Review: relations

A binary relation on a set A is a subset $R \subseteq A \times A$, where elements (a, b) are written as $a \sim b$.

Example: $A = \mathbb{Z}$ and $R = \{a \sim b \mid a \equiv b \pmod{n}\}$.

A binary relation on a set A is...

(R) reflexive if $a \sim a$ for all $a \in A$;

(S) symmetric if $a \sim b$ implies $b \sim a$;

(T) transitive if $a \sim b$ and $b \sim c$ implies $a \sim c$, i.e.

$$(a \sim b \wedge b \sim c) \Rightarrow a \sim c$$

An equivalence relation on a set A is a binary relation that is reflexive, symmetric, *and* transitive.

Review: set theoretic definition of the numbers.

Natural numbers:

Let $0 = \varnothing$.

Given n, define the successor to n as $S(n) = n \cup \{n\}$.

(By "successor to n" we basically mean $n + 1$.)

Let $\mathbb{Z}_{\geqslant 0}$ be the set of all sets generated by 0 and S.

Integers:

Define $\mathbb{Z}$ by formally letting

$$-\mathbb{Z}_{\geqslant 0} = \{-n \mid n \in \mathbb{Z}_{\geqslant 0}\}, \quad \text{where } -0 = 0;$$

and $\mathbb{Z} = \mathbb{Z}_{\geqslant 0} \cup -\mathbb{Z}_{\geqslant 0}$. Extend $S : \mathbb{Z} \to \mathbb{Z}$ by defining $S(-a)$ for any $-a \in -\mathbb{N} - \{0\}$ as

$$S(-a) = -b, \quad \text{where } S(b) = a.$$

Some operations:

- Define $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$, by

$$a + 0 = a \qquad \text{and} \qquad a + S(b) = S(a + b).$$

- Define $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$,

$$n \cdot 0 = 0 \quad \text{and} \quad a \cdot S(b) = (a \cdot b) + a.$$

Review:

Some properties of $+$ and $\cdot$ (we present without proof):

1. Addition and multiplication satisfy commutativity, associativity, and distributivity.
2. We still have $a + 0 = a = 0 + a$ (additive identity) and $a \cdot 1 = a = 1 \cdot a$ (multiplicative identity) for all $a \in \mathbb{Z}$.
3. We also have $a + (-a) = 0$ (prove). (additive inverses)

We call any number system that has an addition and multiplication that satisfy all these properties a (commutative) ring.

Order: For $a, b \in \mathbb{Z}$, we say $a \leqslant b$ if $b = S(S(\cdots S(a)\cdots))$.

Properties of order (we present without proof):

(i) For all $a, b \in \mathbb{N}$, we have $a \leqslant b$ or $b \leqslant a$.

(ii) If $a \leqslant b$ and $b \leqslant a$, then $a = b$.

(iii) If $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.

(iv) If $a \leqslant b$ then $a + c \leqslant b + c$.

(v) If $a \leqslant b$ then $a \cdot c \leqslant b \cdot c$.

Rational numbers

Let

$$Q = \mathbb{Z} \times (\mathbb{Z} - \{0\}),$$

and define an equivalence relation on Q by

$$(a, b) \sim (x \cdot a, x \cdot b) \quad \text{for all} \quad x \in \mathbb{Z} - \{0\}.$$

Under this equivalence relation, write

$$\frac{a}{b} = [(a, b)].$$

Then rational numbers are

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

(Note that we get lazy, and write $\frac{a}{1} = a$.)

Define $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ and $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \qquad \text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Let $Q = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ and define an equivalence relation on Q by

$$(a, b) \sim (x \cdot a, x \cdot b) \quad \text{for all} \quad x \in \mathbb{Z} - \{0\}.$$

Under this equivalence relation, write $\frac{a}{b} = [(a, b)]$ (writing $\frac{a}{1} = a$). Then rational numbers are

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Define $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ and $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \qquad \text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Again...

1. Addition and multiplication still satisfy commutativity, associativity, and distributivity.
2. We still have $x + 0 = x$ (additive identity) and $x \cdot 1 = x$ (multiplicative identity) for all $x \in \mathbb{Q}$.
3. We also have that $x + (-x) = 0$. (additive inverses)

So $\mathbb{Q}$ is also a (commutative) ring.
In addition, for all $a/b \in \mathbb{Q}$ with $a \neq 0$,

$$\frac{a}{b} \cdot \frac{b}{a} = 1 \quad \text{(multiplicative inverses)}.$$

This makes $\mathbb{Q}$ a field (again, modern algebra).

Order on $\mathbb{Q}$

Define $-\frac{a}{b} = \frac{-a}{b}$ (you can show $\frac{-a}{b} = \frac{a}{-b}$).

We define $\leqslant$ on $\mathbb{Q}$ by the following: for $a, b, c, d \in \mathbb{N}$, we have

1. $\frac{a}{b} \leqslant \frac{c}{d}$ whenever $a \cdot d \leqslant b \cdot c$;
2. $-\frac{a}{b} \leqslant \frac{c}{d}$; and
3. $-\frac{a}{b} \leqslant -\frac{c}{d}$ whenever $\frac{c}{d} \leqslant \frac{a}{b}$.

Then, again,

(i) For all $a, b \in \mathbb{N}$, we have $a \leqslant b$ or $b \leqslant a$.
(ii) If $a \leqslant b$ and $b \leqslant a$, then $a = b$.
(iii) If $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.
(iv) If $a \leqslant b$ then $a + c \leqslant b + c$.
(v) If $a \leqslant b$ and $0 \leqslant c$, then $ac \leqslant bc$.

This makes $\mathbb{Q}$ into an ordered field.

Let X be an ordered set of numbers (think $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and, eventually, $\mathbb{R}$), and let S be a nonempty subset of X.

(a) If S contains a largest element x ($x \in S$ and for all $y \in S$, $y \leqslant x$), then we call $x = \max(S)$ the maximum if S.

Careful writing note: Compare to, "The *maximum* of S is an element $x \in S$ satisfying $y \leqslant x$ for all $y \in S$. What's wrong ?

(b) If S contains a smallest element x ($x \in S$ and for all $y \in S$, $y \geqslant x$), then we call $x = \min(S)$ the minimum of S.

Ex: If $S = \{-2, 1/2, 100/3\}$, then $\min(S) = -2$, $\max(S) = 100/3$.

Ex: If $S \subseteq \mathbb{Z}_{\geqslant 0}$ is finite, then

$$\max(S) = \bigcup_{s \in S} s \quad \text{and} \quad \min(S) = \bigcap_{s \in S} s.$$

Ex: If S is finite, then $\max(S)$ and $\min(S)$ exist.

Ex: For $S = \mathbb{Z}_{>0}$, $\min(S) = 1$ and $\max(S)$ does not exist.

Ex: For $S = \mathbb{Q}_{>0}$, $\min(S)$ and $\max(S)$ do not exist.

Note: Min/max don't depend on the set X!

Let X be an ordered set of numbers (think $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and, eventually, $\mathbb{R}$), and let S be a nonempty subset of X.

(a) If there exists $u \in X$ such that $s \leqslant u$ for all $s \in S$, then u is called an upper bound of S and the set S is said to be bounded above (by u).

Ex: $S = \mathbb{Q}_{<0} \subseteq \mathbb{Q}$ doesn't have a maximal element, but it *does* have an upper bound: $u = 0$. In fact, it has *lots* of upper bounds: $u = 1$, $u = 100$, $u = 101/15$, etc. But $u = -1$ is not an upper bound since $-1/2 \in S$ and $-1/2 > -1$.

Ex: $S = \mathbb{Q}_{>0} \subseteq \mathbb{Q}$ doesn't have any upper bounds.

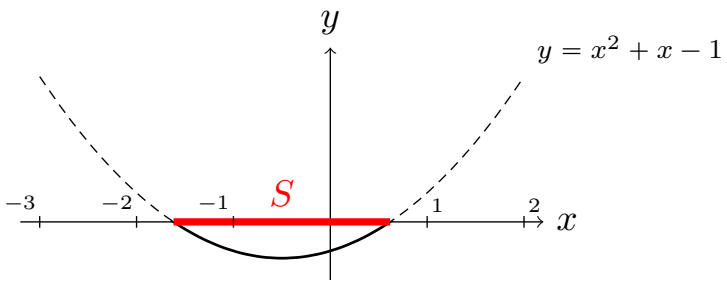
Ex: As a subset of $X = \mathbb{Q}_{>0}$, $S = \mathbb{Q}_{>0}$ doesn't have an upper bound.

(b) Similarly, if there exists $\ell \in X$ such that $s \geqslant \ell$ for all $s \in S$, then ℓ is called a lower bound of S and the set S is said to be bounded below (by ℓ).

Note: Upper and lower bounds *do* depend on the set X.

Consider $X = \mathbb{Q}$ and

$$S = \{x \in \mathbb{Q} \mid x^2 + x - 1 \leqslant 0\}$$



Math Oracle: *"We can compute*

$$x^2 + x - 1 = 0 \quad \Leftrightarrow \quad x = \frac{1}{2}(-1 \pm \sqrt{5}) \notin \mathbb{Q}.$$

So S doesn't have a minimum or a maximum."

But S *is* bounded above and below,

e.g. $u = 1$ and $\ell = -2$; or $u = .62$ and $\ell = -1.62$; or...

But what is the "best" bound? Does it even have a "best" bound?

Oracle: *"In $\mathbb{R}$, the 'best' bounds are*

$$\ell = \tfrac{1}{2}(-1 - \sqrt{5}) \quad \textit{and} \quad u = \tfrac{1}{2}(-1 + \sqrt{5})."$$

Let X be an ordered set of numbers (think $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and, eventually, $\mathbb{R}$), and let S be a nonempty subset of X.

From before: If there exists $u \in X$ such that $s \leqslant u$ for all $s \in S$, then u is called an upper bound of S and the set S is said to be bounded above (by u). Similarly, a lower bound is a number $\ell \in X$ such that $s \geqslant \ell$ for all $s \in S$; if ℓ exists, we say S is bounded below.

(a) If S is bounded above, we call an upper bound U satisfying

$$U \leqslant u \quad \text{for all upper bounds } u$$

the least upper bound or supremum of S, denoted by $\sup S$.

$$\sup S = \min\left(\{u \in X \mid u \geqslant s \text{ for all } s \in S\}\right)$$

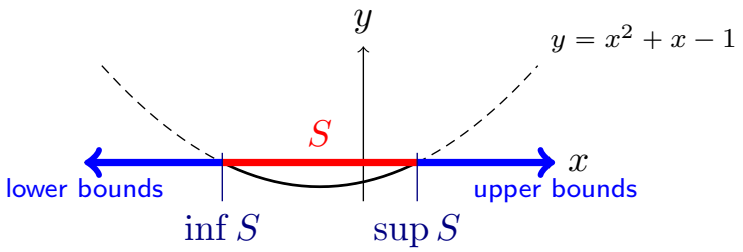
(b) If S is bounded below, we call a lower bound L satisfying

$$L \geqslant \ell \quad \text{for all lower bounds } \ell$$

the greatest lower bound or infimum of S, denoted by $\inf S$.

$$\inf S = \max\left(\{\ell \in X \mid \ell \leqslant s \text{ for all } s \in S\}\right)$$

Back to $X = \mathbb{Q}$ and $S = \{x \in \mathbb{Q} \mid x^2 + x - 1 \leqslant 0\}$.



Oracle: *"In* $\mathbb{R}$,

$$\inf S = \tfrac{1}{2}(-1 - \sqrt{5}) \quad \textit{and} \quad \sup S = \tfrac{1}{2}(-1 + \sqrt{5}).$$

Therefore, even though

$$\{\ell \in X \mid \ell \leqslant s \textit{ for all } s \in S\} \quad \textit{and} \quad \{u \in X \mid u \geqslant s \textit{ for all } s \in S\}$$

are non-empty, $\inf S$ *and* $\sup S$ *don't exist in* $\mathbb{Q}$.

Thm. The rational numbers are incomplete in the sense that there exist bounded subsets that do not have infimums or supremums.

Goal: Define the completion of $\mathbb{Q}$—the smallest set containing $\mathbb{Q}$ so that every set that's bounded above/below has a sup/inf. $(\mathbb{R})$

Completeness Axiom: Every non-empty subset of $\mathbb{R}$ that is bounded above has a least upper bound, i.e. for all $S \subseteq \mathbb{R}$, if S is bounded above, then $\sup S$ exists and is in $\mathbb{R}$.

The real numbers

Let $\mathcal{R}$ be the set of subsets of $\mathbb{Q}$ that satisfy the following:
$C \in \mathcal{R}$ whenever

1. $C \subsetneq \mathbb{Q}$ and $C \neq \varnothing$ (C is a proper, non-empty subset of $\mathbb{Q}$);
2. for all $x \in C$, if $y \in \mathbb{Q}$ satisfies $y \leqslant x$, then $y \in C$
   (if $x \in C$, then everything less than x is also in C);
3. $\max C$ does not exist.
   (Recall, in contrast to upper bounds, $\max C$ has to be an element of C.)

Oracle: *"*$\mathcal{R}$ *consists entirely of sets of the form*

$$a^* = \{x \in \mathbb{Q} \mid x < a\} = (-\infty, a) \quad \textit{for some fixed } a \in \mathbb{R}."$$

Sets in $\mathcal{R}$ are called Dedekind cuts,
and $\mathcal{R} = \mathbb{R}$ is the set of real numbers.

Intuition: identify $a \in \mathbb{R}$ with the cut $a^* = \{x \in \mathbb{Q} \mid x < a\} \in \mathcal{R}$.

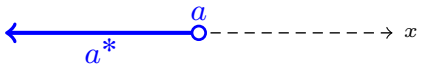
Thm. The completeness axiom holds.

(This *should* feel uncomfortable. . . an axiom shouldn't have to be proven!
Whether this is an axiom or a theorem depends on your perspective. . .)

Operations

Intuition: $\mathcal{R}$ consists entirely of sets of the form

$$a^* = \{x \in \mathbb{Q} \mid x < a\} = (-\infty, a) \quad \text{for some fixed } a \in \mathbb{R}.$$



For $\alpha, \beta \in \mathcal{R}$, define

$$\alpha + \beta = \{a + b \mid a \in \alpha, b \in \beta\}.$$

Careful: we **do not** want to define $\alpha \cdot \beta$ by $\{a \cdot b \mid a \in \alpha, b \in \beta\}$!

Example: Consider $(-1)^* \cdot (-1)^*$.

We certainly *need* this to be $1^* = \{x \in \mathbb{Q} \mid x < 1\}$.

Compare to

$$\{a \cdot b \mid a, b \in (-1)^*\}.$$

This latter set contains, for example, $(-2)(-3) = 6 \notin 1^*$.

Instead: for non-negative $\alpha, \beta \in \mathcal{R}$ (i.e. $\alpha_{\geqslant 0}, \beta_{\geqslant 0} \neq \varnothing$), define

1. $\alpha \cdot \beta = \{a \cdot b \mid a \in \alpha_{\geqslant 0}, b \in \beta_{\geqslant 0}\} \cup \mathbb{Q}_{<0}$;
2. $-\alpha = \{-x \in \mathbb{Q} \mid x > a \text{ for all } a \in \alpha\}$;
3. $-\alpha \cdot \beta = -(\alpha \cdot \beta)$; and
4. $(-\alpha) \cdot (-\beta) = \alpha \cdot \beta$.

Addition: For $\alpha, \beta \in \mathcal{R}$, define

$$\alpha + \beta = \{a + b \mid a \in \alpha, b \in \beta\}.$$

Multiplication: For non-negative $\alpha, \beta \in \mathcal{R}$ (i.e. $\alpha_{\geqslant 0}, \beta_{\geqslant 0} \neq \varnothing$), define

$$\alpha \cdot \beta = \{a \cdot b \mid a \in \alpha_{\geqslant 0}, b \in \beta_{\geqslant 0}\} \cup \mathbb{Q}_{<0};$$
$$-\alpha = \{-x \in \mathbb{Q} \mid x > a \text{ for all } a \in \alpha\};$$
$$-\alpha \cdot \beta = -(\alpha \cdot \beta); \quad \text{and} \quad (-\alpha) \cdot (-\beta) = \alpha \cdot \beta.$$

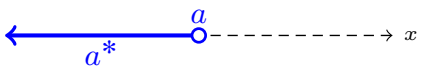
Again...

1. Addition and multiplication still satisfy commutativity, associativity, and distributivity.
2. We still have $\alpha + 0^* = x$ (additive identity) and $\alpha \cdot 1^* = \alpha$ (multiplicative identity) for all $\alpha \in \mathcal{R}$.
3. We also have that $\alpha + (-\alpha) = 0^*$. (additive inverses)
4. Dor all $\alpha \in \mathcal{R}$ with $\alpha \neq 0^*$, there exists $\alpha^{-1} \in \mathcal{R}$ that satisfies
$$\alpha \cdot \alpha^{-1} = 1^* \quad \text{(multiplicative inverses)}.$$

So $\mathcal{R}$ a field (again, modern algebra).

Intuition: $\mathcal{R}$ consists entirely of sets of the form

$$a^* = \{x \in \mathbb{Q} \mid x < a\} = (-\infty, a) \quad \text{for some fixed } a \in \mathbb{R}.$$



For all $a \in \mathbb{Q}$, we can concretely identify a with $a^* = \{x \in \mathbb{Q} \mid x < a\} \in \mathcal{R}$. Namely,

$$\mathbb{Q} \to \mathcal{R} \quad \text{defined by} \quad a \mapsto a^*$$

is an injective map, which will respect addition, multiplication, and order (once we define them).

Comparisons:

For $\alpha, \beta \in \mathcal{R}$, define

$$\alpha \leqslant \beta \quad \text{whenever} \quad \alpha \subseteq \beta.$$

Thm. (Archimedean property) If $a^*, b^* > 0^*$, then there exists $n \in \mathbb{N}$ such that $a^* \cdot n^* > b^*$.

Thm. (Denseness of $\mathbb{Q}$) If $a^* < b^*$, then there exists $c \in \mathbb{Q}$ such that $a^* < c^* < b^*$.

Wrapping up

1. **Context is king!**
   You can do most math at any level of abstraction.
   For example, there's a huge difference between what you can assume when working in set theory versus calculus.
2. **Go slowly when reading/writing new math.**
   Pay attention to details! For example, the simple inversion of quantifiers can mess a whole statement up.
3. **Always do examples!**
   Illustrative examples can help you understand the big picture; extreme examples help you understand the details. And if you don't know where to start, then do an example!
4. **Revise, revise, revise.**
   When solving math problems, a lot goes on behind the scenes. Don't be afraid to write down logical fallacies (like starting with the conclusion, or "proof by example") in the privacy of your own home. Just don't *stop* there!
   Tip: Keep old ideas or notes to yourself in your .tex file, commented out with %'s, in case you need them again later.
5. **Math isn't linear; math is fractal.**
   While a logical argument needs to come in a logical order, there isn't just one good order to explain all of math. In particular, every good answer spins off many good questions!
6. **You can do it!!**
   Be kind to yourself! If you don't get something right away, that doesn't mean you're stupid, or that you can't get there. Math is hard, but doable; and the struggle is what makes the breakthroughs so fun!