# MAS439 Lecture 5 Isomorphism Theorem

October 13th

Yesterday, we motivated and defined the quotient ring R/I, proved it was a ring, and looked at some examples.

Today is centred around the first isomorphism theorem, which states that for any homomorphism

 $\varphi: R \to S$ ,  $\operatorname{Im}(\varphi) \cong R / \ker(\varphi)$ . However, the possibly new to you part, and a main player, is the Universal Property of quotient rings.

# The Universal Property for Quotient rings

Suppose that  $\varphi:R\to S$  is a ring homomorphism such that  $I\subset \ker(\varphi)$ , and let  $p:R\to R/I$  be the quotient map. Then there exists a unique ring homomorphism  $\overline{\varphi}:R/I\to S$  satisfying  $\varphi=\overline{\varphi}\circ p$ .

### Put another way

The following diagram commutes:

$$R \xrightarrow{f} S$$

$$p \downarrow \qquad \qquad \downarrow \uparrow \\ R/I$$

# What the universal property "really means"

### Universal property as a slogan:

Maps out of R/I are the same thing as maps out of R whose kernel contains I

This property *defines* the quotient ring R/I.

### Categorical thinking as a slogan:

Understand an object by understanding how it relates to other objects. As an example, if you know all the maps out of an object, you know the object.

# Proof of the Universal Property

### Uniqueness of $\overline{\varphi}$ :

If  $[r] \in R/I$ , we want to know  $\overline{\varphi}([r])$ . Noting that [r] = p(r), we see that having  $\varphi = \overline{\varphi} \circ p$  is equivalent to:

$$\overline{\varphi}([r]) = \overline{\varphi}(p(r)) = \varphi(r)$$

Thus, we take as a definition  $\overline{\varphi}([r]):=\varphi(r)$  to guarantee  $\varphi=\overline{\varphi}\circ p$ .

### What's left?

- Show  $\overline{\varphi}$  is a homomorphism;
- ▶ We are defining what  $\overline{\varphi}$  in terms of representatives, so we must show it's well defined.

# Proof of the Universal Property

 $\overline{\varphi}$  is a ring homomorphism:

We check addition:

$$\begin{split} \overline{\varphi}([s] + [r]) &= \overline{\varphi}([r+s]) \\ &= \varphi(r+s) \\ &= \varphi(r) + \varphi(s) \\ &= \overline{\varphi}([r]) + \overline{\varphi}([s]) \end{split}$$

Multiplication and unit are similar.

# Proof of the Universal Property

### $\overline{\varphi}$ is well defined:

Suppose that  $r\sim s$ ; we must show  $\overline{\varphi}([s])=\overline{\varphi}([r])$ , i.e., that  $\varphi(r)=\varphi(s)$ .

But  $r \sim s$  means r = s + i for  $i \in I$ , so

$$\varphi(r) = \varphi(s+i) = \varphi(s) + \varphi(i) = \varphi(s)$$

since  $I \subset \ker(\varphi)$ .

# Digging old tools out of the shed

To prove the isomorphism theorem, we are going to use the following two facts we've already seen:

- ▶ Any ring homomorphism  $\varphi : R \to S$  factors as the surjection from  $\varphi : R \to \operatorname{Im}(\varphi)$  and the inclusion  $i : \operatorname{Im}(\varphi) \to S$
- ▶ A homomorphism  $\varphi$  is injective if and only if  $\ker(\varphi) = 0$ .

## Isomorphism Theorem Restated

Any ring homomorphism  $\varphi:R o S$  can be written uniquely in the form

$$\varphi = i \circ \overline{\varphi}' \circ p$$

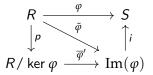
#### where

- ▶  $p: R \to R / \ker \varphi$  is the quotient map
- ▶  $\overline{\varphi}'$  :  $R / \ker(\varphi) \to \operatorname{Im}(\varphi)$  is an isomorphism
- $i: \operatorname{Im}(\varphi) \to S$  is the inclusion

$$egin{aligned} R & \stackrel{arphi}{----} & S \ & \downarrow^p & \uparrow^i \ R / \ker arphi & \stackrel{\overline{arphi}'}{----} & \operatorname{Im}(arphi) \end{aligned}$$

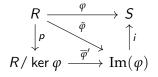
# Proof of the First isomorphism theorem

From the toolshed, we have a surjective map  $\tilde{\varphi}: R \to \operatorname{Im}(\varphi)$  with  $\varphi = i \circ \tilde{\varphi}$ . That is, we have the upper right triangle commutes:



Furthermore, since i is injective, we have  $\ker \tilde{\varphi} = \ker i \circ \varphi = \ker \varphi$ 

### Proof of the first isomorphism theorem



To get the bottom triangle, we apply the universal property of  $R/\ker \varphi$  to  $\widetilde{\varphi}$  to construct the map  $\overline{\varphi}'$ .

- Bottom triangle commutes by universal property
- $ightharpoonup \overline{\phi}'$  surjective since  $\widetilde{\phi}$  is
- $ightharpoonup \overline{\phi}'$  injective since:

$$\overline{\varphi}'([r]) = 0 \iff \tilde{\varphi}(r) = 0 \iff r \in \ker(\tilde{\varphi}) \iff r \sim 0_R$$



- ♣ Let's all go to the lobby ♣
- Let's all go to the lobby →(2 minute intermission)

# Application of Isomorphism theorem: $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

Evaluation at i gives a map

$$f: \mathbb{R}[x] \to \mathbb{C}$$
  $f: p \mapsto p(i)$ 

- ▶ We have  $x^2 + 1 \in \ker(f)$ , and so by definition  $(x^2 + 1) \in \ker(f)$
- lacktriangle By universal property, get a map  $\overline{f}:R[x]/(x^2+1) o \mathbb{C}$
- ► First isomorphism theorem says this map is an  $\cong$  if  $ker(f) = (x^2 + 1)$
- ▶ If  $g \notin (x^2 + 1)$ , can see  $g \notin \ker(f)$  using division algorithm:

$$g = (x^2 + 1)p(x) + ax + b \implies f(g) = ai + b$$



# The pullback of an ideal is an ideal

### Lemma

Let f:R o S a map,  $I\subset S$  an ideal. Then  $f^{-1}(I)\subset R$  an ideal

### Proof.

Suppose  $a, b \in f^{-1}(I), r \in R$ 

- $f^{-1}(I)$  is nonempty since it contains 0.
- ▶ We have  $a + b \in f^{-1}(I)$  since

$$f(a+b) = f(a) + f(b) \in I$$

▶ We have  $r \cdot a \in f^{-1}(I)$  since

$$f(ar) = f(a)f(r) \in I$$



#### Lemma

If  $I \subset J \subset R$  are two ideals, then

$$J/I = \{ [r] \in R/I : r \in J \}$$

is an ideal in R/I.

### Proof.

Need to check:

- ▶ Well defined: i.e., if  $[r_1] = [r_2]$  then  $[r_1] \in J/I \iff [r_2] \in J/I$ .
- nonempty
- Closed under addition
- $\triangleright$  closed under multiplication by elements of R/I.

The lemmas give us maps back and forth between ideals of R containing I and ideals of R/I:

- ▶ If  $K \subset R/I$  an ideal, then  $I \subset p^{-1}(K) \subset R$  an ideal.
- ▶ If  $I \subset J \subset K$ , then J/I an ideal of R/i.

### Lemma

The above maps are inverse

The fact that  $p^{-1}(J/I) = J$  is exactly the definition.

Now suppose  $K \subset R/I$  an ideal; we must show  $p^{-1}(K)/I = K$ .

- ▶ If  $[a] \in p^{-1}(K)$ , then  $a \in p^{-1}(K)$ , so  $p(a) = [a] \in K$ .
- ▶ If  $[a] \in K$ , then  $a \in p^{-1}(K)$ , and so  $[a] \in p^{-1}(K)/I$

# A corollary

#### Lemma

If R is a principal ideal domain, then R/I is a principal ideal domain.

### Proof.

Suppose that KR/I is an ideal. Then K is of the form J/I for some ideal  $I \subset J \subset R$ . Since R is a principal ideal domain, J = (r). But then ([r]) generates J/I.

Since  $\mathbb{Z}$  is a principal ideal domain, we have  $\mathbb{Z}/k$  is.

# Third isomorphism theorem

#### **Theorem**

If  $I \subset J \subset R$  ideals, then  $R/J \cong (R/I) \cong (J/I)$ 

### Proof.

We construct a map  $f: R/J \to R/I$  by taking  $f([r]_{R/J}) = [r]_{R/I}$ . Need to check:

- Well defined
- Surjective
- ring homomorphism
- $ightharpoonup \ker(f) = J/I$

Then it follows from first isomorphism theorem.

## **Examples**

▶ What do we get from  $(2) \subset (8) \subset \mathbb{Z}$ ?

$$(\mathbb{Z}/8)/(2) \cong \mathbb{Z}/2$$

▶ What do we get from  $(2) \subset (2, x^2 + x + 1) \subset \mathbb{Z}[x]$ ?

$$\mathbb{Z}[x]/(2, x^2 + x + 1) \cong (\mathbb{Z}[x]/(2))/(2, x^2 + x + 1)$$
$$\cong \mathbb{F}_2[x]/(x^2 + x + 1)$$
$$\cong \mathbb{F}_4$$