Paweł Czyż

Crash Course in Mathematical Physics

– Monograph –

July 10, 2018

Springer

For the people whom I learned mathematics from:
Wiktor Bartol,
Michał Bączyk,
Jerzy Bednarczuk,
Beata Czyż,
Frederic Grabowski,
Wojciech Guzicki,
Maciej Kiliszek,
Anna Kowalska,
Andre Lukas,
Jakub Perlin,
Krzysztof Reczek,
Arun Shanmuganathan

Preface

So what I told you was true, from a certain point of view.

Star Wars, Episode VI — Obi-Wan Kenobi

Contents

Part I Logic, sets and categories

1 Introduction 3

2 Logic and sets 7
2.1 Propositional calculus 7
2.1.1 New sentences from old 7
2.1.2 Quantifiers 10
2.2 Basic set theory 10
2.2.1 New sets from old 12
2.2.2 Subsets and complements 14
2.2.3 Cartesian product 14
2.3 Relations 15
2.4 Functions 18
2.4.1 Injectivity, surjectivity and bijectivity 19
2.4.2 Function composition 20
2.4.3 Commutative diagrams 21
2.5 Cardinality 22
2.5.1 Finite sets 22
2.5.2 Characteristic functions 23
2.5.3 Comparing cardinalities 24
2.6 Axiom of choice 26
2.6.1 Kuratowski-Zorn (Zorn's) lemma 28
2.7 Numbers 28
2.7.1 Real numbers 29
2.7.2 Absolute value 31
2.7.3 Mathematical induction 32

3 Taste of category theory 35
3.0.1 Morphisms 36
3.1 Functors 38

3.2 Limits and colimits 38

Part II Abstract algebra

4 Groups 41
4.1 The category of groups 43

5 Linear algebra 45
5.1 Vector spaces 45
5.1.1 Bases of vectos spaces 46
5.1.2 Subspaces, direct sum and quotient spaces 49
5.1.3 Quotient spaces 51
5.2 Linear maps 51
5.2.1 Kernel and cokernel 52
5.2.2 Rank-nullity theorem 52
5.2.3 Exact sequences 53
5.3 Dual spaces 54
5.4 Tensors 56
5.4.1 Universal property of tensor spaces 56
5.4.2 Construction 57

Part III General topology

6 General topology 61
6.1 The category of topological spaces 61
6.2 New spaces from old 63
6.2.1 Closed sets and closure 64
6.2.2 Boundary and exterior 65
6.2.3 Bases and countability axioms 65
6.3 Continuous maps and homeomorphisms 66
6.4 Connected spaces 66

7 Pseudometric spaces 69
7.1 Pseudometric spaces 69
7.2 Topology of $\mathbb{R}$ 70

Part IV Analysis

8 Banach spaces 73

References 75

Part I

Logic, sets and categories

1

Introduction

There are many excellent books on mathematical physics and differential geometry, so a question araises - how does this book differ from any other? I had a few aims working on it:

- Understandable for any person that wants to learn. It does not matter if you are a physicists, mathematician, english literature major or a high-school student. If you have enough self-determination, you can understand the mathematics in this book.
- Self-containing. Mathematics is both broad and deep, so it must be split into many different branches. But I personally found discouraging that if you want to read one book, as prerequsities you need to read two other books, and so on. Here, you can understand that everything contained here with no access to libraries or other mathematical books. Obviously, we don't cover the whole subject, but it is a good start to own research.
- Problem-solving approach. I want you to prove all the theorems in this book, with adjustable amount of hints. This way you can understand what we are actually doing, instead of ommiting proofs that look discouraging at the beginning.
- Abstract concepts first. We start with very abstract concepts and then move to examples and special cases. It is not always possible if we want to provide enough examples, but this is the aim. Starting from abstract, more general terms usually makes the whole situation easier - you have less properties and assumptions to use, so the solutions are more straightforward.
- "So what I told you was true, from a certain point of view." - many mathematical objects look differently for different mathematicians. We will always try to cover many "points of view" to increase the understanding of the subject.
- Objects and maps. We define precisely what are our objects and transformations, that are in some sense natural, that change one object into

another. While we don't use the language of the category theory, you can get some taste.

- Properties, then construction. When we talk about a mathematical object, we usually think about it's *properties*. Explicit construction is useful - as it proves the existence of the object under consideration - but usually hides many important properties of the object. Therefore we define objects by a few properties, then we think about theorems that can be proved using these initial properties (so we end up with many more properties) and then think how to construct the object having the initial properties.
- Notation abusements explained. Mathematics has been evolving for centuries in many different countries, so the notation is rather diverse and sometimes is not the best possible. We will abuse it as it is a standard in mathematical world, but you will always understand what objects are involved in expressions you are manipulating with.
- No jumps. In mathematics we prove theorems and then use these theorems to prove other theorems and so on. In many textbooks I know, these auxilary theorems are referenced as „Check section 3, problem 2.". I don't associate theorems with specific numbers and I don't like going to a specified section. Therefore I reference theorems by their mathematical content or commonly used name, rather than an artificial number. I believe that you will be able to prove such mentioned theorems quickly and without problems.
- You will encounter two types of problems in this book - some of them you will encounter in the text, and they are called exercises. These are strongly related to the investigated subject and are essential for the continuity of the lecture. Others, called problems, you will find at the end of sections of chapters. These are problems that does not need to be connected with the discussed subject at all. If you read the book carefully, without jumps, you will be able to solve all of them. But it will give you an opportunity to come up with new insights - without subject specified you'll need to come up with ideas what tools, methods and theorems will be useful. I hope this helps you becoming a scientist.[1]

We use the following notation: **bold** will be used for definitions of new objects, and *italics* will be used for additional subtle remarks that should be taken into account. We use footnote[2] to provide additional comments.

Remember that the subject is big and it may be very hard to finish the book in just one day. I strongly advise working on it every day starting from just two minutes a day and increasing the time spend every week. I tried to make the learning curve flat, what leghtens the book. Any mistakes are

---

[1] I recommend watching an excellent talk given by Barbara Oakley "Learning how to lean" at Google. It's available on YouTube, under the link `https://www.youtube.com/watch?v=vd2dtkMINIw`. I especially recommend to think about focused and diffusive modes.

[2] Like this one.

my own failure and I would be grateful if you pointed them to me. Also any suggestions and comments are welcome. You can create new issues on GitHub: `https://github.com/pawel-czyz/MathematicalPhysics` or write an email to `pczyz@protonmail.com`. Good luck on your road!

2

Logic and sets

Logic is a huge and beautiful branch of mathematics. We will focus on it's basics, topic called "propositional calculus". It is a powerful machinery, that will be used later to prove theorems and define new objects. Moreover, it gives a good grasp on Boolean algebras, a concept that we will later meet in topology.

2.1 Propositional calculus

2.1.1 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 2.1. *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 2.2. Sentences "Each square is a rectangle" and "2+2=3+1" are both true, so trivially they are equivalent.

Example 2.3. 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 2.4. Prove that $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$. Hint: what does the sentence in the first bracket mean? What about the second? Why are they equivalent?

Exercise 2.5. Prove that if we know that $p \Leftrightarrow q$ and we know that $q \Leftrightarrow r$, then also $p \Leftrightarrow r$.

Definition 2.6. *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 2.7. Sentence: "(2+2=5) and (2+1=3)" is false, as one of them (namely, the first one) is false.

Exercise 2.8. 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 2.9. 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 2.10. *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 2.11. 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 2.12. Prove that disjunction is both associative and commutative.

Definition 2.13. ***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 2.14. Prove that if $\neg p$ 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 2.15. 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 2.16. 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 2.17. 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 2.18. Prove **De Morgan's laws**:

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

Definition 2.19. *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 2.20. Prove that $(p \Rightarrow q) \Leftrightarrow (\neg p) \vee q$. Hint: 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?

Exercise 2.21. Prove that implication is **transitive**, that is

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

Exercise 2.22. Assuming that every topological space is homeomorphic to itself and that homeomorphic spaces are homotopic, prove that every topological is homotopic to itself. Hint: you don't need to know what the terms here mean to solve this exercise (but eventually will reach them!).

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

Exercise 2.23. Prove that $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$.

2.1.2 Quantifiers

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

Definition 2.24. *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"* [1]*.*

Example 2.25. 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 2.26. 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?

2.2 Basic set theory

In modern mathematics we do not define a set nor 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 2.27. 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] $\forall$ is a rotated "A" symbolising "for **A**ll" and $\exists$ is a rotated "E" symbolising "**E**xists"

2.1. Russel's paradox Let X be a set built from all sets such that $A \notin A$. Prove that X does not exist. Hint: what if $X \in X$? What if $X \notin X$?

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[2] $\mathbb{R}$
3. natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$
4. integers $\mathbb{Z}$
5. rational numbers $\mathbb{Q}$

Definition 2.28. ***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 2.29. *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 2.30. We can write $A \subseteq B \Leftrightarrow \forall_{a \in A} a \in B$.

Exercise 2.31. 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 2.32. 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 $\theta = \varnothing$.

[2] 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.

2.2.1 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 2.33. ***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*[3]*:*

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

Example 2.34. 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 2.35. Prove that there is *no* set of all sets. Hint: assume there is one and select some elements to create Russel's paradox.

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

Definition 2.36. ***Axiom of power set*** *Consider a set A. We assume that there exists* [4] ***the power set of*** *A defined as a set of all subsets of A:*

$$\mathcal{P}(A) := 2^A := \{A' : A' \subseteq A\}.$$

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

Exercise 2.37. 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 2.38.
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 now why $\mathcal{P}(A)$ is sometimes referenced as 2^A? Hint: every subset is specified by elements that are inside it. For every element you have two options - to select it or not.

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

[4] 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.

Definition 2.39. *By a* ***collection of sets*** *or* ***family of sets*** *we understand a set of some sets.*

Definition 2.40. ***Axiom of union*** *Assume that we are given a family of sets A. There is a set called their* ***union***[5]*:*

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

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

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

Exercise 2.41. 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 2.42. ***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 2.43. Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Then $A \setminus B = \{1\}$.

Exercise 2.44. Is $(A \setminus B) \cup B$ always equal to A?

Exercise 2.45. Let A and B be sets. Prove that $A \subseteq (A \setminus B) \cup B$, where the equality holds iff $B \subseteq A$.

Definition 2.46. *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 2.47. Find sum and intersection of family of subsets of $\mathbb{R}$:

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

for $r \geq 0$.

[5] Again, we cannot use the axiom schema of specification as there is no everything - we would select set of sets it it existed.

Exercise 2.48. 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 2.49. Prove distributivity:

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

2.2.2 Subsets and complements

Definition 2.50. *Let A be subset of a set U. We say that* ***the complement***[6] ***of*** *A is a set $A^c = U \setminus A$.*

2.2. 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 $(A \cap B)^c = A^c \cup B^c$

2.3. 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 2.51. Let $A \subseteq X_i$ for $i \in I$. Prove that

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

Exercise 2.52. For every point $a \in A$ there is a set $U_a \subseteq A$ such that $a \in U_a$. Prove that

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

2.2.3 Cartesian product

First of all, we need a useful concept:

Definition 2.53. *We define* ***an ordered pair*** *or* ***a 2-tuple*** *as*

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

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

[6] Just adding an index c is not the best symbol possible as we need to have U in mind.

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

Definition 2.54. ***An ordered*** n***-tuple*** *or simply* ***a tuple*** *is defined as:*

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

It's single most important property is that:

$$(a_1, a_2, \ldots, a_n) = (a_1', a_2', \ldots, a_n')$$

iff $a_1 = a_1', a_2 = a_2', \ldots, a_n = a_n'$.

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 2.55. 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 2.56. *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 2.57. Prove that Cartesian product is *not* commutative (that is $A \times B \neq B \times A$ in general).

2.6. 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 address this issue.

Definition 2.58. *We define a* ***square*** *of a set X as:*

$$X^2 = X \times X,$$

that is a set of all pairs made from elements of X. Similarily, we define X^n as the collection of all n-tuples made from elements of X.

2.3 Relations

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

Definition 2.59. *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 2.60. Consider the ordering of natural numbers: $1 < 2, 2 < 3$, $4 < 27$. It is in fact a relation on $\mathbb{N}$: $a < b$ means exactly $(a,b) \in <\subseteq \mathbb{N} \times \mathbb{N}$.

Exercise 2.61. 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 2.62. Let X and Y be any sets. Prove that there exists the **set** of all relations between X and Y. Hint: what is a power set?

Exercise 2.63. 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 2.64. *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 2.65. 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 2.66. 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 2.67. *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 2.68. 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 2.69. 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 they are a partition).

Exercise 2.70. 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: for $n \geq 2$ construct n equivalence relations with two classes.

Usually our sets will be equipped with some additional structure - for example integers can be added together[7]. Sometimes we can move this structure to the equivalence classes. Let's start by finding a nice equivalence class on them.

Exercise 2.71. Modulo arithmetics

1. Prove that $m \equiv n \Leftrightarrow p|m - n$ is an equivalence relation on $\mathbb{Z}$ ($p|q$ means: p divides q, or equivalently: there exists an integer a such that $q = p \cdot a$).
2. Let's define the sum of equivalence classes:

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

Prove that this definition does not depend on class representatives - that is if $n \equiv n'$ and $m \equiv m'$, then $[n] + [m] = [n'] + [m']$.

Exercise 2.72. Construction of rationals

1. Let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Consider $X = \mathbb{Z} \times \mathbb{Z}^*$. Prove that relation $\equiv$ 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:
   a) $[m, n] = [am, an]$
   b) $[0, 1] + [m, n] = [m, n]$
   c) $[1, 1] \cdot [m, n] = [m, n]$

---

[7] A fancy word for that will be given later: they form an additive Abelian group

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?

You can ask whether integers also can be somehow constructed using most basic, natural, numbers. Yes - 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.

2.4 Functions

Definition 2.73. *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 2.74. $f : \mathbb{N} \to \mathbb{R}$ given by $f(n) = n^2$. We can also write:

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

Example 2.75. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^{10} + x^2 - 1$.

Example 2.76. $f : X \to \mathcal{P}(X)$ given by $f(x) = \{x\}$.

Exercise 2.77. Let X and Y be two sets. Prove that there exists a set of all functions from X to Y. Hint: you can form a set of all relations between X and Y. How are functions related to relations?

Exercise 2.78. How many[8] are there functions from the empty set to $\{1,2,3,4\}$? Hint: what is a function in set-theoretical terms?

Exercise 2.79. 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 $y = |Y|$.

[8] Thanks to Antek Hanke

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: for first element in X you have y possibilities to choose.
3. Prove that for every non-zero natural numbers x and y the following holds:

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

Exercise 2.80. Let X and Y be any two sets. Prove that you can create a set of all functions from X to Y. Sometimes it is called Y^X. Do you know why?

Exercise 2.81. 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.

2.7. 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 2.82. *Consider a set X. We say that it's **identity function** is $f : X \to X$ given by $f(x) = x$ for all $x \in X$.*

2.4.1 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 2.83. *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 $Im\, f = B$.*

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

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 2.84. *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 2.85. 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 2.86. 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 2.87. 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 2.88. *If a function f is both surjective and injective, we say that is* ***bijective***[9].

Exercise 2.89. 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 $g(f(a)) = a$.

2.9. Prove that, if exists, g is unique.

Definition 2.90. *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** [10]: $g = f^{-1}$.

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

2.4.2 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 2.91. Recall that for two relations $R \subseteq X \times Y$ and $T \subseteq Y \times Z$ we defined their composition as

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

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

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

Exercise 2.92. 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 2.93. 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 2.94. 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 2.95. *We will rephrase the definition of the inverse function using the identity function*[11]*:*

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

2.4.3 Commutative diagrams

Use a picture. It's worth a thousand words.
- Tess Flanders

Consider functions $f : X \to Y$ and $g : Y \to Z$. We introduced the composition of them given us $g \circ f : X \to Z$. We can visualise it using a following **diagram** (Fig. 2.1):

We say that this diagram **commutes** (or we say that this is a **commutative diagram**) as you can use follow any path and obtain the same result.

Exercise 2.97. Prove that the diagram 2.2 commutes iff $h = g \circ f$?

Exercise 2.98. What can you say if diagram 2.3 commutes?

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

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

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "g\circ f"'] & & Y \arrow[dl, "g"] \\ & Z & \end{tikzcd}$$

Fig. 2.1. An example of a diagram.

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "h"'] & & Y \arrow[dl, "g"] \\ & Z & \end{tikzcd}$$

Fig. 2.2. What can you say about f, g, h if the diagram commutes?

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "h"] & Y \arrow[d, "g"] \\ Z \arrow[r, "j"] & T \end{tikzcd}$$

Fig. 2.3. What can you say about the functions involved if the diagram commutes?

2.5 Cardinality

2.5.1 Finite sets

Definition 2.99. *The **cardinality** $|X|$ of a finite set X is defined as the number of elements in X.*

Example 2.100. Let $A = \{0, 1, 2, 3\}$. Then $|A| = 4$.

Exercise 2.101. What is the cardinality of $\{a, a+1, a+2, \dots, a+n\}$?

Theorem 2.102. ***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 2.103. 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: $X \setminus A$ and A are disjoint and sum up to X...

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: what is $(X \setminus (X \cap Y)) \cup Y$?

Exercise 2.104. Prove that if $B \subseteq A$, and A is finite, then $|B| \leq |A|$. When does the equality hold?

Exercise 2.105. 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 2.106. 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 2.107. Let $X = \{1, 2, \ldots, 2018\}$.

2.5.2 Characteristic functions

Definition 2.108. *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 2.109. 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 2.110. Let $A, B \subseteq U$. Prove that:

1. $1_{A \cap B} = 1_A \cdot 1_B$[12]
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 2.111. Prove inclusion-exclusion principle for finite sets using characteristic functions. Hint: write $1_{A \cup B}$ in terms of $1_A, 1_B, 1_{A \cap B}$ and sum it's values over all elements in *finite* set $A \cup B$.

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

2.5.3 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 2.112. *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 2.113. $|\mathbb{N}| = |2\mathbb{N}|$, 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 $2\mathbb{N} \subsetneq \mathbb{N}$ is a *proper* subset. If $\mathbb{N}$ was finite, all it's proper subsets would have smaller cardinalities!

Exercise 2.114. Being of the same cardinality has similar properties to these of equivalence relation[13]. Prove that:

1. $|A| = |A|$
2. $|A| = |B|$ implies that $|B| = |A|$ (hint: bijections have inverses)
3. if $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$ (hint: what is a composition of bijections?)

Definition 2.115. *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 2.116. Sets $\mathbb{N}, 2\mathbb{N}, \{0, 1, 6, 41\}$ are countable.

Example 2.117. $\mathbb{Z}$ is countable: $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto -1, 3 \mapsto 2, 4 \mapsto -2, \ldots$

Exercise 2.118. Prove that a subset of a countable set is countable.

Exercise 2.119. Let A and B be countable sets. Prove that $A \cup B$ and $A \cap B$ are countable.

Exercise 2.120. Let A and B be countable. Prove that $A \times B$ is countable. Hint: 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).

Exercise 2.121. Prove that $\mathbb{Q}$ is countable.

---

[13] ... but as there is no sets of all sets, it is not formally an equivalence relation.

Exercise 2.122. Let $\mathcal{A}$ be a countable family of countable sets. Prove that $\bigcup \mathcal{A}$ is countable.

Exercise 2.123. Prove that is X is an infinite subset, 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 $A \to B$.

Definition 2.124. *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).*

Exercise 2.125. Let A, B and C be sets. Prove that if $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

2.11. Here you can prove that there are more real numbers than naturals or rationals. We define $X = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ and choose one convention of writing reals (e.g 0.999... = 1.000..., so we can choose to use nines)

1. Assume that you have written all the elements of X in a single column. Can you find a real number that does not occur in the list?
2. Using the above, prove that $|\mathbb{N}| < |X|$
3. Prove that $|\mathbb{Q}| < |\mathbb{R}|$.

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

2.13. Cantor's theorem You will prove that $|A| < |\mathcal{P}(A)|$ for any set A. Let A be a set and $f : A \to \mathcal{P}(A)$.

1. Consider $X = \{a \in A : a \notin f(a)\} \in \mathcal{P}(A)$. Is there $x \in A$ for which $f(x) = X$?
2. Is f surjective?
3. Find an injective function $g : A \to \mathcal{P}(A)$.
4. Prove that $|A| < |\mathcal{P}(A)|$ for any set A.
5. Use Cantor's theorem to prove that there is no set of all sets.

2.14. Cantor-Schroeder-Bernstein theorem Let's prove that if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

1. (Knaster-Tarski) Now assume that F has *monotonicity* property: $F(X) \subseteq F(Y)$ if $X \subseteq Y$. Prove that F has a fixed point S (that is $F(S) = S$), where:
$$S = \bigcup_{X \in U} X, \text{ where } U = \{Y \in \mathcal{P}(A) : Y \subseteq f(Y)\}.$$

2. (Banach) Let $f : A \to B$ and $g : B \to A$ be injections. We introduce new symbol: $f[X] = \{b \in B : b = f(x) \text{ for some } x \in X\}$. Prove that function

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

has the monotonicity property.
3. Prove that $A \setminus S \subseteq \operatorname{Im} g$, where F and S are taken from above.
4. Prove that function

$$h(x) = \begin{cases} f(x), x \in S \\ g^{-1}(x), x \notin S \end{cases}$$

is a bijection.

2.6 Axiom of choice

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

Exercise 2.126. 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 2.127. 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 2.128. ***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 2.129. ***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 2.130. 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 2.131. 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 2.132. 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

Exercise 2.133. 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[14] 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[15].

[14] Yes, eventually we'll prove it!

[15] 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.

2.6.1 Kuratowski-Zorn (Zorn's) lemma

Definition 2.134. *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 2.135. Natural numbers, integers and reals are totally ordered.

Example 2.136. 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.

Definition 2.137. *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 2.138. 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 2.139. *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 2.140. 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 2.141. ***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"[16].

2.7 Numbers

At the beginning we assumed that you know how to work with different kinds of numbers. This aim of this section is to give a few properties of them.

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

2.7.1 Real numbers

Definition 2.142. *A **field** is a tuple* $(\mathbb{F}, +, \cdot)$ *such that:*

- $\mathbb{F}$ *is a set*
- $+$ *and* $\cdot$ *are functions from* $\mathbb{F} \times \mathbb{F}$ *to* $\mathbb{F}$. *We write* $a + b$ *for* $+(a, b)$ *and* $a \cdot b$ *for* $\cdot(a, b)$.

They have these properties:

1. $a + (b + c) = (a + b) + c$ *for all* a, b, c *(addition is associative)*
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* a, b, c *(multiplication is associative)*
3. $a + b = b + a$ *for all* a, b *(addition is commutative)*
4. $a \cdot b = b \cdot a$ *for all* a, b *(multiplication is commutative)*
5. *there is an element* $0 \in \mathbb{F}$ *such that* $a + 0 = a$ *for all* a *(addition has a neutral element). We call it **zero***
6. *there is an element* $1 \in \mathbb{F}$ *such that* $a \cdot 1 = a$ *for all* a *(so 1 is neutral element of multiplication). We call if **one***
7. *for every* a *there is* a' *such that* $a + a' = 0$ *(existence of an inverse element for addition)*
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* a, b, c *(multiplication distributesover addition)*
9. *for every* $a \neq 0$ *there is* $\tilde{a}$ *such that* $a \cdot \tilde{a} = 1$ *(multiplication has an inverse element for all non-zero numbers)*
10. $1 \neq 0$ *(so* $\mathbb{F}$ *has at least two elements)*

Usually we will reference a field just as $\mathbb{F}$.

Exercise 2.143. Check that

1. real numbers understood informally, have the field properties
2. rational numbers form a field

From the above field axioms, you can derive many facts that may be obvious to you:

Exercise 2.144. Prove that there is 0 and 1 are unique. Hint: assume that 0 and 0' have property such that $a = a + 0 = a + 0'$ and try $a = 0$ and $a = 0'$.

Exercise 2.145. Prove that if $a + a' = 0$ and $a + a'' = 0$, then $a' = a''$. Therefore we can introduce special symbol for *the* additiv inverse: $a + (-a) = 0$ and define subtraction as $a - b := a + (-b)$.

Exercise 2.146. Prove that $-a = (-1) \cdot a$.

As you see, many of the algebraic properties we are used to can be recovered from the axioms, but sometimes it can be complicated. Both real numbers and rational numbers have also an order on them - for example $2 > 1$. It leads to the definition of *total order*.

Definition 2.147. *We call a pair* $(\mathbb{F}, \leq)$ *a totally ordered set if for every* $a, b \in \mathbb{F}$ *we have:*

1. *$a \le b$ or $b \le a$ (we call this property totality)*
2. *$a \le b$ and $b \le a$ imply $a = b$ (it's called antisymmetry)*
3. *$a \le b$ and $b \le c$ imply $a \le c$ (transitivity)*

Having relation $\le$ we can define others: $b \ge a$ means that $a \le b$ and $a < b$ means that $a \le b$ and $a \ne b$.

Definition 2.148. ***Ordered field*** *is a field $\mathbb{F}$ with a total order such that:*

- *$a \le b$ implies $a + c \le b + c$*
- *$0 \le a$ and $0 \le b$ imply that $0 \le a \cdot b$*

We say that $\mathbb{F}_+ := \{x \in \mathbb{F} : x \le 0\}$ is a set of ***non-negative*** *numbers.*

Exercise 2.149. Check that non-negative numbers are closed under summation and multiplication (the sum and product of two non-negative numbers is non-negative).

Definition 2.150. *Consider a subset of a totally-ordered set $A \subseteq \mathbb{F}$. We say that x is an* ***upper bound*** *of A iff $x \ge a$ for every $a \in A$. In such case we say that A* ***is bounded from above****.*

Exercise 2.151. Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{Q}$. Prove that a set $A \subseteq \mathbb{F}$ can have no upper bounds or infinitely many of them.

Definition 2.152. *Let $A \subseteq \mathbb{F}$ be a set bounded from above. It's* ***supremum*** *or* ***lower upper bound*** *is a number $\sup A \in F$ such that:*

- *$\sup A$ is an upper bound of $\mathbb{F}$*
- *if y is an upper bound of A, then $y \ge \sup A$*

Supremum is often referenced as lub or l.u.b.

Exercise 2.153. Prove that supremum is unique, so if x and x' are supremums of A, then $x = x'$.

Exercise 2.154. Prove that $x = \sup A$ if and only if $x \ge a$ for every $a \in A$ and for every $\varepsilon > 0$ there is $a \in A$ such that $x < a + \varepsilon$.

Definition 2.155. ***Completeness axiom*** *- each non-empty, bounded from above subset of $\mathbb{R}$ has a supremum.*

This axiom allows us to prove many interesting things:

Exercise 2.156. Prove that natural numbers are *not* bounded from above. Hint: if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$.

Exercise 2.157. Prove the **Archimedean axiom**[17] that for every $r \in R$, there is $n \in \mathbb{N}$ such that $n > r$.

[17] In fact we do not need to call it axiom, as we are able to prove it.

Exercise 2.158. Prove that for any $r > 0$ there is $n \in \mathbb{N}$ such that $1/n < r$.

Exercise 2.159. Find infinite sum and intersection for the families of subsets of $\mathbb{R}$:

1. $A_i = (0, 1/i)$ for $i = 1, 2, \ldots$
2. $B_i = [0, 1/i)$ for $i = 1, 2, \ldots$

Exercise 2.160. Prove that rational numbers do *not* have the completeness property:

1. Let $p, q \in \mathbb{Z} \setminus \{0\}$. Prove that $p^2 \neq 2q^2$.
2. Prove that root of two, defined as $x > 0, x^2 = 2$ is not rational.
3. Find a subset of $\mathbb{Q}$ that is bounded above, but has no rational supremum.

Exercise 2.161. You should prove that in each nonempty interval there is at least one rational number:

1. Assume that $0 < a < b$. Define
$$A = \left\{\frac{m}{N} : m \in \mathbb{N}\right\}, \quad \frac{1}{b-a} < N \in \mathbb{N}$$
and prove that $A \cap (a, b)$ is non-empty.
2. Use the above result to prove that in *each* interval there is at least one rational number.
3. Prove that in each interval there are infinitely but countably many, rational numbers.
4. Prove that in each interval there is an irrational number.
5. How many irrational numbers are in each interval?

2.7.2 Absolute value

Another concept that will be further useful is the **absolute value** of a real number: if $x \in \mathbb{R}$ we write $|x| \in \mathbb{R}$ for:

$$|x| = \begin{cases} x & \text{for } x \geq 0 \\ -x & \text{otherwise} \end{cases}.$$

Exercise 2.162. Prove that for every $x, y \in \mathbb{R}$:

1. $|x| = |-x|$
2. if $|x| = |y|$ then $x = y$ or $x = -y$.
3. $|x + y| \leq |x| + |y|$ (this is called **triangle inequality**)
4. $|x - y| \leq |x| + |y|$
5. $||x| - |y|| \leq |x-y|$ (this is sometimes calles **reverse triangle inequality**)

2.7.3 Mathematical induction

We characterise natural numbers as a subset of $\mathbb{R}$ with some properties.

Definition 2.163. *Let $A \subseteq \mathbb{R}$ be a set such that:*

- $0 \in A$
- *if $n \in A$, then $n+1 \in A$*

*The intersection of all sets with this property is called **the set of natural numbers**. Alternatively, natural numbers is the smallest set (in sense of subset order) with the properties listed above.*

These properties allow us to define a powerful proof technique:

Definition 2.164. ***Principle of mathematical induction*** *- let f be a logical statement defined for all natural numbers (that is $f(n)$ is either true or false). Then if $f(0)$ is true and an implication:*

$$f(n) \Rightarrow f(n+1)$$

is true for every n, then $f(n)$ is true for every n.

Have you ever seen falling dominoes? To be sure that all domino falls, we need to:

1. punch the first domino
2. every domino must punch the next domino (if this particular domino falls, the next one also falls)

And that's all, we can be sure that all the dominoes will eventually fall.

Example 2.165. We'll prove that $2|n(n+1)$ for every $n \in \mathbb{N}$ ($a|b$ means: a divides b).

1. the statement is true for 0: $2|0 \cdot 1$ as $0 = 2 \cdot 0$
2. I need to prove that $(2|n(n+1)) \Rightarrow (2|(n+1)(n+2))$ for every n. Assume that n is such a number that $2|n(n+1)$. Then $(n+1)(n+2) = n(n+1) + 2 \cdot (n+1)$ is divisible by 2, what we needed to prove.

Therefore from the principle of mathematical induction we know that for all number of the form $n(n+1)$ are divisible by 2[18].

Exercise 2.166. 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...)

[18] 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.

Exercise 2.167. 1. Prove[19] that 6 divides $n^3 - n$ for all natural n.
2. Prove[20] 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 2.168. (Bernoulli's inequality) Prove that for real $x > -1$ and natural $n \geq 1$, the following inequality holds:

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

Exercise 2.169. In Mathsland 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: 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.
2. Prove that there is a city[21] to which you can drive from all the others.

Exercise 2.170. 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?

---

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

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

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

3

Taste of category theory

> Category theory [...] is the "mathematics of mathematics". Robert Geroch

As you have had training in sets and functions, we are able to introduce some category theory that will quickly become useful - most of the objects in mathematics form a category and this language will be extremely convenient to find similarities between different branches of mathematics. As we remember, it is not possible to create a set of all sets without having a contradiction. So let's use a word **collection** of sets or **class** [1] of sets - that is not a set and we don't know how to express it formally - but what has an intuitive sense.

Definition 3.1. *A **category** is:*

1. *a collection of objects such that*
2. *for each pair objects A, B in the collection there is a* set[2] *$Hom(A, B)$ called the set of **morphisms** or **maps** or **arrows** such that*
3. *for morphisms $f \in Hom(A, B), g \in Hom(B, C)$ there is a morphism $g \circ f \in Hom(A, C)$. We also require:*
   - *that composition of morphisms is associative: $h \circ (g \circ f) = (h \circ g) \circ f$, where $h \in Hom(C, D)$*
   - *we have morphisms $Id_X : X \to X$ for every object X such that $f \circ Id_A = f = Id_B \circ f$ for $f \in Hom(A, B)$*

*If $f \in Hom(A, B)$, we can also write $f : A \to B$ or $A \xrightarrow{f} B$. Some authors also write $Mor(A, B)$ for $Hom(A, B)$ and gf for $g \circ f$. If the collection of objects happens to be a set, we call it **small category**.*

Example 3.2. We already know very well a category - the category of sets and functions. Let's check carefully that is actually is a category:

[1] Formal treatment of classes - collections that are in some sense bigger than sets - is introduced in von Neumann–Bernays–Gödel and Morse-Kelley set theories.

[2] Many authors don't assume that it is a set. Our definition is their "locally small" category.

1. objects are just sets
2. take $\mathrm{Hom}(A, B)$ as a set of all functions from A to B (why is it a set?)
3. define composition of morphisms just as function composition
   - composition of functions is associative (recall why)
   - identity morhpism is just identity function of a set

Exercise 3.3. Consider a category with one singleton: $\{\{0\}\}$, where $\{0\}$ is the only object, and functions as arrows. How many arrows are in this category?

Exercise 3.4. Consider a category with two singletons: $\{\{0\}, \{1\}\}$, and functions as arrows. How many arrows can be in this category? Hint: 4 numbers.

3.0.1 Morphisms

In set theory we introduced special functions - injections, surjections and bijections. We would like to generalise it into category theory. Unfortunately, we cannot just state their properties in terms of elements, as objects do not need to be sets and we cannot take a look at elements. Therefore, let's introduce the following:

Definition 3.5. *Let $f : A \to B$ be a morphism. We say that is it* ***left-cancellative*** *or that it is a* ***monomorphism*** *iff for every two morphisms $g, g' \in Hom(X, A)$ we have:*

$$f \circ g = f \circ g' \Rightarrow g = g'.$$

Sometimes monomorphism is written as $f : A \hookrightarrow B$. We will also refer to monomorphism as ***monic*** *morphisms*[3]*.*

As you can prove, this works as injections in the category of sets:

Exercise 3.6. Here you should prove that in the category of sets, "injective" are identical to "monic".

1. Prove that an injection in the category of sets is a monomorphism.
2. Prove that if function $f : A \to B$ is not injective, then it is not monic. Hint: if $f(x) = f(y)$ for $x \neq y$, create functions from $\{x, y\}$ to A showing that f is not monic.

You can see that if we considered a different category, with less morphisms, the construction wouldn't work. So even if we consider sets and functions, but with some restrictions or additional structure, we need to carefully investigate the relation between monomorphisms and injections.

Exercise 3.7. Consider a set $\{\{0, 1\}, \{10, 11\}\}$. Construct three morphisms such that this set becomes a category, but there is a non-injective monomorphism.

[3] Note that some authors distinguish between monomorphisms and monic morphisms.

Definition 3.8. *Let $f : A \to B$ be a morphism. We say that is it* ***right-cancellative*** *or that it is a* ***epimorphism*** *iff for every two morphisms $g, g' \in Hom(B, Y)$ we have:*

$$g \circ f = g' \circ f \Rightarrow g = g'.$$

We will also refer to epimorphisms as ***epic*** *morphisms*[4].

Exercise 3.9. Here you should prove that in the category of sets, "surjective" is identical to "epic".

1. Prove that a surjection in the category of sets is an epimorphism.
2. Prove that if function $f : A \to B$ is not surjective, then it is not epic. Hint: if f is not surjective, then both $\operatorname{Im} f$ and $B \setminus \operatorname{Im} f$ are non-empty. Define suitable functions.

Also here a problem may appear - there are categories in which surjections make sense, but are not identical to epimorphisms.

Exercise 3.10. Create a category with a non-surjective epimorphism.

Also we have an object looking as bijection:

Definition 3.11. *Let $f : A \to B$ be a morphism. We say that is is an* ***isomorphism*** *if there is a morphism $g : B \to A$ such that $f \circ g = Id_B$ and $g \circ f = Id_A$.*

Exercise 3.12. Prove that in every category an isomorphism is both monic and epic.

Exercise 3.13. Create a category with a morphism that is both monic and epic, but is not an isomorphism.

But there are nice categories, as the category of sets, for which it holds.

Exercise 3.14. Prove that in the category of sets, a morhpism is an isomorphism iff is bijective.

Isomorphisms will occur frequently in this book - in the section describing equivalence relations, we discovered a concept of identifying some objects (like splitting integers into two equivalence classes odd and even numbers). We will usually try to identify some objects in a given category. Isomorphisms are very suitable for that.

Exercise 3.15. "Equivalence" properties of isomorphisms:

1. Prove that if there is an isomorphism from A to B, then there is an isomorphism from B to A.
2. Prove that there is an isomorphism from A to A.

[4] Note that some authors distinguish between epimorphisms and epic morphisms.

3. Prove that if there is an isomorphism from A to B and B to C, then there is also an isomorphism from A to C.

This "equivalence" structure will be used to idenfify some spaces. Note that if this has properties of an equivalence relation, but being formal, a relation on a *set* A is a subset of $A \times A$. As we are dealing with categories now, that are not necessarily sets, we cannot say formally that isomorphisms give an equivalence relation. However, we will sometimes say that informally.

3.1 Functors

Definition 3.16. *Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A **covariant functor** $\mathcal{F}$ from $\mathcal{C}$ to $\mathcal{D}$ is an assignment*[5] *such that:*

1. *for each object X of $\mathcal{C}$ there is an object $\mathcal{F}(X)$ in category $\mathcal{D}$*
2. *for each morphism $f : X \to Y$ in $\mathcal{C}$ there is a morphism $\mathcal{F}(f) : \mathcal{F}(X) \to \mathcal{F}(Y)$ such that:*
   a) *$\mathcal{F}(Id_X) = Id_{\mathcal{F}(X)}$*
   b) *$\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$ for $f : X \to Y$ and $g : Y \to Z$ being morphisms of $\mathcal{C}$.*

3.2 Limits and colimits

[5] We cannot use word function - functions are special subsets of the Cartesian product of two sets: domain and codomain. Here you should think intuitively about it - as collections are in some sense bigger sets, functors are bigger versions of functions.

Part II

Abstract algebra

4

Groups

Definition 4.1. *A **group** is a pair $(G, \cdot)$, where G is a set and $\cdot : G \times G \to G$ is a function called **group law** with properties listed below. It's a common practice to write $a \cdot b := \cdot(a, b)$ or even $ab := \cdot(a, b)$. These properties are:*

1. *associativity: for every $a, b, c \in S$ we have $(ab)c = a(bc)$*
2. *existence of right identity: there is $e \in G$ such that $ae = a$ for every $a \in G$*
3. *existence of right inverse: for each $a \in G$ there exists an element called a^{-1} such that $aa^{-1} = e$*

*If $ab = ba$ for every $a, b \in G$, we say that the group is **abelian**. If $|G|$ is finite, we say that the group is **finite**. Sometimes group $(G, \cdot)$ is referenced as just G, if group law is known from the context.*

Before we start investigating the properties, we will provide some examples.

Example 4.2. Pair $(\mathbb{Z}, +)$ is a group, as $(a + b) + c = a + (b + c)$, $a + 0 = a$ and $a + (-a) = 0$ for every $a, b, c \in \mathbb{Z}$. The role of e is played by 0 and right inverse a^{-1} is known just as $-a$. Moreover it is abelian, as $a + b = b + a$ for every $a, b \in \mathbb{Z}$.

Exercise 4.3. Let S be a set and $\mathcal{S}$ be a set of all bijections from S to S. Prove that $(\mathcal{S}, \circ)$ is a group, where $\circ$ is usual function composition. Why this group is usually not abelian?

As we are faimilar with groups, we can start investigating their properties. First concern is the word *right* - why is it right, and not left?

Exercise 4.4. Right, left, whatever - it is two-sided. Let $(G, \cdot)$ be a group with right identity e. You will prove that e is two-sided identity, that is $ae = ea$ for every a. Moreover you will prove that a^{-1} is two-sided inverse: $a^{-1}a = aa^{-1} = e$.

1. Prove that if $a \in G$ is indempotent, that is $aa = a$, then $a = e$. Hint: what is aaa^{-1}?
2. Prove that right inverse is also left inverse, that is $a^{-1}a = e$ for every a. Hint: what is $a^{-1}aa^{-1}a$?
3. Prove that right identity is also left identity. Hint: what is $aa^{-1}a$?

As we fixed this issue, we can start thinking about uniqueness of identity and inverse

Exercise 4.5. Consider a group G with identity e.

1. Prove that identity is unique, that is if there is an element e' such that $ae' = a$ for every a, then $e = e'$.
2. Prove that inverse is unique, that is if $ab = e$, then $b = a^{-1}$
3. What is the inverse of a^{-1}?

Therefore we can give an equivalent definition of group:

Definition 4.6. *A **group** is a pair $(G, \cdot)$, where G is a set and $\cdot : G \times G \to G$ is a function called **group law** (written as $\cdot(a, b) = ab$) with the following properties:*

1. *associativity: for every $a, b, c \in S$ we have $(ab)c = a(bc)$*
2. *existence of identity: there is* a unique *$e \in G$ such that $ae = ea = a$ for every $a \in G$*
3. *existence of inverse: for each $a \in G$ there exists* a unique *$a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$*

This definition looks much better than the previous - we have more properties clearly listed and we do not need to reference each time e.g. the proof that inverse is two-sided, we can just use it. The disadvantage is that proving that something is a group is *longer* - we have more properties to check. So our strategy will be to check whether group law candidate is associative, provide *an* identity and a rule how to find *an* inverse, and since then using all the properties listed in our "powerful" definition.

Exercise 4.7. Prove that in every group: $(ab)^{-1} = b^{-1}a^{-1}$.

Exercise 4.8. Let G be a group. Prove that it is abelian iff for every $a, b \in G$ the equality $(ab)^2 = a^2b^2$, where $(ab)^2 := abab$ and $a^2b^2 := aabb$.

Exercise 4.9. Let G be an abelian group[1]. Prove that there is exactly one $x \in G$ such that $ax = xa = b$ and define division in a group. Do you understand now what is $a - b$ in abelian group $(\mathbb{Z}, +)$?

Exercise 4.10. Let G be a finite group with an element such that $a^2 = e$, where e is the identity and $a \neq e$. Prove that $|G|$ is odd.

[1] Look, we dropped a group law sign.

4.1 The category of groups

To make all groups into a category, we need a notion of a morphism. As the only operation that is allowed in groups is group law, it makes sense to define the following map.

Definition 4.11. *Consider two groups:* $(G, \cdot)$ *and* $(H, \star)$*. A function* $f : G \to H$ *such that:*
$$f(a \cdot b) = f(a) \star f(b)$$
is called a ***homomorphism****.*

To prove that it is indeed a category, we need to check a few things:

Exercise 4.12. Prove that:

1. All homomorphisms between groups G and H form a set
2. If $f : F \to G$ and $g : G \to H$ are homomorphisms, then $g \circ f$ is a homomorphism
3. moreover $f \circ \mathrm{Id}_F = f = \mathrm{Id}_G \circ F$, where Id_X is the usual identity function on a set X

Exercise 4.13. Let G be a group with 3 elements. Prove that it is isomorphic to $(\mathbb{Z}_3, +)$. (So in fact there is only one group with three elements.)

Exercise 4.14. Find all the groups of order 4. You should find just two, both abelian.

5

Linear algebra

5.1 Vector spaces

Exactly as we did with fields or topological spaces, we will define vector spaces as a tuple with some properties. **Vector space**[1] over a field F is a tuple: $(F, V, +, \cdot)$, where the objects involved are:

- F is a field. It's elements are called **scalars**.
- V is a set. It's elements are called **vectors**.
- $+$ is a function $V \times V \to V$. We always write $v + u$ instead of $+(v, u)$.
- $\cdot$ is a function $F \times V \to V$. We always write $f \cdot v$ instead of $\cdot(f, v)$.

They should have the following properties:

1. $(u + v) + w = u + (v + w)$ for every $u, v, w \in V$ (associativity of addition)
2. $u + v = v + u$ for every $u, v \in V$ (commutativity)
3. There is $o \in V$ such that $v + o = v$ for all v (neutral element of addition)
4. For every $v \in V$ there is a $\tilde{v} \in V$ such that $v + \tilde{v} = o$ (additive inverse)
5. For every $f, g \in F$ and $v \in V$ we have $(fg) \cdot V = f \cdot (g \cdot V)$ (so the multiplication agrees with that for scalars)
6. As F is a field, we have $1 \in F$. For every $v \in V$ we want $1 \cdot v = v$.
7. For every $f \in F$ and $u, v \in V$ we have $f \cdot (u + v) = f \cdot u + f \cdot v$ (distributivity)
8. For every $f, g \in F$ and $u \in V$ we have $(f + g) \cdot u = f \cdot u + g \cdot u$

5.1. We know that the set of vectors must contain at least one vector (neutral element). Construct a vector space that has *exactly* one vector (so in some sense it is the smallest space).

It's high time we started to abuse our notation making it less explicit, but more convenient. First of all we usually ommit (as in the case of field) $\cdot$ for multiplication: $fv = f \cdot v$, for $f \in F, v \in V$. But that's not all!

5.2. We want to modify our notation in the following way:

[1] Sometimes vector spaces are also called**linear spaces**

1. Prove that o is unique element with the property $v + o = v$ for $v \in V$
2. Prove that $0 \cdot v = o$ for every v. Hint: remember that $1 + 0 = 1$. This suggests to write 0 for o (so 0 since now technically has two different meanings, practically we will never have any problems with that)
3. Let $v \in V$ and $\tilde{v} \in V$ be such an element that $v + \tilde{v} = 0$. Prove that $\tilde{v}$ is unique (so if $v' + v = 0$, then $\tilde{v} = v'$)
4. Prove that the $\tilde{v}$ is exactly $(-1)v$. It suggests to write $-v$ for additive inverse, and we will do it since now.

Moreover, if we specify the field od scalars and operations, we will say V for the vector space, without invoking the all tuple elements (as in the case with topological spaces or fields- we write a single $\mathbb{R}$ and everyone knows what field operations we allow and what topology is assumed).

In most cases we will be interested in non-patological vector spaces, namely „big enough" in some sense. Why?

5.3. The **characteristic** of a field F is the smallest natual number n such that $1 + 1 + \cdots + 1 = 0$, where we have n ones on the left hand side. If there is no such number we say that characteristic is 0.

1. Prove that $\mathbb{R}$ has characteristic 0.
2. Let (F, V) be a vector space with at least two elements. Prove that $v = -v$ for every $v \in V$ if and only if the scalar field has characteristic 2.
3. Prove that if F has characteristic different from 2, then we have $v = -v$ iff $v = 0$.

5.4. An important example of a vector space over a field F is F^n, where addition and scalar multiplication are defined pointwise: $f \cdot (a_1, a_2, \ldots, a_n) = (fa_1, fa_2, \ldots, fa_n)$, $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$. Prove that it is indeed a vector space.

5.1.1 Bases of vectos spaces

In topology we introduced a basis as a family of open sets from each every open set could be constructed in some natural way. This useful concept occurs also in vector spaces - as you can see, F^n has an interesting property: each element $(a_1, a_2, \ldots, a_n) \in F^n$ can be written in a form $a_1e_1 + a_2e_2 + \cdots + a_ne_n$, where e_k has 1 at k-th place and 0s in the other. Moreover, if $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$, then the only possibility for the equation $\lambda_1e_1 + \lambda_2e_2 + \cdots + \lambda_ne_n = 0$ to hold is $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$. This suggests the following definitions: let $U \subseteq V$. A set $\operatorname{span} U$ is defined as:

$$\operatorname{span} U = \{\lambda_1u_1 + \lambda_2u_2 + \cdots + \lambda_nu_n : \lambda_1, \ldots, \lambda_n \in F, u_1, \ldots, u_n \in U\}.$$

Alternatively, we can say that $\operatorname{span} U$ is a subset of V such that each $v \in \operatorname{span} U$ can be wrtitten as a finite **linear combination** of elements from U. It is important to *disallow* infinite combinations - the concept of an infinite sum is essentialy topological and we have *not* assumed any topology on our space yet! Therefore we cannot define convergence and infinite sums.

5.5. Consider infinite real sequences with addition and multiplication by a real number defined pointwise: $c = a + b$ iff $c_n = a_n + b_n$ for all n and $b = ra, r \in \mathbb{R}$ iff $b_n = ra_n$ for all n.

1. Prove that this is a vector space, let's call it $\mathbb{R}^{\mathbb{N}}$.
2. Prove that set $B = \{e_k : k \in \mathbb{N}\}$, e_k has 1 at k-th place and 0 at all the others, does *not* span $\mathbb{R}^{\mathbb{N}}$.
3. Let $\hat{\mathbb{R}}^{\mathbb{N}} \subseteq \mathbb{R}^{\mathbb{N}}$ contain all the sequences that have a *finite* number of non-zero elements. Prove that this is a vector space and that it is spanned by B defined above.

Definition 5.1. *Let V be a vector space. We say that set $U \subseteq V$ is* ***linearly independent*** *if for every finite subset of U: $\{v_1, v_2, \dots, v_n\}$, the only solution of the equation*

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$$

is trivial: $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$. If a set of vectors is not linearly independent, we say that it is ***linearly dependent****. Sometimes we abuse the terminology and say that vectors $v_1, v_2, \dots, v_n$ are linearly independent - it means that the set $\{v_1, v_2 \dots, v_n\}$ is linearly independent - linear independence is a property of a set of vectors, not a property of a single vector!*

Exercise 5.2. Let V be a vector space and consider a finite set $\{v_1, v_2, \dots, v_n\} \subseteq V$. Prove that it is linearly independent iff the only solution to the equation:

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$$

is $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Exercise 5.3. Consider a finite set $U = \{v_1, v_2, \dots, v_n\}$ with at least two vectors. Prove that the following two statements are equivalent:

- U is linearly dependent
- there is $v_i \in U$ such can be written as linear combination of other vectors: $v_i \in \operatorname{span}\{v_1, \dots, v_{i-1}, v_{i+1}, v_n\}$

Definition 5.4. *We say that a vector space V has* ***finite dimension*** *(or is finite dimensional) if there is a finite $U \subseteq V$ such that $V = span U$.*

Exercise 5.5. You can prove that every finite dimensional vector space has a basis in two steps:

1. Assume that you have a set $\{e_1, e_2, \dots, e_n\}$ that spans V. Prove that if $e_1 \in \operatorname{span}\{e_2, \dots, e_n\}$, then $V = \operatorname{span}\{e_2, \dots, e_n\}$.
2. Using the reduction step given above, show an algorithm finding a basis from a finite spanning set.

3. Prove that a vector space is finite dimensional iff it has a finite basis.

5.6. Prove that $\mathbb{F}^n$ is finite dimensional. Hint: just find a basis.

5.7. Prove that $\hat{\mathbb{R}}^{\mathbb{N}}$ has a basis.

Apparently the proof that *every* vector space is equivalent[2] to the Axiom of Choice!

Exercise 5.6. You can see how to prove the basis existence with the help of Zorn's lemma. Let V be a vector space.

1. Let $\mathcal{A} = \{U \subseteq V : U \text{ is linearly independent}\}$. Prove that $\mathcal{A}$ is not empty.
2. Prove that relation on A given by $A \preceq B \Leftrightarrow A \subseteq B$ is a partial order.
3. Consider any chain $\mathcal{C} \subseteq \mathcal{A}$. Define $C = \bigcup \mathcal{C}$. We want to prove that C is linearly independent.
4. Assume that C is linearly dependent, so $0 = \lambda_1 v_1 + \ldots \lambda_n v_n$ for some $v_i \in C$. If $v_i \in C_i \in \mathcal{C}$, what can you conclude about $C_1 \cup C_2 \cup \cdots \cup C_n$?
5. From Zorn's lemma we know that there is a *maximal* element A in $\mathcal{A}$. What if A does not span V? Hint: add an element that is not in the span and think about linear independence of new set. A is maximal, isn't it?

5.8. Here you will prove that all the bases of a *finite dimensional* vector space have the same number of elements. Let $v_1, v_2, \ldots, v_n$ be a basis of a vector space V and $w_1, w_2, \ldots, w_m \in V$, where $m > n$.

1. **(Steinitz exchange lemma)** Prove that if $w_1 \neq 0$, then $v_1 \in \operatorname{span}\{w_1, v_2, v_3, \ldots, v_n\}$.
2. Prove that if $w_k \neq 0$ for $k \in \{1, 2, \ldots, n\}$, then $w_{n+1} \in V = \operatorname{span}\{w_1, w_2, \ldots, w_n\}$
3. Prove that $w_1, w_2, \ldots, w_m$ *cannot* be linearly independent.
4. Prove that each basis of V has the same number of elements. This number is called **the dimension of** V and written as $\dim V$.

Exercise 5.7. Let V be a finite dimensional vector space of dimension n. Prove that:

1. every linearly independent set of n vectors spans V (so must span V)
2. every set with n elements spanning V is a basis (so must be linearly independent)

5.9. Here you will prove that every linearly independent set of vectors can be extended to a basis of a finite dimensional vector space. Let V be a finite dimensional vector space of dimension n.

1. Let $S = \{v_1, v_2, \ldots, v_k\} \subseteq V$ be linearly independent. Prove that if $u \in V$, but $u \notin \operatorname{span} S$, then $\{u\} \cup S$ is linearly independent.

[2] Proof that AC is implied by statement "every vector space has a basis" was given by Andreas Blass in 1984! It can be found here: `http://www.math.lsa.umich.edu/ ablass/bases-AC.pdf`

2. Prove that there are $u_1, u_2, \dots, u_{n-k}$ such that $v_1, v_2, \dots, v_k, u_1, u_2, \dots, u_{n-k}$ is a basis of V.

5.10. Assume that you have a basis $e_1, e_2, \dots, e_n$ of a finite dimensional vector space V over a field $\mathbb{F}$. Therefore every vector v can be written as a sum $v = v_1e_1 + v_2e_2 + \cdots + v_ne_n$ for some $v_i \in \mathbb{F}$. Prove that these numbers are unique, that is if $v = v_1e_1 + v_2e_2 + \cdots + v_ne_n = v_1'e_1 + v_2'e_2 + \cdots + v_n'e_n$, then $v_i = v_i'$ for all i. Hint: $0 = v - v$ and e_i are linearly independent.

5.1.2 Subspaces, direct sum and quotient spaces

As in the case of topological spaces, there are many ways of constructing *new* vector spaces from old. In topology we could construct new spaces taking a subset of a known topological space, take disjoint unions (sums) of topological spaces, divide topological spaces by some relations and take product of them. In this subsection we cover first three constructions - fourth one gives a raise to the concept of tensors and multilinear algebra and we will cover it in great detail later. Consider a vector space V over field F and a subset $U \subset V$ such that $0 \in U$ and for all $v, u \in U, f \in F$, we have $fv + u \in U$. You can check that it is indeed a vector space:

5.11. Prove that $fv + u \in U$ for all v, $u \in U, f \in F$ is equivalent to: for every v, $u \in U$, we have $v + u \in U$ and for every $v \in U, f \in F$ we have $fv \in U$.

Such a U we call a **vector subspace** of V.

5.12. Let V be a finite dimensional vector space and $U \subseteq V$ be a vector subspace. Prove that U is finite dimensional and $\dim U \leq \dim V$.

5.13. Let V be a finite dimensional vector space and $U \subseteq V$ be a vector subspace. Prove that $\dim U = \dim V$ iff $U = V$.

There is also a method of constructing direct sums: assume that you have two vector spaces V, W over *the same field* F. We define their direct sum as:

$$V \oplus W = V \times W = \{(v, w) : v \in V,\ w \in W\}$$

with addition and multiplication defined entrywise:

$$a(v, w) + (v', w') = (av + v', aw + w').$$

We often identify $v \in V$ with $(v, 0) \in V \oplus W$ and $w \in W$ with $(0, w) \in V \oplus W$. Then $av + bu, a, b \in F, v \in V, u \in U$ should be understood as $(av, bu) \in V \oplus U$.

5.14. Prove that each $w \in V \oplus U$ has a *unique* decomposition: $w = v + u$, $v \in V$, $u \in U$. That is if $w = v + u = v' + u'$, then $v = v'$ and $u = u'$ for $v, v' \in V$, $u, u' \in U$.

5.15. Let U and V be finite dimensional vector spaces. Prove that $\dim U \oplus V = \dim U + \dim V$.

5.16. Let V_1, V_2, V_n be finite dimensional vector spaces. Prove that

$$\dim V_1 \oplus V_2 \oplus \cdots \oplus V_n = \dim V_1 + \dim V_2 + \cdots + \dim V_n.$$

Our general definition has a very nice interpretation when we go to subspaces - now assume that you have two subspaces of V: $U, W \subseteq V$ such that $U \cap W = 0$. Their **direct product** is a set:

$$U \oplus W = \{u + v : u \in U,\, v \in V\}$$

5.17. Prove that the direct product of two vector subspaces is a special case of the general definition if we identify $U \ni u \leftrightarrow (u, 0) \in U \times V$, $V \ni v \leftrightarrow (0, v) \in U \times V$ employed.

5.18. Prove directly that direct product of two vector subspaces of V is a vector subspace of V. Hint: check if 0 is inside and use the handy, one-line criterion.

5.19. Let U be a subspace of V and V be a subspace of W. Prove that U is subspace of W.

5.20. Let $V = \mathbb{R}^2$ and $U = \{(0, r) : r \in \mathbb{R}\},\ W = \{(r, 0) : r \in \mathbb{R}\}$. Prove that:

1. $V = U \oplus W$.
2. Prove that $U \cup V$ is *not* a vector space.

5.21. Let $U, W \subseteq V$ be two vector subspaces of a finite vector space V. Prove that:

1. $U \cap W$ is a subspace of U, W and V.
2. $U + W := \{u + w : u \in U, w \in W\}$ is a vector subspace[3] of V
3. Take a basis B_i of $U \cap W$ and extend it using some vectors $B_U \subseteq U$ such that $B_i \cup B_U$ is a basis of U. Repeat this procedure of W defining B_W and prove that $V = \operatorname{span} B_i \cup B_U \cup B_W$.
4. Prove that $B_i \cup B_U \cup B_V$ is linearly independent. Hint: write the condition of linear independence. Express the linear combination of the elements of B_U as a linear combination of B_i and B_V. Why is this linear combination in $U \cap V$? What you can conclude from the fact that $B_i \cup B_U$ is a basis?
5. Prove that $\dim U + V = \dim U + \dim V - \dim U \cap V$.

[3] if $U \cap W = \varnothing$ we have just $U + W = U \oplus W$

5.1.3 Quotient spaces

Let us introduce a relation:

5.22. Consider vector space V and it's subspace U. We introduce a relation on V: $v \approx u$ iff $v - u \in V$. Prove that $\approx$ is an equivalence relation.

We have an equivalence relation, so it splits V into equivalence classes $V/\approx$.

5.23. Prove that addition and scalar multiplication on $V/\approx$ are well-defined (independent on the class representative), that is:

1. if $v \approx v'$ and $u \approx u'$, then $v + u \approx v' + u'$
2. if α is a scalar and $v \approx v'$ are vectors in V, then $\alpha v \approx \alpha v'$.

5.24. Prove that under relation $\approx$, U is identified with 0.

We have vector addition and scalar multiplication, we have a neutral element - we have a new vector space! This vector space is called **quotient space** and usually written as V/U.

5.25. Let $U \subseteq V$ be finite-dimensional vector spaces. Prove that $\dim V/U = \dim V - \dim U$. Hint: guess what is the basis of V/U starting with basis of U and completing it to the basis ov V.

5.2 Linear maps

As continous functions are in some kind, natural mappings between topological spaces, we can define such natural mappings between vector spaces. Let V and W be vector spaces over the same field $\mathbb{F}$. We say that a function $L : V \to W$ is **linear** iff $L(\alpha v + \beta u) = \alpha L(v) + \beta L(u)$ for every $v, u \in V$, $\alpha, \beta \in \mathbb{F}$.

5.26. Let $L : V \to W$ be a function between vector spaces over field $\mathbb{F}$. Prove that the following sentences are equivalent:

1. L is linear
2. for every $u, v \in V$ and $\alpha \in \mathbb{F}$, we have $L(\alpha u + v) = \alpha L(u) + L(v)$
3. for every $v, u \in V$ we have $L(v + u) = L(v) + L(u)$ and for every $v \in V, \alpha \in \mathbb{F}$ we have $L(\alpha v) = \alpha L(v)$

5.27. Let U be a vector subspace of V. Prove that **the inclusion map** $\iota : U \to V$ given as $\iota(u) = u$ is linear.

5.28. Let U be a vector subspace of V. Prove that **the quotient map** $q : V \to V/U$ given as $q(v) = [v]$ is linear.

5.2.1 Kernel and cokernel

5.29. Let $L : V \to W$ be a linear map between vector spaces.

1. Prove that $L(0_V) = 0_W$, where 0_V is the neutral element in V and 0_W is the neutral element in W.
2. Prove that the **kernel of** L defined as: $\ker L = \{v \in V : L(v) = 0_W\}$ is a vector subspace of V.
3. Prove that the image of L is a vector subspace of W. The dimension of $\operatorname{Im} L$ is called **the rank** of L: $\operatorname{rk} L = \dim \operatorname{Im} L$.
4. Let $V = \operatorname{span} S$. Prove that $\operatorname{Im} L = \operatorname{span} L(S)$. Here $L(S)$ has meaning $\{L(s) : s \in S\}$.
5. Prove that if V is finite dimensional, then $\operatorname{Im} L$ is also finite dimensional.

Using kernel we can say whether a linear function is injective:

5.30. Prove that $\varphi : V \to U$ is injective iff $\ker \varphi = \{0\}$.

There is a similar concept, checking the surjectivity. We say that the cokernel of a linear map $L : V \to U$ is a *quotient* vector space: $U/\operatorname{Im} L$.

5.31. Prove that $\varphi : V \to U$ is surjective iff $\operatorname{coker} \varphi$ has exactly one element (is a trivial vector space).

5.2.2 Rank-nullity theorem

You can prove the rank-nullity theorem:

5.32. Prove the **rank-nullity theorem** - if V is a finite dimensional vector space and $L : V \to W$ is linear, then $\dim \ker L + \operatorname{rk} L = \dim V$.

5.33. You can do a beuatiful and simple proof of $\dim U + V = \dim U + \dim V - \dim U \cap V$, where U and V are finite-dimensional subspaces of some greater space S. Consider a map $L : U \times V \to S$ defined as $L(u, w) = u - w$. Prove that it is a linear map (we give $U \times V$ a linear space structure using entry-wise operations, as in $U \oplus V$). What is it's range and kernel?

5.34. Let $\varphi : V \to U$ be a map between finite-dimensional vector spaces. Prove that the **index** of φ defined as $\operatorname{index} \varphi = \dim \ker \varphi - \dim \operatorname{coker} \varphi$ is equal to: $\operatorname{index} \varphi = \dim V - \dim U$.[4]

In the category of topological spaces, homeomorphic spaces have the same topological properties (as connectedness or Haussdorf property). We say that a map $L : W \to W$ is a **isomorphism**[5] **of vector spaces** iff is bijective and

[4] This is a very important result - index, defined with the help of a chosen function is doesn't in fact depend on this function! A beautiful generalisation of this result, is called Atiyah-Singer index theorem.

[5] from the Ancient Greek *isos* - equal and *morphe* - shape

both L and L^{-1} are linear and we can say that abstract[6] vector spaces are identical if they are isomorphic.

5.35. Prove that V and $\{0\} \times V$ are isomorphic. (Do you remember the direct sum of two subspaces? In fact we used there this isomorphism).

You can also classify all finite-dimensional vector spaces over the same field, up to isomorphism:

5.36. Prove that two finite-dimensional vector spaces are isomorphic if and only if they have the same dimension. Hint: right implication - rank-nullity theorem, left - write down bases.

As we remember $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$. Therefore many people learn how to work only on them, as all the vector space properties can be just transferred from $\mathbb{F}^n$. We will not do it, as the isomorphism is usually not-unique and does not preserve additional structures, very important in more advanced geometry. Such chosen isomorphisms will later give a raise to objects called metric tensors and symplectic forms.

5.2.3 Exact sequences

In algebraic topology topological spaces are investigated by assigning to them algebraic objects, like vector spaces or groups. One of frequently-occuring concept are exact sequences. Consider a sequence of vector spaces[7] $V_i,\ i \in \{1, 2, \dots\}$ and linear maps between them $\varphi_i : V_i \to V_{i+1}$. It is often written as:

$$\dots \xrightarrow{\varphi_{i-1}} V_i \xrightarrow{\varphi_i} V_{i+1} \xrightarrow{\varphi_{i+1}} \dots,$$

and map φ_i is referenced as $V_i \to V_{i+1}$. We say that the sequence is **exact** if $\operatorname{Im} \varphi_i = \ker \varphi_{i+1}$ for all i.

5.37. Prove that if sequence of vector spaces V_i and maps $\varphi_i : V_i \to V_{i+1}$, is exact, then $\varphi_i \circ \varphi_{i+1} = \mathbf{0}$, where $\mathbf{0}$ is a null [8] map $\mathbf{0} : V_i \to V_{i+2}$ defined as $\mathbf{0}(v) = 0$.

Consider a 0-dimensional vector space $\{0\}$, which is usually abbreviated to just 0[9]. An exact sequence (Remember! Here 0 means $\{0\}$):

[6] Later we will define additional structures on vector spaces for which just arbitrary isomorphisms are not sufficient

[7] Or, more generally, Abelian groups as we will need only to use such properties as kernel, image and quotient spaces.

[8] Later we will refer to this map just as 0 - now this symbol has at least three meanings! It can be an additive neutral element of a field, a neutral element in a vector space or a linear map!

[9] Similar notational discrepancy was in the set theory - we wanted to write $f^{-1}(a)$ for $f^{-1}(\{a\})$.

$$0 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_3} V_4 \xrightarrow{\varphi_4} 0$$

is called a **short exact sequence**. Longer exact sequences are called, obviously, **long exact sequences**.

5.38. Prove the following:

1. sequence $V \xrightarrow{\varphi} U \longrightarrow 0$ is exact iff φ is surjective. Hint: what is kernel of the map $U \to 0$?
2. sequence $0 \longrightarrow V \xrightarrow{\varphi} U$ is exact iff φ is injective. Hint: do you remember how injectivity is related to some kernel?
3. sequence $0 \longrightarrow V \xrightarrow{\varphi} U \longrightarrow 0$ is exact iff V and U are isomorphic.
4. short sequence $0 \longrightarrow V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_3} V_4 \longrightarrow 0$ is exact iff φ_2 is injective and φ_3 is surjective.

5.39. Use the rank-nullity theorem and prove that if $0 \to V_0 \to V_1 \to \cdots \to V_{n-1} \to V_n \to 0$ is exact, then

$$0 = \sum_{i=0}^{n} (-1)^i \dim V_i.$$

5.40. Consider a linear map $L : V \to U$. Prove that the sequence:

$$0 \longrightarrow \ker L \xrightarrow{\kappa} V \xrightarrow{L} U \longrightarrow \operatorname{coker} L \longrightarrow 0$$

is exact, where $\kappa : \ker L \to V$ is inclusion map: $\kappa : \ker L \ni l \to l \in V$.

5.41. Let $L : V \to U$ be a map between finite-dimensional vector spaces. Prove once again that the index $L := \dim \ker L - \dim \operatorname{coker} L = \dim V - \dim U$.

5.3 Dual spaces

Consider a vector space V over a field $\mathbb{F}$ and the set of all *linear* functions from V to $\mathbb{F}$. This set is called **the dual space** V^*. Apparently, this set is a vector space!

5.42. Prove that V^* is a vector space by:

1. Finding the neutral element. Hint: function that always yields 0 is linear.
2. Proving that addition and scalar multiplication can be defined, so if μ, $\omega \in V^*$ and $a \in \mathbb{F}$, then function $a\mu+\omega$, defined as: $(a\mu+\omega)(v) = a\cdot\mu(v)+\omega(v)$ for all $v \in V$, is linear.

Sometimes we write $\langle \omega, v\rangle := \omega(v) \in \mathbb{F}$ for $v \in V$ and $\omega \in V^*$.

5.43. Let $V^{**} = (V^*)^*$ be the dual space of the dual space to V. We will try to prove that, in some sense, V is a subset of it. Prove that:

1. For each $v \in V$ there is a $\tilde{v} \in V^{**}$ such that for every $\omega \in V^*$ such that $\langle \tilde{v}, \omega \rangle = \langle \omega, v \rangle$
2. Prove that the map $v \mapsto \tilde{v}$ is a monomorphism (an injective linear map).

5.44. Let $f : V \to U$ be a linear map between finite dimensional spaces. We define $f^* : U^* \to V^*$ as follows: Prove that such map is linear and that

$$\begin{tikzcd} V \arrow[rr, "f"] \arrow[dr, "f^*(\omega)"'] & & U \arrow[dl, "\omega"] \\ & \mathbb{R} & \end{tikzcd}$$

$f^* \circ \omega = \omega \circ f$ for every $\omega \in U^*$. Here we see how a function sending vectors in one direction can naturally induce a linear map that „pulls-back" dual vectors.

Therefore we can think about V as a set of *some* linear functions on V^* and write $v(\omega)$ as well as $\omega(v)$. The word *some* is necessary - we have proven that it is a monomorphism, but we don't know whether it is an isomorphism[10]! Fortunately, there is a nice theorem for vector spaces of finite dimension:

5.45. Let V be a finite dimensional space with basis $e_1, e_2, \ldots, e_n$. Prove that $\mu^1, \mu^2, \ldots, \mu^n \in V^*$ defined as

$$\mu^i(e_j) = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ otherwise} \end{cases},$$

is a basis of V^*.

As we know that in this case V and V^* have the same dimension, we can find an isomorphism between them - so they can be identified. Unfortunately, for our future needs, just an isomorphism is not enough. We will be interested mostly in **natural** or **canonical** isomorphisms, that is isomorphisms that don't need a basis to be defined. For example, definitions of quotient spaces or $V \times \{0\} \approx V$ did not invoke bases, so these are examples of naturally isomorphic spaces. It has a great geometrical meaning - we don't want to choose one special basis, it would be rather more convenient to use *any* basis we would like to. This is exactly what we do in differential geometry - we manipulate with objects that are basis and coordinate independent, what allows us to prove theorems in bases that fit to the problem.

---

[10] Unfortunately for vector spaces V of *infinite* dimension, V^* is greater than V and consequently V^{**} is greater than both V^* and V.

5.4 Tensors

Consider vector spaces $V_1, V_2, \dots V_n$ and a function $f : V_1 \times V_2 \times \cdots \times V_n \to \mathbb{F}$. We say that f is **multilinear** if for every i we have:

$$f(v_1, \dots, v_i + \alpha v_i', \dots, v_n) = f(v_1, \dots v_i, \dots, v_n) + \alpha f(v_1, \dots, v_i', \dots, v_n).$$

Being linear and multilinear is not equivalent:

5.46. Find such f that f is a linear mapping from $V_1 \oplus V_2 \oplus \cdots \oplus V_n$,to $\mathbb{F}$, but f *cannot* be treated as a mutlilinear function from $V_1 \times V_2 \times \cdots \times V_n$ to $\mathbb{F}$.

5.4.1 Universal property of tensor spaces

We should on some way improve this vulnerability by creating an object that would interplay between linear and multilinear mappings. Consider finite dimensional V and W. We want to create a vector space called **tensor produt** and denoted as $V \otimes W$ such that:

- for $(v, w) \in V \times W$, there is a vector $v \otimes w \in V \otimes W$
- map $\varphi : V \times W \to V \oplus W$ is bilinear, where $\varphi(v, w) = v \otimes w$. That is we require: $(v + \alpha v') \otimes w = v \otimes w + \alpha v' \otimes w$ and $v \otimes (w + \alpha w') = v \otimes w + \alpha v \otimes w'$.

Then such vector space $V \otimes W$ and map φ have **universal factorisaction property**, that is let $f : V \times W \to U$ be any bilinear map. Then there is *unique* linear function $\tilde{f} : V \otimes W \to U$ such that $f = \tilde{f} \circ \varphi$. It can be expressed in terms of the following diagram:

$$\begin{tikzcd}
V \times W \arrow[r, "\varphi"] \arrow[dr, "f"'] & V \otimes W \arrow[d, "\tilde{f}"] \\
& U
\end{tikzcd}$$

Using this property, we can prove that tensor product of vector spaces is unique, commutative and associative.

5.47. Let V and W be vector spaces. Assume that there is a space T and bilinear map φ have the universal property and space U an bilinear map θ also have the universal property. Prove that T and U are naturally isomorphic.

5.48. Define $f : V \times W \to W \otimes V$ as $f(v, w) = w \otimes v$. Using the universal property, prove that there is an isomorphism $v \otimes w \mapsto w \otimes v$.

5.49. Prove that there is a canonical isomorphism between $(U \otimes V) \otimes W$ and $U \otimes (V \otimes W)$ by:

1. Proving that map $\lambda_u : V \times W \to (U \otimes V) \otimes W$ given by $\lambda_u(v, w) = (u \otimes v) \otimes w$ is bilinear.
2. As λ_u is bilinear, you can find linear map $\tilde{\lambda}_u : V \otimes W \to (U \otimes V) \otimes W$. Prove that map $\Lambda : U \times (V \otimes W) \to (U \otimes V) \otimes W$ given by $\Lambda(u, \omega) = \tilde{\lambda}_u(\omega)$ is bilinear. Find therefore a map $U \otimes (V \otimes W)$ to $(U \otimes V) \otimes W$.

5.4.2 Construction

But a question arises - is it possible to contruct such space? We give two equivalent constructions. Consider a set S and a field $\mathbb{F}$.

5.50. Let V be a set of all functions from set S to field $\mathbb{F}$ such that $f(s) = 0$ for all but finitely many $s \in S$. Prove that V is a vector space.

We usually write $f \in V$ as $f = a_1 s_1 + a_2 s_2 + \cdots + a_n s_n$, where $s_i \in S$ are some elements and $a_i = f(s_i) \in F$.

5.51. Consider a set S and a free vector space generated by it V_S. We define inclusion mapping $\iota : S \to V_S$ as $S \ni s \mapsto s \in V_s$. Prove that for every function $f : S \to U$, where U is a vector space, there is a unique linear map $\tilde{f} : V_S \to U$ such that $f = f \circ \iota$. This can be written as a commutative diagram:

$$\begin{tikzcd} S \arrow[r, "\iota"] \arrow[dr, "f"'] & V_S \arrow[d, "\tilde{f}"] \\ & U \end{tikzcd}$$

5.52. Let V and W be vector spaces over a field $\mathbb{F}$. Let A be a free vector space over $V \times W$. Consider set S containing elements of the forms

$$(v + v', w + w') - (v', w'), \quad (\alpha v, \alpha w) - \alpha(v, w)$$

for $(v, w) \in V \times W$ and it's free vector space B. Prove that $V \oplus U$ is naturally isomorphic to A/B.

5.53. Let V and W be vector spaces over a field $\mathbb{F}$. Let A be a free vector space over $V \times W$. Consider a set S containing all the elements of the forms:

$$(v + v', w) - (v, w) - (v', w), \ (\alpha v, w) - \alpha(v, w) \tag{5.1}$$
$$(v, w + w') - (v, w) - (v, w'), \ (v, \alpha w) - \alpha(v, w) \tag{5.2}$$

and it's free vector space B. Prove that A/B has the universal property of tensor product, with $v \otimes w = [(v, w)]$.

For finite dimensional spaces another construction is possible (as we know - that must be naturally isomorphic to the previous one).

5.54. Let V and W be finite dimensional over $\mathbb{F}$. Consider a set S of all bilinear functions from $V^* \times W^* \to \mathbb{F}$. As we remember, for finite dimensional V we have a natural isomorphism $V \approx V^{**}$, so we can write $v(\nu) \in \mathbb{F}$ for $v \in V$, $\nu \in V^*$. Let's define: $v \otimes w(\nu, \omega) = v(\nu) \times w(\omega)$. Prove that:

1. $v \otimes w \in S$ (so it must be a bilinear function)

2. $\{v_i \otimes w_j\}$ form a basis of S if $\{v_i\}$ and $\{w_j\}$ are bases of V and W.
3. $V \otimes W$ defined as above is naturally isomorphic to S.
4. $\dim V \otimes W = \dim V \cdot \dim W$

5.55. Let V, W, U be finite dimensional vector spaces over the same field. Prove that there is a natural isomorphism:

$$V \otimes (W \oplus U) \approx (V \otimes W) \oplus (V \otimes U).$$

5.56. Prove that for finite dimensional V and W, there is a natural isomorphism between $\mathrm{Hom}(V, W)$ and $V^* \otimes W$.

5.57. Prove that for finite dimensional V, $\mathrm{End}\, V$ is naturally isomorphic to to $\mathrm{End}\, V^*$.

5.58. Let V be a finite dimensional vector space over F. Prove that there is a natural linear map $\mathrm{tr} : V^* \otimes V \to \mathbb{F}$ such that $\mathrm{tr}\,(\omega \otimes v) = \omega(v)$. Therefore we can say that we have a map that takes an endomorphism of V and returns a number - this map is called **trace** - $\mathrm{tr} : \mathrm{End}\,(V) \to F$.

Part III

General topology

6

General topology

So far we have been studying *algebraic* structures - that is we considered a set X and functions $X \times X \to X$ (as multiplication or addition) or functions $X \to X$ (as taking the inverse). Each of these functions is in fact a subset of X^n for some integer n. Now we will start with structures of a different type - for a set X we will consider a subset of $\mathcal{P}(X)$, that is we will select a family of some "special" subsets of X.

Eventually you will see, that these new concepts will enable us to derive very quickly and elegantly the majority of the results taught in undergraduate real analysis courses.

6.1 The category of topological spaces

Consider a set X. A topology is a set $\mathcal{T}_X \subseteq \mathcal{P}(X)$ such that:

1. $\varnothing, X \in \mathcal{T}_X$
2. if $A, B \in \mathcal{T}_X$, then $A \cap B \in \mathcal{T}_X$
3. if $A_i \in \mathcal{T}_X$ for $i \in I$, then $\bigcup_{i \in I} A_i \in \mathcal{T}_X$

Members of topology we call **open sets**.

6.1. Using mathematical induction prove that the intersection of finitely many open sets is open. Therefore in the definition of topology, we could require that finite intersections of open sets should be open.

You may wonder whether, for a given set, topology is unique. As you can prove, there can be many topologies.

Exercise 6.1. Let X be a set. Prove that the following families of subsets are topologies:

1. **Trivial topology:** $\{\varnothing, X\}$.
2. **Discrete topology:** The power set of X: $\mathcal{P}(X)$.

3. **Cofinite topology** $\mathcal{T}_C = \{\varnothing\} \cup \{A \subseteq X : X \setminus A \text{ is finite}\}$ Hint: think in terms of complements.

Exercise 6.2. How many (at least) topologies?

1. Prove that for an infinite set, there are at least three distinct topologies.
2. For what sets, there is exactly one topology on them?

Therefore there is a need for a new definition.

Definition 6.3. *A **topological space** is a pair $(X, \mathcal{T})$, where X is a set and $\mathcal{T} \subseteq \mathcal{P}(X)$ is a topology on X. Sometimes we will abuse our notation and write just X for a topological space, assuming that topology is known out from context.*

Now we have good candidates for objects of a new category - category of topological spaces. We need morphisms and operation of morphism composition. As we are dealing with a family of sets, we are now not interested in functions that preserve some properties of operations on elements - we are looking for a function that will preserve set operations.

Exercise 6.4. Let $f : X \to Y$ be a function. Prove that:

1. $f(\cup_i U_i) = \cup_i f(U_i)$ but $f(\cap_i U_i) \subseteq \cap_i f(U_i)$. Find a case proving that sign $\subseteq$ cannot be replaced with the equality sign.
2. Prove that $f^{-1}(\cup_i V_i) = \cup_i f^{-1}(V_i)$ and $f^{-1}(\cap_i V_i) = \cap_i f^{-1}(V_i)$

Therefore we will be interested in the pre-image of a set.

Definition 6.5. *Let $(X, \mathcal{T})$ and (Y, τ) be two topological spaces. We say that a function $f : X \to Y$ is **continuous** if for every $V \in \tau$, we have $f^{-1}(V) \in \mathcal{T}$. We will write: $f : (X, \mathcal{T}) \to (Y, \tau)$ or just $f : X \to Y$ if topologies are known from the context.*

To prove that continuous functions are category morphisms, we need to check other conditions:

Exercise 6.6. Prove that topological spaces and continuous functions form a category:

1. Consider two topological spaces. Prove that continuous functions from one space to the other form a set.
2. Prove that identity mappings are continuous.
3. Prove that the composition of two continuous maps is continuous.

Definition 6.7. *The category of topological spaces and continuous functions is usually written as **Top**.*

Exercise 6.8. Prove that **Top** can be given a structure of a **concrete category**, that is there exists a faithful functor $U : \mathbf{Top} \to \mathbf{Set}$, where faithful means that for any two objects X, Y induced function $U_{XY} : \mathrm{Hom}(X, Y) \to \mathrm{Hom}(U(X), U(Y))$ is injective.

We have a (concrete) category, and now we can investigate different morphisms:

Exercise 6.9. Types of morphisms

1. Prove that monomorphisms are exactly injective continuous mappings
2. Prove that epimorphisms are exactly surjective continuous mappings
3. Prove that isomorphisms are continuous bijective maps with continuous inverse

Apparently, this category looks almost like **Set**. The most important for us will be isomorphisms, that traditionally are given a different name in topology.

Definition 6.10. *A **homeomorphism**[1] is an isomorphism in **Top**, that is a continuous function with a continuous inverse. Two spaces are **homeomorphic** if there exists a homeomorphism between them.*

We are interested in identifying properties that are preserved by homeomorphisms - homeomorphic spaces should be indistinguishable for us and we will identify them. One of topology aims is to classify all the spaces up to homeomorphisms. This is a hard problem, but we can try to classify a smaller class of spaces:

Exercise 6.11. Classification of discrete spaces. Prove that two *discrete* spaces X and Y are homeomorphic iff $|X| = |Y|$.

6.2 New spaces from old

We have at least four possibilities of creating new topological spaces: we have

This was „global" point of view - we have a structure of subsets of X. We can also try to express these global properties using local properties - by considering special constructions around a single point and using a set of these points to recover a global property. Consider a topological space $(X, \mathcal{T}_X)$ and a point $x \in X$. If $x \in U \in \mathcal{T}_X$, we say that U is an open neighborhood of x. If $x \in U \subseteq V$, where U is open, we call V a neighborhood of x.

6.2. Prove that each point has an open neighborhood.

6.3. Prove that A is an open set if and only if each point a has a neighborhood $U_a \in A$ contained in A (that is $U_a \subseteq A$).

[1] from the Ancient Greek *homois* - similar and *morphe* - shape

For a set A in a topological space, we define **the interior of** A as:

$$\operatorname{int} A = \bigcup \mathcal{U}, \text{ where } \mathcal{U} = \{U \in \mathcal{T} : U \subseteq A\}.$$

6.4. Prove that:

1. $\operatorname{int} A$ is an open set.
2. if $A' \subseteq A$ is open, then $A' \subseteq \operatorname{int} A$ (so in some sense, $\operatorname{int} A$ is the biggest open set contained in A)
3. $\operatorname{int} A = A$ iff A is open
4. $\operatorname{int}\operatorname{int} A = \operatorname{int} A$ for any A

6.5. Let $A' \subseteq A$. Prove that:

1. $\operatorname{int} A' \subseteq \operatorname{int} A$
2. $\operatorname{int} A \cup \operatorname{int} B \subseteq \operatorname{int}(A \cup B)$

You can prove also that the union can be arbitrary.

6.6. We say that a is an **interior point** of A if there is open $U_a \subseteq A$ such that $a \in U_a$. Prove that $\operatorname{int} A$ is the set of all interior points of A.

6.2.1 Closed sets and closure

Consider a topological space $(X, \mathcal{T}_X)$. We say that $A \subseteq X$ is closed if and only if $X \setminus A$ is open.

6.7. Prove these properties of closed sets in space $(X, \mathcal{T}_X)$:

1. $\varnothing$ and X are closed
2. If $A_1, A_2, \ldots, A_n$ are closed, then their union $A_1 \cup A_2 \cup \cdots \cup A_n$ is closed.
3. If $\mathcal{A}$ is any family of closed sets, then the intersection $\bigcap \mathcal{A}$ is closed.

6.8. We say that p is a limit point of $A \subseteq X$ if for every every open neighborhood U of p there is $q_U \neq p$ such that $q_U \in A \cap U$. Prove that A is closed iff it contains all of it's limit points.

We define **the closure** of a set A as:

$$\operatorname{cl} A = \bigcap \mathcal{X},$$

where $\mathcal{X} = \{X \subseteq A : X \text{ is closed}\}$.

6.9. Prove that:

1. $\operatorname{cl} A$ is a closed set.
2. if C is closed and $A \subseteq C$, then $\operatorname{cl} A \subseteq C$ (so in some sense, $\operatorname{cl} A$ is the smallest closed set containing A)
3. $A \subseteq \operatorname{cl} A$
4. $\operatorname{cl}(A \cup B) = \operatorname{cl} A \cup \operatorname{cl} B$

5. $\operatorname{cl} A = A$ iff A is closed
6. $\operatorname{cl}\operatorname{cl} A = \operatorname{cl} A$ for any A

6.10. We say that p is an **adherent point** of A (or **point of closure**) if for any neighborhood V of p we have $A \cap V \neq \varnothing$. Alternatively, we can say that every neighborhood of p contains a point from A. Prove that $\operatorname{cl} A$ is the set of all adherent points of A.

6.11. We say that $A \subseteq X$ is **dense** if $\operatorname{cl} A = X$. Prove that A is dense iff for every $U \in \mathcal{T}_X$, $A \cap U \neq \varnothing$

6.12. 1. Let $r \in \mathbb{R}$. Prove that for every neighborhood V of r there is $q \in \mathbb{Q}$ such that $q \in V$. Hint: each neighborhood must have an interval. And you should have proven that in each interval there is a rational.
2. Conclude that rationals are dense in reals.

6.2.2 Boundary and exterior

We define the **boundary of** A as:

$$\partial A = \operatorname{fr} A = \operatorname{cl} A \setminus \operatorname{int} A$$

6.13. We say that p is a **frontier** point of A if every open neighborhood of p intersects both A and A^c, so if for every open neighborhood U_p we have $U_p \cap A \neq \varnothing$ and $U_p \cap A^c \neq \varnothing$. Prove that the boundary of A is exactly the set of frontier points of A.

6.14. Prove that boundary is always closed.

6.15. Prove that $\partial\partial A \subseteq \partial A$.

6.16. Prove that $\partial A = \partial A^c$.

6.17. Prove that $\partial A = \varnothing$ iff A is simultaneously open and closed.

We define the **exterior of** A as

$$\operatorname{ext} A = X \setminus \operatorname{cl} A$$

6.18. Prove that $\partial A = \operatorname{cl} A \cap \operatorname{cl} \operatorname{ext} A$

6.2.3 Bases and countability axioms

As we have seen, there can be many open sets. Let's try to simplify the situation by considering a smaller family of open sets from which we will be able to recover the whole topology.

Let $(X, \mathcal{T})$ be a topological space. We say that a family of sets $\mathcal{B} \subseteq \mathcal{T}$ is a **basis of topology** iff every open set can be written as a sum of a subfamily of $\mathcal{B}$. Namely for each $U \in \mathcal{T}$ there is $\mathcal{B}_U \subseteq \mathcal{B}$ such that:

$$U = \bigcup \mathcal{B}_U$$

6.19. Prove that $\mathcal{B}$ is a basis for $(X, \mathcal{T})$ iff for every $x \in X$ and every neighborhood U_i of x, there is $B_i \in \mathcal{B}$ such that $x \in B_i \subseteq U_i$.

6.20. Let $\mathcal{B}$ be a basis of $(X, \mathcal{T})$. Prove that:

1. $\bigcup \mathcal{B} = X$
2. If $U, V \in \mathcal{T}$ and $x \in U \cap V$, then there is a set $B_x \in \mathcal{B}$ such that $x \in B_x \subseteq U \cap V$.

We say that a space $(X, \mathcal{T})$ is **second countable** iff it has a countable basis.

6.21. Consider $\mathbb{R}$ with it's standard topology. If $x \in \mathbb{R}$ and U is an open set containing x, we can find a ball $B(x, r),\ r > 0$ such that $B(x, r) \subseteq U$. Using the fact that rationals are dense in reals, prove that you can find $p, q \in \mathbb{Q}$ such that $x \in (p, q) \subseteq U$.

6.22. Prove that $\mathbb{R}$ is second countable.

6.3 Continuous maps and homeomorphisms

Consider two topological spaces $(X, \mathcal{T})$ and (Y, τ). We say that function (or **map**) $f : X \to Y$ is **continuous** iff for every open set $U \in \tau$, it's preimage is open: $f^{-1}(U) \in \mathcal{T}$.

6.23. Prove that a function is continuous iff preimage of every *closed* set is closed.

6.24. Assuming that $\mathbb{R}$ is equipped with it's standard topology, prove that functions from $\mathbb{R}$ to $\mathbb{R}$ are continuous:

1. $f(x) = ax + b$
2. $f(x) = x^2$

6.25. Let $f : (X, \mathcal{T}) \to (Y, \tau)$. Prove that f is continuous iff $f(\operatorname{cl} A) \subseteq \operatorname{cl} f(A)$ for every $A \subseteq X$.

We say that a map $f : (X, \mathcal{T}) \to (Y, \tau)$ is a **homeomorphism** iff is bijective and both f and f^{-1} are continuous. We say that two topological spaces are **homeomorphic** iff there is a homeomorphism between them.

6.4 Connected spaces

We say that a topological space $(X, \mathcal{T})$ is **disconnected** if there exists two disjoint, non-empty sets such their union is the whole space X. Or using symbols: $(X, \mathcal{T})$ is disconnected if $U, V \in \mathcal{T}$ such that $U, V \neq \varnothing,\ U \cap V = \varnothing,\ U \cup V = X$.

6.26. Let $(X, \mathcal{T})$ be a topological space. Prove that these conditions are equivalent:

1. The space is disconnected.
2. There are two *open* sets $A, B \subseteq X$ such that $A, B \neq \varnothing,\ A \cap B = \varnothing,\ A \cup B = X$.
3. There are no two *closed* sets $A, B \subseteq X$ such that $A, B \neq \varnothing,\ A \cap B = \varnothing,\ A \cup B = X$.
4. There is a set $S \subset X,\ S \neq \varnothing, X$ such that and S is open and closed simultaneously (sometimes sets that are both open and closed are called **clopen**).
5. There is a set $S \subset X,\ S \neq \varnothing, X$ such that $\partial S = \varnothing$.
6. There are subsets $A, B \subseteq X,\ A, B \neq \varnothing$ such that $A \cap \operatorname{cl} B = B \cap \operatorname{cl} A = \varnothing$ and $A \cup B = X$.

If a space is not disconnected, it is called **connected**.

6.27. Let $(X, \mathcal{T})$ be a topological space. Prove that these conditions are equivalent:

1. The space is connected.
2. There are no two *open* sets $U, V \subseteq X$ such that $U, V \neq \varnothing,\ U \cap V = \varnothing,\ U \cup V = X$.
3. There are no two *closed* sets $U, V \subseteq X$ such that $U, V \neq \varnothing,\ U \cap V = \varnothing,\ U \cup V = X$.
4. The only sets that are open and closed simultaneously are $\varnothing$ and X.
5. All continuous maps from $(X, \mathcal{T})$ to $(\{0, 1\}, \text{discrete topology})$ are constant.
6. If $S \subseteq X$ and $\partial S = \varnothing$, then $S = \varnothing$ or $S = X$.

Exercise 6.12. Prove that if A and B are connected and $A \cap B \neq \varnothing$, then $A \cup B$ is connected.

Exercise 6.13. Prove that if A is connected, then any set B such that $A \subseteq B \subseteq \operatorname{cl} A$ is connected (including $\operatorname{cl} A$).

Exercise 6.14. Connected space that is not path-connected[2]

1. We define a function $f : \mathbb{R} \to \mathbb{R}$ such that:

$$f(x) = \begin{cases} 1 - |1 - x| \text{ if } x \in [0, 2] \\ f(x + 2) \text{ if } x < 0 \\ f(x - 2) \text{ if } x > 2 \end{cases}$$

   Prove that this function is continuous.
2. Let $A = \{(x, f(1/x)) \in \mathbb{R}^2 : x \in (0, 1]\}$. Why is it connected?
3. Prove that the $\operatorname{cl} A$ is connected, but not path-connected.

[2] An example that can be found in most textbooks uses sine instead of our f and is called "the topologist's sine curve". As we haven't discovered sine yet, I needed to come up with another example.

7

Pseudometric spaces

We have already seen how general topology works. Now we will focus on another collection of spaces, with richer structure, called pseudometric spaces. We will follow Cain's approach (which is one of my favourite book on this subject).

7.1 Pseudometric spaces

Consider a set X. We say that a function $d : X \times X \to \mathbb{R}$ is a **pseudometric** if:

1. for all $x \in X$, $d(x, x) = 0$
2. for all $x, y \in X$, $d(x, y) = d(y, x)$
3. for all $x, y, z \in X$, $d(x, z) \leq d(x, y) + d(y, z)$

7.1. Prove that for a pseudometric d and every $x, y \in X$, there is $d(x, y) \geq 0$.

7.2. Prove that $d(x, y) = 0$ for any $x, y \in X$ is a pseudometric on X. This is called **trivial pseudometric**.

7.3. Prove that $d(x, y) = 1$ for $x \neq y$ is a pseudometric on X. This is called **discrete pseudometric**.

7.4. Prove that $d(x, y) = |x - y|$ is a pseudometric on $\mathbb{R}$.

As we can see above, pseudometric is not determined by the underlying set (as in the case with topology!). Therefore we introduce the concept of pseudometric space (X, d). As we said, these spaces have richer structure - each pseudometric space is a topological space, as you can prove in a minute. Essential concept is the concept of a ball of radius $r > 0$ centered at $x \in X$:

$$B(x, r) = \{y \in X : d(x, y) < r\}.$$

7.5. We say that $S \subseteq X$ is an open set if for every s in S there is r_s such that $B(s, r_s) \subseteq S$. Prove that this is indeed a topology on X.

7.6. Prove that

1. Topology obtained from trivial pseudometric is the trivial topology
2. Topology obtained from discrete pseudometric is the discrete topology.

As any pseudometric space is a topological space, we have many results and concepts that may work for them! In this chapter we will try to derive stronger results (we have more assumptions, so we can obtain more results). As we remember basis of the topology can simplify many results. Let's find it.

7.7. Let (X, d) be a pseudometric space. Prove that:

1. Any $B(x, r)$ is open
2. $\{B(x, r) : x \in X \text{ and } r > 0\}$ is a basis
3. This space is first-countable. Hint: consider $r = 1/n$ for $n = 1, 2, \ldots$.

7.2 Topology of $\mathbb{R}$

Now, we will focus on the „natural" topology of the real line. As we remember real numbers is a complete ordered field.

Part IV

Analysis

8

Banach spaces

Q: What's yellow, normed, and complete?
A: A Bananach space.
Standard Functional Analysis joke, from
`http://dominic-mazzoni.com/mathanswers.html`

We know quite well vector spaces and metric spaces, it's high time we started investigating the mixture of these properties - a vector spaces with sufficiently nice topology placed on them.

Definition 8.1. *Let V be a vector space over real or complex numbers and $n : V \to R$ be a function such that:*

1. $n(v) \geq 0$ *for all* v
2. $n(\alpha v) = |\alpha| \cdot n(v)$
3. $n(v + u) \leq n(v) + n(u)$

Then we call n a ***seminorm****. A seminorm such that:*

4. $n(v) = 0$ *iff* $v = 0$

is called a ***norm****. A pair (V, n) is called then a (semi)normed space. We usually write $\|v\| := n(v)$ and $n = \|\cdot\|$.*

Each normed space is in a natural way a metric, and therefore, a topological space, as you can prove.

Exercise 8.2. Let $(V, \|\cdot\|)$ be a seminormed space. Prove that

$$d(v, u) = \|v - u\|$$

is a pseudometric on V. Prove that d is metric iff $\|\cdot\|$ is a norm.

A simple corollary from that is:

Exercise 8.3. Prove that in a normed space:

1. limits of sequences are unique (hint: metric spaces are Haussdorff)
2. we can use just sequences to characterise compactness and continuity (without nets and filters) (hint: how does it work in metric spaces?)

Similarily to pseudometric spaces, we can introduce turn any seminormed space V into a normed space. Let's think now what changes if we change a norm.

Definition 8.4. *Let n and m be two norms on a vector space V. We say that norm n is* ***stronger*** *than norm m iff the topology generated than n is stronger than the topology generated by m. We say that they are* ***equivalent*** *iff they generate the same topology.*

Exercise 8.5. Let n and m be two norms on a vector space V. Prove that the following statements are equivalent:

1. n is stronger than m
2. for arbitrary $v \in V$ and arbitrary sequence $v_n \to v$ in sense of topology generated by n, we have $v_n \to v$ in sense of topology generated by m
3. function $v \mapsto m(v)/n(v)$ is bounded on set $V \setminus \{0\}$
4. there exists a number $a > 0$ such that $m(v) \leq a \cdot n(v)$ for every $v \in V$

Exercise 8.6. Prove that "norm n is equivalent to norm m" is an equivalence relation on the set of all norms defined on a given vector space.

Exercise 8.7. Equivalence of norms on finite-dimensional space Let V be a finite dimensional space.

1. Let $\{e_i : i = 1, 2, \ldots, n\}$ be a basis. Prove that function
$$n(v^i e_i) = \max\{|v^i| : i = 1, 2, \ldots\}$$
is a norm
2. Prove that all norms are equivalent.

Definition 8.8. *A normed and* complete *vector space is called a* ***Banach space****.*

-p;;

References

1. Isham C (2003) Modern differential geometry for physicists. World Scientific Publishing, Singapore
2. Barden D, Thomas C (2005) An introduction to differential manifolds. Imperial College Press, London
3. Spivak M (1965) Calculus on Manifolds. W. A. Benjamin, USA
4. Cain G (1994) Introduction to General Topology. Addison-Wesley, USA
5. Lee J (2000) Introduction to Topological Manifolds. Springer-Verlag, New York
6. Renteln P (2014) Manifolds, Tensors and Forms. Cambridge University Press, Cambridge
7. Abraham R, Marsden J, Ratiu T (1988) Manifolds, Tensor Analysis and Applications. Springer-Verlag, New York
8. Geroch R (1985) Mathematical Physics. The University of Chicago Press, Chicago
9. Maurin K (2010) Analiza. PWN SA, Warszawa
10. Ash R. B. (2013) Basic abstract algebra for graduates. Dover publications.