Chapter 1

Naive Set Theory

Theoretical Foundations of Computer Science
Last update of lecture notes: Saturday, October 29, 2005
Last update of this chapter: Friday, August 26, 2005.

1.1 Sets

1.1.1 Notation
We often use the symbol $\implies$ in place of the English word "implies". We also often use the symbol $\iff$ in place of the English words "if and only if".

1.1.2 Notation
Let x and y be two objects. We write $x = y$ when x and y are equal, that is, when they are precisely the same object. We write $x \neq y$ when x and y are not equal.

1.1.3 Definition
A set is a collection of objects sharing a common property.

1.1.4 Notation
We write $x \in A$ when the object x belongs to the set A; otherwise we write $x \notin A$.

1.1.5 Notation
A set can be specified by stating the common property of its objects. In particular, we write

$$A = \{x \mid P(x)\}$$

when A is the set of all objects x that have the property P.

1.1.6 Example
Using the method described in Notation 1.1.5, we can specify the following sets:

$$\begin{aligned}
\textit{Rainbow} &= \{x \mid x \text{ is a color of the rainbow }\}, \\
\textit{Planets} &= \{x \mid x \text{ is a planet of the solar system }\}, \\
\textit{Suits} &= \{x \mid x \text{ is a suit in an Anglo-French deck of cards }\}, \\
\textit{Vowels} &= \{x \mid x \text{ is a vowel of the Latin alphabet}\}, \\
\textit{Letters} &= \{x \mid x \text{ is a letter of the Latin alphabet}\}, \\
\textit{Even} &= \{x \mid x \text{ is an even natural number }\}, \\
\textit{Odd} &= \{x \mid x \text{ is an odd natural number }\}, \\
\textit{Prime} &= \{x \mid x \text{ is a prime natural number }\}.
\end{aligned}$$

1.1.7 Notation
If the number of its objects is finite, a set can be specified by listing its objects between braces. In particular, we write

$$A = \{x_1, \ldots, x_n\}$$

when A contains the objects x_1, ..., x_n, and nothing else.

1.1.8 Example
Using the method described in Notation 1.1.7, we can specicy the following sets:

$$\begin{aligned}
\textit{Rainbow} &= \{\text{red}, \text{orange}, \text{yellow}, \text{green}, \text{blue}, \text{indigo}, \text{violet}\}, \\
\textit{Planets} &= \{\text{Mercury}, \text{Venus}, \text{Earth}, \text{Mars}, \text{Jupiter}, \text{Saturn}, \text{Uranus}, \text{Neptune}, \text{Pluto}\}, \\
\textit{Suits} &= \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}, \\
\textit{Vowels} &= \{\text{a}, \text{e}, \text{i}, \text{o}, \text{u}\}, \\
\textit{Letters} &= \{\text{a}, \text{b}, \text{c}, \text{d}, \text{e}, \text{f}, \text{g}, \text{h}, \text{i}, \text{j}, \text{k}, \text{l}, \text{m}, \text{n}, \text{o}, \text{p}, \text{q}, \text{r}, \text{s}, \text{t}, \text{u}, \text{v}, \text{w}, \text{x}, \text{y}, \text{z}\}.
\end{aligned}$$

1.1.9 Notation
Sometimes, we may informally specify a set by listing some of its objects, and then let the context help us "figure out" the rest. In particular, we write

$$A = \{x_1, x_2, x_3, \ldots, \}$$

when A contains the objects x_1, x_2, x_3, as well as other objects more or less determined by the context. This method is convenient when the number of objects of the set is infinite. It is also convenient when the number of objects of the set if finite but "large".

1.1.10 Notation
Using the method described in Notation 1.1.9, we can informally specify the following sets

$$\begin{aligned}
\textit{Letters} &= \{\text{a}, \text{b}, \text{c}, \ldots\}, \\
\textit{Even} &= \{0, 2, 4, \ldots\}, \\
\textit{Odd} &= \{1, 3, 5, \ldots\}.
\end{aligned}$$

1.1.11 Notation
We use the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ to denote the following sets of numbers:

- $\mathbb{N} = \{0, 1, 2, \ldots, \}$ is the set of natural numbers.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of integer numbers.
- $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.
- $\mathbb{C} = \left\{ a + ib \mid a, b \in \mathbb{R} \text{ and } i = \sqrt{-1} \right\}$ is the set of complex numbers.

1.1.12 Axiom
Let A and B be sets. Then the following are equivalent:

1. *$A = B$;*
2. *$x \in A \iff x \in B$, for all objects x.*

1.1.13 Example
Axiom 1.1.12 implies that when we specify a set by listing its objects, their order does not matter. For instance, we have

$$\mathit{Suits} = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\} = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\},$$

and

$$\mathit{Vowels} = \{\mathrm{a}, \mathrm{e}, \mathrm{i}, \mathrm{o}, \mathrm{u}\} = \{\mathrm{u}, \mathrm{o}, \mathrm{i}, \mathrm{e}, \mathrm{a}\}.$$

Axiom 1.1.12 also implies that repetitions do not matter too. For instance:

$$\mathit{Suits} = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\} = \{\spadesuit, \spadesuit, \heartsuit, \diamondsuit, \clubsuit\}.$$

1.1.14 Definition
A set is EMPTY if it has no objects.

1.1.15 Notation
Axiom 1.1.12 implies that there is only one empty set. We denote it with the symbol $\varnothing$.

1.2 Subsets

1.2.1 Definition
Let A and B be sets. We say that A is a SUBSET of B, written $A \subseteq B$, if all objects of A are also objects of B. Thus,

$$A \subseteq B$$

whenever

$$x \in A \implies x \in B, \qquad \text{for all objects } x.$$

1.2.2 Example
Let

$$\begin{aligned} \mathit{Vowels} &= \{x \mid x \text{ is a vowel of the Latin alphabet}\}, \\ \mathit{Letters} &= \{x \mid x \text{ is a letter of the Latin alphabet}\}. \end{aligned}$$

Then:

$$\mathit{Vowels} \subseteq \mathit{Letters}.$$

1.2.3 Proposition
$\varnothing \subseteq A$, for all sets A.

PROOF. Immediate.

1.2.4 Proposition
Let A, B, and C be sets. Then the following properties hold:

$$\begin{aligned} &A \subseteq A, && (\textit{reflexivity}) \\ &A \subseteq B \text{ and } B \subseteq A \implies A = B, && (\textit{antisymmetry}) \\ &A \subseteq B \text{ and } B \subseteq C \implies A \subseteq C, && (\textit{transitivity}). \end{aligned}$$

PROOF. Reflexivity is immediate. Antisymmetry follows by Axiom 1.1.12. Concerning transitivity, suppose that $A \subseteq B$ and $B \subseteq C$. Then we have

$$\begin{aligned} x \in A &\implies x \in B && \text{since } A \subseteq B \\ &\implies x \in C && \text{since } B \subseteq C. \end{aligned}$$

Thus,

$$x \in A \implies x \in C, \qquad \text{for all objects } x,$$

which implies $A \subseteq C$.

1.2.5 Definition
Let A and B be set. We say that A is a PROPER SUBSET of B, written $A \subset B$, if $A \subseteq B$ and $A \neq B$.

1.2.6 Example
Let

$$\begin{aligned} \mathit{Vowels} &= \{x \mid x \text{ is a vowel of the Latin alphabet}\}, \\ \mathit{Letters} &= \{x \mid x \text{ is a letter of the Latin alphabet}\}. \end{aligned}$$

Then:

$$\mathit{Vowels} \subset \mathit{Letters}.$$

1.2.7 Notation
Given two sets A and B, we let:

$$\begin{aligned}
A \supseteq B &\iff A \subseteq B\,,\\
A \supset B &\iff B \subset A\,,\\
A \nsubseteq B &\iff \text{not } A \subseteq B\,,\\
A \not\subset B &\iff \text{not } A \subset B\,,\\
A \not\supseteq B &\iff \text{not } A \supseteq B\,,\\
A \not\supset B &\iff \text{not } A \supset B\,.
\end{aligned}$$

1.2.8 Definition
Let A be a set. The POWER SET of A is the set

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}\,.$$

1.2.9 Example
Let $x \neq y$ and $A = \{x, y\}$. Then

$$\mathcal{P}(A) = \{\varnothing, \{x\}, \{y\}, A\}\,.$$

1.3 Set operators

1.3.1 Definition
Let A and B be sets. The UNION of A and B is the set

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

1.3.2 Example
Let

$$\begin{aligned}
\mathit{Even} &= \{0, 2, 4, \ldots\}\,,\\
\mathit{Digits} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}\,.
\end{aligned}$$

Then:

$$\mathit{Even} \cup \mathit{Digits} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, \ldots\}\,.$$

1.3.3 Proposition
Let A and B be sets. Then the following are equivalent:

1. $A \subseteq B$.
2. $A \cup B = B$.

PROOF. ($1 \implies 2$). Suppose that $A \subseteq B$. Then clearly $B \subseteq A \cup B$. On the other hand, if $x \in A \cup B$ then either $x \in A$ or $x \in B$, and in both cases we have $x \in B$.

($2 \implies 1$). Suppose that $A \cup B = B$ and let $x \in A$. Then $x \in A \cup B$, which implies $x \in B$.

1.3.4 Proposition
Let A, B, and C be sets. Then the following properties hold:

$$\begin{aligned} A \cup A &= A\,, && (\textit{idempotency}) \\ A \cup B &= B \cup A\,, && (\textit{commutativity}) \\ (A \cup B) \cup C &= A \cup (B \cup C)\,, && (\textit{associativity})\,. \end{aligned}$$

PROOF. Concerning idempotency, we have

$$\begin{aligned} x \in A \cup A &\iff x \in A \text{ or } x \in A \\ &\iff x \in A\,. \end{aligned}$$

Concerning commutativity, we have

$$\begin{aligned} x \in A \cup B &\iff x \in A \text{ or } x \in B \\ &\iff x \in B \text{ or } x \in A \\ &\iff x \in B \cup A\,. \end{aligned}$$

Concerning associativity, we have

$$\begin{aligned} x \in (A \cup B) \cup C &\iff x \in A \cup B \text{ or } x \in C \\ &\iff x \in A \text{ or } x \in B \text{ or } x \in C \\ &\iff x \in A \text{ or } x \in B \cup C \\ &\iff x \in A \cup (B \cup C)\,. \end{aligned}$$

1.3.5 Notation
Since by Proposition 1.3.4 the set operator $\cup$ is associative, we can conveniently drop the parenthesis when writing set expressions like $A \cup B \cup C$.

1.3.6 Definition
Let A and B be sets. The INTERSECTION of A and B is the set

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

1.3.7 Example
Let

$$\begin{aligned} \mathit{Even} &= \{0, 2, 4, \ldots\}\,, \\ \mathit{Digits} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}\,. \end{aligned}$$

Then:

$$\mathit{Even} \cap \mathit{Digits} = \{0, 2, 4, 6, 8\}\,.$$

1.3.8 Definition
Two sets A and B are DISJOINT if $A \cap B = \varnothing$.

1.3.9 Example
The sets

$$Even = \{0, 2, 4, \ldots\},$$

and

$$Odd = \{1, 3, 5, \ldots\},$$

are disjoint.

1.3.10 Proposition
Let A and B be sets. Then the following are equivalent:

1. $A \subseteq B$.
2. $A \cap B = A$.

PROOF. (1 $\implies$ 2). Suppose that $A \subseteq B$. Then clearly $A \cap B \subseteq A$. On the other hand, if $x \in A$ then $x \in B$, and therefore $x \in A \cap B$.

(2 $\implies$ 1). Suppose that $A \cap B = A$ and let $x \in A$. Then $x \in A \cap B$, which implies $x \in B$.

1.3.11 Proposition
Let A, B, and C be sets. Then the following properties hold:

$$\begin{aligned} A \cap A &= A, && (\textit{idempotency}) \\ A \cap B &= B \cap A, && (\textit{commutativity}) \\ (A \cap B) \cap C &= A \cap (B \cap C), && (\textit{associativity}). \end{aligned}$$

PROOF. Concerning idempotency, we have

$$\begin{aligned} x \in A \cap A &\iff x \in A \text{ and } x \in A \\ &\iff x \in A. \end{aligned}$$

Concerning commutativity, we have

$$\begin{aligned} x \in A \cap B &\iff x \in A \text{ and } x \in B \\ &\iff x \in B \text{ and } x \in A \\ &\iff x \in B \cap A. \end{aligned}$$

Concerning associativity, we have

$$\begin{aligned} x \in (A \cap B) \cap C &\iff x \in A \cap B \text{ and } x \in C \\ &\iff x \in A \text{ and } x \in B \text{ and } x \in C \\ &\iff x \in A \text{ and } x \in B \cap C \\ &\iff x \in A \cap (B \cap C). \end{aligned}$$

1.3.12 Notation
Since by Proposition 1.3.11 the set operator $\cap$ is associative, we can conveniently drop the parenthesis when writing set expressions like $A \cap B \cap C$.

1.3.13 Proposition
Let A, B, and C be sets. Then the following properties hold:

$$\begin{aligned}
&A \cup (A \cap B) = A\,, && (\textit{absorption of } \cup \textit{ over } \cap)\\
&A \cap (A \cup B) = A\,, && (\textit{absorption of } \cap \textit{ over } \cup)\\
&A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\,, && (\textit{distributivity of } \cup \textit{ over } \cap)\\
&A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\,, && (\textit{distributivity of } \cap \textit{ over } \cap)\,.
\end{aligned}$$

PROOF. Concerning the absorption of $\cup$ over $\cap$, suppose first that $x \in A \cup (A \cap B)$. Then $x \in A$ or $x \in A \cap B$, and in both cases we have $x \in A$. Conversely, if $x \in A$ we clearly have $x \in A \cup (A \cap B)$.

The absorption of $\cap$ over $\cup$ is proved similarly to the absorption of $\cup$ over $\cap$.

Concerning the distributivity of $\cup$ over $\cap$, Suppose first that $x \in A \cup (B \cap C)$. If $x \in A$ we have $x \in A \cup B$ and $x \in A \cup C$, which implies $x \in (A \cup B) \cap (A \cup C)$. If instead $x \notin A$ we have $x \in B \cap C$, which implies $x \in B$ and $x \in C$, which implies $x \in A \cup B$ and $x \in A \cup C$, which implies $x \in (A \cup B) \cap (A \cup C)$.

Conversely, suppose that $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in (A \cup C)$. If $x \in A$, then clearly $x \in A \cup (B \cap C)$. If instead $x \notin A$, we have $x \in B$ and $x \in C$, which implies $x \in B \cap C$, which implies $x \in A \cup (B \cap C)$.

The distributivity of $\cap$ over $\cup$ is proved similarly to the distributivity of $\cup$ over $\cap$.

1.3.14 Definition
Let A and B be sets. The DIFFERENCE of A and B is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}\,.$$

1.3.15 Example
Let

$$\begin{aligned}
\mathit{Even} &= \{0, 2, 4, \ldots\}\,,\\
\mathit{Digits} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}\,.
\end{aligned}$$

Then:

$$\begin{aligned}
\mathit{Even} - \mathit{Digits} &= \{10, 12, 14, \ldots\}\,,\\
\mathit{Digits} - \mathit{Even} &= \{1, 3, 5, 7, 9\}\,.
\end{aligned}$$

1.3.16 Proposition
Let A and B be sets. Then the following are equivalent:

1. $A \subseteq B$.
2. $A - B = \varnothing$.

PROOF. ($1 \implies 2$). Suppose by contradiction that $A - B \neq \varnothing$. Then there exists $x \in A - B$. It follows that $x \in A$ and $x \notin B$. Since $A \subseteq B$ we have $x \in B$, a contradiction.

($2 \implies 1$). Suppose by contradiction that $A \nsubseteq B$. Then there exists $x \in A$ such that $x \notin B$. It follows that $x \in A - B$, which implies $A - B \neq \varnothing$, a contradiction.

1.3.17 Proposition
Let A, B, and C be sets. Then the following properties hold:

$$A - (B \cup C) = (A - B) \cap (A - C), \qquad (\textit{de Morgan law for } \cup)$$
$$A - (B \cap C) = (A - B) \cup (A - C), \qquad (\textit{de Morgan law for } \cap).$$

PROOF. Concerning the de Morgan law of $\cup$, suppose first that $x \in A - (B \cup C)$. Then $x \in A$ and $x \notin B \cup C$. If follows that $x \notin B$ and $x \notin C$. Therefore, $x \in A - B$ and $x \in A - C$, which implies $x \in (A - B) \cap (A - C)$.

Conversely, suppose that $x \in (A - B) \cap (A - C)$. Then $x \in A - B$ and $x \in A - C$. It follows that $x \in A$ and $x \notin B$ and $x \notin C$. But then $x \notin B \cup C$. Thus, $x \in A - (B \cup C)$.

The de Morgan law for $\cap$ is proved similarly to the de Morgan law for $\cup$.

1.4 Ordered pairs

1.4.1 Definition
An ORDERED PAIR is a collection of the form

$$(a, b),$$

where a is the first object and b is the second objects.

1.4.2 Axiom
Let (a, b) and (c, d) be ordered pairs. Then the following are equivalent:

1. *$(a, b) = (c, d)$;*
2. *$a = c$ and $b = d$.*

1.4.3 Definition
Let A and B be sets. The CARTESIAN PRODUCT of A and B is the set

$$A \times B = \{(a, b) \mid a \in A \text{ and } a \in B\}.$$

1.4.4 Notation
If A is a set, we let $A^2 = A \times A$.

1.5 Functions

1.5.1 Definition
Let A and B be nonempty sets. A FUNCTION

$$f : A \to B$$

from A to B is a correspondence that associates, to each object $a \in A$, a unique object $f(a) \in B$.

1.5.2 Axiom
Let $f : A \to B$ and $g : C \to D$ be functions. Then the following are equivalent:

1. *$f = g$.*
2. *$A = C$ and $B = D$ and*

$$f(a) = g(a)\,, \qquad \text{for all } a \in A\,.$$

1.5.3 Definition
Let $f : A \to B$ be a function. Then:

- The DOMAIN of f is the set A.
- The CODOMAIN of f is the set B.
- The RANGE of f is the set

$$\mathit{range}(f) = \{f(a) \mid a \in A\}\,.$$

1.5.4 Notation
Let A and B be nonempty sets. We denote with B^A the set of all functions whose domain is A and codomain is B.

1.5.5 Definition
A function $f : A \to B$ is INJECTIVE if

$$f(a_1) = f(a_2) \implies a_1 = a_2\,, \qquad \text{for all } a_1, a_2 \in A.$$

1.5.6 Notation
We write $f : A \hookrightarrow B$ to emphasize that the function f is injective.

1.5.7 Definition
A function $f : A \to B$ is SURJECTIVE if for every $b \in B$ there exists an $a \in A$ such that $b = f(a)$.

1.5.8 Notation
We write $f : A \twoheadrightarrow B$ to emphasize that the function f is surjective.

1.5.9 Proposition
Let $f : A \to B$ be a function. Then the following are equivalent.

1. *f is surjective;*

2. *$range(f) = B$.*

PROOF. (1 $\implies$ 2). Let $b \in range(f)$. Then there exists $a \in A$ such that $b = f(a)$. Thus, $b \in B$.

Conversely, let $b \in B$. Since f is surjective, there exists $a \in A$ such that $b = f(a)$. Thus, $b \in range(f)$.

(2 $\implies$ 1). Let $b \in B$. Then $b \in range(f)$, which implies that there exists $a \in A$ such that $b = f(a)$. Since b is arbitrary, it follows that f is surjective.

1.5.10 Definition
A function $f : A \to B$ is BIJECTIVE if it is both injective and surjective.

1.5.11 Notation
We write $f : A \rightarrowtail\!\!\!\!\!\rightarrow B$ to emphasize that the function f is bijective.

1.5.12 Definition
Let $f : A \to B$ and $g : B \to C$ be functions. The COMPOSITION of f and g is the function

$$g \circ f : A \to C$$

defined by letting

$$(g \circ f)(a) = g(f(a)), \qquad \text{for all } a \in A.$$

1.5.13 Proposition
Let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be functions. Then

$$h \circ (g \circ f) = (h \circ g) \circ f, \qquad (\textit{associativity}).$$

PROOF. Let $a \in A$. Then

$$\begin{aligned}(h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a).\end{aligned}$$

1.5.14 Definition
Let A be a nonempty set. The IDENTITY FUNCTION of A is the function

$$\mathbf{I}_A : A \to A$$

defined by letting

$$\mathbf{I}_A(a) = a, \qquad \text{for all } a \in A.$$

1.5.15 Proposition
Let $A \neq \varnothing$. Then $\mathbf{I}_A$ is a bijective function.

PROOF. We want to show that $\mathbf{I}_A$ is both injective and surjective. To show that f is injective, note that $\mathbf{I}_A(a_1) = \mathbf{I}_A(a_2) \implies a_1 = a_2$. To show that $\mathbf{I}_A$ is surjective, note that if $b \in A$ then $b = \mathbf{I}_A(b)$.

1.5.16 Proposition
Let $f : A \to B$ be a function. Then

(i) $f \circ \mathbf{I}_A = f$.

(ii) $\mathbf{I}_B \circ f = f$.

PROOF. Concerning (i), let $a \in A$. Then $(f \circ \mathbf{I}_A)(a) = f(\mathbf{I}_A(a)) = f(a)$. Property (ii) is proved similarly to property (i).

1.5.17 Proposition
Let $f : A \hookrightarrow\!\!\!\!\rightarrow B$ be a bijective function, and let $b \in B$. Then there exists a unique $a \in A$ such that $b = f(a)$.

PROOF. Let $b \in B$. Since f is surjective then there exists $a \in A$ such that $b = f(a)$. To prove uniqueness, suppose that there exist $a_1, a_2 \in A$ such that $b = f(a_1)$ and $b = f(a_2)$. Since f is injective, we have $a_1 = a_2$.

1.5.18 Definition
Let $f : A \hookrightarrow\!\!\!\!\rightarrow B$ be a bijective function. In virtue of Proposition 1.5.17, we define the INVERSE FUNCTION of f as the unique function

$$f^{-1} : B \to A$$

such that

$$a = f^{-1}(b) \iff b = f(a)\,, \qquad \text{for all } a \in A \text{ and } b \in B\,.$$

1.5.19 Proposition
Let $f : A \to B$ be a function. Then

(i) $f^{-1} \circ f = \mathbf{I}_A$.

(ii) $f \circ f^{-1} = \mathbf{I}_B$.

PROOF. Concerning (i), let $a \in A$. Then $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a = \mathbf{I}_A(a)$. Property (ii) is proved similarly to property (i).

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

(i) if f and g are injective then $g \circ f$ is injective.

(ii) if f and g are surjective then $g \circ f$ is surjective.

(iii) if f and g are bijective then $g \circ f$ is bijective.

PROOF. Concerning (i), suppose that $(g \circ f)(a_1) = (g \circ f)(a_2)$. Then $g(f(a_1) = g(f(a_2))$. Since g is injective, we have $f(a_1) = f(a_2)$. Since f is injective, we have $a_1 = a_2$.

Concerning (ii), let $c \in C$. Since g is surjective there exists $b \in B$ such that $c = g(b)$. Since f is surjective there exists $a \in A$ such that $b = f(a)$. Thus, $c = g(b) = g(f(a)) = (g \circ f)(a)$.

Property (iii) clearly follows by properties (i) and (ii).

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

(i) if $g \circ f$ is injective, then f is injective.

(ii) if $g \circ f$ is surjective, then g is surjective.

(iii) if f is surjective then range$(g \circ f)$ = range(g).

PROOF. Concerning (i), let $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$ which implies $(g \circ f)(a_1) = (g \circ f)(a_2)$. Since $g \circ f$ is injective, we have $a_1 = a_2$.

Concerning (ii), let $c \in C$. Since $g \circ f$ is surjective there exists $a \in A$ such that $c = (g \circ f)(a)$. Thus $c = g(f(a))$. Since c is arbitrary, it follows that g is surjective.

Concerning (iii), let $c \in$ *range*$(g \circ f)$. Then there exist $a \in A$ such that $c = (g \circ f)(a)$. It follows that $c = g(f(a))$, which implies $c \in$ *range*(g).

Conversely, let $c \in$ *range*(g). Then there exist $b \in B$ such that $c = g(b)$. Since f is surjective there exists $a \in A$ such that $b = f(a)$. Thus, $c = g(f(a)) = (g \circ f)(a)$, which implies $c \in$ *range*$(g \circ f)$.

1.5.22 Proposition
Let $f : A \to B$ and $g : B \to A$ be functions. Suppose that

(a) $f \circ g = \mathbf{I}_B$.

(b) $g \circ f = \mathbf{I}_A$.

Then:

(i) f is bijective.

(ii) g is bijective.

(iii) $g = f^{-1}$.

(iv) $f = g^{-1}$.

PROOF. Properties (i) and (ii) follow by Proposition 1.5.21.

Concerning (iii), it suffices to show that $a = g(b) \iff b = f(a)$. To see this, note that:

$$\begin{aligned} a = g(b) &\implies \mathbf{I}_A(a) = g(b) \\ &\implies g(f(a)) = g(b) \\ &\implies f(a) = b\,, \end{aligned}$$

and that

$$\begin{aligned} b = f(a) &\implies \mathbf{I}_B(b) = f(a) \\ &\implies f(g(b)) = f(a) \\ &\implies g(b) = a\,. \end{aligned}$$

Property (iv) is proved similarly to property (iii).

1.5.23 Proposition
Let $f : A \hookrightarrow\!\!\!\!\rightarrow B$ be a bijective function. Then $f^{-1} : B \hookrightarrow\!\!\!\!\rightarrow A$ is bijective and $(f^{-1})^{-1} = f$.

PROOF. f^-1 is bijectice by Proposition 1.5.22 (i) and (ii). By the same proposition, we have also $(f^{-1})^{-1} = f$, using (iii) and (iv).

1.5.24 Definition
Let $f : A^2 \to A$ be a function. We say that f is:

- IDEMPOTENT, if

$$f(a, a) = a\,, \qquad \text{for all } a \in A\,.$$

- COMMUTATIVE, if

$$f(a, b) = f(b, a)\,, \qquad \text{for all } a, b \in A\,.$$

- TRANSITIVE, if

$$f(f(a, b), c) = f(a, f(b, c))\,, \qquad \text{for all } a, b, c \in A\,.$$

1.6 Binary relations

1.6.1 Definition
Let $A \neq \varnothing$. A BINARY RELATION R of A is a subset $R \subseteq A^2$.

1.6.2 Notation
If R is a binary relation, we often write aRb in place of $(a, b) \in R$.

1.6.3 Definition
Let R be a binary relation of A, and let $X \subseteq A$. We say that R is:

- REFLEXIVE with respect to X if

$$aRa\,, \qquad \text{for all } a \in X\,.$$

- IRREFLEXIVE with respect to X if

$$\text{not } (aRa)\,, \qquad \text{for all } a \in X\,.$$

- SYMMETRIC with respect to X if

$$aRb \implies bRa\,, \qquad \text{for all } a, b \in X\,.$$

- ANTISYMMETRIC with respect to X if

$$aRb \text{ and } bRa \implies a = b\,, \qquad \text{for all } a, b \in X\,.$$

- TRANSITIVE with respect to X if

$$aRb \text{ and } bRc \implies aRc\,, \qquad \text{for all } a, b, c, \in X\,.$$

1.7 Equivalence relations

1.7.1 Definition
Let $A \neq \varnothing$. An EQUIVALENCE RELATION E of A is a binary relation of A satisfying the following properties:

- E is reflexive with respect to A.
- E is symmetric with respect to A.
- E is transitive with respect to A.

1.7.2 Definition
Let $A \neq \varnothing$. A PARTITION P of A is a set satisfying the following properties:

1. If $X \in P$ then $\varnothing \neq X \subseteq A$.
2. For every $a \in A$ there exists a set $X \in P$ such that $a \in X$.
3. $X \neq Y \implies X \cap Y = \varnothing$, for all sets $X, Y \in P$.

1.7.3 Definition
Let P be a partition of A. The BINARY RELATION INDUCED BY P is the binary relation $\sim$ of A defined by letting

$$a \sim b \iff \text{there exists a set } X \in P \text{ such that } a, b \in X\,,$$

for all $a, b \in A$.

1.7.4 Proposition
Let P be a partition of A, and let $\sim$ be the binary relation of A induced by P. Then $\sim$ is an equivalence relation of A.

PROOF. We want to show that $\sim$ is reflexive, symmetric, and transitive with respect to A.

Concerning reflexitivity, let $a \in A$. Then there exists a set $X \in P$ such that $a \in X$. Thus, $a \sim a$.

Concerning symmetry, suppose that $a \sim b$. Then there exists a set $X \in P$ such that $a, b \in X$. Thus, $b \sim a$.

Concerning transitivity, suppose that $a \sim b$ and $b \sim c$. Then there exists sets X, Y such that $a, b \in X$ and $b, c \in Y$. Since $X \cap Y \neq \varnothing$, it follows that $X = Y$. Thus, $a \sim c$.

1.7.5 Definition
Let $\sim$ be an equivalence relation of A, and let $a \in A$. The EQUIVALENCE CLASS of a with respect to $\sim$ is the set

$$[a]_{\sim} = \{b \in A \mid a \sim b\}.$$

1.7.6 Definition
Let $\sim$ be an equivalence relation of A. The QUOTIENT of A with respect to A is the set

$$A/_{\sim} = \{[a]_{\sim} \mid a \in A\}.$$

1.7.7 Proposition
Let $\sim$ be an equivalence relation of A. Then $A/_{\sim}$ is a partition of A.

PROOF. We want to prove that $A/_{\sim}$ satisfies properties (1)–(3) of Definition 1.7.2.

Concerning property (1), let $X \in A/_{\sim}$. It follows that $X = [a]_{\sim}$, for some $a \in A$. Thus, $\varnothing \neq X \subseteq A$.

Concerning property (2), let $a \in A$. Then $[a]_{\sim} \in P$ and $a \in [a]_{\sim}$.

Concerning property (3), let $X, Y \in P$ and $X \neq Y$. Then there exist $a, b \in A$ such that $X = [a]_{\sim}$ and $Y = [b]_{\sim}$. By contradiction, suppose that $X \cap Y \neq \varnothing$. Then there exists u such that $u \in X$ and $u \in Y$. It follows that $a \sim u$ and $b \sim u$, and therefore $a \sim b$. But then, for all $c \in A$, we have:

$$\begin{aligned} c \in [a]_{\sim} &\iff a \sim c \\ &\iff b \sim c \\ &\iff c \in [b]_{\sim}. \end{aligned}$$

It follows that $[a]_{\sim} = [b]_{\sim}$, which implies $X = Y$, a contradiction.

1.8 Partial orders

1.8.1 Definition
Let $A \neq \varnothing$. An PARTIAL ORDER $\leq$ of A is a binary relation of A satisfying the following properties:

1. $\leq$ is reflexive with respect to A.
2. $\leq$ is antisymmetric with respect to A.
3. $\leq$ is transitive with respect to A.

1.8.2 Definition
Let $A \neq \varnothing$. A STRICT ORDER $<$ of A is a binary relation of A satisfying the following properties:

1. $<$ is antireflexive with respect to A.
2. $<$ is transitive with respect to A.

1.8.3 Proposition
Let $\leq$ be a partial order of A. Let $<$ be the binary relation of A defined by

$$a < b \iff a \leq b \text{ and } a \neq b\,, \qquad \text{for all } a, b \in A\,.$$

Then $<$ is a strict order of A.

PROOF. We want to show that $<$ is antireflexive and transitive with respect to A.

Concerning antireflexivity, suppose by contradiction that $a < a$. Then $a \neq a$, a contradiction.

Concerning transitivity, suppose that $a < b$ and $b < c$. Then $a \leq b$ and $b \leq c$, which implies that $a \leq c$. Next, suppose by contradiction that $a = c$. Since $a \leq b$, we have $c \leq b$. Moreover, since $b \leq c$ we have $b = c$, which by antireflexivity contradicts $b < c$.

1.8.4 Proposition
Let $<$ be a partial order of A. Let $\leq$ be the binary relation of A defined by

$$a \leq b \iff a < b \text{ or } a = b\,, \qquad \text{for all } a, b \in A\,.$$

Then $\leq$ is a partial order of A.

PROOF. We want to show that $\leq$ is reflexive, antisymmetric, and transitive with respect to A.

Concerning reflexivity, let $a \in A$. Since $a = a$, we have $a \leq a$.

Concerning antisymmetry, suppose by contradiction that $a \leq b$, $b \leq a$, and $a \neq b$. Then $a < b$ and $b < a$, which implies $a < a$, a contradiction.

Concerning transitivity, suppose that $a \leq b$ and $b \leq c$. If $a = b$ or $b = c$ then clearly $a \leq c$. If instead $a \neq b$ and $b \neq c$ then we have $a < b$ and $b < c$. It follows that $a < c$, and therefore $a \leq c$.

1.8.5 Notation

If $\leq$ is a partial order of A, we denote with $<$ the strict order of A defined by:

$$a < b \iff a \leq b \text{ and } a \neq b\,, \qquad \text{for all } a, b \in A\,.$$

If $<$ is a strict order of A, we denote with $\leq$ the partial order of A defined by:

$$a \leq b \iff a < b \text{ or } a = b\,, \qquad \text{for all } a, b \in A\,.$$

We also use the following notations:

- $a \geq b \iff a \leq b$.
- $a > b \iff a < b$.
- $a \not\leq b \iff$ not $a \leq b$.
- $a \not< b \iff$ not $a < b$.
- $a \not\geq b \iff$ not $a \geq b$.
- $a \not> b \iff$ not $a > b$.

1.8.6 Definition

A LINEAR PARTIAL ORDER $\leq$ of A is a binary relation of A satisfying the following properties:

1. $\leq$ is a partial order of A.
2. $a \leq b$ or $a \geq b$, for all $a, b \in A$.

1.8.7 Definition

A LINEAR STRICT ORDER $<$ of A is a binary relation of A satisfying the following properties:

1. $<$ is a strict order of A.
2. $a < b$ or $a = b$ or $a > b$, for all $a, b \in A$.