I. ELEMENTS OF SET THEORY

1.1 Operations over sets. We shall use the following intuitive definition of a set offered by the founder of the set theory Georg Cantor(1845-1918):

"A set is any collection into a whole of definite, distinguishable objects, called *elements*, of our intuition or thought."

Certainly this is not a very precise definition however we shall stick to it. The right approach is to define sets by axioms but this is too complicated to use as a working definition.

We shall usually denote sets by capital letters (Latin, Greek, Russian, etc). They may come with some additional attributes like indices, primes, thickening, or something else. Elements of a set will be usually denoted by small letters of the same or other alphabet. The fact that an object a is an element of a set A is denoted by

$$a \in A.$$

If we want to say that an object a is not an element of a set A we write

$$a \notin A.$$

We consider two sets equal and write $A = B$ if they consist of the same elements. This means that $a \in A$ implies $a \in B$ and conversely $b \in B$ implies $b \in A$. If a set A contains finitely many elements it is called a *finite* set. Otherwise it is called an *infinite set*. A finite set can be (in principle) given by listing all its elements, for example we write

$$A = \{a, b, c, d\}.$$

For the sake of convenience we include in the definition the set without elements. It is denoted by

$$\emptyset$$

and is called the *empty* set.

Definition. A set A is called a *subset* of a set B if any element of A is an element of B. In other words

$$a \in A \Longrightarrow a \in B.$$

Here the symbol $\Longrightarrow$ stands for the word "implies". By definition the empty set is a subset of any set. We write

$$A \subseteq B$$

to express the fact that A is a subset of B. We use

$$\not\subseteq$$

to express the fact that A is not a subset of B.

Clearlly $A = B$ is equivalent to $A \subseteq B$ and $B \subseteq A$. If A is a subset of B but A is not equal to B ($A \neq B$) then we say that A is a *proper subset* of B and write

$$A \subset B.$$

Very often we shall define a set A as a subset of some other set B by declaring the property which distinguish elements of A among all elements of B. We write it in the form

$$A = \{a \in B \mid a \text{ satisfies Property}\}.$$

For example, let B be the set of people, A is the set of teenagers, then

$$A = \{a \in B \mid a \text{ is of age between 13 and 19}\}.$$

Of course, a set can be defined like this in many ways. For example we can define the empty set by saying

$$\emptyset = \{x \in \mathbf{R} \mid x^2 = -1\} = \{x \in \mathbf{R} \mid x^2 < 0\}.$$

Here $\mathbf{R}$ stands for the set of real numbers which we shall properly define later. For the future use let us remind the definition of *intervals* of the numerical line. They are subsets of $\mathbf{R}$ defined as follows

$$[a,b] = \{x \in \mathbf{R} \mid a \le x \le b\} \text{ (\textit{segment} or \textit{closed interval})},$$

$$(a,b) = \{x \in \mathbf{R} \mid a < x < b\} \text{ (\textit{interval} or \textit{open interval})},$$

$$(a,b] = \{x \in \mathbf{R} \mid a < x \le b\},\ [a,b) = \{x \in \mathbf{R} \mid a \le x < b\} \text{ (\textit{semi-interval})},$$

$$[a,\infty) = \{x \in \mathbf{R} \mid x \ge a\},\ (-\infty,a] = \{x \in \mathbf{R} \mid x \le a\} \text{ (\textit{unbounded segment})},$$

$$(a,\infty) = \{x \in \mathbf{R} \mid x \ge a\},\ (-\infty,a) = \{x \in \mathbf{R} \mid x < a\} \text{ (\textit{unbounded interval})}.$$

The following operations can be performed over sets:

The *union* (or *sum*)

$$A \cup B$$

of two sets A and B is the set of objects which are elements of A **or** of B.

The *intersection*

$$A \cap B$$

of two sets A and B is the set of objects which are elements of A **and** B.

The *complement*

$$A \setminus B$$

of a set B in a set A is the set of objects in A which are not objects of B, i.e.,

$$A \setminus B = \{a \in A \mid a \notin B\}.$$

The *power set* (or *Boolean*)

$$\mathcal{P}(A)$$

of a set A is the set whose elements are subsets of A.

The Cartesian product

$$A \times B$$

of two sets A and B is the set whose elements are pairs (a,b) where $a \in A$ and $b \in B$. Here the order is essential, two pairs (a,b) and (c,d) are considered equal only if $a = c$ and $b = d$.

There are many properties of the introduced operations, most of them is very easy to prove. Let us state and prove some of them to get some experience in formal mathematical proofs.

Proposition 1. *Let A, B, C be three sets. Then*

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Here the brackets are used to indicate the order in which we apply our operations.

Proof. To show that the two sets are equal we have to prove the following two assertions:

$$x \in (A \cup B) \cap C \Longrightarrow x \in (A \cap C) \cup (B \cap C),$$

$$x \in (A \cap C) \cup (B \cap C) \Longrightarrow x \in (A \cup B) \cap C.$$

Let us prove the first one. By definition of $\cap$, $x \in A \cup B$ and also $x \in C$. By definition of $\cup$, $x \in A$ or $x \in B$. Thus we have two possibilities: (a) $x \in C$ and $x \in A$; (b) $x \in C$ and $x \in B$. In case (a), $x \in A \cap C$ and by definition of $\cup$, we get $x \in (A \cap C) \cup (B \cap C)$. Similarly, in case (b), $x \in B \cap C$, and hence again $x \in (A \cap C) \cup (B \cap C)$. This proves the first assertion. Let us prove the second one. By definition of $\cup$, we get $x \in A \cap C$ or $x \in B \cap C$. In both cases $x \in C$, and also we have $x \in A \cup B$. Thus $x \in C \cap (A \cup B)$ as wanted.

Proposition 2. *Let A, B, and C be sets. Then*

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C).$$

Proof. Again we have to check the two statements

$$x \in A \times (B \setminus C) \Longleftrightarrow x \in (A \times B) \setminus (A \times C).$$

Here we combine the two arrows $\Longleftarrow$ and $\Longrightarrow$ in one. This can be read as "if and only if". Let us prove $\Longrightarrow$. By definition of $\times$, $x = (a, b)$, where $a \in A, b \in B, b \notin C$. Thus $x \in A \times B$ but $x \notin A \times C$. By definition of $\setminus$ we are done. Let us prove the assertion $\Longleftarrow$. By definition of $\times$ and $\setminus$, $x = (a, b)$ where $a \in A, b \in B$. Since $x \notin A \times C$, we observe that $b \notin C$. Thus $a \in A, b \in B \setminus C$, and we obtain that $x \in A \times (B \setminus C)$. This ends the proof of the proposition.

Proposition 3. *Let A and B be two sets. Then*

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B).$$

Proof. We have to prove that

$$X \subset A \cap B \Longleftrightarrow X \subset A, X \subset B.$$

The left-hand side is equivalent to the assertion $x \in X \Longrightarrow x \in A \cap B$. The right-hand side is equivalent to the assertion $x \in X \Longrightarrow x \in A, x \in B$. However by definition of $\cap, x \in A \cap B \Longleftrightarrow x \in A, x \in B$. Thus the two assertions are equivalent (that is, one implies the other).

Remark. To escape contradictions one should avoid considering all possible sets and restrict oneself with subsets of one chosen set, the *universum*. It must be large enough for all our needs (it could be enlarged it if our needs require so). The following contradiction (called the Russel Paradox) shows that the set whose elements are arbitrary sets does not exist. Let us prove it. Suppose this set, denoted by $\mathcal{U}$, exists. Let

$$X = \{A \in \mathcal{U} \mid A \notin A\}.$$

This set is obviously non-empty. I claim that $X \notin X$. In fact if $X \in X$ then $X \notin X$ by construction of X. On the other hand I claim that $X \in X$. In fact if $X \notin X$ then $X \in X$. This is a contradiction. So we have both $X \notin X$ and $X \in X$ which is absurd.

Exercises 1.1 In spite of the obviousness of some of the following statements try to write a formal proof).
1. Prove that
(a) $A \subseteq B, B \subseteq C \Longrightarrow A \subseteq C$;
(b) $A \subseteq B, B \subset C \Longrightarrow A \subset C$;
(c) $A \subseteq B \cap C \Longrightarrow A \subseteq B \cup C$.
2. Determine whether the following statement is true or false. If it is true prove it, if it is false give an example showing that it is wrong.
(a) if $x \in A$ and $A \nsubseteq B$, then $x \notin B$;
(b) $A \in \mathcal{P}(A)$;
(c) $x \in A \Leftrightarrow x \in \mathcal{P}(A)$;
(d) $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$;
(e) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$;
(f) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.
3. Let $A = \{a, b, c, d\}, B = \{a, b\}$. List the elements of the sets $\mathcal{P}(A),\ A \setminus B,\ A \times A,\ A \times B,\ \mathcal{P}(A) \setminus \mathcal{P}(B)$, $\mathcal{P}(A) \times \mathcal{P}(B), \mathcal{P}(\mathcal{P}(B))$.
4. Prove that for any sets A, B and C
(a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
(b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
5. Prove the "associativity" laws
(a) $(A \cup B) \cup C = A \cup (B \cup C)$ (any of this sets is denoted by $A \cup B \cup C$);
(b) $(A \cap B) \cap C = A \cap (B \cap C)$ (any of this sets is denoted by $A \cap B \cap C$).

1.2 Maps of sets. The concept of a function, or a map of sets, is the most fundamental in mathematics.

Definition. A *map* (or a *function*, or a *mapping*) is a triple consisting of a non-empty set X, a non-empty set Y, and a rule f which assigns to each element x from X a unique element of Y, denoted by $f(x)$.

The map is usually denoted by

$$f : X \to Y$$

or by

$$X \xrightarrow{f} Y,$$

or sometimes just by f if the sets X and Y are obvious from the context. The set X is called the *domain* of the map and the set Y is called the *range* of the map. The element $f(x)$ is called the *value* of f at x. Sometimes we use the expression $x \mapsto f(x)$ to define the rule of the map.

Note that the map $f : X \to Y$ is like the Holy Trinity, we cannot change any attributes of it without changing the map. For example, we may replace X with its subset A and use the same rule f and the same range set Y. The result is another map denoted by $f|A$ and called the *restriction* of f to the subset A. If all the values of the map f belong to a subset B of Y, we may keep X and the rule f to define another map $f : X \to B$, called the *restriction of the range* of f to the subset B of Y.

Examples. 1. The functions $y = f(x)$ studied in Calculus are the maps with the domain and the range sets being subsets of $\mathbf{R}$. For example the function $y = \sin x$ can be considered as the map $f : \mathbf{R} \to \mathbf{R}$ or as the map $f : \mathbf{R} \to [-1, 1]$.
2. Let A be a non-empty set, we can define the map $f : A \to \mathcal{P}(\mathcal{A})$ by assigning to each element $x \in X$ the subset $\{x\}$ of X.
3. Let $A \times B$ be the cartesian product of two non-empty sets. We define the map $pr_1 : A \times B \to A$ by assigning to each pair $(a, b) \in A \times B$ the element a. It is called the *first projection* map. Similarly, one defines the *second projection* map $pr_2 : A \times B \to B$.
4. Let A be a subset of a non-empty set X, and $\{0, 1\}$ be the set consisting of numbers 0 and 1. Define the function $\chi_A : X \to \{0, 1\}$ by the following rule

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

This function is called the *characteristic function* of the subset A.
5. For any non-empty set X we define the *identity map* $\mathrm{id}_X : X \to X$, where for any $x \in X$,

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

More generally, if X is a subset of Y we define the map $\mathrm{id}_{X,Y} : X \to Y$ by the rule

$$\mathrm{id}_{X,Y}(x) = x.$$

It is called the *canonical inclusion* map of the subset X.
6. For any non-empty sets X and Y, and a fixed element $y \in Y$ we define the *constant* map $c_y : X \to Y$ by the rule $c_y(x) = y$ for any $x \in X$.
7. Let $f : X \to Y$ be a map. For any non-empty subset A of X set

$$f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}.$$

This is a non-empty subset of Y which we shall call the *image* of the subset A under the map f. By definition we put

$$f(\emptyset) = \emptyset.$$

Now we can define the map

$$\mathcal{P}(f) : \mathcal{P}(X) \to \mathcal{P}(Y)$$

by the rule

$$\mathcal{P}(f)(A) = f(A)$$

for any subset A of X.

8. Let $f : X \to Y$ be a map. For any non-empty subset B of Y we put

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

This is a subset (maybe empty) of X which we shall call the *pre-image* of the subset B under the map f. Now we can define the map

$$\mathcal{P}^{-1}(f) : \mathcal{P}(Y) \to \mathcal{P}(X)$$

by the rule

$$\mathcal{P}^{-1}(f)(B) = f^{-1}(B)$$

for any subset B of Y.

The following operations over maps can be defined:

1) **Composition of maps**. Let $f : X \to Y$ and $g : Y \to Z$ be two maps such that the range of the first is equal to the domain of the second. We define the *composition map*

$$g \circ f : X \to Z$$

by the rule

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

for any $x \in X$.

Note that we can generalize a little the definition by requiring that the range of the first function is a subset of the domain of the second one.

2) **Cartesian product**. Let $f : X \to Y$ and $g : X' \to Y'$ be two maps. We define the map

$$f \times g : X \times X' \to Y \times Y'$$

by the rule

$$f \times g(x, x') = (f(x), g(x'))$$

for any $(x, x') \in X \times X'$. This map is called the *Cartesian product* of the maps f and g.

3) **Gluing**. Let $f : X \to Y$ and $g : X' \to Y'$ be two maps. Suppose $f(X \cap X') \subset Y \cap Y', g(X \cap X') \subset Y \cap Y'$ and $f(x) = g(x)$ for any $x \in X \cap X'$. Then we define the map

$$f \cup g : X \cup X' \to Y \cup Y'$$

by the rule

$$f \cup g(x) = \begin{cases} f(x) & \text{if } x \in X, \\ g(x) & \text{if } x \in X'. \end{cases}$$

This rule is legal since, if $x \in X \cap X'$ the value $f \cup g(x)$ can be computed by using either f or g.

For example we may apply this operation in the case when $X \cap X' = \emptyset$, or in the case when $Y = Y'$ and $f(x) = g(x)$ for any $x \in X \cap X'$.

Examples. 1. Let $f : \mathbf{R} \to \mathbf{R}$ be given by the rule $f(x) = x^2$ and let $g : \mathbf{R} \to \mathbf{R}$ be given by the rule $g(x) = x^3$. Then the composition $g \circ f : \mathbf{R} \to \mathbf{R}$ is the function $y = x^6$. The composition $f \circ g$ is the same function as $g \circ f$. But this is just an "accident". For example if $g : \mathbf{R} \to \mathbf{R}$ is given by $g(x) = \sin x$ then $f \circ g(x) = \sin x^2$ but $g \circ f(x) = \sin x^2$. Obviously they are different functions.

In general, the composition of functions studied in Calculus corresponds to the notion of superposition of function. If $y = f(x)$ and $w = g(y)$ are two functions such that the values of the first one belong to the domain of the definition of the second one, then the superposition is the function $w = g(f(x))$.

2. Let $f : X \to Y$ be any map. Then

$$f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f.$$

3. Let $X = \{a, b, c\}, Y = X, Z = \{d, e\}$. Let $f : X \to Y$ be given by the rule

$$f(a) = b, f(b) = c, f(c) = a,$$

and let $g : Y \to Z$ be given by the rule

$$g(a) = d, g(b) = g(c) = e.$$

Then the composition $g \circ f : X \to Z$ is given by the rule

$$g \circ f(a) = g \circ f(b) = e, g \circ f(c) = d.$$

4. Let $f : X \to Y$ be a map, and $\chi_B : Y \to \{0, 1\}$ be the characteristic function of a subset B of Y. Then the composition $\chi_B \circ f : X \to \{0, 1\}$ coincides with the characteristic function $\chi_{f^{-1}(B)}$ of the pre-image of B. In fact, by definition of the composition and the function χ_B we have

$$\chi_B \circ f(x) = \chi_B(f(x)) = \begin{cases} 1 & \text{if } f(x) \in B \\ 0 & \text{if } f(x) \notin B \end{cases} = \begin{cases} 1 & \text{if } x \in f^{-1}(B) \\ 0 & \text{if } x \notin f^{-1}(B). \end{cases}$$

5. Let $A = [0, \infty)$ (we shall denote this set by $\mathbf{R}_{\geq 0}$), and let $B = (-\infty, 0]$ (denoted by $\mathbf{R}_{\leq 0}$). Both are considered as subsets of $\mathbf{R}$. Let $f : \mathbf{R}_{\geq 0} \to \mathbf{R}$ be the restriction of the identity function $\mathrm{id}_{\mathbf{R}}$ to the subset A, and let $g : \mathbf{R}_{\leq 0} \to \mathbf{R}$ be defined by the rule $g(x) = -x$. Then the gluing of these two functions is the absolute value function $y = |x|$.
6. Let $A \subseteq X$, and $\chi_A : X \to \{0, 1\}$ be its characteristic function. Let $c_1 : A \to \{0, 1\}$ be the constant function with the value 1 and let $c_0 : X \setminus A :\to \{0, 1\}$ be the constant function with the value 0. Then the gluing $c_1 \cup c_0$ is equal to χ_A. 1

The following theorem will be used often.

Theorem (Associativity of composition). *Let $f : X \to Y, g : Y \to Z, h : Z \to W$ be three maps. Then*

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

Proof. To show that two maps are equal we have to check that their domains, their ranges, and their rules are equal. In our case we have to verify only the latter since the rest is obvious. Let $x \in X$. By definition of $g \circ f$, we have $g \circ f(x) = g(f(x)) \in Z$. By definition of $h \circ (g \circ f)$ we have

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

Now by definition of $(h \circ g) \circ f$ and $h \circ g$ we have

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

Thus both rules are the same and equal to the rule which assigns to an element $x \in X$ the element $h(g(f(x)))$. We can think about this rule as the composition

$$h \circ g \circ f : X \to W.$$

The notion of the graph of a function $y = f(x)$ can be easily extended to the case of arbitrary maps.

Definition. Let $f : X \to Y$ be a map. Its *graph* is the subset

$$\Gamma_f = \{(a, b) \in X \times Y \mid b = f(a)\}.$$

For example, when $X = Y = \mathbf{R}$, the graph is a subset of $\mathbf{R} \times \mathbf{R}$.

Proposition. *Let X and Y be two sets. A subset Γ of $X \times Y$ is equal to the graph of a map $f : X \to Y$ if and only if for any $x \in X$ the subset $\{x\} \times Y$ has exactly one element in common with Γ.*

Proof. If $\Gamma = \Gamma_f$ for some $f : X \to Y$, then

$$(\{x\} \times Y) \cap \Gamma = \{(x, f(y))\}$$

consists of one element. Conversely, if this intersection consists of one element, say (x, y), then we define the map $f : X \to Y$ by the rule $f(x) = y$. It is easy to see that $\Gamma = \Gamma_f$.

One may use the previous proposition as an equivalent definition of a map: A map is a triple (X, Y, Γ) consisting of two sets X and Y and a subset Γ of $X \times Y$ satisfying the property stated in the Proposition. This definition does not appeal to the understanding of the word "rule" which we used in our definition of a map.

Exercises 1.2

1. Let $f : \mathbf{R} \to \mathbf{R}$ be given as follows

$$f(x) = \begin{cases} x^2 - 1 & \text{if } x > 1 \\ log(|x| + 2) & \text{if } -1 \leq x \leq 1 \\ 1/x & \text{if } x < -1. \end{cases}$$

Find $f(2), f(-1), f(-2)$.

2. Suppose X consists of n elements and Y consists of m elements.
(a) Show that there are m^n maps from X to Y (Hint: use induction on n).
(b) How many elements in the power set $\mathcal{P}(X)$ (Hint: Use the notion of the characteristic function).

3. Each of the following expressions represent the rule for a function from $\mathbf{R}$ to $\mathbf{R}$:

$$f(x) = x^2, \ f(x) = \sin x, f(x) = \frac{1}{x^2 + 1}.$$

Find the images of the following subsets of $A \subseteq \mathbf{R}$ under each map
(a) $A = \mathbf{R}$;
(b) $A = \{x \in \mathbf{R} \mid -\pi \leq x \leq \pi\}$;
(c) $A = \mathbf{R}_{\geq 0}$.

4. For the functions from the previous exercise find the formula for the compositions of any pair of the functions. Check the associativity for the composition of the three functions in all possible orders.

5. Let $f : X \to Y$ be a map of sets, $A \subseteq X, B \subseteq Y$. Prove that
(a) $f(f^{-1}(B)) \subseteq B$;
(b) $A \subseteq f^{-1}(f(A))$. Give examples when $\subseteq$ can be replaced by $\subset$.

6. Let $f : A \to X$ and $g : A \to Y$ be two maps. Show that there exists a unique map $h : A \to X \times Y$ such that $pr_1 \circ h = f, pr_2 \circ h = g$.

7. Let $f : X \to Y$ be a map and $\Gamma_f \subseteq X \times Y$ be its graph. Show that
(a) $f(X) = pr_2(\Gamma_f)$;
(b) $\Gamma_f = (f \times \mathrm{id}_Y)^{-1}(\Gamma_{\mathrm{id}_Y})$.

1.3 Equivalence of sets. When we are talking about two sets consisting of the same number of elements, for most purposes it does not matter what these objects really are, the only important thing is that the two sets consist of the same number of elements. Just renaming the elements allows one to go from one set to another. The mathematical idea behind of this is the notion of equivalent sets. It will apply even to infinite sets.

Definition. A map $f : X \to Y$ of sets is called *injective* if

$$f(x) = f(y) \Longrightarrow x = y.$$

The map f is called *surjective* if for any $y \in Y$ there exists $x \in X$ with $f(x) = y$, or in other words,

$$f(X) = Y.$$

The map $f : X \to Y$ is called *bijective* or *a one-to-one correspondence* if it is both injective and surjective.

Using the definitions of the images and pre-images of subsets, we can restate the definition as follows:

Definition. A map $f : X \to Y$ of sets is called *injective* if for any $y \in Y$,

$$f^{-1}(\{x\}) \quad \text{consists of at most one element.}$$

The map f is called *surjective* if for any $y \in Y$,

$$f^{-1}(\{x\}) \neq \emptyset.$$

The map $f : X \to Y$ is called *bijective* if for any $y \in Y$,

$$f^{-1}(\{x\}) \quad \text{consists of one element.}$$

It must be clear that the restriction of the range of an injective map $f : X \to Y$ to $f(X)$ defines a bijective map $f : X \to f(X)$.

Examples. 1. The function $\mathbf{R}_{\geq 0} \to \mathbf{R}$ defined by the formula $f(x) = x^2$ is injective but not surjective. In fact any negative number is not in $f(\mathbf{R}_{\geq 0})$ but $a^2 = b^2$ implies $a = b$ since both a and b are non-negative numbers. If we use the same formula to define the function from $\mathbf{R}$ to $\mathbf{R}_{\geq 0}$ then we get a surjective but not injective map. Finally if we use the same rule to define the function from $\mathbf{R}$ to $\mathbf{R}$ we get neither surjective nor injective map.
2. In example 3 from section 1.1 we find that the map f is bijective and the map g is surjective but not injective.
3. The constant map $c_y : X \to Y$ is injective only if X consists of one element and is surjective only if Y consists of one element.
4. The characteristic function $\chi_A : X \to \{0, 1\}$ is surjective if $A \neq \emptyset$ and $A \neq X$. If neither case occurs, χ_A is injective only if X consists of two elements.
5. The function $f : [-\pi/2, \pi/2] \to [-1, 1]$ defined by the rule $f(x) = \sin x$ is a bijective map. The same rule defines an injective but surjective map from $[-\pi/2, \pi/2]$ to $\mathbf{R}$ and a surjective but not injective map from $\mathbf{R}$ to $[-1, 1]$.
6. Let $X = A_1 \cup A_2$ and $Y = B_1 \cup B_2$. Suppose $A_1 \cap A_2 = \emptyset, B_1 \cap B_2 = \emptyset$. Let $f_1 : A_1 \to B_1$ and $f_2 : A_2 \to B_2$ are injective (surjective) maps. Then the gluing map $f_1 \cup f_2 : X \to Y$ is injective (surjective).
7. Let X be a finite set consisting of n elements. Suppose $n \neq 0$, i.e., $X \neq \emptyset$. Take any element from X and denote it by x_1. If $X \neq \{x_1\}$, take any element from $X \setminus \{x_1\}$ and denote it by x_2. Continuing in this way we will be able to list all elements of X in the form $X = \{x_1, \ldots, x_n\}$. Suppose now Y is another finite set consisting of m elements. We can write $Y = \{y_1, \ldots, y_m\}$. Assume $n \leq m$, then we can define the map $f : X \to Y$ by the formula

$$f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_n) = y_n.$$

Obviously this map is injective. Suppose $n \geq m$. Then we can define the map $f : X \to Y$ by the formula

$$f(x_1) = y_1, \ldots, f(x_m) = y_m, f(x_i) = y_1 \text{ if } i > m.$$

Obviously this map is surjective but not injective if $n > m$. It is bijective if $n = m$.

Proposition 1. *Let $f : X \to Y$ and $g : Y \to Z$ be two maps. 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 bjective.

Proof. (i) We have to check the definition. Let $a, b \in X$ with $g \circ f(a) = g \circ f(b)$. We have to show that this implies that $a = b$. By definition of composition, we have $g(f(a)) = g(f(b))$. Since g is injective this implies that $f(a) = f(b)$. Since f is injective this implies that $a = b$.

(ii) We have to verify that $g \circ f(X) = Z$. This means that for any $z \in Z$ there exists $x \in X$ such that $g \circ f(x) = g(f(x)) = z$. Let us find this x as follows. Since g is surjective, we can find $y \in Y$ such that $g(y) = z$. Since f is surjective we can find x such that $f(x) = y$. Thus $g(f(x)) = g(y) = z$ as needed.

(iii) Follows from (i) and (ii).

Definition. Let $f : X \to Y$ be a map. A map $f : Y \to X$ is called an inverse map for f if

$$g \circ f = \mathrm{id}_X, \quad f \circ g = \mathrm{id}_Y.$$

Theorem 1. *Let $f : X \to Y$ be a map of sets. An inverse map for f exists if and only if f is bijective. If f is bijective an inverse map is unique.*

Proof. First let us prove the part "if", that is, an inverse map exists if f is bijective. We define the map $g : Y \to X$ by the following rule. Let y be an element of Y. Since f is surjective we can find an element $x \in X$ such that $f(x) = y$. Since f is injective such x is unique. So we can set $g(y) = x$. This defines g. Now let us check that g is an inverse map for f. By definition, if $f(x) = y$ we have $x = g(y) = g(f(x))$. This checks that $g \circ f = \mathrm{id}_X$. Again by construction of g, for any $y \in Y$ we have $f(g(y)) = y$. This checks that $f \circ g = \mathrm{id}_Y$. Thus g is an inverse map for f.

Let us prove the part "only if", that is, f must be bijective if an inverse map g exists. Suppose that g exists. We have to check first that f is injective. Let $a, b \in X$ with $f(a) = f(b)$. Applying to both sides the function g we obtain $g(f(x)) = g \circ f(a) = g(f(b)) = g \circ f(b)$. However, by definition of the inverse, $g \circ f = \mathrm{id}_X$. Thus $a = b$. Let us prove that f is surjective. For any $y \in Y$ we have to find some $x \in X$ with $f(x) = y$. Let us take x equal to $g(y)$. Since $f \circ g = \mathrm{id}_Y$, we obtain $f(g(y)) = f(x) = y$. This proves the assertion.

Definition. Let $f : X \to Y$ be a bijective map. The unique inverse map for f is denoted by f^{-1} and is called *the inverse map* for f.

Warning. Don't confuse the notation $f^{-1}(x)$ for the value of the inverse map $f^{-1} : Y \to X$ with the notation $f^{-1}(x)$ for the pre-image of the subset $\{x\}$ under the map $f : X \to Y$. If f^{-1} is defined, then

$$\{f^{-1}(x)\} = f^{-1}(\{x\}).$$

Inspite of this confusion one often uses the notation $f^{-1}(y)$ for $f^{-1}(\{y\})$. This set is called the *fibre* of f over y.

On the positive side there is no confusion to write $f^{-1}(A)$ for the pre-image of a set A under a bijective map $f : X \to Y$ and the image $f^{-1}(A)$ of the same set under the inverse map f^{-1}. They are equal subsets of X. In fact,

$$x \in f^{-1}(A)\ (\mathrm{pre-image}) \iff f(x) = a \in A \iff x = f^{-1}(a), a \in A \iff x \in f^{1}(A)\ (\mathrm{image})$$

Examples. 8. The map $f : \mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$ defined by the formula $f(x) = x^2$ has the inverse map defined by the formula $g(x) = \sqrt{x}$.
9. The map $[-\pi/2, \pi/2] \to [-1, 1]$ defined by the formula $f(x) = \sin x$ has the inverse map $f^{-1} : [-1, 1] \to [\pi/2, \pi/2]$ defined by the formula $f^{-1}(x) = \mathrm{arcsin} x$.
10. Let $f : \{a, b, c\} \to \{a, b, c\}$ be the map from Example 3 of section 1.1. Its inverse is given by the formula $f^{-1}(a)c), f^{-1}(b) = a, f^{-1}(c) = b$.
11. Let X be a set and $\mathcal{P}(X)$ be its power set. Define $f : \mathcal{P}(X) \to \mathcal{P}(X)$ by the formula $f(A) = X \setminus A$. Then $f^{-1} = f$.

Proposition 2. *Let $f : X \to Y$ be a bijective map of sets. Then*
(i) f^{-1} is bijective and its inverse coincides with f;
(ii) if $g : Y \to Z$ is another bijective map, then

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

Proof. (i) follows from the definition of the inverse map.
(ii) We have to check that the map $h = f^{-1} \circ g^{-1} : Z \to X$ satisfies $h \circ (g \circ f) = \mathrm{id}_X, f^{-1} \circ g^{-1} \circ h = \mathrm{id}_Z$. using the associativity property of composition we have

$$h \circ (g \circ f) = (f^{-1} \circ g^{-1}) \circ (g \circ f) = ((f^{-1} \circ g^{-1}) \circ g) \circ f =$$

$$(f^{-1} \circ (g^{-1}) \circ g)) \circ f = (f^{-1} \circ \mathrm{id}_Y) \circ f = f^{-1} \circ f = \mathrm{id}_X.$$

Similarly we verify the second propery (do it!).

Definition. A set X is called *equivalent* (or *equipotent*) to a set Y (we write $X \sim Y$) if there exists a bijective map from X to Y.

Proposition 3.
(i) Each set is equivalent to itself.
(ii) If X is equivalent to Y, then Y is equivalent to X.
(iii) If X is equivalent to Y, and Y is equivalent to Z, then X is equivalent to Z.

Proof. (i) The identity map $\mathrm{id}_X : X \to X$ is obviously bijective.
(ii) Apply Proposition 2.
(iii) Apply Proposition 1.

Examples. 12. From example 7 we obtain that any two finite sets consisting of the same number elements are equivalent. Converse is also true: equivalent finite sets have the same number of elements.
13. From example 11 we conclude that the sets $[-\pi/2, \pi/2]$ and $[-1, 1]$ are equivalent. In fact any two segments $[a, b]$ and $[c, d]$ with $a < b, c < d$ are equivalent. To see this we define the function $f : [a, b] \to [c, d]$ by the formula

$$f(x) = \frac{c-d}{a-b}\, x + \frac{ad-bc}{a-b}.$$

Its graph is a segment of the line with the slope $\frac{c-d}{a-b}$ which joins the points (a, c) and (b, d). The inverse function $f^{-1} : [c, d] \to [a, b]$ is defined by the formula

$$f^{-1}(x) = \frac{(a-b)x - ad + bc}{c-d}.$$

In fact $f(f^{-1}(x)) = \frac{c-d}{a-b}\,(\frac{(a-b)x-ad+bc}{c-d}) + \frac{ad-bc}{a-b} = x$, for any $x \in [c, d]$ and similarly we check that $f^{-1}(f(x)) = x$ for any $x \in [a, b]$. Thus f is bijective.
14. Any intervals (a, b) and (c, d) are equivalent. To see this we use the function from the previous example and restrict it to the subset (a, b) of $[a, b]$. Similarly we show that semi-intervals $(a, b]$ and $(c, d]$ are equivalent, and semi-intervals $[a, b)$ and $[c, d)$ are equivalent.
15. Now let us see that interval $(0, 2)$ is equivalent to $\mathbf{R}$. We define the map $f : \mathbf{R} \to (0, 2)$ by the formula

$$f(x) = \begin{cases} \frac{1}{x^2+1} & \text{if } x \geq 0 \\ \frac{1}{x^2+1} + 1 & \text{if } x < 0. \end{cases}$$

This map is obtained by gluing two maps $g : [0, \infty) \to (0, 1]$ and $h : (-\infty, 0) \to (1, 2)$ defined by the formula $g(x) = \frac{1}{x^2+1}$ and $h(x) = \frac{1}{x^2+1} + 1$ (see Exercise 1.2 3)). Each of this map is bijective. The inverse functions are defined by the rules $g^{-1}(x) = \sqrt{(\frac{1}{x} - 1)}$, $h^{-1}(x) = -\sqrt{(\frac{1}{x-1} - 1)}$. By example 6, the map f is bijective. Thus any interval is equivalent to the set of real numbers.

16. Now let us see that any segment is equivalent to an interval. Since $(0,1) \sim \mathbf{R}$, it is enough to show that $[0,1]$ is equivalent to $\mathbf{R}$. Suppose we show that $\mathbf{R} \setminus \{0,1\} \sim \mathbf{R}$. Then, by transitivity (Proposition 3 (iii)), there exists a bijective map $f : \mathbf{R} \setminus \{0,1\} \to (0,1)$. Since $[0,1] = (0,1) \cup \{0,1\}$, we can extend this map to a bijective map $\mathbf{R} \to [0,1]$ by gluing f with the identity map $\{0,1\} \to \{0,1\}$. Write

$$\mathbf{R} = \mathbf{N} \cup (\mathbf{R} \setminus \mathbf{N}), \quad \mathbf{R} \setminus \{0,1\} = \mathbf{N} \setminus \{0,1\} \cup (\mathbf{R} \setminus \mathbf{N}).$$

where $\mathbf{N}$ denotes the set of natural numbers (to which we include 0). Suppose we find a bijective map $g : \mathbf{N} \to \mathbf{N} \setminus \{0,1\}$, then we will be able to define the needed bijection $f : \mathbf{R} \to \mathbf{R} \setminus \{0,1\}$ as the gluing $f = g \cup \mathrm{id}_{\mathbf{R} \setminus \mathbf{N}}$. So it remains to define a bijective map $g : \mathbf{N} \to \mathbf{N} \setminus \{0,1\} = \{2,3,\ldots\}$. But this is easy : send 0 to 2, 1 to 3, and so on. In other words, define g by the rule $g(x) = x + 2$.

Definition. A set is called *countable* if it is equivalent to a subset of the set $\mathbf{N}$ of natural numbers. If moreover the set is infinite, it is called *countably infinite* or *denumerable*.

Examples. 17. The set $\mathbf{Z}$ of integers is countably infinite. The map $f : \mathbf{Z} \to \mathbf{N}$ defined by the formula

$$f(m) = \begin{cases} 2m & \text{if } m \geq 0 \\ -2m - 1 & \text{if } m < 0 \end{cases}$$

is bijective.
18. The set $\mathbf{Q}$ of rational numbers is countable. This is less obvious than the previous example. Each rational number can be written uniquely in the form $\frac{p}{q}$ where $p \in \mathbf{Z}, q \in \mathbf{N} \setminus \{0\}$ and the greatest common divisor of p and q is equal to 1. Call the number $|p| + q$ the height of $\frac{p}{q}$. For example $\frac{-2}{3}$ has height 5. It is clear that the set of all rational numbers with the same height is finite. Now we can define the map $\mathbf{N} \to \mathbf{Q}$ by the following rule. Start with sending 0 to the only number of height 1 (equal to $0 = \frac{0}{1}$). List all numbers of height 2 (they are $-1 = \frac{-1}{1}$ and $1 = \frac{1}{1}$). Write them in the increasing order ($-1, 1$), send 1 to the smallest number, 2 to the next one. Next list all rational numbers of height 3 in the increasing order : $\frac{-2}{1}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{1}$. Send 3 to the first one, 4 to the next one, and so on. Then go to numbers of height 4 and so on. In this way each rational number becomes the image of a unique natural number under the map which we construct. This proves that our map is bijective.

Proposition 4.
(i) Any subset of a countable set is countable;
(ii) The union of two countable subsets is countable;
(iii) An infinitely countable set is equivalent to the set $\mathbf{N}$.

Proof (i) Let $A \subseteq X$ be a subset of a countable set X. By definition there exists a subset Y of $\mathbf{N}$ and a bijective map $f : X \to Y$. Define the map $\phi : A \to f(A)$ using the rule of f, i.e., $\phi(a) = f(a)$ for any $a \in A$. Then $\phi(A) = f(A)$ and so ϕ is surjective. Since f was injective, ϕ is obviously also injective. Thus ϕ is a bijective map from A to the subset $f(A)$ of $\mathbf{N}$. By definition of a countable set, A is countable.

(ii) Since $X \cup Y = X \cup (Y \setminus (X \cap Y))$ and, by (i), $Y \setminus (X \cap Y)$ is countable, we may assume that $X \cap Y = \emptyset$. Let $f_1 : X \to A \subseteq \mathbf{N}$ and $f_2 : Y \to B \subseteq \mathbf{N}$ be two bijective maps. Then we define the map $f : X \cup Y \to \mathbf{Z} = \mathbf{N} \cup (\mathbf{Z} \setminus \mathbf{N})$ by the following rule $f(a) = f_1(a)$ if $a \in X$, $f(a) = -f_2(a) - 1$ if $a \in Y$. This map is an injective map from $X \cup Y$ to $\mathbf{Z}$. It is glued from two injective maps, one from X to $\mathbf{N}$, another one from Y to $\mathbf{Z} \setminus \mathbf{N}$. Thus $X \cup Y$ is equivalent to a subset of $\mathbf{Z}$ (the image of the map f). Since we have seen that $\mathbf{Z}$ is countable, by (i), $X \cup Y$ is countable too.

(iii) Let $f : X \to A$ be bijective map from X to a subset A of $\mathbf{N}$. If we prove that $A \sim \mathbf{N}$, by Proposition 3, we obtain that $X \sim \mathbf{N}$. So we may assume that $X \subseteq \mathbf{N}$. Let n_1 be the smallest n such that $n_1 \in Y$, and let n_2 be the smallest number such that $n_2 \in Y \setminus \{n_1\}$. Continuing in this way we find a map $g : \mathbf{N} \to Y$ which sends k to n_k such that $n_k \in Y \setminus \{n_1, \ldots, n_{k-1}\}$. This is obviously a bijective map.

Theorem 2(Cantor). *Let X be a set and $\mathcal{P}(X)$ be its power set. Then X is not equivalent to $\mathcal{P}(X)$.*

Proof. The assertion is obvious for the empty set (verify it!). Assume that $X \neq \emptyset$ and $f : X \to \mathcal{P}(X)$ is a bijective map. Let

$$S = \{x \in X \mid x \notin f(x)\}$$

be the set of elements in X which are not contained in the subset $f(x)$ of X. Since S is a subset of X, it is an element of $\mathcal{P}(X)$ and hence there exists an element $s \in X$ with $f(s) = S$. There are two possibilities: either $s \in S$ or $s \notin S$. Assume the first case occurs, i.e., $s \in S$. By definition of S, $s \notin S$ which is absurd. Assume the second case occurs, i.e., $s \notin S$. Then by definition of S, s must belong to S. Again this is absurd. This proves that assumption $X \sim \mathcal{P}(X)$ leads to a contradiction, hence X is not equivalent to $\mathcal{P}(X)$.

Remark. Compare the proof with the Russel Paradox from section 1.1.

Corollary. *The set of real numbers is not countable.*

Proof. By Proposition 4, it suffices to show that $\mathbf{R}$ contains a subset which is not countable. We shall use the following property of real numbers which we shall prove later (when we properly define the notion of a real number).

Let

$$X_0 \supset X_1 \supset \ldots \supset X_n \supset \ldots$$

be an infinite set of segments in $\mathbf{R}$, one is strictly contained in the next one. Then there exists a unique real number contained in all of these segments.

Assume this. Let $\mathcal{P}(\mathbf{N})$ be the power set of the set of natural numbers, let $\mathcal{P}(\mathbf{N})_{inf}$ be its subset which consists of infinite subsets of $\mathbf{N}$, and $\mathcal{P}(\mathbf{N})_{fin}$ be the subset of $\mathcal{P}(\mathbf{N})$ which consist of finite subsets of $\mathbf{N}$. Let us show first that the second set is countable. To any finite subset $A \subseteq \mathbf{N}$ we assign the rational number

$$f(A) = \chi_A(0) + \frac{\chi_A(1)}{2} + \ldots + \frac{\chi_A(n)}{2^n}$$

where n is the largest number from A. Note that this number is rational and is less or equal than the number $1 + \frac{1}{2} + \ldots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$ (we used the formula for the sum of a geometric progression). Also the map $f : \mathcal{P}(\mathbf{N})_{fin} \to \mathbf{Q}$ defined by the above formula is injective. In fact, $0 \in A \iff \chi_A(0) = 1 \iff f(A) > 1$, $1 \in A \iff \chi_A(1) = 1 \iff 2f(A) - 2\chi_A(0) > 1$ and so on. This shows that A can be reconstructed from $f(A)$. Thus we see that f defines a bijective map from $\mathcal{P}(\mathbf{N})_{fin}$ to a subset of $\mathbf{Q}$, and hence the domain of this map must be a countable set. Since the whole set $\mathcal{P}(\mathbf{N})$ is not countable, by Proposition 4 we obtain that $\mathcal{P}(\mathbf{N})_{inf}$ must be uncountable. Now let us construct an injective map from the set $\mathcal{P}(\mathbf{N})_{inf}$ to the set $\mathbf{R}$. Then we will be done, since we find a subset of $\mathbf{R}$ (the image of our map) which is uncountable.

Let A be an infinite subset of natural numbers. We assign to A a sequence of subsets $X_0 \supset X_1 \supset X_2 \supset \ldots$ of $[0, 1]$ as follows. Consider the segment $[0, 1]$. Divide it in two halves $[0, \frac{1}{2}]$ and $[\frac{1}{2}, 1]$. If $0 \notin A$ we take X_0 to be left half $[0, \frac{1}{2}]$, if $0 \in A$ we take X_0 to be the right part $[\frac{1}{2}, 1]$. Now divide X_0 in two halves again. If $1 \in A$, we take X_1 to be the right half of X_0, if $1 \notin A$ we take X_1 to be the left half. Continue in this way, each time defining the new set X_n as the right half of X_{n-1} if $n \notin A$ and the left half if $n \in A$. One easily checks the following formula for X_n:

$$X_n = [\frac{\chi_A(0)}{2} + \frac{\chi_A(1)}{2^2} + \ldots + \frac{\chi_A(n)}{2^{n+1}}, \frac{\chi_A(0)}{2} + \frac{\chi_A(1)}{2^2} + \ldots + \frac{\chi_A(n)}{2^{n+1}} + \frac{1}{2^{n+1}}].$$

The intersection of the subsets X_n contains a unique real number which we assign to the subset A. In this way we obtain a map from $\mathcal{P}(\mathbf{N})_{inf} \to \mathbf{R}$ (in fact to $[0, 1]$). Clearly this map is injective because X_0 determines $\chi_A(0)$, X_1 determines $\chi_A(1)$ and so on. This proves the assertion.

Remark. The following assertion is called the *Continuum Hypothesis*:

"Every subset of $\mathbf{R}$ is either countable or is equivalent to the whole set $\mathbf{R}$."

In 1900, at the International Congress of Mathematicians in Paris, the great German mathematican David Hilbert proposed 23 the most important unsolved problems for the new century. The first of them was the Continuum Hypothesis. Since the foundation of the set theory many mathematicians tried unsuccessfully to prove it. In 1939 K. Gödel proved that it is impossible to find a counterexample to this Hypothesis (although they may exist). In 1966 Paul Cohen proved that it is impossible to prove this hypothesis. In other words this problem is unsolvable, i.e. it cannot be deduced from the axioms of the set theory.

Exercises 1.3.1

1. Give your own examples of injective, surjective, bijective, injective but not surjective, surjective but not injective maps.

2. Let $f : \mathbf{R} \to \mathbf{R}$ be defined by the rule $f(x) = ax + b$ for some fixed (independent of x) real numbers a, b. When is this map bijective? In the case when it is bijective, find the inverse map.

3. Let $pr_1 : X \times Y \to X$ be the projection map defined in section 1.2. Prove that pr_1 is surjective. When is it injective?

4. (a) Let $f : X \to Y$ be an injective map. Show that there exists a map $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$.
(b) Let $f : X \to Y$ be a surjective map. Show that there exists a map $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.
(c) State the definition of injectivity and surjectivity in terms of the graph of the map.

5*. Let X be a finite set of n elements. Prove that the number of bijective maps from X to X is equal to $n! = 1 \cdot 2 \cdots (n-1) \cdot n$.

6. Prove that $X \times Y \sim Y \times X$.

7. Let X be a countable set. Prove that the subset of $\mathcal{P}(X)$ consisting of finite sets is countable.

8. Let $f : X \to Y$ be a surjective map. Suppose that X is countable. Prove that Y is countable.

9. Prove that the following sets are countably infinite:
(a) The set of even integers.
(b) The set $\mathbf{N} \times \mathbf{N}$.
(c) The set of numbers of the form 2^n where $n \in \mathbf{N}$.

10*. Let A be a set and $f : \mathbf{N} \to \mathcal{P}(A)$ be a map whose values are countable subsets of A. Let $X = \{a \in A \mid \text{there exists } n \in \mathbf{N} \text{ such that } a \in f(n)\}$. Prove that X is a countable set.

11*. A real number a is called *algebraic* if it is a root of an algebraic equation $x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$ with rational coefficients $a_1, \ldots, a_n$. A real number is called *transcendental* if it is not algebraic. Prove that the set of algebraic numbers is countable and the set of transcendental numbers is not countable.

12. Prove that any infinite set contains a countably infinite subset.

13. Prove that any infinite set is equivalent to a proper subset (Hint: use the previous problem and Example 14).

14. Let X be a countable set. Prove that $X \cup \mathbf{R} \sim \mathbf{R}$.

15. Prove that $\mathbf{R} \sim \mathcal{P}(\mathbf{N})$. (Hint:Use the proof of the Corollary to Cantor's theorem and the previous problem).

1.4. Relations in a set. Let (a, b) be a pair of elements of a set X. If it satisfies some special property we think that there a relation between a and b. All pairs satisfying this property form a subset of $X \times X$.

Definition A *relation* in a set X is a subset $R \subseteq X \times X$. If $(a, b) \in R$, we say that a is R-related to b.

Examples. 1. Let X be the set of people, and $R = \{(a, b) \in X \times X \mid$ a and b are siblings$\}$. Recall that two persons are siblings if they have the same natural parents.
2. Same X but $R = \{(a, b) \in X \times X \mid$ a is taller than b $\}$.
3. Let $\mathbf{Z}$ be the set of integers and $R = \{(a, b) \in \mathbf{Z} \times \mathbf{Z} \mid a - b$ is even$\}$.
4. Let A be a set, $X = \mathcal{P}(A)$ be its power set, $R = \{(A, B) \in X \mid A \subseteq B\}$.
5. Let $f : X \to Y$ be a map and $R = \{((a, b) \in X \times X \mid f(a) = f(b)\}$.
6. Let $f : X \to X$ be a map. Then its graph Γ_f is a relation in X.

We shall often use relations satisfying some special properties.

Definition. A relation $R \subseteq X \times X$ is called an *equivalence relation* if it satisfies the following properties:
(reflexivity) $(a, a) \in R$ for any $a \in X$;
(symmetry) $(a, b) \in R \Longleftrightarrow (b, a) \in R$;
(transitivity) $(a, b) \in R, (b, c) \in R \Longrightarrow (a, c) \in R$.

We write $a \sim_R b$ when $(a, b) \in R$ if R is an equivalence relation. We say that a is equivalent to b with respect to R. With this notation we can rewrite the previous properties as follows:
(i) $a \sim_R a$,
(ii) $a \sim_R b \Longleftrightarrow b \sim_R a$,
(iii) $a \sim_R b, b \sim_R c \Longleftarrow a \sim_R c$.

Definition. A relation $R \subseteq X \times X$ is called an *order relation* if it satisfies the properties of transitivity and reflexivity from the previous definition and the following property:
(anti-symmetry) $(a, b) \in R, (b, a) \in R \Longrightarrow a = b$.

We say that a is less or equal to b if a and b are related with respect to an order relation. Often we express it in the form $a \leq_R b$ (or just $a \leq b$ if no confusion arise).

Examples. Examples 1,3 and 5 are equivalence relations. Example 6 is an example of an equivalence relation only if $f = \mathrm{id}_X$ (use the reflexivity property).
Examples 2 and 4 are relations of order.
7. Let $X = \mathcal{P}(\mathcal{U})$ be the power set of the universum (i.e the set of all sets we allowed to consider). Define the equivalence relation by $X \sim_R Y \Longleftrightarrow X \sim Y$, i.e. two sets are equivalent if and only if there is a bijective map from one to another. Proposition 3 of section 1.3 checks the properties of equivalence relation.
8. Let $R = \{(a, b) \in X \times X \mid a = b\}$. This is both an equivalence relation and an order relation. It is called the *trivial relation.*

Let $R \subseteq X \times X$ be an equivalence relation on a set X. For any $x \in X$ let

$$[x]_R = \{x' \in X \mid x' \sim_R x\}$$

be the set of elements from X which are R-equivalent to x.

Definition. A subset C of X is called an *R-equivalence class* if $C = [x]_R$ for some $x \in X$.

Proposition 1. *Let C be an equivalence class. Then*
(i) $C = [x]_R \Longleftrightarrow x \in C$;
(ii) if $C' \neq C$ is another equivalence class, then $C \cap C' = \emptyset$;
(iii) any $x \in X$ belongs to some equivalence class.

Proof. (i) Assume $C = [x]_R$. Since $x \sim_R x$, we get $x \in C$ which proves $\Longrightarrow$. Assume $x \in C$. By definition, $C = [x']_R = \{x'' \in X \mid x'' \sim_R x'\}$ for some $x' \in X$. Since $x \in C, x \sim_R x'$, and, by symmetry, $x' \sim_R x$. Now, by transitivity, $x'' \sim_R x' \Longrightarrow x'' \sim_R x$. This shows that $C = [x]_R$.

(ii) Assume $C \cap C' \neq \emptyset$. Let $x \in C \cap C'$. By (i), $C = [x]_R, C' = [x]_R$, hence $C = C'$.

(iii) By reflexivity, $x \in [x]_R$.

Examples. In example 1, the equivalence classes are the sets of children of the same couple of parents. In example 3, there are two equivalence classes: the set of even integers and the set of odd integers. In example 5, the equivalence classes are non-empty subsets of the form $f^{-1}(\{y\}), y \in Y$.

Definition. A *partition* of a set X is a set of its subsets (called partition subsets) such that any element of X belongs to exactly one of these subsets.

We see that the set of R-equivalence classes in a set X is a partition of X. Conversely, assume we have a partition of X. Define an equivalence relation R on X as follows:

$$x \sim_R x' \Longleftrightarrow x, x' \quad \text{belong to the same partition subset.}$$

This is a equivalence relation. In fact, since x belongs to some partition subset, $x \sim_R x$. Thus the relation R is reflexive. Obviously it is symmetric. Now if x, x' belong to the same partition subset A, and x', x'' belong to the same partition subset B, then $x' \in A \cap B$. Since any element of X belongs to exactly one partition subset, we must have $A = B$. Hence x, x'' belong to the same partition subset and therefore $x \sim_R x''$. This checks the transitivity property. It is clear that the partition classes are the R-equivalence classes.

Theorem 1. *Let $R \subseteq X \times X$ is an equivalence relation on a set X. There exists a surjective map $f : X \to Y$ such that for any $x, x' \in X$,*

$$x \sim_R x' \Longleftrightarrow f(x) = f(x').$$

Proof. We take for Y the set of R-equivalence classes (a subset of $\mathcal{P}(X)$). Define the map $f : X \to Y$ by the formula

$$f(x) = [x]_R.$$

Then all the properties are easily checked. The map f is surjective because each equivalence class C has the form $C = [x]_R = f(x)$ for some $x \in X$. By property (i) of Proposition 2, we have

$$x \sim_R x' \Longleftrightarrow f(x) = [x]_R = [x']_R = f(x').$$

Definition The set Y of equivalence classes we used in the proof of the previous theorem is called the *factor set* of X by the equivalence relation R and is denoted by X/R. The map $p : X \to X/R, x \mapsto [x]_R$, is called the canonical map from X to the factor set.

Remark. There is a similar description of order relations. Let R be an order relation on a set X. We write $x' \leq_R x$ if $(x', x) \in R$ and set $\mathrm{maj}_R(x) = \{x' \in X \mid x' \leq_R x\}$ (the *majorant* of x). A subset C of X of the form $\mathrm{maj}_R(x)$ is called a majorant. We have the analog of Proposition 1:

(i) each $x \in X$ belongs to some majorant (since $x \leq_R x$);
(ii) $\mathrm{maj}_R(x) = \mathrm{maj}_R(x'') \Longleftrightarrow x = x'$;
(iii) two majorant have non-empty intersection if and only if one is contained in another.

Let $Y \subseteq \mathcal{P}(X)$ be the set of majorants. Define the map $f : X \to Y$ by sending x to $\mathrm{maj}_R(x)$. This map is injective, and $x \leq_R x' \Longleftrightarrow f(x) \subseteq f(x')$.

Exercises 1.4.

1. Give your own examples of equivalence relations, relations of order, relations which are neither equivalence relations nor relations of order (two of each).
2. How many equivalence relations exist on a set of 2, 3, 4 elements?
3. How many equivalence relations exist on a set of 2, 3 elements?.
4. Check that the following relations are equivalence relations. Describe the equivalence classes.
   (a) X is the set of points on the xy-plane. Two points are equivalent if they are equidistant from the origin.
   (b) X is the set of integers. Two integers are equivalent if the difference is divisible by 3
   (c) $X = \mathbf{R}$, two real numbers are equivalent if their difference is an integer.
5. Let R be an equivalence relation on a set X and $f : X \to Y$ be any surjective map satisfying $f(x) = f(x') \Longleftrightarrow x \sim_R x'$. Prove that there exists a bijective map $f' : X/R \to Y$ such that $f = f' \circ p$ where $p : X \to X/R$ is the canonical map from the set to the factor set. (Hint: Define $f'([x]_R) = f(x)$ and check that it is well-defined and satisfies the requirements).

6. A set X with an order relation R is called *total order* for each non-empty subset A of X there exists an element $x \in X$ such that $x \leq_R a$ for all $a \in A$. Show that any finite set admits a total order. Is the set $(0,1)$ totally ordered with respect to the usual order $\leq$?
7. Let R be the equivalence relation from Problem 4 (a). Prove that the factor set is equipotent to the set $\mathbf{R}_{\geq 0}$.
8* Let R be the equivalence relation from Problem 4 (c). Prove that the factor set is equipotent to the set of points on the unit circle.

II. REAL NUMBERS

2.1 Natural numbers. The notion of a natural number certainly preceeds everyting in mathematics and is familiar since childhood. As a famous German mathematician Leopold Kronecker said:

"God created the natural numbers, all the rest is the work of man."

In fact the notion of a natural number represents the first example of mathematical abstraction. It attributes to any finite set a certain property (the number of elements) which does not depend on the nature of its elements. From our point of view, this is of course can be expressed with help of the notion of equivalence classes.

We define the natural numbers as follows. For any set X let $\mathrm{Card}(X)$ denote the equivalence class of X with respect to the equivalence relation defined by equipotence of sets. Thus $\mathrm{Card}(X)$ consists of all sets equipotent to X. We write $Card(X) - 1$ to denoe the equivalence class of the set $X \setminus \{a\}$ where a is any element of X. This does not depend on the choice of a. In fact, for any $a, a' \in X$, we can define a bijective map $f : X \setminus \{a\} \to X \setminus \{a'\}$, for example by the formula

$$f(x) = \begin{cases} x & \text{if } x \neq a, a' \\ a & \text{if } x = a'. \end{cases}$$

We define the number 0 as $\mathrm{Card}(\emptyset)$. We define the number 1 as $\mathrm{Card}(\{x\})$. It is clear that all sets consisting of a single element (*singletons*) are equipotent. We define 2 as $\mathrm{Card}(X)$ where X is a set such that for any $a \in X$, $\mathrm{Card}(X \setminus \{a\}) = 1$. It clear that each set from the equivalence class 2 consists of an element a and an element $b \neq a$. Also it is clear that $1 \neq 2$ since it is impossible to find a surjective map from a singleton to a set which is not a singleton. We go like this to introduce the numbers 3,4,5,6,7,8,9. Then the next number will be denoted by 10, then by 11 and so on. So in general, the expression $n = ab \dots c$ where $a, b, \dots c \in \{0, 1, \dots, 9\}$ and $a \neq 0$ is equal to $\mathrm{Card}(X)$ where $\mathrm{Card}(X \setminus \{a\}) = n - 1$ is obtained from n by the usual arithmetic rule of subtracting 1. Note that at each step we check that n is not equal to any of the previously defined numbers by reducing to the previous case.

This defines the set of natural numbers. We denote it, as before, by $\mathbf{N}$. Note that the number 0 is included in this set. Recall that by our definition, a natural number is the equivalence classes of a set such that throwing its elements one by one each time we arrive at the empty set in a finite number of steps. Equivalently they are obtained from the empty set by adding one element each time in finitely many steps. We call such sets *finite sets*. Obviously the empty set is finite and $\mathrm{Card}(\emptyset) = 0$. Take some element from a finite non-empty set X, and denote it by x_1. If $\mathrm{Card}(X) = 1$, we have $X = \{x_1\}$. If $\mathrm{Card}(X) \neq 1$, there is an element in X different from x_1. Denote it by x_2. If $\mathrm{Card}(X) = 2$, we have $X = \{x_1, x_2\}$. Contunuing in this way we will be able to write $X = \{x_1, x_2, \dots, x_n\}$ where $\mathrm{Card}(X) = n$. Thus we see that the notion of a finite set agrees with our earlier intuitive notion of a finite set.

The natural number $n = Card(\mathrm{X})$ is sometimes denoted by $\#X$ (or by $|X|$) and is called the *cardinality* of X or the *number of elements* in X.

Let

$$\mathbf{N}_n = \{1, \dots, n\}$$

be the subset of $\mathbf{N}$ of all natural numbers starting from 1 until n. It is clear that all finite sets X with $\#X = n$ are equivalent to the set $\mathbf{N}_n$.

Proposition 1. *(i) A subset of a finite set is finite.*
(ii) The union of two finite sets is finite.

(iii) The Cartesian product of two finite sets is finite.

Proof. This easily follows from the definition.

Now let us define addition of natural numbers. Let $n = \mathrm{Card}(X)$ and let $m = \mathrm{Card}(X)$. Assume that $X \cap Y = \emptyset$. Define

$$n + m = \mathrm{Card}(X \cup Y).$$

Theorem 1. *(i) (commutativity law for addition) $n + m = m + n$ for any $n, m \in \mathbf{N}$;*
(ii) (associativity law for addition) $(n + m) + k = n + (m + k)$ for any $n, m, k \in \mathbf{N}$;
(iii) (the zero element) $n + 0 = n$ for any $n \in \mathbf{N}$.

Proof. (i) This follows from the equality of sets $X \cup Y = Y \cup X$.
(ii) This follows from the associativity of the union of sets $(X \cup Y) \cup Z = X \cup (Y \cup Z)$.
(iii) This is obvious since $\emptyset \cup X = X$.

Now let us define multiplication of natural numbers. Let $n = \mathrm{Card}(X)$ and let $m = \mathrm{Card}(Y)$. Define

$$n \cdot m = \mathrm{Card}(X \times Y).$$

Theorem 2. *(i) (commutativity law for multiplication) $n \cdot m = m \cdot n$ for any $n, m \in \mathbf{N}$;*
(ii) (associativity law for multiplication) $(n \cdot m) \cdot k = n \cdot (m \cdot k)$ for any $n, m, k \in \mathbf{N}$;
(iii) (the unit element) $n \cdot 1 = n$ for any $n \in \mathbf{N}$;
(iv) (distributivity law) $n \cdot (m + k) = (n \cdot m) + (n \cdot k)$ for any $n, m, k \in \mathbf{N}$.

Proof. (i) This follows from the equipotency $X \times Y \sim Y \times X$ defined by the map $(a, b) \mapsto (b, a)$.
(ii) This follows from the equipotency $(X \times Y) \times Z = X \times (Y \times Z)$. It is defined by the map $((x, y), z) \mapsto (x, (y, z))$.
(iii) This follows from the equipotency $\{x\} \times X \sim X$ defined by the map pr_2.
(iv) This follows from exercise 2 (e) from section 1.1 where we have to set $B = D$.
Observe that there is a natural order relation on the set $\mathbf{N}$. If $n = \#\mathbf{N}_n, m = \#\mathbf{N}_m$ then we write

$$n \leq m \Longleftrightarrow \mathbf{N}_n \subseteq \mathbf{N}_m.$$

The next theorem is called the well-ordering principle:

Theorem 3. *For any non-empty subset X of $\mathbf{N}$ there is an element $a \in X$ such that $a \leq x$ for every $x \in X$. Such element is called the minimal element of X.*

Proof. If $0 \in X$, then 0 is certainly the minimal element of X. If $\{0\} \neq X$, we try 1, then 2 and so on. The first time we arrive at an element of X will be the minimal element.

Corollary (Principle of Mathematical Induction). *Let X be a subset of the set of natural numbers. Suppose X satisfies the following properties:*
(i) $a \in X$ for some n;
(ii) $n \in X \Longrightarrow n + 1 \in X$.

Then $X \supset \mathbf{N} \setminus \{0, 1, \ldots, a - 1\} = \{a \in \mathbf{N} \mid n \geq a\}$.

Proof. Let $A = \{x \in \mathbf{N} \setminus X \mid x \geq a\}$. If the assertion is not true $A \neq \emptyset$. By the well-ordering principle, A contains the minimal element x. Since $x \neq a$, and $x \geq a$, we get $x - 1 \geq a$. Since x is the minimal element of A, $x - 1 \notin A$, hence $x - 1 \in X$. By property (ii), $x = (x - 1) + 1 \in X$. But x was taken from $\mathbf{N} \setminus X$. This contradiction proves the theorem.

Here how the Principle of Mathematical Induction works. Suppose we have an infinitely countable set S whose elements are some statements. Let us list elements of S in the form $S = \{S_1, \ldots, S_n, \ldots\}$. Let X

be the subset of S which consists of true statements. Suppose we prove that the statement S_1 is true, and suppose we can prove that for any $n \geq 1$

$$S_n \quad \text{is true} \Longrightarrow S_{n+1} \quad \text{is true.}$$

Then all statements S_n are true.

Using the Principle of Mathematical Induction let us prove two additional properties of addition and multiplication of natural numbers.

For any finite set of natural numbers $\{n_1, \ldots, n_k\}$ we denote $n_1 + \ldots + n_k$ the sum obtained by first adding two numbers from the set, then adding to the sum the third number from the set, and so on. By commutativity and associativity of addition, the result does not depend on the order of elements in which take the elements of the set. Similarly we define the product $n_1 \cdots n_k$ of k natural numbers.

Proposition 2. *For any $n, m \in \mathbf{N}$,*

$$n \cdot m = \underbrace{m + \ldots + m}_{n}$$

where the underbrace indicates that we add up n numbers equal to m.

Proof. Let us apply the principle of mathematical induction. We fix m and consider the assertions S_n

$$n \cdot m = \underbrace{m + \ldots + m}_{n}.$$

The assertion S_1 says that $1 \cdot m = m$ and is true in virtue of Theorem 2. Now, by disributivity law, we have

$$n \cdot m = ((n-1)+1) \cdot m = (n-1) \cdot m + 1 \cdot m.$$

Suppose the assertion S_{n-1} is true. Then

$$(n-1) \cdot m = \underbrace{m + \ldots + m}_{n-1}.$$

This implies that

$$n \cdot m = (\underbrace{m + \ldots + m}_{n-1}) + m = \underbrace{m + \ldots + m}_{n},$$

that is, S_n is true. So the assumptions of the mathematical induction are fulfilled and all the assertions S_n are true.

Proposition 3 (Cancellation law for addition). *Let $n \in \mathbf{N}$. For any $m, k \in \mathbf{N}$,*

$$n + m = n + k \Longrightarrow m = k.$$

Proof. Denote this implication by S_{n+1} (this is the statement "LHS implies RHS"). The assertion S_1 reads as $m = k \Longrightarrow m = k$ is obviously true. Assume that S_n is true. Let us prove that S_{n+1} is true. Using our assumption and associativity of addition, we obtain

$$(n+1) + m = (n+1) + k \Longrightarrow n + (1 + m) = n + (1 + k) \Longrightarrow 1 + m = 1 + k$$

So we will be done as soon as we prove assertion $S_2 : 1 + m = 1 + k \Longrightarrow m = k$. Let $m = \#X, k = \#Y, 1 = \#\{a\}$ where we take $a \notin X \cup Y$. By definition of addition, $1 + m = \#(X \cup \{a\}) = 1 + k = \#(Y \cup \{a\})$. Thus there exists a bijective map $f : X \cup \{a\} \to Y \cup \{a\}$. The restriction of f to X defines a bijection $f|X : X \to f(X) = (Y \cup \{a\}) \setminus \{f(a)\}$. Thus $f(X)$ is obtained from $Y \cup \{a\}$ by throwing away the element $f(a)$, and Y is obtained from the same set by throwing away the element a. But in the beginning of the

section we proved that this implies that $f(X) \sim Y$. Thus $X \sim Y$, and $m = \#X = \#Y = k$, and we are done.

Remark. One can generalize the notion of natural numbers by defining *cardinal numbers* as the equivalence classes of any sets (not necessary finite) with respect to the equivalence relation defined by equipotency of sets. Then we can introduce the operations of addition and multiplication of cardinal numbers in the same way as we did for natural numbers. There are analogues of Theorems 1-3 which are proved in the same way. For example, we may introduce the numbers

$$\aleph_0 = \mathrm{Card}(\mathbf{N}), \quad \aleph = \mathrm{Card}(\mathbf{R}).$$

Here, as customary, we use the first letter of the Hebrew alphabeth $\aleph$ (aleph). The operations over cardinal numbers have some "funny properties". For example, since the union and the Cartesian product of two infinite countable sets is infinitely countable, we have

$$\aleph_0 + \aleph_0 = \aleph_0, \quad \aleph_0 \cdot \aleph_0 = \aleph_0.$$

We can also introduce the operation of exponentiation of cardinal numbers by setting

$$\mathrm{Card}(Y)^{\mathrm{Card}(X)} = \mathrm{Card}(\mathcal{M}ap(X, Y))$$

where $\mathcal{M}ap(X, Y)$ denotes the set of all maps from X to Y. Since

$$\mathcal{P}(X) \sim \mathcal{M}ap(X, \{0, 1\})$$

(using the map $A \mapsto \chi_A$), we get

$$\mathrm{Card}(\mathcal{P}(X)) = 2^{\mathrm{Card}(X)}.$$

Since we know that $\mathbf{R} \sim \mathcal{P}(\mathbf{N})$ (Exercises 1.3, 14), we obtain

$$\aleph = 2^{\aleph_0}.$$

One can also introduce a relation of order on the set of cardinal numbers. We say that $\mathrm{Card}(X) \leq \mathrm{Card}(Y)$ if there exists an injective map from X to Y (equivalently, there exists a surjective map $Y \to X$). To verify the antisymmetry property we have to prove the following statement (called *Cantor-Bernstein Theorem*):

Let X and Y be two sets. Suppose X is equipotent to a subset of Y and Y is equipotent to a subset of X. Then X is equipotent to Y.

Unfortunately, the proof of this statement is very difficult and requires further development of set theory which is beyound our goals. In these new notations the Continuum Hypothesis from Remark in 1.4 can be stated as follows:

There is no cardinal numbers a such that $\aleph_0 < a < 2^{\aleph_0}$.

The operations of addition and multiplication on the set $\mathbf{N}$ are first examples of *algebraic structures* on a set. Here we deal with a binary operation on a set.

Definition. A *binary operation* on a set X is a map $\mu : X \times X \to X$. A binary operation is called *commutative* if, with notation $\mu((a, b)) = a * b$, it satisfies

$$a * b = b * a \quad \text{for any } a, b \in X.$$

It is called *associative* if it satisfies

$$(a * b) * c = a * (b * c) \quad \text{for any } a, b, c \in X.$$

A *neutral* element of the binary operation is an element $e \in X$ such that

$$e * a = a * e = a \quad \text{for any } a \in X.$$

A set X together with a binary operation is called a *semi-group* if its binary operation is associative. A semi-group is called a *commutative semi-group* if its binary operation is commutative. A semi-group is called a *monoid* if its binary operation admits a neutral element.

There exists only one neutral element e in a monoid. In fact, if e' is another neutral element, then we must have $e * e' = e'$ because e is a neutral element, and we have $e * e' = e$ because e' is a neutral element. Thus $e = e'$.

Using the previous definition we can say that the set $\mathbf{N}$ admits two binary operations $a * b = a + b, a * b = a \cdot b$. With respect to any of these operations $\mathbf{N}$ is a commutative monoid. The distributivity property is an additional bonus.

Exercises 2.1.

2.1.1. Prove the cancellation law for multiplication of natural numbers: $n \cdot m = n \cdot k \Longrightarrow m = k$ for any $n, m, k \in \mathbf{Z}, n \neq 0$.

2.1.2 Define the operation of exponentiation over natural numbers by

$$n^m = \underbrace{n \cdot \cdots n}_{m},$$

that is, we multiply n with itself m times. Put $n^0 = 1$. Prove that n^m is equal to $\#\mathcal{M}ap(X, Y)$, where $\mathcal{M}ap(X, Y)$ denotes the set of maps from X to Y, and $\#X = m, \#Y = n$.

2.1.3 Using mathematical induction, prove

(a) $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$ for each $n \in \mathbf{N}$;

(b) $1^3 + 2^3 + \ldots + n^3 = n^2(n+1)^2/4$ for each $n \in \mathbf{N}$;

(c) $2^{n-1} \leq n!$ for each $n \in \mathbf{N}$.

4. Give your own example of a set with a binary operation which is

(a) neither commutative nor associative;

(b) associative but not commutative;

(c) commutative but not associative;

(d) commutative and associative without neutral element;

(e) commutative, associative and with a neutral element.

2.2. Integers. We create integers to be able to solve the equation

$$n + x = m$$

where n and m are natural numbers.

Let R be the equivalence relation on the set $S = \mathbf{N} \times \mathbf{N}$ of pairs of natural numbers defined as follows:

$$(n, m) \sim_R (n', m') \Longleftrightarrow n + m' = n' + m.$$

It is indeed an equivalence relation. The properties of reflexivity and symmetry are obvious. To prove the property of transitivity we assume that $(n, m) \sim_R (n', m')$, $(n', m') \sim_R (n'', m'')$. Then, by definition of R,

$$n + m' = m + n',\ n' + m'' = n'' + m'.$$

Adding up, we get, using the properties of addition operation over natural numbers:

$$(n + m') + (n' + m'') = (m + n') + (n'' + m').$$

Regrouping the summands we get

$$(n' + m') + (n + m'') = (n' + m') + (m + n'').$$

Using the cancellation law for addition from Proposition 2, we deduce from this that $m + n'' = m'' + n$, i.e., $(n, m) \sim_R (n'', m'')$.

Definition. An integer is an equivalence class $[(n, m)]$ of an ordered pair (n, m) of natural numbers with respect to the equivalence relation $(n, m) \sim (n', m') \Longleftrightarrow n + m' = n' + m$. The set of integers is denoted by $\mathbf{Z}$.

Observe that for each pair of natural numbers (n, m) we have

$$(n, m) \sim \begin{cases} (k, 0) & \text{if } n = m + k \quad \text{for some } k \in \mathbf{N} \\ (0, k) & \text{if } m = n + k \quad \text{for some } k \in \mathbf{N}. \end{cases}$$

So $\mathbf{Z}$ consists of the equivalence classes of the form $[(k, 0)]$ or $[(0, k)]$ where $k \in \mathbf{N}$. Also each element of $\mathbf{Z}$ is equal to a unique class of this form. In fact, by definition of our equivalence relation

$$(k, 0) \sim (k', 0) \Longleftrightarrow k + 0 = k' + 0 \Longleftrightarrow k = k',$$
$$(0, k) \sim (0, k') \Longleftrightarrow 0 + k' = k + 0 \Longleftrightarrow k = k',$$
$$(k, 0) \sim (0, k') \Longleftrightarrow k + k' = 0 + 0 \Longleftrightarrow k = k' = 0.$$

Define the map from $i : \mathbf{N} \to \mathbf{Z}$ by the formula $k \to [(k, 0)]$. This map is injective as the previous remark shows. We shall identify $\mathbf{N}$ with its image $i(\mathbf{N})$ under the map i and denote the integers of the form $[(n, 0)]$ by n. Hopefully no confusion will arise.

Of course, the integers of the form $[(0, k)]$ must be thought as negative natural numbers and will be denoted by $-k$. We call $-k \neq 0$ a *negative integer*. The map $\mathbf{N} \setminus \{0\} \to \mathbf{Z} \setminus i(\mathbf{N})$ defined by the rule $k \to -k = [(0, k)]$ is bijective. So the set $\mathbf{Z}$ is equal to the union of two countable set $i(\mathbf{N})$ and $\mathbf{Z} \setminus i(\mathbf{N})$ and hence is countable.

To justify our notation $-k$ let us define the operation of *addition* of integers by the formula

$$[(k, 0)] + [(k', 0)] = [(k + k', 0)],\ [(0, k)] + [(0, k')] = [(0, k + k')],$$
$$[(k, 0)] + [(0, k')] = [(k, k')] = \begin{cases} (a, 0) & \text{if } k = k' + a \quad \text{for some } a \in \mathbf{N} \\ (0, a) & \text{if } k' = k + a \quad \text{for some } a \in \mathbf{N}. \end{cases}$$

Rewriting this in the notations $[(k, 0)] = k, [(0, k)] = -k$ we have for any $k, k' \in \mathbf{N}$

$$k + k' = [(k + k', 0)] = k + k',\quad -k + -k' = [(0, k + k')] = -(k + k'),$$
$$k + -k' = \begin{cases} a & \text{if } k = k' + a \text{ for some } a \in \mathbf{N} \\ -a & \text{if } k' = k + a \text{ for some } a \in \mathbf{N}. \end{cases}$$

Obviously this agrees with our addition of natural numbers and also with our elementary school arithmetic .

Similarly we define the *multiplication* of integers by the formula

$$k \cdot k' = [(k, 0)] \cdot [(k', 0)] = [(k \cdot k', 0)],\ -k \cdot -k' = [(0, k)] \cdot [(0, k')] = [(k \cdot k', 0)] = k \cdot k',$$
$$-k' \cdot k = k \cdot -k' = -(k \cdot k').$$

Proposition 1. *(i)* $\mathbf{Z}$ *is a commutative monoid with respect to addition with* $0 = [(0,0)]$ *as the neutral element;*
(ii) for any integer a *there exists a unique integer* a' *(called the negative of* a*) such that*

$$a + a' = 0.$$

Proof. (i) Observe that our addition law for equivalence classes coincides with the following law

$$[(n,m)] + [(n',m')] = [(n+n', m+m')] \quad (*)$$

In fact, if $[(n,m)] = [(a,0)]$ and $[(n',m')] = [(a',0)]$ then $n = m + a, n' = m' + a$, hence $n + n' = m + m' + a + a'$ and $[(n+n', m+m')] = [(a+a', 0)]$. Similarly we check the case when $[(n,m)] = [(0,a)]$ and $[(n',m')] = [(0,a')]$. If $[(n,m)] = [(a,0)]$ and $[(n',m')] = [(0,a')]$ then $n = m + a, m' = n' + a'$, hence $n + n' = m + n' + a, m + m' = m + n' + a'$. This implies $[(n+n', m+m')] = [(a,a')]$ and agrees with our definition of $a + -a'$. Now the formula $(*)$ checks commutativity and associativity since $\mathbf{N}$ is a commutative monoid with respect to addition. By $(*)$,

$$[(0,0)] + [(n,m)] = [(n,m)] + [(0,0)] = [(n,m)]$$

so $0 = [(0,0)]$ is the neutral element with respect to addition.
(ii) If $a = [(n,m)]$, take a' equal to $[(m,n)]$. Then we get

$$a + a' = [(n,m)] + [(m,n)] = [(n+m, n+m)] = [(0,0)].$$

If a'' is another integer satisfying $a + a'' = 0$, then we have $(a + a'') + a' = 0 + a' = a'$. By commutativity and associativity of addition, $(a + a'') + a' = (a + a') + a'' = 0 + a'' = a''$. Hence $a' = a''$. This proves the uniqueness of a'.

We shall denote the negative a' of a by $-a$. Notice that there is no confusion with the notation for negative integers since $a + -a = 0$ if $a \in \mathbf{N}$. We can define the operation of *subtraction* of integers by setting for any $a, b \in \mathbf{Z}$

$$a - b = a + -b.$$

Corollary. *For any integers* a, b *the equation* $a + x = b$ *has the unique solution in* $\mathbf{Z}$ *given by* $x = b - a$.

Proof.

$$a + x = b \Longrightarrow -a + (a + x) = -a + b = b + -a = b - a \Longrightarrow (-a + a) + x = b - a \Longrightarrow x = 0 + x = b - a.$$

Lemma. *For any* $a, b \in \mathbf{Z}$
(i) $a \cdot b = (-a) \cdot (-b) = -(a \cdot -b) = -(-a \cdot b)$;
(ii) $-(a + b) = -a + -b$;
(iii)

$$a \cdot b = \begin{cases} \underbrace{b + \ldots + b}_{a \text{ times}} & \text{if } a \in \mathbf{N} \\ \underbrace{-b + \ldots - b}_{-a \text{ times}} & \text{if } a \notin \mathbf{N}. \end{cases}$$

(iv) $-1 \cdot a = -a$.

Proof. (i) If $a, b \in \mathbf{N}$ this follows from Proposition 2 of the previous section. If $-a, -b \in \mathbf{N}$, we have $a = -(-a)$ since $a + -a = 0$ and again the equalities follow from the definition of multiplication of integers. If $a \in \mathbf{N}, b \notin \mathbf{N}$, we write $b = -(-b)$, and obtain

$$a \cdot b = a \cdot -(-b) = -(a \cdot -b) = -(-(-a \cdot -b) = -a \cdot -b.$$

We leave to the reader to verify the other identities.

(ii) By associativity and commutativity of addition,

$$(a+b)+(-a+-b)=(a+-a)+(b+-b)=0+0=0.$$

By the uniqueness of the negative, we obtain $-(a+b)=-a+-b$.

(iii) If $a,b\in\mathbf{N}$ this follows from Proposition 3 of the previous section. If $a\in\mathbf{N}$ but $b\notin\mathbf{N}$, we have

$$a\cdot b=-(a\cdot -b)=-\underbrace{-b+\ldots+-b}_{a\text{ times}}=-[(\underbrace{-b+\ldots+-b}_{a\text{ times}},0)]=$$

$$=[(0,\underbrace{-b+\ldots+-b}_{a\text{ times}})]=\underbrace{[(0,-b)]+\ldots[(0,-b)]}_{a\text{ times}}=\underbrace{b+\ldots+b}_{a\text{ times}}.$$

Now if $a\notin\mathbf{N}$ then $a=-(-a)$ where $-a\in\mathbf{N}$ and by property (i)

$$a\cdot b=(-a)\cdot(-b)=\underbrace{-b+\ldots+-b}_{-a\text{ times}}.$$

(iv) Follows from (*iii*) by taking $a=-1$.

Proposition 2. *(i)* $\mathbf{Z}$ *is a commutative monoid with respect to multiplication with* $1=[(1,0)]$ *as the neutral element.*

(ii) two binary operations $+$ *and* $\cdot$ *satisfy the distributivity law*

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c),\ (b+c)\cdot a=(b\cdot a)+(c\cdot a).$$

Proof (i) The commutativity of multiplication is clear. To check the associativity we observe that by associativity of multiplication of natural numbers $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ if all $a,b,c\in\mathbf{N}$. If one of a,b,c is negative, replacing it by $-a$ and using the previous Lemma we replace each side by its negative. Replacing all negative integers we reduce the verification to the case when a,b,c are natural numbers. Now $1\cdot a=a$ if $a\in\mathbf{N}$. If $-a\in\mathbf{N}$ then

$$1\cdot a=-(1\cdot -a)=-(-a)=a.$$

Thus 1 is the neutral element with respect to multiplication.

(ii) Assume $a\in\mathbf{N}$. By the Lemma and Proposition 1, we have

$$a\cdot(b+c)=\underbrace{(b+c)+\ldots+(b+c)}_{a\text{ times}}=\underbrace{b+\ldots+b}_{a\text{ times}}+\underbrace{c+\ldots+c}_{a\text{ times}}=a\cdot b+a\cdot c.$$

If $-a\in\mathbf{N}$ we have, using the Lemma,

$$a\cdot(b+c)=-(-a\cdot(b+c))=-(-a\cdot b+-a\cdot c)=-(-a\cdot b)+-(-a\cdot c)=a\cdot b+a\cdot c.$$

Definition. A *ring* is a set R with two binary operations $\mu:R\times R\to R$ and $\nu:R\times R\to R$ satisfying the following properties. Let us put for each $(a,b)\in R\times R$,

$$\mu((a,b))=a+b,\quad \nu((a,b))=a\cdot b.$$

and call the first operation addition and the second operation multiplication. Then

(i) R is a commutative monoid with respect to addition;

(ii) For each $a\in R$ there exists an element $a'\in R$ such that

$$a+a'=a'+a=0$$

where 0 denotes the neutral element with respect to addition.

(iii) R is a monoid with respect to multiplication.

(iv) operations of addition and multiplication satisfy the distributivity laws

$$a\cdot(b+c)=a\cdot b+a\cdot c,\ (b+c)\cdot a=b\cdot a+c\cdot a\quad\text{ for all } a,b,c\in R.$$

A ring is called *commutative* if the multiplication operation satisfies the commutativity law. The element a' in (ii) is unique for each a and is denoted by $-a$.

Theorem 1. *The set of integers* $\mathbf{Z}$ *is a commutative ring with respect to the operations of addition and multiplication defined in this section.*

Proof. Follows from Proposition 1 and 2.

Examples. 1. Let $R = \mathbf{Z} \times \mathbf{Z}$. Define addition and multiplication by the rule

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b) \cdot (a', b') = (aa', bb').$$

Then R becomes a commutative ring. Its neutral element with respect to addition is $(0, 0)$, and with respect multiplication is $(1, 1)$. For any $(a, b) \in R$, the negative $-(a, b)$ is equal to $(-a, -b)$.
2. Let X be a set and $R = \mathcal{P}(X)$ be its Boolean. Define the operation of addition by setting $A + B = A \cup B$ and operation of multiplication by setting $A \cdot B = A \cap B$. Then R becomes a commutative ring. The subset $A = \emptyset$ plays the role of 0 (the neutral element with respect to addition). However, R is not a ring since thee is no negative $-A$ neither with respect to the first operation no with respect to second.

Finally we define the relation of order in $\mathbf{Z}$ by setting

$$a \leq b \Longleftrightarrow b - a \in \mathbf{N}.$$

Obviously this relation is reflexive and anti-symmetric. It is also transitive since

$$b - a \in \mathbf{N}, c - b \in \mathbf{N} \Longrightarrow (b - a) + (c - b) = (c - a) + (b - b) = c - a \in \mathbf{N}.$$

We write $a \geq b$ if $b \leq a$. We use $<$ (resp.$>$) to express that $a \leq b$ (resp. $a \geq b$) but $a \neq b$.

Obviously, $a \geq 0$ if $a \in \mathbf{N}$ so we can call natural numbers *non-negative integers*. The remaining integers satisfy $a < 0$ and can be called *strictly negative integers*. Observe also that our order agrees with the order in $\mathbf{N}$ since

$$n \leq m \Longleftrightarrow i(n) \leq i(m).$$

Exercises 2.2
2.2.1. Prove that the operation of multiplication of integers can be defined by the rule

$$[(n, m)] \cdot [(n', m')] = [(n \cdot n' + m \cdot m', n \cdot m' + m \cdot n')].$$

2.2.2. Prove the cancellation laws for integers:

$$a + b = a + c \Longrightarrow b = c \quad \text{for any } a, b, c \in \mathbf{Z};$$

$$a \cdot b = a \cdot c \Longrightarrow b = c \quad \text{for any } a, b, c \in \mathbf{Z}, a \neq 0.$$

2.2.3. Let R be any ring and 0 be its neutral element with respect to addition. Prove that for any $a \in R$, $0 \cdot a = 0$.
2.2.4. Let X be any set and let R be a ring with addition operation $a + b$ and multiplication operation $a \cdot b$ (for example $R = \mathbf{Z}$). Let M be the set of maps from X to R. Define addition $\phi + \psi$ of functions by setting

$$\phi + \psi(x) = \phi(x) + \psi(x) \quad \text{for any } x \in X \ (+ \text{ in RHS is the addition in } R).$$

Define multiplication $\phi \cdot \psi$ of functions by setting

$$\phi \cdot \psi(x) = \phi(x) \cdot \psi(x) \quad \text{for any } x \in X \ (\cdot \text{ in RHS is the multiplication in } R).$$

Prove that M is a ring with respect to the defined operations of addition and multiplication.
2.2.5. Give your own example of a commutative ring.

2.3. Rational numbers.

We create rational numbers to be able to solve the equation

$$a \cdot x = b$$

where $a, b \in \mathbf{Z}, a \neq 0$.

Let $X = \mathbf{Z} \times \mathbf{Z} \setminus \{0\}$. Define equivalence relation in X as follows:

$$(p, q) \sim (p', q') \Longleftrightarrow pq' - p'q = 0.$$

Obviously this relation is reflexive and symmetric. Let us check the property of transitivity. We shall often use the following property of multiplication of integers

$$a \neq 0, b \neq 0 \Longrightarrow a \cdot b \neq 0.$$

This immediately follows from the definition of our multiplication. It does not follow from the definition of a ring and it is not true for arbitrary rings as we shall see later.

Since $(p, q) \sim (p', q'), (p', q') \sim (p'', q'')$ we have $p \cdot q' = p' \cdot q, p' \cdot q'' = q' \cdot p''$. This implies $(p \cdot q')(p' \cdot q'') = (p' \cdot q) \cdot (q' \cdot p'')$, hence $(p' \cdot q') \cdot (p \cdot q'') = (p' \cdot q') \cdot (q \cdot p'')$. If $p' = 0$ then from $p \cdot q' = p' \cdot q, p' \cdot q'' = q' \cdot p''$ we obtain $p = p'' = 0$ (since $q' \neq 0$). Thus $p \cdot q'' = p'' \cdot q'' = 0$ and $(p, q) \sim (p'', q'')$. If $p' \neq 0$ then $p' \cdot q' \neq 0$ and we can apply the cancellation law for integers (Exercise 2.2.2) to deduce that $p \cdot q'' = p'' \cdot q$, i.e., $(p, q) \sim (p'', q'')$. This checks the property of transitivity.

Definition. A rational number is an equivalence class $[(p, q)] \subset \mathbf{Z} \times \mathbf{Z} \setminus \{0\}$ with respect to the equivalence relation $(p, q) \sim (p', q') \Longleftrightarrow p \cdot q' - p' \cdot q = 0$. The set of rational numbers is denoted by $\mathbf{Q}$.

Let us denote the equivalence class $[(p, q)]$ by $\frac{p}{q}$ (or p/q). By definition

$$\frac{p}{q} = \frac{p'}{q'} \Longleftrightarrow q' \cdot p - q \cdot p' = 0.$$

This reminds us our notion of a rational number from school algebra.

Now let us define the operations of additions and multiplication of rational numbers.

Definition. For any rational numbers p/q and p'/q' we define their *sum* by the formula:

$$\frac{p}{q} + \frac{p'}{q'} = \frac{p \cdot q' + p' \cdot q}{q \cdot q'}.$$

and we define their *product* by the formula:

$$\frac{p}{q} \cdot \frac{p'}{q'} = \frac{p \cdot p'}{q \cdot q'}.$$

Observe that this definition is legal (i.e defines two binary operations). The problem could be that the RHS depends on the way we write the rational number in the form p/q (i.e., choose a representative of the equivalence class). Let us check this. If $p/q = a/b, p'/q' = a'/b'$ then $p \cdot b = q \cdot a, p' \cdot b' = a' \cdot q'$ and

$$(p \cdot q' + p' \cdot q) \cdot b \cdot b' = p \cdot b \cdot q' \cdot b' + p' \cdot b' \cdot q \cdot b = q \cdot a \cdot q' \cdot b' + a' \cdot q' \cdot q \cdot b = q \cdot q' \cdot (a \cdot b' + a' \cdot b)$$

showing that

$$\frac{p}{q} + \frac{p'}{q'} = \frac{p \cdot q' + p' \cdot q}{q \cdot q'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} = \frac{a}{b} + \frac{a'}{b'}.$$

Similarly we have $p \cdot p' \cdot b \cdot b' = q \cdot a \cdot a' \cdot q'$ implying that

$$\frac{p}{q} \cdot \frac{p'}{q'} = \frac{p \cdot p'}{q \cdot q'} = \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'}.$$

For any integer n consider the rational number $[(n,1)] = \frac{n}{1}$. The map $i : \mathbf{Z} \to \mathbf{Q}$ defined by the formula $i(n) = \frac{n}{1}$ is injective since $[(n,1)] = [(m,1)] \Longrightarrow m \cdot 1 = m \cdot 1 \Longrightarrow m = n$. If no confusion arises we denote the rational numbers of the form $n/1$ by n and identify them with integers. In this way we shall consider the set of integers $\mathbf{Z}$ as a subset of $\mathbf{Q}$. Also we see that the operations of addition and multiplication agrees with the previously defined operations of additions and multiplication of integers. In fact

$$i(n) + i(m) = \frac{n}{1} + \frac{m}{1} = \frac{1 \cdot n + m \cdot 1}{1 \cdot 1} = \frac{n+m}{1} = i(n+m),$$

$$i(n) \cdot i(m) = \frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1 \cdot 1} = \frac{n \cdot m}{1} = i(nm).$$

Proposition 1. *(i) The set of rational numbers* $\mathbf{Q}$ *is commutative ring with respect to the operation of addition and multiplication. Its neutral element with respect to addition is* $0 = 0/1$ *and its neutral element with respect to multiplication is* $1 = 1/1$.

(ii) For any $x \in \mathbf{Q} \setminus \{0\}$, *there exists a unique element* x^{-1} *(this is just the notation for this element) such that*

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

Proof. (i) The commutativity of addition follows imeddiately from the definition. Let us verify the associativity. We have

$$(\frac{p}{q} + \frac{p'}{q'}) + \frac{p''}{q''} = \frac{p \cdot q' + p' \cdot q}{q \cdot q'} + \frac{p''}{q''} = \frac{(p \cdot q' + p' \cdot q) \cdot q'' + p'' \cdot q \cdot q'}{q \cdot q' \cdot q''} = \frac{p \cdot q' \cdot q'' + p' \cdot q \cdot q'' + p'' \cdot q \cdot q'}{q \cdot q' \cdot q''},$$

$$\frac{p}{q} + (\frac{p'}{q'} + \frac{p''}{q''}) = \frac{p}{q} + \frac{p' \cdot q'' + p'' \cdot q'}{q' \cdot q''} = \frac{(p \cdot q' \cdot q'' + q \cdot (p' \cdot q'' + p'' \cdot q')}{q \cdot q' \cdot q''} = \frac{p \cdot q' \cdot q'' + p' \cdot q \cdot q'' + p'' \cdot q \cdot q'}{q \cdot q' \cdot q''}.$$

So both results of multiplication are equal. The rest of assertions are easy to verify and are left to the reader.

(ii) Let $x = p/q$. Since $x \neq 0, p \neq 0$. We take $x^{-1} = q/p$. Obviously $(p/q) \cdot (q/p) = 1/1 = 1$. Let us check the uniqueness of x^{-1}. Suppose $y \cdot x = x \cdot y = 1$. Then, multiplying the both sides by x^{-1} we get, by associativity and commutativity of multiplication,

$$x^{-1}(\cdot y \cdot x) = (x^{-1} \cdot x) \cdot y = 1 \cdot y = y = x^{-1} \cdot 1 = x^{-1}.$$

This checks the assertion.

Corollary 1. *For any integers* a, b *with* $a \neq 0$ *the equation*

$$a \cdot x = b$$

has a unique solution in $\mathbf{Q}$.

Proof. Take $x = a^{-1} \cdot b$. We have

$$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b.$$

This checks that $a^{-1} \cdot b$ is a solution. It is also unique since

$$a \cdot x = b \Longrightarrow a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b \Longrightarrow (a^{-1} \cdot a) \cdot x = a^{-1} \cdot b \Longrightarrow 1 \cdot x = a^{-1} \cdot b \Longrightarrow x = a^{-1} \cdot b.$$

Definition. A *field* is a commutative ring F with the additional property that for any $x \neq 0$ (0 is the neutral element with respect to addition) there exist an element y (denoted usually by x^{-1}) such that $x \cdot y = 1$ (1 is the neutral element with respect to multiplication).

Corollary 2. *The set* $\mathbf{Q}$ *is a field with respect to the operations of addition and multiplication.*

Example. Let $F = \{0, 1\}$. Define addition by the rule

$$0 + 0 = 0 + 1 = 1 + 0 = 1, 1 + 1 = 0.$$

Define the multiplication by the rule

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, 1 \cdot 1 = 1.$$

We leave to the reader to verify that F is a field with respect to these binary operations.

For any rational number x and an integer a we define

$$x^a = \begin{cases} \underbrace{x \cdots x}_{a \text{ times}} & \text{for } a \geq 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{-a \text{ times}} & \text{for } a < 0. \end{cases}$$

Finally we define the relation of order in $\mathbf{Q}$ as follows. First we say that a rational number p/q is *non-negative* if $pq \geq 0$. We write $p/q \geq 0$ to express that p/q is non-negative. Note that this definition does not depend on the way we write the number as a fraction. Indeed if $p/q = p'/q'$, then $pq' = p' \cdot q$ hence

$$p' \cdot q' \cdot q^2 = (p' \cdot q) \cdot (q' \cdot q) = (p \cdot q') \cdot q \cdot q' = p \cdot q \cdot q'^2 \geq 0$$

Since $q^2 \geq 0$, this implies that $p' \cdot q' \geq 0$. Here we use the trivial observation which follows from the rule of multiplication of integers:

$$a \geq 0, b \geq 0 \Longrightarrow a \cdot b \geq 0,\ a \geq 0, a \cdot b \geq 0 \Longrightarrow b \geq 0.$$

Now we set

$$\frac{p}{q} \leq \frac{p'}{q'} \Longleftrightarrow \frac{p'}{q'} - \frac{p}{q} \geq 0.$$

We leave to the reader to define the meaning of $\geq, <, >$ for rational numbers. We set

$$\mathbf{Q}_{\geq 0} = \{x \in Q \mid x \geq 0\}.$$

Elements from this set are called *non-negative rational numbers*. Non-negative numbers not equal to 0 are called *positive rational numbers*. Numbers from the set $\mathbf{Q} \setminus \mathbf{Q}_{\geq o}$ are called *negative rational numbers*.

Proposition 2. *For any* $x, y \in \mathbf{Q}$

(i) $x \geq 0, y \geq 0 \Longrightarrow x + y \geq 0$.
(ii) $x \geq 0, y \geq 0 \Longrightarrow x \cdot y \geq 0$.
(iii) (Archimedian Property) If $x, y \geq 0$ *there exists a non-negative integer* n *such that* $n \cdot x \geq y$.
(iv) If $x \geq y, x' \geq y', y, y' \geq 0$, *then* $x \cdot x' \geq y \cdot y'$.
(v) If $x, y > 0$ *then* $x \geq y \Longrightarrow x^{-1} \leq y^{-1}$.
(vi) If $x \geq y$ *and* $x' \geq y'$ *then* $x + x' \geq y + y'$.

Proof. (i) Let $x = p/q, y = p'/q'$, then $p \cdot q \geq 0, p' \cdot q' \geq 0, x + y = \frac{p \cdot q' + p' \cdot q}{q \cdot q'}$, and

$$(p \cdot q' + p' \cdot q) \cdot (q \cdot q') = p \cdot q' \cdot q \cdot q' + p' \cdot q \cdot q \cdot q' = (p \cdot q) \cdot (q'^2) + (p' \cdot q') \cdot (q^2) \geq 0.$$

(ii) Left to the reader.

(iii) Let $x = p/q, y = p'/q'$. We may assume that p, q, p', q' are all non-negative. Choose n such that $n \cdot p \cdot q' > q \cdot p'$. For example one may take $n = 2q \cdot p'$. Then $n \cdot \frac{p}{q} - \frac{p'}{q'} = \frac{n \cdot p \cdot q' - q \cdot p'}{q \cdot q'}$ is obviously positive. Thus $n \cdot \frac{p}{q} > \frac{p'}{q'}$.

(iv) We have $x - y \geq o, x' - y' \geq 0$, and, by (ii), $(x - y) \cdot (x' - y') \geq 0$. Thus

$x \cdot x' - y \cdot y' = (x \cdot x' + y \cdot y' - x \cdot y' - y \cdot x') + (x \cdot y' - y \cdot y') + (y \cdot x' - y \cdot y') = (x - y) \cdot (x' - y') + y \cdot (x - y) + y' \cdot (x - y) \geq 0.$

This shows that $x \cdot x' \geq y \cdot y'$.

(v) We have

$$x \cdot y \cdot (x^{-1} - y^{-1}) = (x \cdot y) \cdot x^{-1} - (x \cdot y) \cdot y^{-1} = y - x \leq 0.$$

It follows from the definition of order in $\mathbf{Q}$ that $x > 0 \Longleftrightarrow x^{-1} > 0$. Multiplying the both sides by $(x \cdot y)^{-1} > 0$ we get, by (ii), $x^{-1} - y^{-1} \leq 0$.

(vi) Left to the reader.

Exercises 2.3

2.3.1 Let R be a subset of $\mathbf{Q}$. Assume that R is a field with respect to the operations of addition and multiplication in $\mathbf{Q}$. Show that $R = \mathbf{Q}$.

2.3.2 Give an example of a proper subset R of $\mathbf{Q}$ different from the set $\mathbf{Z}$ such that R is a ring with respect to the operations of addition and multiplication of rational numbers.

2.3.3 Let $F = \{0, 1, 2\}$. Define operations of additions and multiplications in F such that F becomes a field.

2.3.4 Let $F = \{0, 1\}$ be the field if two elements defined in this section. Show that there is no non-constant maps from $f : F \to \mathbf{Q}$ such that $f(a + b) = f(a) + f(b)$ for any $a, b \in F$.

2.3.5. Let F be a field and $x, y \in F$. Prove that

(i) the inverse element x^{-1} is determined uniquely by x;

(ii) for any $x \in F$, $(x^{-1})^{-1} = x$

(iii) for any $x, y \in F$, $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$.

2.3.6 Show that there is only one non-constant map $f : \mathbf{Z} \to \mathbf{Q}$ satisfying $f(a + b) = f(a) + f(b), f(a \cdot b) = f(a) \cdot f(b)$ for any $a, b \in \mathbf{Z}$.

2.3.7*. Let $F = \{0, 1, 2, 3, 4, 5\}$. Prove that it is impossible to define operations of addition and multiplication in F such that F becomes a field.

2.4. Real numbers. Finally we shall define real numbers. This set will be an object of our study for a long time.

From now on, to simplify the notation we drop $\cdot$ from the notation of product of rational numbers (if no confusion arises). We shall also write sometimes $1/a$ instead of a^{-1} and a/b instead of $a \cdot b^{-1}$. Obviously,

$$1/(a/b) = (a/b)^{-1} = b/a.$$

Definition. Let X be a set. A *sequence in* X is a map $f : \mathbf{N} \to X$.

Let $f : \mathbf{N} \to X$ be a sequence. We denote its values $f(n)$ by x_n. We write f as $(x_0, x_1, \ldots, x_n, \ldots)$. or as $\{x_n\}$. The image of f is the set $\{x_0, x_1, \ldots, x_n, \ldots\}$ where we have to delete from this list all repetetions of the values x_n.

We define operations of addition and multiplication of sequences following the rules from Exercise 2.2.4:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}, \quad \{a_n\} \cdot \{b_n\} = \{a_n b_n\}.$$

With respect to these rule the set $Seq(\mathbf{Q})$ of sequences of rational numbers becomes a commutative ring. Its zero is the sequence $\{0\} = (0, 0, \ldots)$. Its 1 is the sequence $\{1\} = (1, 1, 1, \ldots)$.

For any rational number a we set

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a \leq 0. \end{cases}$$

The number $|a|$ is called the *absolute value* of a.

Lemma 1. *Let $a, b \in \mathbf{Q}$. Then*

(i) $|a| = |-a|$;

(ii) $|ab| = |a||b|$;

(iii) (Triangle inequality) $|a + b| \leq |a| + |b|$;

(iv) $|a| - |b| \leq |a - b| \leq |a| + |b|$;

Proof. (i) Follows from the definition of absolute value.

(ii) Assume that $ab \geq 0$. Then either $a, b \geq 0$, or $a, b \leq 0$. In both cases the assertion is easily checked. If $ab \leq 0$, then either $a \geq 0, b \leq 0$, or $a \geq 0, b \leq 0$. Then $|ab| = -ab, |a||b| = (-a)b = a(-b) = -ab$.

(iii) The assertion is obvious since we can drop the absolute value notation in the both sides. If $a \geq 0, b \leq 0$, and $a + b \geq 0$, then $(a + b) - (a - b) = 2b \leq 0$. Therefore $0 \leq a + b \leq a - b$, and

$$|a + b| = a + b \leq a - b = |a - b| = |a + -b| \leq |a| + |-b| = |a| + |b|.$$

If $a \geq 0, b \leq 0$, and $a+b \leq 0$, then $-b \geq 0, -a \leq 0, -a+-b = -(a+b) \geq 0$. Therefore, the numbers $-b, -a$ satisfy the previous assumption and we get

$$|a+b| = |-(a+b)| = |-a+-b| \leq |-a|+|-b| = |a|+|b|.$$

Changing the roles of a and b, we deal with the case $a < 0, b \geq 0$. If $a < 0, b < 0$, then

$$|a+b| = |-(a+b)| = |-a+-b| \leq |-a|+|-b| = |a|+|b|.$$

(iv) By (iii), $|a-b| = |a+-b| \leq |a|+|-b| = |a|+|b|$. Also, by (iii), we get $|a| = |a-b+b| \leq |a-b|+|b|$ which implies $|a-b| \geq |a|-|b|$.

Definition. A sequence $(a_0, a_1, \ldots, a_n, \ldots)$ in $\mathbf{Q}$ is called a *Cauchy sequence* (or *fundamental sequence*) if given any rational number ϵ there is a natural number N (dependent on ϵ) such that

$$n, m \geq N \Longrightarrow |a_n - a_m| < \epsilon.$$

Examples. 1. Any constant sequence $(a, a, a, \ldots)$, i.e., the constant map $c_a : \mathbf{N} \to \mathbf{Q}$, is obviously a Cauchy sequence.
2. The sequence $\{\frac{1}{n}\} = (1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots)$ is a Cauchy sequence. In fact for any $\epsilon > 0$ choose a natural number N such that $N > 2/\epsilon$ (using the Archimedian Property of $\mathbf{Q}$). Then

$$n, m \geq N \Longrightarrow n > 2/\epsilon, \quad m > 2/\epsilon \Longrightarrow 1/n < \epsilon/2, \quad 1/m < \epsilon/2.$$

By the Triangle Inequality we get

$$|1/n - 1/m| \leq |1/n| + |1/m| \leq |\epsilon/2| + |\epsilon/2| = \epsilon/2 + \epsilon/2 = \epsilon.$$

Note that the choice of N depends on ϵ. Taking smaller ϵ we are forced to choose larger N.
3. The sequence $\{n\} = (0, 1, 2, 3, \ldots)$ is not a Cauchy sequence. In fact if we take $\epsilon = 1/2$, then for any n, m, I get $|a_n - a_m| = |n - m| = 1 > 1/2$.

Definition. A sequence $\{a_n\}$ of rational numbers is called *bounded* if there exists a positive rational number C such that $|a_n| < C$ for all $n \in \mathbf{N}$.

Proposition 1. *A Cauchy sequence is bounded.*

Proof. Let $\{a_n\}$ be a Cauchy sequence. Choose a natural number N such that $|a_n - a_m| < 1$ for any $n, m \geq N$. In particular $|a_n - a_N| < 1$ for all $n \geq N$. Thus for any $n \geq N$,

$$|a_n| = |(a_n - a_N) + a_N| \leq |a_n - a_N| + |a_N| < 1 + |a_N|.$$

Now if we choose any number C such that $C > 1 + |a_N|, a_0, a_1, \ldots, a_{N-1}$ we obtain that $|a_n| < C$ for all $n \in \mathbf{N}$.

Example. 4. Not every bounded sequence is a Cauchy sequence. For example define $\{a_n\}$ by the formula $a_n = 1$ if n is even (i.e., equal to $2k$ for some integer k) and $a_n = 0$ if n is odd (i.e., not even). It is obviously bounded but $|a_n - a_{n+1}| = 1$ for any n. Obviously it cannot be a Cauchy sequence.

Proposition 2. *Let $\{a_n\}, \{b_n\}$ be two Cauchy sequences. Then*
(i) the sum $\{a_n\} + \{b_n\}$ is a Cauchy sequence;
(ii) the product $\{a_n\} \cdot \{b_n\}$ is a Cauchy sequence;
(iii) for any rational number r, the sequence $\{ra_n\}$ is a Cauchy sequence.

Proof. (i) Let ϵ be any positive rational number. Since $\{a_n\}$ is a Cauchy sequence there exists a natural number N such that $|a_n - a_m| < \epsilon/2$ for any $n, m \geq N$. Similarly we find a natural number N' such that $|b_n - b_m| < \epsilon/2$ for any $n, m \geq N'$. Thus for any $n, m \geq N, N'$ we have, by using the Triangle Inequlaity,

$$|(a_n + b_n) - (a_m + b_m)| = |(a_n - a_m) + (b_n - b_m)| \leq |(a_n - a_m)| + |(b_n - b_m)| < \epsilon/2 + \epsilon/2 = \epsilon.$$

This proves that $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ is a Cauchy sequence.

(ii) Let ϵ be any positive rational number. By Proposition 1, both sequences are bounded. Choose A and B such that $|a_n| < A, |b_n| < B$ for any $n \in \mathbf{N}$. We also can assume, by replacing A and B by larger numbers, that $A = B, \epsilon/3A^2 < 1$. We can find a natural number N such that $|a_n - a_m| < \epsilon/3A, |b_n - b_m| < \epsilon/3A$ for all $n, m \geq N$. Then for any $n, m \geq N$, by using Lemma 1, we have

$$|(a_n b_n) - (a_m b_m)| = |(a_n - a_m)(b_n - b_m) + a_m(b_n - b_m) + b_m(a_n - a_m)| \leq$$

$$\leq |(a_n - a_m)(b_n - b_m)| + |a_m(b_n - b_m)| + |b_m(a_n - a - a_m)| = |(a_n - a_m)(b_n - b_m)| + |a_m||(b_n - b_m)| + |b_m||(a_n - a_m)|$$

$$< (\epsilon/3A)^2 + A(\epsilon/3A) + A(\epsilon/3A) = (\epsilon/3)(\epsilon/3A^2) + \epsilon/3 + \epsilon/3 < \epsilon/3 + \epsilon/3 + \epsilon/3 = \epsilon.$$

(iii) This follows from (ii) since $\{ra_n\}$ is the product of the constant sequence $\{r\}$ and $\{a_n\}$. A constant sequence is a Cauchy sequence.

Corollary. *The set $CSeq(\mathbf{Q})$ of Cauchy sequences is a commutative ring with respect to the operations of addition and multiplication.*

Proof. We have already observed that the set of all sequences of rational numbers is a commuttive ring with respect to the operations of addition and multiplication. By the proposition, the result of each of these two binary operation at a pair of Cauchy sequences is again a Cauchy sequence. Now all the properties of commutativity, associativity and distributivity of addition and multiplication apply to Cauchy sequences. To verify that $CSeq(\mathbf{Q})$ is a ring, we have to check that the neutral elements in $Seq(\mathbf{Q})$ are Cauchy sequences, and also that the negative of a Cauchy sequence is a Cauchy sequence. But this is easy. The neutral element with respect to addition (resp, multiplication) are constant sequences $\{0\}$ (resp. $\{1\}$). By Example 1, they are Cauchy sequences. Finally the negative of a Cauchy sequence $\{a_n\}$ is the sequence $\{-a_n\}$. It is equal to the sequence $\{(-1)a_n\}$ and, by assertion (iii) of Proposition 2, it is a Cauchy sequence.

Let $CSeq(\mathbf{Q})$ be the set of Cauchy sequences. Define the equivalence relation on this set by

$$\{a_n\} \sim \{b_n\} \iff \quad \text{for any positive } \epsilon \in \mathbf{Q} \text{ there exists } N \in \mathbf{N} \text{ such that } |a_n - b_n| < \epsilon \text{ for any } n \geq N.$$

Let us check that this is indeed an equivalence relation. It is obviously reflexive and symmetric. Let us verify transitivity. Suppose $\{a_n\} \sim \{b_n\}$, $\{b_n\} \sim \{c_n\}$. For any positive $\epsilon \in \mathbf{Q}$ we can choose a natural number N such that $|a_n - b_n| < \epsilon/2, |b_n - c_n| < \epsilon/2$ for any $n \geq N$ (choosing first one N_1 for the first inequality, then N_2 for the second one and then taking any $N \geq N_1, N_2$). Then, for any $n \geq N$,

$$|a_n - c_n| = |(a_n - b_n) + (b_n - c_n)| \leq |(a_n - b_n)| + |(b_n - c_n)| < \epsilon/2 + \epsilon/2 = \epsilon.$$

This shows that $\{a_n\} \sim \{c_n\}$.

Here comes our promised definition of a real number

Definition. A *real number* is an equivalence class in the set of Cauchy sequences with respect to the above defined equivalence relation. The set of real numbers is denoted by $\mathbf{R}$.

Let us first see how rational numbers become a special case of real numbers. For any rational number a consider the equiavlance class of the constant sequence $c_a = \{a\}$. It is a Cauchy sequence by example 1. If $\{a\} \sim \{b\}$, then $|a - b|$ can not be made smaller of arbitrary positive ϵ unless $a = b$. This shows that the map $i : \mathbf{Q} \to \mathbf{R}$ defined by the formula $i(a) = [\{a\}]$ is injective. We shall denote real numbers of the form $i(a)$ by a, hopefully no confusion will arise.

Using Proposition 2 we can define *addition* and *multiplication* of real numbers by the following rules

$$[\{a_n)\}] + [\{b_n)\}] = [\{a_n\} + \{b_n\}],$$

$$[\{a_n)\}] \cdot [\{b_n)\}] = [\{a_n\} \cdot \{b_n\}].$$

We have to verify that this definition is legal, i.e, is independent of the choice of writing an equivalence class as the equivalence class of some of its elements. Assume $[\{a_n)\}] = [\{a'_n)\}], [\{b_n)\}] = [\{b'_n)\}]$. Then for any positive rational ϵ we can find a natural number N such that $|a_n - a'_n| < \epsilon/2, |b_n - b'_n| < \epsilon/2$ for any $n \geq n$. This implies that

$$|(a_n + b_n) - (a'_n + b'_n)| = |(a_n - a'_n) + (b_n - b'_n)| \leq |a_n - a'_n| + |b_n - b'_n| < \epsilon/2 + \epsilon/2 = \epsilon$$

for any $n \geq N$. Thus $[\{a_n\} + \{b_n\}] = [\{a'_n\} + \{b'_n\}]$ and the two definitions agree.

Following the proof of Proposition 2 (ii), we easily check that $[\{a_n)\} \cdot \{b_n\}] = [\{a'_n\} \cdot \{b'_n\}]$. We leave it as an execise to the reader.

We shall always use the following simple observation.

Lemma 2. *Let $\{a_n\}$ be a Cauchy sequence and let $\{a'_n\}$ be a sequence obtained from $\{a_n\}$ by changing finitely many of its values. Then $\{a'_n\}$ is a Cauchy sequence and $\{a_n\} \sim \{a'_n\}$.*

Proof. This is obvious since there exists some natural number N such that $a_n = a'_n$ for $n \geq N$.

Theorem 1. *The set of real numbers is a field with respect to the operation of addition and multiplication defined above.*

Proof. By Corollary to Proposition 2, the set $CSeq(\mathbf{Q})$ of Cauchy sequences is a commutative ring. Using this we immediately verify that $\mathbf{R}$ is a commutative field. Its zero 0 and the unit element 1 are the numbers $i(0)$ and $i(1)$ reprsentable by by constant sequences $\{0\}$ and $\{1\}$. It remain to check only the axiom of the existence of the inverse of a non-zero element with respect to multiplication. Let $x = \{a_n\}$ be a non-zero Cauchy sequence. First we claim that there exists some natural number N such that $a_n \neq 0$ for $n \geq N$. Let us prove it. Suppose this is not true, i.e., for any N there exists $k_N \geq N$ such that $a_{k_N} = 0$. Since our sequence is Cauchy sequence, for any ϵ we can find N such that $|a_n - a_m| < \epsilon$ when $n, m \geq N$. Taking $m = k_N$, we see that $|a_n| < \epsilon$ for $n \geq n$. This shows that the sequence $\{a_n\}$ is equivalent to the constant sequence $\{0\}$, hence $[\{a_n\}] = 0$. This contradiction proves our claim. Now we can define the inverse. Suppose all $a_n \neq 0$ starting from some N. Define the sequence $\{b_n\}$ by taking $b_n = 0$ for $n < N$ and $b_n = a_n^{-1}$ for $n \geq N$. Then $a_n \cdot b_n = 1$ for $n \geq N$, and hence, by Lemma 2, $\{a_n \cdot b_n\} \sim \{1\}$. This proves our assertion.

Exercises 2.4.

2.4.1. Prove that the sequence $\{\frac{1}{n^2+1}\}$ is a Cauchy sequence and is equivalent to the constant sequence $\{0\}$.

2.4.2. Prove that sum and product of bounded sequences of rational numbers is a bounded sequence.

2.4.3 Give your own example of a bounded sequence of rational numbers which is not a Cauchy sequence.

2.4.4. Decide whether the following sequences of rational numbers are Cauchy sequences:

(a) $\{(-1)^n\}$;

(b) $\{\frac{2n^2+n}{n^2-n+1}\}$;

(c) $\{1 + \frac{1}{2} + \frac{1}{2^2} + \ldots + \frac{1}{2^n}\}$.

2.4.5 Let $\{a_n\}$ be a Cauchy sequence. Set $b_n = (a_n + a_{n+1})/2$. Prove that the sequence $\{b_n\}$ is a Cauchy sequence.

2.4.6 Prove the inequality $||a| - |b|| \leq |a - b|$ for any $a, b \in \mathbf{R}$.

2.5 Further properties of real numbers. In this section I shall try to convince you that our definition of real numbers agrees with your old intuitive notion of a real number.

First let us define the relation of order in the set $\mathbf{R}$.

Definition. A real number $x = [\{a_n\}]$ is called *positive* (we write $x > 0$) if there exists a positive rational number ρ and a natural number N such that $a_n > \rho$ for all $n \geq N$. We write $x \geq 0$ if either $x > 0$ or $x = 0$.

Note that this definition is independent of the choice of a representative $\{a_n\}$ in the equivalence class x. In fact, if $x = [\{b_n\}]$, then we may find a natural number M such that $|a_n - b_n| < \rho/2$ for $n \geq M$. Hence $a_n - b_n > -\rho/2$ for $n \geq M$, and we obtain

$$b_n - \rho = (b_n - a_n) + (a_n - \rho) \geq (b_n - a_n) > -\rho/2 \quad \text{for any } n \geq N + M.$$

From this we deduce that $b_n \geq \rho - \rho/2 = \rho/2$ for all $n \geq N + M$.

Lemma 1. *Let x, y be two positive real numbers. Then $x + y$ and xy are positive.*

Proof. Let $x = [\{a_n\}, y = [\{b_n\}]$. By assumption, there exist some positive rational numbers ρ and σ, and a natural number N such that for all $n \geq N$, we have $a_n \geq \rho, b_n \geq \sigma$. Applying Proposition 3 from section 2.3, we get

$$a_n + b_n \geq \rho + \sigma, \ a_n b_n \geq \rho\sigma \quad \text{for all } n \geq N.$$

Since $\rho + \sigma, \rho\sigma \geq 0$, this proves the assertion

Proposition 1. *The relation $R = \{(x, x') \in \mathbf{R} \times \mathbf{R} \mid x' - x \geq 0\}$ is an order relation.*

Proof. Let us write $x \leq y$ if $(x, y) \in R$. The reflexivity is obvious. Let us check the transitivity. Suppose $x \leq y, y \leq z$. We have to show that $x \leq z$. Clearly we may assume that x, y, z are all different real numbers. Then

$$y - x > 0, \quad z - y > 0.$$

Adding up, we get, by Lemma 1, $z - x > 0$. This shows that $x \leq z$.

Let us check the anti-symmetry property. Suppose $x \leq y, y \leq x$. We have to show that $x = y$. Assume $x \neq y$, then $y - x > 0, x - y > 0$. By Lemma 1, $0 = \{0\} > 0$. This is obviously absurd.

We shall write $x \geq y$ if $y \leq x$, and $x > y$ if $y \leq x, x \neq y$.

Lemma 2. *A real number x is positive if and only if $x = [\{a_n\}]$ where all a_n are greater than some positive rational number ρ.*

Proof. The condition is obviously sufficient. Let us show that it is necessary. Suppose $x > 0$. By definition, $x = [\{x_n\}]$ where $x_n > \rho$ for $n \geq N$ where ρ is a positive rational number and N is some natural number. Now, using Lemma 2 from 2.4, we replace $\{x_n\}$ by the equivalent sequence $\{a_n\}$ where $a_0 = a_1 = \ldots = a_{N-1} = \rho + 1$ and $a_n = x_n$ for $n \geq N$. This proves the assertion.

Proposition 2. *Let $x, y \in \mathbf{R}$.*
(i) one and only one of the the following three cases occurs: $x < y, x = y, y < x$;
(ii) (Archimedian Property) if $x, y > 0$, there exists a natural number N such that $Ny > x$;
(iii) $x \leq y, x' \leq y' \Longrightarrow x + x' \leq y + y'$;
(iv) $x \leq y, x' \leq y', y, y' \geq 0 \Longrightarrow xx' \leq yy'$;
(v) $x \geq y, y \geq 0 \Longrightarrow x^{-1} \leq y^{-1}$.

Proof. (i) Let $x = \{a_n\} \in \mathbf{R}$. If $x = 0$, we are done. Assume $x \neq 0$. Then there exists a positive rational number ϵ such that for any natural N there is $n(N) \geq N$ with $|a_{n(N)}| > \epsilon$. The latter inequality is equivalent to that $a_{n(N)} > \epsilon$ if $a_{n(N)} > 0$ and $a_{n(N)} < -\epsilon$ if $a_n < 0$. Suppose the first case occurs. Since $\{a_n\}$ is a Cauchy sequence, there exists a natural number M such that $|a_n - a_m| < \epsilon/2$ for $n, m \geq M$. Now if we take $N \geq M$, we would have $|a_{n(N)} - a_n| < \epsilon/2$ for any $n \geq M$, hence $-\epsilon/2 < a_n - a_{n(N)}$ and we get, for any $n \geq M$,

$$a_n > -\epsilon/2 + a_{n(N)} > -\epsilon/2 + \epsilon = \epsilon/2.$$

This shows that $\{a_n\} > 0$. In the case when $a_{n(N)} < -\epsilon$ we replace x by $-x = \{-a_n\}$. Then $-a_{n(N)} > \epsilon$, and repeating the argument we get $-x > 0$. The latter is equivalent to that $x < 0$.

(ii) Since x, y are positive, and y is bounded, by Lemma 2, we may find some positive rational numbers p/q and r/s such that $x = \{a_n\}, y = \{b_n\}$ where $a_n > p/q, 0 < b_n < r/s$ for all n. By Archimedian property for rational numbers there exists a natural number N such that $N(p/q) > r/s + 1$. But then

$$Na_n > N(p/q) > r/s + 1 > b_n + 1$$

for all n. This implies $Na_n - b_n > 1$ for all n. By definition of positivity of real numbers, $Ny > x$.

(iii) -(v) Proved word by word similar to the proof of assertions (iv),(v),(vi) from Proposition 2 in section 2.3.

Recall that we have defined an injective map

$$i : \mathbf{Q} \to \mathbf{R},\ r \mapsto \{r\},$$

which allows us to consider rational numbers as real numbers represented by constant Cauchy sequences. This map is consistent with all the properties of rational numbers we established in the previous sections. Looking at the definitions we observe that, for any $r, q \in \mathbf{Q}$,

$$i(r + q) = i(r) + i(q);$$

$$i(r \cdot q) = i(r) \cdot i(q);$$

$$i(r^{-1}) = i(r)^{-1} \quad \text{if } r \neq 0;$$

$$r \leq q \Longleftrightarrow i(r) \leq i(q).$$

From now on, we call real numbers of the form $i(r), r \in \mathbf{R}$, *rational real numbers* (or just rational numbers). We denote the set $i(\mathbf{Q})$ of rational real numbers by $\mathbf{Q}$ hoping that no confusion will arise.

For any two real numbers $a \leq b$ let us use our old notations and definitions for segments, intervals and semi-intervals. For example

$$[a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}.$$

We shall also extend the function of absolute value to the set $\mathbf{R}$ by setting

$$|x| = \begin{cases} x & \text{if } x > 0 \\ -x & \text{if } x < 0. \end{cases}$$

The following properties of absolute value are proven word by word repeting the proof of Lemma 1 from section 2.4:

Lemma 3. *Let $a, b \in \mathbf{R}$. Then*
(i) $|a| = |-a|$;
(ii) $|ab| = |a||b|$;
(iii) (Triangle inequality) $|a + b| \leq |a| + |b|$;
(iv) $|a| - |b| \leq |a - b| \leq |a| + |b|$.

Lemma 4. *Let $x \in \mathbf{R}$. There exists a unique integer, denoted by* $\mathrm{int}(x)$ *such that*

$$0 \leq x - \mathrm{int}(x) < 1.$$

Proof. The uniqueness is easy. If $x = A + a = B + b$ where A, B are integers and $0 \leq a, b < 1$, then after subtracting x from x, we get $A - B = b - a$. Since $-1 < -b \leq a - b \leq a < 1$, we get $|A - B| = |a - b| < 1$. Since A, B are integers this implies $A = B$.

Let $x = [\{x_n\}] \in \mathbf{R}$. Since $\{x_n\}$ is bounded we can find a positive rational number C such that $|x_n| < C$ for all n. Obviously we may assume that C is a natural number (replacing $C = p/q$ with p). Thus $-C < x_n < C$, and we can find an integer $\mathrm{int}(x_n) \in \mathbf{Z}$ uniquely determined by the property

$$\mathrm{int}(x_n) \le x_n < \mathrm{int}(x_n) + 1,$$

or equivalently,

$$x_n = \mathrm{int}(x_n) + a_n, \quad \text{where } 0 \le a_n < 1.$$

To do this we start with $C - 1$ and go down to $-C$ until we hit the number satisfying this property. Since $\{x_n\}$ is a Cauchy sequence, for any positive rational ϵ we can find $n \in \mathbf{N}$ such that for all $n, m \ge N$, we have $|x_n - x_m| < \epsilon$. Since $-1 < -a_m < a_n - a_m < a_n < 1$, we get $|a_n - a_m| < 1$ and, for all $n, n \ge N$,

$$\epsilon > |x_n - x_m| = |\mathrm{int}(x_n) + a_n - \mathrm{int}(x_m) - a_m| = |(\mathrm{int}(x_n) - \mathrm{int}(x_m)) - (a_m - a_n)|$$

$$\ge |\mathrm{int}(x_n) - \mathrm{int}(x_m)| - |a_m - a_n| \ge |\mathrm{int}(x_n) - \mathrm{int}(x_m)| - 1.$$

Taking $\epsilon < 1$ we obtain that $|\mathrm{int}(x_n) - \mathrm{int}(x_m)| < 1 + \epsilon < 2$. Since the numbers $\mathrm{int}(x_n)$ are integers this implies that the numbers $\mathrm{int}(x_n)$ and $\mathrm{int}(x_m)$ are either equal or differ by one. There are two possible cases:

(a) $int(x_n) = A$ for all $n \ge N$ with exception of finetely many n, or

(b) there are infinitely many $n \ge N$ for which $int(x_n) = A$ and there are infinitely many $m \ge N$ for which $x_m = A + 1$.

Consider the first case. Then replacing finitely many values of our sequence (namely x_n with $int(x_n) \ne A$), we may replace $\{x_n\}$ by an equivalent Cauchy sequence to assume that $\mathrm{int}(x_n) = A$ for all n. Hence $x - A = \{a_n\}$ where $0 \le a_n < 1$ for all n. The sequence $\{a_n\}$ defines a real number $a \ge 0$. Since obviously $a > 1$ is impossible we get $a = 0$ or $a < 1$. Thus we get

$$x = \mathrm{int}(a) = A + 1.$$

In the second case

$$x = A + a \quad \text{where } 0 \le a < 1.$$

This proves the assertion in case (a).

It remains to consider case (b). Let

$$X = \{n \in \mathbf{N} \mid \mathrm{int}(x_n) = A.$$

Replacing $\{x_n\}$ by an equivalent sequence we may assume that

$$\mathbf{N} \setminus X = \{n \in \mathbf{N} \mid \mathrm{int}(x_n) = A + 1.$$

Since $\{x_n\}$ is a Cauchy sequence, for any given ϵ there exists $N \in \mathbf{N}$ such that $|x_n - x_m| < \epsilon$ for all $n, m \ge N$. Since X and $\mathbf{N} \setminus X$ are infinite sets, we can choose $n \in X$ and $m \notin X$ with $n, m \ge N$. Then

$$\epsilon > |x_n - x_m| = |(A + 1 + a_m) - (A + a_n)| = |a_m + (1 - a_n)| = a_m + 1 - a_n > a_m, 1 - a_n.$$

This implies that

$$|x_n - A - 1| = |A + a_n - (A - 1)| = |1 - a_n| < \epsilon \quad \text{for } n \in X, n \ge N.$$

$$|x_n - A - 1| = |A + 1 + a_n - (A + 1)| = |a_n| < \epsilon \quad \text{for } n \notin X, n \ge N.$$

Thus $|x_n - A - 1| < \epsilon$ for all $n \ge N$. By definition of equivalence of Cauchy sequences we obtain $\{x_n\} \sim \{A + 1\}$, hence

$$x = \mathrm{int}(x) = A + 1.$$

Example. Let $x = \{1 + (-1)^n(1/n)\}$. Then $\mathrm{int}(x_n) = 1$ if n is even, and $\mathrm{int}(x_n) = 0$ if n is odd. However, $x = \mathrm{int}(x) = 1$ since $x - 1 = \{(-1)^n(1/n)\} = [\{0\}] = 0$.

Definition. Let x be a real number. The integer $\mathrm{int}(x)$ defined in the previous lemma is called the *integral part* of x.

Now we are ready to define the decimal expresion.

Theorem 1 (On decimal expressions). *Let x be a real number. Then $x = [\{x_n\}]$ where*

$$x_n = A_0 + \frac{A_1}{10} + \dots \frac{A_n}{10^n}$$

where $A_0 \in \mathbf{Z}, A_1, \dots, A_n \in \{0, 1, 2, \dots, 9\}$.

Proof. Write first $x = \text{int}(x) + a$ as in Lemma 3. Then write $10a = \text{int}(10a) + a_1$ for some $0 \leq a_1 < 1$. If $a = 0$ we get that $x = \text{int}(x) \in \mathbf{Z}$. Assume $a \neq 0$. Since $a < 1$, we get $10 - \text{int}(10a) = 10 - 10a + a_1 = 10(1 - a) + a_1 > 0$ hence $0 \leq \text{int}(10a) < 10$, i.e., $\text{int}(10a) \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Dividing by 10 (i.e. multiplying by 10^{-1}), we get

$$x = \text{int}(a) + a = \text{int}(x) + \frac{\text{int}(10a)}{10} + \frac{a_1}{10}$$

for some $a_1 \in \mathbf{R}$ satisfying $0 \leq a_1 < 1$. If $a_1 = 0$ we stop getting

$$x = \text{int}(a) + \frac{\text{int}(10a)}{10} \in \mathbf{Q}.$$

If $a_1 \neq 0$, we repeat this process, replacing in above, a with a_1. We obtain

$$a_1 = \frac{\text{int}(10a_1)}{10} + \frac{a_2}{10}.$$

Plugging in, we get

$$x = \text{int}(x) + \frac{\text{int}(10a)}{10} + \frac{\frac{\text{int}(10a_1)}{10} + \frac{a_2}{10}}{10} = \text{int}(x) + \frac{\text{int}(10a)}{10} + \frac{\text{int}(10a_1)}{10^2} + \frac{a_2}{10^2}$$

where $\text{int}(10a_1) \in \{0, \dots, 9\}, 0 \leq a_2 < 1$. Continuing in this way, we find for any natural n a rational number

$$x_n = A_0 + \frac{A_1}{10} + \dots + \frac{A_n}{10^n}$$

where $A_0 \in \mathbf{Z}, A_1, \dots, A_n \in \{0, 1, 2, \dots, 9\}$ such that

$$x = x_n + \frac{a_{n+1}}{10^{n+1}}$$

for some real number $a_{n+1} \in [0, 1)$. Consider the sequence of rational numbers $\{x_n\}$. We claim that $\{x_n\}$ is a Cauchy sequence and

$$x = [\{x_n\}].$$

Let ϵ be a positive rational number. Choose N such that $10^{N+1}\epsilon > 2$. This is easy to arrange. First, by Archimedian property, we find a natural number M such that $M\epsilon > 1$. Then we choose N such that $10^{N+1} > M$. Now for any $n, m \geq N$ we have

$$|x_n - x_m| = |(x - \frac{a_{n+1}}{10^{n+1}}) - (x - \frac{a_{m+1}}{10^{m+1}})| = |\frac{a_{n+1}}{10^{n+1}} - \frac{a_{m+1}}{10^{m+1}}| < |\frac{a_{n+1}}{10^{n+1}}| + |\frac{a_{m+1}}{10^{m+1}}| \leq \frac{2}{10^{N+1}} < \epsilon.$$

This checks that the sequence $\{x_n\}$ is a Cauchy sequence. Now let us prove that $x = [\{x_n\}]$. Let $x' = [\{x_n\}]$. Since $\{x_n\}$ is Cauchy, given rational $\epsilon/2 > 0$ we can find N such that $|x_n - x_N| < \epsilon/2$ for $n \geq N$. Thus, by definition of order for real numbers, $|x' - x_N| \leq \epsilon/2$. Now $|x - x_N| = a_N/10^N < 1/10^N$ also can be made strictly smaller then $\epsilon/2$ (replacing N by a larger number if needed). From this we infer that $|x - x'| = |(x - x_N) - (x' - x_N)| < \epsilon/2 + \epsilon/2 = \epsilon$. Since we can choose ϵ arbitrary, this implies that $x = x'$ (by definition of order, for any positive real number a there exists a positive rationa number ρ such that $x > \rho$). This proves the assertion.

We may write

$$x = A_0.A_1A_2 \dots A_n \dots$$

to express the fact that

$$x = [\{A_0 + \frac{A_1}{10} + \dots \frac{A_n}{10^n}\}].$$

For example,

$$\frac{1}{3} = 0.333\dots = [\{\frac{3}{10} + \dots \frac{3}{10^n}\}],$$

$$\frac{3}{2} = 1.5 = [\{1 + \frac{5}{10}\}].$$

Conversely any expression $A_0.A_1A_2\dots A_n\dots$ (*decimal*) can be thought as the real number

$$x = [\{A_0 + \frac{A_1}{10} + \dots \frac{A_n}{10^n}\}].$$

However, two such expressions may represent the same number. For example,

$$0.999\dots = [\{\frac{9}{10} + \dots \frac{9}{10^n}\}] = 1$$

(where as usual we define the value of the sequence at 0 arbitrary). In fact, using the formula for the geometric progression, we get

$$1 - (\frac{9}{10} + \dots \frac{9}{10^n}) = 1 - \frac{9}{10}(1 + \dots + \frac{1}{10^n}) = 1 - \frac{9}{10}(\frac{1 - \frac{1}{10^{n+1}}}{1 - \frac{1}{10}}) = 1 - (1 - \frac{1}{10^{n+1}}) = \frac{1}{10^{n+1}}.$$

Since the sequence $\{\frac{1}{10^{n+1}}\}$ is obviously equivalent to the zero sequence, we obtain the equality.

Remark. Instead of multiplying the number $x - \text{int}(x)$ by 10 and then taking the integral part we can multiply by 2 and get the expression of $x - \text{int}(x)$ as the equivalance class of the Cauchy sequence

$$\{x_n\} = \{\frac{A_1}{2} + \frac{A_2}{2^2} + \dots + \frac{A_n}{2^n}\}$$

where $A_1, \dots, A_n \in \{0, 1\}$. This is the expressions of real numbers from $(0, 1)$ which we used for proving uncountability of the set of real numbers. Also we can write any positive integer in the form $b_0 + b_1 2 + \dots + b_k 2^k$ where $b_0, \dots, b_k \in \{0, 1\}, b_k \neq 0$. In this way we obtain a binary-decimal expression of real numbers in the form

$$x = \pm b_k b_{k-1} \dots b_0.a_1 \dots a_n \dots$$

where all "digits" $b_0, \dots, b_k, a_1, \dots, a_n, \dots$ belong to the set $\{0, 1\}$ and $b_k \neq 0$. For example,

$$\frac{1}{3} = .01010\dots, \quad \frac{3}{2} = 1.1, \quad 7 = 111.$$

Similarly we can use 3 (or any other natural number) instead of 10 to get *ternary-decimal* expressions for real numbers.

Theorem 2(On nested segments). *Let $\{a_n\}, \{b_n\}$ be two sequences of rational numbers. Suppose*
(i) $a_n < b_n$ for all $n \in \mathbf{N}$;
(ii) $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ for all $n \in \mathbf{N}$;
(ii) the sequence $\{b_n - a_n\}$ is a Cauchy sequence equivalent to $\{0\}$.

Then there exists a unique real number x such that

$$x \in [a_n, b_n] \quad \text{for all } n \in \mathbf{N}.$$

Proof. Set $x_n = (a_n + b_n)/2$. Since $x_n - a_n = b_n - x_n = (b_n - a_n)/2 > 0$, we get, for all n,

$$a_n < x_n < b_n.$$

Let us show that the sequence $\{x_n\}$ is Cauchy sequence. For any positive rational ϵ, using condition (iii), we can choose a natural number N such that $|b_n - a_n| = b_n - a_n < \epsilon$ if $n \geq N$. Then for any $n, m \geq N$,

$$a_n < x_n < b_n, a_m < x_m < b_m \Longrightarrow a_n - b_m < x_n - x_m < b_n - a_m.$$

Without loss of generality we may assume $m \geq n$ (otherwise we replace n by m in the argument below). Then, by (ii), $b_m \leq b_n, a_m \geq a_n$, hence

$$a_n - b_n \leq a_n - b_m < x_n - x_m < b_n - a_m \leq b_n - a_n$$

which implies that for any $n, m \geq N$, we have $|x_n - x_m| < |b_n - a_n| < \epsilon$. This shows that the sequence of rational numbers $\{x_n\}$ is a Cauchy sequence. Let $x = [\{x_n\}]$ be the corresponding real number. For each n, we have, by (ii), $a_n < a_m < x_m < b_m < b_n$ for all $m > n$. Thus by definition of order for real numbers, $a_n \leq x \leq b_n$ hence $x \in [a_n, b_n]$ for each n.

It remains to show the uniqueness of x with the property that $x \in [a_n, b_n]$ for each n. Suppose $x' = \{x'_n\}$ is another real number satisfying this property. Then $x, x' \in [a_n, b_n]$ implies that $a_n - b_n < x - x' < b_n - a_n$, i.e., $|x - x'| < b_n - a_n$. By definition of order this means that there exists some natural number N such that $|x'_m - x_m| < b_n - a_n$ for $m \geq N$. Since by condition (iii), $|b_n - a_n|$ can be made smaller than any given ϵ provided n is large enough, we can make $|x'_m - x_m| < \epsilon$ provided m is large enough. This means that the Cauchy sequences x and x' are equivalent.

The property of real numbers we have just proved was used earlier to prove that the set $\mathbf{R}$ is uncountable. We repeat the proof word by word to obtain

Theorem 3. *The set* $\mathbf{R}$ *is not countable.*

Finally let us relate our definition of real numbers with the definition based on the Dedekind cut method.

Definition. Two non-empty subsets A and B of $\mathbf{Q}$ form a *Dedekind cut* of $\mathbf{Q}$ if $\mathbf{Q} = A \cup B$ and

$$a \in A, b \in B \Longrightarrow a < b.$$

Theorem 4 (Dedekind cuts). *For any Dedekind cut of* $\mathbf{Q}$ *there exists a unique real number* $x \in \mathbf{R}$ *such that*

$$A \subset (-\infty, x] = \{y \in \mathbf{R} \mid y \leq x\} \quad B \subset [x, \infty) = \{y \in \mathbf{R} \mid y \geq x\}.$$

Proof. Let us take any $a \in A$ and denote it by a_0. Let us take any $b \in B$ and denote it by b_0. We have $a_0 < b_0$. Next we take the rational number $a = (a_0 + b_0)/2$. Either it belongs to A or to B. In the former case occurs we put $a_1 = a, b_1 = b_0$, in the latter case we put $a_1 = a_0, b_1 = a$. We have $[a_1, b_1] \subset [a_0, b_0]$ and $b_1 - a_1 = (b_0 - a_0)/2$. Next we take the number $(a_1 + b_1)/2$ and define the segement $[a_2, b_2]$ with the property $[a_2, b_2] \subset [a_1, b_1] \subset [a_0, b_0]$, and $b_2 - a_2 = (b_1 - a_1)/2 = (b_0 - a_0)/2^2$. Continuing in this way we obtain a sequence $\{a_n\}$ in A and a sequence $\{b_n\}$ in B such that $[a_{n+1}, b_{n+1}] \subset [a_n, b_n]$ and $b_n - a_n = (b_0 - a_0)/2^n$. Now we can apply the Theorem on nested segments to obtain a unique real number x such that $x \in [a_n, b_n]$ for any $n \in \mathbf{N}$. Let us see that this is the needed x. Let $a \in A$, if $a > x$, we find some n with $b_n - a_n < a - x$. Then $b_n < a$ since otherwise $b_n - a_n > a - x$. But $b_n \in B$ hence $a < b_n$. This contradiction shows that $A \subset (-\infty, a]$. Similarly we prove that $B \subset [x, \infty)$.

An element of the set $\mathbf{R} \setminus \mathbf{Q}$ is called an *irrational number*. We know already (for example from Theorem 3) that there are irrational numbers. In some sense we have more irrational then rational numbers. More precisely, the set of irrational numbers is not a countable set since otherwise $\mathbf{R}$ will be the union of countable sets, hence countable. However the next theorem shows that rational numbers sit "densely" in the set $\mathbf{R}$.

Theorem 5 (Density Property of rational numbers). *Any interval $(a, b) \subset \mathbf{R}$ with $a < b$ contains a rational number.*

Proof. For any $a \in \mathbf{R}$ the interval $(-\infty, a]$ contains a rational number. Indeed, if $a = [\{a_n\}]$, we know that $|a_n| < C$ for some rational number C. Hence $0 < a_n - (-C)$ for all n, hence by definition of order for real numbers, $-C \leq a$. Similarly we prove that $([a, \infty) \cap \mathbf{Q} \neq \emptyset$. Now from

$$\mathbf{R} \setminus (a, b) = (-infty, a]) \cup [b, \infty)$$

follows that $\mathbf{Q} \cap (a, b) = \emptyset$ implies that $\mathbf{Q} = ((-infty, a] \cap \mathbf{Q}) \cup ([b, \infty) \cup \mathbf{Q})$. Thus $A = (-infty, a] \cap \mathbf{Q}, B = [b, \infty) \cup \mathbf{Q}$ is a Dedekind cut of $\mathbf{Q}$. Clearly any real number in (a, b) (for example, $a + b/2$ and $b + 2a/3$) satisfies the assertion of Theorem 4. By the uniqueness assertion, we get $a = b$ (sinse $a + b/2 = b + 2a/3$ implies $a = b$). This contradicts tehassumption of the theorem.

Example. Let us use Dedekind cuts to construct an irrational number x such that $x^2 = 2$. First of all, let us see that there is no rational number p/q with $(p/q)^2 = 2$. This must be very well-known for you but I repeat the proof. Obviously we may assume that $p/q > 0$. If $(p/q)^2 = p^2/q^2 = 2$ we obtain, by multiplying both sides by q^2

$$p^2 = 2q^2.$$

We may assume that either p or q is odd since otherwise we get $p/q = 2n/2m = n/m$ and continuing this process (decreasing numerator and denominator) we get the needed property. Suppose p is odd, then $p = 2n + 1$ for some integer n, and plugging in, we obtain

$$0 = p^2 - 2q^2 = (2n + 1)^2 - 2q^2 = 4n^2 + 4n + 1 - 2q^2 = 2(2n^2 + 2n - q^2) + 1.$$

This is obviously impossible (since 2 has no inverse in $\mathbf{Z}$). Thus p is even, i.e., $p = 2n$ for some integer n. Plugging in, we get $4n^2 = 2q^2$ hence $q^2 = 2n^2$. Repeating the argument from above, we get that q must be even. Thus p is even, and q is even, which is impossible by our assumption.

Set

$$A = \{a \in \mathbf{Q} \mid a^2 < 2, a \geq 0\} \cup \{a \in \mathbf{Q} \mid a \leq 0\},$$
$$B = \{a \in \mathbf{Q} \mid a^2 > 2, a \geq 0\}.$$

I claim that these two sets form a Dedekind cut. In fact, we have just proved that for any non-negative rational number a, there are only two possibilities, either $a^2 < 2$, or $a^2 > 2$ (the third possibility $a^2 = 2$ does not occur!). So, any nonnegative rational number is either in A or in B. Any negative rational number is in A. Also, if $a \geq 0$ and $a^2 < 2, b^2 > 2$ then $a^2 < b^2$ implies $a < b$. Clearly any negative number from A is less than any number from B. Thus we get ourselves a Dedekind cut. Let x be the real number defined by this Dedekind cut. Suppose $x^2 < 2$. Let us find a positive real number ρ such that $(x + \rho)^2 < 2$. For this we need that $2\rho x + \rho^2 < 2 - x^2$. Since obviously $x < 2$ (otherwise $x^2 \geq 4$) we need $4\rho + rho^2 < 2 - x^2 - 2$. If we take $\rho < 1/2$, then $\rho^2 = \rho\rho < \rho/2$ and we need $4\rho + \rho^2 < 7\rho/2 < 2 - x^2$. This is easy to achieve by taking $\rho < 2(2 - x^2)/7$. For example we may take a rational number ρ contained in the interval $(0, 2(2 - x^2)/7)$. Now, using Theorem 5, take any rational number a in $(x, x + \rho)$. Since $a > x$, we have $a \in B$. However $a^2 < (x + \rho)^2 < 2$, showing that $a \in A$. This contradiction shows that $x^2 < 2$ is impossible. Similarly we prove that $x^2 > 2$ is impossible. The remaining possibility is $x^2 = 2$.

We define a Dedekind cut of $\mathbf{R}$ similar to the definition of the Dedekind cut of the set $\mathbf{Q}$.

Theorem 6 (Completeness of real numbers). *Let A, B be a Dedekind cut of $\mathbf{R}$. Then there exists a unique real number x such that $A = (-\infty, x), B = [x, \infty)$ or $A = (-infty, x], B = (x, \infty)$.*

Proof. Let $A' = A \cap \mathbf{Q}, B' = B \cap \mathbf{Q}$. Then the pair (A', B') is a Dedekind cut of $\mathbf{Q}$. In fact, $A' \cup B' = (A \cup B) \cap \mathbf{Q} = \mathbf{R} \cap \mathbf{Q} = \mathbf{Q}$. Also for any $a \in A', b \in B'$ we have $a < b$. By Theorem 4, there exists a unique real number x such that $A' \subset (-\infty, x], B' \subset [x, \infty)$. Since $\mathbf{R} = A \cup B$ we have $x \in A$ or $x \in B$. Assume $x \in A$. Then for any $a \in A$, we must have $a \leq x$. In fact, if this were false, we can find $a \in A$ such that $x < a$. By Theorem 5, we can find a rational number $a' \in (x, a)$. Since $a' < a < b$ for all $b \in B$ we must have $a' \in A'$. But then $a' > x$ contradicts the choice of x. Thus $x \in A$, and then $A \subset [x, \infty), B \subset (x, \infty)$. Similarly we consider the case $x \in B$ where we must have $A \subset (-\infty, x), B \subset [x, \infty)$. Since $\mathbf{R} = A \cup B$, we must have the equalities of sets in each case.

Theorem 7 (On the least upper bound). *Let $X \subset \mathbf{R}$. Assume there exists a real number c such that $X \subseteq (-\infty, c]$ (such c is called an upper bound for X). Then there exists a real number c_0 such that $X \subseteq (-\infty, c_0]$ and $X \not\subseteq (\infty, c']$ for any $c' < c_0$ (such number c_0 is called the least upper bound for X).*

Proof. Let $B = \{c \in \mathbf{R} \mid X \subseteq (-\infty, c]\}$ be the set of upper bounds for X. Let $A = \{c \in \mathbf{R} \mid B \subset [c, \infty)\}$. Clearly $X \subseteq A$. For any $x \notin B$ there exists some $a \in X$ such that $a > x$. Since $a < c$ for any $c \in B$, we must have $c > x$ for any $c \in B$. Thus $x \in A$. This shows that $\mathbf{R} = A \cup B$. Obviously $a \in A, b \in B \Longrightarrow a < b$. Therefore the pair (a, B) form a Dedekind cut of $\mathbf{R}$. Let c_0 the real number chosen as in Theorem 6. We get $A = (-\infty, c_0), B = [c, \infty)$ or $A = (-\infty, c_0], B = (c, \infty)$ Since $X \subseteq A$, we get $X \subseteq (-\infty, c_0]$. If $X \subseteq (-\infty, c']$ for some $c' < c_0$, then for any $b \in B$, we get $b \geq c_0 > c'$. This contradicts any of the equalities $B = [c, \infty)$ or $B = (c, \infty)$. This proves that $X \not\subseteq (-\infty, c']$ for any $c' < c_0$. The assertion is proven.

Exercises 2.5.
2.5.1 Show by example that the analog of the statement of Theorem 7 for rational numbers is not true.
2.5.2 Define the notion of a lower bound and the greatest lower bound for a set of real numbers. State and prove the analog of Theorem 7 for lower bounds.
2.5.3 Find
(a) decimal expression for the rational numbers: $1/6, 15/7, 33/6$
(b) binary-decimal expression for the same numbers;
(c) first five terms of the decimal expressing the positive solution of the equation $x^2 = 2$.
2.5.4 Prove that there is a an irrational number between any two rational numbers (i.e., $(a, b) \cap (\mathbf{R} \setminus \mathbf{Q}) \neq \emptyset$ for any rational numbers a, b).
2.5.6 Consider segments $S_i = [a_i, b_i] \subset \mathbf{R}, i = 1, \ldots, n$. Show that $S_1 \cap \ldots \cap S_n$ is either empty, a singleton, or a segment.
2.5.7 Find the least upper bound of the following sets
(a) $A = \{x \in \mathbf{R} \mid |x| < 1\}$;
(b) $B = \{x \in \mathbf{R} \mid x^2 < 5\}$;
(c) $C = \{x \in \mathbf{R} \mid x = \frac{a}{a-1} \quad \text{for some } a \text{ with } 0 < a < 1\}$;
(d) $D = A \cap B$;
(e) $E = C \setminus A$.
2.5.8 For any positive real number x prove the existence of a real number y such that $y^2 = x$. Show that there is only one non-negative solution of this equation.
2.5.9 Prove that the numbers, $\sqrt{3}, \sqrt{5}, \sqrt{3} + \sqrt{5}$ are irrational. Here $\sqrt{a}$ denotes the positive solution of the equation $x^2 = a$.

Appendix 1. The Euler number e.

Recall that the product of the first n natural numbers $1 \cdot 2 \cdots n$ is denoted by $n!$. It is called *n factorial*. We set $0! = 1$.

Consider the sequence of rational numbers $\{x_n\}$ where

$$x_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}.$$

Lemma 1. *The sequence $\{x_n\}$ is convergent.*

Proof. Since

$$x_{n+1} = x_n + \frac{1}{(n+1)!}$$

the sequence is monotone increasing. We also have

$$x_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} \leq 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \ldots \frac{1}{2^{n-1}} = 1 + \frac{1 - \frac{1}{2^n}}{\frac{1}{2}} = 1 + 2 - \frac{1}{2^{n-1}} < 3$$

because, for any $k \geq 1$,

$$\frac{1}{(k+1)!} = \frac{1}{2 \cdots k \cdot (k+1)} \leq \frac{1}{2^k}$$

Thus we see that our sequence is monotone increasing and bounded. Then the least upper bound of its set of values is the limit.

Definition.

$$e = \lim_{n \to \infty} \{1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}\}.$$

Since we saw above that

$$2 < 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} < 3$$

we obtain

$$2 < e < 3.$$

The following proposition tells how to compute approximately the number e.

Proposition 1. *For any k*

$$0 < e - (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!}) < \frac{1}{k!k}.$$

Proof. The fist inequality is obvious since, being an upper bound,

$$e \geq (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{(k+1)!}) > (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!}).$$

In general if $x = \lim_{n \to \infty}\{x_n\}$, then for any k

$$x - x_k = \lim_{n \to \infty}\{x_n - x_k\}.$$

In our case

$$e - x_k = e - (\frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!}) = \lim_{n \to \infty}\{\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots + \frac{1}{n!}\}$$

where we replaced all the terms of the sequence $\{x_n - x_k\}$ for $n \leq k$ by 0 without changing the limit. Since

$$\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots + \frac{1}{n!} = \frac{1}{(k+1)!}(1 + \frac{1}{(k+2)} + \frac{1}{(k+2)(k+3)!} + \ldots + \frac{1}{(k+2)\cdots n}) <$$

$$\frac{1}{(k+1)!}(1 + \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \ldots + \frac{1}{(k+1)^{n-k}}) = \frac{1}{(k+1)!}(\frac{1 - \frac{1}{(k+1)^{n-k+1}})}{1 - \frac{1}{k+1}}) < \frac{1}{(k+1)!}(\frac{k+1}{k}) = \frac{1}{k!k},$$

we obtain

$$e - x_k = \lim_{n \to \infty} \frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots + \frac{1}{n!}\frac{1}{k!k} < \frac{1}{k!k}$$

as asserted.

Thus given any $\epsilon > 0$ if we choose k large enough such that $\frac{1}{k!k} < \epsilon$ we obtain

$$e - 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!} < \epsilon.$$

For example, taking $k = 5$ we obtain

$$e - (2 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120}) = e - \frac{163}{60} < \frac{1}{600}.$$

Corollary. *e is a irrational number.*

Proof. Assume the contrary so that $e = p/q$ for some natural numbers p, q. Obviously $q > 1$ since there are no integers between 2 and 3. Applying Proposition 1 we have

$$0 < \frac{p}{q} - (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}) < \frac{1}{q!q}.$$

Multiplying both sides by $q!$ we get

$$0 < p(q-1)! - (q! + q! + 3 \cdots q + \ldots + 1) < \frac{1}{q} < 1.$$

But this is absurd since a positive integer cannot be less than 1.

You may remember that in Calculus the number e was defined as

$$e = \lim_{n\to\infty} (1 + \frac{1}{n})^n.$$

There is no contradiction. Different sequences may have the same limit. Before we show that e is equal to this limit let me recall (or introduce) the following

Theorem (Binomial Formula). *For any real numbers a, b and a natural number n*

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \ldots + \binom{n}{k} a^{n-k}b^k \ldots + \binom{n}{n-1} ab^{n-1} + b^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k,$$

where for any natural k

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!} \quad \text{if } k > 0, \quad \binom{n}{0} = 1.$$

Proof. We use induction on n. The assertion is obvious for $n = 1$. Assume the formula

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$

is true. We want to show that the formula

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k}b^k$$

is true. We have

$$(a+b)^{n+1} = (a+b)^n(a+b) = a\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k + b\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k}b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1} = \sum_{k=0}^{n} \Big[\binom{n}{k} + \binom{n}{k-1} \Big] a^{n+1-k}b^k.$$

It remains to use the formula

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

This is checked in straightforward way:

$$\binom{n}{k}+\binom{n}{k-1}=\frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!}=\frac{n!(n-k+1)+n!k}{k!(n+1-k)!}=\frac{(n+1)!}{k!(n+1-k)!}=\binom{n+1}{k}.$$

Remark. The numbers $\binom{n}{k}$ (pronounced n choose k) are called *binomial coefficients*. They have the following meaning:

Let X be a non-empty set of n elements and $\mathcal{P}(X)_k=\{A\in\mathcal{P}(X)\mid \#A=k\}$. Then

$$\#\mathcal{P}(X)_k=\binom{n}{k}.$$

In fact, let $X'=X\setminus\{x\}$ where x is any element of X. Then each $A\in\mathcal{P}(X)_k$ is either contains x or does not contain x. In the first case $A\in\mathcal{P}(X')_k$, in the second one, $A=A'\cup\{x\}$ where $A'\in\mathcal{P}(X')_{k-1}$. This imediately implies that

$$\#\mathcal{P}(X)_k=\#\mathcal{P}(X')_k+\#\mathcal{P}(X')_{k-1}.$$

Now, the assertion is obviously true for $n=1$. If we assume that it is true for $n-1=\#X'$ then we get, by using the formula from the proof of the previous Proposition,

$$\#\mathcal{P}(X)_k=\binom{n-1}{k}+\binom{n-1}{k-1}=\binom{n}{k}.$$

By induction on n we are done.

Using this interpretation of binomial coeffcients, we can give another proof of the Binomial Formula. It is clear that the product

$$(a+b)^n=\underbrace{(a+b)\cdots(a+b)}_{n\text{times}}$$

consists of the sum of monomials of the form $a^{n-k}b^k$. Each such monomial is obtained when we designate $n-k$ bracketes from which we pick up a and from the rest we pick up b. Thus

$$(a+b)^n=\sum_{k=0}^{n}c_k a^{n-k}b^k$$

where c_k is equal to the number of choices of a subset of $n-k$ brackets out of the set of n bracketes. But this number is the binomial coeffcients $\binom{n}{k}$.

Now back to our number e.

Proposition 3.

$$e=\lim_{n\to\infty}\{(1+\frac{1}{n})^n\}.$$

Proof. Let $y_n=(1+\frac{1}{n})^n, x_n=1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!}$. Applying the Binomial formula we have

$$y_n=(1+\frac{1}{n})^n=1+\sum_{k=1}^{n}\binom{n}{k}(\frac{1}{n})^k=1+\sum_{k=1}^{n}\frac{n(n-1)\cdots(n-k+1)}{k!}(\frac{1}{n})^k$$

$$=1+\sum_{k=1}^{n}\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k-1}{n})\le 1+\sum_{k=1}^{n}\frac{1}{k!}=\le 1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!}<3.$$

Thus our sequence $\{y_n\}$ is bounded, and if its limit exists then it is $\le e$. Our sequence is also monotone increasing. In fact

$$y_{n+1}=\sum_{k=0}^{n+1}\binom{n+1}{k}(\frac{1}{n+1})^k=1+\sum_{k=1}^{n}\frac{1}{k!}(1-\frac{1}{n+1})(1-\frac{2}{n+1})\cdots(1-\frac{k}{n+1})+(\frac{1}{n+1})^{n+1}$$

$$> 1 + \sum_{k=1}^{n} \frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k-1}{n}) = y_n.$$

Thus the sequence $\{y_n\}$ is convergent.

For any $M \leq n$ set

$$z_n(M) = 1 + \sum_{k=1}^{M-1} \frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k}{n}) = 1 + 1 + \frac{1}{2!}(1-\frac{1}{n}) + \ldots + \frac{1}{M!}(1-\frac{1}{n})\cdots(1-\frac{M-1}{n}).$$

Put $z_n(M) = 0$ if $M > n$. We have

$$y_n = 1 + \sum_{k=1}^{n} \frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k-1}{n}) > z_n(M).$$

Thus

$$\lim_{n\to\infty}\{y_n\} \geq \lim_{n\to\infty}\{z_n(M)\} = \sum_{k=0}^{M} \lim_{n\to\infty}\{\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k}{n})\}$$

$$= \sum_{k=0}^{M} \frac{1}{k!} \lim_{n\to\infty}\{1-\frac{1}{n}\}\ldots\lim_{n\to\infty}\{1-\frac{k}{n}\} = \sum_{k=0}^{n} \frac{1}{k!} = x_M.$$

Since this is true for all M, we get

$$\lim_{n\to\infty}\{y_n\} \geq \lim_{M\to\infty}\{x_M\} = e.$$

Since we have previously showed that $\lim_{n\to\infty}\{y_n\} \leq e$ we are done.

Additional Notes 1. The Euler number e.

Recall that the product of the first n natural numbers $1\cdot 2\cdots n$ is denoted by $n!$. It is called n *factorial*. We set $0! = 1$.

Consider the sequence of rational numbers $\{x_n\}$ where

$$x_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}.$$

Lemma 1. *The sequence $\{x_n\}$ is convergent.*

Proof. Since

$$x_{n+1} = x_n + \frac{1}{(n+1)!}$$

the sequence is monotone increasing. We also have

$$x_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} \leq 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \ldots \frac{1}{2^{n-1}} = 1 + \frac{1-\frac{1}{2^n}}{\frac{1}{2}} = 1 + 2 - \frac{1}{2^{n-1}} < 3$$

because, for any $k \geq 1$,

$$\frac{1}{(k+1)!} = \frac{1}{2\cdots k\cdot(k+1)} \leq \frac{1}{2^k}$$

Thus we see that our sequence is monotone increasing and bounded. Then the least upper bound of its set of values is the limit.

Definition.

$$e = \lim_{n\to\infty}\{1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}\}.$$

Since we saw above that

$$2 < 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} < 3$$

we obtain

$$2 < e < 3.$$

The following proposition tells how to compute approximately the number e.

Proposition 1. *For any k*

$$0 < e - (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!}) < \frac{1}{k!k}.$$

Proof. The fist inequality is obvious since, being an upper bound,

$$e \geq (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{(k+1)!}) > (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!}).$$

In general if $x = \lim_{n\to\infty}\{x_n\}$, then for any k

$$x - x_k = \lim_{n\to\infty}\{x_n - x_k\}.$$

In our case

$$e - x_k = e - (\frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!}) = \lim_{n\to\infty}\{\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots + \frac{1}{n!}\}$$

where we replaced all the terms of the sequence $\{x_n - x_k\}$ for $n \leq k$ by 0 without changing the limit. Since

$$\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots + \frac{1}{n!} = \frac{1}{(k+1)!}(1 + \frac{1}{(k+2)} + \frac{1}{(k+2)(k+3)!} + \ldots + \frac{1}{(k+2)\cdots n}) <$$

$$\frac{1}{(k+1)!}(1 + \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \ldots + \frac{1}{(k+1)^{n-k}}) = \frac{1}{(k+1)!}(\frac{1 - \frac{1}{(k+1)^{n-k+1}})}{1 - \frac{1}{k+1}}) < \frac{1}{(k+1)!}(\frac{k+1}{k}) = \frac{1}{k!k},$$

we obtain

$$e - x_k = \lim_{n\to\infty} \frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \ldots + \frac{1}{n!}\frac{1}{k!k} < \frac{1}{k!k}$$

as asserted.

Thus given any $\epsilon > 0$ if we choose k large enough such that $\frac{1}{k!k} < \epsilon$ we obtain

$$e - 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{k!} < \epsilon.$$

For example, taking $k = 5$ we obtain

$$e - (2 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120}) = e - \frac{163}{60} < \frac{1}{600}.$$

Corollary. *e is a irrational number.*

Proof. Assume the contrary so that $e = p/q$ for some natural numbers p, q. Obviously $q > 1$ since there are no integers between 2 and 3. Applying Proposition 1 we have

$$0 < \frac{p}{q} - (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}) < \frac{1}{q!q}.$$

Multiplying both sides by $q!$ we get

$$0 < p(q-1)! - (q! + q! + 3\cdots q + \ldots + 1) < \frac{1}{q} < 1.$$

But this is absurd since a positive integer cannot be less than 1.

You may remember that in Calculus the number e was defined as

$$e = \lim_{n\to\infty}(1 + \frac{1}{n})^n.$$

There is no contradiction. Different sequences may have the same limit. Before we show that e is equal to this limit let me recall (or introduce) the following

Theorem (Binomial Formula). *For any real numbers a, b and a natural number n*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \ldots + \binom{n}{k}a^{n-k}b^k \ldots + \binom{n}{n-1}ab^{n-1} + b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k,$$

where for any natural k

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n\cdot(n-1)\cdots(n-k+1)}{k!} \quad \text{if } k>0, \quad \binom{n}{0} = 1.$$

Proof. We use induction on n. The assertion is obvious for $n=1$. Assume the formula

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

is true. We want to show that the formula

$$(a+b)^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}b^k$$

is true. We have

$$(a+b)^{n+1} = (a+b)^n(a+b) = a\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k + b\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

$$= \sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1} = \sum_{k=0}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]a^{n+1-k}b^k.$$

It remains to use the formula

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

This is checked in straightforward way:

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!(n-k+1)+n!k}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.$$

Remark. The numbers $\binom{n}{k}$ (pronounced n choose k) are called *binomial coefficients*. They have the following meaning:

Let X be a non-empty set of n elements and $\mathcal{P}(X)_k = \{A \in \mathcal{P}(X) \mid \#A = k\}$. Then

$$\#\mathcal{P}(X)_k = \binom{n}{k}.$$

In fact, let $X' = X \setminus \{x\}$ where x is any element of X. Then each $A \in \mathcal{P}(X)_k$ is either contains x or does not contain x. In the first case $A \in \mathcal{P}(X')_k$, in the second one, $A = A' \cup \{x\}$ where $A' \in \mathcal{P}(X')_{k-1}$. This imediately implies that

$$\#\mathcal{P}(X)_k = \#\mathcal{P}(X')_k + \#\mathcal{P}(X')_{k-1}.$$

Now, the assertion is obviously true for $n=1$. If we assume that it is true for $n-1 = \#X'$ then we get, by using the formula from the proof of the previous Proposition,

$$\#\mathcal{P}(X)_k = \binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}.$$

By induction on n we are done.

Using this interpretation of binomial coeffcients, we can give another proof of the Binomial Formula. It is clear that the product

$$(a+b)^n = \underbrace{(a+b)\cdots(a+b)}_{n\text{times}}$$

consists of the sum of monomials of the form $a^{n-k}b^k$. Each such monomial is obtained when we designate $n-k$ bracketes from which we pick up a and from the rest we pick up b. Thus

$$(a+b)^n = \sum_{k=0}^{n} c_k a^{n-k} b^k$$

where c_k is equal to the number of choices of a subset of $n-k$ brackets out of the set of n bracketes. But this number is the binomial coeffcients $\binom{n}{k}$.

Now back to our number e.

Proposition 3.

$$e = \lim_{n\to\infty}\{(1+\frac{1}{n})^n\}.$$

Proof. Let $y_n = (1+\frac{1}{n})^n, x_n = 1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!}$. Applying the Binomial formula we have

$$y_n = (1+\frac{1}{n})^n = 1+\sum_{k=1}^{n}\binom{n}{k}(\frac{1}{n})^k = 1+\sum_{k=1}^{n}\frac{n(n-1)\cdots(n-k+1)}{k!}(\frac{1}{n})^k$$

$$= 1+\sum_{k=1}^{n}\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k-1}{n}) \le 1+\sum_{k=1}^{n}\frac{1}{k!} =\le 1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!} < 3.$$

Thus our sequence $\{y_n\}$ is bounded, and if its limit exists then it is $\le e$. Our sequence is also monotone increasing. In fact

$$y_{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}(\frac{1}{n+1})^k = 1+\sum_{k=1}^{n}\frac{1}{k!}(1-\frac{1}{n+1})(1-\frac{2}{n+1})\cdots(1-\frac{k}{n+1})+(\frac{1}{n+1})^{n+1}$$

$$> 1+\sum_{k=1}^{n}\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k-1}{n}) = y_n.$$

Thus the sequence $\{y_n\}$ is convergent.

For any $M \le n$ set

$$z_n(M) = 1+\sum_{k=1}^{M-1}\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k}{n}) = 1+1+\frac{1}{2!}(1-\frac{1}{n})+\ldots+\frac{1}{M!}(1-\frac{1}{n})\cdots(1-\frac{M-1}{n}).$$

Put $z_n(M) = 0$ if $M > n$. We have

$$y_n = 1+\sum_{k=1}^{n}\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k-1}{n}) > z_n(M).$$

Thus

$$\lim_{n\to\infty}\{y_n\} \ge \lim_{n\to\infty}\{z_n(M)\} = \sum_{k=0}^{M}\lim_{n\to\infty}\{\frac{1}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\cdots(1-\frac{k}{n})\}$$

$$= \sum_{k=0}^{M}\frac{1}{k!}\lim_{n\to\infty}\{1-\frac{1}{n}\}\ldots\lim_{n\to\infty}\{1-\frac{k}{n}\} = \sum_{k=0}^{n}\frac{1}{k!} = x_M.$$

Since this is true for all M, we get

$$\lim_{n\to\infty}\{y_n\} \ge \lim_{M\to\infty}\{x_M\} = e.$$

Since we have previously showed that $\lim_{n\to\infty}\{y_n\} \le e$ we are done.