Math Club Notes: 2005 June 13

1 An integral

A fun problem: evaluate

$$\int_0^\pi \ln \sin x \, dx \, .$$

Note that the integral is improper — the integrand isn't defined at either endpoint. So you might want to show that the integral converges. But even assuming convergence, evaluating it is tricky.

2 Circular relations

A relation R is called *circular* if

$$\forall x, y, z\colon x R y \text{ and } y R z \implies z R x \, .$$

Circularity is like transitivity, but backwards.

Transitivity Circularity

In these figures, the solid arrows indicate what is given, and the dashed arrows indicate what may be inferred. The cycle in the right-hand graph is the basis for the name "circular".

A question seen in the Cmpt 272 seminar last winter: Show that if a relation is reflexive and circular then it is an equivalence relation.

Recall that to be an equivalence relation consists of having three properties:

1. Reflexivity: $\forall x\colon x R x$
2. Symmetry: $\forall x, y\colon x R y \implies y R x$
3. Transitivity: $\forall x, y, z\colon x R y \text{ and } y R z \implies x R z$

Reflexivity is given, so we need only show symmetry and transitivity. Given the remark above that circularity is like transitivity but backwards, it's easy to spot that, once you have symmetry, transitivity quickly follows. Ray and Eileen did it by reversing the hypothesis:

$$\begin{aligned} x R y \text{ and } y R z &\implies y R x \text{ and } z R y && \text{(symmetry)} \\ &\implies z R y \text{ and } y R x && \text{(commutativity of "and")} \\ &\implies x R z && \text{(circularity)} \end{aligned}$$

It can also be done by reversing the conclusion:

$$\begin{aligned} xRy \text{ and } yRz &\implies zRx && \text{(circularity)} \\ &\implies xRz && \text{(symmetry)} \end{aligned}$$

So now it remains only to show symmetry.

What we want to show is

$$xRy \implies yRx\,.$$

There is a simple proof-finding strategy which happens to work here. The idea is to make something you know look like what you're trying to prove. In this case, we are given reflexivity and circularity; of the two, circularity looks more like what we want to show. It has a "$\Rightarrow$", and the conclusion is that something R something else. Lining these up, we have

$$\begin{aligned} xRy \text{ and } yRz &\implies zRx && \text{(known)} \\ xRy &\implies yRx && \text{(desired)} \end{aligned}$$

In fact, there is a further similarity between these two: both have "xRy" in the hypothesis. Line that up:

$$\begin{aligned} xRy \text{ and } yRz &\implies zRx && \text{(known)} \\ xRy &\implies yRx && \text{(desired)} \end{aligned}$$

So now, make what is known look more like what is desired. The desired conclusion has y where we have z; so replace z with y:

$$\begin{aligned} xRy \text{ and } yRy &\implies yRx && \text{(known)} \\ xRy &\implies yRx && \text{(desired)} \end{aligned}$$

If only we could show that yRy! But wait — that's just reflexivity, which is given.

So here's a proof of symmetry:

$$\begin{aligned} xRy &\implies xRy \text{ and } yRy && \text{(reflexivity)} \\ &\implies yRx && \text{(circularity)} \end{aligned}$$

(You could also come up with this proof by trying to find some way — any way — to combine the givens.)

Historical note: I think Hilbert used this in his development of the foundations of geometry. He took as axioms that the relation "is congruent to" is reflexive and circular, then proved as a theorem that it is an equivalence relation. (I think this is mentioned in Hartshorne, but I can't check because my copy is out on loan.)

3 Cauchy Mean Value Theorem

For another example of this proof-finding strategy, the Cauchy Mean Value Theorem:

> If f and g are continuous on $[a, b]$ and differentiable on (a, b), then
>
> $$f'(c)(g(b) - g(a)) = g'(c)(f(b) - f(a))$$
>
> for some $c \in (a, b)$.

(This is more or less the same as saying that

$$\frac{f'(c)}{g'(c)} = \frac{f(b) - f(a)}{g(b) - g(a)} = \frac{(f(b) - f(a))/(b - a)}{(g(b) - g(a))/(b - a)} .$$

On the far right, we have the ratio of the average velocities of f and g; the theorem states that at some point betwen a and b, the instantaneous velocities are in that same ratio. Of course, this reformulation ignores the possibility that $g'(c)$ or $g(b) - g(a)$ might be zero, but the point of the reformulation is just to express the intuitive content of the theorem, so it's okay to reason a bit sloppily. This theorem is, by the way, handy for proving L'Hôpital's Rule. Note also that if $g(x) = x$, we get the usual MVT.)

How to prove this theorem? Its overall structure reminds us of Rolle's Theorem, which states:

> If f is continuous on $[a, b]$ and differentiable on (a, b), then $f'(c) = 0$ for some $c \in (a, b)$.

Just as in the theorem to be proved, here we assume continuity and differentiability on some interval, and deduce the existence of a value in that interval with a certain property.

We can find a proof of the Cauchy Mean Value Theorem by trying to make it look more like Rolle's Theorem. (This is the same proof-finding strategy, but in reverse; in the previous example, we made what we knew look like what we wanted, while here we are making what we want look like what we know.)

$$\exists c \in (a, b) \colon f'(c) = 0 \qquad \text{(Rolle)}$$
$$\exists c \in (a, b) \colon f'(c)(g(b) - g(a)) = g'(c)(f(b) - f(a)) \qquad \text{(Cauchy MVT)}$$

First, let's rename the function that appears in Rolle's Theorem; there's no reason it has to be the same f as in the Cauchy MVT.

$$\exists c \in (a, b) \colon \varphi'(c) = 0 \qquad \text{(Rolle)}$$
$$\exists c \in (a, b) \colon f'(c)(g(b) - g(a)) = g'(c)(f(b) - f(a)) \qquad \text{(Cauchy MVT)}$$

Rolle concludes that something is zero; rewrite Cauchy MVT in that form:

$$\exists c \in (a,b)\colon \varphi'(c) = 0 \qquad \text{(Rolle)}$$
$$\exists c \in (a,b)\colon f'(c)(g(b)-g(a)) - g'(c)(f(b)-f(a)) = 0 \qquad \text{(Cauchy MVT)}$$

If only we could find a function φ such that

$$\varphi'(c) = f'(c)(g(b)-g(a)) - g'(c)(f(b)-f(a))\,.$$

Well, that's not too hard. We can just take

$$\varphi(x) = f(x)(g(b)-g(a)) - g(x)(f(b)-f(a))\,.$$

(Note that $g(b)-g(a)$ and $f(b)-f(a)$ are constants.)

With this definition, the conclusion of Rolle's Theorem is equivalent to what we wish to prove. So all we need to do is show that the hypotheses of Rolle's Theorem hold; as it happens, they do.

The resulting proof:

Suppose f and g are continuous on $[a,b]$ and differentiable on (a,b). Define a function φ on $[a,b]$ by

$$\varphi(x) = f(x)(g(b)-g(a)) - g(x)(f(b)-f(a))\,.$$

Then φ is continuous on $[a,b]$ (since f and g are), and differentiable on (a,b) (since f and g are), and

$$\begin{aligned}\varphi(a) &= f(a)(g(b)-g(a)) - g(a)(f(b)-f(a)) \\ &= f(a)g(b) - g(a)f(b) \\ &= f(b)(g(b)-g(a)) - g(b)(f(b)-f(a)) \\ &= \varphi(b)\end{aligned}$$

So φ satisfies the hypotheses of Rolle's Theorem; thus for some $c \in (a,b)$ we have

$$0 = \varphi'(c) = f'(c)(g(b)-g(a)) - g'(c)(f(b)-f(a))\,,$$

that is,

$$f'(c)(g(b)-g(a)) = g'(c)(f(b)-f(a))\,,$$

QED.

Incidentally, the algebra to show that $\varphi(a) = \varphi(b)$ can also be written in terms of determinants:

$$\begin{aligned}
\varphi(a) &= \begin{vmatrix} f(a) & g(a) \\ f(b)-f(a) & g(b)-g(a) \end{vmatrix} \\
&= \begin{vmatrix} f(a) & g(a) \\ f(b) & g(b) \end{vmatrix} && (R_2 \to R_2 + R_1) \\
&= -\begin{vmatrix} f(b) & g(b) \\ f(a) & g(a) \end{vmatrix} && (R_1 \leftrightarrow R_2) \\
&= \begin{vmatrix} f(b) & g(b) \\ -f(a) & -g(a) \end{vmatrix} && (R_2 \to -R_2) \\
&= \begin{vmatrix} f(b) & g(b) \\ f(b)-f(a) & g(b)-g(a) \end{vmatrix} && (R_2 \to R_2 + R_1) \\
&= \varphi(b)
\end{aligned}$$

4 Series

A few sessions ago we considered the geometric series

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}\,.$$

Replacing x with $-x$, we obtain

$$1 - x + x^2 - x^3 + \cdots = \frac{1}{1+x}\,.$$

Integrating both sides, we obtain

$$x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \tfrac{1}{4}x^4 + \cdots = \ln|1+x|\,.$$

(Well, we do need a constant of integration; maybe these antiderivatives differ by a constant. But by taking $x = 0$, we see that both sides are zero; so the constant is zero.) Now take $x = 1$ to obtain

$$1 - \tfrac{1}{2} + \tfrac{1}{3} - \tfrac{1}{4} + \cdots = \ln 2\,,$$

a famous result. Replacing x with $-x^2$ at the beginning instead yields

$$1 - \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{7} + \cdots = \tfrac{\pi}{4}\,,$$

another famous result. (What if we replace x with $-x^3$? A cute puzzle: what's the next number in the sequence $\ln 2, \frac{\pi}{4}, \ldots$?)

These derivations seem a little dubious. For one thing, the original formula for the geometric series is only valid when $-1 < x < 1$; otherwise the left-hand side diverges. But then later we apply a derived formula to one of the

endpoints; it turns out it's okay here, but it does need proof. For another, when we integrate the series term by term and say that's the same as integrating the closed form, we're really saying that

$$\sum_{n=0}^{\infty} \left(\int (-x)^n \, dx \right) = \int \left(\sum_{n=0}^{\infty} (-x)^n \right) dx \, .$$

It's not at all clear that we can swap $\sum$ and $\int$ like this. Well, if the sum is finite we can, but this sum is infinite, so it's really a limit of partial sums; and the integral is a limit of Riemann sums. Alas, we cannot always swap limits. (There's a great example of this on Timothy Gowers's website: http://www.dpmms.cam.ac.uk/~wtg10/justdoit.html. He effortlessly constructs an example in which swapping limits changes the result.)

Dubious or not, these derivations are pretty cool.

5 Upper bounds on the integers

Last session, I asked whether it was possible to embed $\mathbb{Z}$ in a larger structure such that $\mathbb{Z}$ would then be bounded above. More precisely: does there exist an ordered ring with a subring that is isomorphic to $\mathbb{Z}$ and bounded above?

(If we happen to construct a ring where the subring is not "really" $\mathbb{Z}$, just isomorphic to $\mathbb{Z}$, then naturally we will want the isomorphism to preserve both arithmetic and order.)

It turns out that there are such rings. One way to find one is to just add an upper bound to $\mathbb{Z}$, and see what the ring axioms then force you to do. One hopes to get enough information about what the ring has to look like to figure out what it is (or, if it's not a familiar ring, enough information that one can craft a definition of it).

So, let's call our upper bound "∞". (Just a name, but suggestive of its intended role.) Our ring contains at least

$$\begin{array}{ccccccccccc} \ldots & & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \ldots \\ & & & & & \infty & & & & \end{array}$$

What else do we need? Well, the ring must be closed under addition, so we will need $\infty + 1$ and $\infty + 2$ and so on. Now, under the usual conception of ∞ (if there is such a thing), we might think that $\infty + 1 = \infty$. But we cannot do this and keep the ring structure. For since rings contain additive inverses, we can cancel by subtracting; that is, $\infty + 1 = \infty$ would entail that $1 = 0$, which is no good. So we'll have to have $\infty + 1 \neq \infty$. In fact, by the order axioms, we'll need $\infty + 1 > \infty$, because $1 > 0$. So:

$$\begin{array}{ccccccccc} \ldots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \ldots \\ \ldots & \infty - 3 & \infty - 2 & \infty - 1 & \infty & \infty + 1 & \infty + 2 & \infty + 3 & \ldots \end{array}$$

In previous notes, we observed that if $0 < x$ then $-x < 0$; since ∞ is supposed to be an upper bound for the integers, in particular we'll have $0 < \infty$, and so $-\infty < 0$. This, and closure under addition again, mean we have to have

$$\begin{array}{cccccccc} \ldots & -\infty-3 & -\infty-2 & -\infty-1 & -\infty & -\infty+1 & -\infty+2 & -\infty+3 & \ldots \\ \ldots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & \ldots \\ \ldots & \infty-3 & \infty-2 & \infty-1 & \infty & \infty+1 & \infty+2 & \infty+3 & \ldots \end{array}$$

What else? Well, we need closure under multiplication too; in particular, we'll need integer multiples of ∞. (We can't have $2\infty = \infty$, because then subtracting ∞ from both sides yields $\infty = 0$, which is no good.)

$$\begin{array}{cccccc} \ldots & -2\infty-2 & -2\infty-1 & -2\infty & -2\infty+1 & -2\infty+2 & \ldots \\ \ldots & -\infty-2 & -\infty-1 & -\infty & -\infty+1 & -\infty+2 & \ldots \\ \ldots & -2 & -1 & 0 & 1 & 2 & \ldots \\ \ldots & \infty-2 & \infty-1 & \infty & \infty+1 & \infty+2 & \ldots \\ \ldots & 2\infty-2 & 2\infty-1 & 2\infty & 2\infty+1 & 2\infty+2 & \ldots \end{array}$$

By closure under multiplication again, we need ∞^2, which also cannot be the same as ∞. Recall that one consequence of order is that if $0 < x$ then multiplying an inequality by x preserves its sense (i.e., does not reverse it). So: since ∞ is an upper bound for the integers, we have $1 < \infty$. Multiplying by ∞ (which is okay because $0 < \infty$) yields $\infty < \infty^2$, whence $\infty \neq \infty^2$.

After a while, it begins to look like our ring will consist of things like

$$a_0 + a_1\infty + a_2\infty^2 + \cdots + a_n\infty^n ,$$

where the a_i are integers. Look familiar? These are just polynomials in ∞.

So, how about $\mathbb{Z}[x]$, the ring of polynomials with integer coefficients? It's a ring; it contains $\mathbb{Z}$ as a subring; as a bonus, it has unity, commutativity, and even unique factorization. Can it be ordered? Replacing ∞ with x above, we see that we want an order $\sqsubseteq$ such that, for example,

$$0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \cdots \sqsubseteq x-1 \sqsubseteq x \sqsubseteq x+1 \sqsubseteq \cdots \sqsubseteq x^2-1 \sqsubseteq x^2 \sqsubseteq x^2+1 \sqsubseteq \cdots$$

There's a couple ways to define the order that's implied here. One way is to think of these polynomials as functions, and note that we want $p \sqsubseteq q$ if and only if, er, $p(\infty) \leq q(\infty)$, that is, p is smaller than q "at infinity". What does that mean? The usual rewrite-to-eliminate-"infinity" maneuver yields the statement "$p(x) \leq q(x)$ for sufficiently large x", which we could express as

$$p \sqsubseteq q \iff \lim_{x\to\infty} (p(x) - q(x)) \leq 0$$

(For the (typical) case where the limit is infinite, we define $-\infty < 0 < +\infty$.)

Everything so far is investigation, that is, it's all stuff you'd do on scrap paper before writing your solution. The solution would consist of a proof that

$\mathbb{Z}[x]$ is in fact an ordered ring under this relation $\sqsubseteq$, and that its subring $\mathbb{Z}$ is bounded above under that order. So we need to prove the order axioms:

1. $\forall p\colon p \sqsubseteq p$. (Reflexivity.)
2. $\forall p, q\colon$ either $p \sqsubseteq q$ or $q \sqsubseteq p$. (Totality?)
3. $\forall p, q\colon p \sqsubseteq q$ and $q \sqsubseteq p \implies p = q$. (Antisymmetry.)
4. $\forall p, q, r\colon p \sqsubseteq q$ and $q \sqsubseteq r \implies p \sqsubseteq r$. (Transitivity.)
5. $\forall p, q, r\colon p \sqsubseteq q \implies p + r \sqsubseteq q + r$. (Compatibility with $+$.)
6. $\forall p, q\colon 0 \sqsubseteq p$ and $0 \sqsubseteq q \implies 0 \sqsubseteq pq$. (Compatibility with $\cdot$.)

I leave these proofs as exercises; they're mostly straightforward. You'll need the fact that, as $x \to \infty$, a polynomial either tends to a finite value, increases without bound, or decreases without bound. (For example, a polynomial can't fail to have a limit by oscillation, as the sine function does.) You'll also need the fact that the only way for the limit to be finite is if the polynomial is constant.

(It's also instructive to find out how this relation $\sqsubseteq$ fails to order the field of rational functions of x, for example.)

The technique used here is of fairly wide applicability. It can be used to define $\mathbb{C}$, for example: imagine that all you know is $\mathbb{R}$, and you wonder whether you can make a larger field in which -1 has a square root. Call that square root i, and see what you are forced to do by the field axioms.

It can also be used to solve the following problem: show that every ring is a subring of a ring with unity. (That is, given a ring A, construct a ring with unity that contains a subring isomorphic to A.)

Another neat thing about the particular example considered here is that it could be used to treat infinity in a rigorous way. We replaced ∞ with x because we're familiar with polynomials, but we don't have to. We could do all of our arithmetic with ∞, and talk about a hierarchy of infinities in which $\infty < \infty + 1 < 2\infty < \infty^2$ and so on, all the while using "naïve" arithmetic (i.e., the arithmetic of an ordered ring). If someone challenges what we're doing, say, complaining that ∞ isn't a number and so it's not legitimate to do arithmetic with it, we can explain that we're not "really" talking about infinity the number, we're talking about infinite functions, that is, functions whose values increase or decrease without bound under a certain limiting process.

I have seen and heard hints here and there that a similar thing can be done with "infinitesimals", understood intuitively as infinitely small quantities, sometimes treated as zero (except that you can divide by them, because they're not really zero, just infinitely small), and understood formally as functions that tend to zero under some limiting process. In fact, I think there's a way to develop all of calculus from this point of view.