MAS439 Lecture 6
Examples of Quotient Rings
What's the Universal Property all about?

October 12th

Last time, we introduced the quotient ring R/I

Definition

Let R be a ring, and I an ideal. Then the ring R/I is the set of equivalence classes of elements of R, where $r \sim s$ if $r - s \in I$. Addition and multiplication are given by adding and multiplying representatives:

$$[r] + [s] = [r + s]$$

$$[r] \cdot [s] = [r \cdot s]$$

$$1_{R/I} = [1]$$

Lemma

The map $p : R \to R/I$ defined by $p(r) = [r]$ is a homomorphism.

The problem with this definition:

To talk about what the elements are, we need to understand what the equivalence classes are.

Usually we want to pick a unique representative from each class

This is exactly like thinking:

$$\mathbb{Z}/n = \{0, 1, \ldots, n-1\}$$

instead of the strict definition:

$$\mathbb{Z}/n = \left\{ \{a + n\mathbb{Z}\} : a \in \mathbb{Z} \right\}$$

The division algorithm is a good way to do this

Examples

Example: $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$

The division algorithm gives unique representatives

Any polynomial $p(x)$ can be written uniquely as

$$p(x) = (x^2+1)q(x) + bx + a$$

.

This means that $[p(x)] = [bx + a]$, so every class can be represented by a linear polynomial; furthermore, this representation is unique.

It's clear $[a + bx] + [c + dx] = [a + c + (b + d)x]$.

Example: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$

Multiplication of representatives

$$[a+bx]\cdot[c+dx] = [ac+(ad+bc)x+bdx^2]$$

But this isn't linear; we need to get rid of the x^2 term. Note that $bdx^2 = bd(x^2+1) - bd$, and so $[bdx^2] = [-bd]$.
Thus, we see

$$[a+bx]\cdot[c+dx] = [ac-bd+(ad+bc)x]$$

which, if we replace x with i, is exactly the formula for multiplying complex numbers.

Example: $\mathbb{R}[x]/(x^2)$

First, we have to understand it as a set – we want to give a *unique* name to each element of R/I. This is usually done by picking a representative from each coset in some systematic way.
I consists of linear combinations of monomials of degree 2 or bigger. So every equivalence class contains exactly one linear term $a + bx$. We see that

$$[a + bx] \cdot [c + dx] = [ac + adx + bcx + adx^2] = [ac + (ad + bc)x]$$

Constructing $\mathbb{F}_4$

We claim that $R = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a field with 4 elements. Exactly as in the last two examples, the division algorithm gives every equivalence class has a unique linear representative $a + bx$; now $a, b \in \mathbb{F}_2$, so there are indeed four elements.
We check:

$$[x] \cdot [x + 1] = [x^2 + x] = [1]$$

So every nonzero element has an inverse, and so R is a field.

A case where the division algorithm doesn't hold:

Consider the ring $\mathbb{Z}[x]/(10x-1)$:

Can't divide x by $10x-1$ and get a polynomial of lower degree.

What is this ring, intuitively?

Since we're setting $10x-1=0$, then x "should be" $1/10$. So, we've taken the integers and added $1/10$.

How to make this intuition formal?

To really understand the ring $\mathbb{Z}[x]/(10x-1)$, will find two different systems ofunique representatives for the equivalence classes.

Method 1: Muddle along with division algorithm

Lemma

For any polynomial $p(x) \in \mathbb{Z}[x]$, there is a unique polynomials $q(x)$ and a unique integer r, so that

- $p(x) = q(x)(10x - 1) + r$
- $q(x) = \sum a_n x^n$ *with* $0 \leq a_i \leq 9$

Proof.

- Existence
- Uniqueness

□

Every number in $\mathbb{Z}[1/10]$ has a unique terminating binary expansion.

Method 2: Divide "backwards"

Lemma

For any $p(x) \in \mathbb{Z}[x]$, there is a unique $q(x) \in \mathbb{Z}[x]$, $n \geq 0$, and $a \in \mathbb{Z}$, so that

$$p(x) = q(x)(1 - 10x) + ax^n$$

and a is not divisible by 10 if $n > 0$.

Proof.

- Existence: divide backwards as power series to get remainder ax^m, if 10 divides a, then backtrack
- Uniqueness

□

This is writing an element of $\mathbb{Z}[1/10]$ as $a/10^n$, and then if a is divisible by 10 we can cancel some powers of 2.

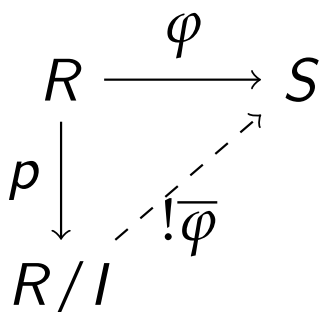
The Universal Property of Quotient Rings

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:



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.

Lemma

Let R be a ring, and I be an ideal. If $q : R \to T$ also satisfies the universal property of the quotient ring, then we have $T \cong R/I$.

Proof.

All we have is the Universal Property, so we're going to use it over and over again. . . □

. Universal properties are an idea from category theory

Definition of a category

A category $\mathcal{C}$ consists of

- A collection of objects $Ob(\mathcal{C})$
- For every pair of objects A, B a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of morphisms (or arrows)

We write $f : X \to Y$ to mean $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.
We can compose arrows that line up (i.e., if
$f : X \to Y, g : Y \to Z$ then we can make $gf : X \to Z$)
This composition is associative; and every object has an identity morphism 1_A so that $f1_A = 1_B f = f$.

Examples of categories

- Sets and functions between them
- Groups and group homomorphisms
- Rings and ring homomorphisms
- Vector spaces over a field k and linear maps between them
- Topological spaces and continuous maps between then

All of the above are examples where our objects are sets, and our morphisms are maps between the sets preserving some kind of structure, but categories don't have to be this way.

Category theory is a philosophy

- Rather than study an object itself, we should study how it relates to other object of its kinds.
- moves the focus to the *morphisms*
- Really focus goes farther, between how different categories relate to each other...
- Captures when you do the same thing in different categories

Example tying this together: product as a Universal Property

Definition

Let X, Y be two objects in a category $\mathcal{C}$. The product, $X \times Y$, is an object of $\mathcal{C}$ together with maps $p_1 : X \times Y \to X$ and $p_2 : X \times Y \to Y$ satisfying the following universal property: for every object Z and pair of maps $f : Z \to X, g : Z \to Y$, there is a unique map h so that $f = p_1 h$ and $g = p_2 h$.