MthSc 453

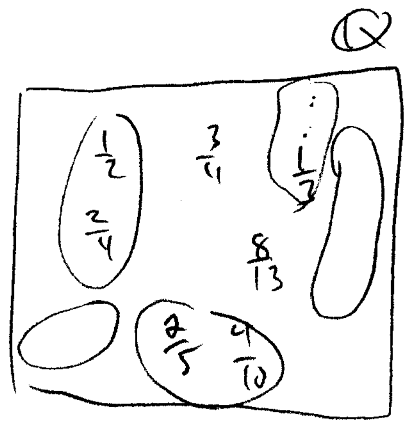
Lecture 2: Properties of $\mathbb{Q}$.

Recall that $\mathbb{Q} = \{ \frac{p}{q} : q \neq 0 \}$ where $\frac{p}{q}$ = equiv. class of pairs (p,q) s.t.

$(p,q) \sim (m,n)$ if $pn = qm$ and $qn \neq 0$.

Ex: $\frac{1}{2} = \{ (1,2), (2,4), (3,6), \dots \} = \frac{2}{4} = \frac{3}{6} = \dots$

Next goal: Define arithmetic structure on $\mathbb{Q}$.



- **Addition:**

Try this: $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$.

This is a bit odd, but can we do this?

Let's see:

$$\frac{1}{2} + \frac{1}{3} = \frac{2}{5}$$

$$\frac{2}{4} + \frac{1}{3} = \frac{3}{7}$$

not equivalent

equiv.

Problem: This definition *depends* on the choice of representative from the class. We say that this definition fails to be **well-defined**. (Important!)

Ex: Birthdays. (How many days until your next b-day).

Requirement: Our defn of + must be well-defined, ie, does not depend on the representatives chosen.

Try 2: $\frac{a}{b} + \frac{c}{d} = \frac{0}{1}$.

Is this well-defined? Yes! But it's meaningless.

Def: (Actual one): $\boxed{\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}}$

To show well-defined, must show

If $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then

$$(ad+bc,\ bd) \sim (a'd'+b'c',\ b'd'). \quad [HW].$$

- Multiplication: $\boxed{\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}}$. Check well-defined. [HW]

Question: In what sense does $\mathbb{Q}$ extend $\mathbb{Z}$?

Ans: Check that $\{\frac{n}{1} : n \in \mathbb{Z}\}$ "behaves" like $\mathbb{Z}$. "isomorphic!"

$$\mathbb{Z} \longrightarrow \mathbb{Q}, \quad n \longmapsto \frac{n}{1}$$

+ & $\times$ is respected, i.e., $n+m \longmapsto \frac{n+m}{1} = \frac{n}{1} + \frac{m}{1}$ Same for $\times$.

Also, $\mathbb{Z}$ has a natural order.

First what's an "order"?

Def: An order on a set S (called an ordered set) is a relation $<$ satisfying:

(1) (trichotomy) If $x, y \in S$, exactly one of these is true:

$$x<y, \quad x=y, \quad y<x;$$

(2) (transitivity) If $x, y, z \in S$ and $x<y<z$, then $x<z$.

Remark: If we drop the exactly requirement, we get a partial order.

Ex: In $\mathbb{Z}$, say $m<n$ if $n-m$ is positive, i.e, in the set $\{1,2,3\ldots\}$.

Ex: In $\mathbb{Z}\times\mathbb{Z}$, say $(a,b)<(c,d)$ if

$a<c$ or $a=c$ and $b<d$ (dictionary, or lexicographical order).

Ex: In $\mathbb{Q}$, say $\frac{m}{n}$ is positive if $nm>0$.

Must check: This is well-defined. (exercise)

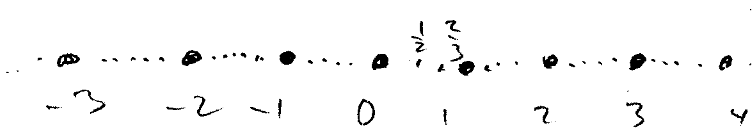
Now, say $\frac{m}{n} < \frac{m'}{n'}$ if $\frac{m'}{n'} - \frac{m}{n}$ is positive.

Notation: • Write "$y>x$" for $x<y$.

• Write $x \le y$ for $x<y$ or $x=y$.

Remark: Define $\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + \frac{-1}{1}\cdot\frac{c}{d} = \frac{ad-bc}{bd}$

We have now turned $\mathbb{Q}$ into an ordered set.



$\mathbb{Q}$ is good enough to solve: $5x = 3$. Note: $x = \frac{3}{5}$ solves.

But not good enough to solve: $x^2 = 2$.

Theorem: $x^2 = 2$ has no solution in $\mathbb{Q}$.

Proof: (by contradiction). Assume $x^2 = 2$ has a sol'n in $\mathbb{Q}$, i.e.,

$x = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$, and p, q have no common factors.

So, $\left(\frac{p}{q}\right)^2 = 2$, hence $p^2 = 2q^2$

Then p^2 is even (divisible by 2), so p is even too.

So $p = 2m$, for some $m \in \mathbb{Z}$. hence $p^2 = 4m^2$ and $4m^2 = 2q^2$

Thus $2m^2 = q^2$, so q^2 is even $\Rightarrow$ q is even.

This contradicts that p, q have no common factors.

So $x^2 = 2$ must have no solution in $\mathbb{Q}$. $\square$

- $\mathbb{Q}$ is a field.

Def: A field is a set F with two operations $+, \times$ satisfying axioms:

(A1) F is closed under $+$: If $x, y \in F$, then $x + y \in F$.

(A2) $+$ is commutative $x + y = y + x$ $\forall x, y \in F$

(A3) $+$ is associative $(x + y) + z = x + (y + z)$ $\forall x, y, z \in F$.

(A4) F has additive identity; call it 0: $0 + x = x$ for all $x \in F$

(A5) Every element has an additive inverse: For each $x \in F$, $\exists$ $-x \in F$ s.t. $x + (-x) = 0$.

(M1) F is closed under $\times$:

(M2) $\times$ is commutative

(M3) $\times$ is associative

(M4) F has an multip. id., call it 1.

(M5) Every element except 0 has a mult. inverse.

(D) $\times$ distributes over $+$: $x(y+z) = xy + xz \quad \forall x,y,z \in F$.

In $\mathbb{Q}$: 0 element is $\frac{0}{1}$.

1 element is $\frac{1}{1}$.

Check these axioms hold.

Remark: • $\mathbb{Z}$ is not a field because it does not satisfy M5.

• $\mathbb{Q}$ is an ordered field: A field with an order, so that order is "preserved" by the field ops, i.e.,

① $y < z \Rightarrow x + y < x + z$

different, but equiv. in Rudin. ② $y < z,\ x > 0 \Rightarrow xy < xz$.

Next goal: Construct the real numbers, $\mathbb{R}$.

They'll extend the rationals, $\mathbb{Q}$, and

complete ordered field. → fill in "holes" in number line.