7.3

Def: Let R and S be rings.

(1) A **ring homomorphism** is a function $\varphi : R \to S$ satisfying

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

and (ii) $\varphi(ab) = \varphi(a)\varphi(b)$

for all $a, b \in R$.

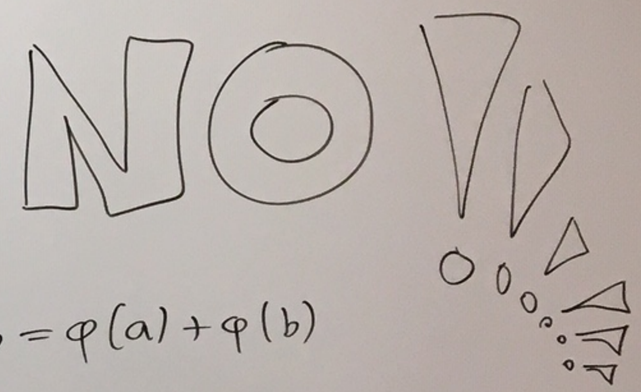
② The <u>kernel</u> of a ring homomorphism $\varphi: R \to S$ is

$$\ker(\varphi) = \{ x \in R \mid \varphi(x) = 0_S \}$$

where 0_S is the additive identity of S.

③ A <u>ring isomorphism</u> is a bijective ring homomorphism.

<u>Ex:</u> Is $\varphi: \mathbb{Z} \to \mathbb{Z}$ given by $\varphi(x) = 2x$ a ring homomorphism?



Let $a, b \in \mathbb{Z}$.

Then

$$\varphi(a+b) = 2(a+b) = 2a+2b = \varphi(a) + \varphi(b)$$

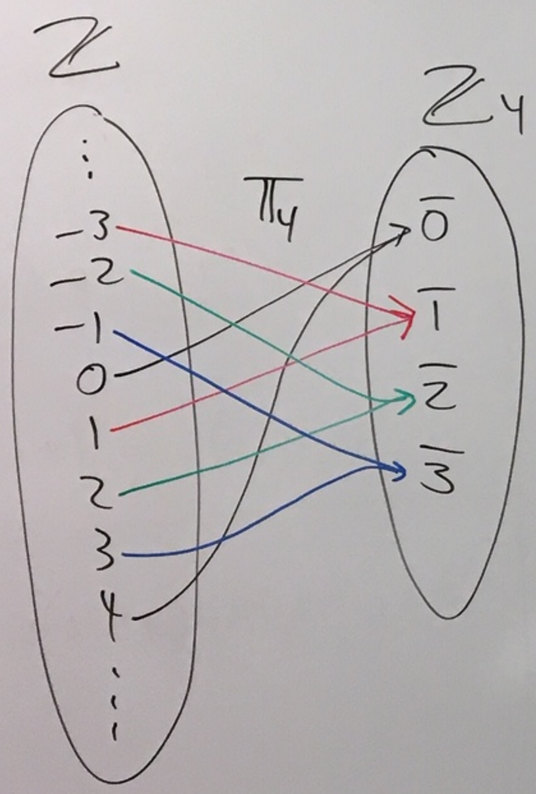
however

$$\varphi(ab) = 2ab$$

$$\varphi(a)\varphi(b) = 2a\,2b = 4ab$$

$\varphi(ab) \neq \varphi(a)\varphi(b)$ not always equal

<u>ex:</u> $a = 1$, $b = 1$



Ex: Let $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\pi_n(x) = \overline{x}$.

Then if $a, b \in \mathbb{Z}$ then

$$\pi_n(ab) = \overline{ab} = \bar{a}\,\bar{b} = \pi_n(a)\,\pi_n(b)$$

and

$$\pi_n(a+b) = \overline{a+b} = \bar{a}+\bar{b} = \pi_n(a) + \pi_n(b).$$

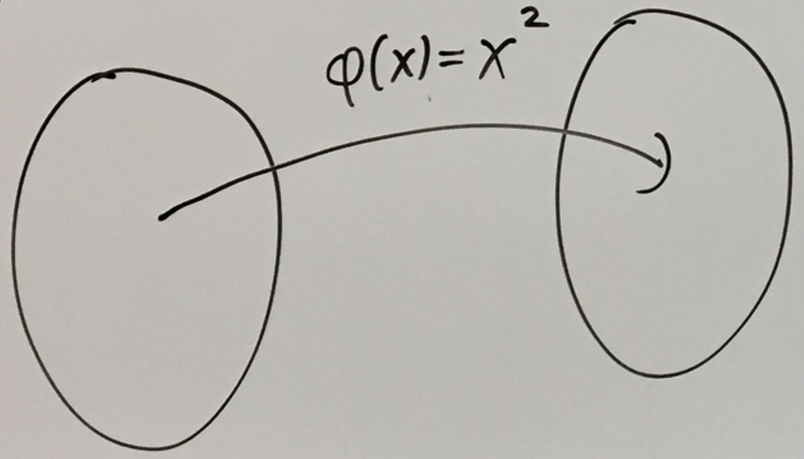
So, π_n is a ring homomorphism.

Test your memory

$\mathbb{Z}$

normal +

$a \cdot b = 0$



$$\varphi(\underline{ab} + c) = \underline{\varphi(a)\varphi(b)} + \varphi(c)$$
$$\quad\ 0 \qquad\qquad\ \ 0$$

Def: Let R be a ring.

① If I is a subset of R and $r \in R$, define

$$rI = \{rx \mid x \in I\} \quad \text{and} \quad Ir = \{xr \mid x \in I\}$$

② A subset I of R is called an ideal of R if

(i) I is a subgroup of R under addition

and (ii) $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$.

Ideal criteria test

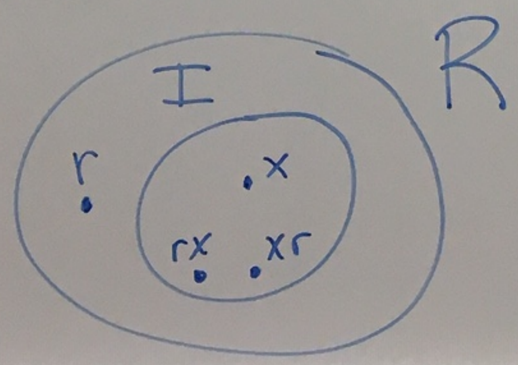
Let $I \subseteq R$ where R is a ring.

Then I is an ideal if

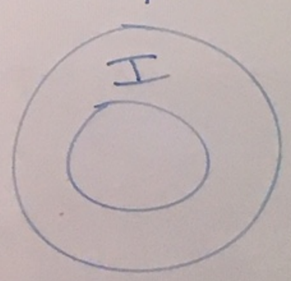
(a) $I \neq \emptyset$

(b) for all $x, y \in I$ we have $x - y \in I$] part (i) of ideal def.

and (c) for all $r \in R$ and $x \in I$ we have $rx \in I$ and $xr \in I$] part (ii) of ideal def.



Prop: Let R be a ring. Let I be an ideal of R. Then I is a subring of R.



Proof:

By def of ideal, I is a group under $+$.

Is I closed under multiplication?

Yes. By def of ideal part (ii), if $x, y \in I$ then $xy \in I$.

Since R is a ring, it has associativity of mult. and distributive laws. Thus I does since $I \subseteq R$. ∎

What are the ideals of $\mathbb{Z}$?

An ideal is a subgroup under $+$.

The subgroups under addition of $\mathbb{Z}$ are

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

$\mathbb{Z} = 1 \cdot \mathbb{Z}$

$2\mathbb{Z}$

$3\mathbb{Z}$

$4\mathbb{Z}$

$\vdots$

} $n\mathbb{Z}$, $n \geq 0$

of $\mathbb{Z}$?

under +.

tion of

$n\mathbb{Z}$
$n \geq 0$

Consider $n\mathbb{Z}$, $n \geq 0$.

Let $r \in \mathbb{Z}$ and $x \in n\mathbb{Z}$.

Then, $x = nz$ where $z \in \mathbb{Z}$.

Hence,

$$rx = r(nz) = n(rz) \in n\mathbb{Z}$$

and $$xr = (nz)r = n(zr) \in n\mathbb{Z}.$$

So, $n\mathbb{Z}$ is an ideal.

BECAUSE:
- $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under +
- $rx \in n\mathbb{Z}$ & $xr \in n\mathbb{Z}$ $\forall r \in \mathbb{Z}$ and $x \in n\mathbb{Z}$

Ideals of $\mathbb{Z}$

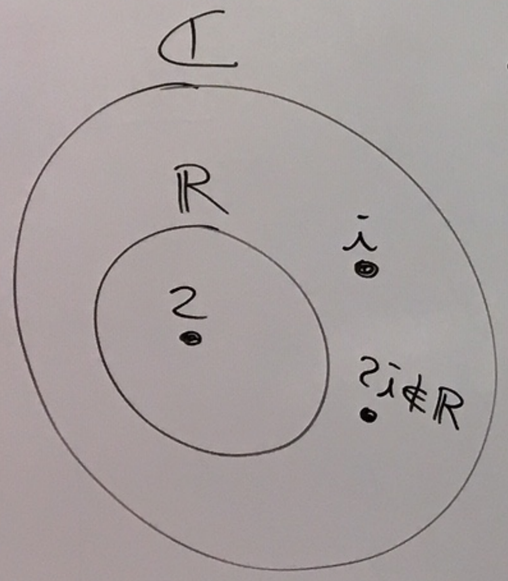
$n\mathbb{Z}$, $n \geq 0$

Ex: $\mathbb{R}$ is a subring of $\mathbb{C}$.

But $\mathbb{R}$ is not an ideal of $\mathbb{C}$ because

$2 \in \mathbb{R}$ and $i \in \mathbb{C}$

but $2i \notin \mathbb{R}$.



Note: Let R be a ring and I be an ideal of R.

Recall that R is an abelian group under $+$.

So, I is a normal subgroup under $+$.

So we can construct the quotient group R/I using $+$.

ing

R.

belian

e

ng +.

But we can go further !

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 operations:

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

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

where $r,s \in R$.

In this case we call R/I the quotient ring of R by I.

Ex: $R = \mathbb{Z}$
$I = 3\mathbb{Z}$

$0+3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$
$1+3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
$2+3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

$\mathbb{Z}/3\mathbb{Z} = \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$

$(2+3\mathbb{Z})(2+3\mathbb{Z}) + (1+3\mathbb{Z})$

$= (4+3\mathbb{Z}) + (1+3\mathbb{Z})$

$= (1+3\mathbb{Z}) + (1+3\mathbb{Z})$

$= 2+3\mathbb{Z}$

32)

First isomorphism theorem for rings

Thm: Let R and S be rings and $\varphi : R \to S$ is a ring homomorphism.

Then

(i) $\text{im}(\varphi)$ is a subring of S.

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

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