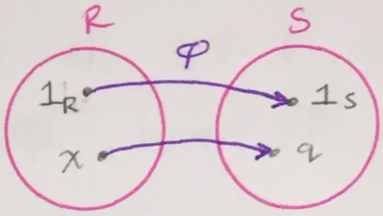
P.3 3/14

Lemma

Suppose R and S are rings with mult. identities 1_R and 1_S and $\varphi : R \to S$ is an onto ring homomorphism

Then $\varphi(1_R) = 1_S$



Proof: Let $q \in S$

since φ is onto there exists $x \in R$ with $\varphi(x) = q$. Thus

$$q \cdot \varphi(1_R) = \varphi(x)\varphi(1_R) = \varphi(x 1_R) = \varphi(x) = q$$

and $\varphi(1_R) \cdot q = \varphi(1_R)\varphi(x) = \varphi(1_R \cdot x) = \varphi(x) = q$

So, $\varphi(1_R)$ is a mult. identity of S. But mult. identities are unique so $\varphi(1_R) = 1_S$ ☒

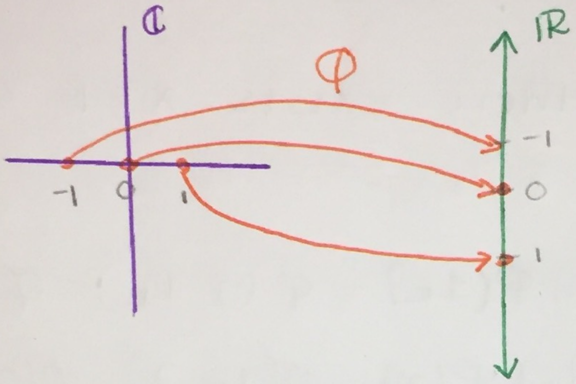
HW #4

(2) Show $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic as rings.

idea: $\mathbb{C}$ has i that satisfies $i^2 = -1$

Suppose $\varphi : \mathbb{C} \to \mathbb{R}$ is a ring isomorphism

By Lemma, $\varphi(1) = 1$



Recall $\varphi(-x) = -\varphi(x)$ for all x

so, $\varphi(-1) = -\varphi(1) = -1$

using $i^2 = -1$ we get $\varphi(i^2) = \underbrace{\varphi(-1)}_{-1}$

so, $[\varphi(i)] = -1$

But $\varphi(i) \in \mathbb{R}$. There is no real number whose square is -1. Thus we have a contradiction so there doesn't exist a ring homomorphism $\varphi : \mathbb{C} \to \mathbb{R}$.

TRY TO PROVE
Given $R \cong R'$
Then R is an integral domain iff R' is an integral domain.

HW5 #6

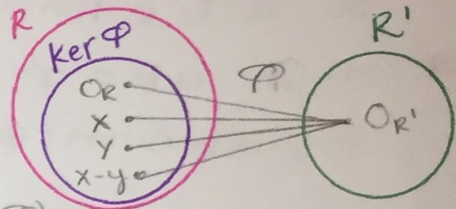
Let R and R' be rings.

Let $\varphi : R \to R'$ be a ring homomorphism

(a) Prove that $\ker(\varphi)$ is an ideal of R

(b) Prove that $\varphi(R) = \{\varphi(r) \mid r \in R\}$ is a subring!

proof: Let 0_R and $0_{R'}$ be the additive identities of R and R'



(a) Recall $\ker(\varphi) = \{x \in R \mid \varphi(x) = 0_{R'}\}$

* From class, $\varphi(0_R) = 0_{R'}$ so, $0_R \in \ker(\varphi)$

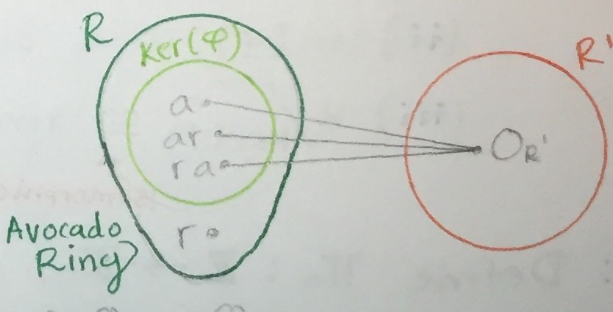
* Let $x, y \in \ker(\varphi)$

Then $\varphi(x) = \varphi(y) = 0_{R'}$

notes & HW

So, $\varphi(x-y) = \varphi(x) + \varphi(-y) \stackrel{\downarrow}{=} \varphi(x) - \varphi(y) = 0_{R'} - 0_{R'} = 0_{R'}$

Thus, $x-y \in \ker\varphi$



* Let $a \in \ker(\varphi)$ and $r \in R$

Then $\varphi(a) = 0_{R'}$

hence, $\varphi(ra) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0_{R'} = 0_{R'}$

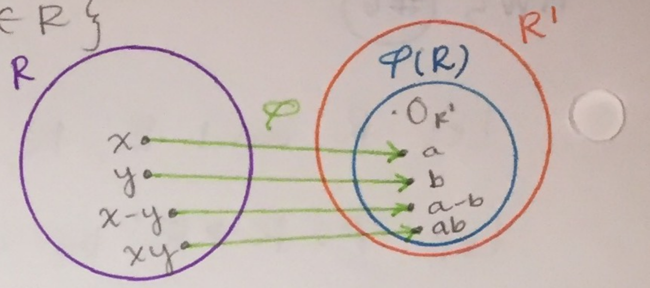
and $\varphi(ar) = \varphi(a) \cdot \varphi(r) = 0_{R'} \cdot \varphi(r) = 0_{R'}$

So $ra, ar \in \ker(\varphi)$

Thus $\ker(\varphi)$ is an ideal of R. ☒

proof of (b) $\varphi(R) = \mathrm{im}(\varphi)$ is a subring of R'

Recall $\varphi(R) = \mathrm{im}(\varphi) = \{\varphi(x) \mid x \in R\}$



* We have that $0_{R'} = \varphi(0_R)$

So, $0_{R'} \in \mathrm{im}(\varphi)$

* Let $a, b \in \mathrm{im}(\varphi)$

So there exists $x, y \in R$ with $\varphi(x) = a$ and $\varphi(y) = b$

Then $a - b = \varphi(x) - \varphi(y) = \varphi(x - y)$

So $a - b \in \mathrm{im}(\varphi)$

and $ab = \varphi(x)\varphi(y) = \varphi(xy)$

So, $ab \in \mathrm{im}(\varphi)$. $\boxtimes$

First Isomorphism Theorem

Let R and R' be rings

Let $\varphi : R \to R'$ be a ring homomorphism

Then,

(i) $\ker(\varphi)$ is an ideal of R

(ii) $\mathrm{im}(\varphi)$ is a subring of R'

(iii) $R/\ker(\varphi) \cong \mathrm{im}(\varphi)$

↑ isomorphic

Note:

The isomorphism is given by

$\psi : R/\ker\varphi \to \mathrm{im}(\varphi)$

where

$\psi(a + \ker\varphi) = \varphi(a)$

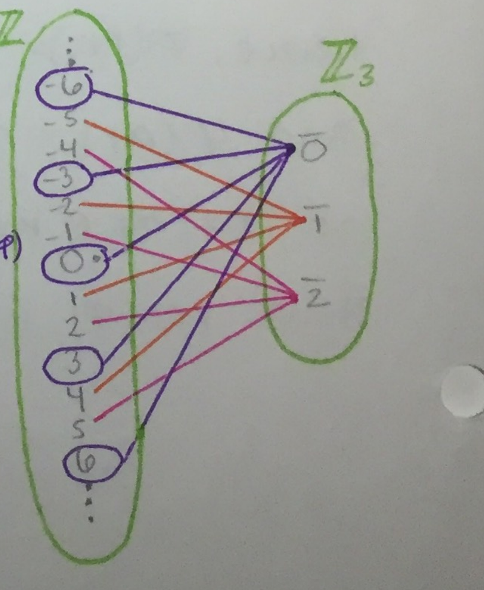
Ex: Define $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$, where $\pi_n(x) = \overline{x}$

From earlier, we showed $\ker(\pi_n) = n\mathbb{Z}$

and π_n is a ring homomorphism

$n = 3$

What is $\mathbb{Z}/\ker(\varphi)$?



$3\mathbb{Z} = \ker(\varphi)$

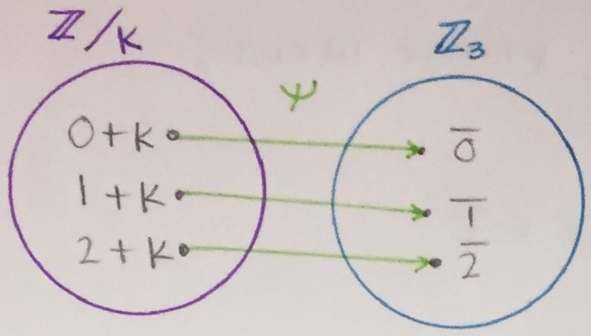
all the left cosets

$0 + K = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$1 + K = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$2 + K = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

P.2 3/16



1^{st} isomorphism theorem says: $\mathbb{Z}/K \cong \operatorname{im}(\pi_n) = \mathbb{Z}_n$

π_n is onto

ψ is a ring isomorphism

$\psi(0+K) = \pi_3(0) = \bar{0}$

$\psi(1+K) = \pi_3(1) = \bar{1}$

$\psi(2+K) = \pi_3(2) = \bar{2}$

* In general, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ via the π_n map and the 1^{st} isom. thm.

Prime and Maximal Ideals

(Q1) when is R/I an integral ideal? ← when I is a "prime" ideal

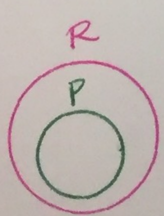
(Q2) when is R/I a field? ← When I is a "Maximal" Ideal

Def: Let R be a commutative ring with identity $1 \neq 0$ let P be an ideal of R, then P is called a prime ideal if

(1) $P \neq R$

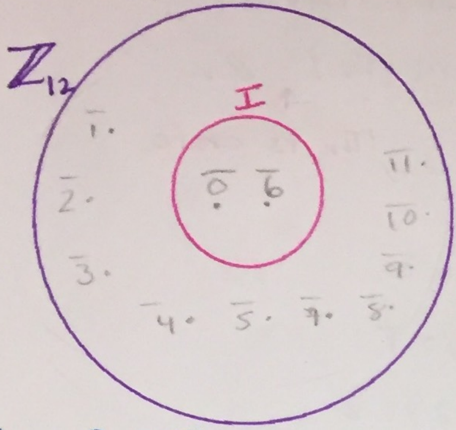
(2) For all $a, b \in R$ the following is true

If $ab \in P$, then $a \in P$ or $b \in P$ (it could be both)



Ex: $R = \mathbb{Z}_{12}$

$I = \langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$, Is I a prime ideal?



$\bar{4} \cdot \bar{3} = \bar{0} \in I$

not in I

I is not prime

Ex: $R = \mathbb{Z}$

$I = 4\mathbb{Z}$

$4\mathbb{Z}$ is circled

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

$-4 = ab$, $\quad -2 = a$, $\quad 2 = a$

$2 \cdot (-2) = -4 \leftarrow$ in I , I is not prime

not in I