I
$-I$
$d \in I$
$-bd$
$-d)$

2/5
Weds
week 3

Prop: Let R be a commutative ring with identity $1 \neq 0$.
Let I be an ideal of R with $I \neq R$.
Then R/I is a commutative ring with identity $1+I \neq 0+I$.

proof: We know R/I is a ring.
R/I is commutative since for all $a,b \in R$ we have

$$(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I).$$

R is commutative

$1+I$ is an identity for R/I since

$$(1+I)(a+I) = 1a+I = a+I$$
$$= a1+I = (a+I)(1+I)$$

for all $a \in R$.

Why is $1+I \neq 0+I$?

If $1+I = 0+I = I$, then $1 \in I$.

So, I contains a unit.

Thus, $I = R$ (previous prop).

But we assumed $I \neq R$.

Thus, $1+I \neq 0+I$. ▨

Recall
$a+I = b+I$
iff
$a \in b+I$
iff
$a-b \in I$

$(a+I)$.

Thm that we stated but didn't prove on Weds 1/29

Prop: Let R be a ring and I be an ideal of R. Then the (additive) quotient group R/I is a ring under the following operations:

$$(r+I)+(s+I)=(r+s)+I$$

and $$(r+I)(s+I)=rs+I$$

whenever $r,s\in R$.

$$\boxed{\begin{aligned} R/I &= \{a+I \mid a\in R\} \\ a+I &= \{a+x \mid x\in I\}\end{aligned}}$$

<u>proof:</u> Since R is an abelian group under $+$ and I is a subgroup under $+$, we know I is a normal subgroup of R under $+$.

So, R/I is a group using the operation

$$(r+I)+(s+I)=(r+s)+I.$$

And the above operation is well-defined.

Since R is abelian under $+$, so is R/I.

MATH 5401

Let's now show that $(r+I)(s+I)=rs+I$ is well-defined on R/I.

Suppose $a+I=b+I$ and $c+I=d+I$ where $a,b,c,d\in R$.

We want to show that $(a+I)(c+I)=(b+I)(d+I)$.

I.e, we want to show $ac+I=bd+I$.

S
S
N

So,
So, m

Since $a+I=b+I$ we have $a-b \in I$.

Since $c+I=d+I$ we have $c-d \in I$.

Note that

$$
\begin{aligned}
ac-bd &= ac-bc+bc-bd \\
&= \underbrace{\underbrace{\underbrace{c}_{\text{in } R}\underbrace{(a-b)}_{\text{in } I}}_{\text{in } I} + \underbrace{\underbrace{b}_{\text{in } R}\underbrace{(c-d)}_{\text{in } I}}_{\text{in } I}}_{\text{in } I} \in I.
\end{aligned}
$$

So, $ac+I=bd+I$.

So, mult. in well-defined in R/I.

R/I is associative under mult.

Let $a, b, c \in R$.

Then

$$(a+I)\left[(b+I)(c+I)\right]$$

$$= (a+I)(bc+I)$$

$$= a(bc)+I$$

$$\overset{\text{R is associative}}{=} (ab)c+I =$$

$$= [ab+I](c+I]$$

$$[(a+I)(b+I)](c+I]$$

R/I satisfies the distributive laws:

Let $a, b, c \in R$. Then

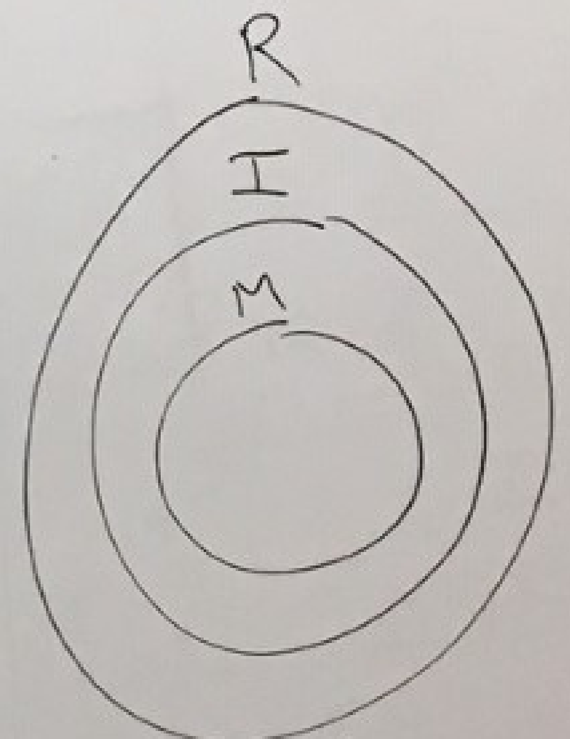
$$(a+I)\left[(b+I)+(c+I)\right] = (a+I)\left[(b+c)+I\right]$$
$$= a(b+c) + I$$
$$\overset{\text{R has the distributive laws}}{=} (ab+ac) + I$$
$$= \left[ab+I\right] + \left[ac+I\right]$$
$$= (a+I)(b+I) + (a+I)(c+I)$$

The other distributive law has the same proof $\square$

Questions: When is R/I a field?
When is R/I an integral domain?

Def: An ideal M of a ring R is called a **maximal ideal** if $M \neq R$ and the only ideals of R that contain M are M and R.

Another way to say this is:
1. $M \neq R$
2. If I is an ideal of R with $M \subseteq I \subseteq R$ then either $I = M$ or $I = R$.



We can't have this picture if M is maximal

Thm: Let R be a commutative ring with identity $1 \neq 0$. Let $M \neq R$ be an ideal of R.

Then M is maximal iff R/M is a field.

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

$(\Rightarrow)$ Let M be maximal. Let $a+M \in R/M$ with $a+M \neq 0+M$. We need to show $a+M$ is a unit in R/M. Then we've shown R/M is a field.

Let $I_a = \{m + ar \mid r \in R, m \in M\}$

Side note:

$I_a = M + (a)$

C

pro

•

• L

x

W

Th

x

$M\}$

Claim: I_a is an ideal of R

proof of claim:

- $0 \in M$ since M is an ideal of R.

  So, $0 = \underbrace{0}_{\text{in } M} + a\underbrace{0}_{\text{in } R} \in I_a$.

- Let $x, y \in I_a$. Then

  $x = m_1 + ar_1$ and $y = m_2 + ar_2$

  where $m_1, m_2 \in M$ and $r_1, r_2 \in R$.

  Then

  $$x - y = \underbrace{(m_1 - m_2)}_{\text{in } M} + a\underbrace{(r_1 - r_2)}_{\text{in } R} \in I_a.$$

- Let $z \in I_a$ and $r \in R$.

  So, $z = m' + ar'$ where $m' \in M$ and $r' \in R$.

  And

  $$rz = rm' + rar' = \underbrace{\underbrace{r}_{\text{in } R}\underbrace{m'}_{\text{in } M}}_{\text{in } M} + a\underbrace{(rr')}_{\text{in } R} \in I_a.$$

Since our ring is commutative $zr = rz \in I_a$.

$\boxed{\text{Claim}}$

Claim: $M \subseteq I_a$ and $M \neq I_a$.

proof of claim: Let $m \in M$.

Then, $m = m + a0 \in I_a$.

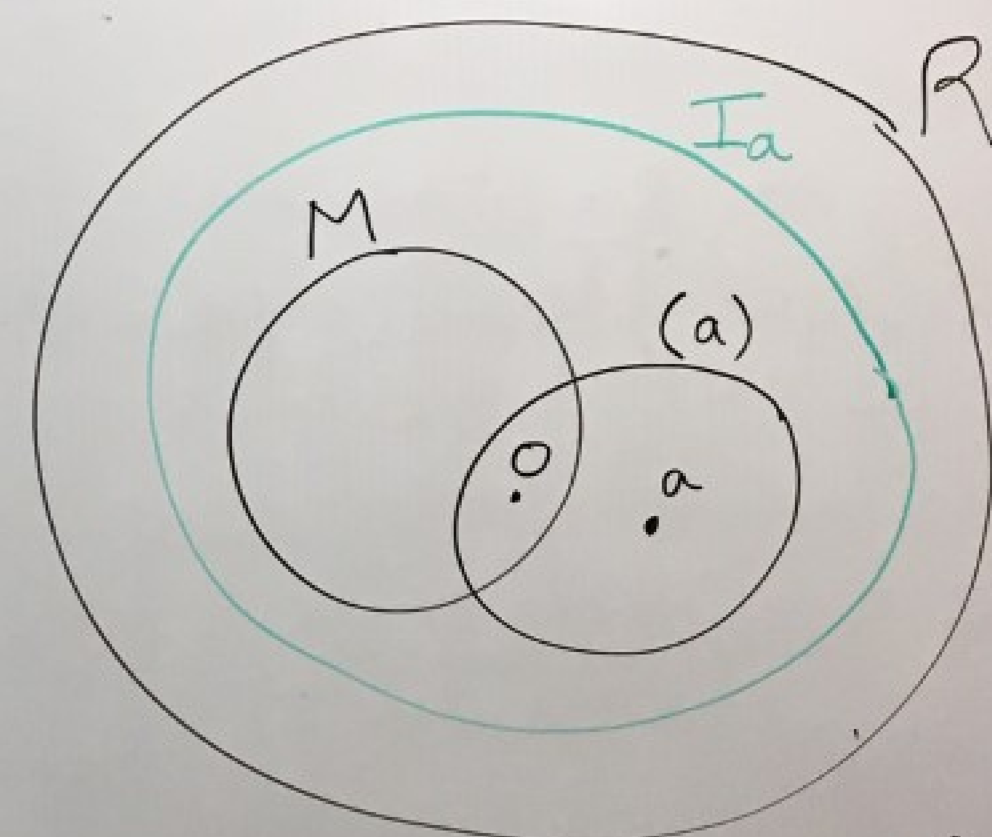
So, $M \subseteq I_a$.

Note: $a = 0 + a \cdot 1 \in I_a$.

But since $a + M \neq \underbrace{0 + M}_{M}$

we know $a \notin M$.

So, $M \neq I_a$.



Since M is maximal and

$M \subseteq I_a \subseteq R$ with $M \neq I_a$

we know $I_a = R$.

So, $1 \in I_a$.

Thus, $1 = m + ab$ for some $b \in R$.

Hence, $ab - 1 = -m \in M$.

So, $ab + M = 1 + M$.

Thus, $(a+M)(b+M) = 1 + M$.

So, $a+M$ is a unit in R/M.

$$\boxed{(\Longrightarrow)}$$