2/12
Weds

In $\mathbb{Z}$, if p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Def: Let R be a commutative ring with identity $1 \neq 0$. An ideal P of R is called prime if $P \neq R$ and the following holds for all $a, b \in R$:

If $ab \in P$, then $a \in P$ or $b \in P$.

Ex: p is prime

Suppose

So, $ab =$

That is,

Since p is

This me

So, $p\mathbb{Z}$

Ex: Let $I = p\mathbb{Z} = (p)$ where p is prime in $\mathbb{Z}$.

Suppose $ab \in p\mathbb{Z}$ where $a, b \in \mathbb{Z}$.

So, $ab = pk$ for some $k \in \mathbb{Z}$.

That is, $p \mid ab$.

Since p is prime, $p \mid a$ or $p \mid b$.

This means $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

So, $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

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

Then P is a prime ideal iff R/P is an integral domain.

proof:

($\Rightarrow$) Suppose that P is a prime ideal.

Since $P \neq R$ we know R/P is a commutative ring with identity $1 + P \neq 0 + P$.

So we just need to show that R/P has no zero divisors.

Suppose that $(a+P)(b+P) = 0+P$ where $a,b \in R$.

Then, $ab+P = 0+P$.

So, $ab = ab-0 \in P$.

Since P is a prime ideal and $ab \in P$, we have $a \in P$ or $b \in P$.

So, either $a+P = 0+P$ or $b+P = 0+P$.

Thus, R/P has no zero divisors, and hence is an integral domain.

($\Leftarrow$) Suppose R/P is an integral domain.

Let's show that P is a prime ideal.

P.

Suppose $ab \in P$ for some $a, b \in R$.

So, $ab + P = 0 + P$.

Thus, $(a+P)(b+P) = 0 + P$.

Since R/P is an integral domain either $a+P = 0+P$ or $b+P = 0+P$.

Thus, $a \in P$ or $b \in P$.

Therefore, P is a prime ideal. ▨

ne $a, b \in R$.

.

$0 + P$.

ral

$P = 0 + P$

P.

ne ideal.

Corollary: Let R be a commutative ring with identity $1 \neq 0$.
Let M be a maximal ideal of R,
then M is a prime ideal.

proof: Suppose M is a maximal ideal of R.
Then, R/M is a field.
So, R/M is an integral domain.
Thus, M is a prime ideal

Thm: If $n \geq 2$ and $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, then n is prime in $\mathbb{Z}$.

proof: Suppose $n = ab$ where $a, b \in \mathbb{Z}$, $1 \leq a, b$.

We will show n is prime by showing $a = 1$ or $b = 1$.

Since $ab = n$ we know $ab \in n\mathbb{Z}$.

Since $n\mathbb{Z}$ is a prime ideal either $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$.

WLOG (without loss of generality) assume $a \in n\mathbb{Z}$.

Thus, $a = nk$ where $k \geq 1$.

So, $n = ab = (nk)b$. Thus, $1 = kb$. Since, $k \geq 1$ and $b \geq 1$ we get $k = 1$ and $\boxed{b = 1}$

Thus, n is prime. ▨

Ex

id

Pf:

So

Thu

Her

Th

Ex: $\{0\} = 0\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

pf: Suppose $ab \in \{0\}$ where $a, b \in \mathbb{Z}$.

So, $ab = 0$.

Thus, $a = 0$ or $b = 0$.

Hence $a \in \{0\}$ or $b \in \{0\}$.

Thus, $\{0\}$ is a prime ideal. ▨

We used that $\mathbb{Z}$ is an integral domain

et

e. ▨

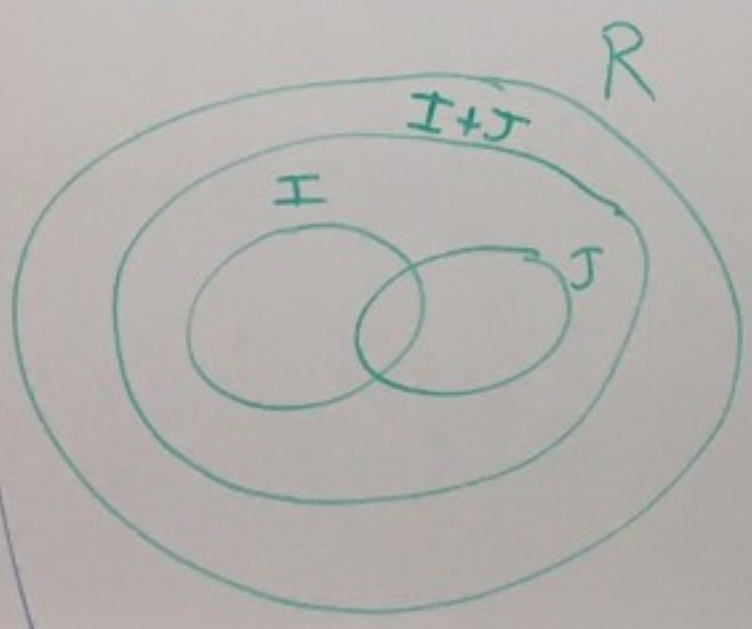
Class question
answer

Use fact that
$d = nx + my$ for some $x, y \in \mathbb{Z}$

$n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$

$d = \gcd(m, n)$

I, J ideals of R



$I + J = \{ i + j \mid i \in I, j \in J \}$

is the smallest ideal containing I and J.

That is if K is an ideal with $I \subseteq K$ and $J \subseteq K$ then

$I + J \subseteq K$

maximal ideals of $\mathbb{Z}$	prime ideals of $\mathbb{Z}$
$p\mathbb{Z}$, p prime	$p\mathbb{Z}$, p prime $\{0\}$

$\mathbb{Z}$ is neither maximal nor prime.

If n is composite, then $n\mathbb{Z}$ is neither maximal nor prime.

9.2

Thm 3

Let F be a field.
If $a(x), b(x) \in F[x]$
with $b(x) \neq 0$,
then there exist unique
$q(x), r(x) \in F[x]$
such that

$$a(x) = b(x)q(x) + r(x)$$

and $r(x) = 0$ or $\deg(r) < \deg(b)$

Pf: See book. It's Thm 3 in 9.2. You do poly division. ▨

Ex: In $\mathbb{Z}_5[x]$, divide $b(x) = x^2 + \bar{2}$ into $a(x) = x^5 + \bar{4}x^3 + x^2 + \bar{3}x + \bar{3}$.

$$\begin{array}{r} x^3 + \bar{2}x + \bar{1} \leftarrow q(x) \\ x^2 + \bar{2} \;\overline{)\; x^5 + \bar{4}x^3 + x^2 + \bar{3}x + \bar{3}} \\ -(x^5 + \bar{2}x^3) \\ \hline \bar{2}x^3 + x^2 + \bar{3}x + \bar{3} \\ -(\bar{2}x^3 + \bar{4}x) \\ \hline x^2 + \bar{4}x + \bar{3} \\ -(x^2 + \bar{2}) \\ \hline \bar{4}x + \bar{1} \leftarrow r(x) \end{array}$$

$\deg(r) = 1$, $\deg(b) = 2$, $1 < 2$

$(\bar{3} - \bar{4})x = \bar{-1}x = \bar{4}x$ (in $\mathbb{Z}_5$)

So,

$$x^5 + \bar{4}x^3 + x^2 + \bar{3}x + \bar{3} = (x^2 + \bar{2})(x^3 + \bar{2}x + \bar{1}) + (\bar{4}x + \bar{1})$$

$a(x) = b(x)q(x) + r(x)$