Last time: • If I is an ideal in a ring R then R/I is a ring and $\pi: R \to R/I$, $\pi(a) = a+I$ is a ring homomorphism.

• 1st isomorphism theorem: $\varphi: R \to S$ unital homomorphism, $I = \ker\varphi$. Then $\bar{\varphi}: R/I \to \varphi(R)$, $\bar{\varphi}(a+I) = \varphi(a)$ is an isomorphism of rings.

• if R is commutative then $aR := \{ar \mid r \in R\}$ is an ideal in R.

Aside if $\{I_\alpha\}_{\alpha\in A}$ is a family of ideals in a ring R then
$$I = \bigcap_{\alpha \in I} I_\alpha$$
is also an ideal. (exercise)

Hence $\forall$ set S, $\langle S \rangle = \bigcap_{\substack{I \text{ ideal} \\ S \subseteq I}} I$ is an ideal.

It's the smallest ideal containing the set S.

Not hard to show: if $S = \{a\}$, and R is commutative then
$$\langle \{a\} \rangle = aR.$$

Definition Let R be a ring. An element $b \in R$ is a <u>zero divisor</u> if $b \neq 0$ and $\exists\, a \in R$, $a \neq 0$ so that either $ab = 0$ or $ba = 0$. (or both)

Ex $R = M_2(\mathbb{R})$ $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Then $b^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
$\Rightarrow$ b is a zero divisor.

Ex $R = \mathbb{Z}_6$. Then $[2], [3], [4]$ are zero divisors since $[2][3] = [0]$ and $[3][4] = [12] = [0]$.

Lemma 24.1 Let R be a ring. Then
$\{a \in R \mid a \text{ is a zero divisor}\} \cap \{u \in R \mid u \text{ a unit}\} = \emptyset$.

Proof Suppose b is a zero divisor and a unit.

Then $\exists a \in R$, $a \neq 0$ s.t. $ab = 0$ or $ba = 0$. Say $ab = 0$.
Since b is a unit, $\exists v \in R$ s.t. $bv = 1$. And then
$$0 = 0v = (ab)v = a(bv) = a$$
Contradiction since $a \neq 0$. $\square$

Ex In $\mathbb{Z}$, ± 1 are units and there are no zero divisors.
So $2 \in \mathbb{Z}$ is neither a unit nor a zero divisor.
In $\mathbb{Z}_6[x]$, $x = [1]x$ is neither a unit nor a zero divisor.

Lemma 24.2 Let R be a ring, $a \in R$ s.t. $a \neq 0$ and $ax = 0 \Rightarrow x = 0$ $\forall x \in R$.
Then $ab = ac \Rightarrow b = c$ for all $b, c \in R$.

Proof $ab = ac \Rightarrow 0 = ab - ac = a(b-c)$. Hence $b - c = 0$ by the property of a. $\Rightarrow b = c$. $\square$

Definition A ring R is an integral domain iff
1) R is commutative
2) R has no zero divisors

Note: 1) For any integral domain R, $\forall a \in R$, $a \neq 0$
$$ab = ac \Rightarrow b = c$$
by 24.2.
2) Any subring of an integral domain is an integral domain.
3) Any field is an integral domain since any nonzero element in a field is a unit.

Lemma 24.3 Any finite integral domain is a field.

Proof Let D be a finite integral domain, $a \in D$, $a \neq 0$.
Consider $f: D \to D$, $f(b) = ab$.
Then $ab = ac \Rightarrow b = c$. $\Rightarrow f$ is injective

Since D is finite, f has to be surjective $\Rightarrow \exists v \in D$
s.t. $1 = f(v) = av$ $(= va)$
$\Rightarrow$ a is a unit.
$\therefore$ D is a field. $\square$

Lemma 24.4 $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime
Hence $\mathbb{Z}_p$ is a field $\Leftrightarrow$ p is prime.

Proof $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$
$\forall k, \ell \in \mathbb{Z}$ $[k][\ell] = [0] \Rightarrow [k] = [0]$ or $[\ell] = [0]$
$\Leftrightarrow$ $\forall k, \ell \in \mathbb{Z}$ $n \mid k\ell \Rightarrow n \mid k$ or $n \mid \ell$
$\Leftrightarrow$ n is prime. $\square$

Proposition 24.5 Let D be an integral domain. Then
$\forall f, g \in D[x]$, $\deg(fg) = \deg f + \deg g$.

Proof If f or g is zero, nothing to prove: $-\infty = -\infty$.
Suppose $f, g \neq 0$. Then $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ for some n,
some $a_0, \ldots a_n$ with $a_n \neq 0$,
$g(x) = b_0 + b_1 x + \cdots + b_m x^m$, some m, some $b_1 \ldots b_m$, $b_m \neq 0$.
And then
$f(x) g(x) = a_n b_m x^{n+m}$ + lower order terms.
Since D is an integral domain, $a_n, b_m \neq 0$, $a_n \cdot b_m \neq 0$
$\Rightarrow \deg(fg) = n + m = \deg f + \deg g$ $\square$

Definition An ideal I in a ring R is principal if
$I = \langle a \rangle$ for some $a \in R$
(If R is commutative, $I = \langle a \rangle \Leftrightarrow I = aR$)

In $\mathbb{Z}$ all ideals are principal. In $\mathbb{Z}[x]$ there are non principal ideals

<u>Claim</u> $\langle 2, x\rangle = \langle \{2, x\}\rangle \subseteq \mathbb{Z}[x]$ is <u>not</u> a principal ideal.

<u>Proof</u> Suppose $\langle 2, x\rangle = \langle p\rangle$ for some $p \in \mathbb{Z}[x]$

Then $2 \in \langle p\rangle$ hence $2 = pq$ for some $q \in \mathbb{Z}[x]$

$\Rightarrow 0 = \deg 2 = \deg pq = \deg p + \deg q \Rightarrow \deg p = \deg q = 0$

$\Rightarrow p, q \in \mathbb{Z}$. Since 2 is prime, $p = \pm 1$ or $p = \pm 2$.

Now $\langle 2, x\rangle = \{a(x)\cdot 2 + b(x)\cdot x \mid a, b \in \mathbb{Z}[x]\}$

$= \{2a_0 + x \cdot r(x) \mid a_0 \in \mathbb{Z},\ r(x) \in \mathbb{Z}[x]\}$

If $p = \pm 1$, $\langle p\rangle = \mathbb{Z}[x]$.

$\Rightarrow 1 \in \langle 2, x\rangle \Rightarrow \exists a_0 \in \mathbb{Z},\ r(x) \in \mathbb{Z}[x]$ s.t.

$$1 = 2\cdot a_0 + x\, r(x)$$

This is impossible since $2 \nmid 1$.

If $p = \pm 2$, then $x \in \langle \pm 2\rangle = 2\mathbb{Z}[x]$, i.e. $\exists b_0, \ldots b_n$ s.t.

$$x = 2b_0 + 2b_1 x + \cdots + 2b_n x^n \quad (\text{for some } n)$$

This is impossible again.

<u>Thm</u> (Division algorithm for $F[x]$, F a field)

Let F be a field, $f, g \in F[x]$, $g \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ s.t. 1) $f = qg + r$ and

2) $0 \leq \deg r < \deg g$.

<u>Corollary</u> Any ideal I in $F[x]$ (F a field) is principal: $\exists\, p \in F[x]$ s.t. $I = \langle p\rangle = pF[x]$.

<u>Proof</u> If $I = 0$, ie $I = \{0\}$, let $p = 0$. Otherwise let

$S = \{\deg f \mid f \in I, \deg f \geq 0\}$

Since $I \neq 0$, $S \neq \emptyset$. By well-ordering principle

$\exists n \in S$ s.t. $n = \min S$. Then $\exists p \in I$ s.t. $n = \deg p$. Note: $p \neq 0$!

For any $f \in I$ $\exists q, r$ s.t. $f = qp + r$, $\deg r < \deg p$.

Since $f, p \in I$, $r = f - qp \in I$. $\deg r < \deg p \Rightarrow \deg r \notin S$.

$\Rightarrow \deg r = -\infty$ and $r = 0$. $\Rightarrow f \in \langle p\rangle$. $\Rightarrow I \subseteq \langle p\rangle \subseteq I$.