Real Analysis

P. Ouwehand

Department of Mathematics and Applied Mathematics
University of Cape Town

Note to the Student

These notes are a *very rough first draft* for a short course in Real Analysis at the undergraduate level. This is the first time that I am teaching this particular course, and I'm still thinking hard about how to present the material; I'm likely to change my mind at short notice. At present, these notes are *unfinished*, i.e. still being written. There is no guarantee that you will be provided with a finished product by the end of this course, though I will try to do so. These notes are therefore meant as a *supplement* to the notes you take in class, and are *not* a *substitute.* Expect mistakes, but note that though all mistakes are *my* fault, it's *your* responsibility to find and correct them.

How will you do that? Go to the library, which houses many books on real analysis. Two books that you will find particularly useful are *Principles of Mathematical Analysis*, by Walter Rudin, and *The Elements of Real Analysis*, by Robert G. Bartle.

This course is but thirty lectures long. There is more material in the notes than can be covered in class, and many sections can be safely ignored. (Already the preliminary Chapter 0 is ridiculously long, and needs some serious editing.) What you need to know, and what you can omit, will be made clear in lectures.

The content of the course remains similar to what it has been in previous years, though the perspective has shifted slightly: More emphasis is placed on the the importance of *sets* of reals, and on *topological* notions. I'm also hoping to tackle some additional topics, such as the Riemann–Stieltjes integral, if time permits.

Peter Ouwehand
June 2004

Contents

Chapter 0

Preliminaries

0.1 What is Analysis?

Roughly speaking, analysis deals with numbers, sets of numbers, and operations on numbers. It is particularly concerned with what happens if certain operations are performed an arbitrarily large number of times, perhaps infinitely often.

These days we perform most calculations on a computer. Now a computer can handle only rational numbers: Each number is stored using only a finite number of bits, 0 and 1, and thus necessarily rational. For example,

$$101.11_{\text{binary}} = (1)(2^2) + (0)(2^1) + (1)(2^0) + (1)(2^{-1}) + (1)(2^{-2}) = \frac{23}{4}$$

It is clear, therefore, that any number expressed in finitely many bits is equal to $\frac{\text{integer}}{\text{power of 2}}$, and thus necessarily rational.

Since practically all our calculations are handled by computers, and since computers handle only rational numbers, it would seem that the set of rational numbers is sufficiently rich for all our calculations. However, *we* can imagine an operation being performed infinitely often, something that a computer cannot do. Allowing the infinite to creep into our operations results in the creation of something new, namely *irrational numbers.*

For example, start with 1 and perform the following operations over and over: add 1, invert the result, and then add 1, i.e.

$$\begin{aligned} x_0 &= 1 \\ x_{n+1} &= \frac{1}{x_n + 1} + 1 \qquad \text{for } n \geq 1 \end{aligned}$$

Each x_n is a *rational* number (i.e. a *ratio* of integers). If we perform this operation infinitely often, we "get" $\sqrt{2}$, i.e. the limit of the x_n is $\sqrt{2}$, an *irrational* number[1].

[1] A proof that $\sqrt{2}$ is irrational, i.e. not the ratio of two integers, will be provided shortly.

Also consider the following pseudo–code:

```
LET $X = 1$;
LET $Y = 1$;
FOR $N = 1$ TO $\infty$ {
    LET $Y = Y/N$;
    LET $X = X + Y$;
                    }
PRINT $X$;
```

Of course, the output is just $\sum_{n=1}^{\infty} \frac{1}{n!} = e$ Thus this algorithm starts with two rational values for X and Y, and uses only the operations of addition and division. Both these operations preserve rational numbers, yet the output of this algorithm is an irrational number.

In the first example, we took the limit of a sequence of rational numbers, and in the second a limit of a sum of rational numbers. The concept of *limit* captures the notion performing an operation infinitely often. The rational numbers are not sufficiently rich to handle limits, forcing us to extend the number system to also include irrational numbers. Thus the set of *real* numbers is in essence obtained from the set of rational numbers by allowing the taking limits.

The notion of limit is fundamental to analysis, and many of the results we prove in these notes about the set of real numbers are simply not true for the set of rational numbers. Most of the fundamental concepts of calculus involve limits.

- A derivative is a limit:
$$\frac{df}{dx} = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$
- A Taylor series is a limit:
$$e^x = \sum_{k=1}^{\infty} \frac{x^k}{k!} = \lim_{n \to \infty} \sum_{k=1}^{n} \frac{x^k}{k!}$$
If we write $p_n(x) = \sum_{k=1}^{n} \frac{x^k}{k!}$, then each $p_n(x)$ is a polynomial. Thus we have here a sequence of polynomials whose limit is *not* a polynomial. Again, the taking of limits has created a new kind of object.
Similarly, every Fourier series is a limit of sums.
- A definite integral is a limit: If f is continuous on the interval $[a, b]$, then $\int_a^b f(x)\, dx$ is a limit of left–hand sums
$$\int_a^b f(x)\, dx = \lim_{\Delta x \to 0} \sum_{k=1}^{[\frac{b-a}{\Delta x}]} f(a + k\Delta x)\Delta x$$
Here $[y]$ denotes the greatest integer less than or equal to y.
- *Continuity* is defined in terms of a limit: A function f is continuous at a point x_0 if and only if $\lim_{h \to 0} f(x_0 + h) = f(x_0)$.

0.2 Basic Set Theory

Because it became accepted in the 20th century that, in principle, mathematical objects should be sets and mathematical notions should be expressible as relationships between sets, every mathematician needs just a little set theory. The material in this section is not difficult, and no doubt you have seen it all before. We include it merely as a reminder and to fix notation.

$$\boxed{\text{Intuitively, a } \textit{set} \text{ is just a collection of objects.}}$$

If A is a set and x is some mathematical object, we say that

$$x \in A \qquad (x \text{ is an } \textbf{element} \text{ of } A)$$

if x is amongst the objects collected in A, and we write

$$x \notin A$$

if it isn't.

The idea is that a set is *characterized entirely by its elements.* Thus if two sets A and B have exactly the same elements, then we must have $A = B$. For example, the sets $A = \{a\}$ and $B = \{a, a\}$ have the same elements, namely only a. Thus $A = B$. The fact that B seems to have two copies of A is immaterial.

For the philosophically minded: This means, for example that

$$\{\text{Evening Star}\} = \{\text{Morning Star}\}$$

as both sets are equal to the {planet *Venus*}. Yet the Evening Star is seen only in the evening, whereas the Morning Star is seen only in the morning...

Instead of *set*, we will also sometimes say *class*, *collection* or *family*; instead of saying *x is an element of A* we will sometimes say *x is a member of A* or *x belongs to A*.

There are two ways to represent sets: (i) by *listing* its elements, and (ii) by some defining *property.* For example, if a set A has finitely many elements $a_1, \ldots, a_n$ then it can be represented by $A = \{a_1, a_2, \ldots, a_n\}$. On the other hand if A is the set of all x having a certain property $P(x)$, then A can be denoted by $A = \{x : P(x)\}$.

Example 0.2.1 The set A of all integers between -1 and 3 can be represented in two ways:

(i) $A = \{-1, 0, 1, 2, 3\}$

(ii) $A = \{n : n \text{ is an integer and } -1 \leq n \leq 3\}$

□

In analysis, the following sets are important:

- The set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- The set of integers or whole numbers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- The set of rational numbers $\mathbb{Q} = \{\frac{n}{m} : n, m \in \mathbb{Z}, m \neq 0\}$

- The set of real numbers $\mathbb{R}$, and the set of non–negative real numbers is denoted by $\mathbb{R}^+$.
- The set of complex numbers $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$

Another way to represent a set is by *indexing* its elements using another set. This is actually just a method of listing the elements of the set in some coherent way. We write $A = \{a_i : i \in I\}$. Here a_i are the elements of A indexed by the set I. Basically, the set I can be thought of as a set of labels attached in some way to the elements of A.

For example, define $x_n = 2n$. Then $\{x_n : n \in \mathbb{N}\}$ is the set of even numbers, indexed by $\mathbb{N}$.

Or define, for $r \in \mathbb{R}^+$, I_r to be the interval $(-r, r)$. Then $\{I_r : r \in \mathbb{R}^+\}$ is the set of all open intervals centered at zero.

A set doesn't even have to have any elements:

Definition 0.2.2 We define the *empty set* to be the set with no members, and denote it by the symbol $\emptyset$.

□

For example, $\{x : x \in \mathbb{R} \text{ and } x^2 < 0\} = \emptyset$. One could also define the empty set by $\emptyset = \{x : x \neq x\}$. The empty set plays roughly the same role in set theory that the number zero plays in ordinary mathematics.

Definition 0.2.3 We say that a set A is a *subset* of another set B, and write

$$A \subseteq B$$

if and only if every element of A is also an element of B.

We say that A is a *proper subset* of B if A is subset of B, but $A \neq B$.

□

We may also write $B \supseteq A$ instead of $A \subseteq B$; they mean the same thing (just as $x \leq y$ and $y \geq x$ mean the same thing).

Remarks 0.2.4 Note that $A = B$ if and only if $A \subseteq B$ *and* $B \subseteq A$.
Further note that

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

□

Exercises 0.2.5 (1) Prove that $\emptyset$ is a subset of every set.
[Hint: Give a proof by contradiction. Assume that there is a set A such that $\emptyset \not\subseteq A$.]

(2) Show formally that if $A \subseteq B$ and if $B \subseteq C$, then $A \subseteq C$.

□

0.2.1 Operations on sets

There are several ways of combining sets to form new sets. In this section we define and give some examples of the set–operations *union, intersection, difference, complementation, cartesian product* and *power set formation.*

Definition 0.2.6 (Union, intersection and difference of two sets)
Suppose that A, B are sets.

(a) The *union* of A and B is the set of all elements which are either in A or in B (or both).

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

(b) The *intersection* of A and B is the set of all elements which belong to *both* A and B.

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

(c) The *set difference* of A and B is the set of all elements which belong to A, but not to B.

$$A - B = \{x : x \in A \text{ and } x \notin B\}$$

□

Two sets A, B are said to be *disjoint* if they have no members in common, i.e. if $A \cap B = \emptyset$. In that case, $A - B = A, B - A = B$.

Often we work within some *universe*, which is just the set of all objects under consideration at that time. The sets that we deal with are then typically subsets of the universe. *Which* set is the universe depends very much on context. If one is dealing with real numbers, the obvious choice of universe is $\mathbb{R}$, but if one is dealing with complex numbers as well, then it would be $\mathbb{C}$. If one is trying to find the solution of an n^{th} order differential equation, then the universe will generally be the set of all n–times differentiable functions.

Given a universe, we also have a unary operation on sets, called *complementation.*

Definition 0.2.7 Let the universe be Ω, and let $A \subseteq \Omega$. The *complement* of A is the set of all elements in the universe which are not in A.

$$A^c = \{x \in \Omega : x \notin A\}$$

□

Note that $A^c = \Omega - A$. Also note that $A - B = A \cap B^c$.

Exercise 0.2.8 Show that A, B are disjoint if and only if $A \subseteq B^c$.

□

Here are some standard identities involving the operations:

Proposition 0.2.9 *Suppose that A, B, C are subsets of some universe Ω.*

(a) Idempotent laws:

$$A \cup A = A; \qquad A \cap A = A$$

(b) Commutative laws:

$$A \cup B = B \cup A; \qquad A \cap B = B \cap A$$

(c) Associative laws:

$$(A \cup B) \cup C = A \cup (B \cup C); \qquad (A \cap B) \cap C = A \cap (B \cap C)$$

(d) Distributive laws:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C); \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

(e) Absorption laws:

$$A \cup (A \cap B) = A; \qquad A \cap (A \cup B) = A$$

(f) Complementation laws:

$$A \cup A^c = \Omega; \qquad A \cap A^c = \emptyset$$
$$(A^c)^c = A$$

(g) De Morgan's laws:

$$(A \cap B)^c = A^c \cup B^c; \qquad (A \cup B)^c = A^c \cap B^c$$

□

Note that each of the identities remains true if

- $\cap$ and $\cup$ are interchanged, and
- $\emptyset$ and Ω are interchanged.

Proof: We show how to prove one of the above laws, and leave the remainder as an exercise. Let us prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

First suppose that $x \in A \cap (B \cup C)$. Then $x \in A$ *and* $x \in B \cup C$, by definition of $\cap$. Thus $x \in A$ and *either* (1) $x \in B$, *or* (2) $x \in C$ (or both), by definition of $\cup$. Thus either (1) $x \in A$ and $x \in B$, *or* (2) $x \in A$ and $x \in C$. It follows that either (1) $x \in A \cap B$ *or* (2) $x \in A \cap C$, and thus that $x \in (A \cap B) \cup (A \cap C)$. We have now shown that if $x \in A \cap (B \cup C)$, then also $x \in (A \cap B) \cup (A \cap C)$, i.e. that

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \qquad (*)$$

Next, assume that $x \in (A \cap B) \cup (A \cap C)$. Then either (1) $x \in A \cap B$, *or* (2) $x \in A \cap C$. In either case, it follows that $x \in A$. Also we must have either (1) $x \in B$, *or* (2) $x \in C$, and thus $x \in B \cup C$. We see, therefore, that we have *both* $x \in A$ *and* $x \in B \cup C$, so that

$x \in A \cap (B \cup C)$. It follows that whenever $x \in (A \cap B) \cup (A \cap C)$, then also $x \in A \cap (B \cup C)$, i.e. that

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \tag{†}$$

Putting $(*)$ and (†) together, we obtain

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

as required.

$\dashv$

Exercise 0.2.10 Prove the remaining identities in the proposition above.
(By the way, drawing a Venn diagram does **not** constitute a proof! Venn diagrams work only when you are dealing with a small number of sets.)

□

A set is completely determined by its elements. The order in which those elements are arranged does not matter. For example, $\{a, b\} = \{b, a\}$. When we want the order to matter, we have to deal with ordered tuples. An *ordered pair* is denoted by (a, b), and should be thought of as a collection containing a and b, *in that order.* Thus $(a, b) \neq (b, a)$. Note that

$$(a, b) = (c, d) \iff a = c \text{ and } b = d$$

Generally, an *ordered n–tuple* is denoted by $(a_1, a_2, \dots, a_n)$, and should be thought of as a collection containing $a_1, a_2, \dots, a_n$, *in that order.*

The pair (a, b) is often defined to be the *set* $\{\{a\}, \{a, b\}\}$. You can check that this definition yields the required property that $(a, b) = (c, d)$ iff $a = c$ and $b = d$.
(a, b, c) is then defined to be $(a, (b, c))$ (which is just the set $\{\{a\}, \{a, \{\{b\}, \{b, c\}\}\}\}$), etc. This is in keeping with the notion that all mathematical objects should be sets. On first encounter, however, you might find this arbitrary, clumsy, and unnecessary, and you wouldn't be far wrong: The *main* thing that you need to keep in mind is that *an ordered tuple is a collection in which the order matters.*

Using ordered tuples, we can define one more way of making new sets from old:

Definition 0.2.11 (Cartesian product) Suppose that $A_1, A_2, \dots, A_n$ are sets. The *cartesian product* of $A_1, \dots, A_n$ is the set of *all* n–tuples $(a_1, \dots, a_n)$, with each $a_k \in A_k$.

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) : a_k \in A_k \text{ for } k = 1, 2, \dots, n\}$$

□

Example 0.2.12 If $A = \{a, b\}$ and $B = \{1, 2, 3\}$, then their product is the 6–element set

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

□

Proposition 0.2.13 *If A has n elements and B has m elements, then $A \times B$ has $n \times m$ elements.*

$\dashv$

Exercises 0.2.14 (1) Prove the preceding theorem by induction.
[Hint: Let B be a fixed set with m elements, and proceed by induction on the number of elements in A. First show that if A has 0 elements, then $A \times B$ has $0 \cdot m$ elements. Now *assume* that whenever A has $n = k$ elements, $A \times B$ has km elements. Show that this implies that if A has $n = k + 1$ elements, then $A \times B$ has $(k + 1)m$ elements.]

(2) Prove that $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(3) Is it true that $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$?

□

We will identify the sets $(A \times B) \times C$ and $A \times (B \times C)$ with $A \times B \times C$, although, strictly speaking, they are not equal.

For example, $((a, b), c))$ is an element of the first set, but not of the second or third. $(a,(b, c))$ belongs to the second, but not to the first or third. (a, b, c) belongs to the third, but not to the first two. However, we shall simply *identify* $(a,(b, c)),((a, b), c)$ and (a, b, c), i.e. we shall not distinguish between them. After all, all that matters is the order of a, b, c and that is the *same* in each of these tuples.

Example 0.2.15 The n–dimensional Euclidean space, denoted by $\mathbb{R}^n$, is just the n–fold cartesian product of $\mathbb{R}$:

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ times}} = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R}\}$$

We will identify the sets $\mathbb{R}^n \times \mathbb{R}^m$ and $\mathbb{R}^{n+m}$.

Strictly speaking, the first is the set

$$\mathbb{R}^n \times \mathbb{R}^m = \{((x_1, \ldots, x_n), (y_1, \ldots, y_m)) : x_i, y_j \in \mathbb{R}\}$$

whereas the second set is

$$\mathbb{R}^{n+m} = \{(x_1, \ldots, x_n, y_1, \ldots, y_m) : x_i, y_j \in \mathbb{R}\}$$

but the two sets clearly have the same basic structure, in that they are made up of tuples with x_1 followed by x_2, ..., followed by y_m.

□

Exercises 0.2.16 (1) Draw the following sets in the xy–plane (i.e. $\mathbb{R}^2$):

(i) $\{-1, 2, 3\} \times \{3, 4, 5\}$

(ii) $\{1\} \times [0, 1]$

(iii) $[0, 1] \times \{1\}$

(iv) $(0, 1] \times [2, 3)$

(2) Describe the set $[0,1] \times [0,1] \times [0,1]$.

(3) Consider the cylinder of unit radius about the z–axis in $\mathbb{R}^3$:

$$\mathcal{C} = \{(x,y,z) : x^2 + y^2 = 1\}$$

Represent $\mathcal{C}$ as a product of two sets.

□

Thus far, we have considered union, intersection and cartesian product as *binary operations*, involving just two sets. Frequently, however, we may need to consider these as *infinitary* operations: We can, for example, take the union of infinitely many sets. We define the union, intersection and cartesian product of a family of sets as follows:

Definition 0.2.17 (Union, intersection and product of a family of sets)
If $\mathcal{A} = \{A_i : i \in I\}$ is a family of sets, we may define

(a) the *union*

$$\bigcup \mathcal{A} = \bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\}$$

(b) the *intersection*

$$\bigcap \mathcal{A} = \bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for all } i \in I\}$$

(c) the *cartesian product*

$$\prod \mathcal{A} = \prod_{i \in I} A_i = \{(a_i)_I : a_i \in A_i \text{ for all } i \in I\}$$

Here $(a_i)_I$ is a generalized tuple, indexed by I.
In essence, $(a_i)_I$ is a function with domain I and range $\bigcup\limits_{i \in I} A_i$. We will return to this later.

We will frequently write $\bigcup\limits_{I} A_i$ or $\bigcup_i A_i$ instead of $\bigcup\limits_{i \in I} A_i$. We will also write $\bigcup\limits_{n=1}^{\infty} A_n$ instead of $\bigcup\limits_{n \in \mathbb{N}} A_n$. The same holds for $\bigcap$ and $\prod$.

□

Remarks 0.2.18 Note that

(i) $\bigcup\{A, B\} = A \cup B$

(ii) $\prod\{A, B, C\} = A \times B \times C$

(iii) $\bigcap\{X_1, X_2, \ldots, X_n\} = X_1 \cap X_2 \cap \cdots \cap X_n$

etc.

□

Exercises 0.2.19 (1) Define $A_n = (\frac{1}{n+1}, 1]$ for $n \in \mathbb{N}$. Calculate $\bigcup_{n=1}^{\infty} A_n$ and $\bigcap_{n=1}^{\infty} A_n$.

(2) Let $B_r = \{\vec{x} \in \mathbb{R}^3 : |x| \leq r\}$. Calculate $\bigcup_{r \in (0,1]} B_r$ and $\bigcap_{r \in (0,1]} B_r$.

□

Definition 0.2.20 Let $\mathcal{A} = \{A_n : n \in \mathbb{N}\}$ be a family of sets.

(a) We define the **limit superior** of the sets (A_n) by

$$\limsup_n A_n = \bigcap_{n=1}^{\infty} \bigcup_{m \geq n} A_m$$

(b) We define the **limit inferior** of the sets (A_n) by

$$\liminf_n A_n = \bigcup_{n=1}^{\infty} \bigcap_{m \geq n} A_m$$

□

Note that $a \in \limsup A_n$ if and only if $a \in \bigcup_{m \geq n} A_m$ for all n, i.e. if and only if for all n there is $m \geq n$ such that $a \in A_m$. Thus $a \in \limsup_n A_n$ if and only if *a belongs to infinitely many of the sets* A_n.

Exercises 0.2.21 (1) Show that $a \in \liminf A_n$ if and only if *a belongs to almost all of the* A_n. ("Almost all" mean "all except possibly finitely many". Thus we are claiming that $a \in \liminf A_n$ if and only if there are at most finitely many n such that $a \notin A_n$.)

(2) Let $A_n = [0, \frac{1}{n}]$ if n is even, and let $A_n = [-\frac{1}{n}, 0]$ if n is odd. Calculate $\limsup_n A_n$ and $\liminf_n A_n$.

(3) Let $A_n = [0, n]$ if n is even, and let $A_n = [-n, 0]$ if n is odd. Calculate $\limsup_n A_n$ and $\liminf_n A_n$.

(4) Let $A_n = (-1, 1 + \frac{1}{n})$ if n is even, and let $A_n = [-1 - \frac{1}{n}, 1]$ if n is odd. Calculate $\limsup_n A_n$ and $\liminf_n A_n$.

(5) Given a sequence of sets A_n, and a positive integer N, define $B_n = A_{N+n}$. Show that $\limsup_n A_n = \limsup_n B_n$ and that $\liminf_n A_n = \liminf_n B_n$. This shows that $\limsup$ and $\liminf$ are determined by the "tail" of the sequence A_n only.

□

Here is another way of making new sets from old: Given a particular set, one should be able to collect all of its subsets together into a new set, called the *power set*.

Definition 0.2.22 (Power set)
If A is a set, then the *power set* of A is the set of all subsets of A.

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

□

Note that $\emptyset, A \in \mathcal{P}(A)$. They are, respectively, its smallest and biggest members.

Example 0.2.23 Let $A = \{1, 2, 3\}$. Then the powerset of A is the 8–element set

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

□

Proposition 0.2.24 *If A has n elements, then $\mathcal{P}(A)$ has 2^n elements.*

Proof: We prove this proposition by *mathematical induction.* Firstly, the proposition is true for all sets with 0 elements (i.e. if a set has 0 elements, then it has 2^0 subsets. To see this, note that the only set with 0 elements is $\emptyset$, and that $\emptyset$ has only one subset, namely itself. Since $2^0 = 1$, the proposition holds for all sets with 0 elements.)

Next *assume* that the proposition holds for all sets with n elements. We now want to prove that the proposition is also true for sets with $n+1$ elements. So let A be a set with $n+1$ elements, and pick $a \in A$. Let $B = A - \{a\}$. Then B has n elements, and so by assumption, 2^n subsets.

Now reason as follows: The subsets of A can be divided into two classes, namely (1) those which have a as element, and (2) those which do not. It is obvious that no subset of A belongs to both classes, and that every subset of A belongs to one of them.

(1): If $C \subseteq A$ does not have a as element, then $C \subseteq B$. The former are just subsets of B, and there are 2^n of them.

(2): If $C \subseteq A$ does have $a \in C$, then $C = C' \cup \{a\}$, where $C' \subseteq B$. Since to each such C there corresponds a C', there are as many subsets of A containing a as there are subsets of B, i.e. 2^n.

Hence A has $2^n + 2^n = 2^{n+1}$ subsets. We have therefore proved the following:

(i) Every set with 0 elements has 2^0 subsets;

(ii) If every set with n elements has 2^n subsets, then every set with $n+1$ elements has 2^{n+1} subsets

Thus since every set with 0 elements has 2^0 subsets, we deduce that every set with 1 element has 2^1 subsets. From *that* we deduce that every set with 2 elements has 2^2 subsets, and from *that*, that every set with 3 elements has 2^3 subsets, etc.

$\dashv$

Exercises 0.2.25 Prove the above proposition again, using the **binomial theorem**.
[Hint: Recall that the binomial coefficient $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ describes the number of ways in which m objects can be chosen from a collection of n objects.For example , there are $\binom{20}{11}$ ways of choosing a soccer team from a group of twenty individuals. Also recall the binomial theorem:

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}$$

Use these facts to prove that if A is a set with n elements, then $\mathcal{P}(A)$ is a set with 2^n elements.]

□

0.2.2 Functions

Originally, a function was regarded as a *rule* (or a *formula*, or an *algorithm*) for associating one real number with another. For example,

$$f(x) = 2x^3$$

explicitly shows how to calculate a number $f(x)$ which is to be associated with x: First cube x, and then multiply the resultant by 2. However, this original formulation proved to be unduly restrictive. For one thing, Fourier showed that practically any continuous curve of finite length could be give a "formula" as an infinite trigonometric series. For another, we may want to associate numbers with other mathematical objects, or one kind of mathematical object with another — there is no reason to restrict ourselves solely to numbers.

For example, we may want to associate with each rectangle its area. Thus we have a function which assigns a number to each rectangle.
Or, we may want to assign to each subset of $\mathbb{R}$ its power set. This yields a function which assigns a set to each set.

Thus a general definition of function dispenses with the idea that it is a rule, but keeps the idea of associating one object with another:

Definition 0.2.26 Let A, B be sets. A *function* (or *map*) f from A to B, written

$$f : A \to B \quad \text{or} \quad A \xrightarrow{f} B$$

is a subset of the cartesian product $A \times B$ with the following property:

for each $a \in A$ there exists *exactly one* $b \in B$ such that $(a, b) \in f$

In that case write

$$f(a) = b \quad \text{instead of } (a, b) \in f$$

We call b the *image* (or *value*) of a under f, and call a a *preimage* of b. We also say that *a maps to b* under f.
The set A is called the *domain* of f, and the set B is called the *codomain* of f

$$A = \mathrm{dom}(f) \qquad B = \mathrm{codom}(f)$$

The *range* of f is the set of all possible values of f, and denoted $\mathrm{ran}(f)$.

□

Essentially, this concept of function is arrived at by deliberately confusing a function with its graph. For example, the graph of the function $f : \mathbb{R} \to \mathbb{R} : x \mapsto 2x^3$ is a curve in the cartesian plane. This curve is therefore a set of ordered pairs:

$$\mathrm{Graph}(f) = \{(x, y) : y = 2x^3\}$$

For example, the points $(0,0),(1,2),(2,16),(3,54)$ belong to the graph. Now we assert that a function *is* its graph. Thus the function $f(x)=2x^3$ is nothing but the set $\{(x,y) : y=2x^3\} \subseteq \mathbb{R}\times\mathbb{R}$.

You've already met more than just a few functions in your mathematical education up to date. The most obvious ones are functions from $\mathbb{R}^n$ to $\mathbb{R}^m$, such as $f(x)=x^2, g(x,y)=\sin(x^3+y), h(x,y,z)=(xy, x\ln z)$, etc. Here are a few more that you might not yet have considered as functions:

Examples 0.2.27 (a) Define $\mathbb{Z}\xrightarrow{f}\mathcal{P}(\mathbb{Z})$ by: $f(n)=\{m : m \text{ divides } n\}$. Then f is a function which maps a number to a set. For example,

$$f(12)=\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm12\}=f(-12)$$

(b) Let $\mathcal{C}^0(\mathbb{R},\mathbb{R})=\{f : f \text{ is a continuous map from } \mathbb{R} \text{ to } \mathbb{R}\}$, and let $a\le b\in\mathbb{R}$. Then $\int_a^b : \mathcal{C}^0(\mathbb{R},\mathbb{R})\longrightarrow\mathbb{R}$ is a function which assigns to every continuous map its definite integral.

(c) Let $\mathcal{C}^1(\mathbb{R},\mathbb{R})$ be the set of all maps from $\mathbb{R}$ to $\mathbb{R}$ which have continuous first derivatives. Then the derivative operator is a map $D:\mathcal{C}^1(\mathbb{R},\mathbb{R})\longrightarrow\mathcal{C}^0(\mathbb{R},\mathbb{R})$.

(d) **curl** is a map from the set of vector fields on $\mathbb{R}^3$ to itself. **div** is a map from the set of vector fields on $\mathbb{R}^3$ to the set of functions on $\mathbb{R}^3\to\mathbb{R}$. **grad** is a map from the set of differentiable functions $\mathbb{R}^3\to\mathbb{R}$ to the set of vector fields on $\mathbb{R}^3$.

(e) An $n\times m$ matrix A can be regarded as a map from $A:\mathbb{R}^m\longrightarrow\mathbb{R}^n$.

(f) Addition and multiplication are functions from $\mathbb{R}^2$ to $\mathbb{R}$. Addition can, in fact, be described by the 1×2–matrix $(1\;\;1)$, for $(1\;\;1)\binom{a}{b}=a+b$.

(g) If Ω is a universal set, then union and intersection can be regarded as functions from $\mathcal{P}(\Omega)\times\mathcal{P}(\Omega)$ to $\mathcal{P}(\Omega)$, which map the ordered pair (A,B) to $A\cup B$ and $A\cap B$ respectively.

(h) We can also regard the bigger version $\bigcup$ of union as a map, but this time we have $\bigcup : \mathcal{P}(\mathcal{P}(\Omega))\longrightarrow\mathcal{P}(\Omega)$. It assigns to any family of subsets of Ω its union. (Note that a family of subsets of Ω is just a set of elements of $\mathcal{P}(\Omega)$, i.e. it is a subset of $\mathcal{P}(\Omega)$, and therefore an element of $\mathcal{P}(\mathcal{P}(\Omega))$.) The same goes for intersection.

□

For any set A, there is an important function on A called the *identity function.* It is denoted by id_A, and is defined by

$$\mathrm{id}_A : A\longrightarrow A \qquad \mathrm{id}_A(a)=a$$

Thus $\mathrm{id}_A=\{(a,a) : a\in A\}$.

Examples 0.2.28 (a) The identity function on $\mathbb{R}$ is just the function $y=x$.

(b) The identity function on $\mathbb{R}^n$ is the identity matrix

$$I_n=\begin{pmatrix} 1 & 0 & 0 & \dots & 0\\ 0 & 1 & 0 & \dots & 0\\ 0 & 0 & 1 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \dots & 1\end{pmatrix}$$

□

Definition 0.2.29 Let $f : A \to B$. If $A' \subseteq A$, we can define the *restriction* of f to A' as follows:

$$f|A' \text{ is a map from } A' \text{ to } B\text{, such that } (f|A')(a) = f(a) \text{ for all } a \in A'$$

□

Definition 0.2.30 Let $A \xrightarrow{f} B$ be a function.

(a) f is said to be *one-to-one* (or 1-1, or *injective*) if and only if the following condition holds:

$$\text{If } f(a_1) = f(a_2)\text{, then } a_1 = a_2.$$

(b) f is said to be *onto* (or *surjective*) if and only if

$$\text{For every } b \in B \text{ there exists an } a \in A \text{ such that } f(a) = b.$$

(c) f is said to be a *bijection* (or a *one-to-one correspondence*) if it is both an injection and a surjection.

□

Remarks 0.2.31 A function $f : A \to B$ is injective if no two distinct members of a map to the same $b \in B$, i.e. if every $b \in B$ has *at most one* preimage.
f is surjective if and only if every b in B gets mapped onto by some $a \in A$, i.e. if every $b \in B$ has *at least one preimage.* In that case B is the range of f, i.e. $\text{ran}(f) = \text{codom}(f)$.
f is a bijection if and only if every $b \in B$ has *exactly one* preimage.

It should be clear that there is a bijection from a finite set A to another set B if and only if A and B have the same number of elements.

□

Examples 0.2.32 (a) Let $f(x) = x^2$. We would generally regard f as a function with domain $\mathbb{R}$ and codomain $\mathbb{R}$. The range of f is $[0, +\infty)$, since f takes no negative values. f is not injective, because, for example $f(1) = f(-1)$. f is not surjective either, since -1 is not in the range of f.

(b) If we define $g(x) : [0, 1] \longrightarrow [0, 1]$ by $g(x) = x^2$, then we may regard g as the restriction of f to $[0, 1]$, i.e. $g = f|[0, 1]$. Now g is clearly a bijection.

(c) $x^3 : \mathbb{R} \longrightarrow \mathbb{R}$ is a bijection.

(d) Let $\mathbb{Q}^+$ denote the set of all non–negative rational numbers. The map $h : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Q}^+$ defined by $h(n, m) = \frac{n}{m}$ is surjective, but not injective.

(e) If $A \subseteq B$, then the **inclusion** $f : A \to B$ defined by: $f(a) = a$ is an injection. It is a bijection if and only if $A = B$.

(f) Let A be an $n \times n$–matrix, regarded as a map from $\mathbb{R}^n$ to $\mathbb{R}^n$. Then A is injective if and only if $\det(A) \neq 0$.

□

Next, we discuss how functions can be combined:

Definition 0.2.33 If $f : A \to B$ and $g : B \to C$, then $g \circ f$ is a function from A to C, defined by

□

Note that the composition does in one step what f and g do in two:

$$\begin{array}{ll} A \overset{f}{\to} B \overset{g}{\to} C & \qquad a \overset{f}{\mapsto} f(a) \overset{g}{\mapsto} g(f(a)) \\ A \overset{g\circ f}{\to} C & \qquad a \overset{g\circ f}{\mapsto} g(f(a)) \end{array}$$

Also note that $g \circ f$ means:

Do f first, then g

i.e. the last shall be first.

An often used fact is that *composition is an associative operation* on functions, i.e.

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

By this equation we mean that: one side is defined if and only if the other side is defined, and in that case they are equal.

For if $A \xrightarrow{f} B, B \xrightarrow{g} C$, and $C \xrightarrow{h} D$, then $h \circ (g \circ f)$ is a function from A to D which works as follows: First do $g \circ f$, then do h. But to do $g \circ f$, you must first do f, then g. The combined result is

$$\text{First do } f\text{, then } g\text{, and then } h\text{: } (h \circ (g \circ f))(a) = h(g(f(a)))$$

Similarly, $(h \circ g) \circ f$ is a function from A to D which works as follows: First do f, then $h \circ g$. But to do $h \circ g$, you must first do g, then h. The combined result is therefore

$$\text{First do } f\text{, then } g\text{, and then } h\text{: } ((h \circ g) \circ f)(a) = h(g(f(a)))$$

and thus $h \circ (g \circ f) = (h \circ g) \circ f$, as claimed.

Example 0.2.34 Consider the following functions (note their domains and codomains):

$$\mathbb{R} \xrightarrow{f} \mathbb{R}^+ : x \mapsto x^2 + 1$$
$$\mathbb{R}^+ \xrightarrow{g} \mathbb{R}^+ : y \mapsto \sqrt{y}$$
$$\mathbb{R}^+ \xrightarrow{h} [-1, 1] : z \mapsto \sin(z)$$

Then

$$\mathbb{R} \overset{g\circ f}{\longrightarrow} \mathbb{R}^+ : x \mapsto \sqrt{x^2 + 1}$$
$$\mathbb{R}^{+1} \overset{h\circ g}{\longrightarrow} [-1, 1] : y \mapsto \sin(\sqrt{y})$$

and thus

$$\mathbb{R} \overset{h\circ(g\circ f)}{\longrightarrow} [-1, 1] : x \mapsto \sin(\sqrt{x^2 + 1})$$
$$\mathbb{R} \overset{(h\circ)g\circ f}{\longrightarrow} [-1, 1] : x \mapsto \sin(\sqrt{x^2 + 1})$$

□

Exercises 0.2.35 (1) Let $f : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$, and let $g : \mathbb{N} \to \mathbb{N} : n \to n + 2$. Calculate $(f \circ g)(5)$ and $g \circ f(5)$.
Write down formulas for $f \circ g$ and $g \circ f$.

(2) Suppose that $f(x) = x^2$ and $g(x) = x + 3$. Calculate $g \circ f(x)$ and $f \circ g(x)$. Note that $g \circ f \neq f \circ g$.

(3) If A is an $n \times m$–matrix, and B is an $m \times r$–matrix, then we can regard them as functions $\mathbb{R}^m \xrightarrow{A} \mathbb{R}^n$, $\mathbb{R}^r \xrightarrow{B} \mathbb{R}^m$. The composition $A \circ B$ is therefore a map $\mathbb{R}^r \to \mathbb{R}^n$. It is not hard to show that the composition is just the matrix product, i.e. that $A \circ B = AB$. Do so!

(4) Suppose that $g \circ f_1 = g \circ f_2$. Prove that if g is injective then we can "cancel" g to conclude $f_1 = f_2$. Give an example to show that left–cancellation may fail if g is not injective.

(5) Suppose that $g_1 \circ f = g_2 \circ f$. Prove that if f is surjective then we can "cancel" f to obtain $g_1 = g_2$. Show that right–cancellation may fail if f is not surjective.

□

Note that if $f : A \longrightarrow B$, then $f \circ \mathrm{id}_A = f$, and $\mathrm{id}_B \circ f = f$. Thus the identity function behaves like an identity element for the operation of composition.

The number 0 is an identity element for the operation of addition, because $x + 0 = x$.
The number 1 is an identity element for the operation of multiplication, because $x \cdot 1 = x$.

Next, we tackle the idea of *inverting* (or *reversing*) the effect of a function. Take the function $f(x) = 3x$. It transforms the number x into the number $3x$. To *undo* this transformation, you just multiply $3x$ by $\frac{1}{3}$. The function $g(x) = \frac{1}{3}x$ inverts the effect of f, in that

$$g \circ f(x) = x \qquad f \circ g(y) = y$$

Thus applying first f, and then g gets you back to the starting point x. The same holds true if you apply g first, and then f.

Can every function be inverted? No, as is easy to see: Consider the function $f(x) = x^2$. Then $f(2) = 4 = f(-2)$. Now if g is a function which reverses the effect of f, then we cannot decide whether $g(4) = 2$ or $g(4) = -2$. The problem arises because g is not 1-1.

Let's make the preceding discussion precise:

Definition 0.2.36 Let $f : A \to B$. We say that f is *invertible* if and only if there is a function $g : B \to A$ such that

$$g(f(a)) = a \quad \text{for all } a \in A, \qquad f(g(b)) = b \quad \text{for all } b \in B \qquad (*)$$

The function g, *if it exists*, is called the *inverse* of f, and denoted $g = f^{-1}$. Then $(*)$ amounts to saying

$$f^{-1} \circ f = \mathrm{id}_A \qquad \text{and} \qquad f \circ f^{-1} = \mathrm{id}_B$$

□

Note that if f^{-1} exists, then

$$f^{-1}(b) = a \quad \text{if and only if} \quad f(a) = b$$

Proposition 0.2.37 *A function $f : A \longrightarrow B$ is invertible if and only if it is a bijection.*

Proof: Suppose that f is invertible, i.e. that f^{-1} exists. Then f^{-1} is a function from B to A. We first show that f is surjective: Let $b \in B$. Since the domain is B, $f^{-1}(b)$ must be defined, i.e. there must be some $a \in A$ such that $f^{-1}(b) = a$. But then $f(a) = b$. Hence every $b \in B$ has a preimage.
Next we show that f is injective. For suppose that $f(a_1) = f(a_2) = b$. Then $f^{-1}(b) = a_1$ and $f^{-1}(b) = a_2$. Since f^{-1} is a function, we must have $a_1 = a_2$ (check the definition of function), and hence f is injective.
This proves that if f is invertible, then f is a bijection.

Now we prove the converse. If f is a bijection, then it is onto B. Hence for every $b \in B$ there is some $a \in A$ such that $f(a) = b$. Moreover, since f is one-to-one, that a has to be unique. So we may define $f^{-1}(b)$ to be the unique a such that $f(a) = b$. This makes f^{-1} into a well–defined function $f^{-1} : B \to A$.

$\dashv$

Examples 0.2.38 (a) The function $f(x) = x^3$ is a bijection on the reals, and its inverse is $g(x) = \sqrt[3]{x}$.

(b) The function $f(x) = x^2$ does not have an inverse, since it is not a bijection. However, if we *restrict* f to the non–negative reals, then $f|\mathbb{R}^+$ is a bijection. Its inverse is the square root function.

(c) The function $f : \mathbb{R} \longrightarrow (0, +\infty)$ defined by $f(x) = e^x$ is bijective. Its inverse is the natural logarithm $\ln x$.

(d) The function $\sin x$ is neither injective, nor surjective; however, if we restrict $\sin x$ and regard it as a function $[-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow [-1, 1]$, then it is a bijection, and its inverse is $\arcsin x$.

(e) If A is an $n \times n$–matrix, regarded as a function on $\mathbb{R}^n$, then A has an inverse function if and only if A has an inverse matrix. Since composition is just matrix multiplication, the *inverse function* of A is just the *inverse matrix* A^{-1}.

□

Remarks 0.2.39 Note that, in general,

$$f^{-1}(x) \quad \neq \quad \frac{1}{f(x)}$$

e.g. $\sqrt[3]{x} \neq \frac{1}{x^3}$.

The number $x^{-1} = \frac{1}{x}$ is the inverse of x under the operation of *multiplication*, in that

$$x \cdot x^{-1} = 1 \qquad x^{-1} \cdot x = 1$$

noting that 1 is the identity for multiplication.
The function f^{-1} is the inverse of f under the operation of *composition*, in that

$$f \circ f^{-1} = \mathrm{id} \qquad f^{-1} \circ f = \mathrm{id}$$

noting that id is the identity for composition.
The same notation for inverse, i.e. ${}^{-1}$, refers to *different operations*, so there's no reason to believe that there is any relationship between them.

□

The notion of invertibility can be refined:

Definition 0.2.40 Let $f : A \to B$ and $g : B \to A$.

(a) g is called a *left inverse* of f if $g \circ f = \mathrm{id}_A$.

(b) g is called a *right inverse* of f if $f \circ g = \mathrm{id}_B$.

□

Note that if f is invertible, then f^{-1} is both a left and a right inverse of f, and vice versa.

Exercises 0.2.41 (1) Prove that a function f has a left inverse if and only if it is injective.

(2) Prove that a function f has a right inverse if and only if it is surjective.

(3) Prove that if a function f has a left inverse g *and* a right inverse h, then f is invertible, and $g = h$.

(4) Consider $f : \{a, b, c\} \to \{1, 2\}$ defined by $f(a) = f(b) = 1, f(c) = 2$. Find two distinct right inverses of f.

(5) Consider the inclusion $\iota : \mathbb{Z} \to \mathbb{Q}$. Construct two distinct left inverses of ι.

□

We have already noted the confusion that may possibly arise by the two uses of the symbol ${}^{-1}$. We have but few symbols at our disposal, and many of them must therefore serve more than one function. Thus you must *always be aware of the context* in which a particular symbol is used.

You have to do this when using ordinary language: You *know* in what sense the newspaper headline

"School kids make great snacks at fund raiser"

is meant, even though the other sense offers greater amusement value.

I say this because we are about to add to the possible confusion. With every function $f : A \to B$ (not necessarily invertible), we can associate two new functions between the power sets of A and B

$$f[\cdot] : \mathcal{P}(A) \to \mathcal{P}(B) : A' \mapsto \{b \in B : \text{ There is } a' \in A' \text{ such that } f(a') = b\} \quad \text{where } A' \subseteq A$$
$$f^{-1}[\cdot] : \mathcal{P}(B) \to \mathcal{P}(A) : B' \mapsto \{a \in A : f(a) \in B'\} \quad \text{where } B' \subseteq B$$

Thus $f[\cdot]$ assigns to each subset A' of A a subset $f[A'] \subseteq B$. Similarly, $f^{-1}[\cdot]$ transforms each subset B' of B into a subset $f^{-1}[B'] \subseteq A$.
We will, for the moment, use square brackets to distinguish the various functions, but will drop this convention later. Which function is meant will be clear from context. We shall also call $f[A']$ the *direct image* of A' along f, and $f^{-1}[B']$ the *inverse image* of B' along f. Note that

$$f[A'] = \text{set of all images of } a \in A'$$

whereas

$$f^{-1}[B'] = \text{set of all preimages of } b \in B'$$

Remarks 0.2.42 Sometimes the notation $f^{\rightarrow}$ is used for direct image, and $f^{\leftarrow}$ for inverse image.

□

Inverse images play a very important role in mathematics. It is therefore useful to remember the following:

$$a \in f^{-1}[B'] \quad \text{if and only if} \quad f(a) \in B'$$

Similarly,

$$b \in f[A'] \quad \text{if and only if there is } a' \in A' \text{ such that } f(a') = b$$

Examples 0.2.43 (a) Suppose that $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$. Then

$$f[-1,2] = [0,4] \quad , f[\mathbb{Z}] = \{0,1,4,9,\dots\}, \quad f[\{4\}] = \{16\}$$

Also

$$f^{-1}[0,1] = [-1,1], \quad f^{-1}[\{4\}] = \{2,-2,\}, \quad f^{-1}[\{-4\}] = \emptyset$$

In each case, a *set* is transformed into a *set*.

(b) Suppose that $A = \{a_1, a_2, a_3\}, B = \{b_1, b_2, b_3\}$, and that $f : A \to B$ is defined by $f(a_1) = f(a_3) = b_1$, and $f(a_2) = b_3$. Then

$$f[\{a_1\}] = f[\{a_3\}] = f[\{a_1,a_3\}] = \{b_1\}, \quad f[\{a_2\}] = b_3, \quad f[A] = \{b_1,b_3\}, \quad f[\emptyset] = \emptyset$$

and

$$f^{-1}[\{b_3\}] = \{a_2\}, \quad f^{-1}[\{b_2\}] = f^{-1}[\emptyset] = \emptyset, \quad f^{-1}(B) = f^{-1}[\{b_1,b_3\}] = A$$

□

Exercises 0.2.44 1. Let $f : A \to B$ be a function, and let $A' \subseteq A$, $B' \subseteq B$.

(a) Show that $A' \subseteq f^{-1}[f[A']]$

(b) Show that $B' \supseteq f[f^{-1}[B']]$

(c) Show that $A' = f^{-1}[f[A']]$ if and only if f is injective.

(d) Show that $B' = f[f^{-1}[B']]$ if and only if f is surjective.

[Hints: Reason along the following lines:
(b) If $b \in f[f^{-1}[B']]$ then $b = f(a)$ for some $a \in f^{-1}[B']$. But then $f(a) \in B'$, and so $b \in B'$.
(c) If $a \in f^{-1}[f[A']]$ then $f(a) \in f[A']$. Thus there is $a' \in A'$ such that $f(a) = f(a')$. But since f is injective, $a = a'$, and so $a \in A'$.]

2. Inverse images preserve the set operations: Let $f : A \to B$, and suppose that G, H are subsets of B. Then

   (a) If $G \subseteq H$, then $f^{-1}[G] \subseteq f^{-1}[H]$;

   (b) $f^{-1}[G \cap H] = f^{-1}[G] \cap f^{-1}[H]$;

   (c) $f^{-1}[G \cup H] = f^{-1}[G] \cup f^{-1}[H]$;

   (d) $f^{-1}[G - H] = f^{-1}[G] - f^{-1}[H]$;

3. Direct images are not quite so well behaved: Let $f : A \to B$, and suppose that $G, H \subseteq A$.

   (a) Suppose that $G \subseteq H$. Show that $f[G] \subseteq f[H]$;

   (b) Show that $f[G \cup H] = f[G] \cup f[H]$;

   (c) Show that $f[G \cap H] \subseteq f[G] \cap f[H]$;

   (d) Give an example to show that we may not have $f[G \cap H] = f[G] \cap f[H]$;

   (e) Show that $f[G] - f[H] \subseteq f[G - H] \subseteq f[G]$;

   (f) Give an example to show, in (e), that both $\subseteq$'s may fail to be $=$'s.

□

We end this section with some notation: Suppose that A, B are finite sets, and that A has n elements, and B m elements. How many functions are there from A to B?
For each $a \in A$ we have m choices for the value $f(a) \in B$. Thus there are m^n functions from A to B. For that reason

Definition 0.2.45 Let A, B be sets. Then we define

$$B^A = \text{set of all functions from } A \text{ to } B$$

Some authors use ${}^AB$ instead of B^A.

□

Note that each function $f : A \to B$ is a subset of $A \times B$. Hence B^A is a set of subsets of $A \times B$, i.e. $B^A \in \mathcal{P}(\mathcal{P}(A \times B))$.

0.2.3 Relations

We want to capture mathematically the idea that two objects are somehow related. For example, suppose that we have two sets

$$M = \{\text{Archie, Reggie, Forsythe}\} \qquad W = \{\text{Betty, Veronica, Ethel}\}$$

and suppose that A is married to B, and that R is married to V, but that F and E remain unmarried. The relation of being married is described by the set

$$\mathbf{R} = \{(\text{A,B}), (\text{R,V})\}$$

Note that $\mathbf{R}$ is a subset of the cartesian product $M \times W$. We will sometimes write $x\mathbf{R}y$ instead of $(x, y) \in \mathbf{R}$. Thus in this case, $x\mathbf{R}y$ if and only if x is married to y.

As for functions, the general definition of a relation is quite abstract:

Definition 0.2.46 A *relation* from a set A to a set B is just a subset of $A \times B$. If $A = B$, we just say that $\mathbf{R}$ is a relation on A.

□

Thus if $A = \mathbb{N}$ and $B = \mathbb{N} \cup \{0\}$, then

$$\mathbf{L} = \{(1, 3), (2, 1), (3, 4), (4, 1), (5, 5), (6, 9) \dots\} \subseteq A \times B$$

is a relation from A to B. Here what the relation actually *is* may not be obvious. Could you have guessed that $7\mathbf{L}2$ and $8\mathbf{L}6$? In fact, $n\mathbf{L}m$ if and only if m is the n^{th} number in the decimal expansion of $\pi = 3.14159265\dots$. Since there may often be a relation without you being able to see it, we have adopted a completely general definition of *relation*, which does not assume any visible relationship between the objects.

Relations are ubiquitous in mathematics, and you know many already:

Examples 0.2.47 (a) Consider the relation $\leq$ on $\mathbb{R}$:

$$\leq = \{(x, y) \in \mathbb{R}^2 : x \leq y\}$$

(b) If A is a set, there is a similar relation $\subseteq$ on $\mathcal{P}(A)$:

$$\subseteq = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : X \subseteq Y\}$$

(c) The divisor relation on $\mathbb{Z}$: We say that $n|m$ if and only if m is a multiple of n. It is described by the set

$$\{(n, m) \in \mathbb{Z}^2 : \text{There exists } a \in \mathbb{Z} \text{ such that } m = an\}$$

(d) Congruency modulo n: Two integers are *congruent modulo n* if they leave the same remainder when divided by n. For example $3, 8, 13, 18\dots$ all leave a remainder of 3 when divided by 5, and thus they are congruent modulo 5. Symbolically, we say that

$$a \equiv b \mod n \text{ if } n|(b - a)$$

(e) Perpendicularity is a relation between vectors in $\mathbb{R}^3$. We have

$$(x_1, x_2, x_3) \perp (y_1, y_2, y_3) \Longleftrightarrow x_1y_1 + x_2y_2 + x_3y_3 = 0$$

(f) *Equality* is a relation. Actually, it is several relations, all denoted by the same symbol =. Thus we have equality of numbers, of vectors, of sets, etc. If A is a set, then the relation of equality on A is called the *identity* relation. It is just

$$\Delta_A = \{(a,a) : a \in A\}$$

□

Note that function is a special kind of relation: We defined a function $f : A \times B$ to be a subset of $A \times B$ with the additional property that for every a there is exactly one b such that $a\, f\, b$. Instead of writing $a\, f\, b$, however, we write $f(a) = b$.

If $\mathbf{R}$ is a relation from A to B, then its *inverse* $\mathbf{R}^{-1}$ is a relation from B to A. It is defined by:

$$b\,\mathbf{R}^{-1}a \iff a\mathbf{R}b$$

i.e. $(b,a) \in \mathbf{R}^{-1}$ if and only if $(a,b) \in \mathbf{R}$.

If R is a relation from A to B and S is a relation from B to C, we can define a relation $S \circ R$ from A to C as follows:

$$(a,c) \in S \circ R \quad \Leftrightarrow \exists b \in B[(a,b) \in R \wedge (b,c) \in S]$$

Thus

$$a(S \circ R)c \text{ iff there is } b \in B \text{ such that } a\,R\,b\,S\,c$$

Note the change in order!!
$S \circ R$ is called the *composition* of S with R.

Exercise 0.2.48 If the relations R, S are functions, then their composition as relations is the same as their composition as functions.
Similarly, if the relation R is a bijective function, then the inverse R^{-1} of R as a relation is the same as its inverse as a function.

□

Examples 0.2.49 (a) If X is the set of all people, and if $\mathbf{P}$ is the relation "parent of", then $\mathbf{P}^{-1}$ is the relation "child of".

(b) Similarly, if $\mathbf{P}$ is the relation "parent of", then $\mathbf{P} \circ \mathbf{P}$ is the relation "grandparent of": For $a(\mathbf{P} \circ \mathbf{P})c$ if and only if there is b such that $a\mathbf{P}b$ and $b\mathbf{P}c$.

(c) Moreover, $\mathbf{S} = \mathbf{P} \circ \mathbf{P}^{-1} - \Delta_X$ is the relation "sibling of": For $a(\mathbf{P} \circ \mathbf{P}^{-1})c$ if and only if there is a b such that $a\,\mathbf{P}^{-1}\,b\,\mathbf{P}\,c$, i.e. iff a is the child of b and b is the parent of c, i.e. iff a, c have a common parent. Thus $(a,c) \in \mathbf{S}$ implies that a, c have a common parent. Since $(a,c) \in \mathbf{S}$ implies $(a,c) \notin \Delta_X$, we see that $a \neq c$, and thus that a, c are brother and/or sister.

(d) $\leq^{-1} = \geq$, since $b \geq a$ if and only if $a \leq b$.

(e) n divides m if and only if m is a multiple of n. Thus the "multiple of" relation is the inverse of the "divisor of" relation.

(f) Perpendicularity between vectors is its own inverse, i.e. $\perp^{-1}=\perp$: $\vec{x} \perp \vec{y}$ iff $\vec{y} \perp \vec{x}$.

□

Exercises 0.2.50 1. Let W be the set of all women, and let S, M be relations from W to W described as follows: aSb iff a us a sister of b; aMb iff a is a mother of b. Describe

(a) $M \circ S$;

(b) $(M \circ S)^{-1}$;

(c) S^{-1} and M^{-1};

(d) $S^{-1} \circ M^{-1}$

2. Suppose that R is a relation from A to B and that S is a relation form B to C. Show that

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$$

□

There are two important classes of relations in mathematics, namely *equivalence relations* and *partial orderings*. Equivalence relations have many of the same properties of $=$, and partial orderings have similar properties to $\leq$ and $\subseteq$.

Definition 0.2.51 Suppose that $\mathbf{R}$ is a relation from on a set A. R is said to be

(i) *reflexive* if $a\mathbf{R}a$ for all $a \in A$.

(ii) *symmetric* if $a\mathbf{R}b$ implies $b\,\mathbf{R}a$ for all $a, b \in A$.

(iii) *antisymmetric* if $a\mathbf{R}b$ *and* $b\,\mathbf{R}a$ together imply $a = b$, for all $a, b \in A$.

(iv) *transitive* if $a\mathbf{R}b$ and $b\mathbf{R}c$ together imply $a\mathbf{R}c$, for all $a, b, c \in A$.

An *equivalence relation* is a reflexive, symmetric, transitive relation.
A *partial ordering* is a reflexive, antisymmetric, transitive relation.

□

Exercises 0.2.52 1. $=$ is an equivalence relation on any set.

2. $\leq$ is a partial ordering on the set of reals.

3. $\subseteq$ is a partial ordering on $\mathcal{P}(A)$.

4. Congruency modulo n is an equivalence relation on $\mathbb{Z}$. (Recall that $a \equiv b \mod n$ if and only if a, b leave the same remainder when divided by n, if and only if $a - b$ is divisible by n.)

5. The divisor relation $n|m$ on $\mathbb{Z}$ is reflexive and transitive, but not symmetric, nor antisymmetric.

6. Define a relation $\mathbf{L}_1$ on $\mathbb{R}$ by:

$$\vec{x}\,\mathbf{L}_1\vec{y} \text{ if } |x| \leq |y|$$

Is $\mathbf{L}_1$ is a partial ordering?

7. Is $\perp$ an equivalence relation or a partial ordering (on $\mathbb{R}^3$)?

8. Let R be a relation on a set A.

(a) $\Delta_A \subseteq R$ iff R is reflexive.

(b) $R = R^{-1}$ iff R is symmetric.

(c) $R \cap R^{-1} = \Delta_A$ if and only if R is antisymmetric.

(d) $R \circ R \subseteq R$ if and only if R is transitive.

□

Let's take a look at equivalence relations from another angle: They are very closely related to *partitions*.

Definition 0.2.53 Let A be a set. A family $\mathcal{A} = \{A_i : i \in I\}$ is called a **partition** of A provided that

(i) The A_i are **mutually disjoint**, i.e. if $i \neq j$, then $A_i \cap A_j = \emptyset$ for all $i, j \in I$.

(ii) $\bigcup_I A_i = A$

□

Thus $\{A_i : i \in I\}$ is a partition of A provided that every element of A belongs to exactly one A_i. If $\{A_i : i \in I\}$ is a partition of A, then we can define an equivalence relation $\approx$ on A by:

$$a \approx b \Longleftrightarrow a, b \text{ belong to the same } A_i$$

Exercise 0.2.54 Prove that $\approx$ is an equivalence relation.

□

On the other hand, if $\approx$ is an equivalence relation on A, then $\approx$ behave roughly like $=$. When we lump together all elements that are the same under $\approx$, we get an *equivalence class.*

Definition 0.2.55 Let $\approx$ be an equivalence relation on A. For each $a \in A$, define the *equivalence class* $E(a)$ of a as follows:

$$E(a) = \{b \in A : a \approx b\}$$

□

Note that $E(a) = E(b)$ if and only if $a \approx b$. If $a \not\approx b$, then $E(a) \cap E(b) = \emptyset$. Thus the sets $E(a)$ are either equal or disjoint. Hence the set $\{E(a) : a \in A\}$ is a partition of A.

Exercise 0.2.56 Verify the above statements.

□

Examples 0.2.57 (a) If $\approx$ is the identity relation on A, then the equivalence classes are singletons: $E(a) = \{a\}$.

(b) Suppose that $\approx$ is congruency modulo 3. Then the equivalence classes are $A_1 = \{\dots, -6, -3, 0, 3, 6, \dots\}$, $A_2 = \{\dots, -5, -2, 1, 4, 7, \dots\}$ and $A_3 = \{\dots, -4, -1, 2, 6, 8, \dots\}$. The elements of A_1 leave remainder 0 when divided by 3, those of A_2 leave remainder 1, and those of A_3 leave remainder 2. Note that A_1, A_2, A_3 are mutually disjoint, and that $A_1 \cup A_2 \cup A_3 = \mathbb{Z}$.

(c) Let $\approx$ be the "equal length" relation $\mathbf{L}_2$ on $\mathbb{R}^3$. The equivalence classes are spheres centred at the origin.

□

0.2.4 Countable and Uncountable Sets

In this section, we investigate the idea of the *size* or *cardinality* of a set. For finite sets, we can determine the size of a set by counting its elements. Thus for example, the set $\{a, b, c\}$ has cardinality 3 (it has 3 elements). We are going to extend this idea of counting to obtain the size to infinite sets, and we will show that infinity comes in many sizes.

Let's explore the idea of *counting*: For the moment, let $\mathbf{n} = \{1, 2, \ldots, n\}$ be the set of the first n natural numbers. To say that $A = \{a, b, c\}$ has 3 elements is equivalent to saying that there is a one-to-one correspondence between the sets A and $\mathbf{3}$. Indeed, this is the heart of the idea of counting: When we count the elements of A, we are setting up a bijection between A and $\mathbf{3}$. We go "a first, b second, c third". This is equivalent to a map $f : A \cong \mathbf{3}$ defined by $f(a) = 1, f(b) = 2, f(c) = 3$. Thus the idea of counting the elements of a finite set X involves finding a bijection between X and some $\mathbf{n}$. If there is a bijection from X to $\mathbf{n}$, then X has n elements.

Now for some reason, mathematicians often like to start counting at zero. In the mathematical literature, the sets $\mathbf{n}$ are therefore often defined as

$$\mathbf{n} = \{0, 1, 2, \ldots, n-1\}$$

This is the convention that we shall adopt henceforth.

It is obvious that two finite sets A and Δ have the same size if and only if there is a one-to-one correspondence $f : A \cong \Delta$. We don't even have to count A and Δ to know that they have the same number of elements. If $A = \{a, b, c, d\}$ and $\Delta = \{\alpha, \beta, \gamma, \delta\}$, then the existence of the bijection $f : A \cong \Delta$ given by

$$f(a) = \beta, f(b) = \delta, f(c) = \alpha, f(d) = \gamma$$

is sufficient to show that A and Δ have the same number of elements. It doesn't tell us that this number is 4.

Thus two sets have the same size if and only if there is a bijection between them; we can bypass the idea of number. This is important, because we cannot actually *count* infinite sets. But we can establish bijective correspondences between infinite sets. We shall adopt this idea as our basic idea of size.

Definition 0.2.58 *We define an equivalence relation $\approx$ between sets as follows: If A, B are sets, we say that $A \approx B$ if and only if there is a bijection from A to B. If $A \approx B$, we say that A and B have the same* cardinality. *We may also indicate this by saying $|A| = |B|$.*

□

Note that having the same cardinality is an *equivalence relation* between sets, i.e. that

(i) $|A| = |A|$ (Reflexivity)

(ii) If $|A| = |B|$, then $|B| = |A|$ (Symmetry)

(iii) If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$ (Transitivity)

Exercise 0.2.59 Prove this assertion. (Note that the assertion is *not obvious*: When we say that $|A| = |B|$, we are not actually claiming that there are two equal numbers. What we *are* saying is that there is a bijection from A to B. To prove (i), for example, you have to find a bijection from A to A.)

□

Examples 0.2.60 (a) Two finite sets have the same cardinality if and only if they have the same number of elements.

(b) For finite sets, if A is a *proper subset* of B, then $|A| < |B|$. This breaks down completely for infinite sets. Consider, for example, the sets $\mathbb{N}$ and $\mathbb{Z}$. It is certainly true that $\mathbb{N} \subset \mathbb{Z}$. However, the map $\mathbb{N} \xrightarrow{f} \mathbb{Z}$ defined by

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ -\dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

is a bijection: $f(1) = 0, f(2) = 1, f(3) = -1, f(4) = 2, f(5) = -2, f(6) = 3 \ldots.$ (Note that we are zig–zagging from the positive integers to the negative integers.) Thus $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality, even though $\mathbb{N}$ seems to contain fewer elements than $\mathbb{Z}$.

(c) We also have $|\mathbb{Q}| = |\mathbb{N}|$. This can be seen as follows. Put the set of strictly positive rational numbers $\mathbb{Q}^+$ in an array

$$\begin{array}{cccccc} 1/1 & 2/1 & 3/1 & 4/1 & 5/1 & \ldots \\ 1/2 & 2/2 & 3/2 & 4/2 & 5/2 & \ldots \\ 1/3 & 2/3 & 3/3 & 4/3 & 5/3 & \ldots \\ 1/4 & 2/4 & 3/4 & 4/4 & 5/4 & \ldots \\ 1/5 & 2/5 & 3/5 & 4/5 & 5/5 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{array}$$

We can then trace a zig–zag path that moves through all the rational numbers as follows. Start at the top line and move diagonally down to the left until you reach the leftmost line. Repeat. We thus obtain a sequence

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1} \ldots$$

All of the strictly positive rational numbers occur in this sequence, and they all occur infinitely many times. For example, $\frac{1}{1}, \frac{2}{2}, \frac{3}{3} \ldots$ lie along the diagonal, and they are all equal. To obtain a bijection from $\mathbb{N}$ to $\mathbb{Q}^+$, we follow the above sequence of rationals, but we omit any number that has already occurred to ensure that the function is one-to-one, i.e. we *prune* away the repeated values. We therefore define the function $\mathbb{N} \xrightarrow{f} \mathbb{Q}^+$ by

$$f(1) = \frac{1}{1},\ f(2) = \frac{2}{1},\ f(3) = \frac{1}{2},\ f(4) = \frac{3}{1},\ f(5) = \frac{1}{3},\ f(6) = \frac{4}{1}, \dots$$

Note that $f(5) \neq \frac{2}{2}$, which is after $f(4) = \frac{3}{1}$ in the sequence, because $\frac{2}{2} = \frac{1}{1}$ has already occurred as $f(1)$. Then f is a bijection from $\mathbb{N}$ to $\mathbb{Q}^+$. Now even though we haven't found a *formula* for f, it is nevertheless a perfectly good function, and all its values can be calculated. Can you see that $f(16) = \frac{2}{5}$?

In the same way, we can set up a bijection g from $\mathbb{N}$ to the negative rationals. Just put $g(n) = -f(n)$. Finally, we can define a bijection $h : \mathbb{N} \longrightarrow \mathbb{Q}$ using f, g and another zig–zag: We define

$$\begin{gathered} h(1) = 0, h(2) = f(1),\ h(3) = g(1),\ h(4) = f(2), \\ h(5) = g(2), h(6) = f(3),\ h(7) = g(3), \dots \end{gathered}$$

Again, we have no formula for h, but it is certainly a well–defined function, and all its values can be calculated. Check that $h(23) = -\frac{1}{5}$.

(d) If A is any set, finite or infinite, then $\mathcal{P}(A) \approx \mathbf{2}^A$.(Recall that $\mathbf{2}^A$ is the set of all functions from A to $\mathbf{2} = \{0, 1\}$). This can be seen as follows: If $B \subseteq A$, define the *indicator function* (or *characteristic function*) $I_B : A \longrightarrow B$ by

$$I_B(a) = \begin{cases} 1 \text{ if } a \in B \\ 0 \text{ else} \end{cases}$$

Clearly $I_B = I_C$ if and only if $B = C$, and so the map $\mathcal{I} : \mathcal{P}(A) \longrightarrow \mathbf{2}^A$ defined by $\mathcal{I}(B) = I_B$ is an injection. Now suppose that $\chi \in \mathbf{2}^A$, i.e. $A \xrightarrow{\chi} \{0, 1\}$. Define a subset $B \subseteq A$ by

$$a \in B \Longleftrightarrow \chi(a) = 1$$

It is clear that $\mathcal{I}(B) = I_B = \chi$, and thus that $\mathcal{I}$ is surjective as well. This proves that $|\mathcal{P}(A)| = |\mathbf{2}^A|$.

□

Definition 0.2.61 A set A is said to be *countable* if it is either finite or can be put into a one-to-one correspondence with the natural numbers, i.e. if $|A| = \mathbf{n}$ for some $n \in \mathbb{N}$, or $|A| = |\mathbb{N}|$.

□

Remarks 0.2.62 (a) Basically a set A is countable if its elements can be indexed by the natural numbers, i.e. if it *can* be written as $A = \{a_n : n \in \mathbb{N}\}$. For if A is countable and not finite, then there is a bijection $\mathbb{N} \xrightarrow{f} A$, and we can take $a_n = f(n)$. Conversely, if $A = \{a_n : n \in \mathbb{N}\}$ is infinite, we can define a bijection from $\mathbb{N}$ to A by letting $f(n) = a_n$ (although here some *pruning* is necessary if the a_n aren't all distinct; see Example 0.2.60(c)).

(b) In Example 0.2.60, we proved that the sets $\mathbb{Z}$ and $\mathbb{Q}$ are countable sets.

(c) The "zig–zag" technique, used above to prove that the rational numbers are countable, is often very useful.

□

A very basic question that arises is the following: Are all infinite sets countable? The answer is **"No!"**

Example 0.2.63 We show that the unit interval $I = [0, 1]$ is *uncountable*, i.e. that we cannot find an enumeration

$$I = \{x_n : n \in \mathbb{N}\}$$

The proof is by *contradiction*: Suppose that we *can* find such an enumeration $I = \{x_1, x_2, x_3, x_4, \dots\}$, i.e that every real number in $[0, 1]$ is equal to x_n for some n. Now every number x_n has a decimal expansion of the form

$$x_n = 0.x_{n1}x_{n2}x_{n3}x_{n4}x_{n5}\dots$$

where x_{nm} is the m^{th} number in the decimal expansion of x_n. Of course some real numbers have two distinct decimal expansions, a terminating one and a non–terminating one. For example, $1.0000\dots = 0.9999\dots$. We will choose the non–terminating decimal expansions for our x_n.

We now create a new real number x from the x_n by a process called *diagonalization*. We choose $a_n \in \{1, 2, \dots, 9\}$ such that the following hold:

$$a_1 \neq x_{11}, a_2 \neq x_{22}, a_3 \neq x_{33}, \dots, a_n \neq x_{nn}, \dots$$

To avoid a situation where we obtain a number x with a terminating decimal expansion, we haven't permitted $a_n = 0$; this is just a technicality. We can now define x: Put

$$x = 0.a_1a_2a_3a_4\dots$$

Here comes the heart of the argument: Clearly $x \in I = [0, 1]$. Now if I can be written as a list $\{x_1, x_2, x_3, \dots\}$, then there must be some n such that $x = x_n$. But the first decimal place of x differs from the first decimal place of x, since $a_1 \neq x_{11}$; hence $x \neq x_1$. Similarly, the second decimal place of x differs from the second decimal place of x_2, since $a_2 \neq x_{22}$;

hence $x \neq x_2$. We can continue in this way to show that $x \neq x_n$ for any $n \in \mathbb{N}$, i.e. x is not on the list $\{x_1, x_2, x_3, \dots\}$.

This proves the result! Given any list $x_1, x_2, x_3, \dots$ of real numbers in $[0, 1]$, we now have a technique for producing a new real number x that is not on the list. It thus follows that no such list can contain all the real numbers in $[0, 1]$, i.e. there is no bijection from $\mathbb{N}$ to $[0, 1]$.

□

Remarks 0.2.64 Cantor, who discovered the above argument for the uncountability of the reals, wrote to a friend

"I see it, but I don't believe it."

□

Hence there are uncountable sets. Clearly $\mathbb{R}$ is also uncountable, because otherwise we could find an enumeration $\{r_1, r_2, r_3, \dots\}$ of $\mathbb{R}$. By omitting any reals which are not in $[0, 1]$, we could prune this into an enumeration of $[0, 1]$.

The fact that $\mathbb{R}$ is uncountable causes much trouble in analysis. We shall see some more examples of uncountable sets later on.

Definition 0.2.65 *If A, B are sets, we say that the cardinality of A is less than or equal to the cardinality of B, and write*

$$|A| \leq |B|$$

if there is an injection from A into B. We write $|A| < |B|$ if $|A| \leq |B|$, but $|A| \neq |B|$, i.e. if there is an injection from A to B, but no bijection.

□

The idea is that $|A| < |B|$ if and only if A has "fewer" elements than $|B|$. Clearly the following holds:

Proposition 0.2.66 *(a) If $A \subseteq B$, then $|A| \leq |B|$.*

(b) If $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

(c) If $|A| \leq |B|$, then $|\mathcal{P}(A)| \leq |\mathcal{P}(B)|$.

(d) If $|A| \leq |B|$, then $|C^A| \leq |C^B|$

□

Exercise 0.2.67 Prove the above proposition.

□

In fact, the $\leq$–relation is a *partial ordering* between sets: Reflexivity is obvious, and transitivity was left to the exercise above. The main thing that needs to be shown is *antisymmetry*:

Theorem 0.2.68 *(Schröder–Bernstein Theorem) Suppose that $|A| \leq |B|$ and that $|B| \leq |A|$. Then $|A| = |B|$.*

⊣

We will omit the proof. It can be found in any text–book on set theory. Again, I must stress that this result is **not obvious**, because $|A|, |B|$ aren't really numbers. What we *have* to do is show that if there exists an injection from A to B, and an injection from B to A, then there exists a bijection from A to B.

Proposition 0.2.69 *(a) If A is countable, and if B is a subset of A, then B is countable.*

(b) If A, B are countable, then $A \times B$ is countable.

(c) If A, B are countable, the $A \cup B$ is countable.

(d) If $\mathcal{A} = \{A_n : n \in \mathbb{N}\}$ is a family of countable sets, then $\bigcup_n A_n$ is countable.

Proof: (a) If $\{a_n : n \in \mathbb{N}\}$ is an enumeration of A, we can obtain an enumeration of B by pruning the elements of A which are not in B. This can be accomplished inductively as follows. Let $b_1 = a_n$, where n is the least positive integer such that $a_n \in B$. Suppose now that b_m has been defined and that $b_m = a_i$. Then let $b_{m+1} = a_j$, where j is the least positive integer $> i$ such that $a_j \in B$. Clearly $\{b_m : m \in \mathbb{N}\}$ is an enumeration of B.
(b) One can easily prove that $\mathbb{N} \times \mathbb{N}$ is countable by copying Example 0.2.60(c). Just form an array

$$\begin{array}{ccccc}
(1,1) & (2,1) & (3,1) & (4,1) & \dots \\
1,2) & (2,2) & (3,2) & (4,2) & \dots \\
(1,3) & (2,3) & (3,3) & (4,3) & \dots \\
\vdots & \vdots & \vdots & \vdots &
\end{array}$$

and zig–zag your way across this array. Let $A \xrightarrow{f} \mathbb{N}$ and $B \xrightarrow{g} \mathbb{N}$ be bijections. Then the map $h : A \times B \longrightarrow \mathbb{N} \times \mathbb{N}$ defined by $h(a,b) = (f(a), g(b))$ is clearly a bijection. Hence $|A \times B| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ as required.
(c) follows from (d).
(d) Again we use a zig–zag: Let $\{a_{n1}, a_{n2}, a_{n3}, \dots\}$ be a listing of the elements of A_n. Form an array

$$\begin{array}{cccc}
a_{11} & a_{12} & a_{13} & \dots \\
a_{21} & a_{22} & a_{23} & \dots \\
a_{31} & a_{32} & a_{33} & \dots \\
\vdots & \vdots & \vdots &
\end{array}$$

and take a path which goes through each element once, pruning duplications.

$\dashv$

This proposition shows that you can't make uncountable sets using finite products and countable unions. You can, however, make uncountable sets using infinite products and the powerset operation.

Proposition 0.2.70 *Let A be a set. Then $|A| < |\mathcal{P}(A)| = \mathbf{2}^A$.*

Proof: We know that for any set A, $\mathcal{P}(A) \approx \mathbf{2}^A$, by Example 0.2.60(d). So it suffices to show that $|A| < |\mathcal{P}(A)|$. Now it is obvious that there is an injection from A into $\mathcal{P}(A)$: The map $a \mapsto \{a\}$ will do the trick. Hence certainly $|A| \leq |\mathcal{P}(A)|$. Suppose now that there is a bijection $A \xrightarrow{f} \mathcal{P}(A)$, and define $A_a \subseteq A$ by $A_a = f(a)$. Since a bijection is surjective, we must have $\mathcal{P}(A) = \{A_a : a \in A\}$. We shall now show that this is impossible.

Note that $A_a \subseteq A$ and that $a \in A$. Thus it may happen that $a \in A_a$, or it may not. Define B to be the set of all a for which it does not happen, i.e. let

$$a \in B \Longleftrightarrow a \notin A_a$$

The $B \subseteq A$. Since the listing $\{A_a : a \in A\}$ is supposed to be a *complete* list of all the elements of $\mathcal{P}(A)$, there must be some $b \in A$ such that $B = A_b$. However, if $b \in B$, then $b \notin A_b$, and if $b \notin B$, then $b \in A_b$. Hence B cannot equal A_b, since b belongs to one set, but not the other. The assumption that $\{A_a : a \in A\}$ is a complete list of all the subsets of A therefore leads to a contradiction.

⊣

The following proposition is very useful:

Proposition 0.2.71 *Suppose that A, B are infinite sets, and that $|A| \leq |B|$. Then:*

(a) $|A \cup B| = |B|$

(b) $|A \times B| = |B|$

(c) $|A^B| = |\mathbf{2}^B|$.

⊣

We omit the proof, which can be found in almost any textbook on set theory.

Exercises 0.2.72 (1) Prove that if A is uncountable and B is countable, then $A - B$ is uncountable.

(2) Prove that $\mathbb{R} \approx [0, 1]$. (Hint: Note that all non-empty finite intervals have the same cardinality as $[0, 1]$. First prove that all closed intervals have the same cardinality. If I is any finite interval, whether open, closed, or half–open, we can find closed intervals I_1, I_2 such that $I_1 \subseteq I \subseteq I_2$. The Schröder–Bernstein Theorem then implies that they all have the same cardinality. Now define a map $\mathbb{Z} \times [0, 1) \xrightarrow{f} \mathbb{R}$ as follows: If $n \in \mathbb{Z}$ and if $x \in [0, 1)$, then define

$$f(n, x) = n + x$$

This is clearly a bijection. Now $|\mathbb{Z}| \leq |[0, 1]| = |[0, 1)|$, and therefore $\mathbb{R} \approx \mathbb{Z} \times [0, 1) \approx [0, 1]$.)

□

Example 0.2.73 $\mathbb{R} \approx \mathbf{2}^{\mathbb{N}}$. Here's a clever way of seeing this: Every real number has a *dyadic* or *binary* expansion, as opposed to a decimal expansion. The dyadic expansion uses only the numbers 0 and 1. For example, if we have a dyadic number 101.011, this is

$$\underbrace{101.011}_{\text{dyadic}} = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 + 0 \cdot 2^{-1} + 1 \cdot 2^{-2} + 1 \cdot 2^{-3} = \underbrace{5.375}_{\text{decimal}}$$

Hence every real number can be turned into a sequence of zeroes and ones, and vice versa. Now such a sequence is essentially just a map from $\mathbb{N}$ to $\mathbf{2}$. For example, the sequence $1011001\ldots$ can be thought of as the function $f : \mathbb{N} \longrightarrow \mathbf{2}$ which has $f(1) = 1, f(2) = 0, f(3) = 1, f(4) = 1, f(5) = 0, f(6) = 0, f(7) = 1 \ldots$. There are only two problems: (i) Where to put the decimal point, and (ii) Some real numbers have two distinct dyadic expansions. For example, $\frac{1}{2} = 0.1000\cdots = 0.01111\ldots$. However, if a real number has two dyadic expansions, it is easy to see that the one must eventually end in all $0^{\text{'s}}$, and the other must end in all $1^{\text{'s}}$. We call the former expansion terminating, and the latter expansion non–terminating.

We now overcome the two problems as follows: Since $\mathbb{R} \approx [0, 1)$, it suffices to show that $\mathbf{2}^{\mathbb{N}} \approx [0, 1)$. Now given any $x \in [0, 1)$, its non–terminating dyadic expansion $x = 0.x_1x_2x_3\ldots$ will give us a sequence $x_1, x_2, x_3\ldots$ of zeroes and ones. This clearly gives us an injective map $F : [0, 1) \longrightarrow \mathbf{2}^{\mathbb{N}}$. It is, however, not a surjective map. But only the sequences that eventually end in all zeroes have been missed out, and there are only countably many such. To be precise, if $\mathcal{X} = \text{range } F$, then $\mathcal{Y} = \mathbf{2}^{\mathbb{N}} - \mathcal{X}$ is countable. Hence $|\mathbf{2}^{\mathbb{N}}| = |\mathcal{X} \cup \mathcal{Y}| = |\mathcal{X}| = |(0, 1]| = |\mathbb{R}|$.

□

Example 0.2.74 (The Cantor set) The *Cantor set* is a subset of $[0,1]$ which is constructed as follows: Let $C_0 = [0,1]$. It is a single interval of length 1. Now let C_1 be C_0 with its *middle third* removed, i.e. $C_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$. Thus C_1 consists of two disjoint intervals, each of length $\frac{1}{3}$. Now remove the middle thirds of these two intervals to form C_2, i.e. $C_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$. Then C_2 is a disjoint union of 4 intervals, each of length $\frac{1}{9}$. Continue in this way, removing the middle thirds of each of the intervals comprising C_n to form C_{n+1}. It follows that C_n consists of 2^n intervals, each of length $(\frac{1}{3})^n$, and thus that $\lambda(C_n) = (\frac{2}{3})^n$. Finally, let $C = \bigcap\limits_{n=0}^{\infty} C_n$. C is the Cantor set.

How much of $[0,1]$ did we remove when we created C? First we removed an interval of length $\frac{1}{3}$, then we removed 2 intervals, each of length $\frac{1}{9}$. After that, we removed 4 intervals, each of length $\frac{1}{27}$, etc. Thus we have removed disjoint sets with a total length

$$\frac{2^0}{3^1} + \frac{2^1}{3^2} + \frac{2^2}{3^3} + \cdots = \frac{1}{3} \sum_{k=0}^{\infty} \left(\frac{2}{3}\right)^k$$

which is a geometric series with sum $\dfrac{1}{3} \cdot \dfrac{1}{1 - \frac{2}{3}} = 1$. It seems, therefore, that we have removed the entire length of the unit interval $[0,1]$. There is no length left.

Nevertheless, C is not empty; in fact, C is uncountable. Here is one way to see this: Every real number $a \in [0,1]$ can be written as an infinite sum $\sum\limits_{i=1}^{\infty} \dfrac{a_i}{3^i}$, where $a_i = 0, 1$ or 2. Thus the *ternary expansion* (as opposed to *decimal expansion*) of a is $0.a_1a_2a_3\ldots$. For example, $\frac{1}{3} = 0.1000\ldots$, $\frac{5}{9} = \frac{1}{3} + \frac{2}{9} = 0.1200\ldots$, etc. A little thought will reveal that the Cantor set is formed by removing all numbers which have a 1 occurring in their ternary expansion. Thus C_1 is formed by removing all numbers which have a 1 in the first decimal place, C_2 is formed by removing all numbers in C_1 which have a 1 in the second decimal place, and so on. Thus the Cantor set is just the set of all numbers a in $[0,1]$ which can be written as a sum $\sum\limits_{i=1}^{\infty} \dfrac{a_i}{3^i}$, where $a_i = 0$ or 2, but not 1. There is a bijection $\Phi : 2^{\mathbb{N}} \longrightarrow C$ defined as follows: If $f \in 2^{\mathbb{N}}$, then $\Phi(f)$ is the number with decimal expansion $0.a_1a_2a_3\ldots$, where $a_n = 0$ if $f(n) = 0$, and $a_n = 2$ if $f(n) = 1$. Hence $|C| = |2^{\mathbb{N}}| = |\mathbb{R}|$.

□

0.3 Prelude to an Axiomatic Development of the Real Number System

0.3.1 Why we need Axioms

Consider the following questions:

Question 1: Many years ago, you were taught the following algorithm for multiplying two numbers:

$$\begin{array}{r} 23 \\ \underline{17} \\ 161 \\ \underline{230} \\ 391 \end{array}$$

Why does this algorithm work?

Question 2: Why is $-1 \times -1 = 1$? Alternatively, why is the product of two negative numbers a positive number?

If you think that these are silly questions, think again. The answers to these questions are *not* obvious. You are merely so used to the answers that the questions never occur to you.

An explanation for why the multiplication algorithm works might go along the following lines:

$$\begin{aligned} 23 \times 17 &= 23 \cdot (7 + 10) \\ &= 23 \cdot 7 + 23 \cdot 10 \\ &= (20 + 3) \cdot 7 + (20 + 3) \cdot 10 \\ &= [20 \cdot 7 + 3 \cdot 7] + [20 \cdot 10 + 3 \cdot 10] \\ &= [140 + 21] + [200 + 30] \qquad\qquad = 161 + 230 \\ &= 391 \end{aligned}$$

To do this calculation, we performed the following operations:

(i) We used the fact that $a \cdot (b + c) = a \cdot b + a \cdot c$ several times.

(ii) We retrieve certain results, like $3 \cdot 7 = 21$, from memory. Such results were learnt by rote, in the form of multiplication tables. Thus all the values of $a \times b$ for $1 \leq a, b \leq 10$ are stored in a mental look–up table.
The values in the look–up table were determined *empirically*, i.e. by observation. To see that $7 \times 8 = 56$, take 8 small bags, each containing 7 stones, and empty them into a big bag. If you now count the number of stones in the big bag, you will get 56. That's just a fact that's been observed over and over again, in many different places and at many different times.

(iii) We use the fact that multiplying a number by 10 is accomplished by adding a zero to the end of that number. Thus $20 \cdot 10 = 200$.

(iv) To calculate the value of a term such as $20 \cdot 7$ (which is not in the mental look–up table), we have to argue that $20 \cdot 7 = 7 \cdot 20 = 7 \cdot (2 \cdot 10) = (7 \cdot 2) \cdot 10 = 14 \cdot 10 = 140$. Thus, in addition to the look–up table and the multiply–by–ten rule, we also used the following facts about multiplication: $a \cdot b = b \cdot a$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(v) We used another algorithm (also learnt long ago) for adding numbers, such as $161 + 230$. Try and justify that algorithm yourself.

As you can see, in order to explain why the multiplication algorithm works, you need to invoke quite a few simpler results about addition and multiplication. Question 1 is not as obvious as it looks! As for Question 2, you should be able to explain why $-1 \times -1 = 1$ by the end of this chapter.

Now note the following (empirically verifiable) facts: Human beings have a certain intuition (or idea) about non–physical objects called numbers. These numbers can be combined in various ways to form new numbers, e.g. they can be added and multiplied. Moreover, there are some simple rules which govern the combination of numbers, e.g.

(i) The product of two numbers does not depend on where or when the multiplication is performed.

(ii) $a + b = b + a \qquad ab = ba$

(iii) $a + (b + c) = (a + b) + c \qquad a(bc) = (ab)c$

(iv) $a(b + c) = ab + ac$

et cetera. Our aim is now to find a set of rules, or *axioms*, which completely captures our intuition about the arithmetic of the reals. In other words, we seek a set of rules which (1) is in accord with our intuition about arithmetic, and (2) is sufficiently rich that any informal, intuitive arithmetic argument can be made *formal*, i.e. we can reach the same conclusion by applying no intuition at all, but just the axioms.

Why do we need axioms? For several reasons.

- Axioms tend to be simple, and most people will accept them as in agreement with their intuition. Thus the axioms are a common starting point for all people. People who disagree on the axioms are probably talking about different things.

- The agreed–upon rules can be applied over and over again, to arbitrary levels of complexity. Any two people who agree on the (simple) axioms will also agree on the (complicated) conclusions that may be reached by formal application of those axioms.

  On the other hand, intuition becomes less and less reliable as we increase the level of complexity, and thus conclusions obtained solely by a intuition are more suspect. For example, you and I may agree that Euclid's 5 axioms for geometry are in accordance with our intuition of *space*. These axioms are simple, and difficult to disbelieve. *You* may have a powerful intuition, however: You intuit that the square of the (length of) the hypotenuse of a right–angled triangle is equal to the sum of the squares of the other two sides. But *my* intuition is far less developed than yours: I just don't see it, and so I don't believe you. Should you provide a step–by–step argument, starting from our common ground (the 5 axioms), using only commonly agreed rules, I will be forced to admit that your intuition is correct. In this way, I can verify the truth of your assertion myself, and don't just have to take your word for it.

- If we use the axiomatic method, we are constantly aware of our assumptions. It therefore becomes much simpler to discern similarities and differences between various mathematical objects and operations. This will make the arguments *portable* (in the Computer Science sense — arguments (computer code) can easily be moved from one problem to (platform) to another).

  For example, the rules $a \cdot (b+c) = a \cdot b + a \cdot c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ apply not only to multiplication of numbers, but also to multiplication of matrices. Thus any proposition that can be proved about numbers, using just those rules, will also be true for matrices. However, the rule $a \cdot b = b \cdot a$ does not hold for matrices.

- Finally, axioms allow us to circumvent metaphysical speculation about the nature and existence of mathematical objects. What, for example *is* a real number? Is it an irreducible, or is it made up of simpler things? This question was first given a satisfactory answer in 1872. Indeed, it was given *two* different but satisfactory answers in that year, by Dedekind and Cantor. In each case, the real numbers are ”constructed” from some previously constructed, simpler, objects, e.g. the rational numbers.

  And the rational numbers are in turn constructed from the positive integers, which are constructed from the empty set — We'll go into a bit more depth later in this chapter, but for a proper explanation, you will need to read a book on set theory.

  Thus there is no single answer to the question: ”What is a real number?”. But the exact nature of the reals is unimportant for mathematical purposes. What is important is how they *behave*, i.e. how they can be recombined, using various operations, to form new numbers. The axioms are essentially just a description of such behaviour, and though the three constructions disagree about the essential nature of the reals, they *do* agree on how they behave.

(i) George Cantor held that a real number *is* a set of sequences of rational numbers. Thus, for example, $\sqrt{2}$ is just the set of all rational sequences that converge to $\sqrt{2}$. (This definition may seem circular, but the apparent circularity can be removed.)

(ii) For Richard Dedekind, a real number *is* an ordered pair of sets of rational numbers. Thus,

$$\sqrt{2} = (\{q \in \mathbb{Q} : q^2 \leq 2\}, \{q \in \mathbb{Q} : Q^2 > 2\})$$

(iii) John Horton Conway regards a real number as a *game* played by two individuals. I won't elaborate.

0.3.2 A Brief Note on the Philosophy of Mathematics*

In the previous section, we got quite philosophical. Before we continue, it's a good idea to have a look at the main mathematical schools of thought. Our main concern is with the schools of *Platonism* and *Formalism.* For completeness, I present brief and over–simplified caricatures of these and other leading schools below. If you want an honest exposition, you'd better consult a book on the philosophy of mathematics.

- **Platonism:** The belief that mathematical objects, though not part of the physical universe, nevertheless have an existence which is independent of the human mind. We speak of making mathematical *discoveries*, which suggests that we are somehow able to observe mathematical objects.

  Some people also speak about mathematical *creations*. Did da Vinci have the freedom to create a Mona Lisa with a grimace, rather than a smile? Probably. He preferred a smile. But did Pythagoras have the freedom to create a right–angled triangle for which his theorem — that the square of the hypotenuse is the sum of the squares on the right–angle sides — fails?

- **Logicism:** An attempt to reduce mathematics to logic. Frege and Russell are the main protagonists. The four–volume *Principia Mathematica*, by Russell and Whitehead, is the most well–known exposition of this school.

- **Constructivism:** Constructivists require that, in order to show that a mathematical object exists, one must explicitly show *how* to construct it. This leads them to reject of the *Law of the Excluded Middle*, which states that for any statement φ, either φ is true, or not-φ is true, i.e. there's no "middle" between φ and not-φ. It also leads to the rejection of proofs by contradiction. There are many varieties of constructivism; the most well–known is *Intuitionism*, whose main proponent was Brouwer.

  For example, suppose that S is a set, and that φ is a property. In *classical logic*, the following statement is true:

  Either there is a member of S that has property φ,
  or every member of S has property not-φ. $(*)$

  For example, consider the *Riemann Hypothesis*, which states that all the (complex) roots of the Riemann ζ–function have a real part equal to $\frac{1}{2}$:

$$1+\frac{1}{2^z}+\frac{1}{3^z}+\cdots=0 \quad\Longrightarrow\quad \mathrm{Re}(z)=\frac{1}{2}$$

  This is currently *the* unsolved problem in mathematics. For the classical logician, the Riemann Hypothesis is either true or false — we just don't know which. Not so for the constructivist: To say that it is either true or false, we must either prove that it is true, or show that it is false. So the constructivist does not accept $(*)$. For this statement to hold, we must either show how to construct a member of S with the property φ, or we must show that each member of S has the property not-φ.

  If S is a finite set, we could, in principle, look at each of the elements of S in turn, to see if it satisfies φ. If S is infinite, however, this is generally not possible. Constructivists are happy to apply the Law of the Excluded Middle to finite sets; its application to infinite sets they regard as a colossal mistake — an unwarranted and unjustifiable extrapolation of methods of reasoning designed for the finite to the infinite. Indeed, some constructivists deny the existence of infinite objects altogether.

  As another example, suppose that we want to prove that every real cubic polynomial $p(x) = x^3 + ax^2 + bx + c$ has a real root. One way to do it is to appeal to the *Intermediate Value Theorem*: We see that $p(x) > 0$ for all sufficiently large positive x, and thus that $p(x)$ lies above the X–axis, for all sufficiently large positive x. Similarly, $p(x) < 0$ for all sufficiently large negative x, so that $p(x)$ lies below the X–axis, for all sufficiently large negative x. Hence, since $p(x)$ is continuous, there must be a place where $p(x)$ cuts the X–axis, and that place would be a root of $p(x)$. This proof is *non–constructive*: We've shown that there is a root, but we haven't shown how to find it.

- **Formalism:** This school of thought dates back to Hilbert in the late 19th century. At that time, certain paradoxes in *set theory* shook the foundations of mathematics, and mathematicians were suddenly confronted with the possibility that their subject is inconsistent, i.e. self–contradictory.
  The most famous of these is *Russell's paradox.* If we admit a naive concept of set — a set is any old collection of objects — then it is possible for a set to belong to itself. For example if

  $$A = \text{The set of all objects that can be defined in English using fewer than twenty words}$$

  then $A \in A$, because we've just defined A using fewer than twenty words. Now consider a set of sets R, defined as follows:

  $$A \in R \quad \text{iff} \quad A \notin A$$

  Since R is a set, we may legitimately ask if it belongs to itself. By definition of R, we see that

  $$R \in R \quad \text{iff} \quad R \notin R$$

  If R belongs to R, then it doesn't; and if R does not belong to R, then it does! This paradox, usually credited to the logicist Russell in 1899??, but already noted by Zermelo in 1896?? caused quite a lot of concern.

  Hilbert, the most powerful mathematician of his era, set up a programme aimed at proving the internal consistency of mathematics by so–called *finitist means.* The formalist regards mathematics as a one–player game, rather like Patience (or Freecell). A proof of a statement ψ, for example, is merely a sequence of statements $\varphi_1, \varphi_2, \ldots, \varphi_n$, ending with $\varphi_n = \psi$. Each φ_k must either be an axiom, or must be obtained from previous φ_j by certain permitted "moves", or rules of deduction.
  For example, a commonly used rule of deduction is *Modus Ponens*:

  $$\text{From } \varphi \to \psi \text{ and } \varphi \text{ deduce } \psi$$

  The mathematician seeking to prove the statement ψ is like the player of Patience, trying out permitted sequences of moves until she hits upon a sequence that works. The idea behind the Hilbert Programme is to *formalize* mathematics:

  – Write all mathematics in a *formal language*;

  – Reduce all proofs to *formal deductions*;

  – Show that no contradictions can be derived within this formal system.

  Hilbert had hoped that it would be possible to show that all of mathematics could be thus reduced, and proved consistent. Thus commenced a massive attempt to formalize and axiomatize all of mathematics, and the way that we now do and see mathematics has been heavily influenced by the Hilbert programme.

  One of the first branches of mathematics to be formalized was *set theory*, where the paradoxes had been found. The Zermelo–Fraenkel axioms of set theory banish Russell's paradox, but at a costs: It is no longer possible for a set to belong to itself, and the intuition of a set as "just any old collection of objects" had to be abandoned. It was found possible to squeeze nearly all of mathematics inside the formal system of axiomatic set theory. Unfortunately, Hilbert's student Gödel proved in 1931 that the Hilbert programme was doomed to failure. In a paper entitled *On formally undecidable statements in Principia Mathematica and related systems* he showed that in any formalist reduction of mathematics there would be statements that are *true*, but *unprovable*. He also showed that no such reduction is capable of proving its own consistency. This proved the death knell for the Hilbert programme, though not for the Formalist school. (Gödel himself was a Platonist.) With hindsight, it is remarkable how close the Hilbert programme came to succeeding.

Platonism and Formalism disagree (quite violently) about the *nature* of mathematical objects: For the Platonist, these have an existence independent of the human mind; by the mysterious faculty of intuition we apprehend basic truths (axioms) about mathematical objects, and then use reason to deduce ever more complex truths (theorems). For the Formalist, there are no mathematical objects, just rules for transforming one string of symbols into another.

Nevertheless, both schools of thought *agree* on what constitutes a valid mathematical proof. The average practicing mathematician has been described as "a Platonist on weekdays, and a Formalist on Sundays. That is, when he is doing mathematics he is convinced hat he is dealing with an objective reality whose properties he is attempting to determine. But then, when challenged to give a philosophical account of this reality, he finds it easiest to pretend that he does not believe in it after all."

And that's what our position will be. To begin with, we will be firm Platonists: We will believe in the objective existence of the real number system, and use our intuition to apprehend basic truths. Recognising that our intuition is fallible, however, we won't let it stray to far. Instead, we opt soon to formalise our intuitions into a system of axioms. After that, intuition is only allowed to make suggestions, and only those statements that can be seen to admit a *formal* proof will be admitted to the status of theoremhood.

0.3.3 Logic, Formal Languages, Quantifiers

The aim of this section is to cover the bare minimum about formal theories — just enough to make our construction of the real number system intelligible.

A *formal language* is a collection of $\mathcal{L}$ whose *logical symbols* include

- **Logical Connectives**

$\wedge$	and
$\vee$	or
$\rightarrow$	implies
$\leftrightarrow$	if and only if
$\neg$	not

It is enough to use just two connectives, e.g. $\wedge$ and $\neg$. We can then define the remainder by

$$\begin{aligned}\varphi \vee \psi &\equiv \neg(\neg\varphi \wedge \neg\psi)\\ \varphi \to \psi &\equiv \neg\varphi \vee \psi\\ \varphi \leftrightarrow \psi &\equiv (\varphi \to \psi) \wedge (\psi \to \varphi)\end{aligned}$$

Just a reminder: $\vee$ is *inclusive–or*: $p \vee q$ is true if and only if at least one of p, q is true, possibly both.

- **Quantifiers**

$\forall$	For all
$\exists$	There exists

We have

$$\forall x\varphi \equiv \neg\exists x(\neg\varphi) \qquad \exists x\varphi \equiv \neg\forall x(\neg\varphi)$$

- **Variables**
  $x, y, z, x_1, x_2, x_3 \ldots$

- **Identity relation**
  A special binary relation symbol denoted $=$.

Logical symbols have the same meaning, regardless of context. $\mathcal{L}$ also has *non–logical* symbols, whose meaning depends on context:

- **Relation symbols**
  For example, if we want to talk about partial orderings, we will want a symbol $\leq$; if we want to talk about sets, we will want symbols $\in$ and $\subseteq$.

- **Function symbols**
  For example, if we want to talk about arithmetic, we will want binary function symbols $+, \times$. We may want unary function symbols $-, ^{-1}$. If we want to talk about sets, we will want binary function symbols $\cap, \cup$, unary function symbols $^c, \mathcal{P}$;

- **Constant symbols**
  These are specially named elements, and are often regarded as *nullary* function symbols. For example, if we want to talk about addition, a *distinguished element* denoted by 0 plays an important role. If we want to talk about sets, the set $\emptyset$ deserves its own name.

A formal language will generally not contain all of the above non–logical symbols, only those needed to talk about the domain of discourse. $\mathcal{L}$ will also have brackets $(,), [,]$, etc.

The symbols of a formal language may be "strung" together to form two types: *terms* and *formulas.*

- **Terms** are defined as follows:

(i) Every variable and every constant is a term;

(ii) If $t_1, \dots, t_n$ are terms, and if F is an n–ary function symbol, then $F(t_1, \dots, t_n)$ is a term;

(iii) A string is a term only if it can be shown to be so by a finite number of applications of (i) and (ii);

- **Formulas** are defined as follows:

(i) If $t_1, \dots, t_n$ are terms, and if R is an n–ary relation symbol, then $R(t_1, \dots, t_n)$ is a formula. (This includes the case where R is the logical binary relation symbol $=$).

(ii) If φ, ψ are formulas, then so are $(\varphi \wedge \psi)$, $(\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi)$;

(iii) If φ is a formula, then so is $\neg\varphi$;

(iv) If φ is a formula and x is a variable, then $\forall x\varphi$ and $\exists x\varphi$ are formulas;

(v) A string is a formula only if it can be shown to be so by a finite number of applications of (i)-(iv).

We often omit brackets when there is no danger of confusion. Moreover, we may also abbreviate $\forall x\forall y\varphi$ by $\forall x, y\varphi$.

If φ is a formula, we write $\varphi(x, y, z)$ to show that the variables of φ are (amongst) x, y, z.

Example 0.3.1 Partial orderings
Consider the following language $\mathcal{L}$: In addition to the logical symbols, $\mathcal{L}$ has a single binary relation symbol $\leq$. There are no function and constant symbols. Thus the only terms of $\mathcal{L}$ are the variables. Some example of formulas are

$$x \leq y, \ \ \forall x(x \leq y \wedge y \leq z) \rightarrow \exists z(\neg(z \leq x))$$

The theory of partial orderings has the following axioms

(i) $\forall x(x \leq x)$;

(ii) $\forall x, y(x \leq y \wedge y \leq x \rightarrow x = y)$;

(iii) $\forall x, y, z(x \leq y \wedge y \leq z \rightarrow x \leq z)$.

This theory has many *interpretations*. One is the two–element chain $C_2 = \{0, 1\}$ with $0 \leq 1$. This is a linear ordering, i.e. it satisfies the axiom $\forall x, y(x \leq y \vee y \leq x)$. Another example is the powerset $\mathcal{P}(A)$ of a set A, where $\leq$ is interpreted as “subset”. This ordering is non–linear if A has more than one element.

Thus different structures may satisfy the same axioms.

□

Example 0.3.2 Peano Arithmetic
We give here another example of a formal theory. In addition to the logical symbols, $\mathcal{L}$ has the following non–logical symbols:

- Binary function symbols $+$ and $.$;
- A unary function symbol S;

- A constant symbol 0.

Some examples of terms are:

$$x,\ S(x),\ 0,\ S(S(S(0))),\ x+y,\ (x+S(y))\cdot z,\ (y\cdot S(z))+w$$

Some examples of formulas are:

$$x+y=0,\ \forall x\exists y(x+S(S(0))=y),\ \forall x(x=S(y)\vee\neg(S(x)=y))$$

Peano arithmetic is a formal theory in the language $\mathcal{L}$. The axioms are:

(i) $\forall x[\neg(S(x)=0)]$;

(ii) $\forall x\forall y(S(x)=S(y)\rightarrow x=y)$;

(iii) $\forall x(x+0=x)$;

(iv) $\forall x\forall y(x+S(y)=S(x+y))$;

(v) $\forall x(x\cdot 0=0)$;

(vi) $\forall x\forall y(x\cdot S(y)=x\cdot y+x)$;

(vii) For every formula $\varphi(x_0,\dots,x_n)$, we have

$$\begin{aligned}\forall x_1\dots\forall x_n[(\varphi(0,x_1,\dots,x_n)\wedge(\forall x_0(\varphi(x_0,x_1,\dots,x_n)\rightarrow\varphi(S(x_0),x_1,\dots,x_n))\\ \rightarrow\forall x_0\varphi(x_0,x_1,\dots,x_n)]\end{aligned}$$

We will now show that in this system we can prove the following identity:

$$\forall x,y[x+y=y+x]$$

- We first show that for all x, $0+x=x$. Let $\varphi(x)$ be the formula

  $$0+x=x$$

  Then certainly $\varphi(0)$ is true, because $0+0=0$ by (iii). Now suppose that $\varphi(x)$ is true. Then by (iv)

  $$0+S(x)=S(0+x)=S(x)$$

  and so $\varphi(S(x))$ is also true. We have thus shown that $\varphi(0)$ holds, and that if $\varphi(x)$ holds, then so does $\varphi(S(x))$. Axiom (vii) allows us to deduce that $\forall x\varphi(x)$.

- Next, let $\psi(y,x)$ be the formula

  $$x+S(y)=S(x)+y$$

  Then $x+S(0)=S(x+0)=S(x)=0+S(x)$, by (iv) and what we've just shown. Hence $\psi(0,x)$ is true, for every x. Next, suppose that $\psi(y,x)$ is true for every x. Then

  $$\begin{aligned}x+S(S(y))&=S(x+S(y)) &&\text{by (iv)}\\ &=S(S(x)+y) &&\text{because } \psi(y,x)\\ &=S(x)+S(y) &&\text{by (iv)}\end{aligned}$$

  so that $\psi(S(y),x)$ is true, for every x.
  By (vii), it follows that $\psi(y,x)$ is true for all y and all x.

- Finally, let $\xi(y,x)$ be the formula
$$x+y=y+x$$
Then we know that $\xi(0,x)$ is true, for all x, because $\varphi(x)$ is true for all x. Assume now that $\xi(y,x)$ is true for all x. Then
$$\begin{aligned} S(S(y)+x) &= S(y)+S(x) && \text{by (iv)} \\ &= y+S(S(x)) && \text{because } \psi(S(x),y) \\ &= S(S(x))+y && \text{because } \xi(y,S(S(x))) \\ &= S(x)+S(y) && \text{because } \psi(y,S(x)) \\ &= x+S(S(y)) && \text{because } \psi(S(y),x) \\ &= S(x+S(y)) && \text{by (iv)} \end{aligned}$$
Thus by (ii), $S(y)+x=x+S(y)$. Hence $\xi(y,x) \to \xi(S(y),x)$, so that by (vii) we can conclude that $\xi(y,x)$ is true for all x,y.

Right now, you probably don't know what $S(x)$ actually *means*. Like good formalists,we've proved the commutativity of the binary operation $+$ by playing a game of deduction from the axioms. We invoked the mysterious symbol S in several places, without knowing its meaning.

The meaning, or *natural interpretation*, or *canonical model* of the Peano axioms is as follows: The axioms are "about" the natural numbers $\mathbb{N}=\{0,1,2,\dots\}$. The binary function symbol $+,\cdot$ are to be interpreted, respectively, as addition and multiplication. The unary symbol S is to be interpreted as *successor*: $S(x)=x+1$. (However, there is no constant symbol 1.) The constant symbol 0 is to be interpreted as the number zero. Thus $S(0)=1$ (1 is the successor of 0), $S(S(0))=2$, etc.

The first axiom says that 0 is not the successor of any other number. The second axiom says that if x,y have the same successor, then x,y are equal. You can interpret the other axioms yourself. Just note that (vii) is not a single axiom, but an infinite set of axioms, one for every formula φ. The *axiom schema* (vii) formalizes mathematical induction: If 0 has property φ, and if whenever x_0 has property φ, then also $S(x)$ has property φ, then we can conclude that every number x_0 has property φ.

Just like the axioms for partial orderings, the Peano axioms have many other interpretations as well. These are the so–called *non–standard* models of arithmetic.

□

In this section, I have presented the briefest possible introduction to formal theories, and I've taken numerous short cuts. If you want more extensive (and more accurate) coverage, you will have to consult a text on mathematical logic. We end this section with some brief comments on quantifiers and negation.

Consider the following formulas:
$$\forall x \exists y (y>x)$$
To check the truth of such a statement, it is convenient to regard it as a game between two players, $\forall$ and $\exists$. In this game, $\forall$ opens play and chooses and x. If $\exists$ can find a y such that $y>x$, then $\exists$ wins the game. If she can't, $\forall$ wins. The formula is true if $\exists$ can always win, i.e. if $\exists$ has a *winning strategy*; else, the formula is false.

Whether or not the formula is true or false depends on where it is played. If we play it on the natural numbers $\mathbb{N}$, then $\exists$ has a winning strategy: If $\forall$ chooses x, the $\exists$ can choose $y=x+1$. Then $y>x$. This works for any x that $\forall$ might choose. Hence $\exists$ has a winning strategy: The formula is true for $\mathbb{N}$.

Suppose, however, that the game is played not in $\mathbb{N}$, but on the two–element chain $C_2 = \{0, 1\}$. Then if $\forall$ chooses $x = 1$, $\exists$ cannot find a $y \in C_2$ with $y > x$. Hence $\forall$ has a winning strategy, and the statement is false for C_2.

Exercise 0.3.3 Give a similar analysis for the statement

$$\exists y \forall x (y > x)$$

□

Finally, a note about negating quantifiers: A negation sign can "creep" past a quantifier, but it *flips* the quantifier in the process:

$$\neg \forall x \varphi \equiv \exists x (\neg \varphi) \qquad \neg \exists x \varphi \equiv \forall x (\neg \varphi)$$

For example,

$$\begin{aligned} \neg[\forall x \exists y (y > x)] &\equiv \exists x \neg [\exists y (y > x)] \\ &\equiv \exists x \forall y (y \not> x) \end{aligned}$$

Real Analysis

P. Ouwehand

Department of Mathematics and Applied Mathematics
University of Cape Town

Contents

Chapter 1

An Axiomatic Development of the Real Number System

In this chapter, we present an axiomatization of the real number system. We shall do this in three stages:

(1) First we shall discuss the purely arithmetic properties of the reals. The reals form an algebraic system called a *field*. Intuitively, a field is a set in which addition, subtraction, multiplication and division are possible, and obey the usual rules.

(2) Next, we shall discuss the properties of a field equipped with an ordering relation $\leq$.

(3) Finally, we shall add an axiom, the *Completeness Axiom*, which ensures that it is possible to take limits.

A word of warning:
Throughout this section, I refer to the reals as though you already know what they are and how they behave (which, of course, to a large extent you do). The more philosophically minded may therefore come to believe that much of the discussion is *circular*: I *define* the properties of the reals by *observing* the properties of the reals.
That is not the case. As explained in Section 0.3, we operate on two levels, the *intuitive* and the *formal*: We have an intuitive idea of real numbers, to which I make frequent appeal. This intuition is then used to inform the *formal* level.

1.1 Fields and Arithmetic

Definition 1.1.1 A *field* is a tuple $\langle F, +, \cdot, -, ^{-1}, 0, 1\rangle$, satisfying all the properties below:

- F is a *set*;
- $+, \cdot$ are binary operations on F.
  This means that $+, \cdot$ are functions of two variables on F:

$$+, \cdot : F \times F \to F$$

It is customary to write $a+b$ instead of $+(a,b)$, and $a\cdot b$ or ab instead of $\cdot(a,b)$.

- $0,1$ are *distinct* designated members of F.
  Such elements are also called *nullary operations* on F, or constants. We call 0 the *zero element*, or *additive identity*. Similarly, we call 1 the *unit element*, or the *multiplicative identity*.

- $-,^{-1}$ are unary operations on F.
  Thus $-,^{-1}$ are functions from F to F. However, $^{-1}$ is a *partial function*: a^{-1} is defined if and only if $a\neq 0$.

In order to prevent a plethora of brackets, we will assume that the operations satisfy the usual order of precedence: $^{-1}$ before $\cdot$ before $-$ before $+$. Thus $ab^{-1}=a\cdot(b^{-1})$ (and not $(ab)^{-1}$), $ab+c=(ab)+c$ (and not $a(b+c)$), etc. We also write $b-a$ instead of $b+(-a)$ and x^2y instead of xxy, etc.

In addition, the operations are required to satisfy the following properties:

(C^+)	$a+b=b+a$	(Commutativity of addition)
(A^+)	$(a+b)+c=a+(b+c)$	(Associativity of addition)
(Id^+)	$a+0=a=0+a$	(Additive identity)
(Inv^+)	$a+(-a)=0=(-a)+a$	(Additive inverse)
$(\mathrm{C}^\cdot)$	$a\cdot b=b\cdot a$	(Commutativity of multiplication)
$(\mathrm{A}^\cdot)$	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$	(Associativity of multiplication)
$(\mathrm{Id}^\cdot)$	$a\cdot 1=a=1\cdot a$	(Multiplicative identity)
$(\mathrm{Inv}^\cdot)$	$a\cdot(a^{-1})=1=(a^{-1})\cdot a$ when $a\neq 0$	(Multiplicative inverse)
(D)	$a\cdot(b+c)=a\cdot b+a\cdot c$	(Distributivity of $\cdot$ over $+$)

□

A set G equipped with a binary operation ("multiplication" or "addition") which is associative, has an identity element, and has all inverses is called a *group*. If the operation is also commutative, then G is called an *abelian group*. Thus if $\langle F,+,\cdot,-,^{-1},0,1\rangle$ is a field, then $\langle F,+,-,0\rangle$ is an abelian group, as is $\langle F-\{0\},\cdot,^{-1},1\rangle$.

Examples 1.1.2 (1.) The set $\mathbb{Q}$ of rational numbers with the usual operations is a field.

(2.) The set $\mathbb{R}$ of real numbers with the usual operations is a field.

(3.) The set $\mathbb{Z}$ of integers with the usual operations is *not* a field. Why not?

(4.) The set $\mathbb{C}$ of complex numbers with the usual operations is a field.

(5.) Let $F=\{a,b\}$. Define the operations $+,\cdot$ on F as follows:

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

It is easy to verify that $+, \cdot$ are commutative and associative.

For example, $a + b = b = b + a$, $a + (a + b) = a + b = b = a + b = (a + a) + b$.

We see that a behaves like an additive identity, in that $a + x = x$ for all $x \in F$. Furthermore, b behaves like a multiplicative identity, in that $b \cdot x = x$ for all $x \in F$. Let's therefore make a the designated element 0, and make b the designated element 1, so that $F = \{0, 1\}$ and our tables look like:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

To make F into a field, we must also see if we can define two unary operations $-$ and $^{-1}$. Now $1 + 1 = 0$ and $0 + 0 = 0$ so we can define $- : F \to F$ by: $-1 = 1$, $-0 = 0$. The operation $^{-1}$ needs only be defined for the element 1. As $1 \cdot 1 = 1$, we can define $1^{-1} = 1$. Thus

x	$-x$
0	0
1	1

x	x^{-1}
1	1

It is easy to see that the addition and multiplication defined on F are just ordinary division and multiplication, modulo 2.
The field F goes by the name $\mathbb{Z}_2$.

(6.) For any positive integer n, we define $\mathbb{Z}_n = \{1, 2, \ldots, n - 1\}$. We can then define the operations of addition $+_n$ and multiplication $\cdot_n$ to be ordinary division and multiplication, modulo n. Thus

$$a +_n b \text{ is the remainder when } a + b \text{ is divided by } n$$

and

$$a \cdot_n b \text{ is the remainder when } a \cdot b \text{ is divided by } n$$

We will omit the subscript n from the operations $+, \cdot$.
Below are the tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$:

$\mathbb{Z}_3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Can we make $\mathbb{Z}_n$ into a field? If we look at the addition and multiplication tables for $\mathbb{Z}_3$, we see that it can be made into a field:

$\mathbb{Z}_3$

x	$-x$
0	0
1	2
2	1

x	x^{-1}
1	1
2	2

You must check that these operations satisfy the axioms: e.g. $2 \cdot 2^{-1} = 2 \cdot 2 = 1$.

But, though we can define $-$ for $\mathbb{Z}_4$, we cannot define $^{-1}$. The problem is that $2 \cdot 2 = 0$ in $\mathbb{Z}_4$. Since $2 \neq 0$, it should have an inverse $2^{-1} \in \mathbb{Z}_4 = \{0, 1, 2, 3\}$. But then

$$2 = 2 \cdot 1 = 2 \cdot (2 \cdot 2^{-1}) = (2 \cdot 2) \cdot 2^{-1} = 0 \cdot 2^{-1} = 0$$

because, from the tables, $0 \cdot x = 0$ for all $x \in \mathbb{Z}_4$.

It should not be hard to convince yourself that for $\mathbb{Z}_n$ to be a field it is necessary that n is a prime. It also turns out to be a sufficient condition.

We present a proof of this assertion, which you may omit. It is easy to see that $\mathbb{Z}_n$ satisfies all the field axioms, except possibly the existence of a multiplicative inverse.

To prove the existence of a multiplicative inverse, we need the following fact: If a, b are natural numbers, and if d is the greatest common divisor of a, b (denoted $g.c.d(a, b)$), then d is a linear combination of a, b (with integer coefficients) i.e. there exist integers x, y such that

$$d = ax + by$$

To see how this fact solves our problem, note that if n is prime, then $g.c.d(n, m) = 1$ for all natural numbers $m < n$. It follows that for all such m we can find integers x, y such that

$$1 = nx + my$$

Thus

$$m \cdot y = 1$$

in $\mathbb{Z}_n$ (i.e. $m \cdot_n y = 1$, because the remainder when my is divided by n is 1: $my = -nx + 1$) and thus each element of $\mathbb{Z}_n$ has a multiplicative inverse (namely its corresponding y).

So it remains to show that if $d = g.c.d(a, b)$, then d is a linear combination of a, b. To do this, we introduce the *Euclidean algorithm* for finding the greatest common divisor $g.c.d(a, b)$ of two natural numbers a, b (with $a > b$). This is an extremely efficient algorithm, and heavily used in *cryptography.* It works *recursively*, as follows: Define $r_0 = a, r_1 = b$. First divide r_0 by r_1, and write down the quotient q_2 and the remainder r_2, i.e.

$$r_0 = r_1 \cdot q_2 + r_2$$

Note that $r_2 < r_1 < r_0$. Now divide r_1 by r_2, and write down the quotient q_3 and the remainder r_3, i.e.

$$r_1 = r_2 \cdot q_3 + r_3$$

Note that $r_3 < r_2$. Repeat this process, so that

$$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$$

with $r_{n+1} < r_n$. because the natural numbers $r_0, r_1, r_2, \ldots$ form a strictly decreasing sequence, there is some n such that $r_{n+1} = 0$.

We claim that $r_n = g.c.d(a, b)$. Before we prove this, let's look at an example. To find $g.c.d.(56, 21)$, we apply the Euclidean algorithm to obtain

$$\begin{aligned} 56 &= 21 \cdot 2 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 + 0 \end{aligned}$$

and thus, according to the Euclidean algorithm, $g.c.d(56, 35) = 7$.

To see that the Euclidean algorithm does find the g.c.d., note that if $a = r_0, b = r_1, r_2, \ldots, r_n, r_{n+1} = 0$ is the sequence provided by the algorithm, then

$$r_{n-1} = r_n \cdot q_n + 0$$

and so r_n divides r_{n-1}. Next,

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$

and so r_n divides r_{n-2}. Moving back in this way, we see that r_n divides each r_m for $m \leq n$. In particular, r_n divides a and b, so that r_n is a common divisor of a, b. If d is another common divisor of a, b, then we see that

$$a = b \cdot q_2 + r_2$$

implies that d divides r_2. Then

$$b = r_2 \cdot q_3 + r_3$$

implies that d divides r_3. Moving forward in this way, we conclude that d divides every r_m. In particular, d divides r_n.

Hence r_n has the following properties:

(i) r_n is a common divisor of a, b, and

(ii) Every common divisor d of a, b divides r_n.

It follows that $r_n = g.c.d(a, b)$, as claimed.

Now we are able to prove that r_n is a linear combination of a, b (with integer coefficients) as claimed: Working from the bottom up, we have that

$$r_n = r_{n-2} - r_{n-1} \cdot q_n$$

so that r_n is a linear combination of r_{n-1} and r_{n-2}. Then

$$r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$$

implies that

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n = r_{n-2} \cdot (1 + q_{n-1} \cdot q_n) - r_{n-3} \cdot q_n$$

so that r_n is a linear combination of r_{n-2} and r_{n-3}. Moving back, we finally see that r_n is a linear combination of a, b.

□

Exercises 1.1.3 1. Let $F = \mathbb{R}^2$ be the set of ordered pairs of reals. Define operations $+_F$ and $\cdot_F$ on F by

$$\begin{aligned}(x_1, y_1) +_F (x_2, y_2) &= (x_1 + x_2, y_1 + y_2) \\ (x_1, y_1) \cdot_F (x_2, y_2) &= (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)\end{aligned}$$

(a) Show that $+_F$ and $\cdot_F$ are commutative and associative.

(b) Show that $\cdot_F$ distributes over $+_F$.

(c) Show that $0_F = (0, 0)$ acts as a zero element (additive identity), and that $1_F = (1, 0)$ acts as a unit element (multiplicative identity).

(d) Consider the unary operations $-_F$, ${}^{-1_F}$ defined by

$$\begin{aligned}-_F(x, y) &= (-x, -y) \\ (x, y)^{-1_F} &= (x/(x^2 + y^2), -y/(x^2 + y^2))\end{aligned}$$

Show that these define, respectively, an additive inverse operation on F, and a multiplicative inverse operation on $F - \{(0, 0)\}$.

(e) You have now shown that $\langle F, +_F, \cdot_F, -_F, {}^{-1_F}, 0_F, 1_F\rangle$ is a field. Now convince yourself that it is essentially the same as the field $\mathbb{C}$ of complex numbers if we regard the ordered pair (x, y) in the real plane as the number $x + iy$ in the Argand diagram.

In essence, this is a *construction* of the field of complex numbers from the field of real numbers: Once we've constructed the reals, then we can *define* the field of complex numbers to be the set $\mathbb{R}^2$ together with the above operations.

2. Let F be the set of 2×2–matrices, together with matrix addition and multiplication. Note that these operations satisfy the associative and distributive laws, and that addition is commutative, but that multiplication is not commutative. Can we define

   (i) a zero element?

   (ii) a unit element?

   (iii) an additive inverse?

   (iv) a multiplicative inverse?

3. Let $F_4 = \{0, 1, a, b\}$. Construct tables for operations $+$ and $\cdot$ on F_4 to make it into a field (with zero 0 and unit 1).

4. Let $\mathbb{Q}[\sqrt{2}]$ be the set of all real numbers of the form

$$a + b\sqrt{2} \qquad a, b \in \mathbb{Q}$$

and let the operations $+, \cdot, -, ^{-1}, 0, 1$ have their usual meaning. Show that F is a field which lies strictly between the field of rationals and the field of reals.

□

We will now prove some results about arithmetic inside a field. Most of these *look* obvious, but that's only because they will are already so familiar. We will use only the field axioms to prove these results, and, as a consequence, these results will be true in *any* field — not just the familiar ones, such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, but also unfamiliar ones, such as $\mathbb{Z}_p$ (p a prime).

Proposition 1.1.4 *The axioms* C$^+$, A$^+$, Id$^+$, Inv$^+$ *imply the following statements:*

(a) If $x + y = x + z$, then $y = z$; (cancellation)

(b) If $x + y = x$, then $y = 0$; (uniqueness of additive identity)

(c) If $x + y = 0$, then $y = -x$; (uniqueness of additive inverse)

(d) $-(-x) = x$;

Proof: (a) Suppose that $x + y = x + z$. Then

$$\begin{aligned} y &= 0 + y && \text{Id}^+ \\ &= (-x + x) + y && \text{Inv}^+ \\ &= -x + (x + y) && \text{A}^+ \\ &= -x + (x + z) && \text{assumption} \\ &= (-x + x) + z && \text{A}^+ \\ &= 0 + z && \text{Inv}^+ \\ &= z && \text{Id}^+ \end{aligned}$$

(b) If $x + y = x$, then $x + y = x + 0$, so the result follows from (a).
(c) If $x + y = 0$, then

$$\begin{aligned} y &= 0 + y \\ &= (-x + x) + y \\ &= -x + (x + y) \\ &= -x + 0 \\ &= -x \end{aligned}$$

(d) $-x + x = 0$, so by (c), we must have $x = -(-x)$.

⊣

Proposition 1.1.5 *The axioms* C$^{\cdot}$, A$^{\cdot}$, Id$^{\cdot}$, Inv$^{\cdot}$ *imply the following statements:*

(a) If $xy = xz$, and $x \neq 0$, then $y = z$; (cancellation)

(b) If $xy = x$, and $x \neq 0$, then $y = 1$; (uniqueness of multiplicative identity)

(c) If $xy = 1$*, and* $x \neq 0$*, then* $y = x^{-1}$*;* (uniqueness of multiplicative inverse)

(d) If $x \neq 0$*, then* $(x^{-1})^{-1} = x$*;*

⊣

Exercise 1.1.6 Prove the preceding proposition.

□

Note that the distributive law (D) was not used in proving the above statements. If we invoke the distributive law, we can prove more:

Proposition 1.1.7 *The field axioms imply the following statements:*

(a) $0 \cdot x = 0$*;*

(b) If $x \neq 0$*,* $y \neq 0$*, then* $xy \neq 0$*;*

(c) $(-x)y = -xy = x(-y)$*;*

(d) $(-x)(-y) = xy$*;*

⊣

Exercise 1.1.8 Prove the preceding proposition. Here are some hints:
(a) Justify the following string of equalities: $x + 0 \cdot x = 1 \cdot x + 0 \cdot x = (1 + 0) \cdot x = 1 \cdot x = x$. Now use Proposition 1.1.4(b).
If x, y are non–zero, then $(x^{-1}y^{-1})(xy) = 1$. Hence, by (a), $xy \neq 0$. (Why can't we have $0 = 1$?)
(c) $(-x)y + xy = (-x + x)y = 0$, so $(-x)y = -(xy)$, by Proposition 1.1.4(c).
(d) Apply (c) twice, and invoke Proposition 1.1.4(d).

□

Any field F contains a distinguished element 1. If $n \in \mathbb{N}$, we may define a member, also called n, of F by

$$n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

This allows us to write, for example, $3a$ instead of $a + a + a$.

But beware! This notation may lead to some confusion, as you have to take care to distinguish between the natural number n and the field element n. In what follows, we shall take care to say whether we are operating in F or in $\mathbb{N}$.

Arithmetic using these F–natural numbers is very similar to arithmetic with ordinary natural numbers. For example, $2+3$ in F is just:

$$(1+1)+(1+1+1) = 1+1+1+1+1 = 5 \in F$$

by associativity of addition. Similarly, $2 \cdot 3$ in F is just:

$$(1+1)\cdot(1+1+1) = 1\cdot(1+1+1)+1\cdot(1+1+1) = (1+1+1)+(1+1+1) = 1+1+1+1+1+1 = 6 \in F$$

Here, we used the distributive law, the fact that 1 is the multiplicative identity, and the associativity of addition.

Consider now the following derivation:

$$\begin{aligned} & 2x = 2y \\ \Rightarrow\ & 2^{-1}(2x) = 2^{-1}(2y) \\ \Rightarrow\ & (2^{-1}\cdot 2)x = (2^{-1}2)y \\ \Rightarrow\ & x = y \end{aligned} \tag{$*$}$$

It thus seems that we have proved that the following holds in any field:

$$2x = 2y \to x = y$$

Now consider the field $\mathbb{Z}_2$ of Example 1.1.2(5). Here we have $2\cdot1 = (1+1)\cdot1 = 0\cdot1 = 0 = 2\cdot0$, yet $1 \neq 0$. Thus $2x = 2y$ does not imply $x = y$.

Further, consider the field $F_4 = \{0, 1, a, b\}$ of Exercises 1.1.3(3). If you did this exercise correctly, you will note that $2a = 0$, yet $a \neq 0$. *What went wrong*?!

The problem arises when we multiply both sides of the equation $2x = 2y$ by $2^{-1} = (1+1)^{-1}$. For 2^{-1} exists only if $2 \neq 0$. But our field axioms cannot guarantee this. Indeed, both fields $\mathbb{Z}_2$ and F_4 satisfy the identity $x + x = 0$ (i.e., this equation is true for any x belonging to the field). So what we really proved in $(*)$ above is: "If $1 + 1 \neq 0$, then $2x = 2y$ implies $x = y$."

It is clear, therefore, that the field axioms are not strong enough to prove the following simple fact about the real numbers: $2 \neq 0$.

We now add some new axioms which will, amongst others, ensure that $n = 0$ in F if and only if $n = 0$ in $\mathbb{Z}$.

1.2 Ordered Fields

Recall that a *totally ordered set* (or a *chain*) is a tuple $\langle S, L\rangle$ such that S is a set, and L is a subset of $S \times S$, satisfying the following axioms

(PO-R)	$\forall s[(s,s) \in L]$	(Reflexivity)
(PO-A)	$\forall s \forall t[(s,t) \in L \wedge (t,s) \in L \to s = t]$	(Antisymmetry)
(PO-T)	$\forall s \forall t \forall u[(s,t) \in L \wedge (t,u) \in L \to (s,u) \in L]$	(Transitivity)
(TO)	$\forall s \forall t[(s,t) \in L \vee (t,s) \in L]$	(Total ordering)

The intuition behind this is that $s \leq t$ if and only if $(s,t) \in L$. Viewed like that, we see that axioms (PO-R), (PO-A), (PO-T) are just the axioms for a *partial ordering*:

$$\begin{array}{ll} \text{(PO-R)} & s \leq s \\ \text{(PO-A)} & s \leq t \text{ and } t \leq s \text{ imply } s = t \\ \text{(PO-T)} & s \leq t \text{ and } t \leq u \text{ implies } s \leq u \end{array}$$

Axiom (TO) guarantees that the partial ordering is a total ordering:

$$\text{(TO)} \quad \text{Either } s \leq t \text{ or } t \leq s \text{ (or both)}$$

We write "$s < t$" instead of "$s \leq t$ and $s \neq t$". Similarly "$s \geq t$" is just another way of saying "$t \leq s$". An analogous statement holds for "$s > t$".

An ordered field is a field which is also a totally ordered set, subject to two additional conditions:

Definition 1.2.1 An *ordered field* is a tuple $\langle F, +, \cdot, -, ^{-1}, 0, 1, \leq \rangle$ satisfying the field axioms (C^+), (A^+), (Id^+), (Inv^+), ($C^\cdot$), ($A^\cdot$), ($Id^\cdot$), ($Inv^\cdot$), (D), and the order axioms (PO-R), (PO-A), (PO-T), (TO), such that, in addition

$$\begin{array}{ll} (\text{OF}^+) & \forall x \forall y \forall z [x \leq y \rightarrow x + z \leq y + z] \\ (\text{OF}^\cdot) & \forall x \forall y [x > 0 \wedge y > 0 \rightarrow xy > 0] \end{array}$$

□

The fields $\mathbb{Q}, \mathbb{Q}[\sqrt{2}], \mathbb{R}$ are ordered fields (with the usual ordering).

- No finite field is an ordered field.
- The field $\mathbb{C}$ cannot be made into an ordered field.

You will be required to prove these facts soon.

If $x > 0$, we say that x is *positive*; if $x < 0$, we say that x is *negative*. We say that x, y have *opposite signs* if one of x, y is positive and the other negative.

Proposition 1.2.2 *Let $\langle F, +, \cdot, -, ^{-1}, 0, 1, \leq \rangle$ be an ordered field.*

(a) $x < y$ if and only if $y - x > 0$;

(b) If $x \neq 0$, then x and $-x$ have opposite signs.

(c) If $x > 0$ and $y < z$, then $xy < xz$; If $x < 0$ and $y < z$, then $xy > xz$;

(d) If $x \neq 0$, then $x^2 > 0$;

(e) $1 > 0$;

(f) If $x \neq 0, y \neq 0$, then x, y have opposite signs if and only if $xy < 0$.

(g) $x > 0$ implies $x^{-1} > 0$; $x < 0$ implies $x^{-1} < 0$;

(h) If $0 < x < y$*, then* $0 < y^{-1} < x^{-1}$*;*

Proof: (a) $x < y$ implies $x + (-x) < y + (-x)$ by (OF$^+$), so $0 < y - x$. Similarly $0 < y - x$ implies $x + 0 < x + (y - x)$.
(b) If $x > 0$, then $x + (-x) > 0 + (-x)$, so $-x < 0$. A similar proof works for the other case.
(c) $x > 0$ and $z - y > 0$ implies $x(z - y) > 0$ by (OF$^\cdot$). A similar proof works for the other case.
(d) This is clear if $x > 0$. Else, $-x > 0$ (why?), and so $(-x) \cdot (-x) > 0$, by (OF$^\cdot$). But $(-x) \cdot (-x) = x^2$, by Proposition 1.1.7(d).
(e) By (d);
(f) If $x > 0, y < 0$, then $xy < 0$, by (c). Conversely, suppose that $xy < 0$. Then $x \neq 0$ and $y \neq 0$. Now if x, y are both positive, then xy is positive, by (OF$^\cdot$); if x, y are both negative, then $-x, -y$ are both positive (by (b)), so that $(-x)(-y) = xy$ is positive, by (OF$^\cdot$).
(g) Since $xx^{-1} = 1 > 0$, x and x^{-1} cannot have opposite signs.
(h) Suppose that $0 < x < y$. Then $x^{-1}, y^{-1} > 0$, so $0 < x \cdot x^{-1} < yx^{-1}$, by (OF$^\cdot$). Hence $1 < yx^{-1}$, and so $y^{-1} < y^{-1}(yx^{-1})$.

⊣

Exercise 1.2.3 (a) Suppose that $\langle F, +, \cdot, -, ^{-1}, 0, 1\rangle$ is a field, and that $P \subseteq F$ has the following properties:

(i) For each $x \in F$, exactly *one* of the following is true:

$$x = 0 \quad \text{or} \quad x \in P \quad \text{or} \quad -x \in P$$

(ii) $x, y \in P$ implies $xy \in P$

(iii) $x, y \in P$ implies $x + y \in P$;

Define a binary relation $\leq$ on F by

$$x \leq y \Leftrightarrow x = y \text{ or } y - x \in P$$

Show that $\leq$ makes F into an ordered field. Also show that P is precisely the set of positive elements.

(b) Prove that there are no finite ordered fields.
[Hint: For $m \in \mathbb{N}$, denote the element $1 + \cdots + 1$ (m terms) of F by m as well. Show that if F is an ordered field, then $0 < m$, for all m. Conclude that F has infinitely many elements.]

(c) Show that $\mathbb{C}$ cannot be made into an ordered field — it is impossible to define a total ordering $\leq$ on $\mathbb{C}$ so that (OF$^+$) and (OF$^\cdot$) are satisfied.

□

A field is said to have *characteristic* p if $p = 0$ in F, and if $q \neq 0$ in F for any $q < p$ in $\mathbb{N}$. (where p denotes the field element $1 + \cdots + 1$ with p terms). It is said to have *characteristic zero* if $p \neq 0$ for any $p \in \mathbb{N}$. The above exercise shows that an ordered field has characteristic zero.

1.3 The Continuum

Let's take stock for a moment: We are trying to find a complete set of axioms for the real numbers, i.e we are attempting find a set of rules which completely capture our intuition about the behaviour of the reals. Our intuition involves both algebraic and order–theoretic properties, and, so far, we've written down 15 axioms, the axioms of an ordered field: (C^+), (A^+), (Id^+), (Inv^+), ($\mathrm{C}^\cdot$), ($\mathrm{A}^\cdot$), ($\mathrm{Id}^\cdot$), ($\mathrm{Inv}^\cdot$), (D),(PO-R), (PO-A), (PO-T), (TO), (OF^+), and ($\mathrm{OF}^\cdot$). Using these axioms, *and nothing else*, we've managed to prove a number of interesting properties: $(-x)(-y) = xy$; squares (x^2) are non–negative, etc. These properties hold in any ordered field.

So do the ordered field axioms completely capture our intuition about the behaviour of the reals? No. We have an additional intuition about non–negative real numbers as being *lengths* of straight line segments. We can measure the length of a line segment using a ruler, and the length will be a real number. In this way, we come to regard the set of real numbers as points on a straight line which extends indefinitely in both directions.

Example 1.3.1 (1) Consider an isosceles right–angled triangle, with right–angle sides both 1 unit in length. Our intuition dictates that the hypotenuse have a length. By Pythagoras' Theorem, the length of the hypotenuse is a number x satisfying $x^2 = 2, x \geq 0$.

(2) Consider the graph of the parabola $f(x) = x^2 - 2$ in the Cartesian plane. We see that $f(0) < 0$, and that $f(2) > 0$. Our intuition dictates that the graph cut the x–axis *somewhere* between 0 and 2. It is cut at an x satisfying $x^2 = 2, x \geq 0$.

□

Of course, you say, in both examples we are seeking the number $x = \sqrt{2}$. However, we want to take an *axiomatic approach* to the real numbers.

We shall now prove a remarkable fact:

> *It is impossible to prove, from the ordered field axioms alone, the existence of a field element x with the property that $x^2 = 2$ (where $2 = 1 + 1$)*

Note that we are going to prove that a statement is impossible to prove, a remarkable achievement. How shall we accomplish this? Do we need to examine every possible proof about ordered fields?

The method is much simpler, and is at the root of *model theory*, a branch of mathematical logic: Suppose that $\mathcal{A}$ is a set of axioms, and that φ is some statement. A *model* of $\mathcal{A}$ is simply a structure in which all the axioms in $\mathcal{A}$ are true. In order to prove that φ cannot be proved from the axioms in $\mathcal{A}$ it suffices to show that there is a model of $\mathcal{A}$ in which φ is false. For if M is a model in which $\mathcal{A}$ is true, then anything which can be proved from $\mathcal{A}$ must also be true in M. If φ is false in M, therefore, we can deduce that φ cannot be proved from $\mathcal{A}$ alone.

We proceed as follows: Let F be an ordered field. If $n \in \mathbb{N}$, we may regard n as a member of the field F in the usual way:

$$n = \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}}$$

Let's give such elements $n, -n$ in F the name *F–integers*. We shall say that an F–integer n is *F–even* if there is another F–integer m such that $n = 2m$. If there is no such m, we shall call n *F–odd*.

Now if $m, n \in \mathbb{N}$, then we may denote by $\frac{m}{n}$ the field element

$$\frac{m}{n} = m \cdot n^{-1} = \underbrace{(1 + 1 + \cdots + 1)}_{m \text{ times}}\underbrace{(1 + 1 + \cdots + 1)^{-1}}_{n \text{ times}}$$

Similarly $-\frac{m}{n}$ is just the field element $(-m) \cdot n^{-1}$. We call the elements of F which can be written in the form $\frac{m}{n}$ (for some $m, n \in \mathbb{Z}$) the *F–rationals*. The remainder are called *F–irrational*.

The arithmetic of F–integers is similar to that of ordinary integers: By associativity and distributivity, the sum (difference) of two F–integers is an F–integer, the product of two F–integers is an F–integer, etc. The same is true for F–rational numbers, as you ought to check. We thus conclude that:

Proposition 1.3.2 *The field $\mathbb{Q}$ of rational numbers is the smallest ordered field, in the following sense: Any ordered field contains (a copy of) $\mathbb{Q}$ as a subfield.*

$\dashv$

Note that the $\mathbb{R}$–integers are just the ordinary integers, and the $\mathbb{R}$–rationals are just the ordinary rationals.

Lemma 1.3.3 *Let F be an ordered field.*

(a) 2^{-1} is not an F–integer.

(b) An F–integer n is F–odd if and only if there is an F–integer m such that $n = 2m + 1$.

(c) If n is an F–integer, then n^2 is F–even if and only if F–even.

Proof: (a) We have $0 < 1 < 2 < 3 < \dots$ in any ordered field , and hence $0 < 2^{-1} < 1 < 2 < 3 < \dots$, by Proposition 1.2.2(h). Thus 2^{-1} is not equal to any F–integer n.
(b) It is clear that if n is F–odd, then $n = 2m + 1$ for some F–integer m — a positive F–integer is either the sum of even–many 1's or odd–many 1's. Conversely, if $2m + 1$ is F–even, then $2m + 1 = 2k$ for some F–integer k, and hence $2^{-1} = k - m$ is an F–integer. This contradicts (a).
(c) It's clear that if n is F–even, then so is n^2. Conversely, if n^2 is F–even, say $n^2 = 2m$, and if n is F–odd, i.e. $n = 2k + 1$, then $2^{-1} = m - 2k^2 - 2k$, and this contradicts (a). Hence n must be F–even if n^2 is.

⊣

Proposition 1.3.4 *Let F be an ordered field. If $x \in F$ is such that $x^2 = 2, x \geq 0$, then x is F–irrational.*

Proof: First note that if x, y and $x^2 = y^2$, then $x = \pm y$: For $0 = x^2 - y^2 = (x-y)(x+y)$. Hence either $x - y = 0$, or $x + y = 0$ — if neither were zero, then $0 = 1$ follows upon multiplication by $(x-y)^{-1}(x+y)^{-1}$.

Hence if $x, y \geq 0$ in F, with $x^2 = y^2$, then $x = y$.

Now suppose that $x^2 = 2, x \geq 0$ in F. Suppose further that x is F–rational, i.e. $x = \frac{m}{n}$ in F. Since x is positive, and since $2 > 1$, we may assume that $m > n > 0$. Now let m_0 be the *least* integer (in $\mathbb{N}$) such that $x = \frac{m_0}{n_0} = 2$ for some $n_0 < m_0$ (in F). Then $2 = m_0^2 n_0^{-2}$, so m_0^2 is F–even. Hence m_0 is F–even also, say $m_0 = 2k$ for some F–integer $k > 0$. But then $(\frac{n_0}{k})^2 = 2$, so that $\frac{n_0}{k} = x$. This contradicts the fact that m_0 is the least numerator of a fractional representation of x. Hence x cannot be F–rational.

⊣

We can now prove that it is *impossible to prove* the existence of a field element x satisfying $x^2 = 2$ from the ordered field axioms alone.

For the field of rational numbers $\mathbb{Q}$ is an ordered field, i.e. it satisfies all the ordered field axioms: it is a *model* of the ordered field axioms. Now *every* member of $\mathbb{Q}$ is $\mathbb{Q}$–rational, i.e. there are no $\mathbb{Q}$–irrationals in $\mathbb{Q}$. In particular, there cannot be an element $x \in \mathbb{Q}$ satisfying $x^2 = 2$. Thus we have found a model of the ordered field axioms in which there is no element x with $x^2 = 2$. It follows that the existence of such an x cannot be proved from the ordered field axioms alone. [If the ordered field axioms implied the existence of such an x, then such an x would have to exist in $\mathbb{Q}$, because $\mathbb{Q}$ satisfies the axioms.]

Exercise 1.3.5 This exercise serves to illuminate the *method* behind the above proof.

(a) Consider the order axioms (PO–R), (PO–A), (PO–T) and (TO). Show that (TO) cannot be proved from (PO–R), (PO–A) and (PO–T) alone.

(b) Consider the axioms for an abelian group: (C^+), (A^+), (Id^+) and (Inv^+). Show that (C^+) cannot be proved from the other three axioms.

□

Exercise 1.3.6 (a) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an n^{th}–degree polynomial with integer coefficients $a_0, \ldots, a_n$, where $a_n \neq 0$. Suppose that $\frac{p}{q} \in \mathbb{Q}$ is a root of $f(x)$, where $p, q \in \mathbb{Z}$ are relatively prime[1]. Show that p is a factor of a_0 and that q is a factor of a_n.

(b) Consider the special case where $a_n = 1$. Show that all roots of $f(x)$ must be integers.

[1] Two integers are relatively prime if their greatest common divisor is 1. In this case, this means that the fraction $\frac{p}{q}$ cannot be simplified any further.

(c) Conclude that the following numbers, if they exist, are irrational: $\sqrt{2}, \sqrt[3]{12}$, $(5-\sqrt{2})^{\frac{1}{3}}$.

□

Here's a brief summary of the salient points of this section:

- We have provided a set of axioms that capture our intuition about the arithmetic and order–theoretic properties of real numbers.
- We also have a geometric intuition about non–negative real numbers as being the lengths of line segments. Considering the hypotenuse of an isosceles right–angled triangle, this leads us to believe that there should exist a non–negative real number x with the property that $x^2 = 2$.
- However, we proved that x, if it exists, cannot be a rational number.
- Because the field $\mathbb{Q}$ of rational numbers satisfies all the axioms proposed, it follows that the existence of x cannot be proved from those axioms alone.
- Thus the set of axioms proposed so far is inadequate: It does not completely capture our intuition about the real number system, because there are "truths" that we cannot prove.
- It is therefore necessary to find at least one more axiom.

From where will we get such an axiom? The intuition that leads us to believe in the existence of the number $\sqrt{2}$ has its origins in the geometric concept of length. Thus far, we have not considered any geometric axioms at all. We would like to keep things as simple as possible, and avoid an axiomatization that depends too much on geometric concepts. Is it really necessary to incorporate, say, Euclid's axioms of plane geometry, to formalize the notion of the length of a line segment and the notion of a right–angled triangle, all in order to prove Pythagoras' Theorem, so that we can finally obtain the existence of $\sqrt{2}$?

Fortunately not. Perform the following thought experiment, an exercise in visualization: Let N be a natural number, and consider an arbitrary, but non–empty, set $\mathcal{L} = \{L_i : i \in I\}$ of line segments, each of length $\leq N$. Align them, and stack them together on top of each other, so that you see just a *single* line segment L. Clearly the following hold:

(i) The length of L is greater than or equal to the length of each $L_i \in \mathcal{L}$;

(ii) The length of L is finite, being less than or equal to N.

(iii) Any line segment which is strictly shorter than L is also shorter than some $L_i \in \mathcal{L}$.

(iv) Thus L is the *shortest* line segment which has length greater than or equal to the length of each $L_i \in \mathcal{L}$.

Rephrase and slightly generalize the above intuition as follows:

> *If $A = \{a_i : i \in I\}$ is a non–empty set of real numbers which is bounded above, then it has a* least *upper bound, i.e. there exists a number a such that $a \geq a_i$ for all $a_i \in A$, and if $a' < a$, then there is $a_i \in A$ such that also $a' < a_i$.*

It turns out that with this final axiom we have completely characterized the set of real numbers.

1.4 The Completeness Axiom

We begin with some definitions:

Definition 1.4.1 Let $(P, \leq)$ be a total ordering[2] and let $A \subseteq P$.

(a) We say that an element $u \in P$ is an *upper bound* for A if and only if

$$\forall a \in A (a \leq u)$$

(b) Similarly, we say that $l \in P$ is an *lower bound* for A if and only if

$$\forall a \in A (l \leq a)$$

(c) We say that A is *bounded* if and only if it has both an upper bound and a lower bound.

(d) We say that u_0 is the *supremum*, or *least upper bound* of A if and only if the following hold:

(i) u_0 is an upper bound of A;

(ii) If u is any upper bound of A, then $u_0 \leq u$.

We write

$$u_0 = \sup A \quad \text{or} \quad u_0 = \text{l.u.b.}(A)$$

(e) We say that l_0 is the *infimum*, or *greatest lower bound* of A if and only if the following hold:

(i) l_0 is a lower bound of A;

(ii) If l is any lower bound of A, then $l \leq l_0$.

We write

$$l_0 = \inf A \quad \text{or} \quad l_0 = \text{g.l.b.}(A)$$

[2] i.e. $(P, \leq)$ satisfies (PO-R), (PO-A), (PO-T) and (TO).

(f) We say that u_0 is the *maximum* of A, and write $u_0 = \max A$, if and only if

$$u_0 \in A \quad \text{and} \quad u_0 = \sup A$$

(g) Similarly, we say that l_0 is the *minimum* of A, denoted $l_0 = \min A$, if and only if

$$l_0 \in A \quad \text{and} \quad l_0 = \inf A$$

□

Definition 1.4.2 Let $(P, \leq)$ be a total ordering.

(a) Let $a, b \in P$ with $a \leq b$. We define the following sets:

$$\begin{aligned}
[a, b] &= \{x \in P : a \leq x \leq b\} \\
(a, b) &= \{x \in P : a < x < b\} \\
(a, b] &= \{x \in P : a < x \leq b\} \\
[a, b) &= \{x \in P : a \leq x < b\}
\end{aligned}$$

(b) A set $A \subseteq P$ is called an *interval* if and only if whenever $a, b \in A$ with $a \leq b$, then $[a, b] \subseteq A$.

(c) A set $A \subseteq P$ is called *order dense* in P if and only if given any $p_1 < p_2$ in P, we can find $a \in A$ such that $p_1 < a < p_2$: Between any two distinct elements of P we can find a member of A.

□

Examples 1.4.3 (1) If $a < b$ in a total ordering $(P, \leq)$, then $[a, b], (a, b), (a, b], [a, b)$ are intervals.

(2) A subset A of a total ordering $(P, \leq)$ is bounded if and only if there exist $a, b \in P$ such that $A \subseteq [a, b]$.

(a) $\mathbb{Q}$, regarded as a subset of $\mathbb{R}$, is order dense in $\mathbb{R}$: Between any two distinct real numbers lies a rational number.

(b) $\mathbb{Z}$ is not order dense in $\mathbb{R}$, nor is it order dense in $\mathbb{Q}$: There is no integer between, say, 0.1 and 0.2.

(c) $\mathbb{R}$ is *order dense in itself*: Between any two real numbers there lies another real number. $\mathbb{Q}$ is also order dense in itself, but $\mathbb{Z}$ is not.

(3) In $(\mathbb{R}, \leq)$, we have:

(a) $1 = \max[0, 1] = \sup[0, 1]; \quad 0 = \min[0, 1] = \inf[0, 1]$

(b) $1 = \sup[0,1)$, but $\max[0,1)$ does not exist.

(c) If $A = \{x \in \mathbb{R} : x^2 \leq 2\}$, then $\sup A = \sqrt{2}$.

(d) If $A = \emptyset$, then A has no supremum and no infimum. First note that any $u \in \mathbb{R}$ is an upper bound for A; if not, there would be $a \in A$ such that $u < a$. Similarly, every real number is also a lower bound for A. We therefore write

$$\sup \emptyset = -\infty \qquad \inf \emptyset = +\infty$$

(4) In $(\mathbb{Q}, \leq)$, the set $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$ has no supremum: If $u \in \mathbb{Q}$ is an upper bound for A, then u is a rational number which is greater than $\sqrt{2}$. We can then choose a rational number u' such that $\sqrt{2} < u' < u$. Thus: given any upper bound u for A, we can find another upper bound $u' < u$. Hence A has no least upper bound (in $\mathbb{Q}$).

□

Exercise 1.4.4
Define a relation $\prec$ on the set $\mathbb{R}^2$ as follows:

$$(a,b) \prec (c,d) \quad \text{iff} \quad a < c \ \vee \ (a = c \ \wedge \ b < d)$$

Define a relation $\preceq$ on $\mathbb{R}^2$ by

$$(a,b) \preceq (c,d) \quad \text{iff} \quad (a,b) = (c,d) \ \vee \ (a,b) \prec (c,d)$$

(a) Arrange in increasing order: $(3,1), (2,2), (1,2), (2,3), (1,1), (2,1), (1,3), (3,2)$.

(b) Prove that $\preceq$ is a total ordering on $\mathbb{R}^2$.

(c) Let $A = \{(a,b) : a^2 + b^2 \leq 1\}$. Show that A is a bounded set (w.r.t. $\preceq$).

(d) Calculate $\sup A$ and $\inf A$.

(e) Give an example of a bounded set which has no supremum and no infimum.

□

Definition 1.4.5 (Completeness Axiom)
Let F be an ordered field. We say that F is *complete* if and only whenever a non–empty $A \subseteq F$ has an upper bound, then it has a least upper bound, i.e. $\sup A$ exists (and belongs to F).

□

Exercise 1.4.6 Show that if an ordered field F is complete, then any non–empty subset of F which is bounded below has a greatest lower bound. Thus: In a complete ordered field any non-empty bounded set has both a supremum and an infimum.

□

Note that $\mathbb{Q}$ is not complete: The set $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$ has an upper bound in $\mathbb{Q}$, but no supremum. However, our intuition about real numbers as lengths of line segments led us to conclude, via an experiment in visualization, that the set of real numbers is complete. Thus the Completeness Axiom allows us to distinguish between $\mathbb{R}$ and $\mathbb{Q}$.

We state the following result without proof:

Theorem 1.4.7 *There exists a complete ordered field* $(\mathbb{R}, +, \cdot -, ^{-1}, 0, 1, \leq)$.

⊣

More can be said: Any two complete ordered fields are *isomorphic.*, i.e. they have essentially the same structure, and, mathematically speaking, are essentially the same object. Thus we can define the set of reals, up to isomorphism, as the *unique* complete ordered field.

Theorem 1.4.8 *(a) Any complete ordered field F satisfies the* archimedean property*: For any $x > 0$ and any y in F there exists $n \in \mathbb{N}$ such that $nx > y$.*

(b) The field $\mathbb{Q}$ of rationals is dense in F: whenever $x < y$ in F there is $q \in \mathbb{Q}$ such that $x < q < y$.

Proof: (a) Let $A = \{nx : n \in \mathbb{N}\}$. Then $A \neq \emptyset$. If there is no $n \in \mathbb{N}$ such that $nx > y$, then y is an upper bound for A. Thus the completeness axiom guarantees that $a_0 = \sup A$ exists (in F). Now $a_0 - x < a_0$, as $x > 0$, so $a_0 - x$ is not an upper bound of A. Hence there exists $m \in \mathbb{N}$ such that $a_0 - x < mx$. Then $a_0 < (m+1)x$. But $(m+1)x \in A$, and a_0 is an upper bound for A — contradiction.
(b) Recall that any ordered field contains (a copy of) the field $\mathbb{Q}$, by Proposition 1.3.2. We shall show that there exist $m \in \mathbb{Z}, n \in \mathbb{N}$ such that (regarded as a member of F), $x < \frac{m}{n} < y$.

Now if $x < y$, then $y - x > 0$, and so the archimedean property allows us to find a non–negative integer n such that $n(y - x) > 1$. Similarly, there are non–negative integers m_1, m_2 such that $m_1 > nx, m_2 > -nx$ — just consider the two cases $x \geq 0, x < 0$. It follows that $-m_2 < nx < m_1$, and so there is a smallest integer m such that $nx < m$. It follows that $m - 1 \leq nx$, and so

$$nx < m \leq 1 + nx < ny$$

which yields $x < \frac{m}{n} < y$. Division by n is possible, because $n > 0$.

⊣

How did we get to the completeness axiom? Our intuition about real numbers as lengths led us to believe in the existence of a number x such that $x^2 = 2$. We subsequently found that such an x could not be rational, and we concluded that we could not deduce the existence of x from the ordered field axioms alone. We then performed a experiment in visualization, stripped it of its geometric content, and wrote down the completeness axiom.

So can we prove the existence of $\sqrt{2}$ from just the ordered field axioms and the completeness axiom? Indeed, we can:

Proposition 1.4.9 *Let F be a complete ordered field, let $n \in \mathbb{N}$, and let $x > 0$ in F. Then there exists a unique $y \in F$ such that $y > 0$ and $y^n = x$. We denote this y by $y = \sqrt[n]{x}$.*

Proof: It is easy to see that there cannot be more than one such y. For if $0 < y_1 < y_2$, then the ordered field axioms guarantee that $0 < y_1^n < y_2^n$.

Let $A = \{t \in F : t > 0, t^n \le x\}$. Note that A is non–empty, because if $t = \frac{x}{x+1}$, then $t < x$ and $0 < t < 1$, so that $0 < t^n < t < x$. Hence $\frac{x}{x+1} \in A$.

Next note that A has an upper bound: If $u = 1 + x$, then $u^n > u > x$, so that $u \notin A$.

Since A is non–empty and bounded above, there exists an element $y = \sup A$ in F. We shall show that $y^n = x$.

First note that if $0 < a < b$ in F, then the identity $b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \cdots + ba^{n-2} + a^{n-1})$ immediately yields the following inequality:

$$b^n - a^n \le (b-a)nb^{n-a}$$

We apply, and this inequality twice — once to show that we cannot have $y^n > x$, and once to show that we cannot have $y^n < x$.

For suppose $y^n > x$. Define

$$k = \frac{y^n - x}{ny^{n-1}}$$

Clearly $k > 0$. Also $k < \frac{y}{n} \le y$. Now if $t > y - k$, then

$$y^n - t^n \le y^n - (y-k)^n < kny^{n-1} = y^n - x$$

so that $t^n > x$. Thus t is an upper bound for A. Yet $t = y - k < y$, a contradiction.

Next suppose that $y^n < x$. Choose h such that $0 < h < 1$ and

$$h < \frac{x - y^n}{n(y+1)^{n-1}}$$

This is possible, because $\mathbb{Q}$ is a dense subfield of F. Now put $t = y + h$. Then

$$t^n - y^n < hnt^{n-1} < hn(y+1)^{n-1} < x - y^n$$

so that $t^n < x$. Hence t is not an upper bound for A, even though $t > y$, another contradiction.

⊣

Exercise 1.4.10 Let F be an ordered field $a < b$ in F. We have seen that sets of the form $[a,b], (a,b), (a,b], [a,b)$ are bounded intervals.

(a) Show that not every bounded non–empty interval need be of this form.

(b) Show that if F is a *complete* ordered field, then every bounded non–empty interval must be of this form.

□

Exercise 1.4.11 Let F be a complete ordered field, and let $n \in \mathbb{N}$. If $x, y > 0$ in F, show that $(xy)^{\frac{1}{n}} = x^{\frac{1}{n}} y^{\frac{1}{n}}$.

□

The following exercise proves an important property.

Exercise 1.4.12 (Nested Interval Property)
A family $\mathcal{A} = \{A_i : i \in I\}$ be a family of subintervals of an ordered field is said to be *nested* if and only if it satisfies the following condition: Whenever $i, j \in I$, either $A_i \subseteq A_j$ or $A_j \subseteq A_i$.

(a) Prove that $\mathbb{R}$ has the nested interval property: Any nested family of intervals has non–empty intersection.

(b) Show that the field $\mathbb{Q}$ does not have the nested interval property.

[Hint: (a) Let A_i be an interval with endpoints a_i and b_i. Show that for all $i, j \in I$ we have $a_i < b_j$. Conclude that $\{a_i : \imath \in I\}$ has an upper bound.]

□

1.5 Construction of the Set of Reals*

UNDER CONSTRUCTION. . .

Real Analysis

P. Ouwehand

Department of Mathematics and Applied Mathematics
University of Cape Town

Contents

Chapter 2

The Geometry and Topology of $\mathbb{R}^n$

Having studied the algebraic and order–theoretic properties of the real number system in Chapter 1, we are now in a position to attack the fundamental notions of analysis, such as limits and continuity. Nevertheless, we will delay this briefly, in order to look at some of the metric and topological properties of Euclidean space $\mathbb{R}^n$. This short detour will enable us to discuss the afore–mentioned analytical notions in greater generality, while also providing additional visual intuition.

2.1 The Geometry of $\mathbb{R}^n$

I will assume that you are thoroughly familiar with the following facts and notions:

- $\mathbb{R}^n$ is the set of all ordered n–tuples with components in $\mathbb{R}$:

  $$\mathbb{R}^n = \{(r_1, \ldots, r_n) : r_i \in \mathbb{R}, 1 \leq i \leq n\}$$

  $\mathbb{R}^1$ is identified with $\mathbb{R}$, and called the *real line*; $\mathbb{R}^2$ is called the *real plane.*
  $\mathbb{R}^n$ is commonly referred to as n–dimensional *Euclidean space*, and also *Cartesian space.*
  The elements of $\mathbb{R}^n$ may also be referred to as real n–dimensional *vectors.*

- $\mathbb{R}^n$ can be endowed with operations of *addition* and *scalar multiplication*:

  $$\begin{aligned}(x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n)\\ \alpha(x_1, \ldots, x_n) &= (\alpha x_1, \ldots, \alpha x_n) \qquad \alpha \in \mathbb{R}\end{aligned}$$

  This makes $\mathbb{R}^n$ into an n–dimensional vector space (over the scalar field $\mathbb{R}$). The vector

  $$0 = (0, \ldots, 0)$$

  is an identity element for the operation of addition. We denote it simply by 0.
  Thus we use the same symbol 0 for the number 0, the vector $(0, 0)$, the vector $(0, 0, 0)$, etc. Which zero is meant will be obvious from context.

- $\mathbb{R}^n$ can be equipped with an *inner product*, a map

$$\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$

defined as follows: If $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$, then

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$$

The inner product on $\mathbb{R}^1$ is just ordinary multiplication. On $\mathbb{R}^n$, the inner product is also called the *dot product* and often denoted by $\langle x, y \rangle = x \cdot y$. It has the following properties, which you are invited to verify yourself:

(i) $\langle x, x \rangle \geq 0 \qquad$ for all $x \in \mathbb{R}$;

(ii) $\langle x, x \rangle = 0$ if and only if $x = 0$;

(iii) $\langle x, y \rangle = \langle y, x \rangle \qquad$ for all $x, y \in \mathbb{R}^n$;

(iv) $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle \qquad$ for all $x, y, z \in \mathbb{R}^n$;

(v) $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle \qquad$ for all $x, y \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$.

A vector space V equipped with a map $\langle \cdot, \cdot \rangle$ which satisfies (i)–(v) is called an *inner product space.*

- The space $\mathbb{R}^n$ can be equipped with a *norm* or length

$$|| \cdot || : \mathbb{R}^n \to \mathbb{R}^+$$

defined by

$$||x|| = \sqrt{\langle x, x \rangle} = \sqrt{x_1^2 + \cdots + x_n^2}$$

The norm in $\mathbb{R}^1$ is just the usual absolute value. The norm satisfies the following conditions:

(i) $||x|| \geq 0 \qquad$ for all $x \in \mathbb{R}^n$;

(ii) $||x|| = 0$ if and only if $x = 0$;

(iii) $||\alpha x|| = |\alpha| ||x|| \qquad$ for all $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$;

(iv) $||x + y|| \leq ||x|| + ||y|| \qquad$ for all $x, y \in \mathbb{R}^n \qquad$ (Triangle Inequality);

A vector space V equipped with a map $|| \cdot ||$ which satisfies (i)–(iv) is called a *normed vector space.* An inner product will always *induce* a norm by putting $||x|| = \langle x, x \rangle$. However, a norm need not be induced by an inner product.

- $\mathbb{R}^n$ can be equipped with a *metric*, or distance

$$d(\cdot, \cdot) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$$

defined by

$$d(x, y) = ||x - y|| = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

$d(x, y)$ is simply the distance between x and y. The metric d satisfies the following conditions:

(i) $d(x, y) \geq 0 \qquad$ for all $x, y \in \mathbb{R}^n$;

(ii) $d(x, y) = 0$ if and only if $x = y$;

(iii) $d(x, y) = d(y, x) \qquad$ for all $x, y \in \mathbb{R}^n$;

(iv) $d(x, z) \leq d(x, y) + d(y, z) \qquad$ for all $x, y, z \in \mathbb{R}^n$ (Triangle Inequality);

The Triangle Inequality for the metric follows directly from the Triangle Inequality for the norm:

$$d(x, z) = ||x - z|| = ||(x - y) + (y - z)|| \leq ||x - y|| + ||y - z|| = d(x, y) + d(y, z)$$

Note that properties (i)–(iv) for d, unlike the properties for the inner product and norm, do not mention addition or scalar multiplication at all. A *set* X (not necessarily a vector space) equipped with a map d satisfying (i)–(iv) is called a *metric space.* A norm will always induce a metric by putting $d(x, y) = ||x - y||$.

2.2 Some Inequalities in $\mathbb{R}^n$ *

In this section, we prove some useful inequalities. We start with an exercise.

Exercise 2.2.1 (1.) Prove that if $x, y \in \mathbb{R}^n$, then

$$||x - y|| \geq \big|\, ||x|| - ||y||\, \big|$$

(2.) (Parallelogram Law)
Prove that if $x, y \in \mathbb{R}^n$, then

$$||x + y||^2 + ||x - y||^2 = 2\big(||x||^2 + ||y||^2\big)$$

Why (do you think) is this identity called the Parallelogram Law?

[Hint: Show that $||x \pm y||^2 = ||x||^2 \pm 2\langle x, y\rangle + ||y||^2$.]

(3.) (**Cauchy–Schwarz Inequality**)[1]
Prove that if $x, y \in \mathbb{R}^n$, then

$$\langle x, y\rangle \leq ||x|| \cdot ||y||$$

and that if x, y are non–zero, then equality holds only if x is a positive scalar multiple of y.

[Hint: First show that $||\alpha x - \beta y||^2 = \alpha^2 ||x||^2 - 2\alpha\beta\langle x, y\rangle + \beta^2||y||^2$. Then put $\alpha = ||y||$ and $\beta = ||x||$ to deduce

$$||y||^2||x||^2 - 2||y||\,||x||\,\langle x, y\rangle + ||x||^2||y||^2 \geq 0 \qquad (*)$$

Deduce that $||x||\,||y|| \geq \langle x, y\rangle$. Next note that we have equality in(*) if and only if $\alpha x - \beta y = 0$. Conclude that if $||x||\,||y|| = \langle x, y\rangle$, then x is a positive scalar multiple of y, Finally, suppose that $x = \gamma y$ for some scalar $\gamma > 0$.Show that $||x||\,||y|| = \langle x, y\rangle$.]

[1] Also called the Cauchy–Bunyakovskii–Schwarz Inequality

□

In the preceding section, we saw one way to provide $\mathbb{R}^n$ with a norm:

$$||x| = \sqrt{x_1^2 + \cdots + x_n^2}$$

There are other ways to equip $\mathbb{R}^n$ with a norm. For $p \geq 1$, define the p–norm $||\cdot||_p : \mathbb{R}^n \to \mathbb{R}^+$ by

$$||x||_p = \left(|x_1|^p + \ldots |x_n|^p\right)^{\frac{1}{p}}$$

The usual norm, introduced earlier, is just $||\cdot||_2$.

We have not yet proved that $||\cdot||_p$ is a norm, and will spend a little time doing so now. Along the way, we shall prove some very powerful inequalities.

To prove that $||\cdot||_p$ is a norm, we have to show that

(i) $||x||_p \geq 0$ for all $x \in \mathbb{R}^n$;

(ii) $||x||_p = 0$ if and only if $x = 0$;

(iii) $||\alpha x||_p = |\alpha|||x||_p$ for all $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$;

(iv) $||x+y||_p \leq ||x||_p + ||y||_p$ for all $x, y \in \mathbb{R}^n$ (Triangle Inequality);

Now (i)–(iii) are easy to see. It is the Triangle Inequality that will take some work.

Definition 2.2.2 A function $f : \mathbb{R}^n \to \mathbb{R}$ is said to be *convex* if and only if whenever $x, y \in \mathbb{R}^n$ and $0 \leq \lambda \leq 1$ we have

$$f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda)f(y)$$

□

Geometrically, this means that any chord joining two points on the graph of f lies entirely above the graph.

The *graph* of f is just the set of points

$$\mathrm{Graph}(f) = \{(x, f(x)) : x \in \mathbb{R}^n\}$$

The graph of f is thus a subset of $\mathbb{R}^{n+1}$. The point $(x, f(x))$ is the point on the graph of f that is "above" x. Suppose that $x, y \in \mathbb{R}^n$, and that $z = \lambda x + (1-\lambda)y$. Then z lies on the line segment between x and y. If $(x, f(x))$ and $(y, f(y))$ lie on the graph of f, then $(z, f(z)) = (z, f(\lambda x + (1-\lambda)y))$ is the point on the graph of f which is above z. On the other hand, the point $(z, \lambda f(x) + (1-\lambda)f(y)) = \lambda(x, f(x)) + (1-\lambda)(y, f(y))$ is the point above z on the line segment joining $(x, f(x))$ and $(y, f(y))$. If f is convex, then the point on the graph lies below the point on the line segment.

Clearly the function $f : \mathbb{R}^+ \to \mathbb{R} : x \mapsto x^p$ is convex if and only if $p \geq 1$.

We now prove a result that has many applications in probability theory:

Proposition 2.2.3 (Jensen's Inequality)
Suppose that $f : \mathbb{R} \to \mathbb{R}$ is a convex function. Let $x_1, \dots, x_n$ be real numbers, and suppose that $\lambda_1, \dots, \lambda_n \geq 0$ such that $\sum_{k=1}^n \lambda_k = 1$. Then

$$\sum_{k=1}^n \lambda_k f(x_k) \geq f(\sum_{k=1}^n \lambda_k x_k)$$

Proof: By induction: This is clearly true if $n = 1$, because then we must have $\lambda_1 = 1$. Next suppose that $\sum_{k=1}^n \lambda'_k f(x_k) \geq f(\sum_{k=1}^n \lambda'_k x_k)$ whenever $x_1, \dots, x_n \in \mathbb{R}$ and $\lambda'_1, \dots, \lambda'_n \geq 0$ with $\sum_{k=1}^n \lambda'_k = 1$. Let $x_1, \dots, x_{n+1} \in \mathbb{R}$, and let $\lambda_1, \dots, \lambda_{n+1} \geq 0$ with $\sum_{k=1}^{n+1} \lambda_k = 1$. Without loss of generality, we may assume $\lambda_{n+1} < 1$. Note that $\lambda_1 + \cdots + \lambda_n = 1 - \lambda_{n+1}$, and define $\lambda'_k = \frac{\lambda_k}{1-\lambda_{n+1}}$, so that $\sum_{k=1}^n \lambda'_k = 1$. Then

$$\begin{aligned} f(\lambda_1 x_1 + \cdots + \lambda_{n+1} x_{n+1}) &= f\big((1-\lambda_{n+1})(\lambda'_1 x_1 + \cdots + \lambda'_n x_n) + \lambda_{n+1} x_{n+1}\big) \\ &\leq (1-\lambda_{n+1}) f(\lambda'_1 x_1 + \cdots + \lambda'_n x_n) + \lambda_{n+1} f(x_{n+1}) \\ &\qquad \text{because } f \text{ is convex} \\ &\leq (1-\lambda_{n+1})\big(\lambda'_1 f(x_1) + \cdots + \lambda'_n f(x_n)\big) + \lambda_{n+1} f(x_{n+1}) \\ &\qquad \text{by induction hypothesis} \\ &= \lambda_1 f(x_1) + \cdots + \lambda_{n+1} f(x_{n+1}) \end{aligned}$$

$\dashv$

Next, we prove the Arithmetic–Geometric Mean Inequality. The arithmetic mean of $x_1, \dots, x_n$ is defined to be $\frac{x_1+\cdots+x_n}{n}$ — just the average value. We define the *geometric mean* of a sequence $x_1, \dots, x_n \geq 0$ to be $\sqrt[n]{x_1 \cdot \cdots \cdot x_n}$. It is then easy to see that the arithmetic mean of two numbers $a, b > 0$ exceeds their geometric mean:

$$(\sqrt{a} - \sqrt{b})^2 \geq 0 \Rightarrow \frac{a+b}{2} \geq \sqrt{ab}$$

This can be generalized to sets of more than just two numbers. Moreover, we can also adjust the *weights*. In the above example, the weights are $\frac{1}{2}$ for each of a, b. We may prefer to assign a weight of λ_1 to a, and λ_2 to b, where $\lambda_1, \lambda_2 \geq 0$ with $\lambda_1 + \lambda_2 = 1$. We then get the following useful inequality:

Proposition 2.2.4 (Arithmetic–Geometric Mean Inequality)
Let $x_1, \dots, x_n > 0$, and suppose that $\lambda_1, \dots, \lambda_n \geq 0$ with $\sum_{k=1}^n \lambda_k = 1$. Then

$$\prod_{k=1}^n x_k^{\lambda_k} \leq \sum_{k=1}^n \lambda_k x_k$$

In particular,

$$\sqrt[n]{x_1 \cdot \cdots \cdot x_n} \leq \frac{x_1 + \cdots + x_n}{n}$$

Proof: Note that $f(x) = -\ln x$ is a convex function. Thus by Jensen's inequality,

$$-\ln\big(\prod_{k=1}^{n} x_k^{\lambda_k}\big) = -\sum_{k=1}^{n} \lambda_k \ln(x_k) \geq -\ln\big(\sum_{k=1}^{n} \lambda_k x_k\big)$$

⊣

Multiply both sides by -1 (which reverses the inequality), and note that $\ln x$ is an increasing function to obtain the result.

⊣

Next, we prove Hölder's Inequality, for which we need the following result:

Exercise 2.2.5 Show that if $a, b > 0$ and $p, q > 1$ are such that $\frac{1}{p} + \frac{1}{q} = 1$, then

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}$$

[Hint: Apply the AGM inequality,to $x_1 = a^p, x_2 = b^q$, with $\lambda_1 = \frac{1}{p}, \lambda_2 = \frac{1}{q}$.]

□

Proposition 2.2.6 (Hölder's Inequality)
Let $p > 1$ and let q be such that $\frac{1}{p} + \frac{1}{q} = 1$. If $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ are non–negative real numbers, then

$$\sum_{i=1}^{n} x_i y_i \leq \big(\sum_{i=1}^{n} x_i^p\big)^{\frac{1}{p}} \big(\sum_{i=1}^{n} y_i^q\big)^{\frac{1}{q}}$$

Proof: Let $A = \left(\sum_{i=1}^{n} x_i^p\right)^{\frac{1}{p}}$ and $B = \left(\sum_{i=1}^{n} y_i^q\right)^{\frac{1}{q}}$. Put $a_j = \frac{x_j}{A}$ and $b_j = \frac{y_j}{B}$, and apply Exercise 2.2.5 to conclude that

$$a_j b_j \leq \frac{a_j^p}{p} + \frac{b_j^q}{q} \qquad \text{i.e.}$$
$$\frac{x_j y_j}{AB} \leq \frac{x_j^p q B^q + y_j^q p A^p}{pqA^pB^q}$$

Summing over j, we obtain

$$\frac{\sum_{j=1}^{n} x_j y_j}{AB} \leq \frac{A^p q B^q + B^q p A^p}{pqA^pB^q} = \frac{p+q}{pq} = 1$$

so that

$$\sum_{j=1}^{n} x_j y_j \leq AB = \big(\sum_{i=1}^{n} x_i^p\big)^{\frac{1}{p}} \big(\sum_{i=1}^{n} y_i^q\big)^{\frac{1}{q}}$$

as required.

$\dashv$

Our final inequality is

Proposition 2.2.7 (Minkowski's Inequality)
Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be non–negative real numbers, and let $p \geq 1$. Then

$$\Big(\sum_{i=1}^{n}(x_i + y_i)^p\Big)^{\frac{1}{p}} \leq \Big(\sum_{i=1}^{n} x_i^p\Big)^{\frac{1}{p}} + \Big(\sum_{i=1}^{n} y_i^p\Big)^{\frac{1}{p}}$$

Proof: This is obvious if $p = 1$. Assume $p > 1$, and let $q = \frac{p-1}{p}$, so that $\frac{1}{p} + \frac{1}{q} = 1$. Then

$$(x_j + y_j)^p = x_j(x_j + y_j)^{\frac{p}{q}} + y_j(x_j + y_j)^{\frac{p}{q}}$$

Put $z_j = (x_j + y_j)^{\frac{p}{q}}$. Then, by Hölder's inequality, we obtain

$$\begin{aligned}
\sum_{j=1}^{n}(x_j + y_j)^p &= \sum_{j=1}^{n} x_j z_j + \sum_{j=1}^{n} y_j z_j \\
&\leq \Big(\sum_{j=1}^{n} x_j^p\Big)^{\frac{1}{p}}\Big(\sum_{j=1}^{n} z_j^q\Big)^{\frac{1}{q}} + \Big(\sum_{j=1}^{n} y_j^p\Big)^{\frac{1}{p}}\Big(\sum_{j=1}^{n} z_j^q\Big)^{\frac{1}{q}} \\
&= \Big(\sum_{j=1}^{n} x_j^p\Big)^{\frac{1}{p}}\Big(\sum_{j=1}^{n}(x_j + y_j)^p\Big)^{\frac{1}{q}} + \Big(\sum_{j=1}^{n} y_j^p\Big)^{\frac{1}{p}}\Big(\sum_{j=1}^{n}(x_j + y_j)^p\Big)^{\frac{1}{q}}
\end{aligned}$$

so that the result follows after we multiply both sides by $\big(\sum_{j=1}^{n}(x_j + y_j)^p\big)^{-\frac{1}{q}}$.

$\dashv$

Using Minkowski's inequality, it is easy to see that

$$||x||_p = \Big(\sum_{j=1}^{n} |x_j|^p\Big)^{\frac{1}{p}}$$

is indeed a norm on $\mathbb{R}^n$, when $p \geq 1$. We need only verify the Triangle Inequality. Now

$$\begin{aligned}
||x + y||_p &= \Big(\sum_{j=1}^{n} |x + y|^p\Big)^{\frac{1}{p}} \\
&\leq \Big(\sum_{j=1}^{n}(|x| + |y|)^p\Big)^{\frac{1}{p}} \\
&\qquad \text{by the Triangle Inequality for absolute values} \\
&\leq \Big(\sum_{j=1}^{n} |x|^p\Big)^{\frac{1}{p}} + \Big(\sum_{j=1}^{n} |y|^p\Big)^{\frac{1}{p}} \\
&\qquad \text{by Minkowski's inequality} \\
&= ||x||_p + ||y||_p
\end{aligned}$$

2.3 Sets in $\mathbb{R}^n$

Recall that each Euclidean space $\mathbb{R}^n$ comes equipped with a "natural" *metric* $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ defined by

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \qquad (= ||x - y||_2)$$

where $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$. $d(x, y)$ is simply the distance between the points x and y.

Definition 2.3.1 (a) If $x \in \mathbb{R}^n$ and $r \geq 0$, then the *open ball* with radius r centered at x is the set of all points y whose distance from x is (strictly) less than r:

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

(b) Similarly, the *closed ball* with radius r centered at x is the set of all points y whose distance from x is less than or equal to r:

$$\bar{B}(x, r) = \{y : d(x, y) \leq r\}$$

(c) A *rectangle* R in $\mathbb{R}^n$ is a cartesian product of n intervals (of finite length)

$$R = I_1 \times \cdots \times I_n$$

where each I_n is an interval in $\mathbb{R}$.
If $I_i = (a_i, b_i)$, where $a_i \leq b_i$ for $i = 1, \ldots, n$, then the set

$$(a_1, b_1) \times \cdots \times (a_n, b_n) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : a_i < x_i < b_i \text{ for } i = 1, \ldots, n\}$$

is called an *open rectangle.*
Thus an open rectangle is a Cartesian product of open intervals of finite length.
Similarly,

$$[a_1, b_1] \times \cdots \times [a_n, b_n] = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : a_i \leq x_i \leq b_i \text{ for } i = 1, \ldots, n\}$$

is called a *closed rectangle.*
Thus a closed rectangle is a Cartesian product of closed intervals of finite length. Closed rectangles are also called *n–cells* in the literature.

□

Roughly, a set is *open* if it contains none of its boundary points; it is *closed* if it contains all its boundary points. We will make this precise in the next section.

Examples 2.3.2 (a) In $\mathbb{R}$, an open ball is just an *open interval* of finite length, e.g.

$$B(3,2) = (1,5) \qquad (-1,4) = B(1.5, 2.5)$$

More generally, $B(x,r) = (x-r, x+r)$ and $(a,b) = B(\frac{b+a}{2}, \frac{b-a}{2})$.
Similarly a closed ball is a *closed interval.*

(b) In $\mathbb{R}^1$ an open rectangle is just an open interval; a closed rectangle is a closed interval.

(c) in $\mathbb{R}^2$, an open ball is (the interior of) a circle. In $\mathbb{R}^3$, it is (the interior of) a ball.

(d) In $\mathbb{R}^2$, a rectangle is an *actual* rectangle. In $\mathbb{R}^3$, it is a rectangular block.

□

Note that the definition of *open ball* invokes a metric, whereas the definition of rectangle uses only the ordering on $\mathbb{R}$. The next exercise shows that the *shape* of an open ball depends on the metric. Open balls look *round* only under the usual metric.

Exercise 2.3.3 Consider the function $d_m : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ defined by

$$d_m(x,y) = \max\{|x_1 - y_1|, |x_2 - y_2|\}$$

on $\mathbb{R}^2$ (where $x = (x_1, x_2)$ and $y = (y_1, y_2)$). Show that d_m is a metric on $\mathbb{R}^2$. Describe (or draw) the "open ball"

$$B_m(0,1) = \{x \in \mathbb{R}^2 : d_m(0,x) < 1\}$$

□

Note that the empty set is both an open ball and an open rectangle:

- $\emptyset = B(x,0)$, for any $x \in \mathbb{R}^n$;
- Note that $\emptyset = (x,x)$ is an open interval in $\mathbb{R}$. If $I_1, \dots, I_n$ are open intervals in $\mathbb{R}$, and if $I_k = \emptyset$ for some $k \leq n$, then $I_1 \times \cdots \times I_n = \emptyset$.

Sometimes balls will be easiest to work with, and sometimes rectangles. When we make heavy use of the metric, open balls will be easiest. On the other hand, it is quite easy to assign a *volume* to a rectangle: The volume is simply the product of the lengths of the sides. Thus the volume of a rectangle with side length r is r^n (in $\mathbb{R}^n$).

It is not so easy to see what the volume of a ball is however. In $\mathbb{R}^1$ it is $2r$ (the *length* of $(-r,r)$), in $\mathbb{R}^2$ it is πr^2 (the *area* of a circle), in $\mathbb{R}^3$ it is $\frac{4\pi}{3}r^3$. It takes quite a bit of work to discover that in $\mathbb{R}^n$, the volume of a ball of radius r is given by

$$\text{Volume} = \frac{\pi^{n/2} r^n}{\Gamma(\frac{n}{2}+1)}$$

Here $\Gamma(x)$ is the *gamma function*, defined by

$$\Gamma(x) = \int_0^\infty u^x e^{-u} \, \frac{du}{u}$$

It has the property that $\Gamma(x+1) = x\Gamma(x)$, as you can easily verify by integrating by parts. Moreover, $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ and $\Gamma(1) = 1$. This is enough information to calculate $\Gamma(\frac{n}{2}+1)$. As an exercise, you can show that the volumes of a 4– and 5–dimensional ball of radius r are, respectively, $\frac{1}{2}\pi^2 r^4$ and $\frac{8}{15}\pi^2 r^5$.

One useful property of rectangles that is not shared by balls is:

Proposition 2.3.4 *The intersection of a family of rectangles is a rectangle.*

Proof: We first consider the one–dimensional case, i.e. we show that the intersection of a family of sub–intervals of $\mathbb{R}$ is again an interval. Let $\mathcal{I} = \{I_j : j \in J\}$ be a family of intervals. We must show that if $x, y \in \bigcap \mathcal{I}$, and if $x < z < y$, then $z \in \bigcap \mathcal{I}$ — that's the *definition* of "interval".

Suppose, therefore, that $x, y \in \bigcap \mathcal{I}$, and that $x < z < y$. Then $x, y \in I_j$ for all $j \in J$, and thus

$$[x, y] \subseteq I_j \qquad \text{all } j \in J$$

Clearly, since $z \in [x, y]$, we have $z \in I_j$ for all $j \in J$, i.e. $z \in \bigcap \mathcal{I}$, as required.

It is now easy to lift this result to higher dimensions. Suppose that $\mathcal{R} = \{R_\gamma : \gamma \in \Gamma\}$ is a family of rectangles in $\mathbb{R}^n$. Each R_γ is a cartesian product of intervals,

$$R_\gamma = I_{\gamma,1} \times \cdots \times I_{\gamma,n}$$

Now it is not hard to see that

$$\bigcap_\gamma R_\gamma = \big(\bigcap_\gamma I_{\gamma,1}\big) \times \cdots \times \big(\bigcap_\gamma I_{\gamma,n}\big)$$

Each set $\bigcap_\gamma I_{\gamma,m}$ is an intersection of intervals, and thus itself an interval. It follows that $\bigcap_\gamma R_\gamma$ is a product of intervals, and thus a rectangle.

$\dashv$

Note that an intersection of rectangles may well be empty, in which case it is still a rectangle. Further note the following:

- If $x, y \in B(x_0, r)$, then $d(x, y) \leq d(x, x_0) + d(x_0, y) \leq 2r$. Thus no two points in an open ball of radius r lie further than a distance $2r$ apart.
- If R is a rectangle with sides of length L in $\mathbb{R}^n$, then the *diagonal* of R has length $L\sqrt{n}$. This can be seen by successively applying the Theorem of Pythagoras. Similarly, the distance from a vertex to the centre of R is $\frac{L\sqrt{n}}{2}$.
- Thus no two points in a rectangle of side length L lie further than a distance $L\sqrt{n}$ apart, and no point is further than $\frac{L\sqrt{n}}{2}$ from the centre.

Proposition 2.3.5 *(a) An open ball can be represented as a union of open rectangles.*

(b) An open rectangle can be represented as a union of open balls.

Proof: (a) Let $x \in B(x_0, r)$. Choose $\varepsilon > 0$ so that $d(x_0, x) + \varepsilon < r$. (For example, take $\varepsilon = \frac{r - d(x, x_0)}{2}$.) Now choose L such that $0 < L < \frac{2\varepsilon}{\sqrt{n}}$, so that $\frac{L\sqrt{n}}{2} < \varepsilon$, and let R_x be an open rectangle with side length L and centre x. If $y \in R_x$, then $d(x, y) \leq \frac{L\sqrt{n}}{2} < \varepsilon$, and so

$d(x_0, y) \leq d(x_0, x) + d(x, y) < d(x_0, x) + \varepsilon < r$. It follows that if $y \in R_x$, then $y \in B(x_0, r)$, and thus that $R_x \subseteq B(x_0, r)$.

Thus, for every $x \in B(x_0, r)$, we have found an open rectangle R_x such that $x \in R_x$ and such that $R_x \subseteq B(x_0, r)$. It is now not hard to see that

$$B(x_0, r) = \bigcup_{x \in B(x_0,r)} R_x$$

Thus $B(x_0, r)$ is a union of open rectangles.

The proof of (b) is similar, and left as an exercise.

⊣

Exercise 2.3.6 (a) Show that an open rectangle can be represented as a union of open balls.

(b) Can closed balls be represented as unions of closed rectangles, or vice versa?

□

Definition 2.3.7 A set $A \subseteq \mathbb{R}^n$ is said to be *bounded* if it is contained in some open ball, i.e. if there exist $x_0 \in \mathbb{R}^n$ and $r > 0$ such that $A \subseteq B(x_0, r)$.

□

Examples 2.3.8 (a) Every finite subset of $\mathbb{R}^n$ is bounded — why?

(b) Every open (closed) ball is bounded.

(c) Every rectangle is bounded.

(d) $\mathbb{R}^n$ is unbounded.

(e) A subset of a bounded set is bounded.

□

Remarks 2.3.9 Instead of using open balls in the definition of boundedness, we could equally well have used open or closed rectangles: A set $A \subseteq \mathbb{R}^n$ is bounded if and only if there is a closed rectangle which contains A. For any open ball can be contained in a closed rectangle; similarly, any closed rectangle can be contained in an open ball.

$$B(x, r) \subseteq [x_1 - r, x_1 + r] \times \cdots \times [x_n - r, x_n + r] \subseteq B(x, r\sqrt{n})$$

(using the usual metric).
The radius $r\sqrt{n}$ is the simply, the distance from the centre to a vertex of rectangle of with sides of length $2r$, as you can easily verify.

□

2.4 Sets in $\mathbb{R}^n$: Open and Closed Sets

Definition 2.4.1 (a) A subset $U \subseteq \mathbb{R}^n$ is said to be an *open set* if and only if for every $x \in U$ there is $r > 0$ such that $B(x, r) \subseteq U$.
Thus a set U is open if and only if around every one of the points of it is possible to find an open ball contained entirely within U.

(b) A subset $C \subseteq R^n$ is said to be a *closed set* if and only if its complement[2] is open.

□

Equivalently, a set C is closed if and only if around every point $x \notin c$ we can find an open ball which is disjoint from C. Further note that not every set is either open or closed, i.e. it is possible for a set to be *neither*. Some examples of such sets are given below.

Examples 2.4.2 (a) Every open ball is an open set. To see this (yes! this *does* need proof!), let $U = B(x_0, r)$ be an open ball in $\mathbb{R}^n$, and let $x \in U$. We must show that there is an open ball about x which is contained entirely within U.

Since $x \in B(x_0, r)$, we have $d(x_0, x) < r$. Now choose a number $\varepsilon > 0$ which is sufficiently small that $d(x_0, x) + \varepsilon < r$ (e.g. $\varepsilon = \frac{r-d(x_0,x)}{2}$ will do). We claim that $B(x, \varepsilon) \subseteq U$.
For suppose that $y \in B(x, \varepsilon)$. Then $d(x, y) < \varepsilon$, and so

$$\begin{aligned} d(x_0, y) &\leq d(x_0, x) + d(x, y) \qquad \text{(Triangle Inequality)} \\ &< d(x_0, x) + \varepsilon \\ &< r \end{aligned}$$

Thus $d(x_0, y) < r$, i.e. $y \in B(x_0, r) = U$.
We have now shown that any y that belongs to $B(x, \varepsilon)$ also belongs to U, i.e. that $B(x, \varepsilon) \subseteq U$.

(b) Every closed ball is a closed set. To see this, let $C = \bar{B}(x_0, r)$. We must show that the complement C^c is open. This means that about in any point in C^c we must find an open ball contained entirely within C^c.
So let $x \in C^c$. Then $d(x_0, x) > r$ (why?), and thus we can find $\varepsilon > 0$ such that $d(x_0, x) - \varepsilon > r$. (Find such a ε.) We claim that $B(x, \varepsilon) \subseteq C^c$. For if $y \in B(x, \varepsilon)$, then

$$\begin{aligned} & d(x_0, x) \leq d(x_0, y) + d(x, y) \qquad \text{(Triangle Inequality)} \\ \Rightarrow\ & d(x_0, y) \geq d(x_0, x) - d(x, y) > d(x_0, x) - \varepsilon > r \end{aligned}$$

so that $y \notin \bar{B}(x_0, r)$, i.e. $y \in C^c$. Hence $B(x, \varepsilon) \subseteq C^c$, as required.

[2] The complement of C is the set $C^c = \mathbb{R}^n - C = \{x \in \mathbb{R}^n : x \notin C\}$

(c) In particular, every open interval in $\mathbb{R}$ is an open set, and every closed interval is a closed set.

(d) The entire set $\mathbb{R}^n$ is open. Indeed if $x \in \mathbb{R}^n$ and $r > 0$, then certainly $B(x,r) \subseteq \mathbb{R}^n$.

(e) The empty set $\emptyset$ is open…

This may seem wrong: How can the empty set contain an open ball???!

Look carefully at the definition of *open set*: A set U is open if and only if around every point in U there is an open ball contained entirely within U, i.e.

$$\forall x \in U \exists r > 0 [B(x,r) \subseteq U]$$

Hence a set U is *not open* if there is a point x in U around which no such open ball can be found: Every open ball about x contains a point not in U.

$$\exists x \in U \forall r > 0 [B(x,r) \not\subseteq U]$$

Thus for U to be *not open* there must exist an $x \in U$ such that…

But we don't need to go any further: If a set U is not open, then it is necessary that there exists an $x \in U$, i.e. it is necessary that $U \neq \emptyset$.

Hence $\emptyset$ cannot be *not open*, and so it is open.

(f) $\mathbb{R}^n$ and $\emptyset$ are both closed: For their complements $(\mathbb{R}^n)^c = \emptyset$ and $\emptyset^c = \mathbb{R}^n$ are both open.

A set which is both open and closed is called a *clopen set*. It can be shown that $\mathbb{R}^n$ and $\emptyset$ are the *only* clopen sets in the space $\mathbb{R}^n$.

(g) A set $U \subseteq \mathbb{R}^n$ is open if and only if its complement U^c is closed: For if U is open, then $(U^c)^c = U$ is open, which means that U^c is closed. On the other hand, if U^c is closed, then $(U^c)^c = U$ must be open.

(h) The set

$$U = \{(x,y) \in \mathbb{R}^2 : 0 < x < 1,\ 2 < y < 3\}$$

is open.

(i) The set

$$C = \{(x,y) \in \mathbb{R}^2 : 0 \leq x \leq 1,\ 2 \leq y \leq 3\}$$

is closed.

(j) Any *finite* subset of $\mathbb{R}^n$ is closed. No non–empty finite set is open.

(k) The interval $(a,b]$ in $\mathbb{R}$ (with $a < b$) is neither open nor closed. It is not open, because no open ball around b is contained in $(a,b]$. It is not closed, because no open ball about a is disjoint from $(a,b]$. (Note that $a \in (a,b]^c$.)

(l) The set

$$A = \{(x,y) \in \mathbb{R}^2 : 0 < x < 1,\ 2 \leq y \leq 3\}$$

is neither open nor closed in $\mathbb{R}^2$: No open ball about the point $(\frac{1}{2}, 3)$ is contained entirely within A. No open ball about the point $(0, \frac{5}{2})$ is entirely disjoint from A.

□

Exercise 2.4.3 Prove that an open rectangle is an open set. Prove that a closed rectangle is a closed set.

□

Proposition 2.4.4 *In $\mathbb{R}^n$, the following are true:*

(a) $\mathbb{R}^n$ and $\emptyset$ are open;

(b) The intersection of finitely many open sets is open;

(c) The union of arbitrarily many open sets is open.

Proof: (a) was proved in Example 2.4.2.
(b) Suppose that $U_1, \ldots, U_m$ are open subsets of $\mathbb{R}^n$, and that $x \in \bigcap_{k=1}^m U_k$. We must show that there is an open ball about x which is contained entirely within $\bigcap_{k=1}^n U_k$. Now $x \in U_k$ for each $k = 1, \ldots, m$, and so, since U_k is open, there is $r_k > 0$ such that $B(x, r_k) \subseteq U_k$, for each $k = 1, \ldots, m$. Let $r = \min\{r_1, \ldots, r_n\}$. Clearly we have

$$B(x,r) \subseteq B(x,r_k) \subseteq U_k \qquad \text{for each } k = 1, \ldots, m$$

Hence $B(x,r) \subseteq U_k$ for each k, i.e. $B(x,r) \subseteq \bigcap_{k=1}^m U_k$.
(c) Let $\{U_i : i \in I\}$ be a family of open subsets of $\mathbb{R}^n$, and let $U = \bigcup_I U_i$. If $x \in U$, then there is $i_0 \in I$ such that $x \in U_{i_0}$. Since U_{i_0} is open, there is $r > 0$ such that $B(x,r) \subseteq U_{i_0}$. Then

$$B(x,r) \subseteq U_{i_0} \subseteq U$$

⊣

A *topological space* is a pair $(X, \mathcal{T})$, where X is a set and $\mathcal{T}$ a family of subsets of X, with the following properties:

(i) X and $\emptyset$ belong to $\mathcal{T}$;

(ii) $\mathcal{T}$ is *closed under finite intersections*: If $U_1, \ldots, U_m \in \mathcal{T}$, then $\bigcap_{k=1}^m U_k \in \mathcal{T}$.

(iii) $\mathcal{T}$ is *closed under arbitrary unions*: If $\{U_i : i \in I\}$ is a family of sets in $\mathcal{T}$, then $\bigcup_I U_i \in \mathcal{T}$.

Theorem 2.4.4 shows that if $\mathcal{T}$ is the set of open subsets of $\mathbb{R}^n$, then $(\mathbb{R}^n, \mathcal{T})$ is a topological space.

The following characterization of the notion of open set is often useful:

Proposition 2.4.5 *A subset $U \subseteq \mathbb{R}^n$ is open if and only if it is a union of open balls.*

Proof: ($\Rightarrow$) Suppose that U is a union of open balls. Then it is a union of open sets (because open balls are open sets, by Example 2.4.2), and thus itself an open set (because unions of open sets are open, by Theorem 2.4.4).

($\Leftarrow$) Next, suppose that U is an open set. For each $x \in U$, choose $r_x > 0$ so that $B(x, r_x) \subseteq U$. Then certainly

$$\bigcup_{x \in U} B(x, r_x) \subseteq U$$

Now if $x_0 \in U$, then $x_0 \in B(x_0, r_{x_0}) \subseteq \bigcup_{x \in U} B(x, r_x)$. Hence also

$$U \subseteq \bigcup_{x \in U} B(x, r_x)$$

and thus

$$U = \bigcup_{x \in U} B(x, r_x)$$

This proves that U is a union of open balls.

⊣

Exercise 2.4.6 Show that the intersection of an arbitrary family of open sets need not be open.
[Hint: In $\mathbb{R}$, let $U_n = (-1 - \frac{1}{n}, 1 + \frac{1}{n})$ and compute $\bigcap_n U_n$.]

□

Because the closed sets are just complements of the open sets, the following proposition is an easy application of de Morgan's Laws[3]:

Proposition 2.4.7 In $\mathbb{R}^n$, the following are true:

(a) $\mathbb{R}^n$ and $\emptyset$ are closed;

(b) The intersection of arbitrarily many closed sets is closed;

(c) The union of finitely many closed sets is closed.

Proof: Exercise!

⊣

Exercise 2.4.8 (a) Show that the union of an arbitrary family of closed sets need not be closed.

(b) Write the interval $(a, b]$ as a union of closed intervals.

(c) Write the interval $(a, b]$ as an intersection of open intervals.

(d) Let $\mathbb{Q} \subseteq \mathbb{R}$ be the set of rational numbers. Is $\mathbb{Q}$ an open subset of $\mathbb{R}$? Is it closed? Supply reasons for your answers.

[3] $(A \cup B)^c = A^c \cap B^c$; $(A \cap B)^c = A^c \cup B^c$.

□

Definition 2.4.9 (a) A set $A \subseteq R^n$ is a *neighbourhood* of a point $a \in \mathbb{R}^n$ if and only if there is $r > 0$ such that $B(x, r) \subseteq A$. In that case, a is said to be an *interior point* of A.

(b) A point $x \in \mathbb{R}^n$ is called a *cluster point* of a set $A \subseteq \mathbb{R}^n$ if and only if for every $r > 0$ there is $y \in B(x, r) \cap A$ such that $y \neq x$.

Cluster points are also called *limit points* or *points of accumulation.*

□

Exercise 2.4.10 Prove that

(a) a is an interior point of A if and only if there is an open set U such that $a \in U$ and $U \subseteq A$.

(b) a is a cluster point of A if and only if every neighbourhood U of x contains a point of A which is distinct from x (i.e. $A \cap E - \{x\} \neq \emptyset$).

(c) If $A \subseteq B$ and if a is an interior point of A, then a is an interior point of B.

(d) If $A \subseteq B$, and if a is a cluster point of A, then a is a cluster point of B.

□

Examples 2.4.11 (a) In $\mathbb{R}$, 1 is an interior point of $(0, 2]$, but 2 is not.

(b) Both $0, 2$ are cluster points of $(0, 2]$.

(c) Every point $x \in (0, 2]$ is a cluster point of $(0, 2]$.

(d) 3 is not a cluster point of $(0, 1] \cup \{3\}$.

(e) The only cluster point of the set $A = \{\frac{1}{n} : n \in \mathbb{N}\}$ is the point 0. $\partial A = A \cup \{0\}$.

(f) The set of cluster point of $B(x, r) \subseteq \mathbb{R}^n$ is $\bar{B}(x, r)$.

(g) Every $x \in \mathbb{R}$ is a cluster point of $\mathbb{Q}$, because every open interval about x contains both a rational and an irrational number. Thus $\partial\mathbb{Q} = \mathbb{R}$.

□

Remarks 2.4.12 (1) Intuitively, A is a neighbourhood of a if and only if A contains the points a and all points “close” to a. In particular, $a \in A$.

(2) Note that a set $U \subseteq \mathbb{R}^n$ is open if and only if it is a neighbourhood of each of its elements — proof?

(3) Intuitively, a point x is a cluster point of A if and only if there are points of A distinct from x, but lying *arbitrarily close* to x:

$$\forall \varepsilon > 0 \exists y [y \in E \wedge 0 < d(x,y) < \varepsilon]$$

For given a $\varepsilon > 0$, then $B(x,\varepsilon)$ is a neighbourhood of x, so we can choose a $y \in B(x,\varepsilon) \cap A - \{x\}$. That y will have the property that $d(x,y) > 0$ (because $y \neq x$) and $d(x,y) < \varepsilon$ (because $y \in B(x,\varepsilon)$).

(4) A finite subset $A \subseteq \mathbb{R}^n$ has no cluster points and no interior points — why not?

□

Exercise 2.4.13 Suppose that x is a cluster point of A, and that U is a neighbourhood of x. Show that $U \cap A$ is an infinite set.
[Hint: Suppose that $B(x,r) \subseteq U$. Then $U_n = B(x, \frac{r}{n}) \subseteq U$ for each $n \in \mathbb{N}$. Now U_n is a neighbourhood of x, so there is $a_n \in A \cap U_n$ such that $a_n \neq x$. Show that $\{a_n : n \in \mathbb{N}\} \subseteq U \cap A$, and also show that $\{a_n : n \in \mathbb{N}\}$ is an infinite set.]

□

Proposition 2.4.14

A set $C \subseteq \mathbb{R}^n$ is closed if and only every cluster point of C belongs to C.

Proof: Suppose that C is closed and that $x \notin C$. Then $x \in C^c$. Since C^c is open, there is an open ball $B(x,r)$ such that $B(x,r) \subseteq C^c$, i.e. $B(x,r) \cap C = \emptyset$. Hence x is not a cluster point of C. It follows that if x is a cluster point of C, then $x \in C$.
Conversely, suppose that every cluster point of C belongs to C . We must show that C is closed, i.e. that C^c is open. Suppose that C^c is not open. Then there is $x \in C^c$ such that no open ball about x is contained in C^c, i.e.

$$\forall r > 0 [B(x,r) \cap C \neq \emptyset$$

Now if $y \in B(x,r) \cap C$, then $y \neq x$, since $x \notin C$. It follows that every open ball about x contains a point of C distinct from x, and thus that x is a cluster point of C. But then $x \in C$, contradiction! Thus C^c is open, and so C is closed.

$\dashv$

Definition 2.4.15 Let $A \subseteq \mathbb{R}^n$. We define:

(a) The *interior* of A is the set of all interior points of A, and denoted A° or $\mathrm{int}(A)$.

$$A^\circ = \{x \in \mathbb{R}^n : \exists r > 0 \; [B(x,r) \subseteq A]\}$$

(b) The *closure* of A is denoted $\bar{A}$ or $\mathrm{cl}(A)$ and defined by

$$\bar{A} = A \cup \{\text{cluster points of } A\}$$

□

Proposition 2.4.16 *Let $A \subseteq \mathbb{R}^n$.*

(a) $A^\circ = \bigcup\{U \subseteq A : U \text{ is open}\}$
Thus A° is the biggest open set contained in A.

(b) $\bar{A} = \bigcap\{C \supseteq A : C \text{ is closed}\}$
Thus $\bar{A}$ is the smallest closed set which contains A.

(c) $(A^\circ)^c = \bar{A^c}$*, i.e.* $(\mathrm{int}(A))^c = \mathrm{cl}(A^c)$

Proof: (a) Suppose that $x \in A^\circ$. Then there is an $r > 0$ such that the open ball $B(x,r)$ is contained in A. But $B(x,r)$ is an open set, and hence $B(x,r) \in \{U \subseteq A : U \text{ is open}\}$. It follows that

$$x \in B(x,r) \subseteq \bigcup\{U \subseteq A : U \text{ is open}\}$$

Since x was an arbitrary, we have now shown that $x \in A^\circ$ implies $x \in \bigcup\{U \subseteq A : U \text{ is open}\}$, i.e. that

$$A^\circ \subseteq \bigcup\{U \subseteq A : U \text{ is open}\}$$

The $\supseteq$–direction is obvious, because each U in the union is a subset of A.
Now note that A° is *open*, because we it is a union of open sets (and a union of open sets is open, by Proposition 2.4.4). Now if $U \subseteq A$ is open, then clearly $U \subseteq A^\circ$. Hence A° is the biggest open set contained in A.
(b) We first show that $\bar{A}$ is closed, and, for that, it suffices to show that every cluster point of $\bar{A}$ belongs to $\bar{A}$, by Proposition 2.4.14. Now if $x \notin \bar{A}$, then x is not a cluster point of A, nor does x belong to A. Hence there exists an open neighbourhood U of x such that $\cap A = \emptyset$.

But then $U \cap \bar{A} = \emptyset$ as well: For if $y \in U \cap \bar{A}$, then y is a cluster point of A (since $\bar{A} = A \cup$ cluster points of A, and $U \cap A = \emptyset$). Yet y has a neighbourhood which does not intersect A, namely U. Thus y is not a cluster point of A, contradiction.

Since $x \in U$ and $U \cap \bar{A} = \emptyset$, it follows that x is not a cluster point of A. We have thus shown that if $x \notin \bar{A}$, then x is not a cluster point of $\bar{a}$. It follows that if x *is* a cluster point of A, then it must belong to $\bar{A}$. Hence $\bar{A}$ contains all its cluster points, and so $\bar{A}$ is closed.

To prove that $\bar{A}$ is the smallest closed set that contains A, we need only prove that any closed set which contains A also contains $\bar{A}$. Suppose, therefore, that C is a closed set, and that $C \supseteq A$. Then every cluster point of A is a cluster point of C (by Exercise 2.4.10), and thus every cluster point of A belongs to C (since C is closed). Hence $C \supseteq \bar{A}$.

(c)

$$\begin{aligned}(A^\circ)^c &= \Big(\bigcup\{U : U \subseteq A, U \text{ open}\}\Big)^c \\ &= \bigcap\{U^c : U \subseteq A, U \text{ open}\} \\ &= \bigcap\{C : C \supseteq A^c, C \text{ closed}\} \\ &= \bar{A^c}\end{aligned}$$

⊣

In topology, the formulation of A° and $\bar{A}$ given in Proposition 2.4.16 is taken as a *definition* of interior and closure. Note this formulation only depends on the concept of open set, and not on a norm or a metric.

Exercise 2.4.17 A point a is called a *boundary point* of a set $E \subseteq \mathbb{R}^n$ if and only if every neighborhood of a intersects both E and E^c: For any neighbourhood A of a we have both

$$A \cap E \neq \emptyset \quad \text{and} \quad A \cap E^c \neq \emptyset$$

The set of all boundary points of a set E is denoted by ∂E.

(a) Every point of a finite set $E \subseteq \mathbb{R}^n$ is a boundary point — why?

(b) E and E^c have the same boundary points: $\partial E = \partial E^c$ – why?

(c) If A is a non–empty subset of $\mathbb{R}$, then $\sup A$ and $\inf A$ both belong to ∂A — why?

(d) Give examples to show that a boundary point of a set need not be a cluster point, nor need a cluster point be a boundary point.

(e) Prove that every boundary point of a set $A \subseteq \mathbb{R}^n$ either belongs to A or is a cluster point of A. Similarly, every cluster point of A either belongs to A or is a boundary point of A.

(f) A set C is closed if and only if it contains all its boundary points, i.e. $\partial C \subseteq C$.

(g) A set U is open if and only if it contains none of its boundary points, i.e. $\partial U \cap U = \emptyset$.

□

2.5 The Bolzano–Weierstrass Theorem

The Bolzano–Weierstrass Theorem asserts that every infinite bounded subset of $\mathbb{R}^n$ has a cluster point. It is one of the fundamental pillars of real analysis.

We begin by generalizing the Nested Interval Property (cf. Exercise 1.4.12) to closed rectangles in $\mathbb{R}^n$:

Theorem 2.5.1 (Nested Rectangles Property)
Let $(I_k)_k$ be a decreasing sequence of closed rectangles in $\mathbb{R}^n$, i.e.

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_k \supseteq \ldots$$

Then $\bigcap_k I_k \neq \emptyset$.

Proof: Each closed rectangle I_k is of the form

$$I_k = \{(x_1, \dots, x_n) : a_{k,1} \le x_1 \le b_{k,1}, \dots, a_{k,n} \le x_n \le b_{k,n}\}$$

for some real numbers $a_{k,1}, \dots a_{k,n}$ and $b_{k,1}, \dots, b_{k,n}$ with $a_{k,i} \le b_{k,i}$. Now suppose that $k \le m$ in $\mathbb{N}$. Then $I_k \supseteq I_m$, and so

$$a_{k,i} \le a_{m,i} \le b_{m,i} \le b_{k,i} \qquad i = 1, \dots, n$$

(Why?). In particular, for each $i = 1, \dots, n$, we have

$$a_{1,i} \le a_{2,i} \le \cdots \le a_{k,i} \le \cdots \le b_{k,i} \le \cdots \le b_{2,i} \le b_{1,i}$$

By the Completeness axiom, let

$$y_i = \sup\{a_{k,i} : k \in \mathbb{N}\}$$

Then $a_{k,i} \le y_i \le b_{k,i}$ for each $i = 1, \dots, n$ and each $k \in \mathbb{N}$. Hence $(y_1, \dots, y_n) \in I_k$ for each $k \in \mathbb{N}$, and thus

$$(y_1, \dots, y_n) \in \bigcap_k I_k$$

⊣

Remarks 2.5.2 The Nested Rectangles Property can be used to give an easy proof that the set of real numbers is uncountable.

We proceed as follows: Let $A = \{a_n : n \in \mathbb{N}\}$ be a set of real numbers. We shall show that there is a $x \in \mathbb{R}$ such that $x \notin A$.

If we can do this, then no countable subset of $\mathbb{R}$ contains all the real numbers (because, given any countable subset $A \subseteq \mathbb{R}$, we can find an x which does not belong to A).

Let I_0 be a closed (and bounded) subinterval of $\mathbb{R}$ such that $a_0 \notin I_0$. Now let I_1 be a closed subinterval of I_0 such that $a_1 \notin I_1$. Continue inductively: Given a a closed interval I_n, let I_{n+1} be a closed subinterval of I_n such that $a_{n+1} \notin I_{n+1}$.

By construction, $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \dots$ is a nested sequence of closed intervals. By the Nested Intervals Property, there is $x \in \bigcap_n I_n$. Now, for any n, we have $x \neq a_n$, as $x \in I_n$, but $a_n \notin I_n$.

The following exercise will be useful in the proof of the Bolzano–Weierstrass Theorem:

Exercise 2.5.3 Suppose that R is a closed rectangle in $\mathbb{R}^n$ (endowed with the usual metric), and that R has maximum side length L. If $a \in R$, and if $L \le \frac{r}{\sqrt{n}}$, then $R \subseteq B(a, r)$. [Hint: If $x, y \in R$, then $|x_i - y_i| \le L$ for each $i = 1, \dots, n$. Hence $d(x, y) \le L\sqrt{n}$.]

□

Theorem 2.5.4 (Bolzano–Weierstrass)
Every bounded infinite subset of $\mathbb{R}^n$ has a cluster point.

Proof: Suppose that B is a bounded infinite set. Let R_1 be a closed rectangle which contains B. By enlarging R_1, if necessary, we may assume that all sides of R_1 have the same length, L.

If you bisect each of the sides of R_1, you will obtain 2^n closed subrectangles, each with sides of length $\frac{L}{2}$. At least one of those subrectangles must contain infinitely many points of B (for if each of the 2^n subrectangles contained only a finite number of points of B, then B would necessarily be a finite set). Choose R_2 to be such a closed subrectangle of R_1, so that R_2 contains infinitely many points of B.

Now repeat the construction: If you bisect the sides of R_2, you will obtain 2^n closed subrectangles of R_2, each with sides of length $\frac{L}{4}$. At least one such subrectangle must contain infinitely many points of B, so let R_3 be such a closed subrectangle.

Continuing in this way, we find, for each $k \in \mathbb{N}$, a closed rectangle R_k which contains infinitely many points of B, and which has sides of length $\frac{L}{2^{k-1}}$. Clearly

$$R_1 \supseteq R_2 \supseteq R_2 \supseteq \cdots \supseteq R_k \supseteq \dots$$

By the Nested Rectangle Property there is a point x which belongs to every R_k. We shall show that x is the desired cluster point of B.

What we must show is that every neighbourhood of x contains a point of B which is distinct from x. So let U be a neighbourhood of x. By definition of *neighbourhood* there is $r > 0$ such that $B(x,r) \subseteq U$. Now $x \in R_k$ for each k. By choosing k sufficiently large, we can ensure that $R_k \subseteq B(x,r)$. (Indeed, if we choose k so large that

$$\frac{L}{2^{k-1}} \leq \frac{r}{\sqrt{n}}$$

then $R_k \subseteq B(x,r)$, by Exercise 2.5.3. This can be done by the *archimedean property*.)

So choose k_0 so that $R_{k_0} \subseteq B(x,r)$. Then R_{k_0} contains *infinitely* many elements of B, and thus at least one element b of B which is distinct from x. Since $R_{k_0} \subseteq B(x,r) \subseteq U$, we have $b \in U$. Hence U also contains a point of B which is distinct from x.

⊣

Exercise 2.5.5 Give an example of a infinite subset of $\mathbb{R}$ which has no cluster point.

□

2.6 Sets in $\mathbb{R}^n$: Compact Sets

In this section, we introduce and characterize the notion of a compact set, one of the most use.

Definition 2.6.1 (a) Let $A \subseteq \mathbb{R}^n$. An *open cover* of A is a family $\{U_i : i \in I\}$ of open sets such that

$$A \subseteq \bigcup_I U_i$$

(b) A set $K \subseteq \mathbb{R}^n$ is said to be *compact* if and only if every open cover of K has a *finite subcover*, i.e. if and only if whenever $\{U_i : i \in I\}$ is an open cover of K, there is a finite set of indices $i_1, \dots i_n \in I$ such that

$$K \subseteq U_{i_1} \cup \cdots \cup U_{i_n}$$

□

Examples 2.6.2 (a) Every *finite* subset of $\mathbb{R}^n$ is compact— why?

(b) $\mathbb{R}^n$ itself is *not* compact. For example, if $U_n = B(0, n)$, then $\{U_n : n \in \mathbb{N}\}$ is an open cover of $\mathbb{R}^n$. Yet it clearly has no finite subcover — why not?

(c) No open interval (a, b) is compact in $\mathbb{R}$: Let $U_n = (a + \frac{1}{n}, b - \frac{1}{n})$. Then clearly $(a, b) = \bigcup_n U_n$ (i.e. $\{U_n\}_n$ is an open cover of (a, b)). Yet $\{U_n\}_n$ clearly has no finite subcover of (a, b) — why not?

□

The following exercise shows that there are infinite compact sets in $\mathbb{R}$:

Exercise 2.6.3 We prove that the closed unit interval $[0, 1]$ is a compact subset of $\mathbb{R}$.

(a) Let $I = [0, 1]$ be the closed unit interval, and let $\mathcal{U} = \{U_\gamma : \gamma \in \Gamma\}$ be an open cover of I. Define I^* to be the set of all those $x \in I$ for which $[0, x]$ can be covered by a finite subfamily of $\mathcal{U}$:

$$I^* = \{x \in [0, 1] : \exists \gamma_1, \dots, \gamma_m \in \Gamma \;\; ([0, x] \subseteq U_{\gamma_1} \cup \cdots \cup U_{\gamma_m})\}$$

(b) Explain why $0 \in I^*$.

(c) Show that I^* is a subinterval of I: If $x \in I^*$ and $0 \leq y \leq x$, then $y \in I^*$.

(d) Define $x^* = \sup I^*$. Explain why $0 \leq x^* \leq 1$.

(e) Explain why there is $\gamma^* \in \Gamma$ such that $x^* \in U_{\gamma^*}$.

(f) Explain why $x^* \in I^*$.

(g) Assume now that $x^* < 1$. Explain why there is $\varepsilon > 0$ such that $[x^* - \varepsilon, x^* + \varepsilon] \subseteq U_{\gamma^*} \cap [0, 1]$.

(h) Explain why $[0, x^* + \varepsilon]$ can be covered by a finite subfamily of $\mathcal{U}$.

(i) Conclude that $x^* + \varepsilon \in I^*$.

(j) Explain why this is a contradiction.

(k) Deduce that $1 \in I^*$, and thus that I can be covered by a finite subfamily of $\mathcal{U}$.

□

The above exercise can easily be generalized to show that any closed interval $[a, b]$ in $\mathbb{R}$ is compact.

Generally, it is no trivial matter to show that a set is compact from the definition. We therefore turn our attention to a characterization of the compact subsets of $\mathbb{R}^n$. To begin with, we show that compact sets are closed.

Proposition 2.6.4 *If $K \subseteq \mathbb{R}^n$ is compact, then it is closed.*

Proof: We shall show that K^c is open. If $K^c = \emptyset$, it is certainly open[4], so we may assume that $K^c \neq \emptyset$. To show that K^c is open, it suffices to find, for each $y \in K$, an open neighbourhood V of y with $V \subseteq K^c$.

Choose, therefore a $y_0 \in \mathbb{R}^n - K$. For each $x \in K$, define $r_x = \frac{d(x,y_0)}{2}$ and put

$$V_x = B(y_0, r_x) \qquad U_x = B(x, r_x)$$

Then $U_x \cap V_x = \emptyset$ (for if $z \in U_x \cap V_x$, then $d(x, y_0) \leq d(x, z) + d(z, y_0) < r_x + r_x = d(x, y_0)$.). Now clearly

$$K \subseteq \bigcup_{x \in K} U_x$$

i.e. $\mathcal{U} = \{U_x : x \in K\}$ is an open cover of K. Since K is compact, there are $x_1, \dots, x_m \in K$ such that

$$K \subseteq U_{x_1} \cup \cdots \cup U_{x_m}$$

Define $U = U_{x_1} \cup \cdots \cup U_{x_m}$, and put $V = V_{x_1} \cup \cdots \cup V_{x_m}$. Then V is an open neighbourhood of y_0 (because finite intersections of open sets are open, and because y_0 belongs to each V_x).

We now claim that $V \subseteq K^c$. Indeed, if $x \in K$, then $x \in U$, and thus $x \in U_{x_k}$ for some $k = 1, \dots, m$. But then $x \notin V_{x_k}$ (as $U_{x_k} \cap V_{x_k} = \emptyset$), and thus $x \notin V$ (as $V \subseteq V_{x_k}$). Hence $x \in K$ implies $x \notin V$, so that $V \subseteq K^c$, as required.

It follows that every $y_0 \in K^c$ has a neighbourhood V contained entirely within K^c. hence K^c is open.

⊣

Next, we show that compact sets are bounded. (Recall that a set $A \subseteq \mathbb{R}^n$ is bounded if it is contained in an open ball of finite radius. Equivalently, A is bounded if it is contained in a closed rectangle.)

Proposition 2.6.5 *Suppose that $K \subseteq \mathbb{R}^n$ is compact. Then it is bounded.*

[4] although we know that $\mathbb{R}^n$ is not compact anyway.

Proof: If K is *unbounded*, then no open ball $B(0,n)$ of radius n about the origin contains K. But then $\{B(0,n) : n \in \mathbb{N}\}$ is an open cover of K with no finite subcover.

⊣

Exercise 2.6.6 Show that a closed subset of a compact set is compact.
[Hint: Suppose that $C \subseteq K$, where C is closed, and K is compact. Let $\mathcal{U}$ be an open cover of C. Show that $\mathcal{U} \cup \{C^c\}$ is an open cover of K.]

□

Closedness and boundedness completely capture the notion of compactness in $\mathbb{R}^n$. The proof of this fact has much in common with the proof of the Bolzano–Weierstrass Theorem.

Theorem 2.6.7 (Heine–Borel) *A set $K \subseteq \mathbb{R}^n$ is compact if and only if it is closed and bounded.*

Proof: We have just shown that any compact set is both closed and bounded.

Now let $K \subseteq \mathbb{R}^n$ be closed and bounded, and suppose that K is not compact. Let $\mathcal{U} = \{U_i : i \in I\}$ be an open cover of K with no finite subcover. Also, let R_1 be a closed rectangle which contains K. Without loss of generality, we may assume that each side of R_1 has length L.

Bisecting each of the sides of R_1, we obtain 2^n closed subrectangles of R_1. Let $R_{2,1}, \dots, R_{2,2^n}$ be those rectangles, and let $K_j = K \cap R_{2,k}$, for $j = 1, \dots 2^n$. Thus K_j is that part of K which is contained in the j^{th} subrectangle of R_1. Now if every K_j can be covered by a finite subfamily of $\mathcal{U}$, then K itself can also be covered by a finite subfamily of $\mathcal{U}$, as there are only finitely many j. This contradicts our hypothesis, and thus there is at least one j such that K_j cannot be covered by a finite subfamily of $\mathcal{U}$. Let R_2 be a corresponding $R_{2,j}$, so that $K \cap R_2$ cannot be covered by a finite subfamily. Note that R_2 has sides of length $\frac{L}{2}$.

Now repeat the entire procedure. Bisect the sides of R_2 to obtain closed subrectangles $R_{3,1}, \dots, R_{3,2^n}$, and *redefine* $K_j = K \cap R_{3,j}$. There is at least one j such that K_j cannot be covered by a finite subfamily of $\mathcal{U}$. Let R_3 be a corresponding $R_{3,j}$. R_3 has sides of length $\frac{L}{4}$

Continuing in this way, we obtain a nested sequence of closed subrectangles

$$R_1 \supseteq R_2 \supseteq \cdots \supseteq R_k \supseteq \dots$$

with the property that

No $K \cap R_k$ can be covered by a finite subfamily of $\mathcal{U}$.

By the Nested Rectangle Property, there is a point $y \in \bigcap_k R_k$. Now each R_k clearly contains infinitely many points of K, and hence y is a cluster point of K. (For if U is an open neighbourhood of y, we can choose k sufficiently large that $R_k \subseteq U$, as we did in the proof of the Bolzano–Weierstrass Theorem. Thus U contains infinitely many points of K, and thus at least one point of K which is distinct from y.)

Now K is closed, and thus contains all its cluster points. Hence $y \in K$. It follows that there is an open $U \in \mathcal{U}$ such that $y \in U$. Yet, as above, we may choose k sufficiently large to ensure $R_k \subseteq U$. But then the elements of $K \cap R_k$ *can* be covered by a finite subfamily of $\mathcal{U}$, namely the one–element subfamily $\{U\}$, a contradiction.

Proceeding from the assumption that a closed and bounded set K is not compact, we obtained a contradiction. Hence every closed and bounded set *is* compact.

$\dashv$

Exercise 2.6.8 1. We improve the *Nested Rectangle Property*: If $K_1 \supseteq K_2 \supseteq \cdots \supseteq K_m \supseteq \dots$ is a nested sequence of *non–empty* compact subsets of $\mathbb{R}^n$, then

$$K = \bigcap_m K_m$$

is a non–empty compact subset of $\mathbb{R}^m$.

This result is known as the *Cantor Intersection Theorem.*

(a) Explain why K is compact.

(b) Now we must show that K is non–empty. Choose $a_m \in K_m$, and let $A = \{a_m : m \in \mathbb{N}\}$. Then A is either finite or infinite. First assume that A is finite. Show that K is non–empty.
[Hint: There must be an $a \in A$ such that $a = a_m$ for infinitely many m. Explain why $a \in K$.]

(c) Next we deal with the other case: Assume that A is infinite. Explain why A has a cluster point.

(d) Let b be a cluster point of A. Show that b is a cluster point of each K_m.
[Hint: Let U be a neighbourhood of b. Then U contains infinitely many points of A, by Exercise 2.4.13. Show that U contains at least one point of K_m which is distinct from x.]

(e) Conclude that $b \in K$.

2. We present here an alternative proof of (1.). Let $K_1 \supseteq K_2 \supseteq \cdots \supseteq K_m \supseteq \dots$ be a nested sequence of non–empty compact subsets of $\mathbb{R}^n$, and let $K = \bigcap_m K_m$. We will show that K is non–empty.

(a) Suppose that $K = \emptyset$. Show that $\mathcal{U} = \{K_m^c : m \in \mathbb{N}\}$ is an open cover of K_1.

(b) Explain why there exists an $m_0 \in \mathbb{N}$ such that

$$K_1 \subseteq K_1^c \cup \cdots \cup K_{m_0}^c$$

(c) Thus $K_1 \subseteq K_{m_0}^c$. Why?

(d) Deduce that $K_{m_0} = \emptyset$.

(e) Explain why we have now obtained a contradiction.

□

We end this section with one more useful result, the *Lebesgue Covering Theorem.*

Theorem 2.6.9 (Lebesgue Covering Theorem)
Suppose that $\mathcal{U} = \{U_i : i \in I\}$ is an open cover of a compact set $K \subseteq \mathbb{R}^n$. Then there exists a number $\lambda > 0$ such that if $x, y \in K$ and if $||x - y|| < \lambda$, then there is $U_i \in \mathcal{U}$ such that $x, y \in U_i$.
(i.e. $\exists \lambda > 0\ \forall x, y \in K\ \exists i \in I\ [x \in U_i \wedge y \in U_i]$.)

Proof: Define $\iota : K \to I$ as follows: For each $x \in K$, $\iota(x)$ is such that $x \in U_{\iota(x)}$. Now since each U_i is open, we may choose ε_x such that $B(x, \varepsilon_x) \subseteq U_{\iota(x)}$. Let

$$V_x = \{y \in \mathbb{R}^n : ||x - y|| \leq \frac{1}{2}\varepsilon_x\}$$

Then $V(x)$ is an open neighbourhood of x, and thus the family

$$\mathcal{V} = \{V_x : x \in K\}$$

is an open cover of K. As K is compact, we may chooses $x_1, \dots, x_m \in K$ such that

$$K \subseteq V_{x_1} \cup \cdots \cup V_{x_m}$$

Now let $\lambda = \frac{1}{2}\min\{\varepsilon_{x_1}, \dots, \varepsilon_{x_n}\}$. Now take $x, y \in K$, with $||x - y|| < \lambda$. Firstly, $x \in V_{x_k}$ for some x_k $(1 \leq k \leq m)$, and thus $||x_k - x|| < \frac{1}{2}\varepsilon_{x_k}$. Secondly,

$$||x_k - y|| \leq ||x_k - x|| + ||x - y|| < \frac{1}{2}\varepsilon_{x_k} + \lambda \leq \varepsilon_{x_k}$$

as $\lambda \leq \frac{1}{2}\varepsilon_{x_k}$. But then both $x, y \in B(x_k, \varepsilon_{x_k}) \subseteq U_{\iota(x_k)}$.

⊣

The number λ is called the *Lebesgue number* of the covering $\mathcal{U}$.