Ended with: Ring homomorphisms preserve ring structure

Definition

A ring homomorphism $\varphi : R \to S$ is a function so that

1. $\varphi(0_R) = 0_S$
2. $\varphi(1_R) = 1_S$
3. $\varphi(-r) = -\varphi(r)$
4. $\varphi(r + s) = \varphi(r) + \varphi(s)$
5. $\varphi(rs) = \varphi(r)\varphi(s)$

Two of these properties follow from the other three...

Examples of ring homomorphisms.

Non-examples

- det : $M_{n\times n}(R) \to R$ is not a homomorphism: doesn't preserve addition
- The map $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ defined by $f([n]) = [4n]$ satisfies everything but doesn't preserve the identity
- The map zero map $R \to S$ sending everything to 0_S is only a homomorphism if S is the trivial ring; otherwise it doesn't preserve multiplicative identities

Is there a ring homomorphism $\varphi : \mathbb{Z} \to M_{3\times 3}(\mathbb{R})$?

How many such ring homomorphisms?

A useful lemma

Lemma

For any ring R, there is a unique ring homomorphism $f : \mathbb{Z} \to R$.

To prove the lemma, we need to write down a ring homomorphism $f : \mathbb{Z} \to R$ to show there *is* one.

Then, we need to prove that any other ring homomorphism *has* to be the same as f (uniqueness).

Isomorphisms

Informally, we think of things as being isomorphic if they are "the same". This is subtly and importantly different than being "equal".

Definition

A ring homomorphism $\varphi : R \to S$ is a *isomorphism* if there is another ring homomorphism $: S \to R$ with

$$\varphi \circ \psi = \mathrm{Id}_S, \quad \psi \circ \varphi = \mathrm{Id}_R$$

A silly example

Let R be a copy of $\mathbb{Z}$ painted red. Let S be a copy of $\mathbb{Z}$ painted green.
Then R and S are isomorphic, but they aren't equal.

A more serious example

Let R be a commutative ring, and for a set X recall that $\text{Fun}(X, R)$, the set of functions from X to R, is a ring under pointwise addition and multiplication. Let $\{x\}$ be a one element set.

$\text{Fun}(\{x\}, R) \cong R$

To prove this, we define $\varphi : \text{Fun}(\{x\}, R) \to R$ by $\varphi(f) = f(x)$.

For $r \in R$ let $g_r \in \text{Fun}(\{x\}, R)$ be defined by $g_r(x) = r$. Then we define $\psi : R \to \text{Fun}(\{x\}, R)$ by $\psi(r) = g_r$.

Then ϕ and ψ are inverses to each other.

Similarly, $\text{Fun}(\{x, y\}, R) \cong R \times R$.

Another viewpoint on isomorphisms

Lemma

If $\varphi : R \to S$ is a bijective homomorphism, then φ is an isomorphism.

Proof.

Since φ is a bijection, we know from first year that there is an inverse map φ^{-1} of sets, we need to show that φ^{-1} is a ring homomorphism.

We need to check... (See board and/or notes)

$\square$

Nonisomorphic rings

Any *reasonable* property of rings (i.e., defined in terms of properties of the ring structure, and not in terms of something extraneous like being green or red) are invariant under isomorphism.

So, for example, if R and S are isomorphic, and R is an integral domain, than so is S.

To show two rings R and S are *not* isomorphic, it is usually easiest to find something true about one ring but not the other.

Lemma

None of the rings $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *or* $\mathbb{C}$ *are isomorphic to each other.*

Kernels and Images, ideals and subrings

From a ring homomorphism $\varphi : R \to S$, we define the kernel $\ker(\phi)$ and the image $\mathrm{Im}(\varphi)$ in the same way we did for linear maps of vector spaces:

$$\mathrm{Im}(\varphi) = \{s \in S : s = \varphi(r) \text{ for some } r \in R\}$$
$$\ker(\varphi) = \{r \in R : \varphi(r) = 0_S\}$$

Though the kernel and the image are both subsets of a ring, it turns out they are very different types of subsets.

- The kernel is the prototypical (only!) example of an *ideal*
- The image is the prototypical (only!) example of a *subring*

A simple use of image and kernel

Lemma

Let $\varphi : R \to S$ a ring homomorphism. Then

1. *φ is surjective if and only if $Im(\varphi) = S$*
2. *φ is injective if and only if $\ker(\varphi) = \{0_R\}$*

Proof

? ? ?