Mathematics Bootcamp Lecture Notes

Department of Statistical Sciences, University of Toronto

Emma Kroell

Last updated: July 25, 2022

Preface

These lecture notes were prepared for the Mathematics course at the inaugural Department of Statistical Sciences Graduate Student Bootcamp at the University of Toronto. The course teaches an overview of necessary mathematics prerequisites to incoming statistics graduate students, with an emphasis on proofs.

These lectures are based on the following books or lecture notes:

1. *An Introduction to Mathematical Structures and Proofs* by Larry J. Gerstein
2. *The Tools of Mathematical Reasoning* by Tamara J. Lakins
3. *A Taste of Topology* by Volker Runde
4. *Real Mathematical Analysis* by Charles C. Pugh
5. *Linear Algebra Done Right* by Sheldon Axler
6. *Linear Algebra Done Wrong* by Sergei Treil
7. *Lecture notes in Mathematics for Economics and Statistics* by Piotr Zwiernik
8. *Real Analysis Lecture Notes* by Laurent Marcoux

Chapter 1 of Gerstein (2012) and the first three chapters of Lakins (2016) are used as references for the proof technique section. Runde (2005) is the main text for the sections on set theory, metric spaces, and topology, which follow chapters 1, 2, and 3 of his book, respectively. Some additional topics come from Pugh (2015). The linear algebra content comes mostly from Axler (2015), with Treil (2017) used in some sections for an alternate perspective.

Most of the material in these notes belongs to these texts. All of these texts are available online to University of Toronto users (some to everyone).

I would like to acknowledge the assistance of Jesse Gronsbell, Stanislav Volgushev, Piotr Zwiernik, and Robert Zimmerman in developing the list of topics for the course.

Please notify me of any typos or corrections at emma.kroell@mail.utoronto.ca .

Contents

A short note on notation:

$\mathbb{N}$ denotes the whole numbers, i.e. $\mathbb{N} = \{1, 2, \ldots\}$

$\mathbb{N}_0$ denotes the non-negative integers, i.e. $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$

$\mathbb{Z}$ denotes the integers, i.e. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ denotes the rational numbers, i.e. $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}$

$\mathbb{R}$ denotes the real numbers

$\mathbb{C}$ denotes the complex numbers

1 Review of proof techniques

1.1 Propositional logic

Propositions are statements that could be true or false. They have a corresponding *truth value*. We will use capital letters to denote propositions. For example, "n is odd" and "n is divisible by 2" are propositions. Let's call them P and Q. Whether they are true or not (i.e. their truth value) depends on what n is.

We can negate statements: $\neg P$ is the statement "n is not odd".

We can combine statements:

- $P \wedge Q$ is the statement "n is odd and n is divisible by 2".
- $P \vee Q$ is the statement "n is odd or n is divisible by 2".

We always assume the inclusive or unless specifically stated otherwise.

Example 1.1 *Here are some statements, which we want to write in propositional logic.*

- *If it's not raining, I won't bring my umbrella.*
- *I'm a banana or Toronto is in Canada.*
- *If I pass this exam, I'll be both happy and surprised.*

For the first one, let A be the statement "it's raining" and B be the statement "I will bring my umbrella". In logic, the statement is $\neg A \implies \neg B$.

For the second, let C be the statement "I'm a banana" and let D be the statement "Toronto is in Canada". We write this as $C \vee D$.

For the third, let P be the statement "I pass this exam", let Q be the statement "I am happy", and let R be the statement "I am surprised". This one is written $P \implies (Q \wedge R)$.

1.1.1 Truth values

Example 1.2 *Write the following using propositional logic:*
If it is snowing, then it is cold out.
It is snowing.
Therefore, it is cold out.

Solution.
$P \implies Q$
P
Conclusion: Q

To examine if a statement is true or not, we use a truth table, where we write out all the possibilities.

Example 1.3 *The truth table for $P \implies Q$ where P, Q are propositions is:*

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

1.1.2 Logical equivalence

We say that two statements are *logically equivalent* if they have the same truth tables.

Example 1.4 *Let P, Q be propositions. $P \implies Q$ is logically equivalent to $\neg P \vee Q$.*

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg P$	$\neg P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Theorem 1.5 (De Morgan's Laws) *Let P, Q be propositions.*

(i) $\neg(P \wedge Q)$ *is logically equivalent to* $\neg P \vee \neg Q$.

(ii) $\neg(P \vee Q)$ *is logically equivalent to* $\neg P \wedge \neg Q$.

Proving this is your first exercise.

The following fact is often useful.

Example 1.6 $\neg(P \implies Q)$ *is logically equivalent to* $P \wedge \neg Q$. *This follows from Example 1.4 and Theorem 1.5.*

1.1.3 Quantifiers

There are two important logical operators that we have not yet discussed. They are denoted using the following symbols: $\forall$, read as "for all" or "for each", and $\exists$, read as "there exists". We will explore their meanings, how they can help us simplify statements we need to prove, and how we prove such statements.

For all

"for all", $\forall$, is also called the universal quantifier. If $P(x)$ is some property that applies to x from some domain, then $\forall x P(x)$ means that the property P holds for every x in the domain. An example is the statement "Every real number has a non-negative square." We write this as $\forall x \in \mathbb{R}$, $x^2 \geq 0$. In logic, people often use brackets to separate parts of the logical expression, ex. $(\forall x \in \mathbb{R})(x^2 \geq 0)$.

How do we prove a for all statement? We need to take an arbitrary element of the domain, and show the property holds for that element.

There exists

"there exists", $\exists$, is also called the existential quantifier. If $P(x)$ is some property that applies to x from some domain, then $\exists x P(x)$ means that the property P holds for some x in the domain. An example is the statement that 4 has a square root in the reals. We write this as $\exists x \in \mathbb{R}$ such that $x^2 = 4$ or in proper logic notation, $(\exists x \in \mathbb{R})\ (x^2 = 4)$.

How do we prove a there exists statement? We need to find an element in the domain for which the property holds (find an example).

There is also a special way of writing when there exists a unique element. We use $\exists!$ for this case. For example, the statement "there exists a unique positive integer such that the integer squared is 64" is written $\exists! z \in \mathbb{N}$ such that $z^2 = 64$.

Combining quantifiers

Often we will need to prove statements where we combine quantifiers. Here are some examples:

Statement	Logical expression
Every non-zero rational number has a multiplicative inverse	$\forall q \in \mathbb{Q} \setminus \{0\}$, $\exists s \in \mathbb{Q}$ such that $qs = 1$
Each integer has a unique additive inverse	$\forall x \in \mathbb{Z}\,, \exists! y \in \mathbb{Z}$ such that $x + y = 0$
$f : \mathbb{R} \to \mathbb{R}$ is continuous at $x_0 \in \mathbb{R}$	$\forall \epsilon > 0\ \exists \delta > 0$ such that whenever $\lvert x - x_0\rvert < \delta$, $\lvert f(x) - f(x_0)\rvert < \epsilon$

The order of quantifiers is important! Changing the order changes the meaning. Consider the following example. Which are true? Which are false?

$$\forall x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2$$
$$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2$$
$$\exists x \in \mathbb{R}\, \forall y \in \mathbb{R}\ x + y = 2$$
$$\exists x \in \mathbb{R}\, \exists y \in \mathbb{R}\ x + y = 2$$

It's also important to know how to negate logical statements that include quantifiers, as it will often help us prove or disprove the statements. The results are intuitive, but things can get complicated when we have more complex statements. The negation of a statement being true for all x is that is isn't true for at least one x. The negation of a statement being true for at least one x is that is isn't true for any x.

In summary,

$$\neg \forall x P(x) = \exists x (\neg P(x))$$
$$\neg \exists x P(x) = \forall x (\neg P(x))$$

The negations of the statements above are:

Logical expression	Negation
$\forall q \in \mathbb{Q} \setminus \{0\}$, $\exists s \in \mathbb{Q}$ such that $qs = 1$	$\exists q \in \mathbb{Q} \setminus \{0\}$ such that $\forall s \in \mathbb{Q}$, $qs \neq 1$
$\forall x \in \mathbb{Z}\,, \exists! y \in \mathbb{Z}$ such that $x + y = 0$	$\exists x \in \mathbb{Z}$ such that $(\forall y \in \mathbb{Z}, x+y \neq 0) \vee (\exists y_1, y_2 \in \mathbb{Z}$ such that $y_1 \neq y_2 \wedge x + y_1 = 0 \wedge x + y_2 = 0\ )$
$\forall \epsilon > 0\ \exists \delta > 0$ such that whenever $\lvert x - x_0\rvert < \delta$, $\lvert f(x) - f(x_0)\rvert < \epsilon$	$\exists \epsilon > 0$ such that $\forall \delta > 0$, $\lvert x - x_0\rvert < \delta$ and $\lvert f(x) - f(x_0)\rvert \geq \epsilon$

Note that we use De Morgan's laws (Theorem 1.5), as well as the negation of an implication (Example 1.6). What do these negations mean in English?

1.2 Types of proof

1.2.1 Direct proof

In a direct proof, our approach is to use the definition and known results.

Example 1.7 *The product of an even number with another integer is even.*

To prove this statement, we will use the definition of even. First we state that definition.

Definition 1.8 *We say that an integer n is* even *if there exists another integer j such that $n = 2j$. We say that an integer n is* odd *if there exists another integer j such that $n = 2j + 1$.*

Now we prove the example directly.

Proof. Let $n, m \in \mathbb{Z}$, with n even. By definition, there $\exists\ j \in \mathbb{Z}$ such that $n = 2j$. Then

$$nm = (2j)m = 2(jm)$$

Therefore nm is even by definition. □

Here is another example, which uses the concept of divisibility.

Definition 1.9 *Let $a, b \in \mathbb{Z}$. We say that "a divides b", written $a|b$, if the remainder is zero when b is divided by a, i.e. $\exists j \in \mathbb{Z}$ such that $b = aj$.*

Example 1.10 *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Prove that if $a|b$ and $b|c$, then $a|c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Suppose $a|b$ and $b|c$. Then by definition, there exists $j, k \in \mathbb{Z}$ such that $b = aj$ and $c = kb$. Combining these two equations gives $c = k(aj) = a(kj)$. Thus $a|c$ by definition. □

1.2.2 Proof by contrapositive

Sometimes instead of proving an implication $P \implies Q$ directly, it is easier to prove $\neg Q \implies \neg P$. This is called the contrapositive. First, we show that these two statements are logically equivalent using truth tables.

$P \implies Q$

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

$\neg Q \implies \neg P$

P	Q	$\neg P$	$\neg Q$	$\neg Q \implies \neg P$
T	T	F	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Note that $\neg P \implies \neg Q$ is *not* logically equivalent to $P \implies Q$ (can you think of an example?). This is a common mistake.

Here is an example of a statement that is easier to prove using the contrapositive as opposed to directly.

Example 1.11 *If an integer squared is even, then the integer is itself even.*

Proof. We prove the contrapositive. Let n be odd. Then there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. We compute

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus n^2 is odd. □

1.2.3 Proof by contradiction

Another proof technique is to assume something we know to be (or think to be) false, and then try to derive a contradiction. A contradiction is something that is impossible, like 0=1 or showing that a number is both odd and even.

In sum, to prove that a statement P is true by contradiction, we assume $\neg P$ is true, derive a contradiction, and conclude that P is true. Here is an example.

Example 1.12 *The sum of a rational number and an irrational number is irrational.*

Proof. Let $q \in \mathbb{Q}$ and $r \in \mathbb{R} \setminus \mathbb{Q}$. Suppose in order to derive a contradiction that their sum is rational, i.e. $r + q = s$ where $s \in \mathbb{Q}$. But then $r = s - q \in \mathbb{Q}$. Contradiction. Therefore the sum of a rational number and an irrational number is irrational. □

1.2.4 Summary

In sum, to prove $P \implies Q$:

Direct proof:	assume P, prove Q
Proof by contrapositive:	assume $\neg Q$, prove $\neg P$
Proof by contradiction:	assume $P \wedge \neg Q$ and derive something that is impossible

1.2.5 Induction

Finally, we consider a special proof technique for proving statements about the natural numbers (or subsets of them of certain forms). It is based on the following theorem, which we state without proof.

Theorem 1.13 (Well-ordering principle for $\mathbb{N}$) *Every nonempty set of natural numbers has a least element.*

Because of the well-ordering principle, we can prove something holds for the natural numbers by proving it holds for the smallest one, and then creating a logical ladder linking them together as follows:

Theorem 1.14 (Principle of mathematical induction) *Let n_0 be a non-negative integer. Suppose P is a statement about positive integers n such that*

1. *(base case) $P(n_0)$ is true*
2. *(induction step) For every integer $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.*

Then $P(n)$ is true for every integer $n \geq n_0$

Here is an example of a proof by induction.

Example 1.15 *$n! > 2^n$ if $n \geq 4$.*

Proof. We prove this by induction on n.
Base case: Let $n = 4$. Then $n! = 4! = 24 > 16 = 2^4$.
Inductive hypothesis: Suppose for some $k \geq 4$, $k! > 2^k$.
Then

$$(k+1)! = (k+1)k! > (k+1)2^k > 2(2^k) = 2^{k+1}.$$

Thus the statement holds by induction on n. □

Sometimes we use a different version of induction, called strong induction.

Theorem 1.16 (Principle of strong mathematical induction) *Let n_0 be a non-negative integer. Suppose P is a statement about positive integers n such that*

1. *(base case) $P(n_0)$ is true*
2. *(induction step) For every integer $k \geq n_0$, if $P(m)$ is true for every integer m with $n_0 \leq m \leq k$, then $P(m+1)$ is true.*

Then $P(n)$ is true for every integer $n \geq n_0$.

Next, we will consider an example where it is much simpler to use the strong version of induction than the regular one. First, we recall the definition of a prime number.

Definition 1.17 *A positive integer p is prime if p has exactly two positive integer factors: 1 and p. Note that 1 is not prime. We can write this as*

$$p > 1 \text{ is prime if } \forall\, a, b \in \mathbb{N},\ p = ab \implies (a = 1 \text{ or } b = 1).$$

We want to prove the existence part of the Fundamental Theorem of Arithmetic, that every integer greater than or equal to 2 has a prime factorization. The fact that such a factorization is unique is left as an exercise.

Example 1.18 *Every integer $n \geq 2$ can be written as the product of primes.*

Proof. We prove this using the Principle of Strong Mathematical Induction on n.

Base case: $n = 2$ is prime.

Inductive hypothesis: Suppose for some $k \geq 2$ that one can write every integer n such that $2 \leq n \leq k$ as a product of primes.

We must show that we can write $k + 1$ as a product of primes.

Case 1: if $k + 1$ is prime, then we are done.

Case 2: if $k + 1$ is not prime, then by Definition 1.17, there exists $a, b \in \mathbb{N}$ such that $k + 1 = ab$ where $a, b \neq 1$. Then it must also be the case that $a, b \leq k$.

By the inductive hypothesis, we can write a and b as products of primes, i.e. $\exists p_1, \ldots p_\ell, q_1, \ldots q_m$, all prime, such that

$$a = p_1 \cdots p_\ell, \qquad b = q_1 \cdots q_m.$$

Then

$$k + 1 = ab = p_1 \cdots p_\ell \, q_1 \cdots q_m,$$

therefore we can write $k + 1$ as a product of primes.

Thus the claim holds by strong induction. □

The Principle of Strong Mathematical Induction and the Principle of Mathematical Induction are logically equivalent, but sometimes it is easier to use one or the other, as we saw.

1.3 Exercises

1. Prove De Morgan's Laws for propositions: $\neg(P \wedge Q) = \neg P \vee \neg Q$ and $\neg(P \vee Q) = \neg P \wedge \neg Q$ (Hint: use truth tables).
2. Write the following statements and their negations using logical quantifier notation and then prove or disprove them:
   (i) Every odd integer is divisible by three.
   (ii) For any real number, twice its square plus twice itself plus six is greater than or equal to five. *(You may assume knowledge of calculus.)*
   (iii) Every integer can be written as a unique difference of two natural numbers.
3. Prove the following statements:
   (i) If $a|b$ and $a, b \in \mathbb{N}$ (positive integers), then $a \leq b$.
   (ii) If $a|b$ and $a|c$, then $a|(xb + yc)$, where $a, b, c, x, y \in \mathbb{Z}$.
   (iii) Let $a, b, n \in \mathbb{Z}$. If n does not divide the product ab, then n does not divide a and n does not divide b.
4. Prove that for all integers $n \geq 1$, $3|(2^{2n} - 1)$.
5. Prove the Fundamental Theorem of Arithmetic, that every integer $n \geq 2$ has a unique prime factorization (i.e. prove that the prime factorization from the last proof is unique).

1.4 References

Most of this content may be found in Chapter 1 of [Ger12], though many of the examples are my own. [Lak16] is also a great resource. In particular, the content on induction comes from there. Unfortunately the latter text is not freely available online or at U of T.

2 Set theory

2.1 Basics

For our purposes, we define a *set* to be a collection of mathematical objects. If S is a set and x is one of the objects in the set, we say x is an element of S and denote it by $x \in S$. The set of no elements is called empty set and is denoted by $\emptyset$.

Definition 2.1 (Subsets, Union, Intersection) *Let S, T be sets.*

- *We say that S is a* subset *of T, denoted $S \subseteq T$, if $s \in S$ implies $s \in T$.*
- *We say that $S = T$ if $S \subseteq T$ and $T \subseteq S$.*
- *We define the* union *of S and T, denoted $S \cup T$, as all the elements that are in* either *S or T.*
- *We define the* intersection *of S and T, denoted $S \cap T$, as all the elements that are in* both *S and T.*
- *We say that S and T are* disjoint *if $S \cap T = \emptyset$.*

Example 2.2 $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Example 2.3 *Let $a, b \in \mathbb{R}$ such that $a < b$.*
Open interval: $(a, b) := \{x \in \mathbb{R} : a < x < b\}$ (a, b may be $-\infty$ or $+\infty$)
Closed interval: $[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}$
We can also define half-open intervals.

Example 2.4 *Let $A = \{x \in \mathbb{N} : 3|x\}$ and $B = \{x \in \mathbb{N} : 6|x\}$ Show that $B \subseteq A$.*

Proof. Let $x \in B$. Then $6|x$, i.e. $\exists j \in \mathbb{Z}$ such that $x = 6j$. Therefore $x = 3(2j)$, so $3|x$. Thus $x \in A$. □

Definition 2.5 *Let $A, B \subseteq X$. We define the* set-theoretic difference *of A and B, denoted $A \setminus B$ (sometimes $A - B$) as the elements of X that are in A but* not *in B.*

The complement of a set $A \subseteq X$ is the set $A^c := X \setminus A$.

We extend the definition of union and intersection to an arbitrary family of sets as follows:

Definition 2.6 *Let S_α, $\alpha \in A$, be a family of sets. A is called the* index set*. We define*

$$\bigcup_{\alpha \in A} S_\alpha := \{x : \exists \alpha \text{ such that } x \in S_\alpha\},$$

$$\bigcap_{\alpha \in A} S_\alpha := \{x : x \in S_\alpha \text{ for all } \alpha \in A\}.$$

Example 2.7

$$\bigcup_{n=1}^{\infty} [-n, n] = \mathbb{R}$$

$$\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) = \{0\}$$

Theorem 2.8 (De Morgan's Laws) *Let $\{S_\alpha\}_{\alpha \in A}$ be an arbitrary collection of sets. Then*

$$\left(\bigcup_{\alpha \in A} S_\alpha\right)^c = \bigcap_{\alpha \in A} S_\alpha^c \quad \text{and} \quad \left(\bigcap_{\alpha \in A} S_\alpha\right)^c = \bigcup_{\alpha \in A} S_\alpha^c$$

Proof. For the first part: Let $x \in \left(\bigcup_{\alpha \in A} S_\alpha\right)^c$. This is true if and only if $x \notin \left(\bigcup_{\alpha \in A} S_\alpha\right)$, or in other words $x \in S_\alpha^c$ for all $\alpha \in A$. This is true if and only if $x \in \bigcap_{\alpha \in A} S_\alpha^c$, which gives the result.
The second part is similar and is left as an exercise. □

Since a set is itself a mathematical object, a set can itself contain sets.

Definition 2.9 *The power set $\mathcal{P}(S)$ of a set S is the set of all subsets of S.*

Example 2.10 *Let $S = \{a, b, c\}$. Then $\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, S\}$.*

Another way of building a new set from two old ones is the Cartesian product of two sets.

Definition 2.11 *Let S, T be sets. The* Cartesian product *$S \times T$ is defined as the set of tuples with elements from S, T, i.e*

$$S \times T = \{(s, t) : \ s \in S \ \text{ and } \ t \in T\}.$$

This can also be extended inductively to a finite family of sets.

2.2 Ordered sets

Definition 2.12 *A* relation *R on a set X is a subset of $X \times X$. We say that $x \leq y$ if $(x, y) \in \mathbb{R}$. A relation $\leq$ is called a* partial order *on X if it satisfies*

1. *Reflexivity: $x \leq x$ for all $x \in X$*
2. *Transitivity: for $x, y, z \in X$, $x \leq y$ and $y \leq z$ implies $x \leq z$*
3. *Anti-symmetry: for $x, y \in X$, $x \leq y$ and $y \leq x$ implies $x = y$*

The pair $(X, \leq)$ is called a partially ordered set.

A chain *or* totally ordered set *$C \subseteq X$ is a subset with the property $x \leq y$ or $y \leq x$ for any $x, y \in C$.*

Example 2.13 *The real numbers with the usual ordering, $(\mathbb{R}, \leq)$, are totally ordered.*

Example 2.14 *The power set of a set X with the ordering given by subsets, $(\mathcal{P}(X), \subseteq)$ is partially ordered set.*

Example 2.15 *Let $X = \{a, b, c, d\}$. What is $\mathcal{P}(X)$? Find a chain in $\mathcal{P}(X)$.*

$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{b, c\}, \{c, d\}, \{b, d\}, \{a, c\}, \{a, d\}, \{a, b, c\}, \{b, c, d\}, \{a, b, d\}, \{a, c, d\}, X\}$

An example of a chain $C \subseteq \mathcal{P}(X)$ is $C = \{\emptyset, \{b\}, \{b, c\}, \{a, b, c\}, X\}$

Example 2.16 *Consider the set $C([0, 1], \mathbb{R}) := \{f : [0, 1] \to \mathbb{R} : f \text{ is continuous}\}$.*

For two functions $f, g \in C([0, 1], \mathbb{R})$, we define the ordering as $f \leq g$ if $f(x) \leq g(x)$ for $x \in [0, 1]$. Then $(C([0, 1], \mathbb{R}), \leq)$ is a partially ordered set. Can you think of a chain that is a subset of $(C([0, 1], \mathbb{R})$?

Definition 2.17 *A non-empty partially ordered set $(X, \leq)$ is* well-ordered *if every non-empty subset $A \subseteq X$ has a mimimum element.*

Recall that we already saw that $\mathbb{N}$ is well-ordered, as we used it to prove the principle of mathematical induction. $\mathbb{R}$ with the usual order does not have this property.

Having a partially ordered set allows us to talk about upper and lower bounds.

Definition 2.18 *Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$. Then $x \in X$ is an* upper bound *for S if for all $s \in S$ we have $x \leq s$. Similarly $y \in X$ is a* lower bound *for S if for all $s \in S$, $y \leq s$. If there exists an upper bound for S, we call S* bounded above *and if there exists a lower bound for S, we call S* bounded below*. If S is bounded above and bounded below, we say S is* bounded*.*

We can also ask if there exists a least upper bound or a greatest lower bound.

Definition 2.19 *Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$. We call $x \in X$* least upper bound *or* supremum*, denoted $x = \sup S$, if x is an upper bound and for any other upper bound $y \in X$ of S we have $x \leq y$. Likewise $x \in X$ is the* greatest lower bound *or* infimum *for S, denoted $x = \inf S$, if it is a lower bound and for any other lower bound $y \in X$, $y \leq x$.*

Note that the supremum and infimum of a bounded set do not necessarily need to exist. However, if they do exists they are unique, which justifies the article *the* (see Exercise 4). Nevertheless, the reals have a remarkable property, which we will take as an axiom.

Axiom 2.20 *[Completeness Axiom] Let $S \subseteq \mathbb{R}$ be bounded above. Then there exists $r \in \mathbb{R}$ such that $r = \sup S$, i.e. S has a least upper bound.*

By setting $S' = -S := \{-s : s \in S\}$ and noting $\inf S = -\sup S'$, we obtain a similar statement for infima if S is bounded below. As mentioned above, this property is fairly special, for example it fails for the rationals.

Example 2.21 *Let $S = \{q \in \mathbb{Q} : x^2 < 7\}$. Then S is bounded above in $\mathbb{Q}$, but there exists no least upper bound in $\mathbb{Q}$.*

There is a nice alternative characterization for suprema in the real numbers.

Proposition 2.22 *Let $S \subseteq \mathbb{R}$ be bounded above. Then $r = \sup S$ if and only if r is an upper bound and for all $\epsilon > 0$ there exists an $s \in S$ such that $r - \epsilon < s$.*

Proof. ($\Rightarrow$) We will prove the forward direction ($\implies$) by contrapositive. Suppose r is either not an upper bound or there exists an $\epsilon > 0$ such that for all $s \in S$, $r - \epsilon \geq s$. In the first case, r is not the supremum by definition. In the second case, $r - \varepsilon$ is an upper bound which is smaller than r. Thus $r \neq \sup S$.

($\Leftarrow$) For the backward direction we will proceed by contradiction. Suppose r is an upper bound and for all $\epsilon > 0$ there exists an $s \in S$ such that $r - \epsilon < s$, but $r \neq \sup S$. Then $\sup S < r$ or equivalently $r - \sup S > 0$. Then by assumption there exists an $s \in S$ such that $\sup S = r - (r - \sup S) < s$, which contradicts the definition of supremum. □

Using the same trick, we may obtain a similar result for infima.

Proposition 2.23 *Let $S \subseteq \mathbb{R}$ be bounded below. Then $r = \inf S$ if and only if r is a lower bound and for all $\epsilon > 0$ there exists an $s \in S$ such that $r + \epsilon > s$.*

Example 2.24 *Consider $S = \{1/n : n \in \mathbb{N}\}$. Then $\sup S = 1$ and $\inf S = 0$.*

2.3 Functions

One way to define a function is as follows :

Definition 2.25 ([Run05, Definition 1.1.14]) *A function f from a set X to a set Y is a subset of $X \times Y$ with the properties:*

1. *For every $x \in X$, there exists a $y \in Y$ such that $(x, y) \in f$*
2. *If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.*

X is called the domain *of f.*

How does this connect to other descriptions of functions you may have seen? Instead of writing $f \subseteq X \times Y$, we often write $f : X \to Y$, $x \mapsto y$, where $(x, y) \in f$.

Example 2.26 *For a set X, the identity function is:*

$$1_X : X \to X, \quad x \mapsto x$$

Definition 2.27 (Image and pre-image) *Let $f : X \to Y$ and $A \subseteq X$ and $B \subseteq Y$. The image of f is the set $f(A) := \{f(x) : x \in A\}$ and the pre-image of f is the set $f^{-1}(B) := \{x : f(x) \in B\}$*

The following re-statements of the above may be helpful way to think about it for proofs:
If $y \in f(A)$, then $y \in Y$, and there exists an $x \in A$ such that $y = f(x)$.
If $x \in f^{-1}(B)$, then $x \in X$ and $f(x) \in B$.

Definition 2.28 (Surjective, injective and bijective) *Let $f : X \to Y$, where X and Y are sets. Then*

- *f is* injective *if $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$*
- *f is* surjective *if for every $y \in Y$, there exists an $x \in X$ such that $y = f(x)$*
- *f is* bijective *if it is both injective and bijective*

Example 2.29 *Let $f : X \to Y$, $x \mapsto x^2$.*
If $X = \mathbb{R}$ and $Y = [0, \infty)$: f is surjective.
If $X = [0, \infty)$ and $Y = \mathbb{R}$: f is injective.
If $X = Y = [0, \infty)$: f is bijective.
If $X = Y = \mathbb{R}$, then f is neither surjective nor injective.

Proposition 2.30 *Let $f : X \to Y$ and $A \subseteq X$. Prove that $A \subseteq f^{-1}(f(A))$, with equality if f is injective.*

Proof. First we show $A \subseteq f^{-1}(f(A))$. Let $x \in A$. Let $B = f(A)$, $B \subseteq Y$. By definition, $f(x) \in B$. So then again by definition, $x \in f^{-1}(B)$. Thus $x \in f^{-1}(f(A))$.

Next, suppose f is injective. We have already shown that $A \subseteq f^{-1}(f(A))$, so it remains to show that $f^{-1}(f(A)) \subseteq A$. Let $x \in f^{-1}(f(A))$. Then $f(x) \in f(A)$ by the definition of the pre-image. This means that there exists a $\tilde{x} \in A$ such that $f(x) = f(\tilde{x})$. Since f is injective, we have $x = \tilde{x}$, and hence $x \in A$. □

2.4 Cardinality

Intuitively, the *cardinality* of a set A, denoted $|A|$, is the number of elements in the set. For sets with only a finite number of elements, this intuition is correct. We call a set with finitely many elements finite.

We say that the empty set has cardinality 0 and is finite.

Proposition 2.31 *If X is finite set of cardinality n, then the cardinality of $\mathcal{P}(X)$ is 2^n.*

Proof. We proceed by induction. First, suppose $n = 0$. Then $X = \emptyset$, and $\mathcal{P}(X) = \{\emptyset\}$ which has cardinality $1 = 2^0$.

Next, suppose that the claim holds for some $n \in \mathbb{N}_0$. Let X have $n + 1$ elements. Let's call them $\{x_1, \ldots, x_n, x_{n+1}\}$. Then we can split X up into subsets $A = \{x_1, \ldots, x_n\}$ and $B = \{x_{n_1}\}$. By the inductive hypothesis, $\mathcal{P}(A)$ has cardinality 2^n. Any subset of X must either be a subset of A or contain x_{n+1}. How many subsets are there for the latter form? Let's count them out. Each subset will be formed by taking elements from A and combining them with x_{n+1}. We start with no elements from A and count up to all of them:

$$\begin{aligned} &1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} \\ =&\sum_{k=0}^{n} \binom{n}{k} \\ =&2^n \end{aligned}$$

Therefore the total number of elements in $\mathcal{P}(X)$ is the number of subsets of A (2^n) plus the number of mixed subsets (2^n), i.e. the cardinality of $\mathcal{P}(X)$ is $2^n + 2^n = 2^{n+1}$.

Thus the claim holds by induction. □

Note: you do not need to prove this by induction. There are other ways to do it. You can try to prove it without using induction as an exercise.

Definition 2.32 *Two sets A and B have same cardinality, $|A| = |B|$, if there exists bijection $f : A \to B$.*

Example 2.33 *Which is bigger, $\mathbb{N}$ or $\mathbb{N}_0$?*
Intuitively, it seems that $\mathbb{N}_0$ should be bigger, since it includes exactly one more element than $\mathbb{N}$, namely 0. However, clearly the function $f : \mathbb{N}_0 \to \mathbb{N}$ defined by $n \mapsto n + 1$ is a bijection. Therefore $\mathbb{N}_0$ and $\mathbb{N}$ have the same cardinality! One way to think about this is that $\mathbb{N}_0$ and $\mathbb{N}$ are the "same size" of infinity.

It may sometimes be difficult to find such a bijection. However you can also use the following definition and theorem to instead show that two sets have the same cardinality by finding two injective functions between them.

Definition 2.34 *We say that the cardinality of a set A is less than the cardinality of a set B, denoted $|A| \leq |B|$ if there exists an injection $f : A \to B$.*

Theorem 2.35 (Cantor-Schröder-Bernstein) *Let A, B, be sets. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Proof is omitted. See [Run05, Theorem 1.2.7]

Example 2.36 $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$

Proof. First, we show $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$. The function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined by $n \mapsto (n, 1)$ is an injection, thus $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$.

Next, we show $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$. We define the function $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $(n, m) \mapsto 2^n 3^m$. Why is this an injection? Assume we have n_1, n_2, m_1, m_2 such that $2^{n_1} 3^{m_1} = 2^{n_2} 3^{m_2}$. We need to show $n_1 = n_2$ and $m_1 = m_2$. By the Fundamental Theorem of Arithmetic, every natural number greater than 1 has a unique prime factorization, so therefore the result must hold. □

Definition 2.37 *Let A be a set.*

1. *A is* finite *if there exists an $n \in \mathbb{N}$ and a bijection $f : \{1, \ldots, n\} \to A$*
2. *A is* countably infinite *if there exists a bijection $f : \mathbb{N} \to A$*
3. *A is* countable *if it is finite or countably infinite*
4. *A is* uncountable *otherwise*

Example 2.38 *The rational numbers are countable, and in fact $|\mathbb{Q}| = |\mathbb{N}|$.*
Let's look at $\mathbb{Q}^+ := \{x \in \mathbb{Q} : x > 0\}$. The fact that the rationals are countable relies on this famous way of listing the rational numbers:

$$\begin{array}{cccccc} 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\ 2 & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \cdots \\ 3 & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \cdots \\ 4 & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

This is a map from $\mathbb{N}$ to $\mathbb{Q}^+$. As long as we skip any fraction that is already in our list as we go along, it is injective. Since we can find an injection from $\mathbb{Q}^+$ to $\mathbb{N} \times \mathbb{N}$ (take $q/p \mapsto (q, p)$), and $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$ by Example 2.36, we have that $|\mathbb{Q}^+| = |\mathbb{N}|$.

We can extend this to $\mathbb{Q}$. To do so, let $f : \mathbb{N} \to \mathbb{Q}^+$ be a bijection (which exists by the previous part). Then we can define another bijection $g : \mathbb{N} \to \mathbb{Q}$ by setting $g(1) = 0$ and

$$g(n) = \begin{cases} f(n) & \text{if } n \text{ is even,} \\ -f(n) & \text{if } n \text{ is odd,} \end{cases}$$

for $n > 1$.

Next we show that $\mathbb{N}$ is "smaller" than $(0,1)$.

Theorem 2.39 *The cardinality of $\mathbb{N}$ is smaller than that of $(0,1)$.*

Proof. First, we show that there is an injective map from $\mathbb{N}$ to $(0,1)$. The map $n \to \frac{1}{n}$ fulfils this.

Next, we show that there is no surjective map from $\mathbb{N}$ to $(0,1)$. We use the fact that every number $r \in (0,1)$ has a binary expansion of the form $r = 0.\sigma_1\sigma_2\sigma_3\ldots$ where $\sigma_i \in \{0,1\}$, $i \in \mathbb{N}$.

Now we suppose in order to derive a contradiction that there does exist a surjective map f from $\mathbb{N}$ to $(0,1)$., i.e. for $n \in \mathbb{N}$ we have $f(n) = 0.\sigma_1(n)\sigma_2(n)\sigma_3(n)\ldots$. This means we can list out the binary expansions, for example like

$$\begin{aligned} f(1) &= 0.00000000\ldots \\ f(2) &= 0.11111111111\ldots \\ f(3) &= 0.0101010101\ldots \\ f(4) &= 0.1010101010\ldots \end{aligned}$$

We will construct a number $\tilde{r} \in (0,1)$ that is not in the image of f. Define $\tilde{r} = 0.\tilde{\sigma}_1\tilde{\sigma}_2\ldots$, where we define the nth entry of $\tilde{r}$ to be the the opposite of the nth entry of the nth item in our list:

$$\tilde{\sigma}_n = \begin{cases} 1 & \text{if } \sigma_n(n) = 0, \\ 0 & \text{if } \sigma_n(n) = 1. \end{cases}$$

Then $\tilde{r}$ differs from $f(n)$ at least in the nth digit of its binary expansion for all $n \in \mathbb{N}$. Hence, $\tilde{r} \notin f(\mathbb{N})$, which is a contradiction to f being surjective. This technique is often referred to as Cantor's diagonal argument. □

Proposition 2.40 *(0,1) and $\mathbb{R}$ have the same cardinality.*

Proof. The map $f : \mathbb{R} \to (0,1)$ defined by $x \mapsto \frac{1}{\pi}\left(\arctan(x) + \frac{\pi}{2}\right)$ is a bijection. □

We have shown that there are different sizes of infinity, as the cardinality of $\mathbb{N}$ is infinite but still smaller than that of $\mathbb{R}$ or $(0,1)$. In fact, we have

$$|\mathbb{N}| = |\mathbb{N}_0| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|.$$

Because of this, there are special symbols for these two cardinalities: The cardinality of $\mathbb{N}$ is denoted $\aleph_0$, while the cardinality of $\mathbb{R}$ is denoted $\mathfrak{c}$.

2.5 Exercises

1. Let $A = \{x \in \mathbb{R} : x < 100\}$, $B = \{x \in \mathbb{Z} : |x| \geq 20\}$, and $C = \{y \in \mathbb{N} : y \text{ is prime}\}$ $(A, B, C \subseteq \mathbb{R})$. Find $A \cap B$, $B^c \cap C$, $B \cup C$, and $(A \cup B)^c$.
2. Is $\mathbb{R} \times \mathbb{R}$ with the ordering $(x_1, y_1) \preceq (x_2, y_2)$ if $x_1 \leq x_2$ a partially ordered set?
3. [Run05, Exercise 1.3.1] Let S be a non-empty set. A relation R on S is called an equivalence relation if it is
   (i) Reflexive: $(x, x) \in R$ for all $x \in S$
   (ii) Symmetric: if $(x, y) \in R$ then $(y, x) \in R$ for all $x, y \in S$
   (iii) Transitive: if $(x, y), (y, z) \in R$ then $(x, z) \in R$ for all $x, y, z \in S$

Given $x \in S$, the equivalence class of x (with respect to a given equivalence relation R) is defined to consist of those $y \in S$ for which $(x, y) \in R$. Show that two equivalence classes are either disjoint or identical.

4. Let $(X, \leq)$ be a partially ordered set and $S \subseteq X$ be bounded. Show that the infimum and supremum of S are unique (if they exist).
5. Let $S, T \subseteq \mathbb{R}$ and suppose both are bounded above. Define $S + T = \{s + t : \ s \in S, t \in T\}$. Show that $S + T$ is bounded above and $\sup(S + T) = \sup S + \sup T$.
6. Let $f : X \to Y$, $X, y \subseteq \mathbb{R}$ be defined by the map $x \mapsto \sin(x)$. For what choices of X and Y is f injective, surjective, bijective, or neither?
7. Show that for sets $A, B \subseteq X$ and $f : X \to Y$, $f(A \cap B) \subseteq f(A) \cap f(B)$.
8. Let $f : X \to Y$ and $B \subseteq Y$. Prove that $f(f^{-1}(B)) \subseteq B$, with equality iff f is surjective.
9. Prove that :
   (a) $f(\cup_{i \in I} A_i) = \cup_{i \in I} f(A_i)$, where $f : X \to Y$, $A_i \subseteq X \, \forall i \in I$
   (b) $f^{-1}(\cup_{i \in I} B_i) = \cup_{i \in I} f^{-1}(B_i)$, where $f : X \to Y$, $B_i \subseteq Y \, \forall i \in I$
10. Show that $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality.
11. Show that $|(0, 1)| = |(1, \infty)|$.

2.6 References

The content in this section mostly follows [Run05], but is supplemented by [Mar19] (ordered sets) and [Zwi22] (introductory set theory).

3 Metric spaces and sequences

3.1 Metric spaces

Definition 3.1 *A* metric *on a set X is a function $d : X \times X \to \mathbb{R}$ that satisfies:*

(a) Positive definiteness: $d(x, y) \geq 0$ for $x, y \in X$ and $d(x, y) = 0 \Leftrightarrow x = y$

(b) Symmetry: for $x, y \in X$, $d(x, y) = d(y, x)$

(c) Triangle inequality: for $x, y, z \in X, d(x, z) \leq d(x, y) + d(y, z)$

A set together with a metric is called a metric space.

Example 3.2 *$\mathbb{R}^n$ with the Euclidean distance*

$$d(x, y) = \sqrt{\sum_{j=1}^{n} (x_j - y_j)^2} \quad \text{for } x, y \in \mathbb{R}^n$$

is a metric space.

Many metric spaces we know are in fact normed spaces, which have more structure than metric spaces. We will briefly discuss normed spaces. This assumes some knowledge of vector spaces, which we will discuss in a further section. In particular, we denote a field by $\mathbb{F}$. For now, we can think of this as $\mathbb{R}$ or $\mathbb{C}$.

Definition 3.3 *A* norm *on an $\mathbb{F}$-vector space E is a function $\| \cdot \| : E \to \mathbb{R}$ that satisfies:*

(a) Positive definiteness: $\|x\| \geq 0$ for $x \in E$ and $||x|| = 0 \Leftrightarrow x = 0$

(b) Homogeneity: for $x \in E$ and $\alpha \in \mathbb{F}$, $||\alpha x|| = |\alpha| ||x||$

(c) Triangle inequality: for $x, y \in E, ||x + y|| \leq ||x|| + ||y||$

A vector space with a norm is called a normed space. A normed space is a metric space using the metric $d(x, y) = \|x - y\|$.

Example 3.4 *The p-norm is defined for* $p \geq 1$ *for a vector* $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ *as*

$$||x||_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}.$$

The infinity norm is the limit of the p-norm as $p \to \infty$*, defined as*

$$||x||_\infty = \max_{i=1,\ldots,n} |x_i|.$$

If we look at the space of continuous functions $C([0, 1]; \mathbb{R})$*, the p-norm is*

$$||f||_p = \left(\int_0^1 |f(x)|^p dx \right)^{1/p}$$

and the $\infty-$*norm (or sup norm) is*

$$||f||_\infty = \max_{x \in [0,1]} |f(x)|.$$

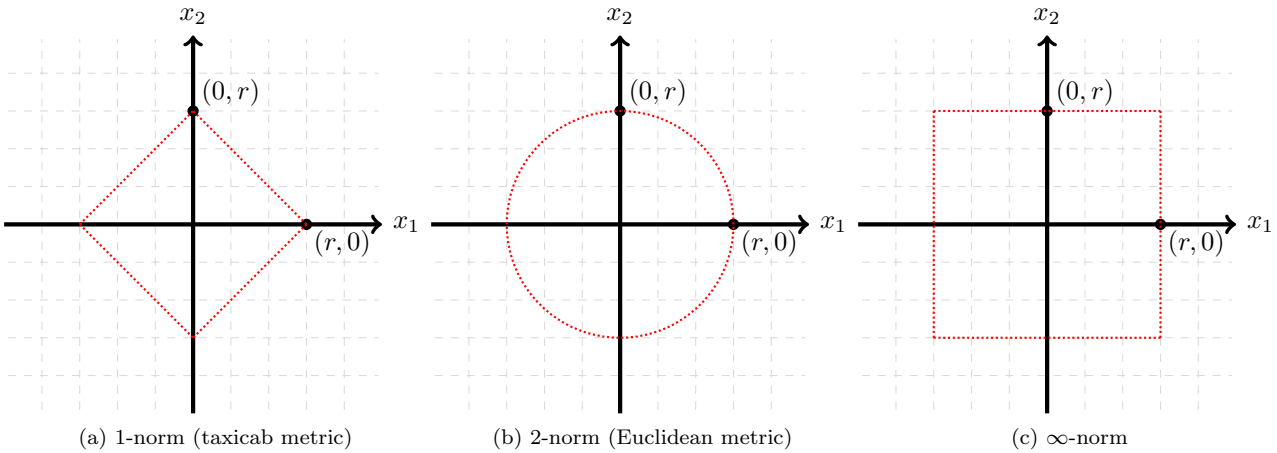
Definition 3.5 *A subset* A *of a metric space* (X, d) *is* bounded *if there exists* $M > 0$ *such that* $d(x, y) < M$ *for all* $x, y \in A$.

Definition 3.6 *Let* (X, d) *be a metric space. We define the* open ball *centred at a point* $x_0 \in X$ *of radius* $r > 0$ *as*

$$B_r(x_0) := \{x \in X : d(x, x_0) < r_0\}.$$

Example 3.7 *In* $\mathbb{R}$ *with the usual norm (absolute value), open balls are symmetric open intervals, i.e.* $B_r(x_0) = (x_0 - r, x_0 + r)$.

Example 3.8 *Consider* $\mathbb{R}^2$ *with the taxicab or Manhattan metric (1-norm)* $d(x, y) = \sum_{i=1}^{2} |x_i - y_i|$*, the usual Euclidean distance (2-norm)* $d(x, y) = \sqrt{\sum_{j=1}^{2} (x_j - y_j)^2}$*, and the* ∞*-norm* $d(x, y) = \max_{j=1,2} |x_j - y_j|$*. The open ball* $B_r(0)$ *in these three metric spaces is shown in Fig. 1.*



(a) 1-norm (taxicab metric) (b) 2-norm (Euclidean metric) (c) ∞-norm

Figure 1: $B_r(0)$ for different metrics

Definition 3.9 (Open and closed sets) *Let (X, d) be a metric space.*

- *A set $U \subseteq X$ is* open *if for every $x \in U$ there exists $\epsilon > 0$ such that $B_\epsilon(x) \subseteq U$.*
- *A set $F \subseteq X$ is* closed *if $F^c := X \setminus F$ is open.*

We note that $\emptyset$ and X are both open and closed!

Proposition 3.10 *Let (X, d) be a metric space.*

(i) Let $A_1, A_2 \subseteq X$. If A_1 and A_2 are open, then $A_1 \cap A_2$ is open.

(ii) If $A_i \subseteq X$, $i \in I$ are open, then $\cup_{i\in I} A_i$ is open.

Proof. (i) Since A_1 is open, for each $x \in A_1$, there exists an $\epsilon_1 > 0$ such that $B_{\epsilon_1}(x) \subseteq A_1$. Since A_2 is open, for each $x \in A_2$, there exists an $\epsilon_2 > 0$ such that $B_{\epsilon_2}(x) \subseteq A_2$. Let $x \in A_1 \cap A_2$. Choose $\epsilon = \min\{\epsilon_1, \epsilon_2\}$. Then $B_\epsilon(x) \subseteq A_1 \cap A_2$ as required.

(ii) Let $x \in \cup_{i\in I} A_i$. Then there exists $i \in I$ such that $x \in A_i$, and since A_i is open there exists $\epsilon > 0$ such that $B_\epsilon(x) \subseteq A_i$. Since $A_i \subseteq \cup_{i\in I} A_i$, we are done. □

Using DeMorgan, we immediately have the following corollary:

Corollary 3.11 *Let (X, d) be a metric space.*

(i) Let $A_1, A_2 \subseteq X$. If A_1 and A_2 are closed, then $A_1 \cup A_2$ is closed.

(ii) If $A_i \subseteq X$, $i \in I$ are closed, then $\cap_{i\in I} A_i$ is closed.

Definition 3.12 (Interior and closure) *Let $A \subseteq X$ where (X, d) is a metric space.*

- *The* closure *of A is $\overline{A} := \{x \in X : \forall \epsilon > 0\ B_\epsilon(x) \cap A \neq \emptyset\}$*
- *The* interior *of A is $\mathring{A} := \{x \in X : \exists \epsilon > 0 \text{ s.t. } B_\epsilon(x) \subseteq A\}$*
- *The* boundary *of A is $\partial A := \{x \in X : \forall \epsilon > 0,\ B_\epsilon(x) \cap A \neq \emptyset$ and $B_\epsilon(x) \cap A^c \neq \emptyset\}$*

The closure of a set is the smallest closed set that contains it while the interior of a set is the largest open set contained by it.

Example 3.13 *Let $X = (a, b] \subseteq \mathbb{R}$ with the ordinary (Euclidean) metric. Then $\overline{X} = [a, b]$, $\mathring{X} = (a, b)$ and $\partial X = \{a, b\}$.*

Proposition 3.14 *Let $A \subseteq X$ where (X, d) is a metric space. Then $\mathring{A} = A \setminus \partial A$.*

Proof. First, we show $\mathring{A} \subseteq A \setminus \partial A$. Let $x \in \mathring{A}$. Then by definition $\exists \epsilon > 0$ s.t. $B_\epsilon(x) \subseteq A$. Clearly $x \in A$ and also $\exists \epsilon > 0$ such that $B_\epsilon(x) \cap A^c = \emptyset$. Thus by definition, $x \notin \partial A$. Thus $x \in A \setminus \partial A$.

Next, we show $A \setminus \partial A \subseteq \mathring{A}$. Let $x \in A \setminus \partial A$. Then $x \in A$ and $x \notin \partial A$. The latter means that $\exists \epsilon > 0$ such that $B_\epsilon(x) \cap A = \emptyset$ or $B_\epsilon(x) \cap A^c = \emptyset$. Since $x \in A$, $x \in B_\epsilon(x) \cap A$ for any $\epsilon > 0$, so the former cannot be true. Therefore $\exists \epsilon > 0$ such that $B_\epsilon(x) \cap A^c = \emptyset$, i.e. $B_\epsilon(x) \subseteq A$. Thus $x \in \mathring{A}$. □

3.2 Sequences

Definition 3.15 *Let (X, d) be a metric space. A* sequence *is an ordered list of points x_n, $n \in \mathbb{N}$, in X, denoted $(x_n)_{n\in\mathbb{N}}$. We say that a sequence $(x_n)_{n\in\mathbb{N}}$* converges *to a point $x \in X$ if*

$$\forall \epsilon > 0\, \exists\, n_\epsilon \in \mathbb{N} \text{ s.t. } d(x_n, x) < \epsilon \text{ for all } n \geq n_\epsilon.$$

Proposition 3.16 *Let (X, d) be a metric space, and let $A \subseteq X$. Then $\overline{A}$ is equal to the set of points in X which are limits of a sequence in A.*

Proof. Let $x \in \overline{A}$. Then by definition, for every $\epsilon > 0$, $B_\epsilon(x) \cap A \neq \emptyset$. In particular this is true for $\epsilon = 1/n$. Thus, for any $n \in N$, we can choose an $x_n \in A$ such that $x_n \in B_{1/n}(x)$, which means $d(x, x_n) < \frac{1}{n}$ by the definition of an open ball. Since $1/n$ decreases monotonically to zero, we must have $x_n \to x$.

Let $x \in X$ be the limit of a sequence $(x_n)_{n\in\mathbb{N}} \in A$. Then for $\epsilon > 0$, $\exists\, n_\epsilon \in \mathbb{N}$ such that $d(x_n, x) < \epsilon$ for all $n \geq n_\epsilon$. This means $x_n \in B_\epsilon(x)$, and since $x_n \in A$, $B_\epsilon(x) \cap A \neq \emptyset$. Thus $x \in \overline{A}$. □

Combining this result with the fact that $A \subseteq X$ is closed if and only if $A = \overline{A}$ (exercise), gives the following useful way to characterize closed sets.

Corollary 3.17 *A set $F \subseteq X$, where (X, d) is a metric space, is closed if and only if every sequence in F which converges in X converges to a point in F.*

We also define a concept related to the closure of a set: a cluster or accumulation point.

Definition 3.18 *Let (X, d) be a metric space and $A \subseteq X$. A point $x \in X$ is a* cluster point *of A (also called accumulation point) if for every $\epsilon > 0$, $B_\epsilon(x)$ contains infinitely many points in A.*

Proposition 3.19 *$x \in X$ is a cluster point of $A \subseteq X$ where (X, d) is a metric space if and only if there exists a sequence of points $x_n \in A$, $n \in \mathbb{N}$, such that $x_n \to x$.*

Proof. ($\Leftarrow$) Suppose there exists a sequence $(x_n)_{n\in N}$ in A such that $x_n \to x$. Then for every $\epsilon > 0$, by the definition of a convergent sequence, $B_\epsilon(x)$ contains infinitely many elements of the sequence x_n (in particular, $\exists n_0 \in \mathbb{N}$ such that $x_n \in B_\epsilon(x)$ for all $n \geq n_0$). Since each $x_n \in A$, x is a cluster point of A.

($\Rightarrow$) Suppose x is a cluster point of A. Then for any $\epsilon > 0$, $\exists x_\epsilon \in A$ such that $x_\epsilon \in B_\epsilon(x)$. In particular, take $\epsilon = 1/n$. Then $\exists x_n \in A$ such that $x_n \in B_{1/n}(x)$. By construction, such x_n form a sequence in A that converges to x.

□

Combining Proposition 3.16 and Proposition 3.19 gives the following:

Corollary 3.20 *For $A \subseteq X$, (X, d) a metric space, we have $\overline{A} = A \cup \{x \in X : x \text{ is a cluster point of } A\}$.*

3.2.1 Cauchy sequences

Definition 3.21 (Cauchy sequence) *Let (X, d) be a metric space. A sequence denoted $(x_n)_{n\in\mathbb{N}} \in X$ is called a* Cauchy sequence *if*

$$\forall \epsilon > 0\ \exists\, n_\epsilon \in \mathbb{N} \text{ s.t. } d(x_n, x_m) < \epsilon \text{ for all } n, m \geq n_\epsilon.$$

Proposition 3.22 *Let (X, d) be a metric space, and let $(x_n)_{n\in\mathbb{N}}$ be a convergent sequence in X. Then $(x_n)_{n\in\mathbb{N}}$ is Cauchy.*

Proof. Let $\epsilon > 0$ be arbitrary. Let $(x_n)_{n\in\mathbb{N}}$ be a convergent sequence in a metric space (X, d). Then there exists $n_\epsilon \in \mathbb{N}$ such that $d(x_n, x) < \frac{\epsilon}{2}$ for all $n \geq n_\epsilon$. Then for $n, m \geq n_\epsilon$, using the triangle inequality we have

$$d(x_n, x_m) \leq d(x_n, x) + d(x, x_m) < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Thus $(x_n)_{n\in\mathbb{N}}$ is Cauchy. □

Definition 3.23 *A metric space where every Cauchy sequence converges (to a point in the space) is called* complete.

In addition, a normed space that is complete with respect to the metric induced by the norm is called a *Banach space*. $\mathbb{R}^n$ with the Euclidean distance is complete (and is, in fact, a Banach space).

Proposition 3.24 ([Run05, Proposition 2.4.5]) *Let (X, d) be a metric space, and let $Y \subseteq X$.*

(i) If X is complete and if Y is closed in X, then Y is complete.

(ii) If Y is complete, then it is closed in X.

Proof. (i) Let X be a complete metric space and Y be a closed subset of X. Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in Y. Since $Y \subseteq X$, $(x_n)_{n\in\mathbb{N}}$ is also a Cauchy sequence in X. Therefore $(x_n)_{n\in\mathbb{N}}$ converges to an $x \in X$ since X is complete. But since Y is closed, by Proposition 3.16, we must have $x \in Y$. Therefore Y is complete.

(ii) Let (X, d) be a metric space and let $Y \subseteq X$ be complete. Let $(y_n)_{n\in\mathbb{N}}$ be a sequence in Y that converges to some point $y \in X$. By Proposition 3.22, $(y_n)_{n\in\mathbb{N}}$ is Cauchy in X and therefore also in Y. Since Y is complete, $(y_n)_{n\in\mathbb{N}}$ converges to a point $y' \in Y$. Since sequences in metric spaces converge to unique points (see exercises), $y = y'$. Thus Y is closed by Corollary 3.17. □

3.2.2 Subsequences

Definition 3.25 *Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in a metric space (X, d). Let $(n_k)_{k\in\mathbb{N}}$ be a sequence of natural numbers with $n_1 < n_2 < \cdots$. The sequence $(x_{n_k})_{k\in\mathbb{N}}$ is called a* subsequence *of $(x_n)_{n\in\mathbb{N}}$. If $(x_{n_k})_{k\in\mathbb{N}}$ converges to $x \in X$, we call x a* subsequential limit*.*

Example 3.26 *The sequence $((-1)^n)_{n\in\mathbb{N}}$ diverges but the subsequences $\left((-1)^{2n}\right)_{n\in\mathbb{N}}$ and $\left((-1)^{2n-1}\right)_{n\in\mathbb{N}}$ converge to subsequential limits 1 and -1, respectively.*

Proposition 3.27 *A sequence $(x_n)_{n\in\mathbb{N}}$ in a metric space (X, d) converges to $x \in X$ if and only if every subsequence of $(x_n)_{n\in\mathbb{N}}$ also converges to x.*

Proof. ($\Leftarrow$) If every subsequence of $(x_n)_{n\in\mathbb{N}}$ converges to $x \in X$, then $(x_n)_{n\in\mathbb{N}}$ must converge to it as well, since a sequence is a subsequence of itself.

($\Rightarrow$) Suppose $(x_n)_{n\in\mathbb{N}}$ converges to $x \in X$ and let $(x_{n_k})_{k\in\mathbb{N}}$ be an arbitrary subsequence of $(x_n)_{n\in\mathbb{N}}$. Let $\epsilon > 0$ be arbitrary. There exists $n_\epsilon \in \mathbb{N}$ such that $d(x_n, x) < \epsilon$ for all $n \geq n_\epsilon$. Choose k_ϵ such that $n_{k_\epsilon} \geq n_\epsilon$, which must exist since $(n_k)_{k\in\mathbb{N}}$ is strictly increasing. Then for all $k \geq k_\epsilon$, $d(x_{n_k}, x) < \epsilon$. Thus $(x_{n_k})_{k\in\mathbb{N}}$ converges to x. □

3.3 Continuity

Definition 3.28 *Let (X, d_X) and (Y, d_Y) be metric spaces, let $x_0 \in X$, and let $f : X \to Y$. f is* continuous *at x_0 if for every sequence $(x_n)_{n\in\mathbb{N}}$ in X that converges to x_0, we have $\lim_{n\to\infty} f(x_n) = f(x_0)$. We say that f is* continuous *if it is continuous at every point in X.*

Theorem 3.29 ([Run05, Theorem 2.3.7.]) *Let (X, d_X) and (Y, d_Y) be metric spaces, let $x_0 \in X$, and let $f : X \to Y$. The following are equivalent:*

(i) f is continuous at x_0

(ii) for all $\epsilon > 0$, there exists $\delta > 0$ such that $d_Y(f(x), f(x_0))) < \epsilon$ for all $x \in X$ with $d_X(x, x_0) < \delta$

(iii) for each $\epsilon > 0$, there is $\delta > 0$ such that $B_\delta(x_0) \subseteq f^{-1}(B_\epsilon(f(x_0)))$

Proof. (i) $\Rightarrow$ (ii) We prove the contrapositive. Assume

$$\exists \epsilon_0 \text{ such that } \forall \delta > 0 \text{ there exists an } x_\delta \in X \text{ with } d_X(x_\delta, x_0) < \delta \text{ and } d_Y(f(x_\delta), f(x_0))) \geq \epsilon_0 \qquad (\star)$$

We need to find a sequence in X that converges to x_0 but the sequence of images does not converge. Let's construct such a sequence.

Let $\delta = \frac{1}{n}$ in $(\star)$ for $n \in \mathbb{N}$. Then we can pick a sequence $x_n := x_{1/n}$ given by $(\star)$ which converges to x_0. However, for each $n \in \mathbb{N}$, we have $d_Y(f(x_n), f(x_0))) \geq \epsilon_0$, so we cannot have $\lim_{n\to\infty} f(x_n) = f(x_0)$.

(ii) $\Rightarrow$ (iii) Follows from the definitions of the pre-image and open balls.

(iii) $\Rightarrow$ (i) Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in X that converges to x_0. Let $\epsilon > 0$. Then by (iii), there exists $\delta > 0$ such that $B_\delta(x_0) \subseteq f^{-1}(B_\epsilon(f(x_0)))$, i.e. if x is such that $d_X(x, x_0) < \delta$, then x is such that

$d_Y(f(x), f(x_0)) < \epsilon$. By the definition of convergence, there exists an $N \in \mathbb{N}$ such that $d(x_n, x_0) < \delta$ for all $n \geq N$. Then by (iii), $d(f(x_n), f(x_0)) < \epsilon$ for all $n \geq N$. Thus $\lim_{n\to\infty} f(x_n) = f(x_0)$. □

Corollary 3.30 *Let (X, d_X) and (Y, d_Y) be metric spaces and let $f : X \to Y$. The following are equivalent:*

(i) f is continuous

(ii) if $U \subseteq Y$ is open, then $f^{-1}(U)$ is open

(iii) if $F \subseteq Y$ is closed, then $f^{-1}(F)$ is closed

Note: the following proof uses the following results, which you may wish to prove as an exercise using techniques from the set theory section if they are not clear to you: Let X and Y be sets and $f : X \to Y$. Let $A, B \subseteq Y$. Then

1. $A \subseteq B \implies f^{-1}(A) \subseteq f^{-1}(B)$
2. $f^{-1}(Y \setminus A) = X \setminus f^{-1}(A)$

Proof. Let (X, d_X) and (Y, d_Y) be metric spaces and let $f : X \to Y$.

(i) ⇒ (ii): Suppose f is continuous (on every point in X) and let $U \subseteq Y$ be open. Let $x \in f^{-1}(U)$, then $f(x) \in U$, and since U is open, there exists $\epsilon_0 > 0$ such that $B_{\epsilon_0}(f(x)) \subseteq U$. By Theorem 3.29(iii), there exists a $\delta_0 > 0$ such that $B_{\delta_0}(x) \subseteq f^{-1}(B_{\epsilon_0}(f(x)))$. Since $B_{\epsilon_0}(f(x))) \subseteq U$, $f^{-1}(B_{\epsilon_0}(f(x))) \subseteq f^{-1}(U)$. Thus for each $x \in f^{-1}(U)$, there exists δ_0 such that $B_{\delta_0}(x) \subseteq f^{-1}(B_{\epsilon_0}(f(x))) \subseteq f^{-1}(U)$, so $f^{-1}(U)$ is open.

(ii) ⇒ (i): We want to prove that f is continuous at every $x \in X$ using the definition from Theorem 3.29(iii), i.e. we must show that for $x \in X$, for each $\epsilon > 0$, there is $\delta > 0$ such that $B_\delta(x) \subseteq f^{-1}(B_\epsilon(f(x)))$.

Let $x \in X$ and let $\epsilon > 0$ be arbitrary. Since $B_\epsilon(f(x))$ is an open set, by (ii), $f^{-1}(B_\epsilon(f(x)))$ is also open. Since $x \in f^{-1}(B_\epsilon(f(x)))$, there exists a $\delta > 0$ such that $B_\delta(x) \subseteq f^{-1}(B_\epsilon(f(x)))$ by the definition of a set being open, so we are done.

(ii) ⇒ (iii): Let $F \subseteq Y$ be closed. Then $Y \setminus F$ is open, so by (ii), $f^{-1}(Y \setminus F)$ is open as well. Since $f^{-1}(Y \setminus F) = X \setminus f^{-1}(F)$, $f^{-1}(F)$ is closed.

(iii) ⇒ (ii) follows from the above, exchanging "open" and "closed".

□

Definition 3.31 *Let (X, d_X) and (Y, d_Y) be metric spaces and let $f : X \to Y$.*

- *f is* uniformly continuous *if for all $\epsilon > 0$, there exists $\delta > 0$ such that for every $x_1, x_2 \in X$ with $d_X(x_1, x_2) < \delta$, we have $d_Y(f(x_1), f(x_2))) < \epsilon$*
- *f is* Lipschitz continuous *if there exists a $K > 0$ such that for every $x_1, x_2 \in X$ we have $d_Y(f(x_1), f(x_2))) \leq K d_X(x_1, x_2)$*

Proposition 3.32 *Let (X, d_X) and (Y, d_Y) be metric spaces and let $f : X \to Y$.*

$$f \text{ is Lipschitz continuous } \Rightarrow f \text{ is uniformly continuous } \Rightarrow f \text{ is continuous}$$

The proof is left as an exercise.

Definition 3.33 *Let (X, d) be a metric space and let $f : X \to X$. We say that $x^* \in X$ is a* fixed point *of f if $f(x^*) = x^*$.*

Definition 3.34 *Let (X, d) be a metric space and let $f : X \to X$. f is a* contraction *if there exists a constant $k \in [0, 1)$ such that for all $x, y \in X$, $d(f(x), f(y))) \leq k d(x, y)$.*

Observe that a function is a contraction if and only if it is Lipschitz continuous with constant $K < 1$.

Theorem 3.35 *Suppose that $f : X \to X$ is a contraction and the metric space X is complete. Then f has a unique fixed point x^*.*

We omit the proof here; see [Pug15, p.240] for the proof as well as more details on how to find the fixed point.

Example 3.36 *Let $f : \left[-\frac{1}{3}, \frac{1}{3}\right] \to \left[-\frac{1}{3}, \frac{1}{3}\right]$ be defined by the mapping $x \mapsto x^2$. Assume we use the standard Euclidean metric, $d(x, y) = |x - y|$. f has a unique fixed point because $\left[-\frac{1}{3}, \frac{1}{3}\right]$ is a complete metric space (see Proposition 3.24) and f is a contraction with Lipschitz constant 2/3.*

To see that it is a contraction, let $x, y \in \left[-\frac{1}{3}, \frac{1}{3}\right]$. Then

$$|x^2 - y^2| = |x + y||x - y| \leq \frac{2}{3}|x - y|.$$

3.4 Equivalence of metrics

Definition 3.37 (Equivalent metrics) *Two metrics d_1 and d_2 on a set X are* equivalent *if the identity maps from (X, d_1) to (X, d_2) and from (X, d_2) to (X, d_1) are continuous.*

The following result follows from the definition and Corollary 3.30:

Proposition 3.38 *Two metrics d_1, d_2 on a set X are equivalent if and only if they have the same open sets or the same closed sets.*

So, in a certain sense, equivalent metrics induce the same structure.

Definition 3.39 *Two metrics d_1 and d_2 on a set X are* strongly equivalent *if for every $x, y \in X$, there exists constants $\alpha > 0$ and $\beta > 0$ such*

$$\alpha d_1(x, y) \leq d_2(x, y) \leq \beta d_1(x, y).$$

If two metrics are strongly equivalent then they are equivalent. The proof of this is part of the exercises.

Example 3.40 *We show that the Euclidean distance (induced by 2-norm) and the metric induced by the ∞-norm are equivalent on $\mathbb{R}^n$.*

Let $\|x-y\|_2 = \sqrt{\sum_{j=1}^n (x_j - y_j)^2}$ be the Euclidean metric and $\|x-y\|_\infty = \max_{j=1,\ldots,n} |x_j - y_j|$ be the metric induced by the ∞-norm. We have

$$\|x - y\|_2 = \sqrt{\sum_{j=1}^{n} (x_j - y_j)^2} \leq \sqrt{n \max_{j=1,\ldots,n} (x_j - y_j)^2} = \sqrt{n} \max_{j=1,\ldots,n} |x_j - y_j| = \sqrt{n}\, \|x - y\|_\infty$$

and

$$\|x - y\|_\infty = \max_{j=1,\ldots,n} |x_j - y_j| = \sqrt{\max_{j=1,\ldots,n} (x_j - y_j)^2} \leq \sqrt{\sum_{j=1}^{n} (x_j - y_j)^2} = \|x - y\|_2 .$$

Thus the two metrics are strongly equivalent.

3.5 Extra properties of $\mathbb{R}$

Using the definition of continuity in terms of ϵ-balls and equipping $\mathbb{R}$ with the metric induced by the absolute value, i.e. $d(x, y) = |x - y|$ for $x, y \in \mathbb{R}$, we obtain the usual $\epsilon - \delta$ definition of continuity. Hence, a function $f\colon \mathbb{R} \to \mathbb{R}$ is continuous at $x_0 \in \mathbb{R}$ if for all $\epsilon > 0$ there exists a $\delta > 0$ such that $|x_0 - y| < \delta$ implies $|f(x_0) - f(y)| < \epsilon$. Since $\mathbb{R}$ is also totally ordered we can also talk about left and right continuity, by separating $B_\epsilon(x) = (x - \epsilon, x + \epsilon) = (x - \epsilon, x] \cup [x, x + \epsilon)$.

Definition 3.41 *Let $f\colon \mathbb{R} \to \mathbb{R}$.*

- *f is* left continuous *at $x_0 \in \mathbb{R}$ if for all $\epsilon > 0$ there exists a $\delta > 0$, such $|f(x_0) - f(x)| < \epsilon$ whenever $x_0 - \delta < x < x_0$.*

- f *is* right continuous *at* $x_0 \in \mathbb{R}$ *if for all* $\epsilon > 0$ *there exists a* $\delta > 0$*, such* $|f(x_0) - f(x)| < \epsilon$ *whenever* $x_0 < x < x_0 + \delta$.

We say that f is left continuous if it is left continuous at all points in the domain, and similar for right continuous.

Similar to the ordinary sense of continuity, one can describe left and right continuity in terms of sequences.

Proposition 3.42 *A function $f : \mathbb{R} \to \mathbb{R}$ is continuous if and only if it is left and right continuous.*

Proof. ($\Leftarrow$) Suppose $f : \mathbb{R} \to \mathbb{R}$ is both right and left continuous. Let $\epsilon > 0$ be arbitrary. Then by the definition of left continuous, there exists a $\delta_1 > 0$, such $|f(x_0) - f(x)| < \epsilon$ whenever $x_0 - \delta_1 < x < x_0$, and by the definition of right continuous, there exists a $\delta_2 > 0$, such $|f(x_0) - f(x)| < \epsilon$ whenever $x_0 < x < x_0 + \delta_2$.

Let $\delta = \min\{\delta_1, \delta_2\}$. Let $x \in \mathbb{R}$ such that $|x_0 - x| < \delta$. Then $x_0 - \delta < x < x_0 + \delta$.

Case 1: Suppose $x < x_0$. Then $x_0 - \delta_1 < x < x_0$, so $|f(x_0) - f(x)| < \epsilon$, so f is continuous.

Case 2: Suppose $x > x_0$. Then $x_0 < x < x_0 + \delta_2$, so $|f(x_0) - f(x)| < \epsilon$, so f is continuous.

If $x = x_0$, the result is trivial, so we conclude that f is continuous.

($\Rightarrow$) Let $f : \mathbb{R} \to \mathbb{R}$ be continuous. Then for every $\epsilon > 0$, $\exists \delta_0 > 0$ such that when x is such that $|x - x_0| < \delta$, then $|f(x) - f(x_0)| < \epsilon$.

For $\epsilon > 0$ arbitrary, take δ_0 from the definition of f being continuous. Take $x \in \mathbb{R}$ such that $x_0 < x < x_0 + \delta_0$. Then $x_0 - \delta_0 < x < x_0 + \delta_0$, which implies $|x - x_0| < \delta_0$. Thus $|f(x) - f(x_0)| < \epsilon$, so f is right-continuous.

The proof for left-continuity is similar. □

Using the least upper bound property of sets, we can introduce the concepts of limit inferior and limit superior as the limit of infima and suprema when we view the sequence as a set. First, we recall what it means for a sequence to be bounded.

Definition 3.43 *Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{R}$. We call $(x_n)_{n\in\mathbb{N}}$* bounded *if there exists an $M > 0$ such that $|x_n| < M$ for all $n \in \mathbb{N}$.*

This definition is equivalent to the set of sequence elements being bounded in the metric space setting. Similarly, one can talk about a sequence being bounded above or below in the order theoretic setting (see Section 2.2), by looking at the set of sequence elements. The next theorem is useful.

Theorem 3.44 (Monotone convergence theorem)

(i) Suppose $(x_n)_{n\in\mathbb{N}}$ is an increasing sequence, i.e. $x_n \leq x_{n+1}$ for all $n \in \mathbb{N}$, and that it is bounded (above). Then the sequence converges. Furthermore, $\lim_{n\to\infty} x_n = \sup_{n\in\mathbb{N}} x_n$, where $\sup_{n\in\mathbb{N}} x_n := \sup\{x_n : n \in \mathbb{N}\}$.

(ii) Suppose $(x_n)_{n\in\mathbb{N}}$ is a decreasing sequence, i.e. $x_n \geq x_{n+1}$ for all $n \in \mathbb{N}$, which is bounded (below). Then the sequence converges and $\lim_{n\to\infty} x_n = \inf_{n\in\mathbb{N}} x_n := \inf\{x_n : n \in \mathbb{N}\}$.

The proof is omitted. We call increasing or decreasing sequences monotone, hence the theorem name.

If the sequence is increasing but not bounded above, then $\lim_{n\to\infty} x_n = \infty$, and if it is decreasing but not bounded below, then $\lim_{n\to\infty} x_n = -\infty$.

We would like to use the monotone convergence theorem for arbitrary sequences. We do so by building an increasing sequence (or decreasing) sequence from an arbitrary one. First, we recall some facts about infima and suprema and introduce the convention that $\sup A = \infty$ if $A \subseteq \mathbb{R}$ is not bounded above and $\inf A = -\infty$ if A is not bounded below.

Lemma 3.45 *If $A \subseteq B \subseteq \mathbb{R}$ is non-empty, then $\inf A \leq \sup A$, $\sup A \leq \sup B$, and $\inf A \geq \inf B$.*

The proof of this follows from the definition of greatest lower and least upper bound.

Definition 3.46 *Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{R}$. We define the* limit superior *of $(x_n)_{n\in\mathbb{N}}$ as*

$$\limsup_{n\to\infty} x_n := \lim_{n\to\infty} \sup_{k\geq n} x_k.$$

Similarly we define the limit inferior *of $(x_n)_{n\in\mathbb{N}}$ as*

$$\liminf_{n\to\infty} x_n := \lim_{n\to\infty} \inf_{k\geq n} x_k.$$

Proposition 3.47 *Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{R}$.*

- *The sequence of suprema, $s_n = \sup_{k\geq n} x_k$, is decreasing and the sequence of infima, $i_n = \inf_{k\geq n} x_k$, is increasing.*
- *The limit superior and the limit inferior of a bounded sequence always exist and are finite.*

Proof. The first part is true by Lemma 3.45. The second bullet point follows by the Monotone Convergence Theorem. □

Conceptually, we can think of the limit superior as the greatest cluster point of a sequence, and of the limit inferior as the least. If the sequence $(x_n)_{n\in\mathbb{N}}$ is not bounded above, then $\limsup_{n\to\infty} x_n = \infty$. Similarly, if the sequence $(x_n)_{n\in\mathbb{N}}$ is not bounded below, then $\liminf_{n\to\infty} x_n = -\infty$. This is in line with our convention that $\sup A = \infty$, if A is not bounded above and $\inf A = -\infty$, if A not bounded below.

Theorem 3.48 *Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{R}$. Then the sequence converges to $x \in \mathbb{R}$ if and only if $\limsup_{n\to\infty} x_n = x = \liminf_{n\to\infty} x_n$.*

Proof. For convenience, denote $i_n := \inf_{k\geq n} x_k$ and $s_n := \sup_{k\geq n} x_k$ for $n \in \mathbb{N}$.

($\Rightarrow$) Suppose $\lim_{n\to\infty} x_n = x \in \mathbb{R}$ and let $\epsilon > 0$. Since the sequence converges, there exists an $N \in \mathbb{N}$ such that $|x - x_n| < \epsilon$, i.e. $x - \epsilon < x_n < x + \epsilon$, for all $n \geq N$.

In particular, $x - \epsilon < x_n$ for all $n \geq N$, so $x - \epsilon$ is a lower bound for the set $\{x_n \colon n \geq N\}$. Therefore $x - \epsilon \leq i_N$.

Similarly, since $x_n < x - \epsilon$ for all $n \geq N$, $x + \epsilon$ is an upper bound for the set $\{x_n \colon n \geq N\}$. Therefore $s_N \leq x + \epsilon$.

By Proposition 3.47 the sequence of infima is increasing and by the Monotone Convergence Theorem, its limit is given by the supremum of the sequence. Hence, we obtain

$$x - \epsilon \leq i_N \leq \lim_{n\to\infty} i_n = \liminf_{n\to\infty} x_n.$$

Similarly, since the sequence of suprema is decreasing and using the Monotone Convergence theorem again, we obtain

$$\limsup_{n\to\infty} x_n \leq s_N < x + \epsilon.$$

Now observe that $\liminf_{n\to\infty} x_n \leq \limsup_{n\to\infty} x_n$, since $i_n \leq s_n$ for all $n \in \mathbb{N}$ by Lemma 3.45 (exercise: $x_n \leq y_n$ for all $n \in \mathbb{N}$ implies $\lim_{n\to\infty} x_n \leq \lim_{n\to\infty} y_n$). Thus we have

$$x - \epsilon \leq \liminf_{n\to\infty} x_n \leq \limsup_{n\to\infty} x_n \leq x + \epsilon.$$

Since this holds for any ϵ, the desired result follows.

($\Leftarrow$) Now suppose $\limsup_{n\to\infty} x_n = x = \liminf_{n\to\infty} x_n$. We need to show that $\lim_{n\to\infty} x_n = x$.

Let $\epsilon > 0$. Then since $\limsup_{n\to\infty} x_n = \lim_{n\to\infty} s_n = x$, there exists an $N_1 \in \mathbb{N}$ such that $|s_n - x| < \epsilon$ for all $n \geq N_1$. In particular,

$$x_k \leq s_{N_1} < x + \epsilon \qquad \text{for all } k \geq N_1.$$

Similarly, there exists $N_2 \in \mathbb{N}$ such that $|i_n - x| < \epsilon$ for all $n \geq N_2$ giving

$$x - \epsilon < i_{N_2} \leq x_k \qquad \text{for all } k \geq N_2.$$

Hence, by setting $N = \max\{N_1, N_2\}$ we see $x - \epsilon < x_k < x + \epsilon$ or equivalently $|x_k - x| < \epsilon$ for all $k \geq N$, which proves the result. □

Note that we only talked about limit superior and limit inferior for real sequences. However, we can extend this easily to a sequence of functions $f_n \colon X \to \mathbb{R}$ by setting $f = \limsup_{n\to\infty} f_n$ to be the function defined pointwise by $f(x) = \limsup_{n\to\infty}(f_n(x))$ and similar for the limit inferior. There also exists a set theoretic version in terms of unions and intersections which you will encounter in probability.

3.6 Exercises

1. Show that the infinity norm $||x||_\infty$, $x \in \mathbb{R}^n$, defined in Example 3.4 is a norm.
2. Let (X, d) be any metric space, and define $\tilde{d} : X \times X \to \mathbb{R}$ by

$$\tilde{d}(x, y) = \frac{d(x, y)}{1 + d(x, y)}, \quad x, y \in X.$$

   Show that $\tilde{d}$ is a metric on X.
3. Let X be a set and define $d \colon X \times X \to \mathbb{R}$ by $d(x, x) = 0$ and $d(x, y) = 1$ for $x \neq y \in X$. Prove that d is a metric on X. What do open balls look like for different radii $r > 0$? What does an arbitrary open set look like?
4. Following up on Proposition 3.10 and Corollary 3.11: Show that the infinite intersection of open sets may not be open and that the infinite union of closed sets may not be closed.
5. Find the closure, interior, and boundary of the following sets using Euclidean distance:
   (i) $\{(x, y) \in \mathbb{R}^2 : y < x^2\} \subseteq \mathbb{R}^2$
   (ii) $[0, 1) \times [0, 1) \subseteq \mathbb{R}^2$
   (iii) $\{0\} \cup \{1/n \colon n \in \mathbb{N}\} \subseteq \mathbb{R}$
6. Prove the following: Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in a metric space (X, d) that converges to a point $x \in X$. Then x is unique.
7. Let $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ be sequences in $\mathbb{R}$ such that $x_n \to x$ and and $y_n \to y$, with $\alpha, x, y, \in \mathbb{R}$.
   (i) Show that $\alpha\, x_n \to \alpha\, x$.
   (i) Show that $x_n + y_n \to x + y$.
8. Let (x_n), (y_n) be two convergent sequences in $\mathbb{R}$ such that $x_n \leq y_n$ for all $n \in \mathbb{N}$. Show that $\lim_{n\to\infty} x_n \leq \lim_{n\to\infty} y_n$.
9. Show that discrete metric spaces (i.e. those with the metric from exercise 3) are complete.
10. Let (X, d_X) and (Y, d_Y) be metric spaces and let $f : X \to Y$. Prove that

$$f \text{ is Lipschitz continuous } \Rightarrow f \text{ is uniformly continuous } \Rightarrow f \text{ is continuous.}$$

    Provide examples to show that the other directions do not hold.
11. Show that the function $f(x) = \frac{1}{2}\left(x + \frac{5}{x}\right)$ has a unique fixed point on a subset of $(0, \infty)$. What is it? (Hint: you will have to restrict the interval in such a way that f is a contraction.)
12. Prove the following: If two metrics are strongly equivalent then they are equivalent.
13. Let $(x_n)_{n\in N}$ be a sequence in $\mathbb{R}$. Show that $\lim_{n\to\infty} x_n = 0$ if and only if $\limsup_{n\to\infty} |x_n| = 0$.

3.7 References

The content in this section comes mostly from [Run05]. [Pug15] is used to supplement, and in particular the content on accumulation points and contractions comes from there. For lim sup and lim inf, see [Leb22].

4 Topology

4.1 Basic definitions

Let X be a set. If X is not a metric space, can we still have open and closed sets? This question motivates the concept of a topology. One can think of a topology on X as a specification what of subsets of X are open. In the metric space section we already saw some properties of open and closed sets, which motivates the following definition.

Definition 4.1 *Let $\mathcal{T} \subseteq \mathcal{P}(X)$. We call $\mathcal{T}$ a* topology *on X if the following holds:*

(i) $\emptyset, X \in \mathcal{T}$

(ii) Let A be an arbitrary index set. If $U_\alpha \in \mathcal{T}$ for $\alpha \in A$, then $\bigcup_{\alpha \in A} U_\alpha \in \mathcal{T}$ ($\mathcal{T}$ is closed under taking arbitrary unions)

(iii) Let $n \in \mathbb{N}$. If $U_1, \dots, U_n \in \mathcal{T}$, then $\bigcap_{i=1}^n U_i \in \mathcal{T}$ ($\mathcal{T}$ is closed under taking finite intersections)

If $U \in \mathcal{T}$, we call U open*. We call $U \subseteq X$* closed*, if $U^c \in \mathcal{T}$. We call $(X, \mathcal{T})$ a* topological space*.*

Alternatively we could have specified closed sets, and obtained similar axioms using De Morgan's rules.

Example 4.2 *For a set X, the following $\mathcal{T} \subseteq \mathcal{P}(X)$ are examples of topologies on X.*

- *Trivial topology: $\mathcal{T} = \{\emptyset, X\}$,*
- *Discrete topology: $\mathcal{T} = \mathcal{P}(X)$,*
- *Topology induced by a metric: i.e. if d is a metric on X we can define*

$$\mathcal{T}_d = \{U \subseteq X \mid \forall x \in U \ \exists \epsilon > 0 \text{ such that } B_\epsilon(x) \subseteq U\}.$$

  The discrete topology is also induced by a metric, can you guess which one?

- *Let X be an infinite set. Then, $\mathcal{T} = \{U \subseteq X : U^c \text{ is finite}\} \cup \emptyset$ defines a topology on X.*

Given a topological space $(X, \mathcal{T})$ and a subset $Y \subseteq X$, we can restrict the topology on X to Y which leads to the next definition.

Definition 4.3 (Relative topology) *Given a topological space $(X, \mathcal{T})$ and an arbitrary non-empty subset $Y \subseteq X$, we define the relative topology on Y as follows*

$$\mathcal{T}|_Y = \{U \cap Y : U \in \mathcal{T}\}.$$

Recall that in the metric space setting, we had set theoretic descriptions of closures and interiors of sets. We will generalize this in the next definition.

Definition 4.4 *Let $(X, \mathcal{T})$ be a topological space and let $A \subseteq X$ be any subset.*

- *The* interior *of A is $\mathring{A} := \{a \in A : \exists U \in \mathcal{T} \text{ s.t. } U \subseteq A \text{ and } a \in U\}$.*
- *The* closure *of A is $\overline{A} := \{x \in X : \forall U \in \mathcal{T} \text{ with } x \in U, U \cap A \neq \emptyset\}$.*
- *The* boundary *of A is $\partial A := \{x \in X : \forall U \in \mathcal{T} \text{ with } x \in U, U \cap A \neq \emptyset \text{ and } U \cap A^c \neq \emptyset\}$.*

One can see that the definitions are taken fairly verbatim from the metric space setting, except that we are now looking at arbitrary open sets given by the topology instead of balls of the form $B_\epsilon(x)$.

Example 4.5 *Let $X = \{a, b, c\}$ and $\mathcal{T} = \{\emptyset, \{a\}, \{b\}, \{a, b\}, X\}$. Then the following holds*

- $\mathring{\{a\}} = \{a\}$,
- $\mathring{\{c\}} = \emptyset$,
- $\overline{\{a\}} = \{a, c\}$,
- $\overline{\{c\}} = \{c\}$.

Note that even though we do not necessarily have a characterization of closures in terms of limits of sequences as in metric spaces for arbitrary topological spaces, there exists an alternative characterization that still holds in this general setting (and thus in particular also for metric spaces).

Proposition 4.6 (Proposition 3.1.18 in [Run05]) *Let $(X, \mathcal{T})$ be a topological space and $A \subseteq X$. Then,*

$$\overline{A} = \bigcap \{F \colon F \text{ is closed and } A \subseteq F\}.$$

Proof. For convenience define $A' = \bigcap \{F \colon F \text{ is closed and } A \subseteq F\}$. We will show $\overline{A} \subseteq A'$ by showing that $(A')^c \subseteq \overline{A}^c$ (contrapositive). Suppose $x \notin A'$. Then, since an arbitrary intersection of closed sets is closed, $(A')^c$ is an open set containing x. But since $A \subseteq A'$ we have $A \cap (A')^c = \emptyset$, showing that $x \notin \overline{A}$.

Conversely, assume $x \notin \overline{A}$. Then there exists an open set U with $x \in U$ such that $U \cap A = \emptyset$. Thus, $A \subseteq U^c$. Since U^c is closed, we have by the definition of closure $A' \subseteq U^c$ and since $x \notin U^c$, we have $x \notin A'$. Thus, $A' \subseteq \overline{A}$. □

Similarly, one can show $\mathring{A} = \bigcup \{U : U \text{ is open and } U \subseteq A\}$. Hence, we see that the interior of A is the largest open set contained in A and the closure is the smallest closed set that contains A.

Another important concept in topology (and thus also in metric spaces) is density.

Definition 4.7 *Let $(X, \mathcal{T})$ be a topological space. A subset $A \subseteq X$ is called* dense *if $\overline{A} = X$.*

Using the definition of closure, we see that $A \subseteq X$ is dense if and only if for all non-empty $U \in \mathcal{T}$, $U \cap A \neq \emptyset$.

Example 4.8

- *The rationals $\mathbb{Q}$ are dense in the reals $\mathbb{R}$.*
- *The only dense subset in $(X, \mathcal{P}(X))$ is X itself.*
- *Any non-empty subset is dense in $(X, \{\emptyset, X\})$.*

The concept of a dense subset allows us in a way to look at that set instead of the whole space. In the metric space setting, this means that elements in X can be approximated arbitrarily well with elements from the dense subset.

Definition 4.9 *A topological space $(X, \mathcal{T})$ is* separable *if it contains a countable dense subset.*

As stated in the previous example, $\mathbb{Q}$ is dense in $\mathbb{R}$, and since $\mathbb{Q}$ is countable, $\mathbb{R}$ is separable. We could extend this example to $\mathbb{R}^n$. However, if we look at all bounded real-valued sequences with the metric induced by the supremum norm, this space fails to be separable.

Example 4.10 *Define $\ell_\infty = \{(x_n)_{n\in\mathbb{N}} : x_n \in \mathbb{R},\ \sup_{n\in\mathbb{N}} |x_n| < \infty\}$, the space of bounded real valued sequences. We can endow ℓ_∞ with a metric induced by the supremum norm, namely $d((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) = \sup_{n\in\mathbb{N}} |x_n - y_n|$. Then ℓ_∞ is not separable with respect to the topology induced by this metric.*

To see this, for each $M \subseteq \mathbb{N}$ define

$$e_n^M = \begin{cases} 1 & \text{if } n \in M, \\ 0 & \text{otherwise,} \end{cases}$$

for $n \in \mathbb{N}$.
Then if $M_1, M_2 \subseteq \mathbb{N}$ are non-empty with $M_1 \neq M_2$, $d((e_n^{M_1})_{n\in\mathbb{N}}, (e_n^{M_2})_{n\in\mathbb{N}}) = 1$. Thus the open balls $B_{1/3}((e_n^{M_1})_{n\in\mathbb{N}})$, $B_{1/3}((e_n^{M_2})_{n\in\mathbb{N}})$ are disjoint for all non-empty $M_1, M_2 \subseteq \mathbb{N}$ with $M_1 \neq M_2$ (check using contradiction and triangle inequality).

Now suppose towards contradiction that there exists $A \subseteq \ell^\infty$ is dense and countable. Then by density, for all non-empty open sets $U \subseteq \ell_\infty$, $U \cap A \neq \emptyset$. In particular for all $M \subseteq \mathbb{N}$, $B_{1/3}((e_n^M)_{n\in\mathbb{N}}) \cap A \neq \emptyset$.

However, there are uncountably many such M (see the cardinality of $\mathcal{P}(\mathbb{N})$ in the set theory section), but only countably many elements in A. Since the balls are disjoint, this is a contradiction.

4.2 Compactness

We will start off by giving the definition of an important separation axiom.

Definition 4.11 *A topological space $(X, \mathcal{T})$ is called* Hausdorff *if for all $x \neq y \in X$ there exist open sets U_x, U_y with $x \in U_x$ and $y \in U_y$ such that $U_x \cap U_y = \emptyset$.*

So in a Hausdorff space, we can separate any two elements using open sets.

Example 4.12 *Let (X, d) be a metric space. Then $(X, \mathcal{T}_d)$ is Hausdorff, where $\mathcal{T}_d$ is the topology induced by the metric d.*

Proof. If $x \neq y \in X$, then choose $\epsilon := d(x, y) > 0$. Then $U_x = B_{\epsilon/2}(x)$ and $U_y = B_{\epsilon/2}(y)$ are disjoint. (If this is not clear, prove using contradiction.) □

Example 4.13 *Let X be an infinite set and $\mathcal{T} = \{U \subseteq X : U^c \text{ is finite}\} \cup \emptyset$. Then $(X, \mathcal{T})$ is not Hausdorff.*

Proof. Suppose in order to derive a contradiction that it is Hausdorff and take $x \neq y \in X$. Then there exist open sets U_x, U_y with $x \in U_x$ and $y \in U_y$ such that $U_x \cap U_y = \emptyset$.

Then $X = \emptyset^c = (U_x \cap U_y)^c = U_x^c \cap U_y^c$. But since U_x and U_y are open and nonempty, U_x^c and U_y^c are both finite. The union of two finite sets is again finite, so this gives us that X is finite, which is a contradiction. □

Definition 4.14 (Compact) *Let $(X, \mathcal{T})$ be a topological space and $K \subseteq X$. A collection $\{U_i\}_{i\in I}$ of open sets is called* open cover *of K if $K \subseteq \cup_{i\in I} U_i$. The set K is called* compact *if for all open covers $\{U_i\}_{i\in I}$ there exists a finite subcover, meaning there exists an $n \in \mathbb{N}$ and $\{U_1, \ldots, U_n\} \subseteq \{U_i\}_{i\in I}$ such that $K \subseteq \cup_{i=1}^n U_i$.*

Example 4.15 *Let $S \subseteq X$ where $(X, \mathcal{T})$ is a topological space. If S is finite, then it is compact.*

Proof. Since S is finite, we can write $S = \{x_1, \ldots, x_n\}$. For any open cover $\mathcal{U} = \{U_i\}_{i\in I}$, for $j = 1, \ldots, n$ there exists $U_j \in \mathcal{U}$ such that $x_j \in U_j$. Thus $S \subseteq \cup_{j=1}^n U_j$, so S is compact. □

Example 4.16 $(0, 1)$ *is not compact.*

Proof. The set $\{U_n\}_{n\in N}$ where $U_n = \left(\frac{1}{n}, 1\right)$ is an open cover for $(0, 1)$ since $(0, 1) \subseteq \cup_{n=1}^\infty \left(\frac{1}{n}, 1\right)$. Suppose in order to derive a contradiction that there exists a finite subcover, i.e. there exists $N \in \mathbb{N}$ such that $(0, 1) \subseteq \cup_{j=1}^N \left(\frac{1}{n_j}, 1\right)$. Since $\left(\frac{1}{n}, 1\right) \subseteq \left(\frac{1}{m}, 1\right)$ for $m \geq n$ (the sets are nested), this means $(0, 1) \subseteq \left(\frac{1}{n_N}, 1\right)$. But clearly there exists an $x \in (0, 1)$ such that $0 < x < \frac{1}{n_N}$ for any finite n_N. Contradiction. Therefore $(0, 1)$ is not compact. □

Proposition 4.17 ([Run05, Proposition 3.3.6]) *Let $(X, \mathcal{T})$ be a topological space and take a non-empty subset $K \subseteq X$. The following holds:*

1. *If X is compact and K is closed, then K is compact (i.e. closed subsets of compact sets are compact).*
2. *If $(X, \mathcal{T})$ is Hausdorff, then K being compact implies that K is closed.*

Proof. 1. We need to show that any open cover of K has a finite subcover. Let $\{U_i\}_{i\in I}$ be an open cover of K. Then, since K^c is open, $\{U_i\}_{i\in I} \cup K^c$ is an open cover of X. Since X is compact there exists a finite subcover. There are two possibilities, the finite subcover is either of the form $\{U_1, \ldots, U_n, K^c\}$ or $\{U_1, \ldots, U_n\}$. In either case, $\{U_1, \ldots, U_n\}$ is a finite subcover for K since $K \subseteq X$. Hence, K is compact.

2. We will show that K^c is open. We do this by showing that there exist open sets $\{U_i\}_{i\in I} \subseteq \mathcal{T}$ such that $K^c = \cup_{i\in I} U_i$.

For each $x \in K^c$, we construct an open set in K^c that contains x.

Let $x \in K^c$. Since X is Hausdorff, for all $y \in K$ there exist disjoint open sets $U_{x,y}$ and U_y with $x \in U_{x,y}$ and $y \in U_y$. Since K is compact and $\{U_y\}_{y\in K}$ is an open cover of K, there exist $y_1, \ldots, y_n$ such that $K \subseteq \cup_{i=1}^n U_{y_i}$.

Then $\tilde{U}_x := \cap_{i=1}^n U_{x,y_i}$ is an open set that contains x by definition, and it is a subset of K^c since each set in the intersection is disjoint from a set that forms the open cover for K.

Since each $\tilde{U}_x \subseteq K^c$, $\cup_{x\in K^c} \tilde{U}_x \subseteq K^c$. Since by construction for any $x \in K^c$ there exists a $\tilde{U}_x$ such that $x \in \tilde{U}_x$, $K^c \subseteq \cup_{x\in K^c} \tilde{U}_x$. Thus $K^c = \cup_{x\in K^c} \tilde{U}_x$, so K^c is open, and thus K is closed. □

In undergraduate math classes you may have seen an equivalent definition for compactness on $\mathbb{R}^n$. This is a nice feature of Euclidean space.

Theorem 4.18 (Heine-Borel Theorem) *Let $K \subseteq \mathbb{R}^n$. Then K is compact with respect to the topology induced by the Euclidean distance if and only if it is closed and bounded.*

The proof is omitted. See [Run05, Corollary 2.5.12].

Just as we had a sequential characterization of the closure of a set in metric spaces, we similarly have a sequential characterization of compactness.

Theorem 4.19 *Let (X, d) be a metric space. Then $K \subset X$ is compact with respect to the metric induced by d if and only if every sequence in K admits a subsequence converging to some point in K.*

Again the proof is omitted. See [Run05, Theorem 2.5.10]. A corollary of this statement together with Heine-Borel is the Bolzano-Weierstrass theorem.

Corollary 4.20 (Bolzano-Weierstrass) *Any bounded sequence in $\mathbb{R}^n$ has a convergent subsequence.*

4.3 Continuity

Lastly, we will discuss continuity in this general setting.

Definition 4.21 *Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces. A map $f\colon X \to Y$ is called* continuous *if for all $U \in \mathcal{T}_Y$, $f^{-1}(U) \in \mathcal{T}_X$, i.e. the preimage of open sets is open.*

We can also specify continuity at a point $x_0 \in X$.

Definition 4.22 *Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces. A map $f\colon X \to Y$ is called* continuous at *$x_0 \in X$ if for all $U \in \mathcal{T}_Y$ with $f(x_0) \in U$, $f^{-1}(U) \in \mathcal{T}_X$, i.e. the preimage of open sets containing $f(x_0)$ is open (and contains x_0).*

The next proposition is, in a certain sense, a generalization of the extreme value theorem to topological spaces.

Proposition 4.23 *Let $(X, \mathcal{T}_X)$ and $(Y, \mathcal{T}_Y)$ be topological spaces. Suppose $K \subset X$ is compact and let $f\colon K \to Y$ be continuous. Then $f(K)$ is compact.*

Proof. Let $\{U_i\}_{i\in I}$ be an open cover of $f(K)$, i.e. $f(K) \subseteq \bigcup_{i\in I} U_i$. Then $f^{-1}(f(K)) \subseteq f^{-1}(\bigcup_{i\in I} U_i)$.

By Exercise 9 in **??**, we have $f^{-1}(\bigcup_{i\in I} U_i) = \bigcup_{i\in I} f^{-1}(U_i)$ and by Proposition 2.30, we have $K \subseteq f^{-1}(f(K))$. Hence, we obtain $K \subseteq \bigcup_{i\in I} f^{-1}(U_i)$.

Since f is continuous, each $f^{-1}(U_i)$ is open and thus $\{f^{-1}(U_i)\}_{i\in I}$ is an open cover of K. Since K is compact, there exist $f^{-1}(U_1), \ldots, f^{-1}(U_n)$ such that $K \subseteq \bigcup_{i=1}^n f^{-1}(U_i)$.

Then $f(K) \subseteq f(\bigcup_{i=1}^n f^{-1}(U_i)) = \bigcup_{i=1}^n f(f^{-1}(U_i)) \subseteq \bigcup_{i=1}^n U_i$, where we use that images preserve set inclusions (check!), and Exercises 8 and 9 in **??**. Thus, $\{U_1, \ldots, U_n\}$ is a finite subcover for $f(K)$ and $f(K)$ is compact. □

As you can see, a lot of results from introductory real analysis or calculus have extensions to a more general topological setting. However, topology is a large field with many powerful tools that we do not have time to cover. The final result in this section is an important result in topology.

Definition 4.24 *A topological space $(X, \mathcal{T})$ is* normal *if the following hold:*

(i) For all $x \in X$, $\{x\}$ is closed.

(ii) For all (non-empty) disjoint closed sets $F_1, F_2 \subseteq X$ there exist disjoint open sets U_1, U_2 such that $F_1 \subseteq U_1$ and $F_2 \subseteq U_2$.

Example 4.25

- *Any metric space (X, d) is normal.*
- *Let $(X, \mathcal{T})$ be Hausdorff and compact. Then X is normal.*
- *If $(X, \mathcal{T})$ is normal, then it is Hausdorff.*

Theorem 4.26 (Urysohn's Lemma) *Let $(X, \mathcal{T})$ be normal and $F_1, F_2 \subseteq X$ be closed with $F_1 \cap F_2 = \emptyset$. Then there exists a continuous function $f\colon X \to [0, 1]$ such that $f(F_1) = \{0\}$ and $f(F_2) = \{1\}$. (Here the topology on $[0, 1]$ is the relative topology inherited from the usual metric topology on $\mathbb{R}$.)*

Proof omitted. See [Run05, Theorem 4.1.2].

4.4 Exercises

1. Let $(X, \mathcal{T})$ be a topological space. Prove that $A \subseteq X$ is closed if and only if $\overline{A} = A$.
2. Let $(X, \mathcal{T})$ be a topological space and $\{A_i\}_{i\in I}$ be a collection of subsets of X. Show that
$$\bigcup_{i\in I} \overline{A_i} \subseteq \overline{\bigcup_{i\in I} A_i}.$$
Show that if the collection is finite, the two sets are equal.
3. Let $(X, \mathcal{T})$ be a topological space and $\{A_i\}_{i\in I}$ be a collection of subsets of X. Prove that
$$\overline{\bigcap_{i\in I} A_i} \subseteq \bigcap_{i\in I} \overline{A_i}.$$
Find a counterexample that shows that equality is not necessarily the case.
4. Let $(X, \mathcal{T})$ be a topological space and $A \subseteq X$ be dense. Show that if $A \subseteq B \subseteq X$, then B is dense as well.
5. Let $(X, \mathcal{T})$ be a Hausdorff topological space. Show that the singleton $\{x\}$ is closed for all $x \in X$. Hint: Show that the complement is open.
6. Let $(X, \mathcal{T}_X)$, $(Y, \mathcal{T}_Y)$ and $(Z, \mathcal{T}_Z)$ be topological spaces and let $f\colon X \to Y$, $g\colon Y \to Z$ be continuous. Show that $g \circ f\colon X \to Z$ is continuous as well.
7. Let (X, d) be a metric space and $K \subset X$ compact. Show that for all $\epsilon > 0$ there exists $\{x_1, x_2, \ldots, x_n\} \subseteq K$ such that for all $y \in K$ we have $d(y, x_i) < \epsilon$ for some $i = 1, \ldots, n$.

4.5 References

The content in this section comes mostly from [Run05], with additional examples inspired by [Mar19].

5 Linear Algebra

5.1 Vector spaces and subspaces

Let V be a set and let $\mathbb{F}$ be a field.

Definition 5.1 *We call V a* vector space *if the following hold:*
Addition:

(A) Commutativity in addition: $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$ for all $\mathbf{u},\mathbf{v}\in V$

(B) Associativity in addition: $\mathbf{u}+(\mathbf{v}+\mathbf{w})=(\mathbf{u}+\mathbf{v})+\mathbf{w}$ for all $\mathbf{u},\mathbf{v},\mathbf{w}\in V$

(C) Existence of a neutral element, addition: There exists a vector $\mathbf{0}$ such that for any $\mathbf{v}\in V$, $\mathbf{0}+\mathbf{v}=\mathbf{v}$

(D) Additive inverse: For every $\mathbf{v}\in V$, there exists another vector, which we denote $-\mathbf{v}$, such that $\mathbf{v}+(-\mathbf{v})=\mathbf{0}$.

Multiplication by a scalar:

(E) Existence of a neutral element, multiplication: For any $\mathbf{v}\in V$, $1\times\mathbf{v}=\mathbf{v}$

(F) Associativity in multiplication: Let $\alpha,\beta\in\mathbb{F}$. For any $\mathbf{v}\in V$, $(\alpha\beta)\mathbf{v}=\alpha(\beta\mathbf{v})$

Associativity:

(G) Let $\alpha\in\mathbb{F},\mathbf{u},\mathbf{v}\in V$. $\alpha(\mathbf{u}+\mathbf{v})=\alpha\mathbf{u}+\alpha\mathbf{v}$.

(H) Let $\alpha,\beta\in\mathbb{F},\mathbf{v}\in V$. $(\alpha+\beta)\mathbf{v}=\alpha\mathbf{v}+\beta\mathbf{v}$.

Elements of a vector space are called vectors. Most often we will assume $\mathbb{F}=\mathbb{C}$ or $\mathbb{R}$.

Example 5.2 *Examples of vector spaces are:*

- *$\mathbb{R}^n$ as a $\mathbb{R}$-vector space and $\mathbb{C}^n$ as a $\mathbb{C}$-vector space,*
- *$C(\mathbb{R};\mathbb{R})$, continuous functions from $\mathbb{R}$ to $\mathbb{R}$,*
- *$M_{m\times n}$ (matrices of size $m\times n$ with entries in $\mathbb{F}$) as an $\mathbb{F}$-vector space,*
- *$\mathbb{P}_n$ (polynomials of degree n and coefficients in $\mathbb{F}$, $p(x)=a_0+a_1x+\ldots+a_nx^n$) as an $\mathbb{F}$-vector space.*

Proposition 5.3 *Let $\mathbf{v}\in V$, where V is a vector space.*

(i) $0\mathbf{v}=\mathbf{0}$.

(ii $-\mathbf{v}=(-1)\times\mathbf{v}$.

Proof. (i) Using the distributive property:

$$0\mathbf{v}=(0+0)\mathbf{v}=0\mathbf{v}+0\mathbf{v}$$

Add the additive inverse of $0\mathbf{v}$ to both sides. we have $\mathbf{0}=0\mathbf{v}$.

(ii) Our goal is to show that $(-1)\times\mathbf{v}$ is the additive inverse of $\mathbf{v}$. We show this as follows:

$$\mathbf{v}+(-1)\times\mathbf{v}=\mathbf{v}\times(1+(-1))=\mathbf{v}\times 0=\mathbf{0}.$$

□

Definition 5.4 *A subset U of V is called a* subspace *of V if U is also a vector space (using the same addition and scalar multiplication as on V).*

Proposition 5.5 *A subset U of V is a subspace of V if and only if U satisfies the following three conditions:*

1. $\mathbf{0} \in U$
2. *Closed under addition:* $\mathbf{u}, \mathbf{v} \in U$ *implies* $\mathbf{u} + \mathbf{v} \in U$
3. *Closed under scalar multiplication:* $\alpha \in \mathbb{F}$ *and* $\mathbf{u} \in U$ *implies* $\alpha\mathbf{u} \in U$

Proof. $\Rightarrow$ If U is a subspace of V, then U satisfies these 3 properties by Definition 5.1.

$\Leftarrow$ Suppose U satisfies the given 3 conditions. Then for any $\mathbf{v} \in U$, there must exist $-\mathbf{v} \in U$ by property 3, since $-\mathbf{v} = (-1) \times \mathbf{v}$ by Proposition 5.3 (property D). Property 1 assures property C. Properties 2 and 3, and the fact that $U \subseteq V$, assure the remaining properties hold. □

Proposition 5.6 *Let V be a vector space and let $U_1, U_2 \subseteq V$ be subspaces. Then $U_1 \cap U_2$ is also a subspace of V.*

Proof. We use the characterization in Proposition 5.5. First, since $\mathbf{0} \in U_1$ and $\mathbf{0} \in U_2$, we have $\mathbf{0} \in U_1 \cap U_2$. Second, for $\mathbf{u}, \mathbf{v} \in U_1 \cap U_2$, since in particular $\mathbf{u}, \mathbf{v} \in U_1$ and $\mathbf{u}, \mathbf{v} \in U_2$ and U_1, U_2 are subspaces, $\mathbf{u} + \mathbf{v} \in U_1$ and $\mathbf{u} + \mathbf{v} \in U_2$. Thus, $\mathbf{u} + \mathbf{v} \in U_1 \cap U_2$. Similarly, one shows $\alpha\mathbf{u} \in U_1 \cap U_2$ for $\alpha \in \mathbb{F}$. □

On the contrary the union of two subspaces is not a subspace in general (see exercise). However, the next definition introduces the smallest subspace containing the union.

Definition 5.7 *Suppose $U_1, ..., U_m$ are subsets of V. The sum of $U_1, ..., U_m$, denoted $U_1 + ... + U_m$, is the set of all possible sums of elements of $U_1, ..., U_m$. More precisely,*

$$U_1 + ... + U_m = \{\mathbf{u}_1 + ... + \mathbf{u}_m : \mathbf{u}_1 \in U_1, ..., \mathbf{u}_m \in U_m\}$$

Proposition 5.8 *Suppose $U_1, ..., U_m$ are subspaces of V. Then $U_1 + ... + U_m$ is the smallest subspace of V containing $U_1, ..., U_m$.*

This follows, since on the one hand clearly $U_1 + \ldots + U_m$ clearly contains $\cup_{i=1}^m U_i$ (to see that $\mathbf{u}_i \in U_i$ is in the sum just set all the other summands $\mathbf{0}$). On the other hand any vector space that contains the union needs to contain all sums of the above form otherwise we do not have a vector space.

5.1.1 Exercises

1. Suppose that $\alpha \in \mathbb{F}, \mathbf{v} \in V$, and $\alpha\mathbf{v} = \mathbf{0}$. Prove that $a = 0$ or $v = 0$.
2. Show that $-(-\mathbf{v}) = \mathbf{v}$ for $\mathbf{v} \in V$.
3. Let U_1 and U_2 be subspaces of a vector space V. Prove that $U_1 \cup U_2$ is a subspace of V if and only if $U_1 \subseteq U_2$ or $U_2 \subseteq U_1$.
4. Give an example of a nonempty subset U of $\mathbb{R}^2$ such that U is closed under scalar multiplication, but U is not a subspace of $\mathbb{R}$.

5.2 Linear (in)dependence and bases

For the following let V be a fixed $\mathbb{F}$-vector space.

Definition 5.9 *A linear combination of vectors $\mathbf{v}_1, ..., \mathbf{v}_n$ in V is a vector of the form*

$$\alpha_1\mathbf{v}_1 + ... + \alpha_n\mathbf{v}_n = \sum_{k=1}^{n} \alpha_k\mathbf{v}_k$$

where $\alpha_1, ..., \alpha_m \in \mathbb{F}$.

Definition 5.10 *The set of all linear combinations of a list of vectors* $\mathbf{v}_1, ..., \mathbf{v}_n$ *in* V *is called the* span *of* $\mathbf{v}_1, ..., \mathbf{v}_n$*, denoted* $\text{span}\{\mathbf{v}_1, ..., \mathbf{v}_n\}$*. In other words,*

$$\text{span}\{\mathbf{v}_1, ..., \mathbf{v}_n\} = \{\alpha_1\mathbf{v}_1 + ... + \alpha_m\mathbf{v}_n : \alpha_1, ..., \alpha_n \in \mathbb{F}\}$$

The span of the empty list is defined to be $\{\mathbf{0}\}$.

Definition 5.11 *A system of vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *is called a basis (for the vector space* V *) if any vector* $\mathbf{v} \in V$ *admits a unique representation as a linear combination*

$$\mathbf{v} = \alpha_1\mathbf{v}_1 + \ldots + \alpha_n\mathbf{v}_n = \sum_{k=1}^{n} \alpha_k\mathbf{v}_k.$$

In undergrad, you likely thought about this as: the equation $\mathbf{v} = \alpha_1\mathbf{v}_1 + \ldots + \alpha_n\mathbf{v}_n$, where the α_i are unknown, has a unique solution.

Example 5.12

- *For* $\mathbb{F}^n$*,* $e_1 = (1, 0, \ldots, 0)$*,* $e_2 = (0, 1, 0, \ldots, 0)$*,* $\ldots$*,* $e_n = (0, \ldots, 0, 1)$ *is a basis*
- *The monomials* $1, x, x^2, \ldots, x^n$ *form a basis for* $\mathbb{P}_n$*.*

A basis can be characterized by two important properties.

Definition 5.13 *A system of vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *in* V *is called* linearly independent *if* $\sum_{i=1}^{n} \alpha_i\mathbf{v}_i = \mathbf{0}$ *implies* $\alpha_i = 0$ *for all* $i = 1, \ldots, n$*. Otherwise, we call the system* linearly dependent*.*

Linear combinations $\alpha_1\mathbf{v}_1 + ... + \alpha_n\mathbf{v}_n$ such that $\alpha_k = 0$ for every k are called trivial.

Definition 5.14 *A system of vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *in* V *is called* spanning *if any vector in* V *can be written as a linear combination of* $\mathbf{v}_1, \ldots, \mathbf{v}_n$*. In other words,*

$$V = \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}.$$

Such a system is also often called generating or complete. The next proposition relates spanning and linearly independent to a basis.

Proposition 5.15 *A system of vectors* $\mathbf{v}_1, \ldots \mathbf{v}_n \in V$ *is a basis if and only if it is linearly independent and spanning.*

Proof. Suppose that $\mathbf{v}_1, \ldots \mathbf{v}_n \in V$ is a basis. Then, by definition every vector admits a unique representation as a linear combination of $\mathbf{v}_1, \ldots \mathbf{v}_n$. In particular, $\mathbf{v}_1, \ldots \mathbf{v}_n$ is spanning. Also, since the linear combinations are unique and setting all coefficients 0 is one linear combination that adds up to $\mathbf{0}$, we see that it is the only one. Hence, $\mathbf{v}_1, \ldots \mathbf{v}_n$ is linearly independent.

Conversely, suppose $\mathbf{v}_1, \ldots \mathbf{v}_n$ is linearly independent and spanning and let $\mathbf{v} \in V$. Then, since the system is spanning there exist coefficients $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ such that $\sum_{i=1}^{n} \alpha_i\mathbf{v}_i = \mathbf{v}$. We need to show it is unique. Suppose there exist $\beta_1, \ldots, \beta_n \in \mathbb{F}$ such that $\sum_{i=1}^{n} \beta_i\mathbf{v}_i = \mathbf{v}$. Then

$$\mathbf{0} = \mathbf{v} - \mathbf{v} = \sum_{i=1}^{n} (\alpha_i - \beta_i)\mathbf{v}_i.$$

By linear independence this linear combination is trivial, meaning $\alpha_i - \beta_i = 0$ for all $i = 1, \ldots, n$ or equivalently $\alpha_i = \beta_i$. Thus, the linear combination is unique and $\mathbf{v}_1, \ldots \mathbf{v}_n$ forms a basis. □

The next proposition shows that a basis can be thought of as a optimal spanning set in some sense.

Proposition 5.16 *Let* $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ *be spanning. Then* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *contains a basis.*

Proof. Since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is spanning, if the system is also linearly independent, we are done by Proposition 5.15. Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is linearly dependent. Then, there exists coefficients $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ with some $\alpha_i \neq 0$) such that $\sum_{i=1}^n \alpha_i \mathbf{v}_i = \mathbf{0}$. Rearranging leads to $\mathbf{v}_i = \frac{1}{\alpha_i} \sum_{j=1, j\neq i}^n \alpha_j \mathbf{v}_j$. Thus, $\mathbf{v}_i \in \operatorname{span}\{\mathbf{v}_j \colon j = 1, \ldots, n \text{ and } j \neq i\}$ and the latter system of vectors is still spanning. To see this take $\mathbf{v} \in V$. Then since the original system is spanning there exist coefficients such that $\mathbf{v} = \sum_{k=1}^n \beta_k \mathbf{v}_k$. Hence we obtain

$$\mathbf{v} = \sum_{k=1}^n \beta_k \mathbf{v}_k = \beta_i \mathbf{v}_i + \sum_{k=1, k\neq i}^n \beta_k \mathbf{v}_k = \sum_{k=1, k\neq i}^n \left(\beta_k + \frac{\alpha_k}{\alpha_i}\right) \mathbf{v}_k.$$

We can continue this procedure until we arrive at a linearly independent spanning set. □

Next we will describe finite-dimensional vector spaces and show that any such vector space has a basis.

Definition 5.17 *An $\mathbb{F}$-vector space V is called* finite dimensional *if there exists a finite list of vectors that span it, i.e. there exist $n \in \mathbb{N}$ and $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ such that $V = \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Otherwise, we call V* infinite dimensional.

Example 5.18

- *$\mathbb{F}^n$, $M_{m\times n}$, $\mathbb{P}_n$ are examples of finite dimensional vector spaces*
- *The $\mathbb{F}$-vector space $\mathbb{P} = \{\sum_{i=1}^n \alpha_i x^i \ : \ n \in \mathbb{N}, \alpha_i \in \mathbb{F}, i = 1, \ldots, n\}$ is infinite dimensional. Why? Suppose it was finite dimensional. Then there exists a finitely many polynomials $p_1, \ldots, p_n$ which span $\mathbb{P}$. Let N be the maximum degree of the polynomials $p_1, \ldots, p_n$. Then $x^{N+1} \notin \operatorname{span}\{p_1, \ldots, p_n\}$ - contradiction.*

Using Proposition 5.16 we immediately obtain the following result.

Corollary 5.19 *Every finite dimensional vector space has a basis.*

This can also be extended to infinite dimensional vector spaces, i.e. when we do not assume that there exists a finite spanning set. However, this relies on the Axiom of Choice and is beyond the scope of this course.

Proposition 5.20 *Every linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis of the vector space.*

Proof. If $\mathbf{u}_1, \ldots, \mathbf{u}_m$ is a linearly independent list in a vector space U, we can extend it to span V by adding in the basis of V, $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Then $\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}_1, \ldots, \mathbf{v}_n$ spans V and by Proposition 5.16 it can be reduced to a basis for V, which will contain all the $\mathbf{u}$'s since they are linearly independent. □

Lastly, we introduce the dimension of a vector space.

Proposition 5.21 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m$ be a basis for V. Then $m = n$.*

The proof is omitted, see [Axl15, Chapter 2, Proposition 2.35]. It relies on the fact that the number of elements in linearly independent systems are always less than or equal to the number of elements in spanning systems.

Definition 5.22 *Let V be a finite dimensional $\mathbb{F}$-vector space. The number of elements in a basis of V is called the* dimension *of V and is denoted* $\dim(V)$.

By the previous definition, the notion of dimension is well-defined.

Example 5.23

- $\dim(\mathbb{F}^n) = n$
- $\dim(\mathbb{P}_n) = n + 1$
- $\dim\{\mathbf{0}\} = 0$ *(the only linearly independent set in $\{\mathbf{0}\}$ is the empty set)*

5.2.1 Exercises

1. Suppose $\mathbf{v}_1, ..., \mathbf{v}_m$ is linearly independent in V and $\mathbf{w} \in V$. Prove that if $\mathbf{v}_1 + \mathbf{w}, ..., \mathbf{v}_m + \mathbf{w}$ is linearly dependent, then $\mathbf{w} \in \text{span}(\mathbf{v}_1, ..., \mathbf{v}_m)$.
2. Suppose that $\mathbf{v}_1, ..., \mathbf{v}_m$ is linearly independent in V and $\mathbf{w} \in V$. Show that $\mathbf{v}_1, ..., \mathbf{v}_m, \mathbf{w}$ is linearly independent if and only if
$$\mathbf{w} \notin \text{span}\{\mathbf{v}_1, ..., \mathbf{v}_m\}$$

5.3 Linear maps

Throughout we assume that U, V, and W are $\mathbb{F}$-vector spaces.

Definition 5.24 *A map from a vector space U to a vector space V is* linear *if*
$$T(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha T(\mathbf{u}) + \beta T(\mathbf{v}) \quad \text{for any } \mathbf{u}, \mathbf{v} \in V,\ \alpha, \beta \in \mathbb{F}$$

Let's denote the set of all linear maps from vector space U to vector space V by $\mathcal{L}(U, V)$.

Example 5.25 (Zero map) *The map that maps everything to zero, i.e. $0 : U \to V$ such that $0\mathbf{v} = \mathbf{0}$, is linear.*

Example 5.26 (Identity map) *The map $I : V \to V$ such that $I\mathbf{v} = \mathbf{v}$ for every $\mathbf{v} \in V$ is called the identity map.*

Example 5.27 (Differentiation is a linear map) *Let $D \in \mathcal{L}(\mathbb{P}(\mathbb{R}), \mathbb{P}(\mathbb{R}))$, (i.e. D is a linear map from the polynomials on $\mathbb{R}$ to the polynomials on $\mathbb{R}$), defined as $Dp = p'$. The fact that such a map is linear follows from basic facts about derivatives, i.e. $\frac{d}{dx}(\alpha f(x) + \beta g(x)) = \alpha f'(x) + \beta g'(x)$.*

Other examples: integration, rotation of vectors, reflection of vectors.

Theorem 5.28 ([Axl15, Theorem 3.5]) *Suppose $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is a basis for U and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis for V. Then there exists a unique linear map $T : U \to V$ such that $T\mathbf{u}_j = \mathbf{v}_j$ for $j = 1, \ldots, n$.*

The proof can be found in the book.

Theorem 5.29 *Let $S, T \in \mathcal{L}(U, V)$ and $\alpha \in \mathbb{F}$. $\mathcal{L}(U, V)$ is a vector space with addition defined as the sum $S + T$ and multiplication as the product αT.*

The proof follows from properties of linear maps and vector spaces. Note that the additive identity is the zero map.

Lemma 5.30 *Let $T \in \mathcal{L}(U, V)$. Then $T(\mathbf{0}) = \mathbf{0}$.*

Proof. By linearity, $T(\mathbf{0}) = T(\mathbf{0} + \mathbf{0}) = T(\mathbf{0}) + T(\mathbf{0})$. Add $-T(\mathbf{0})$ to both sides to obtain the result. □

Definition 5.31 *Let $T : U \to V$ be a linear transformation. We define the following important subspaces:*

- Kernel or null space*:* $\text{null}\, T = \{\mathbf{u} \in U : T\mathbf{u} = 0\}$
- Range*:* $\text{range}\, T = \{\mathbf{v} \in V : \exists \mathbf{u} \in U \text{ such that } \mathbf{v} = T\mathbf{u}\}$

The dimensions of these spaces are often called the following:

- Nullity*:* $\text{nullity}(T) = \dim(\text{null}(T))$
- Rank*:* $\text{rank}(T) = \dim(\text{range}(T))$

Proposition 5.32 *Let $T : U \to V$. The null space of T is a subspace of U and the range of T is a subspace of V.*

Proof. First, the null space. By Lemma 5.30, $T(\mathbf{0}) = \mathbf{0}$, so $\mathbf{0}$ is in the null space. Next, show it is closed under addition. Let $\mathbf{u}, \mathbf{v} \in \operatorname{null} T$. Then $T(\mathbf{u}+\mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v}) = \mathbf{0} + \mathbf{0} = \mathbf{0}$. Finally, it is closed under scalar multiplication since if $\mathbf{v} \in \operatorname{null} T$ and $\alpha \in \mathbb{F}$, then $T(\alpha\mathbf{v}) = \alpha\mathbf{0} = \mathbf{0}$.

Second, the range. Again by Lemma 5.30, there exists an element that maps to 0 (namely 0 itself), so $0 \in \operatorname{range} T$. Next, suppose $\mathbf{v}_1, \mathbf{v}_2 \in \operatorname{range} T$. Then $\exists \mathbf{u}_1, \mathbf{u}_2 \in U$ such that $T(\mathbf{u}_1) = \mathbf{v}_1$ and $T(\mathbf{u}_2) = \mathbf{v}_2$. Then $T(\mathbf{u}_1 + \mathbf{u}_2) = T(\mathbf{u}_1) + T(\mathbf{u}_2) = \mathbf{v}_1 + \mathbf{v}_2$ so $\mathbf{v}_1 + \mathbf{v}_2 \in \operatorname{range} T$. Finally, let $\mathbf{v} \in \operatorname{range} T$ and $\alpha \in \mathbb{F}$. Then $\exists \mathbf{u} \in U$ such that $T(\mathbf{u}) = \mathbf{v}$ and $T(\alpha\mathbf{u}) = \alpha\mathbf{v}$ so $\alpha\mathbf{v} \in \operatorname{range} T$. □

Example 5.33 *Zero map from a vector space U to a vector space V:*

- *The null space is U.*
- *The range is $\{\mathbf{0}\}$.*

Differentiation map from $\mathbb{P}(\mathbb{R})$ to $\mathbb{P}(\mathbb{R})$:

- *The null space is the set of all constant functions.*
- *The range is all of $\mathbb{P}(\mathbb{R})$.*

Definition 5.34 (Injective and surjective) *Let $T : U \to V$. T is* injective *if $T\mathbf{u} = T\mathbf{v}$ implies $\mathbf{u} = \mathbf{v}$ and T is* surjective *if $\forall \mathbf{u} \in U$, $\exists \mathbf{v} \in V$ such that $\mathbf{v} = T\mathbf{u}$, i.e. if $\operatorname{range} T = V$.*

Theorem 5.35 *$T \in \mathcal{L}(U, v)$ is injective if and only if $\operatorname{null} T = \{\mathbf{0}\}$.*

Proof. ($\Rightarrow$) Suppose T is injective. By Lemma 5.30, we know that $\mathbf{0}$ is in the null space of T, i.e. $T(\mathbf{0}) = \mathbf{0}$. Suppose in order to derive a contradiction that $\exists \mathbf{v} \neq \mathbf{0} \in \operatorname{null} T$. Then $T(\mathbf{v}) = \mathbf{0} = T(\mathbf{0})$, and by injectivity, $\mathbf{v} = 0$ Therefore $\operatorname{null} T = \{\mathbf{0}\}$.

($\Leftarrow$) Suppose $\operatorname{null} T = 0$. Let $T\mathbf{u} = T\mathbf{v}$; we want to show $\mathbf{v} = \mathbf{u}$. $T\mathbf{u} = T\mathbf{v}$ implies $T(\mathbf{u} - \mathbf{v}) = \mathbf{0}$, which implies $\mathbf{u} - \mathbf{v} \in \operatorname{null} T$. But $\operatorname{null} T = \{\mathbf{0}\}$, so then $\mathbf{u} - \mathbf{v} = \mathbf{0}$, which gives $\mathbf{u} = \mathbf{v}$. □

Theorem 5.36 (Rank Nullity Theorem) *Let $T : U \to V$ be a linear transformation, where U and V are finite-dimensional vector spaces. Then*

$$\operatorname{rank} T + \operatorname{nullity} T = \dim U.$$

Proof. Let $\mathbf{u}_1, \ldots, \mathbf{u}_m$ be a basis for $\operatorname{null} T$. We can extend it to a basis for U by Proposition 5.20. Suppose we add $\mathbf{w}_1, \ldots, \mathbf{w}_n$ to achieve the basis. Then $\operatorname{nullity} T = \dim \operatorname{null} T = m$ and $\dim U = m + n$. We need to show that $\operatorname{rank} T = \dim \operatorname{range} T = n$.

We show that $T\mathbf{w}_1, \ldots, T\mathbf{w}_n$ is a basis for $\operatorname{range} T$. Let $\mathbf{u} \in U$. Then $\exists, \alpha_i, \beta_j \in \mathbb{F}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$ such that

$$\mathbf{u} = \alpha_1\mathbf{u}_1 + \cdots + \alpha_m\mathbf{u}_m + \beta_1\mathbf{w}_1 + \cdots + \beta_n\mathbf{w}_n.$$

Apply T:

$$\begin{aligned} T\mathbf{u} &= \alpha_1 T\mathbf{u}_1 + \cdots + \alpha_m T\mathbf{u}_m + \beta_1 T\mathbf{w}_1 + \cdots + \beta_n T\mathbf{w}_n \\ &= \beta_1 T\mathbf{w}_1 + \cdots + \beta_n T\mathbf{w}_n \qquad \text{(since the } \mathbf{u} \text{ are in } \operatorname{null} T) \end{aligned}$$

Thus $T\mathbf{w}_1, \ldots, T\mathbf{w}_n$ spans $\operatorname{range} T$, so $\operatorname{range} T$ is finite-dimensional. Also, $T\mathbf{w}_1, \ldots, T\mathbf{w}_n$ are linearly independent:

To show this, let $c_1, \ldots, c_n \in \mathbb{F}$. Then

$$\begin{aligned} 0 &= c_1 T\mathbf{w}_1 + \cdots + c_n T\mathbf{w}_n \\ &= T(c_1\mathbf{w}_1 + \cdots + c_n\mathbf{w}_n), \end{aligned}$$

i.e. $c_1\mathbf{w}_1 + \cdots + c_n\mathbf{w}_n \in \operatorname{null} T$, so since $\mathbf{u}_1, \ldots, \mathbf{u}_m$ is a basis for $\operatorname{null} T$, there exist $d_1, \ldots, d_n \in \mathbb{F}$ such that

$$c_1\mathbf{w}_1 + \cdots + c_n\mathbf{w}_n = d_1\mathbf{u}_1 + \cdots + d_m\mathbf{u}_m.$$

Since $\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n$ is a basis for U it is linearly independent, and so $c_1 = \cdots = c_n = d_1 = \cdots = d_m = 0$. Since all the c's are zero, $T\mathbf{w}_1, \ldots, T\mathbf{w}_n$ is linearly independent, and thus a basis for $\operatorname{range} T$. Thus $\operatorname{rank} T = \dim \operatorname{range} T = n$ as required. □

Definition 5.37 (Product of linear maps) *Let $S \in \mathcal{L}(U, V)$ and $T \in \mathcal{L}(V, W)$. We define the product $ST \in \mathcal{L}(U, W)$ for $\mathbf{u} \in U$ as $ST(\mathbf{u}) = S(T(\mathbf{u}))$.*

Definition 5.38 *A linear map $T : U \to V$ is* invertible *if there exists a linear map $S : V \to U$ such that ST is the identity map on U and TS is the identity map on V. Such a map S is called the* inverse *of T.*

If T is invertible, we denote the inverse by T^{-1}. This is justified by the fact that the inverse is unique:

Proposition 5.39 *Any invertible linear map has a unique inverse.*

Proof. Let $T : U \to V$ be invertible. Suppose it has two inverses, i.e. there exists S_1, S_2, both mapping from V to U, such that S_1T, S_2T are identity maps on U and TS_1 and TS_2 are identity maps on V. Then

$$S_1 = S_1TS_2 = S_2,$$

so S_1 and S_2 are the same. □

Theorem 5.40 ([Axl15, Theorem 3.56]) *A linear map is invertible if and only if it is injective and surjective.*

See proof in the book, [Axl15, p.81].

Definition 5.41 *An invertible linear map is called an* isomorphism*. If there exists an isomorphism from one vector space to another, we say that the vector spaces are* isomorphic*.*

Theorem 5.42 *Two finite-dimensional vector spaces over $\mathbb{F}$ are isomorphic if and only if they have the same dimension.*

Proof. ($\Rightarrow$) Let U and V be finite-dimensional isomorphic vector spaces. Then there exists an invertible map $T : U \to V$. By Theorem 5.40, T is both injective and surjective, so $\operatorname{null} T = \{\mathbf{0}\}$ and $\operatorname{range} T = V$. Then by the rank nullity theorem,

$$\dim \operatorname{range} T + \dim \operatorname{null} T = \dim U \implies \dim V + \dim\{\mathbf{0}\} = \dim U \implies \dim V = \dim U$$

($\Leftarrow$) Let U and V be finite-dimensional vector spaces with the same dimension, with bases $\mathbf{u}_1, \ldots, \mathbf{u}_n$ and $\mathbf{v}_1, \ldots, \mathbf{v}_n$, respectively. Define the map $T : U \to V$ using Theorem 5.28:

$$T(c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n) = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n,$$

where $c_i \in \mathbb{F}$, $i = 1, \ldots, n$. Since the $\mathbf{v}$ span V, the map is surjective, and since they are linearly independent, we have $T = \{\mathbf{0}\}$. Thus T is both surjective and injective, and therefore an isomorphism by Theorem 5.40. □

Definition 5.43 *A linear map from a vector space to itself is called an* operator*.*

5.3.1 Exercises

1. Let $T \in \mathcal{L}(\mathbb{P}(\mathbb{R}), \mathbb{P}(\mathbb{R}))$ be the map $T(p(x)) = x^2p(x)$ (multiplication by x^2).
   (i) Show that T is linear.
   (ii) Find the null space and range of T.
2. [Axl15, 3.B Exercise 22] Let U and V be finite-dimensional vector spaces and $S \in \mathcal{L}(V, W)$ and $T \in \mathcal{L}(U, V)$. Show that
$$\dim \operatorname{null} ST \leq \dim \operatorname{null} S + \dim \operatorname{null} T$$

5.4 Linear maps and matrices

Example 5.44 *Let $A \in M_{m\times n}$ be a fixed matrix. Then, we can define a linear map $T_A\colon \mathbb{F}^n \to \mathbb{F}^m$ via $T_A(\mathbf{v}) = A\mathbf{v}$, where we recall matrix vector multiplication $(A\mathbf{v})_i = \sum_{k=1}^n A_{ik}v_k$ for $i = 1, \dots, m$.*

Next we will see that we can use matrices to represent linear maps between finite dimensional vector spaces.

Definition 5.45 *Let $T \in \mathcal{L}(U, V)$ where U and V are vector spaces. Let $\mathbf{u}_1, \dots, \mathbf{u}_n$ and $\mathbf{v}_1, \dots, \mathbf{v}_m$ be bases for U and V respectively. The matrix of T with respect to these bases is the $m \times n$ matrix $\mathcal{M}(T)$ with entries A_{ij}, $i = 1, \dots, m$, $j = 1, \dots, n$ defined by*

$$T\mathbf{u}_k = A_{1k}\mathbf{v}_1 + \cdots + A_{mk}\mathbf{v}_m$$

i.e. the kth column of A is the scalars needed to write $T\mathbf{u}_k$ as a linear combination of the basis of V:

$$T\mathbf{u}_k = \sum_{i=1}^m A_{ik}\mathbf{v}_i$$

Note that since a linear map $T \in \mathcal{L}(U, V)$ is uniquely determined by its image on a basis of U, we see that once we pick basis of U and V its matrix representation is uniquely determined.

Example 5.46 *Let $D \in \mathcal{L}(\mathbb{P}_4(\mathbb{R}), \mathbb{P}_3(\mathbb{R}))$ be the differentiation map, $Dp = p'$. Find the matrix of D with respect to the standard bases of $\mathbb{P}_3(\mathbb{R})$ and $\mathbb{P}_4(\mathbb{R})$.*

Standard basis: $1, x, x^2, x^3, (x^4)$
$T(u_1) = (1)' = 0$
$T(u_2) = (x)' = 1$
$T(u_3) = (x^2)' = 2x$
$T(u_4) = (x^3)' = 3x^2$
$T(u_5) = (x^4)' = 4x^3$

The matrix is:

$$\mathcal{M}(D) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

Now observe that if we choose bases $\mathbf{u}_1, \dots, \mathbf{u}_n$ and $\mathbf{v}_1, \dots, \mathbf{v}_m$ for U, V and represent $T \in \mathcal{L}(U, V)$ as a matrix $\mathcal{M}(T)$, then the corresponding map can be obtained by just working with the coordinates of vectors in U, V with respect to the chosen basis. In particular, if $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{u}_i$, then the coordinates of $T(\mathbf{u})$ with respect to $\mathbf{v}_1, \dots, \mathbf{v}_m$ can be obtained by the matrix vector multiplication $\mathcal{M}(T)\boldsymbol{\alpha}$, where $\boldsymbol{\alpha}$ is the $n \times 1$ matrix with entries α_i. Hence, after a choice of basis $T \in \mathcal{L}(U, V)$ is in a 1-1 correspondence with maps $T_{\mathcal{M}(T)}\colon \mathbb{F}^n \to F^m$.

Example 5.47 *If we want to find the derivative of $p = x^4 + 12x^3 - 5x^2 + 7$ with respect to the standard monomial basis of $\mathbb{P}_4(\mathbb{R})$, we use $\mathcal{M}(D)$ from the previous example to obtain*

$$\mathcal{M}(D)\boldsymbol{\alpha} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} 7 \\ 0 \\ -5 \\ 12 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -10 \\ 36 \\ 4 \end{pmatrix}.$$

Thus, translating back into the monomial basis of $\mathbb{P}_3(\mathbb{R})$ gives $D(p) = -10x + 36x^2 + 4x^3$.

Looking at matrices as representations of linear maps gives us an intuitive explanation for why we do matrix multiplication the way we do! In fact, we want matrix multiplication to represent composition of linear

maps. Let $T : U \to V$ and $S : V \to W$, where T, S are linear maps and U, V, W are vector spaces with bases $\mathbf{u}_1, \ldots, \mathbf{u}_n$, $\mathbf{v}_1, \ldots, \mathbf{v}_m$, and $\mathbf{w}_1, \ldots, \mathbf{w}_p$. If we want to have

$$\mathcal{M}(ST) := \mathcal{M}(S)\mathcal{M}(T),$$

how would we need to define matrix multiplication?
Let $A = \mathcal{M}(S)$ and $B = \mathcal{M}(T)$. Then using Definition 5.45

$$(ST)\mathbf{u}_k = S(T(\mathbf{u}_k)) = S\left(\sum_{i=1}^{m} B_{ik}\mathbf{v}_i\right) = \sum_{i=1}^{m} B_{ik}S(\mathbf{v}_i) = \sum_{i=1}^{m} B_{ik}\sum_{j=1}^{p} A_{ji}\mathbf{w}_j = \sum_{j=1}^{p}(\sum_{i=1}^{m} A_{ji}B_{ik})\mathbf{w}_j.$$

Thus the jk entry of $\mathcal{ST}$ is given by $\sum_{i=1}^{m} A_{ji}B_{ik}$, leading to an $m \times p$ matrix. This recovers the matrix multiplication learned in undergrad!
Similarly, we also see that $\mathcal{M}(S + T) = \mathcal{M}(S) + \mathcal{M}(T)$ when $S, T \in \mathcal{L}(U, V)$ and $\mathcal{M}(\alpha T) = \alpha\mathcal{M}(T)$ for $\alpha \in \mathbb{F}$.

Another useful application of matrices is solving systems of linear equations. If we have a system of m linear equations with n unknowns $x_1, \ldots, x_n$ and coeffcients in $\mathbb{F}$, we can write this the following way:

$$\begin{aligned} A_{11}x_1 + A_{12}x_2 + \ldots + A_{1n}x_n &= b_1, \\ A_{21}x_1 + A_{22}x_2 + \ldots + A_{2n}x_n &= b_2, \\ &\vdots \\ A_{m1}x_1 + A_{m2}x_2 + \ldots + A_{mn}x_n &= b_m. \end{aligned}$$

Alternatively, we can represent this using matrix vector multiplication, leading to $A\mathbf{x} = \mathbf{b}$, where A is the $m \times n$ matrix with entries A_{ij}, $\mathbf{x}$ is the vector with entries x_i, and $\mathbf{b}$ is the vector with entries b_i. Such systems can then be solved by performing appropriate row operations on the matrix A. However, details of this are omitted and if in need of a refresher we recommend [Tre17, Chapter 2].

5.4.1 Exercises

1. Let $D \in \mathcal{L}(\mathbb{P}_4(\mathbb{R}), \mathbb{P}_3(\mathbb{R}))$ be the differentiation map, $Dp = p'$. Find bases of $\mathbb{P}_4(\mathbb{R})$ and $\mathbb{P}_3(\mathbb{R})$ such that the matrix representation of $\mathcal{M}(D)$ with respect to these basis is given by

$$\mathcal{M}(D) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

2. Show that matrix multiplication of square matrices is not commutative, i.e find matrices $A, B \in M_2$ such that $AB \neq BA$.

5.5 Determinants

The determinant is a function of the entries of a square matrix. The determinant has many applications, including in computing the eigenvalues of a matrix. We review how to compute it and a few of its properties.

The determinant of a 2×2 matrix is

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

There is also a trick for finding the determinant of a 3×3 matrix:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - gec - hfa - idb.$$

You get this by adding the three downward diagonals and subtracting the three upward diagonals from the following:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \begin{matrix} a & b \\ d & e \\ g & h \end{matrix}$$

For other $n \times n$ matrices, one can compute the determinant using cofactor expansion.

Definition 5.48 (Cofactor expansion) *Let $A = \{a_{j,k}\}_{j,k=1}^n$ be a $n \times n$ matrix. Let $M_{j,k}$ denote the determinant of the $(n-1) \times (n-1)$ matrix obtained by removing the j^{th} row and the k^{th} column of A. For each row $j = 1, \ldots, n$*

$$|A| = \sum_{k=1}^{n} a_{j,k}(-1)^{j+k} M_{j,k}.$$

Similarly, for each column $k = 1, \ldots, n$

$$|A| = \sum_{j=1}^{n} a_{j,k}(-1)^{j+k} M_{j,k}.$$

The numbers $C_{j,k} = (-1)^{j+k} M_{j,k}$ are called cofactors.

Repeating the co-factor expansion $n-1$ times would allow us to compute the determinant of a $n \times n$ matrix by hand. However, it is not an efficient way to do so [Tre17, p.92]. Nevertheless, it can be useful in proving properties of the determinant, as well as finding the inverse of a matrix.

We recall that one can easily compute the determinant of matrices of certain forms:

Proposition 5.49 *The determinant of a diagonal matrix or triangular matrix is the product of the entries on the diagonal.*

Proof. One can see this using the cofactor expansion. Take the cofactor expansion across a row or column i with only one entry (in the diagonal). Note that in the diagonal, $j + k$ will always be even. One obtains the entry $a_{i,i}$ times $M_{i,i}$. Repeating this to reduce $M_{i,i}$ will give the product of the entries on the diagonal. □

Recall that from Section 5.3, a matrix A is invertible if and only if the linear map represented by the matrix is an isomorphism. We have a representation for this inverse.

Theorem 5.50 *Let A be an $n \times n$ invertible matrix and let $C = \{C_{j,k}\}_{j,k=1}^n$ be its cofactor matrix. Then*

$$A^{-1} = \frac{1}{|A|} C^T$$

To prove this, show that $AC^T = |A|I$ using the cofactor expansion of A.

This can be useful in solving linear systems. If we have the linear system $A\mathbf{x} = \mathbf{b}$, we know that if A is invertible, the solution is given by $\mathbf{x} = A^{-1}\mathbf{b}$. The above Theorem gives us Cramer's rule for the solution to a linear system:

Corollary 5.51 *Suppose A is an $n \times n$ invertible matrix. The linear system $A\mathbf{x} = \mathbf{b}$ has a unique solution given by*

$$x_i = \frac{|A_i|}{|A|}, \quad i, \ldots, n,$$

where A_i is the matrix obtained by replacing the i^{th} column of A with $\mathbf{b}$.

Here are a few more properties of determinants, stated here without proof.

Proposition 5.52 *$|A| \neq 0$ if and only if A is invertible.*

Proposition 5.53 (Properties of the determinant) *Let A be an $n \times n$ real matrix.*

1. *If A has a zero column, then $|A| = 0$.*
2. *If A has two equal columns, then $|A| = 0$.*
3. *If one column of A is a multiple of another, then $|A| = 0$.*
4. $|AB| = |A||B|$
5. $|\alpha A| = \alpha^n |A|$ *for* $\alpha \in \mathbb{F}$
6. $|A^T| = |A|$

Note that for the last item we need the following definition:

Definition 5.54 *The* transpose *of an $m \times n$ matrix A is the $n \times m$ matrix, denoted A^T, defined entry-wise as $\{A^T_{j,k}\} = \{A_{k,j}\}$ for $j = 1, \ldots, m$ and $k = 1, \ldots n$ (i.e. the rows of A are the columns of A^T and the columns of A are the rows of A^T)*

5.6 Exercises

The following are from [Tre17, p.85]:

1. A square matrix is called *nilpotent* if $\exists k \in \mathbb{N}$ such that $A^k = 0$. Show that for a nilpotent matrix A, $|A| = 0$.
2. A real square matrix Q is called *orthogonal* if $Q^T Q = I$. Prove that if Q is orthogonal, then $|Q| = \pm 1$.
3. An $n \times n$ matrix is called *antisymmetric* if $A^T = -A$. Prove that if A is antisymmetric and n is odd, then $|A| = 0$.

5.7 Inner product spaces

Recall that for a complex number $z = a + ib$, we define the following:

- Real part: $Re(z) = a$,
- Imaginary part: $Im(z) = b$,
- Complex conjugate: $\overline{z} = a - ib$,
- Modulus: $|z| = \sqrt{Re(z)^2 + Im(z)^2} = \sqrt{a^2 + b^2}$

In the metric space section, we saw the definition of a norm. Now we will introduce inner products, which can be viewed as a special case of a norm.

Definition 5.55 *Let V be an $\mathbb{F}$-vector space. A function $\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{F}$ is called* inner product *on V if the following holds:*

1. *(Conjugate) symmetry: $\langle \mathbf{x}, \mathbf{y} \rangle = \overline{\langle \mathbf{y}, \mathbf{x} \rangle}$ for all $\mathbf{x}, \mathbf{y} \in V$, where $\overline{a}$ denotes the complex conjugate for $a \in \mathbb{C}$*
2. *Linearity in the first argument: $\langle \alpha \mathbf{x} + \beta \mathbf{y}, \mathbf{z} \rangle = \alpha \langle \mathbf{x}, \mathbf{z} \rangle + \beta \langle \mathbf{y}, \mathbf{z} \rangle$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ and $\alpha, \beta \in \mathbb{F}$*
3. *Positive definiteness: $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$ and $\langle \mathbf{x}, \mathbf{x} \rangle = 0$ if and only if $\mathbf{x} = \mathbf{0}$*

A vector space equipped with an inner product is called an inner product space.

If V is an $\mathbb{R}$-vector space, property 1 in Definition 5.55 precisely means that the function is symmetric, i.e. $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$ for all $\mathbf{x}, \mathbf{y} \in V$. Similarly, combining symmetry with property 2 we obtain that $\langle \cdot, \cdot \rangle$ is also linear in the second argument.
In the case $\mathbb{F} = \mathbb{C}$, property 2 together with conjugate symmetry leads to $\langle \cdot, \cdot \rangle$ being conjugate linear in the second argument, meaning $\langle \mathbf{x}, \alpha \mathbf{y} + \beta \mathbf{z} \rangle = \overline{\alpha} \langle \mathbf{x}, \mathbf{y} \rangle + \overline{\beta} \langle \mathbf{x}, \mathbf{z} \rangle$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ and $\alpha, \beta \in \mathbb{C}$.

Also note that conjugate symmetry guarantees that $\langle \mathbf{x}, \mathbf{x} \rangle \in \mathbb{R}$ for either choice of $\mathbb{F}$. Hence, property 3 merely forces positivity.

Note that in the following proofs we will often use the complex conjugate so that the proofs hold for both choices of $\mathbb{F}$. If one is only interested in the real case, this might add some notational clutter, however, the proofs are still valid since $r = \overline{r}$ for all $r \in \mathbb{R}$.

Example 5.56

- *Standard inner product on* $\mathbb{R}^n$*:* $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$ *for* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$
- *Standard inner product on* $\mathbb{C}^n$*:* $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i \overline{y}_i$ *for* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$
- *On the space of polynomials* $\mathbb{P}_n(\mathbb{R})$*:* $\langle \boldsymbol{p}, \boldsymbol{q} \rangle = \int_{-1}^1 p(x)q(x)\mathrm{d}x$ *for* $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{P}_n(\mathbb{R})$

Proposition 5.57 *Let* V *be an inner product space. Then* $\mathbf{x} = \mathbf{0}$ *if and only if* $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ *for all* $\mathbf{y} \in V$*.*

Proof. Suppose $\mathbf{x} = \mathbf{0}$, then by linearity in the first argument and since $0\mathbf{x} = \mathbf{x}$, we obtain $\langle \mathbf{x}, \mathbf{y} \rangle = 0\langle \mathbf{x}, \mathbf{y} \rangle = 0$ for all $\mathbf{y} \in V$.

Conversely, suppose $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ for all $\mathbf{y} \in V$. Then, in particular, this holds for $\mathbf{y} = \mathbf{x}$ leading to $\langle \mathbf{x}, \mathbf{x} \rangle = 0$. Hence, $\mathbf{x} = \mathbf{0}$ by positive definiteness. □

An important result regarding inner products is the Cauchy-Schwarz inequality.

Proposition 5.58 (Cauchy-Schwarz Inequality) *Let* V *be an inner product space. Then*

$$|\langle \mathbf{x}, \mathbf{y} \rangle| \leq \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} \sqrt{\langle \mathbf{y}, \mathbf{y} \rangle}$$

for all $\mathbf{x}, \mathbf{y} \in V$*.*

Proof. Let $t \in \mathbb{F}$. Then using linearity and (conjugate) linearity

$$0 \leq \langle \mathbf{x} - t\mathbf{y}, \mathbf{x} - t\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle - t\langle \mathbf{y}, \mathbf{x} \rangle - \overline{t}\langle \mathbf{x}, \mathbf{y} \rangle + |t|^2 \langle \mathbf{y}, \mathbf{y} \rangle.$$

This holds for all $t \in \mathbb{F}$. Setting $t = \langle \mathbf{x}, \mathbf{y} \rangle / \langle \mathbf{y}, \mathbf{y} \rangle$ leads to

$$0 \leq \langle \mathbf{x}, \mathbf{x} \rangle - 2\frac{|\langle \mathbf{x}, \mathbf{y} \rangle|^2}{\langle \mathbf{y}, \mathbf{y} \rangle} + \frac{|\langle \mathbf{x}, \mathbf{y} \rangle|^2}{\langle \mathbf{y}, \mathbf{y} \rangle^2} \langle \mathbf{y}, \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle - \frac{|\langle \mathbf{x}, \mathbf{y} \rangle|^2}{\langle \mathbf{y}, \mathbf{y} \rangle},$$

where we used (conjugate) symmetry. Hence,

$$|\langle \mathbf{x}, \mathbf{y} \rangle|^2 \leq \langle \mathbf{x}, \mathbf{x} \rangle \langle \mathbf{y}, \mathbf{y} \rangle$$

and taking the square root leads the result. □

As alluded to before an inner product can be used to define a norm.

Proposition 5.59 *Let* V *be an inner product space. Then* $\langle \cdot, \cdot \rangle$ *induces a norm on* V *via* $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$ *for all* $\mathbf{x} \in V$*.*

Proof. By property 3 in Definition 5.55, $\|\mathbf{x}\| \geq 0$ for all $\mathbf{x} \in V$ and $\|\mathbf{x}\| = 0$ if and only if $\mathbf{x} = 0$.

By linearity and conjugate symmetry we obtain for $\alpha \in \mathbb{F}$ and $\mathbf{x} \in V$:

$$\|\alpha\mathbf{x}\| = \sqrt{\langle \alpha\mathbf{x}, \alpha\mathbf{x} \rangle} = \sqrt{\alpha\overline{\alpha}\langle \mathbf{x}, \mathbf{x} \rangle} = \sqrt{|\alpha|^2 \langle \mathbf{x}, \mathbf{x} \rangle} = |\alpha| \|\mathbf{x}\|.$$

Lastly, linearity in the first argument and (conjugate) linearity and the Cauchy-Schwarz inequality will give the triangle inequality. For $\mathbf{x}, \mathbf{y} \in V$ we observe

$$\|\mathbf{x} + \mathbf{y}\|^2 = \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle + \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle$$

$$
\begin{aligned}
&= \|\mathbf{x}\|^2 + 2\mathrm{Re}(\langle \mathbf{x}, \mathbf{y}\rangle) + \|\mathbf{y}\|^2 \\
&\leq \|\mathbf{x}\|^2 + 2|(\langle \mathbf{x}, \mathbf{y}\rangle)| + \|\mathbf{y}\|^2 \\
&\leq \|\mathbf{x}\|^2 + 2\|\mathbf{x}\|\|\mathbf{y}\| + \|\mathbf{y}\|^2 = (\|\mathbf{x}\| + \|\mathbf{y}\|)^2,
\end{aligned}
$$

where $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}$ denotes the real part of a complex number $z \in \mathbb{C}$ and we used $\mathrm{Re}(z) \leq |z|$ for all $z \in \mathbb{C}$. Taking the square root of the above inequality leads to the desired result. □

Note: With this identification the Cauchy-Schwarz inequality can be restated as: $|\langle \mathbf{x}, \mathbf{y}\rangle| \leq \|\mathbf{x}\|\|\mathbf{y}\|$ for all $\mathbf{x}, \mathbf{y} \in V$.

Example 5.60 *The norm introduced by the standard inner product on $\mathbb{R}^n$ is the Euclidean distance.*

5.7.1 Adjoints, unitaries and orthogonal matrices

Definition 5.61 *Let U, V be inner product spaces and $S\colon U \to V$ be a linear map. The* adjoint *S^* of S is the linear map $S^*\colon V \to U$ defined such that*

$$
\langle S\mathbf{u}, \mathbf{v}\rangle_V = \langle \mathbf{u}, S^*\mathbf{v}\rangle_U \qquad \text{for all } \mathbf{u} \in U, \mathbf{v} \in V.
$$

If it is clear from context, we sometimes omit the subscripts for the inner products. The next proposition shows that the definition makes sense, i.e. this uniquely defines a linear operator.

Proposition 5.62 *Let U, V be inner product spaces and $S\colon U \to V$ be a linear map. Then S^* is unique and linear.*

Proof. First, we show uniqueness. Suppose there exists $T\colon V \to U$ such that $\langle S\mathbf{u}, \mathbf{v}\rangle_V = \langle \mathbf{u}, T\mathbf{v}\rangle_U$ for all $\mathbf{u} \in U, \mathbf{v} \in V$. Then, $\langle \mathbf{u}, T\mathbf{v}\rangle_U = \langle \mathbf{u}, S^*\mathbf{v}\rangle$ for all $\mathbf{u} \in U, \mathbf{v} \in V$. Then using (conjugate) symmetry and Exercise 1, we see that $S^* = T$.

To see linearity take $\alpha \in \mathbb{F}$ and $\mathbf{v}, \mathbf{w} \in V$. Then, by the definition of adjoint and using conjugate linearity in the second argument we obtain

$$
\begin{aligned}
\langle \mathbf{u}, S^*(\alpha\mathbf{v} + \mathbf{w})\rangle_U &= \langle S\mathbf{u}, \alpha\mathbf{v} + \mathbf{w}\rangle_V = \overline{\alpha}\langle S\mathbf{u}, \mathbf{v}\rangle_V + \langle S\mathbf{u}, \mathbf{w}\rangle_V \\
&= \langle \mathbf{u}, \alpha S^*\mathbf{v}\rangle_U + \langle \mathbf{u}, S^*\mathbf{w}\rangle_U \\
&= \langle \mathbf{u}, \alpha S^*\mathbf{v} + S^*\mathbf{w}\rangle_U
\end{aligned}
$$

for all $\mathbf{u} \in U$. Hence, $0 = \langle \mathbf{u}, S^*(\alpha\mathbf{v} + \mathbf{w}) - \alpha S^*\mathbf{v} + S^*\mathbf{w}\rangle$ for all $\mathbf{u} \in U$ and so by (conjugate) symmetry and Proposition 5.57 we obtain $S^*(\alpha\mathbf{v} + \mathbf{w}) = \alpha S^*\mathbf{v} + S^*\mathbf{w}$. □

Example 5.63 *Define $S\colon \mathbb{R}^3 \to \mathbb{R}^2$ by $S\mathbf{x} = (2x_1 + x_3, -x_2)$. Then, for all $\mathbf{y} = (y_1, y_2) \in \mathbb{R}^2$ the defining equation for the adjoint operator leads to*

$$
\begin{aligned}
\langle S\mathbf{x}, \mathbf{y}\rangle_{\mathbb{R}^2} &= \langle (2x_1 + x_3, -x_2), (y_1, y_2)\rangle \\
&= 2x_1y_1 + x_3y_1 - x_2y_2 \\
&= \langle (x_1, x_2, x_3), (2y_1, -y_2, y_1)\rangle_{\mathbb{R}^3} \\
&= \langle \mathbf{x}, S^*\mathbf{y}\rangle_{\mathbb{R}^3}.
\end{aligned}
$$

Hence, $S^*\mathbf{y} = (2y_1, -y_2, y_1)$.

Next we will record some properties of the adjoint.

Proposition 5.64 *Let U, V, W be inner product spaces and $S, T \in \mathcal{L}(U, V)$ and $R \in \mathcal{L}(V, W)$. Then, the following holds*

1. *$(S + \alpha T)^* = S^* + \overline{\alpha}T^*$ for all $\alpha \in \mathbb{F}$*
2. *$(S^*)^* = S$*

3. $(RS)^* = S^*R^*$

4. $I^* = I$, *where* $I\colon U \to U$ *is the identity operator on* U

The proof of this is an exercise.

The adjoint of a linear map also always exists, which we will handle by constructing the adjoint of a matrix. Then, since any linear map between abstract finite-dimensional vector spaces can be represented as a matrix (after a choice of basis), we obtain a matrix representation for the adjoint. In [Axl15] a slightly different and arguably more abstract proof is presented.

Proposition 5.65 *Let* $A \in M_{m\times n}(\mathbb{F})$ *be a matrix and* $T_A\colon \mathbb{F}^n \to F^m\colon \mathbf{x} \mapsto A\mathbf{x}$. *Then,* $T_A^*(\mathbf{x}) = A^*\mathbf{x}$, *where* $A^* \in M_{n\times m}(\mathbb{F})$ *with* $(A^*)_{ij} = \overline{A_{ji}}$ *for* $i = 1, \dots, n$ *and* $j = 1, \dots, m$.

In particular if $\mathbb{F} = \mathbb{R}$, *the adjoint of the matrix is given by its transpose,denoted* A^T, *and if* $\mathbb{F} = \mathbb{C}$, *it is given by its conjugate transpose, denoted* A^*.

Proof. Let $\mathbf{x} \in \mathbb{F}^n$ and $\mathbf{y} \in \mathbb{F}^m$. Then

$$\begin{aligned}\langle A\mathbf{x}, \mathbf{y}\rangle &= \sum_{j=1}^{m}\left(\sum_{i=1}^{n} A_{ji}x_i\right)\overline{y_j}\\ &= \sum_{i=1}^{n} x_i\left(\overline{\sum_{j=1}^{m}\overline{A_{ji}}y_j}\right)\\ &= \langle \mathbf{x}, A^*\mathbf{y}\rangle.\end{aligned}$$

□

Using the adjoint we can identify the matrices that preserve the inner product (and hence also the norm induced by the inner product).

Definition 5.66 *A matrix* $O \in M_n(\mathbb{R})$ *is called* orthogonal *if its inverse is given by its transpose, i.e.* $O^TO = OO^T = I$. *A matrix* $U \in M_n(\mathbb{C})$ *is called* unitary *if the inverse is given by the conjugate transpose, i.e.* $U^*U = UU^* = I$.

Example 5.67

- *Let* $\varphi \in [0, 2\pi]$. *Then*
$$\begin{pmatrix}\cos(\varphi) & -\sin(\varphi)\\ \sin(\varphi) & \cos(\varphi)\end{pmatrix}$$
is an orthogonal matrix. What does it describe geometrically?
- *The following is a unitary matrix:*
$$\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$$

By the definition we immediately see that for $U \in M_n(\mathbb{C})$ unitary we have

$$\langle U\mathbf{x}, U\mathbf{y}\rangle = \langle \mathbf{x}, U^*U\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{C}^n$ and similarly for orthogonal matrices. This essentially gives the equivalent characterization.

Proposition 5.68 *A matrix* $U \in M_n(\mathbb{C})$ *(*$O \in M_n(\mathbb{R})$*) is unitary (*O *is orthogonal) if and only if* U *(*O*) is an isometry with respect to the norm induced by the inner product, i.e.* $\|U\mathbf{x}\| = \|\mathbf{x}\|$ *for all* $\mathbf{x} \in \mathbb{C}^n$ *(*$\|O\mathbf{x}\| = \|\mathbf{x}\|$ *for all* $\mathbf{x} \in \mathbb{R}^n$*)*

Another important class of matrices related to the adjoint are self-adjoint matrices.

Definition 5.69 *Let $A \in M_n(\mathbb{F})$. We call A* self-adjoint *if $A^* = A$. In the case $\mathbb{F} = \mathbb{R}$, such an A is called* symmetric *and if $\mathbb{F} = \mathbb{C}$, such an A is called* Hermitian*.*

Lastly, we mention that the square matrices can be equipped with an inner product.

Definition 5.70 *The* trace *is the linear function* $\mathrm{Tr}\colon M_n\mathbb{F} \to \mathbb{F}$ *given by* $\mathrm{Tr}(A) = \sum_{i=1}^n A_{ii}$*.*

The trace is especially nice due to its cyclic property $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for all $A, B \in M_n(\mathbb{F})$. The proof of this is an exercise. Note that this also shows that the trace is independent of the choice of basis, since any change of basis transformation can be expressed using an invertible matrix U, i.e. UAU^{-1}.

Proposition 5.71 *The following defines an inner product on $M_n(\mathbb{F})$:*

$$\langle A, B\rangle = \mathrm{Tr}(B^*A)$$

for $A, B \in M_n(\mathbb{F})$. This is often called Hilbert-Schmidt inner product*.*

The proof that this actually defines an inner product is an exercise.

5.7.2 Orthogonality and Gram-Schmidt

In the following V is always an inner product space.

Definition 5.72 *Two vectors $\mathbf{x}, \mathbf{y} \in V$ are called* orthogonal *if $\langle \mathbf{x}, \mathbf{y}\rangle = 0$, denoted $\mathbf{x} \perp \mathbf{y}$. We call them* orthonormal *if additionally the vectors are normalized, i.e. $\|\mathbf{x}\| = \|\mathbf{y}\| = 1$. A basis $\mathbf{x}_1, \dots, \mathbf{x}_n$ of V is called* orthonormal basis (ONB)*, if the vectors are pairwise orthogonal and normalized.*

Orthonormal bases are particularly nice, since the coefficients of an arbitrary vector in the basis expansion with respect to this ONB are given by inner products (see Exercises). Note that being orthonormal already implies being linearly independent.

Proposition 5.73 *Let $\mathbf{x}_1, \dots, \mathbf{x}_k \in V$ be orthonormal. Then, the system of vectors is linearly independent.*

Proof. Suppose $\sum_{i=1}^k \alpha_i \mathbf{x}_i = \mathbf{0}$. Then, $\|\sum_{i=1}^k \alpha_i \mathbf{x}_i\|^2 = 0$. In particular,

$$\begin{aligned} 0 = \|\sum_{i=1}^k \alpha_i \mathbf{x}_i\|^2 = \langle \sum_{i=1}^k \alpha_i \mathbf{x}_i, \sum_{j=1}^k \alpha_j \mathbf{x}_j\rangle = \sum_{i,j=1}^k \langle \alpha_i \mathbf{x}_i, \alpha_j \mathbf{x}_j\rangle \\ = \sum_{i=1}^n |\alpha_i|^2 \|\mathbf{x}_i\|^2 + \sum_{i,j=1, i\neq j}^n \alpha_i \overline{\alpha_j} \langle \mathbf{x}_i, \mathbf{x}_j\rangle = \sum_{i=1}^n |\alpha_i|^2, \end{aligned}$$

which shows that $\alpha_i = 0$ for all $i = 1, \dots, n$ and thus, the system is linearly independent. □

Given two vectors we can decompose one into orthogonal parts with respect to the other.

Proposition 5.74 (Orthogonal Decomposition,[Axl15, 6.14, p.171]) *Let $\mathbf{x}, \mathbf{y} \in V$ with $\mathbf{y} \neq 0$. Then, there exist $c \in F$ and $\mathbf{z} \in V$ such that $\mathbf{x} = c\mathbf{y} + \mathbf{z}$ with $\mathbf{y} \perp \mathbf{z}$.*

Proof. Set $c = \frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{y}\|^2}$ and $\mathbf{z} = \mathbf{x} - c\mathbf{y}$. □

Given a basis we can obtain an ONB from it using the Gram-Schmidt algorithm by reiterating the orthogonal decomposition from above.

Proposition 5.75 (Gram-Schmidt Algorithm, [Axl15, 6.31, p.183]) *Let $\mathbf{x}_1, \dots, \mathbf{x}_n \in V$ be a system of linearly independent vectors. Define $\mathbf{y}_1 = \mathbf{x}_1/\|\mathbf{x}_1\|$. For $i = 2, \dots, n$ define $\mathbf{y}_j$ inductively by*

$$\mathbf{y}_i = \frac{\mathbf{x}_i - \sum_{k=1}^{i-1} \langle \mathbf{x}_i, \mathbf{y}_k\rangle \mathbf{y}_k}{\|\mathbf{x}_i - \sum_{k=1}^{i-1} \langle \mathbf{x}_i, \mathbf{y}_k\rangle \mathbf{y}_k\|}.$$

Then the $\mathbf{y}_1, \dots, \mathbf{y}_n$ are orthonormal and

$$\mathrm{span}\{\mathbf{x}_1, \dots, \mathbf{x}_n\} = \mathrm{span}\{\mathbf{y}_1, \dots, \mathbf{y}_n\}.$$

The proof is omitted but can be found in the book.

Definition 5.76 *Let $U \subseteq V$ be a non-empty subset. The* orthogonal complement $U^\perp$ *of U is given by*

$$U^\perp = \{\mathbf{x} \in V : \langle \mathbf{x}, \mathbf{u} \rangle = 0 \text{ for all } \mathbf{u} \in U\}.$$

In the exercises you will show that the orthogonal complement is a subspace.

5.7.3 Exercises

1. Let V be an inner product space, U a vector space and $S : U \to V$, $S : U \to V$ be linear maps . Show that $\langle S\mathbf{u}, \mathbf{v} \rangle = \langle T\mathbf{u}, \mathbf{v} \rangle$ for all $\mathbf{u} \in U$ and $\mathbf{v} \in V$ implies $S = T$.
2. Let U, V, W be inner product spaces and $S, T \in \mathcal{L}(U, V)$ and $R \in \mathcal{L}(V, W)$. Show that the following holds
   (a) $(S + \alpha T)^* = S^* + \overline{\alpha} T^*$ for all $\alpha \in \mathbb{F}$
   (b) $(S^*)^* = S$
   (c) $(RS)^* = S^* R^*$
   (d) $I^* = I$, where $I : U \to U$ is the identity operator on U
3. Let $A, B \in M_n(\mathbb{F})$. Show that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.
4. Show that $\langle A, B \rangle = \mathrm{Tr}(B^* A)$ for $A, B \in M_n(\mathbb{F})$ defines an inner product on $M_n(\mathbb{F})$.
5. Let V be an inner product space and $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be an orthonormal basis and $\mathbf{y} \in V$. Then, $\mathbf{x}$ has a unique representation $\mathbf{y} = \sum_{i=1}^n \alpha_i \mathbf{x}_i$. Show that $\alpha_i = \langle \mathbf{y}, \mathbf{x}_i \rangle$ for all $i = 1, \ldots, n$.
6. Let V be an inner product space and $U \subseteq V$ a subset. Show that $U^\perp$ is a subspace of V.

5.8 Spectral theory

Note: here we will assume $\mathbb{F} = \mathbb{C}$, so that we are working on an algebraically closed field.

Let $T : V \to V$ be a linear map, where V is a vector space. We would like to describe the action of this linear map in a particularly "nice" way. For example, if there exists a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ of V such that $T\mathbf{v}_i = \lambda_i \mathbf{v}_i$ where $\lambda_i \in \mathbb{F}$ for $i = 1, \ldots, n$, then T acts on this basis merely by scaling the basis vectors. If we look at the matrix of T with respect to this basis, T is a diagonal matrix with λ_i in the diagonal.

In what follows, we will frame our discussion in terms of matrices. Given a choice of basis, it could be applied more broadly to linear maps.

Definition 5.77 *Given an operator $A : V \to V$ and $\alpha \in \mathbb{F}$, λ is called an* eigenvalue *of A if there exists a non-zero vector $\mathbf{v} \in V \setminus \{\mathbf{0}\}$ such that*

$$A\mathbf{v} = \lambda \mathbf{v}.$$

We call such $\mathbf{v}$ an eigenvector *of A with eigenvalue λ. We call the set of all eigenvalues of A* spectrum *of T and denote it by $\sigma(T)$.*

Note that $A\mathbf{v} = \lambda \mathbf{v}$ can be rewritten as $(A - \lambda I)\mathbf{v} = 0$. Thus, if λ is an eigenvalue, we can find the corresponding eigenvectors by finding the null space of $A - \lambda I$. The subspace $\mathrm{null}(A - \lambda I)$ is called the *eigenspace*.

To find the eigenvalues of A, one must find the scalars λ such that $\mathrm{null}(A - \lambda I)$ has a non-trivial solution. By Section 5.3, this means that λ is an eigenvector if and only if $A - \lambda I$ is not invertible. By Proposition 5.52, this means we need $|A - \lambda I| = 0$.

Theorem 5.78 *The following are equivalent*

1. *$\lambda \in \mathbb{F}$ is an eigenvalue of A,*

2. $(A - \lambda I)\mathbf{v} = 0$ *has a non-trivial solution,*

3. $|A - \lambda I| = 0$.

If A is an $n \times n$ matrix, $|A - \lambda I|$ is a polynomial of degree n.

Definition 5.79 *If A is an $n \times n$ matrix, $p_A(\lambda) = |A - \lambda I|$ is a polynomial of degree n called the* characteristic polynomial *of A.*

To find the eigenvectors of A, one needs to find the roots of the characteristic polynomial.

Example 5.80 *The eigenvalues of*

$$\begin{bmatrix} 4 & -2 \\ 5 & -3 \end{bmatrix}$$

are -1 and 2. The eigenvalues of

$$\begin{bmatrix} -1-2i & 2i+2 & -2i-2 \\ i-1 & 2-i & 2i-2 \\ 2i & -2i & 3i \end{bmatrix}$$

are 1,$-i$, and i.

Since the characteristic polynomial associated with an $n \times n$ matrix A is always of degree n, A will always have n eigenvalues. However, some of them may be repeated, so A may not have n distinct eigenvalues. Recall that if λ is a root of $p(z)$, then $z - \lambda$ divides $p(z)$. We say that λ has *multiplicity* k if k is the largest positive integer such that $(z - \lambda)^k$ divides $p(z)$.

Definition 5.81 *The multiplicity of the root λ in the characteristic polynomial is called the* algebraic multiplicity *of the eigenvalue λ. The dimension of the eigenspace* $\text{null}(A - \lambda I)$ *is called the* geometric multiplicity *of the eigenvalue λ.*

Definition 5.82 (Similar matrices) *Square matrices A and B are called* similar *if there exists an invertible matrix S such that*

$$A = SBS^{-1}.$$

Similar matrices have the same characteristic polynomials and hence the same eigenvalues (see exercise).

Theorem 5.83 *Suppose A is a square matrix with distinct eigenvalues $\lambda_1, \ldots, \lambda_n$. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be eigenvectors corresponding to these eigenvalues. Then $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent.*

Similar matrices have the same characteristic polynomials and hence the same eigenvalues (see exercise).

Proof. We prove this using induction on k. The base case, $k = 1$, is trivial since any non-zero vector is linearly independent. Suppose that the statement holds for some $k \geq 1$, i.e. the eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ corresponding to distinct eigenvectors $\lambda_1, \ldots, \lambda_k$ are linearly independent and suppose λ_{k+1} is a distinct eigenvalue with eigenvector $\mathbf{v}_{k+1}$. We will show that any linear combination $\sum_{i=1}^{k+1} \alpha_i \mathbf{v}_i = \mathbf{0}$ is trivial.

Let $\sum_{i=1}^{k+1} \alpha_i \mathbf{v}_i = \mathbf{0}$. Then, applying $A - \lambda_{k+1} I$ leads to

$$\mathbf{0} = \sum_{i=1}^{k+1} \alpha_i (A - \lambda_{k+1} I)\mathbf{v}_i = \sum_{i=1}^{k} \alpha_i (\lambda_i - \lambda_{k+1})\mathbf{v}_i + \alpha_{k+1}(\lambda_{k+1} - \lambda_{k+1})\mathbf{v}_{k+1} = \sum_{i=1}^{k} \alpha_i (\lambda_i - \lambda_{k+1})\mathbf{v}_i.$$

Since by hypothesis $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are linearly independent, this implies $\alpha_i(\lambda_i - \lambda_{k+1}) = 0$ for all $i = 1, \ldots, k$. Since the eigenvalues are distinct, $\lambda_i - \lambda_{k+1} \neq 0$ and thus $\alpha_i = 0$ for all $i = 1 \ldots, k$. Hence, we have $\mathbf{0} = \sum_{i=1}^{k+1} \alpha_i \mathbf{v}_i = \alpha_{k+1} \mathbf{v}_{k+1}$. By definition of eigenvector $\mathbf{v}_{k+1} \neq \mathbf{0}$ and thus $\alpha_{k+1} = 0$, which shows the desired linear independence.

□

Hence, if all the eigenvalues are distinct, there exists a basis of eigenvectors. This gives the next result.

Corollary 5.84 *If a $A \in M_n(\mathbb{C})$ has n distinct eigenvalues, then A is diagonalizable. That is there exists an invertible matrix $S \in M_n(\mathbb{C})$ such that $A = SDS^{-1}$, where D is a diagonal matrix with the eigenvalues of A in the diagonal.*

If we think about this in terms of linear maps, this is saying that if $T : V \to V$ is an operator with n distinct eigenvalues, then there exists a basis for V such that the matrix of T is diagonal, i.e. T acts only by scaling the basis vectors.

Theorem 5.85 *Let $A : V \to V$ be an operator with n eigenvalues. A is diagonalizable if and only if for each eigenvalue λ, the geometric multiplicity of λ and the algebraic multiplicity of λ are the same.*

Example 5.86 *Consider the matrices*

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 1 & -1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

Both matrices have eigenvalues 1 and 2, where the latter has algebraic multiplicity 2. However, the geometric multiplicty of the eigenvalue 2 is 2 for A, but only 1 for B. Hence, A is diagonalizable, but B is not.

Theorem 5.87 *Let $A \in M_n(\mathbb{R})$ be a symmetric matrix. Then, there exists an orthogonal matrix $O \in M_n(\mathbb{R})$ such that $A = ODO^T$, where D is a diagonal matrix with the eigenvalues of A in the diagonal. Furthermore, all eigenvalues of A are real.*

We can also state this for $M_n(\mathbb{C})$:

Theorem 5.88 *Let $A \in M_n(\mathbb{C})$ be a Hermitian matrix. Then, there exists a unitary matrix $U \in M_n(\mathbb{C})$ such that $A = UDU^*$, where D is a diagonal matrix with the eigenvalues of A in the diagonal. Furthermore, all eigenvalues of A are real.*

The proof is omitted, see [Tre17, Chapter 6, Theorem 2.2]. The fact that the eigenvalues are real is an exercise. Note that in the previous theorem, the orthogonality of the eigenvectors is special. In general, even if a matrix is diagonalizable, there might not exists a orthogonal eigenbasis. The next theorem states a characterization of matrices that exhibit an orthogonal eigenbasis.

Theorem 5.89 *A matrix A is diagonalizable by a unitary matrix if and only if $AA^* = A^*A$. We call such a matrix* ***normal****.*

Proof omitted, see [Tre17, Chapter 6, Theorem 2.4].

5.8.1 Jordan canonical form

Definition 5.90 *A block matrix is a matrix that can be broken into sections called blocks, which are smaller matrices.*

Example 5.91

$$\begin{bmatrix} 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

where

$$A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

In the above example, A and B are blocks on the main diagonal, while B and C are off-diagonal blocks. C has a special form as it is a zero block.

Definition 5.92 *A square matrix is called* block diagonal *if it can be written as a block matrix where the main-diagonal blocks are all square matrices and the off-diagonal blocks are all zero.*

Example 5.93 *The matrix*

$$\begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{bmatrix}$$

is block diagonal.

Definition 5.94 *A vector* $\mathbf{v}$ *is called a* generalized eigenvector *of* A *corresponding to an eigenvalue* λ *if there exists* $k \geq 1$ *such that*

$$(A - \lambda I)^k \mathbf{v} = 0.$$

The set of generalized eigenvectors of an eigenvalue λ (plus $\mathbf{0}$) is called the *generalized eigenspace* of λ.

Proposition 5.95 *The algebraic multiplicity of an eigenvalue* λ *is the same as the dimension of the corresponding generalized eigenspace.*

Theorem 5.96 (Jordan decomposition theorem) *For any operator* A *there exists a basis such that* A *is block diagonal with blocks that have eigenvalues on the diagonal and 1s on the upper off-diagonal. In other words,* A *can be written in the form*

$$A = \begin{bmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_k \end{bmatrix}$$

where the blocks J_i *on the main diagonal are Jordan block of the form*

$$\begin{bmatrix} \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}, \text{ etc.}$$

This form is called Jordan canonical form.

Connection to algebraic and geometric multiplicity:

- The algebraic multiplicity of an eigenvalue λ is the number of times λ appears on the diagonal.
- The geometric multiplicity of λ is the number of Jordan blocks associated with λ.

Jordan form is useful because, while not ever square matrix is diagonalizable, every square matrix can be written in JCF. In addition, the Jordan form is useful when taking a matrix exponential. The matrix exponential if a matrix A is

$$e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k.$$

We note that the Jordan form of a matrix is equal to $D + N$ where D is a diagonal matrix and N is a nilpotent matrix. Since $e^{D+N} = e^D e^N$, JCF gives a useful way to calculate the matrix exponential of A. One often needs to do this to find the solution of systems of linear differential equations.

5.8.2 Singular value decomposition

Note that $A^T A$ is symmetric, so it is orthogonally diagonalizable and has real eigenvalues by Theorem 5.87. In fact the eigenvalues are non-negative, which is part of the exercises. This justifies the following definition.

Definition 5.97 *Let* A *be an* $m \times n$ *matrix. Let* $\lambda_1, \dots, \lambda_n$ *be the eigenvalues of* $A^T A$*. Then the* singular values *of* A *are defined as*

$$\sigma_1 = \sqrt{\lambda_1}, \dots, \sigma_n = \sqrt{\lambda_n}.$$

Theorem 5.98 *If A is an $m \times n$ matrix of rank k, then we can write*

$$A = U\Sigma V^T$$

where Σ is an $m \times n$ matrix of the form

$$\begin{bmatrix} D_{k\times k} & 0_{k\times(n-k)} \\ 0_{(m-k)\times k} & 0_{(m-k)\times(n-k)} \end{bmatrix},$$

D is a diagonal matrix with the singular values of A, $\sigma_1, \ldots, \sigma_n$, on the diagonal and U and V are both orthogonal matrices (of size $m \times n$ and $n \times n$, respectively).

In contrast to the diagonalization discussed at the beginning, both Jordan canonical form and singular value decomposition can be applied to arbitrary square matrices (note that SVD can also be applied to rectangular matrices). However, they achieve different things. On the one hand, for a matrix $A \in M_n(\mathbb{C})$, the JCF says that there exists an invertible matrix $U \in M_n(\mathbb{C})$ such that $U^{-1}AU$ has block diagonal form with the eigenvalues in the diagonal. One can think of the invertible matrix U describing a preferred basis in which A has block diagonal form. However, this basis is not necessarily orthonormal and since A only has block diagonal form and is not necessarily diagonal, the action of A on this basis is not only given by scaling. On the other hand, the SVD of A leads to $A = U\Sigma V^*$, where U, V are orthogonal and Σ is a diagonal matrix. Since U, V are orthogonal, we can think of them as encoding orthonormal bases and since Σ is diagonal, it only acts by scaling. Hence, A is written in a way that maps one orthonormal basis to another orthonormal basis with additional stretching factors given by the singular values of A encoded in Σ. However, the caveat here is that we change the basis going from V^* to U.

Jordan canonical form and singular value decomposition each have some nice applications. For example, the former can be useful to solve linear systems of differential equations, since it can be used to determine the matrix exponential function. The latter has some uses in statistics, as for example it can be used to motivate principal component analysis.

5.8.3 Exercises

1. Let $A, B \in M_n(\mathbb{F})$ be similar matrices. Show that their characteristic polynomials coincide.
2. Show that $A \in M_n(\mathbb{C})$ is invertible if and only if $0 \notin \sigma(A)$.
3. Suppose N is a nilpotent matrix. Show that $\sigma(N) = \{0\}$.
4. Let $A \in M_n(\mathbb{C})$ be an invertible matrix. Show that λ is an eigenvalue of A if and only if λ^{-1} is an eigenvalue of A^{-1}.
5. Suppose $A \in M_n(\mathbb{C})$ is Hermitian. Show that all the eigenvalues of A are real. Hint: Note that if $\mathbf{x}$ is a normalized eigenvector of A with eigenvalue λ, then $\langle A\mathbf{x}, \mathbf{x}\rangle = \lambda$.
6. Let $A \in M_n(\mathbb{R})$. Show that the eigenvalues of A^TA are non-negative.

5.9 Other matrix decompositions

We briefly discuss two other matrix decompositions which have applications in numerical methods.

First, LU-decomposition is used to solve linear systems of the form $A\mathbf{x} = \mathbf{b}$.

Definition 5.99 (LU-decomposition) *The LU-decomposition of a square matrix A is the factorization of A into a lower triangular matrix L and an upper triangular matrix U as follows:*

$$A = LU.$$

For A to have an LU-decomposition, A must be reducible to row echelon form.

This is done to make solving linear systems numerically more efficient. If one can write $A = LU$, then one can solve $A\mathbf{x} = \mathbf{b}$ as follows: First solve $L\mathbf{y} = \mathbf{b}$ for an unknown $\mathbf{y}$. Then solve $U\mathbf{x} = \mathbf{y}$ for $\mathbf{x}$. This means that

rather than solve one linear system, $A\mathbf{x} = \mathbf{b}$, we now solve two, $L\mathbf{y} = \mathbf{b}$ and $U\mathbf{x} = \mathbf{y}$, but the latter problems are much easier to solve. If one has to solve repeated linear problems of the form $A\mathbf{x} = \mathbf{b}_1$, $A\mathbf{x} = \mathbf{b}_2$, etc, then there is increased efficiency in first factoring A into LU and then solving the problems.

Next, we discuss QR-decomposition.

Definition 5.100 (QR-decomposition) *The QR-decomposition of an $m \times n$ matrix A with linearly independent column vectors is the factorization of A as follows:*

$$A = QR,$$

where Q is an $m \times n$ matrix with orthonormal column vectors and R is an $n \times n$ invertible upper triangular matrix.

One obtains the factorization by applying the Gram-Schmidt algorithm to the columns of A. Let $\mathbf{u}_1, \ldots, \mathbf{u}_n$ be the column vectors of A. Let $\mathbf{q}_1, \ldots, \mathbf{q}_n$ be the orthonormal vectors obtained by applying Gram Schmidt. Then one can write:

$$\begin{aligned}
\mathbf{u}_1 &= \langle \mathbf{u}_1, \mathbf{q}_1 \rangle \mathbf{q}_1 + \langle \mathbf{u}_2, \mathbf{q}_2 \rangle \mathbf{q}_2 + \ldots + \langle \mathbf{u}_n, \mathbf{q}_n \rangle \mathbf{q}_n \\
\mathbf{u}_2 &= \langle \mathbf{u}_2, \mathbf{q}_2 \rangle \mathbf{q}_2 + \ldots + \langle \mathbf{u}_n, \mathbf{q}_n \rangle \mathbf{q}_n \\
&\vdots \\
\mathbf{u}_n &= \langle \mathbf{u}_n, \mathbf{q}_n \rangle \mathbf{q}_n
\end{aligned}$$

Thus the orthonormal vectors obtained using Gram-Schmidt form the columns of Q, while R is the terms needed to go between the columns of A and thsoe of Q, i.e.

$$R = \begin{bmatrix}
\langle \mathbf{u}_1, \mathbf{q}_1 \rangle & \langle \mathbf{u}_2, \mathbf{q}_2 \rangle & \ldots & \langle \mathbf{u}_n, \mathbf{q}_n \rangle \\
0 & \langle \mathbf{u}_2, \mathbf{q}_2 \rangle & \ldots & \langle \mathbf{u}_n, \mathbf{q}_n \rangle \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & \langle \mathbf{u}_n, \mathbf{q}_n \rangle
\end{bmatrix}$$

Why use QR-decomposition? As mentioned before, orthogonal matrices have nice numerical properties, since they can be easily inverted and create less error. As with the LU decomposition, we can write the linear problem $A\mathbf{x} = \mathbf{b}$ as two problems, $R\mathbf{x} = \mathbf{y}$, which can be solved easily, and $Q\mathbf{y} = \mathbf{b}$, which has solution $\mathbf{y} = Q^T\mathbf{b}$ since Q is orthogonal.

5.9.1 Exercises

1. Show that an $Q \in M_n(\mathbb{R})$ is orthogonal if and only if its columns are orthonormal.

5.10 References

This section is based on the books [Axl15] and [Tre17]. [Axl15] is the main source for sections 1, 2, and 3, while [Tre17] is used for sections 4 and 5. [AR14], which is focused more on applications than the two main texts, was used for the content on matrix decompositions.

References

[AR14] Howard Anton and Chris Rorres. *Elementary Linear Algebra*. Wiley, 11 edition, 2014.

[Axl15] Sheldon Axler. *Linear Algebra Done Right*. Undergraduate Texts in Mathematics. Springer, 3 edition, 2015. URL: https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/978-3-319-11080-6.

[Ger12] Larry J. Gerstein. *Introduction to Mathematical Structures and Proofs*. Undergraduate Texts in Mathematics. 2012. URL: https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/978-1-4614-4265-31.

[Lak16] Tamara J. Lakins. *The Tools of Mathematical Reasoning*. Pure and Applied Undergraduate Texts. 2016.

[Leb22] Jiří Lebl. *Basic Analysis I*, volume 1 of *Introduction to Real Analysis*. 2022. URL: https://www.jirka.org/ra/realanal.pdf.

[Mar19] Laurent W. Marcoux. Pmath 351 notes, 2019. URL: https://www.math.uwaterloo.ca/~lwmarcou/notes/pmath351.pdf.

[Pug15] Charles C. Pugh. *Real Mathematical Analysis*. Undergraduate Texts in Mathematics. 2015. URL: https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/978-3-319-17771-7.

[Run05] Volker Runde. *A Taste of Topology*. Universitext. 2005. URL: https://link-springer-com.myaccess.library.utoronto.ca/book/10.1007/0-387-28387-0.

[Tre17] Sergei Treil. *Linear Algebra Done Wrong*. 2017. URL: https://www.math.brown.edu/streil/papers/LADW/LADW.html.

[Zwi22] Piotr Zwiernik. Lecture notes in mathematics for economics and statistics, 2022. URL: http://84.89.132.1/~piotr/docs/RealAnalysisNotes.pdf.