MAS439 Lecture 5
Quotient Rings

October 12th

Recall an ideal $I \subset R$ was a subset that was closed under addition, and closed under multiplication by elements of R; in shorthand:

$$I + I \subset I$$

$$R \cdot I \subset I$$

Today, given an ideal $I \subset R$, we will define a *quotient ring* R/I. Tomorrow, we will prove the *first isomorphism theorem*, which at ti's simplest level says that given any homomorphism $\varphi : R \to S$, we have $\mathrm{Im}(\varphi) \cong R/I$.

A first example: $\mathbb{Z}/n\mathbb{Z}$

We've seen that the ideals of $\mathbb{Z}$ are precisely the principal ideals $(n) = n\mathbb{Z}$.
Thus $\mathbb{Z}/(n) = \mathbb{Z}/\mathbb{Z}$.

Something to keep in mind:

We often *think* "$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$."
This isn't quite right, really:

$$\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z}\}$$

We do this because awkward to think of ring elements as being themselves sets; and things in the second description have more than one name, i.e., $2 + 7\mathbb{Z} = -5 + 7\mathbb{Z}$.

You've seen this before: quotient groups

Recall that, given a normal subgroup $N \subset G$, we have the quotient subgroup G/N. The elements of G/N are the *cosets* of N – sets of the form gN. Alternatively, elements of G/N are equivalence classes, where $g \sim h$ if $gh^{-1} \in N$.

Why did N need to be normal?

To make multiplication well defined.

Equivalence relations and set partitions

Stuff

Definition of R/I as a set

As a set, the quotient ring R/I is defined to be the set of equivalence classes under the relation $r \sim s$ if $r - s \in I$.
If $r \in R$ any element, and $i \in I$ any element, we see that $r + i \sim r$. Furthermore, if $s \sim r$, then $s - r = i \in I$, and so $s = r + i$. Thus, we see that the equivalence classes of $\sim$ are exactly the cosets of I – sets of the form $r + I$.

Operations on R/I

We have defined what R/I is as a set; we now need to turn R/I into a ring. We define addition and multiplication on R/I by adding/multiplying representatives from the equivalence classes. That is,

$$[a] + [b] = [a + b]$$
$$[a] \cdot [b] = [a \cdot b]$$

To do list:

- Check that these operations are well defined
- Check that these operations satisfy the axioms of a ring

Addition is well defined

Suppose we chose $a' \sim a$ and $b' \sim b$. For addition to be well defined we need:

$$[a' + b'] := [a'] + [b'] = [a] + [b] =: [a + b]$$

- Since $a' \sim a$, we have $a' - a = i \in I$
- Since $b' \sim b$, we have $b' - b = i \in I$
- $(a' + b') - (a + b) = (a' - a) + (b' - b) = i + j$
- Since I closed under addition, $i + j \in I$, so $(a' + b') \sim (a + b)$

Multiplication is well defined

Suppose

$$a' - a = i \in I, \qquad b' - b = j \in I$$

We need to show that

$$a' \cdot b' - a \cdot b \in I$$

Then:

$$a' \cdot b' - a \cdot b = (a + i) \cdot (b + j) - a \cdot b = a \cdot j + b \cdot i + i \cdot j$$

- Since $i, j \in I$ and I an ideal, we have $a \cdot i, b \cdot j, i \cdot j \in I$.
- Since I is an ideal, their sum is also in I.
- Hence $a' \cdot b' \sim a \cdot b$ and multiplication is well defined.

R/I satisfies the ring axioms

These proofs are all just symbol pushing. For instance, to show that the distributive law holds, we have:

$$\begin{aligned}([a]+[b])\cdot[c] &= [a+b]\cdot[c]\\ &= [(a+b)\cdot c]\\ &= [a\cdot c+b\cdot c]\\ &= [a\cdot c]+[b\cdot c] = [a]\cdot[c]+[b]\cdot[c]\end{aligned}$$

In words

To me, that last proof was rather unenlightening.
The ring axioms are satisifed in R/I because the operations $+, \cdot$ are defined in terms of lifting to representatives in R; and the axioms hold there.

♫ Let's all go to the lobby ♫
♫ Let's all go to the lobby ♫
(2 minute intermission)

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

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

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.

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.