Lecture Note: Introduction to Algebra and Introduction to Analysis (in MAM 202)

E. O. D. Andriantiana

June 5, 2023

Contents

Chapter 1

Introduction

In this course, we revisit several notions that you studied in MAT1C: sets, mappings, arithmetics, sequence, limits, functions and Taylor series. This time, we make effort to study those topics using more formal mathematical language. We will see more frequent proofs, they are chosen to illustrate the proof techniques that were pointed out to you in first year. This will prepare you to more advanced Algebra and Analysis in 3rd year.

On the exam or tests of this course, you are expected to be able to

- reproduce the proofs that are discussed in class;
- use similar ideas as in the proofs discussed in class for a slightly different situation;
- apply the theorems, lemmas and propositions that you learned in class to solve mathematical problems.

The course will have 1 period tutorial every week. It is particularly important to attend tutorial, because we usually include in the tutorials examples that we did not have time to discuss in class.

Chapter 2

Algebra

2.1 Preliminaries

2.1.1 Set

Define a set

A *set* is a well defined collection of distinct objects. In principle, any objects (people, cars, planets,..) can be gathered to make-up a set. But in this course we will be interested in sets of mathematical objects such as numbers, functions or sets.

An object belonging to a set S is called an *element* of S. If x is an element of a set S, then we write

$$x \in S.$$

We write

$$x \notin S$$

to say that x is not an element of S.

The number of elements in a set S is called *cardinality* of S, and it is denoted by $|S|$.

There are several ways to define a set:

- We can list all its elements. For example

  $$A = \{a, 3, \maltese, \spadesuit\}$$

  is the set whose elements are $a, 3, \maltese$ and $\spadesuit$. The cardinality of A is $|A| = 4$.

  $$B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

  is the set of positive integers less than 10. It has cardinality 9.

- Sometimes, it is not possible to list all the elements in a set. An alternative way to define a set is to use the so-called *set-builder* notation:

  $$\{x : x \text{ has property } P\}.$$

  It describes the set of all objects which has property P. The last part of the notation provides the condition to be an element of the set. For example, we can write

  $$E = \{x : x \text{ is even integer }\}$$

  to describe the set of all even integer. In this case we have $2 \in E$ and $-6 \in E$, these are just examples of elements in E. The set E has infinitely many elements.

Special sets

We will use the following sets very often in this course:

- The *empty set* is the set which does not contain an element. It is denoted by $\emptyset$ or by $\{\}$. It is the only set with cardinality 0.
- The set of positive integers

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

- The set of integers

$$\mathbb{Z} = \{\dots, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \dots\}$$

- The set of rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z} \text{ and } b \in \mathbb{N} \right\}.$$

Subsets

Definition 1. *A set S is called a* subset *of a set R if each element of S is an element of R (i.e $x \in S \Rightarrow x \in R$), we then write $S \subseteq R$.*

For any set A, we always have

$$\emptyset \subseteq A \qquad \text{and} \qquad A \subseteq A.$$

If $A \subseteq B$ and $B \neq A$, then we say A is a *proper subset* of B.

Equality of sets: Two sets A and B are equals (and we write $A = B$) if and only if $A \subseteq B$ and $B \subseteq A$. i.e. each element in A is an element of B, and each element in B is an element of A. In brief, we have the equivalence

$$(A = B) \Leftrightarrow (A \subseteq B \text{ and } B \subseteq A).$$

The set of all subsets of a set A is called *power set* of A, and it is denoted by $\mathcal{P}(A)$. In particular the set A and the empty set are elements of $\mathcal{P}(A)$. The cardinality of $|\mathcal{P}(A)| = 2^{|A|}$ for any finite set A.

Exercises 1. *Prove by induction that $|\mathcal{P}(A)| = 2^{|A|}$ for any finite set A.*

Exercises 2. *1) Let A and B be two sets. Show that the following are equivalent:*

(i) $A \subseteq B$.

(ii) If $x \notin B$ then $x \notin A$.

2) Let A, B and C be sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$.

The statements to prove in the above exercises are as important as any parts of the note, you should understand and remember them.

Intersection and union

The *intersection* of two sets A and B are defined by

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

It means that x is an element of $A \cap B$ if and only if $x \in A$ and $x \in B$.

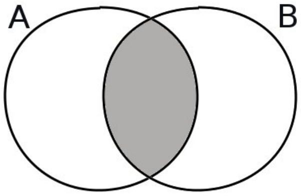


Figure 2.1: The shaded part is $A \cap B$

The *union (or join)* of A and B is

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

It is enough for x to be an element of one of A and B in order to be an element of $A \cup B$.

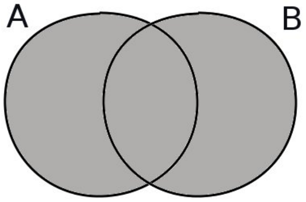


Figure 2.2: In grey is $A \cup B$

Example 1. *If* $A = \{1, 3, 5, 7, 9, 11, 13, 15\}$ *and* $B = \{3, 6, 9, 12, 15, 18\}$*, then we have*

$$A \cap B = \{3, 9, 15\}$$

and

$$A \cup B = \{1, 3, 5, 6, 7, 9, 11, 12, 13, 15, 18\}.$$

The following properties are easy to check, I leave it for you as exercises to prove them: For any sets A, B and C we have

- $(A \cup B) = (B \cup A)$, commutativity of $\cup$,
- $(A \cap B) = (B \cap A)$, commutativity of $\cap$,
- $(A \cup B) \cup C = A \cup (B \cup C)$, associativity of $\cup$,
- $(A \cap B) \cap C = A \cap (B \cap C)$, associativity of $\cap$,
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, distributivity of $\cap$ over $\cup$,

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, distributivity of $\cup$ over $\cap$,
- $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$,
- $A \subseteq (A \cup B)$ and $B \subseteq (A \cup B)$,
- $(A \cap B) \subseteq A$ and $(A \cap B) \subseteq B$,
- $(A \cap B) \subseteq (A \cup B)$.

Definition 2. *A set of subsets $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ of A is a* partition *of A if it satisfies the following:*

(i) $\emptyset \notin \mathcal{A}$.

(ii) $A_1 \cup A_2 \cup \cdots \cup A_n = \displaystyle\bigcup_{i=1}^{n} A_i = A$.

(iii) For any $R, S \in \mathcal{A}$, if $R \neq S$ then $R \cap S = \emptyset$.

Example 2. $\big\{\{a\}, \{b, c, d\}, \{e\}\big\}$ *is a partition of* $\{a, b, c, d, e\}$.

Complement and difference of sets

Let A and B be two sets. The *difference* of a set A and B is

$$A \smallsetminus B = \{x \in A : x \notin B\}.$$

$A \smallsetminus B$ is a set which contains all elements in A which are not in B. Note that the difference is **not commutative**: $A \smallsetminus B$ and $B \smallsetminus A$ are not always the same. For example, if $A = \{0, 2, 4, 6, 8, 10, 12\}$ and $B = \{0, 4, 8, 12, 16, 20\}$ then we have

$$A \smallsetminus B = \{2, 6, 10\} \qquad \text{and} \qquad B \smallsetminus A = \{16, 20\}.$$

When all sets under consideration are considered to be subsets of a given universal set U, then the difference of U and A is called *complement* of A, and denoted simply $\overline{A}$ instead of $U \smallsetminus A$, i.e.

$$\overline{A} = U \smallsetminus A.$$

Some books use the notation A^c for $\overline{A}$.

Theorem 1 (DeMorgan's Theorem)**.** *For any sets A and B, the following relations holds:*

i) $\overline{A \cup B} = \overline{A} \cap \overline{B}$,

ii) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof. For any sets A and B, we have

$$\begin{aligned} x \in \overline{A \cup B} &\iff x \notin A \cup B \\ &\iff \neg(x \in A \cup B) \\ &\iff \neg(x \in A \text{ or } x \in B) \\ &\iff x \notin A \text{ and } x \notin B \\ &\iff x \in \overline{A} \text{ and } x \in \overline{B} \\ &\iff x \in \overline{A} \cap \overline{B}. \end{aligned}$$

The onward implications leads to $\overline{A \cup B} \subseteq \overline{A}\cap\overline{B}$, and the backward implications gives $\overline{A \cup B} \supseteq \overline{A}\cap\overline{B}$. Hence, we obtain $\overline{A \cup B} = \overline{A} \cap \overline{B}$, which proves i).

The proof of ii) is left for you as exercise! □

The *symmetric difference* of A and B is defined by

$$A \triangle B = (A \smallsetminus B) \cup (B \smallsetminus A).$$

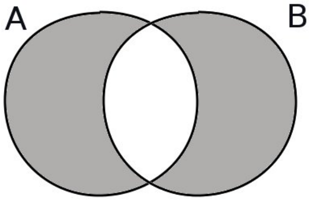


Figure 2.3: In grey is $A \triangle B$

Familiarise yourself with the following properties, by trying to prove them:

- If $A \subseteq B$, then $\overline{B} \subseteq \overline{A}$.
- $A \triangle B = B \triangle A$.
- $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.
- $A \triangle \emptyset = A$.
- $A \triangle A = \emptyset$.
- $A \triangle B = \overline{A} \triangle \overline{B}$. This follows from the fact that $\overline{A} \smallsetminus \overline{B} = B \smallsetminus A$ for any sets A and B.

Cartesian product

The *Cartesian product* $A \times B$ of two sets A and B is defined by

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\},$$

where each of (x, y) is an ordered pair, in a sense that two elements (x, y) and (x', y') in $A \times B$ are equal if and only if $x = x'$ and $y = y'$.

Example 3. *If $A = \{1, b, 3\}$ and $B = \{1, 2, 3, 4, 5, 6\}$, then we have*

$$\begin{aligned} A \times B = \{&(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(b,1),(b,2),(b,3),(b,4),(b,5),\\ &(b,6),(3,1),(3,2),(3,3),(3,4),(3,5),(3,6)\}. \end{aligned}$$

Note that $(1, 3) \neq (3, 1)$.

More generally, we define

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i \text{ for } i = 1, 2 \ldots, n\},$$

We will see more interesting properties of sets along the course. For now, let us discuss mappings.

2.1.2 Mappings

In this section, we describe relationships between sets.

Definition 3. *A mapping f from a set A to a set B is a relationship (rule, correspondence) that assigns to each element x of A a* ***uniquely*** *determined element $f(x)$ of B.*

- *The set A is called the* domain *of the mapping f.*
- *The set B is the* codomain *of f.*
- *$f(x)$ is the image of x.*
- *x is the* antecedent *of $f(x)$.*

We write $f : A \longrightarrow B$ to indicate that f is a mapping from A to B.
Mappings can be represented by diagrams, for example

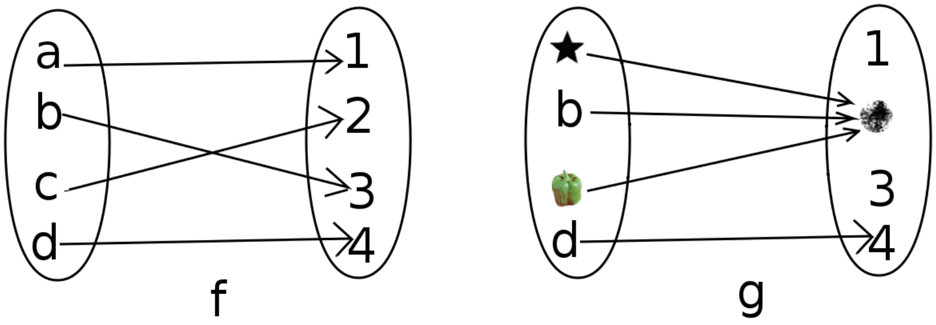


Figure 2.4: f is a mapping, where $f(a) = 1, f(b) = 3, f(c) = 2, f(d) = 4$. g is also a mapping, where $g(a) = g(b) = g(c) = 2$ and $g(d) = 4$.

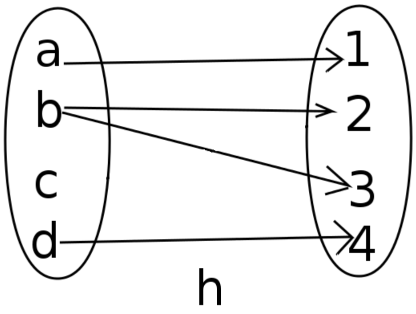


Figure 2.5: But, this is not a mapping, $h(b)$ would not be unique!

If one of the domain and codomain is a large set, then it is not practical anymore to draw a diagram for a mapping. A (very common) alternative way, is to describe how to find the image, say $f(x)$, for each given x: provide a formula relating $f(x)$ to x. For example, we can write

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ x &\longmapsto f(x) = x^2 \end{aligned}$$

to describe the mapping which associates an integer to its square: 1 to 1, 2 to 4, 3 to 9 . . . .

Definition 4. *Two mappings $f : A \longrightarrow B$ and $g : C \longrightarrow D$ are equal if and only if the following three conditions hold:*

(i) The domain of f is equal to the domain of g, i.e $A = C$ (equality of sets).

(ii) f and g have the same codomain, i.e. $B = D$.

(iii) For any $x \in A$ we have $f(x) = g(x)$.

For example, let us take

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto f(x) = x^2 + 1 \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathbb{Z} &\longrightarrow \mathbb{N} \\ x &\longmapsto g(x) = x^2 + 1. \end{aligned}$$

The two functions f and g have the same domain $\mathbb{Z}$. So, condition (i) is satisfied. For any x in their domain $\mathbb{Z}$, we will always have $f(x) = g(x) = x^2 + 1$. This means that condition (iii) is satisfied. But, since the codomain of f is $\mathbb{Z}$, and it is different to the codomain of g which is $\mathbb{N}$, we conclude that the two mappings f and G are different.

Special functions

The following types of function will often be encountered in this course:

(i) The *identity mapping* on a set A, denoted by Id_A, is defined by

$$\begin{aligned} \mathrm{Id}_A : A &\longrightarrow A \\ x &\longmapsto \mathrm{Id}_A(x) = x. \end{aligned}$$

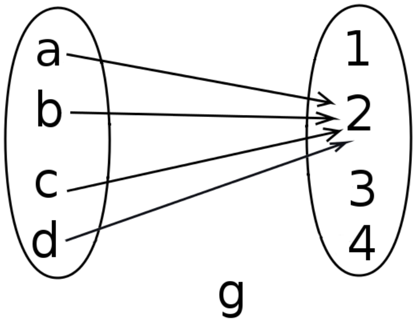
Any element x of A is being associated to itself: $\mathrm{Id}_A(x) = x$.

We simply write Id instead of Id_A if it is clear which set is being considered.

(ii) *Constant functions:* Let $y_0 \in B$. A mapping f defined by

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longmapsto f(x) = y_0, \end{aligned}$$

is a constant function. All the elements of A has the same image y_0 under f. For example, the following mapping g is a constant mapping where $g(a) = g(b) = g(c) = g(d) = 2$:



(iii) A mapping $f : A \longrightarrow B$ is said to be *one-to-one* or an *injection* if

$$x_1 \neq x_2 \qquad \text{implies} \qquad f(x_1) \neq f(x_2) \qquad (x_1, x_2 \in A), \tag{2.1}$$

that is, if any two different elements of A have different images.

Note that condition (2.1) is equivalent to

$$f(x_1) = f(x_2) \qquad \text{implies} \qquad x_1 = x_2 \qquad (x_1, x_2 \in A).$$

Example 4. *The mapping*

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto f(x) = 3x + 6 \end{aligned}$$

is one-to one because for $x_1, x_2 \in \mathbb{Z}$ we have

$$\begin{aligned} f(x_1) = f(x_2) &\Longrightarrow 3x_1 + 6 = 3x_2 + 6 \\ &\Longrightarrow 3x_1 + 6 - 6 = 3x_2 + 6 - 6 \\ &\Longrightarrow 3x_1 = 3x_2 \\ &\Longrightarrow \frac{3x_1}{3} = \frac{3x_2}{3} \\ &\Longrightarrow x_1 = x_2. \end{aligned}$$

But

$$\begin{aligned} g : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto g(x) = x^2 \end{aligned}$$

is not a one-to-one mapping, just because $-1 \neq 1$ and $g(1) = 1 = g(-1)$.

iv) A mapping $f : A \longrightarrow B$ is said to be *onto* or a *surjection* if

$$\forall y \in B, \exists x \in A \qquad \text{such that} \qquad f(x) = y.$$

In other words, any element in B has an antecedent under f.

Example 5. *The mapping*

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto f(x) = x^2 \end{aligned}$$

is not onto. Because for any $x \in \mathbb{Z}$ we have $f(x) = x^2 \geq 0$, and thus any negative number such as -1 does not have antecedent under f.

But

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = -2x + 1 \end{aligned}$$

is onto: for any $y \in \mathbb{R}$ we can always find an antecedent which is $x = -\frac{y-1}{2} \in \mathbb{R}$. Because by definition of f we have

$$f\left(-\frac{y-1}{2}\right) = -2\left(-\frac{y-1}{2}\right) + 1 = y - 1 + 1 = y.$$

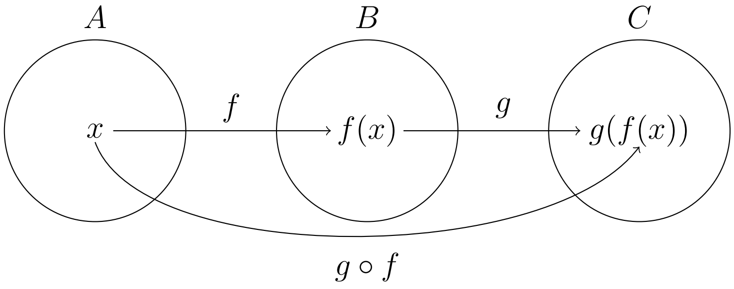
v) A mapping which is one-to-one and onto are called a bijection.

Composite mappings

Definition 5. *Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be two functions. The* composition *(or* composite*) $g \circ f$ of f and g is defined by*

$$\begin{aligned} g \circ f : A &\longrightarrow C \\ x &\longmapsto (g \circ f)(x) = g(f(x)). \end{aligned}$$

Note that, $g(f(x))$ is well defined because the codomain of f coincide with the domain of g.



Example 6. *If*

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{N} \\ n &\longmapsto f(n) = n^2 \end{aligned} \qquad \textit{and} \qquad \begin{aligned} g : \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto g(n) = 3n + 2 \end{aligned}$$

then we have

$$\begin{aligned} g \circ f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto (g \circ f)(n) = g(f(n)) = g(n^2) = 3n^2 + 2. \end{aligned}$$

The following exercises are on important properties of composition of mappings. I provide a solution for the first one to give you some ideas on how to do the remaining three:

Exercises 3. *Assume that $f : A \longrightarrow B$ and $g : B \longrightarrow C$. Show that the following statements hold:*

(i) *If f and g are onto, then $g \circ f$ is onto.*

Solution: *Assume that f and g are onto. This means that*

$$\forall y \in B, \exists x \in A \textit{ such that } f(x) = y$$

and

$$\forall z \in C, \exists y \in B \textit{ such that } g(y) = z.$$

What we want to prove is that

$$\forall z \in C, \exists x \in A \textit{ such that } (g \circ f)(x) = z.$$

So, let $z \in C$. Because g is onto, there exists $y \in B$ such that $g(y) = z$. Furthermore, because f is onto, there exists $x \in A$ such that $f(x) = y$. Therefore we have

$$g(y) = z \Longrightarrow g(f(x)) = z \Longrightarrow (g \circ f)(x) = z.$$

Hence $g \circ f$ is onto.

(ii) If $g \circ f$ is onto , then g is onto.

(iii) If f and g are one-to-one, then $g \circ f$ is one-to-one.

iv) $g \circ f$ is one-to-one, then f is one-to-one.

Definition 6. *A mapping $f : A \longrightarrow B$ is an* inverse *of $g : B \longrightarrow A$ if $f \circ g = \mathrm{Id}_B$ and $g \circ f = \mathrm{Id}_A$. We then write $f = g^{-1}$ or $g = f^{-1}$. And we say that a mapping is* invertible *if it has an inverse.*

Theorem 2. *A mapping is invertible if and only if it is a bijection (i.e. one-to-one and onto).*

Proof. Assume that a mapping $f : A \longrightarrow B$ is invertible, and let $g : B \longrightarrow A$ be its inverse. Then by definition of invertible mapping, we know that $f \circ g = \mathrm{Id}_B$ and $g \circ f = \mathrm{Id}_A$.

First we show that f is onto: For any $y \in B$ we have

$$y = \mathrm{Id}_B(y) = (f \circ g)(y) = f(g(y)),$$

where $g(y) \in A$. The antecedent of y with respect to f is $g(y)$, this is for all $y \in B$, hence f is onto.

Next we show that f is one-to-one: Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. Then we have

$$\begin{aligned} f(x_1) = f(x_2) &\Longrightarrow g(f(x_1)) = g(f(x_2)) \\ &\Longrightarrow (g \circ f)(x_1) = (g \circ f)(x_2) \\ &\Longrightarrow \mathrm{Id}_A(x_1) = \mathrm{Id}_A(x_2) \\ &\Longrightarrow x_1 = x_2. \end{aligned}$$

Hence f is a one-to-one mapping.

Now we assume that $f : A \longrightarrow B$ is onto and one-to-one. To show that f is invertible, we are going to describe its inverse.

Note that, since f is onto, any $y \in B$ can be written as $f(x)$ for some $x \in A$.

Let $g : B \longrightarrow A$ be a mapping defined as follows: For any $y = f(x)$ in B, $g(y) = g(f(x)) = x$. The image x of y by g is unique because f is one-to-one. Hence g is well-defined. Moreover, for any $u \in A$ and for any $y = f(x) \in B$ we have

$$(g \circ f)(u) = g(f(u)) = u = \mathrm{Id}_A(u)$$

and

$$(f \circ g)(y) = f(g(y)) = f(g(f(x))) = f(x) = y = \mathrm{Id}_B(y).$$

These means that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_b$. □

2.2 Binary operations

Binary operations are not completely new for us, we have seen many of them in previous studies: The addition and multiplication of integers or real numbers are among them. Both addition and multiplication consist of taking two integers, say n and m, and then associate a unique integer to them. In this section, we study operation in a more general setting.

Definition 7. *A* binary operation *on a set A is a rule (law) that assigns to each ordered pair of elements of A a uniquely determined element of A.*

In other words, an operation $\star$ on a set A can be viewed as a mapping

$$\begin{aligned}\star : A\times A &\longmapsto A\\ (x,y) &\longmapsto \star((x,y)).\end{aligned}$$

Taking an ordered pair of elements of A amounts to take an element of the Cartesian product $A\times A$.

If $\star$ is a binary operation, then instead of writing $\star((x,y))$ we write $x\star y$.

Example 7. *The usual* addition *"$+$" is a binary operation on each of the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.*

The usual subtraction *"$-$" is a binary operation on each of the sets $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$. But it is not a binary operation on the set $\mathbb{N}$. Because the difference of two positive integers is not always a positive integer: For instance $1-3=-2\notin\mathbb{N}$.*

The usual division "$\div$" is a binary operation on each of the sets $\mathbb{Q}\smallsetminus\{0\}$ and $\mathbb{R}\smallsetminus\{0\}$.

Example 8. *Let A be a set. We know that for any two subsets B and C of A, each of $B\cap C$ and $B\cup C$ are again subsets of A, and they are uniquely defined. Hence, the* intersection *"$\cap$" is a binary operation on the power set $\mathcal{P}(A)$. Similarly, the* union *"$\cup$" is a binary operation on $\mathcal{P}(A)$.*

Example 9. *Let A be a set, and let $\mathcal{S}_A$ be the set of all bijections from A to A. Then the* composition of mappings *"$\circ$" is a binary operation on $\mathcal{S}_A$: For any two bijections $f:A\longrightarrow A$ and $g:A\longrightarrow A$, the composition $(f\circ g):A\longrightarrow A$ is an element of $\mathcal{S}_A$, and it is unique.*

Let $*$ be a binary operation in B. Let $\mathcal{S}_{A,B}$ be the set of all mappings from A to B. Then we can have a binary operation $\circledast$ on $\mathcal{S}_{A,B}$ defined as follows: For any f and g in $\mathcal{S}_{A,B}$ we have

$$\begin{aligned}(f\circledast g): A &\longrightarrow B\\ x &\longmapsto (f\circledast g)(x)=f(x)*g(x).\end{aligned}$$

Definition 8. *Let $*$ be a binary operation on A.*

We say that $*$ is commutative *if*

$$x*y=y*x$$

for any $x,y\in A$.

$*$ is associative *if*

$$(x*y)*z=x*(y*z)$$

for any $x,y,z\in A$.

The addition "$+$" on $\mathbb{Z}$ is commutative and associative.

The subtraction on $\mathbb{Z}$ is not associative, and it is not commutative: We can find integers m and n such that $m-n\neq n-m$, for example if we take $m=1$ and $n=3$ we have $1-3=-2\neq 2=3-1$.

The division on $\mathbb{Q}\smallsetminus\{0\}$ is also not commutative.

The set difference "$\smallsetminus$ " is a binary operation on the power set $\mathcal{P}(A)$, for any given set A. But "$\smallsetminus$ " is **not** commutative and it is **not** associative: For example if we take $S=\{a,b\}, R=\{a\}$ and $P=\{b\}$, then we have

$$R\smallsetminus S=\emptyset\neq P=S\smallsetminus R,$$

and

$$(S\smallsetminus R)\smallsetminus P=\{b\}\smallsetminus P=\emptyset\neq\{b\}=S\smallsetminus R=S\smallsetminus(R\smallsetminus P).$$

2.3 Equivalence relation and order

Definition 9. *Given two sets A and B, a* (binary) relation *from A to B is a subset of $A \times B$.*

We are more interested in the case where $A = B$, in which case $\mathcal{R}$ is called a relation on A. Instead of writing $(x, y) \in \mathcal{R}$, we write $x\mathcal{R}y$.

Example 10. *The usual equality "$=$" is a relation on $\mathbb{R}$. Let us denote it by $\mathcal{R}_=$, then we have*

$$\mathcal{R}_= = \{(x, x) : x \in \mathbb{R}\}.$$

The usual inequality "$\leq$" (smaller or equal to) is a relation on $\mathbb{Z}$. For convenience, let denote the relation as $\mathcal{R}_\leq$, then we have

$$\mathcal{R}_\leq = \{(n, n+m) : n \in \mathbb{Z}, m \in \mathbb{N} \cup \{0\}\}.$$

Example 11. *To any mapping $f : A \longrightarrow A$ we can associate a relation $\mathcal{R}_f$ defined by*

$$\mathcal{R}_f = \{(x, f(x)) : x \in A\}.$$

2.3.1 Order

A special type of binary relation that we are interested in is the order.

Definition 10. *A binary relation $\mathcal{R}$ on a set A is a* partial order *if it satisfies the following conditions:*

(i) ***Reflexivity:*** *for any $x \in A$ we have $x\mathcal{R}x$.*

(ii) ***Antisymmetry:*** *for all $x, y \in A$ if $x\mathcal{R}y$ and $y\mathcal{R}x$ then $x = y$.*

(iii) ***Transitivity:****for all $x, y, z \in A$ if $x\mathcal{R}y$ and $y\mathcal{R}z$ then $x\mathcal{R}z$.*

We say that $(A, \mathcal{R})$ is a partially ordered *set.*

Definition 11. *If $(A, \mathcal{R})$ is a partially ordered set, we say that $(A, \mathcal{R})$ is a* totally ordered *set (and $\mathcal{R}$ is a* total order *on A) provided that for all $x, y \in A$ we have*

$$x\mathcal{R}y \qquad \text{or} \qquad y\mathcal{R}x,$$

i.e any two elements in A can be compared using $\mathcal{R}$.

Exercises 4. *Show that if $(A, \mathcal{R})$ is a totally ordered set and $B \subseteq A$, then $(B, \mathcal{R})$ is also a totally ordered set.*

Exercises 5. *Show that the relation $\mathcal{R}$ on $\mathbb{N}$ defined for all $x, y \in \mathbb{N}$ by*

$$x\mathcal{R}y \Leftrightarrow x|y$$

is a partial order, and it is not a total order.

Exercises 6 (Squeezing)**.** *Let $\preccurlyeq$ be an order on a set A, and $x, y, z \in A$. If $x \preccurlyeq y \preccurlyeq z \preccurlyeq x$, then $y = z$.*

The usual inequality "$\leq$" is a total order in $\mathbb{N}$ (check the **four** conditions).

We end this subsection by discussing properties of the totally ordered set $(\mathbb{N}, \leq)$, they are useful in algebra:

- **Archimedean property (AP) of real numbers and integers:**

There are several equivalent forms of the AP, we only look at few of them.

Theorem 3 (AP of real numbers)**.** *For any real $a > 0$ and any $b > 0$, there is a positive integer such that $na > b$.*

The AP of integers is a particular case of Theorem 3:

Proposition 1 (AP of integers)**.** *Given $a, b \in \mathbb{N}$, there is a positive integer n such that $na > b$.*

Clearly any integer larger than $\frac{b}{a}$ would do, because

$$n > \frac{b}{a} \Rightarrow na > b.$$

But how do we know that there is always such an integer. This leads to another form of the AP of real numbers:

Proposition 2. *Let c be a real number, then there exist an integer n such that $n > c$.*

Theorem 3 implies Proposition 2, because we can just apply Theorem 3 to $a = 1$ and $b = c$ to obtain Proposition 2.

We can also obtain Theorem 3 by applying Proposition 2 to $c = \frac{b}{a}$. Since $n > \frac{b}{a} \Rightarrow na > b$.

Hence Theorem 3 and Proposition 2 are equivalent.

The following other form of AP of real numbers also looks like a particular case of Theorem 3 where we take $a = \epsilon$ and $b = 1$, but in fact the two propositions are again equivalent (take $\epsilon = \frac{a}{b}$).

Proposition 3 (AP of real numbers)**.** *For any real $\epsilon > 0$, there is a positive integer such that $n\epsilon > 1$.*

2.3.2 Equivalence relations

Equivalence relations are special type of binary relation, it plays important roles in the study of algebraic structure, which is the focus of this course.

Definition 12. *An* equivalence relation *$\mathcal{R}$ on a set A is any relation on A which satisfies the following properties:*

(i) For any $x \in A$ we have $x\mathcal{R}x$ *(This means that $\mathcal{R}$ is reflexive)*

(ii) For any $x, y \in A$, if $x\mathcal{R}y$ then $y\mathcal{R}x$ *(i.e. $\mathcal{R}$ is symmetric)*

(iii) For any $x, y, z \in A$, if $x\mathcal{R}y$ and $y\mathcal{R}z$ then $x\mathcal{R}z$ *($\mathcal{R}$ is transitive).*

Exercises 7.

- *Check that the relation $\mathcal{R}_=$ defined above is an equivalence relations, while $\mathcal{R}_\leq$ is not an equivalence relation.*
- *Let k be an integer, and let $\mathcal{R}_k$ be a relation on $\mathbb{Z}$ defined as follows: for any $x, y \in \mathbb{Z}$, $x\mathcal{R}_k y$ if and only if k divides $x - y$. Show that $\mathcal{R}_k$ is an equivalence relation on $\mathbb{Z}$.*

If $\mathcal{R}$ is an equivalence relation on A and $x \in A$, then the set

$$[x]_{\mathcal{R}} = \{y \in A : x\mathcal{R}y\}$$

is called *equivalence class* of x (relative to $\mathcal{R}$). Since for any $x \in A$ we have $x\mathcal{R}x$ (reflexivity), we also have $x \in [x]_{\mathcal{R}}$. In particular, we have

$$\bigcup_{x\in A} [a]_{\mathcal{R}} = A \tag{2.2}$$

Example 12.

- *Consider the relation $\mathcal{R}$ on $\mathbb{Z}$ defined by $n\mathcal{R}m$ if and only if n divides m. This relation is* **not** *and equivalence relation. This is because it is not symmetrict $2\mathcal{R}4$ but $4 \not\mathcal{R} 2$.*
- *Now consider the relation $\mathcal{R}'$ defined on $\mathbb{Z}$ as follows:*

  $$n\mathcal{R}'m \Leftrightarrow n + m \textit{ is an even integer.}$$

  $\mathcal{R}'$ is an equivalence relation. Check that it satisfies the three required properties. Determine the equivalence classes.

Proposition 4 (Equivalence classes are disjoint or equal.)**.** *Let $\mathcal{R}$ be an equivalence relation on a set A, and let x_1 and x_2 be two elements of A. Then, there are two possible cases:*

(i) If $x_1\mathcal{R}x_2$, then we have $[x_1]_{\mathcal{R}} = [x_2]_{\mathcal{R}}$.

(ii) Otherwise (if ***not*** *$x_1\mathcal{R}x_2$), then $[x_1]_{\mathcal{R}}$ and $[x_2]_{\mathcal{R}}$ are disjoint:*

$$[x_1]_{\mathcal{R}} \cap [x_2]_{\mathcal{R}} = \emptyset.$$

Proof. Assume that $x_1\mathcal{R}x_2$. For any $x \in [x_1]_{\mathcal{R}}$, we have $x_1\mathcal{R}x$ (by definition of equivalence class). Since $\mathcal{R}$ is an equivalence relation (see definition), we have

$$x_1\mathcal{R}x \Leftrightarrow x\mathcal{R}x_1 \qquad \text{(by symmetry)}$$

and

$$\begin{aligned} x\mathcal{R}x_1 \text{ and } x_1\mathcal{R}x_2 &\Rightarrow x\mathcal{R}x_2 \qquad \text{(by transitivity)} \\ &\Rightarrow x_2\mathcal{R}x \\ &\Rightarrow x \in [x_2]_{\mathcal{R}}. \end{aligned}$$

This means that $[x_1]_{\mathcal{R}} \subseteq [x_2]_{\mathcal{R}}$.

By similar way, we can also prove that $[x_2]_{\mathcal{R}} \subseteq [x_1]_{\mathcal{R}}$ (do it as exercise). Then

$$[x_1]_{\mathcal{R}} \subseteq [x_2]_{\mathcal{R}} \text{ and } [x_2]_{\mathcal{R}} \subseteq [x_1]_{\mathcal{R}} \Rightarrow [x_2]_{\mathcal{R}} = [x_1]_{\mathcal{R}}.$$

This ends the proof of (i).

Now assume that x_1 is not related to x_2 by $\mathcal{R}$ (i.e not $x_1\mathcal{R}x_2$). We reason by contradiction and assume that $[x_1]_{\mathcal{R}} \cap [x_2]_{\mathcal{R}} \neq \emptyset$ and $x \in [x_1]_{\mathcal{R}} \cap [x_2]_{\mathcal{R}} \neq \emptyset$. Then, we would have $x_1\mathcal{R}x$ and $x_2\mathcal{R}x$. By symmetry $x_2\mathcal{R}x$ implies $x\mathcal{R}x_2$, and by transitivity

$$x_1\mathcal{R}x \text{ and } x\mathcal{R}x_2 \Rightarrow x_1\mathcal{R}x_2.$$

But, this is in contradiction with the above assumption. Hence, we deduce that $[x_1]_{\mathcal{R}} \cap [x_2]_{\mathcal{R}} = \emptyset$. □

Equation (2.2) and Proposition 4 mean that

$$\{[x]_{\mathcal{R}} : x \in A\}$$

forms a partition of A.

In fact, whenever we have a partition $\mathcal{P}$ of A, we can always find an equivalence relation such that the elements of the partition are the equivalence classes:

Exercises 8. *Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a partition of A. Show that the binary operation $\mathcal{R}$, defined by*

$$x\mathcal{R}y \Leftrightarrow \exists i \in \{1, 2, \ldots, n\}, x \in P_i \text{ and } y \in P_i$$

for any $x, y \in A$, is an equivalence relation.

2.4 Congruence relation (in $\mathbb{Z}$)

The set

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

of **integers**, will often be used to illustrate algebraic properties studied in this course. In this section we review basic arithmetic in $\mathbb{Z}$, including order, division and congruence relation.

Divisibility

Definition 13. *Let n and m be two integers. We say that m is* divisible *by n (or n* divides *m, or m is a* multiple *of n, or n is a* factor *of m) if there exists an* ***integer*** *q such that $m = nq$.*

We write $n|m$ if n divides m, and $n \not| m$ if n does not divide m.

The following properties of $|$ are noteworthy:

- For any $n \in \mathbb{Z}$ we have $n|n$, because $n = n \times 1$.
- If $n|m$, then $n|(-m)$, because $m = nq \Rightarrow -m = n(-q)$ and q being integer implies that $-q$ is also an integer.
- If $n|m_1$ and $n|m_2$, then $m|(am_1 + bm_2)$ for any integers a and b. This follows from the fact that $m_1 = nq_1$ and $m_2 = nq_2$ implies that $am_1 + bm_2 = n(aq_1 + bq_2)$, and $aq_1 + bq_2$ is an integer if q_1 and q_2 are integers.
- If $n|m$ and $m \neq 0$, then we must have $|n| \leq |m|$. This is because if q is such that $m = qn$, then $q \neq 0$, hence $|q| \geq 1$ and thus $|m| = |q||n| \geq |n|$.

Under Definition 13, any integer n divides 0, because $0 = 0n$.

Theorem 4 (**Division Algorithm**). *If n and m are integers with $m > 0$, then there exist integers q and r such that*

$$n = mq + r \qquad \text{with } 0 \leq r < m.$$

Moreover, q and r are unique: If $n = mq' + r'$ for some integers q' and $0 \leq r' < m$, then we must have $q = q'$ and $r = r'$.

We say that q is the quotient *and r is the* reminder *in the division of n by m.*

Examples: If we divide 13 and -13 by 5 we have

$$13 = 5 \times 2 + 3 \qquad \text{and} \qquad -13 = 5 \times (-3) + 2.$$

Congruence relation

Definition 14. *Let d be a **positive** integer. Two integers n and m are said to be congruent modulo d if $d|(n-m)$. We then write $n \equiv m \mod (d)$.*

For instance, $8 \equiv 3 \mod (5)$, $41 \equiv 1 \mod (8)$ and $41 \equiv 1 \mod (5)$.

$n \equiv m \mod (d)$ means that $d|(n-m)$, which in turn means that $n = m + kd$ for some integer k. Thus the set of all integers congruent modulo d with n is

$$[n]_d = \{n + kd : k \in \mathbb{Z}\} = \{\dots, n-3d, n-2d, n-d, n, n+d, n+2d, n+3d, \dots\}.$$

Sometime we write $\overline{n}$ instead of $[n]_d$, if there is no risk of confusion. In the notation $\overline{n}$, n can be replaced by any element of $\overline{n}$.

Choose a positive integer d, then the congruence relation modulo d satisfies the following properties for any integers n, m, l:

(i) **Reflexivity:** $m \equiv m \mod (d)$, because $d|(m-m)$ (any integer divides $m - m = 0$).

(ii) **Symmetry:** If $n \equiv m \mod (d)$, then we have $m \equiv n \mod (d)$. This is because

$$\begin{aligned} d|(n-m) &\Rightarrow d|(-(n-m)) \\ &\Rightarrow d|(m-n). \end{aligned}$$

(ii) **Transitivity:** If $n \equiv m \mod (d)$ and $m \equiv l \mod (d)$ then we have $n \equiv l \mod (d)$, because

$$\begin{aligned} d|(n-m) \text{ and } d|(m-l) &\Rightarrow d|((n-m)+(m-l) \\ &\Rightarrow d|(n-m+m-l) \\ &\Rightarrow d|(n-l). \end{aligned}$$

(iv) From (i), (ii) and (iii) we deduce that the congruence relation modulo d (for any given integer d) is an **equivalence relation** on $\mathbb{Z}$.

The equivalence classes for this equivalence relation are called *congruence classes modulo d*, or *residue classes modulo d*. The congruence class modulo d of n is $[n]_d$.

Remark 1. *If $[n]_d \neq [m]_d$, then $[n]_d \cap [m]_d = \emptyset$, because $[n]_d$ and $[m]_d$ are equivalence classes (see Proposition 4).*

Proposition 5. *For any integer d there are exactly d congruence class modulo d, and they are $[0]_d, [1]_d, [2]_d, \dots, [d-1]_d$.*

Proof. First, we show that $[0]_d, [1]_d, [2]_d, \dots, [d-1]_d$ are the only possible congruence classes modulo d. For this we need to show that $[0]_d \cup [1]_d \cup [2]_d \cup \dots \cup [d-1]_d = \mathbb{Z}$. It is clear that

$$[0]_d \cup [1]_d \cup [2]_d \cup \dots \cup [d-1]_d \subseteq \mathbb{Z}.$$

Let n be an integer. Then, by the Division Algorithm, $n = dq + r$ for some integers q and r such that $0 \leq r < d$. Hence $d|(n-r)$, meaning that $n \in [r]_d \subseteq [0]_d \cup [1]_d \cup [2]_d \cup \dots \cup [d-1]_d$.

Next, we show that $[0]_d, [1]_d, [2]_d, \dots, [d-1]_d$ are pairwise different. Let $r, r' \in \{0, 1, \dots, r-1\}$ such that $r < r'$. If by contradiction we assume that $[r]_d = [r']_d$, then we would have $r' \equiv r \mod (d)$ and $d|(r'-r)$. This is impossible because $0 < r' - r \leq r' < d$. Thus, we must have $[r]_d \neq [r']_d$. □

We define

$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, [1]_d, [2]_d, \ldots, [d-1]_d\} = \{\overline{0}, \overline{1}, \ldots, \overline{d-1}\}.$$

(v) If $n_1 \equiv m_1 \mod (d)$ and $n_2 \equiv m_2 \mod (d)$ then

$$n_1 + n_2 \equiv m_1 + m_2 \mod (d) \qquad \text{and} \qquad n_1 n_2 \equiv m_1 m_2 \mod (d).$$

Proof. If $n_1 \equiv m_1 \mod (d)$ and $n_2 \equiv m_2 \mod (d)$, then $n_1 - m_1 = k_1 d$ and $n_2 - m_2 = k_2 d$ for some integers k_1 and k_2. Thus we have

$$(n_1 + n_2) - (m_1 + m_2) = n_1 - m_1 + n_2 - m_2 = k_1 d + k_2 d = (k_1 + k_2)d,$$

which means that $n_1 + n_2 \equiv m_1 + m_2 \mod (d)$.

Similarly, we also have

$$n_1 n_2 = (m_1 + k_1 d)(m_2 + k_2 d) = m_1 m_2 + m_1 k_2 d + k_1 d m_2 + k_1 d k_2 d = m_1 m_2 + (m_1 k_2 + k_1 m_2 + k_1 d k_2)d$$

which implies

$$n_1 n_2 - m_1 m_2 = (m_1 k_2 + k_1 m_2 + k_1 d k_2)d$$

and thus $n_1 n_2 \equiv m_1 m_2 \mod (d)$. □

Property (v) implies that we can have the following well-defined addition and multiplication in $\mathbb{Z}/d\mathbb{Z}$: The operations

$$\begin{aligned} + : \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} &\longrightarrow \mathbb{Z}/d\mathbb{Z} \\ ([n]_d, [m]_d) &\longmapsto [n]_d + [m]_d = [n+m]_d \end{aligned}$$

and

$$\begin{aligned} \cdot : \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z} &\longrightarrow \mathbb{Z}/d\mathbb{Z} \\ ([n]_d, [m]_d) &\longmapsto [n]_d \cdot [m]_d = [n \cdot m]_d \end{aligned}$$

are well defined. Because, whenever $[n_1]_d = [n_2]_d$ and $[m_1]_d = [m_2]_d$, we always have $[n_1 + m_1]_d = [n_2 + m_2]_d$ and $[n_1 \cdot m_1]_d = [n_2 \cdot m_2]_d$.

Using the notation $\overline{n}$, these give

$$\overline{n} + \overline{m} = \overline{n+m} \qquad \text{and} \qquad \overline{n} \cdot \overline{m} = \overline{n \cdot m}.$$

We will see some uses of these two operations in the next section.

2.5 Group

We are now ready to introduce the notion of group theory. Group theory is among the central concept in modern mathematics. Loosely speaking, a group is a set together with an operation which satisfies certain properties.

2.5.1 Definition and examples

Definition 15. *A* group *is a pair $(G,\star)$ consisting of nonempty set G and a binary operation*

$$\begin{aligned}\star : G\times G &\longrightarrow G\\ (a,b) &\longmapsto a\star b\end{aligned}$$

satisfying

(i) ***Associativity:*** $(a\star b)\star c = a\star(b\star c)$ *for all* $a,b,c\in G$.

(ii) ***Existence of identity:*** *There exists an element* $e\in G$*, called the* identity*, such that*

$$e\star a = a\star e = a$$

for all $a\in G$.

(iii) ***Existence of inverse:*** *For any* $a\in G$*, there exists* $b\in G$ *such that*

$$a\star b = b\star a = e.$$

We write $b=a^{-1}$.

If furthermore $a\star b = b\star a$ *for all* $a,b\in G$ *(i.e "$\star$" is* ***commutative****), we say G is an* abelian group*.*

Example 13. $(\mathbb{Z},+)$*, where "+" is the usual addition, is an abelian group:*

- *We know that if n and m are integers then $n+m$ are also integers, and $(n+m)+l = n+(m+l)$ for any integers n,m and l.*
- *The identity element in $(\mathbb{Z},+)$ is 0, since $n+0=0+n=n$ for any $n\in\mathbb{N}$.*
- *The inverse of any integer n is $-n$, because $n+(-n)=(-n)+n=0$ for any $n\in\mathbb{Z}$.*
- *We know that $n+m=m+n$ for any $n,m\in\mathbb{Z}$.*

$(\mathbb{Q}\smallsetminus\{0\},\times)$ *is also an abelian group (where "×" is the usual multiplication). Check if it satisfies the three conditions.*

But each of $(\mathbb{Q},\times),(\mathbb{Z},\times),(\mathbb{Z}\smallsetminus\{0\},\times)$ and $(\mathbb{N},+)$ is not a group. Check why.

Example 14. *Let $\mathbb{I}_n=\{1,2,3,\ldots,n-1\}$. Define an operation*

$$\begin{aligned}\oplus : \mathbb{I}_n\times\mathbb{I}_n : &\longrightarrow \mathbb{I}_n\\ (h,\ell) &\longmapsto h\oplus\ell = \begin{cases} h+\ell & \text{if } h+\ell<n\\ h+\ell-n & \text{if } h+\ell\geq n.\end{cases}\end{aligned}$$

Then $(\mathbb{I}_n,\oplus)$ is an abelian group. It is easy to check that $\oplus$ is an operation on $\mathbb{I}_n$, and it is commutative.

- *Associativity(we have seen this in Tutorial 2): For any $i,j,k\in\mathbb{I}_n$ we have the following three cases:*

- *If $i+j+k<n$, then we must also have $i+j<n$ and $j+k<n$, and hence*

  $$(i \oplus j) \oplus k = (i+j) \oplus k = (i+j)+k = i+j+k = i+(j+k) = i \oplus (j+k) = i \oplus (j \oplus k).$$

- *Assume that $n \leq i+j+k < 2n$, which implies $i+j+k-n<n$. Then for $i+j<n$ we have*

  $$(i \oplus j) \oplus k = (i+j) \oplus k = i+j+k-n,$$

  and for $i+j \geq n$ we have

  $$(i \oplus j) \oplus k = (i+j-n) \oplus k = i+j+k-n.$$

  Similarly, for $j+k<n$ we have

  $$i \oplus (j \oplus k) = i \oplus (j+k) = i+j+k-n,$$

  and for $j+k \geq n$ we have

  $$i \oplus (j \oplus k) = i \oplus (j+k-n) = i+j+k-n.$$

  Therefore in all cases we have $(i \oplus j) \oplus k = i+j+k-n = i \oplus (j \oplus k)$.

- *If $i+j+k \geq 2n$ which implies $i+j+k-n \geq n$, then it is impossible to have $i+j<n$ or $j+k<n$ because it would lead to $i+j+k<2n$ given that $i,j,k<n$. Hence, we must have $i+j \geq n$ and $j+k \geq n$ and thus*

  $$(i \oplus j) \oplus k = (i+j-n) \oplus k = (i+j-n)+k-n = i+j+k-2n$$

  and

  $$i \oplus (j \oplus k) = i \oplus (j+k-n) = i+j+k-n-n = i+j+k-2n.$$

- *For any $i \in \mathbb{I}_n$ we have $0+i<n$ and hence $0 \oplus i = i \oplus 0 = 0+i = i$. this means that 0 is the identity in $(\mathbb{I}_n, \oplus)$.*

- *For any $i \in \mathbb{I}_n \smallsetminus \{0\}$ we have $i \oplus (n-i) = i+(n-i)-n = 0$ (note that $i+(n-i)=n \geq n$). This means that Any element i of $\mathbb{I}_n \smallsetminus \{0\}$ has an inverse which is $n-i$, and the inverse of 0 is of course 0 because $0 \oplus 0 = 0+0 = 0$.*

Exercises 9. *Let A be a set. Check if any of $(\mathcal{P}(A), \smallsetminus)$, $(\mathcal{P}(A), \cap)$ and $(\mathcal{P}(A), \cup)$ is a group.*

If $(G, \star)$ is a group, then the cardinality $|G|$ of G is called the *order* of $(G, \star)$.

2.5.2 The group $\mathbb{Z}/d\mathbb{Z}$

We have seen from Chapter 2.5 that

$$\begin{aligned} + : (\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/d\mathbb{Z}) &\longrightarrow \mathbb{Z}/d\mathbb{Z} \\ (\overline{n}, \overline{m}) &\longmapsto \overline{n} + \overline{m} = \overline{n+m} \end{aligned}$$

is a well-defined operation in $\mathbb{Z}/d\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{d-1}\}$. In fact $(\mathbb{Z}/d\mathbb{Z}, +)$ is a group. For simplicity, we use the abbreviation $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$.

- Associativity follows from the associativity of the addition in $\mathbb{Z}$ as follows: For any $\overline{i}, \overline{j}, \overline{k} \in \mathbb{Z}_d$ we have

$$\overline{i} + (\overline{j} + \overline{k}) = \overline{i} + (\overline{j + k}) = \overline{i + j + k}$$

  and

$$(\overline{i} + \overline{j}) + \overline{k} = (\overline{i + j}) + \overline{k} = \overline{i + j + k}.$$

- The identity element is $\overline{0}$, because for any $\overline{i} \in \mathbb{Z}_d$ we have

$$\overline{0} + \overline{i} = \overline{0 + i} = \overline{i} = \overline{i + 0} = \overline{i} + \overline{0}.$$

- The inverse of $\overline{i} \in \mathbb{Z}_d$ is $\overline{d - i}$, because

$$\overline{i} + \overline{d - i} = \overline{i + d - i} = \overline{d} = \overline{0}$$

  and

$$\overline{d - i} + \overline{i} = \overline{d - i + i} = \overline{d} = \overline{0}.$$

2.5.3 Permutation groups:

Let X be any nonempty set and let $\mathcal{S}_X$ be the set of all bijective maps $f : X \longrightarrow X$. Then $(\mathcal{S}_X, \circ)$, where "$\circ$" is the usual composition of maps, is a group.

But $(\mathcal{S}_X, \circ)$ is not an abelian group. If we take $X = \mathbb{Z}$, then

$$\begin{aligned} f : \mathbb{Z} : &\longrightarrow \mathbb{Z} \\ n &\longmapsto f(n) = n + 1 \end{aligned}$$

and

$$\begin{aligned} g : \mathbb{Z} : &\longrightarrow \mathbb{Z} \\ n &\longmapsto g(n) = 2n \end{aligned}$$

are two elements of $\mathcal{S}_X$. But $(f \circ g) \neq (g \circ f)$ because

$$(f \circ g)(0) = f(g(0)) = f(0) = 1 \neq (g \circ f)(0) = g(f(0)) = g(1) = 2.$$

If $X = \mathbb{I}_n = \{1, 2, \ldots, n\}$, then we write $\mathcal{S}_n$ instead of $\mathcal{S}_X$. $(\mathcal{S}_n, \circ)$ is called the *the permutation group*. This naming is because each element of $\mathcal{S}_n$ describes a permutation of $\mathbb{I}_n$. If $\sigma \in \mathcal{S}_n$, then we represent σ by listing the elements of $\mathbb{I}_n$ in a line and then their images respective just below the antecedent, that is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

For example, the identity in $\mathcal{S}_n$ is

$$Id_n = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}.$$

If

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 2 & 1 & 6 & 8 & 7 \end{pmatrix}$$

is an element of $\mathcal{S}_8$, then we have $\beta(1) = 5, \beta(2) = 4, \beta(3) = 3$ and so on.

This representation makes it easy to find inverse or composite of two permutations: To obtain th inverse of a permutation we read from the bottom entry to the top entry rather than from top to bottom: for example if if 5 appears beneath 1 in σ, then 1 will appear beneath 5 in σ^{-1}:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 2 & 3 & 6 & 8 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 2 & 1 & 6 & 8 & 7 \end{pmatrix}.$$

One can check that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 2 & 3 & 6 & 8 & 7 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 2 & 1 & 6 & 8 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = Id_8.$$

For simplicity, one can use the so called *cycle* notation. Let $\sigma \in \mathcal{S}_n$, we write $\sigma = (a_1, a_2, \ldots, a_k)$ if

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$$

and $\sigma(i) = i$ for all $i \notin \{a_1, a_2, \ldots, a_k\}$. We then say σ is a *k-cycle*. For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 2 & 5 & 6 & 7 & 4 \end{pmatrix} = (2, 3, 8, 4).$$

In $\mathcal{S}_5$, we have

$$(1, 2, 3) \circ (1, 5, 2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

Theorem 5. *Any element of the group $\mathcal{S}_n$, for a given n, is either a cycle or can be written as a product of pairwise disjoint cycles; and, except for the order in which the cycles are written, and the inclusion or omission of* 1*-cycles, this can be done in only one way.*

We skip the proof. But let us illustrate how one can find the decomposition into disjoint cycles: Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 3 & 5 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}.$$

Starting from 1 we have

$$\begin{array}{r|l} 1 & (1 \\ \sigma(1) = 9 & (1, 9 \\ \sigma(9) = 2 & (1, 9, 2 \\ \sigma(2) = 1 & (1, 9, 2). \end{array}$$

We stop because the cycle is closed: 1 already appeared before. And we restart by an element not in $(1, 9, 2)$, say 3. Then we have

$$\begin{array}{r|l} 3 & (3 \\ \sigma(3) = 3 & (3). \end{array}$$

We iterate by starting always with element that did not appear in the cycles found, as long as there are such elements:

$$\begin{array}{r|l} 4 & (4 \\ \sigma(4)=5 & (4,5 \\ \sigma(5)=6 & (4,5,6 \\ \sigma(6)=4 & (4,5,6), \end{array}$$

$$\begin{array}{r|l} 7 & (7 \\ \sigma(7)=7 & (7), \end{array}$$

$$\begin{array}{r|l} 8 & (8 \\ \sigma(8)=8 & (8). \end{array}$$

At the end, we collect all the cycles we found, and we have

$$\sigma = (1,9,2)(3)(4,5,6)(7)(8) = (1,9,2)(4,5,6).$$

1-cycles are ignored and the operation "$\circ$" is removed. Since, it is understood that operation is the composition of permutations and if an integer is not in the cycle components shown then it forms a 1-cycles.

2-cycles are called *transposition.* They play special roles in $\mathcal{S}$: Any cycle can be decomposed as a composite of transpositions:

- $Id_n = (a,b)(a,b)$ for any different elements a and b of $\{1,2,\ldots,n\}$.
- Let $a_1, a_2, \ldots, a_k$ be $k \geq 3$ different elements in $\{1,2,\ldots,n\}$. Then we have

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_2, a_3)\ldots(a_{k-1}, a_k).$$

[**Exercise:***Prove this relation by induction.*]

With this observation, Theorem 5 implies the following:

Theorem 6. *Any permutation in $\mathcal{S}_n$, for a given $n \geq 2$, can be decomposed as a product of transpositions.*

We say that $\sigma \in \mathcal{S}_n$ is *even permutation* if it can be decomposed as product of even number of transpositions. If σ is not even, then it is an *odd permutation.*

Chapter 3

Analysis

3.1 Completeness of $\mathbb{R}$

Unlike the set of rational numbers $\mathbb{Q}$, the set of real numbers $\mathbb{R}$ is continuous with no "gaps". This completeness of $\mathbb{R}$, leads to other important properties that are useful in Analysis, such as the existence of suprema and the convergence of Cauchy sequences.

3.1.1 Suprema and infima

Definition 16. *Let $A \subseteq \mathbb{R}$.*

1. *A real number M is an **upper bound** of A if $x \leq M$ for every $x \in A$.*
2. *$m \in \mathbb{R}$ is a **lower bound** of A if $x \geq m$ for every $x \in A$.*

*A set is **bounded from above** if it has an upper bound, **bounded from below** if it has a lower bound, and **bounded** if it has both an upper and a lower bound.*

An equivalent condition for A to be bounded is that there exists $M \in \mathbb{R}$ such that $|x| \leq M$ for every $x \in A$.

Example 15. *The set of natural numbers $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ is bounded from below by 1 (or any $m \in \mathbb{R}$ with $m \leq 1$). It is not bounded from above, and thus $\mathbb{N}$ is unbounded.*

Definition 17. *Suppose that A is a subset of $\mathbb{R}$.*

1. *If $M \in \mathbb{R}$ is an upper bound of A such that $M \leq M'$ for every upper bound M' of A, then M is called the **supremum** or least upper bound of A, denoted*

$$M = \sup(A).$$

2. *If $m \in \mathbb{R}$ is a lower bound of A such that $m \geq m'$ for every lower bound m' of A, then m is called the **infimum** or greatest lower bound of A, denoted by*

$$m = \inf(A).$$

The supremum or infimum of a set may or may not belong to the set. If $\sup(A)$ does belong to A, then we also denote it by $\max(A)$ and refer to it as the **maximum** of A. If $\inf(A) \in A$, then we also denote it by $\min(A)$ and refer to it as the **minimum** of A.

Example 16 (Suprema and infima of intervals)**.** *For any real numbers $a < b$ we have*

$$\sup((a,b)) = \sup([a,b)) = \sup([a,b]) = \sup((a,b]) = b$$

and

$$\inf((a,b)) = \inf([a,b)) = \inf([a,b]) = \inf((a,b]) = a.$$

Example 17. *Every finite set of real numbers*

$$A = \{a_1, a_2, \ldots, a_n\}$$

is bounded. Its supremum is the greatest element,

$$\sup A = \max\{a_1, a_2, \ldots, x_n\},$$

and its infimum is the smallest element,

$$\inf(A) = \min\{a_1, a_2, \ldots, a_n\}.$$

Both the supremum and infimum of a finite set belong to the set.

Example 18. *1. $A = \{x \in \mathbb{R} : x < \sqrt{2}\}$ is bounded from above, and* $\sup(A) = \sqrt{2}$.

2. $B = \{n \in \mathbb{Z} : n > -10\}$ is bounded from below, and $\inf(B) = -9$.

Example 19. *Let*

$$A = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}.$$

Then

$$\sup(A) = 1 \in A \qquad \text{and} \qquad \inf(A) = 0 \notin A.$$

We show that $\inf(A) = 0$*:*

0 is a lowerbound of A: Follows since $0 < n$ for all $n \in \mathbb{N}$, which in turn makes $0 < \dfrac{1}{n}$ for every $n \in \mathbb{N}$.
0 is the greatest lowerbound of A: Assume that there is a lowerbound $x \in \mathbb{R}$ of A such that $x > 0$. By the Archimedean Property (AP) of real numbers, (see Proposition 2), there exists $n \in \mathbb{N}$ such that $n > \dfrac{1}{x}$. This makes $x > \dfrac{1}{n}$.
Since $\frac{1}{n} \in A$, this shows that x cannot be a lowerbound of A, which contradicts that x is a lowerbound of A. Thus 0 is the greatest lowerbound of A.

i) **Least upper bound property (LUBP):** Every nonempty set of real numbers that is bounded from above has a supremum.

ii) **Immediate consequence of the Least upper bound property:** Every nonempty set of real numbers that is bounded from below has an infimum.

Since $\inf(A) = -\sup(-A)$, i) implies ii) and ii) implies i).

Exercises 10. *1. If a is an upperbound of a subset A of $\mathbb{R}$ and $a \in A$, then $a = \sup(A)$. Similarly, if b is a lowerbound of a subset A of $\mathbb{R}$ and $a \in A$, then $a = \inf(A)$.*

Proof. Assume that a is a lowerbound of $A \subseteq \mathbb{R}$ and $a \in A$. Since $\sup(A)$ is an upperbound of A and $a \in A$, then $a \leq \sup(A)$.
Furthermore, since a is an upperbound of A and $\sup(A)$ is the smallest upperbound of A, then $\sup(A) \leq a$.
Thus $a = \sup(A)$. □

2. *Let A be a bounded non-empty subset of $\mathbb{R}$. Define $B = \{-a : a \in A\}$. Show that*

$$\sup(B) = -\inf(A)$$

and

$$\inf(B) = -\sup(A).$$

Proof. $\sup(B) = -\inf(A):$
Since $\sup(B)$ is an upperbound of B, we have $\sup(B) \geq -a$ for every $a \in A$. Therefore $-\sup(B) \leq a$ for all $a \in A$. This means that $-\sup(B)$ is a lowerbound of A. Since $\inf(A)$ is the greatest lowerbound of A, we have $-\sup(B) \leq \inf(A)$. Thus $\sup(B) \geq -\inf(A)$.

On the other hand, we have that $\inf(A) \leq a$ for all $a \in A$. Therefore $-\inf(A) \geq -a$ for all $a \in A$. This means that $-\inf(A)$ is an upperbound of B. Since $\sup(B)$ is the smallest upperbound of B, we have $\sup(B) \leq -\inf(A)$.
Thus $\sup(B) = -\inf(A)$. □

3. *More generally, define $cA = \{ca : a \in A\}$, for some $a \in \mathbb{R}$. Show that if $c > 0$, then*

$$\sup(cA) = c\sup(A) \textit{ and } \inf(cA) = c\inf(A),$$

but if $c < 0$, then

$$\sup(cA) = c\inf(A) \textit{ and } \inf(cA) = c\sup(A).$$

Proof. $\underline{\sup(cA) = c\sup(A):}$
Since $\sup(cA)$ is an upperbound of cA, we have $\sup(cA) \geq ca$ for every $a \in A$. Therefore $\dfrac{\sup(cA)}{c} \geq a$ for all $a \in A$. This means that $\dfrac{\sup(cA)}{c}$ is an upperbound of A. Since $\sup(A)$ is the least upperbound of A, we have $\sup(A) \leq \dfrac{\sup(cA)}{c}$. Thus $c\sup(A) \leq \sup(cA)$.

On the other hand, we have that $\sup(A) \geq a$ for all $a \in A$. Therefore $c\sup(A) \geq ca$ for all $a \in A$. This means that $c\sup(A)$ is an upperbound of cA. Since $\sup(cA)$ is the smallest upperbound of cA, we have $\sup(cA) \leq c\sup(A)$.
Thus $\sup(cA) = c\sup(A)$.

$\underline{\sup(cA) = c\inf(A):}$
Since $\sup(cA)$ is an upperbound of cA, we have $\sup(cA) \geq ca$ for every $a \in A$. Because $c < 0$, we get that $\dfrac{\sup(cA)}{c} \leq a$ for all $a \in A$. This means that $\dfrac{\sup(cA)}{c}$ is a lowerbound of A. Since $\inf(A)$ is the greatest lowerbound of A, we have $\dfrac{\sup(cA)}{c} \leq \inf(A)$. Thus $\sup(cA) \geq c\inf(A)$.

On the other hand, we have that $\inf(A) \leq a$ for all $a \in A$. Therefore $c\inf(A) \geq ca$ for all $a \in A$. This means that $c\inf(A)$ is an upperbound of cA. Since $\sup(cA)$ is the smallest upperbound of cA, we have $\sup(cA) \leq c\inf(A)$.
Thus $\sup(cA) = c\inf(A)$. □

Example 20. *The set $\mathbb{Q}$ of rational numbers does not have least upper bound property: It is possible to find a subset of $\mathbb{Q}$ which has an upper bound but no supremum in $\mathbb{Q}$. For example, consider*

$$A = \{x \in \mathbb{Q} : x < \sqrt{2}\}.$$

Obviously, $3 \in \mathbb{Q}$ is an upper bound of A. Since $\sqrt{2} \notin \mathbb{Q}$, whenever we have an upper bound $M \in \mathbb{Q}$, we will always have $M - \sqrt{2} > 0$, and thus

$$\frac{1}{M - \sqrt{2}} > 0.$$

By Proposition 2, there is $n \in \mathbb{N}$ such that $n > \frac{1}{M-\sqrt{2}}$ and thus

$$n > \frac{1}{M - \sqrt{2}} \Rightarrow M - \sqrt{2} > \frac{1}{n} \Rightarrow M - \frac{1}{n} > \sqrt{2}.$$

This means that $M' = M - \frac{1}{n} \in \mathbb{Q}$ is also an upper bound of A, and M is not the smallest. Since M was chosen arbitrarily, this means that there is no least upper bound of A in $\mathbb{Q}$.

3.2 Sequences

3.2.1 The absolute value (review)

Definition 18. *The **absolute value** of a real number x is defined by*

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

The absolute value satisfies the following property:

Proposition 6. *For all $x, y, z \in \mathbb{R}$:*

i) $|x| \geq 0$,

ii) $|x| = 0$ *if and only if* $x = 0$,

iii) $|-x| = |x|$,

iv) $|x + y| \leq |x| + |y|$, *triangle inequality,*

v) $|xy| = |x||y|$,

vi) if $x \leq z$ *and* $-x \leq z$. *then* $|x| \leq z$.

Definition 19. *Let $a \in \mathbb{R}$.*

1. *The **floor** $\lfloor a \rfloor$ of a is the largest integer* smaller *or equal to a.*
2. *The **ceiling** $\lceil a \rceil$ of a is the smallest integer* larger *or equal to a.*

For example $\lfloor 3.1 \rfloor = 3$, $\lceil 3.1 \rceil = 4$, $\lfloor -3.1 \rfloor = -4$ and $\lceil -3.1 \rceil = -3$.
Note that for any $a \in \mathbb{R}$, we have

$$\lfloor a \rfloor \leq a \leq \lceil a \rceil.$$

3.2.2 Definition and examples

An infinite sequence

$$(x_n)_k^\infty = (x_k, x_{k+1}, x_{k+2}, \dots)$$

of real numbers is an ordered list of numbers $x_n \in \mathbb{R}$. The terms x_n of the sequence (x_n) are indexed by natural numbers $n \in \mathbb{N}$. We simply write (x_n) instead of $(x_n)_1^\infty$.

To define a sequence, sometimes we just list the first few terms, this is if they follow an obvious pattern. Sometimes, an explicit formula for x_n, or a recursive formula satisfied by the terms is provided. For example the sequence of positive powers of 2 can be given as (2^n), or

$$(2, 4, 8, 16, \dots),$$

or

$$(x_n) \text{ where } x_1 = 2 \text{ and } x_{n+1} = 2x_n \text{ for all } n \in \mathbb{N}.$$

The expression of the terms can be more complicated

$$\left(\frac{2 \sin n}{\ln(n^2) + e^{2n+1}} \right).$$

If necessary, we can specify the range of the indices n. For example the sequence $(2n^2 - 4)_{n=2}^\infty$ is

$$(4, 14, 28, 46, \dots).$$

A more formal definition of sequence describes it as mapping:

Definition 20. *A **sequence** $(x_n)_k^\infty$ of real numbers is a mapping*

$$\begin{aligned} \{n \in \mathbb{N} : n \geq k\} &\longrightarrow \mathbb{R} \\ n &\longmapsto x_n. \end{aligned}$$

3.2.3 Convergence and limits

Roughly speaking, we say that a sequence (x_n) converges to a limit x if the terms x_n get arbitrarily close to x for all sufficiently large n.

Definition 21. *A sequence (x_n) of real numbers **converges** to a limit $x \in \mathbb{R}$, and we write*

$$\lim_{n \to \infty} x_n = x \quad OR \quad x_n \to x,$$

if for every $\epsilon > 0$ there is $N \in \mathbb{N}$ such that

$$n > N \Longrightarrow |x_n - x| < \epsilon.$$

i.e. for every $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that $|x_n - x| < \epsilon$ for all $n > N$.

The N in Definition 21 may depend on ϵ.

Typically, the smaller we choose ϵ, the larger we have to make N: $|x_n - x| \to 0$ as $n \to \infty$.

A proof of convergence of a given sequence can be viewed as a game: If someone gives an $\epsilon > 0$, you must find an N that works.

We say that a sequence diverges if it does not converge.

Example 21. *The sequence (x_n), where $x_n = \frac{1}{2n} + 2$ for all $n \in \mathbb{N}$, converges to $x = 2$.*

Proof. Choose $\epsilon > 0$.
Choice of N (we find N by working backwards):

$$\begin{aligned} |x_n - 2| < \epsilon &\Longrightarrow \left|\frac{1}{2n} + 2 - 2\right| < \epsilon \\ &\Longrightarrow \left|\frac{1}{2n}\right| < \epsilon \\ &\Longrightarrow \frac{1}{2n} < \epsilon \\ &\Longrightarrow \frac{1}{2\epsilon} < n. \end{aligned}$$

Now, set $N = \lceil \frac{1}{2\epsilon} \rceil \in \mathbb{N}$.
Then

$$\begin{aligned} n > N &\Longrightarrow n > \left\lceil \frac{1}{2\epsilon} \right\rceil \\ &\Longrightarrow n > \frac{1}{2\epsilon} \\ &\Longrightarrow 1 > \frac{1}{2\epsilon n} \\ &\Longrightarrow \epsilon > \frac{1}{2n} \\ &\Longrightarrow \epsilon > \left|\frac{1}{2n}\right| \\ &\Longrightarrow \epsilon > \left|\frac{1}{2n} - 0\right| \\ &\Longrightarrow \epsilon > \left|\frac{1}{2n} + 2 - 2\right| \\ &\Longrightarrow \epsilon > |x_n - 2|. \end{aligned}$$

Thus $x_n \to 2$. □

Example 22. *The sequence (x_n), where $x_n = \frac{n+1}{2n-1}$ for all $n \in \mathbb{N}$, converges to $\frac{1}{2}$.*

Proof. Choose $\epsilon > 0$.

Choice of N:

$$\begin{aligned}\left|x_n - \frac{1}{2}\right| < \epsilon &\implies \left|\frac{n+1}{2n-1} - \frac{1}{2}\right| < \epsilon \\ &\implies \left|\frac{2n+2-2n+1}{4n-2}\right| < \epsilon \\ &\implies \frac{3}{4n-2} < \epsilon \\ &\implies \frac{3}{\epsilon} < 4n-2 \\ &\implies \frac{\frac{3}{\epsilon}+2}{4} < n.\end{aligned}$$

Now, set $N = \left\lceil \frac{\frac{3}{\epsilon}+2}{4} \right\rceil \in \mathbb{N}$.
Then

$$\begin{aligned} n > N &\implies n > \left\lceil \frac{\frac{3}{\epsilon}+2}{4} \right\rceil \\ &\implies n > \frac{\frac{3}{\epsilon}+2}{4} \\ &\implies n > \frac{\frac{3}{\epsilon}+2}{4} \\ &\implies 4n > \frac{3}{\epsilon} + 2 \\ &\implies 4n - 2 > \frac{3}{\epsilon} \\ &\implies \epsilon > \frac{3}{4n-2} \\ &\implies \epsilon > \left|\frac{2n+2-2n+1}{4n-2}\right| \\ &\implies \epsilon > \left|\frac{n+1}{2n-1} - \frac{1}{2}\right| \\ &\implies \epsilon > |x_n - \frac{1}{2}|.\end{aligned}$$

Thus $x_n \to \dfrac{1}{2}$. □

Example 23. *A constant sequence converges: Let (x_n) be a sequence, where $x_n = 5$ for all $n \in \mathbb{N}$. Then*

$$\lim_{n\to\infty} x_n = 5,$$

because for any $\epsilon > 0$, we can take $N = 1 \in \mathbb{N}$ and have

$$n > N \implies x_n = 5 \implies |x_n - 5| = 0 < \epsilon.$$

Remark 2. *1.* ***TRICHOTOMY PROPERTY:*** *Given $a, b \in \mathbb{R}$, one and only of the following statements holds:*

$$a < b, \quad b < a, \quad or \quad a = b.$$

2. *Let $x, y \in \mathbb{R}$.*

   (a) *$x < y + \epsilon$ for all $\epsilon > 0$ iff $x \leq y$.*

   (b) *$|a| < \epsilon$ for all $\epsilon > 0$ iff $a = 0$.*

Proposition 7. *If a sequence of real numbers converges, then its limit is unique.*

Proof. Suppose that x and x' are two limits of the sequence (x_n).
Let $\epsilon > 0$. By definition of limits, there exists $N \in \mathbb{N}$ such that

$$n > N \Longrightarrow |x_n - x| < \frac{\epsilon}{2}$$

and there exists $N' \in \mathbb{N}$ such that

$$n > N' \Longrightarrow |x' - x_n| = |x_n - x'| < \frac{\epsilon}{2}.$$

Set $N = \max\{N, N'\}$.
Using the triangle inequality, for any $n > N$ we get

$$0 \leq |x' - x| = |x' - x_n + x_n - x| \leq |x' - x_n| + |x_n - x| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Since this is for any $\epsilon > 0$, we must have $|x - x'| = 0$ and thus $x' - x = 0$, which gives $x = x'$. □

Definition 22. 1. *A sequence (x_n) of real numbers is **bounded from above** if there exists $M \in \mathbb{R}$ such that*

$$x_n \leq M \text{ for all } n \in \mathbb{N}.$$

2. *A sequence (x_n) of real numbers is **bounded from below** if there exists $m \in \mathbb{R}$ such that*

$$x_n \geq m \text{ for all } n \in \mathbb{N}.$$

3. *A sequence is **bounded** if it is bounded from above and bounded from below. An equivalent condition for the sequence (x_n) to be bounded is that there exists $M \in \mathbb{R}$ such that*

$$|x_n| \leq M \text{ for all } n \in \mathbb{N}.$$

Remark 3. 1. *To show that a sequence (x_n) is not bounded from above, we negate Definition 22(1): For all $M \in \mathbb{R}$, there is $n \in \mathbb{N}$ with $x_n > M$.*

2. *To show that a sequence (x_n) is not bounded from below, we negate Definition 22(2): For all $m \in \mathbb{R}$, there is $n \in \mathbb{N}$ with $x_n < m$.*

3. *To show that a sequence (x_n) is not bounded, we negate Definition 22(3): For all $M \in \mathbb{R}$, there is $n \in \mathbb{N}$ with $|x_n| > M$.*

Example 24. *The sequence $(\frac{1}{3n})$ bounded: it is bounded from below by 0 and bounded above by $\dfrac{1}{3}$: for any $n \in \mathbb{N}$ we have*

$$0 \leq \frac{1}{3n} \leq \frac{1}{3}.$$

Example 25. *The sequence* $(\frac{2n+1}{3})$ *is bounded from below by* 1*. It is not bounded from above. We show that it is not bounded from above:*
Let $M \in \mathbb{R}$*.*
Choice of n : *Because* $\frac{3M}{2} - 1 \in \mathbb{R}$*, set* $n = \lceil \frac{3M}{2} \rceil \in \mathbb{N}$*.*
Then

$$\frac{2n+1}{3} = \frac{2\lceil \frac{3M}{2} \rceil + 1}{3} \geq \frac{2\frac{3M}{2} + 1}{3} > M.$$

The following proposition describes a relation between boundedness and convergence:

Proposition 8. *A convergent sequence is bounded.*

Proof. Assume that (x_n) is a convergent sequence with limit x.
Then, by definition, for any $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that

$$n > N \Longrightarrow |x_n - x| < \epsilon.$$

In particular, if we choose $\epsilon = 1$, then there exists N' such that

$$n > N' \Longrightarrow |x_n - x| < 1.$$

By the triangle inequality, we have

$$|x_n| = |x_n - x + x| \leq |x_n - x| + |x| \leq 1 + |x|$$

for all $n > N'$. Hence, we can choose

$$M = \max\{|x_1|, |x_2|, \ldots, |x_{N'}, 1 + |x|\},$$

to have $|x_n| \leq M$ for all $n \in \mathbb{N}$, so (x_n) is bounded. □

By taking the contrapositive of Proposition 8, we obtain the following:

Proposition 9. *An unbounded sequence diverges.*

The proof of Proposition 8 suggests that, changing finite number of terms of a sequence does not change the property of sequence being bounded or unbounded.

3.2.4 Properties of limits

Now that we have formal definition of limits, we can prove the properties of limits that we saw in 1st year.

Monotonicity

Limits of convergent sequences preserve (non-strict) inequalities.

Theorem 7. *If* (x_n) *and* (y_n) *are convergent sequences and* $x_n \leq y_n$ *for all* $n \in \mathbb{N}$*, then*

$$\lim_{n\to\infty} x_n \leq \lim_{n\to\infty} y_n.$$

Proof. Suppose that

$$\lim_{n\to\infty} x_n = x$$

and

$$\lim_{n\to\infty} y_n = y.$$

Then for every $\epsilon > 0$, there exist $P, Q \in \mathbb{N}$ such that

$$n > P \Longrightarrow |x - x_n| = |x_n - x| < \frac{\epsilon}{2}$$

and

$$n > Q \Longrightarrow |y_n - y| < \frac{\epsilon}{2}.$$

Setting $N = \max\{P, Q\}$ and choosing $n > N$, we have

$$x = x_n + x - x_n < x_n + \frac{\epsilon}{2} \leq y_n + \frac{\epsilon}{2} = y + y_n - y + \frac{\epsilon}{2} < y + \frac{\epsilon}{2} + \frac{\epsilon}{2} = y + \epsilon.$$

Since $x < y + \epsilon$ for any $\epsilon > 0$, we must have $x \leq y$. □

Theorem 7 still holds even if the inequality $x_n \leq y_n$ is only true for sufficiently large n.

Taking one of (x_n) and (y_n) as constant sequence, Theorem 7 implies the following:

1. If $x_n \leq M$ for all $n \in \mathbb{N}$, then
$$\lim_{n\to\infty} x_n \leq M.$$
2. If $x_n \geq m$ for all $n \in \mathbb{N}$, then
$$\lim_{n\to\infty} x_n \geq m.$$
3. If $M \geq x_n \geq m$ for all $n \in \mathbb{N}$, then
$$M \geq \lim_{n\to\infty} x_n \geq m.$$

Note that limits do not always preserve **strict** inequality. For example, if we consider $(\frac{2}{n})$, we know that $\frac{2}{n} > 0$ for any $n \in \mathbb{N}$, but

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{2}{n} = 0.$$

Theorem 8 (Squeeze Theorem)**.** *Suppose that* (x_n) *and* (y_n) *are convergent sequences of real numbers with the same limit* L*. If* (z_n) *is a sequence such that*

$$x_n \leq z_n \leq y_n \qquad \text{for all } n \in \mathbb{N},$$

then (z_n) *also converges to* L*.*

Proof. Assume that the sequences (x_n), (y_n) and (z_n) are such that

$$\lim_{n\to\infty} x_n = L = \lim_{n\to\infty} y_n$$

for some $L \in \mathbb{R}$.

Let $\epsilon > 0$. Then there exist $P, Q \in \mathbb{N}$ such that

$$n > P \Longrightarrow |x_n - L| < \epsilon \qquad \text{and} \qquad n > Q \Longrightarrow |y_n - L| < \epsilon.$$

Set $N = \max\{P, Q\}$. Then for any $n > N$ we have

$$\begin{aligned} |x_n - L| < \epsilon \text{ and } |y_n - L| < \epsilon &\Longrightarrow -\epsilon < x_n - L \leq z_n - L \leq y_n - L < \epsilon \\ &\Longrightarrow -\epsilon < z_n - L < \epsilon \\ &\Longrightarrow |z_n - L| < \epsilon. \end{aligned}$$

This means that

$$\lim_{n\to\infty} z_n = L.$$

□

Linearity

As we already know from previous year, limits respect addition and multiplication. We now have the necessary tools to prove it.

Theorem 9. *Suppose that each of the sequences (x_n) and (y_n) converges and $c \in \mathbb{R}$. Then the sequences (cx_n), $(x_n + y_n)$, and $(x_n y_n)$ converge and*

i) $\lim_{n\to\infty} cx_n = c \lim_{n\to\infty} x_n$,

ii) $\lim_{n\to\infty} (x_n + y_n) = \lim_{n\to\infty} x_n + \lim_{n\to\infty} y_n$,

iii) $\lim_{n\to\infty} (x_n y_n) = \left(\lim_{n\to\infty} x_n\right)\left(\lim_{n\to\infty} y_n\right)$.

Proof. Assume that

$$\lim_{n\to\infty} x_n = x \qquad \text{and} \qquad \lim_{n\to\infty} y_n = y.$$

1. Proof of i): If $c = 0$, then $(cx_n) = (0)$ is a constant sequence whose terms are all 0. Clearly it converges to

$$c \lim_{n\to\infty} x_n = 0 \lim_{n\to\infty} x_n = 0.$$

Now assume that $c \neq 0$.
Let $\epsilon > 0$ (we want to show that $cx_n \to cx$).
We have that $\dfrac{\epsilon}{|c|} > 0$.
Since x is the limit of (x_n), there exists $N \in \mathbb{N}$ such that

$$n > N \Longrightarrow |x_n - x| < \frac{\epsilon}{|c|}$$

Therefore

$$|c||x_n - x| < |c|\frac{\epsilon}{|c|} \Longrightarrow |cx_n - cx| < \epsilon.$$

This means that

$$\lim_{n\to\infty} cx_n = cx = c \lim_{n\to\infty} x_n.$$

2. Proof of ii): Let $\epsilon > 0$. Then $\frac{\epsilon}{2} > 0$. It follows that there exist $P, Q \in \mathbb{N}$ such that

$$n > P \Longrightarrow |x_n - x| < \frac{\epsilon}{2} \qquad \text{and} \qquad n > Q \Longrightarrow |y_n - x| < \frac{\epsilon}{2}.$$

   Let $N = \max\{P, Q\}$. Then for all $n > N$ we have

$$|(x_n + y_n) - (x + y)| = |x_n - x + y_n - y| \leq |x_n - x| + |y_n - y| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

   This proves that $(x_n + y_n)$ converges to $x + y$.

3. Proof of iii): Exercise! You may need the fact that if a sequence converges, then it is bounded.

□

Infinite limits

The formal definitions of infinite limits are as follows:

Definition 23. *Let (x_n) be a sequence of real numbers. Then*

i) $\lim\limits_{n\to\infty} x_n = \infty$ *means that for every $M > 0$, there is $N \in \mathbb{N}$ such that*

$$n > N \Longrightarrow x_n > M.$$

ii) $\lim\limits_{n\to\infty} x_n = -\infty$ *means that for every $M > 0$, there is $N \in \mathbb{N}$ such that*

$$n > N \Longrightarrow x_n < -M.$$

Example 26. *1. Consider the sequence (x_n), where $x_n = n^2$ for all $n \in \mathbb{N}$.*

$$\lim_{n\to\infty} n^2 = \infty$$

Proof. Let $M > 0$. Choose $N = \sqrt{M}$. Then we have

$$\begin{aligned} n > N &\Longrightarrow n > \sqrt{M} \\ &\Longrightarrow n^2 > (\sqrt{M})^2 \\ &\Longrightarrow n^2 > M \\ &\Longrightarrow x_n > M \end{aligned}$$

which proves the result. □

2. Consider the sequence (x_n), where $x_n = \frac{n^3+1}{n^2}$ for all $n \in \mathbb{N}$.

$$\lim_{n\to\infty} \frac{n^3 + 1}{n^2} = \infty.$$

Proof. Let $M > 0$. Choose $N = M$ (we get this after working out what N would work). Then we have

$$\begin{aligned} n > N &\Longrightarrow n > M \\ &\Longrightarrow n^3 > Mn^2 \\ &\Longrightarrow n^3 + 1 > n^3 > Mn^2 \\ &\Longrightarrow n^3 + 1 > Mn^2 \\ &\Longrightarrow \frac{n^3+1}{n^2} > M. \end{aligned}$$

which proves the result. □

3. *Consider the sequence (x_n), where $x_n = \frac{-n^2+n}{2}$ for all $n \in \mathbb{N}$.*

$$\lim_{n\to\infty} \frac{-n^2+n}{2} = -\infty$$

Proof. Let $M > 0$. Choose $N = 2M + 2$. Then we have

$$\begin{aligned} n > N &\Longrightarrow n > 2M + 2 \\ &\Longrightarrow n - 2 > 2M \\ &\Longrightarrow \frac{n-2}{2} > M \\ &\Longrightarrow \frac{n^2-2}{2} > M \\ &\Longrightarrow \frac{-n^2+2}{2} < -M. \end{aligned}$$

which proves the result □

3.3 Open Sets and closed sets

Open sets play central roles in the study of convergence of sequences, limits and continuity of functions.

Definition 24. *A set $A \subseteq \mathbb{R}$ is* ***open*** *if for each $x \in A$, there exists a $\delta > 0$ such that $(x-\delta, x+\delta) \subseteq A$.*

We say that A is a *neighbourhood* of x if there is $\delta > 0$ such that $(x - \delta, x + \delta) \subseteq A$.

Example 27. 1. *The interval $I = (0, 1)$ is open.*

2. *The set $\mathbb{R}$ of real numbers is open.*

3. *The empty set is open.*

Proposition 10. *An arbitrary union of open sets is open.*

Proof. i) Let $\{A_i : i \in I\}$ be a collection of open sets, and let

$$K = \bigcup_{i \in I} A_i.$$

We need to show that K is an open set.

$$\begin{aligned} x \in K &\Longrightarrow x \in A_{i_0} \text{ for some } i_0 \in I \quad \text{(definition of union of sets)} \\ &\Longrightarrow \exists \delta > 0, (x-\delta, x+\delta) \subseteq A_{i_0} \text{ for some } i_0 \in I \quad \text{(since } A_{i_0} \text{ is open)} \\ &\Longrightarrow \exists \delta > 0, (x-\delta, x+\delta) \subseteq K. \end{aligned}$$

Since x was arbitrary, this implies that K is open. □

Definition 25. *Let $A \subseteq \mathbb{R}$. Then $x \in A$ is:*

1. *an **interior point** of A if there is real number $\delta > 0$ such that*

$$(x-\delta, x+\delta) \subseteq A.$$

2. *an **isolated point** of A if $x \in A$ and there exists $\delta > 0$ such that x is the only point in A that belongs to the interval $(x-\delta, x+\delta)$.*
3. *a **boundary point** of A if for every $\delta > 0$ the interval $(x-\delta, x-\delta)$ contains points in A and points not in A.*

The set of the interior points of A is usually denoted by A°, set of isolated points of A is denoted by A' and set of boundary points of A is denoted by $\text{bd}(A)$.

Example 28. $[2,3)^\circ = (2,3)$. *2 is a boundary point of $[2,3)$, because for any $\delta > 0$ we have $2-\delta < 2-\frac{\delta}{2} < 2$; which means that*

$$2 - \frac{\delta}{2} \in (2-\delta, 2+\delta)$$

but

$$2 - \frac{\delta}{2} \notin [2,3).$$

This also shows that $2 \notin [2,3)^\circ$. But for any $a \in (2,3)$, we have $\beta = \min\{a-2, 3-a\} > 0$ and thus

$$\left(a - \frac{\beta}{2}, a + \frac{\beta}{2}\right) \subseteq [2,3).$$

Thus we can choose $\delta = \frac{\beta}{2}$, and show that $a \in [2,3)^\circ$. We now can conclude that $[2,3)^\circ = (2,3)$.

In fact in general, for any $a, b \in \mathbb{R}$, with $b > a$, we have

$$[a,b]^\circ = (a,b]^\circ = (a,b)^\circ = [a,b)^\circ = (a,b).$$

The proofs are with similar idea as above.

Exercises 11. *Determine the following interiors of sets:*

1. $\emptyset^\circ$.

2. $\{2\}^\circ$.

3. $\{2,3\}^\circ$.

4. $(1,2)^\circ$.

Proposition 11. *For every $A \subseteq \mathbb{R}$, $A^\circ \subseteq A$.*

The following result characterizes open sets using interior points.

Proposition 12. *A set $A \subseteq \mathbb{R}$ is open if and only if every point of A is an interior point.*

In other words, to show that a set is open, one needs to prove that $A \subseteq A^\circ$.

The interval $(1,3)$ is an open set. The union of interval $(-3,1) \cup (3,4) \cup (10,15)$ is an open set. But $[1,3)$ and $[1,3]$ are not open sets.

Definition 26. *A set $F \subseteq \mathbb{R}$ is **closed** if $F^c = \{x \in \mathbb{R} : x \notin F\}$ is open.*

Example 29. *1. The interval $I = [0,1]$ is closed.*

2. The set of real numbers $\mathbb{R}$ is closed.

3. The empty set is closed.

Definition 27. *Let $A \subseteq \mathbb{R}$. The **closure** $\overline{A}$ of A is the set of any $x \in \mathbb{R}$ which is such that for any real number $\delta > 0$ we have*

$$(x-\delta, x+\delta) \cap A \neq \emptyset.$$

In other words,

$$x \in \overline{A} \Longrightarrow \forall \delta > 0, (x-\delta, x+\delta) \cap A \neq \emptyset.$$

Exercises 12. *Determine the following closures of sets:*

1. $\overline{\emptyset}$.

2. $\overline{\{2\}}$

3. $\overline{\{2,3\}}$.

4. $\overline{(1,2)}$.

Proposition 13. *For any $A \subseteq \mathbb{R}$ we have*

$$A \subseteq \overline{A}.$$

Proof. Let $A \subseteq \mathbb{R}$. Let $x \in A$. For any real number $\delta > 0$ we have

$$x \in (x-\delta, x+\delta).$$

Hence we have

$$x \in (x-\delta, x+\delta) \cap A \neq \emptyset$$

which proves the result. □

Note that it is possible that $\overline{A} \neq A$ for some $A \subseteq \mathbb{R}$: for example, if we take $A = (1, 2)$, then $1 \notin A$ but $1 \in \overline{A}$: this is because for any real $\delta > 0$, we have

$$1 + \frac{\delta}{2} \in (1 - \delta, 1 + \delta) \text{ and } 1 + \frac{\delta}{2} \in (1, 2),$$

which implies that $1 + \frac{\delta}{2} \in (1 - \delta, 1 + \delta) \cap (1, 2)$.

Exercises 13. *Prove that for any $a, b \in \mathbb{R}$ with $a < b$ we have*

$$\overline{[a, b]} = \overline{(a, b]} = \overline{[a, b)} = \overline{(a, b)} = [a, b].$$

Using Proposition 13, there is little left to do to prove this.

Proposition 14. *A set $A \subseteq \mathbb{R}$ is closed if and only if $A = \overline{A}$.*

To show that a set is closed, one needs to prove that $\overline{A} \subseteq A$.

In view of Exercise 13, we can see that $[a, b]$ is a closed set, but **none** of $(a, b], [a, b)$ and (a, b) are closed sets.

Theorem 10. *i) Let $A \subseteq \mathbb{R}$. A is an open set if and only if its complement A^c is a closed set.*

ii) The intersection of closed sets is closed. These statements apply to arbitrary collections, finite or infinite, of open and closed sets.

Proof is left as an exercise.

3.4 Limits of Functions

In this section, we study limits of functions using the formal definitions of limits. We first need to define the cluster point of a set.

Definition 28. *Let $A \subseteq \mathbb{R}$. A point $c \in \mathbb{R}$ is a* ***cluster point*** *of A if for every $\delta > 0$ there exists $x \in A$ with $x \neq c$ such that $|x - c| < \delta$.*

A cluster point c of A may and may not be an element of A. For exaple a is a cluster point of the interval $(a, b]$.

Definition 29. *Let $f : A \to \mathbb{R}$, where $A \subseteq \mathbb{R}$, and suppose that c is a cluster point of A. Then*

$$\lim_{x \to c} f(x) = L$$

if for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$|x - c| < \delta \Longrightarrow |f(x) - L| < \epsilon.$$

It follows from this definition that

$$\lim_{x \to c} f(x) = L \qquad \text{if and only if} \qquad \lim_{x \to c} |f(x) - L| = 0.$$

Example 30. *Define*

$$f : [0,9) \cup (9,\infty) \to \mathbb{R} \text{ by } f(x) = \frac{x-9}{\sqrt{x}-3}.$$

We claim that

$$\lim_{x\to 9} f(x) = 6.$$

Proof. Note first that

$$|f(x){-}6| = \left|\frac{x-9}{\sqrt{x}-3} - 6\right| = \left|\sqrt{x}+3-6\right| = \left|\sqrt{x}-3\right| = \left|\frac{(\sqrt{x}-3)(\sqrt{x}+3)}{\sqrt{x}+3}\right| = \left|\frac{x-9}{\sqrt{x}+3}\right| \le \left|\frac{x-9}{3}\right|.$$

For any $\epsilon > 0$, we can take $\delta = 3\epsilon$ and have

$$\begin{aligned} |x-9| < \delta &\implies |x-9| < 3\epsilon \\ &\implies \frac{|x-9|}{3} < \epsilon \\ &\implies |f(x)-6| \le \frac{|x-9|}{3} < \epsilon \text{ Using the inequality above} \\ &\implies |f(x)-6| < \epsilon \end{aligned}$$

which verifies the result. □

Left, right, infinite limits

Definition 30 (Right and left limits)**.** *Let $f : A \to \mathbb{R}$, where $A \subseteq \mathbb{R}$, and suppose that c is a cluster point of A (it can be not in A). Then (**right limit**)*

$$\lim_{x\to c^+} f(x) = L$$

if for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$\begin{cases} c < x < c+\delta \\ x \in A \end{cases} \implies |f(x) - L| < \epsilon.$$

*and (**left limit**)*

$$\lim_{x\to c^-} f(x) = L$$

if for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$\begin{cases} c-\delta < x < c \\ x \in A \end{cases} \implies |f(x) - L| < \epsilon.$$

Example 31. *Define $f : [1,\infty] \to \mathbb{R}$ by $f(x) = 1 + \sqrt{x-1}$. Then*

$$\lim_{x\to 1^+} (1 + \sqrt{x-1}) = 1.$$

This is because for any $\epsilon > 0$, if we choose $\delta = \epsilon^2$, then

$$\begin{aligned} \begin{cases} 1 < x < 1+\delta \\ x \in A \end{cases} &\implies 0 < x-1 < \delta \\ &\implies 0 < \sqrt{x-1} < \sqrt{\delta} \\ &\implies 1 < 1+\sqrt{x-1} < 1+\sqrt{\delta} \\ &\implies 0 < 1+\sqrt{x-1}-1 < \sqrt{\delta} \\ &\implies |1+\sqrt{x-1}-1| < \sqrt{\epsilon^2} \\ &\implies |f(x)-1| < \epsilon. \end{aligned}$$

Definition 31 (Limits as $x \to \pm\infty$)**.** *Let $A \to \mathbb{R}$, where $A \subseteq \mathbb{R}$.*

1. *If A is not bounded from above, then*

$$\lim_{x\to\infty} f(x) = L$$

if for every $\epsilon > 0$, there exists $M \in \mathbb{R}$ such that

$$\begin{cases} x > M \\ x \in A \end{cases} \implies |f(x)-L| < \epsilon.$$

2. *If A is not bounded from below, then*

$$\lim_{x\to-\infty} f(x) = L$$

if for every $\epsilon > 0$, there exists $m \in \mathbb{R}$ such that

$$\begin{cases} x < m \\ x \in A \end{cases} \implies |f(x)-L| < \epsilon.$$

Example 32. *Show that*

$$\lim_{x\to\infty} \frac{2x+1}{x+2} = 2.$$

Proof. Note first that

$$\frac{2x+1}{x+2} = 2 + \frac{-3}{x+2}.$$

For any $\epsilon > 0$, we can take $M = \frac{3}{\epsilon}$ and have

$$\begin{aligned} x > M \implies x > \frac{3}{\epsilon} &\implies x+2 > \frac{3}{\epsilon} \\ &\implies \frac{1}{x+2} < \frac{3}{\epsilon} \implies \left|2 + \frac{-3}{x+2} - 2\right| = \left|\frac{-3}{x+2}\right| < \epsilon \end{aligned}$$

which verifies the result. □

Definition 32 (Divergence to $\pm\infty$)**.** *Let $f : A \to \mathbb{R}$, where $A \subseteq \mathbb{R}$, and suppose that $c \in \mathbb{R}$ is a cluster point of A.*

1. *Then*
$$\lim_{x\to c} f(x) = \infty$$
if for every $M > 0$, there exists $\delta > 0$ such that
$$\begin{cases} |x-c| < \delta \\ x \in A \end{cases} \Longrightarrow f(x) > M.$$

2. *Then*
$$\lim_{x\to c} f(x) = -\infty$$
if for every $M \in \mathbb{R}$, there exists $\delta > 0$ such that
$$\begin{cases} |x-c| < \delta \\ x \in A \end{cases} \Longrightarrow f(x) < M.$$

Example 33. *Prove that*
$$\lim_{x\to 1} \frac{1}{|x|-1} = \infty.$$

Proof. For any $M > 0$, we can choose $\delta = \frac{1}{M} > 0$ and have
$$\begin{aligned} |x-1| < \delta &\Longrightarrow ||x|-1| \leq |x-1| < \delta \\ &\Longrightarrow |x|-1 < \delta \Longrightarrow |x|-1 < \frac{1}{M} \Longrightarrow \frac{1}{|x|-1} > M \\ &\Longrightarrow f(x) > M \end{aligned}$$
which proves the result. □

Limits of functions satisfies similar properties as we saw for the limits of sequences:

i) The limit of a function is unique if it exists.

ii) If $f : A \to \mathbb{R}$, $g : A \to \mathbb{R}$ and the limits $\lim\limits_{x\to c} f(x)$ and $\lim\limits_{x\to c} g(x)$ exist, then

- $\lim\limits_{x\to c} kf(x) = k \lim\limits_{x\to c} f(x)$ for every $k \in \mathbb{R}$,
- $\lim\limits_{x\to c}(f(x) + g(x)) = \lim\limits_{x\to c} f(x) + \lim\limits_{x\to c} g(x)$,
- $\lim\limits_{x\to c}(f(x)g(x)) = \left(\lim\limits_{x\to c} f(x)\right)\left(\lim\limits_{x\to c} g(x)\right)$,
- $\lim\limits_{x\to c} \dfrac{f(x)}{g(x)} = \dfrac{\lim\limits_{x\to c} f(x)}{\lim\limits_{x\to c} g(x)}$ if $\lim\limits_{x\to c} g(x) \neq 0$,
- if $f(x) \leq g(x)$ for all $x \in A$ then $\lim\limits_{x\to c} f(x) \leq \lim\limits_{x\to c} g(x)$.

The proofs are similar to what we saw for the case of sequences, we will discuss some of them in the tutorials.

3.5 Continuous functions

In this section, we define continuous functions and study their properties.

3.5.1 Continuity

Roughly speaking, continuous functions are functions that take nearby values at nearby points.

We already know that a function $f : A \to B$ is continuous at $c \in A$ if

$$\lim_{x \to c} f(x) = f(c).$$

Using the ϵ, δ definition of limits, we now can state a formal definition of continuity.

Definition 33. *Let $f : A \to \mathbb{R}$, where $A \subseteq \mathbb{R}$, and suppose that $c \in A$. Then f is* ***continuous*** *at c if for every $\epsilon > 0$ there exists a $\delta > 0$ such that*

$$|x - c| < \delta \text{ and } x \in A \text{ implies that } |f(x) - f(c)| < \epsilon.$$

Definition 34. *A function $f : A \to \mathbb{R}$ is continuous on a set $B \subseteq A$ if it is continuous at every point in B. We say that f is continuous if it continuous at every point of its domain.*

Example 34. *Let us prove that the function $f : (0, \infty) \to \mathbb{R}$ defined by $f(x) = \sqrt{x}$ is continuous on $(0, \infty)$.*

Let $\epsilon > 0$.
Choice of δ:

$$\begin{aligned} \left|\sqrt{x} - \sqrt{c}\right| &= \left|\frac{x - c}{\sqrt{x} + \sqrt{c}}\right| \\ &< \frac{|x - c|}{\sqrt{c}}. \end{aligned}$$

If $\dfrac{|x - c|}{\sqrt{c}} < \epsilon$, then $|x - c| < \epsilon\sqrt{c}$.
Set $\delta = \epsilon\sqrt{c}$. Then

$$\begin{aligned} |x - c| < \delta &\Longrightarrow |x - c| < \sqrt{c}\epsilon \\ &\Longrightarrow \sqrt{c}|f(x) - f(c)| \leq |x - c| < \sqrt{c}\epsilon \\ &\Longrightarrow \sqrt{c}|f(x) - f(c)| < \sqrt{c}\epsilon \Longrightarrow |f(x) - f(c)| < \epsilon. \end{aligned}$$

3.5.2 Properties of continuous functions

We already know that $f : A \to \mathbb{R}$ and $g : A \to \mathbb{R}$ are continuous then so are

$$\begin{aligned} f + g : A &\to \mathbb{R} \\ x &\mapsto f(x) + g(x), \end{aligned} \qquad \begin{aligned} f.g : A &\to \mathbb{R} \\ x &\mapsto f(x)g(x), \end{aligned} \qquad \begin{aligned} cf : A &\to \mathbb{R} \\ x &\mapsto cf(x) \end{aligned} \quad \text{for any } c \in \mathbb{R}$$

and

$$\begin{aligned} \tfrac{f}{g} : A &\to \mathbb{R} \\ x &\mapsto \tfrac{f(x)}{g(x)} \end{aligned} \quad \text{except at points where } g(x) = 0.$$

These follows from properties of limits. Consequently, every polynomial function is continuous on $\mathbb{R}$ and every rational function is continuous on its domain.

Moreover, we have the following theorem for composite maps.

Theorem 11. *Let $f : A \to \mathbb{R}$ and $g : B \to \mathbb{R}$, where $f(A) \subseteq B$. If f is continuous at $c \in A$ and g is continuous at $f(c) \in B$, then $g \circ f : A \to \mathbb{R}$ is continuous at c.*

Proof. Let $\epsilon > 0$ be given. Since g is continuous at $f(c)$, there exists $\eta > 0$ such that

$$\begin{cases} |y - f(c)| < \eta \\ y \in B \end{cases} \Longrightarrow |g(y) - g(f(x))| < \epsilon.$$

Since f is continuous at c, there exists $\delta > 0$ such that

$$\begin{cases} |x - c| < \delta \\ x \in A \end{cases} \Longrightarrow |f(x) - f(c)| < \eta \Longrightarrow |g(f(x) - g(f(c))| < \epsilon \Longrightarrow |(g \circ f)(x) - (g \circ f)(c)| < \epsilon.$$

This proves that $g \circ f$ is continuous at c. □

3.5.3 Uniform continuity

Definition 35. *Let $f : A \to \mathbb{R}$, where $A \subseteq \mathbb{R}$. Then f is* ***uniformly continuous*** *on A if for every $\epsilon > 0$ there exists $\delta > 0$ such that*

$$\begin{cases} |x - y| < \delta \\ x, y \in A \end{cases} \Longrightarrow |f(x) - f(y)| < \epsilon.$$

The main difference between this definition and the definition of continuity we saw before is that here δ depends only on ϵ, not on x or y.

Example 35. *The function $f : [0, 1] \to \mathbb{R}$ defined by $f(x) = x^2$ is uniformly continuous:*

Proof. For any $\epsilon > 0$, we can take $\delta = \frac{\epsilon}{2} > 0$ and have

$$\begin{cases} |x - y| < \delta \\ x, y \in [0, 1] \end{cases} \Longrightarrow |f(x) - f(y)| = |x^2 - y^2| = |x + y||x - y| \leq 2|x - y| < 2\delta = 2\frac{\epsilon}{2} = \epsilon.$$

□

The following proposition provides a typical way to prove that a given function is not uniformly continuous.

Proposition 15. *A function $f : A \to \mathbb{R}$ is not uniformly continuous on $\mathbb{R}$ if and only if there exists $\epsilon_0 > 0$ and sequences (x_n) and (y_n) of elements of A such that*

$$\lim_{n\to\infty} |x_n - y_n| = 0 \text{ and } |f(x_n) - f(y_n)| \geq \epsilon_0 \text{ for all } n \in \mathbb{N}.$$

Proof. $(\Rightarrow)$: Suppose that f is not uniformly continuous on $\mathbb{R}$. Then there is $\epsilon_0 > 0$ such that for all $\delta > 0$, there are $x, y \in A$ with $|x - y| < \delta$ and $|f(x) - f(y)| \geq \epsilon_0$.
Set $x = x_n$ and $y = y_n$ for $\delta = \dfrac{1}{n}$.
Then $\lim\limits_{n\to\infty} |x_n - y_n| < \lim\limits_{n\to\infty} \dfrac{1}{n} = 0$ which implies that $\lim\limits_{n\to\infty} |x_n - y_n| = 0$.
$(\Leftarrow)$: Let $\delta > 0$. Then there is $n \in \mathbb{N}$ such that $|x_n - y_n| < \delta$ and $|f(x_n) - f(y_n)| \geq \epsilon_0$. This is just a negation of uniformly continuity for $\epsilon = \epsilon_0$. □

Example 36. *The function*

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x : &\mapsto f(x) = x^2 \end{aligned}$$

is continuous, but not uniformly continuous.

Proof. Using Proposition 15, we can consider the sequence

$$x_n = n \text{ and } y_n = n + \frac{1}{n}.$$

Then

$$\lim_{n\to\infty} |x_n - y_n| = \lim_{n\to\infty} \frac{1}{n} = 0,$$

but

$$|f(x_n) - f(y_n)| = \left(n + \frac{1}{n}\right)^2 - n^2 = 2 + \frac{1}{n^2} \geq 2$$

for every $n \in \mathbb{N}$. □

Example 37. *The function*

$$\begin{aligned} f : (0, 1] &\to \mathbb{R} \\ x : &\mapsto f(x) = \frac{1}{x} \end{aligned}$$

is a rational function, and thus continuous on $(0, 1]$. *But* f *is not uniformly continuous on* $(0, 1]$.

Proof. Using Proposition 15 again, this time we consider the sequence

$$x_n = \frac{1}{n} \text{ and } y_n = \frac{1}{n+1}.$$

Then

$$\lim_{n\to\infty} |x_n - y_n| = \lim_{n\to\infty} \left|\frac{1}{n} - \frac{1}{n+1}\right| = \lim_{n\to\infty} \left|\frac{n+1-n}{n(n+1)}\right| = \lim_{n\to\infty} \left|\frac{1}{n(n+1)}\right| = 0,$$

but

$$|f(x_n) - f(y_n)| = \left|\frac{1}{\frac{1}{n}} - \frac{1}{\frac{1}{n+1}}\right| = |n - (n+1)| = 1 \geq 1$$

for every $n \in \mathbb{N}$. □

3.6 Series of functions

We studied series of real numbers in 1st year. Now, we extend this to the notion of series of functions. It is a series where the general terms are functions, instead of numbers.

Definition 36. *Suppose that $f_1(x), f_2(x), f_3(x), \dots$ are functions of a variable x. Then*

$$f(x) = \sum_{n=0}^{\infty} f_n(x) = f_0(x) + f_1(x) + f_2(x) + f_3(x) + \dots$$

*is a **series of functions**. It is a function whose domain is the set of real number a such that the series of real number $\sum_{n=1}^{\infty} f_n(a)$ converges.*

Example 38. *Let $f(x)$ be a function which is differentiable infinitely many times at a point $a \in \mathbb{R}$ (such as e^x and $\cos x$). Then the* Taylor series

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)$$

is a series of functions.

More specifically, here are some examples of a series of functions:

$$\sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)} x^{2n+1}.$$

Those ones are called power series (we will define formally later).

3.6.1 Power series

In MAT1C, we studied the notion of Taylor series and Maclaurin series. It consits of decomposing a given function f, infinitely many times differentiable at a point $x = a$, into a series of function of the form

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n \qquad \text{(Taylor series)}.$$

In the special case where $a = 0$ we obtain

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} x^n \qquad \text{(MacLaurin series)}. \tag{3.1}$$

In this subsection, we start with a series of similar form as the right-hand side of (3.1) and determine if it converges or not; if it does then we try to find its limit.

Definition 37. *A **power series** in x, centered at a, is a series of functions of the form*

$$f(x) = \sum_{n=0}^{\infty} c_n(x-a)^n = c_0 + c_1(x-a) + c_2(x-a)^2 + c_3(x-a)^3 + \dots$$

where $c_0, c_1, c_2, \dots \in \mathbb{R}$ do not depend on x.

Example 39. *1. A power series centered at* 0*:*

$$\sum_{n=0}^{\infty} x^n = 1 + x + x^2 + x^3 + x^4 + \dots$$

2. A power series centered at 1*:*

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{n+1}(x-1)^n = 1 - \frac{x-1}{2} + \frac{(x-1)^2}{3} - \frac{(x-1)^3}{4} + \frac{(x-1)^4}{5} + \dots .$$

It is obvious that a power series $\sum_{n=0}^{\infty} c_n(x-a)^n$ converges if $x = a$, in such case the sum of the series is 0. It is know that the set of values of x for whsich the power series $\sum_{n=0}^{\infty} c_n(x-a)^n$ converges always form an interval.

Theorem 12. *Let*

$$\sum_{n=0}^{\infty} c_n(x-c)^n$$

be a power series. Then there is an R *with* $0 \le R \le \infty$ *such that the series converges absolutely for every* x *with* $0 \le |x-c| < R$ *and diverges for all* x *with* $|x-c| > R$.

Note that in Theorem 12, R can be ∞. In this case, the series converges for all $x \in \mathbb{R} = (-\infty, \infty)$. It is also important to note that for the case of $x = R$, the theorem does not say if the series converges or not.

Definition 38. *If the power series*

$$\sum_{n=0}^{\infty} a_n(x-c)^n$$

converges for all x *with* $|x-c| < R$ *and diverges for all* x *with* $|x-c| > R$ *(for some* $0 \le R \le \infty$*), then* R *is called the* ***radius of convergence*** *of the power series.*

A typical problem in this topic is to find out the radius of convergence of a given power series. One of the simplest techniques uses the ratio test. Ratio test applied to the power series $\sum_{n=0}^{\infty} a_n(x-c)^n$ says that

1. the series converges if $\lim_{n\to\infty} \left| \frac{a_{n+1}(x-c)^{n+1}}{a_n(x-c)^n} \right| < 1$,
2. the series diverges if $\lim_{n\to\infty} \left| \frac{a_{n+1}(x-c)^{n+1}}{a_n(x-c)^n} \right| > 1$.

Note that

$$\lim_{n\to\infty} \left| \frac{a_{n+1}(x-c)^{n+1}}{a_n(x-c)^n} \right| < 1 \iff |x-c| \lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right| < 1 \iff |x-c| < \lim_{n\to\infty} \left| \frac{a_n}{a_{n+1}} \right| .$$

Thus the radius of convergence is $R = \lim_{n\to\infty} \left| \frac{a_n}{a_{n+1}} \right|$.

Exercises 14. *Determine the radius of convergence of the following power series:*

1. $\displaystyle\sum_{n=0}^{\infty} x^n, \qquad \sum_{n=0}^{\infty} \frac{x^n}{n},$

2. $\displaystyle\sum_{n=0}^{\infty} (n!)x^n, \qquad \sum_{n=0}^{\infty} \frac{(-1)^{n+1}}{n}(x-1)^n.$