HW 5 #2

Prove that S is an ideal of $\mathbb{Z}\times\mathbb{Z}$

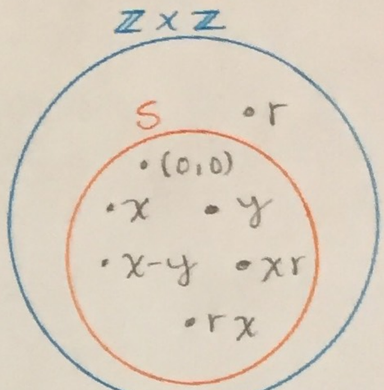
$$S=\{(2a,3b)\mid a,b\in\mathbb{Z}\}=\{\overset{a=b=0}{(0,0)},\overset{a=1,\,b=0}{(2,0)},\overset{a=2,\,b=3}{(4,9)},\dots$$

Proof:

* Set $a=b=0$ to see that $(0,0)\in S$

* Let $x,y\in S$. Then $x=(2a,3b)$ and $y=(2c,3d)$ where $a,b,c,d\in S$

and $x-y=(2\underbrace{(a-c)}_{\text{in }\mathbb{Z}},3\underbrace{(b-d)}_{\text{in }\mathbb{Z}})\in S$



* Pick $r\in\mathbb{Z}\times\mathbb{Z}$

Then $r=(\alpha,\beta)$ where $\alpha,\beta\in\mathbb{Z}$

and $rx=(\alpha\cdot 2a,\beta\cdot 3b)$

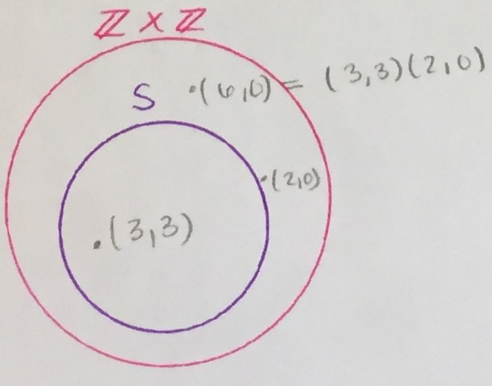
$=(2a\alpha,3b\beta)\in S$

and $xr=(2a\cdot\alpha,3b\cdot\beta)\in S$ ▨

2(a) Is $S=\{(a,a)\mid a\in\mathbb{Z}\}$ an ideal of $\mathbb{Z}\times\mathbb{Z}$?

$S=\{(0,0),(1,1),(2,2),\dots\}$

• S is a subgroup of $\mathbb{Z}\times\mathbb{Z}$, that is $(0,0)\in S$ and if $x,y\in S$, then $x-y\in S$



But given $(3,3)\in S$ and $(2,0)\in\mathbb{Z}\times\mathbb{Z}$, we have $(3,3)(2,0)=(6,0)\notin S$

S is not an ideal of $\mathbb{Z}\times\mathbb{Z}$

Recall

R com. ring with $1 \neq 0$. P is an ideal of R

P is **Prime** if

- $P \neq R$
- For all $a, b \in R$: If $ab \in P$, then $a \in P$ or $b \in P$

where is this coming from?

In $\mathbb{Z}$

- If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$
- $I = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$

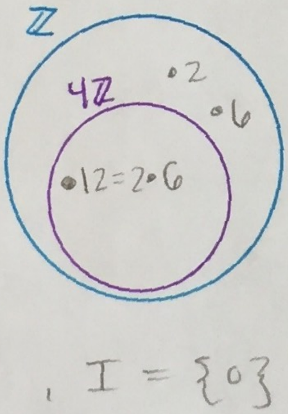
  $k \in n\mathbb{Z}$ iff $n \mid k$

- Suppose p is prime

  Let $ab \in p\mathbb{Z}$, Then $p \mid ab$ so $p \mid a$ or $p \mid b$ so

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

- $\langle 4 \rangle = 4\mathbb{Z}$ is not prime



Ex: $R = \mathbb{C}$, $I = \{0\}$, I is a prime ideal

proof: Suppose $a, b \in \mathbb{C}$ and $ab \in I$

so $ab = 0$, since we are in $\mathbb{C}$, either $a = 0$ or $b = 0$

so either $a \in I$ or $b \in I$.

Theorem: Let R be a commutative ring with identity $1 \neq 0$. Let P be an ideal of R with $\underline{P \neq R}$. Then P is a prime ideal iff R/P is an integral domain.

Proof: In HW 6 #5 you will show that R/P is a commutative ring with additive identity $0+P$ and multiplicative identity $1+P$. $\underbrace{\text{And } 1+P \neq 0+P}_{\text{why?}}$

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

If $1+P = 0+P$ then $1 \in \underbrace{0+P}_{P}$

so, $1 \in P$. Given $r \in R$ since P is an ideal $r = \underbrace{r}_{\text{in } R} \cdot \underbrace{1}_{\text{in } P} \in P$

so $\underline{P = R}$, but $P \neq R$

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

Proof

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

Let $a, b \in R$ with $(a+P)(b+P) = 0+P$

so, $ab+P = 0+P$

thus $ab \in 0+P = P$, since P is prime either $a \in P$ or $b \in P$

thus $a+P = 0+P$ or $b+P = 0+P$. so, R/P is an integral domain.

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

Let $a, b \in R$ with $ab \in P$. Then $ab+P = \underbrace{0+P}_{P}$

so $(a+P)(b+P) = 0+P$

since R/P is an integral domain either $a+P = 0+P$ or $b+P = 0+P$, therefore P is prime $\boxtimes$

Corollary

Let I be an ideal of $\mathbb{Z}$

I is prime iff $I = \{0\}$ or $I = p\mathbb{Z}$ where p is prime

Ideals of $\mathbb{Z}$

$\{0\} \leftarrow$ prime
$\mathbb{Z}$
$2\mathbb{Z} \leftarrow$ prime
$3\mathbb{Z} \leftarrow$ prime
$4\mathbb{Z}$
$5\mathbb{Z} \leftarrow$ Prime
$6\mathbb{Z}$
$7\mathbb{Z} \leftarrow$ prime
$8\mathbb{Z}$
$\vdots$

proof

$I = \mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$ since its the whole ring.

$I = \{0\}$ is a prime ideal since if $a, b \in \mathbb{Z}$ and $ab \in \{0\}$, Then $ab = 0$, either $a = 0$ or $b = 0$ so $a \in \{0\}$ or $b \in \{0\}$.

What if $I = n\mathbb{Z}$ with $n \geq 2$?

well $\boxed{\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n}$ which is an integral domain iff n is prime

so by the previous theorem, $n\mathbb{Z}$ is a prime ideal iff n is prime ☒

1^{st} iso. thm.

$\pi_n : \mathbb{Z} \to \mathbb{Z}_n$

$\ker(\pi_n) = n\mathbb{Z}$

$\mathbb{Z}/\ker(\pi_n) \cong \operatorname{im}(\pi_n)$

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

HW5 #10

$R = \mathbb{Z}_4 \times \mathbb{Z}_4$

$I = \{(\bar{0},\bar{0}), (\bar{2},\bar{0}), (\bar{0},\bar{2}), (\bar{2},\bar{2})\}$

Show I is principal

$\{(\bar{x},\bar{y})(\bar{2},\bar{2}) \mid (\bar{x},\bar{y}) \in \mathbb{Z}_4 \times \mathbb{Z}_4\}$

$\langle(\bar{2},\bar{2})\rangle = \{(\bar{0},\bar{0})(\bar{2},\bar{2}), (\bar{1},\bar{0})(\bar{2},\bar{2}), (2,0)(\bar{2},\bar{2}), (\bar{3},\bar{0})(\bar{2},\bar{2}), (\bar{0},\bar{1})(\bar{2},\bar{2}), (1,1)(2,2), (2,1)(2,2), (3,1)(2,2), (0,2)(2,2), (1,2)(2,2), (2,2)(2,2), (3,2)(2,2), (0,3)(2,2), (1,3)(2,2), (2,3)(2,2), (3,3)(2,2)\}$

$= \{(\bar{0},\bar{0}), (\bar{2},\bar{0}), (\bar{0},\bar{0}), (\bar{2},\bar{0}), (\bar{0},\bar{2})(\bar{2},\bar{2})(\bar{0},\bar{2})(\bar{2},\bar{2}) (\bar{0},\bar{0})(\bar{2},\bar{0})(\bar{0},\bar{0})(\bar{2},\bar{0}) (\bar{0},\bar{2})(\bar{2},\bar{2})(\bar{0},\bar{2})(\bar{2},\bar{2})\} = I$

R is a comm Ring w/1

I is an ideal

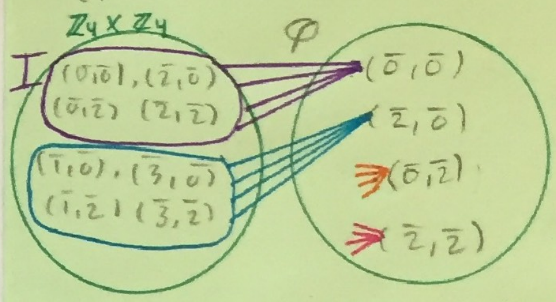
- I is principal means $a \in R$ where $I = \langle a \rangle = \{ra \mid r \in R\} = Ra$

$\varphi: \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4 \times \mathbb{Z}_4$

$\varphi((\bar{x},\bar{y})) = (\bar{x},\bar{y})(\bar{2},\bar{2})$

This is a group under +

$\mathrm{Im}(\varphi) = I$



#3 Show that $I = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2})\}$ is an ideal of $\mathbb{Z}_2 \times \mathbb{Z}_3$

Method 1

You could do this:

- $(\bar{0},\bar{0}) \in I$
- if $x, y \in I$ then $x - y \in I$
- if $x \in I$ and $r \in \mathbb{Z}_2 \times \mathbb{Z}_3$, then $xr, rx \in I$

Method 2

- We can do this by showing that I is principal and this is an ideal. You can show that $I = \langle(\bar{0},\bar{1})\rangle$

$\langle(\bar{0},\bar{1})\rangle = \{(\bar{0},\bar{0})(\bar{0},\bar{1}), (\bar{0},\bar{1})(\bar{0},\bar{1}), (\bar{0},\bar{2})(\bar{0},\bar{1}), (\bar{1},\bar{0})(\bar{0},\bar{1}), (\bar{1},\bar{1})(\bar{0},\bar{1}), (\bar{1},\bar{2})(\bar{0},\bar{1})\}$

$= \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2})\} = I$

Method 3

$\varphi: \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_2$

$\varphi(\bar{x},\bar{y}) = \bar{x}$ φ is a ring hom.

Given $(\bar{x},\bar{y}), (\bar{a},\bar{b}) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ we have

$\varphi((\bar{x},\bar{y})+(\bar{a},\bar{b})) = \varphi(\overline{x+a}, \overline{y+b}) = \bar{x} + \bar{a} = \varphi(\bar{x},\bar{y}) + \varphi(\bar{a},\bar{b})$

$\varphi((\bar{x},\bar{y})(\bar{a},\bar{b})) = \varphi((\bar{x}\bar{a}, \bar{y}\bar{b})) = \bar{x}\bar{a} = \varphi(\bar{x},\bar{y})\,\varphi(\bar{a},\bar{b})$

$\ker(\varphi) = I$, so I is an ideal since $\ker(\varphi)$ is an ideal.

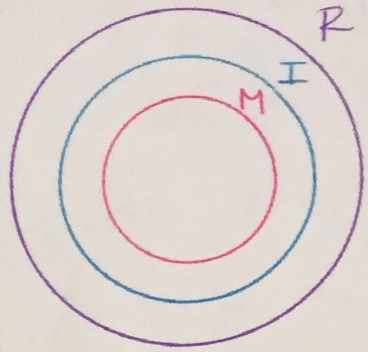
For Fun: $\mathbb{Z}_2 \times \mathbb{Z}_3 / I \cong \mathrm{Im}(\varphi) = \mathbb{Z}_2$

Def: Let M be an ideal of a ring R. We say that M is a **maximal ideal** if

(1) $M \neq R$

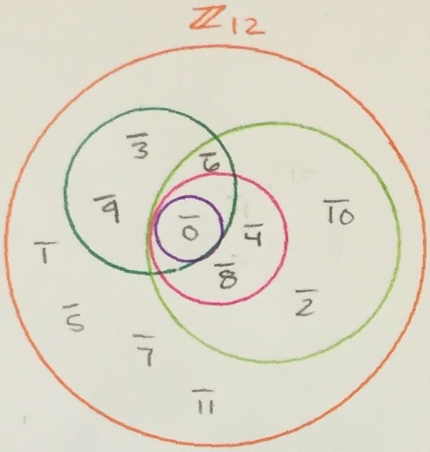
(2) The only ideals that contains M are M and R.

(2) can be rephrased as:
If I is an ideal of R with $M \subseteq I \subseteq R$, then either $I = M$ or $I = R$



Example: Here is a picture of all the ideals of $\mathbb{Z}_{12}$

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



Maximal	Not Maximal
$\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$	$\{0\}$
$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$	$\{\bar{0}, \bar{4}, \bar{8}\}$
	$\mathbb{Z}_{12}$

Ex: Is $4\mathbb{Z}$ a maximal ideal of $\mathbb{Z}$?

$\ldots -8 \quad -7 \quad -6 \quad -5 \quad -4 \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \ldots$

○ $= 4\mathbb{Z}$

○ $= 2\mathbb{Z}$

No, $4\mathbb{Z} \subseteq 2\mathbb{Z}$

$8\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$

$16\mathbb{Z} \subseteq 8\mathbb{Z}$
not max

$\underbrace{8\mathbb{Z}}_{\text{not max}} \subseteq \underbrace{4\mathbb{Z}}_{\text{not max}} \subseteq 2\mathbb{Z}$

Ideals of $\mathbb{Z}$

$0\mathbb{Z} = \{0\}$ $\quad 2\mathbb{Z}$

$1\mathbb{Z} = \mathbb{Z}$ $\quad 3\mathbb{Z}$

$4\mathbb{Z}$

$5\mathbb{Z}$

$6\mathbb{Z}$

$\vdots$

P.2 3/23

Theorem: Let R be a commutative ring with identity $1 \neq 0$. Let I be an ideal of R. If I contains a unit, then $I = R$

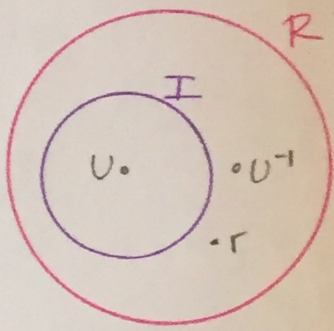
proof:

Let u be a unit where $u \in I$

Since u is a unit, u^{-1} exists in R

Let's show that $R \subseteq I$ and thus $I = R$ because we already know that $I \subseteq R$.

let $r \in R$, then



$r = ru^{-1} \cdot u \in I$ since I is an ideal so, $R \subseteq I$ ☒

Note $1 \in I$ since

$$1 = \underset{\text{in } I}{u} \cdot \underset{\text{in } R}{u^{-1}} \in I$$