

# Commutative Algebra MAS439

## Lecture 2: Homomorphisms

Paul Johnson  
paul.johnson@sheffield.ac.uk  
Hicks J06b

October 5th

# Plan: slow down a little

## Last week - Didn't finish

- ▶ Course policies + philosophy
- ▶ Sections 2-4: Rings, examples, homomorphisms

## Today

- ▶ Finish Section 4: Isomorphisms, image, kernel
- ▶ Cover Section 5: Subrings
- ▶ Start Section 6: Ideals

## Next week

- ▶ Finish Chapter 6: Ideals
- ▶ Discuss Writing/Homework
- ▶ Do Chapter 7: Quotient rings

# 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  $\varphi : R \rightarrow S$  is a *isomorphism* if there is another ring homomorphism  $\psi : S \rightarrow R$  with

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

## A silly example

A green copy of  $\mathbb{Z}$  and a red copy of  $\mathbb{Z}$  are isomorphic, but they aren't equal.

# A nontrivial example

## Lemma

Let  $X = \{x_1, \dots, x_n\}$  be a finite set with  $n$  elements, and let  $R$  be a ring. Then

$$\text{Fun}(X, R) \cong R^n := \underbrace{R \times R \times \cdots \times R}_{n \text{ times}}$$

## Proof

- ▶ Define  $\varphi : \text{Fun}(X, R) \rightarrow R^n$  by  $\varphi(f) = (f(x_1), f(x_2), \dots, f(x_n))$ ,
- ▶ Define  $\psi : R^n \rightarrow \text{Fun}(X, R)$  by  $[\psi(r_1, \dots, r_n)](x_i) = r_i$ .
- ▶ Check a buncha stuff.

## Another viewpoint on isomorphisms

### Lemma

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

### Proof.

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

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

In notes, this is taken as the *definition* of isomorphic rings, but the definition we gave is the *right* one because it generalizes. It is NOT true that if  $f : X \rightarrow Y$  is a bijective continuous map of topological spaces, then  $X \cong Y$ .

# 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, then 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.*

Proof:

???

## Kernels and Images, ideals and subrings

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

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

$$\ker(\varphi) = \{r \in R : \varphi(r) = 0_S\}$$

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  $\varphi : R \rightarrow S$  a ring homomorphism. Then

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

## Proof

???



# Definition of a subring

Let  $R$  be a ring, and let  $S \subset R$  be a subset.

## Idea

We say  $S$  is a subring of  $R$  if it is a ring, and all its structure comes from  $R$ .

## Definition

We say  $S \subset R$  is a subring if:

- ▶  $S$  is closed under addition and multiplication:

$$r, s \in S \text{ implies } r + s, r \cdot s \in S$$

- ▶  $S$  is closed under additive inverses:  $r \in S$  implies  $-r \in S$ .
- ▶  $S$  contains the identity:  $1_R \in S$

## Lemma

*A subring  $S$  is a ring.*

## First examples of subrings

- ▶  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$  is a chain of subrings.
- ▶ if  $R$  any ring,  $R \subset R[x] \subset R[x, y] \subset R[x, y, z]$  is a chain of subrings.

## Another chain of subrings

$$\mathbb{R} \subset \mathbb{R}[x] \subset C^\infty(\mathbb{R}, \mathbb{R}) \subset C(\mathbb{R}, \mathbb{R}) \subset \text{Fun}(\mathbb{R}, \mathbb{R})$$

Where, working backwards:

- ▶  $\text{Fun}(\mathbb{R}, \mathbb{R})$  is the space of all functions from  $\mathbb{R}$  to  $\mathbb{R}$
- ▶  $C(\mathbb{R}, \mathbb{R})$  are the continuous functions
- ▶  $C^\infty(\mathbb{R}, \mathbb{R})$  are the *smooth* (infinitely differentiable) functions
- ▶  $\mathbb{R}[x]$  are the polynomial functions
- ▶ We view  $\mathbb{R}$  as the space of constant functions

## Non-examples of subrings

- ▶  $\mathbb{N} \subset \mathbb{Z}$
- ▶ Let  $\mathcal{K}$  be the set of continuous functions from  $\mathbb{R}$  to itself with bounded support. That is,

$$f \in \mathcal{K} \iff \exists M \text{ s.t. } |x| > M \implies f(x) = 0$$

- ▶ Let  $R = \mathbb{Z} \times \mathbb{Z}$ , and let  $S = \{(x, 0) \in R \mid x \in \mathbb{Z}\}$ .
- ▶  $\{0, 2, 4\} \subset \mathbb{Z}/6\mathbb{Z}$

# The image of a homomorphism is a subring

## Lemma

Let  $\varphi : R \rightarrow S$  be a homomorphism. Then  $\text{Im}(\varphi) \subset S$  is a subring.

## Proof.

We need to check  $\text{Im}(\varphi)$  is closed under addition and multiplication and contains  $1_S$ . □

# Ideals

# Generating subrings

# Motivation for generators from Group theory

When working with groups, we often write groups down in terms of generators and relations.

## Generators are easy

To say a group  $G$  is *generated* by a set of elements  $E$ , means that we can get  $G$  by “mashing together” the elements of  $E$  in all possible ways. More formally,

$$G = \{g_1 \cdot g_2 \cdots g_n \mid g_i \text{ or } g_i^{-1} \in E\}$$

## Relations are harder

Typically there will be many different ways to write the same element in  $G$  as a product of things in  $E$ ; recording how is called relations.



# Reminder example? Okay if it's new to you

## Example

The dihedral group  $D_8$  is the symmetries of the square. It is often written as

$$D_8 = \langle r, f \mid r^4 = 1, f^2 = 1, rf = fr^{-1} \rangle$$

Meaning that the group  $D_8$  is *generated* by two elements,  $r$  and  $f$ , satisfying the *relations*  $r^4 = 1$ ,  $f^2 = 1$  and  $rf = fr^{-1}$ .

We'll want a way to write down commutative rings in the same way

## Preview of rings from generators and relations

We will revisit these examples further after we have developed ideals and quotient rings – you can think of these as the machinery that will let us impose relations on our generators.

### Example (Gaussian integers)

The Gaussian integers are written  $\mathbb{Z}[i]$ ; they're generated by an element  $i$  satisfying  $i^4 = 1$ .

### Example (Field with 4 elements)

The field  $\mathbb{F}_4$  of four elements can be written  $\mathbb{F}_2[x]/(x^2 + x + 1)$  – to get  $\mathbb{F}_4$ , we add an element  $x$  that satisfies the relationship  $x^2 + x + 1 = 0$ .

## Idea of generating set

The subring generated by elements in a set  $T$  will again be “what you get when you mash together everything in  $I$  in all possible ways”, but this is a bit inelegant and not what we will take to be the *definition*.

### Attempted definition

Let  $T \subset R$  be any subset of a ring. The *subring generated by  $T$* , denoted  $\langle T \rangle$ , *should be* the smallest subring of  $R$  containing  $T$ .

This is not a good formal definition – what does “smallest” mean? Why is there a smallest subring containing  $T$ ?

# Intersections of subrings are subrings

## Lemma

Let  $R$  be a ring and  $I$  be any index set. For each  $i \in I$ , let  $S_i$  be a subring of  $R$ . Then

$$S = \bigcap_{i \in I} S_i$$

is a subring of  $R$ .

Proof.

?????



# The elegant definition of $\langle T \rangle$

## Definition

Let  $T \subset R$  be any subset. The *subring generated by  $T$* , denoted  $\langle T \rangle$ , is the intersection of all subrings of  $R$  that contain  $T$ .

## This agrees with our intuitive “definition”

$\langle T \rangle$  is the smallest subring containing  $T$  in the following sense: if  $S$  is any subring with  $T \subset S \subset R$ , then by definition  $\langle T \rangle \subset S$ .

## But it's all a bit airy-fairy

The definition is elegant, and can be good for proving things, but it doesn't tell us what, say  $\langle \pi, i \rangle \subset \mathbb{C}$  actually looks like. Back to “mashing things up” ...

## What *has* to be in $\langle \pi, i \rangle$ ? Start mashing!

Rings are a bit more complicated because there are two ways we can mash the elements of  $T$  – addition and multiplication.

- ▶  $1, \pi, i$
- ▶ Sums of those; say,  $5 + \pi, 7i$
- ▶ Negatives of those, say  $-7i$
- ▶ Products of those, say  $(5 + \pi)^4 i^3$
- ▶ Sums of what we have so far, say  $(5 + \pi)^4 i^3 - 7i + 3\pi^2$
- ▶ ...

leading to things like:

$$\left( ((5 + \pi)^4 i^3 - 7i + 3\pi^2) \cdot (-2 + \pi i) + \pi^3 - i \right)^{27} - 5\pi^3 i$$

Of course, could expand that out into just sums of terms like  $\pm \pi^m i^m \dots$

# Formalizing our insight

## Definition

Let  $T \subset R$  be any subset. Then a *monomial in  $T$*  is a (possibly empty) product  $\prod_{i=1}^n t_i$  of elements  $t_i \in T$ . We use  $M_T$  to denote the set of all monomials in  $T$ .

## Note:

The empty product is the identity  $1_R$ , and so  $1_R \in M_T$ .

## Our insight:

From the “mashing” point of view  $\langle T \rangle$  should be all  $\mathbb{Z}$ -linear combination of monomials.

# The elegant and “mashing” definitions agree

## Lemma

$\langle T \rangle = X_T$ , where  $X_T$  consists of those elements of  $R$  that are finite sums of monomials in  $T$  or their negatives. That is:

$$X_T = \left\{ \sum_{k=0}^n \pm m_k \mid m_k \in M_T \right\}$$

## Proof.

- ▶  $X_T \subset \langle T \rangle$ ?
- ▶  $\langle T \rangle \subset X_T$ ?





# Example: The Gaussian integers

What's  $\langle i \rangle \subset \mathbb{C}$ ?

- ▶ What's the set of monomials?
- ▶ But can we simplify even more?

# Generating sets for rings

## Definition

We say that a ring  $R$  is *generated by* a subset  $T$  if  $R = \langle T \rangle$ . We say that  $R$  is *finitely generated* if  $R$  is generated by a finite set.

## Examples of generating sets

- ▶  $\mathbb{Z} = \langle \emptyset \rangle$
- ▶  $\mathbb{Z}/n\mathbb{Z} = \langle \emptyset \rangle$
- ▶  $\mathbb{Z}[x] = \langle x \rangle = \langle 1 + x \rangle$
- ▶  $\mathbb{Z}[i] = \langle i \rangle$

## Some of your best friends are not finitely generated

- ▶ The rationals  $\mathbb{Q}$  are not finitely generated: any finite subset of rational numbers has only a finite number of primes appearing in their denominator.
- ▶ The real and complex numbers are uncountably; a finitely generated ring is countable

# A non-finitely generated subring of a finitely generated ring

We've seen that  $\mathbb{Z}[x] = \langle x \rangle$  and so is finitely generated.

$$S = \{a_0 + 2a_1x + \cdots + 2a_nx^n\}$$

that is,  $S$  consists of polynomials all of whose coefficients, except possibly the constant term, are even.

**Challenge:**

Show that  $S$  is a subring of  $\mathbb{Z}[x]$  (easy), but that  $S$  is not finitely generated (harder).