Math 141: Lecture 3

Constructing the reals, cardinality questions

Bob Hough

September 7, 2016

The field with 4 elements

Field: A set with 0, 1, and operations $+, -, \times, \div$ such that $+, \times$ are commutative, associative and $\times$ distributes over $+$.

Let F be a field with 4 elements.

- Two of them are $0, 1$.
- Let $n \geq 2$ be the least number of times 1 must be added to itself to reach 0.
- n must divide the size of the field, since the field splits into sets of the form $\{x, x+1, ..., x+n-1\}$ which are disjoint. Hence $n = 2$ or $n = 4$.

If $n = 4$ then $F = \{0, 1, 2, 3\}$, but this forces $2 \times 2 = 0$, whence $2 = 2^{-1} \times 2 \times 2 = 0$, a contradiction, so $n = 2$.

The field with 4 elements

Call the two remaining elements of the field x and $x+1$. We've thus worked out the addition table of the field

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

The field with 4 elements

To know the multiplication table we need to know $x \times x$. Since the product of non-zero elements is non-zero we rule out $x^2 = 0$, $x^2 = 1$ (which forces $(x+1)(x-1) = (x+1)^2 = 0$) and $x^2 = x$ (which forces $(x-1)x = (x+1)x = 0$). Hence $x^2 = x+1$, so $x(x+1) = x^2 - x = -1 = 1$. The multiplication table becomes

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

The field with 4 elements

From the addition and multiplication table, one could directly verify that F is an example of a field.

An alternative route:

- Let F_2 be the field with 2 elements, and verify that $F_2[x]$, that is, polynomials with F_2 coefficients, is a ring.
- $F_4 = F_2[x]/(x^2 + x + 1)$ is the ring which one obtains by setting multiples of $x^2 + x + 1$ equal to 0 in $F_2[x]$.
- The ring properties of F_4 follow from those of $F_2[x]$, and the multiplication table guarantees that multiplicative inverses exist, so F_4 is a field.

Finite fields

- For every prime p and for every $n \geq 1$ there is exactly one field with p^n elements.
- These are all of the finite fields.
- This fact is often proven in advanced undergraduate algebra courses.

Properties of the reals

Last lecture we introduced the reals $\mathbb{R}$ as an ordered field containing the rationals, and satisfying the least upper bound property. Let's briefly recall what this means:

- Field: A set with 0, 1, and operations $+, -, \times, \div$ such that $+, \times$ are commutative, associative and $\times$ distributes over $+$
- Ordered: There exists a set P of positive elements such that $0 \notin P$, but for all $x \neq 0$, x or $-x$ is in P. If $x, y \in P$ then $x + y$ and xy are in P.
- The least upper bound property: Any set which is non-empty and bounded above has a least upper bound.

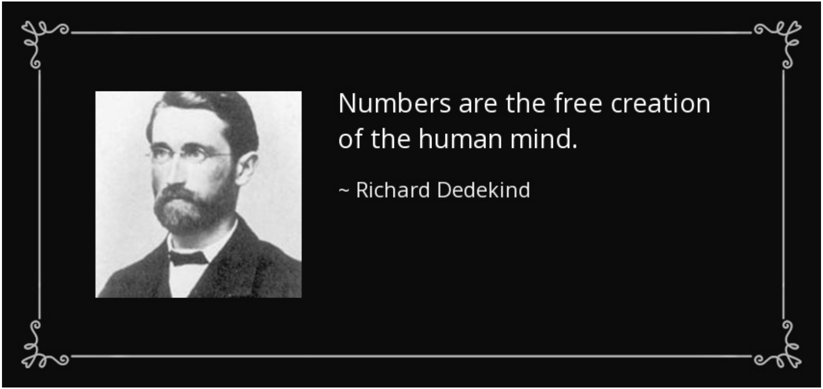
Properties of the reals

Last lecture we verified that $x^2 = 2$ does not have a solution in $\mathbb{Q}$. We also checked that in $\mathbb{R}$, if

$$S = \{y \in \mathbb{R} : 0 < y, y^2 < 2\}$$

then $x = \sup S$ satisfies $x^2 = 2$. Hence $\mathbb{Q} \neq \mathbb{R}$ and $\mathbb{Q}$ does not satisfy the least upper bound property.

Dedekind cuts



(Source: AZ quotes)

Dedekind cuts

A *Dedekind cut* is a subset $\alpha \subset \mathbb{Q}$ satisfying

1. $\alpha \neq \emptyset$ and $\alpha \neq \mathbb{Q}$
2. If $p \in \alpha$ and $q \in \mathbb{Q}$ and $q < p$ then $q \in \alpha$
3. If $p \in \alpha$, then $p < r$ for some $r \in \alpha$.

As a set, $\mathbb{R}$ consists of the set of cuts of $\mathbb{Q}$.
Define $\alpha < \beta$ if $\alpha \subset \beta$ but $\alpha \neq \beta$.

Dedekind cuts

$\mathbb{Q}$ is identified as a subset of $\mathbb{R}$ by identifying $q \in \mathbb{Q}$ with

$$q^* = \{p \in \mathbb{Q} : p < q\}.$$

The additive and multiplicative identities are 0^* and 1^*.

Dedekind cuts

Addition is defined as set addition:

$$\alpha + \beta = \{x + y : x \in \alpha, y \in \beta\}.$$

The additive inverse is

$$-\alpha = \{p \in \mathbb{Q} : \exists r \in \mathbb{Q}, r > 0, -p - r \notin \alpha\}$$

In words, $p \in -\alpha$ if there is a rational $q > p$ with $-q \notin \alpha$.

Dedekind cuts

If $\alpha, \beta > 0$ then

$$\alpha \times \beta = \{p \times q : p, q > 0, p \in \alpha, q \in \beta\} \cup \{x \in \mathbb{Q} : x \leq 0\}.$$

Multiplication is extended by the usual rules $(-\alpha) \times \beta = (\alpha) \times (-\beta) = -(\alpha \times \beta)$, $(-\alpha) \times (-\beta) = \alpha \times \beta$, and $0^* \times \alpha = \alpha \times 0^* = 0^*$.

Dedekind cuts

There is some work to do to verify that these constructions are well defined and make $\mathbb{R}$ an ordered field. For instance, it's necessary to check that $\alpha + \beta$, $\alpha \times \beta$, $-\alpha$, and q^* are all cuts, and that the constructions satisfy the field and order axioms.
In lecture we'll check that $\mathbb{R}$ satisfies the trichotomy and least upper bound properties.

Trichotomy

Theorem (Trichotomy law for $\mathbb{R}$)

Let α and β be cuts. Exactly one of $\alpha < \beta$, $\alpha = \beta$ or $\alpha > \beta$ is true.

Proof.

We need to show that at least one of these is true, since at most one is true by the definition of subset.

- Suppose $\alpha \not< \beta$ and $\alpha \neq \beta$. Then $\alpha \not\subset \beta$ so choose $q \in \alpha \setminus \beta$.
- Let $r \in \beta$. Then $r \neq q$ and $r \not> q$ or else q would be a member of β, so $r < q$.
- Hence $r \in \alpha$ so $\beta \subset \alpha$ and $\beta \neq \alpha$, thus $\beta < \alpha$.

$\square$

The l.u.b. property

Theorem (The l.u.b. property of $\mathbb{R}$)

Let $S \subset \mathbb{R}$ be a non-empty set of cuts, and suppose that there is $\alpha \in \mathbb{R}$ which is an upper bound for S. Then there is $s \in \mathbb{R}$ with

$$s = \sup S.$$

Recall what these definitions mean.

1. α is an upper bound for S means, for each $\beta \in S$, $\beta \leq \alpha$.
2. $s = \sup S$ means that s is an upper bound for S, and if α is any upper bound for S then $s \leq \alpha$.

The l.u.b. property

Proof of the l.u.b. property of $\mathbb{R}$.

Define $s = \bigcup_{\beta \in S} \beta$. We first check that s is a cut and $s \leq \alpha$.

1. Choose $\beta \in S$. Then $\beta \subset s$, so s is non-empty. Let $x \in s$. Then there is $\beta \in S$ such that $x \in \beta$, and since $\beta \leq \alpha$, $x \in \alpha$. Thus $s \subset \alpha$ so $s \neq \mathbb{Q}$.
2. Let $p \in s$ and let $q \in \mathbb{Q}$ with $q < p$. Choose $\beta \in S$ such that $p \in \beta$. Then $q \in \beta$ so $q \in s$.
3. Let $p \in s$ and choose $\beta \in S$ such that $p \in \beta$. Then there is $r > p$ with $r \in \beta$. Hence $r \in s$ satisfies $r > p$.

The verification above shows that s is a cut. $\square$

The l.u.b. property

Proof of the l.u.b. property of $\mathbb{R}$.

Recall $s = \bigcup_{\beta \in S} \beta$. Note that this implies, for all $\beta \in S$, $\beta \le s$, so s is an upper bound for S.

It remains to check that s is the least upper bound for S. Let α be an upper bound for S. For each $\beta \in S$, $\beta \subset \alpha$. Hence $s = \bigcup_{\beta \in S} \beta \subset \alpha$ which proves $s \le \alpha$. $\square$

Binary representation of real numbers

Let $x \in \mathbb{R}$, $0 < x \leq 1$. The binary decimal representation of x is a sequence $a_1, a_2, a_3, \ldots$, where each $a_i \in \{0, 1\}$, and represented as $x = 0.a_1 a_2 a_3 a_4 \ldots$. The a_i are defined as follows.
Define $a_1 = 1$ if $1 \in 2x$, otherwise $a_1 = 0$. In general, define recursively

$$x_0 = x$$

$$\forall i \geq 1, \qquad a_i = \begin{cases} 1 & \text{if } 1 \in 2x_{i-1} \\ 0 & \text{otherwise} \end{cases}$$

$$x_i = 2x_{i-1} - a_i.$$

Binary representation of real numbers

Recall for $0 < x \leq 1$, $x = 0.a_1 a_2 a_3 \ldots$ with

$$\begin{aligned} & x_0 = x \\ \forall i \geq 1, \qquad & a_i = \begin{cases} 1 & \text{if } 1 \in 2x_{i-1} \\ 0 & \text{otherwise} \end{cases} \\ & x_i = 2x_{i-1} - a_i. \end{aligned}$$

Examples:

$$\frac{1}{2} = 0.0111111111111111\ldots$$
$$\frac{1}{3} = 0.0101010101010101\ldots$$

This construction chooses non-terminating expansions.

Binary representation of real numbers

Theorem

Let x and y be real numbers satisfying $0 < x \leq y \leq 1$. The binary representations of x and y are equal if and only if $x = y$.

Proof.

Suppose $x < y$.

1. There exist a pair of rationals $p < q$ such that $p, q \in y$ but neither p nor q is in x.
2. Choose n such that $2^n(q - p) > 2$
3. Find integer $m \geq 1$ such that $p < \frac{m}{2^n} < \frac{m+1}{2^n} < q$
4. Perform the binary expansion procedure simultaneously on x, y, $z = \frac{m}{2^n}$, $w = \frac{m+1}{2^n}$. Stop at the first step i at which there is a disagreement $(i \leq n)$
5. Since the first $i - 1$ steps agree, $x_{i-1} < z_{i-1} < w_{i-1} < y_{i-1}$ and hence the ith digit of x is 0, whilst the ith digit of y is 1.

$\square$

Binary representation of real numbers

Theorem

Let $a_1, a_2, a_3, \ldots$ be a sequence of 0s and 1s, (formally a is a function $a : \{1, 2, 3, \ldots\} \to \{0, 1\}$) containing infinitely many 1s. There is a real number x, $0 < x \leq 1$ with $0.a_1a_2a_3\ldots$ as its binary expansion.

Proof.

- Define $S = \{\sum_{i=1}^{n} \frac{a_i}{2^i} : n \in \{1, 2, 3, \ldots\}\}$. Note $s \leq 1$ for all $s \in S$.
- Define $x = \sup S$ and note $0 < x \leq 1$.
- Let $x = 0.b_1b_2b_3\ldots$ and let i be the first index with $b_i \neq a_i$.
- Since $x > \sum_{j=1}^{i} \frac{a_j}{2^j}$ (there is an $\ell > i$ with $a_\ell = 1$), rule out $b_i = 0$, $a_i = 1$ since $a_i = 1$ implies $2x_{i-1} > 1$.
- If $b_i = 1$, $a_i = 0$, then $x > \sum_{j=1}^{i} \frac{b_j}{2^j}$, but in fact, $\sum_{j=1}^{i} \frac{b_j}{2^j}$ is an upper bound for S, a contradiction (this uses that $\sum_{n=1}^{N} \frac{1}{2^n} < 1$).

$\square$

Composition of functions

Definition

Let A, B, C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. The composition of f and g is the function $g \circ f : A \to C$ defined at $x \in A$ by

$$g \circ f(x) = g(f(x)).$$

Composition of functions

Theorem

Function composition is associative: If A, B, C and D are sets, and $f : A \to B$, $g : B \to C$ and $h : C \to D$ are functions, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Proof.

Let $f : a \mapsto b$, $g : b \mapsto c$, $h : c \mapsto d$, then

$$h \circ (g \circ f) : a \mapsto c \mapsto d, \qquad (h \circ g) \circ f : a \mapsto b \mapsto d.$$

Both combine to $a \mapsto d$. □

Composition of functions

Examples of composition:

- $f : \mathbb{R}^+ \to \mathbb{R}^+$, $g : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x) = x^2$, $g(x) = \frac{1}{x}$. Then $f \circ g(x) = g \circ f(x) = \frac{1}{x^2}$.
- $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$, $f(x) = x + 3$, $g(x) = x^2$. Then

$$f \circ g(x) = x^2 + 3, \qquad g \circ f(x) = x^2 + 6x + 9.$$

Composition is an operation which is not *generally* commutative.

Properties of composition

Theorem

Let $f : A \to B$ and $g : B \to C$ be functions.

- *If f and g are both surjective, then $g \circ f$ is surjective.*
- *If f and g are both injective, then $g \circ f$ is injective.*
- *If f and g are both bijective, then $g \circ f$ is bijective.*

Proof.

- Surjective: Let $z \in C$. Since g is surjective, choose $y \in B$ with $g(y) = z$. Since f is surjective, choose $x \in A$ satisfying $f(x) = y$. Then $g(f(x)) = z$.
- Injective: Suppose that x and y in A satisfy $g \circ f(x) = g \circ f(y)$. Injectivity of g implies $f(x) = f(y)$. Then injectivity of f implies $x = y$.
- Bijective: Combine surjective and injective.

$\square$

Inverse functions

Definition

Let $f : A \to B$ be a bijective function. The *inverse function* of f is the function $f^{-1} : B \to A$ defined at $y \in B$ by $f^{-1}(y)$ is the unique x such that $f(x) = y$.

Note that we already used the notation $f^{-1}(y)$ for the preimage of the point y in the context of a not necessarily bijective function. The notation is used in both ways and must be understood from the context.

Inverse functions

Examples:

- $f(x) = x^2$ is bijective from $\mathbb{R}^+ \to \mathbb{R}^+$ with $f^{-1}(y) = \sqrt{y}$.
- $f(x) = e^x$ is bijective from $\mathbb{R}$ to $\mathbb{R}^+$, with inverse $f^{-1}(y) = \log y$
- $f(x) = \tan x$ is bijective from $\{x \in \mathbb{R} : -\frac{\pi}{2} < x < \frac{\pi}{2}\}$ to $\mathbb{R}$, with inverse $f^{-1}(y) = \tan^{-1}(y)$.

Intervals

We use the usual notation regarding intervals. Let $a < b$ be real numbers.

1. The open interval $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
2. The closed interval $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
3. The half-open intervals $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$ and $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
4. The open infinite intervals $(a, \infty) = \{x \in \mathbb{R} : x > a\}$ and $(-\infty, a) = \{x \in \mathbb{R} : x < a\}$
5. The closed infinite intervals $[a, \infty) = \{x \in \mathbb{R} : x \geq a\}$ and $(-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$.
6. The real line $(-\infty, \infty) = \mathbb{R}$.

The rationals are countable

Recall that a set S is countable if there is an injective function $f : S \to \mathbb{N}$.

Theorem

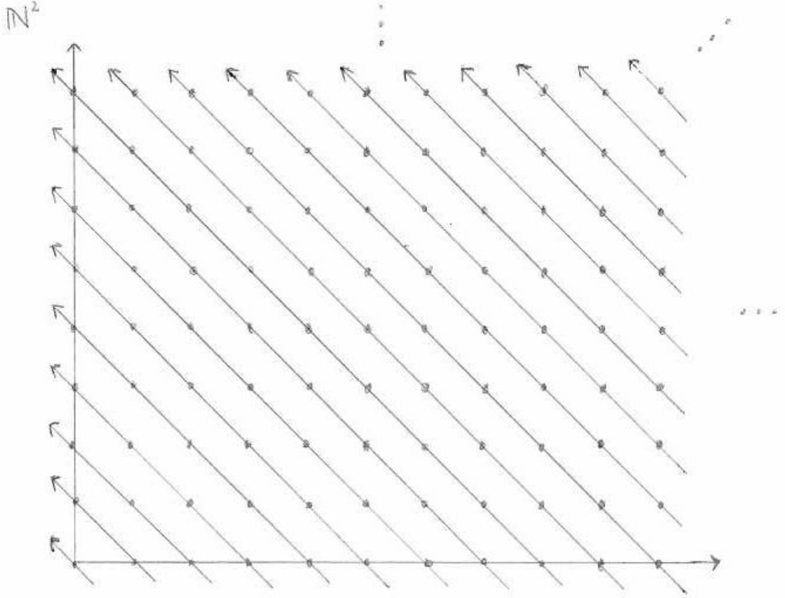
The field of rational numbers is countable.

Proof.

1. Write each $q \in \mathbb{Q}$ as $q = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b > 0$ and $\mathrm{GCD}(a, b) = 1$. The map $f_1 : q \mapsto (a, b)$ is an injective function $\mathbb{Q} \to \mathbb{Z}^2$.
2. Define $p : \mathbb{Z} \to \mathbb{N}$ by $p(x) = 2x$ if $x \geq 0$ and $p(x) = -2x - 1$ if $x < 0$. This is injective. It follows that $f_2 : \mathbb{Z}^2 \to \mathbb{N}^2$, $f_2(x, y) = (p(x), p(y))$ is injective.
3. Given $(a, b) \in \mathbb{N}^2$, set $s = a + b$ and define $f_3(a, b) = \frac{s(s+1)}{2} + b$. We claim that f_3 is a bijective map from $\mathbb{N}^2 \to \mathbb{N}$. Assuming this, $f_3 \circ f_2 \circ f_1 : \mathbb{Q} \to \mathbb{N}$ is an injection.

$\square$

The rationals are countable



The rationals are countable

Theorem

Given $(a, b) \in \mathbb{N}^2$, define $s = a + b$. The map $f_3 : \mathbb{N}^2 \to \mathbb{N}$ defined by $f_3(a, b) = \frac{s(s+1)}{2} + b$ is a bijection.

Proof.

Observe that for each $s = 0, 1, 2, ...,$ f_3 maps the set $\{(a, b) : a + b = s\}$ bijectively onto $\left\{n \in \mathbb{N} : \frac{s(s+1)}{2} \leq n < \frac{(s+1)(s+2)}{2}\right\}$. Since each $n \in \mathbb{N}$ lies in exactly one interval $\frac{s(s+1)}{2} \leq n < \frac{(s+1)(s+2)}{2}$, the claim follows. $\square$

The pigeonhole principle

Define $[1] = \{1\}$, and, recursively, for $n \geq 1$, $[n+1] = [n] \cup \{n+1\}$. Thus for natural number $n \geq 1$, $[n] = \{1, 2, 3, ..., n\}$.

Theorem

Let $1 \leq m < n$ be natural numbers. There does not exist an injective function from $[n]$ to $[m]$.

The pigeonhole principle

Proof of the pigeonhole principle.

- This is true for $m = 1$ for all $n > 1$ since a map $f : [n] \to [1]$ satisfies $f(2) = f(1) = 1$.
- Suppose the statement for some $1 \leq m < n$, and suppose there exists an injection from $f : [n+1] \to [m+1]$. If there is $1 \leq i < n+1$ with $f(i) = m+1$, redefine $f(i) := f(n+1), f(n+1) := f(i)$. f is still an injection, and in fact defines an injection $[n] \to [m]$, a contradiction.

The claim now follows from the variant of induction from HW1 #2: the statement proven is that for any pair m, n either $m \geq n$ or there does not exist an injection $[n] \to [m]$. □

Pigeonhole examples

Theorem

Let $n \geq 1$ and let $x_1, x_2, ..., x_{n+1}$ be $n+1$ real numbers from the half-open interval $(0, 1]$. Prove that there exist $1 \leq i < j \leq n+1$ with $|x_i - x_j| < \frac{1}{n}$.

Proof.

Form n half-open intervals $\{I_i\}_{i=1}^n$, $I_i = \left(\frac{i-1}{n}, \frac{i}{n}\right]$. These intervals are disjoint and their union is $(0, 1]$. Let $f : [n+1] \to [n]$ be defined by letting $f(i)$ be the index of the interval that contains x_i. By the pigeonhole principle, f is not an injection, so there exists some $\ell \in [n]$ and some $1 \leq i < j \leq n+1$ with $f(i) = f(j) = \ell$. It follows that

$$\frac{\ell}{n} < x_i, x_j \leq \frac{\ell + 1}{n}$$

and thus $|x_i - x_j| < \frac{1}{n}$. $\square$

Pigeonhole examples

Theorem

Given a set $S \subset [100]$ *containing at least 51 elements, prove that there are* $x, y \in S$ *with* $x + y = 101$.

Proof.

Form sets $P_j = \{j, 101 - j\}$ for $1 \leq j \leq 50$. Define $f : S \to [50]$ by assigning to $s \in S$ the index of the set to which it belongs. By the pigeonhole principle, two elements of S map to the same index, and hence have sum 101. $\square$