Mon
2/10

Thm: Let R be a commutative ring with identity $1 \neq 0$. Let M be an ideal of R with $M \neq R$. Then M is maximal iff R/M is a field.

pf: We know from previous results that R/M is a commutative ring with identity $1+M \neq 0+M$.

($\Rightarrow$) Last time.

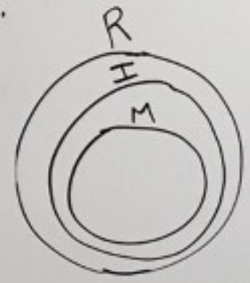
($\Leftarrow$) Suppose that R/M is a field.

We need to show that M is maximal.

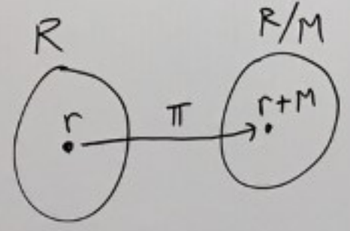
Let I be an ideal of R with

$M \subseteq I \subseteq R$

We need to show $M=I$ or $I=R$.



Consider the ring homomorphism $\pi: R \to R/M$ given by $\pi(r) = r+M$.

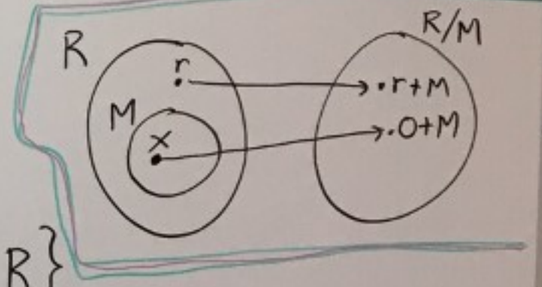


Applying π to $M \subseteq I \subseteq R$ we get $\pi(M) \subseteq \pi(I) \subseteq \pi(R)$.

Note that

$$\pi(M) = \{\pi(x) \mid x \in M\}$$
$$= \{x+M \mid x \in M\}$$
$$= \{0+M\}$$

$x+M = 0+M$ since $(x-0) \in M$

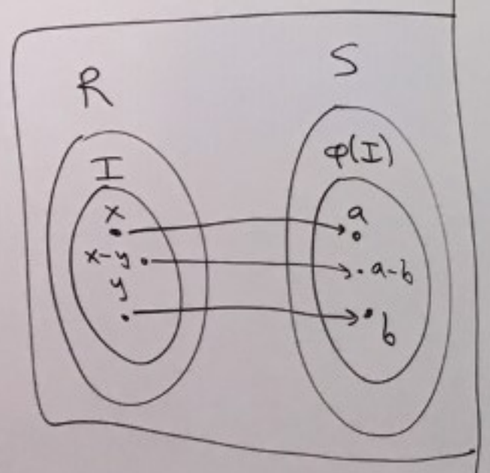


And, $\pi(R) = \{\pi(r) \mid r \in R\}$

$= \{r+M \mid r \in R\} = R/M$

So, $\pi(M) \subseteq \pi(I) \subseteq \pi(R)$ becomes $\{0+M\} \subseteq \pi(I) \subseteq R/M$.

Lemma: Let $\varphi: R \to S$ be an onto ring homomorphism and $I \subseteq R$ be an ideal. Then $\varphi(I)$ is an ideal of S.



proof:

(i) Since φ satisfies $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in S$, we know φ is a group homomorphism under $+$.
So, $\varphi(0_R) = 0_S$.
Thus, $0_S = \varphi(0_R) \in \varphi(I)$ since $0_R \in I$.

(ii) Let $a, b \in \varphi(I)$. Then there exist $x, y \in I$ with $\varphi(x) = a$ and $\varphi(y) = b$. Since I is an ideal, $x - y \in I$. So $a - b = \varphi(x) - \varphi(y) = \varphi(x) + \varphi(-y) = \varphi(x-y) \in \varphi(I)$.

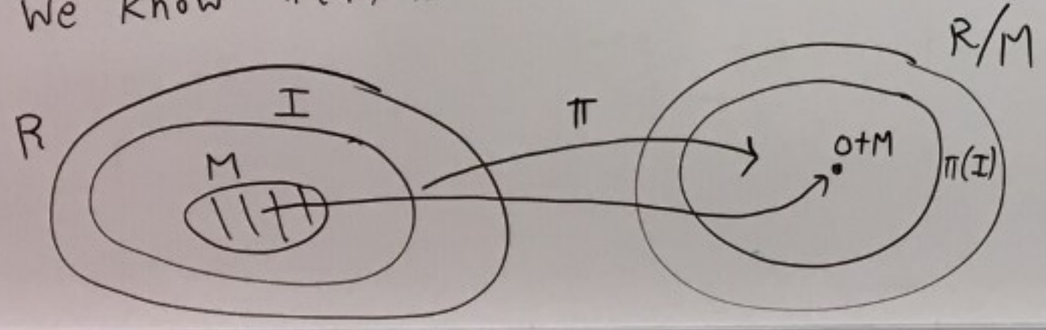
(iii) Let $c \in \varphi(I)$ and $s \in S$. Then there exists $z \in I$ with $\varphi(z) = c$. Since φ is onto, there exists $r \in R$ with $\varphi(r) = s$. Since I is an ideal, $rz \in I$ and $zr \in I$.
So, $sc = \varphi(r)\varphi(z) = \varphi(rz) \in \varphi(I)$ and $cs = \varphi(z)\varphi(r) = \varphi(zr) \in \varphi(I)$.

So by (i), (ii), (iii), $\varphi(I)$ is an ideal of S.

lemma

Back to the main proof ....

By the lemma, since π is onto (because $\pi(R) = R/M$), we know $\pi(I)$ is an ideal of R/M.



Since R/M is a field, its only ideals are $\{0+M\}$ or R/M.

So, either $\pi(I) = \{0+M\}$ or $\pi(I) = R/M$.

case 1: Suppose $\pi(I) = \{0+M\}$.

So, $\pi(i) = 0+M$ for all $i \in I$.

So, $i+M = 0+M$ for all $i \in I$.

Thus, $i = (i-0) \in M$ for all $i \in I$.

So, $I \subseteq M$.

Since $M \subseteq I$, we get $I = M$.

Case 2: Suppose $\pi(I) = R/M$.

We know $I \subseteq R$.

Let's show $R \subseteq I$.

Let $r \in R$.

Since $\pi(I) = R/M$ there exists $i \in I$ with $\pi(i) = r + M$.

So, $i + M = r + M$.

Then, $r - i \in M$.

But $M \subseteq I$, so $r - i \in I$.

Thus,

$$r = \underbrace{i}_{\text{in } I} + \underbrace{(r-i)}_{\text{in } I} \in I.$$

So, $R \subseteq I$.

Thus, $\boxed{I = R}$.

Summary: We assumed that I was an ideal with $M \subseteq I \subseteq R$. We showed either $I = M$ or $I = R$. So, M is maximal. ∎

Let $n \geq 2$.

Thm: $n\mathbb{Z}$ is maximal in $\mathbb{Z}$ iff n is prime.

Proof:

($\Rightarrow$) Suppose $n\mathbb{Z}$ is maximal in $\mathbb{Z}$.

We want that n is prime.

Suppose otherwise.

Then $n = ab$ with $1 < a < n$ and $1 < b < n$.

Then, $n\mathbb{Z} \subseteq a\mathbb{Z} \subseteq \mathbb{Z}$.

Since $1 < a$, then $a\mathbb{Z} \neq \mathbb{Z}$ (no 1 in here)

Since $a < n$, then $n\mathbb{Z} \neq a\mathbb{Z}$ ($n\mathbb{Z}$: no a in here)

Ex: $6 = 3 \cdot 2$

$6\mathbb{Z} \subseteq 3\mathbb{Z} \subseteq \mathbb{Z}$

Then, $n\mathbb{Z}$ is not maximal.

This is ridiculous! (ie a contradiction).

So, n is prime.

($\Leftarrow$) Suppose n is prime.

Let's show $n\mathbb{Z}$ is maximal in $\mathbb{Z}$.

Suppose I is an ideal of $\mathbb{Z}$ with $n\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$.

Since I is an ideal of $\mathbb{Z}$, $I = i\mathbb{Z}$ where $i \geq 1$.

So, $n\mathbb{Z} \subseteq i\mathbb{Z} \subseteq \mathbb{Z}$.

($n\mathbb{Z}$: n lives here, $n = n \cdot 1$)

So, $n \in i\mathbb{Z}$.

Thus, $n = i \cdot j$ where $j \geq 1$.

because $i \geq 1$ and $n \geq 1$

Since n is prime, either $i = 1$ or $i = n$.

If $i = n$, then $I = i\mathbb{Z} = n\mathbb{Z}$.

If $i = 1$, then $I = i\mathbb{Z} = \mathbb{Z}$.

So, $n\mathbb{Z}$ is maximal.

Corollary: Let $n \geq 2$.

n is prime iff $\mathbb{Z}/n\mathbb{Z}$ is a field.

pf: n is prime

iff $n\mathbb{Z}$ is maximal

iff $\mathbb{Z}/n\mathbb{Z}$ is a field. ∎

Ex: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

pf: $\pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(x) = \overline{x}$

π is a ring hom., $\ker(\pi) = n\mathbb{Z}$.

So, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(\pi) \cong \text{im}(\pi) = \mathbb{Z}_n$

$\mathbb{Z}_n$ is a field iff n is prime