Linear Algebra

Manuel Castillo-Lopez

manucalop@gmail.com

October 13, 2021

Abstract

The role of mathematics in science is about casting our concepts about the real world into rigorous mathematical form. But, science doesn't do that for its own sake. It does so, in order to fully explore the implications of what our concepts about the real world are. To certain extent, the spirit of science can be casted into the words of Ludwig Wittgenstein, who said: *What we cannot speak about clearly then we must pass over in silence.* Indeed, if we have concepts about the real world and it's not possible to cast them into precise mathematical language, that is usually an indicator that some aspects of these concepts have not been well understood. But then mathematics is just that, a language. And, if we want to extract physical conclusions from this formulation we must interpret that language. But again citing Wittgenstein: *The theorems of mathematics all say the same: namely nothing.* Obviously, he didn't mean that mathematics is useless. He just refers to the fact that if we have a theorem of the type: A if and only if B. A and B being propositions, then obviously B says nothing else than A does. And A says nothing else than B does. This is what is called in mathematics a tautology. However psychologically, for our understanding of A, it may be very useful to have a reformulation of A in terms of B.

Thus, with the understanding that mathematics just gives us a language for what we want to do, the objective of the course is to provide proper mathematical language to build the concepts addressed later on by the different sciences.

Contents

Chapter 1

Foundations of Mathematics

Mathematics is the language of science. Thus, it is not designed to provide a mean of easygoing communication. Its main purpose is to test our own understanding of what we are trying to write, and to fully explore its implications. The spirit of mathematics can be summarized by the words of Ludwig Wittgenstein, who said: *What we cannot speak about clearly then we must pass over in silence.* Indeed, if we have a notion that we can't express in mathematical language, that is usually an indicator that some aspects have not been well understood. In this chapter, we will start with the first building block of mathematical language: Logic. Propositional and predicate logic will define our language, and will allow us to write the axioms upon which all modern mathematics can be built.

1.1 Propositional logic

The key notion of propositional logic is a proposition.

Definition 1. *A **proposition** p is a variable*[1] *that can take the values true (T) or false (F). No other.*

This is what a proposition is, from the point of view of propositional logic. In particular, it is not the task of propositional logic to decide whether a complex statement of the form: *there is extra-terrestrial life* is true or not. Propositional logic already deals with the complete proposition and it just assumes that is either true or false. Certainly, one can build new propositions from given ones by means of **logical operators**. The simplest kind of logical operators are unary operators. A unary operator takes one proposition and makes from it a new proposition. We define them in the following table:

[1] By this we mean a formal expression, with no extra structure assumed.

p	$\neg p$	id(p)	$\top p$	$\bot p$
F	T	F	T	F
T	F	T	T	F

$\neg$	NOT
id	Identity
$\top$	Tautology
$\bot$	Contradiction

Table 1.1: Unary operators

One can quickly check that, if p can only be true or false, these operators cover all the possibilities to define a unary operator. The next step is to consider binary operators, i.e. operators that take two propositions and return a new one. We have 16 binary operators in total, but we draw some interesting ones in the following table:

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

$\wedge$	AND
$\vee$	OR
$\veebar$	EX-OR
$\uparrow$	NAND (not AND)
$\Rightarrow$	Implication
$\Leftrightarrow$	Equivalence

Table 1.2: Some binary operators

Remark 1. *All higher order operators can be constructed from the single NAND operator.*

We point out the importance of the implication arrow, which is frequently ill-understood. The implication arrow is a binary operator that takes two propositions and constructs a new one that, in total, is true or false, as defined in the previous table.

Remark 2. *From the implication operator, one can conclude anything based on false assumptions, also known as "ex falso quodlibet".*

Then one may wonder why on Earth would you define the implication arrow like this. The answer is hidden in the following theorem:

Theorem 1.1.1. *Let p, q be propositions. Then* $(p \Rightarrow q) \Leftrightarrow ((\neg q) \Rightarrow (\neg p))$.

Proof. We need only to construct the truth table and see that the two last propositions are identical:

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$(\neg q) \Rightarrow (\neg p)$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	F	F
T	T	F	F	T	T

□

Corollary 1.1.1.1. *We can prove assertions by way of contradiction. E.g. assume that* p *is true and we want to prove that* q *is true. Then, what we can do instead, and is fully equivalent, is to assume that what we want to prove is not true, and then prove that the assumption is not true. Then we say we have a contradiction and* q *must have been true.*

1.2 Predicate logic

Definition 2. *A* ***predicate*** *is (informally) a proposition-valued function of some variables(s). In particular, a predicate of two variables is called a relation.*

For example, $Q(x, y)$ is a proposition which value depends on the variables x and y. Just like for propositional logic, it is not the task of predicate logic to examine how predicates are built from the variables on which they depend. Since the notions of set theory have not been yet defined, we leave it completely open, and simply consider x and y formal variables, with no extra conditions imposed. As with propositions, we can construct new predicates from given ones by means of the operators defined in the previous section. For example, we might have:

Example 1. $Q(x, y, z) :\Leftrightarrow P(x) \wedge R(y, z)$

More interestingly, we can construct a new proposition from a given predicate by using *quantifiers*[2]. Let $P(x)$ be a predicate. Then, one can define the proposition

$$p :\Leftrightarrow \forall x : P(x)$$

[2] A quantifier is a language object that specify the elements that satisfy a given predicate.

by using the **universal quantifier** $\forall$. This means that the proposition p is true iff, for every preposition x, the predicate $P(x)$ is true. p is false otherwise.

Then, we can define define the **existential quantifier** $\exists$ and the **unique existential quantifier** $\exists!$ by:

$$\exists\, x : P(x) :\Leftrightarrow \neg(\forall\, x : \neg P(x)).$$

$$\exists!\, x : P(x) :\Leftrightarrow (\exists\, x : \forall\, y : P(y) \Leftrightarrow x = y)$$

1.3 Axiomatic System and theory of proofs

Definition 3. *An* ***axiom*** *a or assumption is a proposition p taken to be true, i.e. a tautology of p* $(a = T(p))$*.*

Definition 4. *An* ***axiomatic system*** *is a finite sequence of axioms* $a_1, a_2, \ldots, a_N$*.*

Definition 5. *A* ***proof*** *of a proposition p within an axiomatic system* $a_1, a_2, \ldots, a_N$ *is a finite sequence of propositions* $q_1, q_2, \ldots, q_M$ *such that* $q_M = p$ *and for any* $1 \leq j \leq M$ *one of the following is satisfied:*

(A) q_j *is a proposition from the list of axioms;*

(T) q_j *is a tautology;*

(M) $\exists\, 1 \leq m, n < j : (q_m \wedge q_n \Rightarrow q_j)$ *is true. This is called modus ponens or deduction rule.*

Remark 3. *If p can be proven within an axiomatic system* $a_1, a_2, \ldots, a_N$*, we write:*

$$a_1, a_2, \ldots, a_N \vdash p$$

and we read "$a_1, a_2, \ldots, a_N$ *proves p".*

Definition 6. *An axiomatic system* $a_1, a_2, \ldots, a_N$ *is said to be* consistent *if there exists a proposition q which cannot be proven from the axioms.*

$$\exists\, q : \neg(a_1, a_2, \ldots, a_N \vdash q).$$

Theorem 1.3.1. *Propositional logic is consistent.*

Theorem 1.3.2 (Godel)**.** *Any axiomatic system powerful enough to encode elementary arithmetic is either inconsistent or contains an undecidable proposition, i.e. a proposition that can be neither proven nor disproven within the system.*

Chapter 2

Axiomatic set theory

Any space, such as the physical space, is a set ”of points” equipped with further structure. But what precisely is a set? Well, one can think of a set as a collection of elements, but that raises the question of what a collection is and what elements are. So certainly we need to do better and, as a fundamental problem, if we start writing a book about mathematics whose pages are all empty yet, what could the first definition be? For a definition you need notions that you already have in order to define a new notion but, if you don't have any notion yet, how do you start? The trick is to start axiomatically, and to do so we will write axiomatic set theory. Again, this raises the question, in what language could you possibly do that? Then, we need another building block called propositional logic, which will allow us to write the axioms of set theory.

2.1 Propositional logic

The key notion of propositional logic is a proposition.

Definition 7. *A* ***proposition*** p *is a variable*[1] *that can take the values true (T) or false (F). No other.*

This is what a proposition is, from the point of view of propositional logic. In particular, it is not the task of propositional logic to decide whether a complex statement of the form: *there is extra-terrestrial life* is true or not. Propositional logic already deals with the complete proposition and it just assumes that is either true or false. Certainly, one can build new propositions from given ones by means of **logical operators**. The simplest kind of logical

[1] By this we mean a formal expression, with no extra structure assumed.

operators are unary operators. A unary operator takes one proposition and makes from it a new proposition. We define them in the following table:

p	$\neg p$	$\mathrm{id}(p)$	$\top p$	$\bot p$
F	T	F	T	F
T	F	T	T	F

$\neg$	NOT
id	Identity
$\top$	Tautology
$\bot$	Contradiction

Table 2.1: Unary operators

One can quickly check that, if p can only be true or false, these operators cover all the possibilities to define a unary operator. The next step is to consider binary operators, i.e. operators that take two propositions and return a new one. We have 16 binary operators in total, but we draw some interesting ones in the following table:

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

$\wedge$	AND
$\vee$	OR
$\veebar$	EX-OR
$\uparrow$	NAND (not AND)
$\Rightarrow$	Implication
$\Leftrightarrow$	Equivalence

Table 2.2: Some binary operators

Remark 4. *All higher order operators can be constructed from the single NAND operator.*

We point out the importance of the implication arrow, which is frequently ill-understood. The implication arrow is a binary operator that takes two propositions and constructs a new one that, in total, is true or false, as defined in the previous table.

Remark 5. *From the implication operator, one can conclude anything based on false assumptions, also known as "ex falso quodlibet".*

Then one may wonder why on Earth would you define the implication arrow like this. The answer is hidden in the following theorem:

Theorem 2.1.1. *Let p, q be propositions. Then $(p \Rightarrow q) \Leftrightarrow ((\neg q) \Rightarrow (\neg p))$.*

Proof. We need only to construct the truth table and see that the two last propositions are identical:

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$(\neg q) \Rightarrow (\neg p)$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	F	F
T	T	F	F	T	T

□

Corollary 2.1.1.1. *We can prove assertions by way of contradiction. E.g. assume that* p *is true and we want to prove that* q *is true. Then, what we can do instead, and is fully equivalent, is to assume that what we want to prove is not true, and then prove that the assumption is not true. Then we say we have a contradiction and* q *must have been true.*

2.2 Predicate logic

Definition 8. *A* ***predicate*** *is (informally) a proposition-valued function of some variables(s). In particular, a predicate of two variables is called a relation.*

For example, $Q(x, y)$ is a proposition which value depends on the variables x and y. Just like for propositional logic, it is not the task of predicate logic to examine how predicates are built from the variables on which they depend. Since the notions of set theory have not been yet defined, we leave it completely open, and simply consider x and y formal variables, with no extra conditions imposed. As with propositions, we can construct new predicates from given ones by means of the operators defined in the previous section. For example, we might have:

Example 2. $Q(x, y, z) :\Leftrightarrow P(x) \wedge R(y, z)$

More interestingly, we can construct a new proposition from a given predicate by using *quantifiers*[2]. Let $P(x)$ be a predicate. Then, one can define the proposition

$$p :\Leftrightarrow \forall x : P(x)$$

[2] A quantifier is a language object that specify the elements that satisfy a given predicate.

by using the **universal quantifier** $\forall$. This means that the proposition p is true iff, for every preposition x, the predicate $P(x)$ is true. p is false otherwise.

Then, we can define define the **existential quantifier** $\exists$ and the **unique existential quantifier** $\exists!$ by:

$$\exists\, x : P(x) :\Leftrightarrow \neg(\forall\, x : \neg P(x)).$$

$$\exists!\, x : P(x) :\Leftrightarrow (\exists\, x : \forall\, y : P(y) \Leftrightarrow x = y)$$

2.3 Axiomatic System and theory of proofs

Definition 9. *An* ***axiom*** *a or assumption is a proposition p taken to be true, i.e. a tautology of p* $(a = T(p))$*.*

Definition 10. *An* ***axiomatic system*** *is a finite sequence of axioms* $a_1, a_2, \ldots, a_N$*.*

Definition 11. *A* ***proof*** *of a proposition p within an axiomatic system* $a_1, a_2, \ldots, a_N$ *is a finite sequence of propositions* $q_1, q_2, \ldots, q_M$ *such that* $q_M = p$ *and for any* $1 \leq j \leq M$ *one of the following is satisfied:*

(A) q_j *is a proposition from the list of axioms;*

(T) q_j *is a tautology;*

(M) $\exists\, 1 \leq m, n < j : (q_m \wedge q_n \Rightarrow q_j)$ *is true. This is called modus ponens or deduction rule.*

Remark 6. *If p can be proven within an axiomatic system* $a_1, a_2, \ldots, a_N$*, we write:*

$$a_1, a_2, \ldots, a_N \vdash p$$

and we read "$a_1, a_2, \ldots, a_N$ *proves p".*

Definition 12. *An axiomatic system* $a_1, a_2, \ldots, a_N$ *is said to be* consistent *if there exists a proposition q which cannot be proven from the axioms.*

$$\exists\, q : \neg(a_1, a_2, \ldots, a_N \vdash q).$$

Theorem 2.3.1. *Propositional logic is consistent.*

Theorem 2.3.2 (Godel)**.** *Any axiomatic system powerful enough to encode elementary arithmetic is either inconsistent or contains an undecidable proposition, i.e. a proposition that can be neither proven nor disproven within the system.*

2.4 The $\in$-relation

Set theory is built on the postulate that there is a fundamental relation (i.e. a predicate of two variables) denoted by $\in$. However, there is no definition of what $\in$ is, or of what a set is. Instead, nine axioms concerning $\in$ and sets formulate the set theory upon which all modern mathematics are built. This axiomatic system is called **Zermelo-Fraenkel set theory**. As an overview, we have:

- 2 basic existence axioms, one about the $\in$ relation and the other about the existence of the empty set;
- 4 construction axioms, which establish rules for building new sets from given ones. They are the pair set axiom, the union set axiom, the replacement axiom and the power set axiom;
- 2 further existence/construction axioms, these are slightly more advanced and newer compared to the others;
- 1 axiom of foundation, excluding some constructions as not being sets.

Using the $\in$-relation we can immediately define the following relations:

- $x \notin y :\Leftrightarrow \neg(x \in y)$
- $x \subseteq y :\Leftrightarrow \forall\, a : (a \in x \Rightarrow a \in y)$
- $x = y :\Leftrightarrow (x \subseteq y) \wedge (y \subseteq x)$
- $x \subset y :\Leftrightarrow (x \subseteq y) \wedge \neg(x = y)$

2.5 Zermelo-Fraenkel axioms of set theory

2.5.1 Axiom on the $\in$-relation

The expression $x \in y$ is a proposition if, and only if, both x and y are sets.

$$\forall\, x : \forall\, y : (x \in y) \veebar \neg(x \in y).$$

2.5.2 Axiom on the existence of an empty set

There exists a set that contains no elements.

$$\exists\, y : \forall\, x : x \notin y.$$

Theorem 2.5.1. *This set is unique and is called the empty set* $\emptyset$*.*

2.5.3 Axiom on pair sets

Let x and y be sets. Then there exists a set that contains as its elements precisely x and y

$$\forall\, x : \forall\, y : \exists\, m : \forall\, u : (u \in m \Leftrightarrow (u = x \vee u = y)).$$

The set m is called the *pair set* of x and y and it is denoted by $\{x, y\}$.

2.5.4 Axiom on union sets

Let x be a set. Then there exists a set whose elements are precisely the elements of the elements of x.

$$\forall\, x : \exists\, u : \forall\, y : (y \in u \Leftrightarrow \exists\, s : (y \in s \wedge s \in x))$$

The set u is denoted by $\bigcup x$, called union of the elements of x.

2.5.5 Axiom of replacement

Let R be a functional relation and let m be a set. Then the image of m under R, denoted by $\mathrm{im}_R(m)$, is again a set.

Definition 13. *A relation R is said to be **functional** if:*

$$\forall\, x : \exists!\, y : R(x, y).$$

Definition 14. *Let m be a set and let R be a functional relation. The **image** of m under R consists of all those y for which there is an $x \in m$ such that $R(x, y)$.*

Theorem 2.5.2. *Let $P(x)$ be a predicate and let m be a set. Then, $\{y \in m \mid P(y)\}$ is a set. This is called **principle of restricted comprehension** and is a consequence of the axiom of replacement.*

The principle of restricted comprehension is not to be confused with the "principle" of universal comprehension which states that $\{y \mid P(y)\}$ is a set for any predicate. This has shown to be inconsistent by Russell. Observe that the $y \in m$ condition makes it so that $\{y \in m \mid P(y)\}$ cannot have more elements than m itself.

Definition 15. *Let x be a set. Then we define the **intersection** of x by:*

$$\bigcap x := \{a \in \bigcup x \mid \forall\, b \in x : a \in b\}.$$

If $a, b \in x$ and $\bigcap x = \emptyset$, then a and b are said to be *disjoint*.

Definition 16. *Let u and m be sets such that $u \subseteq m$. Then the* ***complement*** *of u relative to m is defined as "m without u":*

$$m \setminus u := \{x \in m \mid x \notin u\}.$$

These are both sets by the principle of restricted comprehension, which is ultimately due to axiom of replacement.

2.5.6 Axiom on the existence of power sets

Let m be a set. Then there exists a set, denoted by $\mathcal{P}(m)$, whose elements are precisely the subsets of m.

Example 3. *Let $m = \{a, b\}$. Then $\mathcal{P}(m) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.*

2.5.7 Axiom of infinity

There exists a set that contains the empty set and, together with every other element y, it also contains the set $\{y\}$ as an element.

$$\exists\, x : \emptyset \in x \wedge \forall\, y : (y \in x \Rightarrow \{y\} \in x).$$

Corollary 2.5.2.1. *Let us consider one such set x. Then $\emptyset \in x$ and hence $\{\emptyset\} \in x$. Thus, we also have $\{\{\emptyset\}\} \in x$ and so on. Therefore:*

$$x = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \ldots\}.$$

We can introduce the following notation for the elements of x:

$$0 := \emptyset, \quad 1 := \{\emptyset\}, \quad 2 := \{\{\emptyset\}\}, \quad 3 := \{\{\{\emptyset\}\}\}, \quad \ldots$$

to construct the set $\mathbb{N} := x$ and $\mathbb{R} := \mathcal{P}(\mathbb{N})$ as known as the set of natural and real numbers respectively.

2.5.8 Axiom of choice

Let x be a set whose elements are non-empty and mutually disjoint. Then there exists a set y which contains exactly one element of each element of x.

$$\forall\, x : P(x) \Rightarrow \exists\, y : \forall\, a \in x : \exists!\, b \in a : a \in y,$$

where $P(x) \Leftrightarrow (\exists\, a : a \in x) \wedge (\forall\, a : \forall\, b : (a \in x \wedge b \in x) \Rightarrow \bigcap\{a, b\} = \emptyset)$.

Remark 7. *The axiom of choice is independent of the other 8 axioms, which means that one could have set theory with or without the axiom of choice. However, there are important theorems that can only be proved by using the axiom of choice.*

Axiom of foundation. *Every non-empty set x contains an element y that has none of its elements in common with x. In symbols:*

$$\forall\, x : (\exists\, a : a \in x) \Rightarrow \exists\, y \in x : \bigcap\{x, y\} = \emptyset.$$

An immediate consequence of this axiom is that there is no set that contains itself as an element.

Chapter 3

Classification of sets

3.1 Maps

A recurrent theme in mathematics is the classification of *spaces* by means of structure-preserving *maps* (homomorphisms) between them.

Definition 17. *Let A, B be sets. A* ***map*** *$\phi : A \to B$ is a relation such that for each $a \in A$ there exists exactly one $b \in B$ such that $\phi(a, b)$ holds.*

The standard notation for a map is:

$$\begin{aligned} \phi :A &\to B \\ a &\mapsto \phi(a) \end{aligned} \tag{3.1}$$

The following is standard terminology for a map $\phi : A \to B$:

- the set A is called the **domain** of ϕ;
- the set B is called the **target** of ϕ;
- the set $\phi(A) \equiv \mathrm{im}_\phi(A) := \{\phi(a) \mid a \in A\}$ is called the **image** of A under ϕ.

Definition 18. *A* ***map*** *$\phi : A \to B$ is said to be:*

- ***injective*** *if $\forall\, a_1, a_2 \in A : \phi(a_1) = \phi(a_2) \Rightarrow a_1 = a_2$;*
- ***surjective*** *if $im_\phi(A) = B$;*
- ***bijective*** *if it is both injective and surjective.*

Definition 19. *Two sets A and B are called* ***(set-theoretic) isomorphic*** *if there exists a bijection $\phi : A \to B$. In this case, we write $A \cong_{set} B$.*

Bijections are the “structure-preserving” maps for sets. Intuitively, they pair up the elements of A and B and a bijection between A and B exists only if A and B have the same “size”. This is clear for finite sets, but it can also be extended to infinite sets.

Definition 20 (Classification of sets)**.** *A set A is:*

- ***infinite*** *if there exists a proper subset $B \subset A$ such that $B \cong_{set} A$. In particular, if A is infinite, we further define A to be:*
  - ***countably*** *infinite if $A \cong_{set} \mathbb{N}$;*
  - ***uncountably*** *infinite otherwise.*
- ***finite*** *if it is not infinite. In this case, we have $A \cong_{set} \{1, 2, \dots, N\}$ for some $N \in \mathbb{N}$ and we say that the* ***cardinality*** *of A, denoted by $|A|$, is N.*

Given two maps $\phi : A \to B$ and $\psi : B \to C$, we can construct a third map, called the **composition** of ϕ and ψ, denoted by $\psi \circ \phi$, defined by:

$$\begin{aligned} \psi \circ \phi : A &\to C \\ a &\mapsto \psi(\phi(a)). \end{aligned} \tag{3.2}$$

This is often represented by drawing the following diagram

$$\begin{tikzcd} & B \arrow[dr, "\psi"] & \\ A \arrow[ur, "\phi"] \arrow[rr, "\psi\circ\phi"'] & & C \end{tikzcd}$$

and by saying that “the diagram commutes” means that all paths connecting two nodes in the diagram are equivalent.

Proposition 1. *Composition of maps is associative.*

Definition 21. *Let $\phi : A \to B$ be a bijection. Then the* ***inverse*** *of ϕ, denoted ϕ^{-1}, is defined (uniquely) by:*

$$\phi^{-1} \circ \phi = id_A$$

$$\phi \circ \phi^{-1} = id_B.$$

Equivalently, we say that this diagram commutes:

$$\begin{tikzcd} A \arrow[loop left, "\mathrm{id}_A"] \arrow[r, bend left, "\phi"] & B \arrow[l, bend left, "\phi^{-1}"] \arrow[loop right, "\mathrm{id}_B"] \end{tikzcd}$$

The inverse map is only defined for bijections. However, the following notion, which we will often meet in topology, is defined for any map.

Definition 22. *Let $\phi : A \to B$ be a map and let $V \subseteq B$. Then we define the set:*

$$\mathrm{preim}_\phi(V) := \{a \in A \mid \phi(a) \in V\}$$

*called the **pre-image** of V under ϕ.*

Proposition 2. *Let $\phi : A \to B$ be a map, let $U, V \subseteq B$ and $C = \{C_j \mid j \in J\} \subseteq \mathcal{P}(B)$. Then:*

i) $\mathrm{preim}_\phi(\emptyset) = \emptyset$ *and* $\mathrm{preim}_\phi(B) = A$*;*

ii) $\mathrm{preim}_\phi(U \backslash V) = \mathrm{preim}_\phi(U) \backslash \mathrm{preim}_\phi(V)$*;*

iii) $\mathrm{preim}_\phi(\bigcup C) = \bigcup_{j \in J} \mathrm{preim}_\phi(C_j)$ *and* $\mathrm{preim}_\phi(\bigcap C) = \bigcap_{j \in J} \mathrm{preim}_\phi(C_j)$.

3.2 Equivalence relations

Definition 23. *Let M be a set and let $\sim$ be a relation such that the following conditions are satisfied:*

i) reflexivity: $\forall\, m \in M : m \sim m$;

ii) symmetry: $\forall\, m, n \in M : m \sim n \Leftrightarrow n \sim n$;

iii) transitivity: $\forall\, m, n, p \in M : (m \sim n \wedge n \sim p) \Rightarrow m \sim p$.

*Then $\sim$ is called an **equivalence relation** on M.*

Example 4. *Consider the following wordy examples.*

a) $p \sim q :\Leftrightarrow p$ is of the same opinion as q. This relation is reflexive, symmetric and transitive. Hence, it is an equivalence relation.

b) $p \sim q :\Leftrightarrow p$ is a sibling of q. This relation is symmetric and transitive but not reflexive and hence, it is not an equivalence relation.

c) $p \sim q :\Leftrightarrow p$ is taller q. This relation is transitive, but neither reflexive nor symmetric and hence, it is not an equivalence relation.

Definition 24. *Let $\sim$ be an equivalence relation on the set M. Then, for any $m \in M$, we define the set:*

$$[m] := \{n \in M \mid m \sim n\}$$

*called the **equivalence class** of m. Note that the condition $m \sim n$ is equivalent to $n \sim m$ since $\sim$ is symmetric.*

Proposition 3. *Let $\sim$ be an equivalence relation on M. Then:*

i) $a \in [m] \Rightarrow [a] = [m]$;

ii) either $[m] = [n]$ or $[m] \cap [n] = \emptyset$.

Definition 25. *Let $\sim$ be an equivalence relation on M. Then we define the **quotient set** of M by $\sim$ as:*

$$M/\!\sim \; := \{[m] \mid m \in M\}.$$

This is indeed a set since $[m] \subseteq \mathcal{P}(M)$ and hence we can write more precisely:

$$M/\!\sim \; := \{[m] \in \mathcal{P}(M) \mid m \in M\}.$$

Then clearly $M/\sim$ is a set by the power set axiom and the principle of restricted comprehension.

Remark 8. *Due to the axiom of choice, there exists a complete system of representatives for $\sim$, i.e. a set R such that $R \cong_{set} M/\!\sim$.*

Remark 9. *Care must be taken when defining maps whose domain is a quotient set if one uses representatives to define the map. In order for the map to be **well-defined** one needs to show that the map is independent of the choice of representatives.*

3.3 Construction of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$

Recall that, invoking the axiom of infinity, we defined:

$$\mathbb{N} := \{0, 1, 2, 3, \ldots\},$$

where:

$$0 := \emptyset, \quad 1 := \{\emptyset\}, \quad 2 := \{\{\emptyset\}\}, \quad 3 := \{\{\{\emptyset\}\}\}, \quad \ldots$$

We would now like to define an addition operation on $\mathbb{N}$ by using the axioms of set theory. We will need some preliminary definitions.

Definition 26. *The* successor map S *on* $\mathbb{N}$ *is defined by:*

$$\begin{aligned} S : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \{n\} \end{aligned}$$

Definition 27. *The* predecessor map S *on* $\mathbb{N}^* := \mathbb{N} \setminus \emptyset$ *is defined by:*

$$\begin{aligned} S : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto m \quad \textit{such that } \{m\} = n \end{aligned}$$

Definition 28. *Let* $n \in \mathbb{N}$. *The* n-th power *of* S, *denoted* S^n, *is defined recursively by:*

$$\begin{aligned} S^n &:= S \circ S^{P(n)} \qquad \textit{if } n \in \mathbb{N}^* \\ S^0 &:= id_{\mathbb{N}} \end{aligned}$$

We are now ready to define addition.

Definition 29. *The* addition *operation on* $\mathbb{N}$ *is the map:*

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (m, n) &\mapsto m + n := S^n(m). \end{aligned}$$

Definition 30. *Let* $\sim$ *be the equivalence relation on* $\mathbb{N} \times \mathbb{N}$ *defined by:*

$$(m, n) \sim (p, q) :\Leftrightarrow m + q = p + n.$$

Definition 31. *We define the set of* integers *by:*

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim .$$

The intuition behind this definition is that the pair (m, n) stands for "$m - n$". In other words, we represent each integer by a pair of natural numbers whose (yet to be defined) difference is precisely that integer. There are, of course, many ways to represent the same integer with a pair of natural numbers in this way. For instance, the integer -1 could be represented by $(1, 2)$, $(2, 3)$, $(112, 113)$, ...

Remark 10. *In a first introduction to set theory it is not unlikely to find the claim that the natural numbers are part of the integers, i.e.* $\mathbb{N} \subseteq \mathbb{Z}$. *However, according to our definition, this is obviously nonsense since* $\mathbb{N}$ *and* $\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim$ *contain entirely different elements. What is true is that* $\mathbb{N}$ *can be* embedded *into* $\mathbb{Z}$, *i.e. there exists an* inclusion map ι, *given by:*

$$\begin{aligned} \iota : \mathbb{N} &\hookrightarrow \mathbb{Z} \\ n &\mapsto [(n, 0)] \end{aligned}$$

and it is in this sense that $\mathbb{N}$ *is included in* $\mathbb{Z}$.

Definition 32. *Let* $n := [(n, 0)] \in \mathbb{Z}$. *Then we define the* inverse *of* n *to be* $-n := [(0, n)]$.

We would now like to inherit the + operation from $\mathbb{N}$.

Definition 33. *We define the* addition of integers $+_{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *by:*

$$[(m, n)] +_{\mathbb{Z}} [(p, q)] := [(m + p, n + q)].$$

Definition 34. *In a similar fashion, we define the set of* rational numbers *by:*

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/\sim,$$

where $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ *and* $\sim$ *is a relation on* $\mathbb{Z} \times \mathbb{Z}^*$ *given by:*

$$(p, q) \sim (r, s) :\Leftrightarrow ps = qr,$$

assuming that a multiplication *operation on the integers has already been defined.*

We also have the *canonical embedding* of $\mathbb{Z}$ into $\mathbb{Q}$:

$$\begin{aligned} \iota : \mathbb{Z} &\hookrightarrow \mathbb{Q} \\ p &\mapsto [(p, 1)] \end{aligned}$$

Definition 35. *We define the* addition of rational numbers $+_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ *by:*

$$[(p, q)] +_{\mathbb{Q}} [(r, s)] := [(ps + rq, qs)]$$

and multiplication of rational numbers *by:*

$$[(p, q)] \cdot_{\mathbb{Q}} [(r, s)] := [(pr, qs)],$$

where the operations of addition and multiplication that appear on the right hand sides are the ones defined on $\mathbb{Z}$. *It is again necessary (but easy) to check that these operations are both well-defined.*

There are many ways to construct the reals from the rationals. One is to define a set $\mathcal{A}$ of *almost homomorphisms* on $\mathbb{Z}$ and hence define:

$$\mathbb{R} := \mathcal{A}/\sim,$$

where $\sim$ is a “suitable” equivalence relation on $\mathcal{A}$.

Chapter 4

Topological spaces

4.1 Topology

A topology on a set provides the weakest structure in order to define the notions of convergence of sequences, and continuity of maps.

Definition 36. *Let M be a set. A* ***topology*** *on M is a set $\mathcal{O} \subseteq \mathcal{P}(M)$ such that:*

i) $\emptyset \in \mathcal{O}$ *and* $M \in \mathcal{O}$;

ii) $\{U, V\} \subseteq \mathcal{O} \Rightarrow \bigcap\{U, V\} \in \mathcal{O}$;

iii) $C \subseteq \mathcal{O} \Rightarrow \bigcup C \in \mathcal{O}$.

The pair $(M, \mathcal{O})$ is called a ***topological space****. If we write "let M be a topological space" then some topology $\mathcal{O}$ on M is assumed.*

Remark 11. *Unless $|M| = 1$, there are (usually many) different topologies $\mathcal{O}$ that one can choose on the set M.*

Example 5. *Let $M = \{1, 2, 3\}$. Then $\mathcal{O} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}, \{1, 2, 3\}\}$ is a topology on M.*

Example 6. *Let M be a set. Then $\mathcal{O} = \{\emptyset, M\}$ is a topology on M. This is called the* ***chaotic topology*** *and can be defined on any set.*

Example 7. *Let M be a set. Then $\mathcal{O} = \mathcal{P}(M)$ is a topology on M. This is called the* ***discrete topology*** *and can be defined on any set.*

Definition 37. *For any $x \in \mathbb{R}^d$ and any $r \in \mathbb{R}^+ := \{s \in \mathbb{R} \mid s > 0\}$, we define the* ***open ball*** *of radius r around the point x:*

$$B_r(x) := \big\{y \in \mathbb{R}^d \mid \|y_i - x_i\|_{2n} < r\big\},$$

where $\|y_i - x_i\|_{2n} =^{2n} \sqrt{\sum_{i=1}^{d}(y_i - x_i)^{2n}}$ denotes the 2n-norm for any $n \in \mathbb{N}$

Definition 38. *Let $M = \mathbb{R}^d$. Then, the* ***standard topology*** *$\mathcal{O}_{\text{std}}$, is defined by:*

$$U \in \mathcal{O}_{\text{std}} :\Leftrightarrow \forall\, p \in U : \exists\, r \in \mathbb{R}^+ : B_r(p) \subseteq U.$$

We now give some common terminology regarding topologies.

Definition 39. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two topologies on a set M. If $\mathcal{O}_1 \subset \mathcal{O}_2$, then we say that $\mathcal{O}_1$ is a* ***coarser*** *(or* ***weaker****) topology than $\mathcal{O}_2$. Equivalently, we say that $\mathcal{O}_2$ is a* ***finer*** *(or* ***stronger****) topology than $\mathcal{O}_1$.*

Clearly, the chaotic topology is the coarsest topology on any given set, while the discrete topology is the finest.

Definition 40. *Let $(M, \mathcal{O})$ be a topological space. A subset S of M is said to be* ***open (with respect to $\mathcal{O}$)*** *if $S \in \mathcal{O}$ and* ***closed (with respect to $\mathcal{O}$)*** *if $M \backslash S \in \mathcal{O}$.*

Notice that the notions of open and closed sets, as defined, are not mutually exclusive. A set could be both or neither, or one and not the other.

Example 8. *Let $(M, \mathcal{O})$ be a topological space. Then $\emptyset$ is open since $\emptyset \in \mathcal{O}$. However, $\emptyset$ is also closed since $M \backslash \emptyset = M \in \mathcal{O}$. Similarly for M.*

Example 9. *Let $M = \{a, b, c\}$ and let $\mathcal{O} = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$. Then $\{a\}$ is open but not closed, $\{b, c\}$ is closed but not open, and $\{b\}$ is neither open nor closed.*

4.2 Construction of new topologies from given ones

Definition 41. *Let $(M, \mathcal{O})$ be a topological space and let $N \subset M$. Then:*

$$\mathcal{O}|_N := \{U \cap N \mid U \in \mathcal{O}\} \subseteq \mathcal{P}(N)$$

is a topology on N called the ***induced (subset) topology****.*

Definition 42. *Let $(M, \mathcal{O})$ be a topological space and let $\sim$ be an equivalence relation on M. Then, the quotient set:*

$$M/\sim\, = \{[m] \in \mathcal{P}(M) \mid m \in M\}$$

can be equipped with the ***quotient topology*** $\mathcal{O}_{M/\sim}$ *defined by:*

$$\mathcal{O}_{M/\sim} := \{U \in M/\sim\, \mid \bigcup U = \bigcup_{[a]\in U} [a] \in \mathcal{O}\}.$$

An equivalent definition of the quotient topology is as follows. Let $q : M \to M/\sim$ be the map:

$$\begin{aligned} q : M &\to M/\sim \\ m &\mapsto [m] \end{aligned} \tag{4.1}$$

Then we have:

$$\mathcal{O}_{M/\sim} := \{U \in M/\sim\, \mid \operatorname{preim}_q(U) \in \mathcal{O}\}.$$

Example 10. *Let $\sim$ be the equivalence relation on $\mathbb{R}$ defined by:*

$$x \sim y :\Leftrightarrow \exists\, n \in \mathbb{Z} : x = y + 2\pi n.$$

Then the circle can be defined as the set $S^1 := \mathbb{R}/\sim$ equipped with the quotient topology.

Definition 43. *Let $(A, \mathcal{O}_A)$ and $(B, \mathcal{O}_B)$ be topological spaces. Then the set $\mathcal{O}_{A\times B}$ defined implicitly by:*

$$U \in \mathcal{O}_{A\times B} :\Leftrightarrow \forall\, p \in U : \exists\, (S, T) \in \mathcal{O}_A \times \mathcal{O}_B : S \times T \subseteq U$$

is a topology on $A \times B$ called the ***product topology****.*

Remark 12. *Using the previous definition, one can check that the standard topology on $\mathbb{R}^d$ satisfies:*

$$\mathcal{O}_{\text{std}} = \mathcal{O}_{\underbrace{\mathbb{R}\times\mathbb{R}\times\cdots\times\mathbb{R}}_{d\ times}}.$$

4.3 Convergence

Definition 44. *Let M be a set. A* ***sequence*** *(of points) in M is a function $q : \mathbb{N} \to M$.*

Definition 45. *Let $(M, \mathcal{O})$ be a topological space. A sequence q in M is said to* ***converge*** *against a* ***limit point*** *$a \in M$ if:*

$$\forall\, U \in \mathcal{O} : a \in U \Rightarrow \exists\, N \in \mathbb{N} : \forall\, n > N : q(n) \in U.$$

Where U is called an ***open neighbourhood*** *of a or $U(a)$.*

Example 11. *Consider the chaotic topological space $(M, \{\emptyset, M\})$. Then every sequence in M converges to every point in M.*

Example 12. *Consider the discrete topological space $(M, \mathcal{P}(M))$. Then only definitely constant sequences converge.*

Theorem 4.3.1. *Consider the topological space $(\mathbb{R}^d, \mathcal{O}_{\text{std}})$. Then, a sequence $q : \mathbb{N} \to \mathbb{R}^d$ converges against $a \in \mathbb{R}^d$ if:*

$$\forall\, \varepsilon > 0 : \exists\, N \in \mathbb{N} : \forall\, n > N : \|q(n) - a\|_2 < \varepsilon.$$

4.4 Continuity

Definition 46. *Let $(M, \mathcal{O}_M)$ and $(N, \mathcal{O}_N)$ be topological spaces and let $\phi : M \to N$ be a map. Then, ϕ is said to be* ***continuous*** *(with respect to the topologies $\mathcal{O}_M$ and $\mathcal{O}_N$) if the pre-images of open sets are open sets, i.e:*

$$\forall\, S \in \mathcal{O}_N\,,\ \text{preim}_\phi(S) \in \mathcal{O}_M,$$

Example 13. *If M is equipped with the discrete topology, or N with the chaotic topology, then any map $\phi : M \to N$ is continuous.*

Example 14. *Continuity with the standard topology happens to be the undergraduate (ϵ, δ) definition.*

Definition 47. *Let $(M, \mathcal{O}_M)$ and $(N, \mathcal{O}_N)$ be topological spaces. A bijection $\phi : M \to N$ is called a* ***homeomorphism*** *if both $\phi : M \to N$ and $\phi^{-1} : N \to M$ are continuous.*

$$\begin{tikzcd} M \arrow[r, bend left, "\phi"] & N \arrow[l, bend left, "\phi^{-1}"] \end{tikzcd}$$

Definition 48. *If there exists a homeomorphism between two topological spaces $(M, \mathcal{O}_M)$ and $(N, \mathcal{O}_N)$, we say that the two spaces are* ***homeomorphic*** *or* ***topologically isomorphic*** *and we write $(M, \mathcal{O}_M) \cong_{\text{top}} (N, \mathcal{O}_N)$.*

Clearly, if $(M, \mathcal{O}_M) \cong_{\text{top}} (N, \mathcal{O}_N)$, then $M \cong_{set} N$.

4.5 Separation properties

Definition 49. *A topological space $(M, \mathcal{O})$ is said to be **T1** if for any two distinct points $p, q \in M$, $p \neq q$:*

$$\exists\, U(p) \in \mathcal{O} : q \notin U(p).$$

Definition 50. *A topological space $(M, \mathcal{O})$ is said to be **T2** or **Hausdorff** if, for any two distinct points, there exist non-intersecting open neighbourhoods of these two points:*

$$\forall\, p, q \in M : p \neq q \Rightarrow \exists\, U(p), V(q) \in \mathcal{O} : U(p) \cap V(q) = \emptyset.$$

Example 15. *The topological space $(\mathbb{R}^d, \mathcal{O}_{\text{std}})$ is T2 and hence also T1.*

Example 16. *The Zariski topology on an algebraic variety is T1 but not T2.*

Example 17. *The topological space $(M, \{\emptyset, M\})$ does not have the T1 property since for any $p \in M$, the only open neighbourhood of p is M and for any other $q \neq p$ we have $q \in M$. Moreover, since this space is not T1, it cannot be T2 either.*

4.6 Compactness and paracompactness

Definition 51. *Let $(M, \mathcal{O})$ be a topological space. A set $C \subseteq \mathcal{P}(M)$ is called a **cover** (of M) if:*

$$\bigcup C = M.$$

*Additionally, it is said to be an **open** cover if $C \subseteq \mathcal{O}$.*

Definition 52. *Let C be a cover. Then any subset $\widetilde{C} \subseteq C$ such that $\widetilde{C}$ is still a cover, is called a **subcover**. Additionally, it is said to be a **finite** subcover if it is finite as a set.*

Definition 53. *A topological space $(M, \mathcal{O})$ is said to be **compact** if every open cover has a finite subcover.*

Definition 54. *Let $(M, \mathcal{O})$ be a topological space. A subset $N \subseteq M$ is called **compact** if the topological space $(N, \mathcal{O}|_N)$ is compact.*

Theorem 4.6.1 (Heine-Borel)**.** *Let $\mathbb{R}^d$ be equipped with the standard topology $\mathcal{O}_{\text{std}}$. Then, a subset of $\mathbb{R}^d$ is compact if, and only if, it is closed and bounded.*

A subset S of $\mathbb{R}^d$ is said to be **bounded** if:

$$\exists\, r \in \mathbb{R}^+ : S \subseteq B_r(0).$$

Remark 13. *It is also possible to generalize this result to arbitrary metric spaces. A* ***metric space*** *is a pair (M, d) where M is a set and $d : M \times M \to \mathbb{R}$ is a map such that for any $x, y, z \in M$ the following conditions hold:*

i) $d(x, y) \geq 0$;

ii) $d(x, y) = 0 \Leftrightarrow x = y$;

iii) $d(x, y) = d(y, x)$;

iv) $d(x, y) \leq d(x, z) + d(y, z)$.

A metric structure on a set M induces a topology $\mathcal{O}_d$ on M by:

$$U \in \mathcal{O}_d :\Leftrightarrow \forall\, p \in U : \exists\, r \in \mathbb{R}^+ : B_r(p) \subseteq U,$$

where the open ball in a metric space is defined as:

$$B_r(p) := \{x \in M \mid d(p, x) < r\}.$$

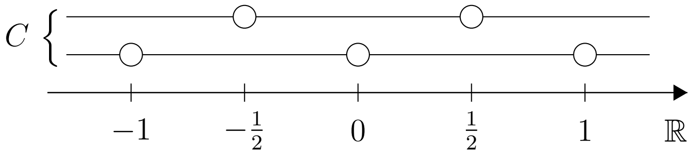
In this setting, one can prove that a subset $S \subseteq M$ of a metric space (M, d) is compact if, and only if, it is complete and totally bounded.

Example 18. *The interval $[0, 1]$ is compact in $(\mathbb{R}, \mathcal{O}_{\text{std}})$. The one-element set containing $(-1, 2)$ is a cover of $[0, 1]$, but it is also a finite subcover and hence $[0, 1]$ is compact from the definition. Alternatively, $[0, 1]$ is clearly closed and bounded, and hence it is compact by the Heine-Borel theorem.*

Example 19. *The set $\mathbb{R}$ is not compact in $(\mathbb{R}, \mathcal{O}_{\text{std}})$. To prove this, it suffices to show that there exists a cover of $\mathbb{R}$ that does not have a finite subcover. To this end, let:*

$$C := \{(n, n+1) \mid n \in \mathbb{Z}\} \cup \{(n + \tfrac{1}{2}, n + \tfrac{3}{2}) \mid n \in \mathbb{Z}\}.$$

This corresponds to the following picture.



It is clear that removing even one element from C will cause C to fail to be an open cover of $\mathbb{R}$. Therefore, there is no finite subcover of C and hence, $\mathbb{R}$ is not compact.

Theorem 4.6.2. *Let $(M, \mathcal{O}_M)$ and $(N, \mathcal{O}_N)$ be compact topological spaces. Then $(M \times N, \mathcal{O}_{M\times N})$ is a compact topological space.*

Definition 55. *Let $(M, \mathcal{O})$ be a topological space and let C be a cover. A* ***refinement*** *of C is a cover R such that:*

$$\forall U \in R : \exists V \in C : U \subseteq V.$$

Any subcover of a cover is a refinement of that cover, but the converse is not true in general. A refinement R is said to be:

- **open** if $R \subseteq \mathcal{O}$;
- **locally finite** if for any $p \in M$ there exists a neighbourhood $U(p)$ such that the set:
$$\{U \in R \mid U \cap U(p) \neq \emptyset\}$$
is finite as a set.

Compactness is a very strong property. Hence often times it does not hold, but a weaker and still useful property, called paracompactness, may still hold.

Definition 56. *A topological space $(M, \mathcal{O})$ is said to be* ***paracompact*** *if every open cover has an open refinement that is locally finite.*

Corollary 4.6.2.1. *If a topological space is compact, then it is also paracompact.*

Definition 57. *A topological space $(M, \mathcal{O})$ is said to be* ***metrisable*** *if there exists a metric d such that the topology induced by d is precisely $\mathcal{O}$, i.e. $\mathcal{O}_d = \mathcal{O}$.*

Theorem 4.6.3 (Stone)**.** *Every metrisable space is paracompact.*

Example 20. *The space $(\mathbb{R}^d, \mathcal{O}_{\text{std}})$ is metrisable since $\mathcal{O}_{\text{std}} = \mathcal{O}_d$ where $d = \|\cdot\|_2$. Hence it is paracompact by Stone's theorem.*

Theorem 4.6.4. *Let $(M, \mathcal{O}_M)$ be a paracompact space and let $(N, \mathcal{O}_N)$ be a compact space. Then $M \times N$ (equipped with the product topology) is paracompact.*

Corollary 4.6.4.1. *Let $(M, \mathcal{O}_M)$ be a paracompact space and let $(N_i, \mathcal{O}_{N_i})$ be compact spaces for every $1 \leq i \leq n$. Then $M \times N_1 \times \cdots \times N_n$ is paracompact.*

Definition 58. *Let $(M, \mathcal{O}_M)$ be a topological space. A **partition of unity** of M is a set $\mathcal{F}$ of continuous maps from M to the interval $[0,1]$ such that for each $p \in M$ the following conditions hold:*

i) there exists $U(p)$ such that the set $\{f \in \mathcal{F} \mid \forall\, x \in U(p) : f(x) \neq 0\}$ is finite;

ii) $\sum_{f \in \mathcal{F}} f(p) = 1$.

*If C is an open cover, then $\mathcal{F}$ is said to be **subordinate** to the cover C if:*

$$\forall\, f \in \mathcal{F} : \exists U \in C : f(x) \neq 0 \Rightarrow x \in U.$$

Theorem 4.6.5. *Let $(M, \mathcal{O}_M)$ be a Hausdorff topological space. Then $(M, \mathcal{O}_M)$ is paracompact if, and only if, every open cover admits a partition of unity subordinate to that cover.*

Example 21. *Let $\mathbb{R}$ be equipped with the standard topology. Then $\mathbb{R}$ is paracompact by Stone's theorem. Hence, every open cover of $\mathbb{R}$ admits a partition of unity subordinate to that cover. As a simple example, consider $\mathcal{F} = \{f, g\}$, where:*

$$f(x) = \begin{cases} 0 \text{ if } x \leq 0 \\ x^2 \text{ if } 0 \leq x \leq 1 \\ 1 \text{ if } x \geq 1 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 1 \text{ if } x \leq 0 \\ 1 - x^2 \text{ if } 0 \leq x \leq 1 \\ 0 \text{ if } x \geq 1 \end{cases}$$

Then $\mathcal{F}$ is a partition of unity of $\mathbb{R}$. Indeed, $f, g : \mathbb{R} \to [0,1]$ are both continuous, condition i) is satisfied since $\mathcal{F}$ itself is finite, and we have $\forall\, x \in \mathbb{R} : f(x) + g(x) = 1$.

Let $C := \{(-\infty, 1), (0, \infty)\}$. Then C is an open cover of $\mathbb{R}$ and since:

$$f(x) \neq 0 \Rightarrow x \in (0, \infty) \quad \text{and} \quad g(x) \neq 0 \Rightarrow x \in (-\infty, 1),$$

the partition of unity $\mathcal{F}$ is subordinate to the open cover C.

4.6.1 Connectedness and path-connectedness

Definition 59. *A topological space $(M, \mathcal{O})$ is said to be **connected** unless there exist two non-empty, non-intersecting open sets A and B such that $M = A \cup B$.*

Example 22. *Consider $(\mathbb{R} \setminus \{0\}, \mathcal{O}_{\text{std}}|_{\mathbb{R} \setminus \{0\}})$, i.e. $\mathbb{R} \setminus \{0\}$ equipped with the subset topology inherited from $\mathbb{R}$. This topological space is not connected since $(-\infty, 0)$ and $(0, \infty)$ are open, non-empty, non-intersecting sets such that $\mathbb{R} \setminus \{0\} = (-\infty, 0) \cup (0, \infty)$.*

Theorem 4.6.6. *The interval $[0,1] \subseteq \mathbb{R}$ equipped with the subset topology is connected.*

Theorem 4.6.7. *A topological space $(M, \mathcal{O})$ is connected if, and only if, the only subsets that are both open and closed are $\emptyset$ and M.*

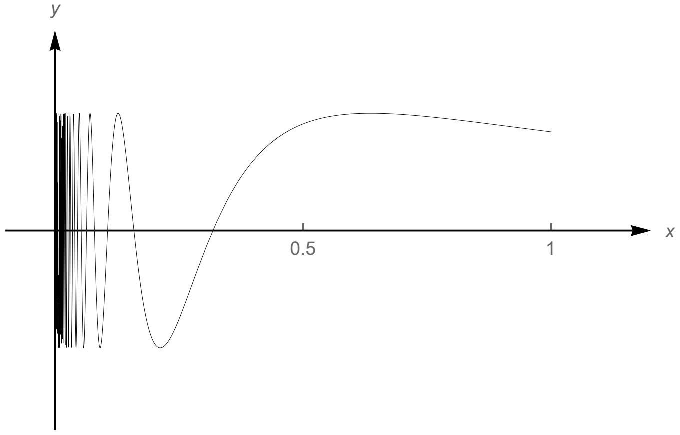
Definition 60. *A topological space $(M, \mathcal{O})$ is said to be* ***path-connected*** *if for every pair of points $p, q \in M$ there exists a continuous curve $\gamma : [0,1] \to M$ such that $\gamma(0) = p$ and $\gamma(1) = q$.*

Example 23. *The space $(\mathbb{R}^d, \mathcal{O}_{\text{std}})$ is path-connected. Indeed, let $p, q \in \mathbb{R}^d$ and let:*

$$\gamma(l) := p + l(q - p).$$

Then γ is continuous and satisfies $\gamma(0) = p$ and $\gamma(1) = q$.

Example 24. *Let $S := \{(x, \sin(\frac{1}{x})) \mid x \in (0,1]\} \cup \{(0,0)\}$ be equipped with the subset topology inherited from $\mathbb{R}^2$.*



The space $(S, \mathcal{O}_{\text{std}}|_S)$ is connected but not path-connected.

Theorem 4.6.8. *If a topological space is path-connected, then it is also connected.*

4.6.2 Homotopic curves and the fundamental group

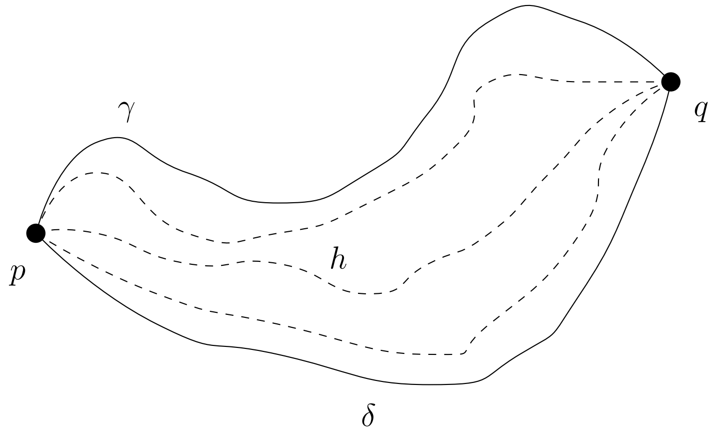
Definition 61. *Let $(M, \mathcal{O})$ be a topological space. Two curves $\gamma, \delta : [0,1] \to M$ such that:*

$$\gamma(0) = \delta(0) \quad \textit{and} \quad \gamma(1) = \delta(1)$$

are said to be ***homotopic*** *if there exists a continuous map $h : [0,1] \times [0,1] \to M$ such that for all $l \in [0,1]$:*

$$h(0, l) = \gamma(l) \quad \textit{and} \quad h(1, l) = \delta(l).$$

Pictorially, two curves are homotopic if they can be continuously deformed into one another.



Proposition 4. *Let $\gamma \sim \delta :\Leftrightarrow$ "γ and δ are homotopic". Then, $\sim$ is an equivalence relation.*

Definition 62. *Let $(M, \mathcal{O})$ be a topological space. Then, for every $p \in M$, we define the **space of loops** at p by:*

$$\mathcal{L}_p := \{\gamma : [0,1] \to M \mid \gamma \textit{ is continuous and } \gamma(0) = \gamma(1)\}.$$

Definition 63. *Let $\mathcal{L}_p$ be the space of loops at $p \in M$. We define the **concatenation** operation $* : \mathcal{L}_p \times \mathcal{L}_p \to \mathcal{L}_p$ by:*

$$(\gamma * \delta)(l) := \begin{cases} \gamma(2l) \textit{if } 0 \leq l \leq \frac{1}{2} \\ \delta(2l-1) \textit{if } \frac{1}{2} \leq l \leq 1 \end{cases}$$

Definition 64. *Let $(M, \mathcal{O})$ be a topological space. The **fundamental group** $\pi_1(p)$ of $(M, \mathcal{O})$ at $p \in M$ is the set:*

$$\pi_1(p) := \mathcal{L}_p / \sim \, = \{[\gamma] \mid \gamma \in \mathcal{L}_p\},$$

where $\sim$ is the homotopy equivalence relation, together with the map

$$\begin{aligned} \bullet : &\pi_1(p) \times \pi_1(p) &&\to \pi_1(p) \\ &(\gamma, \delta) &&\mapsto [\gamma] \bullet [\delta] := [\gamma * \delta]. \end{aligned}$$

Remark 14. *Recall that a group is a pair $(G, \bullet)$ where G is a set and $\bullet : G \times G \to G$ is a map (also called **binary operation**) such that:*

A) $\forall\, a,b,c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$;

N) $\exists\, e \in G : \forall\, g \in G : g \bullet e = e \bullet g = g$;

I) $\forall\, g \in G : \exists\, g^{-1} \in G : g \bullet g^{-1} = g^{-1} \bullet g = e$.

A group is called ***abelian (or commutative)*** *if, in addition, satisfies*

C) $\forall\, a,b \in G : a \bullet b = b \bullet a$

A ***group isomorphism*** *between two groups* $(G, \bullet)$ *and* $(H, \circ)$ *is a bijection* $\phi : G \to H$ *such that:*

$$\forall\, a,b \in G : \phi(a \bullet b) = \phi(a) \circ \phi(b).$$

If there exists a group isomorphism between $(G, \bullet)$ *and* $(H, \circ)$*, we say that* G *and* H *are (group theoretic) isomorphic and we write* $G \cong_{\mathrm{grp}} H$.

The operation $\bullet$ is associative (since concatenation is associative); the neutral element of the fundamental group $(\pi_1(p), \bullet)$ is (the equivalence class of) the constant curve γ_e defined by:

$$\begin{aligned} \gamma_e : [0,1] &\to M \\ l &\mapsto \gamma_e(0) = p \end{aligned}$$

Finally, for each $[\gamma] \in \pi_1(p)$, the inverse under $\bullet$ is the element $[-\gamma]$, where $-\gamma$ is defined by:

$$\begin{aligned} -\gamma : [0,1] &\to M \\ l &\mapsto \gamma(1-l) \end{aligned}$$

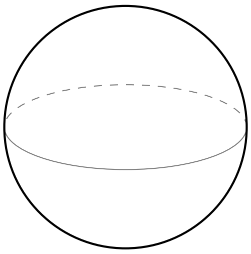
All the previously discussed topological properties are "boolean-valued", i.e. a topological space is either Hausdorff or not Hausdorff, either connected or not connected, and so on. The fundamental group is a "group-valued" property, i.e. the value of the property is not "either yes or no", but a group.

A property of a topological space is called an **invariant** if any two homeomorphic spaces share the property. A **classification** of topological spaces would be a list of topological invariants such that any two spaces which share these invariants are homeomorphic. As of now, no such list is known.

Example 25. *The 2-sphere is defined as the set:*

$$S^2 := \{(x,y,z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$$

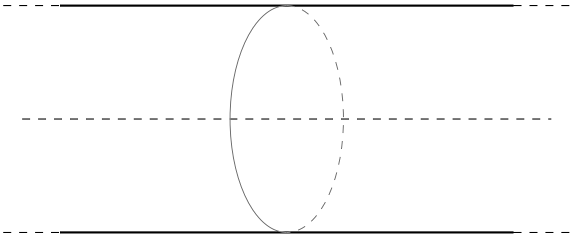
equipped with the subset topology inherited from $\mathbb{R}^3$.



The sphere has the property that all the loops at any point are homotopic, hence the fundamental group (at every point) of the sphere is the trivial group:

$$\forall\, p \in S^2 : \pi_1(p) = 1 := \{[\gamma_e]\}.$$

Example 26. *The cylinder is defined as $C := \mathbb{R} \times S^1$ equipped with the product topology.*

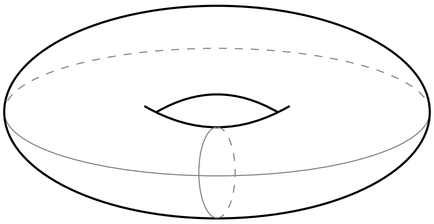


*A loop in C can either go around the cylinder (i.e. around its central axis) or not. If it does not, then it can be continuously deformed to a point (the identity loop). If it does, then it cannot be deformed to the identity loop (intuitively because the cylinder is infinitely long) and hence it is a homotopically different loop. The number of times a loop winds around the cylinder is called the **winding number**. Loops with different winding numbers are not homotopic.*

*Moreover, loops with different **orientations** are also not homotopic and hence we have:*

$$\forall\, p \in C : (\pi_1(p), \bullet) \cong_{\text{grp}} (\mathbb{Z}, +).$$

Example 27. *The 2-torus is defined as the set $T^2 := S^1 \times S^1$ equipped with the product topology.*



A loop in T^2 can intuitively wind around the cylinder-like part of the torus as well as around the hole of the torus. That is, there are two independent winding numbers and hence:

$$\forall\, p \in T^2 : \pi_1(p) \cong_{\mathrm{grp}} \mathbb{Z} \times \mathbb{Z},$$

where $\mathbb{Z} \times \mathbb{Z}$ is understood as a group under pairwise addition.

Chapter 5

Topological manifolds

Roughly, a topological manifold is a topological space that locally looks like $\mathbb{R}^d$.

Definition 65. *A paracompact Housdorff topological space $(M, \mathcal{O})$ is called a d-dimensional (topological)* ***manifold*** *if for every $p \in M : \exists p \in U \in \mathcal{O}$ and a homeomorphism $x : U \to x(U) \subseteq \mathbb{R}^d$*

Definition 66. *Let $(M, \mathcal{O})$ be a d-dimensional topological manifold and $N \subset M$. Then, $(N, \mathcal{O} \mid_N)$ is a* ***submanifold*** *of $(M, \mathcal{O})$ if it is a manifold in its own right.*

Definition 67. *Let $(M, \mathcal{O}_M)$ and $(N, \mathcal{O}_N)$ be a topological manifolds. Then, $(M \times N, \mathcal{O}_M \times \mathcal{O}_N)$ is a manifold of dimension $dim(M) + dim(N)$ called the* ***product manifold****. "We attach a copy of the second manifold to each point of the first".*

5.1 Viewing manifolds from atlases

Definition 68. *Let $(M, \mathcal{O})$ be a d-dimensional topological manifold. Then, a pair (U, x) where $U \in \mathcal{O}$ and $x : U \to x(U) \subseteq \mathbb{R}^d$ is a* ***chart*** *of the manifold. The component functions of x,*

$$\begin{aligned} x_i : U &\to \mathbb{R} \\ p &\mapsto proj_i(x(p)) \end{aligned}$$

are called the ***coordinates*** *of the point p with respect to the chart (U, x).*

Remark 15. *There exists a set of charts $\mathcal{A}$ such that $\bigcup U_i = M,\ (U_i, x_i) \in \mathcal{A}$. $\mathcal{A}$ is called* ***atlas****.*

Definition 69. *Two charts (U, x) and (V, y) are called **$\mathcal{C}^0$-compatible** if either*

1. *$U \cap V = \emptyset$*

2. *$U \cap V \neq \emptyset : y \circ x^{-1}$ is continuous.*

Remark 16. *The map $y \circ x^{-1} : \mathbb{R}^d \to \mathbb{R}^d$ is also called the **coordinate change chart**.*

Remark 17. *Continuity can be described at a topological level, but not differentiability. For that we have to use the chart-transition maps.*

Chapter 6

Algebraic structures

6.1 Group

Definition 70. *A* group $(G, \bullet)$ *is a set G equipped with a map*

$$\begin{aligned} \bullet\ : &\ G \times G \to G \\ &(g_1, g_2) \mapsto g_1 \bullet g_2 \end{aligned}$$

that satisfies ANI (Associative, Neutral element and Inverse element). If the map is commutative ($CANI$), the group is said to be commutative or abelian.

6.2 Ring

Definition 71. *A* ring $(R, +, \cdot)$ *is a set R equipped with two maps*

$$\begin{aligned} + :&\ \ R \times R \to R \\ \cdot\ :&\ \ R \times R \to R \end{aligned}$$

that satisfies $C^+A^+N^+I^+$ for R and $A^{\cdot}N^{\cdot}D^{\cdot}_+$ for $R \setminus \{0\}$. Where $D^{\cdot}_+$ means $\cdot$ is distributive wrt $+$.

6.3 Field

Definition 72. *A* field *(algebraic field)* $(K, +, \cdot)$ *is a set* K *equipped with two maps*

$$\begin{aligned} + :&\ K \times K \to K \\ \cdot\ :&\ K \times K \to K \end{aligned}$$

that satisfies $C^+A^+N^+I^+$ *for* K *and* $C^\cdot A^\cdot N^\cdot I^\cdot D^\cdot_+$ *for* $K \setminus \{0\}$

6.4 Module

Definition 73. *A* R-module $(M, \oplus, \odot)$ *over a ring* $(R, +, \cdot)$ *is a set* M *equipped with the maps*

$$\begin{aligned} \oplus &: M \times M \to M \\ \odot &: R \times M \to M \\ & r \odot m \mapsto r \cdot m \end{aligned}$$

that satisfies $C^\oplus A^\oplus N^\oplus I^\oplus$ *and* $AD^\odot_+ D^\odot_\oplus U^\odot$*.* U *stands for unitary.*

6.5 Vector space

Definition 74. *A* K-vector space $(V, \oplus, \odot)$ *over a field* $(K, +, \cdot)$ *is a set* V *equipped with the maps*

$$\begin{aligned} \oplus &: V \times V \to V \\ \odot &: K \times V \to V \\ & k \odot v \mapsto k \cdot v \end{aligned}$$

that satisfies $C^\oplus A^\oplus N^\oplus I^\oplus$ *and* $AD^\odot_+ D^\odot_\oplus U^\odot$*. A module is a vector space structure over a ring, i.e. non-commutative* $\cdot$*.*

Definition 75. $U \subset V$ *is a vector subspace if* $\forall u, u_1, u_2 \in U$

$$\begin{aligned} u_1 \oplus u_2 \in U \\ \lambda \odot u \in U \end{aligned}$$

Chapter 7

Linear maps

7.1 Linear Map

Definition 76. *Let* $(V, \oplus, \odot), (W, \boxplus, \boxdot)$ *be vector spaces over the same field* $(K, +, \cdot)$*. A map* $f : V \to W$ *is linear if*

$$\begin{aligned} &\forall v_1, v_2 \in V && f(v_1 \oplus v_2) = f(v_1) \boxplus f(v_2) \\ &\forall \lambda \in K,\ v \in V && f(\lambda \odot V) = \lambda \boxdot f(v) \end{aligned}$$

Definition 77. *Linear maps are the structure-preserving maps of vector spaces, i.e. the vector-space homomorphisms. The set containing all linear maps is defined as:*

$$Hom(V, W) := \{f : V \xrightarrow{\sim} W\}$$

Definition 78. $(Hom(V, W), +_H, \cdot_H)$ *can be made into a vector space by inducing the operators from* W*.*

Definition 79. *A linear map is called endomorphism if* $V = W$

Definition 80. *A bijective linear map is called a vector space isomorphism*

$$V \cong_{vec} W \Leftrightarrow \exists f : V \xrightarrow{\sim} W \mid f \text{ bijective}$$

Terminology

Definition 81. *Endomorphisms* $\equiv End(V) := Hom(V, V)$

Definition 82. *Automorphisms* $\equiv Aut(V) := End(V)$ *invertible.*

Definition 83. *Dual vector space* $\equiv V^* := Hom(V, K)$*. Heavily used.* V^* *is the set of linear functions.*

7.2 Linear independence. Basis

Definition 84. *Let V be a vector space. Then, $S = \{s_1, \dots, s_n\} \subseteq V$ is **linearly independent** if the linear combination of the vectors s_i is only degenerate for the degenerate linear combination. Mathematically,*

$$\sum_{i=1}^{n} \lambda_i s_i = 0, \lambda_i \in K \Rightarrow \lambda_i = 0, \forall i = 1, \dots, n$$

Definition 85. *$S \subset V$ is a **generating system** iff*

$$\forall v \in V \ \exists \{\lambda_1, \dots, \lambda_n\} : \sum_{i=1}^{n} \lambda_i s_i = v$$

which is denoted by $V = \langle S \rangle$

Definition 86. *A linearly independent generating system is called a **basis**.*

Remark 18. *One can choose arbitrary basis for V and V^*. However, it's more economical to derive the basis on V^* based on the choice of basis in V.*

$$\epsilon^a(e_b) = \delta^a_b$$

*This uniquely determines the choice of $\epsilon^1, \dots, \epsilon^n$ for a given choice of $e_1, \dots, e_n$. This is called a **dual basis** of V.*

Example 28. *Consider the 3rd degree polynomials. Then, a basis $\{e_0, e_1, e_2, e_3\} = \{1, x, x^2, x^3\}$ can be defined and a dual basis can be defined as*

$$\{\epsilon^0, \epsilon^1, \epsilon^2, \epsilon^3\} : \epsilon^a = \frac{1}{a!}\partial^a(\cdot) \mid_{x=0} = \delta^a_b$$

7.2.1 Change of basis

7.3 Kernel and image of a linear map

Definition 87. *Let $f : V \to W$ be a linear map. Then, its **kernel** is defined as:*

$$Ker(f) := x \in V : f(x) = 0$$

The kernel $Ker(f)$ and image $Im(f)$ are vector subspaces of V and W respectively, with

$$dim(Ker(f)) + dim(Im(f)) = dim(V)$$

Chapter 8

Multilinear maps: Tensors

Definition 88. *Let $(V, +, \cdot)$ be a K-vector space. A $(p, q)-$tensor T over V is a multilinear map*

$$T : \underbrace{V^* \times \cdots \times V^*}_{p\ copies} \times \underbrace{V \times \cdots \times V}_{q\ copies} \xrightarrow{\sim} K$$

Example 29.

$$\varphi \in V^* \Leftrightarrow \varphi : V \xrightarrow{\sim} K \Leftrightarrow \varphi \text{ is a } (0,1)-tensor.$$
$$v \in V \Leftrightarrow v \in (V^*)^* \Leftrightarrow v : V^* \xrightarrow{\sim} K \Leftrightarrow v \text{ is a } (1,0)-tensor.$$

In addition, linear maps are $(1, 1)-$tensor. An inner product on a vector space is a $(0, 2)-$tensor. The "inverse" or dual inner product is a $(2, 0)-$tensor.

8.1 Components of tensors

Definition 89. *Let T be an $(p, q)-$tensor over a finite-dimensional vector space V. Then, define the $(p + q)^{dim(V)}$ real numbers.*

$$T^{i_1,\ldots,i_p}{}_{j_1,\ldots,j_q} := T(\epsilon^{i_1}, \ldots, \epsilon^{i_p}, e^{j_1}, \ldots, e^{j_q}) \in K$$

8.1.1 Reconstruction of T from its components

Example 30. *T is a $(1, 1)-$tensor. Then,*

$$T^i{}_j := T(\epsilon^i, e_j)$$

thus,

$$T(\varphi, v) = T(\sum_{i=1}^{dimV} \varphi_i \epsilon^i, \sum_{j=1}^{dimV} v^j e_j) = \sum_{i=1}^{dimV} \sum_{j=1}^{dimV} \varphi_i v^j T(\epsilon^i, e_j) =: \varphi_i v^j T^i{}_j$$

where the last term is written in Einstein summation convention, where up-down matching indices are summed over.

Chapter 9

Differentiable manifolds

9.1 Adding structure by refining the (maximal) topological atlas

Definition 90. *Let $(M, \mathcal{O})$ be a manifold. An atlas $\mathcal{A}$ is called a $\clubsuit-$**atlas** if any two charts $(U, x), (V, y) \in \mathcal{A}$ are $\clubsuit-$compatible. In other words, either:*

- $U \cap V = \emptyset$
- $U \cap V \neq \emptyset \Rightarrow y \circ x^{-1}$ *must be* $\clubsuit$ *as a* $\mathbb{R}^d \to \mathbb{R}^d$ *map.*

Where $\clubsuit$ can be:

- C^0
- C^k*: The transition maps are k-times continuously differentiable (traditional def.)*
- C^∞*: Smooth.*
- C^ω*: Real analytic (Can be Taylor expanded).*
- *Complex: Transition functions satisfy the Cauchy-Riemman equations.*

Theorem 9.1.1. *Any maximal $C^{k\geq 1}-$atlas contains a $C^\infty-$atlas. Two maximal C^k-atlasses that contain the same $C^\infty-$atlas are identical. This implies that you do not need to distinguish between $C^{k\geq 1}$ and C^∞ in the previous sense.*

Definition 91. *A C^k-manifold is a triple $(M, \mathcal{O}, \mathcal{A})$ where $(M, \mathcal{O})$ is a topological manifold and $\mathcal{A}$ is a C^k-atlas.*

Definition 92. *Let $\phi : M \to N$ be a map, where $(M, \mathcal{O}_M, \mathcal{A}_M)$ and $(N, \mathcal{O}_N, \mathcal{A}_N)$ are C^k-manifolds. Then, ϕ is called **differentiable** at a point $p \in M$ if for some $(U, x) \in \mathcal{A}_M$ with $p \in U$ and some chart $(V, y) \in \mathcal{A}_N$ with $\phi(p) \in V$ the map $y \circ \phi \circ x^{-1}$ is C^k as a map from $\mathbb{R}^{dim(M)} \to \mathbb{R}^{dim(N)}$.*

Definition 93. *If $\phi M \to N$ is bijective and both ϕ and ϕ^{-1} are C^∞, then ϕ is called **diffeomorphism**. They are the structure preserving maps over differentiable manifolds.*

Definition 94. *$(M, \mathcal{O}_M, \mathcal{A}_M)$ and $(N, \mathcal{O}_N, \mathcal{A}_N)$ are called diffeomorphic if there exist a diffeomorphism between them.*

$$M \cong_{diff} N \equiv (M, \mathcal{O}_M, \mathcal{A}_M) \cong_{diff} (N, \mathcal{O}_N, \mathcal{A}_N)$$

Remark 19. *It is custom to consider diffeomorphic smooth manifolds to be the same.*

Remark 20. *The key feature of the differentiable manifolds is that exists a **tangent** (vector) **space** at each point of the manifold.*

9.2 Tangent spaces to a manifold

Definition 95. *Let M be a smooth manifold. Then, we can construct the vector space over $\mathbb{R} : (C^\infty(M), +, \cdot)$ where the operators are inherited from $\mathbb{R}$ and $C^\infty(M)$ is the set of all smooth functions on the manifold $f : M \to \mathbb{R}$.*

Definition 96. *Let $\gamma : \mathbb{R} \to M$ be a smooth curve through a point $p \in M$. Without loss of generality (w.l.o.g.), we may arrange for $p = \gamma(0)$. **The directional derivative operator** at p along the curve γ is a linear map:*

$$\begin{aligned} X_{\gamma,p} : C^\infty(M) &\to \mathbb{R} \\ f &\mapsto (\underbrace{f \circ \gamma}_{\mathbb{R}\to\mathbb{R}})'(0) \end{aligned}$$

*In differential geometry, $X_{\gamma,p}$ is usually called the **tangent vector** to the curve γ at the point $p \in M$. It is also called the velocity of γ at p.*

Definition 97. *The **tangent vector space** is the set*

$$T_pM := \{X_{\gamma,p} \; \forall \; \gamma \text{ smooth curves through } p\}$$

equipped with:

$$\begin{aligned} \oplus &: T_pM \times T_pM \to T_pM \\ \odot &: \mathbb{R} \times T_pM \to T_pM \end{aligned}$$

We can directly inherit the operators from $\mathbb{R}$.

$$\begin{aligned}(X_{\gamma,p} \oplus X_{\delta,p})(f) &:= X_{\gamma,p}(f) + X_{\delta,p}(f) \\ (\lambda \odot X_{\gamma,p})(f) &:= \lambda \cdot X_{\gamma,p}(f)\end{aligned}$$

Chapter 10

Lie groups and their Lie algebras

Chapter 11

Construction of *SE(3)*

Chapter 12

Conceptos básicos I

Para comenzar el estudio del álgebra lineal, es preciso introducir conceptos pertenecientes al álgebra abstracta:

12.1 Conjuntos

Un conjunto es una reunión de determinados objetos bien definidos y diferenciables los unos de los otros. A modo de ejemplo tenemos los siguientes conjuntos numéricos:

- Los números naturales: $\mathbb{N} = \{0, 1, 2, 3, ...\}$
- Los números enteros: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- Los números racionales: $\mathbb{Q} = \{\frac{a}{b} : \ a, b \in \mathbb{Z}, \ b \neq 0\}$
- Los números iracionales: $\mathbb{I} = \{\sqrt{2}, \sqrt{5}, \pi, e, \ldots\}$
- Los números reales: $\mathbb{R} = \{\mathbb{Q} \cup \mathbb{I}\}$
- Los números complejos: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$

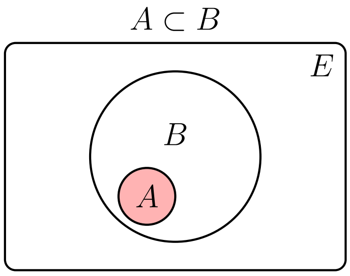
Sea A un conjunto numérico. Denotaremos por A^* al conjunto de elementos de A salvo el cero, mientras que A^+ y A^- designan a los elementos positivos y negativos de A respectivamente. Por ejemplo, $\mathbb{N}^* = \{1, 2, 3, ...\} = \mathbb{Z}^+$, $\mathbb{Z}^- = \{..., -3, -2, -1\}$

Al número de elementos de A lo denominamos cardinal de A y se denota por $card(A)$

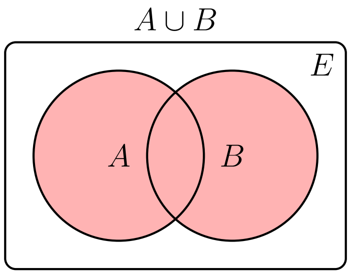
Operaciones entre conjuntos

Sean A y B como dos conjuntos contenidos en un tercero E. Las operaciones básicas que se pueden realizar entre ellos son las siguientes:

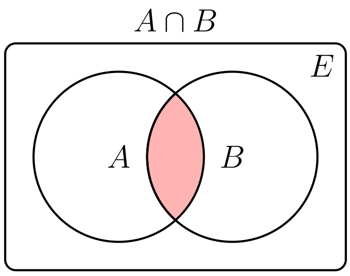
- Inclusión: $A \subset B \equiv \{x: \ x \in A \Rightarrow x \in B\}$



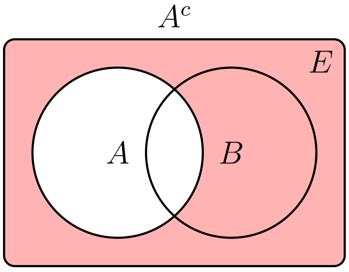
- Unión: $A \cup B \equiv \{x: \ x \in A \text{ ó } x \in B\}$



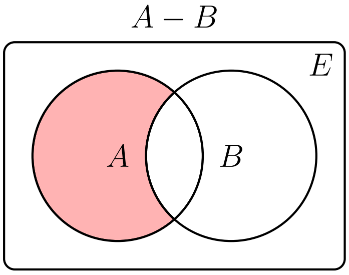
- Intersección: $A \cap B \equiv \{x: \ x \in A \text{ y } x \in B\}$



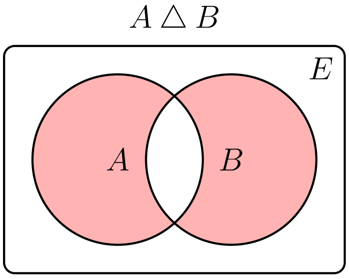
- Contrario o complementario: $A^c = \overline{A} \equiv \{x: \ x \notin A\}$



- Diferencia: $A - B = A \backslash B = A \cap B^c = A - (A \cap B) \equiv \{x \in A: \ x \notin B\}$



- Diferencia simétrica: $A \vartriangle B = (A - B) \cup (B - A)$



Para operar con n conjuntos emplearemos las siguientes notaciones:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n \quad \forall i \neq j$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap ... \cap A_n$$

Ejemplo:

Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{1, 3, 6, 7, 9\}$ y $B = \{2, 3, 5, 7, 10\}$. Entonces:

- $A \cup B = \{1, 2, 3, 5, 6, 7, 9, 10\}$
- $A \cap B = \{3, 7\}$
- $A^c = \{2, 4, 5, 8, 10\}, \quad B^c = \{1, 4, 6, 8, 9\}$
- $A - B = \{1, 6, 9\}, \quad B - A = \{2, 5, 10\}$
- $A \bigtriangleup B = \{1, 2, 5, 6, 9, 10\}$

Partición de un conjunto

Particionar un conjunto E consiste en dividirlo en subconjuntos tales que:

1. $$A_i \cap A_j = \emptyset$$

2. $$E = \bigcup_{i=1}^{n} A_i$$

Ejemplo:

Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ podemos particionarlo, por ejemplo, en tres subconjuntos de diferentes tamaños: $A = \{1, 2\}$, $B = \{3, 5, 7\}$ y $C = \{4, 6, 8, 9, 10\}$. De ésta manera se cumple que:

- $A \cap B = \emptyset$, $A \cap C = \emptyset$ y $B \cap C = \emptyset$
- $E = A \cup B \cup C$

También podemos comprobar que el cardinal de un conjunto es la suma del cardinal de sus particiones: $card(E) = card(A) + card(B) + card(C) = 2 + 3 + 5 = 10$.

Producto cartesiano

Sean dos conjuntos A y B. Se define el producto cartesiano $A \times B$ al conjunto de todos los pares ordenados (a, b) en los que el primer componente pertenece a A y el segundo a B, es decir:

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

Ejemplo:

Sean dos conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3, 4\}$. Entonces:

$$A \times B = \left\{ \begin{matrix} (a,1) & (a,2) & (a,3) & (a,4) \\ (b,1) & (b,2) & (b,3) & (b,4) \\ (c,1) & (c,2) & (c,3) & (c,4) \end{matrix} \right\}$$

Propiedades de los conjuntos

Para facilitar la comprensión de algunas de las siguientes propiedades podemos utilizar las semejanzas entre las propiedades de las operaciones de conjuntos y las operaciones numéricas. Así, la unión se asemeja a la suma numérica, la intersección al producto, el conjunto vacío sería el equivalente del cero y el complementario equivaldría a un cambio de signo.

Sean dos subconjuntos A, B y C pertenecientes al conjunto E. Se dice que las partes de E $P(E)$ forman un Álgebra de Boole si se cumplen las siguientes propiedades.

1. Idempotente: $A \cap A = A \quad A \cup A = A$
2. De complemento: $A \cap A^c = \emptyset \quad A \cup A^c = E$
3. Conmutativa: $A \cap B = B \cap A \quad A \cup B = B \cup A$
4. Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$
   $(A \cap B) \cap C = A \cap (B \cap C)$
5. Distributiva: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. Elemento absorbente: $A \cap \emptyset = \emptyset \quad A \cup E = E$
7. Elemento neutro: $A \cup \emptyset = A \quad A \cap E = A$
8. Simplificativa: $A \cap (A \cup B) = A \quad A \cup (A \cap B) = A$
9. Leyes de Morgan: $(A \cup B)^c = A^c \cap B^c \qquad (A \cap B)^c = A^c \cup B^c$

El lector puede comprobar el cumplimiento de todas estas propiedades gráficamente o numéricamente definiendo los conjuntos A, B, C y E.

12.2 Relaciones binarias

Se denomina relación binaria a la vinculación de dos elementos (a y b por ejemplo) y se denota por aRb.

Sean dos conjuntos A y B. Se llama grafo a cualquier subconjunto G del producto cartesiano $A \times B$.

$$G \subset A \times B$$

Se dirá que $a \in A$ está relacionado con $b \in B$ a través de G (aR_Gb) si el par ordenado (a, b) pertenece a G.

$$aR_Gb \Leftrightarrow (a, b) \in G$$

Ejemplo:

Tomemos el mismo ejemplo que usamos para el producto cartesiano. Sean dos conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3, 4\}$. Definiremos el grafo

$$G = \{(a, 1), (b, 2), (b, 3), (c, 3), (c, 4)\}$$

De ésta manera, tenemos en G qué elementos de A que están relacionados con qué elementos de B mediante pares ordenados (a, b). Así tenemos, por ejemplo, que bR_G2 y que cR_G3.

Otra forma de establecer una relación es mediante una propiedad p. Así diremos que

$$aRb \Leftrightarrow p(a, b) \text{ es cierta}$$

Ejemplo:

Sean los conjuntos $A = \{1, 3, 5, 7\}$ y $B = \{2, 4, 6, 8\}$ y tomemos como propiedad $p(a, b) = a > b$. De ésta manera podemos construir el grafo donde quedan incluidas todas las relaciones que cumplen dicha propiedad:

$$aRb \Leftrightarrow a > b \Rightarrow G = \{(3, 2), (5, 2), (5, 4), (7, 2), (7, 4), (7, 6)\}$$

Propiedades de las relaciones binarias

- Reflexiva: $aRa,\ \forall a \in A$
- Simétrica: $aRb \Rightarrow bRa$
- Antisimétrica: $aRb\ y\ bRa \Rightarrow a = b$
- Transitiva: $aRb\ y\ bRc \Rightarrow aRc$
- Antirreflexiva: $a\not{R}a,\ \forall a \in A$
- Conexa: aRb ó $bRa,\ \forall (a,b) \in A \times A,\ a \neq b$
- Euclídea: aRb y $aRc \Rightarrow bRc$

Relaciones binarias de equivalencia

Se dice que una relación binaria es de equivalencia si verifica las propiedades reflexiva, simétrica y transitiva. Se denota por $a \sim b$.

$$R \text{ es de equivalencia } \Leftrightarrow \ R \text{ es } \begin{cases} \text{Reflexiva} \\ \text{Simétrica} \\ \text{Transitiva} \end{cases}$$

Clase de equivalencia

Sea A un conjunto y $\sim$ una relación binaria de equivalencia definida en A. Se denomina clase de equivalencia del elemento $a \in A$, denotada por $[a]$ o por $\overline{a}$, al subconjunto de A formado por todos los elementos relacionados con a, es decir,

$$[a] \equiv \{b \in A : a \sim b\}$$

Puesto que las relaciones de equivalencia, por definición, son transitivas y simétricas podemos afirmar que la clase de equivalencia de dos elementos relacionados es la misma y, por tanto, cualquiera de los elementos puede representar a dicha clase.

$$a \sim b \Leftrightarrow [a] = [b] \tag{12.1}$$

Además podemos afirmar que dos elementos no relacionados pertenecen a distintas clases de equivalencia.

$$a \nsim b \Leftrightarrow [a] \cap [b] = \emptyset \tag{12.2}$$

Basándonos en lo deducido en las expresiones 12.1 y 12.2, podemos afirmar que cada clase de equivalencia define una partición del conjunto A ya que se cumplen las expresiones 12.3 y 12.4.

$$A = \bigcup_{i=1}^{n} [a_i] \tag{12.3}$$

$$[a_i] \cap [a_j] = \emptyset \quad \text{si} \quad a_i \not\sim a_j \tag{12.4}$$

Conjunto cociente

Al conjunto de todas las clases de equivalencia del conjunto A se le llama conjunto cociente, y se representa por $A/\sim$.

$$A/\sim \equiv \{[a_i] : a_i \in A\}$$

Ejemplo:

Sea $A = \{1, 2, 3, 4, 5\}$ y el grafo

$$G = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1), (2,4), (4,2)\}$$

Apoyándonos en la Figura 12.1, comprobamos que es relación binaria de equivalencia ya que es reflexiva, simétrica y transitiva.

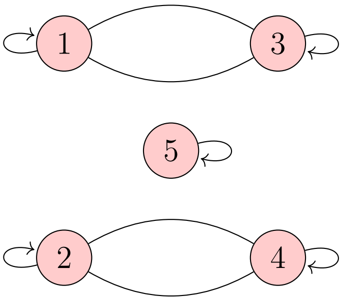


Figure 12.1: Diagrama sagital de las relaciones binarias

Las clases de equivalencia son:

$$\begin{aligned}
[1] &= \{1, 3\} = [3] \\
[2] &= \{2, 4\} = [4] \\
[5] &= \{5\}
\end{aligned}$$

Por tanto, el conjunto cociente será:

$$A/\sim=\{[1],[2],[5]\}$$

Relaciones binarias de orden

Se dice que una relación binaria es de orden si verifica las propiedades reflexiva, antisimétrica y transitiva. Se denota por $a \leq b$. Si $a \leq b$ se dice que a es anterior a b o que b es posterior a a.

$$R \text{ es de equivalencia } \Leftrightarrow R \text{ es } \begin{cases} \text{Reflexiva} \\ \text{Antisimétrica} \\ \text{Transitiva} \end{cases}$$

Una relación es de **orden total** si además es conexa, es decir, todos los elementos están relacionados. Si no es conexa será relación de **orden parcial**. Se dirá entonces que A está totalmente o parcialmente ordenado si en él hay definida una relación de orden total o parcial respectivamente. Se llama cadena a un subconjunto no vacío totalmente ordenado.

Sean $(A, \leq)$ un conjunto ordenado y B un subconjunto no vacío de A.

Llamamos **cota superior** de B a cualquier elemento de A que es posterior a todo elemento de B. Si existe alguna cota superior, se dice que B está acotado superiormente.

Llamamos **cota inferior** de B a cualquier elemento de A que es anterior a todo elemento de B. Si existe alguna cota inferior, se dice que B está acotado inferiormente.

Si B está acotado inferiormente y superiormente, se dirá simplemente que está acotado.

Extremo superior de B o **supremo** de B es la menor de las cotas superiores de B. Se denota por $sup_A(B)$. Si el supremo pertenece a B, se llama **máximo.**

Extremo inferior de B o **ínfimo** de B es la mayor de las cotas inferiores de B. Se denota por $inf_A(B)$. Si el ínfimo pertenece a B, se llama **mínimo.**

Un conjunto se dice que está **bien ordenado** si todo subconjunto suyo no vacío tiene mínimo.

Elemento maximal de B es cualquier elemento de B tal que no existe un elemento posterior a él.

Elemento minimal de B es cualquier elemento de B tal que no existe un elemento anterior a él.

Un conjunto A ordenado se llamará **retículo** si todo subconjunto suyo formado por dos elementos posee ínfimo y supremo.

Ejemplo:

Sea $A = \{2, 3, 5, 6, 8, 16, 18\}$ y consideremos en A la relación de divisibilidad.

$$\forall x, y \in A \quad xRy \Leftrightarrow x|y$$

Inciso: El término $x|y$ significa x divide a y. Ésto se cumple cuando el resto de la división y/x es cero y, por tanto, y es un múltiplo de x. En notación matemática sería:

$$\forall x, y \in \mathbb{Z} \quad x|y \Leftrightarrow \exists\ k \in \mathbb{Z} : y = kx$$

Puede comprobarse fácilmente que ésta relación es reflexiva, antisimétrica y transitiva. Además, no todos los elementos están relacionados por lo que es de orden parcial.

Una herramienta gráfica empleada para las relaciones de orden es el diagrama de Hasse. Está estructurado de abajo a arriba en niveles en función de la anterioridad o posterioridad de cada elemento.

Podemos observar, en la figura 12.2, el diagrama de Hasse de nuestro ejemplo. Comprobamos que los elementos 2 y 3 son minimales y los elementos 16 y 18 son maximales. El 5 es minimal y maximal a la vez.

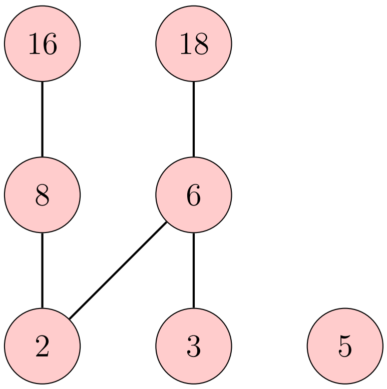


Figure 12.2: Diagrama de Hasse

En éste caso, no tenemos ni máximo ni mínimo ya que no hay ningun elemento de A que acote superior o inferiormente al resto. Puesto que $A \subset \mathbb{N}$ podemos encontrar cotas superiores e inferiores naturales. El 1 divide al resto, por lo que es una cota inferior de A_R. El 720 es múltiplo de los tres maximales, por lo que es cota superior de A_R.

12.3 Principio de Inducción

Sea $P(n)$ una proposición matemática en función de un número entero positivo $n \in \mathbb{Z}^+$. Si $P(n)$ puede ser únicamente verdadera o falsa, entonces podemos emplear el principio de inducción:

Si P(1) es cierta, y si suponiendo que P(k) es verdadera se puede demostrar que P(k+1) también lo es, entonces $P(n)$ es cierta para todo $n \in \mathbb{Z}^+$.

Ejemplo:

Demostrar que la siguiente ecuación es cierta:

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}^*$$

Comprobamos que para $n = 1$ es cierto.

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$$

Supongamos que para $n = k$ es cierto.

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Para $n = k + 1$ tenemos que:

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

12.4 Aplicaciones

Dados dos conjuntos A y B, una función o aplicación $f : A \rightarrow B$ es un caso particular de relación binaria que asocia a cada $a \in A$ un único objeto $b \in B$, que se denomina imagen de a y se denota por $b = f(a)$.

Al conjunto de los elementos de A para los cuales existe imagen se denomina dominio de la función y se denota por $Dom(f)$.

Al conjunto de todas las imágenes de A se denomina imagen de la función y se denota por $Im(f)$.

$$Im(f) = f(A) = B$$

Se define la imagen reciproca de de $b \in B$ como el conjunto de los elementos de A cuya imagen es b. Se denota por $f^{-1}(b)$.

$$f^{-1}(b) := \{a \in A : f(a) = b\}$$

Tipos de aplicaciones

- **Aplicación inyectiva:** Una aplicación es inyectiva si no hay dos objetos del dominio con la misma imagen.

$$f(x) = f(y) \Longleftrightarrow x = y$$

- **Aplicación sobreyectiva:** Una aplicación es sobreyectiva si todos los objetos de B son imagen de almenos un objeto de A:

$$\forall b \in B \ \exists \ a \in A / f(a) = b \Longleftrightarrow Im(f) = B$$

- **Aplicación biyectiva:** Una función es biyectiva si es sobreyectiva e inyectiva a la vez. Por tanto, todos los elementos de A tienen una imagen distinta en B y a cada $b \in B$ le corresponde un único elemento $a \in A$.

Para las aplicaciones biyectivas existe una aplicación o **función inversa**, denotada por f^{-1}, tal que

$$f^{-1}(b) = a$$

Composición de aplicaciones

Sean $f : A \to B$ y $g : C \to D$ dos aplicaciones con $B \subset C$. Se denomina función o aplicación compuesta a

$$(g \circ f)(a) \equiv g(f(a))$$

Propiedades:

- Asociativa: $h \circ (g \circ f) = (h \circ g) \circ f$
- No conmutativa en general.
- La composición de aplicaciones inyectivas es una aplicación inyectiva.
- La composición de aplicaciones sobreyectivas es una aplicación sobreyectiva.
- La composición de aplicaciones biyectivas es una aplicación biyectiva.

Chapter 2

Estructuras algebraicas

2.1 Operación interna

Sea A un conjunto no vacío. Se llama operación interna definida en A a cualquier aplicación de $A \times A$ en A que asocia a cada par (a, b) de elementos de A un único elemento c, resultado de operar a con b. Mátemáticamente, para el operador "$*$", se expresa de la siguiente forma:

$$\begin{array}{c} A \times A \overset{*}{\to} A \\ (a,b) \to c := a * b \end{array} \qquad \text{con } a, b, c \ \in A$$

Ejemplo:

El producto de números reales $(\mathbb{R}, \cdot)$ es una operación interna del conjunto de los números reales, ya que cualquier producto de números reales da como resultado otro número real.

$$x \cdot y \in \mathbb{R} \quad \forall x, y \in \mathbb{R}$$

Propiedades

Sea $(A, *)$ un conjunto no vacío (A) donde hay definida una operación interna $(*)$. Diremos que la operación es:

- **Asociativa** $\Leftrightarrow a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$

- **Conmutativa** $\Leftrightarrow a * b = b * a \quad \forall a, b \in A$

Añadamos una nueva operación interna a nuestro par, obteniendo $(A, *, \circ)$. Diremos que $\circ$ es **distributiva** respecto de $*$ si

$$\forall a, b, c \in A, \begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c), \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

Elementos particulares

- Elemento neutro e: $\quad a * e = e * a = a$
- Elemento simétrico a': $\quad a * a' = a' * a = e$

Ejemplo:

Sea $(\mathbb{R}, +, \cdot)$ el conjunto de los números reales con las operaciones internas de producto y suma. Podemos comprobar que tanto el producto como la suma son asociativos y conmutativos. Además el producto es distributivo respecto de la suma ya que:

$$\forall a, b, c \in \mathbb{R}, \begin{cases} a \cdot (b + c) = (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c = (a \cdot c) + (b \cdot c) \end{cases}$$

2.2 Operación externa

Dados dos conjuntos A y K, se llama operación externa definida en A y con dominio de escalares K, a cualquier aplicación:

$$\begin{array}{c} K \times A \overset{\perp}{\rightarrow} A \\ (k, a) \rightarrow b := k \perp a \end{array} \qquad \text{con} \qquad \begin{array}{c} k \in K \\ a \in A \end{array}$$

Ejemplo:

Sea $V_3 \equiv \{v = (x, y, z) \quad \forall x, y, z \in \mathbb{R}\}$ el conjunto de los vectores reales de tres dimensiones y el conjunto de los escalares enteros $K \equiv \{k \quad \forall k \in \mathbb{Z}\}$. El producto de escalares por vectores es operación externa ya que $k \cdot v \in V_3$.

2.3 Homomorfismos

Sean $(A, *)$ y $(B, \circ)$ dos conjuntos con operaciones internas definidas. Una aplicación $f : A \rightarrow B$ es un **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in A$$

Si f es un homomorfismo y además

- es inyectivo se llamará **monomorfismo**.
- es sobreyectivo se llamará **epimorfismo**.
- es biyectivo se llamará **isomorfismo**.
- $A = B$ se llamará **endomorfismo**.
- es endomorfismo biyectivo se llamará **automorfismo**

Ejemplo:

Sean $G = (\mathbb{R}, +)$ y $H = (\mathbb{R}^+, \cdot)$. Definamos una aplicación

$$\begin{gathered} f : G \leftarrow H \\ x \mapsto e^x \end{gathered}$$

Podemos afirmar que se trata de un homomorfismo ya que

$$\begin{gathered} f(x + y) = f(x) \cdot f(y) \\ e^{x+y} = e^x + e^y \end{gathered}$$

2.4 Grupo

Un **grupo** es una pareja $(G, *)$, donde G es un conjunto en el que está definida una operación interna $*$ que verifica:

1. Asociativa.
2. Existencia de elemento neutro e, es decir, $g * e = g$
3. Todo elemento g posee simétrico g', es decir, $g * g' = e$

Si además la operación interna $*$ es conmutativa, el grupo se llamara **abeliano**.

Propiedades de un grupo

- El elemento neutro es único
- $(a * b)' = b' * a'$
- $(a')' = a$
- $a * x = a * y \Rightarrow x = y$

Orden de un grupo

Sea $(G, *)$ un grupo. El **orden** de un elemento $a \in G$ es el menor entero positivo $k \in \mathbb{N}^*$ para el que $a^k = e$. Si no existe k, el orden es infinito o cero.

Al número de elementos de un grupo se le llama **orden** de G y se denota por $|G|$.

Ejemplo:

El conjunto de los números enteros con la suma $(\mathbb{Z}, +)$ es un grupo abeliano ya que:

1. La suma de numeros enteros es otro número entero.
2. El elemento neutro de los enteros con la suma es el cero: $z + 0 = z$.
3. Todo z posee un simétrico $-z$: $z + (-z) = 0$.
4. La suma de enteros es conmutativa: $z_1 + z_2 = z_2 + z_1$.

A modo de ejemplo diremos que el orden del grupo es infinito $|\mathbb{Z}| = \infty$. El orden de los elementos son

$$\begin{aligned} &|1| = 1 \\ &|-1| = 2 \\ &|z| = \infty \quad \forall z \in \mathbb{Z} - \{-1, 1\} \end{aligned}$$

Subgrupo

Sea $(G, *)$ un grupo y $H \subset G$, un subconjunto suyo no vacío. $(H, *)$ es **subgrupo** si también posee estructura de grupo.

Caracterización

Un subconjunto H es subgrupo si se cumple que

$$\forall a, b \in H \Rightarrow a * b \in H \tag{2.1}$$
$$\forall a \in H \Rightarrow a' \in H \tag{2.2}$$

Las ecuaciones 2.1 y 2.2 se pueden resumir en la siguiente

$$\forall a, b \in H \Rightarrow a * b' \in H$$

Clases de un grupo

Dado un grupo G, un subgrupo H y un elemento $a \in G$ arbitrario fijo, a los conjuntos

$$aH = \{x/x \in G, x = a * h, h \in H\}$$
$$Ha = \{x/x \in G, x = h * a, h \in H\}$$

se les denomina respectivamente **clases** del grupo G a la izquierda y a la derecha módulo el subgrupo H. Se les llama así por ser clases de cierta relación de equivalencia [1] y, por tanto, forman particiones del grupo G.

Si $aH = Ha$ entonces, H es un subgrupo **normal o invariante**.

Supongamos que el grupo G es finito y que posee n clases a la izquierda módulo H. Entonces,

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH$$

$$|G| = |a_1H| + |a_2H| + \cdots + |a_nH| = n|H|$$

por lo que el orden de un grupo finito G será múltiplo del orden de cualquier subgrupo suyo (**teorema de Lagrange**).

Al cociente $n = |G|/|H|$ se le denomina **índice del subgrupo** H.

Un grupo G se dice **finitamente generado** si existe una parte finita A de G que engendra todo G. Si A se reduce a un elemento, el grupo G se llama **monógeno**.

El grupo G es **cíclico** si es monógeno y finito.

$$G =< a >= \{a^n : n \in \mathbb{Z}\}$$

Nota: Con a^n nos referimos a aplicar n veces el operador $*$ sobre a. Ésto coincidirá con la potencia en el caso de que la operación sea el producto pero, en general, no es así.

[1] La relación es $x \sim y \Leftrightarrow x' * y \in H$, aunque no es de interés para ésta explicación.

Homomorfismo de grupos

Al igual que en la sección anterior, dos grupos $(G_1, *)$, $(G_2, \circ)$ y una aplicación $f : G_1 \to G_2$ es **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in G_1$$

Llamamos **núcleo** de f, representándose por $Ker(f)$, al conjunto de los elementos del dominio cuya imagen es el elemento neutro de G_2.

$$Ker(f) = \{x \in G_1 : f(x) = e_2\} = f^{-1}(e_2)$$

Llamamos **imagen** de f, denotándose por $Im(f)$, como el subconjunto de G_2 formado por aquellos elementos que son imagen de algún elemento de G_1. Es decir,

$$Im(f) = \{y \in G_2 : \exists x \in G_1, f(x) = y\}$$

Por tanto, podemos decir que

$$\begin{aligned} &f \textit{ es inyectiva } \Leftrightarrow Ker(f) = \{e_1\} \\ &f \textit{ es sobreyectiva } \Leftrightarrow Im(f) = G_2 \end{aligned}$$

2.5 Anillo

Un anillo es un conjunto dotado con dos operaciones internas llamadas suma y producto. El anillo $(R, +, \cdot)$ cumple que:

1. $(R, +)$ es un grupo abeliano.

2. El producto es asociativo.

3. Existe un elemento neutro para la multiplicación.

4. El producto es distributivo respecto a la suma.

Si el producto es conmutativo se dice que el anillo es conmutativo. Si el producto posee elemento neutro es unitario.

El elemento neutro de la suma será 0 y el del producto 1.

Subanillo

Cuerpo

Un cuerpo es un anillo conmutativo y unitario en el que todo elemento distinto de cero es invertible respecto del producto, es decir, un anillo de división conmutativo.

Por ejemplo, los números reales con la suma y el producto algebraicos $(\mathbb{R}, +, \cdot)$ es un cuerpo ya que:

1. $(\mathbb{R}, +)$ es un grupo abeliano (siendo 0 el elemento neutro de la suma)

2. El producto de números reales es asociativo.

3. El elemento neutro de la multiplicación es el 1.

4. El producto es distributivo respecto de la suma (propiedades de anillo cumplidas).

5. El anillo es conmutativo, ya que el producto de números reales lo es.

6. El anillo es unitario ya que el neutro de la multiplicación es distinto del de la suma.

7. Todo elemento distinto de cero es invertible respecto del producto: Sea $r \in \mathbb{R}$ y $r \neq 0$, entonces $\frac{1}{r} \in \mathbb{R}$.

Así lo serían también $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{Q}, +, \cdot)$.

Chapter 3

Espacios Vectoriales y Aplicaciones lineales

3.1 Espacio vectorial

Un espacio vectorial sobre un cuerpo $(K, +, \cdot)$ es un grupo abeliano $(V, +)$ dotado con una operación externa $K \times V \to V$, que verifica las siguientes propiedades:

1. Distributiva respecto a escalares → $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$
2. Distributiva respecto a vectores → $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
3. Asociativa → $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$
4. Modular → $1 \cdot v = v$

Con $\lambda,\ \mu \in K$ y $v, w\ \in V$.
Si el espacio vectorial en cuestión tiene como cuerpo a los números reales será un espacio vectorial real, mientras que si tiene a los números complejos se denotará como espacio vectorial complejo.
Veamos a continuación un ejemplo práctico para su mejor comprensión:

Ejemplo 1

Demostrar que el conjunto $\mathbb{C}$ de los números complejos, con las operaciones suma y producto usuales, tiene estructura de espacio vectorial sobre el cuerpo de los números reales:

Demostremos que $(\mathbb{C}(\mathbb{R}), +, \cdot)$ tiene estructura de espacio vectorial:

Partiendo de que $(\mathbb{R}, +, \cdot)$ es un cuerpo, comprobamos que $(\mathbb{C}, +)$ es grupo abeliano:

1. Operación interna: La suma de números complejos es una operación interna ya que da como resultado otro número complejo:

$$(a + bi) + (c + di) = (a + b) + (c + d)i \in \mathbb{C}$$

2. Propiedad asociativa: La suma de números complejos es asociativa, ya que:

$$(a+bi)+[(c+di)+(e+fi)] = [(a+bi)+(c+di)]+(e+fi) = (a+c+e)+(b+d+f)i$$

3. Existencia de elemento neutro $(0 + 0i)$, ya que:

$$(a + bi) + (0 + 0i) = a + bi$$

4. Existencia de elemento simétrico $[(-a) + (-b)i]$, ya que:

$$(a + bi) + [(-a) + (-b)i] = (0 + 0i)$$

5. Propiedad conmutativa: La suma de números complejos es conmutativa, ya que:

$$(a + bi) + (c + di) = (c + di) + (a + bi) = (a + b) + (c + d)i$$

Es trivial demostrar que el producto de escalares reales con números complejos es operación externa, ya que el producto de un número real por un número complejo sigue siendo un número complejo:

$$r * (a + bi) = ra + rbi \in \mathbb{C} \quad \text{con } r, a, b \in \mathbb{R}$$

Por lo que $\mathbb{R} \times \mathbb{C} \dot{\to} \mathbb{C}$.

Para terminar demostramos las cuatro propiedades que hacen que un grupo abeliano con operacion externa e interna sea un espacio vectorial sobre el cuerpo, en este caso, de los números reales:

1. Distributiva respecto a escalares:

$$r[(a+bi)+(c+di)] = r(a+bi)+r(c+di) = (ra+rc)+(rb+rd)i$$

2. Distributiva respecto a vectores:

$$(r+s)(a+bi) = r(a+bi)+s(a+bi) = (ra+sa)+(rb+sb)i$$

3. Asociativa:

$$r[(a+bi)(c+di)] = [r(a+bi)](c+di) = (rac-rbd)+(rad+rbc)i$$

4. Modular:

$$1 \cdot (a+bi) = a+bi$$

Con $r, s, a, b, c, d \ \in \mathbb{R}$

Y así queda demostrado que el cuerpo de los números complejos, con las operaciones de suma y producto, tiene estructura de espacio vectorial sobre el cuerpo de los números reales.

3.2 Subespacio vectorial

3.3 Dependencia e independencia lineal

3.3.1 Sistema generador

3.3.2 Base

3.3.3 Base de un subespacio

3.3.4 Cooredenadas y cambio de base

3.4 Operaciones con subespacios

3.5 Aplicación lineal

3.5.1 Matriz de una aplicación lineal

3.5.2 Matriz de una composición

3.5.3 Cambio de base en aplicaciones lineales

3.5.4 Núcleo e imagen de una aplicación lineal

3.6 Matrices y determinantes

3.7 Sistemas y ecuaciones lineales

3.7.1 Teorema de Rouché-Fröbenius

3.7.2 Regla de Cramer

3.7.3 Método de Gauss

3.7.4 Factorización LU

Chapter 4

Formas bilineales y cuadráticas

4.1 Formas bilineales

4.2 Perpendicularidad u ortogonalidad

4.3 Matriz de una forma bilineal

4.4 Bases ortogonales

4.5 Formas bilineales simétricas

4.6 Formas cuadráticas

4.7 Matriz de una forma cuadrática

4.8 Isometrías

4.9 Transformaciones ortogonales

Chapter 5

Espacio afín y euclídeo. Movimientos

5.1 Espacios afines

5.2 Transformaciones afines y afinidades

5.3 Matrices

5.4 Transformaciones ortogonales y movimientos

5.5 Orientación

5.6 Movimientos en el plano afín euclídeo

5.7 Movimientos en el espacio afín euclídeo

Chapter 6

Cónicas y cuádricas

6.1 Estudio afín de las cónicas

6.2 Estuido afín de las cuádricas

Chapter 7

Álgebra lineal numérica

7.1 Normas matriciales

7.2 Métodos de Jacobi y Gauss-Seidel

7.3 Factorización de matrices LU y QR

7.4 Estimación de errores

7.5 Implementación de algoritmos

7.6 Cálculo de autovalores y autovectores

Chapter 8

Geometría diferencial

8.1 Curvas y superficies en el espacio

8.2 Triedro de Frenet

8.3 Curvatura de Gauss y media

Bibliography