Math 330 - Additional Material
Student edition with proofs

Michael Fochler
Department of Mathematics
Binghamton University

This document contains $\boxed{\text{chapter 7}}$ of the Math 330 lecture notes.

Last update: February 17, 2026

Version: **2026-02-17**

Contents

7 Cardinality I: Finite and Countable Sets

Notation: In this entire chapter, if $n \in \mathbb{N}$, the symbol $[n]$ does not denote an equivalence class of any kind but the set $[1, n]_{\mathbb{Z}} = \{1, 2, \dots, n\}$ of the first n natural numbers. we further define $[0] := \emptyset$.

7.1 The Size of a Set

We stated in the preliminary definition of the size of a set (Definition **??** on p.**??**) that the size $|X|$ of a set X is the number of its elements. It is surprisingly difficult to make this definition precise. The following proposition will help us in this endeavor.

Proposition 7.1.

Let $n \in \mathbb{N}$. Let $\emptyset \neq A \subsetneq [n]$ be a proper, nonempty subset of $[n]$.

Then there is no surjection from A onto $[n]$.

PROOF: There is nothing to prove for $n = 1$, since the set $[1] = \{1\}$ does not strictly contain any sets other than the empty set. The proof for $n \geq 2$ will be done by induction on n.

Base case: Let $n = 2$. The only proper subsets of $[2]$ are the singleton sets $\{1\}$ and $\{2\}$. For any function $f : \{1\} \to [2]$ we have either $f(1) = 1$ in which case $2 \notin f(\{1\})$ or $f(1) = 2$ in which case $1 \notin f(\{1\})$. It follows in either case that f is not surjective. The proof for functions $\{2\} \to [2]$ is similar. This proves the base case.

(IA) Induction assumption: Let $n \in [3, \infty[_{\mathbb{Z}}$ such that the following holds:
If $\emptyset \neq \Gamma \subsetneq [n-1]$, then there is no surjection $\Gamma \to [n-1]$.

(a) We need to show the following: If $\emptyset \neq A \subsetneq [n]$, then there is no surjection from A to $[n]$.

(b) We assume to the contrary that a surjective $f : A \to [n]$ exists.

case 1: $n \notin A$**:**

Note that $n \notin A$ implies that $A \subseteq [n-1]$.

(c) Let $\Gamma := A \setminus \{f = n\}$.

Let $j \in [n]$. The domain of f is A; thus, $\{f = j\} \subseteq A$. Also, since f is surjective, $\{f = j\} \neq \emptyset$.

(d) It now follows from $\{f = j\} \subseteq A$ and $\{f = j\} \neq \emptyset$ that $A \cap \{f = j\} = \{f = j\} \neq \emptyset$.

It follows from **(d)** that $A \setminus \{f = n\} \subsetneq A$. By **(c)**, $\Gamma \subsetneq A$.

(e) We assumed tthat $A \subseteq [n-1]$. It follows from $\Gamma \subsetneq A$ that $\Gamma \subsetneq A \subseteq [n-1]$.

From $n \geq 3$ we obtain $n \neq 1$. Thus $\{f = 1\} \cap \{f = n\} = \emptyset$,

(f) Thus $\{f = 1\} \subseteq \{f = n\}^{\complement}$

(g) Thus, $\emptyset \overset{\textbf{(d)}}{\neq} A \cap \{f = 1\} \overset{\textbf{(f)}}{\subseteq} A \cap \{f = n\}^{\complement} = A \setminus \{f = n\} \overset{\textbf{(c)}}{=} \Gamma$.

(h) By **(e)** and **(g)**, $\emptyset \neq \Gamma \subsetneq A \subseteq [n-1]$. It follows that the induction assumption applies to Γ; hence there is no surjective $\psi : \Gamma \to [n-1]$.

(i) We will obtain a contradiction to the above and thus finish the proof of **case 1** by showing that if we restrict the domain of f to Γ and its codomain to $[n-1]$, then $f\big|_{\Gamma} : \Gamma \to [n-1]$ is surjective.

So let $y \in [n-1]$. Since f is surjective, there exists $x \in A$ such that $f(x) = y$.

Since $y \leq n-1$, $y \neq n$. Hence $x \notin \{f = n\}$. This and $x \in A$ and **(c)** implies that $x \in \Gamma$.

We found for arbitrary $y \in [n-1]$ some x in the domain of $f\big|_{\Gamma}$, hence this function is surjective. By **(i)**, this completes the proof of **case 1**.

case 2: $n \in A$**:**

Because $A \subsetneq [n]$ there exists $j \in [n-1]$ such that $j \notin A$. Let $A' := (A \setminus \{n\}) \uplus \{j\}$. It follows from prop.**??** on p.**??** that there is a bijection $g : A' \xrightarrow{\sim} A$. Note that $f \circ g : A' \to [n]$ is surjective, since this function is the composition of a surjection with a bijection (see cor.**??**.b on p.**??**).

But A' satisfies the conditions of **case 1** since $n \notin A'$, and we have already proven that such a surjection cannot exist. Again we have reached a contradiction. ■

Corollary 7.1.

The following contains B/G thm.13.4 and B/G cor.13.5. Let $m, n \in \mathbb{N}$.

(a) *If $m < n$ then there exists no surjective function $f : [m] \to [n]$.*
(b) *If $m > n$ then there exists no injective function $g : [m] \to [n]$. This is commonly referred to as the* ***pigeonhole principle****.*
(c) *If $m \neq n$ then there exists no bijective function $f : [m] \to [n]$.*
(d) *There exists no surjective function $h : [m] \to \mathbb{N}$.*

The proof of **(a)**–**(c)** is left as exercise 7.1 (see p.273). ■

PROOF of **(d)**: Clearly the function

$$\psi : \mathbb{N} \to [n+1]; \qquad m \mapsto \psi(m) := \begin{cases} m & \text{if } m \leq n+1, \\ 1 & \text{if } m > n+1 \end{cases}$$

is surjective. If there were a surjective function $h : [n] \to \mathbb{N}$ then $\psi \circ h : [n] \to [n+1]$ would be surjective by cor.**??(b)** on p.**??**. But we have established in part **(a)** of this corollary that no surjection $[n] \to [n+1]$ exists. ■

Remark 7.1.
The fact that there is no surjective function $[m] \to [n]$ if $m < n$ can be expressed as follows: If a flock of m pigeons flies toward n pigeonholes for shelter then not all of those pigeonholes will be occupied. The pigeonhole principle states the other side of the coin: If a flock of n pigeons flies toward m pigeonholes for shelter then at least one of those pigeonholes will be occupied by more than one pigeon. ☐

Cor.7.1 yields yet another important benefit: We can now make precise the preliminary definition **??** of the size of a set which was given on p.**??**, at the end of ch.**??** (Sets and Basic Set Operations).

Definition 7.1 (Finite and infinite sets)**.**

(a) Let $X \neq \emptyset$ and $n \in \mathbb{N}$ such that there is a bijective mapping $F : [n] \to X$. By Corollary 7.1**(c)**, n is uniquely defined by the property that $[n]$ can be bijected to X. This allows us to define n as the **size** of the set X. We write $\left|X\right| = n$.

(a) If we write x_j for $F(j)$, we see that X is of the form

$$X \;=\; F([n]) \;=\; \{F(j) : j \in [n]\} \;=\; \{x_j : j \in \mathbb{Z} \text{ and } 1 \leq j \leq n\}.$$

In other words, its elements can be enumerated as $x_1, x_2, \dots, x_n$. This is the mathematician's way of stating th

(b) We say that the empty set $\emptyset$ has size $\left|\emptyset\right| = 0$.

(c) We call a set X **finite**, if there exists $n \in [0, \infty[_{\mathbb{Z}}$ such that X has size n. Note that this implies that the empty set is finite. We say that X is **infinite** and we write $\left|X\right| = \infty$, if X is not finite.

As strange as this may seem, there are ways to classify the degree of infinity when looking at infinite sets. The "smallest degree of infinity" is found in sets that can be compared, in a sense, to the set $\mathbb{N}$ of all natural numbers. We have a special name for infinite sets whose elements can be mapped bijectively to $\mathbb{N}$.

(d) Let X be a set such that there is a bijection $f : \mathbb{N} \xrightarrow{\sim} X$. In other words, all of the elements of X can be arranged in a sequence $(x_n)_{n \in \mathbb{N}}$ such that

$$X \;=\; \{\, x_n : n \in \mathbb{N}, x_n = f(n) \,\}\,.$$

Then we call X a **countably infinite** set.

(e) We call a set that is either finite or countably infinite a **countable** set.

(f) A set that is not countable is called **uncountable**

(g) We use the phrase **"finitely many"** items, **"countably many"** items, **"infinitely many"** items, etc., if they would constitute a finite set, a countable set, an infinite set, etc. ☐

Example 7.1. Let $X := \{2n : n \in \mathbb{N}\}$ be the set of all even natural numbers. Then X is countably infinite because the function

$$f : \mathbb{N} \longrightarrow X;\quad n \mapsto 2n \qquad \text{has the function} \quad g : X \longrightarrow \mathbb{N};\quad k \mapsto \frac{k}{2}$$

as its inverse and hence is bijective.

Note that $\frac{k}{2}$ exists (as an integer) for all $k \in X$ since the even natural numbers are divisible by 2. ☐

Proposition 7.2.

A countably infinite set is infinite (and not finite).

Proof: Assume to the contrary that a set A is both finite and countably infinite. Thus we have bijections $g : A \xrightarrow{\sim} \mathbb{N}$ and, for a suitable $n \in \mathbb{N}$, $f : [n] \xrightarrow{\sim} A$. By cor.**??**.b on p.**??** the composition $g \circ f : [n] \xrightarrow{\sim} \mathbb{N}$ is bijective, thus surjective. This contradicts cor.7.1**(d)** on p.254. ■

Proposition 7.3.

Let X and Y be two nonempty sets with a bijection $f : X \xrightarrow{\sim} Y$. Then

(a) *Y is finite if and only if X is finite,*
(b) *Y is countably infinite if and only if X is countably infinite,*
(c) *Y is countable if and only if X is countable,*
(d) *Y is uncountable if and only if X is uncountable.*
(e) *$|Y| = |X|$.*

PROOF: The proof of **(a)**, **(b)** and **(e)** is based on prop.**??**.**(c)** on p.**??** which states that the composition of two bijective functions is bijective.

We only need to prove the " $\Rightarrow$" directions because we obtain " $\Leftarrow$" by switching the roles of X and Y.

PROOF of **(a)** and **(e)**. If X is finite then there exists $n \in \mathbb{N}$ and a bijection $g : X \xrightarrow{\sim} [n]$. $Y \xrightarrow{g \,\circ\, f^{-1}} [n]$ is bijective according to prop.**??**.**(c)** on p.**??**. This proves both that Y is finite and $|Y| = n = |X|$.

PROOF of **(b)**. If X is countably infinite then there exists a bijection $g : X \xrightarrow{\sim} \mathbb{N}$. Because $Y \xrightarrow{g \,\circ\, f^{-1}} \mathbb{N}$ is bijective, Y also is countably infinite.

PROOF of **(c)**. If X is countable then this set is either finite or countably infinite. If X is finite then Y is finite according to part **(a)**; if X is countably infinite then Y is countably infinite according to part **(b)**. This proves that Y is countable.

PROOF of **(d)**. Assume to the contrary that X is uncountable and Y is countable. It follows from part **(c)** that X is countable and we have reached a contradiction. Thus, Y is uncountable. ■

Proposition 7.4.

let A and B two mutually disjoint, finite sets. Then $A \uplus B$ is finite and

$$|A \uplus B| \ = \ |A| \ + \ |B| \,.$$

PROOF: There are $m, n \in \mathbb{N}$ such that $|A| = m$ and $|B| = n$, i.e., there exist bijections $\varphi : [1,m]_{\mathbb{Z}} \to A$ and $\psi : [1,n]_{\mathbb{Z}} \to B$. The function

$$f : [1,n]_{\mathbb{Z}} \to [m+1, m+n]_{\mathbb{Z}}; \qquad j \mapsto m+j$$

is a bijection since the function

$$g : [m+1, m+n]_{\mathbb{Z}} \to [1,n]_{\mathbb{Z}}; \qquad i \mapsto i-m$$

satisfies $g \circ f = id_{[1,n]_{\mathbb{Z}}}$ and $f \circ g = id_{[m+1,m+n]_{\mathbb{Z}}}$, and thus g is the inverse of f.

Thus the function $\psi \circ g$ is a bijection $[m+1, m+n]_{\mathbb{Z}} \xrightarrow{\sim} B$ as the composition of the two bijections g and ψ.

$$\begin{tikzcd}
{[1,n]_{\mathbb{Z}}} \arrow[r, "\psi"] & B \\
{[m+1,m+n]_{\mathbb{Z}}} \arrow[u, "g"] \arrow[ur, "\psi \circ g"'] &
\end{tikzcd}$$

Next, let $F : [1, m+n]_{\mathbb{Z}} \longrightarrow A \uplus B$ be defined as $F(k) \ := \begin{cases} \varphi(k) & \text{if}\, 1 \leq k \leq m, \\ \psi\big(g(k)\big) & \text{if}\, m+1 \leq k \leq m+n. \end{cases}$

We claim that F is bijective.

To prove injectivity we assume that $k, k' \in [1, m+n]_{\mathbb{Z}}$ such that $k \neq k'$. We separately examine the three cases $k, k' \leq m$, $k, k' > m$, and $k \leq m < k'$.

- **(a)** If $k, k' \leq m$ then $F(k) = \varphi(k) \neq \varphi(k') = F(k')$ since φ is injective.
- **(b)** If $k, k' > m$ then $F(k) = \psi\big(g(k)\big) \neq \psi\big(g(k')\big) = F(k')$ since $\psi \circ g$ is injective.
- **(c)** If $k \leq m < k'$ then $F(k) = \varphi(k) \in A$ and $F(k') = \psi\big(g(k')\big) \in B$. Since A and B are disjoint we conclude that $F(k) \neq F(k')$.

To prove surjectivity let $x \in A \uplus B$. Then

- **(a)** either $x \in A$, and the surjectivity of φ allows us to conclude that there exists $k \in [1,m]_{\mathbb{Z}}$ such that $\varphi(k) = x$, i.e., $F(k) = x$;
- **(b)** or $x \in B$, and there exists $k \in [m+1, m+n]_{\mathbb{Z}}$ such that $F(k) = \psi \circ g(k) = x$ since the function $\psi \circ g$ is surjective.

The existence of a bijection $F : [1, m+n]_{\mathbb{Z}} \xrightarrow{\sim} A \uplus B$ proves that $|A \uplus B| = m+n = |a| + |B|$. ■

The assertion of the next lemma is intuitively clear. If one adds a new element ω to X then one obtains for each existing $A \subseteq X$ an additional subset $A \cup \{\omega\}$ of $X \cup \{\omega\}$.

Lemma 7.1. *Let X, Ω be sets such that $X \subsetneq \Omega$ and $\omega \in X^{\complement}$, and let $\mathfrak{B} := \{A \uplus \{\omega\} : A \in 2^X\}$. Then the function $F : 2^X \to \mathfrak{B}$; $A \mapsto A \uplus \{\omega\}$ is a bijection.*

The proof is left as exercise **??** (see p.**??**). ■

Proposition 7.5.

Let $n \in \mathbb{Z}_{\geq 0}$. Let Ω be a set such that $|\Omega| = n$. Then its power set has size $|2^\Omega| = 2^n$.

PROOF:
The proof is done by induction on $n = |\Omega|$.

Base case $n = 0$: $|\Omega| = 0$ means that Ω is empty. Since $|\emptyset| = 0$ and $2^\emptyset = \{\emptyset\}$ has size $1 = 2^0$ the base case is proven.

Induction assumption: Let $n \in \mathbb{Z}_{\geq 0}$ such that $|2^Y| = 2^n$ for all sets Y such that $|Y| = n$. $(\star)$

Let $|\Omega| = n + 1$. We need to show that $|2^\Omega| = 2^{n+1}$. $(\star\star)$

Let $\omega \in \Omega$ and $X := \Omega \setminus \{\omega\}$. Let $\mathfrak{B} := \{A \uplus \{\omega\} : A \in 2^X\}$. Note that $2^\Omega = 2^X \cup \mathfrak{B}$ since 2^X contains all subsets A of Ω such that $\omega \notin A$, and $\mathfrak{B}$ contains all subsets B of Ω such that $\omega \in B$. This characterization of 2^X and $\mathfrak{B}$ also implies that subsets of Ω which are elements of 2^X do not belong to $\mathfrak{B}$ and vice versa, i.e., 2^X and $\mathfrak{B}$ are mutually disjoint, thus $2^\Omega = 2^X \uplus \mathfrak{B}$.

We obtain from lemma 7.1 on p.257 that there is a bijection $2^X \xrightarrow{\sim} \mathfrak{B}$, hence $|\mathfrak{B}| = |2^X|$.

It follows from $\Omega = X \uplus \{\omega\}$ and $|\{\omega\}| = 1$ and prop.7.4 on p.256 that

$$n + 1 = |\Omega| = |X| + |\{\omega\}| = |X| + 1, \quad \text{i.e.,} \quad |X| = n.$$

The induction assumption $(\star)$ thus applies to the set X, and it yields $|2^X| = 2^n$. We apply once more prop.7.4 to $2^\Omega = 2^X \uplus \mathfrak{B}$ and obtain

$$|2^\Omega| = |2^X \uplus \mathfrak{B}| = |2^X| + |\mathfrak{B}| = 2 \cdot 2^n = 2^{n+1}.$$

We have shown $(\star\star)$, and the proof by induction is completed. ■

7.2 The Subsets of $\mathbb{N}$ and Their Size

Proposition 7.6.

Let $\emptyset \neq A \subseteq \mathbb{N}$ and let $A_j \subseteq A$ and $a_j \in A$ $(j \in \mathbb{N})$ be recursively defined as follows.

$$A_1 := A, \qquad a_1 := \min(A_1); \tag{7.1}$$

$$A_{n+1} := A \setminus \{a_j : j \in \mathbb{N}, j \leq n\}; \qquad a_{n+1} := \begin{cases} \min(A_{n+1}) & \text{if } A_{n+1} \neq \emptyset, \\ a_n & \text{else.} \end{cases} \tag{7.2}$$

The following is true for all $i, j, n \in \mathbb{N}$.

- ***(a)*** *The sequence of sets $A_1, A_2, A_3 \dots$ is nonincreasing: if $i < j$ then $A_i \supseteq A_j$.*
- ***(b)*** *If $j < n$ and $A_n \neq \emptyset$ then $a_j < a_n$.*
- ***(c)*** *If $A_n \neq \emptyset$ then $a_n \geq n$.*
- ***(d)*** *Let $n \geq 2$. If $a \in A$ and $a < a_n$ then $a = a_j$ for some $j < n$.*
- ***(e)*** *Let $n \in \mathbb{N}$. There is no $a \in A$ such that $a_n < a < a_{n+1}$.*

(f) *If* $A_n = \emptyset$ *for some* $n \in \mathbb{N}$ *then* A *is bounded. Let* $K := \max\{j \in \mathbb{N} : A_j \neq \emptyset\}$. *Then* $\max(A) = a_K$.

Figure 7.1 illustrates this for the case $K = 4$. *Moreover,*

$$A = \{a_j : j \in \mathbb{N}, j \leq K\} = \{\min(A_j) : j \in \mathbb{N}, j \leq K\}, \tag{7.3}$$

$$\text{If } n \geq K \text{ then } a_n = a_K. \tag{7.4}$$

(g) *The sequence* $a_j : j \in \mathbb{N}$ *is nondecreasing: if* $i < j$ *then* $a_i \leq a_j$.

(h) *If* $A_n \neq \emptyset$ *for all* $n \in \mathbb{N}$ *then* A *is unbounded and*

$$A = \{a_j : j \in \mathbb{N}\} = \{\min(A_j) : j \in \mathbb{N}\}.$$

Figure 7.1: $K = 4$: $a_4 = \max(A)$.

PROOF of **(a)**: Let $i < j$. Then $\{a_k : k \in \mathbb{N}, k < i\} \subseteq \{a_k : k \in \mathbb{N}, k < j\}$, hence $A \setminus \{a_k : k \in \mathbb{N}, k < i\} \supseteq A \setminus \{a_k : k \in \mathbb{N}, k < j\}$, i.e., $A_i \supseteq A_j$.

PROOF of **(b)**: A_n is not empty and $j < n$, hence $A_j \supseteq A_n$, hence $A_j \neq \emptyset$. Thus $a_j = \min(A_j)$ and $a_n = \min(A_n)$. Since $a_j \in \{a_i : i \in \mathbb{N}, i \leq j\}$, it follows that $\min(A_j) = a_j \notin A_n$. We obtain from prop.**??(b)** on p.**??** that $\min(A_j) < \min(A_n)$, i.e., $a_j < a_n$.

PROOF of **(c)**: This is a simple proof by induction on n.

Base case $n = 1$: $A_1 = A \subseteq \mathbb{N}$, hence A_1 is not empty, hence $a_1 = \min(A_1) \geq \min(\mathbb{N}) = 1$ by prop.**??(a)**. This proves the base case.

Induction assumption: Assume that $A_n \neq \emptyset$ and $a_n \geq n$.

We must show that, if $A_{n+1} \neq \emptyset$, then $a_{n+1} \geq n + 1$. It follows from **(b)** that $a_n + 1 \leq a_{n+1}$ and from the induction assumption that $n + 1 \leq a_n + 1$. Thus $n + 1 \leq a_n + 1 \leq a_{n+1}$.

PROOF of **(d)**: We prove this by induction on n.

Base case $n = 2$: $a \in A = A_1$ and $a < a_2 = \min(A_2)$, hence $a \notin A_2$, hence $a \in A_1 \setminus A_2 = \{a_1\}$, hence $a = a_1$. This proves the base case.

Induction assumption: If $n > 2$ and $a \in A$ and $a < a_n$ then $a = a_j$ for some $j < n$.

We must show that if $a \in A$ and $a < a_{n+1}$ then $a = a_j$ for some $j < n + 1$. There are three cases.

Case 1: $a = a_n$. We may choose $j = n$ and we are done.

Case 2: $a < a_n$. The induction assumption implies that there is some $j < n < n + 1$ such that $a = a_j$ and we are done.

Case 3: $a_n < a < a_{n+1}$. We will show that this is not possible. Note that $a_n < a_{n+1}$ implies that A_{n+1} is not empty. Thus part **(b)** implies that $a_j < a_n < a$ for all $j \in [1, n[_{\mathbb{Z}}$, hence $a \neq a_i$ for all $i \in [1, n]_{\mathbb{Z}}$, hence $a \in A \setminus \{a_i : i \in \mathbb{N}, i \leq n\}$, i.e., $a \in A_{n+1}$. It follows that $a \geq a_{n+1}$, and we have reached a contradiction to the assumption $a_n < a < a_{n+1}$. This finishes the proof of **(d)**.

PROOF of **(e)**: If $a_n = a_{n+1}$ this is obviously true. If $a_n < a_{n+1}$ it follows from **(d)** that if $a \in A$ and $a < a_{n+1}$ then $a \leq a_n$. This proves **(e)**.

PROOF of **(f)**: Assume that $A_n = \emptyset$. It follows from **(a)** that A_j is empty for all $j > n$, hence n is an upper bound for the set $J = \{i \in \mathbb{N} : A_i \neq \emptyset\}$. It follows from thm.**??** (Generalization of the Well-Ordering Principle) on p.**??** that J has a maximum, which we denote by K. Note that it follows from $A_K \neq \emptyset$ and $A_{K+1} = \emptyset$ and (7.2) that $A \setminus \{a_j : j \in \mathbb{N}, j \leq K\} = A_{K+1} = \emptyset$. This proves 7.3 and also that $a_n = a_K = \min(A_K)$ for all $n \geq K$.

PROOF of **(g)**: We examine three cases separately. Let K be as defined in part **(f)**. If $i < j \leq K$ then $a_i < a_j$, according to **(b)**. If $K \leq i < j$ then $a_i = a_j$, according to (7.4). If $i < K < j$ then $a_i < a_K = a_j$, according to **(b)** and (7.4).

PROOF of **(h)**: Let $n \in \mathbb{N}$. From $A_n \neq \emptyset$ we obtain $a_n = \min(A_n)$. Also, $n \leq a_n$ by **(c)**.

$$\text{Thus } A_n \subseteq [a_n, \infty[_{\mathbb{Z}} \subseteq [n, \infty[_{\mathbb{Z}}, \quad \text{thus } \bigcap_{n \in \mathbb{N}} A_n \subseteq \bigcap_{n \in \mathbb{N}} [n, \infty[_{\mathbb{Z}} = \emptyset .$$

Let $B := A \setminus \{a_j : j \in \mathbb{N}\}$ By definition, $A_n = A \setminus \{a_j : j \in \mathbb{N}, j \leq n-1\}$.

Thus $B \subseteq A_n$ for all n, thus $B \subseteq \bigcap_{n \in \mathbb{N}} A_n$, thus $B = \emptyset$, thus $A = \{a_j : j \in \mathbb{N}\}$. This proves **(h)**. ■

Proposition 7.7.

Let A be a nonempty subset of $\mathbb{N}$. Let $A_j \subseteq A$ and $a_j \in A$ $(j \in \mathbb{N})$ be defined as in prop. 7.6 on p.258. Then

- *either $A_n \neq \emptyset$ for all $n \in \mathbb{N}$. In this case A is not bounded and there exists a bijection $\mathbb{N} \xrightarrow{\sim} A$. Further $A = \{a_n : n \in \mathbb{N}\}$*
- *or A_n is empty for some $n \in \mathbb{N}$. In this case A is bounded and there exists a bijection $[1, K]_{\mathbb{Z}} \xrightarrow{\sim} A$ for some suitable $K \in \mathbb{N}$. Further $A = \{a_n : n \in \mathbb{N}$ such that $1 \leq n \leq K\}$*

In both cases the integers a_n and a_{n+1} are adjacent for each index n in the sense that there is no $a \in A$ such that $a_n < a < a_{n+1}$.

PROOF: It is immediate that either **(a)** is true or **(b)** is true, since, either $A_n \neq \emptyset$ for all n or A_n is empty for some n. But we still must prove, e.g., that $A_n \neq \emptyset$ for all $n \in \mathbb{N}$ implies that A is not bounded and one can biject $\mathbb{N}$ to A.

PROOF of the statements in **(a)**: Let $F : \mathbb{N} \longrightarrow A$, defined by $F(n) = a_n$. It follows from prop.7.6**(c)** that no $n \in \mathbb{N}$ is an upper bound of A because $a_{n+1} \geq n+1 > n$. This proves that A is unbounded.

Let $n \in A$. We just saw that $a_{n+1} \geq n+1 > n$. It follows from prop.7.6**(d)** that there exists $j \in \mathbb{N}$ such that $F(j) = a_j = n$. This proves that F is surjective. Injectivity of F follows from prop.7.6**(b)**.

Since $F(n) = a_n$ for all $n \in \mathbb{N}$ we obtain $A = F(\mathbb{N}) = \{F(n) : n \in \mathbb{N}\} = \{a_n : n \in \mathbb{N}\}$. This proves **(a)**.

PROOF of the statements in **(b)**: Let

$$K := \max\{j \in \mathbb{N} : A_j \neq \emptyset\} .$$

Let $F : \{j \in \mathbb{N} : j \leq K\} \to A$, defined by $F(n) = a_n$. According to (7.3), $A = \{F(j) : j \in \mathbb{N}, j \leq K\}$, hence F is surjective. It follows from $A_K \neq \emptyset$ and prop.7.6**(b)** that

$$F(i) < F(j) \quad \text{whenever } 1 \leq i < j \leq K , \quad \text{hence, (i) } F \text{ is injective, and (ii), } F(K) = \max(A) .$$

Thus F is bijective, and bounded by 1 and $F(K)$. We have shown **(b)**.
Finally, the adjacency of a_n and a_{n+1} follows for both **(a)** and **(b)** from prop.7.6**(e)** ■

We extend the results of the last proposition to subsets of integers which are bounded below.

Proposition 7.8.

Let J be a nonempty set of integers which is bounded below.Then
- ***(a)*** *If J is bounded above then there exists $K \in \mathbb{N}$ and integers n_j $(1 \leq j \leq K)$ such that $J = \{n_j : 1 \leq j \leq K\}$.*
- ***(b)*** *If J is not bounded above then there exist integers n_j $(j \in \mathbb{N})$ such that $J = \{n_j : j \in \mathbb{N}\}$.*
- ***(c)*** *In both cases **(a)** and **(b)** the integers n_j satisfy $i < j \Rightarrow n_i < n_j$, and n_j and n_{j+1} are adjacent for each index j: There is no $n \in J$ such that $n_j < n < n_{j+1}$.*

PROOF: If $\min(J) \geq 1$, i.e., $J \subseteq \mathbb{N}$ then the above is a direct consequence of prop.7.7, so we may assume that $\min(J) \leq 0$. The function $n \mapsto n + 1 - \min(J)$ is a bijection $\varphi : J \xrightarrow{\sim} \varphi(J)$ since it has the function $m \mapsto m - 1 + \min(J)$ as its inverse. Further $\varphi(J) \subseteq \mathbb{N}$ since $n \in J \Rightarrow n \geq \min(J)$ we obtain $\varphi(n) \geq \varphi\big(\min(J)\big) = 1$ for all $n \in J$ and thus $\varphi(J) \subseteq \mathbb{N}$.
We apply prop.7.7 to $\varphi(J)$ and obtain

$$\text{either } \varphi(J) = \{m_j : 1 \leq j \leq K\} \text{ (case } \textbf{(a)}\text{)} \quad \text{or } \varphi(J) = \{m_j : j \in \mathbb{N}\} \text{ (case } \textbf{(b)}\text{)}$$

for suitable $m_j \in \varphi(J)$ and $K \in \mathbb{N}$ which satisfy the properties stated in **(2)**. We look at the inverse images $n_j := \varphi^{-1}(m_j)$ and obtain $J = \varphi^{-1}\big(\varphi(J)\big)$. Thus $J = \{n_j : 1 \leq j \leq K\}$ (case **(a)**) or $J = \{n_j : j \in \mathbb{N}\}$ (case **(b)**). We have proven parts **(a)** and **(b)** of the proposition.
We still need to prove **(c)**. Since the function φ^{-1} shifts its arguments by a constant number to the left, it follows that $i < j \Rightarrow n_i < n_j$. Finally, assume to the contrary that there exists some index j and $n \in J$ such that $n_j < n < n_{j+1}$. It follows that the φ–images satisfy $\varphi(n_j) < \varphi(n) < \varphi(n_{j+1})$, i.e., $m_j < \varphi(n) < m_{j+1}$. But $\varphi(n) \in \varphi(J)$, and this contradicts the adjacency of the m_j in $\varphi(J)$. ■

Notation 7.1 (Notation Alert for bounded below subsets of the integers)**.**

If J is a nonempty subset of the integers which is bounded below then the last proposition makes it natural to introduce the following notation:
- **(a)** If J is finite, i.e., bounded above and hence of the form $J = \{n_j : 1 \leq j \leq K\}$ then we also say that J consists of the numbers $n_1 < n_2 < ... < n_K$.
- **(b)** If J is infinite, i.e., not bounded above and hence of the form $J = \{n_j : j \in \mathbb{N}\}$ then we also say that J consists of the numbers $n_1 < n_2 < ....$ ☐

Proposition 7.9.

Let A be a nonempty, finite subset of $\mathbb{N}$. Then A is bounded.

The proof is left as exercise 7.3 (see p.273). ■

We will see later that the reverse also is true: Bounded subsets of $\mathbb{N}$ are finite. But first we must prove

Proposition 7.10.

Let $B \subseteq A \subseteq \mathbb{N}$ and assume that A is finite. Then B is finite.

The proof is left as exercise 7.4 (see p.273). ■

Theorem 7.1.

Let A be a nonempty subset of the natural numbers. Then

(a) *A is finite if and only if A is bounded,*
(b) *A is countably infinite if and only if A is not bounded.*
(c) *All subsets of $\mathbb{N}$ are countable.*

PROOF of **(a)**: It follows from prop.7.9 above that nonempty, finite subsets of $\mathbb{N}$ are bounded. We now prove the reverse. If A is bounded then $\max(A)$ exists according to the extended well-ordering principle (thm.**??** on p.**??**). A is a subset of the finite set $[\max(A)]$, hence A is finite according to the previous proposition. This proves **(a)**.

PROOF of **(b)**: First assume that A is countably infinite. It follows from **(a)** and prop.**??** ($\mathbb{N}$ is unbounded in $\mathbb{Z}$) on p.**??** that $\mathbb{N}$ is infinite, hence A is infinite according to prop.7.3**(a)** on p.256. We employ once more the already proven part **(a)** to conclude that A is not bounded.

Now assume that A is not bounded. Then A does not satisfy prop.7.7**(b)** above, hence A satifies prop.7.7**(a)**. Thus there exists a bijection $\mathbb{N} \xrightarrow{\sim} A$, i.e., A is countably infinite. This proves **(b)**.

PROOF of **(c)**: Either A is bounded or A is not bounded. In the first case it follows from **(a)** that A is finite, hence countable. In the second case it follows from **(b)** that A is countably infinite, hence countable. This proves **(c)**. ■

Theorem 7.2.

(a) *Let X be a finite set and $A \subseteq X$. Then A is finite.*
(b) *Let $X_1, X_2, \dots, X_n$ be finite sets. Then $\bigcup\limits_{j=1}^{n} X_j$ is finite.*

PROOF of **(a)**: We may assume that $A \neq \emptyset$ because the empty set is finite. Since X is finite there exists a bijection $\phi : X \to [1,n]_{\mathbb{Z}}$ for some suitable $n \in \mathbb{N}$. Consider $\phi\big|_A : A \to \phi(A)$, i.e., the restriction of ϕ to A with a codomain which is shrunken from $[1,n]_{\mathbb{Z}}$ to $\phi(A)$.

Then $\phi\big|_A$ is bijective according to prop.**??(a)** on p.**??**. Moreover, since $\phi(A) \subseteq [1,n]_{\mathbb{Z}}$, it follows from prop.7.10 above that $\phi(A)$ is finite. Since A is the bijective image $\left(\phi\big|_A\right)^{-1}\big(\phi(A)\big)$ of the finite set $\phi(A)$, It follows from prop.7.3**(a)** on p. 256 that $|A|$ is finite.

PROOF of **(b)**: We give the proof for $n = 2$. The proof for arbitrary $n \in \mathbb{N}$ is done by induction on n and left as an easy exercise.

Let $X := X_1 \cup X_2$ and $A := X_2 \setminus X_1$. Then $X := X_1 \uplus A$. Since $A \subseteq X_2$ and X_2 is finite, A is finite according to the already proven part **(a)**. By Proposition 7.4 on p.256, X is finite. ■

We saw in thm.7.1 on p.262 that subsets of the natural numbers are finite if they are bounded and that they are countably infinite otherwise. We had to establish that subsets of finite subsets are finite to extend this theorem to subsets of the integers.

Theorem 7.3.

Let A be a nonempty set of integers. Then

(a) *A is finite if and only if A is bounded,*

(b) *A is countably infinite if and only if A is not bounded.*

PROOF:

Part 1: bounded $\Rightarrow$ finite:

Let $A' := (1 - \min(A)) + A = \{a - \min(A) + 1 : a \in A\}$. Then $A' \subseteq \mathbb{N}$ and is bounded above by $\max(A) - \min(A) + 1$, hence bounded in $\mathbb{N}$, hence finite by thm.7.1 above. Moreover the function $a \mapsto a - \min(A) + 1$ is a bijection $A \xrightarrow{\sim} A'$, hence A is finite by prop.7.3**(a)** on p.256.

Part 2: not bounded above $\Rightarrow$ infinite:

Let $A' := A \cap \mathbb{N}$. If A has no upper bounds then neither does A'. It follows from thm.7.1 on p.262 that A' is not finite, and from prop.7.10 that A is not finite.

Part 3: not bounded below $\Rightarrow$ infinite:

Let $A' := -A = \{-m : m \in A\}$. The function $\varphi : x \mapsto -x$ is a bijection $A \xrightarrow{\sim} A'$ because it has $y \mapsto -y$ as an inverse. It follows from (**??**) on p.**??** that φ maps lower bounds of A to upper bounds of A', thus A' is not bounded above.

We have proven in part 2 that A' is not finite, hence its bijective image $A = \varphi^{-1}(A')$ is not finite. We are done with the proof of part 3. ■

Remark 7.2.

It follows from the above proposition that subsets of the integers are finite if and only if bounded and infinite otherwise. We will see in ch.7.4 (Countable Sets) that we also can extend thm.7.1**(c)** to the integers: All subsets of $\mathbb{Z}$ are countable. ☐

7.3 Finite Sequences and Subsequences and Eventually True Properties

Definition **??** (p.**??**) of ch.**??** (Relations, Functions and Families) gave the exact definition of sequences and subsequences, more precisely, only of infinite sequences and subsequences: We assumed there that the index set of a sequence $(x_n)_n$ was of the form $[n_\star, \infty[$ for some $n_\star \in \mathbb{Z}$, i.e., we assumed that the index set was not bounded above and hence infinite. Now that we understand the structure of the subsets of $\mathbb{Z}$ which are bounded below we are ready to study finite sequences and finite subsequences.

Definition 7.2 (Finite sequences)**.**

Let $n_\star, n^\star \in \mathbb{Z}$ such that $n_\star \leq n^\star$, let $J := [n_\star, n^\star]_{\mathbb{Z}}$. Then J is a finite set of integers since it is bounded below by $n_\star$ and above by $n^\star$. Let X be a nonempty set. We call an indexed family $(x_n)_{n\in J}$ in X with index set J a **finite sequence**. We write

$$(x_n)_{n_\star \leq n \leq n^\star} \quad \text{or} \quad (x_n)_{n=n_\star}^{n^\star} \quad \text{or} \quad x_{n_\star}, x_{n_\star+1}, \dots, x_{n^\star-1}, x_{n^\star} \quad \text{or} \quad (x_{n_\star}, x_{n_\star+1}, \dots, x_{n^\star-1}, x_{n^\star})$$

for such a finite sequence. We will sometimes call a sequence $(y_n)_{n=n_\star}^{\infty}$ an **infinite sequence** if we want to stress that its set of indices $[n_\star, \infty[$ is infinite.

If all members x_j of the finite sequence are (real) numbers then we also talk about a **vector** [1]of dimension $\big|[n_\star, n^\star]_{\mathbb{Z}}\big| = n^\star - n_\star + 1$. In this case we always must surround the members of that finite sequence with parentheses, and we will often use a symbol with "arrow notation"

$$\vec{x} \;=\; \big(x_1, x_2, x_3, \dots, x_{n-1}, x_n\big) \tag{7.5}$$

when working with such vectors. ☐

Example 7.2.

Here are some examples of finite sequences.

- **(a)** $\big(3.5, -97\pi, 4, \sqrt{8}\big)$ is both a finite sequence and a vector of dimension 4. We have $x_1 = 3.5,\ x_2 - 97\pi,\ x_3 = 4,\ x_4 = \sqrt{8}$.
- **(b)** $\big(3k+2\big)_{k=-2}^{3} \;=\; -4, -1, 2, 5, 8, 11 \;=\; \big(-4, -1, 2, 5, 8, 11\big)$ is both a finite sequence and a vector of size/dimension 6.
- **(c)** Joe, 5, -6.8, Dolores is a finite sequence of size 4. This is not a vector because not all of its members are numeric. ☐

Definition 7.3 (Finite subsequences)**.**

Assume that either $J := [n_\star, \infty[_{\mathbb{Z}}$ or $J := [n_\star, n^\star]_{\mathbb{Z}}$ ($n_\star, n^\star \in \mathbb{Z}$ and $n_\star \leq n^\star$). Let $(n_j)_{j=1}^{K} (K \in \mathbb{N})$ be a finite sequence of integers $n_j \in J$ such that $i < j \Rightarrow n_i < n_j$ for all $i, j \in \mathbb{N}$. Note that if $J = [n_\star, \infty[_{\mathbb{Z}}$ then $n_j \in J$ for all j implies $n_\star \leq n_1 < n_2 < \cdots < n_K$, and if $J = [n_\star, n^\star]_{\mathbb{Z}}$ then this implies $n_\star \leq n_1 < n_2 < \cdots < n_K \leq n^\star$.

---

[1] Vectors can be of a more general nature than just being a finite sequence of numbers. See ch.**??** (General Vector Spaces) on p.**??** (General Vector Spaces).

Let $(x_n)_{n \in J}$ be a sequence in a nonempty set X. We call $(x_{n_j})_{j=1}^K$ a **finite subsequence** of the original sequence since its index set $\{n_j : 1 \leq j \leq K\}$ is finite and we obtain $(x_{n_j})_{j=1}^K$ from $(x_n)_{n \in J}$ by omitting all members x_n for which there is no n_j which equals n. $\square$

Example 7.3. Let $y_k := 2k + 10$. Then $(y_k)_{k=-3}^2$ is the finite sequence $4, 6, 8, 10, 12, 14$. It is a finite subsequence not only of the finite sequences $(y_i)_{i=-10}^{10}$ and $(y_i)_{i=-5}^2$, but also of the (infinite) sequences $(y_m)_{m \geq -10}$ and $(y_j)_{j=-3}^\infty$. $\square$

Definition 7.4.

Let X be a nonempty set, $n_\star \in \mathbb{Z}$, $J := \{k \in \mathbb{Z} : k \geq n_\star\}$, and let $(x_n)_{n=n_\star}^\infty$ be a sequence in X. If the set of indices $n \in J$ for which a certain property does not hold is empty or bounded then we say that the sequence $(x_n)_n$ satisfies this property **eventually** or that it satisfies this property for **eventually all indices** n. $\square$

Remark 7.3.

The mathematical literature also uses the phrase "for **almost all indices** n". We prefer not to do so in the context of the last definition because "almost all" is of central importance in measure and probability theory, and it means something very different there. $\square$

Proposition 7.11.

We have the following equivalent ways to state that a sequence (x_n) satisfies a property P eventually:

(a) *There is $K \in J$ such that if P is false for some x_j then $j \leq K$.*
(b) *There is $K \in J$ such that P is true for all x_j such that $j > K$.*
(c) *The set of all indices j such that P is false for x_j is finite.*

PROOF: Let $F := \{j \in J : P \text{ is false for } x_j\}$ and $T := \{j \in J : P \text{ is true for } x_j\}$ Then Definition 7.4 states that $(x_n)_{n=n_\star}^\infty$ satisfies P eventually if and only if F is empty or bounded. If F is empty then $(x_n)_{n=n_\star}^\infty$ satisfies P eventually and each statement **(a)**, **(b)**, **(c)** is true, so the proposition is proven. We thus may assume that F is not empty. Then $(x_n)_{n=n_\star}^\infty$ satisfies P eventually if and only if F is bounded. Since F is always bounded below (by $n_\star$) we conclude that

$$\begin{aligned} & (x_n)_{n=n_\star}^\infty \text{ satisfies } P \text{ eventually} \Leftrightarrow F \text{ is bounded above} \\ \Leftrightarrow\ & \text{there exists } K \geq n_\star \text{ such that } \big[j > K \Rightarrow j \notin F\big] \\ \Leftrightarrow\ & \text{there exists } K \geq n_\star \text{ such that } \big[j \in F \Rightarrow j \leq K\big] \Leftrightarrow \textbf{(a)}. \end{aligned}$$

This proves the equivalence of Definition 7.4 and **(a)**.

Since the opposite of "there is $K \in J$ such that P is false for some x_j" is "there is $K \in J$ such that P is true for all x_j", and the opposite of "$j \leq K$" is "$j > K$" we conclude that **(a)** $\Leftrightarrow$ **(b)**.

By thm.7.3 on p.263 F is bounded (above) if and only if F is finite. Thus

$$\begin{aligned} \textbf{(a)} &\Leftrightarrow \text{ there exists } K \geq n_\star \text{ such that } \big[j \in F \Rightarrow j \leq K \big] \\ &\Leftrightarrow \text{ there exists } K \geq n_\star \text{ such that } F \subseteq [n_\star, K] \\ &\Leftrightarrow \text{ there exists } K \geq n_\star \text{ such that } F \text{ is bounded} \\ &\Leftrightarrow \text{ there exists } K \geq n_\star \text{ such that } F \text{ is finite } \Leftrightarrow \textbf{(c)}. \end{aligned}$$

This proves the proposition. ■

7.4 Countable Sets

In the last chapter we studied the sizes of subsets of natural numbers, and we were able to obtain a complete answer in the last theorem (thm.7.1): All subsets of $\mathbb{N}$ are countable, and they are finite if and only if they are bounded.

Most of the results in this chapter are for general sets and their subsets: No assumption is made about their nature. We may not deal with natural numbers or any other kind of numbers. They might, e.g., be sets of functions or sets of sets.

Now that we know from thm.7.1 on p.262 that all subsets of $\mathbb{N}$ are countable we are able to characterize countable sets by means of injective and surjective functions.

Proposition 7.12 (Countability Criterion)**.**

Let $X \neq \emptyset$.

The following are equivalent:
- ***(a)*** *X is countable.*
- ***(b)*** *There exists an injective function $f : X \to \mathbb{N}$.*
- ***(c)*** *There exists a surjective function $g : \mathbb{N} \to X$.*

Proof: It follows from thm.**??(c)** on p.**??** that **(b)** and **(c)** are equivalent, hence it suffices to show that **(a)** and **(b)** are equivalent.

PROOF of **(a)** $\Rightarrow$ **(b)**:

Case 1: If X is finite, then there exists $n \in \mathbb{N}$ and bijective $\varphi : X \xrightarrow{\sim} [1, n]_{\mathbb{Z}}$. Let

$$f : X \to \mathbb{N}; \qquad x \mapsto \varphi(x)$$

be the "same" function as φ, except that we enlarge the codomain to $\mathbb{N}$. f inherits injectivity from φ, and we are done.

Case 2: Otherwise, if X is infinite, i.e., countably infinite, there exists a bijective, hence injective, function $f : X \xrightarrow{\sim} \mathbb{N}$. We are done.

PROOF of **(b)** $\Rightarrow$ **(a)**:

We modify f by shrinking its codomain from $\mathbb{N}$ to the range $f(X)$ of f: Let

$$f' : X \to f(X); \qquad x \mapsto f(x).$$

Then f' inherits injectivity from f, and it also is surjective: If $k \in f(X)$ then there is, by definition of the direct image function, some $x_k \in X$ such that $f(x_k) = k$, i.e., $f'(x_k) = f(x_k) = k$. This proves surjectivity, hence bijectivity, of f'.

According to thm.7.1**(c)** on p.262 $f(X)$ is countable as a subset of $\mathbb{N}$ Since $f(X)$ is the codomain of the bijecttion f'. it follows from prop.7.3**(c)** on p.256 that X is countable. ■

Theorem 7.4.

Let X be a countable set and $A \subseteq X$. Then A is countable.

PROOF: If X is finite then A is finite by Theorem 7.2 on p.262, and we are done. So assume that X is countably infinite. Then there exists a bijection $\phi : \mathbb{N} \to X$. Let $Y := \mathbb{N}$.

Note that the inverse $\phi^{-1} : X \xrightarrow{\sim} Y$ of ϕ is bijective. Let $B := \{\phi^{-1}(a) : a \in A\}$, and let $f' : A \to B$ be defined by $f'(a) = \phi^{-1}(a)$ for all $a \in A$, i.e., f' is the restriction of ϕ^{-1} to A, with its codomain consisting of all function values of arguments in A. Then f' is bijective according to prop.**??(a)** on p.**??**. It follows from prop.7.3 on p. 256 that $|A| = |B|$.

Since $B \subseteq Y$ and $Y = \mathbb{N}$ we can apply thm.7.1 on p.262. It follows that B and hence A is countable. ■

Corollary 7.2.

(a) *subsets of countable sets are either finite or countably infinite.*
(b) *supersets of uncountable sets are uncountable.*
(c) *Supersets of infinite sets are infinite,*

The proof is left as exercise 7.6 (see p.273). ■

Proposition 7.13 (B/G prop.13.11)**.**

Every infinite set contains a proper subset that is countably infinite.

The proof is left as exercise 7.7 (see p.274). ■

Proposition 7.14 (B/G prop.13.12)**.**

A set is infinite if and only if it contains a proper subset that is countably infinite.

The proof is left as exercise **??** (see p.**??**). ■

The next proposition is a major stepping stone for proving that countable unions of countable sets are countable.

Proposition 7.15 (B/G Cor.13.16, p.122)**.**
$\mathbb{N}^2$ is countable.

PROOF: $\boxed{\star}$ Let $f : \mathbb{N} \to \mathbb{N}^2;\ k \mapsto (i,j) = f(k)$ be defined recursively as follows.

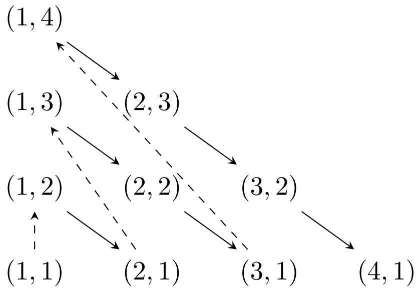
$$f(1) := (1,1); \tag{7.6}$$

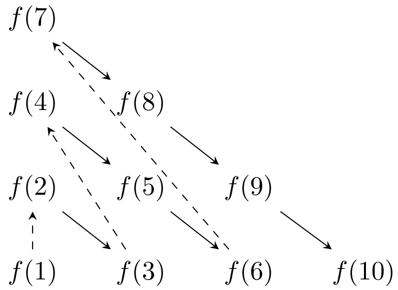
$$f(k+1) := \begin{cases} (i+1, j-1) \text{ if } f(k) = (i,j) \text{ and } j > 1, & \textbf{(a)} \\ (1,n)) \quad\quad\quad \text{ if } f(k) = (n-1,1). & \textbf{(b)} \end{cases} \tag{7.7}$$

We will show that f is surjective and injective. For $n \in \mathbb{N}, n \geq 2$, let $D_n := \{(i,j) \in \mathbb{N}^2 : i + j = n\}$. Then The "diagonals" D_n are mutually disjoint, and $\mathbb{N}^2 = \biguplus_{j=2}^{\infty} D_j$.

The following will help to visualize the definition of f. We think of $\mathbb{N}^2$ as a matrix with "infinitely many rows and columns". The left diagram below shows the points of $\mathbb{N}^2$ that belong to the diagonals $D_2, \dots D_5$ in their (x,y)–coordinate form, the one on the right shows them as images of the bijection $f : \mathbb{N} \to \mathbb{N}^2$.

Let $n := i + j$. Equation (7.7)**(a)** specifies that you march southeast on the diagonal D_n if you are not on the bottom row $j = 1$. Equation (7.7)**(b)** specifies that you move from the bottommost point $(n-1,1)$ of D_n to the uppermost point $(1,n)$ of the next diagonal, D_{n+1}.





Assume to the contrary that f is not surjective. Let $A := \{n \in \mathbb{Z}_{\geq 2} : D_n \setminus f(\mathbb{N}) \neq \emptyset\}$, i.e., A contains the indices of all diagonals that have at least one $(i,j) \in \mathbb{N}^2$ that is not a function value. A is not empty because f is not surjective, so it possesses, according to the well–ordering principle, a minimum $n_\star$. Note that $D_2 = \{f(1)\} \subseteq f(\mathbb{N})$, hence $2 \notin A$, hence $n_\star > 2$.

Let $B := \{i \in \mathbb{N} : 1 \leq i < n_\star \text{ and } (i, n_\star - i) \notin f(\mathbb{N})\}$. This is the set of all x–coordinates i of elements of $(i,j) \in D_{n_\star}$ which are not function values of f, and it is not empty because $n_\star \in A$. We apply the well–ordering principle to B and obtain a minimum $1 \leq i_\star < n_\star$.

Case 1: $i_\star \neq 1$. Then $(i_\star - 1, n - i_\star + 1) \in D_{n_\star}$ is a function value $f(k)$ for some $k \in \mathbb{N}$ because $i_\star$ is minimal in B. It follows from (7.7)**(a)** that $f(k+1) = (i_\star, n - i_\star)$. We have reached a contradiction because $i_\star \in B$, hence $(i_\star, n - i_\star)$ is not a function value.

Case 2: $i_\star = 1$. Then $(n_\star - 2, 1) \in D_{n_\star - 1}$ is a function value $f(k)$ for some $k \in \mathbb{N}$ because $n_\star - 1 \notin A$. It follows from (7.7)**(b)** that $f(k+1) = (1, n_\star - 1)$. We have reached a contradiction because $1 \in B$, hence $(1, n_\star - 1)$ is not a function value.

We have proven that f is surjective. We now prove injectivity. Let $k, k' \in \mathbb{N}$ such that $k \neq k'$. We may assume that $k < k'$. Let $i, j, i', j' \in \mathbb{N}$ such that $f(k) = (i,j)$ and $f(k') = (i', j')$. We must prove that $f(k) \neq f(k')$.

It follows from the surjectivity of f and $\mathbb{N}^2 = \biguplus\limits_{j=2}^{\infty} D_j$ that there exists (unique) $n, n' \in \mathbb{N}$ such that $f(k) \in D_n$ and $f(k') \in D_{n'}$. If $n \neq n'$ then $f(k) \neq f(k')$ because $D_n \cap D_{n'}$ and we are done.

So let us assume that $n = n'$. It follows from (7.7)**(a)** that $i' = i + (k' - k)$ and $j' = j - (k' - k)$, thus $f(k) = (i, j) \neq (i', j') = f(k')$. We have proven injectivity. ■

The proof of prop.7.15 above employs a bijection $f : \mathbb{N} \to \mathbb{N}^2$ which is constructed in a way that can be easily visualized. See the diagrams in the proof of prop.7.15. The drawback is that it was quite complicated to prove that f is in fact bijective. In the following we will construct a different bijection between $\mathbb{N}$ and $\mathbb{N}^2$.

We will first use the uniqueness of prime factorizations to decompose a natural number into a product of factors 2 and an odd number.

Proposition 7.16.

Let $n \in \mathbb{N}$. Then

- ***(a)*** *There exist unique $k \in \mathbb{Z}_{\geq 0}$ and $m \in \mathbb{N}$ such that m is odd and $n = 2^k m$.*
- ***(b)*** *If $n \neq 1$ then k is the number of times the factor 2 occurs in its prime factorization. Further, either m is the product of all other prime factors, or $m = 1$ if there are no prime factors different from 2.*

PROOF:

If $n = 1$ then the unique factorization $1 = 2^k m$ is obtained with $k = 0$ and $m = 1$. and we have shown both **(a)** and **(b)**.

If $n > 1$ then its unique prime factorization contains zero or more factors of 2. Let k be this number of factors. Let m be the product of all those prime factors of n which are not 2. Then $n = 2^k m$, and m is odd, because otherwise 2 would divide m and hence appear in the prime factorization of m. This proves the existence of the sought after representation, and k and m are precisely as was specified in **(b)**.

Note that we have established on the way that the prime factorization of m does not contain the number 2 as factors, and that the prime factorization of 2^k only contains the number 2.

We now prove uniqueness. Let $k' \in \mathbb{Z}_{\geq 0}$ and $m' \in \mathbb{N}$ such that m' is odd, and such that $n = 2^{k'} m'$. Because m' is odd, its prime factorization does not contain the number 2, and that of $2^{k'}$ only contains the number 2 as factors.

It follows that both m and m' contain exactly the prime factors of n which are not 2, and that both 2^k and $2^{k'}$ contain exactly those which equal 2.

We obtain that $m = m'$ and $k = k'$, and we have established uniqueness. ■

Lemma 7.2.

Lemma: *Let $n \in \mathbb{N}$. Then there exist unique $i, j \in [0, \infty[_{\mathbb{Z}}$ such that $n = 2^i (2j + 1)$.*

PROOF: According to prop.7.16 on p.269, there exists a unique pair $(i, m) \in [0, \infty[_{\mathbb{Z}} \times \mathbb{N}$ such that m is odd and

$$n = 2^i \cdot m \tag{7.8}$$

Moreover, it follows from Proposition **??** (B/G prop.6.15) on p.**??** that there exists $j \in \mathbb{Z}$ such that $m = 2j+1$. This integer j is unique for the following reason. Let $j' \in \mathbb{Z}$ such that $m = 2j'+1$. Then $0 = m - m = 2(j-j')$, thus $j = j'$ because there are no zero divisors in $\mathbb{Z}$.

The proof of the lemma is complete if we can prove that $j \geq 0$ and thus $j \in [0,\infty[_{\mathbb{Z}}$. But this is true since $m \in \mathbb{N}$, thus $m \geq 1$, thus $2j+1 \geq 1$, thus $j \geq 0$. ■

Proposition 7.17.

(a) *The function* $G : \big([0,\infty[_{\mathbb{Z}}\big)^2 \to \mathbb{N}$; $(i,j) \mapsto 2^i\,(2j+1)$ *is a bijection.*
(b) *The function* $F : \mathbb{N}^2 \to \mathbb{N}$; $(i,j) \mapsto 2^{i-1}\,(2j-1)$ *is a bijection.*

PROOF of **(a)**: Note that if $i,j \in [0,\infty[_{\mathbb{Z}}$ then the integers 2^i and $2j+1$ both are positive, hence $2^i(2j+1) \in \mathbb{N}$, hence the assignment $(i,j) \mapsto 2^i(2j+1)$ indeed defines a function with domain $\big([0,\infty[_{\mathbb{Z}}\big)^2$ and codomain $\mathbb{N}$. We must show that g is both injective and surjective.

According to the previous lemma any $n \in \mathbb{N}$ can be written as $n = 2^i\,(2j+1)$ for suitable $i,j \in [0,\infty[_{\mathbb{Z}}$. This proves surjectivity of G.

That lemma also showed that those numbers i and j are unique, thus G is injective.

PROOF of **(b)**: This is an immediate consequence of **(a)** since, if we denote the "even factor" of n

$$\begin{aligned} k = 2^{i-1} \text{ for some } i \in \mathbb{N} \quad &\Leftrightarrow \quad k = 2^i \text{ for some } i \in [0,\infty[_{\mathbb{Z}}\,, \\ m = 2j-1 \text{ for some } j \in \mathbb{N} \quad &\Leftrightarrow \quad m = 2j+1 \text{ for some } j \in [0,\infty[_{\mathbb{Z}}\,. \end{aligned}$$ ■

Theorem 7.5 (B/G prop.13.19: Countable unions of countable sets)**.**

The union of countably many countable sets is countable.

PROOF: Let the sets $A_1,\ A_2,\ A_3,\ \dots$ be countable and let $A := \bigcup_{k\in\mathbb{N}} A_k$. We may assume that at least one of those sets A_k is not empty: otherwise their union is empty, hence finite, hence countable, and we are done.

As each of those A_i which is not empty is countable, either A_i is finite and we have an $N_i \in \mathbb{N}$ and a bijective mapping $a_i(\cdot) : A_i \xrightarrow{\sim} [N_i]$, or A_i is countably infinite and we have a bijective mapping $a_i(\cdot) : A_i \xrightarrow{\sim} \mathbb{N}$. We will write $a_{(i,j)}$ for $a_i(j)$

We now define the function $f : A \to \mathbb{N}^2,\ a \mapsto (i_a, j_a)$ as follows: For each $a \in A$ let $I_a := \{i \in \mathbb{N} : a \in A_i\}$. Since $A := \bigcup_{k\in\mathbb{N}} A_k$, $I_a \neq \emptyset$ and hence has a minimum i_a. Since $a \in A_{i_a}$ and since sets do not contain duplicates of their elements, there is a unique index j_a such that $a = a_{(i_a,j_a)}$.

In other words, we have assigned to each $a \in A$ a unique pair $(i_a,j_a) \in \mathbb{N}^2$ such that $a = a_{(i_a,j_a)}$. This assignment $a \mapsto (i_a,j_a)$ defines a function $f : A \to \mathbb{N}^2$.

If $a, a' \in A$ such that $f(a) = f(a') = (i_a,j_a)$ then both a and a' occupy the same slot j_a in the same set A_{i_a}, hence $a = a'$, thus f is injective. We shrink the codomain of f from $\mathbb{N}^2$ to $f(A)$ and the assignment $a \mapsto (i_a,j_a)$ gives us a bijective function $F : A \xrightarrow{\sim} f(A)$.

$f(A)$ is a subset of the countable set $\mathbb{N}^2$. This proves the theorem because any subset of a countable set is countable (see prop.7.4 on p.267). ■

The following is an easy consequence of the above theorem.

Corollary 7.3.

Let the set X be uncountable and let $A \subseteq X$ be countable. Then the complement $A^{\complement}$ of A is uncountable.

The proof is left as exercise 7.5 (see p.273). ■

Here are two more corollaries to thm.7.5. Note that the one about the countability of $\mathbb{Z}$ also follows from Theorem 7.3 on p.263.

Corollary 7.4.

The set $\mathbb{Z}$ of all integers is countable.

PROOF: The set $-\mathbb{N}$ is countable because the function $n \mapsto -n$ is a bijection $\mathbb{N} \xrightarrow{\sim} -\mathbb{N}$, hence

$$Z \;=\; \mathbb{N} \,\cup\, (-\mathbb{N}) \,\cup\, \{0\}$$

is countable as the union of three countable sets. ■

Corollary 7.5.

The rational numbers are countable.

PROOF: Let $n \in \mathbb{N}$ and $Q_n \;:=\; \{\frac{m}{n} : m \in \mathbb{Z}\}$. Then $f_n : Q_n \to \mathbb{Z}$, $\frac{m}{n} \mapsto m$ is a bijection because it has as an inverse the function $m \mapsto \frac{m}{n}$. It follows from cor.7.4 that Q_n is countable. By thm.7.5, $\mathbb{Q} \;=\; \bigcup \big[Q_n : n \in \mathbb{N}\big]$ is countable as the union of countably many sets. ■

We saw in prop.7.15 that the cartesian product of the two countable factors $\mathbb{N}$ also is countable. The next theorem generalizes this considerably.

Theorem 7.6 (Finite Cartesians of countable sets are countable)**.**

The Cartesian product of finitely many countable sets is countable.

Proof by induction: Let $X := X_1 \times \cdots \times X_n$ We may assume that none of the factor sets X_j is empty: Otherwise the Cartesian is empty too and there is nothing to prove.

The proof is a triviality for $k = 1$. It is more instructive to choose $k = 2$ for the base case instead.

So let X_1, X_2 be two nonempty countable sets. We now prove that $X_1 \times X_2$ is countable.

For fixed $x_1 \in X_1$ the function $F_2 : X_2 \to \{x_1\} \times X_2; \quad x_2 \mapsto (x_1, x_2)$ is bijective because it has as an inverse the function $G_2 : \{x_1\} \times X_2 \to X_2; \quad (x_1, x_2) \mapsto x_2$. It follows that $\{x_1\} \times X_2$ is countable.

Hence $X_1 \times X_2 = \bigcup\limits_{x \in X_1} \{x_1\} \times X_2$ is countable according to thm.7.5 on p.270. We have proved the base case.

Our induction assumption is that $X_1 \times \cdots \times X_k$ is countable. We must prove that $X_1 \times \cdots \times X_{k+1}$ is countable. We can "identify"

$$X_1 \times \cdots \times X_{k+1} = (X_1 \times \cdots \times X_k) \times X_{k+1} \tag{7.9}$$

by means of the bijection $(x_1, \ldots, x_n, x_{n+1}) \mapsto \big((x_1, \ldots, x_n), x_{n+1}\big)$. According to the induction assumption the set $X_1 \times \cdots \times X_k$ is countable.

The proof for the base case shows that $X_1 \times \cdots \times X_{k+1}$ as the Cartesian product of the two sets $X_1 \times \cdots \times X_k$ and X_{k+1} is countable. This finishes the proof of the induction step. ■

Corollary 7.6.

Let $n \in \mathbb{N}$. The sets $\mathbb{Q}^n$ and $\mathbb{Z}^n$ are countable.

PROOF: This follows from the preceding theorem because the sets $\mathbb{Q}$ and $\mathbb{Z}$ are countable. ■

We will examine uncountable sets in ch.**??** (Cardinality II: Comparing Uncountable Sets), but we will state a result here concerning a very important example of an uncountable set. The proof of the next theorem is very similar to the proof that the real numbers are uncountable. (See thm.**??** on p.**??**.)

Theorem 7.7.

Let X be a set which contains at least two elements. Then $X^{\mathbb{N}} = \{(x_n)_{n\in\mathbb{N}} : x_j \in X \ \forall j \in \mathbb{N}\}$ (the set of all sequences with values in X) is uncountable.

PROOF: Let $a, b \in X$ such that $a \neq b$. We will prove that the subset $A := \{a, b\}^{\mathbb{N}}$ of X is uncountable.

A certainly is not finite since it contains for each $n \in \mathbb{N}$ the sequence $\vec{y}_n = (y^n_j)_{j\in\mathbb{N}}$ which is defined by $y^n_j := a$ if $n \neq j$, $y^n_n := b$. If A were finite then its subset $B := \{\vec{y}_n : n \in \mathbb{N}\}$ also would have to be finite. (See thm.7.4 on p.267.) But B is countably infinite since $n \mapsto \vec{y}_n$ defines a bijection $\mathbb{N} \xrightarrow{\sim} B$. This proves that A is not finite. We are done if we can prove that A also is not countably infinite.

So assume to the contrary that A is countably infinite, i.e., there exist $\vec{x}_1, \vec{x}_2, \dots \in A$ such that $A = \{\vec{x}_n : n \in \mathbb{N}\}$. Note that each $\vec{x}_n$ itself is a sequence $(x^n_j)_{j\in\mathbb{N}}$ in which each member x^n_j is either a or b. We will reach a contradiction by constructing some $\vec{x} \in A$ which is different from $\vec{x}_n$ for each $n \in \mathbb{N}$ since this implies that $\vec{x} \notin A$.

We will obtain such $\vec{x} = (x_j)_{j \in \mathbb{N}}$ by ensuring that each x_j will be different from the diagonal element x_j^j of the infinite grid to the right. Let

$$x_j \ := \begin{cases} a & \text{if } x_j^j = b, \\ b & \text{otherwise.} \end{cases}$$

$$\begin{array}{r|cccccc} \vec{x_1}: & \boxed{x_1^1} & x_2^1 & x_3^1 & x_4^1 & \dots \\ \vec{x_2}: & x_1^2 & \boxed{x_2^2} & x_3^2 & x_4^2 & \dots \\ \vec{x_3}: & x_1^3 & 3_2^2 & \boxed{x_3^3} & x_4^3 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

Clearly $\vec{x} \in A$ since $A = \{a, b\}^{\mathbb{N}}$ contains any sequence whose members are either a or b. Note that $\vec{x} \neq \vec{x_1}$ since those two sequences differ in their first elements x_1 and x_1^1. Further $\vec{x} \neq \vec{x_2}$ since those two sequences differ in their second elements x_2 and x_2^2. We see that for any $j \in \mathbb{N}$ it is true that $\vec{x} \neq \vec{x_j}$ since those two sequences differ in their j–th elements x_j and x_j^j. It follows from $A = \{\vec{x}_n : n \in \mathbb{N}\}$ that $\vec{x} \notin A$. The assumption that A is countably infinite has allowed us to construct some $\vec{x}$ such that both $\vec{x} \in A$ and $\vec{x} \notin A$. We have reached a contradiction. ■

7.5 Exercises for Ch.7

Exercise 7.1.

Prove the following parts of cor.7.1 on p.254 of this document:

- **(a)** If $m < n$ then there exists no surjective function $f : [1, m]_{\mathbb{Z}} \to [1, n]_{\mathbb{Z}}$.
- **(b)** If $m > n$ then there exists no injective function $g : [1, m]_{\mathbb{Z}} \to [1, n]_{\mathbb{Z}}$.
- **(c)** If $m \neq n$ then there exists no bijective function $f : [1, m]_{\mathbb{Z}} \to [1, n]_{\mathbb{Z}}$. □

Exercise 7.2.

Prove lemma.7.1 on p.257 of this document: Let X, Ω be sets such that $X \subseteq \Omega$ and $\omega \in X^{\complement}$, and let $\mathfrak{B} := \{A \uplus \{\omega\} : A \in 2^X\}$.

Then the function $F : 2^X \to \mathfrak{B};\ A \mapsto A \uplus \{\omega\}$ is a bijection. □

Exercise 7.3.

Prove prop.7.9 on p.262 of this document: Let A be a nonempty, finite subset of $\mathbb{N}$. Then A is bounded. □

Exercise 7.4.

Prove prop.7.10 on p.262 of this document: Let $B \subseteq A \subseteq \mathbb{N}$ and assume that A is finite. Then B is finite. □

Exercise 7.5.

Prove cor.7.3 on p.271 of this document:

If X is uncountable and $A \subseteq X$ is countable then $A^{\complement}$ is uncountable. □

Exercise 7.6.

Prove cor.7.2 on p.267 of this document:

- **(a)** subsets of countable sets are either finite or countably infinite.
- **(b)** supersets of uncountable sets are uncountable.
- **(c)** Supersets of infinite sets are infinite, □

Exercise 7.7.

Prove prop.7.13 on p.267 of this document: Every infinite set contains a proper subset that is countably infinite. ☐

Exercise 7.8.

Prove prop.7.14 on p.267 of this document: A set is infinite if and only if it contains a proper subset that is countably infinite. ☐

References

List of Symbols

$\vec{x}$ – vector, 264

$[n] = \{1, 2, \ldots, n\}$, 253
$|X|$ – size of a set , 255

Index