Paweł Czyż

Mathematical Physics

November 22, 2018

Contents

Part I Sets and categories

Part I

Sets and categories

1

Propositional calculus and sets

To be able to formulate and prove theorems, we need a language. In this chapter we learn propositional calculus and naive set theory, language in which most of the mathematics is expressed. Our treatment will not be exhaustive in any ways.

1.1 Propositional calculus

1.1.1 New sentences from old

Consider declarative sentences as "It's raining in Oxford now." or "$2+2=5$" that can be either true or false. There are many ways how to construct new sentences and decide whether they are true or not.

Definition 1.1. *Consider sentences p and q. We say that they* ***are equivalent*** *(we write then $p \Leftrightarrow q$) if they are either true or false simultaneously. If p and q are equivalent, we usually say "p if and only if q" of even "p iff q".*

Example 1.2. Sentences "Each square is a rectangle" and "$2+2=3+1$" are both true, so trivially they are equivalent.

Example 1.3. Let p be a sentence "There is an odd number of people in this room." and q be "If one person enters the room, then the number of people becomes even". We *do not know* if *any* of these sentences is true - it would require to count all the people in the room! But if p is true, then also q must be true and vice versa - if q is true, then also p must be true. Therefore we can say that p and q are equivalent, or write $p \Leftrightarrow q$.

Exercise 1.4. Prove that $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$. [Hint[1]]

[1] What does the sentence in the first bracket mean? What about the second? Why are they equivalent?

Exercise 1.5. Prove that if we know that $p \Leftrightarrow q$ and we know that $q \Leftrightarrow r$, then also $p \Leftrightarrow r$.

Definition 1.6. *Consider sentences p and q. We say that their* ***conjunction*** *$p \wedge q$ is true iff both of them are true. Usually conjunction of p and q is referred as "p and q".*

Example 1.7. Sentence: "$(2+2=5)$ and $(2+1=3)$" is false, as one of them (namely, the first one) is false.

Exercise 1.8. Let p and q be two sentences. Prove that $p \wedge q$ is true if and only if $q \wedge p$ is true. As we can swap two elements, we say that conjunction is **commutative**.

Exercise 1.9. Let p, q, r be three sentences. Prove that $(p \wedge q) \wedge r$ is true if and only if $p \wedge (q \wedge r)$ is true. Such a property is called **associativity** and implies that we do not need to specify the order of calculation. Therefore we can write just $p \wedge q \wedge r$ without writing brackets.

Definition 1.10. *Consider sentences p and q. We say that their* ***disjunction*** *$p \vee q$ is true if and only if at least one of them is true. Usually disjunction of p and q is referred as "p or q".*

Example 1.11. Sentences "$(2+1=3)$ or $(2+1=4)$" and "$(2+1=3)$ or $(3-1=2)$" are both true while "$(2+1=4)$ or $(1+1=1)$" is false.

Exercise 1.12. Prove that disjunction is both associative and commutative.

Definition 1.13. ***Negation*** *of p is a sentence $\neg p$ such that $\neg p$ is true if and only if p is false. Usually we refer to $\neg p$ as "not p".*

Exercise 1.14. Prove that $\neg p$ is false if and only if p is true.

Now we will think about proof strategies. Sometimes there is an elegant way how to prove that two statements are equivalent (like in the proof of associativity of conjunction, one can see that both sentences are true iff all three basic sentences are true), but in case of more complicated sentences, it may be hard to find it. A common proof strategy is a **truth table** approach: we list in a table all the values that each basis sentence can take and evaluate the value of final expression. Then *two sentences are equivalent iff they have the same truth tables.*

Example 1.15. Truth table for conjunction:

p	q	$p \wedge q$
t	t	t
t	f	f
f	t	f
f	f	f

where t stands for "true" and f stands for "false".

This is a very powerful approach, as it requires no clever tricks but a simple calculation. The only problem is the number of calculations, that grows very quickly with the number of basic sentences!

Exercise 1.16. Assume that you have built a sentence using n sentences: $p_1, p_2, \ldots, p_n$. How many rows does the truth table contain?

Exercise 1.17. Prove **distributivity**:

1. $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$
2. $(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$

Exercise 1.18. Prove **De Morgan's laws**:

1. $\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$
2. $\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$

Definition 1.19. *We say that p **implies** q (or that q **is implied by** p) for a sentence $p \Rightarrow q$ that is false iff p is false and q is true. We can summarise it in a truth table:*

p	q	$p \Rightarrow q$
t	t	t
t	f	f
f	t	t
f	f	t

As you can see, it's a strange behaviour - false implies everything!

Exercise 1.20. Prove that $(p \Rightarrow q) \Leftrightarrow ((\neg p) \vee q)$. [Hint[2]]

Exercise 1.21. Prove that implication is **transitive**, that is

$$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r).$$

Exercise 1.22. Assuming that every topological space is homeomorphic to itself and that homeomorphic spaces are homotopic, prove that every topological is homotopic to itself. [Hint[3]].

You may have discovered a similarity between symbols "$\Leftrightarrow$" and "$\Rightarrow$" - it's not an accident as you can prove!

Exercise 1.23. Prove that $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$.

[2] left sentence is false for very specific p and q. Do you need to write down all four rows in the truth table of the right-hand-side sentence?

[3] You don't need to know what the terms here mean to solve this exercise (but eventually will reach them!)

1.1.2 Quantifiers

Consider a sentence[4] $P(n)$ involving an object n (for example n can be an integer and $P(n)$ can be a sentence "$n = 2n$").

Definition 1.24. *We define the **universal quantifier** as a sentence $\forall_n P(n)$ meaning "for all n, the formula $P(n)$ holds". We define the **existential quantifier** as a sentence $\exists_n P(n)$ meaning "there exists n such that $P(n)$ holds"* [5]*.*

Example 1.25. In the case of $P(n)$ meaning "$2n = n$", the sentence $\forall_n P(n)$ is false (as for $n = 1$ we have $2 \cdot 1 \neq 1$) but the sentence $\exists_n P(n)$ is true, as $2 \cdot 0 = 0$.

Intuitively, it is a much simpler problem to give an example of an object with a special property, than proving that *every* object has a property. In the above example, we gave an example disproving the statement. It may be useful to convert between these quantifiers. As you can prove:

Exercise 1.26. Prove that:

1. $\neg\forall_n P(n) \Leftrightarrow \exists_n \neg P(n)$
2. $\neg\exists_n P(n) \Leftrightarrow \forall_n \neg P(n)$

What do the above state in English?

1.1.3 Mathematical induction

In this section we practice our abilities on the *mathematical induction principle*. Although very simple, this method appears in many proofs in mathematics. Before we define this, we need a simple definition to provide us with many examples:

Definition 1.27. *If $a \neq 0$ and b are integers, we say that a **divides** b iff there exists $k \in \mathbb{Z}$ such that $b = ak$. We can also write this as $a|b$ or say that b **is divisible by** a.*

Example 1.28. $2 \,|\, 84$ as $84 = 2 \cdot 42$.

Exercise 1.29. Let $0 \neq k \in \mathbb{Z}$ divide a and b. Prove that:

1. $k \,|\, a + b$,
2. $k \,|\, a - b$,
3. $k^2 \,|\, ab$.

[4] For experts: In fact we are dealing with a set of sentences.

[5] $\forall$ is a rotated "A" symbolising "for **A**ll" and $\exists$ is a rotated "E" symbolising "**E**xists"

Theorem 1.30. ***Mathematical induction principle*** *Let $P(n)$ be a sentence about a natural number n. If:*

1. *$P(0)$ is true, and*
2. *for every natural k the implication $P(k) \Rightarrow P(k+1)$ is true,*

then $P(n)$ is true for all natural numbers n.

This can be visualised with a row of dominoes. To be sure that all of them eventually fall:

1. hit the first domino
2. the dominoes are set in such manner that if kth domino falls, then it hits the $(k+1)$th.

Example 1.31. We'll prove that $2 \mid n(n+1)$ for every $n \in \mathbb{N}$.

1. The statement is true for 0 as $2 \mid 0 \cdot (0+1)$,
2. I need to prove that $(2 \mid n(n+1)) \Rightarrow (2 \mid (n+1)(n+2))$ for every n.

Assume that n is such a number that $2 \mid n(n+1)$. Then

$$(n+1)(n+2) = n(n+1) + 2 \cdot (n+1)$$

is divisible by 2 as well.

Using the principle of mathematical induction we see that for every natural n, the number $n(n+1)$ is divisible[6] by 2.

Exercise 1.32. Prove that $2^n > n$ for every natural number n.

You can also modify slightly the induction principle - sometimes you should start with number different than 0 or use different induction step (start 0 and step 2 can lead to theorems valid for even numbers, step 0 and steps 1 and -1 can lead to theorems valid for all integers...)

Exercise 1.33. 1. Prove[7] that 6 divides $n^3 - n$ for all natural n.
2. Prove[8] that 6 divides $n^3 - n$ for all integers n. You can use a slight modification mathematical induction principle proving the implication „if the theorem works for n, it works also for $n-1$".

Exercise 1.34. (Bernoulli's inequality) Prove that for every real $x > -1$ and every natural $n \geq 1$, the following inequality holds:

$$(1+x)^n \geq 1 + nx.$$

[6] There is also an alternative proof: it's a product of two consecutive numbers - one of them is divisible by 2 and so is the product.

[7] Another method is to notice that $n^3 - n = (n-1) \cdot n \cdot (n+1)$. Why 2 does divide it? Why 3?

[8] How $n^3 - n$ and $(-n)^3 - (-n)$ are related? Does this simplify the proof?

Exercise 1.35. In a country there are $n \geq 2$ cities. Between each pair of them there is a *one-way* road.

1. Prove that there is a city from which you can drive to all the other cities. [Hint[9]]
2. Prove that there is a city to which you can drive from all the others. [Hint[10]].

1.2 Basic set theory

In modern mathematics we do not define a set or set membership, but rather believe that there exists objects with properties that are listed in this chapter. Heuristically you can think that a set A is a "collection of objects" and a sentence "$x \in A$" means that the object x is inside this collection. We read this as "x belongs to set A" or "x is an element of A". We write $x \notin A$ as a shorthand for $\neg(x \in A)$ (and it means that x is *not* an element of A).

Example 1.36. Consider a library with closed stack and with a webpage. You can check whether there is a specific book inside it - so you can know for example that "Alice's Adventures in Wonderland" is in the stack, but you don't know how many copies there are. Moreover you can't ask about place of the books - there is no concept as being "first" or "second" element, as we can't check the physical stack.

As we can discover, there are collections of objects that do not form a set:

1.1. Russel's paradox Let X be a set built from all sets such that $A \notin A$. Prove that X does not exist. [Hint[11]]

Therefore we need to assume the existence of a few sets, and then construct new out of them using some rules in which we believe. We assume that there exist:

1. finite sets (like real libraries with finite number of books). These are written as $\{a_1, a_2, \dots, a_n\}$. Empty set is written as $\varnothing$ rather than $\{\}$.
2. real numbers[12] $\mathbb{R}$
3. natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$

---

[9] Assume that the hypothesis works for some n and any country with n cities. Now consider an arbitrary $n+1$-city country. Hide one city and use your assumption.

[10] Nice trick: what does happen if you reverse each way? Can you use the former result?

[11] What if $X \in X$? What if $X \notin X$?

[12] You may feel a bit insecure - what are real numbers, integers and so on? We haven't defined them properly yet. We will defer the construction of them to later sections, as what really matters are they *properties* that you learned in elementary school.

4. integers $\mathbb{Z}$
5. rational numbers $\mathbb{Q}$

Having a few sets, we define a few rules how to compare them and construct new sets out of them:

Definition 1.37. ***Axiom of extensionality (Equality of sets)*** *We say that two sets A, B are* **equal** *iff they have the same elements, that is:*

$$A = B \Leftrightarrow \forall_x (x \in A \Leftrightarrow x \in B).$$

Definition 1.38. *We say that A* ***is a subset of*** *B iff every element of A is also in B, that is:*

$$A \subseteq B \Leftrightarrow \forall_a (a \in A \Rightarrow a \in B).$$

If A is a subset of B, we also say that B ***is a superset*** *of A.*

This is a good opportunity to slightly modify our quantifier notation - usually we will be interested in objects belonging to some sets. Formula

$$\forall_{a \in A} P(a)$$

means "for all $a \in A$, statement $P(a)$ is true" and

$$\exists_{a \in A} P(a)$$

means "there is an $a \in A$ such that $P(a)$ holds".

Example 1.39. We can write $A \subseteq B \Leftrightarrow \forall_{a \in A} a \in B$.

Exercise 1.40. Let A and B be two sets. Prove that $A = B$ iff A is a subset of B and B is a subset of A.

Exercise 1.41. Here we will prove that the empty set is a unique set with special property of being a subset of every set:

1. Prove that for every set A, $\varnothing \subseteq A$.
2. Let θ be a set such that $\theta \subseteq A$ for every set A. Prove that $\theta = \varnothing$.

1.2.1 New sets from old

At the moment we do not have many sets. Let's try to define some methods of creating new sets from the know ones:

Definition 1.42. ***Axiom schema of specification*** *Consider a set A and a statement that assigns a truth value $P(a)$ to each $a \in A$. We can select elements a for which formula $P(a)$ is true and create a set*[13]*:*

$$\{a \in A : P(a)\}.$$

[13] Some authors write $\{a \in A \,|\, P(a)\}$

Example 1.43. We assumed that the set $\mathbb{R}$ (of real numbers) exist. We can construct the empty set using the axiom schema of specification:

$$\varnothing = \{r \in \mathbb{R} : r = r + 1\}.$$

The above axiom schema of specification is important - using this we can prove that there is no set of all sets:

Exercise 1.44. Prove that there is *no* set of all sets. [Hint[14]]

Although is is impossible to create the set of all sets, it is possible to create *some* sets of sets.

Definition 1.45. ***Axiom of power set*** *Consider a set A. We assume that there exists* [15] ***the power set of*** *A defined as a set of all subsets of A:*

$$\mathcal{P}(A) := \{A' : A' \subseteq A\}.$$

That is $A' \in \mathcal{P}(A)$ iff $A' \subseteq A$.

Exercise 1.46. Using the axiom of power set and the axiom schema of specification, justify the notation:

$$\{A' \subseteq A : P(A')\},$$

where $P(A')$ assigns true or false to each subset A' of A.

Exercise 1.47.
1. Let $A = \{1, 2, 3\}$. Find it's power set $\mathcal{P}(A)$. What is the number of elements in $\mathcal{P}(A)$? How is it related to the number of elements of A?
2. Let A be a finite set with n elements. Prove that $\mathcal{P}(A)$ has 2^n elements. Do you see why some authors write 2^A for $\mathcal{P}(A)$? [Hint[16]]

Definition 1.48. *By a* ***collection of sets*** *or* ***family of sets*** *we understand a set of some sets.*

Definition 1.49. ***Axiom of union*** *Assume that we are given a family of sets A. There is a set called their* ***union***[17]*:*

$$\bigcup \mathcal{A} = \{x : \exists_{X \in \mathcal{A}} x \in X\}.$$

If the family of sets is indexed by some index, that is: $\mathcal{A} = \{A_i : i \in I\}$, we can also write:

$$\bigcup_{i \in I} A_i := \bigcup \mathcal{A}.$$

[14] Assume there is one and select some elements to create Russel's paradox.

[15] We cannot create it using the axiom schema of specification, as there is no set from which we could select subsets of A. But since now, we can do it.

[16] Every subset is specified by elements that are inside it. For every element you have two options - to select it or not.

[17] Again, we cannot use the axiom schema of specification as there is no set containing *everything*.

Exercise 1.50. Let A, B and C be sets. Prove that:

1. union defined as $A \cup B = \{x : x \in A \vee x \in B\}$ agrees with $\bigcup\{A, B\}$
2. $A \cup B = B \cup A$ (so union is commutative)
3. $(A \cup B) \cup C = \bigcup\{A, B, C\}$
4. $(A \cup B) \cup C = A \cup (B \cup C)$ (this is called associativity)
5. $A \cup A = A$

Definition 1.51. ***Set difference*** *Let A and B be two sets. We define their **difference**:*

$$A \setminus B := A - B := \{a \in A : a \notin B\}$$

Example 1.52. Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Then $A \setminus B = \{1\}$.

Exercise 1.53. Is $(A \setminus B) \cup B$ always equal to A?

Exercise 1.54. Let A and B be sets. Prove that $A \subseteq (A \setminus B) \cup B$, where the equality holds iff $B \subseteq A$.

Definition 1.55. *Consider a family of sets $\mathcal{A}$. We define their **intersection** as a set:*

$$\bigcap \mathcal{A} = \left\{x \in \bigcup \mathcal{A} : \forall_{X \in \mathcal{A}}\, x \in X\right\}.$$

If the family of sets is indexed by some index, that is: $\mathcal{A} = \{A_i : i \in I\}$, we can write:

$$\bigcap_{i \in I} A_i := \bigcap \mathcal{A}.$$

Exercise 1.56. Find sum and intersection of family of subsets of $\mathbb{R}$:

$$A_r = \{r, -r\}$$

for $r \geq 0$.

Exercise 1.57. Let A, B, C be sets. Writing $A \cap B := \bigcap\{A, B\}$, prove that:

1. $A \cap B = B \cap A$ (commutativity)
2. $A \cap (B \cap C) = (A \cap B) \cap C$ (associativity)
3. $A \cap A = A$

Exercise 1.58. Prove distributivity:

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

1.2.2 Subsets and complements

Definition 1.59. *Let A be subset of a set U. We say that* ***the complement***[18] ***of*** *A is a set $A^c = U \setminus A$.*

1.2. Prove the following set identites:

1. Let $A \subseteq U$. Prove that $(A^c)^c = A$.
2. Let A, $B \subset U$. Prove that $(A \cup B)^c = A^c \cap B^c$
3. Let A, $B \subset U$. Prove that $(A \cap B)^c = A^c \cup B^c$

1.3. Let $\mathcal{X} \subseteq \mathcal{P}(U)$ be a family of sets and define: $\mathcal{Y} = \{X^c \subseteq U : X \in \mathcal{X}\}$, where $X^c = U \setminus X$. Prove that:

1. $(\bigcup \mathcal{X})^c = \bigcap \mathcal{Y}$
2. $(\bigcap \mathcal{X})^c = \bigcup \mathcal{Y}$

Exercise 1.60. Let $A \subseteq X_i$ for $i \in I$. Prove that

$$A \subseteq \bigcap_{i \in I} X_i$$

Exercise 1.61. For every point $a \in A$ there is a set $U_a \subseteq A$ such that $a \in U_a$. Prove that

$$A = \bigcup_{a \in A} U_a.$$

1.2.3 Cartesian product

First of all, we need a useful concept:

Definition 1.62. *We define* ***an ordered pair*** *or* ***a 2-tuple*** *as*

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

Exercise 1.63. Prove that $(a, b) = (a', b')$ iff $a = a'$ and $b = b'$.

Exercise 1.64. Prove that $(a, (b, c)) = (d, (e, f))$ iff $a = d \wedge b = e \wedge c = f$.

Definition 1.65. ***An ordered** n**-tuple*** *or simply* ***a tuple*** *is defined as:*

$$(a_1, a_2, \dots, a_n) := (a_1, (a_2, (..., a_n)) \dots).$$

It's single most important property is that:

$$(a_1, a_2, \dots, a_n) = (a'_1, a'_2, \dots, a'_n)$$

iff $a_1 = a'_1, a_2 = a'_2, \dots, a_n = a'_n$.

[18] We need to refer to some U that usually will be clear out from the context.

In fact the property is much more important than the explicit construction. For example we could define a 3-tuple as $((a, b), c)$ instead of $(a, (b, c))$ and the property would still hold! But one needs to be careful about the notation, as shows the next exercise.

Exercise 1.66. Check that, in terms of sets, $(a, (b, c)) \neq ((a, b), c)$, so formally we do need to stick to one convention for (a, b, c).

Definition 1.67. *Let A and B be sets. Then we assume that their* ***Cartesian product*** *exists:*

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Exercise 1.68. Prove that Cartesian product is *not* commutative (that is $A \times B \neq B \times A$ in general).

Exercise 1.69. Prove that in general $(A \times B) \times C \neq A \times (B \times C)$, so Cartesian product is *not* associative and an expression $A \times B \times C$ is ambiguous.

Later we will formally address this issue[19]. As it is easy to identify $((a, b), c)$ with $(a, (b, c))$, many authors do this identification without saying this explicitly.

1.3 Relations

Having defined Cartesian product, we can consider subsets of it. It will lead to two new, important concepts - relations and functions.

Definition 1.70. *A* ***relation*** *R* ***between sets*** *X and Y is a subset of $X \times Y$. If $(x, y) \in R$ we write $x \, R \, y$. A* ***relation on a set*** *X is a subset of $X \times X$.*

Example 1.71. Consider the order of natural numbers (that is $0 < 1$, $1 < 2$, $2 < 3$ and so on). It is in fact a relation on $\mathbb{N}$: $a < b$ means exactly $(a, b) \in < \subseteq \mathbb{N} \times \mathbb{N}$ and is defined as:

$$<:= \bigcup_{n \in \mathbb{N}} \bigcup_{i \in \mathbb{Z}^+} \{(n, n + i)\}, \text{ where } \mathbb{Z}^+ = \{n \in \mathbb{N} : n \neq 0\}.$$

Exercise 1.72. What is "the smallest" relation between X and Y (in such sense that is a subset of *every* relation between X and Y)? What is "the biggest" one (every relation is a subset of the biggest one)?

Exercise 1.73. Let X and Y be any sets. Prove that there exists the **set** of all relations between X and Y. [Hint[20]]

[19] For experts: With the help of natural isomorphisms, a concept from the category theory

[20] Use the power set.

Exercise 1.74. Let X and Y be finite sets. How many relations can be defined between them?

Among all the relations on a set X, we have some with very nice behaviour.

Definition 1.75. *Let $\equiv$ be a relation on X. We say that it is an **equivalence relation** if all of the following hold:*

1. *if $x \equiv y$ and $y \equiv z$, then also $x \equiv z$ (transitivity)*
2. *if $x \equiv y$, then $y \equiv x$ (symmetry)*
3. *$x \equiv x$ for every x (reflexivity)*

Example 1.76. Consider any set X. Then a set

$$\mathrm{Id}_X := \{(x, x) \in X \times X : x \in X\}$$

is an equivalence relation on X.

Exercise 1.77. Prove that $n \equiv m$ iff n and m have the same parity is an equivalence relation on $\mathbb{Z}$.

As you may have noticed, using the equivalence relation with partition the set into some subsets.

Definition 1.78. *Let $X \neq \varnothing$ be a set. We say that a family of subsets $\mathcal{A} \subseteq \mathcal{P}(X)$ **partitions** X iff:*

1. *$\varnothing \neq X$*
2. *$\bigcup \mathcal{A} = X$ (every element is somewhere)*
3. *for $A, A' \in \mathcal{A}$ we have either $A = A'$ or $A \cap A' = \varnothing$ (partitioning sets are pairwise disjoint)*

*Elements of $\mathcal{A}$ are called **equivalence classes**. If $a \in A \in \mathcal{A}$, we write $[a] := A$.*

Why do we call it equivalence classes? Is it somehow related to equivalence relations?

Exercise 1.79. Here you will prove the fundamental relationship between partitions and equivalence relations.

1. Prove that if we have a parition on X, then the relation given by: $x \equiv y$ iff x and y belong to the same equivalence class, is an equivalence relation on X.
2. Let $\equiv$ be an equivalence relation on X. Prove that $\{[x] : x \in X\}$ is a partition on X, where $[x] = \{y \in X : y \equiv x\}$

The partition of X corresponding to relation $\equiv$ is written as $X/\equiv$.

Exercise 1.80. Consider an equivalence relation $\equiv$.

1. Prove that $[a] = [b]$ iff $a \equiv b$.
2. Prove that $[a] \cap [b] = \varnothing$ iff $a \not\equiv b$.

This means that equivalence classes can be either identical or disjoint (what is not surprising as equivalence classes form a partition).

Exercise 1.81. Let X be a set with n elements and q be the number of possible equivalence classes on X. Prove that

$$n \leq q \leq 2^{n^2} - 1.$$

[Hint[21]]

Usually our sets will be equipped with some additional structure - for example integers can be added together. Sometimes we can move this structure to the equivalence classes. Let's start by finding a nice equivalence class on them.

Example 1.82. **Modulo arithmetics** Let p and q be integers. $p \,|\, q$ means that p divides q (there exists a $m \in \mathbb{Z}$ such that $q = pm$). We fix a non-zero number $p \in \mathbb{Z}$ and define **equivalence modulo** p:

$$m \equiv_p n \Leftrightarrow p \,|\, m - n.$$

It's easy to check that this is an equivalence relation. We would like to define a sum on the set of equivalence classes. Let's try to do this intuitively:

$$[m] + [n] := [m + n].$$

Although it looks right, we need to check whether this definition is independent on the chosen representatives! So let's $m \equiv_p m'$ and $n \equiv_p n'$. We would like to show that $m + n \equiv_p m' + n'$. In other words, we want p to divide $(m+n) - (m'+n')$, what is true as $(m+n) - (m'+n') = (m - m') + (n - n')$, that is a sum of numbers divisible by p.

Analogously one can define multplication and subtraction to get the modulo arithmetics known from elementary number theory.

Exercise 1.83. Construction of rationals

1. Let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Consider $X = \mathbb{Z} \times \mathbb{Z}^*$. Prove that relation $\equiv$ on X given as: $(m, n) \equiv (p, q) \Leftrightarrow mq = pn$ is an equivalence relation.
2. To simplify notation, we will write $[m, n]$ for $[(m, n)] \in X/\equiv$. Prove that the following operations do not depend on class representatives:
   a) $[m, n] + [p, q] := [mq + np, nq]$
   b) $[m, n] \cdot [p, q] := [mp, nq]$
3. Prove that:

[21] For $n \geq 2$ construct n equivalence relations with two classes.

a) $[m,n] = [am, an]$
b) $[0,1] + [m,n] = [m,n]$
c) $[1,1] \cdot [m,n] = [m,n]$
d) $[m,n] + [-m,n] = [0,1]$
e) if $[a,b] \neq [0,1]$, then $[a,b] \cdot [b,a] = [1,1]$

4. Consider any rational numbers m/n and p/q. What equivalence classes do they correspond to? What is their sum and product? Do you see now how we can construct rationals using integers only?

The last example and exercise showed us how to move algebraic structures from one set to another (usually corresponding to equivalence classes of some relation). In fact one can define integers using natural numbers only[22] or reals from rationals[23].

1.4 Functions

Definition 1.84. *Consider two sets A and B. We say that a relation f (that is a subset $f \subseteq A \times B$) is a* ***function*** *iff the following two conditions hold:*

- *for every element $a \in A$ there is an element $b \in B$ such that $(a,b) \in f$*
- *if $(a,b) \in f$ and $(a,c) \in f$, then $b = c$*

Therefore for each $a \in A$ there is exactly one $b \in B$ such that $(a,b) \in f$. Such b will be called ***value of*** *f* ***at point*** *a and given a symbol $f(a)$. We will frite $f : A \to B$ for f and call A the* ***domain of*** *f and B the* ***codomain of*** *f.*

Being very concise we can also write f as

$$f : A \ni a \mapsto f(a) \in B.$$

Note that we use two different arrows.

Example 1.85. $f : \mathbb{N} \to \mathbb{R}$ given by $f(n) = n^2$. We can also write:

$$f : \mathbb{N} \ni n \mapsto n^2 \in \mathbb{R}.$$

Example 1.86. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^{10} + x^2 - 1$.

Example 1.87. $f : X \to \mathcal{P}(X)$ given by $f(x) = \{x\}$.

Exercise 1.88. Let X and Y be two sets. Prove that there exists a set of all functions from X to Y. [Hint[24]]

[22] This is even simpler - our equivalence classes are 1-element. Consider $\mathbb{N} \times \{0,1\}$ with $(n,0)$ corresponding to n and $(n,1)$ corresponding to $-n$. Figure how to define addition, subtraction and multiplication. Later we will also discover how to construct reals from rationals.

[23] This actually involves equivalence classes, put on sequences of rationals. We will investigate this construction later.

[24] You can form a set of all relations between X and Y. How are functions related to relations?

Exercise 1.89. How many[25] are there functions from the empty set to $\{1, 2, 3, 4\}$? [Hint[26]]

Exercise 1.90. Here, we will prove a simple inequality using a set-theoretic reasoning. Let X and Y be finite sets, with numbers of elements, respectively, $x = |X|$ and $y = |Y|$.

1. Prove that the number of relations between X and Y is 2^{xy}.
2. Prove that the number of functions from X to Y is y^x. [Hint[27]]
3. Prove that for every non-zero natural numbers x and y the following holds:

$$y^x < 2^{xy}.$$

Exercise 1.91. Let X and Y be any two sets. Prove that you can create the set of all functions from X to Y. Sometimes it is called Y^X. Do you know why?

Exercise 1.92. Consider a function $f : X \to X'$ and assume that there is an equivalence relation R' on X'. We will try to define a natural (in some sense) equivalence relation on X.

1. Define a relation R on X as $xRy \Leftrightarrow f(x)R'f(y)$. Prove that it is an equivalence relation.
2. Consider $r : X \to X/R$ and $r' : X' \to X'/R'$ given by $r(x) = [x]_R$ and $r'(x') = [x']_{R'}$ and inverse function.

Exercise 1.93. Let $f : A \to B$ and $C \subseteq D \subseteq A$. We define: $f[C] = \{b \in B : b = f(c) \text{ for some } c \in C\}$ and analogously $f[D]$. Prove that $f[C] \subseteq f[D]$.

Definition 1.94. *Consider a set X. We say that it's **identity function** is $f : X \to X$ given by $f(x) = x$ for all $x \in X$.*

1.4.1 Injectivity, surjectivity and bijectivity

As we have already seen, there may be some elements in codomain that are not values of f. Such a set is important enough to be given a name:

Definition 1.95. *Let $f : A \to B$ be a function. **The image of** f is a set:*

$$Im\, f = \{b \in B : \text{there is } a \in A \text{ such that } b = f(a)\}.$$

*We say that the function $f : A \to B$ is **surjective** (or **onto**) iff $Im\, f = B$.*

1.4. As we remember, $\mathbb{R}$ stands for real numbers. Are the following functions surjective?

---

[25] Thanks to Antek Hanke

[26] What is a function in set-theoretical terms?

[27] For first element in X you have y possibilities to choose from.

1. $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^3$
2. $g : \mathbb{R} \to \mathbb{R},\ g(x) = x^2$
3. $h : \mathbb{R} \to \{5\}$

Definition 1.96. *Let $f : A \to B$ be a function. If f gives distinct values to distinct arguments (that is, if $f(a) = f(b)$, then $a = b$), we say that the function is **injective** (or **one-to-one**).*

Exercise 1.97. Are the following functions injective?

1. $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$
2. $h : \{0, 1, 2, 3\} \to \mathbb{R},\ h(x) = x$

Exercise 1.98. Let f be a function from A to B. Prove that there exists a function $g : \operatorname{Im} B \to A$ such that $g \circ f = \mathrm{Id}_A$ iff f is injective.

Exercise 1.99. Let $f : A \to B$ and $g : B \to C$ be functions such that $g \circ f$ is injective but g is not. Why isn't f surjective?

Definition 1.100. *If a function f is both surjective and injective, we say that is **bijective**[28].*

Exercise 1.101. Construct a function that is:

1. surjective, but not injective
2. injective, but not surjective
3. neither injective nor surjective
4. bijective

Notice that if a function $f : A \to B$ is bijective, then we can construct a function $g : B \to A$ such that $f(g(b)) = b$ and $g(f(a)) = a$.

Exercise 1.102. Prove that, if exists, g is unique.

Definition 1.103. *Consider a bijective function $f : X \to Y$. We say that it's **inverse function** $f^{-1} : Y \to X$ iff:*

$$f^{-1}(f(x)) = x, f(f^{-1}(y)) = y,$$

for all $x \in X$, $y \in Y$.

We call this function **the inverse function**[29]: $g = f^{-1}$.

Exercise 1.104. Assume that f^{-1} exists. Prove that $(f^{-1})^{-1}$ exists and is equal to f.

[28] If you prefer nouns: surjective function is called a surjection, injective - injection and bijective - bijection

[29] It becomes confusing when working on real numbers: $f^{-1}(x)$ is **not** $(f(x))^{-1} = 1/f(x)$

1.4.2 Function composition

If we have two functions: $f : A \to B$ and $g : B \to C$, we can construct the **composition** using formula: $g \circ f : A \to C,\ (g \circ f)(a) = g(f(a))$.

Exercise 1.105. For two relations $R \subseteq X \times Y$ and $T \subseteq Y \times Z$ we define their composition as

$$R \circ T = \{(x, z) \in X \times Z : \exists_{y \in Y} (x, y) \in R \land (y, z) \in T\}.$$

Prove that if R and T are functions, this leads to the "normal" definition of function composition.

Exercise 1.106. Find functions $f,\ g$ such that:

1. $g \circ f$ exists, but $f \circ g$ is not defined
2. both $f \circ g$ and $g \circ f$ exist, but $f \circ g \neq g \circ f$

Although function composition is not commutative, it is associative:

Exercise 1.107. Left $f : A \to B, g : B \to C, h : C \to D$. Prove that

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

Therefore we can ommit the brackets and write just $h \circ g \circ f$. We will use function composition very often.

Exercise 1.108. 1. Prove that composition of two surjections is surjective.
2. Prove that composition of two injections is injective.
3. Prove that composition of two bijections is bijective.

Definition 1.109. *We will rephrase the definition of the inverse function using the identity function*[30]*:*

consider a function $f : X \to Y$. If there exists a function $f^{-1} : Y \to X$ such that:

$$f^{-1} \circ f = Id_X, f \circ f^{-1} = Id_Y,$$

*we say that f^{-1} if **the inverse** to f.*

Exercise 1.110. Let $f : A \to B$ be an injection. Prove that there is a function $g : \mathrm{Im}\, f \to A$ such that $g \circ f = \mathrm{Id}_A$. Such g is called **left inverse of** f.

[30] For a set X, it's identity function is

$$\mathrm{Id}_X = \{(x, x) \in X \times X : x \in X\}.$$

1.5 Cardinality

1.5.1 Finite sets

Definition 1.111. *The* ***cardinality*** $|X|$ *of a finite set* X *is defined as the number of elements in* X*.*

Example 1.112. Let $A = \{0, 1, 2, 3\}$. Then $|A| = 4$.

Exercise 1.113. What is the cardinality of $\{a, a+1, a+2, \ldots, a+n\}$?

Theorem 1.114. ***Inclusion-exclusion principle*** *If* X *and* Y *are finite sets, then:*

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Intuitively, adding two sets we count elements in each set twice and then subtract the number of elements that were counted twice. The formal proof goes as follows:

Exercise 1.115. Prove the inclusion-exclusion principle:

1. Let X and Y be finite, disjoint (that is $X \cap Y = \varnothing$) sets. Prove that:
$$|X \cup Y| = |X| + |Y|.$$
2. Prove that for $A \subseteq X$, where X is finite, we have $|X \setminus A| = |X| - |A|$. [Hint[31]]
3. Prove that
$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$
for finite sets X, Y (now we don't assume that they are disjoint). [Hint[32]]

Exercise 1.116. Prove that if $B \subseteq A$, and A is finite, then $|B| \leq |A|$. When does the equality hold?

Exercise 1.117. Prove that $|\mathcal{P}(A)| = 2^{|A|}$ for a finite set A. Do you see why the power set $\mathcal{P}(A)$ is often referenced as 2^A?

Exercise 1.118. Let A, B, C be finite sets. Prove that:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Exercise 1.119. Let $X = \{1, 2, \ldots, 2018\}$.

---

[31] $X \setminus A$ and A are disjoint and sum up to X...

[32] What is $(X \setminus (X \cap Y)) \cup Y$?

1.5.2 Characteristic functions

Definition 1.120. *Fix a set U. For each subset $A \subseteq U$ we define it's* ***characteristic function*** *or* ***indicator function*** *as:*

$$1_A : U \to \{0, 1\}$$
$$1_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

Example 1.121. Consider a set U. Then $1_\varnothing(x) = 0$ and $1_U(x) = 1$ for every $x \in U$. It's usually abbreviated as:

$$1_\varnothing = 0, 1_U = 1.$$

Exercise 1.122. Let $A, B \subseteq U$. Prove that:

1. $1_{A \cap B} = 1_A \cdot 1_B$[33]
2. $1_{A^c} = 1 - 1_A$, where $A^c = U \setminus A$
3. $1_{A \cup B} = 1_A + 1_B - 1_A \cdot 1_B$

Exercise 1.123. Prove inclusion-exclusion principle for finite sets using characteristic functions. [Hint[34]]

1.5.3 Comparing cardinalities

Although we feel comfortable in counting elements of *finite* sets, we don't know how to say how to compare infinite sets - there is no natural number we could use to denote their cardinalities!

Therefore, we'll try another approach. Assume that we have a set of children and a set of toys. If we want to compare them, we can either try to calculate how many children and toys there are (it may be very hard if there are lots of children and lots of toys) or to ask each child to get one toy. If every child has *one* toy and no toys are left, we know that there are exactly as many children as toys! We'll use this approach to compare infinite sets.

Definition 1.124. *Let A and B be two sets. If there exists a bijection $f : A \to B$, we say that $|A| = |B|$ (are of the same cardinality).*

Example 1.125. $|\mathbb{N}| = |2\mathbb{N}|$, where $2\mathbb{N}$ is a set of all even natural numbers, as we can find a bijection $n \mapsto 2n$. It's a surprising result, as $2\mathbb{N} \subseteq \mathbb{N}$ is a *proper* subset. If $\mathbb{N}$ was finite, all it's proper subsets would have smaller cardinalities!

---

[33] It means that for every $x \in U$ we have $1_{A \cap B}(x) = 1_A(x) \cdot 1_B(x)$

[34] Write $1_{A \cup B}$ in terms of $1_A, 1_B, 1_{A \cap B}$ and sum its values over all elements in *finite* set $A \cup B$.

Exercise 1.126. Being of the same cardinality has similar properties to these of equivalence relation[35]. Prove that:

1. $|A| = |A|$
2. $|A| = |B|$ implies that $|B| = |A|$ [Hint[36]]
3. if $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$ [Hint[37]]

Exercise 1.127. By considering the function

$$(-1,\, 1) \ni x \mapsto \frac{x}{1-x^2} \in \mathbb{R},$$

prove that *every* non-empty open interval $(a,\, b)$ has the same cardinality as $\mathbb{R}$. [Hint[38]]

Definition 1.128. *We say that a set X is* ***countably infinite*** *if $|X| = |\mathbb{N}|$. Usually we'll write that $\aleph_0 := |\mathbb{N}|$ (read "aleph 0"). We say that a set X is* ***countable*** *if X is finite or countably infinite.*

Example 1.129. Sets $\mathbb{N}, 2\mathbb{N}, \{0, 1, 6, 41\}$ are countable.

Example 1.130. $\mathbb{Z}$ is countable: $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto -1, 3 \mapsto 2, 4 \mapsto -2, \ldots$

Exercise 1.131. Prove that a subset of a countable set is countable.

Exercise 1.132. Let A and B be countable sets. Prove that $A \cup B$ and $A \cap B$ are countable.

Exercise 1.133. Let A and B be countable. Prove that $A \times B$ is countable. [Hint[39]]

Exercise 1.134. Prove that $\mathbb{Q}$ is countable.

Exercise 1.135. Let $\mathcal{A}$ be a countable family of countable sets. Prove that $\bigcup \mathcal{A}$ is countable.

Exercise 1.136. Prove that is X is an infinite set, then it contains a countably-infinite subset $S \subseteq X, |S| = \aleph_0$.

The last exercise shows that we can compare cardinalities. That is, if we can find a bijection between A and *some subset* of B, we can be sure that B contains at least as many elements as A. This is exactly requiring the existence of an *injection* from $A \to B$.

---

[35] ... but as there is no sets of all sets, it *is not* formally an equivalence relation.
[36] Bijections have inverses.
[37] Composition of bijections is a bijection as well.
[38] Can you find a bijection between $(a,\, b)$ and $(-1,\, 1)$?
[39] You can write all elements of A as $a_1, a_2, \ldots$ and the elements of B as $b_1, b_2, \ldots$. Think about an ordering $(a_1, b_1); (a_1, b_2), (a_2, b_1); (a_1, b_3), (a_2, b_2), (a_3, b_1); \ldots$ (some terms may be repeated if A and B are not disjoint, think how to fix it).

Definition 1.137. *If there exists an injection $f : A \to B$ we say that B has greater or equal cardinality than A and write $|A| \leq |B|$. If $|A| \leq |B|$ and $|A| \neq |B|$, we write $|A| < |B|$ (that is: we can find an injection from A to B, but there is no bijection between them).*

As compositions of injections is an injection, we have the following:

Exercise 1.138. Let A, B and C be sets. Prove that if $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

In the following exercise, you will prove that there are more reals that natural numbers.

Exercise 1.139. We define $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$.[40] Prove that there is no surjection from $\mathbb{N}$ onto X (injection is easy to find...). [Hint[41]]

Exercise 1.140. We know that $|\mathbb{R}| > |\mathbb{N}|$. Using binary expansion prove that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. Do you see similarity between the previous result and $2^n > n$ for natural n?

We may suspect the following:

Theorem 1.141. ***Cantor's theorem*** *$|A| < |\mathcal{P}(A)|$ for any set A.*

Exercise 1.142. Prove Cantor's theorem in two steps:

1. Find an injection from A to $\mathcal{P}(A)$.
2. To prove that there is no surjection, you can consider any $f : A \to \mathcal{P}(A)$ and a set
$$X = \{a \in A : a \notin f(a)\} \in \mathcal{P}(A).$$
Is there $x \in A$ for which $f(x) = X$?

Exercise 1.143. Use Cantor's theorem to prove that there is no set of all sets.

The last exercise is a bit more complicated, although it's statement looks rather obvious:

Theorem 1.144. ***Cantor-Schroeder-Bernstein theorem*** *If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

We will prove this repearing the proof of Banach and Tarski. The proof is tricky, so it was split into several parts.

---

[40] We also need to choose one convention of writing reals. Consider a number with finite expansion, e.g. 0.123. We can write this either as 0.123(0) or 0.122(9).

[41] Assume that you have written all the elements of X in a single column. Can you construct a real number that does not occur in the list? It should differ from the first number at least at one digit, and same for other numbers.

Definition 1.145. *We say that a function $F : \mathcal{P}(A) \to \mathcal{P}(B)$ is* ***monotonous*** *if $F(X) \subseteq F(Y)$ whenever $X \subseteq Y$.*

Theorem 1.146. ***Knaster-Tarski fixed point theorem*** *A monotonous function $F : \mathcal{P}(A) \to \mathcal{P}(A)$ posseses a fixed point, that is: there exists a set S such that $F(S) = S$.*

Exercise 1.147. Prove the fixed point theorem by considering a set:

$$S = \bigcup \mathcal{U}, \text{ where } \mathcal{U} = \{Y \in \mathcal{P}(A) : Y \subseteq F(Y)\}.$$

[Hint[42]]

Definition 1.148. *Recall that if $f : A \to B$ and $X \subseteq A$, then we define*

$$f[X] = \{b \in B : b = f(x) \text{ for some } x \in X\}.$$

Exercise 1.149.
1. Let $f : A \to B$ and $g : B \to A$ be injections. Prove that the function

$$F : \mathcal{P}(A) \to \mathcal{P}(A),\ F(X) = A \setminus g[B \setminus f[X]]$$

has the monotonicity property.
2. Let S be the fixed point of F. Prove that $A \setminus S \subseteq \operatorname{Im} g$.
3. Conclude that there exists $\tilde{g} : A \setminus S \to B$ such that $g(\tilde{g}(a)) = a$ for $a \in A \setminus S$.
4. Prove that function

$$h(x) = \begin{cases} f(x), & x \in S \\ \tilde{g}(x), & x \in A \setminus S \end{cases}$$

is a bijection from A to B, what ends the proof of the Cantor-Schroeder-Bernstein theorem.

Exercise 1.150. Recall that every non-empty open interval (a, b) has the same cardinality as $\mathbb{R}$. Prove that every closed interval $[a, b]$ with $b > a$ has the same cardinality as $\mathbb{R}$.

1.6 The Axiom of Choice

We formulated comparision of cardinalities in terms of injections. We based on the following exercise:

---

[42] Each Y is a subset of S, use the monotonicity to conclude that $Y \subseteq F(Y) \subseteq F(S)$ and $S = \bigcup \mathcal{U} \subseteq F(S)$. To prove the other inclusion, use $F(S) \subseteq F(F(S))$, what shows that $F(S) \in \mathcal{U}$.

Exercise 1.151. Let f be a function from A to B. Prove that there exists a function $g : \operatorname{Im} B \to A$ such that $g \circ f = \mathrm{Id}_A$ iff f is injective.

That is for an injective function there exists a "left inverse". We may ask a question - is a some kind of inverse possible for *surjections*?

Exercise 1.152. Consider a surjective function $f : \mathbb{Z} \to \{0, 1\}$ given by $2k + 1 \mapsto 1, 2k \mapsto 0, k \in \mathbb{Z}$.

1. why a *left* inverse does not exist?
2. define a *right* inverse, that is a function $g : \{0, 1\} \to \mathbb{Z}$ such that $f \circ g = \mathrm{Id}_{\{0,1\}}$

In the above exercise we had no problem - just pick an element from the set of odd numbers (these that are mapped to 1) and an element from the set of even numbers (these that are mapped to 0). While there is no problem of picking an element from each set if we have just two (or three, four - any finite number), this issue may apear for *infinite* families of sets.

Definition 1.153. ***Axiom of choice (AC)*** *Let $\mathcal{A}$ be a non-empty family of non-empty sets. Then there exists a* ***choice function*** *$f : \mathcal{A} \to \bigcup \mathcal{A}$ such that $f(A) \in A$ for every $A \in \mathcal{A}$.*

Basically it means that for every family of sets, we can select an element from each set - for a set A, such element is just $f(A)$, where f is the choice function. Alternatively, we could formulate it equivalently as:

Definition 1.154. ***Axiom of choice (AC)*** *Let $\mathcal{S} = \{S_i : i \in I\}$ be any family of non-empty sets such that $S_i \cap S_j = \varnothing$ for $i \neq j$. Then it is possible to create a set C such that for every $i \in I$ there is $s_i \in C$ such that $s_i \in S_i$. Or in natural-language terms: from every set of a family of nen-empty, pairwise-disjoint sets, we can select exactly one element.*

This axiom allows us to construct right inverses:

Exercise 1.155. Prove that AC (the axiom of choice) is equivalent to the statement that every surjection possesses a right inverse. Hint: for $AC \Rightarrow$ right inverse use the same idea as in the previous problem. For right inverse $\Rightarrow AC$ construct a surjective function from $\bigcup \mathcal{S} \to \mathcal{S}$, where $\mathcal{S}$ is a family of non-empty, pairwise-disjoint sets.

Exercise 1.156. Prove, assuming AC, that if $f : A \to B$ is a surjection, then, there exists an injection $g : B \to A$.

Therefore with AC it makes sense to compare cardinalities using surjections:

Exercise 1.157. Prove, assuming AC, that:

1. $A \leq B$ iff there exists a surjection from B to A
2. if there is a surjection from A to B and a surjection from B to A, then there exists a bijection between A and B

It can also be useful in problems involving infinitely many hats:

Exercise 1.158. A king said $\aleph_0$ mathematicians the following: "Tomorrow, you will be standing in a long queue and my servants will place a red or green hat on everyone's head. You will see only the hats of the people standing before you. On a given signal, you need to guess your own hat. If infinitely many of you guess wrong, I will send you to the prison for the rest of your lifes!". By considering a set of all functions from $\mathbb{N} \to \{"red", "green"\}$ and a suitable partition on it, prove, assuming the axiom of choice, that mathematicians can make finitely-many wrong guesses.

In fact, AC implies much more - as Banach-Tarski paradox says using it one can take a solid sphere, cut it into a few pieces and compose *two* spheres of the same size, just by moving the pieces around. Therefore many mathematicians try to avoid it as much as possible - it is a good habit always to explicitly mention it's usage. In many places in this book we will use AC, usually in an equivalent form known as Kuratowski-Zorn lemma[43].

1.6.1 Kuratowski-Zorn (Zorn's) lemma

Definition 1.159. *A* ***partial order*** *is a relation $\leq$ on a set A such that for all a, b, $c \in A$:*

1. $a \leq a$
2. $a \leq b \wedge b \leq a \Rightarrow a = b$
3. $a \leq b \wedge b \leq c \Rightarrow a \leq c.$

If for every a, $b \in A$ we have $a \leq b$ or $b \leq a$, then we say that it is a ***total order*** *or* ***linear order****.*

Example 1.160. Natural numbers, integers and reals are totally ordered.

Example 1.161. Consider a set $\mathcal{P}(A)$ for some set A. It's partially ordered by the relation:

$$B \leq C \Leftrightarrow B \subseteq C.$$

Note that some sets cannot be compared (neither $A \leq B$ nor $B \leq A$), so this order is *not* total.

[43] In English literature it is widely known as **Zorn's lemma**. Kazimierz Kuratowski proved this lemma (although with an unnecessary assumption) in 1922 and Max Zorn, working independently, gave the above formulation in 1935. The Bourbaki group and John Tukey used the latter name in their books published in 1939 and 1940 and since then "Zorn's lemma" is widely recognised.

Definition 1.162. *A* ***partially-ordered set*** *or a* ***poset*** *is a pair* $(A, \leq)$*, where* A *is a set and* $\leq$ *is a partial order on* A*. If* $B \subseteq A$ *is a subset on which* $\leq$ *is total (every two elements of* B *can be compared, or in set-theoretic terms* $B \times B \subseteq \leq$*), we call* B *a* ***a chain****.*

Example 1.163. Consider $A = \{0, 1\}$. Then it's power set ordered by inclusion - $(\mathcal{P}(A), \subseteq)$ - is a poset. If we take $B = \{\varnothing, A\} \subseteq \mathcal{P}(A)$, then every two elements of B can be compared - it's a chain.

Definition 1.164. *Let* $(A, \leq)$ *be a poset and* $B \subseteq A$ *be a chain. We say that* $u \in A$ *is an* ***upper bound*** *of a chain* B *if* $b \leq u$ *for every* $b \in B$*. We say that* $m \in A$ *is a* ***maximal element*** *if for every* $a \in A$ *we have* $m \leq a \Rightarrow m = a$*, that is there is no greater element than* m*.*

Example 1.165. Let $A = \{1, 2, 3, 4, 5\}$ with standard order. Then 5 is a maximal element in A and an upper bound of A.

Theorem 1.166. ***Kuratowski-Zorn (Zorn's) lemma*** *Let* $(P, \leq)$ *be a poset such that every chain in* P *has an upper bound. Then there exists a maximal element in* P*.*

For a proof, you can check Arjun Jain's "Zorn's Lemma An elementary proof under the Axiom of Choice"[44]. We will usually use AC in this form.

1.7 Problems

Exercise 1.167. Let $S \subseteq R$. We say that S is **well-ordered** iff any non-empty subset $X \subset S$ has the smallest element.

1. Prove that reals and integers with the default ordering are not well-ordered.
2. Assume that $X \subseteq \mathbb{N}$ doesn't have the smallest element. Define

   $$A = \{n \in \mathbb{N} : \{0, 1, \ldots, n\} \cap X = \varnothing\}$$

   and use mathematical induction to prove that X is empty.
3. Why are natural numbers well-ordered?

[44] https://arxiv.org/pdf/1207.6698.pdf