MAS439 Lecture 6
Examples of Quotient Rings
First taste of category theory
Universal Property of Quotient Rings

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.

Examples

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:

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

The division algorithm is a good way to do this

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 $\mathbb{Z}[x]/(2x-1)$:

Can't divide x by $2x-1$ and get a polynomial of lower degree.

What is this ring, intuitively?

Since we're setting $2x-1=0$, then x "should be" $1/2$. So, we've taken the integers and added $1/2$.

How to make this intuition formal?

To really understand the ring $\mathbb{Z}[x]/(2x-1)$, 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

- $p(x) = q(x)(2x - 1) + r$
- $q(x) = \sum a_n x^n$ *with* $a_i \in \{0, 1\}$

Proof.

- Existence
- Uniqueness

$\square$

Every number in $\mathbb{Z}[1/2]$ 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*

$$p(x) = q(x)(1 - 2x) + ax^n$$

and a *is odd if* $n > 0$*.*

Proof.

- Existence: divide backwards as power series to get remainder ax^m, if even, backtrack;
- Uniqueness

$\square$

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