CS1231 Chapter 4

Sets

4.1 Basics

Definition 4.1.1. (1) A *set* is an unordered collection of objects.

(2) These objects are called the *members* or *elements* of the set.

(3) Write
$x \in A$ for x is an element of A;
$x \notin A$ for x is not an element of A;
$x, y \in A$ for x, y are elements of A;
$x, y \notin A$ for x, y are not elements of A; etc.

(4) We may read $x \in A$ also as "x is in A" or "A *contains* x (as an element)".

Warning 4.1.2. Some use "contains" for the subset relation, but in this module we do *not*.

Symbol	Meaning	Examples	Non-examples
$\mathbb{N}$	the set of all natural numbers	$0, 1, 2, 3, 31 \in \mathbb{N}$	$-1, \frac{1}{2} \notin \mathbb{N}$
$\mathbb{Z}$	the set of all integers	$0, 1, -1, 2, -10 \in \mathbb{Z}$	$\frac{1}{2}, \sqrt{2} \notin \mathbb{Z}$
$\mathbb{Q}$	the set of all rational numbers	$-1, 10, \frac{1}{2}, -\frac{7}{5} \in \mathbb{Q}$	$\sqrt{2}, \pi, \sqrt{-1} \notin \mathbb{Q}$
$\mathbb{R}$	the set of all real numbers	$-1, 10, -\frac{3}{2}, \sqrt{2}, \pi \in \mathbb{R}$	$\sqrt{-1}, \sqrt{-10} \notin \mathbb{R}$
$\mathbb{C}$	the set of all complex numbers	$-1, 10, -\frac{3}{2}, \sqrt{2}, \pi, \sqrt{-1}, \sqrt{-10} \in \mathbb{C}$	
$\mathbb{Z}^+$	the set of all positive integers	$1, 2, 3, 31 \in \mathbb{Z}^+$	$0, -1, -12 \notin \mathbb{Z}^+$
$\mathbb{Z}^-$	the set of all negative integers	$-1, -2, -3, -31 \in \mathbb{Z}^-$	$0, 1, 12 \notin \mathbb{Z}^-$
$\mathbb{Z}_{\geqslant 0}$	the set of all non-negative integers	$0, 1, 2, 3, 31 \in \mathbb{Z}_{\geqslant 0}$	$-1, -12 \notin \mathbb{Z}_{\geqslant 0}$

$\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{Q}_{\geqslant m}$, $\mathbb{R}^+$, $\mathbb{R}^-$, $\mathbb{R}_{\geqslant m}$, etc. are defined similarly.

Table 4.1: Common sets

Note 4.1.3. Some define $0 \notin \mathbb{N}$, but in this module we do *not*.

Definition 4.1.4 (roster notation)**.** (1) The set whose only elements are $x_1, x_2, \ldots, x_n$ is denoted $\{x_1, x_2, \ldots, x_n\}$.

(2) The set whose only elements are $x_1, x_2, x_3, \ldots$ is denoted $\{x_1, x_2, x_3, \ldots\}$.

Example 4.1.5. (1) The only elements of $A = \{1, 5, 6, 3, 3, 3\}$ are 1, 5, 6 and 3. So $6 \in A$ but $7 \notin A$.

(2) The only elements of $B = \{0, 2, 4, 6, 8, \dots\}$ are the non-negative even integers. So $4 \in B$ but $5 \notin B$.

To check whether an object z is an element of a set $S = \{x_1, x_2, \dots, x_n\}$. If z is in the list $x_1, x_2, \dots, x_n$, then $z \in S$, else $z \notin S$.

☜ **Definition 4.1.6** (set-builder notation)**.** Let U be a set and $P(x)$ be a predicate over U. Then the set of all elements $x \in U$ such that $P(x)$ is true is denoted

$$\{x \in U : P(x)\} \quad \text{or} \quad \{x \in U \mid P(x)\}.$$

This is read as "the set of all x in U such that $P(x)$".

Example 4.1.7. (1) The elements of $C = \{x \in \mathbb{Z}_{\geqslant 0} : x \text{ is even}\}$ are precisely the elements of $\mathbb{Z}_{\geqslant 0}$ that are even, i.e., the non-negative even integers. So $6 \in C$ but $7 \notin C$.

(2) The elements of $D = \{x \in \mathbb{Z} : x \text{ is a prime number}\}$ are precisely the elements of $\mathbb{Z}$ that are prime numbers, i.e., the prime integers. So $7 \in D$ but $9 \notin D$.

To check whether an object z is an element of $S = \{x \in U : P(x)\}$. If $z \in U$ and $P(z)$ is true, then $z \in S$, else $z \notin S$. Hence $z \notin U$ implies $z \notin S$, and $P(z)$ is false implies $z \notin S$.

☜ **Definition 4.1.8** (replacement notation)**.** Let A be a set and $t(x)$ be a term in a variable x. Then the set of all objects of the form $t(x)$ where x ranges over the elements of A is denoted

$$\{t(x) : x \in A\} \quad \text{or} \quad \{t(x) \mid x \in A\}.$$

This is read as "the set of all $t(x)$ where $x \in A$".

Example 4.1.9. (1) The elements of $E = \{x + 1 : x \in \mathbb{Z}_{\geqslant 0}\}$ are precisely those $x + 1$ where $x \in \mathbb{Z}_{\geqslant 0}$, i.e., the positive integers. So $1 = 0 + 1 \in E$ but $0 \notin E$.

(2) The elements of $F = \{x - y : x, y \in \mathbb{Z}_{\geqslant 0}\}$ are precisely those $x - y$ where $x, y \in \mathbb{Z}_{\geqslant 0}$, i.e., the integers. So $-1 = 1 - 2 \in F$ but $\sqrt{2} \notin F$.

To check whether an object z is an element of $S = \{t(x) : x \in A\}$. If there is an element $x \in A$ such that $t(x) = z$, then $z \in S$, else $z \notin S$.

☜ **Definition 4.1.10.** Two sets are *equal* if they have the same elements, i.e., for all sets A, B,

$$A = B \quad \Leftrightarrow \quad \forall z \, (z \in A \Leftrightarrow z \in B).$$

Convention 4.1.11. In mathematical definitions, people often use "if" between the term being defined and the phrase being used to define the term. This is the *only* situation in mathematics when "if" should be understood as a (special) "if and only if".

Example 4.1.12. $\{1, 5, 6, 3, 3, 3\} = \{1, 5, 6, 3\} = \{1, 3, 5, 6\}$.

Slogan 4.1.13. Order and repetition do not matter.

Example 4.1.14. $\{y^2 : y \text{ is an odd integer}\} = \{x \in \mathbb{Z} : x = y^2 \text{ for some odd integer } y\}$
$= \{1^2, 3^2, 5^2, \dots\}$.

Example 4.1.15. $\{x \in \mathbb{Z} : x^2 = 1\} = \{1, -1\}$.

Proof. ($\Rightarrow$) Take any $z \in \{x \in \mathbb{Z} : x^2 = 1\}$. Then $z \in \mathbb{Z}$ and $z^2 = 1$. So

$$\begin{aligned} & z^2 - 1 = (z - 1)(z + 1) = 0. \\ \therefore \quad & z - 1 = 0 \quad \text{or} \quad z + 1 = 0. \\ \therefore \quad & z = 1 \quad \text{or} \quad z = -1. \end{aligned}$$

This means $z \in \{1, -1\}$.

($\Leftarrow$) Take any $z \in \{1, -1\}$. Then $z = 1$ or $z = -1$. In either case, we have $z \in \mathbb{Z}$ and $z^2 = 1$. So $z \in \{x \in \mathbb{Z} : x^2 = 1\}$. □

Exercise 4.1.16. Write down proofs of the claims made in Example 4.1.9. In other words, prove that $E = \mathbb{Z}^+$ and $F = \mathbb{Z}$, where E and F are as defined in Example 4.1.9. 4a

Theorem 4.1.17. There exists a unique set with no element, i.e.,

- there is a set with no element; and (existence part)
- for all sets A, B, if both A and B have no element, then $A = B$. (uniqueness part)

Proof.

- (existence part) The set $\{\}$ has no element.
- (uniqueness part) Let A, B be sets with no element. Then vacuously,

$$\forall z\ (z \in A \Rightarrow z \in B) \quad \text{and} \quad \forall z\ (z \in B \Rightarrow z \in A)$$

because the hypotheses in the implications are never true. So $A = B$. □

Definition 4.1.18. The set with no element is called the *empty set*. It is denoted by $\varnothing$.

4.2 Subsets

Definition 4.2.1. Let A, B be sets. Call A a *subset* of B, and write $A \subseteq B$, if

$$\forall z\ (z \in A \Rightarrow z \in B).$$

Alternatively, we may say that B *includes* A, and write $B \supseteq A$ in this case.

Note 4.2.2. We avoid using the symbol $\subset$ because it may have different meanings to different people.

Example 4.2.3. (1) $\{1, 5, 2\} \subseteq \{5, 2, 1, 4\}$ but $\{1, 5, 2\} \not\subseteq \{2, 1, 4\}$.

(2) $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Remark 4.2.4. Let A, B be sets.

(1) $$A \not\subseteq B \quad \Leftrightarrow \quad \exists z\ (z \in A \text{ and } z \notin B).$$

(2) $$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ and } B \subseteq A.$$

(3) $$A \subseteq A.$$

Definition 4.2.5. Let A, B be sets. Call A a *proper subset* of B, and write $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$. In this case, we may say that the inclusion of A in B is *proper* or *strict*.

Example 4.2.6. All the inclusions in Example 4.2.3 are strict.

Proposition 4.2.7. The empty set is a subset of any set, i.e., for any set A,

$$\varnothing \subseteq A.$$

Proof. Vacuously,

$$\forall z\ (z \in \varnothing \Rightarrow z \in A)$$

because the hypothesis in the implication is never true. So $\varnothing \subseteq A$ by the definition of $\subseteq$. □

Note 4.2.8. Sets can be elements of sets.

Example 4.2.9. (1) The set $A = \{\varnothing\}$ has exactly 1 element, namely the empty set. So A is not empty.

(2) The set $B = \{\{1\}, \{2, 3\}\}$ has exactly 2 elements, namely $\{1\}$, $\{2, 3\}$. So $\{1\} \in B$, but $1 \notin B$.

Note 4.2.10. Membership and inclusion can be different.

Question 4.2.11. Let $C = \{\{1\}, 2, \{3\}, 3, \{\{4\}\}\}$. Which of the following are true? 4b

- $\{1\} \in C$.
- $\{1\} \subseteq C$.
- $\{2\} \in C$.
- $\{2\} \subseteq C$.
- $\{3\} \in C$.
- $\{3\} \subseteq C$.
- $\{4\} \in C$.
- $\{4\} \subseteq C$.

Definition 4.2.12. Let A be a set. The set of all subsets of A, denoted $\mathcal{P}(A)$, is called the *power set* of A.

Example 4.2.13. (1) $\mathcal{P}(\varnothing) = \{\varnothing\}$.

(2) $\mathcal{P}(\{1\}) = \{\varnothing, \{1\}\}$.

(3) $\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

(4) The following are subsets of $\mathbb{Z}_{\geqslant 0}$ and thus are elements of $\mathcal{P}(\mathbb{Z}_{\geqslant 0})$.

$$\varnothing, \{0\}, \{1\}, \{2\}, \ldots \{0, 1\}, \{0, 2\}, \{0, 3\} \ldots \{1, 2\}, \{1, 3\}, \{1, 4\} \ldots$$
$$\{2, 3\}, \{2, 4\}, \{2, 5\} \ldots \{0, 1, 2\}, \{0, 1, 3\}, \{0, 1, 4\}, \ldots$$
$$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \ldots \{2, 3, 4\}, \{2, 3, 5\}, \{2, 3, 6\}, \ldots$$
$$\mathbb{Z}_{\geqslant 0}, \mathbb{Z}_{\geqslant 1}, \mathbb{Z}_{\geqslant 2}, \ldots \{0, 2, 4, \ldots\}, \{1, 3, 5, \ldots\}, \{2, 4, 6, \ldots\}, \{3, 5, 7, \ldots\}, \ldots$$
$$\{x \in \mathbb{Z}_{\geqslant 0} : (x-1)(x-2) < 0\}, \{x \in \mathbb{Z}_{\geqslant 0} : (x-2)(x-3) < 0\}, \ldots$$
$$\{3x + 2 : x \in \mathbb{Z}_{\geqslant 0}\}, \{4x + 3 : x \in \mathbb{Z}_{\geqslant 0}\}, \{5x + 4 : x \in \mathbb{Z}_{\geqslant 0}\}, \ldots$$

4.3 Boolean operations

Definition 4.3.1. Let A, B be sets.

(1) The *union* of A and B, denoted $A \cup B$, is defined by

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

Read $A \cup B$ as "A union B".

(2) The *intersection* of A and B, denoted $A \cap B$, is defined by

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Read $A \cap B$ as "A intersect B".

(3) The *complement* of B in A, denoted $A - B$ or $A \setminus B$, is defined by

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

Read $A \setminus B$ as "A minus B".

Convention and terminology 4.3.2. When working in a particular context, one usually works within a fixed set U which includes all the sets one may talk about, so that one only needs to consider the elements of U when proving set equality and inclusion (because no other object can be the element of a set). This U is called a *universal set*.

Definition 4.3.3. Let B be a set. In a context where U is the universal set (so that implicitly $U \supseteq B$), the *complement* of B, denoted $\overline{B}$ or B^{c}, is defined by

$$\overline{B} = U \setminus B.$$

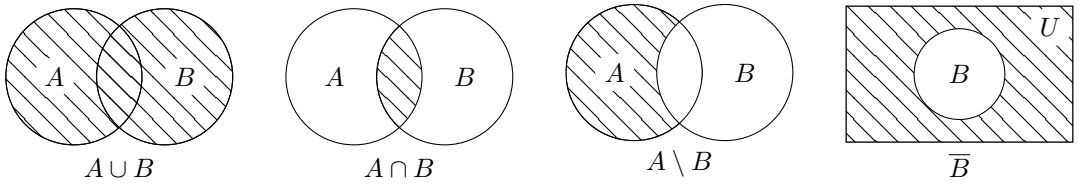


Figure 4.2: Boolean operations on sets

Example 4.3.4. Let $A = \{x \in \mathbb{Z} : x \leqslant 10\}$ and $B = \{x \in \mathbb{Z} : 5 \leqslant x \leqslant 15\}$. Then

$$\begin{aligned} A \cup B &= \{x \in \mathbb{Z} : (x \leqslant 10) \vee (5 \leqslant x \leqslant 15)\} = \{x \in \mathbb{Z} : x \leqslant 15\}; \\ A \cap B &= \{x \in \mathbb{Z} : (x \leqslant 10) \wedge (5 \leqslant x \leqslant 15)\} = \{x \in \mathbb{Z} : 5 \leqslant x \leqslant 10\}; \\ A \setminus B &= \{x \in \mathbb{Z} : (x \leqslant 10) \wedge \sim(5 \leqslant x \leqslant 15)\} = \{x \in \mathbb{Z} : x < 5\}; \\ \overline{B} &= \{x \in \mathbb{Z} : \sim(5 \leqslant x \leqslant 15)\} = \{x \in \mathbb{Z} : (x < 5) \vee (x > 15)\}, \end{aligned}$$

in a context where $\mathbb{Z}$ is the universal set. To show the first equation, one shows

$$\forall x \in \mathbb{Z} \quad \big((x \leqslant 10) \vee (5 \leqslant x \leqslant 15) \Leftrightarrow (x \leqslant 15)\big), \qquad \text{etc.}$$

Theorem 4.3.5 (Set Identities)**.** For all set A, B, C in a context where U is the universal set, the following hold.

Commutativity	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associativity	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Idempotence	$A \cup A = A$	$A \cap A = A$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Identities	$A \cup \varnothing = A$	$A \cap U = A$
Annihilators	$A \cup U = U$	$A \cap \varnothing = \varnothing$
Complement	$A \cup \overline{A} = U$	$A \cap \overline{A} = \varnothing$
Double Complement Law	$\overline{(\overline{A})} = A$	
Top and bottom	$\overline{\varnothing} = U$	$\overline{U} = \varnothing$
Set difference	$A \setminus B = A \cap \overline{B}$	

One of De Morgan's Laws. Work in the universal set U. For all sets A, B,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Venn Diagrams. In the left diagram below, hatch the regions representing A and B with ⧅ and ⧄ respectively. In the right diagram below, hatch the regions representing $\overline{A}$ and $\overline{B}$ with ⧅ and ⧄ respectively.

Then the □ region represents $\overline{A \cup B}$ in the left diagram, and the ⧆ region represents $\overline{A} \cap \overline{B}$ in the right diagram. Since these regions occupy the same region in the respective diagrams, we infer that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Note 4.3.6. This argument depends on the fact that each possibility for membership in A and B is represented by a region in the diagram.

Proof using a truth table. The rows in the following table list all the possibilities for an element $x \in U$:

$x \in A$	$x \in B$	$x \in A \cup B$	$x \in \overline{A \cup B}$	$x \in \overline{A}$	$x \in \overline{B}$	$x \in \overline{A} \cap \overline{B}$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Since the columns under "$x \in \overline{A \cup B}$" and "$x \in \overline{A} \cap \overline{B}$" are the same, for any $x \in U$,

$$x \in \overline{A \cup B} \quad \Leftrightarrow \quad x \in \overline{A} \cap \overline{B}$$

no matter in which case we are. So $\overline{A \cup B} = \overline{A} \cap \overline{B}$. □

Direct proof. Let $z \in U$. Then

$$\begin{array}{lcll} & z \in \overline{A \cup B} & \\ \Leftrightarrow & z \notin A \cup B & \text{by the definition of } \overline{\cdot}; \\ \Leftrightarrow & \sim\big((z \in A) \vee (z \in B)\big) & \text{by the definition of } \cup; \\ \Leftrightarrow & (z \notin A) \wedge (z \notin B) & \text{by De Morgan's Laws for propositions;} \\ \Leftrightarrow & (z \in \overline{A}) \wedge (z \in \overline{B}) & \text{by the definition of } \overline{\cdot}; \\ \Leftrightarrow & z \in \overline{A} \cap \overline{B} & \text{by the definition of } \cap. \end{array}$$ □

Example 4.3.7. Under the universal set U, show that $(A \cap B) \cup (A \setminus B) = A$ for all sets A, B.

Proof.
$$\begin{array}{lll} (A \cap B) \cup (A \setminus B) = (A \cap B) \cup (A \cap \overline{B}) & & \text{by the properties of set difference;} \\ = A \cap (B \cup \overline{B}) & & \text{by distributivity;} \\ = A \cap U & & \text{by the properties of set complement;} \\ = A & & \text{as } U \text{ is the identity for } \cap. \end{array}$$ □

Example 4.3.8. Show that $A \cap B \subseteq A$ for all sets A, B.

Proof. By the definition of $\subseteq$, we need to show that

$$\forall z \; (z \in A \cap B \Rightarrow z \in A).$$

Let $z \in A \cap B$. Then $z \in A$ and $z \in B$ by the definition of $\cap$. In particular, we know $z \in A$, as required. □

Question 4.3.9. Is the following true? 4c

$$(A \setminus B) \cup (B \setminus C) = A \setminus C \quad \text{for all sets } A, B, C.$$

4.4 Russell's Paradox

Example 4.4.1. (1) $\varnothing \notin \varnothing$.

(2) $\mathbb{Z} \notin \mathbb{Z}$.

(3) $\{\varnothing\} \notin \{\varnothing\}$.

Question 4.4.2. Is there a set x such that $x \in x$? 4d

Theorem 4.4.3 (Russell 1901)**.** There is no set R such that

$$\forall x \ (x \in R \quad \Leftrightarrow \quad x \notin x). \tag{$*$}$$

In words, there is no set R whose elements are precisely the sets x that are not elements of themselves.

Proof. We prove this by contradiction. Suppose R is a set satisfying ($*$). Applying ($*$) to $x = R$ gives

$$R \in R \quad \Leftrightarrow \quad R \notin R. \tag{$\dagger$}$$

Split into two cases.

- Case 1: assume $R \in R$. Then $R \notin R$ by the $\Rightarrow$ part of ($\dagger$). This contradicts our assumption that $R \in R$.
- Case 2: assume $R \notin R$. Then $R \in R$ by the $\Leftarrow$ part of ($\dagger$). This contradicts our assumption that $R \notin R$.

In either case, we get a contradiction. So the proof is finished. □

Question 4.4.4 (tongue-in-cheek)**.** Can you write a proof of Theorem 4.4.3 that does not mention contradiction? 4e

CS1231 Chapter 5

Relations

5.1 Basics

Definition 5.1.1. An *alphabet* is a finite set of symbols. A *string* over an alphabet Γ is a finite sequence of symbols from Γ. The set of all strings over an alphabet Γ is denoted Γ^*.

Definition 5.1.2. An *ordered pair* is an expression of the form

$$(x, y).$$

Let (x_1, y_1) and (x_2, y_2) be ordered pairs. Then

$$(x_1, y_1) = (x_2, y_2) \qquad \Leftrightarrow \qquad x_1 = x_2 \quad \text{and} \quad y_1 = y_2.$$

Example 5.1.3. (1) $(1, 2) \neq (2, 1)$, although $\{1, 2\} = \{2, 1\}$.

(2) $(3, 0.5) = (\sqrt{9}, \frac{1}{2})$.

Definition 5.1.4. Let A, B be sets. The *Cartesian product* of A and B, denoted $A \times B$, is defined to be

$$\{(x, y) : x \in A \text{ and } y \in B\}.$$

Read $A \times B$ as "A cross B".

Example 5.1.5. $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

Definition 5.1.6. Let A, B be sets.

(1) A *relation* from A to B is a subset of $A \times B$.

(2) Let R be a relation from A to B and $(x, y) \in A \times B$. Then we may write

$$x \; R \; y \text{ for } (x, y) \in R \quad \text{and} \quad x \not R \; y \text{ for } (x, y) \notin R.$$

We read "$x \; R \; y$" as "x is R-*related* to y" or simply "x is *related* to y".

Example 5.1.7. Let $\Gamma = \{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}, 0, 1, 2, \ldots, 9\}$ and $\Phi = \{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}, \mathrm{a}, \mathrm{b}, \ldots, \mathrm{z}\}$. As in Figure 5.1, define

$$SN = \{(001\mathrm{R}, \text{Gates}), (012\mathrm{B}, \text{Brin}), (062\mathrm{E}, \text{Bezos}), (126\mathrm{N}, \text{Ma}), (254\mathrm{E}, \text{Zuckerberg})\}.$$

Then SN is a relation from Γ^* to Φ^*.

identity	
Student ID	name
001R	Gates
012B	Brin
062E	Bezos
126N	Ma
254E	Zuckerberg

$$SN = \{ \text{(001R, Gates)}, \text{(012B, Brin)}, \text{(062E, Bezos)}, \text{(126N, Ma)}, \text{(254E, Zuckerberg)} \}$$

is enrolled in	
Student ID	module
126N	CS3234
254E	CS3234
001R	MA2001
012B	MA2001
062E	MA2001
126N	MA2001
012B	MU2109
001R	PC2130
062E	PL3103
254E	PL3103

$$SM = \{ \text{(126N, CS3234)}, \text{(254E, CS3234)}, \text{(001R, MA2001)}, \text{(012B, MA2001)}, \text{(062E, MA2001)}, \text{(126N, MA2001)}, \text{(012B, MU2109)}, \text{(001R, PC2130)}, \text{(062E, PL3101)}, \text{(254E, PL3101)} \}$$

progress		
Student ID	faculty	year
062E	Arts	1
254E	Arts	2
012B	Science	2
001R	Science	1
126N	Science	3

$$SFY = \{ \text{(062E, Arts, 1)}, \text{(254E, Arts, 2)}, \text{(012B, Science, 2)}, \text{(001R, Science, 1)}, \text{(126N, Science, 3)} \}$$

teaching			
module	department	faculty	instructor
CS3234	CS	Computing	Turing
MA2001	Mathematics	Science	Gauss
MU2109	Music	Arts	Mozart
PC2130	Physics	Science	Newton
PL3101	Psychology	Arts	Freud

$$MDFI = \{ \text{(CS3234, CS, Computing, Turing)}, \text{(MA2001, Mathematics, Science, Gauss)}, \text{(MU2109, Music, Arts, Mozart)}, \text{(PC2130, Physics, Science, Newton)}, \text{(PL3101, Psychology, Arts, Freud)} \}$$

The set $\{SM, SN, SFY, MDFI\}$ represents the relational database.

Figure 5.1: A fictitious miniature university database and its set-theoretic representation

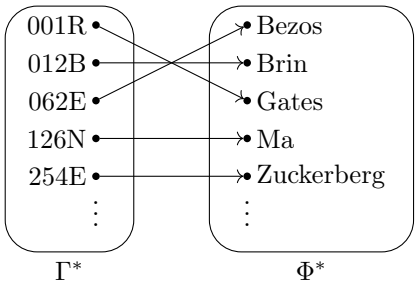
Example 5.1.8. Let $A = \{0, 1, 2\}$ and $B = \{1, 2, 3, 4\}$. Define the relation R from A to B by setting

$$x \; R \; y \quad \Leftrightarrow \quad x < y.$$

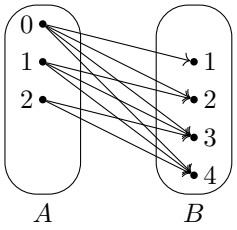
Then $0 \; R \; 1$ and $0 \; R \; 2$, but $2 \not R \; 1$. Thus

$$R = \{(0, 1), (0, 2), (0, 3), (0, 4), (1, 2), (1, 3), (1, 4), (2, 3), (2, 4)\}.$$

Arrow diagrams (for relations from a set to another set). One can use the figure below to represent the relation SN in Example 5.1.7, where the existence of an arrow from x to y indicates x is related to y.



Similarly, one can use the figure below to represent the relation R in Example 5.1.8.



Definition 5.1.9. Let $n \in \{x \in \mathbb{Z} : x \geqslant 2\}$. An *ordered n-tuple* is an expression of the form

$$(x_1, x_2, \ldots, x_n).$$

Let $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ be ordered n-tuples. Then

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \quad \Leftrightarrow \quad x_1 = y_1 \text{ and } x_2 = y_2 \text{ and } \ldots \text{ and } x_n = y_n.$$

Example 5.1.10. (1) $(1, 2, 5) \neq (2, 1, 5)$, although $\{1, 2, 5\} = \{2, 1, 5\}$.

(2) $(3, (-2)^2, 0.5, 0) = (\sqrt{9}, 4, \frac{1}{2}, 0)$

Definition 5.1.11. Let $n \in \{x \in \mathbb{Z} : x \geqslant 2\}$ and $A_1, A_2, \ldots, A_n$ be sets. The *Cartesian product* of $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$, is defined to be

$$\{(x_1, x_2, \ldots, x_n) : x_1 \in A_1 \text{ and } x_2 \in A_2 \text{ and } \ldots \text{ and } x_n \in A_n\}.$$

If A is a set, then $A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{-many } A\text{'s}}$.

Example 5.1.12. $\{0, 1\} \times \{0, 1\} \times \{x, y\} = \{(0, 0, x), (0, 0, y), (0, 1, x), (0, 1, y), (1, 0, x), (1, 0, y), (1, 1, x), (1, 1, y)\}$.

Definition 5.1.13. Let $n \in \{x \in \mathbb{Z} : n \geqslant 2\}$ and $A_1, A_2, \ldots, A_n$ be sets. A *n-ary relation over* $A_1, A_2, \ldots, A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$.

Example 5.1.14. Following Example 5.1.7, let $\Gamma = \{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}, 0, 1, 2, \ldots, 9\}$ and $\Phi = \{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}, \mathrm{a}, \mathrm{b}, \ldots, \mathrm{z}\}$. As in Figure 5.1, define

$$\begin{aligned} \mathit{MDFI} = \{&(\mathrm{CS3234}, \mathrm{CS}, \mathrm{Computing}, \mathrm{Turing}), (\mathrm{MA2001}, \mathrm{Mathematics}, \mathrm{Science}, \mathrm{Gauss}), \\ &(\mathrm{MU2109}, \mathrm{Music}, \mathrm{Arts}, \mathrm{Mozart}), (\mathrm{PC2130}, \mathrm{Physics}, \mathrm{Science}, \mathrm{Newton}), \\ &(\mathrm{PL3101}, \mathrm{Psychology}, \mathrm{Arts}, \mathrm{Freud})\}. \end{aligned}$$

Then MDFI is a 4-ary relation over $\Gamma^*, \Phi^*, \Phi^*, \Phi^*$.

5.2 Operations on relations

Figure 5.2: Relation composition and inversion

Definition 5.2.1. Let R be a relation from A to B, and S be a relation from B to C. Then $S \circ R$ is the relation from A to C defined by

$$S \circ R = \{(x, z) \in A \times C : (x, y) \in R \text{ and } (y, z) \in S \text{ for some } y \in B\}.$$

We read $S \circ R$ as "S composed with R" or "S circle R".

Note 5.2.2. We compose two binary relations together only when there is a common middle set.

Definition 5.2.3 (recall)**.** The *floor* of a real number x, denoted $\lfloor x \rfloor$, is the greatest integer that is less than or equal to x.

Example 5.2.4. Define a relation R from $\mathbb{Q}_{\geqslant 0}$ to $\mathbb{Z}_{\geqslant 0}$ and a relation S from $\mathbb{Z}_{\geqslant 0}$ to $\mathbb{R}$ by:

$$R = \{(x, y) \in \mathbb{Q}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0} : \lfloor x \rfloor = y\}, \quad \text{and}$$
$$S = \{(y, z) \in \mathbb{Z}_{\geqslant 0} \times \mathbb{R} : y = z^2\}.$$

- $(4.8, 2) \in S \circ R$ because $4 \in \mathbb{Z}_{\geqslant 0}$ such that $(4.8, 4) \in R$ and $(4, 2) \in S$.
- $(5/2, -\sqrt{2}) \in S \circ R$ because $2 \in \mathbb{Z}_{\geqslant 0}$ such that $(5/2, 2) \in R$ and $(2, -\sqrt{2}) \in S$.

In general, we have $S \circ R = \{(x, z) \in \mathbb{Q}_{\geqslant 0} \times \mathbb{R} : \lfloor x \rfloor = z^2\}$.

Definition 5.2.5. Let R be a relation from A to B. Then the *inverse of* R is the relation R^{-1} from B to A defined by

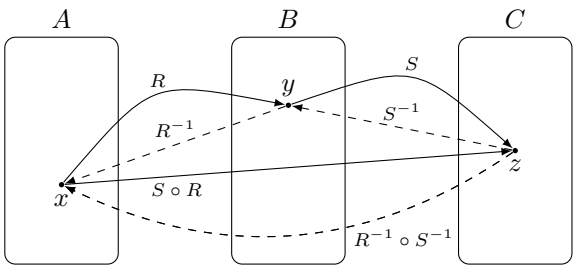
$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}.$$

Example 5.2.6. As in Example 5.1.8, let R be the relation from A to B where

$$A = \{0, 1, 2\}, \qquad B = \{1, 2, 3, 4\},$$
$$R = \{(0, 1), (0, 2), (0, 3), (0, 4), (1, 2), (1, 3), (1, 4), (2, 3), (2, 4)\}.$$

Then $R^{-1} = \{(1, 0), (2, 0), (3, 0), (4, 0), (2, 1), (3, 1), (4, 1), (3, 2), (4, 2)\}$.

Proposition 5.2.7. Let R be a relation from A to B, and S be a relation from B to C. Then $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.



Proof. Since $S \circ R$ is a relation from A to C, we know $(S \circ R)^{-1}$ is a relation from C to A. Since S^{-1} is a relation from C to B, and R^{-1} is a relation from B to A, we know $R^{-1} \circ S^{-1}$ is a relation from C to A as well. Now for all $(z, x) \in C \times A$,

$$\begin{aligned}
&(z,x) \in (S \circ R)^{-1} && \Leftrightarrow \quad (x,z) \in S \circ R && \text{by the definition of inverses;}\\
&\Leftrightarrow && (x,y) \in R \text{ and } (y,z) \in S \text{ for some } y \in B && \text{by the definition of composition;}\\
&\Leftrightarrow && (y,x) \in R^{-1} \text{ and } (z,y) \in S^{-1} \text{ for some } y \in B && \text{by the definition of inverses;}\\
&\Leftrightarrow && (z,x) \in R^{-1} \circ S^{-1} && \text{by the definition of composition.}
\end{aligned}$$

So $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. □

Exercise 5.2.8. Let $A = \{0, 1, 2\}$. Define two relations R, S from A to A by: 5a

$$R = \{(x, y) \in A^2 : x < y\} \quad \text{and} \quad S = \{(0, 1), (1, 2), (2, 0)\}.$$

Is $R \circ S = S \circ R$? Prove that your answer is correct.

5.3 Graphs

Definition 5.3.1. A *(binary) relation on a set* A is a relation from A to A.

Remark 5.3.2. It follows from Definition 5.1.6 and Definition 5.3.1 that the relations on a set A are precisely the subsets of $A \times A$.

Definition 5.3.3. A *directed graph* is an ordered pair (V, D) where V is a set and D is a binary relation on V. In the case when (V, D) is a directed graph,

(1) the *vertices* or the *nodes* are the elements of V;

(2) the *edges* are the elements of D;

(3) an edge *from* x *to* y is the element $(x, y) \in D$;

(4) a *loop* is an edge from a vertex to itself.

Example 5.3.4. Let

$$\begin{aligned}
V &= \{\mathrm{B}, \mathrm{P}, \mathrm{F}, \mathrm{M}, \mathrm{K}, \mathrm{N}\}, \quad \text{and}\\
D &= \{(\mathrm{B}, \mathrm{P}), (\mathrm{P}, \mathrm{B}), (\mathrm{F}, \mathrm{M}), (\mathrm{M}, \mathrm{F}), (\mathrm{B}, \mathrm{B}), (\mathrm{P}, \mathrm{P}), (\mathrm{F}, \mathrm{F}), (\mathrm{M}, \mathrm{M}), (\mathrm{K}, \mathrm{K}), (\mathrm{N}, \mathrm{N})\}.
\end{aligned}$$

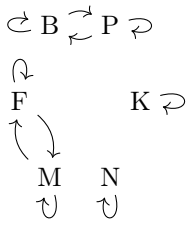
Then (V, D) is a directed graph.

Arrow diagrams (for relations on a set). One can draw an arrow diagram representing a relation R on a set A as follows.

(1) Draw all the elements of A.

(2) For all $x, y \in A$, draw an arrow from x to y if and only if $x \, R \, y$.

Example 5.3.5. The arrow diagram



represents the relation D on the set V from Example 5.3.4.

Definition 5.3.6. An *undirected graph* is an ordered pair (V, E) where V is a set and E is a set all of whose elements are of the form $\{x, y\}$ with $x, y \in V$. In the case when (V, E) is an undirected graph,

(1) the *vertices* or the *nodes* are the elements of V;

(2) the *edges* are the elements of E;

(3) an edge *between* x *and* y is the element $\{x, y\} \in E$;

(4) a *loop* is an edge between a vertex and itself.

Example 5.3.7. Following Example 5.3.5, define

$$V = \{\mathrm{B}, \mathrm{P}, \mathrm{F}, \mathrm{M}, \mathrm{K}, \mathrm{N}\}, \quad \text{and}$$
$$E = \{\{\mathrm{B}, \mathrm{P}\}, \{\mathrm{F}, \mathrm{M}\}, \{\mathrm{B}, \mathrm{B}\}, \{\mathrm{P}, \mathrm{P}\}, \{\mathrm{F}, \mathrm{F}\}, \{\mathrm{M}, \mathrm{M}\}, \{\mathrm{K}, \mathrm{K}\}, \{\mathrm{N}, \mathrm{N}\}\}.$$

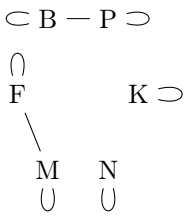
Then (V, E) is an undirected graph.

Drawings of an undirected graph. One can make a drawing representing an undirected graph (V, E) as follows:

(1) Draw all the elements of V.

(2) For all $x, y \in A$, draw a line between x and y if and only if $\{x, y\} \in E$.

Example 5.3.8. Here is a drawing of the undirected graph from Example 5.3.7.



CS1231 Chapter 6

Equivalence relations and partial orders

6.1 Partitions

Definition 6.1.1. Call $\mathscr{C}$ a *partition* of a set A if

(0) $\mathscr{C}$ is a set of *nonempty* subsets of A;

(1) every element of A is in some element of $\mathscr{C}$; and

(2) if two elements of $\mathscr{C}$ have a nonempty intersection, then they are equal.

Elements of a partition are called *components* of the partition.

Remark 6.1.2. One can rewrite the three conditions in the definition of partitions respectively as follows:

(0) $\forall S \in \mathscr{C} \;\; (\varnothing \neq S \subseteq A)$;

(1) $\forall x \in A \;\; \exists S \in \mathscr{C} \;\; (x \in S)$;

(2) $\forall S_1, S_2 \in \mathscr{C} \;\; (S_1 \cap S_2 \neq \varnothing \Rightarrow S_1 = S_2)$.

Yet another way to formulate this is to say that $\mathscr{C}$ is a set of mutually disjoint nonempty subsets of A whose union is A.

Example 6.1.3. One partition of the set $A = \{1, 2, 3\}$ is $\{\{1\}, \{2, 3\}\}$. The others are

$$\{\{1\}, \{2\}, \{3\}\}, \quad \{\{2\}, \{1, 3\}\}, \quad \{\{3\}, \{1, 2\}\}, \quad \{\{1, 2, 3\}\}.$$

Example 6.1.4. One partition of $\mathbb{Z}$ is

$$\{\{2k : k \in \mathbb{Z}\}, \{2k + 1 : k \in \mathbb{Z}\}\}.$$

6.2 Reflexivity, symmetry, and transitivity

Definition 6.2.1. Let A be a set and R be a relation on A.

(1) R is *reflexive* if every element of A is R-related to itself, i.e.,

$$\forall x \in A \;\; (x \; R \; x).$$

(2) R is *symmetric* if x is R-related to y implies y is R-related to x, for all $x, y \in A$, i.e.,

$$\forall x, y \in A \;\; (x \; R \; y \Rightarrow y \; R \; x).$$

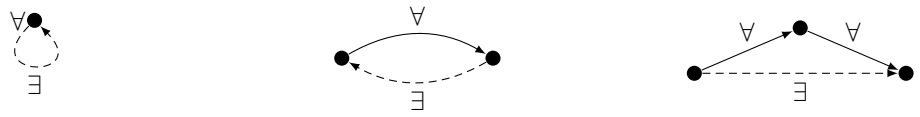
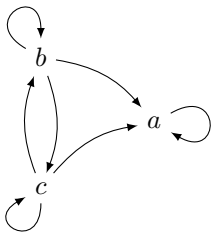


Figure 6.1: Reflexivity, symmetry, and transitivity

(3) R is *transitive* if x is R-related to y and y is R-related to z imply x is R-related to z, for all $x, y, z \in A$, i.e.,

$$\forall x, y, z \in A \ \ (x \ R \ y \wedge y \ R \ z \Rightarrow x \ R \ z).$$

Example 6.2.2. Let R be the relation represented by the following arrow diagram.



Then R is reflexive. It is not symmetric because $b \ R \ a$ but $a \not R \ b$. It is transitive, as one can show by exhaustion:

$$\begin{gathered} a \ R \ a \wedge a \ R \ a \Rightarrow a \ R \ a; \\ a \ R \ a \wedge a \ R \ b \Rightarrow a \ R \ b; \\ a \ R \ a \wedge a \ R \ c \Rightarrow a \ R \ c; \\ a \ R \ b \wedge b \ R \ a \Rightarrow a \ R \ a; \\ \vdots \\ c \ R \ c \wedge c \ R \ b \Rightarrow c \ R \ b; \\ c \ R \ c \wedge c \ R \ c \Rightarrow c \ R \ c. \end{gathered}$$

Example 6.2.3. Let R denote the equality relation on a set A, i.e., for all $x, y \in A$,

$$x \ R \ y \quad \Leftrightarrow \quad x = y.$$

Then R is reflexive, symmetric, and transitive.

Example 6.2.4. Let R' denote the subset relation on a set U of sets, i.e., for all $x, y \in U$,

$$x \ R' \ y \quad \Leftrightarrow \quad x \subseteq y.$$

Then R' is reflexive, may not be symmetric (when U contains x, y such that $x \subsetneq y$), but is transitive.

Example 6.2.5. Let R denote the non-strict less-than relation on $\mathbb{Q}$, i.e., for all $x, y \in \mathbb{Q}$,

$$x \ R \ y \quad \Leftrightarrow \quad x \leqslant y.$$

Then R is reflexive, not symmetric, but transitive.

Example 6.2.6. Let R' denote the strict less-than relation on $\mathbb{Q}$, i.e., for all $x, y \in \mathbb{Q}$,

$$x \; R' \; y \quad \Leftrightarrow \quad x < y.$$

Then R' is not reflexive as $0 \not< 0$. It is not symmetric because $0 < 1$ but $1 \not< 0$. It is transitive.

Definition 6.2.7 (recall)**.** Let $n, d \in \mathbb{Z}$. Then d is said to *divide* n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for "d divides n", and $d \nmid n$ for "d does not divide n". We also say

"n is *divisible* by d" or "n is a *multiple* of d" or "d is a *factor/divisor* of n"

for "d divides n".

Example 6.2.8. Let R denote the divisibility relation on $\mathbb{Z}^+$, i.e., for all $x, y \in \mathbb{Z}^+$,

$$x \; R \; y \quad \Leftrightarrow \quad x \mid y.$$

Then R is reflexive, not symmetric, but transitive.

Proof. (Reflexivity.) For each $a \in \mathbb{Z}^+$, we know $a = a \times 1$ and so $a \mid a$ by the definition of divisibility.

(Non-symmetry.) Note $1 \mid 2$ but $2 \nmid 1$.

(Transitivity.) Let $a, b, c \in \mathbb{Z}^+$ such that $a \mid b$ and $b \mid c$. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = b\ell$. Then $c = b\ell = (ak)\ell = a(k\ell)$, where $k\ell \in \mathbb{Z}$. Thus $a \mid c$ by the definition of divisibility. □

Exercise 6.2.9. Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$. View R as a relation on A. Is R reflexive? Is R symmetric? Is R transitive? 6a

Exercise 6.2.10. Let R be a relation on a set A. Prove that R is transitive if and only if $R \circ R \subseteq R$. 6b

Definition 6.2.11. An *equivalence relation* is a relation that is reflexive, symmetric and transitive.

Convention 6.2.12. People usually use equality-like symbols such as $\sim$, $\approx$, $\simeq$, $\cong$, and $\equiv$ to denote equivalence relations. These symbols are often defined and redefined to mean different equivalence relations in different situations. We may read $\sim$ as "is equivalent to".

Example 6.2.13. The equality relation on a set, as defined in Example 6.2.3, is an equivalence relation.

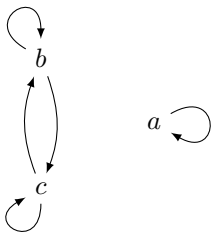
Proposition 6.2.14. Let $\mathscr{C}$ be a partition of a set A. Denote by $\sim_{\mathscr{C}}$ the same-component relation with respect to $\mathscr{C}$, i.e., for all $x, y \in A$,

$$x \sim_{\mathscr{C}} y \quad \Leftrightarrow \quad x, y \in S \text{ for some } S \in \mathscr{C}.$$

Then $\sim_{\mathscr{C}}$ is an equivalence relation on A.

Proof. Reflexivity holds because every element is in the same component as itself. Symmetry holds because if x is in the same component as y, then y is in the same component as x. Transitivity holds because if x is in the same component as y, and y is in the same component as z, then x is in the same component as z. □

Example 6.2.15. Let R be the relation represented by the following arrow diagram.



Then R is reflexive, symmetric, and transitive. So it is an equivalence relation on $\{a, b, c\}$.

6.3 Equivalence classes

Definition 6.3.1. Let $\sim$ be an equivalence relation on a set A. For each $x \in A$, the *equivalence class* of x with respect to $\sim$, denoted $[x]_\sim$, is defined to be the set of all elements of A that are $\sim$-related to x, i.e.,

$$[x]_\sim = \{y \in A : x \sim y\}.$$

When there is no risk of confusion, we may drop the subscript and write simply $[x]$.

Example 6.3.2. Let A be a set. The equivalence classes with respect to the equality relation on A are of the form

$$[x] = \{y \in A : x = y\} = \{x\},$$

where $x \in A$.

Example 6.3.3. If R is the equivalence relation represented by the arrow diagram in Example 6.2.15, then

$$[a] = \{a\} \quad \text{and} \quad [b] = \{b, c\} = [c].$$

Lemma 6.3.4. Let $\sim$ be an equivalence relation on a set A.

(1) $x \in [x]$ for all $x \in A$.

(2) Any equivalence class is nonempty.

Proof. (1) Let $x \in A$. Then $x \sim x$ by reflexivity. So $x \in [x]$ by the definition of $[x]$.

(2) Any equivalence class is of the form $[x]$ for some $x \in A$, and so it must be nonempty by (1). □

Lemma 6.3.5. Let $\sim$ be an equivalence relation on a set A. For all $x, y \in A$, if $[x] \cap [y] \neq \varnothing$, then $[x] = [y]$.

Proof. Assume $[x] \cap [y] \neq \varnothing$. Say, we have $w \in [x] \cap [y]$. This means $x \sim w$ and $y \sim w$ by the definition of $[x]$ and $[y]$.

To show $[x] = [y]$, we need to prove both $[x] \subseteq [y]$ and $[y] \subseteq [x]$. We will concentrate on the former; the latter is similar.

Take $z \in [x]$. Then $x \sim z$ by the definition of $[x]$. By symmetry, we know from the first paragraph that $w \sim x$. Altogether we have $y \sim w \sim x \sim z$. So transitivity tells us $y \sim z$. Thus $z \in [y]$ by the definition of $[y]$. □

Question 6.3.6. Consider an equivalence relation. Is it true that if x is an element of an equivalence class S, then $S = [x]$? 6c

Definition 6.3.7. Let A be a set and $\sim$ be an equivalence relation on A. Denote by $A/\sim$ the set of all equivalence classes with respect to $\sim$, i.e.,

$$A/\sim = \{[x]_\sim : x \in A\}.$$

We may read $A/\sim$ as "the quotient of A by $\sim$".

Example 6.3.8. Let A be a set. Then from Example 6.3.2 we know $A/=$ is equal to $\{\{x\} : x \in A\}$.

Example 6.3.9. If R is the equivalence relation on the set $A = \{a, b, c\}$ represented by the arrow diagram in Example 6.2.15, then from Example 6.3.3 we know

$$A/\sim = \{[a], [b], [c]\} = \big\{\{a\}, \{b, c\}, \{b, c\}\big\} = \big\{\{a\}, \{b, c\}\big\}.$$

Theorem 6.3.10. Let $\sim$ be an equivalence relation on a set A. Then $A/\sim$ is a partition of A.

Proof. Conditions (0) and (1) in the definition of partitions are guaranteed by the definition of equivalence classes and Lemma 6.3.4. Condition (2) is given by Lemma 6.3.5. □

6.4 Partial orders

Definition 6.4.1. Let A be a set and R be a relation on A.

(1) R is *antisymmetric* if $\quad \forall x, y \in A \;\; (x \; R \; y \wedge y \; R \; x \Rightarrow x = y)$.

(2) R is a *(non-strict) partial order* if R is reflexive, antisymmetric, and transitive.

(3) Suppose R is a partial order. Let $x, y \in A$. Then x, y are *comparable (under R)* if

$$x \; R \; y \quad \text{or} \quad y \; R \; x.$$

(4) R is a *(non-strict) total order* or a *(non-strict) linear order* if R is a partial order and every pair of elements is comparable, i.e.,

$$\forall x, y \in A \;\; (x \; R \; y \vee y \; R \; x).$$

Note 6.4.2. A total order is always a partial order.

Example 6.4.3. Let R denote the non-strict less-than relation on $\mathbb{Z}$, i.e., for all $x, y \in \mathbb{Z}$,

$$x \; R \; y \quad \Leftrightarrow \quad x \leqslant y.$$

Then R is antisymmetric. In fact, it is a total order.

Example 6.4.4. Let R denote the subset relation on a set U of sets, i.e., for all $x, y \in U$,

$$x \; R \; y \quad \Leftrightarrow \quad x \subseteq y.$$

Then R is antisymmetric. It is always a partial order, but it may not be a total order.

Example 6.4.5. Let R denote the divisibility relation on $\mathbb{Z}$, i.e., for all $x, y \in \mathbb{Z}$,

$$x \; R \; y \quad \Leftrightarrow \quad x \mid y.$$

Is R antisymmetric? Is R a partial order? Is R a total order? 6d

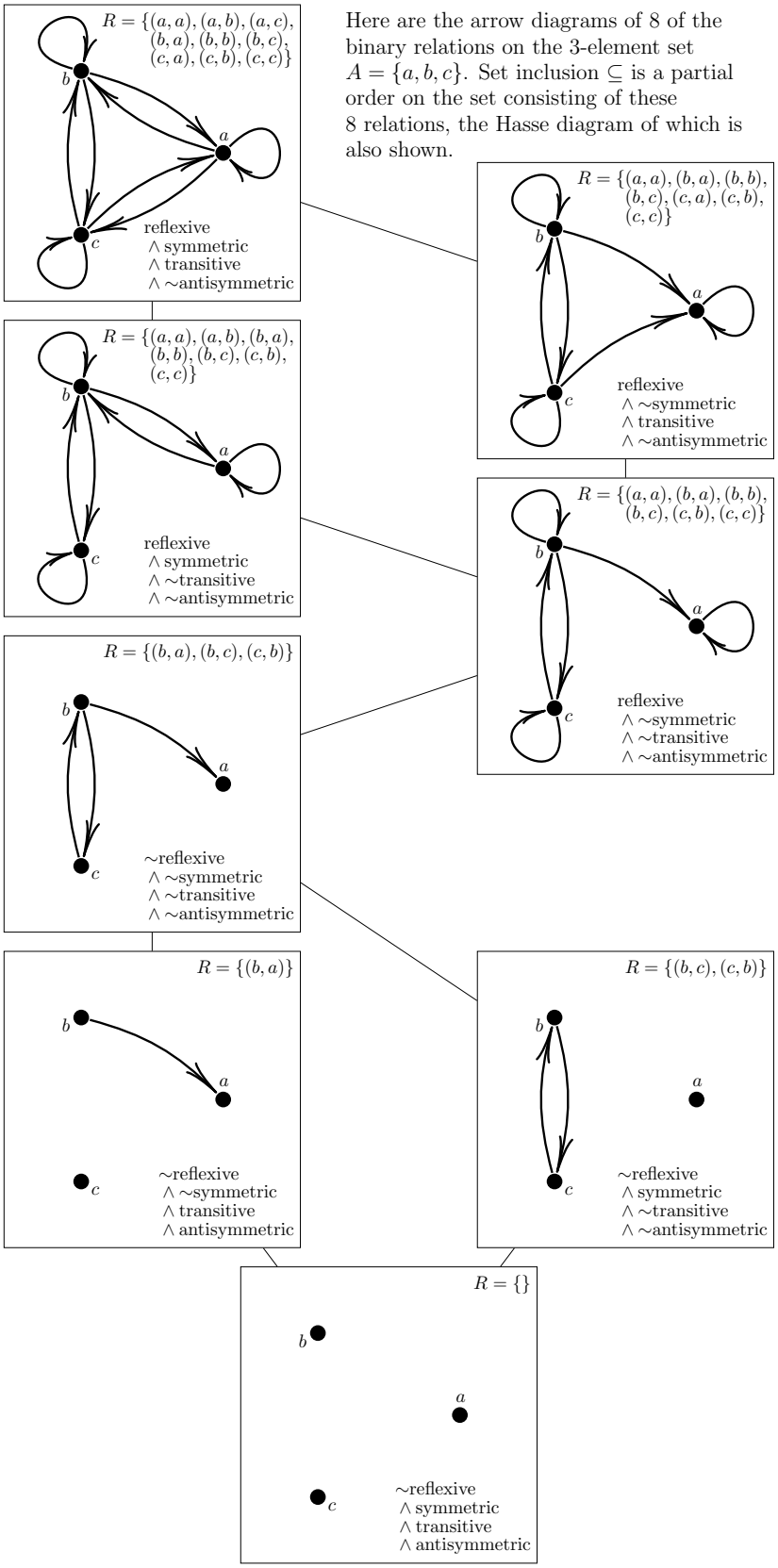


Figure 6.2: A partial order on a set of relations

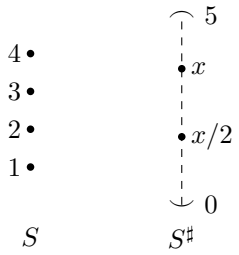


Figure 6.3: A difference between $\mathbb{Z}_{\geqslant 0}$ and $\mathbb{Q}_{\geqslant 0}$

Example 6.4.6. Let R' denote the divisibility relation on $\mathbb{Z}^+$, i.e., for all $x, y \in \mathbb{Z}^+$,

$$x \; R' \; y \quad \Leftrightarrow \quad x \mid y.$$

Is R antisymmetric? Is R a partial order? Is R a total order? 6e

Definition 6.4.7. Let R be a (non-strict) partial order on a set A. A *smallest element* of A (with respect to the partial order R) is an element $m \in A$ such that $m \; R \; x$ for all $x \in A$.

Example 6.4.8. (1) $S = \{x \in \mathbb{Z}_{\geqslant 0} : 0 < x < 5\}$ has smallest element 1.

(2) $S^\sharp = \{x \in \mathbb{Q}_{\geqslant 0} : 0 < x < 5\}$ has no smallest element because if $x \in S^\sharp$, then $x/2 \in S^\sharp$ and $x/2 < x$.

Second Principle of Mathematical Induction (2PI, recall)**.** Let $b, c \in \mathbb{Z}$, and $P(n)$ be a statement for each integer $n \geqslant b$. Here are the steps to prove that $P(n)$ is true for all integers $n \geqslant b$ by 2PI.

Establish the **Basis:** Prove that $P(b), P(b+1), \ldots, P(c)$ are true.

Make the **Induction Hypothesis:** Suppose $k \in \mathbb{Z}_{\geqslant c}$ such that $P(b), P(b+1), \ldots, P(k)$ are true.

Complete the **Induction Step:** Use the Induction Hypothesis to prove that $P(k+1)$ is true.

Theorem 6.4.9 (Well-Ordering Principle)**.** Let $b \in \mathbb{Z}$ and $S \subseteq \mathbb{Z}_{\geqslant b}$. If $S \neq \varnothing$, then S has a smallest element.

Proof. We prove the contrapositive. Assume that S has no smallest element. As $S \subseteq \mathbb{Z}_{\geqslant b}$, it suffices to show that $n \notin S$ for all $n \in \mathbb{Z}_{\geqslant b}$. We prove this by 2PI on n.

Basis: If $b \in S$, then b is the smallest element of S because $S \subseteq \mathbb{Z}_{\geqslant b}$, which contradicts our assumption. So $b \notin S$.

Induction Hypothesis: Suppose $k \in \mathbb{Z}_{\geqslant b}$ such that $b, b+1, \ldots, k \notin S$.

Induction Step: If $k+1 \in S$, then $k+1$ is the smallest element of S, because $S \subseteq \mathbb{Z}_{\geqslant b}$, which contradicts our assumption. So $k+1 \notin S$.

This concludes the induction and the proof. □

CS1231 Chapter 7

Functions

7.1 Basics

Definition 7.1.1. Let A, B be sets. A *function* or a *map* from A to B is a relation f from A to B such that any element of A is f-related to a unique element of B, i.e.,

(F1) every element of A is f-related to at least one element of B, or in symbols,

$$\forall x \in A \;\; \exists y \in B \;\; (x, y) \in f;$$

(F2) every element of A is f-related to at most one element of B, or in symbols,

$$\forall x \in A \;\; \forall y_1, y_2 \in B \;\; \big((x, y_1) \in f \wedge (x, y_2) \in f \;\Rightarrow\; y_1 = y_2\big).$$

We write $f \colon A \to B$ for "f is a function from A to B". Here A is called the *domain* of f, and B is called the *codomain* of f.

Remark 7.1.2. The negations of (F1) and (F2) can be expressed respectively as

(∼F1) $\exists x \in A \;\; \forall y \in B \;\; (x, y) \notin f$; and

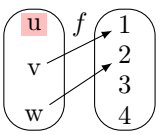
(∼F2) $\exists x \in A \;\; \exists y_1, y_2 \in B \;\; \big((x, y_1) \in f \wedge (x, y_2) \in f \wedge y_1 \neq y_2\big)$.

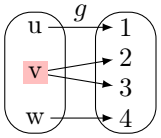
Example 7.1.3. Let $A = \{\mathrm{u}, \mathrm{v}, \mathrm{w}\}$ and $B = \{1, 2, 3, 4\}$.

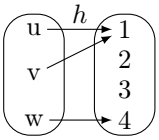
(1) $f = \{(\mathrm{v}, 1), (\mathrm{w}, 2)\}$ is *not* a function $A \to B$ because $\mathrm{u} \in A$ such that no $y \in B$ makes $(\mathrm{u}, y) \in f$, violating (F1).

(2) $g = \{(\mathrm{u}, 1), (\mathrm{v}, 2), (\mathrm{v}, 3), (\mathrm{w}, 4)\}$ is *not* a function $A \to B$ because $\mathrm{v} \in A$ and $2, 3 \in B$ such that $(\mathrm{v}, 2), (\mathrm{v}, 3) \in g$ but $2 \neq 3$, violating (F2).

(3) $h = \{(\mathrm{u}, 1), (\mathrm{v}, 1), (\mathrm{w}, 4)\}$ *is* a function $A \to B$ because both (F1) and (F2) are satisfied.



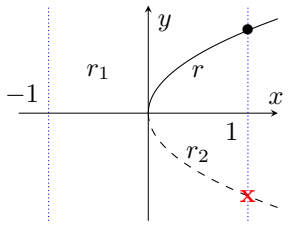




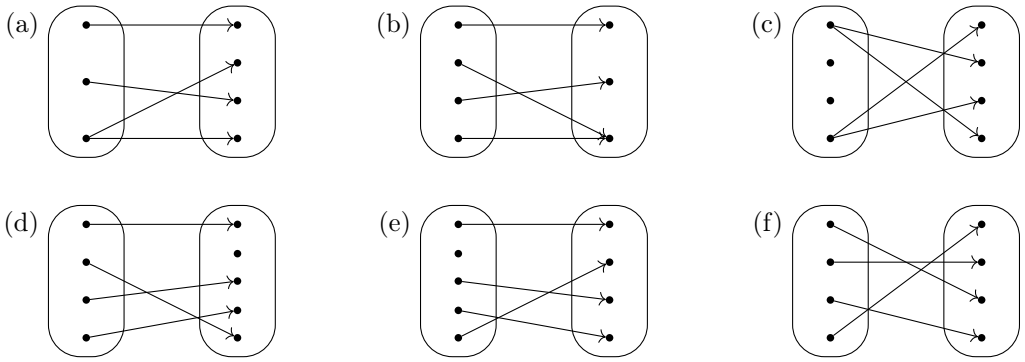
Example 7.1.4. (1) $r = \{(x, y) \in \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0} : x = y^2\}$ *is* a function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ because for every $x \in \mathbb{R}_{\geqslant 0}$, there is a unique $y \in \mathbb{R}_{\geqslant 0}$ such that $(x, y) \in r$, namely $y = \sqrt{x}$.

(2) $r_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R}_{\geqslant 0} : x = y^2\}$ is *not* a function $\mathbb{R} \to \mathbb{R}_{\geqslant 0}$ because $-1 \in \mathbb{R}$ that is not equal to y^2 for any $y \in \mathbb{R}_{\geqslant 0}$, violating (F1).

(3) $r_2 = \{(x, y) \in \mathbb{R}_{\geqslant 0} \times \mathbb{R} : x = y^2\}$ is *not* a function $\mathbb{R}_{\geqslant 0} \to \mathbb{R}$ because $1 \in \mathbb{R}_{\geqslant 0}$ and $-1, 1 \in \mathbb{R}$ such that $1 = (-1)^2$ and $1 = 1^2$ but $-1 \neq 1$, violating (F2).



Question 7.1.5. Which of the arrow diagrams below represent a function from the LHS set to the RHS set? 7a



7.2 Images

Definition 7.2.1. Let $f\colon A \to B$.

(1) If $x \in A$, then $f(x)$ denotes the unique element $y \in B$ such that $(x, y) \in f$. We call $f(x)$ the *image* of x under f.

(2) The *range* of f, denoted $\operatorname{range}(f)$, is defined by

$$\operatorname{range}(f) = \{f(x) : x \in A\}.$$

Remark 7.2.2. It follows from the definition of images that if $f\colon A \to B$ and $x \in A$, then for all $y \in B$,

$$(x, y) \in f \quad \Leftrightarrow \quad y = f(x).$$

Example 7.2.3. The function $r\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ in Example 7.1.4(1) satisfies

$$\forall x, y \in \mathbb{R}_{\geqslant 0} \quad \big(y = r(x) \Leftrightarrow x = y^2\big).$$

Note that $\operatorname{range}(r) = \mathbb{R}_{\geqslant 0}$, because for every $y \in \mathbb{R}_{\geqslant 0}$, there is $x \in \mathbb{R}_{\geqslant 0}$ such that $y = r(x)$, namely $x = y^2$.

Definition 7.2.4. A *Boolean function* is a function $\{\mathrm{T}, \mathrm{F}\}^n \to \{\mathrm{T}, \mathrm{F}\}$ where $n \in \mathbb{Z}^+$.

Example 7.2.5. We can view the inclusive or $\vee$ as the Boolean function $d\colon \{\mathrm{T}, \mathrm{F}\}^2 \to \{\mathrm{T}, \mathrm{F}\}$ satisfying, for all $p, q \in \{\mathrm{T}, \mathrm{F}\}$,

$$d(p, q) = \begin{cases} \mathrm{F}, & \text{if } p = \mathrm{F} = q; \\ \mathrm{T}, & \text{otherwise.} \end{cases}$$

Note that $\operatorname{range}(d) = \{\mathrm{T}, \mathrm{F}\}$, because $d(\mathrm{T}, \mathrm{T}) = \mathrm{T}$ and $d(\mathrm{F}, \mathrm{F}) = \mathrm{F}$.

Proposition 7.2.6. Let $f, g\colon A \to B$. Then $f = g$ if and only if $f(x) = g(x)$ for all $x \in A$.

Proof. ($\Rightarrow$) Assume $f = g$. Let $x \in A$. Then

$$\begin{array}{lll} & (x, f(x)) \in f & \text{by the } \Leftarrow \text{ part of Remark 7.2.2.} \\ \therefore & (x, f(x)) \in g & \text{as } f = g. \\ \therefore & f(x) = g(x) & \text{by the } \Rightarrow \text{ part of Remark 7.2.2.} \end{array}$$

($\Leftarrow$) Assume $f(x) = g(x)$ for all $x \in A$. For each $x \in A$ and each $y \in B$,

$$\begin{array}{lcll} (x, y) \in f & \Leftrightarrow & y = f(x) & \text{by Remark 7.2.2;} \\ & \Leftrightarrow & y = g(x) & \text{by our assumption;} \\ & \Leftrightarrow & (x, y) \in g & \text{by Remark 7.2.2.} \end{array}$$

So $f = g$. □

Example 7.2.7. The descriptions of r and d in Examples 7.2.3 and 7.2.5 in terms of $r(x)$ and $d(p, q)$ uniquely characterize these functions by Proposition 7.2.6, and can thus serve as definitions of r and d.

Example 7.2.8. Let $f\colon \{0, 2\} \to \mathbb{Z}$ and $g\colon \{0, 2\} \to \mathbb{Z}$ defined by setting, for all $x \in \{0, 2\}$,

$$f(x) = 2x \quad \text{and} \quad g(x) = x^2.$$

Then $f = g$ by Proposition 7.2.6, because $f(x) = g(x)$ for every $x \in \{0, 2\}$.

Example 7.2.9. Let $f\colon \mathbb{Z} \to \mathbb{Z}$ and $g\colon \mathbb{Q} \to \mathbb{Q}$ defined by

$$\forall x \in \mathbb{Z} \ \ (f(x) = x^3) \quad \text{and} \quad \forall x \in \mathbb{Q} \ \ (g(x) = x^3).$$

Then $f \neq g$ because $(1/2, 1/8)$ is an element of g but not of f.

7.3 Composition

Proposition 7.3.1. Let $f\colon A \to B$ and $g\colon B \to C$. Then $g \circ f$ is a function $A \to C$. Moreover, for every $x \in A$,

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

Proof. (F1) Let $x \in A$. Use (F1) for f to find $y \in B$ such that $(x, y) \in f$. Use (F1) for g to find $z \in C$ such that $(y, z) \in g$. Then $(x, z) \in g \circ f$ by the definition of $g \circ f$.

(F2) Let $x \in A$ and $z_1, z_2 \in C$ such that $(x, z_1), (x, z_2) \in g \circ f$. Use the definition of $g \circ f$ to find $y_1, y_2 \in B$ such that $(x, y_1), (x, y_2) \in f$ and $(y_1, z_1), (y_2, z_2) \in g$. Then (F2) for f implies $y_1 = y_2$. So $z_1 = z_2$ as g satisfies (F2).

These show $g \circ f$ is a function $A \to C$. Now, for every $x \in A$,

$$\begin{array}{lll} & (x, f(x)) \in f \quad \text{and} \quad \big(f(x), g(f(x))\big) \in g & \text{by the } \Leftarrow \text{ part of Remark 7.2.2;} \\ \therefore & (x, g(f(x))) \in g \circ f & \text{by the definition of } g \circ f; \\ \therefore & g(f(x)) = (g \circ f)(x) & \text{by the } \Rightarrow \text{ part of Remark 7.2.2.} \end{array}$$ □

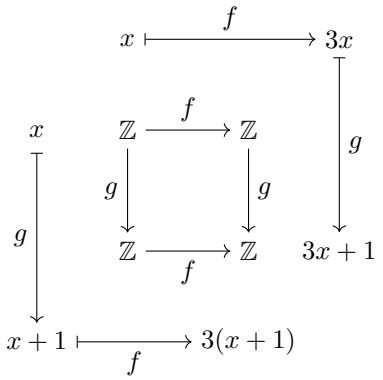
Example 7.3.2. Let $f, g\colon \mathbb{Z} \to \mathbb{Z}$ such that for every $x \in \mathbb{Z}$,

$$f(x) = 3x \quad \text{and} \quad g(x) = x + 1.$$

By Proposition 7.3.1, for every $x \in \mathbb{Z}$,

$$(g \circ f)(x) = g(f(x)) = g(3x) = 3x + 1 \quad \text{and} \quad (f \circ g)(x) = f(g(x)) = f(x + 1) = 3(x + 1).$$

Note $(g \circ f)(0) = 1 \neq 3 = (f \circ g)(0)$. So $g \circ f \neq f \circ g$ by Proposition 7.2.6.



Definition 7.3.3. Let A be a set. Then the *identity function* on A, denoted id_A, is the function $A \to A$ which satisfies, for all $x \in A$,

$$\mathrm{id}_A(x) = x.$$

Example 7.3.4. Let $f\colon A \to B$.

(1) $f \circ \mathrm{id}_A = f$ by Proposition 7.2.6, because Proposition 7.3.1 implies

- $f \circ \mathrm{id}_A$ is a function $A \to B$; and
- $(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x)$ for all $x \in A$.

(2) $\mathrm{id}_B \circ f = f$ by Proposition 7.2.6, because Proposition 7.3.1 implies

- $\mathrm{id}_B \circ f$ is a function $A \to B$; and
- $(\mathrm{id}_B \circ f)(x) = \mathrm{id}_B(f(x)) = f(x)$ for all $x \in A$.

Question 7.3.5. Which of the following define a function $f\colon \mathbb{Z} \to \mathbb{Z}$ that satisfies $f \circ f = f$? 7b

(1) $f(x) = 1231$ for all $x \in \mathbb{Z}$.

(2) $f(x) = x$ for all $x \in \mathbb{Z}$.

(3) $f(x) = -x$ for all $x \in \mathbb{Z}$.

(4) $f(x) = 3x + 1$ for all $x \in \mathbb{Z}$.

(5) $f(x) = x^2$ for all $x \in \mathbb{Z}$.

7.4 Inverse and bijectivity

Definition 7.4.1. Let $f\colon A \to B$.

(1) f is *surjective* or *onto* if

$$\forall y \in B \;\; \exists x \in A \;\; y = f(x). \tag{F^{-1}1}$$

A *surjection* is a surjective function.

(2) f is *injective* or *one-to-one* if

$$\forall x_1, x_2 \in A \;\; (f(x_1) = f(x_2) \Rightarrow x_1 = x_2). \tag{F^{-1}2}$$

An *injection* is an injective function.

Figure 7.1: Surjectivity (left) and injectivity (right)

(3) f is *bijective* if it is both surjective and injective. A *bijection* is a bijective function.

Remark 7.4.2. In view of Remark 7.2.2, one can formulate ($F^{-1}1$) and ($F^{-1}2$) for a general relation f from A to B as follows:

($F^{-1}1$) $\forall y \in B \;\; \exists x \in A \;\; (x, y) \in f$;

($F^{-1}2$) $\forall x_1, x_2 \in A \;\; \forall y \in B \;\; \big((x_1, y) \in f \wedge (x_2, y) \in f \Rightarrow x_1 = x_2\big)$.

By the definition of f^{-1}, these are equivalent respectively to (F1) and (F2) for f^{-1}, i.e.,

- $\forall y \in B \;\; \exists x \in A \;\; (y, x) \in f^{-1}$; and
- $\forall x_1, x_2 \in A \;\; \forall y \in B \;\; \big((y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1} \Rightarrow x_1 = x_2\big)$.

So f^{-1} is a function $B \to A$ if and only if f satisfies the relational version of ($F^{-1}1$) and ($F^{-1}2$). Similarly, the conditions (F1) and (F2) are equivalent to ($F^{-1}1$) and ($F^{-1}2$) for f^{-1}.

Proposition 7.4.3. If f is a bijection $A \to B$, then f^{-1} is a bijection $B \to A$.

Proof. In view of the discussion in Remark 7.4.2, conditions (F1), (F2), ($F^{-1}1$), and ($F^{-1}2$) for f are equivalent respectively to conditions ($F^{-1}1$), ($F^{-1}2$), (F1), and (F2) for f^{-1}. □

Example 7.4.4. The function $f\colon \mathbb{Q} \to \mathbb{Q}$, defined by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$, is surjective.

Proof. Take any $y \in \mathbb{Q}$. Let $x = (y - 1)/3$. Then $x \in \mathbb{Q}$ and $f(x) = 3x + 1 = y$. □

Remark 7.4.5. A function $f\colon A \to B$ is *not* surjective if and only if

$$\exists y \in B \;\; \forall x \in A \;\; (y \neq f(x)).$$

Example 7.4.6. Define $g\colon \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then g is not surjective.

Proof. Note $g(x) = x^2 \geqslant 0 > -1$ for all $x \in \mathbb{Z}$. So $g(x) \neq -1$ for all $x \in \mathbb{Z}$, although $-1 \in \mathbb{Z}$. □

Example 7.4.7. As in Example 7.4.4, define $f\colon \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Then f is injective.

Proof. Let $x_1, x_2 \in \mathbb{Q}$ such that $f(x_1) = f(x_2)$. Then $3x_1 + 1 = 3x_2 + 1$. So $x_1 = x_2$. □

Remark 7.4.8. A function $f\colon A \to B$ is *not* injective if and only if

$$\exists x_1, x_2 \in A \;\; (f(x_1) = f(x_2) \wedge x_1 \neq x_2).$$

Example 7.4.9. As in Example 7.4.6, define $g\colon \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then g is not injective.

Proof. Note $g(1) = 1^2 = 1 = (-1)^2 = g(-1)$, although $1 \neq -1$. □

Question 7.4.10. Amongst the arrow diagrams in Question 7.1.5 that represent a function, which ones represent injections, which ones represent surjections, and which ones represent bijections? ✎ 7c

Proposition 7.4.11. Let $f\colon A \to B$ and $g\colon B \to A$. Then

$$g = f^{-1} \quad \Leftrightarrow \quad \forall x \in A \;\; \forall y \in B \;\; \big(g(y) = x \Leftrightarrow y = f(x)\big).$$

Proof.

$$\begin{aligned}
g = f^{-1} \quad &\Leftrightarrow \quad \forall y \in B \;\; \forall x \in A \;\; \big((y,x) \in g \Leftrightarrow (y,x) \in f^{-1}\big) && \text{as } g, f^{-1} \subseteq B \times A;\\
&\Leftrightarrow \quad \forall x \in A \;\; \forall y \in B \;\; \big((y,x) \in g \Leftrightarrow (x,y) \in f\big) && \text{by the definition of } f^{-1};\\
&\Leftrightarrow \quad \forall x \in A \;\; \forall y \in B \;\; \big(g(y) = x \Leftrightarrow y = f(x)\big) && \text{by Remark 7.2.2.}
\end{aligned}$$

□

Example 7.4.12. As in Example 7.4.7, define $f\colon \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Note that for all $x, y \in \mathbb{Q}$,

$$y = 3x + 1 \quad \Leftrightarrow \quad x = (y - 1)/3.$$

Let $g\colon \mathbb{Q} \to \mathbb{Q}$ such that $g(y) = (y - 1)/3$ for all $y \in \mathbb{Q}$. The equivalence above implies

$$\forall x, y \in \mathbb{Q} \;\; \big(y = f(x) \Leftrightarrow x = g(y)\big).$$

So Proposition 7.4.11 tells us $g = f^{-1}$.

Note 7.4.13. We have no guarantee of a description of the inverse of a general bijection that is much different from what is given by the definition.

Proposition 7.4.14. Let f be a bijection $A \to B$. Then $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$.

Proof. We know f^{-1} is a function by Proposition 7.4.3, because f is bijection.

For the first part, let $x \in A$. Define $y = f(x)$. Then

$$\begin{aligned}
(f^{-1} \circ f)(x) &= f^{-1}(f(x)) && \text{by Proposition 7.3.1;}\\
&= f^{-1}(y) && \text{by the definition of } y;\\
&= x && \text{by Proposition 7.4.11, as } y = f(x);\\
&= \mathrm{id}_A(x) && \text{by the definition of } \mathrm{id}_A.
\end{aligned}$$

So $f^{-1} \circ f = \mathrm{id}_A$ by Proposition 7.2.6.

For the second part, let $y \in B$. Define $x = f^{-1}(y)$. Then

$$\begin{aligned}
(f \circ f^{-1})(y) &= f(f^{-1}(y)) && \text{by Proposition 7.3.1;}\\
&= f(x) && \text{by the definition of } x;\\
&= y && \text{by Proposition 7.4.11, as } f^{-1}(y) = x;\\
&= \mathrm{id}_B(y) && \text{by the definition of } \mathrm{id}_B.
\end{aligned}$$

So $f \circ f^{-1} = \mathrm{id}_B$ by Proposition 7.2.6. □

CS1231 Chapter 8

Cardinality

8.1 Pigeonhole principles

Proposition 8.1.1. Let $f\colon A \to B$ and $g\colon B \to C$.

(1) If f and g are surjective, then so is $g \circ f$.

(2) If f and g are injective, then so is $g \circ f$.

(3) If f and g are bijective, then so is $g \circ f$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. (1) Suppose f and g are surjective. Let $z \in C$. Use the surjectivity of g to find $y \in B$ such that $z = g(y)$. Then use the surjectivity of f to find $x \in A$ such that $y = f(x)$. Now $z = g(y) = g(f(x)) = (g \circ f)(x)$ by Proposition 7.3.1, as required.

(2) Suppose f and g are injective. Let $x_1, x_2 \in A$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$. Then $g(f(x_1)) = g(f(x_2))$ by Proposition 7.3.1. The injectivity of g then implies $f(x_1) = f(x_2)$. So the injectivity of f tells us $x_1 = x_2$, as required.

(3) This follows from (1), (2), and Proposition 5.2.7. □

First Principle of Mathematical Induction (1PI, recall)**.** Let $b \in \mathbb{Z}$, and $P(n)$ be a statement for each integer $n \geqslant b$. Here are the steps to prove that $P(n)$ is true for all integers $n \geqslant b$ by 1PI.

Establish the **Basis:** Prove that $P(b)$ is true.

Make the **Induction Hypothesis:** Suppose $k \in \mathbb{Z}_{\geqslant b}$ such that $P(k)$ is true.

Complete the **Induction Step:** Use the Induction Hypothesis to prove that $P(k+1)$ is true.

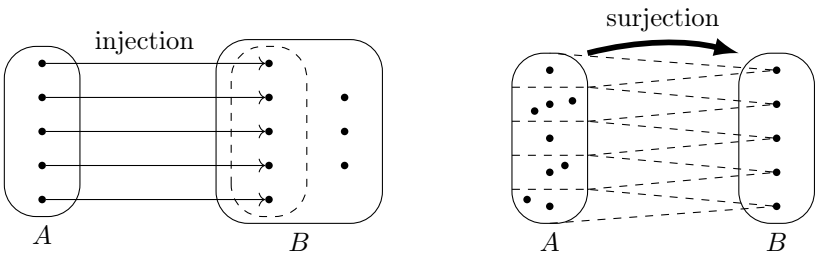


Figure 8.1: Injections, surjections, and the number of elements in the domain and the codomain

Theorem 8.1.2 (Pigeonhole Principle)**.** Let $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $n, m \in \mathbb{Z}_{\geqslant 0}$, the x's are different, and the y's are different. If there is an injection $A \to B$, then $n \leqslant m$.

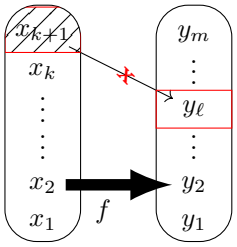


Figure 8.2: Induction proofs for the Pigeonhole Principles

Proof. We prove this by 1PI on n.

Basis: If $n = 0$ and $m \in \mathbb{Z}_{\geqslant 0}$, then $m \geqslant 0 = n$.

Induction Hypothesis: Suppose $k \in \mathbb{Z}_{\geqslant 0}$ such that the theorem is true when $n = k$.

Induction Step: Let $A = \{x_1, x_2, \ldots, x_{k+1}\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $m \in \mathbb{Z}_{\geqslant 0}$, such that the x's are different, and the y's are different. Suppose we have an injection $f\colon A \to B$. Suppose $f(x_{k+1}) = y_\ell$. By the injectivity of f, as the x's are all different, no $i \in \{1, 2, \ldots, k\}$ can make $f(x_i) = f(x_{k+1}) = y_\ell$. All such $f(x_i)$'s must appear in the list

$$y_1, y_2, \ldots, y_{\ell-1}, y_{\ell+1}, \ldots, y_m.$$

Let $y_1^*, y_2^*, \ldots, y_{m-1}^*$ denote the elements of this list. Define $f^*\colon \{x_1, x_2, \ldots, x_k\} \to \{y_1^*, y_2^*, \ldots, y_{m-1}^*\}$ by setting $f^*(x_i) = f(x_i)$ for each $i \in \{1, 2, \ldots, k\}$. Then f^* is injective because if $i, j \in \{1, 2, \ldots, k\}$ such that $f^*(x_i) = f^*(x_j)$, then $f(x_i) = f(x_j)$ by the definition of f^*, and so the injectivity of f implies $x_i = x_j$. As the x's are all different and the y^*'s are all different, the induction hypothesis tells us $k \leqslant m - 1$. Hence $k + 1 \leqslant m$. □

Theorem 8.1.3 (Dual Pigeonhole Principle)**.** Let $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $n, m \in \mathbb{Z}_{\geqslant 0}$, the x's are different, and the y's are different. If there is a surjection $A \to B$, then $n \geqslant m$.

Proof. We prove this by 1PI on n.

Basis: Let $n = 0$ and f be a surjection $\{\} \to \{y_1, y_2, \ldots, y_m\}$, where $m \in \mathbb{Z}_{\geqslant 0}$, such that the y's are different. Suppose $m \geqslant 1$. Consider y_1. The surjectivity of f gives $x \in \{\}$ such that $f(x) = y$. However, no x can be in $\{\}$. This is a contradiction. So $m = 0 = n$.

Induction Hypothesis: Suppose $k \in \mathbb{Z}_{\geqslant 0}$ such that the theorem is true when $n = k$.

Induction Step: Let $A = \{x_1, x_2, \ldots, x_{k+1}\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $m \in \mathbb{Z}_{\geqslant 0}$, such that the x's are different, and the y's are different. Suppose we have a surjection $f\colon A \to B$. Suppose $f(x_{k+1}) = y_\ell$. We split into two cases.

(1) Assume no $i \in \{1, 2, \ldots, k\}$ makes $f(x_i) = y_\ell$. Then all such $f(x_i)$'s must appear in the list

$$y_1, y_2, \ldots, y_{\ell-1}, y_{\ell+1}, \ldots, y_m.$$

Let $y_1^*, y_2^*, \ldots, y_{m-1}^*$ denote the elements of this list. Define $f^*\colon \{x_1, x_2, \ldots, x_k\} \to \{y_1^*, y_2^*, \ldots, y_{m-1}^*\}$ by setting $f^*(x_i) = f(x_i)$ for each $i \in \{1, 2, \ldots, k\}$.

We claim that f^* is surjective. To prove this, consider any y^*. It must equal y_h where $h \in \{1, 2, \ldots, m\} \setminus \{\ell\}$. By the surjectivity of f, we have $i \in \{1, 2, \ldots, k+1\}$ such that $y_h = f(x_i)$. As $\ell \neq h$ and the y's are all different, we know $y_\ell \neq y_h = f(x_i)$. Since $y_\ell = f(x_{k+1})$, we deduce that $i \neq k+1$. Hence $y_h = f(x_i) = f^*(x_i)$. As the x's are all different and the y^*'s are all different, the induction hypothesis tells us $k \geqslant m-1$. So $k+1 \geqslant m$.

(2) Assume some $i \in \{1, 2, \ldots, k\}$ makes $f(x_i) = y_\ell$. Define $f^* \colon \{x_1, x_2, \ldots, x_k\} \to \{y_1, y_2, \ldots, y_m\}$ by setting $f^*(x_i) = f(x_i)$ for each $i \in \{1, 2, \ldots, k\}$. Then f^* is surjective because, for each y_h, the surjectivity of f gives some x_i such that $y_h = f(x_i)$, and we can require this $i \neq k+1$ by our assumption; so $y_h = f(x_i) = f^*(x_i)$. As the x's are all different and the y's are all different, the induction hypothesis tells us $k \geqslant m$. So $k+1 \geqslant m+1 \geqslant m$. □

Theorem 8.1.4. Let $A = \{x_1, x_2, \ldots, x_n\}$ and $B = \{y_1, y_2, \ldots, y_m\}$, where $n, m \in \mathbb{Z}_{\geqslant 0}$, the x's are different, and the y's are different. Then $n = m$ if and only if there is a bijection $A \to B$.

Proof. ($\Rightarrow$) Suppose $n = m$. Define $f \colon A \to B$ by setting $f(x_i) = y_i$ for each $i \in \{1, 2, \ldots, n\}$. This definition is unambiguous because the x's are different.

To show injectivity, suppose $i, j \in \{1, 2, \ldots, n\}$ such that $f(x_i) = f(x_j)$. The definition of f tells us $f(x_i) = y_i$ and $f(x_j) = y_j$. Then $y_i = f(x_i) = f(x_j) = y_j$. So $i = j$ because the y's are different. This implies $x_i = x_j$.

Surjectivity follows from the observation that for every $y_i \in B$, we have $x_i \in A$ such that $f(x_i) = y_i$.

($\Leftarrow$) This follows directly from Theorem 8.1.2 and Theorem 8.1.3. □

Exercise 8.1.5. Prove the converse to Theorem 8.1.2. Prove also the converse to Theorem 8.1.3 when $B \neq \varnothing$. 8a

8.2 Same cardinality

Definition 8.2.1 (Cantor)**.** A set A is said to have the *same cardinality* as a set B if there is a bijection $A \to B$.

Note 8.2.2. We defined it means for a set to have the same cardinality as another set without defining what the cardinality of a set is.

Proposition 8.2.3. Let A, B, C be sets.

(1) A has the same cardinality as A. (reflexivity)

(2) If A has the same cardinality as B, then B has the same cardinality as A. (symmetry)

(3) If A has the same cardinality as B, and B has the same cardinality as C, then A has the same cardinality as C. (transitivity)

Proof. (Reflexivity.) It suffices to show that id_A is a bijection $A \to A$. For surjectivity, given any $x \in A$, we have $\mathrm{id}_A(x) = x$. For injectivity, if $x_1, x_2 \in A$ such that $\mathrm{id}_A(x_1) = \mathrm{id}_A(x_2)$, then $x_1 = x_2$.

(Symmetry.) If f is a bijection $A \to B$, then Proposition 7.4.3 tells us f^{-1} is a bijection $B \to A$.

(Transitivity.) If f is a bijection $A \to B$ and g is a bijection $B \to C$, then $g \circ f$ is a bijection $A \to C$ by Proposition 8.1.1(3). □

Definition 8.2.4. A set A is *finite* if it has the same cardinality as $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{Z}_{\geqslant 0}$. In this case, we call n the *cardinality* or the *size* of A, and we denote it by $|A|$. A set is *infinite* if it is not finite.

8.3 Countability

Definition 8.3.1 (Cantor)**.** A set is *countable* if it is finite or it has the same cardinality as $\mathbb{Z}^+$. A set is *uncountable* if it is not countable.

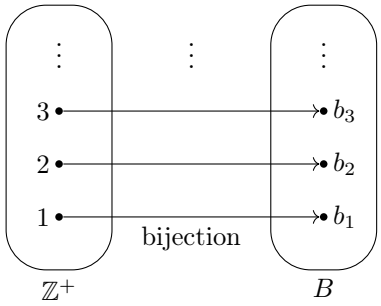


Figure 8.3: A countable infinite set B

Note 8.3.2. Some authors allow only infinite sets to be countable.

Example 8.3.3. (1) $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+\setminus\{1\}$ because the function $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+\setminus\{1\}$ satisfying $f(x) = x+1$ for all $x \in \mathbb{Z}^+$ is a bijection. So $\mathbb{Z}^+\setminus\{1\} = \{2, 3, 4, \dots\}$ is countable.

(2) $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+ \setminus \{1, 3, 5, \dots\}$ because the function $g\colon \mathbb{Z}^+ \to \mathbb{Z}^+ \setminus \{1, 3, 5, \dots\}$ satisfying $g(x) = 2x$ for all $x \in \mathbb{Z}^+$ is a bijection. So $\mathbb{Z}^+ \setminus \{1, 3, 5, \dots\} = \{2, 4, 6, \dots\}$ is countable.

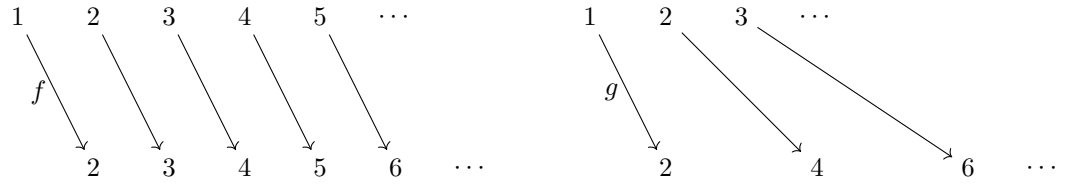


Figure 8.4: Removing 1 or half of the elements from $\mathbb{Z}^+$

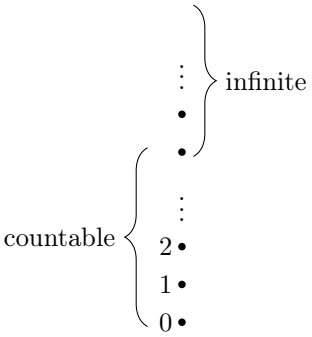


Figure 8.5: The smallest cardinalities

Proposition 8.3.4. Every infinite set B has a countable infinite subset.

Proof. Let B be an infinite set. Run the following procedure.

1. Initialize $i = 0$.
2. While $B \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ do:
   2.1. Pick any $g_{i+1} \in B \setminus \{g_1, g_2, \ldots, g_i\}$.
   2.2. Increment i to $i + 1$.

Suppose this procedure stops. Then a run results in $g_1, g_2, \ldots, g_\ell$, where $\ell \in \mathbb{Z}_{\geqslant 0}$. Define $g\colon \{1, 2, \ldots, \ell\} \to B$ by setting $g(i) = g_i$ for all $i \in \{1, 2, \ldots, \ell\}$. Notice $B \setminus \{g_1, g_2, \ldots, g_\ell\} = \varnothing$ as the stopping condition is reached. This says any element of B is equal to some g_i, thus some $g(i)$. So g is surjective. We know g is injective because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.1. As g is a bijection $\{1, 2, \ldots, \ell\} \to B$, we deduce that B is finite. This contradicts the condition that B is infinite.

So this procedure does not stop. Define $A = \{g_i : i \in \mathbb{Z}^+\}$, and $g\colon \mathbb{Z}^+ \to A$ by setting $g(i) = g_i$ for each $i \in \mathbb{Z}^+$. Then g is surjective by construction. It is injective because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.1. As g is a bijection $\mathbb{Z}^+ \to A$, we deduce that A is countable.

Next, we verify that A is infinite. In view of the definition of infinite sets, it suffices to show that no function $f\colon \{1, 2, \ldots, n\} \to A$ where $n \in \mathbb{Z}_{\geqslant 0}$ can be surjective. Take any function $f\colon \{1, 2, \ldots, n\} \to A$, where $n \in \mathbb{Z}_{\geqslant 0}$. Now $f(1), f(2), \ldots, f(n)$ are all elements of A. Each of these is g_i for some $i \in \mathbb{Z}^+$ by the definition of A. Say $f(1), f(2), \ldots, f(n)$ are $g_{i_1}, g_{i_2}, \ldots, g_{i_n}$ respectively, where $i_1, i_2, \ldots, i_n \in \mathbb{Z}^+$. Let i be the largest element of the nonempty set $\{1, i_1, i_2, \ldots, i_n\}$. Then $g_{i+1} \in A$ and

$$g_{i+1} \notin \{g_1, g_2, \ldots, g_i\} \supseteq \{g_{i_1}, g_{i_2}, \ldots, g_{i_n}\} = \{f(1), f(2), \ldots, f(n)\}.$$

This shows f is not surjective. □

Proposition 8.3.5. Any subset A of a countable set B is countable.

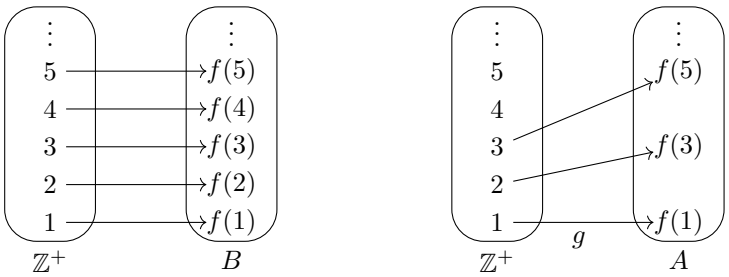


Figure 8.6: Countability of any subset A of a countable set B

Proof. If B is finite, then let f be a bijection $\{1, 2, \ldots, |B|\} \to B$, else let f be a bijection $\mathbb{Z}^+ \to B$. Run the following procedure.

1. Initialize $i = 0$.
2. While $A \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ do:
   2.1. Note that $A \setminus \{g_1, g_2, \ldots, g_i\} \neq \varnothing$ when this line is reached. If $a_i \in A \setminus \{g_1, g_2, \ldots, g_i\}$, then $a_i = f(m)$ for some $m \in \mathbb{Z}^+$ because f is a surjection $\mathbb{Z}^+ \to A$. This says $\{m \in \mathbb{Z}^+ : f(m) \in A \setminus \{g_1, g_2, \ldots, g_i\}\} \neq \varnothing$, and so it must have a smallest element by the Well-Ordering Principle. Call this smallest element m_{i+1}.
   2.2. Set $g_{i+1} = f(m_{i+1})$. Note that $g_{i+1} \in A \setminus \{g_1, g_2, \ldots, g_i\}$ by the choice of m_{i+1}.
   2.3. Increment i to $i + 1$.

Case 1: this procedure stops after finitely many steps. Then a run results in

$$m_1, m_2, \ldots, m_\ell \quad \text{and} \quad g_1, g_2, \ldots, g_\ell$$

where $\ell \in \mathbb{Z}_{\geqslant 0}$. Define $g\colon \{1, 2, \ldots, \ell\} \to A$ by setting $g(i) = g_i$ for all $i \in \{1, 2, \ldots, \ell\}$.

Notice $A \setminus \{g_1, g_2, \ldots, g_\ell\} = \varnothing$ as the stopping condition is reached. This says any element of A is equal to some g_i, thus some $g(i)$. So g is surjective. We know g is injective because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.2.

As g is a bijection $\{1, 2, \ldots, \ell\} \to A$, we deduce that A is finite and hence countable.

Case 2: this procedure does not stop. Then a run results in

$$m_1, m_2, m_3, \ldots \quad \text{and} \quad g_1, g_2, g_3, \ldots.$$

Define $g\colon \mathbb{Z}^+ \to A$ by setting $g(i) = g_i$ for all $i \in \mathbb{Z}^+$.

We claim that $m_{i+1} < m_{i+2}$ for all $i \in \mathbb{Z}_{\geqslant 0}$. Suppose not. Let $i \in \mathbb{Z}_{\geqslant 0}$ such that $m_{i+1} \geqslant m_{i+2}$. Line 2.2 tells us $g_{i+1} = f(m_{i+1})$ and $g_{i+2} = f(m_{i+2})$, but $g_{i+2} \neq g_{i+1}$. So $m_{i+1} \neq m_{i+2}$. This implies $m_{i+1} > m_{i+2}$. Note that $f(m_{i+2}) = g_{i+2} \in A \setminus \{g_1, g_2, \ldots, g_i\} \subseteq A \setminus \{g_1, g_2, \ldots, g_i\}$. So $m_{i+2} \in \{m \in \mathbb{Z}^+ : f(m) \in A \setminus \{g_1, g_2, \ldots, g_i\}\}$. However, we chose m_{i+1} to be the smallest element of this set, and $m_{i+2} < m_{i+1}$. This contradiction shows the claim.

To show the surjectivity of g, assume we have $y \in A$ such that $g(i) \neq y$ for any $i \in \mathbb{Z}^+$. As f is a surjection $\mathbb{Z}^+ \to B$ and $A \subseteq B$, we get $n \in \mathbb{Z}^+$ making $f(n) = y$. The claim in the previous paragraph tells us that $0 < m_1 < m_2 < \cdots < m_{n+1}$. So $m_{n+1} > n$. Also, our assumption on y implies $f(n) = y \in A \setminus \{g(1), g(2), \ldots, g(n)\} = A \setminus \{g_1, g_2, \ldots, g_n\}$. However, we chose m_{n+1} to be the smallest $m \in \mathbb{Z}^+$ such that $f(m) \in A \setminus \{g_1, g_2, \ldots, g_n\}$. This contradiction shows the surjectivity of g.

We know g is injective because each $g_{i+1} \notin \{g_1, g_2, \ldots, g_i\}$ by line 2.2.

As g is a bijection $\mathbb{Z}^+ \to A$, we deduce that A is countable. □

8.4 More countable sets

Definition 8.4.1 (recall)**.** An integer is *even* if it is $2x$ for some $x \in \mathbb{Z}$. An integer is *odd* if it is $2x + 1$ for some $x \in \mathbb{Z}$.

Fact 8.4.2. Any integer is either even or odd, but not both.

Proof. We prove by induction on n that every $n \in \mathbb{Z}_{\geqslant 0}$ is either even or odd. For the basis, we know 0 is even because $0 = 2 \times 0$. For the induction step, assume $k \in \mathbb{Z}_{\geqslant 0}$ that is either even or odd. If k is even, say $k = 2x$ where $x \in \mathbb{Z}$, then $k + 1 = 2x + 1$, which is odd. If k is odd, say $k = 2x + 1$ where $x \in \mathbb{Z}$, then $k + 1 = 2x + 2 = 2(x + 2)$, which is even. So $k + 1$ is either even or odd in either case. This completes the induction.

Consider $n \in \mathbb{Z}^-$. We know $-n \in \mathbb{Z}^+$ and so it must be even or odd by the previous paragraph. If $-n$ is even, say $-n = 2x$ where $x \in \mathbb{Z}$, then $n = 2(-x)$, which is even. If $-n$ is odd, say $-n = 2x + 1$ where $x \in \mathbb{Z}$, then $n = -2x - 1 = 2(-x - 1) + 1$, which is odd. So $-n$ is either even or odd in either case.

Finally, suppose $n \in \mathbb{Z}$ that is both even and odd, say $2x = n = 2y + 1$ where $x, y \in \mathbb{Z}$. Then $x - y \in \mathbb{Z}$ but $x - y = 1/2 \notin \mathbb{Z}$. This is a contradiction. So no $n \in \mathbb{Z}$ can be both even and odd. □

Proposition 8.4.3. $\mathbb{Z}$ is countable.

Proof. Define $f\colon \mathbb{Z} \to \mathbb{Z}^+$ by setting, for each $x \in \mathbb{Z}$,

$$f(x) = \begin{cases} 2x, & \text{if } x > 0; \\ -2x + 1, & \text{if } x \leqslant 0. \end{cases}$$

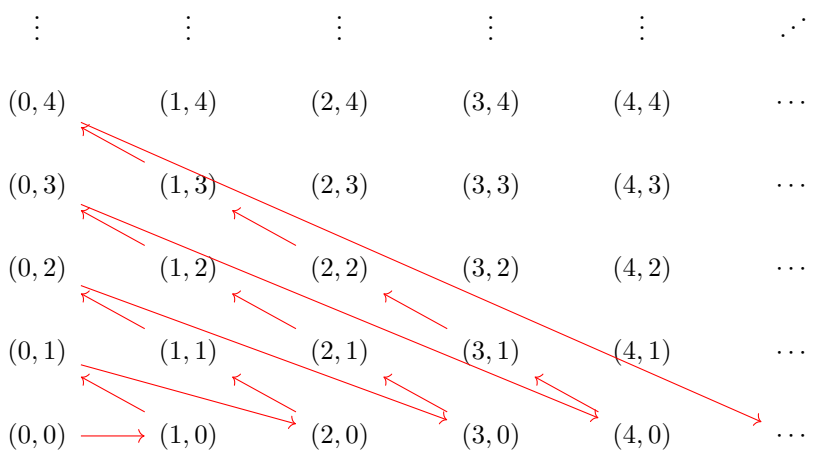
This f is well defined because if $x > 0$, then $2x > 0$ as well; and if $x \leqslant 0$, then $-2x + 1 \geqslant -2 \times 0 + 1 = 1$. In view of Proposition 8.2.3 (2), it suffices to show that f is a bijection.

To show surjectivity, pick any $y \in \mathbb{Z}^+$. Then Fact 8.4.2 tells us that y is either even or odd. If y is even, say $y = 2n$ where $n \in \mathbb{Z}$, then $n = y/2 > 0$, and so $f(n) = 2n = y$. If y is odd, say $y = 2n + 1$ where $n \in \mathbb{Z}$, then $n = (y - 1)/2 \geqslant (1 - 1)/2 = 0$, and so $f(-n) = -2(-n) + 1 = 2n + 1 = y$. Thus some $n \in \mathbb{Z}$ makes $f(n) = y$ in either case.

To show injectivity, pick $x_1, x_2 \in \mathbb{Z}$ such that $f(x_1) = f(x_2)$. If $f(x_1)$ is even, then $f(x_1) = 2x_1$ and $f(x_2) = 2x_2$ by Fact 8.4.2, and so $x_1 = x_2$. If $f(x_1)$ is odd, then $f(x_1) = -2x_1 + 1$ and $f(x_2) = -2x_2 + 1$ by Fact 8.4.2, and so $x_1 = x_2$. Thus $x_1 = x_2$ in either case. □

Theorem 8.4.4 (Cantor 1877)**.** $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable.

Proof sketch.



The function $f\colon \mathbb{Z}^+ \to \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ such that $f(1), f(2), f(3), \ldots$ are respectively

$$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (2,1), (1,2), (0,3), (4,0), (3,1), (2,2), (1,3), (0,4), \ldots$$

following the arrows in the diagram above is a bijection. This shows $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable. □

Proposition 8.4.5. $\{0,1\}^*$ is countable.

Proof sketch. Let $f\colon \mathbb{Z}^+ \to \{0,1\}^*$ such that $f(1), f(2), f(3), \ldots$ are respectively

$$\varepsilon, \underbrace{0, 1}_{\substack{\text{length} \\ 1}}, \underbrace{00, 01, 10, 11}_{\substack{\text{length} \\ 2}}, \underbrace{000, 001, 010, 011, 100, 101, 110, 111}_{\substack{\text{length} \\ 3}}, \ldots,$$

where ε denotes the empty string. Then f is a bijection. This shows $\{0,1\}^*$ is countable. □

Corollary 8.4.6. The set of all computer programs is countable.

Proof sketch. Each program has a unique representation by a string over $\{0,1\}$ within a computer. So we can consider the set of all computer programs as a subset of $\{0,1\}^*$. As the latter set is countable by Proposition 8.4.5, so is the former, by Proposition 8.3.4. □

CS1231 Chapter 9

Diagonalization

9.1 Counting using functions

Example 9.1.1. $\mathbb{Z}^+$ is infinite. In fact, no function $\mathbb{Z}^+ \to \{1, 2, \ldots, n\}$, where $n \in \mathbb{Z}_{\geqslant 0}$, can be injective.

Proof. Let $n \in \mathbb{Z}_{\geqslant 0}$ and $f \colon \mathbb{Z}^+ \to \{1, 2, \ldots, n\}$. Define $f_n \colon \{1, 2, \ldots, n+1\} \to \{1, 2, \ldots, n\}$ by setting $f_n(x) = f(x)$ for all $x \in \{1, 2, \ldots, n+1\}$. Then f_n is not injective by the Pigeonhole Principle. Let $x_1, x_2 \in \{1, 2, \ldots, n+1\}$ such that $x_1 \neq x_2$ but $f_n(x_1) = f_n(x_2)$. Then $f(x_1) = f(x_2)$ by the definition of f_n. This show f is not injective.

The paragraph above shows that there is no bijection between $\mathbb{Z}^+$ and $\{1, 2, \ldots, n\}$, for any $n \in \mathbb{Z}_{\geqslant 0}$. So $\mathbb{Z}^+$ is infinite. □

Lemma 9.1.2. Let A and B be sets of the same cardinality.

(1) A is finite if and only if B is finite.

(2) A is countable if and only if B is countable.

Proof. By symmetry, it suffices to show one direction for each of the two parts. Use the definition of same-cardinality to find a bijection $f \colon A \to B$.

(1) Suppose A is finite. Then the definition of finiteness gives $n \in \mathbb{Z}_{\geqslant 0}$ and a bijection $g \colon \{1, 2, \ldots, n\} \to A$. So $f \circ g$ is a bijection $\{1, 2, \ldots, n\} \to B$ by Proposition 8.1.1(3). This shows B is finite.

(2) Suppose A is countable. If A is finite, then B is also finite by (1); thus B is countable and we are done. So suppose A is infinite. Then the definition of countability gives a bijection $g \colon \mathbb{Z}^+ \to A$. So $f \circ g$ is a bijection $\mathbb{Z}^+ \to B$ by Proposition 8.1.1(3). This shows B is countable. □

Proposition 9.1.3. Any subset A of a finite set B is finite.

Proof. As B is finite, it is countable. So A must be countable by Proposition 8.3.5. By the definition of countability, to show A is finite, it suffices to show that there is no bijection $\mathbb{Z}^+ \to A$. Like in Example 9.1.1, we will show that no function $\mathbb{Z}^+ \to A$ can be injective.

Take any $f \colon \mathbb{Z}^+ \to A$. Use the definition of finiteness to find $n \in \mathbb{Z}_{\geqslant 0}$ and a bijection $g \colon B \to \{1, 2, \ldots, n\}$. Define a function $h \colon \mathbb{Z}^+ \to \{1, 2, \ldots, n\}$ by setting $h(x) = g(f(x))$ for each $x \in \{1, 2, \ldots, n+1\}$. Then h cannot be an injection by Example 9.1.1. Let $x_1, x_2 \in \mathbb{Z}^+$ such that $x_1 \neq x_2$ but $h(x_1) = h(x_2)$. Then

$$\begin{aligned} & g(f(x_1)) = g(f(x_2)) && \text{by the definition of } h. \\ \therefore \quad & f(x_1) = f(x_2) && \text{as } g \text{ is injective.} \end{aligned}$$

Thus f is not injective. □

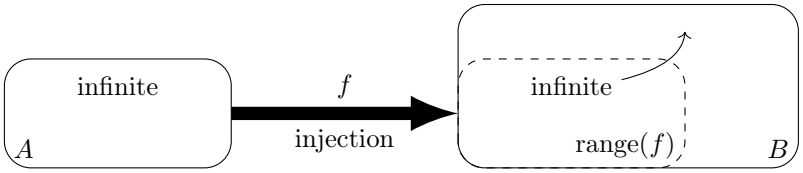


Figure 9.1: Injecting an infinite set into another set

	a_1	a_2	a_3	a_4	a_5	$\dots$
$f(a_1)$	$\boxed{\notin}$	$\in$	$\notin$	$\notin$	$\notin$	$\dots$
$f(a_2)$	$\in$	$\boxed{\notin}$	$\in$	$\notin$	$\in$	$\dots$
$f(a_3)$	$\notin$	$\in$	$\boxed{\in}$	$\notin$	$\in$	$\dots$
$f(a_4)$	$\notin$	$\notin$	$\in$	$\boxed{\notin}$	$\notin$	$\dots$
$f(a_5)$	$\in$	$\notin$	$\in$	$\in$	$\boxed{\notin}$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
R	$\in$	$\in$	$\notin$	$\in$	$\in$	$\dots$

Figure 9.2: Illustration of Cantor's diagonal argument

Corollary 9.1.4. A set B is infinite if there is an injection f from some infinite set A to B.

Proof. Note that f is a bijection $A \to \text{range}(f)$. So A has the same cardinality as $\text{range}(f)$. As A is infinite, Lemma 9.1.2(1) tells us $\text{range}(f)$ is also infinite. This implies that B is infinite by Proposition 9.1.3 because $\text{range}(f) \subseteq B$. □

Question 9.1.5. Which of the following is/are true for all sets A, B? 9a

(1) If there is a bijection $A \to B$, then A has the same cardinality as B.

(2) If there is a surjection $A \to B$ that is not an injection, then A does not have the same cardinality as B.

(3) If there is an injection $A \to B$ that is not a surjection, then A does not have the same cardinality as B.

(4) If there is a function $A \to B$ that is neither a surjection nor an injection, then A does not have the same cardinality as B.

9.2 Uncountability

Theorem 9.2.1 (Cantor 1891)**.** No set A has the same cardinality as $\mathcal{P}(A)$.

Proof. Given any function $f\colon A \to \mathcal{P}(A)$, we will produce an element of $\mathcal{P}(A)$ that is not in $\text{range}(f)$. This will show that there can be no surjection $f\colon A \to \mathcal{P}(A)$, and thus A cannot have the same cardinality as $\mathcal{P}(A)$.

Let $f\colon A \to \mathcal{P}(A)$. We claim that $\{x \in A : x \notin f(x)\} \notin \text{range}(f)$, i.e., there is no $R \in \text{range}(f)$ such that

$$\forall x \in A \quad \big(x \in R \quad \Leftrightarrow \quad x \notin f(x)\big). \tag{$*$}$$

We prove this by contradiction. Suppose $R \in \text{range}(f)$ satisfying $(*)$. As $R \in \text{range}(f)$, we obtain $a \in A$ such that $f(a) = R$. Applying $(*)$ to $x = a$ gives

$$a \in f(a) \quad \Leftrightarrow \quad a \notin f(a). \tag{$\dagger$}$$

Split into two cases.

- Case 1: assume $a \in f(a)$. Then $a \notin f(a)$ by the $\Rightarrow$ part of (†). This contradicts our assumption that $a \in f(a)$.
- Case 2: assume $a \notin f(a)$. Then $a \in f(a)$ by the $\Leftarrow$ part of (†). This contradicts our assumption that $a \notin f(a)$.

In either case, we get a contradiction. This completes the proof of the claim and thus of the theorem. □

Corollary 9.2.2. Let A be a countable infinite set. Then $\mathcal{P}(A)$ is uncountable.

Proof. According to the definition of countability, we need to show that $\mathcal{P}(A)$ is infinite, and that $\mathcal{P}(A)$ does not have the same cardinality as $\mathbb{Z}^+$.

Let $f\colon A \to \mathcal{P}(A)$ defined by setting $f(a) = \{a\}$ for each $a \in A$. Then f is injective because if $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, then $\{a_1\} = \{a_2\}$, and thus $a_1 = a_2$ by the definition of set equality. As A is infinite, Corollary 9.1.4 tells us that $\mathcal{P}(A)$ is infinite too.

As A is countable and infinite, it must have the same cardinality as $\mathbb{Z}^+$ by the definition of countability. However, Theorem 9.2.1 tells us A does not have the same cardinality as $\mathcal{P}(A)$. Thus $\mathcal{P}(A)$ cannot have the same cardinality as $\mathbb{Z}^+$ by Proposition 8.2.3. □

Corollary 9.2.3. $\mathcal{P}(\{0,1\}^*)$ is uncountable.

Proof. In view of Corollary 9.2.2, it suffices to show that $\{0,1\}^*$ is countable and infinite. We already knew $\{0,1\}^*$ is countable from Proposition 8.4.5. To show that $\{0,1\}^*$ is infinite, define $f\colon \mathbb{Z}^+ \to \{0,1\}^*$ by setting, for each $n \in \mathbb{Z}^+$,

$$f(n) = \underbrace{111\ldots1}_{n\text{-many 1's}}.$$

This f is injective because if $m, n \in \mathbb{Z}^+$ such that $f(m) = f(n)$, then

$$\underbrace{111\ldots1}_{m\text{-many 1's}} = \underbrace{111\ldots1}_{n\text{-many 1's}},$$

and so $m = n$. This shows $\{0,1\}^*$ is infinite by Example 9.1.1 and Corollary 9.1.4. □

Corollary 9.2.4. The set $\mathcal{S}$ of all functions $\{0,1\}^* \to \{0,1\}$ has the same cardinality as $\mathcal{P}(\{0,1\}^*)$. Consequently, this $\mathcal{S}$ is uncountable.

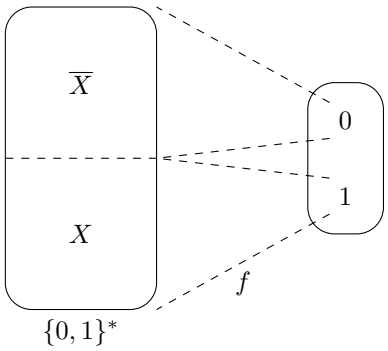


Figure 9.3: Correspondence between a subset $X \subseteq \{0,1\}^*$ and a function $f\colon \{0,1\}^* \to \{0,1\}$

Proof. Define a function $\varphi\colon \mathcal{S} \to \mathcal{P}(\{0,1\}^*)$ by setting

$$\varphi(f) = \{\sigma \in \{0,1\}^* : f(\sigma) = 1\}$$

for every $f \in \mathcal{S}$. We claim that φ is a bijection.

For surjectivity, pick any $X \subseteq \mathcal{P}(\{0,1\}^*)$. Define $f \in \mathcal{S}$ by setting, for each $\sigma \in \{0,1\}^*$,

$$f(\sigma) = \begin{cases} 1, & \text{if } \sigma \in X; \\ 0, & \text{if } \sigma \notin X. \end{cases}$$

Then $\varphi(f) = \{\sigma \in \{0,1\}^* : f(\sigma) = 1\} = X$.

For injectivity, let $f, g \in \mathcal{S}$ such that $\varphi(f) = \varphi(g)$. This means

$$\{\sigma \in \{0,1\}^* : f(\sigma) = 1\} = \{\sigma \in \{0,1\}^* : g(\sigma) = 1\}$$

by the definition of φ. So $f(\sigma) = 1$ if and only if $g(\sigma) = 1$ for all $\sigma \in \{0,1\}^*$. Moreover, for all $\sigma \in \{0,1\}^*$,

$$f(\sigma) = 0 \quad \Leftrightarrow \quad f(\sigma) \neq 1 \quad \Leftrightarrow \quad g(\sigma) \neq 1 \quad \Leftrightarrow \quad g(\sigma) = 0$$

because the codomains of f and g are both $\{0,1\}$. Hence $f = g$ by Proposition 7.2.6. □

Exercise 9.2.5. Which of the following is/are countable? Justify your answer. 9b

(1) $\mathbb{Z}$.

(2) $\mathbb{Q}$.

(3) $\mathbb{R}$.

(4) $\mathbb{C}$.

(5) The set of all finite sets of integers.

(6) The set of all strings over $\{0,1\}$.

(7) The set of all infinite sequences over $\{0,1\}$.

(8) The set of all functions $A \to B$ where A, B are finite sets of integers.

(9) The set of all computer programs.

9.3 Computability

Corollary 9.3.1. A set B is uncountable if there is an injection f from some uncountable set A to B.

Proof. Note that f is a bijection $A \to \text{range}(f)$. So A has the same cardinality as range(f). As A is uncountable, Lemma 9.1.2(2) tells us range(f) is also uncountable. This implies that B is uncountable by Proposition 8.3.5 because range$(f) \subseteq B$. □

Assumption 9.3.2. Our programs have no time and memory limitation.

Corollary 9.3.3. There is a function $\{0,1\}^* \to \{0,1\}$ that cannot be computed by any program.

Proof. Suppose that every function $\{0,1\}^* \to \{0,1\}$ is computed by a program. For each $f\colon \{0,1\}^* \to \{0,1\}$, let $\psi(f)$ be the smallest program that computes f. This defines a function $\psi\colon \mathcal{S} \to \{0,1\}^*$, where $\mathcal{S}$ is the set of all functions $\{0,1\}^* \to \{0,1\}$ as in Corollary 9.2.4. The function ψ is injective because if $f, g \in \mathcal{S}$ such that $\psi(f) = \psi(g)$, then f and g are computed by the same program, and thus $f = g$. Recall that $\mathcal{S}$ is uncountable by Corollary 9.2.4. So Corollary 9.3.1 implies $\{0,1\}^*$ is uncountable as well. This contradicts the countability of $\{0,1\}^*$ from Proposition 8.4.5. □

Theorem 9.3.4 (Turing 1936)**.** There is no program that computes the function $h\colon \{0,1\}^* \to \{0,1\}$ satisfying

$$h(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is a program that does not stop on the empty input;} \\ 0, & \text{otherwise} \end{cases}$$

for all $\sigma \in \{0,1\}^*$.

Proof. Suppose not. Use a program that computes h to devise a program R satisfying

$$\forall \sigma \in \{0,1\}^* \quad \Big(R \text{ stops on input } \sigma \quad \Leftrightarrow \quad \begin{array}{l} \sigma \text{ is a program that does} \\ \text{not stop on input } \sigma \end{array} \Big). \tag{‡}$$

Applying (‡) to $\sigma = R$ gives

$$R \text{ stops on input } R \quad \Leftrightarrow \quad \begin{array}{l} R \text{ is a program that does} \\ \text{not stop on input } R \end{array} \tag{§}$$

Split into two cases.

- Case 1: assume R stops on input R. Then R does not stop on input R by the $\Rightarrow$ part of (§). This contradicts our assumption that R stops on input R.
- Case 2: assume R does not stop on input R. Then R stops on input R by the $\Leftarrow$ part of (§). This contradicts our assumption that R does not stop on input R.

In either case, we get a contradiction, as required. □

Church–Turing Thesis (informal version)**.** If a function : $\mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ can be computed by a program, then it can be computed by a program that uses *only* the following:

- the constants 0 and 1;
- variables that range over $\mathbb{Z}_{\geqslant 0}$;
- equalities $=$ and inequalities $\leqslant$;
- addition $+$ and multiplication $\times$;
- propositional logical connectives, i.e., **and**, **or**, **not**, and **if-then-else**; and
- **for**-loops and **while**-loops.

Answers to selected exercises

4a, page 2

(1) We want to prove that $E = \mathbb{Z}^+$, where $E = \{x + 1 : x \in \mathbb{Z}_{\geqslant 0}\}$.

Proof. ($\Rightarrow$) Let $z \in E$. Use the definition of E to find $x \in \mathbb{Z}_{\geqslant 0}$ such that $x + 1 = z$. Then $x \in \mathbb{Z}$ and $x \geqslant 0$ by the definition of $\mathbb{Z}_{\geqslant 0}$. As $x \in \mathbb{Z}$, we know $x + 1 \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under $+$. As $x \geqslant 0$, we know $x + 1 \geqslant 0 + 1 = 1 > 0$. So $z = x + 1 \in \mathbb{Z}^+$ by the definition of $\mathbb{Z}^+$.

($\Leftarrow$) Let $z \in \mathbb{Z}^+$. Then $z \in \mathbb{Z}$ and $z > 0$. Define $x = z - 1$. As $z \in \mathbb{Z}$, we know $x \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under $-$. As $z > 0$, we know $x = z - 1 > 0 - 1 = -1$, and thus $x \geqslant 0$ as $x \in \mathbb{Z}$. So $x \in \mathbb{Z}_{\geqslant 0}$ by the definition of $\mathbb{Z}_{\geqslant 0}$. Hence the definition of E tells us $z = x + 1 \in E$. □

(2) We want to prove that $F = \mathbb{Z}$, where $F = \{x - y : x, y \in \mathbb{Z}_{\geqslant 0}\}$.

Proof. ($\Rightarrow$) Let $z \in F$. Use the definition of F to find $x, y \in \mathbb{Z}_{\geqslant 0}$ such that $x - y = z$. Then $x, y \in \mathbb{Z}$ by the definition of $\mathbb{Z}_{\geqslant 0}$. So $z = x - y \in \mathbb{Z}$ as $\mathbb{Z}$ is closed under $-$.

($\Leftarrow$) Let $z \in \mathbb{Z}$.

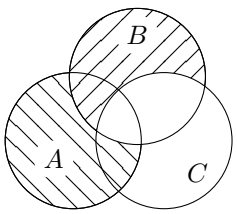
- Case 1: suppose $z \geqslant 0$. Let $x = z$ and $y = 0$. Then $x, y \in \mathbb{Z}_{\geqslant 0}$. So $z = z - 0 = x - y \in F$ by the definition of F.
- Case 2: suppose $z < 0$. Let $x = 0$ and $y = -z$. Then $x, y \in \mathbb{Z}_{\geqslant 0}$ as $z < 0$. So $z = 0 - (-z) = x - y \in F$ by the definition of F.

So $z \in F$ in all the cases. □

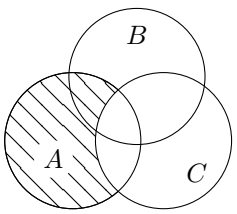
4b, page 3

- $\{1\} \in C$ but $\{1\} \not\subseteq C$;
- $\{2\} \notin C$ but $\{2\} \subseteq C$;
- $\{3\} \in C$ and $\{3\} \subseteq C$; and
- $\{4\} \notin C$ and $\{4\} \not\subseteq C$.

4c, page 6



$(A \setminus B) \cup (B \setminus C)$



$A \setminus C$

No. For a counterexample, let $A = C = \varnothing$ and $B = \{1\}$. Then

$$(A \setminus B) \cup (B \setminus C) = \varnothing \cup \{1\} = \{1\} \neq \varnothing = A \setminus C.$$

✎ 4d, page 6

Ideas. (1) The set of all sets?

(2) $\Big\{\Big\{\Big\{\{\{\dots\ \dots\}\}\Big\}\Big\}\Big\}$?

✎ 4e, page 7

Maybe, but is it better?

Proof. Take any set R. Split into two cases.

- Case 1: assume $R \in R$. Then $\sim(R \notin R)$. So $\sim(R \in R \Rightarrow R \notin R)$. Hence
$$\exists x \sim(x \in R \quad \Leftrightarrow \quad x \notin x).$$
- Case 2: assume $R \notin R$. Then $\sim(R \in R)$. So $\sim(R \notin R \Rightarrow R \in R)$. Hence
$$\exists x \sim(x \in R \quad \Leftrightarrow \quad x \notin x).$$

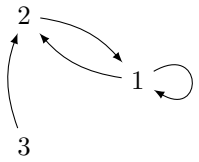
In either case, we showed $\sim\forall x\ (x \in R \Leftrightarrow x \notin x)$. So the proof is finished. □

✎ 5a, page 12

No. For instance, we have $(2, 2) \in R \circ S$ but $(2, 2) \notin S \circ R$.

✎ 6a, page 16

The arrow diagram below represents the relation R in the exercise:



This relation is not reflexive because $2 \not R\ 2$. It is not symmetric because $3\ R\ 2$ but $2 \not R\ 3$. It is not transitive because $2\ R\ 1$ and $1\ R\ 2$ but $2 \not R\ 2$.

✎ 6b, page 16

Proof. ($\Rightarrow$) Assume R is transitive. Let $(x, z) \in R \circ R$. Use the definition of $R \circ R$ to find $y \in A$ such that $(x, y) \in R$ and $(y, z) \in R$. This means $x\ R\ y$ and $y\ R\ z$. So $x\ R\ z$ by the transitivity of R. Hence $(x, z) \in R$.

($\Leftarrow$) Assume $R \circ R \subseteq R$. Let $x, y, z \in A$ such that $x\ R\ y$ and $y\ R\ z$. This means $(x, y) \in R$ and $(y, z) \in R$. So $(x, z) \in R \circ R$ by the definition of $R \circ R$. Our assumption then implies $(x, z) \in R$. Hence $x\ R\ z$. □

6c, page 17

Yes, as shown below.

We know $x \in [x]$ by Lemma 6.3.4(1). So $x \in S \cap [x]$ by the hypothesis. This implies $S \cap [x] \neq \varnothing$. Hence $S = [x]$ by Lemma 6.3.5. □

6d, page 18

The divisibility relation on $\mathbb{Z}$ is not antisymmetric because $1 \mid -1$ and $-1 \mid 1$, but $1 \neq -1$.

6e, page 18

The divisibility relation on $\mathbb{Z}^+$ is antisymmetric, as shown below. So it is a partial order by Example 6.2.8. It is not total because $2 \nmid 3$ and $3 \nmid 2$.

Proof of antisymmetry. Let us first show that if $a, b \in \mathbb{Z}^+$ such that $a \mid b$, then $a \leqslant b$. Let $a, b \in \mathbb{Z}^+$ such that $a \mid b$. Then the definition of divisibility gives $k \in \mathbb{Z}$ such that $b = ak$. Note $k = b/a > 0$ as both a and b are positive. Since $k \in \mathbb{Z}$, this implies $k \geqslant 1$. Thus $b = ak \geqslant a \times 1 = a$, as required.

Now let $a, b \in \mathbb{Z}^+$ such that $a \mid b$ and $b \mid a$. Then the previous paragraph tells us $a \leqslant b$ and $b \leqslant a$. So $a = b$. □

7a, page 22

Only (b), (d) and (f) represent functions.

7b, page 24

(1) Yes, because $(f \circ f)(x) = f(f(x)) = f(1231) = 1231 = f(x)$ for all $x \in \mathbb{Z}$ in this case.

(2) Yes, because $(f \circ f)(x) = f(f(x)) = f(x)$ for all $x \in \mathbb{Z}$ in this case.

(3) No, because $(f \circ f)(1) = f(f(1)) = f(-1) = 1 \neq -1 = f(1)$ in this case.

(4) No, because $(f \circ f)(0) = f(f(0)) = f(1) = 4 \neq 1 = f(0)$ in this case.

(5) No, because $(f \circ f)(2) = f(f(2)) = f(4) = 16 \neq 4 = f(2)$ in this case.

7c, page 25

(b) is a surjection but not an injection; (d) is an injection but not a surjection; and (f) is both an injection and a surjection. Thus only the last one is a bijection.

8a, page 29

Proof of the converse to Theorem 8.1.2. Suppose $n \leqslant m$. Define $f\colon A \to B$ by setting $f(x_i) = y_i$ for each $i \in \{1, 2, \ldots, n\}$. This definition is unambiguous because the x's are different. To show injectivity, suppose $i, j \in \{1, 2, \ldots, n\}$ such that $f(x_i) = f(x_j)$. The definition of f tells us $f(x_i) = y_i$ and $f(x_j) = y_j$. Then $y_i = f(x_i) = f(x_j) = y_j$. So $i = j$ because the y's are different. This implies $x_i = x_j$. □

Proof of the converse to Theorem 8.1.3. Suppose $n \geqslant m > 0$. Define $f\colon A \to B$ by setting, for each $i \in \{1, 2, \ldots, n\}$,

$$f(x_i) = \begin{cases} y_i, & \text{if } i \leqslant m; \\ y_m, & \text{otherwise.} \end{cases}$$

This definition is unambiguous because the x's are different. It is surjective because given any $y_i \in B$, we have $x_i \in A$ such that $f(x_i) = y_i$. □

9a, page 35

(1) True. This follows directly from Definition 8.2.1.

(2) False. The $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ satisfying $f(1) = 1$ and $f(x+1) = x$ for each $x \in \mathbb{Z}^+$ is a surjection that is not an injection, but $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+$.

(3) False. The $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ satisfying $f(x) = x+1$ for each $x \in \mathbb{Z}^+$ is an injection that is not a surjection, but $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+$.

(4) False. The function $f\colon \{0,1\} \to \{0,1\}$ satisfying $f(0) = 0 = f(1)$ is neither a surjection nor an injection, but $\{0,1\}$ has the same cardinality as $\{0,1\}$.

Extra exercise. Show that (2) and (3) both become true if we restrict ourselves to finite sets A, B.

9b, page 37

(1) This is Proposition 8.4.3.

(2) This is Question 4 in Tutorial 8.

(3) As $\mathbb{Z}^+ \subseteq \mathbb{R}$, we know $\mathbb{R}$ is infinite by Example 9.1.1 and Proposition 9.1.3. So it suffices to show that no function $\mathbb{Z}^+ \to \mathbb{R}$ is surjective. We imitate the proof of Theorem 9.2.1. Let $f\colon \mathbb{Z}^+ \to \mathbb{R}$. For each $i, j \in \mathbb{Z}^+$, let $d_{i,j}$ be the jth digit after the decimal point in a decimal representation of $f(i)$. Let $r \in \{x \in \mathbb{R} : 0 < x < 1\}$ whose ith digit d_i after the decimal point in the decimal representation of r is given by

$$d_i = \begin{cases} 2, & \text{if } d_{i,i} = 3; \\ 3, & \text{if } d_{i,i} \neq 3, \end{cases}$$

for each $i \in \mathbb{Z}^+$. Then

$$\forall i \in \mathbb{Z}^+ \quad \left(\begin{array}{l} \text{the } i\text{th digit after the decimal point} \\ \text{in a decimal representation of } r \text{ is } 3 \\ \quad \Leftrightarrow \quad \text{the } i\text{th digit after the decimal point} \\ \qquad \text{in a decimal representation of } f(i) \text{ is not } 3 \end{array} \right).$$

It can then be verified that $r \neq f(i)$ for each $i \in \mathbb{Z}^+$. Thus f is not surjective.

(4) As $\mathbb{R} \subseteq \mathbb{C}$, this follows from (3) and Corollary 9.1.4.

(5) This follows from Question 3 and Question 8 in Tutorial 8.

(6) This is Proposition 8.4.5.

(7) We may represent an infinite sequence $a_1, a_2, a_3, \ldots$ over $\{0,1\}$ by the function $a\colon \mathbb{Z}^+ \to \{0,1\}$ satisfying $a(i) = a_i$ for each $i \in \mathbb{Z}^+$. Having noted this, the uncountability proof is the same as that of Corollary 9.2.4, except that $\{0,1\}^*$ is replaced by $\mathbb{Z}^+$.

(8) By Proposition 8.4.3, we know $\mathbb{Z}$ has the same cardinality as $\mathbb{Z}^+$. Therefore, using Theorem 8.4.4, one can show that $\mathbb{Z} \times \mathbb{Z}$ has the same cardinality as $\mathbb{Z}$. Hence, as in the proof of (5), one has the countability of $\mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$, where $\mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$ denotes the set of all finite subsets of $\mathbb{Z} \times \mathbb{Z}$. Every function $A \to B$, where A, B are finite sets of integers, are elements of $\mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$. So the set of all such functions is a subset of the countable set $\mathcal{P}_\omega(\mathbb{Z} \times \mathbb{Z})$, and thus must itself be countable by Proposition 8.3.4.

(9) This is Corollary 8.4.6.