MAS439 Lecture 5
Quotient Rings

October 11th

Announcements

Homework 1: Whoops

I didn't ask you to justify 1 and 3...

...but then marked them as if I did.

I gave points back for those

Probably not reflected on homework you just corrected – I made a copy of all homeworks, will add points back from those.

In the future, you may lose points for not justifying things

Lots of interesting philosophical questions about fairness, unspoken cultural assumptions, what's the point of pure maths: check the bulletin.

Justify everything – but briefly, humanely

Russell and Whitehead, Principia Mathematica

$*35{\cdot}93.$ $\vdash : (R) . \phi(\mathrm{D}`R) . \equiv . (\alpha) . \phi\alpha$

Dem.

$\vdash . *33{\cdot}12 . *14{\cdot}18 . \supset \vdash : (\alpha) . \phi\alpha . \supset . \phi(\mathrm{D}`R) :$

[$*10{\cdot}11{\cdot}21$] $\supset \vdash : (\alpha) . \phi\alpha . \supset . (R) . \phi(\mathrm{D}`R)$ (1)

$\vdash . *10{\cdot}1 .$ $\supset \vdash : (R) . \phi(\mathrm{D}`R) . \supset . \phi\{\mathrm{D}`(\alpha \uparrow \alpha)\} .$

[$*35{\cdot}9$] $\supset . \phi\alpha :$

[$*10{\cdot}11{\cdot}21$] $\supset \vdash : (R) . \phi(\mathrm{D}`R) . \supset . (\alpha) . \phi\alpha$ (2)

$\vdash . (1) . (2) .$ $\supset \vdash . \mathrm{Prop}$

$*35{\cdot}931.$ $\vdash : (R) . \phi(\mathrm{C}`R) . \equiv . (\alpha) . \phi\alpha$ [Proof as in $*35{\cdot}93$]

$*35{\cdot}932.$ $\vdash : (R) . \phi(C`R) . \equiv . (\alpha) . \phi\alpha$ [Proof as in $*35{\cdot}93$]

$*35{\cdot}94.$ $\vdash : (\exists R) . \phi(\mathrm{D}`R) . \equiv . (\exists\alpha) . \phi\alpha$ [$*35{\cdot}93 . \mathrm{Transp}$]

$*35{\cdot}941.$ $\vdash : (\exists R) . \phi(\mathrm{C}`R) . \equiv . (\exists\alpha) . \phi\alpha$ [$*35{\cdot}931 . \mathrm{Transp}$]

$*35{\cdot}942.$ $\vdash : (\exists R) . \phi(C`R) . \equiv . (\exists\alpha) . \phi\alpha$ [$*35{\cdot}932 . \mathrm{Transp}$]

Thurston: Mathematics is for human understanding

Homework 2: Whoops

I forgot a minus sign. Two possible fixes:

- Keep ω the same, but $\omega^2 - \omega + 1 = 0$
- Instead of ω, use

$$\rho = -1/2 + i\sqrt{3}/2$$

Then $\rho^2 + \rho + 1 = 0$

Results in the same ring: $\{a + b\omega\} = \{c + d\rho\}$ because $\omega = \rho + 1$.

Sorry!

Proofs should go unchanged, won't lose marks because of this.

Pure Math Colloquia: Wednesdays at 2:00

Theoretically, aimed to be understandable by all graduate students. . .

. . . but often fails that in practise.

Usually in J11.

Graduate student seminars/colloquia

Not yet running/just starting. A few fourth years attended last year; bug me next week or two if you're potentially interested.

Next weeks colloquium should definitely be good, though

Pure mathematics in crisis

Kevin Buzzard, Imperial College

Wednesday October 17, 2-3, Hicks Lecture Theatre C

Abstract:

I argue that pure mathematics is walking inexorably towards a cliff edge, and that anyone who believes that current pure mathematics is rigorous, or a science, needs to wake up and look at the facts, which there will be plenty of in this talk, and they are not pretty. Are our results reproducible? Does it matter? What *is* mathematics? Can computer scientists save us? Can *undergraduates* save us? I hope so. This talk is about pure mathematics but will be accessible to undergraduates, mathematicians both pure and applied/applicable and computer scientists.

Buzzard background reading I

High mathematical drama

Mochizuki's "proof" of the ABC conjecture

- ABC: roughly, let $a + b = c$, a, b, c relatively prime, and d be the product of distinct primes in abc. Then d is usually not much smaller than c.
- Put another way, if a and b have large powers of primes, then c usually doesn't.
- Implies Fermat's last theorem $a^n + b^n \neq c^n$
- Shinichi Mochizuki has claimed a proof in 2012; 500 pages of very new mathematics, recently Peter Scholze has claimed a major gap.

Buzzard background reading II

More mathematical drama!

Hales's proof of the Kepler conjecture

- Keper Conjecture: the densest way to pack three dimensional balls are how oranges are stacked in the grocers
- Hales and Ferguson gave a proof in 1998, involved lots of computer proofs
- Referees ran a seminar over several years to check it
- Published in 2005, but disclaimer that referees were only 98% sure it was right
- "Project Flyspeck", a formal proof of the Kepler Conjecture, was completed in 2014

The next few lectures: hard, so we're slowing down

This week

Thu: Intro to quotient rings (Chapter 7)

Fri:
- Examples of quotient rings (Chapter 7 + more)
- Thinking about quotient rings
  (Making things implicitly in notes explicit)
- Start category theory, universal property
  (extra material + Chapter 8)

Next week

Thu: Isomorphism theorem (Chapter 8)

Fri: I'll be gone.
- Clean up?
- Maximal, Prime, radical ideals (Chapter 9)

Quotient Rings

Goal:

Intuition: set everything in I to be 0

Given a ring R and an ideal $I \subset R$, construct a new ring R/I and a homormophsim $p : R \to R/I$ so that

- p is surjective
- $\ker(p) = I$

It's just like...

- If $N \subset G$ a normal subgroup, we can make the quotient group G/N
- If $W \subset V$ a sub-vector space, we can make the quotient vector spave V/W.

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

The map from $p : \mathbb{Z} \to \mathbb{Z}/n$, $p(k) = [k]_n$ is surjective, and has kernel $I = n\mathbb{Z}$.
Thus when $I = (n)$, then $\mathbb{Z}/I = \mathbb{Z}/n\mathbb{Z}$.

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., $2 + 7\mathbb{Z} = -5 + 7\mathbb{Z}$.

Review of 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.

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 $r - s \in I$.

Why?

Recall we want to build a map $p : R \to R/I$ with $\ker(p) = I$. We should have $r \sim s$ if $p(r) = p(s)$. But:

$$p(r) = p(s) \iff p(r - s) = 0 \iff r - s \in I$$

Another perspective: cosets

The equivalence classes are exactly the sets of the form

$$r + I = \{x \in R | x = r + i \text{ for some } i \in I\}$$

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 show this makes R/I into a ring we need to:

- 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:

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

Here for clarity we use $+, \cdot$ for the operations in R and $+', \cdot'$ for the operations in R/I.

In words

That last proof was rather unenlightening.

A paraphrase:

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.

Starting Examples

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.