Lecture March 17, 2020

Section 3.3, continued: Isomorphisms and Homomorphisms

Last Time: Let R, S be rings. We say R and S are <u>isomorphic</u>, denoted $R \cong S$, if $\exists$ a function $f: R \to S$ such that

(i) f is injective

(ii) f is surjective

(iii) f satisfies the homomorphism property:

for all $a, b \in R$,

$$f(a \oplus b) = f(a) \oplus f(b)$$

$$f(ab) = f(a) f(b)$$

A function f that satisfies these conditions is called an <u>isomorphism</u>.

Examples:

(1) from HW 6:

E = even integers = $\{2k : k \in \mathbb{Z}\}$ w/ operations of usual addition and multiplication:

$$a * b = \frac{ab}{2}$$

Claim: E is isomorphic to $\mathbb{Z}$.

Pf: first thing to do: define a function $\phi: E \to \mathbb{Z}$.

We'll define ϕ as: for any $a \in E$,

$$\phi(a) = a/2.$$

If $a \in E$, then $a/2 \in \mathbb{Z}$, because $a = 2k$ f.s. $k \in \mathbb{Z}$.

So, $\phi(a) = a/2 = 2k/2 = k$.

Now, we show that ϕ satisfies the properties of an isomorphism:

(i) Show ϕ is injective

Suppose $\phi(a) = \phi(b)$.

WTS: $a = b$:

$$\phi(a) = \phi(b)$$

$$\frac{a}{\cancel{2}} = \frac{b}{\cancel{2}}$$

$$a = b \quad \checkmark$$

(ii) Let $k \in \mathbb{Z}$. We want $a \in E$ s.t. $\phi(a) = k$.

Set $a = 2k$, so

$$\phi(a) = \phi(2k) = \frac{2k}{2} = k.$$

$\Longrightarrow$ ϕ is surjective

Ex: $\phi(10) = \frac{10}{2} = 5$.

$$\phi(14) = \frac{14}{2} = 7$$

(iii) Homomorphism Property:

Let $a, b \in E$:

$$\phi(a+b) = \frac{a+b}{2} = \frac{a}{2} + \frac{b}{2}$$

$$= \phi(a) + \phi(b) \checkmark$$

$$\phi(a * b) = \phi\left(\frac{ab}{2}\right)$$

$$= \frac{(ab/2)}{2}$$

$$= \frac{ab}{4}$$

$$= \frac{a}{2} \cdot \frac{b}{2}$$

$$= \phi(a) \cdot \phi(b) \checkmark$$

$\Rightarrow$ ϕ is an isomorphism,

$\Rightarrow$ $E \cong \mathbb{Z}$.

Thm: Let X, Y be sets. A function $f: X \to Y$ is a bijection iff f has an inverse function $f^{-1}: Y \to X$.

Remember: f and f^{-1} are inverse functions if:

$$\begin{cases} \text{(i) } \forall x \in X, \quad f^{-1}(f(x)) = x \\ \text{(ii) } \forall y \in Y, \quad f(f^{-1}(y)) = y. \end{cases}$$

So, instead of showing a function is a bijection, you can show that it has an inverse.

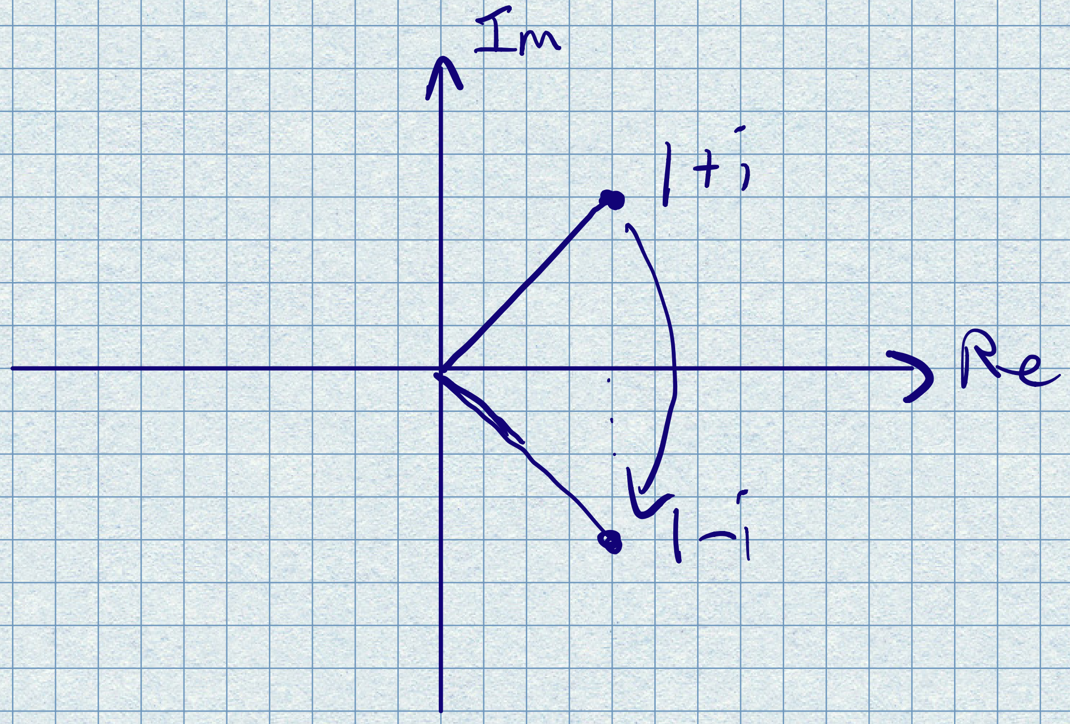
Ex: Consider the function

$$f : \mathbb{C} \to \mathbb{C}$$
$$z \mapsto \bar{z}$$

$$f(z) = \bar{z}$$

i.e. $f(a+bi) = a - bi$.

Show that f is an isomorphism.



f is its own inverse:

for any $a+bi \in \mathbb{C}$,

$$f(f(a+bi)) = f(a-bi)$$
$$= f(a+(-b)i)$$
$$= a-(-b)i$$
$$= a+bi$$

This show f is invertible

$\Rightarrow$ f is a bijection

Homomorphism property:

Let $a+bi, c+di \in \mathbb{C}$,

$$f((a+bi)+(c+di)) = f((a+c)+(b+d)i)$$
$$= (a+c)-(b+d)i$$
$$= (a-bi)+(c-di)$$
$$= f(a+bi)+f(c+di).$$

$$f((a+bi)(c+di)) = f((ac-bd)+(ad+bc)i)$$
$$= (ac-bd)-(ad+bc)i$$
$$= (a-bi)(c-di)$$
$$= f(a+bi)\,f(c+di). \checkmark$$

$\Longrightarrow$ f is an isomorphism.

From the test:

Let R, S, T be rings.

(1) if $R \cong S$, then $S \cong R$.

If $R \cong S$, then $\exists$ isomorphism $f: R \to S$.

To show $S \cong R$, find function from $S \to R$ that is also an isomorphism.

On your test, you can assume $\exists$ an inverse $f^{-1}: S \to R$ that is a bijection.

What's left to you: show f^{-1} satisfies the homomorphism properties.

(2) If $R \cong S$ and $S \cong T$, then $R \cong T$.

So, $\exists$ isomorphisms $f: R \to S$ and $h: S \to T$

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[rr, bend right, "h \circ f"'] & S \arrow[r, "h"] & T \end{tikzcd}$$

You can assume that if f, h are bijections, then so is $h \circ f$.

You need to show that $h \circ f$ satisfies the homomorphism property.

Showing Rings are <u>not</u> isomorphic

This is more difficult than showing two rings are isomorphic.

A common way to do this: show the two rings have different <u>structural properties</u>.

List of common structural properties:

(1) Cardinality - if two sets have different sizes, then there is no bijection between them.

Ex: $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are <u>not</u> isomorphic, since $|\mathbb{Z}_3| = 3$, and $|\mathbb{Z}_5| = 5$.

So, $\mathbb{Z}_n \cong \mathbb{Z}_m$ iff $n = m$.

(2) Commutative multiplication.
if two rings are isomorphic, then they need to both be comm. or both not be commutative.

Ex: $\mathbb{R}$ and $M_2(\mathbb{R})$ are not isomorphic.

$\mathbb{R}$ is commutative,

$M_2(\mathbb{R})$ is not.

(3) zero divisors

are both sets integral domains? fields?

Ex: (1) $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic, since $\mathbb{Z}$ is not a field, but $\mathbb{Q}$.

(2) $\mathbb{Z}_2 \times \mathbb{Z}_3$ is an integral domain.

$\mathbb{Z}_6$ is not an integral domain.

So, $\mathbb{Z}_2 \times \mathbb{Z}_3 \not\cong \mathbb{Z}_6$, even though $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_6| = 6$.

(4) Characteristic

to show two rings (w/ identity) aren't isomorphic, show that they have different characteristic

Ex: $\mathbb{Z}_2 \times \mathbb{Z}_2$ has characteristic 2:

$$2 \cdot (1,1) = (1,1) + (1,1) = (0,0)$$

$\mathbb{Z}_4$ has chacteristic 4:

$$4 \cdot [1]_4 = [4]_4 = [0]_4$$

(5) identity: if one ring has identity and the other does not, then the rings are not isomorphic.

Ex: $2\mathbb{Z}$ w/ regular addition and mult. has no identity, so it's <u>not</u> isomorphic to $\mathbb{Z}$.