I. Cardinal Numbers

UBC M320 Lecture Notes by Philip D. Loewen

A. Set Theory and Logic; Notation

Statements. We're interested in "statements", also known as "logical propositions": these are unambiguous declarative sentences that are either true or false. They could involve symbols as well as words. Examples include the statements a and b below.

$$a: \qquad 2+2=4.$$
$$b: \qquad 2+2=5.$$

Statement a is true; statement b is false. It is possible to string words together and form grammatically correct sentences whose meanings depend on interpretation, or might be both a little bit true and a little bit false all at once. Such constructions are outside the scope of our course.

Sets. Everything comes down to sets. A **set** is a collection of **objects.** We define neither of these terms, relying instead on the following naïve operational understanding. A set is like a **data structure,** with three capabilities:

(i) Simple Lookup: For any object x and set S, exactly one of the statements "$x \in S$" or "$x \notin S$" is true; the other is false. An object x is an *element of* S if and only if $x \in S$.

(ii) Automatic Redundancy Suppression: The sets $A = \{0,1,0,1,0,1,0,1,\dots\}$ and $B = \{0,1\}$ are identical. (A precise definition of equality between sets is given below.)

(iii) Indexing: Any given set S can release each object it contains in some systematic fashion that makes it possible to assign unambiguous true/false values to definitions or statements of the form, "For every object x in S, ..." [E.g., "For every real number t, define $A_t = \{x \in \mathbb{R} : x \geq t\}$."]

Synonyms. There is no restriction on the types of "object" inside a set. Since a set is itself a type of object, a set can contain other sets. So it's logically possible, and sometimes useful, to think about a "set of sets". It can be more understanable to speak of a "family of sets", or a "collection of sets", or something similar, but in such cases the terms below are all considered equivalent:

$$\text{set} = \text{family} = \text{collection} \;=\; \cdots \;= \text{aggregate} = \text{bag} = \text{sack} = \;\cdots.$$

The Empty Set. We use $\emptyset$ to denote **the empty set.** Its defining property is that the statement "$x \in \emptyset$" is *false* for every object x. In other words, it is *true* to say "For all x, $x \notin \emptyset$". Now the empty set is an object itself, so it may (or may not) lie inside other sets. But be careful: The set $A = \{\emptyset\}$ is different from the set $\emptyset$: $\emptyset \in A$ is true, whereas $\emptyset \in \emptyset$ is false. The notation $\{\}$ is a plausible replacement for $\emptyset$; Rudin uses the notation 0. We avoid this because the symbol 0 also stands for an important number, and it's confusing to use the same name for two different things.

Russell's Paradox (1901) [optional]. The setup outlined above sounds utterly sensible, but it conceals some logical dangers. To illustrate these, start by classifying sets according to this definition:

$$\begin{aligned} &\text{A set } S \text{ is} \quad \textbf{normal} \Leftrightarrow \ S \notin S; \\ &\text{A set } S \text{ is } \textbf{abnormal} \Leftrightarrow \ S \in S. \end{aligned}$$

Clearly every set is either normal or abnormal, and its impossible for a set to be both at once. Now let N be the collection of all normal sets. What type of set is N?

- If N is normal, then the definition gives $N \notin N$. Being outside the set N means that N is abnormal. But no set can be both normal and abnormal, so this can't happen.
- If N is abnormal, then the definition gives $N \in N$. Being an element of the set N means that N must be normal. But no set can be both normal and abnormal, so this can't happen either.

Something terrible is happening here. The normal/abnormal scheme classifies all sets into two distinct categories, and our N cannot logically belong to either one. What's wrong? Our naïve view of "sets" and "objects"! To be completely solid, we need some fundamental rules about what kinds of collections get to be called "sets", and these rules should disqualify N from that category. For the purposes of MATH 320, we adopt the 9-axiom setup named ZFC, named after Zermelo and Fraenkel plus the Axiom of Choice. Wikipedia has details, on the page entitled "Zermelo-Fraenkel_set_theory". This is the standard axiomatic basis for working mathematicians, and it is largely compatible with the naïve approach. We will stay out of trouble by taking care never to contemplate something as vast and vague as the set of all sets. Let us press on.

Notation for Logic. For logical propositions a and b,

$a \vee b$	means "a or b": it's true exactly when a or b or both are true,
$a \wedge b$	means "a and b": it's true exactly when a and b are true simultaneously,
$\sim a$	means "not a": its truth value is opposite to that of a,
$[a \Rightarrow b]$	means "a implies b": its truth value is $(\sim a) \vee b$. (Think about *rejecting* it.)
$[a \Leftrightarrow b]$	means "a if and only if b": it's true exactly when the truth values of a and b are the same.

Definitions (Sets). For given subsets A and B of some "universal" set X,

$$\begin{aligned} A \cup B &\stackrel{\text{def}}{=} \{x \in X \,:\, (x \in A) \vee (x \in B)\} && \text{is the } \textit{union} \text{ of } A \text{ and } B, \\ A \cap B &\stackrel{\text{def}}{=} \{x \in X \,:\, (x \in A) \wedge (x \in B)\} && \text{is the } \textit{intersection} \text{ of } A \text{ and } B \\ A^c &\stackrel{\text{def}}{=} X \setminus A = \{x \in X \,:\, \sim(x \in A)\} && \text{is the } \textit{complement} \text{ of } A, \text{ and} \\ B \setminus A &\stackrel{\text{def}}{=} B \cap A^c = \{x \in X \,:\, (x \in B) \wedge \sim(x \in A)\}. \end{aligned}$$

Note the connections between $\cup$ and $\vee$, $\cap$ and $\wedge$, $()^c$, and $\sim$. For sets A and B, the four expressions below have identical meanings:

$$A \subseteq B, \qquad A \subset B, \qquad B \supseteq A, \qquad B \supset A.$$

They all mean this: "$\forall x \in A$, one has $x \in B$"; or, $x \in A \Rightarrow x \in B$. The definition of "$A = B$" is $(A \subseteq B) \wedge (B \subseteq A)$; equivalently, $(x \in A) \Leftrightarrow (x \in B)$.

Tautologies. Imagine doing algebra with logical propositions. A *tautology* is a statement like "$a \vee (\sim a)$" that comes out true for all possible T/F values of the variables involved. These can be useful, especially when the central feature is "$\Leftrightarrow$". Favourites include

$$\begin{aligned}
[a \Rightarrow b] &\iff [(\sim b) \Rightarrow (\sim a)] && \text{(contraposition)}\\
[a \Leftrightarrow b] &\iff [a \Rightarrow b] \wedge [b \Rightarrow a] && \text{(equivalence)}\\
\sim(a \wedge b) &\iff (\sim a) \vee (\sim b) && \text{(de Morgan)}\\
\sim(a \vee b) &\iff (\sim a) \wedge (\sim b) && \text{(de Morgan)}
\end{aligned}$$

Here are the corresponding statements about sets:

$$\begin{aligned}
A \subseteq B &\iff A^c \supseteq B^c\\
A = B &\iff [A \subseteq B] \wedge [B \subseteq A]\\
(A \cap B)^c &= A^c \cup B^c\\
(A \cup B)^c &= A^c \cap B^c.
\end{aligned}$$

Quantifiers and Their Negations. Suppose S is a set, and for every object x in S, we have a statement $a(x)$ that involves x.

$(\forall x \in S)\, a(x)$ means "for each object x in set S, statement $a(x)$ is true". This true automatically when $S = \emptyset$; otherwise $\forall$ works like a generalized form of "ans". [E.g., if $S = \{0, 1, 2\}$, $(\forall x \in S)\, a(x)$ is the same as $a(0) \wedge a(1) \wedge a(2)$.]

$(\exists x \in S)\, a(x)$ means "there exists some object x in set S for which statement $a(x)$ is true". It's automatically false when $S = \emptyset$; otherwise $\exists$ works like a generalized "or". [E.g., if $S = \{0, 1, 2\}$, $(\exists x \in S)\, a(x)$" says $a(0) \vee a(1) \vee a(2)$.]

Important: The quantifiers $\forall$ and $\exists$ do not commute. If S and T are sets, the two statements below are quite different (think of a specific example!):

(i) $\forall x \in S,\ \exists y \in T\ :\ a(x, y)$

(ii) $\exists y \in T\ :\ \forall x \in S,\ a(x, y)$.

Negations. As de Morgan's laws suggest, and common sense confirms,

$$\begin{aligned}
\sim[(\forall x \in S)\, a(x)] &\iff (\exists x \in S)[\sim a(x)]\\
\sim[(\exists x \in S)\, a(x)] &\iff (\forall x \in S)[\sim a(x)].
\end{aligned}$$

Families of Sets. If $\mathcal{A}$ is a set in which every element is itself a set ["a family of sets"], we define the large-scale union and intersection operators as follows:

$$\bigcup \mathcal{A} \stackrel{\text{def}}{=} \bigcup_{A\in\mathcal{A}} A = \{x \in X \,:\, \exists A \in \mathcal{A} \text{ s.t. } x \in A\}\,,$$
$$\bigcap \mathcal{A} \stackrel{\text{def}}{=} \bigcap_{A\in\mathcal{A}} A = \{x \in X \,:\, \forall A \in \mathcal{A},\ x \in A\}\,.$$

De Morgan's Laws here take the form

$$\left[\bigcup \mathcal{A}\right]^c = \bigcap_{A\in\mathcal{A}} A^c, \qquad \left[\bigcap \mathcal{A}\right]^c = \bigcup_{A\in\mathcal{A}} A^c.$$

When the family $\mathcal{A}$ contains one set for each positive integer, labelled so that $\mathcal{A} = \{A_1, A_2, A_3, \dots\}$, we mimic classic sigma-notation as follows:

$$\bigcup \mathcal{A} = \bigcup_{i\in\mathbb{N}} A_i = \bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots,$$
$$\bigcap \mathcal{A} = \bigcap_{i\in\mathbb{N}} A_i = \bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots.$$

B. Hilbert's Hotel; Mappings

06 Sep 2023

The rooms in Hilbert's Hotel are numbered $1, 2, 3, \dots$, one for each positive integer. All rooms are occupied when the King arrives to stay the night. No problem: for each room n in $\mathbb{N}$, ask the occupant to move to room $n+1$. No current guests have to share a bed or sleep outdoors, and the King gets Room 1, which is now vacant. Sketch.

Mathematically, the mapping $f\colon (\mathbb{N}\cup\{0\}) \to \mathbb{N}$ defined by

$$f(n) = n + 1$$

is a "one-to-one correspondence" between the sets $\mathbb{N}\cup\{0\}$ (the guests) and $\mathbb{N}$ (the rooms). One-to-one correspondence is how we "count" elements of sets—including infinite sets.

08 Sep 2023

Definition. (Mappings) Let X and Y be sets.

(a) The *cartesian product* is the set of all ordered pairs (x, y) where $x \in X$, $y \in Y$. I.e.,

$$X \times Y = \{(x, y) \,:\, x \in X,\ y \in Y\}\,.$$

(Extend: $X_1 \times X_2 \times \cdots \times X_n = \prod_{k=1}^{n} X_k = \{(x_1, \dots, x_n) \,:\, x_k \in X_k,\ \forall k = 1, \dots, n\}$.)

(b) Any subset G of $X \times Y$ defines a *set-valued mapping* (or *multifunction*, or *relation*) from X to Y; the notation $G\colon X \rightrightarrows Y$ encodes the sets involved. We write

$$G(x) = \{y \in Y \,:\, (x,y) \in G\}\,,$$
$$G^{-1}(y) = \{x \in X \,:\, (x,y) \in G\}\,,$$
$$\operatorname{dom}(G) = \{x \in X \,:\, G(x) \neq \emptyset\}\,.$$

(Thus $G^{-1}\colon Y \rightrightarrows X$ corresponds to the set $\{(y,x) \,:\, (x,y) \in G\}$.)

(c) We extend the notation to subsets $A \subseteq X$ and $B \subseteq Y$ as follows:

$$G(A) = \bigcup_{a \in A} G(a) = \{y \in Y \,:\, y \in G(a) \text{ for some } a \in A\}$$
$$G^{-1}(B) = \bigcup_{b \in B} G^{-1}(b) = \{x \in X \,:\, G(x) \cap B \neq \emptyset\}\,.$$

(d) A set-valued mapping $G\colon X \rightrightarrows Y$ is a *mapping* or *function* when the set $G(x)$ contains exactly one point for each x in X. (In particular, $\operatorname{dom}(G) = X$.) These properties are encoded in the single-arrow notation $G\colon X \to Y$, and in such cases we typically write $G(x) = y$ instead of $G(x) = \{y\}$.

(e) It is possible that $G\colon X \to Y$ is a function (i.e., single-valued), but $G^{-1}(y)$ is not. The original notation applies:

$$G^{-1}(y) = \{x \in X \,:\, (x,y) \in G\} = \{x \in X \,:\, G(x) = y\}\,.$$

When the function G is one-to-one (see below), the shorthand in (c) is mirrored by writing $G^{-1}(y) = x$ instead of $G^{-1}(y) = \{x\}$.

Example. (a) $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x_1, x_2) \,:\, x_1 \in \mathbb{R},\ x_2 \in \mathbb{R}\}$.

(b) With $X = \mathbb{R}$, $Y = \mathbb{R}$, take $G = \{(x,y) \,:\, |y| \leq x\}$. Sketch; note

$$\operatorname{dom} G = \{x \in \mathbb{R} \,:\, x \geq 0\} = [0, +\infty),$$
$$G(x) = \begin{cases} \emptyset, & \text{if } x < 0, \\ [-x, x], & \text{if } x \geq 0, \end{cases}$$
$$G^{-1}(y) = [|y|, +\infty).$$

(c) [*There is no f.*] Writing just $y = x^2$ triggers healthy reflexes in Calculus veterans. But there is no function ... yet. Even the letters x and y are not required or special in any way. The reflex interpretation of "$y = x^2$" is to think of a certain subset of the Cartesian plane $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. Another way to define this same set (without mentioning x or y) is to say $G = \big\{(t, t^2) \,:\, t \in \mathbb{R}\big\}$. This defines a famous single-valued $G\colon \mathbb{R} \to \mathbb{R}$, namely, $G(x) = x^2$. This function is not invertible, but our set-valued notation still applies, and it produces

$$G^{-1}(y) = \begin{cases} \emptyset, & \text{if } y < 0, \\ \big\{\sqrt{y}, -\sqrt{y}\big\}, & \text{if } y \geq 0. \end{cases}$$

(Aside: How many elements in the set $G^{-1}(0)$? Literal interpretation of the definition above says $G^{-1}(0) = \{0, -0\}$, but that set contains just one element, since $0 = -0$.)

(d) [Skipped.] We can draw this set as a solid cone in $3D$:

$$\begin{aligned} G &= \left\{(r,x) \in \mathbb{R} \times \mathbb{R}^2 \,:\, |x| \le r\right\} \\ &= \left\{(r,x_1,x_2) \in \mathbb{R}^3 \,:\, r \ge 0,\ x_1^2 + x_2^2 \le r^2\right\}. \end{aligned}$$

Here

$$G(r) = \begin{cases} \emptyset, & \text{if } r < 0, \\ \{(0,0)\}, & \text{if } r = 0, \\ \left\{(x_1,x_2) \,:\, x_1^2 + x_2^2 \le r^2\right\}, & \text{if } r > 0. \end{cases}$$

Thus $\text{dom}(G) = \{r \in \mathbb{R} \,:\, r \ge 0\} = [0, +\infty)$, and, for example,

$$G^{-1}\left((0,1)\right) = \{r \in \mathbb{R} \,:\, r \ge 1\} = [1, +\infty).$$

////

Definition. (Mapping Properties) Let $f: X \to Y$ be a (single-valued) mapping defined on X.

(a) To call f *one-to-one* (or 1-1, or *injective*) means this:

$$\begin{gathered} \forall x_1, x_2 \in X,\ f(x_1) = f(x_2) \implies x_1 = x_2 \\ \text{i.e.,} \quad \forall x_1, x_2 \in X,\ x_1 \ne x_2 \implies f(x_1) \ne f(x_2). \end{gathered}$$

(b) To call f *onto* (or *surjective*) means that $f(X) = Y$, i.e.,

$$\forall y \in Y,\ \exists x \in X \ :\ y = f(x).$$

(c) To call f a *one-to-one correspondence* (or *bijection*) means that f is **both** 1-1 and onto.

Example. Consider $f: \mathbb{R} \to \mathbb{R}$, defined by $f(x) = \dfrac{x}{\sqrt{1+x^2}}$.

(i) f is not onto.
Any choice $y \ge 1$ or $y \le -1$ violates definition (b). (Sketch.)

(ii) f is 1-1.
To prove this, assume $f(x) = f(y)$ and deduce $x = y$. Indeed,

$$x\sqrt{1+y^2} = y\sqrt{1+x^2} \implies x^2 + x^2y^2 = y^2 + x^2y^2 \implies y = \pm x.$$

If $y = x$, we are finished. But if $y = -x$, $f(y) = f(-x) = -x/\sqrt{1+(-x)^2} = -f(x)$. Together with $f(x) = f(y)$, this entails $f(x) = 0$, so $x = 0$. Thus $y = x$.

(iii) The mapping f puts $\mathbb{R}$ into one-to-one correspondence with the interval $(-1, 1)$.

////

Remark. If $\phi: X \to Y$ is both 1-1 and onto, then $\phi^{-1}: Y \to X$ is single-valued, 1-1 and onto. [Pf.]

C. Countability

Recall $\mathbb{N} = \{1, 2, 3, \dots\}$, the set of **natural numbers**.

Definition. A set S is **finite** if either $S = \emptyset$ or there exists some $n \in \mathbb{N}$ and some bijection $\phi\colon \{1, 2, \dots, n\} \to S$. [Notation: $|\emptyset| = 0$, $|\{1, 2, \dots, n\}| = n$.]

Definition. A set Y is **countable** if there exists some bijection $\phi\colon \mathbb{N} \to Y$. [Notation: $|S| = \aleph_0$.]

Sidebar. If every infinite set were countable, we wouldn't need to invent a special term. It may be interesting to explore the ways this concept can break down.

Example. Some countable sets:

(a) $\mathbb{N}$ itself. Use $\phi(y) = y$, the identity mapping on $\mathbb{N}$.

(b) Hilbert's Hotel: $\mathbb{N} \cup \{0\}$. (Use $\phi(n) = n - 1$.)

(c) $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. Use $\psi\colon \mathbb{N} \to \mathbb{Z}$ defined by

$$\psi(n) = \begin{cases} -n/2, & \text{if } n \text{ is even, i.e., } n = 2k \ \exists k \in \mathbb{N}, \\ (n-1)/2, & \text{if } n \text{ is odd, i.e., } n = 2k - 1 \ \exists k \in \mathbb{N}. \end{cases}$$

11 Sep 2023

(d) $\mathbb{N} \times \mathbb{N}$.

Proof. Enumerate the ordered pairs in $\mathbb{N} \times \mathbb{N}$ as indicated below:

$$\begin{array}{ccccccc} (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & \cdots \\ (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & \cdots \\ (3,1) & (3,2) & (3,3) & (3,4) & (3,5) & \cdots \\ (4,1) & (4,2) & (4,3) & (4,4) & (4,5) & \cdots \\ (5,1) & (5,2) & (5,3) & (5,4) & (5,5) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Note that diagonal number k includes all pairs whose elements sum to $k + 1$. This makes it easy to show that the enumeration scheme is onto: the pair (m, n) shows up on diagonal number $m + n - 1$, so it's easy to calculate its index in the sequence described above. ////

Countability and Sequences. If A is countable, with $\phi\colon \mathbb{N} \to A$ bijective, defining $a_n = \phi(n)$ lets us write $A = \{a_1, a_2, a_3, \dots\}$. Conversely, if $A = \{a_1, a_2, a_3, \dots\}$ is the collection of values from some sequence with distinct terms, then defining $\psi(n) = a_n$ produces a bijection and shows A is countable.

Well-Ordering Property for $\mathbb{N}$. Every nonempty subset S of $\mathbb{N}$ contains a smallest element. In symbols,

$$S \subseteq \mathbb{N},\ S \neq \emptyset \implies \exists \widehat{s} \in S : \forall s \in S,\ \widehat{s} \leq s. \qquad (*)$$

We take this as known; it's the basis for Mathematical Induction. Typical notation for $\widehat{s}$ is $\min S$ or $\min(S)$.

Proposition. *Every subset of $\mathbb{N}$ is either finite or countable.*

Proof. Let $A \subseteq \mathbb{N}$. If A is finite, we're done, so assume A is infinite. Write $A_1 = A$. Clearly $A_1 \neq \emptyset$, so let $a_1 = \min(A_1)$. Clearly $a_1 \geq 1$.

Then let $A_2 = A \setminus \{a_1\}$: Since A is infinite, $A_2 \neq \emptyset$, so let $a_2 = \min(A_2)$. Notice $a_2 \geq 1 + a_1$, so $a_2 \geq 2$.

Continue inductively. Having chosen a_n, let $A_{n+1} = A \setminus \{a_1, a_2, \ldots, a_n\}$. Since A is infinite, $A_{n+1} \neq \emptyset$, so pick $a_{n+1} = \min A_{n+1}$. Notice $a_{n+1} \geq 1 + a_n$, so $a_{n+1} \geq n+1$. By induction, this defines a_n for each $n \in \mathbb{N}$.

Now define $\phi\colon \mathbb{N} \to A$ by $\phi(n) = a_n$.

This ϕ is $1-1$. Indeed, if $m \neq n$, choosing the labels to arrange $m < n$ implies $\phi(m) < \phi(n)$.

To see that ϕ is onto, pick any $a \in A$. Then $\phi(a) \geq a$, so $a = \phi(k)$ for some $k \leq a$.

Thus ϕ is a bijection, and this confirms the definition that A is countable. ////

Proposition. *Every subset of any countable set is either finite or countable.*

Proof. Let X be a countable set, with subset S. Then there must be some bijection $\psi\colon \mathbb{N} \to X$. Define $f\colon S \to \mathbb{N}$ like this

$$f(s) = \psi^{-1}(s), \qquad s \in S.$$

Then f is a bijection between S and $f(S)$, a subset of $\mathbb{N}$. By above, $f(S)$ is either finite or countable. Thus the same holds for S. ////

> *Proof.* (If only we had Schroeder-Bernstein, it would be this easy.) Let A be a countable set, with a subset S. If S is finite, the conclusion is automatic. If S is infinite, then it has a countable subset S_1. Then $S_1 \subseteq S \subseteq A$ and $S_1 \sim A$. By the Proposition above, $S \sim A$ also, i.e., S is countable. ////

Proposition. *Every infinite set contains a countably infinite subset.*

Proof. Mimic previous proof, but drop the stipulation that each new point have some relation to the earlier selections. (You still get a sequence, only now it may fail to include all elements of the original set.) ////

Terminology. "Finite or countable" ≡ "at most countable".

Theorem (Proving Countability). *Given a set A, either* (a) *or* (b) *below implies that A is finite-or-countable:*

(a) *There exist a countable set X and a* **one-to-one** *mapping $f\colon A \to X$,*

(b) *There exist a countable set X and an* **onto** *mapping $g\colon X \to A$.*

Proof. (a) Write $S = f(A) = \{f(x) : x \in A\}$. Since $S \subseteq X$, S is either finite or countable. Since $f\colon A \to S$ is a bijection, the same is true for A.

(b) Enumerate $X = \{x_1, x_2, \dots\}$. For each a, let $f(a) = \min\{n \in \mathbb{N} : g(x_n) = a\}$. (That set is nonempty because g is onto.) This defines a mapping $f\colon A \to \mathbb{N}$ that establishes a one-to-one correspondence between A and $f(A)$. Since $f(A)$ is a subset of $\mathbb{N}$, it must be finite or countable; the same therefore holds for A.

Details (1-1): Suppose $a_1, a_2 \in A$ obey $f(a_1) = f(a_2)$. Then, since $g(x_{f(a)}) = a$ for each $a \in A$,

$$a_1 = g(x_{f(a_1)}) = g(x_{f(a_2)}) = a_2.$$

////

More Countable Sets. The countability of $\mathbb{N} \times \mathbb{N}$ has useful consequences:

1. If A and B are countable sets, then $A \times B$ is countable too.

   [Write $A = \{a_1, a_2, \dots\}$, $B = \{b_1, b_2, \dots\}$, and define $g\colon \mathbb{N} \times \mathbb{N} \to A \times B$ by $g(m, n) = (a_m, b_n)$. This g is ONTO, and $\mathbb{N} \times \mathbb{N}$ is countable; result follows from (b) above.]

2. Let $\mathcal{S}_2$ be the collection (set) of all nonempty subsets of $\mathbb{N}$ with one or two elements. Then $\mathcal{S}_2$ is countable.

   Pf: Define $g\colon \mathbb{N} \times \mathbb{N} \to \mathcal{S}_2$ by $g(m, n) = \{m, n\}$. Clearly g is onto; since $\mathbb{N} \times \mathbb{N}$ is countable, result follows from (b) above. [E.g., $\{5\} = \phi(5, 5)$; $\{1, 2\} = \phi(1, 2) = \phi(2, 1)$; etc. Note that g is not 1-1.]

13 Sep 2023

3. The union of countably many sets, each one countable, is a countable set.

   Pf: Suppose $A^{(1)}, A^{(2)}, \dots$ is a list of countable sets. Enumerate each set—for each $m \in \mathbb{N}$, arrange

   $$A^{(m)} = \left\{a_1^{(m)}, a_2^{(m)}, a_3^{(m)}, \dots\right\}.$$

   Then define $g\colon \mathbb{N} \times \mathbb{N} \to \bigcup_{m \in \mathbb{N}} A^{(m)}$ by

   $$g(m, n) = a_n^{(m)}.$$

This g might not be 1-1 if the sets $A^{(m)}$ overlap, but it's certainly onto. Since $\mathbb{N} \times \mathbb{N}$ is countable, that's enough to show $\bigcup_{m\in\mathbb{N}} A^{(m)}$ is countable. [Again we have used (b) above.]

4. The set $\mathbb{Q}$ of rational numbers is countable.

   Pf: We showed earlier that $\mathbb{Z}$ is countable. Hence the set of pairs $\mathbb{Z} \times \mathbb{N}$ is countable, by item 1. The mapping $\phi\colon \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ defined by $\phi(p, q) = p/q$ is clearly onto, so $\mathbb{Q}$ is countable by part (b) of the theorem above.

5. The set $\mathbb{N}^3 = \mathbb{N} \times \mathbb{N} \times \mathbb{N} = \{(p, q, r) : p, q, r \in \mathbb{N}\}$ is countable. So is $\mathcal{S}_3$, the collection of nonempty subsets of $\mathbb{N}$ with 3 or fewer elements.

   Pf: Since both $\mathbb{N}\times\mathbb{N}$ and $\mathbb{N}$ are countable, so [by item 1] is the set $P = (\mathbb{N}\times\mathbb{N})\times\mathbb{N}$. A bijection $f\colon \mathbb{N}^3 \to P$ is

   $$f(p, q, r) = ((p, q), r)\,.$$

   Clearly $g(p, q, r) = \{p, q, r\}$ maps $\mathbb{N}^3$ **onto** $\mathcal{S}_3$.

6. The collection of all finite subsets of $\mathbb{N}$ is countable.

   Pf: Extend items 1–2 and 5 into an obvious induction proof that for each fixed $k \in \mathbb{N}$, the set $\mathbb{N}^k$ is countable and hence so is the family $\mathcal{S}_k$ consisting of all subsets of $\mathbb{N}$ with k or fewer elements. Now consider

   $$\mathcal{F} = \{\emptyset\} \cup \bigcup_{k\in\mathbb{N}} \mathcal{S}_k.$$

   As a countable union of countable sets, $\mathcal{F}$ is countable. Every finite subset of $\mathbb{N}$ is an element of $\mathcal{F}$; every element of $\mathcal{F}$ is a finite subset of $\mathbb{N}$.

Definition. A set Y is **uncountable** if both

(i) Y is infinite, and

(ii) no mapping $\phi\colon \mathbb{N} \to Y$ is bijective.

(Typically prove (ii) by showing every $\phi\colon \mathbb{N} \xrightarrow{1-1} Y$ is not onto.)

Theorem. *The real interval* $[0, 1)$ *is uncountable.*

Proof. It suffices to show that any $f\colon \mathbb{N} \xrightarrow{1-1} [0, 1)$ is not onto.

To do this, pick such an f and use decimal notation to write

$$f(1) = 0\,.\,x_1^1\,x_2^1\,x_3^1\,x_4^1\,\ldots$$
$$f(2) = 0\,.\,x_1^2\,x_2^2\,x_3^2\,x_4^2\,\ldots$$
$$f(3) = 0\,.\,x_1^3\,x_2^3\,x_3^3\,x_4^3\,\ldots$$
$$\vdots$$

always choosing representations not ending with an infinite string of 9's. Then define $y \in \mathbb{R}$ via

$$y = 0\,.\,y_1\,y_2\,y_3\,y_4\,\ldots$$

with digits

$$y_k = \begin{cases} 5, & \text{if } x_k^k = 7, \\ 7, & \text{otherwise.} \end{cases}$$

The digits show $5/9 \le y \le 7/9$, but for each k we have $y_k \neq x_k^k$ so $y \neq f(k)$. Hence $y \in [0,1) \setminus f(\mathbb{N})$, so f is not onto. ////

Corollary. (a) $\mathbb{R}$ *is uncountable.*

(b) *The set* $\mathbb{R} \setminus \mathbb{Q}$ *of irrational numbers is uncountable.*

Proof. (a) If $\mathbb{R}$ were countable, its infinite subset $[0,1)$ would be countable too. But this is false.

(b) Clearly $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$. If $\mathbb{R} \setminus \mathbb{Q}$ were countable, this would express $\mathbb{R}$ as a union of two countable sets. This would make $\mathbb{R}$ countable, which is known to be false. ////

D. Cardinal Numbers

15 Sep 2023

Definition. Given sets X and Y, write $X \sim Y$ if there exists a **one-to-one** mapping from X **onto** Y. (Say "$X \sim Y$ under ϕ" as shorthand for "$\phi\colon X \to Y$ is one-to-one and onto".)

We will often use the following immediate consequence of the definition:

If $f\colon X \xrightarrow{1-1} Y$ and $A \subseteq X$, then $A \sim f(A)$.

Proposition. *For any sets* X, Y, Z,

(R) $X \sim X$ *('$\sim$' is* **R***eflexive),*

(S) $X \sim Y \implies Y \sim X$ *('$\sim$' is* **S***ymmetric),*

(T) $X \sim Y$ and $Y \sim Z \implies X \sim Z$ *('$\sim$' is* **T***ransitive).*

Proof. (Exercise outline.) For (R), consider the identity mapping $\phi\colon X \to X$, defined by $\phi(x) = x$.

For (S), show that if $\phi\colon X \to Y$ is both 1-1 and onto, then $\phi^{-1}\colon Y \to X$ is well-defined, 1-1, and onto.

For (T), suppose $X \sim Y$ under ϕ and $Y \sim Z$ under ψ. Then $X \sim Z$ under $\psi \circ \phi$. ////

For sets X, the symbol $|X|$ denotes "the cardinal number of X", intuitively "the number of points in X". With this symbol, $X \sim Y$ is written $|X| = |Y|$.

Cardinal Inequalities. For sets X and Y,

(a) $|X| \leq |Y|$ means there is a one-to-one map $f\colon X \to Y$. So does $|Y| \geq |X|$.

(b) $|X| < |Y|$ means $|X| \leq |Y|$ but every $f\colon X \xrightarrow{1-1} Y$ fails to be onto. So does $|Y| > |X|$.

Standard symbols. $|\mathbb{N}| = \aleph_0$, $|\mathbb{R}| = c$. Thus X is finite or countable iff $|X| \leq \aleph_0 = |\mathbb{N}|$, and we know "$c > \aleph_0$".

Beyond Uncountability. Given any set X, consider the collection of all its subsets:

$$\mathcal{P}(X) \stackrel{\text{def}}{=} \{U \,:\, U \subseteq X\}\,.$$

This is called "the power set" for X, and in some presentations it is denoted by 2^X.

Proposition. *For any set X, $|X| < |\mathcal{P}(X)|$.*

Proof. (Case $X = \emptyset$ trivial: see Rudin Problem 2.1.) To show $|X| \leq |\mathcal{P}(X)|$, define $f\colon X \xrightarrow{1-1} \mathcal{P}(X)$ by $f(x) = \{x\}$.

To deduce that $|X| < |\mathcal{P}(X)|$, let any $f\colon X \xrightarrow{1-1} \mathcal{P}(X)$ be given. We'll show f is not onto.

Indeed, define $S \in \mathcal{P}(X)$ like this:

$$S = \{x \in X \,:\, x \notin f(x)\}\,.$$

Claim: $S \notin f(X)$.
Suppose not, i.e., $S \in f(X)$. Then $S = f(y)$ for some $y \in X$. Two cases arise:

(i) $y \in S = f(y)$. Then, by def of S, $y \notin f(y)$ — contradiction.

(ii) $y \notin S = f(y)$. Then, by def of S, $y \in S$ — contradiction.

Thus $S \notin f(X)$, so f is not onto. ////

This shows that there is an infinite chain of distinct cardinal numbers:

$$0 < 1 < 2 < \cdots < |\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \cdots.$$

Remarks. It can be shown that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. The *continuum hypothesis* is the assertion that there is no set S for which $\aleph_0 < |S| < c$. This turns out to be undecidable in the ZFC axiom system: both the claim and its negation are compatible with ZFC! The details are beyond the scope of MATH 320.)

Theorem (Schroeder-Bernstein). *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Proof. Nontrivial. [See Section E, below.] ////

Example. If $a < b$ and $c < d$, then as real intervals $(a, b) \sim [c, d]$.

Proof. Choose $a_1, b_1 \in \mathbb{R}$ satisfying $[a_1, b_1] \subseteq (a, b)$; also choose $c_1, d_1 \in \mathbb{R}$ such that $[c_1, d_1] \subseteq (c, d)$. Then $[c, d] \sim [a_1, b_1] \subseteq (a, b)$ by a linear bijection, and $(a, b) \sim (c_1, d_1) \subseteq [c, d]$ by a linear bijection, so $(a, b) \sim [c, d]$ by Schroeder-Bernstein. ////

E. Schroeder-Bernstein Theorem

When dealing with inequalities between real numbers, the following statement feels "obvious" because it is so familiar; it's also a reasonably direct consequence of the defining properties of the symbols "$\leq$" and "$=$":

$$\Big[a \leq b \quad \text{and} \quad b \leq a\Big] \implies a = b. \tag{$*$}$$

Now we have recycled the same symbols for use in comparing cardinal numbers, but given both of them new meanings in this context. So if two sets A and B are given, the following statement is similar to the previous one *in appearance only, and not in meaning*:

$$\Big[|A| \leq |B| \quad \text{and} \quad |B| \leq |A|\Big] \implies |A| = |B|. \tag{$**$}$$

Proving ($**$) is by no means as simple as saying, "That's how inequalities work"! On the contrary, the only way to justify hijacking familiar comparison symbols like "$\leq$" for new uses is to provide an independent proof that the new definitions work the way inequalities are expected to behave. That's the point of this section.

Proposition. *If both $A_0 \supseteq A_1 \supseteq A_2$ and $A_0 \sim A_2$, then $A_0 \sim A_1$.*

Proof. The hypothesis allows for the extreme situations where either $A_0 = A_1$ or $A_0 = A_2$. In either case the conclusion is obvious, so we only need to handle the case where both inclusions in the setup are strict. In symbols, we will assume

$$A_0 \setminus A_1 \neq \emptyset \quad \text{and} \quad A_1 \setminus A_2 \neq \emptyset.$$

This preamble is not necessary, but it adds some reassuring nondegeneracy to the ingredients we build later.

Since $A_0 \sim A_2$ by hypothesis, there exists a bijection $f\colon A_0 \to A_2$. Use this f to define a sequence of nested sets:

$$A_3 = f(A_1),\ A_4 = f(A_2),\ \ldots,\ A_{n+2} = f(A_n),\ \ldots.$$

Applying f to the each set in the chain of inclusions $A_0 \supseteq A_1 \supseteq A_2$ gives $A_2 \supseteq A_3 \supseteq A_4$, and this process can be repeated inductively to reveal that

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq A_4 \supseteq \cdots.$$

Since $A_0 \neq A_1 \neq A_2$ and f is 1-1, every inclusion in this infinite chain is strict.

Now observe that

$$A_0 = \left(\bigcap_{k=0}^{\infty} A_k\right) \cup \left(\bigcup_{k=0}^{\infty} (A_k \setminus A_{k+1})\right). \tag{$\dagger$}$$

To prove (†), notice that the inclusion $\supseteq$ is obvious. For the reverse inclusion, $\subseteq$, pick any specific element x of A_0. If this x lies in each set A_n, $n \in \mathbb{N}$, then x appears in the first parenthesized set on the right of (†). Otherwise, the set $\{n \in \mathbb{N} : x \notin A_n\}$ must be nonempty, so we can use the well-ordering property of $\mathbb{N}$ to define $k = (-1) + \min\{n : x \notin A_n\}$. For this k, we have $n \geq 0$ and $x \in A_k \setminus A_{k+1}$. Therefore x appears in the second parenthesized set on the right of (†).

To simplify notation, let's write

$$S = \bigcap_{k=0}^{\infty} A_k, \qquad D_n = A_n \setminus A_{n+1},\ n \geq 0.$$

Now f is a bijection from A_n to A_{n+2} for every $n = 0, 1, 2, \ldots$. Therefore, for every $n \geq 0$, we have

$$f(D_n) = f(A_n \setminus A_{n+1}) = f(A_n) \setminus f(A_{n+1}) = A_{n+2} \setminus A_{n+3} = D_{n+2}. \qquad (\ddagger)$$

Then equation (†) expresses A_0 as a union of disjoint sets, as follows:

$$A_0 = \Big(D_0 \cup D_1 \cup D_2 \cup \cdots \Big) \cup S.$$

Recall that $D_0 = A_0 \setminus A_1$, so

$$A_1 = \Big(D_1 \cup D_2 \cup D_3 \cup \cdots \Big) \cup S.$$

To define a bijection $\phi\colon A_0 \to A_1$, we just make a "Hilbert's Hotel"-style shift of the even-subscripted sets in this disjoint union, leaving everything else unchanged:

$$\phi(x) = \begin{cases} f(x), & \text{if } x \in D_{2n} \text{ for some } n \geq 0, \\ x, & \text{otherwise.} \end{cases}$$

This ϕ is clearly 1-1 and onto, as required. ////

The following corollary is known as the **Schroeder-Bernstein Theorem (SBT)**.

Corollary (SBT). *Given sets A and B, suppose there are subsets $A_1 \subseteq A$ and $B_1 \subseteq B$ such that $A \sim B_1 \subseteq B$ and $B \sim A_1 \subseteq A$. Then $A \sim B$.*

Proof. Since $B \sim A_1$, there exists a bijection $f\colon B \to A_1$. Use it to define

$$A_2 \stackrel{\text{def}}{=} f(B_1) \subseteq f(B) = A_1 \subseteq A. \qquad (*)$$

Then $A_2 \sim B_1$ thanks to f, while $B_1 \sim A$ is given, so $A_2 \sim A$. Using $(*)$ with the Proposition above, we have $A \sim A_1$. But $A_1 \sim B$ by hypothesis, so $A \sim B$. ////

Example. Let A denote the real interval $[0,1)$, and let $B = [0,1) \times [0,1)$ denote the unit square in the Cartesian plane (with part of its boundary removed). Then $|B| = |A|$.

Proof. It suffices to define a 1-1 function $f\colon B \to A$. Why? Because then $A_1 \stackrel{\text{def}}{=} f(B)$ obeys $B \sim A_1 \subseteq A$, while $A \sim A \times \{0\} \subseteq B$ is obvious, so $A \sim B$ by Schroeder-Bernstein.

To define f, let any (x,y) in B be given. Write the decimal expansions

$$x = 0\,.\,x_1\,x_2\,x_3\,\ldots = \sum_{k=1}^{\infty} \frac{x_k}{10^k}, \qquad x_k \in \{0,\ldots,9\}\,,$$

$$y = 0\,.\,y_1\,y_2\,y_3\,\ldots = \sum_{k=1}^{\infty} \frac{y_k}{10^k}, \qquad y_k \in \{0,\ldots,9\}\,,$$

always choosing the (unique) representation that does not end with an infinite string of 9's. Then let

$$f(x,y) = 0\,.\,x_1\,y_1\,x_2\,y_2\,x_3\,y_2\,\ldots = \sum_{k=1}^{\infty} \frac{x_k}{10^{2k-1}} + \sum_{k=1}^{\infty} \frac{y_k}{10^{2k}}.$$

The digit string specified for $f(x,y)$ will not end in an infinite chain of 9's, and $f(x_1,y_2) = f(x_2,y_2)$ clearly implies $(x_1,y_1) = (x_2,y_2)$, so f is a 1-1 mapping from B into A.

Q: Is this f surjective?

A: No. One element of $A = [0,1)$ lying outside $f(B)$ is $1/11 = 0\,.\,\overline{09}$. ////