M.Sc. program in mathematics

INTRODUCTORY SET THEORY

Katalin Károlyi
Department of Applied Analysis, Eötvös Loránd University
H-1088 Budapest, Múzeum krt. 6-8.

CONTENTS

1. SETS

Set, equal sets, subset, the empty set, power set of a set;
union, intersection, difference of sets; de Morgan's laws;
ordered pairs, Cartesian product of sets 1

EXERCISES 4

2. LOGIC

Proposition, logical values; negation, conjunction, disjunction,
implication, equivalence, truth tables; universal and existential quantifiers;
negation of propositions; direct and indirect methods of proofs 5

EXERCISES 8

3. RELATIONS

Relation, domain and range of relations; reflexive, irreflexive, symmetric,
antisymmetric, transitive relations; equivalence relation, order relation;
inverse relation; classifications of sets, equivalence classes,
classifications corresponding to equivalence relations 9

EXERCISES 13

4. FUNCTIONS

Function, domain, range, target of functions; restrictions of functions;
injective, surjective, bijective functions; equality of functions;
inverse function, composition of functions; image of sets under a function,
inverse image of sets under a function 14

EXERCISES 16

5. CARDINALITY OF SETS

Cardinality of sets, equivalent sets, Bernstein's theorem;
finite and infinite sets, countably infinite sets, countable and uncountable sets;
continuum cardinality, Cantor's theorem 17

EXERCISES 21

M.Sc. program in mathematics | *Department of Applied Analysis, Eötvös Loránd University, Budapest*

INTRODUCTORY SET THEORY

1. SETS

Undefined terms: *set* and *to be an element of a set*

We do not define neither the *set* nor the *element* of a set, their meanings can be understood intuitively (not needing definition).
However, we say that *a set is any collection of definite, distinguishable objects*, and we call these objects *the elements of the set.*

Notations.

(1) Sets are usually denoted by capital letters $(A, B, C, ...)$.
The elements of the set are usually denoted by small letters $(a, b, c, ...)$.

(2) If X is a set and x is an element of X, we write $x \in X$.
(We also say that x belongs to X.)

If X is a set and y is not an element of X, we write $y \notin X$.
(We also say that y does not belong to X.)

(3) When we give a set, we generally use braces, e.g.:

(i) $S := \{a, b, c, \ldots\}$ where the elements are listed between braces,
three dots imply that the law of formation of other elements is known,

(ii) $S := \{x \in X : \ p(x) \text{ is true}\}$ where "x" stands for a generic element of the set S and p is a property defined on the set X.

Remark.

If we want to emphasize that the elements of the set are also sets, we denote the set by script capital letter, such as:

(i) $\mathcal{A} := \{A, B, C, \ldots\}$ where $A, B, C, \ldots$ are sets,
(ii) $\mathcal{A} := \{A_\alpha : \ \alpha \in \Gamma\}$ where Γ is the so called *indexing set* and A_α's are sets.

Examples.

1. $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$ the set of all natural numbers,
   $\mathbb{N}^+ := \{n \in \mathbb{N} : \ n > 0\}$,
2. $\mathbb{Z} := \{0, -1, +1, -2, +2, \ldots\}$ the set of all integers,
3. $\mathbb{Q} := \{p/q : \ p \in \mathbb{Z}, \ q \in \mathbb{N}^+\}$ the set of all rational numbers,
   $\mathbb{Q}^+ := \{r \in \mathbb{Q} : \ r > 0\}$,
4. $\mathbb{R} :=$ the set of all real numbers,
   $\mathbb{R}^+ := \{x \in \mathbb{R} : \ x > 0\}$,
5. $\mathbb{C} :=$ the set of all complex numbers.

Definitions.

(1) ***Equal sets:***
We define $A = B$ if A and B have the same elements.

(2) ***Subset:***
We say that A is a *subset* of B and we write $A \subset B$ or $B \supset A$
if every element of A is also an element of B.
(We also say that A is included in B or B includes A or B is a *superset* of A.)

(3) ***Proper subset:***
We say that A is a *proper subset* of B and we write $A \subset B$ *strictly*
if $A \subset B$ and $A \neq B$.
(There exists at least one element $b \in B$ such that $b \notin A$.)

(4) ***The empty set:***
The set which has no element is called the *empty set* and is denoted by $\emptyset$.
(That is $\emptyset = \{x \in A : \ x \notin A\}$, where A is any set.)

(5) ***Power set of a set:***
Let X be any set. The set of all subsets of X is called the *power set* of X
and is denoted by $\mathcal{P}(X)$.
(That is we define $\mathcal{P}(X) := \{A : \ A \subset X\}$)

Remarks.

Let A and B be any sets. Then the following propositions can be proved easily:

(1) $A = B$ if and only if $A \subset B$ and $B \subset A$,
(2) $A \subset A$ and $\emptyset \subset A$,
(3) $A \in \mathcal{P}(A)$ and $\emptyset \in \mathcal{P}(A)$,
(4) $\mathcal{P}(\emptyset) = \{ \ \emptyset \ \}$. ($\mathcal{P}(\emptyset)$ is not empty, it has exactly one element, the $\emptyset$.)

OPERATIONS BETWEEN SETS

Let H be a set including all sets $A, B, C, \ldots$ which occur in the following.
Let us call H the *basic set.*

Union of sets: (denoted by $\cup$, called "union" or "cup")

(1) The *union* of sets A and B is defined by $A \cup B := \{x \in H : \ x \in A \ \text{ or } \ x \in B\}$.
(2) The *union* of a set $\mathcal{A}$ of sets is defined by $\bigcup \mathcal{A} := \{x \in H : \ \exists A \in \mathcal{A} \ \ x \in A\}$.
(x belongs to at least one element of $\mathcal{A}$)

Intersection of sets: (denoted by $\cap$, called "intersection" or "cap")

(1) The *intersection* of sets A and B is defined by $A \cap B := \{x \in H : \ x \in A \ \text{ and } \ x \in B\}$.
(2) The *intersection* of a set $\mathcal{A} \neq \emptyset$ is defined by $\bigcap \mathcal{A} := \{x \in H : \ \forall A \in \mathcal{A} \ \ x \in A\}$.
(x belongs to all elements of $\mathcal{A}$)

Definition. *(Disjoint sets.)*
A and B are called *disjoint sets* if $A \cap B = \emptyset$ (they have no elements in common).

Difference of sets: (denoted by $\setminus$)

(1) The *difference* of sets A and B is defined by $A \setminus B := \{x \in H : x \in A \text{ and } x \notin B\}$.
(We also say that $A \setminus B$ is the *complement of* B *with respect to* A.)

(2) $H \setminus B$ is called the *complement of* B and is denoted by B^c,
that is $B^c := \{x \in H : x \notin B\}$.

The following theorems can be proved easily.

Theorem. (Commutativity, associativity, distributivity)

(1) The *union* and the *intersection* are *commutative* and *associative* operations:
(i) $A \cup B = B \cup A, \quad (A \cup B) \cup C = A \cup (B \cup C)$,
(ii) $A \cap B = B \cap A, \quad (A \cap B) \cap C = A \cap (B \cap C)$.

(2) The *union* is *distributive* with respect to the *intersection* and
the *intersection* is *distributive* with respect to the *union*:
(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Theorem. (De Morgan's laws)

(1) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B), \qquad C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$,
(2) $C \setminus \left(\bigcup \mathcal{A}\right) = \bigcap \{C \setminus A : A \in \mathcal{A}\}, \qquad C \setminus \left(\bigcap \mathcal{A}\right) = \bigcup \{C \setminus A : A \in \mathcal{A}\}$.

Definitions. *(Ordered pairs, Cartesian product of sets.)*

Ordered pairs:

Let x and y be any objects (e.g. any elements of the basic set H).
The *ordered pair* (x, y) is defined by $(x, y) := \{ \{x\}, \{x, y\} \}$.
We call x and y the *first* and the *second components* of the ordered pair (x, y), respectively.
In case $x = y$ we have $(x, x) = \{ \{x\} \}$.

Cartesian product of sets:

Let A and B be sets. The *Cartesian product* of A and B is defined by
$A \times B := \{(a, b) : a \in A \text{ and } b \in B\}$, i.e. the *Cartesian product* $A \times B$ is the set of all ordered pairs (a, b) with $a \in A$, $b \in B$.

Remarks.
(1) $(x, y) = (u, v)$ if and only if $x = u$ and $y = v$.
(2) More generally, we can define the *ordered n-tuples* $(x_1, x_2, \ldots, x_n)$ and
the *Cartesian product* $A_1 \times A_2 \times \ldots \times A_n$ $(n \in \mathbb{N}^+, n > 2)$ in a similar way.
(3) For $A \times A$ we often write A^2, and similarly, A^n stands for $\underbrace{A \times A \times \ldots \times A}_{n}$.

EXERCISES 1.

1. Prove that $A \cup B = B$ if and only if $A \subset B$.

2. Prove that $A \cap B = B$ if and only if $B \subset A$.

3. Prove that $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$.

4. Prove that $A \backslash B = A \cap B^c$.

5. Let $\mathcal{A} := \{A_\alpha : \alpha \in \Gamma\}$. Prove that for all $\alpha \in \Gamma$ $\bigcap \mathcal{A} \subset A_\alpha \subset \bigcup \mathcal{A}$,
   that is for all $\alpha \in \Gamma$ $\bigcap \{A_\beta : \beta \in \Gamma\} \subset A_\alpha \subset \bigcup \{A_\beta : \beta \in \Gamma\}$.

6. Let H be the *basic set* (which includes all the sets $A, B, C, \ldots$ that we consider).
   $A \cup A = ?$ $A \cup H = ?$ $A \cup \emptyset = ?$
   $A \cap A = ?$ $A \cap H = ?$ $A \cap \emptyset = ?$
   $A \setminus A = ?$ $A \setminus H = ?$ $A \setminus \emptyset = ?$ $(A^c)^c = ?$ $\emptyset^c = ?$ $H^c = ?$

7. Prove the following statements:
   (i) $\left(\bigcup \mathcal{A} \right) \setminus C = \bigcup \{A \setminus C : A \in \mathcal{A}\}$,
   (ii) $\left(\bigcap \mathcal{A} \right) \setminus C = \bigcap \{A \setminus C : A \in \mathcal{A}\}$.

8. Prove the following statements:
   (i) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$,
   (ii) $\mathcal{P}(A \cup B) \supset \mathcal{P}(A) \cup \mathcal{P}(B)$ (strictly, if $A \not\subset B$ or $B \not\subset A$),
   (iii) $\mathcal{P}(A \setminus B) \setminus \{ \emptyset \} \subset \mathcal{P}(A) \setminus \mathcal{P}(B)$ (strictly, if $A \not\subset B$).

9. Let $H := \{1, 2, 3, 4, 5\}$, $A := \{1, 2\}$, $B := \{1, 3, 5\}$.
   $A \cup B = ?$ $A \cap B = ?$ $A \setminus B = ?$ $B \setminus A = ?$ $A^c = ?$ $B^c = ?$
   $A \times B = ?$ $B \times A = ?$ $\mathcal{P}(A) = ?$ $\mathcal{P}(B) = ?$

10. Let A_1, A_2 be any sets. Find disjoint sets B_1, B_2 such that $A_1 \cup A_2 = B_1 \cup B_2$.

11. Prove that $A \times (B \cap C) = (A \times B) \cap (A \times C)$ for any sets A, B, C .

12. Determine which of the following sets are empty:
    $A_1 := \{n \in \mathbb{Z} : n^2 = 2\}$,
    $A_2 := \{x \in \mathbb{R} : x^3 - 2x^2 + x - 2 = 0\}$,
    $A_3 := \{(x, y) \in \mathbb{R}^2 : x^2 + xy + y^2 < 0\}$.

2. LOGIC

Basic ideas of logic: *proposition* and *logical values*

Proposition:

We define a *proposition* to be a statement which is *either true or false.*
When we deal with propositions in logic we consider sentences without being interested in their meanings, only examining them as true or false statements.
In the following, propositions will be denoted by small letters ($p, q, r, \dots$).

Logical values:

There are two logical values: *true* and *false*,
denoted by T and F, respectively.

Examples.

1. $p :=$ for each real number x, x^2+1 is positive .
   The logical value of the proposition p is *true.*
2. $q :=$ if $x=2$ then $x^2-1=0$.
   The logical value of the proposition q is *false.*

OPERATIONS BETWEEN PROPOSITIONS

Negation: (denoted by $\neg$, called *"not"*)

The *negation* of a proposition p is defined by

$$\neg p := \begin{cases} \textit{true} & \text{if } p \text{ is } \textit{false} \\ \textit{false} & \text{if } p \text{ is } \textit{true}\ . \end{cases}$$

Conjunction: (denoted by $\wedge$, called *"and"*)

The *conjunction* of propositions p and q is defined by

$$p \wedge q := \begin{cases} \textit{true} & \text{if } p \text{ and } q \text{ are both } \textit{true} \\ \textit{false} & \text{if at least one of } p \text{ and } q \text{ is } \textit{false}\ . \end{cases}$$

Disjunction: (denoted by $\vee$, called *"or"*)

The *disjunction* of propositions p and q is defined by

$$p \vee q := \begin{cases} \textit{true} & \text{if at least one of } p \text{ and } q \text{ is } \textit{true} \\ \textit{false} & \text{if } p \text{ and } q \text{ are both } \textit{false}\ . \end{cases}$$

Implication: (denoted by $\Rightarrow$, read *"implies"*)

The *implication* between propositions p and q is defined by

$$p \Rightarrow q := \begin{cases} \textit{true} & \text{if } p \text{ and } q \text{ are both } \textit{true}, \text{ or } p \text{ is } \textit{false} \\ \textit{false} & \text{if } p \text{ is } \textit{true} \text{ and } q \text{ is } \textit{false}\ . \end{cases}$$

Equivalence: (denoted by $\Leftrightarrow$, read *"is equivalent to"*)

The *equivalence* between propositions p and q is defined by

$$p \Leftrightarrow q := \begin{cases} \textit{true} & \text{if } p \text{ and } q \text{ have the same logical value} \\ \textit{false} & \text{if } p \text{ and } q \text{ have different logical values .} \end{cases}$$

Remarks.

(1) For $p \Rightarrow q$ we can also say that

if p then q,
p only if q,
p is a sufficient condition for q,
q is a necessary condition for p.

(2) For $p \Leftrightarrow q$ we can also say that
p if and only if q, (p *iff* q),
p is a necessary and sufficient condition for q.

(3) The following ***truth tables*** can be useful to resume the definitions of the logical operations:

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

(4) The following propositions can be proved easily:

(i) $p \Leftrightarrow q$ is equivalent to $(p \Rightarrow q) \wedge (q \Rightarrow p)$,
that is, for all values of p and q $p \Leftrightarrow q = (p \Rightarrow q) \wedge (q \Rightarrow p)$,

(ii) $p \Rightarrow q = (\neg p) \vee q$ for all values of p and q .

(5) A proposition which is always *true* is called ***tautology***, and
a proposition which is always *false* is called ***contradiction***.

According to (4) we have

(i) $\big(p \Leftrightarrow q\big) \Leftrightarrow \big((p \Rightarrow q) \wedge (q \Rightarrow p)\big) \equiv \mathsf{T}$, (ii) $\big(p \Rightarrow q\big) \Leftrightarrow \big((\neg p) \vee q\big) \equiv \mathsf{T}$,

i.e., $\big(p \Leftrightarrow q\big) \Leftrightarrow \big((p \Rightarrow q) \wedge (q \Rightarrow p)\big)$ and $\big(p \Rightarrow q\big) \Leftrightarrow \big((\neg p) \vee q\big)$ are tautologies;

$p \vee (\neg p)$ is also a *tautology*, while $p \wedge (\neg p)$ is a *contradiction*.

Universal and existential quantifiers:

Let S be a set and for all elements s of S let $p(s)$ be a proposition.
We define the propositions $\forall s \in S \; p(s)$ and $\exists s \in S \; p(s)$ such as

$$\text{(i)} \quad \forall s \in S \;\; p(s) := \begin{cases} \textit{true} & \text{if } p(s) \text{ is } \textit{true} \text{ for all } s \in S \\ \textit{false} & \text{if there exists at least one } s \in S \text{ such that } p(s) \text{ is } \textit{false} \,, \end{cases}$$

$$\text{(ii)} \quad \exists s \in S \;\; p(s) := \begin{cases} \textit{true} & \text{if there exists at least one } s \in S \text{ such that } p(s) \text{ is } \textit{true} \\ \textit{false} & \text{if } p(s) \text{ is } \textit{false} \text{ for all } s \in S \,. \end{cases}$$

The symbol $\forall$ is read *"for all"* and is called the ***universal quantifier***,
the symbol $\exists$ is read *"there exists"* and is called the ***existential quantifier***.

Negation of propositions.

It is of crucial importance that we can negate propositions correctly. In the following we show *how to negate propositions* in accordance with the definitions of the logical operations and the universal and existential quantifiers.

(1) When the quantifiers do not occur in the proposition, we have

(i) $\neg(p \wedge q) \;\equiv\; (\neg p) \vee (\neg q)$,

(ii) $\neg(p \vee q) \;\equiv\; (\neg p) \wedge (\neg q)$,

(iii) $\neg(p \Rightarrow q) \;\equiv\; \neg\big((\neg p) \vee q\big) \;\equiv\; \big(\neg(\neg p)\big) \wedge (\neg q) \;\equiv\; p \wedge (\neg q)$,

(iv) $\neg(p \Leftrightarrow q) \;\equiv\; \neg\big((p \Rightarrow q) \wedge (q \Rightarrow p)\big) \;\equiv\; \big(\neg(p \Rightarrow q)\big) \vee \big(\neg(q \Rightarrow p)\big) \;\equiv$
$\equiv\; \big(p \wedge (\neg q)\big) \vee \big(q \wedge (\neg p)\big) \;\equiv\; \big(p \vee q\big) \wedge \big((\neg p) \vee (\neg q)\big)$.

(2) When quantifiers occur in the proposition, we have

(i) $\neg\big(\forall s \in S \;\; p(s)\big) \;\equiv\; \exists s \in S \;\; \neg p(s)$,

(ii) $\neg\big(\exists s \in S \;\; p(s)\big) \;\equiv\; \forall s \in S \;\; \neg p(s)$.

As a general rule, we have to *change* $\forall$ *into* $\exists$ and *change* $\exists$ *into* $\forall$, and finally *negate the proposition* which follows the quantifier.

Methods of proofs.

There are two main methods to prove theorems:

(1) ***direct methods:*** Since $\big((p \Rightarrow r) \wedge (r \Rightarrow q) \big) \;\Rightarrow\; \big(p \Rightarrow q \big) \;\equiv\; \mathsf{T}$,
we can prove $p \Rightarrow q$ by proving $p \Rightarrow r$ and $r \Rightarrow q$, where r is any other proposition.

(2) ***indirect methods:***

(i) Since $(p \Rightarrow q) \equiv \big((\neg p) \vee q\big) \equiv \big((\neg q) \Rightarrow (\neg p)\big)$, we can prove $p \Rightarrow q$ by proving its *contrapositive*, $(\neg q) \Rightarrow (\neg p)$ (***contrapositive proof***).

(ii) If r is any *false* proposition, then $\big(p \wedge (\neg q)\big) \Rightarrow r \;\equiv\; p \Rightarrow q$, thus we can prove $p \Rightarrow q$ by proving $\big(p \wedge (\neg q)\big) \Rightarrow r$ (***proof by contradiction***).

EXERCISES 2.

1. Prove that for all values of $p,\ q,\ r$ the following statements are true.

$$p \wedge q = q \wedge p \qquad (p \wedge q) \wedge r = p \wedge (q \wedge r)$$
$$p \vee q = q \vee p \qquad (p \vee q) \vee r = p \vee (q \vee r)$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$$

2. Answer the questions for any values of p.

$$p \wedge p = ? \qquad p \wedge \mathsf{T} = ? \qquad p \wedge \mathsf{F} = ?$$
$$p \vee p = ? \qquad p \vee \mathsf{T} = ? \qquad p \vee \mathsf{F} = ?$$
$$p \Rightarrow p = ? \qquad p \Rightarrow \mathsf{T} = ? \qquad p \Rightarrow \mathsf{F} = ?$$
$$p \Leftrightarrow p = ? \qquad p \Leftrightarrow \mathsf{T} = ? \qquad p \Leftrightarrow \mathsf{F} = ?$$

3. Determine which of the following propositions are true:

(a) $n \in \mathbb{Z} \ \Rightarrow \ n^2 > 1$

(b) $\exists x \in \mathbb{R} \quad x^3 - 2x^2 + x - 2 = 0$

(c) $\forall (x, y) \in \mathbb{R}^2 \quad x^2 + xy + y^2 < 0$

4. Negate the following propositions, then determine which of them are true.

(a) $\forall p \in \mathbb{R}^+ \quad \exists K \in \mathbb{R}^+ \quad \forall x \in (K, +\infty) \quad x^2 - px + 1 > 0$

(b) $\forall p \in \mathbb{R}^+ \quad \exists K \in \mathbb{R}^+ \quad \forall x \in (K, +\infty) \quad x \cdot \sin \dfrac{p}{x} > 0$

(c) $\forall p \in \mathbb{R}^+ \quad \exists K \in \mathbb{R}^+ \quad \forall x \in (K, +\infty) \quad \cos \dfrac{p}{x} > 0$

(d) $\forall p \in \mathbb{R}^+ \quad \exists K \in \mathbb{R}^+ \quad \forall x \in (K, +\infty) \quad p < \log_2 x$

(e) $\forall p \in \mathbb{R}^+ \quad \exists K \in \mathbb{R}^+ \quad \forall x \in (K, +\infty) \quad x^{-p} < 10^{-6}$

(f) $\forall p \in \mathbb{R}^+ \quad \exists K \in \mathbb{R}^+ \quad \forall x \in (K, +\infty) \quad (p+1)^{-x} < 10^{-6}$

(g) $\forall \varepsilon \in \mathbb{R}^+ \quad \exists x \in (0, \pi/4] \quad \sin x = \dfrac{1}{\sqrt{\varepsilon + 1/\varepsilon}}$

(h) $\exists \delta \in \mathbb{R}^+ \quad \forall x \in (0, \delta] \quad \exists \varepsilon \in \mathbb{R}^+ \quad \sin x = \dfrac{1}{\sqrt{\varepsilon + 1/\varepsilon}}$

5. Prove that $\big((p \Rightarrow r) \wedge (r \Rightarrow q) \big) \Rightarrow \big(p \Rightarrow q \big) \equiv \mathsf{T}$.

6. Prove that $\forall k \in \mathbb{N}^+ \ \forall n \in \mathbb{N}^+ \quad \sqrt[n]{k}$ is an integer or an irrational number.

7. Prove that $\big((n \in \mathbb{N}^+) \wedge (n^2 \text{ is odd}) \big) \Rightarrow (n \text{ is odd})$.

3. RELATIONS

Definition. *(Relations.)*

Any subset of a Cartesian product of sets is called a *relation*.
(I.e., a *relation* is a set of ordered pairs.)

If X and Y are sets and $\rho \subset X \times Y$, we say that ρ is a *relation from* X *to* Y.
(We can also say that ρ is a *relation between the elements of* X *and* Y.)

If $\rho \subset X \times X$, we say that ρ is a *relation in* X.

If $(x, y) \in \rho$, we often write $x \rho y$.

Examples.

1. The relation of *equality* in a nonempty set X.
   $\rho_1 := \{ (x, x) : \ x \in X \}$,
   thus $(x, y) \in \rho_1 \subset X \times X$ iff $x = y$.
2. The relation of *divisibility* in $\mathbb{N}^+$.
   $\rho_2 := \{ (m, n) \in \mathbb{N}^+ \times \mathbb{N}^+ : \ \exists k \in \mathbb{N}^+ \quad n = k \cdot m \}$,
   thus $(m, n) \in \rho_2 \subset \mathbb{N}^+ \times \mathbb{N}^+$ iff $m \mid n$,
   that is n can be divided by m without remainder (n is divisible by m).
3. The relation of *congruence modulo* m in $\mathbb{Z}$.
   $\rho_3 := \{ (a, b) \in \mathbb{Z} \times \mathbb{Z} : \ \exists k \in \mathbb{Z} \quad a - b = k \cdot m \}, \quad (m \in \mathbb{N}^+)$,
   thus $(a, b) \in \rho_3 \subset \mathbb{Z} \times \mathbb{Z}$ iff $m \mid a - b$,
   that is $(a - b)$ can be divided by m without remainder;
   $(a - b)$ is divisible by m; dividing a and b by m we get the same remainder.
4. The relation of *"less"* in $\mathbb{R}$.
   $\rho_4 := \{ (x, y) \in \mathbb{R} \times \mathbb{R} : \ x < y \}$,
   thus $(x, y) \in \rho_4 \subset \mathbb{R} \times \mathbb{R}$ iff $y - x$ is a positive number.
5. The relation of *"greater or equal"* in $\mathbb{R}$.
   $\rho_5 := \{ (x, y) \in \mathbb{R} \times \mathbb{R} : \ x \geq y \}$,
   thus $(x, y) \in \rho_5 \subset \mathbb{R} \times \mathbb{R}$ iff $x - y$ is a nonnegative number.
6. Relation between the elements of the set T of all triangles of the plane and the elements of the set $\mathbb{R}_0^+$ of all nonnegative numbers,
   $\rho_6 := \{ (t, a) \in T \times \mathbb{R}_0^+ : \ \text{the area of the triangle } t \text{ is } a \}$.
7. Relation between the elements of the set $\mathbb{R}_0^+$ of all nonnegative numbers and the elements of the set T of all triangles of the plane,
   $\rho_7 := \{ (a, t) \in \mathbb{R}_0^+ \times T : \ \text{the area of the triangle } t \text{ is } a \}$.
8. Relation between the elements of the set C of all circles of the plane and the elements of the set L of all lines of the plane,
   $\rho_8 := \{ (c, l) \in C \times L : \ l \text{ is a tangent of } c \}$.

Definitions. *(Domain and range of relations.)*
Let X and Y be sets and ρ be a relation from X to Y $(\rho \subset X \times Y)$.

(1) ***Domain of the relation ρ:***
The *domain* of ρ is defined by $D(\rho) := \{x \in X : \ \exists y \in Y \ \ (x, y) \in \rho\}$.

(2) ***Range of the relation ρ:***
The *range* of ρ is defined by $R(\rho) := \{y \in Y : \ \exists x \in X \ \ (x, y) \in \rho\}$.

Definitions. *(Properties of relations.)*
Let X be a set and ρ be a relation in X $(\rho \subset X^2)$.

(1) ***Reflexivity:***
ρ is called *reflexive* if $\forall x \in X \ \ (x, x) \in \rho$.

(2) ***Irreflexivity:***
ρ is called *irreflexive* if $\forall x \in X \ \ (x, x) \notin \rho$.

(3) ***Symmetry:***
ρ is called *symmetric* if $\forall (x, y) \in \rho \ \ (y, x) \in \rho$,
that is $(x, y) \in \rho$ implies $(y, x) \in \rho$.

(4) ***Antisymmetry:***
ρ is called *antisymmetric* if $\big((x, y) \in \rho$ and $(y, x) \in \rho\big)$ implies $x = y$.

(5) ***Transitivity:***
ρ is called *transitive* if $\big((x, y) \in \rho$ and $(y, z) \in \rho\big)$ implies $(x, z) \in \rho$.

Examples. (*see page 9*)
1. *Equality* is a reflexive, symmetric, antisymmetric and transitive relation.
2. *Divisibility* is a reflexive, antisymmetric and transitive relation.
3. *Congruence modulo m* is a reflexive, symmetric and transitive relation.
4. The relation *"less"* is irreflexive, antisymmetric and transitive.
5. The relation *"greater or equal"* is reflexive, antisymmetric and transitive.

Definitions. *(Special relations.)*
Let X be a nonempty set and ρ be a relation in X $(\rho \subset X^2)$.

(1) ***Equivalence relation:***
We say that ρ is an *equivalence relation* if it is
(a) *reflexive,* (b) *symmetric,* (c) *transitive.*

(2) ***Order relation:***
We say that ρ is an *order relation* if it is
(a) *reflexive,* (b) *antisymmetric,* (c) *transitive.*

We say that the *order* relation ρ is a *total (linear) order relation* if
for each $(x, y) \in X^2$ $(x, y) \in \rho$ or $(y, x) \in \rho$ is satisfied;
otherwise ρ is said to be a *partial order relation.*

Examples. (*see page 9*)

1. *Equality* (both equivalence and order relation) is *a partial order relation.*
2. *Divisibility* is *a partial order relation.*
5. The relation *"greater or equal"* is *a total order relation.*

Definition. *(Inverse relation.)*
Let X and Y be sets and ρ be a relation from X to Y.
The *inverse* of ρ (denoted by ρ^{-1}) is defined by $\rho^{-1} := \{(y,x) \in Y \times X : \ (x,y) \in \rho\}$.

Definition. *(Classifications of sets.)*
Let X be a nonempty set. A set $\mathcal{A}$ (of subsets of X) is called *a classification* of X if the following properties are satisfied:

(i) $\forall A \in \mathcal{A}$ A is a nonempty subset of X,
(ii) $\big(A, B \in \mathcal{A}$ and $A \neq B \big)$ implies $A \cap B = \emptyset$,
(iii) $\bigcup \mathcal{A} = X$.

The elements of $\mathcal{A}$ are called the *classes* of the *classification.*

Definition. *(Equivalence classes.)*
Let X be a nonempty set and ρ be an *equivalence relation* in X.
For each $x \in X$ we define $A_x := \{y \in X : \ (x,y) \in \rho\} \quad \in \mathcal{P}(X)$.
A_x is called *the (equivalence) class of* x.

***Theorem* (3.1).**
Let X be a nonempty set and ρ be an equivalence relation in X. Then

(i) $\forall x \in X$ A_x is a nonempty subset of X,
(ii) $\big(x, y \in X$ and $x \neq y \big)$ implies $\big(A_x \cap A_y = \emptyset$ or $A_x = A_y \big)$,
(iii) $\bigcup \{ A_x : \ x \in X \} = X$,

that is $\{A_x : \ x \in X\}$ is a *classification* of X.

Proof.

(i) Since ρ is *reflexive* we have $x \in A_x$ for all $x \in X$, hence we have (i).

(ii) We prove (ii) *by contradiction.*
Let us suppose that $\exists x, y \in X,\ x \neq y,$ such that $\big(A_x \cap A_y \neq \emptyset$ and $A_x \neq A_y \big)$.
We prove that $A_x = A_y$, which is a *contradiction.*
Let z be an element of $A_x \cap A_y$. Then $(x,z) \in \rho$ and $(y,z) \in \rho$,
thus $(x,y) \in \rho$ and $(y,x) \in \rho$ (by the symmetry and transitivity of ρ).
 (a) $A_x \subset A_y$ since
 $p \in A_x \Rightarrow (x,p) \in \rho \Rightarrow (p,x) \in \rho$ (and $(x,y) \in \rho$) $\Rightarrow (p,y) \in \rho \Rightarrow (y,p) \in \rho$
 $\Rightarrow p \in A_y$,
 (b) $A_y \subset A_x$ can be proved similarly to (a).

(iii) If $z \in X$ then $z \in A_z$, thus $z \in \bigcup \{A_x : \ x \in X\} \subset X$, hence we have (iii).

♠

Definition. *(Classifications corresponding to equivalence relations.)*
Let X be a nonempty set and ρ be an *equivalence relation* in X.
The set of all equivalence classes corresponding to ρ (which is a classification of X according to the theorem (3.1)) is called the ***classification of*** X ***corresponding to the relation*** ρ, and is denoted by X/ρ, i.e. $X/\rho := \{A_x : \ x \in X\}$.
(We also say that X/ρ is the *classification of* X *defined by* ρ.)

Examples. (*see page 9*)

1. The *classification* of X corresponding to the relation of *equality* is the set $X/\rho_1 = \{ \ \{x\} \in \mathcal{P}(X) : \ x \in X \ \}$.
3. The *classification* of $\mathbb{Z}$ corresponding to the relation of *congruence modulo* m is the set of all *remainder classes modulo* m $(m \in \mathbb{N}^+)$, that is $\mathbb{Z}/\rho_3 = \{ \ \{r + k \cdot m : \ k \in \mathbb{Z}\} \in \mathcal{P}(\mathbb{Z}) : \ r \in \{0, 1, \ldots, m{-}1\} \ \}$.

Remark.
Theorem (3.1) shows that *each equivalence relation determines a classification of the set.* The following theorem shows the opposite direction, that is *each classification of a set determines an equivalence relation* in the set.

***Theorem* (3.2).**

Let X be a nonempty set and $\mathcal{A}$ be a classification of X. Then

(i) the relation defined by $\rho := \{ \ (x,y) \in X \times X : \ \ \exists A \in \mathcal{A} \ \ x, y \in A \ \}$ is an equivalence relation in X,

(ii) the classification of X corresponding to ρ is equal to $\mathcal{A}$, that is $X/\rho = \mathcal{A}$.

Proof.

(i) $x \in X \Rightarrow \ (\exists A \in \mathcal{A} \ \ x \in A) \Rightarrow \ (x,x) \in \rho \Rightarrow \ \rho$ is *reflexive*,
$(x,y) \in \rho \Rightarrow \ (\exists A \in \mathcal{A} \ \ x, y \in A) \Rightarrow \ y, x \in A \Rightarrow \ (y,x) \in \rho \Rightarrow \ \rho$ is *symmetric*,
$(x,y) \in \rho$ and $(y,z) \in \rho \Rightarrow \ (\exists A_1 \in \mathcal{A} \ \ x, y \in A_1)$ and $(\exists A_2 \in \mathcal{A} \ \ y, z \in A_2)$
$\Rightarrow \ y \in A_1 \cap A_2 \Rightarrow \ A_1 = A_2 \Rightarrow \ x, z \in A_1 \Rightarrow \ (x,z) \in \rho \Rightarrow \ \rho$ is *transitive*,
thus ρ is an *equivalence relation.*

(ii) We prove that $X/\rho \subset \mathcal{A}$ and $\mathcal{A} \subset X/\rho$.

(a) Let $B \in X/\rho \ \Rightarrow \ \exists b \in B$ and $B = \{x \in X : \ \ (b,x) \in \rho\}$,
$b \in X \ \Rightarrow \ \exists A \in \mathcal{A} \ \ \ b \in A$,
$x \in B \ \Rightarrow \ (b,x) \in \rho$ (and $b \in A$) $\Rightarrow \ x \in A$, $\Rightarrow \ B \subset A$,
$x \in A$ (and $b \in A$) $\Rightarrow \ (b,x) \in \rho \ \Rightarrow \ x \in B$, $\Rightarrow \ A \subset B$,
$\Rightarrow \ B = A \ \Rightarrow \ B \in \mathcal{A}$,

(b) Let $A \in \mathcal{A} \ \Rightarrow \ \exists a \in A$,
let $B := \{x \in X : \ \ (a,x) \in \rho\} \ \in X/\rho$,
$x \in A$ (and $a \in A$) $\Rightarrow \ (a,x) \in \rho \ \Rightarrow \ x \in B$, $\Rightarrow \ A \subset B$,
$x \in B \ \Rightarrow \ (a,x) \in \rho$ (and $a \in A$) $\Rightarrow \ x \in A$, $\Rightarrow \ B \subset A$,
$\Rightarrow \ A = B \ \Rightarrow \ A \in X/\rho$. ♠

EXERCISES 3.

1. Let X be a nonempty set and ρ be a relation in X.
   Prove the following propositions:
   (a) if ρ is reflexive, then $D(\rho) = R(\rho) = X$ and ρ^{-1} is also reflexive,
   (b) if ρ is irreflexive, then ρ^{-1} is also irreflexive,
   (c) if ρ is symmetric, then $D(\rho) = R(\rho)$ and ρ^{-1} is also symmetric,
   (d) if ρ is antisymmetric, then ρ^{-1} is also antisymmetric,
   (e) if ρ is transitive, then ρ^{-1} is also transitive.

2. Which properties have the following relations?
   (a) $\rho := \{ \ (x, y) \in \mathbb{Q} \times \mathbb{Q} : \quad x > y \ \}$,
   (b) $\rho := \{ \ (x, y) \in \mathbb{R} \times \mathbb{R} : \quad x \leq y \ \}$,
   (c) $\rho := \{ \ (A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) : \quad A \subset B \ \}, \quad (X \neq \emptyset)$,
   (d) $\rho := \{ \ ((m_1, m_2), (n_1, n_2)) \in (\mathbb{N}^+)^2 \times (\mathbb{N}^+)^2 : \quad m_1 \mid n_1 \ \text{ and } \ m_2 \mid n_2 \ \}$.

3. Prove that the following relations are equivalence relations and
   determine the corresponding classifications.
   (a) $\rho := \{ \ (p, q) \in \mathbb{N} \times \mathbb{N} : \quad m \mid q-p \ \}, \quad (m \in \mathbb{N}^+)$,
   (b) $\rho := \{ \ ((m_1, m_2), (n_1, n_2)) \in (\mathbb{N}^+)^2 \times (\mathbb{N}^+)^2 : \quad m_1 + n_2 = m_2 + n_1 \ \}$,
   (c) $\rho := \{ \ ((m_1, m_2), (n_1, n_2)) \in (\mathbb{Z} \times \mathbb{Z} \backslash \{0\}) \times (\mathbb{Z} \times \mathbb{Z} \backslash \{0\}) : \quad m_1 \cdot n_2 = m_2 \cdot n_1 \ \}$,
   (d) $\rho := \{ \ (x, y) \in \mathbb{R} \times \mathbb{R} : \quad y - x \in \mathbb{Q} \ \}$,
   (e) $\rho := \{ \ (p, q) \in \mathbb{Q} \times \mathbb{Q} : \quad \exists n \in \mathbb{Z} \ \ n \leq p < n+1 \ \text{ and } \ n \leq q < n+1 \ \}$.
   (f) $\rho := \{ \ (x, y) \in (\mathbb{R} \backslash \{0\})^2 : \quad x \cdot |y| = y \cdot |x| \ \}$,

4. Determine the equivalence classes A_α determined by the following
   equivalence relations:
   (a) $\rho := \{ \ (p, q) \in \mathbb{N} \times \mathbb{N} : \quad m \mid q-p \ \}, \quad (m \in \mathbb{N}^+)$,
   $\alpha = 3$,
   (d) $\rho := \{ \ (x, y) \in \mathbb{R} \times \mathbb{R} : \quad y - x \in \mathbb{Q} \ \}$,
   $\alpha = \pi$,
   (e) $\rho := \{ \ (p, q) \in \mathbb{Q} \times \mathbb{Q} : \quad \exists n \in \mathbb{Z} \ \ n \leq p < n+1 \ \text{ and } \ n \leq q < n+1 \ \}$,
   $\alpha = 3,14$.

5. Determine the inverse relations of the relations given in “Examples” on page 9.

4. FUNCTIONS

Definition. *(Functions.)*

Let X and Y be sets.
A relation $f \subset X \times Y$ is called a *function from X to Y* if
(i) $D(f) = X$,
(ii) $\forall x \in X$ the set $\{ y \in Y : (x,y) \in f \}$ has *exactly one* element.

(I.e. $\forall x \in X$ there exists exactly one element $y \in Y$ such that $(x,y) \in f$.)

We also say that f is a *map*, *mapping* or *transformation* from X to Y.

If f is a *function from X to Y*, we write $f : X \to Y$.
The notations $y = f(x)$ (traditionally said "y is a *function* of x") and $x \mapsto y$ mean that $(x,y) \in f$.

We call $f(x)$ the element associated with x.
We also say that $f(x)$ is the *image* of x under f or the *value* of f at x.

Remarks. *(Domain, range and target of functions.)*

Let X, Y be sets and $f : X \to Y$ be a function.

According to the definitions for relations, $D(f)$ is the *domain* of the function f and $R(f) = \{ f(x) : x \in D(f) \}$ is the *range* of the function f.

If $X \subset Z$, we can also write $f : Z \supset\!\!\to Y$, which means that $D(f) \subset Z$.
Y is called the *target* of the function f.

Definition. *(Restrictions of functions.)*

Let X, Y, A be sets, $A \subset X$, and $f : X \to Y$ be a function.
The function $g : A \to Y$, $g(x) := f(x)$ is called the *restriction of f to A*, and we use the notation $f\,|_A := g$.

Definitions. *(Injective, surjective, bijective functions.)*
Let X, Y be sets and $f : X \to Y$ be a function.

(1) ***Injective function:***
We say that f is *injective* if for all $x, z \in X$ $f(x) = f(z)$ implies $x = z$, that is $x \neq z$ implies $f(x) \neq f(z)$.
(We also say that f is an *injection*, or a *one–to–one correspondence.*)

(2) ***Surjective function:***
We say that f is *surjective* if $\forall y \in Y$ there exists $x \in X$ such that $f(x) = y$, that is $R(f) = Y$.
(We also say that f is a *surjection*, or f is a map *onto* Y.)

(3) ***Bijective function:***
We say that f is *bijective* if it is both *injective* and *surjective.*
(We also say that f is a *bijection.*)

Remark. *(Equality of functions.)*
Let f and g be functions. f and g are *equal functions* $(f = g)$, *iff*
(i) $D(f) = D(g) =: X$ and (ii) $\forall x \in X \quad f(x) = g(x)$.

Definition. *(Inverse function.)*
If $f : X \to Y$ is *injective*, then $\tilde{f} : X \to R(f)$, $\tilde{f}(x) := f(x)$ is *bijective*, thus the relation $\tilde{f}^{-1} \subset R(f) \times X$ is a function that we call the *inverse function* of f.

I.e., *the inverse function of f* is defined by $f^{-1} : R(f) \to X$, $f^{-1}(y) := x$, where x is the *unique* element of X such that $f(x) = y$.

Definition. *(Composition of functions.)*
Let $g : X \to Y_1$ and $f : Y_2 \to Z$ be functions.
We define the *composition* of f and g, denoted by $f \circ g$, such as

$(f \circ g) : X \supset\!\!\to Z, \quad D(f \circ g) := \{\, x \in X : \; g(x) \in Y_2 \,\}, \quad (f \circ g)(x) := f(g(x))$.

Definition. *(Image and inverse image of sets under functions.)*
Let $f : X \to Y$ be a function and A, B be any sets.

(1) ***Image of*** A ***under*** f***:***
We define the set $f(A) := \{\, f(x) : \; x \in A \,\}$
and call $f(A)$ the *image* of A *under* the function f.

(Note that $f(A) = f(A \cap X) \subset f(X) = R(f) \subset Y$.)

(2) ***Inverse image of*** B ***under*** f***:***
We define the set $f^{-1}(B) := \{\, x \in X : \; f(x) \in B \,\}$
and call $f^{-1}(B)$ the *inverse image* of B *under* the function f.

(Note that $f^{-1}(B) = f^{-1}(B \cap Y) \subset f^{-1}(Y) = f^{-1}(R(f)) = X$.)

Remarks.
It is important to see that the set $f^{-1}(B)$ can be defined for any set B, even if f is not injective (thus, the inverse function of f does not exist). The notation f^{-1} in "$f^{-1}(B)$" does not mean the inverse function of f. However, we can easily prove that if f is *injective*, then for any set B $f^{-1}(B)$ is the image of B under the *inverse function* of f.

We can also prove that the function f is *injective* **if and only if** for each $y \in R(f)$ the set $f^{-1}(\{y\})$ has exactly **one element**.

EXERCISES 4.

1. Determine the *domain* and the *range* of the following functions $f : \mathbb{R} \supset\!\!\to \mathbb{R}$ and examine which of them are *injective* or *surjective*:

   (a) $f(x) := \mid x \mid$,
   (b) $f(x) := \sqrt{\mid x \mid}$,
   (c) $f(x) := [x]$,
   (d) $f(x) := x - [x]$,
   (e) $f(x) := \ln x$,
   (f) $f(x) := \ln \mid x \mid$,
   (g) $f(x) := \mid \ln x \mid$,
   (h) $f(x) := \mid \ln \mid x \mid \mid$,
   (i) $f(x) := \lg \sqrt{x}$,
   (j) $f(x) := \sqrt{\lg x}$,
   (k) $f(x) := \lg x^2$,
   (l) $f(x) := 2 \lg x$,
   (m) $f(x) := (\sqrt{x-3})^2$,
   (n) $f(x) := \sqrt{(x-3)^2}$.

2. Let f be any *injective* function. Prove the following propositions:

   (a) $D(f \circ f^{-1}) = R(f), \quad (f \circ f^{-1})(y) = y \quad$ for all $y \in R(f)$,
   that is $f \circ f^{-1}$ is the *identity* function on $R(f)$.

   (b) $D(f^{-1} \circ f) = D(f), \quad (f^{-1} \circ f)(x) = x \quad$ for all $x \in D(f)$,
   that is $f^{-1} \circ f$ is the *identity* function on $D(f)$.

3. Determine the following functions:

   (a) $\ln \circ \exp$,
   (b) $\exp \circ \ln$,
   (c) $\sin \circ \arcsin$,
   (d) $\arcsin \circ \sin$,
   (e) $\cos \circ \arccos$,
   (f) $\arccos \circ \cos$.

4. Let $f : X \to Y, \quad A, B \subset X$ and $C, D \subset Y$. Prove the following propositions:

   (a) $A \subset B$ implies $f(A) \subset f(B)$,
   (b) (f is *injective* and $f(A) \subset f(B)$) implies $A \subset B$,
   (c) $A \subset f^{-1}(f(A))$,
   (d) $f(f^{-1}(C)) \subset C$,
   (e) $f(A \cup B) = f(A) \cup f(B)$,
   (f) $f(A \cap B) \subset f(A) \cap f(B)$,
   (g) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$,
   (h) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

5. Let $h : X \to Y_1, \quad g : Y_2 \to Z_1, \quad f : Z_2 \to W$ functions.
   Prove the following propositions:

   (a) $f \circ (g \circ h) = (f \circ g) \circ h$,

   (b) If g and h are both *injective*,
   then $g \circ h$ is also *injective* and $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$,

   (c) If g and h are both *surjective* and $Y_1 = Y_2$,
   then $g \circ h : X \to Z_1$ is also *surjective.*

6. Let $f : \mathbb{R} \supset\!\!\to \mathbb{R}, \quad f(x) := \ln^3(1+\sqrt{x})$. Determine the *inverse* of f.

5. CARDINALITY OF SETS

We do not define the cardinality (cardinal number) of a set in general, but we compare sets considering the "number" of their elements by putting them in one–to–one correspondance.

Definitions.
Let X and Y be any sets.

(i) We say that X and Y have the *same cardinality* and write $|X|=|Y|$ or say that X and Y are *equivalent sets* and write $X \sim Y$ if there exists a *bijective function* $f : X \to Y$.

(ii) We say that the *cardinality* of X is *not greater* than the *cardinality* of Y (or the *cardinality* of Y is *not less* than the *cardinality* of X) and write $|X| \leq |Y|$ if there exists an *injective function* $f : X \to Y$.

(iii) We say that the *cardinality* of X is *less* than the *cardinality* of Y (or the *cardinality* of Y is *greater* than the *cardinality* of X) and write $|X| < |Y|$ if $|X| \leq |Y|$ and $|X| \neq |Y|$.

***Theorem* (5.1).**
Let X, Y and Z be sets. Then
(i) $X \sim X$, (ii) $X \sim Y \Rightarrow Y \sim X$, (iii) $(X \sim Y$ and $Y \sim Z) \Rightarrow X \sim Z$.

Proof.
(i) $id_X : X \to X,\ x \mapsto x$ is *bijective*,
(ii) If $f : X \to Y$ is *bijective*, then $f^{-1} : Y \to X$ is also *bijective*,
(iii) If $g : X \to Y$ and $f : Y \to Z$ are *bijective*, then $(f \circ g) : X \to Z$ is also *bijective*.

♠

***Theorem* (5.2).**
Let X and Y be sets. Then the following statements are equivalent:
(i) There exists an *injective function* $f : X \to Y$.
(ii) There exists a *surjective function* $g : Y \to X$.

Proof.
If $X = \emptyset$ or $Y = \emptyset$, then (i) and (ii) are obviously equivalent.

If $X \neq \emptyset$ and $Y \neq \emptyset$, then

(1) if $f : X \to Y$ is *injective*, then, choosing any $x_0 \in X$, the function $g : Y \to X$ defined by

$$g(y) := \begin{cases} f^{-1}(y) & \text{if } y \in R(f) \\ x_0 & \text{if } y \in Y \setminus R(f) \end{cases} \quad \text{is a } \textit{surjection.}$$

(2) if $g : Y \to X$ is *surjective*, then, choosing any $y_x \in g^{-1}(\{x\})$ *for each* $x \in X$, the function $f : X \to Y,\ f(x) := y_x$ is an *injection.*

♠

Remarks.

(i) According to the previous theorem we can say that $| X | \leq | Y |$ *if and only if* there exists a *surjective function* $f : Y \to X$.

(ii) The following theorem (whose proof is omitted) shows that $| X | = | Y |$ *if and only if* $(| X | \leq | Y |$ and $| Y | \leq | X |)$.

***Theorem* (5.3).** *(Bernstein's theorem.)*
Let X and Y be sets. Then the following statements are equivalent:

(i) There exists a *bijective function* $f : X \to Y$.

(ii) There exist *injective functions* $g_1 : X \to Y$ and $g_2 : Y \to X$.

(iii) There exist *surjective functions* $h_1 : Y \to X$ and $h_2 : X \to Y$.

Definition. *(Finite and infinite sets.)*

(i) A set X is called *finite* if either $X = \emptyset$ or $\exists\, m \in \mathbb{N}^+$ such that $X \sim \{1, 2, \dots, m\}$.

We call m (that is uniquely determined) the *cardinality (cardinal number)* of X and write $| X | := m$.
The *cardinality (cardinal number)* of the *empty set* is defined by $| \emptyset | := 0$.

(ii) A set X is called *infinite* if it is *not finite.*

***Theorem* (5.4).**
A set X is *finite* *if and only if* $| X | < | \mathbb{N}^+ |$.

Proof.

(1) If $X = \emptyset$, then we evidently have $| X | < | \mathbb{N}^+ |$.
If $| X | = m \in \mathbb{N}^+$, then $\exists$ a *bijection* $\tilde{f} : X \to \{1, 2, \dots, m\}$,
thus $f : X \to \mathbb{N}^+$, $f(x) := \tilde{f}(x)$ is an *injection*, so we have $| X | \leq | \mathbb{N}^+ |$.
If we suppose that $\exists$ a *bijection* $g : X \to \mathbb{N}^+$, then $(g \circ \tilde{f}^{-1}) : \{1, 2, \dots, m\} \to \mathbb{N}^+$ is a *bijection*, which is obviously *impossible.* Thus, we have $| X | < | \mathbb{N}^+ |$.

(2) If $| X | < | \mathbb{N}^+ |$, then either $X = \emptyset$ (thus X is *finite*) or $\exists$ an *injection* $f : X \to \mathbb{N}^+$ and there is *no bijection* from X to $\mathbb{N}^+$.
If we suppose that X is *infinite*, then evidently $R(f)$ is also *infinite*, which implies that $g : R(f) \to \mathbb{N}^+$, $g(n) := | \{x \in R(f) : x \leq n\} |$ is a *bijective* function.
Thus, $(g \circ f)$ is a *bijection* from X to $\mathbb{N}^+$, which is a *contradiction.*
Hence, we obtain X to be a *finite* set.

♠

***Theorem* (5.5).**
If X is an *infinite set*, then $| X | \geq | \mathbb{N}^+ |$ and $\exists$ $Y \subset X$ such that $| Y | = | \mathbb{N}^+ |$.

Proof.

Let $x_0 \in X$ and define $f : \mathbb{N}^+ \to X$ recursively: $f(1) := x_0$, and for each $n \in \mathbb{N}^+$ choosing any $x_n \in X \setminus \{x_0, \dots, x_{n-1}\}$ let $f(n+1) := x_n$.
Since f is injective, it follows that $| \mathbb{N}^+ | \leq | X |$ and $\mathbb{N}^+ \sim R(f) =: Y$.

♠

Definition. *(Countably infinite sets.)*

A set X is called *countably infinite* if $\mid X \mid=\mid \mathbb{N}^+ \mid$.
According to (5.5) *countably infinite sets* have the *least* infinite cardinality.

Definition. *(Countable and uncountable sets.)*

(i) A set X is called *countable* if $\mid X \mid\leq\mid \mathbb{N}^+ \mid$.

According to the theorem (5.2) X is *countable* if and only if
$\exists\, f : X \to \mathbb{N}^+$ *injection* or $\exists\, g : \mathbb{N}^+ \to X$ *surjection.*

According to the theorems (5.4) and (5.5) X is *countable* if and only if it is *finite* or *countably infinite.*

(ii) A set X is called *uncountable* if it is not countable.

According to the theorem (5.5) X is *uncountable* if and only if $\mid X \mid>\mid \mathbb{N}^+ \mid$.

Examples.

1. $\mathbb{N}^+$ is *countably infinite,* since $id^{\mathbb{N}^+} : \mathbb{N}^+ \to \mathbb{N}^+$ is a *bijection.*
2. $\mathbb{N}$ is *countably infinite,* since $f : \mathbb{N} \to \mathbb{N}^+,\ f(n) := n{+}1$ is a *bijection.*
3. $\mathbb{Z}$ is *countably infinite,* since $f : \mathbb{N}^+ \to \mathbb{Z}$,
   $f(1) := 0,\ f(2n) := n,\ f(2n{+}1) := -n \quad (n \in \mathbb{N}^+)$ is a *bijection.*
4. $\mathbb{Q}^+$ is *countably infinite,* since it is infinite and countable
   ($f : \mathbb{Q}^+ \to \mathbb{N}^+,\quad f(p/q) := 2^p \cdot 3^q \quad p, q \in \mathbb{N}^+,\ (p, q){=}1$ is an *injection*).
5. $\mathbb{N}^+ \times \mathbb{N}^+$ is *countably infinite,* since it is infinite and countable
   ($f : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+,\quad f(m, n) := 2^m \cdot 3^n$ is an *injection*).

***Theorem* (5.6).**

If $\mathcal{A}$ is a *countable* set and for all $A \in \mathcal{A}$ A is *countable*,
then $\bigcup \mathcal{A}$ is also *countable.*

Proof.

(1) If $\mathcal{A} = \emptyset$ or $\mathcal{A} = \{\, \emptyset \,\}$ then $\bigcup \mathcal{A}$ is the empty set which is *countable.*

(2) If $\bigcup \mathcal{A} \neq \emptyset$ then we define an *injection* from $\bigcup \mathcal{A}$ to $\mathbb{N}^+$ as follows:

There exists an *injection* $f : \mathcal{A} \to \mathbb{N}^+$ and
for all $A \in \mathcal{A}$ there exists an *injection* $g_A : A \to \mathbb{N}^+$.

For each $x \in \bigcup \mathcal{A}$ there exists at least one set $A \in \mathcal{A}$ such that $x \in A$.
Now we define $F : \bigcup \mathcal{A} \to\ \mathbb{N}^+ \times \mathbb{N}^+,\quad F(x) := (f(A), g_A(x)) \ \in \mathbb{N}^+ \times \mathbb{N}^+$.

F is *injective*, since if $F(x){=}F(y) =: (m, n)$ then $x, y \in f^{-1}(m) =: A$,
thus $n = g_A(x) = g_A(y)$, which implies that $x = y$.

Let $G : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$ be an *injection* (e.g. $(m, n) \mapsto 2^m \cdot 3^n$).

Since $(G \circ F) : \bigcup \mathcal{A} \to \mathbb{N}^+$ is *injective*, it follows that $\bigcup \mathcal{A}$ is *countable.*

♠

***Theorem* (5.7).**
The set $\mathbb{R}$ of all real numbers is *uncountable.*

Proof.

(1) First we prove (by contradiction) that $(0,1) \subset \mathbb{R}$ is *uncountable.*
If we suppose that $(0,1)$ is *countable*, then $\exists$ a *surjection* $f : \mathbb{N}^+ \to (0,1)$.
Let $x \in (0,1)$ be defined such that $\forall n \in \mathbb{N}^+$, the n–th digit in the decimal representation of x is different from the n–th digit in the decimal representation of $f(n)$ and from 0 and 9. It is evident that $x \notin R(f)$, which is a *contradiction*, since $R(f) = (0,1)$. Thus, $(0,1)$ is *uncountable.*

(2) It is easy to see that $(0,1) \subset \mathbb{R}$ implies that $\mathbb{R}$ is also *uncountable.*

♠

Definition. *(Continuum cardinality.)*
We say that a set X has *continuum cardinality* if $| X |=| \mathbb{R} |$.
We also say that X is a *continuum set.*

Examples.

1. Intervals (a,b), $[a,b)$, $(a,b]$, $[a,b]$ are continuum sets. $(a, b \in \mathbb{R},\ \ a < b)$
2. The power set $\mathcal{P}(\mathbb{N}^+)$ is a continuum set.
3. The set $\mathbb{R} \setminus \mathbb{Q}$ of all irrational numbers is a continuum set.

***Theorem* (5.8).** *(Cantor's theorem.)*
The power set of any set X has *greater cardinality* than the set X.
$(\, | \mathcal{P}(X) | > | X | \, .)$

Proof.

(1) If $X = \emptyset$ then $\mathcal{P}(X) = \{ \emptyset \}$, thus $| X |= 0 < 1 =| \mathcal{P}(X) |$.

(2) If $X \neq \emptyset$ then
$| X | \leq | \mathcal{P}(X) |$, since $f : X \to \mathcal{P}(X)$, $f(x) := \{ x \}$ is an *injection.*
If we suppose that $| X |=| \mathcal{P}(X) |$, then $\exists$ a *bijection* $f : X \to \mathcal{P}(X)$.
Let $A \in \mathcal{P}(X)$ be defined by $A := \{ x \in X :\ \ x \notin f(x) \}$.
Then $\exists\, y \in X$ such that $f(y) = A$.
If $y \in A$ then by the definition of A $y \notin f(y) = A$, while
if $y \notin A = f(y)$ then by the definition of A $y \in A$.
Since it is a *contradiction*, $| X | \neq | \mathcal{P}(X) |$ must hold.

♠

Remark. (5.9).
If X is an *infinite set*, then there exists $Z \subset X$ *strictly* such that $| Z |=| X |$.

Proof.

Let $Y \subset X$ such that $| Y |=| \mathbb{N}^+ |$. Then $\exists$ a *bijection* $f : \mathbb{N}^+ \to Y$,
thus $g : \mathbb{N}^+ \to Y$, $g(n) := f(2n)$ is *injective* and $R(g) \subset Y$ *strictly.*
Hence, the function $h : X \to X$ defined by

$$h(x) := \begin{cases} (g \circ f^{-1})(x) & \text{if } x \in Y \\ x & \text{if } x \in X \setminus Y \end{cases}$$

is *injective* and $Z := R(h) = R(g) \cup (X \setminus Y) \subset X$ strictly. ♠

EXERCISES 5.

1. Let X, Y and Z be sets. Prove the following propositions:
   (a) If $|X| \leq |Y|$ and $|Y| \leq |Z|$, then $|X| \leq |Z|$.
   (b) If $X \subset Y$ then $|X| \leq |Y|$.

2. Let X be any *infinite set* and C be a *countable set*. Prove the propositions:
   (a) $|X \cup C| = |X|$.
   (b) If $X \setminus C$ is infinite, then $|X \setminus C| = |X|$.
   (c) If C is finite, then $|X \setminus C| = |X|$.

3. Prove that the examples on page 20 are *continuum sets.*

4. Let A be a *finite* set.
   (a) Prove that if $B \subset A$ *strictly*, then $|B| < |A|$.
   (b) Determine the *cardinal number* of $\mathcal{P}(A)$. ($|\mathcal{P}(A)| = ?$)

5. Let $X_1, X_2, \ldots, X_n$ $(n \in \mathbb{N}^+,\ n > 1)$ be *countable* sets.
   Prove that $X_1 \times X_2 \times \ldots \times X_n$ is also *countable.*

6. Prove that $\mathbb{Q}^n$ is *countably infinite* for all $n \in \mathbb{N}^+$.

7. Prove that $\mathbb{R}^n$ is a *continuum set* for all $n \in \mathbb{N}^+$,
   using (without proof) that $\mathbb{R}^2$ is a *continuum set.*

8. Let X and Y be sets such that $|Y| > 1$.
   Prove that $|Y^X| > |X|$, where Y^X is the set of all functions from X to Y.

9. Let X be a set. Prove that $\mathcal{P}(X) \sim \{0, 1\}^X$.

10. Determine the *cardinality* of the set X, if
    (a) $X := \{(a, b) \subset \mathbb{R} :\ a, b \in \mathbb{Z},\ a < b\}$.
    (b) $X := \{(a, b) \subset \mathbb{R} :\ a, b \in \mathbb{Q},\ a < b\}$.
    (c) $X := \{(a, b) \subset \mathbb{R} :\ a, b \in \mathbb{R},\ a < b\}$.

11. Determine the *cardinality* of the set X, if
    (a) $X := \{x \in \mathbb{R} :\ ax^2 + bx + c = 0,\ a, b, c \in \mathbb{Z},\ a \neq 0\}$.
    (b) $X := \{x \in \mathbb{R} :\ ax^2 + bx + c = 0,\ a, b, c \in \mathbb{Q},\ a \neq 0\}$.
    (c) $X := \{x \in \mathbb{R} :\ ax^2 + bx + c = 0,\ a, b, c \in \mathbb{R},\ a \neq 0\}$.