1.5 Cardinality

For any two sets A and B, we say they have the same *cardinality* if there exists a bijection $f\colon A \to B$. Intuitively, this means that the sets "have the same number of elements".

Having the same cardinality is an equivalence relation on the class of all sets.

We write $|A| = |B|$ to denote that the sets A and B have the same cardinality.

We say A has cardinality less than or equal to B (or B has cardinality greater than or equal to A), denoted $|A| \leq |B|$ or $|B| \geq |A|$, if there exists an injection $f\colon A \to B$.

Remark 1.51. By convention, we say the emptyset $|\emptyset| \leq |A|$ for any set A.

Lemma 1.52. *Consider two nonempty sets A and B. Then, $|A| \leq |B|$ if and only if there exists a surjective function $g\colon B \to A$.*

Proof. ($\Rightarrow$) Suppose there is an injection $f : A \to B$. Fix $a_0 \in A$. Define $g : B \to A$ by

$$g(b) = \begin{cases} f^{-1}(b), & b \in f(A), \\ a_0, & b \notin f(A). \end{cases}$$

Then g is surjective.

($\Leftarrow$) Suppose there is a surjection $g : B \to A$. For each $a \in A$ choose (one) $b_a \in g^{-1}(a)$; this choice defines a function $h : A \to B$, $h(a) = b_a$. Now for any $a \neq a' \in A$, we have that $g^{-1}(a) \cap g^{-1}(a') = \emptyset$, so $h(a) \neq h(a')$. Thus, h is injective. $\square$

You might ask whether we can prove the second direction without AC. Unfortunately no as they are equivalent. Think about it.

Theorem 1.53.

1. *$|A| \leq |A|$*
2. *$|A| \leq |B|$ and $|B| \leq |C|$ imply $|A| \leq |C|$*
3. *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$ (This is quite nontrivial! It is the Bernstein-Cantor-Schröder theorem.)*
4. *For any two sets A, B, either $|A| \leq |B|$ or $|B| \leq |A|$.*

Proof. the first two are trivial. The third one requires a bit more work and we will leave it to the end of this part. We can use the well-ordering theorem to prove 4 here.

For any two sets A, B, we first well-order them to be $(A, \leq_A)$ and $(B, \leq_B)$ using the well-ordering theorem. Then, by Theorem 1.43, we have that one poset is order-isomorphic to an initial segment of the other. This isomorphism gives rise to an injective map that we want and hence concludes the proof. $\square$

1.5.1 Finite sets

Now, let's consider the finite case.

Definition 1.54. A set A is said to be *finite* if there is a bijection $f\colon A \to \{1, 2, \dots, n\}$ for some $n \in \mathbb{N}$ or A is empty. Otherwise, we say that A is *infinite*.

We intuitively say that A has cardinality n or 0.
Goal: Show that cardinality of a finite set is unique.

Lemma 1.55. *Let A be finite and $a_0 \in A$. Then, there exists a bijection $f\colon A \to \{1, \dots, n+1\}$ for some $n \in \mathbb{N}$ if and only if there exists a bijection $g\colon A \setminus \{a_0\} \to \{1, \dots, n\}$ for some $n \in \mathbb{N}$.*

Theorem 1.56. *Suppose $f : A \to \{1, \dots, n\}$ is a bijection and let $B \subsetneq A$. Then, there is no bijection $g\colon B \to \{1, \dots, n\}$.*

Proof. For $n = 1$, then $B = \emptyset$, and there is no bijection $g\colon \emptyset \to \{1\}$ (there is no even functions).

If the theorem is true for n, we will next show that it is true for $n+1$. Then, we use the inductive principle to conclude that the theorem is true for all $n \in \mathbb{N}$ (see homework).

Let $f\colon A \to \{1, \dots, n+1\}$ be a bijection. Let $B \subsetneq A$.

If $B = \emptyset$, same as before.

If $B \neq \emptyset$, choose $a_0 \in B$. Apply Theorem 1.55 to get a bijection $h : A\setminus\{a_0\} \to \{1, \dots, n\}$. Note $B\setminus\{a_0\} \subsetneq A\setminus\{a_0\}$. Since the theorem holds true for n, there is no bijection $g\colon B\setminus\{a_0\} \to \{1, \dots, n\}$. By Theorem 1.55 again, there is no bijection $g\colon B \to \{1, \dots, n+1\}$. □

Corollary 1.57. *If A is finite, then there is no bijection from A onto a proper subset of itself.*

Proof. Suppose for contradiction that $f : A \to B$ is a bijection with $B \subsetneq A$. Let $g : A \to \{1, \dots, n\}$ be a bijection (existence follows from finiteness). Then the composite

$$g \circ f^{-1} : B \longrightarrow \{1, \dots, n\}$$

is a bijection from the proper subset B to $\{1, \dots, n\}$, contradicting Theorem 1.56. A commutative diagram summarising the argument:

$$\begin{tikzcd} A \arrow[r, "f", "\cong"'] \arrow[d, "g"', "\cong"] & B \arrow[dl, "g\circ f^{-1}"] \\ \{1, \dots, n\} & \end{tikzcd}$$

Hence such an f cannot exist. □

Corollary 1.58 (Uniqueness of finite cardinality)**.** *If A is finite and there are bijections $f : A \to \{1, \dots, n\}$ and $g : A \to \{1, \dots, m\}$, then $n = m$.*

Proof. Suppose $m < n$. Then $g^{-1} : \{1, \dots, m\} \to A$ and $f : A \to \{1, \dots, n\}$ yield a bijection

$$f \circ g^{-1} : \{1, \dots, m\} \longrightarrow \{1, \dots, n\}.$$

Since $m < n$, the set $\{1, \dots, m\}$ is a proper subset of $\{1, \dots, n\}$, contradicting Theorem 1.57 applied to $A = \{1, \dots, n\}$. Similarly $n < m$ leads to a contradiction. Thus $n = m$. Diagrammatically:

$$\begin{tikzcd} A \arrow[r, "f", "\cong"'] \arrow[d, "g"', "\cong"] & \{1, \dots, n\} \\ \{1, \dots, m\} \arrow[ur, "f\circ g^{-1}"'] & \end{tikzcd}$$

□

From now on, for a finite A with a bijection to $\{1, \dots, n\}$, we can say that the cardinality of A is n. So in the finite case, the cardinality is no different from counting the number of elements.

1.5.2 Infinite sets

Corollary 1.59. *The set* $\mathbb{N} = \{1, 2, 3, \dots\}$ *is infinite.*

Proof. Consider the map $f : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ defined by $f(n) = n + 1$. This is a bijection onto the proper subset $\mathbb{N} \setminus \{1\}$. If $\mathbb{N}$ were finite, this would contradict Theorem 1.57. Hence $\mathbb{N}$ is not finite (i.e. infinite). □

Definition 1.60. A set A is

- *infinite* if it is not finite.
- *countably infinite* if it is in bijection with $\mathbb{N}$; in this case, we write $|A| = \aleph_0$.
- *countable* if it is either finite or countably infinite.
- *uncountable* if it is not countable.

Example 1.61. Now we try to compare $\mathbb{N}$ and $\mathbb{Z}$. We define a function $f\colon \mathbb{N} \to \mathbb{Z}$ as follows: we let $f(1) = 0$ and for $n \geq 0$,

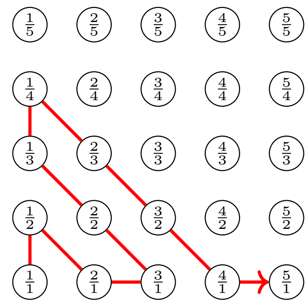
$$f(2n) = n, \qquad f(2n+1) = -n.$$

The enumeration is visualised below:

$$\begin{array}{lccccccccccc} \mathbb{N}: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots & 2i & 2i+1 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow \\ \mathbb{Z}: & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \cdots & i & -i \end{array}$$

Hence f is a bijection, so $|\mathbb{Z}| = \aleph_0$.

Example 1.62. The set of positive rational numbers $\mathbb{Q}_+$ is countably infinite. We can enumerate it as follows: Represent each rational number as a pair $(m, n) \in \mathbb{N}^2$ by the (not necessarily reduced) fraction m/n. Enumerate lattice points by successive anti-diagonals in a zig-zag (Cantor) pattern:



Skipping repetitions (keep only reduced fractions) we obtain an enumeration of $\mathbb{Q}_+$, i.e., an bijection from $\mathbb{Q}_+$ to $\mathbb{N}$. Therefore, $|\mathbb{Q}_+| = \aleph_0$.

Now let's see some criteria for countability.

Lemma 1.63. *Let $C \subset \mathbb{N}$ be infinite. Then C is countably infinite.*

Proof. Define $f : \mathbb{N} \to C$ inductively as follows: let $f(1) = \min C$. If $f(1), \ldots, f(n)$ have been defined, let $f(n+1) = \min(C \setminus \{f(1), \ldots, f(n)\})$.

f is injective: for $m < n$, $f(n) \in C \setminus \{f(1), \ldots, f(n-1)\}$, but $f(m)$ is not in the set. So, $f(n) \neq f(m)$.

f is surjective: for any $c \in C$, there exists $n \in \mathbb{N}$ such that $f(n) \geq c$. Let m be the smallest integer with $f(m) \geq c$. So for any $i < m$, $f(i) < c$. So $c \notin \{f(1), \ldots, f(m-1)\}$ and hence $f(m) \leq c$ by its definition. This implies that $f(m) = c$. □

The same proof can be used to prove the following result.

Proposition 1.64. *If A is infinite, then $|A| \geq \aleph_0$.*

Proof. Since A is infinite, so A is not empty and hence we can choose $\leq$ to make A well-ordered. We define a map $f : \mathbb{N} \to A$ inductive as follows: $f(1) = \min A$. If $f(1), \ldots, f(n)$ have been defined, let $f(n+1) = \min(A \setminus \{f(1), \ldots, f(n)\})$. Then, f is injective. So $|A| \geq \aleph_0$. □

Theorem 1.65. *For any nonempty A, the following are equivalent:*

1. *A is countable;*
2. *there exists a surjection $f : \mathbb{N} \to A$;*
3. *there exists an injection $g : A \to \mathbb{N}$.*

Proof. We prove the implications as follows:

(1) ⇒ (2) If A is countably finite, then there exists a bijection and hence surjection $f : \mathbb{N} \to A$. If A is finite, then the composition is what we need: $\mathbb{N} \to \{1, \ldots, n\} \to A$.

(2) ⇒ (3) If there exists a surjection $f : \mathbb{N} \to A$, then we can define an injection $g : A \to \mathbb{N}$ by $g(a) = \min\{n \in \mathbb{N} : f(n) = a\}$ for all $a \in A$.

(3) ⇒ (1) If there exists an injection $g : A \to \mathbb{N}$, then we can decompose this as $A \to im(g) \to \mathbb{N}$. If $im(g)$ is finite, then A is finite. If $im(g)$ is infinite, then by the lemma above, $im(g)$ is countably infinite and hence so is A.

□

Theorem 1.66. *The product of finitely many countable sets is countable.*

Instead of proving the general theorem, we show a special case.

Proposition 1.67. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Proof. We can define a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$f(m, n) = 2^m 3^n.$$

This function is injective, hence $\mathbb{N} \times \mathbb{N}$ is countable. Since $\mathbb{N} \times \mathbb{N}$ is obviously infinite, we have that $|\mathbb{N} \times \mathbb{N}| = \aleph_0$. □

As a consequence, we have that taking countable unions still cannot increase cardinality.

Theorem 1.68. *Let A_n be a countable set for each $n \in \mathbb{N}$. Then $\bigcup_n A_n$ is countable.*

Proof. Since A_n is countable, there is a surjection $f_n : \mathbb{N} \to A_n$. Define a function $f : \mathbb{N} \times \mathbb{N} \to \bigcup_n A_n$ by

$$f(m, n) = f_n(m).$$

This function is surjective, hence $\bigcup_n A_n$ is countable. □

How about the product of countably many countable sets?

Theorem 1.69. $\{0, 1\}^{\mathbb{N}}$ *is uncountable. So the countable product of countable sets need not be countable.*

Proof. Suppose $\{0, 1\}^{\mathbb{N}}$ were countable. Then we could list all infinite 0–1 sequences as

$$s^{(1)}, s^{(2)}, s^{(3)}, \ldots, \qquad s^{(k)} = (s_1^{(k)}, s_2^{(k)}, s_3^{(k)}, \ldots),\ s_n^{(k)} \in \{0, 1\}.$$

Define a new sequence $t = (t_1, t_2, \ldots)$ by flipping the diagonal bits:

$$t_n = 1 - s_n^{(n)} \quad (n \geq 1).$$

Then $t \in \{0, 1\}^{\mathbb{N}}$, but $t \neq s^{(k)}$ for every k because they differ in the k-th coordinate. This contradicts the assumption that the list was complete. Hence $\{0, 1\}^{\mathbb{N}}$ is uncountable. □