I = M$ or $I = R$ (i.e., there is no ideal I with $M \subsetneq I \subsetneq R$)

Ex Let F be a field. Then $0 = \{0\}$ is a maximal ideal.
Proof The only ideals in a field F are 0 and F.

We will prove: Let R be a comm. ring and $M \subseteq R$ an ideal. Then R/M is a field $\iff$ M is maximal.

Definition (sum of two ideals) Let R be a ring, $I, J \subseteq R$ ideals.

We define $I+J = \{ i+j \mid i \in I, j \in J \}$, and call it the Sum of I and J.

Exercise $I+J$ is an ideal.

Lemma 26.1 Let $f: R \to S$ be a surjective ring homomorphism. Then for any ideal $I \subseteq R$, $f(I) = \{ f(i) \mid i \in I \}$ is an ideal in S.

Proof We know that $f(I)$ is a subgroup of $(S, +, 0)$.
Need to check: $\forall s \in S$, $\forall x \in f(I)$ $sx, xs \in f(I)$.
Since f is onto, $s = f(r)$ for some $r \in R$. Since $x \in f(I)$, $x = f(i)$ for some $i \in I$. $\Rightarrow$ $sx = f(r)f(i) = f(ri) \in f(I)$
since I is an ideal (which forces $ri \in I$)
Similarly $xs \in f(I)$ □

WARNING if f is not onto, this is false: let $R = \mathbb{Z}$, $S = \mathbb{Q}$
$f: \mathbb{Z} \to \mathbb{Q}$ the inclusion: $f(n) = n$ $\forall n \in \mathbb{Z}$.
$\forall k \in \mathbb{Z}$ $k\mathbb{Z}$ is an ideal in $\mathbb{Z}$. But $\mathbb{Q}$ is a field, so its only ideals are 0 and $\mathbb{Q}$.

Lemma 26.2 Let M be an ideal in a commutative ring R. Then M is maximal $\Leftrightarrow$ R/M is a field.

Proof ($\Rightarrow$) Suppose M is maximal, $a+M \in R/M$, $a+M \neq 0+M$.
Then $a \notin M$. Consider the sum $\langle a \rangle + M$. It's an ideal and
$$M \subseteq \langle a \rangle + M \subseteq R.$$
Since $a \notin M$, $M \neq \langle a \rangle + M$ (otherwise $a = a+0 \in \langle a \rangle + M = M$)
Since M is maximal, $\langle a \rangle + M = R$. Since $1 \in R$
$\exists\ x \in \langle a \rangle$, $y \in M$ s.t. $x+y = 1$, ie $x - 1 = y \in M$
Since $x \in \langle a \rangle$, $x = ab$ for some $b \in R$. $\Rightarrow$ $ab - 1 \in M$.

$\Rightarrow$ $1+M = ab+M = (a+M)(b+M)$

$a+M$ is a unit in R/M. $\Rightarrow$ R/M is a field.

($\Leftarrow$) Suppose R/M is a field, $I \subseteq M$ an ideal with $M \subseteq I \subseteq R$

Since $\pi: R \to R/M$ is onto, $\pi(M) \subseteq \pi(I) \subseteq \pi(R) = R/M$ are ideals in R/M. $\pi(M) = \{0\}$, the zero ideal in R/M.

Since R/M is a field, either $\pi(I) = \{0\}$

or $\pi(I) = R/M$.

If $\pi(I) = R/M$, $\forall r \in R$ $\exists i \in I$ s.t. $i+M = r+M$

$\Rightarrow$ $r = i+m$ for some $m \in M \subseteq I$ $\Rightarrow$ $r \in M$ $\Rightarrow$ $R \subseteq M$.

So $\pi(I) = R/M \to M = R$.

Similarly if $\pi(I) = \{0\} = \{0+M\}$, $\forall i \in I$, $i+M = M$. $\Rightarrow i \in M$. $\Rightarrow I \subseteq M$

and then, since $M \subseteq I$, $I = M$.

$\therefore$ M is maximal in R. □

Ex We've seen: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ n is prime.

Therefore $n\mathbb{Z} \subseteq \mathbb{Z}$ is maximal $\Leftrightarrow$ n is prime. by 26.2

Note: If I is an ideal with $n\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$ then $I = m\mathbb{Z}$ for some m

And $n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow n \in m\mathbb{Z} \Leftrightarrow n = km$ for some $k \in \mathbb{Z} \Leftrightarrow m \mid n$.

So if n is prime and $m \mid n$ then $m = n$ or $m = 1$

If $m = 1$, $m\mathbb{Z} = \mathbb{Z}$. If $m = n$, $m\mathbb{Z} = n\mathbb{Z}$.

So conclusion of 26.2 agrees with what we knew.

Ex $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ and $\mathbb{Z}$ is not a field.

By 26.2 $\langle x \rangle \subseteq \mathbb{Z}[x]$ is not a maximal ideal

And indeed $\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$.

Definition An ideal P in a commutative ring R is prime

if $I \neq R$ and $\forall a, b \in R$ $ab \in P \Rightarrow a \in P$ or $b \in P$ [or both].

Ex If $p \in \mathbb{Z}$ is prime $p\mathbb{Z} \neq \mathbb{Z}$ and $ab \in p\mathbb{Z} \Rightarrow ab = kp$ for some $k \in \mathbb{Z}$
$\Rightarrow p \mid (ab) \Rightarrow p \mid a$ or $p \mid b$ (since p is prime)
$\Rightarrow a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$
$\Rightarrow p\mathbb{Z}$ is a prime ideal

Ex For any integral domain R, $0 = \{0\} \subseteq R$ is a prime ideal.
This is because $ab \in 0 \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$
(since R is an integral domain) $\Rightarrow a \in 0$ or $b \in 0$.

Lemma 26.3 Let I be an ideal in a comm. rng R. Then
I is prime $\Leftrightarrow$ R/I is an integral domain.
Proof ($\Rightarrow$) Suppose I is prime and $(a+I)(b+I) = 0+I$ in R/I
Then $ab + I = I \Rightarrow ab \in I$. Since I is prime, $a \in I$ or $b \in I$.
But then $a+I = 0+I$ or $b+I = 0+I$.
$\therefore$ R/I is an integral domain.
($\Leftarrow$) Suppose R/I is an integral domain and $ab \in I$. Then
$0+I = ab+I = (a+I)(b+I)$
Since R/I is a domain, either $a+I = 0+I$ (and then $a \in I$)
or $b+I = 0+I$ (and then $b \in I$)
$\therefore$ I is prime.

Ex $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z} \Rightarrow \langle x \rangle$ is prime in $\mathbb{Z}[x]$

Corollary 26.4 Any maximal ideal M in a comm rng R is prime.
Proof M maximal $\Rightarrow R/M$ is a field $\Rightarrow R/M$ is an integral domain. $\Rightarrow M$ is prime.