Last time Proved homomorphism (1^{st} isomorphism) theorem for rings: given a (unital) ring homomorphism $f: R \to S$, the map $\bar{f}: R/\ker f \to f(R) \leq S$, $\bar{f}(r + \ker f) = f(r)$ is a well-defined isomorphism of rings.

Ex $f: \mathbb{R}[x] \to \mathbb{C}$, $f(p) = p(\sqrt{-1})$

$\ker f = \langle x^2+1 \rangle := (x^2+1)\mathbb{R}[x]$

$\bar{f}: \mathbb{R}[x]/\langle x^2+1 \rangle \to \mathbb{C}$, $\bar{f}(p + \langle x^2+1 \rangle) = p(\sqrt{-1})$ is an isomorphism of rings.

Proposition 30.1 (compare with 6.3.7 in Goodman)

Suppose $f: R \to R'$ is a surjective ring homomorphism, $K = \ker f$. Then

(1) For any ideal $J' \leq R'$, $f^{-1}(J') := \{r \in R \mid f(r) \in J'\}$ is an ideal in R containing K.

(2) Conversely suppose $I \subseteq R$ is an ideal. Then $f(I) = \{f(i) \mid i \in I\}$ is an ideal in R'.

Remarks I. If $f: R \to R'$ is not onto then (2) is false:

$f: \mathbb{Z} \to \mathbb{R}$, $f(n) = n$, is a homomorphism of rings

$2\mathbb{Z}$ is an ideal in $\mathbb{Z}$, $f(2\mathbb{Z}) = 2\mathbb{Z}$ is not an ideal in $\mathbb{R}$

II. If $f: R \to R'$ is onto and $I \subseteq R$ is an ideal then $f^{-1}(f(I))$ is an ideal in R.

In general $f^{-1}(f(I))$ need not be I.

Ex $f: \mathbb{Z} \to \mathbb{Z}_4$ $f(n) = [n]$

$I = 3\mathbb{Z} \leq \mathbb{Z}$. $f(I) = [3]\mathbb{Z}_4 = \{[3][0], [3][1], [3][2], [3][3]\}$

$= \{[0], [3], [2], [1]\} = \mathbb{Z}_4$

so $f^{-1}(f(3\mathbb{Z})) = \mathbb{Z} \neq 3\mathbb{Z}$.

Proof of 30.1 (1) Since $0 \in J'$, $K = f^{-1}(0) \subseteq f^{-1}(J')$.

We now check that $f^{-1}(J')$ is an ideal in R.

If $x, y \in f^{-1}(J')$, $r \in R$ then $f(x), f(y) \in J'$.

$\Rightarrow$ $f(x-y) = f(x) - f(y) \in J'$ since J' is an ideal.

$\Rightarrow$ $x - y \in f^{-1}(J')$.

$f(rx) = f(r) f(x) \in J'$ since $f(x) \in J'$ and J' is an ideal.

$\Rightarrow$ $rx \in f^{-1}(J')$.

Similarly $xr \in f^{-1}(J')$.

$\therefore$ $f^{-1}(J')$ is an ideal in R.

[Note: the proof above works even if f is not onto]

(2) Suppose $a, b \in f(I)$. Then $a = f(x)$, $b = f(y)$ for some $x, y \in I$. $\Rightarrow$ $a - b = f(x) - f(y) = f(x-y) \in f(I)$ since $x - y \in I$.

Moreover $\forall\, r' \in R'$, $\exists\, r \in R$ st $r' = f(r)$ (since f is onto)

$\Rightarrow$ $r'x = f(r) f(a) = f(ra) \in f(I)$ since $ra \in I$.

Similarly $xr' \in f(I)$. □

Lemma 30.2 Suppose $f : R \to R'$ is a ring homomorphism, $K = \ker f$. For any ideal $I \subseteq R$,

$$f^{-1}(f(I)) = I + K$$

Proof $y \in f^{-1}(f(I)) \Leftrightarrow f(y) \in f(I)$

$\Leftrightarrow$ $f(y) = f(i)$ for some $i \in I$

$\Leftrightarrow$ $f(y) - f(i) = 0$ —//—

$\Leftrightarrow$ $y - i \in \ker f = K$

$\Leftrightarrow$ $y - i = k$ for some $k \in K$, $i \in I$

$\Rightarrow$ $y = i + k$ —//—

$\Rightarrow$ $y \in I + K$. □

Remark If $K \subseteq I$, then $f^{-1}(f(I)) = I + K = I$

Example Suppose $n > 0$, $0 < k < n$. Then $[k]\mathbb{Z}_n$ is an ideal in $\mathbb{Z}_n$. Q. What is the ring $\mathbb{Z}_n / [k]\mathbb{Z}_n$?

A. $\mathbb{Z}_n / [k]\mathbb{Z}_n$ is isomorphic to $\mathbb{Z} / \gcd(k,n)\mathbb{Z}$.

Proof Recall: $\forall a, b \in \mathbb{Z}$, $a, b \neq 0$, $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$.

Consider $f: \mathbb{Z} \to \mathbb{Z}_n / [k]\mathbb{Z}_n$, $f(\ell) = [\ell] + [k]\mathbb{Z}_n$

f is the composite of two surjective ring homomorphisms:

$f = \sigma \circ \pi$ where $\pi: \mathbb{Z} \to \mathbb{Z}_n$, $\pi(\ell) = [\ell]$

and $\sigma: \mathbb{Z}_n \to \mathbb{Z}_n / [k]\mathbb{Z}_n$, $\sigma([\ell]) = [\ell] + [k]\mathbb{Z}_n$.

$\Rightarrow$ f is onto.

Homomorphism Theorem $\Rightarrow$ $\bar{f}: \mathbb{Z} / \ker f \to \mathbb{Z}_n / [k]\mathbb{Z}_n$

$\bar{f}(\ell + \ker f) = f(\ell) = [\ell] + [k]\mathbb{Z}_n$

is an isomorphism.

$\ker f = (\sigma \circ \pi)^{-1}(0) = \pi^{-1}(\sigma^{-1}(0)) = \pi^{-1}([k]\mathbb{Z}_n)$

Now $\pi(k\mathbb{Z}) = [k]\mathbb{Z}_n$.

Hence $\pi^{-1}([k]\mathbb{Z}_n) = k\mathbb{Z} + \ker\pi = k\mathbb{Z} + n\mathbb{Z} = \gcd(k,n)\mathbb{Z}$.

$\Rightarrow$ $\ker f = \gcd(k,n)\mathbb{Z}$

$\Rightarrow$ $\bar{f}: \mathbb{Z} / \gcd(k,n)\mathbb{Z} \to \mathbb{Z}_n / [k]\mathbb{Z}_n$

is an iso.

Definition An ideal I in a ring R is proper if $I \neq \{0\}$ and $I \neq R$.

An ideal M in a ring R is maximal if $M \neq R$ and for any ideal $I \subseteq R$ with $I \neq R$

$M \subseteq I \Rightarrow M = I$.

"Ex" If F is a field, then $\{0\}$ is a maximal ideal:

Recall If $I \subseteq F$ is an ideal then $I = \{0\}$ or $I = F$.

So there are no ideals $I \leq F$ st $\{0\} \subsetneq I \subsetneq F$.

"Recall" In $\mathbb{Z}$, $a\mathbb{Z} \leq b\mathbb{Z} \Leftrightarrow a \in b\mathbb{Z} \Leftrightarrow a = bk$ for some k
$\Leftrightarrow b \mid a$

So if $a \in \mathbb{Z}$ is prime and I is an ideal with $a\mathbb{Z} \leq I$
Then $I = b\mathbb{Z}$ for some $b \geq 0$.

$a\mathbb{Z} \leq b\mathbb{Z} \Rightarrow b \mid a. \Rightarrow b = a$ or 1

$\Rightarrow I = a\mathbb{Z}$ or $I = \mathbb{Z}$.

$\therefore$ $a\mathbb{Z} \leq \mathbb{Z}$ is maximal for any prime $a \in \mathbb{N}$.

(compare with 6.3.14)

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

Corollary For any prime $p \in \mathbb{N}$, $\mathbb{Z}_p$ is a field.
Reason We've seen that if p is prime then $p\mathbb{Z} \leq \mathbb{Z}$ is maximal. By 30.3, $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ is a field.

Proof of 30.3 ($\Rightarrow$) Suppose $M \leq R$ is maximal, $a + M \neq 0 + M$ in R/M. We want to show: $\exists\, b \in R$ st $(a+M)(b+M) = 1 + M$
Since $a + M \neq 0 + M = M$, $a \notin M$. $\Rightarrow \langle a \rangle = aR \not\subseteq M$.

$\Rightarrow M \subsetneq \langle a \rangle + M$.

Since M is maximal $\langle a \rangle + M = R$. $\Rightarrow 1 \in \langle a \rangle + M$

$\Rightarrow 1 = x + m$ for some $m \in M$, $x \in \langle a \rangle = aR$. $\Rightarrow x = ab$ for some $b \in R$. $\Rightarrow$ $1 = ab + m$ for some $m \in M$

$\rightarrow$ $1 + M = ab + M = (a+M)(b+M)$.

($\Leftarrow$) Suppose R/M is a field, $M \leq I$ for some ideal I.
Then $\pi : R \to R/M$ is onto. $\Rightarrow \pi(I)$ is an ideal in R/M.
Since R/M is a field, $\pi(I) = \{0_{R/M}\}$ or $\pi(I) = R/M$.
If $\pi(I) = \{0_{R/M}\}$, $I = M$. If $\pi(I) = R/M$, $I = R$. ∎