Last time: let R and S be rings.

A map $\varphi: R \to S$ is an isomorphism if it's a bijection,

$\varphi(1) = 1$

$\varphi(x+y) = \varphi(x) + \varphi(y)$

$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

We say that R and S are isomorphic (we write $R \cong S$) if $\exists$ an isomorphism $\varphi: R \to S$

think of them as (secretly) the same.

examples:

$\mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$

$\bar{a} \mapsto (\bar{a}, \bar{a})$

non-examples:

$\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

not only is the obvious map

$\mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$

$\bar{a} \mapsto (\bar{a}, \bar{a})$

not an iso,

but no other map is an iso. either.

another example:

low-brow model of $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

$x+y$ = take $x+y$ and take the remainder after $\div n$.

$x \cdot y$ = similar

high-brow model:

$\mathbb{Z}_m$ = set of equivalence classes

$\bar{0} = \{0, \pm m, \pm 2m, \dots\}$

$\bar{1} = \{1, 1 \pm m, 1 \pm 2m, \dots\}$

$\bar{2} = \{2, 2 \pm m, 2 \pm 2m, \dots\}$

define $\bar{x} + \bar{y} = \overline{x+y}$ $\quad \bar{x} \cdot \bar{y} = \overline{xy}$

check that they're well-defined

the map $n \longmapsto \bar{n}$ is an iso between these two rings.

same with high- and low-brow models of $\mathbb{Q}$, or of $\mathbb{R}$, ...

---

one more isomorphism:

let $R = \{$ maps $f: \mathbb{R}^2 \longrightarrow \mathbb{Z}_2 \}$

define $(f+g)(\vec{x}) = f(\vec{x}) + g(\vec{x})$

$(f \cdot g)(\vec{x}) = f(\vec{x}) \cdot g(\vec{x})$

happening in $\mathbb{Z}_2$

let $S = \{$ subsets of $\mathbb{R}^2 \}$

$X + Y = X \cdot Y \cup Y \cdot X$

$X \cdot Y = X \cap Y$

the map $R \longrightarrow S$

$f \longmapsto \{\vec{x} \in \mathbb{R}^2 \mid f(\vec{x}) = \bar{1}\}$

is an isomorphism.

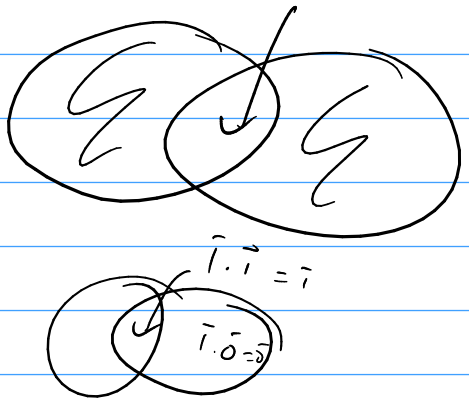
bijection ✓

respects + ✓

respects · ✓

$\bar{1} + \bar{1} = \bar{0}$ in $\mathbb{Z}_2$

$$f(x) = \begin{cases} \bar{1} & \text{if } x \in X \\ \bar{0} & \text{if } x \notin X \end{cases} \qquad X \subset \mathbb{R}^2$$



Homomorphisms

A map $\varphi: R \to S$ is a homomorphism if

$$\varphi(1) = 1$$
$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \forall x, y \in R$$
$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \quad \forall x, y \in R$$

not necessarily a bijection, just a map that respects the algebraic structure.

example: ① reduction map $\mathbb{Z} \to \mathbb{Z}_m$

$$a \longmapsto \bar{a}$$

know that $\overline{a+b} = \bar{a} + \bar{b}$ and $\overline{ab} = \bar{a} \cdot \bar{b}$

or $\mathbb{Z}_6 \to \mathbb{Z}_3$

$\bar{0} \longmapsto \bar{0}$ ★

$\bar{1} \longmapsto \bar{1}$

$\bar{2} \longmapsto \bar{2}$

$\bar{3} \longmapsto \bar{0}$ ★

$\bar{4} \longmapsto \bar{1}$

$\bar{5} \longmapsto \bar{2}$

(2) $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$

$f \longmapsto \bar{f}$

$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \longmapsto \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0$

used this when we were studying irreducible polynomials in §3.3

(3) if R is commutative ring and $a \in R$

then $\varphi: R[x] \longrightarrow R$ is a hom.

$f \longmapsto f(a)$

"plugging in a"

$$\varphi(f) = f(a)$$

(4) all the isos we've seen are also homomorphisms.

(5) inclusion maps

$\mathbb{Z} \hookrightarrow \mathbb{Q}$ or $\mathbb{Q} \hookrightarrow \mathbb{R}$ or $\mathbb{R} \hookrightarrow \mathbb{C}$

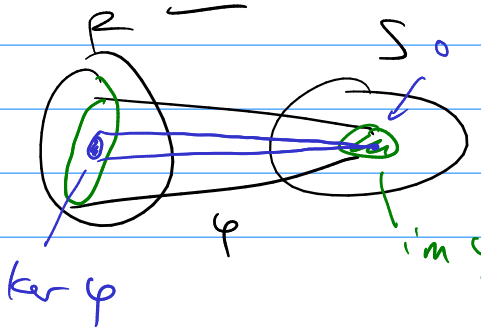
---

if $\varphi: R \to S$ is a homomorphism,

talk about the image and the kernel of φ.

$$\text{im}(\varphi) = \{ \varphi(r) \mid r \in R \} \subset S$$

$$\ker \varphi = \{ r \in R \mid \varphi(r) = 0 \} \subset R$$



examples: $\mathbb{Z}_6 \xrightarrow{\varphi} \mathbb{Z}_3$ from earlier.

$\bar{a} \longmapsto \bar{a}$

$\text{im}(\varphi) = \text{all of } \mathbb{Z}_3$

$\ker(\varphi) = \{\bar{0}, \bar{3}\} < \mathbb{Z}_6$

$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{C}$

$f \longmapsto f(i)$

$\varphi(f) = f(i)$

if $f = a_n x^n + \cdots + a_1 x + a_0 \qquad a_i \in \mathbb{Z}$

then $\varphi(f) = a_n (i)^n + \cdots - a_2 + a_1 i + a_0$

$\text{im}(\varphi) = \mathbb{Z}[i]$ that we met last time.

$\ker(\varphi) =$ all multiples of $x^2 + 1$