Last time Suppose $f: R \to S$ is a homomorphism of rings.

(1) If $J \subseteq S$ is an ideal, then $f^{-1}(J)$ is an ideal in R

(2) If f is onto and $I \subseteq R$ is an ideal, then $f(I)$ is an ideal in S

(3) If $f: R \to S$ is onto, $I \subseteq R$ is an ideal then
$$f^{-1}(f(I)) = I + \ker f \quad (\text{sum of ideals})$$

Def An ideal M in a ring R is maximal if $M \neq R$ and there is no ideal $I \subseteq R$ with $M \subsetneq I \subsetneq R$. That is, if $M \subseteq I$ then either $M = I$ or $I = R$.

Lemma 30.3 (similar to 6.3.14) Let R be a commutative ring (with 1). An ideal $M \subseteq R$ is maximal $\Leftrightarrow$ R/M is a field.

We proved: M maximal $\Rightarrow$ R/M is a field.

($\Leftarrow$) Suppose R/M is a field, $M \subseteq I$ for some ideal I.
Since $\pi: R \to R/M$ is onto, $\pi(I)$ is an ideal in R/M.
Since R/M is a field, $\pi(I)$ is either $\{0_{R/M}\}$ or R/M.
If $\pi(I) = \{0\}$, $\forall i \in I$, $0_{R/M} = \pi(i)$. $\Rightarrow$ $0 + M = i + M$
$\Rightarrow i \in M$. $\Rightarrow I \subseteq M$. $\Rightarrow I = M$ (since $M \subseteq I$).
If $\pi(I) = R/M$, $\pi^{-1}(\pi(I)) = \pi^{-1}(R/M) = R$
$\pi^{-1}(\pi(I)) = I + \ker \pi = I + M = I$ (since $M \subseteq I$)
$\therefore$ $I = R$ $\square$

Recall

Def 6.4.1 Let R be a commutative ring. A zero-divisor is $x \in R$ s.t. $x \neq 0$ and $\exists y \in R$ with $y \neq 0$, $xy = 0$.

Ex In $\mathbb{Z}_6$, $[2], [3], [4]$ are zero divisors.

Ex Let $R = \mathbb{R}[x]/I$ where $I = (x-1)(x+2)\,\mathbb{R}[x]$

Then $(x-1)+I$, $(x+2)+I$ are zero divisors in R:

$x-1$, $x+2 \notin I$ since if $g \in I$, $g = q(x)\cdot(x-1)(x+2)$
for some $q(x)$. $\Rightarrow \deg g \geq 2$ or $g = 0$,

But $\deg(x-1)$, $\deg(x+2) = 1 < 2$.

$\Rightarrow (x-1)+I \neq 0+I$, $(x+2)+I \neq 0+I$.

But $I = (x-1)(x+2)+I = ((x-1)+I)((x+2)+I)$

Definition A commutative ring R is an integral domain iff R has no zero divisors.

Thus in an integral domain R, $a \in R$, $a \neq 0$ and $ab = 0$ for some $b \in R$. $\Rightarrow b = 0$.

Lemma 31.1 Let R be an integral domain Suppose $a \in R$, $a \neq 0$. Then $ax = ay \Rightarrow x = y$ $\forall x, y \in R$

Proof $ax = ay \Rightarrow 0 = ax - ay = a\cdot(x-y)$

Since $a \neq 0$ and R is an integral domain, $x - y = 0$ $\square$

Theorem 31.2 Any finite integral domain is a field.

Proof Let R be an integral domain, $a \in R$, $a \neq 0$.

We want to show: $\exists\, b \in R$ s.t. $ab = 1$.

Consider $L_a : R \to R$, $L_a(x) = ax$

If $L_a(x) = L_a y$, $ax = ay$.

By Lemma 31.1, $x = y$. $\Rightarrow L_a$ is 1-1

Since R is finite, L_a is also onto.

$\Rightarrow \exists\, b \in R$ st. $L_a(b) = 1$

$\Rightarrow$ $ab = 1$ $\square$

Definition A ideal I in a commutative ring R is prime if $I \neq R$ and

$$ab \in I \Rightarrow a \in I \text{ or } b \in I \quad (\text{or both})$$

Ex $R = \mathbb{Z}$, $p \in \mathbb{Z}$ a prime, $I = p\mathbb{Z}$ is a prime ideal:

$$ab \in p\mathbb{Z} \Rightarrow ab = pk \text{ for some } k \in \mathbb{Z}$$

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

$$\Rightarrow a \in p\mathbb{Z} \text{ or } b \in p\mathbb{Z}.$$

Theorem 31.3 (6.4.11 in Goodman) An ideal I in a commutative ring R is prime $\Leftrightarrow$ R/I is an integral domain.

Proof ($\Rightarrow$) Suppose I is prime, $(a+I)(b+I) = 0+I$ in R/I

$$\Rightarrow ab + I = I \Rightarrow ab \in I \Rightarrow (a \in I \text{ or } b \in I)$$

$$\Rightarrow (a+I = 0+I \text{ or } b+I = 0+I)$$

($\Leftarrow$) Suppose R/I is an integral domain and $ab \in I$. Then $0+I = ab+I = (a+I)(b+I)$

Since R/I is an integral domain, either

$$a+I = 0_{R/I} = I \quad \text{or} \quad b+I = 0_{R/I} = I$$

In the first case $a \in I$. In the second case $b \in I$.

"Ex" For any prime $p \in \mathbb{Z}$, $p\mathbb{Z}$ is a prime ideal

$$\Rightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p \text{ is an integral domain.}$$

Remark Fields are integral domains.
Reason: if $ab=0$ and $a\neq 0$, then
$$b = a^{-1}ab = a^{-1}0 = 0.$$

Corollary 31.4 In a commutative ring R maximal ideals are prime.

Proof $M \leq R$ is maximal $\Rightarrow$ R/M is a field $\Rightarrow$ R/M is an integral domain. $\Rightarrow$ M is prime

WARNING Not all prime ideals are maximal.

Ex $\langle x\rangle = x\mathbb{Z}[x] \leq \mathbb{Z}[x]$

Note $\langle x\rangle = \ker\left(f : \mathbb{Z}[x] \to \mathbb{Z}\right.$, $\left. p \mapsto p(0)\right)$

1^{st} iso Thm $\Rightarrow$ $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$

$\mathbb{Z}$ is an integral domain and is not a field.
$\Rightarrow \langle x\rangle$ is not maximal.

In fact $\langle x\rangle \subsetneq \langle 2\rangle + \langle x\rangle$ since $2 \notin \langle x\rangle$
and $\langle 2\rangle + \langle x\rangle = \{a_0 + a_1x + \dots + a_nx^n \mid a_0 \text{ is even}\}$
$\neq \mathbb{Z}[x]$.