

CHAPTER

0



INTRODUCTION

In this chapter we introduce key concepts that will be used in later chapters. For this reason, unlike other chapters it contains many statements, sometimes given without thorough explanations or reasoning. While all of these statements are grounded in deep ideas and can be formulated in a rigorous manner, it is advised to first get an intuitive understanding of the ideas before diving into their more formal construction.

Note 0.1 In case you are already familiar with the topics

It is recommended for readers who are familiar with the topics to at least gloss over this chapter and make sure they know and understand all the concepts presented here.



0.1 EXERCISES

0.1. Write the following sets explicitly:

- (i) $\{x \in \mathbb{N} \mid 1 < x \leq 7\}$
- (ii) $\{x \in \mathbb{Z} \mid x < 5\}$
- (iii) $\{x \in \mathbb{R} \mid x^2 = -1\}$
- (iv) $\{x \in \mathbb{N} \wedge x \in \mathbb{Q}\}$
- (v) $\{x \in \mathbb{R} \mid x^2 - 3x - 4 = 0\}$
- (vi) $\{x \in \mathbb{R} \mid x < 5 \wedge x \geq 2\}$

0.2. Determine the relation between the sets:

- (i) $A = \{1, 2, 3\}, B = \{1, 2\}$
- (ii) $A = \emptyset, B = \{2, -5, \pi\}$
- (iii) $A = \mathbb{Z}, B = \{\pm x \mid x \in \mathbb{N} \cup \{0\}\}$
- (iv) $A = \{\pi, e, \sqrt{2}\}, B = \mathbb{Q}$

0.3. Write all elements in $S^2 \times W$, where $S = \{\alpha, \beta, \gamma\}$ and $W = \{x, y, z\}$. Find a condition that guarantees $S^2 \times W = W \times S^2$.

0.4. How many different injective functions $f : \{1, 2\} \rightarrow \{1, 2\}$ exist? How many injective functions $f : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ exist? How many inject functions $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ exist for a given $n \in \mathbb{N}$?

0.5. For each of the real functions below, find a set on which it is surjective (use a graphing calculator if you are not familiar with the shape of a function):

$$x^2, x^3 - 5, e^{-x^2/2}, \sin(x), \sin(x) + \cos(x), xe^x.$$

0.6. Given two sets A, B such that $|B| = |A| - 1$, can a bijective function $f : A \rightarrow B$ exist? Explain your answer.

0.7. MORE EXERCISES TO BE WRITTEN...

CHAPTER

1



LINEAR ALGEBRA

(INTUITIVE APPROACH)

Linear algebra is one of the most important and often used fields, both in theoretical and applied mathematics. It brings together the analysis of systems of linear equations and the analysis of linear functions (in this context usually called linear transformations), and is employed extensively in almost any modern mathematical field, e.g. approximation theory, vector analysis, signal analysis, error correction, 3-dimensional computer graphics and many, many more.

In this book, we divide our discussion of linear algebra into two chapters: the first (this chapter) deals with a wider, birds-eye view of the topic: it aims to give an intuitive understanding of the major ideas of the topic. For this reason, in this chapter we limit ourselves almost exclusively to discussing linear algebra using 2- and 3-dimensional analysis (and higher dimensions when relevant) using real numbers only. This allows us to first create an intuitive picture of what is linear algebra all about, and how to use correctly the tools it provides us with.

The next chapter takes the opposite approach: it builds all concepts from the ground-up, defining precisely (almost) all basic concepts and proving them rigorously, and only

then using them to build the next steps. This approach has two major advantages: it guarantees that what we build has firm foundations and does not fall apart at any future point, and it also allows us to generalize the ideas constructed during the process to such extent that they can be used as foundation to build ever newer tools we can apply in a wide range of cases.

Note 1.1 Why present rigorous mathematics in this book?

Rigorous mathematics is rarely necessary for those who are interested in the tools mathematics provides us with, rather than the full and deep understanding of the concepts these tools are based on. However, it can be useful to students of scientific fields to experience rigorous mathematics at least once in their course of study. Usually, the choice for the topic to be analyzed rigorously is between linear algebra and calculus - for this book the latter was chosen.



1.1 VECTORS

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1.2 LINEAR TRANSFORMATIONS

1.3 MATRICES

1.4 SYSTEMS OF LINEAR EQUATIONS

1.5 EIGENVECTORS AND EIGENVALUES

1.6 DECOMPOSITIONS

1.7 SOME REAL LIFE USES OF LINEAR ALGEBRA

1.8 EXERCISES



CALCULUS IN 1D

2.1 SEQUENCES AND SERIES

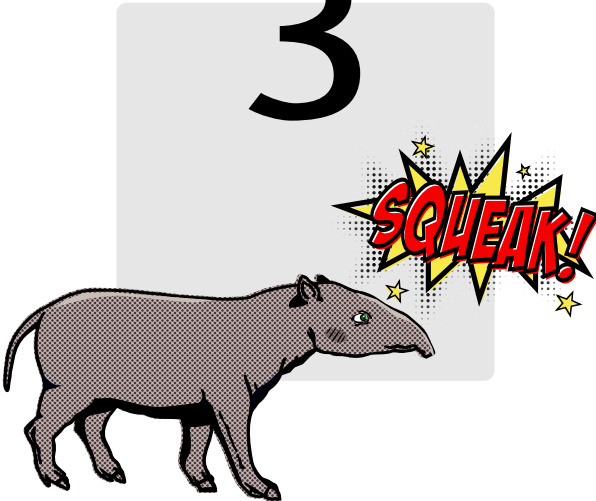
2.2 LIMITS OF REAL FUNCTIONS

2.3 DERIVATIVES

2.4 INTEGRALS

2.5 ANALYZING REAL FUNCTIONS

CHAPTER 3



LINEAR ALGEBRA

(RIGOROUS APPROACH)

Something about formalism, theorems, proofs, etc.

3.1 FIELDS

We begin our dive into the rigorous analysis of linear algebra by defining an algebraic construction call a **field**, which we need in order to properly define vector spaces later. In essence, a field has most of the important properties of the real numbers, namely the closure, commutativity, associativity, identity and inverse of addition and multiplication of any two elements in the field (except the product inverse of the field equivalent object for the number 0). In a later section we will use fields to construct the general notion of **vector spaces**.

Definition 3.1 Field

A field \mathbb{F} is a set of objects together with two operations called **addition** and **multiplication** (denoted $+$ and \cdot , respectively), for which the following axioms hold:

- **Closure of under addition and multiplication:** for any $a, b \in \mathbb{F}$,

1. $(a + b) \in \mathbb{F}$,
2. $(a \cdot b) \in \mathbb{F}$.

- **Commutativity under addition multiplication:** for any $a, b \in \mathbb{F}$,

1. $a + b = b + a$,
2. $a \cdot b = b \cdot a$.

- **Associativity under addition and multiplication:** for any $a, b, c \in \mathbb{F}$,

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

- **Additive and multiplicative identity:** there exist an element in \mathbb{F} called the *additive identity* and denoted by 0 , for which $a + 0 = a$ for any $a \in \mathbb{F}$.

Similarity, there exists an element in \mathbb{F} called the *multiplicative identity* and denoted by 1 , for which $a \cdot 1 = a$ for any $a \in \mathbb{F}$.

- **Additive and multiplicative inverses:** for any element $a \in \mathbb{F}$ (except the additive identity) there exists:

1. $b \in \mathbb{F}$ such that $a + b = 0$, and
2. $c \in \mathbb{F}$ such that $a \cdot c = 1$.

(usually b is denoted as $-a$, while c is denoted as a^{-1})

- **Distributivity of multiplication over addition:** for any $a, b, c \in \mathbb{F}$,

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

 π **3.1.1 Infinite fields**

We start with one of the most obvious examples of a field: the real numbers together with the standard addition and product.

Theorem 3.1 \mathbb{R} as a field

The set of real numbers \mathbb{R} forms a field together with the standard addition and product.

We leave the proof of 3.1 to the reader, as it is pretty straight forward using the known properties of the standard addition and product over \mathbb{R} (and rather uninteresting). Instead, we jump forward to using 3.1 for proving the same idea about the complex numbers:

Theorem 3.2 \mathbb{C} as a field and more more more

The set of complex numbers \mathbb{C} forms a field together with the addition and product operations as defined in ?? (namely ??, ?? and ??).

Proof 3.1 \mathbb{C} as a field

(note: in the following proof, equalities marked with ! use the respective property of the real numbers)

- **Closure under both operations:** for any two complex numbers $z_1 = a + ib$ and $z_2 = c + id$,

- Addition: since addition in \mathbb{R} is closed, $(a+c) \in \mathbb{R}$ and $(b+d) \in \mathbb{R}$. Therefore

$$z = z_1 + z_2 = a + c + (b + d)i$$

is also a complex number with $\Re(z) = a + c$ and $\Im(z) = b + d$.

- Multiplication: since multiplication in \mathbb{R} is also closed, $(ac - bd) \in \mathbb{R}$ and $(ad + bc) \in \mathbb{R}$. Therefore

$$z = z_1 \cdot z_2 = ac - bd + (ad + bc)i$$

is a complex number with $\Re(z) = ac - bdc$ and $\Im(z) = ad + bc$.

- **Commutativity of both operation:** for any two complex numbers $z_1 = a + ib$ and $z_2 = c + id$,

- Addition: since addition in \mathbb{R} is commutative, $a + c = c + a$ and $b + d = d + b$. Therefore

$$z_1 + z_2 = a + c + (b + d)i \stackrel{!}{=} c + a + (d + b)i = z_2 + z_1.$$

- Multiplication: since multiplication in \mathbb{R} is also commutative, $ac - bd = ca - db$ and $ad + bc = da + cb$. Therefore

$$z_1 \cdot z_2 = ac - bd + (ad + bc)i \stackrel{!}{=} ca - db + (da + cb)i = z_2 \cdot z_1.$$

- **Associativity of both operation:** for any three complex numbers $z_1 = a + ib$, $z_2 = c + id$ and $z_3 = g + ih$ (where $a, b, c, d, g, h \in \mathbb{R}^a$),

• Addition: since addition in \mathbb{R} is associative, $a + (c + g) = (a + c) + g$ and $b + (d + h) = (b + d) + h$. Therefore

$$z_1 + (z_2 + z_3) = a + (c + g) + [b + (d + h)]i \stackrel{!}{=} (a + c) + g + [(b + d) + h]i = (z_1 + z_2) + z_3.$$

• Multiplication: since multiplication in \mathbb{R} is also associative, the following equalities apply:

$$a \cdot (c \cdot g) = (a \cdot c) \cdot g,$$

$$b \cdot (c \cdot h) = (b \cdot c) \cdot h,$$

$$a \cdot (d \cdot h) = (a \cdot d) \cdot h,$$

$$b \cdot (d \cdot g) = (b \cdot d) \cdot g,$$

$$a \cdot (c \cdot h) = (a \cdot c) \cdot h,$$

$$a \cdot (d \cdot g) = (a \cdot d) \cdot g,$$

$$b \cdot (c \cdot g) = (b \cdot c) \cdot g,$$

$$b \cdot (d \cdot h) = (b \cdot d) \cdot h.$$

Therefore,

$$\begin{aligned} z_1 \cdot (z_2 \cdot z_3) &= a \cdot (c \cdot g) - a \cdot (d \cdot h) - b \cdot (c \cdot h) - b \cdot (d \cdot g) \\ &\quad + [a \cdot (c \cdot h) + a \cdot (d \cdot g) + b \cdot (c \cdot g) - b \cdot (d \cdot h)]i \\ &\stackrel{!}{=} (a \cdot c) \cdot g - (a \cdot d) \cdot h - (b \cdot c) \cdot h - (b \cdot d) \cdot g \\ &\quad + [(a \cdot c) \cdot h + (a \cdot d) \cdot g + (b \cdot c) \cdot g - (b \cdot d) \cdot h]i \\ &= (z_1 \cdot z_2) \cdot z_3. \end{aligned}$$

- **Identity for both operations:**

• Addition: the complex number $0 = 0 + 0i$ is the complex addition identity: for any real number $x \in \mathbb{R}$, $x + 0 = x$. Therefore, for any complex number $z = a + ib$,

$$z + 0 = a + ib + 0 + 0i = a + 0 + (b + 0)i \stackrel{!}{=} a + ib.$$

• Multiplication: the complex number $1 = 1 + 0i$ is the complex multiplication identity: for any real number $x \in \mathbb{R}$, $x \cdot 1 = x$ and $x \cdot 0 = 0$. Therefore, for any complex number $z = a + ib$,

$$z \cdot 1 = (a + ib) \cdot (1 + 0i) \stackrel{!}{=} a \cdot 1 - \cancel{b \cdot 0i} + (\cancel{a \cdot 0i} + b \cdot 1)i = a + ib.$$

- **Inverse for both operations:**

- **Addition:** for any complex number $z_1 = a + ib$, the number $z_2 = -a - ib$ is also a complex number for which

$$z_1 + z_2 = a + ib + -a - ib \stackrel{!}{=} a - a + (b - b)i = 0 + 0i = 0.$$

- **Multiplication:** for any complex number $z = re^{i\theta}$ where $r \neq 0$, the number $z^{-1} = \frac{1}{r}e^{-i\theta}$ is also a complex number for which

$$z \cdot z^{-1} = re^{i\theta} \cdot \frac{1}{r}e^{-i\theta} \stackrel{!}{=} \frac{r}{r}e^{i\theta - i\theta} = 1 \cdot 1 = 1.$$

Note: for $z = a + ib$,

$$z^{-1} = \frac{1}{r}e^{-i\theta} = \frac{1}{|z|} \cdot \frac{a - ib}{|z|} = \frac{1}{|z|} \cdot \frac{\bar{z}}{|z|} = \frac{\bar{z}}{|z|^2}.$$

Therefore, for any $z \neq 0$, $z^{-1} = \frac{\bar{z}}{|z|^2}$.

- **Distributivity of multiplication over addition:** for any $z_1 = a + ib$, $z_2 = c + id$ and $z_3 = g + ih$,

$$\begin{aligned} z_1 \cdot (z_2 + z_3) &= (a + ib) \cdot (c + id + g + ih) = (a + ib) \cdot (c + g + [d + h]i) \\ &= ac + ag + (bd)i^2 + (bh)i^2 \\ &\quad + (ad)i + (ah)i + (bc)i + (bg)i \\ &= ac + ag - bd - bh + (ad + ah + bc + bg)i \\ &= ac - bd + (ad + bc)i + ag - bh + (ah + bg)i \\ &= (z_1 \cdot z_2) + (z_1 \cdot z_3). \end{aligned}$$

^aThe letters g and h are used instead of e and f to avoid confusion with Euler's constant and the common notation for real functions, respectively.

QED

The sets \mathbb{R} and \mathbb{C} are examples of **infinite fields**, since they each have infinite number of elements. The set \mathbb{Q} (rational numbers) can be shown to also be an infinite field, however unlike \mathbb{R} and \mathbb{C} it has **countable** number of elements, i.e. each number in \mathbb{Q} can be assigned an index $1, 2, 3, \dots$ ¹.

Challenge 3.1 \mathbb{Q} as a field

Prove that \mathbb{Q} (together with the usual addition and product operation) is indeed a field.

?

¹For proof, see ...

3.1.2 Finite fields

While all three examples of fields we encountered so far have each an infinite number of elements, some fields only have a finite number of elements (called their **order**). For example, consider the set $S = \{0, 1, a, b\}$ and the addition and product operations described using the following tables (left table describes addition, right table describes multiplication):

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

By examining the tables above, several points become clear:

- all the possible combinations of operands in both addition and multiplication give elements from S itself, meaning that the set is closed under both these operations.
- both tables are symmetric around their main diagonal, meaning that both addition and multiplication are commutative operations.
- in the addition table, the first row and first column both show that $x + 0 = x$ for any $x \in S$, meaning that 0 is the additive identity in S .
- in the product table, the second row and second column both show that $x \cdot 1 = x$ for any $x \in S$, meaning that 1 is the multiplicative identity in S .
- in the addition table, the element 0 appears in each row and each column exactly once. This means that every element x has a single additive inverse $y \in S$.
- in the product table, the element 1 appears in each row and each column exactly once, except for the first row and first column. This means that every element $x \neq 0$ has a single multiplicative inverse $z \in S$.

We therefore only need to prove two points to show that S is a field together with the operations described by the above tables: associativity of both operations and distributivity of multiplication over addition. We leave these proofs as a challenge to the reader. Such a field is sometime denoted as \mathbb{F}_4 . There are, of course, infinitely many finite fields.

3.1.3 Modulo fields

Another example of finite fields are sets of integers of the form $\{0, 1, 2, 3, \dots, n\}$ where n is a prime, together with **modular addition** and **modular product**. To understand modular arithmetics, we recall the fact that on a circle, an angle can have a negative value but also greater than 360° values are possible (see ??): 390° is equivalent to 30° , -30° is equivalent to 330° , etc. The set of integer values $0^\circ, 1^\circ, 2^\circ, \dots, 359^\circ$ on a circle is

an example of a modular set: if for example we add together two angles of values $\text{deg } 100$ and $\text{deg } 300^\circ$ we get the equivalent angle $\text{deg } 60$. If we subtract $\text{deg } 300$ from $\text{deg } 100$ the result is an angle of $\text{deg } 160$.

We say that on a circle, the values $360^\circ, 720^\circ, -360^\circ$ etc. are all **congruent** to 0 modulo 360. In mathematical notation we represent this fact as e.g.

$$720 \equiv 0 \pmod{360}. \quad (3.1.1)$$

Note that from this point forward we drop the degrees unit, and deal with pure integers. The notation for the set $\{0, 1, 2, \dots, 359\}$ is \mathbb{Z}_{360} . Generally speaking, the set $\{0, 1, 2, \dots, n\}$ is denoted as \mathbb{Z}_n .

Note 3.1 About modulo set notation

It is not common to use the notation \mathbb{Z}_n for the modulo- n set, since it is also used for a different algebraic construct, namely the n -adic ring. However, due to the simplicity of the notation, and the fact that we don't discuss rings in this chapter we are using it in this book. Common notations for the set are $\mathbb{Z}/n\mathbb{Z}$ and \mathbb{Z}/n .

Addition and multiplication on \mathbb{Z}_n is done by the following rather straight forward definition:

Definition 3.2 Operations in \mathbb{Z}_n

In the set \mathbb{Z}_n addition and multiplication are defined as the following:

- **Addition:** for any two elements $a, b \in \mathbb{Z}_n$, $a + b := (a + b) \pmod{n}$.
- **Multiplication:** for any two elements $a, b \in \mathbb{Z}_n$, $a \cdot b := (a \cdot b) \pmod{n}$.

Example 3.1 Operations in \mathbb{Z}_n

The tables below show addition and multiplication results of numbers in different modulo sets \mathbb{Z}_n for some values of n :

n	$2 + 3$	$2 \cdot 3$	n	$4 + 7$	$4 \cdot 7$
4	1	2	8	3	4
5	0	1	9	2	1
6	5	0	10	1	8
7	5	6	15	11	13
8	5	6	20	11	8
9	5	6	27	11	1
10	5	6	28	11	0
11	5	6	30	11	28

Figure 3.1 shows the equivalency between integers and the elements of \mathbb{Z}_5 .

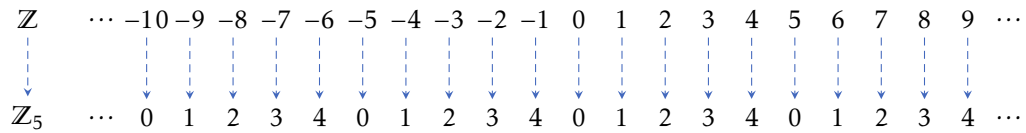


Figure 3.1 An example of the periodicity of \mathbb{Z}_5 : the top numbers are the ordinary integers, each showing their respective congruent modulo 5 below (blue dashed arrow).

Only the sets \mathbb{Z}_n for which n is a prime number are also fields. Let's define this property precisely:

Theorem 3.3 \mathbb{Z}_p is a field

Any modulo set \mathbb{Z}_p where p is a prime number greater than 1 is also a field together with the operations as defined in 3.2.

In order to prove 3.3 we use two lemmas: the first is known as **Bézout's lemma**:

Lemma 3.1 Bézout's lemma

For any two positive integers a, b there exist two integers x, y such that

$$\gcd(a, b) = xa + yb.$$

Note 3.2 $\gcd(a, b)$

$\gcd(a, b)$ is the **greatest common divisor** of the two integers a and b . For example, $\gcd(36, 24) = 12$ since the divisors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36, and the divisors of 24 are 1, 2, 3, 4, 6, 8, 12, 24.

An example of Bézout's lemma is the following:

Example 3.2 Bézout's lemma in action

For the two positive integers $a = 60$, $y = 114$

$$\gcd(60, 114) = 6.$$

Therefore, Bézout's lemma says that there exist two integers x, y such that

$$6 = 60x + 114y.$$

Indeed, two such integers exist: $x = 2$ and $y = -1$.

(SHOULD WE PROVE THE LEMMA?..)

The second lemma we use is the following:

Lemma 3.2 $\gcd(n, p) = 1$

Given a positive prime number p , then for any positive integer $n < p$,

$$\gcd(p, n) = 1.$$

—○

Proving the lemma:

Proof 3.2 $\gcd(n, p) = 1$

We assume that $\gcd(p, n) \neq 1$. Then there exist an integer $a \leq n < p$ which divides both n and p , meaning that p has a divider, contrary to the assumption that p is a prime number. Therefore $\gcd(n, p)$ must equal 1.

QED

Now we can proceed to the proof of 3.3:

Proof 3.3 \mathbb{Z}_p is a field

- **Closure under both operations:** the definition of the modulo operator limit any $M \pmod{p}$ (where $M \in \mathbb{Z}$) to be in $[0, p - 1]$. Therefore the result of using the operators given in 3.2 must be within the same range, and thus in \mathbb{Z}_p .
- **Commutativity and associativity of both operations:** for any two numbers $a, b \in \mathbb{Z}_p$ the result $a + b$ and $a \cdot b$ under \mathbb{Z} is both commutative and associative. Therefore the result modulo n is the same no matter the order of operations.
- **Additive identity:** the number $0 \in \mathbb{Z}_p$ is the additive identity, since for each $a \in \mathbb{Z}_p$, $a + 0 = a$.
- **Multiplicative identity:** the number $1 \in \mathbb{Z}_p$ is the additive identity, since for each $a \in \mathbb{Z}_p$, $a \cdot 1 = a$.
- **Additive inverse:** for each $a \in \mathbb{Z}_p$ the element $n = p - a$ is in \mathbb{Z}_p since $p > a$. Adding n to a results in 0:

$$a + n = a + (p - a) = p \equiv 0 \pmod{p}.$$

- **Multiplicative inverse:** let $a \in \mathbb{Z}_p$ and $a \neq 0$. Since p is a prime, $\gcd(a, p) = 1$ and from Bézout's theorem we know that there exist two integers x, y such that

$$xa + yp = 1.$$

Rearrangement gives $p = \frac{1 - xa}{y}$ meaning that p divides $1 - xa$, and thus

$$xa \equiv 1 \pmod{p}.$$

Therefore x is the multiplicative inverse of a .

- **Distributivity of multiplication over addition:** ...

QED

The only part of the proof that uses the fact that p is a prime number is the multiplicative inverse. When n is not a prime, \mathbb{Z}_n is not a field.

Challenge 3.2 \mathbb{Z}_n is not a field when n is not a prime number

Prove that the modulo set \mathbb{Z}_n where n is **not** a prime number, is not a field. (hint: what property of prime numbers is used in the above proof to show that there is always a multiplicative inverse in \mathbb{Z}_p where p is prime?)

?

3.2 VECTOR SPACES

As we've seen in [Chapter 1](#) vectors are found at the heart of linear algebra. We first defined them in a geometric way as objects with magnitude and direction, and later as lists of real numbers, analyzing the connections between these two mostly parallel definitions. We also spoke about vector spaces of the type \mathbb{R}^n as the structures vectors exist in. However, we haven't defined vectors nor vector spaces formally - which is exactly what we do in this section, by defining the concept of **vector spaces**.

Note 3.3 \mathbb{R}^n as a guide to general vector spaces

While reading the definition below, it is worthwhile to reflect on each of the given axioms as it relates to the familiar vector space \mathbb{R}^n .

!

Definition 3.3 Vector space

A vector space over a field \mathbb{F} is a set V which, together with two operations described below, fulfils a list of axioms. The two operations are

- **Vector addition:** an operation which takes two elements of V and returns a single element of V , i.e. $+: V \times V \rightarrow V$.
- **Scalar multiplication:** an operation which takes a single element of \mathbb{F} and a single element of V and returns a single element of V , i.e. $\cdot: \mathbb{F}, V \rightarrow V$.

The axioms to be fulfilled are:

- **Commutativity of vector addition:** for any $u, v \in V$,

$$u + v = v + u.$$

- **Associativity of vector addition:** for any $u, v, w \in V$,

$$u + (v + w) = (u + v) + w.$$

- **Additive identity:** there exist an element $0 \in V$ for which, for any $v \in V$,

$$v + 0 = v.$$

- **Scalar multiplicative identity:** for any $v \in V$

$$1 \cdot v = v,$$

where 1 is the multiplicative identity in \mathbb{F} .

- **Additive inverse:** for any $v \in V$ there exist an element $u \in V$ for which

$$v + u = 0.$$

- **Associativity of scalar multiplication:** for any $\alpha, \beta \in \mathbb{F}$ and $v \in V$

$$\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v,$$

where $\alpha\beta$ is the multiplication defined for \mathbb{F} .

- **Distributivity of vector addition:** for any $\alpha \in \mathbb{F}$ and $u, v \in V$,

$$\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v).$$

- **Distributivity of scalar addition:** for any $\alpha, \beta \in \mathbb{F}$ and $v \in V$,

$$(\alpha + \beta) \cdot v = (\alpha \cdot v) + (\beta \cdot v).$$

The elements of V are then called **vectors**, and the elements of \mathbb{F} are called **scalars**.

π

Since we discussed \mathbb{R}^n thoroughly in [Chapter 1](#), let's prove that it is indeed a vector space under the above definition. First, the claim:

Theorem 3.4 \mathbb{R}^n is a vector space

The set of elements of the form

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

where $v_i \in \mathbb{R}$, forms a vector space over \mathbb{R} together with the following two operations:

- **Vector addition:**

$$\vec{u} + \vec{v} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{bmatrix}.$$

- **Scalar multiplication:**

$$\alpha \cdot \vec{v} = \begin{bmatrix} \alpha v_1 \\ \alpha v_2 \\ \vdots \\ \alpha v_n \end{bmatrix}.$$



The proof itself is pretty easy, based on the fact that \mathbb{R} is a field:

Proof 3.4 \mathbb{R}^n is a vector space

Since the results of both operations defined for \mathbb{R}^n only depend on the respective components of a vector $v \in \mathbb{R}^n$, all the axioms of a vector space apply, since they derive directly from the fact that \mathbb{R} is a field. As an example, we will elaborate on two of the axioms:

- **Additive inverse:** Given a vector $\vec{v} \in \mathbb{R}^n$, each of its components v_i has an inverse under \mathbb{R} , namely $-v_i$. Therefore,

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} + \begin{bmatrix} -v_1 \\ -v_2 \\ \vdots \\ -v_n \end{bmatrix} = \begin{bmatrix} v_1 - v_1 \\ v_2 - v_2 \\ \vdots \\ v_n - v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \vec{0},$$

which is the additive identity in \mathbb{R}^n .

- **Distributivity of vector addition:** for each component of two vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$, given the rules for vector addition and scalar multiplication, together with the distributivity of numbers in \mathbb{R} :

$$\begin{aligned} \alpha(\vec{u} + \vec{v}) &= \alpha \left(\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \right) = \alpha \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{bmatrix} \\ &= \begin{bmatrix} \alpha u_1 + \alpha v_1 \\ \alpha u_2 + \alpha v_2 \\ \vdots \\ \alpha u_n + \alpha v_n \end{bmatrix} = \begin{bmatrix} \alpha u_1 \\ \alpha u_2 \\ \vdots \\ \alpha u_n \end{bmatrix} + \begin{bmatrix} \alpha v_1 \\ \alpha v_2 \\ \vdots \\ \alpha v_n \end{bmatrix} = \alpha \vec{u} + \alpha \vec{v}. \end{aligned}$$

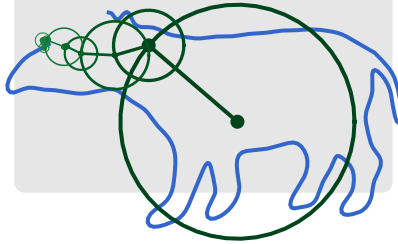
QED

(it is advisable for the reader to go over the rest of the axioms and prove them for \mathbb{R}^n)

3.3 EXERCISES

CHAPTER

4

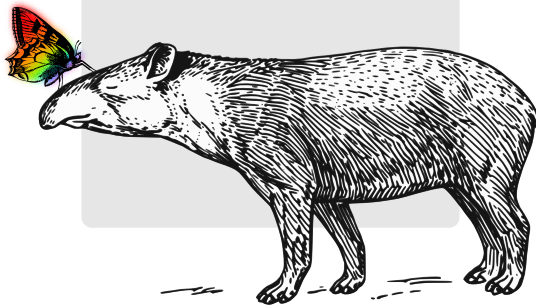


FOURIER TRANSFORM

4.1 EXERCISES

CHAPTER

5



SYMMETRY GOURPS

5.1 EXERCISES
