University of Cambridge

Part IA
Mathematical Tripos

Lee, Junwoo

Trinity College, Cambridge

Transcribed lecture notes from 23-24 academic year

Contents

CHAPTER 1

Numbers and Sets

Lecture given by Professor Julia Wolf, Michaelmas Term 2023.[1][2]

1.1 Sets, Functions, and Relations

As they contain concepts that we have not yet formally defined, one may want to revisit the examples on this section after studying them in detail later.

1.1.1 Sets

A *set* is a collection of mathematical objects, e.g.

$$\mathbb{R}, \mathbb{N}, \{1,5,9\}, (-2,3]$$

The order of elements in the set is immaterial, and elements are counted only once. For instance, $\{1,7,3\} = \{1,3,7\}$ and $\{3,4,4,8\} = \{3,4,8\}$. We write $x \in \mathbb{A}$ if x is an element of the set A, and $x \notin A$ if not. Two sets are equal if they have the same elements. That is, $A = B$ if and only if for all x,

$$x \in A \Leftrightarrow x \in B$$

In particular, there is only one empty set $\varnothing$.

A set B is a *subset* of A, written $B \subseteq A$, if every element of B is an element of A. B is said to be a *proper subset* of A if $B \subseteq A$ and $B \neq A$, and we write $B \subset A$.[3] Note that if $A = B$, then

$$A \subseteq B \text{ and } B \subseteq A$$

If A is a set and P is a property of (some) elements of A, we can write

$$\{x \in A : P(x)\}$$

[1] Subsection about sequences and series are ommited since they are also thoroughly covered in the Analysis I course.

[2] Although I recommend listening lectures covering those parts to check if there are any distinctions.

[3] Some authors may write both $\subset$ and $\subseteq$ for subset, and only $\subsetneq$ for proper subset.

or

$$\{x \in A \mid P(x)\}$$

for the subset of A comprising those elements for which $P(x)$ holds. If A and B are sets, then their *union*, $A \cup B$, is

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

Their *intersection*, $A \cap B$, is defined to be

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

and we say A and B are disjoint if $A \cap B = \varnothing$. Note that we can view intersection as a special case of subset selection:

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

Similarly, have *set differences*

$$A \backslash B = \{x \in A : x \notin B\}$$

Note that $\cup$ and $\cap$ are *commutative* and *associative*, i.e.

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

and

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

Also, $\cup$ is *distributive* over $\cap$, i.e.

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

and $\cap$ is distributive over $\cup$ too, i.e.

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

Let's prove the last statement. If $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$, so $x \in A$ and ($x \in B$ or $x \in C$). If $x \in B$, then $x \in A \cap B$, and if $x \in C$, then $x \in A \cap C$. In any case, $x \in (A \cap B) \cup (A \cap C)$. Conversely, if $x \in (A \cap B) \cup (A \cap C)$, then $x \in A \cap B$ or $x \in A \cap C$. Either cases, $x \in A$ and $x \in B \cup C$. Hence $x \in A \cap (B \cup C)$. This implies that

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

Given an index set I and a collection of sets A_i indexed by $i \in I$, we write

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \quad \forall i \in I\}$$

and

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

Given sets A and B, we can form their *cartesian product*

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

which is the set of *ordered pairs* (a, b) with $a \in A$, $b \in B$. N.b. we can define $(a, b) = \{\{a, b\}, a\}$; and also we can extend the definition to ordered triples (a, b, c) and so on.

For any set X, we can form the *power set* $\mathcal{P}(X)$ consisting of all subsets of X, i.e.

$$\mathcal{P}(X) = \{Y : Y \subseteq X\}$$

For example, if $X = \{1,2\}$, $\mathcal{P}(X) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$.

Finally, observe that we cannot form a set such that

$$\{x : P(x)\}$$

for some property P. Suppose

$$X = \{x : x \text{ is a set and } x \notin x\}$$

were a set. Then $X \in X$ implies $X \notin X$, which is a contradiction. On the other hand, $X \notin X$ implies $X \in X$. This is known as *Russell's paradox*. Similarly, there is no 'universal' set Y, meaning a set Y such that $\forall x, x \in Y$. Otherwise, we could form X above by subset selection:

$$X = \{x \in Y : x \notin x\}$$

1.1.2 Functions

Given sets A and B, a function f from A to B is a *rule* that assigns to every $x \in A$ a unique element $f(x) \in B$. More formally, a *function* from A to B is a subset

$$f \subseteq A \times B$$

such that for all $x \in A$, there is a unique $y \in B$ such that $(x,y) \in f$. If f is a function from A to B, we write

$$f : A \to B$$

If $(x,y) \in f$, we can write

$$f(x) = y$$

or

$$x \mapsto y$$

We say $f : A \to B$ is *injective* if $\forall a, a' \in A$,

$$a \neq a' \Rightarrow f(a) \neq f(a')$$

Equivalently, f is injective if $f(a) = f(a') \Rightarrow a = a'$. We say f is *surjective* if $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$. If f is both injective and surjective, we say f is *bijective*.

Example 1.1.1.

(1) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is a function.

(2) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 1/x$ is not a function.

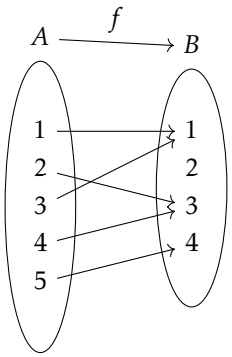
(3) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \pm\sqrt{|x|}$ is not a function.

(4) $f : \mathbb{R} \to \mathbb{R}$,

$$x \mapsto \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

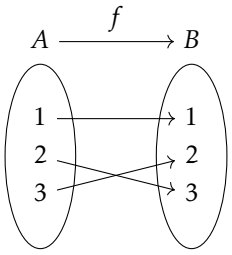
is a function.

(5) $f : A \to B$ given by following



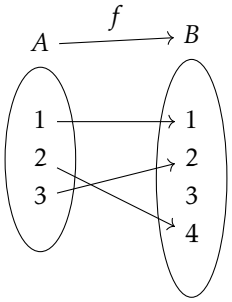
is a function, but it is neither injective nor surjective.

(6) $f : A \to B$ given by following



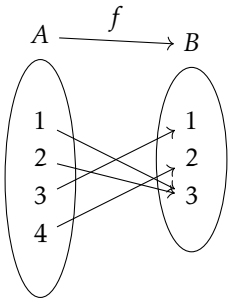
is a bijection.

(7) $f : A \to B$ given by following



is a injection, but not surjective.

(8) $f : A \to B$ given by following



is a surjection, but not injective.

Given $f : A \to B$, we say A is the *domain* of f and B is its *codomain* (or *range*). The *image* of f is the set

$$\mathrm{im}(f) = f(A) = \{f(a) : a \in A\} = \{b \in B : f(a) = b \text{ for some } a \in A\}$$

For example, image of a function $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ is

$$\mathrm{im}(f) = \{y \in \mathbb{R} : y \geqslant 0\}$$

Note that we must specify the domain and codomain of a function when specifying it. Observe that f is surjective if and only if $f(A) = B$. In particular, if $|B| > |A|$, then there can be no surjective function from A to B. Also, there is no injection from A to B if $|A| > |B|$.

For finite sets, if $f : A \to A$, then f is injective $\Leftrightarrow$ f is surjective; and there is no bijection from A to any subset of A. N.b. they might not hold for infinite sets, e.g. $f : \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$ is injective but not surjective, $g : \mathbb{N} \to \mathbb{N}$

$$x \mapsto \begin{cases} x - 1 & x \neq 1 \\ 1 & x = 1 \end{cases}$$

is surjective but not injective, and $h : \mathbb{N} \to \mathbb{N}\backslash\{1\}$, $x \mapsto x + 1$ is a bijection from $\mathbb{N}$ to a proper subset.

Example 1.1.2.

(1) For any set X, we say $\mathrm{id}_X : X \to X$, $x \mapsto x$ is the *identity function* on X.

(2) Given a set X and $A \subseteq X$, we have the *indicator function* or *characteristic function* of A, $1_A : X \to \{0, 1\}$,

$$x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

(3) A sequence of reals $x_1, x_2, \ldots$ is a function $\mathbb{N} \to \mathbb{R}$, $n \mapsto x_n$.

(4) The operation $+$ on $\mathbb{N}$ is a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(a, b) \mapsto a + b$.

(5) A set X has size n if and only if there is a bijection

$$\{1, 2, \ldots, n\} \to X = \{a_1, a_2, \ldots, a_n\}, \quad i \mapsto a_i$$

Given $f : A \to B$ and $g : B \to C$, the *composition*

$$g \circ f : A \to C$$

is defined by

$$a \mapsto g(f(a))$$

In general, $\circ$ is not commutative. However, $\circ$ is associative, i.e. given $f : A \to B$, $g : B \to C$, $h : C \to D$, we have

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

Indeed, for every $x \in A$,

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

and

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

We may therefore drop the brackets and write $h \circ g \circ f$ without ambiguity. We say $f : A \to B$ is *invertible* if there exists $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$, and we write $g = f^{-1}$.

Proposition 1.1.1. f is invertible if and only if it is bijective.

Proof. Given $f : A \to B$, suppose there is a map $g : B \to A$ such that $g \circ f = \mathrm{id}_A$. Then for $a, a' \in A$ such that $f(a) = f(a')$, $g(f(a)) = g(f(a'))$ so $a = a'$. Thus f must be injective. Conversely, if f is injective, we can find g such that $g \circ f = \mathrm{id}_A$ if $b \in f(A)$. If $b \in f(A)$, We let $g(b) = a$ where a is the unique element of A with $f(a) = b$; otherwise, we may choose $g(b)$ freely.

Meanwhile, for a map $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ to exist, we need $f(g(B)) = B$, hence f must be surjective. Conversely, if f is surjective, we can find $g : B \to A$ with $f \circ g = \mathrm{id}_B$: for each $b \in B$, pick some $a \in A$ with $f(a) = b$ and put $g(b) = a$. ∎

N.b. given $f : A \to B$ and $U \subseteq B$, we might use notation

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

to denote the *preimage* of U, even when f does not have an inverse.

1.1.3 Relations

A *relation* on a set X is a subset

$$R \subseteq X \times X$$

and we write

$$aRb$$

for $(a, b) \in R$ to denote that a is related to b. For example, "aRb if $a|b$" is a relation on $\mathbb{N}$. There are three properties a relation might have are of special interest:

- R is *reflective* if $\forall x \in X$, xRx.
- R is *symmetric* if $\forall x, y \in X$, $xRy \Rightarrow yRx$.
- R is *transitive* if $\forall x, y, z \in X$, xRy and $yRz \Rightarrow xRz$.

A relation R is an *equivalence relation* if it is reflective, symmetric, and transitive; and we can write $a \sim b$ for aRb if R is an equivalence relation. For example, "$a \sim b$ if $a \equiv b \mod 5$" is a equivalence relation on $\mathbb{Z}$. This equivalence relation partitions $\mathbb{Z}$ into pieces consisting of related elements,[4] namely

$$\{x \in \mathbb{Z} : x \equiv 0 \mod 5\}, \{x \in \mathbb{Z} : x \equiv 1 \mod 5\}, \ldots, \{x \in \mathbb{Z} : x \equiv 4 \mod 5\}$$

Given a set X, a *partition* of X is a collection of pairwise disjoint subsets, i.e. *parts*, whose union is X. If $\sim$ is an equivalent relation on X, then the *equivalence class* of $x \in X$ is denoted by

$$[x] = \{y \in X : y \sim x\}$$

E.g. for the equivalence relation above,

$$[12] = \{y : y \equiv 2 \mod 5\}$$

Theorem 1.1.2. Let $\sim$ be any equivalence relation on X. Then the equivalence classes form a partition of X.

Proof. Since $\sim$ is reflective, we have $x \in [x]$ for all $x \in X$. Thus

$$\bigcup_{x \in X} [x] = X$$

It remains to show that $\forall x, y \in X$, either $[x] \cap [y] = \varnothing$, or $[x] = [y]$. Suppose $[x] \cap [y] \neq \varnothing$, and let $z \in [x] \cap [y]$. Then $z \sim x$, so by symmetry, $x \sim z$. This with $z \sim y$, we have $x \sim y$ by transitivity. Let now $w \in [y]$, so $y \sim w$. Since $x \sim y$, by transtivity, $x \sim w$. Thus, $w \in [x]$. Hence if $[x] \cap [y] \neq \varnothing$, then $[y] \subseteq [x]$. Similarly, $[x] \subseteq [y]$.
So $[x] = [y]$. ∎

Conversely, given any partition of X, there is an equivalence relation R whose equivalence classes are precisely the parts of the partition: just define aRb if a and b lie in the same part.

Given an equivalence relation R on a set X, the *quotient of X by R* is

$$X/R = \{[x] : x \in X\}$$

The map $q : X \to X/R$, $x \mapsto [x]$ is the *quotient map* or *projection map*.

Example 1.1.3. On $\mathbb{Z} \times \mathbb{N}$, define $(a, b)R(c, d)$ if $ad = bc$, where it turns out that R is an equivalence relation. E.g. one of the equivalence classes will be

$$[(1, 2)] = \{(1, 2), (2, 4), (3, 6), \ldots\}$$

Observe that we may regard $(\mathbb{Z} \times \mathbb{N})/R$ as a copy of $\mathbb{Q}$, by identifying $[(a, b)]$ with $a/b \in \mathbb{Q}$. The quotient map is $q : \mathbb{Z} \times \mathbb{N} \to (\mathbb{Z} \times \mathbb{N})/R$, $(a, b) \mapsto a/b$.

1.2 Numbers and Counting

1.2.1 Natural Number

Intuitively speaking, the natural numbers consists of

$$1, 1 + 1, 1 + 1 + 1, \ldots$$

[4] Elements in each set are related.

But we cannot be sure if the list above contains all of the natural numbers, or if there are no duplicate numbes. Hence, for more rigorous understanding, we assume the natural numbers, $\mathbb{N}$, is a set containing "1", with an operation "$+$" satisfying

(1) $\forall n \in \mathbb{N}$, $n+1 \neq 1$.

(2) $\forall m, n \in \mathbb{N}$, if $m \neq n$, then $m+1 \neq n+1$.

(3) For any property $P(n)$, if $P(1)$ is true and $\forall n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$, then $P(n)$ is true for all natural numbers.

(1), (2), and (3) are known as the *Peano axioms*, and (3) is called the *induction axiom*. (1) and (2) capture the idea that any two natural numbers are distinct; (3) captures our intuition that the list is complete.[5] Now we can write 2 for $1+1$, 3 for $1+1+1$ etc. and we can define "$+k$" for any natural number k:

Definition 1.2.1. For every natural number n,

$$n + (k+1) = (n+k) + 1$$

It can be thought from induction, taking $P(k) =$ "$+k$ is defined". Similarly, we can define multiplication, powers etc. satisfying

(1) $\forall a, b$, $a + b = b + a$ ($+$ is commutative).

(2) $\forall a, b$, $ab = ba$ ($\cdot$ is commutative).

(3) $\forall a, b, c$, $a + (b + c) = (a + b) + c$ ($+$ is associative).

(4) $\forall a, b, c$, $a(bc) = (ab)c$ ($\cdot$ is associative).

(5) $\forall a, b, c$, $a(b + c) = ab + ac$ (multiplication is distributive over addition).

We define "$a < b$" if $a + c = b$ for some $c \in \mathbb{N}$, satisfying

(6) $\forall a, b, c$, $a < b \Rightarrow a + c < b + c$.

(7) $\forall a, b, c$, $a < b \Rightarrow ac < bc$.

(8) $\forall a, b, c$, $a < b$ and $b < c \Rightarrow a < c$.

(9) $\forall a$, $\neg(a < a)$.

The induction axiom is also known as the *weak principle of induction* (WPI). Equivalent form of this is the strong principle of induction (SPI):

Theorem 1.2.1. (*Strong Principle of Induction*) If

(1) $P(1)$ holds, and

(2) $\forall n \in \mathbb{N}$, we have $(P(m)\, \forall m \leqslant n) \Rightarrow P(n+1)$,

then $P(n)$ holds $\forall n \in \mathbb{N}$.

Clearly, SPI $\Rightarrow$ WPI. To see that WPI $\Rightarrow$ SPI, apply the former to

$$Q(n) = \text{"}P(m) \text{ holds } \forall m \leqslant n\text{"}$$

[5] Take $P(n) =$ "n is on this list".

Theorem 1.2.2. (*Well-Ordering Principle* (WOP)) If $P(n)$ holds for some $n \in \mathbb{N}$, then there is a least $n \in \mathbb{N}$ such that $P(n)$ holds. "*Every non-empty subset of* $\mathbb{N}$ *has a minimal element*."

Theorem 1.2.3. SPI is equivalent to WOP.

Proof. First we show that WOP implies SPI. We assume (1) and (2) of SPI, and show that $P(n)$ holds $\forall n \in \mathbb{N}$, using WOP. Suppose, on the contrary, that $P(n)$ is not true for all $n \in \mathbb{N}$. Then,

$$C = \{n \in \mathbb{N} \mid P(n) \text{ is false}\} \neq \varnothing$$

By well-ordering principle, C has a minimal element, say m. Now $\forall k < m$, $k \notin C$ (by minimality of m), so $P(k)$ holds $\forall k < m$. But by (2) of strong principle of induction, $P(m)$ holds, contradicting $m \in C$. Hence SPI holds.

To show that SPI implies WOP, suppose there is no least $n \in \mathbb{N}$ such that $P(n)$ holds. We want to show that $P(n)$ does not hold for any $n \in \mathbb{N}$, using SPI. Consider

$$Q(n) = \neg P(n)$$

Certainly $P(1)$ is false,[6] so $Q(1)$ holds. Given $n \in \mathbb{N}$, suppose that $Q(k)$ is true $\forall k < n$. Then $P(k)$ is false $\forall k < n$. So $P(n)$ is false as otherwise n would be the minimal element for which P holds. Hence $Q(n)$ is true, and (2) of SPI is satisfied, so $Q(n)$ holds for all $n \in \mathbb{N}$. Thus $P(n)$ is false $\forall n \in \mathbb{N}$. ■

Well-ordering principle enables us to prove $P(n)$ is true $\forall n \in N$ as follows: if not, there is a minimal counterexample, and we may try and derive a contradiction.

1.2.2 Integer

The integer set, $\mathbb{Z}$, consist of all symbols n, $-n$, where $n \in \mathbb{N}$, along with 0. We can also define $+$ and $\cdots$ etc. on $\mathbb{Z}$ from $\mathbb{N}$, and check that the usual rules (1) - (5) of arithmetic hold. We also have

(10) $\forall a \in \mathbb{Z}$, $a + 0 = 0$ (identity for $+$).

(11) $\forall a \in \mathbb{Z}$, $\exists b \in \mathbb{Z}$ such that $a + b = 0$ (inverses for $+$). Here, $b = -a$.

Similarly define $a < b$ if $a + c = b$ for some $c \in \mathbb{N}$. Rules (6), (8), and (9) continue to hold, but (7) must be modified:

(7) $\forall a, b, c \in \mathbb{Z}$, $a < b$ and $c > 0 \Rightarrow ac < bc$.

1.2.3 Rational Number

The rational number set, $\mathbb{Q}$, consist of all expressions a/b, where a, b are integers, $b \neq 0$, and a/b and c/d are regarded as the same if $ad = bc$. Define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and one can check it does not matters how we wrote a/b or c/d (commutivity). We similarly define multiplication, and

$$\frac{a}{b} < \frac{c}{d}$$

where $b, d > 0$ if $ad < bc$. All the previous rules apply to rational numbers, but, furthermore,

[6] Else 1 would be the minimal element.

(12) $\forall a \in \mathbb{Q}$, $a \neq 0$, $\exists b$ such that $ab = 1$ (inverse for $\cdot$).

Finally, note that

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

1.2.4 Finite and Infinite Sets

$*$ Binomial coefficients

We write

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$$

to include 0 in the natural number set. Given $n \in \mathbb{N}_0$, we say a set A has *size* n if we can write

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

with the elements a_i distinct. For example, $\{1, 3, 7\}$ has size 3, $\varnothing$ has size 0. We say A is *finite* if $\exists n \in \mathbb{N}_0$ such that A has size n, and A is *infinite* otherwise.

Proposition 1.2.4. A set of size n has exactly 2^n subsets.

Proof. (*Method 1*) We may assume that our set is $\{1, 2, \ldots, n\}$. To specify a subset S of $\{1, 2, \ldots, n\}$, we must specify if $1 \in S$ or $1 \notin S$, then $2 \in S$ or $2 \notin S$, and so on. Hence the number of choices for S is

$$2 \cdot 2 \cdot 2 \cdots 2 = 2^n$$

■

Proof. (*Method 2*) We prove by induction on n. Clearly true for $n = 0$. Given $n > 0$, and $T \subseteq \{1, 2, \ldots, n-1\}$, how many $S \subseteq \{1, 2, \ldots, n\}$ are there such that

$$S \cap \{1, 2, \ldots, n-1\} = T$$

There are exactly 2, namely T and $T \cup \{n\}$. Hence the number of subsets of $\{1, 2, \ldots, n\}$ is $2(2^{n-1}) = 2^n$ by the induction hypothesis. ■

If a set A has size n, we write

$$|A| = n$$

or $\#A = n$. So Proposition 1.2.4 states that

$$|A| = n \Rightarrow |\mathcal{P}(A)| = 2^n$$

Given $n \in \mathbb{N}_0$ and $0 \leqslant k \leqslant n$, we write $\binom{n}{k}$ for the number of subsets of an n-element set that are of size k. That is,

$$\binom{n}{k} = |\{S \subseteq \{1, 2, \ldots, n\} : |S| = k\}|$$

$\binom{n}{k}$ is called a *binomial coefficient*. For example, the subsets of size 2 of $\{1, 2, 3, 4\}$ are precisely $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$ so $\binom{4}{2} = 6$. Note that by definition $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = n$ (for $n > 0$), and

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

Also, we have

$$\binom{n}{k} = \binom{n}{n-k}$$

for all $n \in \mathbb{N}_0$, $0 \leqslant k \leqslant n$. Moreover,

$$\binom{n}{k} = \binom{n-1}{k-1}\binom{n-1}{k}$$

for all $n \in \mathbb{N}$, $1 \leqslant k \leqslant n-1$. N.b. we can use this property to obtain the *Pascal's triangle*.

Proposition 1.2.5. We have

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \frac{n!}{(n-k)!k!}$$

Proof. Given a set of size n, there are $n(n-1)\cdots(n-k+1)$ ways to pick k elements, in order, one by one. But each subset of size k is picked in $k(k-1)\cdots 1$ ways by this method. Hence the number of subsets of size k in $\{1,2,\ldots,n\}$ is

$$\frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$$

■

Note that the formula tells us, for example, that

$$\binom{n}{2} = \frac{n(n-1)}{2} \sim \frac{n^2}{2}$$

and

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{3!} \sim \frac{n^3}{6}$$

for large n.

Theorem 1.2.6. (*Binomial Theorem*) For all $a, b \in \mathbb{R}$, $n \in \mathbb{N}$,

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

Proof. When we expand

$$(a+b)^n = (a+b)(a+b)\cdots(a+b)$$

we obtain terms of the form $a^{n-k}b^k$, $0 \leqslant k \leqslant n$, and the number of terms of the form $a^{n-k}b^k$ is $\binom{n}{k}$ as we must specify k brackets from which to pick b. Hence

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

■

∗ Sizes of sets

Theorem 1.2.7. (*Inclusion-Exclusion Principle*) Let $S_1, S_2, \ldots, S_n$ be finite sets. Then

$$|S_1 \cup S_2 \cup \cdots \cup S_n| = \sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \cdots + (-1)^{n+1} \sum_{|A|=n} |S_A|$$

where $S_A = \bigcap_{i \in A} S_i$ and $\sum_{|A|=k}$ is taken over all $A \subseteq \{1, 2, \ldots, n\}$ of size k. Equivalently,

$$\left| \bigcup_{i=1}^{n} S_i \right| = \sum_{r=1}^{n} (-1)^{r+1} \sum_{|A|=r} \left| \bigcap_{i \in A} S_i \right|$$

Let $x \in S_1 \cup S_2 \cdots \cup S_n$, say $x \in S_i$ for k of the S_i. We want x to be counted exactly once in the right hand side. Indeed,

$$\#\{A : |A| = 1 \text{ with } x \in S_A\} = k$$

$$\#\{A : |A| = 1 \text{ with } x \in S_A\} = \binom{k}{2}$$

and in general,

$$\#\{A : |A| = 1 \text{ with } x \in S_A\} = \begin{cases} \binom{k}{r} & r \leqslant k \\ 0 & r > k \end{cases}$$

Thus the number of times x is counted on the right hand side is

$$\begin{aligned} k - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k+1} \binom{k}{k} &= 1 - \left(1 - k + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k \binom{k}{k} \right) \\ &= (1 + (-1))^k + 1 = 1 \end{aligned}$$

for $k \geqslant 1$ by the binomial theorem.

1.3 Elementary Number Theory

1.3.1 Primes

Definition 1.3.1. A natural number $n \geqslant 2$ is *prime* if its only factors are ± 1 and $\pm n$. If $n \geqslant 2$ is not prime, then it is *composite*.

Proposition 1.3.1. Every natural number $n \geqslant 2$ can be written as a product of primes.

Proof. It is true for $n = 2$. Let $n > 2$ and suppose that claim holds up to and including $n - 1$. If n is prime, done. If n is composite, then $n = ab$ for some $1 < a, b < n$.

By the induction hypothesis, we have

$$\begin{aligned} a &= p_1 p_2 \cdots p_k \\ b &= q_1 q_2 \cdots q_l \end{aligned}$$

for some primes $p_1, \ldots, p_k, q_1, \ldots, q_l$. Hence

$$n = ab = p_1 \cdots p_k q_1 \cdots q_l$$

is a product of primes. Proof is complete by induction. ■

Theorem 1.3.2. There are infinitely many primes.

Proof. (Euclid, 300 B.C.) Suppose there are finitely many primes, say $p_1, \ldots, p_k$. Let $N = p_1 \cdots p_k + 1$. Then $p_1 \nmid N$, else

$$p_1 | N - p_1 \cdots p_k = 1$$

Likewise, none of $p_2, p_3, \ldots, p_k$ divide N, contradicting the fact that N can be written as a product of primes (Proposition 1.3.1). ■

Can a number have more than one representation as a product of primes? Our proof of Proposition 1.3.1 does not give uniqueness.

Definition 1.3.2. Given $a, b \in \mathbb{N}$, a natural number c is the *highest common factor* (hcf) or *greatest common divisor* (gcd) of a and b if

(1) $c|a$ and $c|b$;

(2) $d|a$ and $d|b \Rightarrow d|c$.

We write $c = \text{hcf}(a, b)$, or $c = \gcd(a, b)$, or $c = (a, b)$.

For example, the factors of 12 are $1, 2, 3, 4, 6, 12$, and those of 18 are $1, 2, 3, 6, 9, 18$. So the common factors are $1, 2, 3, 6$, hence $\gcd(12, 18) = 6$. But observe that if a and b had common factors $1, 2, 3, 4, 6$, then a and b would have no gcd according to Definition 1.3.2 (2). We will need to show that $\gcd(a, b)$ always exists.

Proposition 1.3.3. (*Division Algorithm*) Let $n, k \in \mathbb{N}$. Then we can write

$$n = qk + r$$

where q and r are integers with $0 \leqslant r \leqslant k - 1$.

Proof. It is true for $n = 1$. Suppose $n \geqslant 2$ and statement holds for $n - 1$, i.e.

$$n - 1 = qk + r$$

for some $q, r \in \mathbb{Z}$, $0 \leqslant r \leqslant k - 1$.

- If $r < k - 1$, then $n = (n - 1) + 1 = qk + (r + 1)$.
- If $r = k - 1$, then $n = (n - 1) + 1 = qk + (k - 1) + 1 = (q + 1)k$.

■

Note that q and r obtained by the division algorithm are unique: if $n = qk + r = q'k + r'$, then

$$(q - q')k = r' - r$$

is an integer smaller than k and larger than $-k$ so $q = q'$ and $r = r'$.

We now introduce the *Euclid's Algorithm*. We break down a and b until $r_{n+1} = 0$ as follows;

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + r_{n+1} \end{aligned}$$

and the algorithm returns r_n. N.b. the algorithm terminates in $n < b$ steps, since

$$b > r_1 > r_2 > \ldots > r_n > 0$$

Theorem 1.3.4. The output of Euclid's algorithm with input a, b is $\gcd(a,b)$.

Proof. We show (1) and (2) from Definition 1.3.2.

(1) Have r_n/r_{n-1} (as $r_{n+1}=0$), so r_n/r_{n-2} and r_n/r_i $\forall i = 1,2,\ldots,n-1$ by induction. Hence r_n/b and r_n/a.

(2) Given d such that $d|a$ and $d|b$, have $d|r_1$, so $d|r_2$ and $d|r_i$ $\forall i = 1,2,\ldots,n$ by induction.

■

By the division algorithm and Euclid's algorithm, we have found out that the gcd of any two natural numbers always exists, and is unique. For example, consider Euclid's algorithm with 87 and 52 as inputs:

$$\begin{aligned} 87 &= 1\cdot 52 + 35 \\ 52 &= 1\cdot 35 + 17 \\ 35 &= 2\cdot 17 + 1 \\ 17 &= 17\cdot 1 \end{aligned}$$

so $\gcd(87,52) = 1$.

Definition 1.3.3. When $\gcd(a,b) = 1$, we say that a and b are *coprime*.

Observe that we can reverse the Euclid's algorithm:

$$\begin{aligned} 1 &= 35 - 2\cdot 17 \\ &= 35 - 2(52 - 1\cdot 35) \\ &= -2\cdot 52 + 3\cdot 35 \\ &= -2\cdot 52 + 3(87 - 1\cdot 52) \\ &= -5\cdot 52 + 3\cdot 87 \end{aligned}$$

Theorem 1.3.5. $\forall a,b \in \mathbb{N}$, $\exists x,y \in \mathbb{Z}$ such that

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

"*We can write* $\gcd(a,b)$ *as a linear combination of a and b.*"

Proof. (*Method 1*) Run Euclid's algorithm with input a, b to obtain an output r_n. At step n, have

$$r_n = xr_{n-1} + yr_{n-2}$$

for some $x,y \in \mathbb{Z}$. But from step $n-1$, we see that r_{n-1} is expressible as

$$r_{n-1} = xr_{n-2} + yr_{n-3}$$

for some $x,y \in \mathbb{Z}$, whence

$$r_n = xr_{n-2} + yr_{n-3}$$

for some $x,y \in \mathbb{Z}$. Continuing inductively, we have $\forall i = 2,\ldots,n-1$,

$$r_n = xr_i + yr_{i-1}$$

for some $x,y \in \mathbb{Z}$. Thus

$$r_n = xa + yb$$

for some $x,y \in \mathbb{Z}$, by steps one and two. ■

Remark 1.3.1. Euclid's algorithm not only proves the existence of $x, y \in \mathbb{Z}$, but gives a quick way to find them.

Proof. (*Method 2*) Let g be the least positive linear combination of a and b, i.e. the least positive integer of the form $xa + yb$ for some $x, y \in \mathbb{Z}$. We shall show that $g = \gcd(a, b)$ (Definition 1.3.2).

To see (2), observe that given d such that $d|a$ and $d|b$, we have

$$d|ax + by \quad \forall x, y \in \mathbb{Z}$$

so in particular, $d|g$.

To see (1), suppose that $g \nmid a$. Then we can write

$$a = qg + r$$

for some $q, r \in \mathbb{Z}$ with $0 < r < g$. Hence

$$r = a - qg = a - q(xa + yb)$$

is also a positive linear combination of a and b, and strictly smaller than g, contradicting the definition of g. Therefore, $g|a$ and by the same argument, $g|b$. ■

Remark 1.3.2. (*Method 2*) tells us that $\gcd(a, b)$ exists and is a linear combination of a and b, but gives no way to find $\gcd(a, b)$ or the coefficients $x, y \in \mathbb{Z}$.

With help of Theorem 1.3.5, we can tell

$$160x + 72y = 33$$

does not have any integer solution, but

$$87x + 52y = 33$$

does. Let's formalise this.

Corollary 1.3.5.1. (*Bézout's Theorem*) Let $a, b \in \mathbb{Z}$. Then the equation

$$ax + by = c$$

has a solution in integers x, y if and only if

$$\gcd(a, b)|c$$

Proof. Let $g = \gcd(a, b)$. Suppose there are $x, y \in \mathbb{Z}$ such that

$$ax + by = c$$

Then, since $g|a$ and $g|b$, $g|c$.

Conversely, suppose $g|c$. But Theorem 1.3.5 implies that there exist $x, y \in \mathbb{Z}$ such that

$$g = ax + by$$

But then

$$c = \frac{c}{g}g = \frac{c}{g}(ax + by) = a\left(x\frac{c}{g}\right) + b\left(y\frac{c}{g}\right)$$

■

Proposition 1.3.6. If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Proof. Suppose $p|ab$ but $p \nmid a$. We claim $p|b$.

Since p is prime and $p \nmid a$, $\gcd(a,p) = 1$. Thus by Theorem 1.3.5, there exists $x, y \in \mathbb{Z}$ such that $xp + ya = 1$. It follows that $xpb + yab = b$, whence b is a multiple of p (as each of p and ab is). ■

Remark 1.3.3.

(1) Similarly,

$$p|a_1 a_2 \cdots a_n \Rightarrow p|a_i$$

for some $i = 1, 2, \ldots, n$. Indeed, Proposition 1.3.1 tells us that if $p|a_1 a_2 \cdots a_n$, the $p|a_1$ or $p|a_2 \cdots a_n$, so we may conclude by induction on the number of terms in the product.

(2) We do need p to be prime.

Theorem 1.3.7. (*Fundamental Theorem of Arithmetic*) Every natural number $n \geqslant 2$ is expressible as a product primes, uniquely up to reordering.

Proof. Existence of factorisation follows from Proposition 1.3.1. We can show uniqueness by induction. Clearly it is unique for $n = 2$. Given $n \geqslant 2$, suppose

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

where p_i, q_j are all prime. Want to show that $k = l$, and, after reordering, $p_i = q_i$ $\forall i = 1, \ldots, k$. We have

$$p_1 | n = q_1 q_2 \cdots q_l$$

so by Proposition 1.3.6,

$$p_1 | q_i$$

for some i. Relabelling the q_i, we may assume that $p_1|q_1$. Since q_1 is prime, $p_1 = q_1$, so

$$\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l < n$$

By the induction hypothesis, $k = l$, and, after reordering, $p_2 = q_2, \ldots, p_k = q_k$. ■

Remark 1.3.4. There are arithmetical systems (permitting addition and multiplication) in which factorisation is not unique.

For example, consider $\mathbb{Z}[\sqrt{-3}]$, meaning all complex numbers of the form $x + y\sqrt{-3} = x + y\sqrt{3}i$ where $x, y \in \mathbb{Z}$. We can add and multiply two elements of $\mathbb{Z}[\sqrt{-3}]$ to get another element of $\mathbb{Z}[\sqrt{-3}]$, e.g.

$$(1 + \sqrt{-3}) + (q - \sqrt{-3}) = 2$$

$$(1 + \sqrt{-3})(q - \sqrt{-3}) = 4$$

In $\mathbb{Z}[\sqrt{-3}]$, we can define what it means to be a prime, and both $1+\sqrt{-3}$ and $1-\sqrt{-3}$ happen to be prime in this sense. But, we can also write $4 = 2 \cdot 2$, so factorisation is not unique.

Let's take a look at some applications of the fundamental theorem of arithmetic.

(1) What are the factors of $n = 2^3 3^7 11$? – All numbers of the form $2^a 3^b 11^c$ where $0 \leqslant a \leqslant 3$, $0 \leqslant b \leqslant 7$, $0 \leqslant c \leqslant 1$. There are no others: if, for example, $7|n$, then we would have a factorisation of n involving 7, contradicting uniqueness. More generally, the factors of $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ are precisely the numbers of the form

$$p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

with $0 \leqslant b_i \leqslant a_i \ \forall i = 1, 2, \ldots, k$.

(2) What are common factors of $2^3 \cdot 3^7 \cdot 5 \cdot 11^3$ and $2^4 \cdot 3^2 \cdot 11 \cdot 13$? – All numbers of the form $2^3 3^b 11^c$ where $0 \leqslant a \leqslant 3$, $0 \leqslant b \leqslant 2$, $0 \leqslant c \leqslant 1$. Thus the gcd is $2^3 \cdot 3^2 \cdot 11$. In general, the gcd of $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where $a_i, b_i \geqslant 0$, is

$$p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}$$

(3) What are the common multiples of the two numbers in (2)? – All numbers of the form $2^a 3^b 5^c 11^d 13^2$ where $a \geqslant 4$, $b \geqslant 7$, $c \geqslant 1$, $d \geqslant 3$, $e \geqslant 1$, times any integer. Hence $2^4 \cdot 3^7 \cdot \cdot 5 \cdot 11^3 \cdot 13$ is a common multiple, and any other common multiple is a multiple of it. We say that it is the *least common multiple* (lcm) of the two numbers. In general, the lcm of $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where $a_i, b_i \geqslant 0$, is

$$p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}$$

Since $\min\{a_i, b_i\} + \max a_i, b_i = a_i + b_i$, we have

$$\gcd(x, y) \cdot \operatorname{lcm}(x, y) = xy$$

for any x, y.

(4) Another proof of Theorem 1.3.2, due Erdös (1930): let $p_1, p_2, \ldots, p_k$ be all the primes. Any number which is a product of jest these primes is of the form $(*)$:

$$p_1^{j_1} p_2^{j_2} \cdots p_k^{j_k} = m^2 p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$$

where $i_l = 0$ or 1. Let $M \in \mathbb{N}$. If a number is equal or less than M is of the form $(*)$, then $m \leqslant \sqrt{M}$. So there are at most $\sqrt{M} 2^k$ numbers of the form $(*)$ that are equal or less than M. If $M > \sqrt{M} 2^k$, i.e. if $M > 4^k$, then there must be a number equal or less than M which is not of the form $(*)$. But this number must have a prime factor not amongst the $p_1, \ldots, p_k$. ■

Proof by Euclid tells us that k^{th} prime is less than 2^{2^k}, while the proof by Erdös tells us k^{th} prime is less than 4^k. In fact, we know k^{th} prime is $\sim k \ln k$ (*Prime Number Theorem*).

1.3.2 Modular Arithmetic

Let $n \geqslant 2$ be a natural number. Then the *integer modulo n*, written as $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$ consist of the integers, with two regarded as the same if they differ by a multiple of n. If x and y are the same in $\mathbb{Z}_n$, we write

$$x \equiv y \mod n$$

or $x \equiv y \quad (n)$ or $x = y$ in $\mathbb{Z}_n$. Thus

$$\begin{aligned} x \equiv y \mod n &\Leftrightarrow n|x-y \\ &\Leftrightarrow x = y + kn \text{ for some } k \in \mathbb{Z} \end{aligned}$$

N.b. if $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then

$$n|(a-a') + (b-b') = (a+b) - (a'+b')$$

so $a + b \equiv a' + b' \mod n$. Similarly,

$$n|(a-a')b + a'(b-b') = ab - a'b'$$

so $ab = a'b' \mod n$. Hence we can do arithmetic on modulo n with inheriting the usual rules of arithmetic in $\mathbb{Z}$.

Example 1.3.1. Does $2a^2 + 3b^3 = 1$ have a solution with $a, b \in \mathbb{Z}$?
If there is a solution, then $2a^2 \equiv 1 \mod 3$, but $2 \cdot 0^2 \equiv 0$, $2 \cdot 1^2 \equiv 2$, $2 \cdot 2^2 \equiv 2 \mod 3$ so there is no solution.

∗ Solution of congruences

Example 1.3.2. Solve $7n \equiv 2 \mod 10$.
We note $3 \cdot 7 \equiv 1 \mod 10$ so $3 \cdot 7n \equiv 3 \cdot 2 \mod 10$ and $n \equiv 6 \mod 10$.

As shown in the example above, given $a, b \in \mathbb{Z}$, we say that b is an *inverse of a modulo n* if

$$ab \equiv 1 \mod n$$

We say that a is *invertible modulo n* or that a is a *unit modulo n*, if it has an inverse. For example, in $\mathbb{Z}_{10}$, 3 is an inverse of 7, and both 3 and 7 are units modulo 10; but 4 is not a unit modulo 10 since $4n \not\equiv 1 \mod 10$ for all $n \in \mathbb{Z}$.

Remark 1.3.5. If a is a unit modulo n, then

(1) its inverse is unique. Suppose $\exists b, b'$ such that

$$ab \equiv ab' \equiv 1 \mod n$$

then

$$b \equiv bab \equiv bab' \equiv b' \mod n$$

(2) we can write a^{-1} for its inverse.

(3) if $ab \equiv ac \mod n$, then $b \equiv c \mod n$.

However, this is not true in general, e.g.

$$4 \cdot 3 \equiv 4 \cdot 8 \mod 10$$

but $3 \not\equiv 8 \mod 10$.

Proposition 1.3.8. Let p be prime. Then every $a \neq 0 \mod p$ is a unit modulo p.

Proof. From $\gcd(a, p) = 1$, $\exists x, y \in \mathbb{Z}$ such that $ax + py = 1$ (Corollary 1.3.5.1). Hence $ax = 1 - py$, so

$$ax \equiv 1 \mod p$$

for some $x \in \mathbb{Z}$. ■

Proposition 1.3.9. Let $n \geqslant 2$. Then a is a unit modulo n if and only if $\gcd(a,n) = 1$.

Proof.

$$\begin{aligned}\gcd(a,n) = 1 &\Leftrightarrow ax + ny = 1 \text{ for some } x, y \in \mathbb{z} \\ &\Leftrightarrow ax = 1 - ny : \text{ for some } x, y \in \mathbb{z} \\ &\Leftrightarrow ax \equiv 1 \mod n : \text{ for some } x, y \in \mathbb{z}\end{aligned}$$

Corollary 1.3.9.1. If $\gcd(a,n) = 1$, then the congruence

$$ax \equiv b \mod n$$

has a unique solution. In particular, if $\gcd(a,n) = 1$, then there is a unique inverse of a modulo n.

For cases like $ax \equiv b \mod n$ with $\gcd(a,n) = d \neq 1$, the solution may not exist. $n|ax - b$ so $d|ax - b$ and thus $d|b$ for solution to exist. If $d|b$, write $n = dn'$, $a = da'$, $b = db'$. Then,

$$\begin{aligned}ax \equiv b \mod n &\Leftrightarrow ax - b = kn \text{ for some } k \in \mathbb{Z} \\ &\Leftrightarrow da'x - db' = kdn' : \text{ for some } k \in \mathbb{Z} \\ &\Leftrightarrow a'x - b' = kn' : \text{ for some } k \in \mathbb{Z} \\ &\Leftrightarrow a'x \equiv b' \mod n'\end{aligned}$$

Since $\gcd(a', n') = 1$, $a'x \equiv b' \mod n'$ has a unique solution.

Example 1.3.3. Solve $7x \equiv 4 \mod 30$.
We have $\gcd(7, 30) = 1$, so by Euclid's algorithm, $13 \cdot 7 - 3 \cdot 30 = 1$. Hence $13 \cdot 7 \equiv 1 \mod 30$, whence

$$x \equiv 13 \cdot 4 \equiv 22 \mod 30$$

Example 1.3.4. Solve $10x \equiv 12 \mod 34$.
This is equivalent with $5x \equiv 6 \mod 17$, and we can now solve as the example above to obtain $x \equiv 6 \cdot 7 \equiv 8 \mod 17$.

∗ Simultaneous congruences

Note

$$x \equiv 5 \mod 12 \Rightarrow \begin{cases} x \equiv 2 \mod 3 \\ x \equiv 1 \mod 4 \end{cases}$$

However, we cannot be sure if the converse is true, i.e. does $x \equiv 2 \mod 3$ and $x \equiv 1 \mod 4$ imply that $x \equiv 5 \mod 12$? It turns out that it is true for the case above, but it is not generally true – see $x \equiv 1 \mod 4$ and $x \equiv 2 \mod 6$.

Theorem 1.3.10. (*The Chinese Remainder Theorem*) Let m, n be coprime, and $a, b \in \mathbb{Z}$. Then there is a unique solution modulo mn to the simultaneous congruences

$$x \equiv a \mod m \text{ and } x \equiv b \mod n$$

That is, there is a solution x to

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

and y is a solution if and only if $x \equiv y \mod mn$.

Proof. We first prove existence. Since $\gcd(m,n) = 1$, $\exists s,t \in \mathbb{Z}$ with $sm + tn = 1$. Note

$$sm \equiv 1 \mod n, \quad sm \equiv 0 \mod m$$

and

$$tn \equiv 1 \mod m, \quad tn \equiv 0 \mod n$$

Hence

$$\begin{aligned} x = a(tn) + b(sm) &\equiv a \mod m \\ &\equiv b \mod n \end{aligned}$$

Next, for uniqueness, suppose y is also a solution, i.e. $y \equiv a \mod m$ and $y \equiv b \mod n$. This implies

$$\begin{aligned} y \equiv x \mod m \text{ and } y \equiv x \mod n &\Leftrightarrow m|y-x \text{ and } n|y-x \\ &\Leftrightarrow mn|y-x \text{ since } \gcd(m,n) = 1 \\ &\Leftrightarrow y \equiv x \mod mn \end{aligned}$$

■

Remark 1.3.6. Theorem 1.3.10 can be extended, by induction, to more than two moduli:
if $m_1, m_2, \ldots, m_k$ are pairwise coprime, then $\forall a_1, a_2, \ldots, a_k \in \mathbb{Z}$, $\exists x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

Definition 1.3.4. We define the *Euler totient function*, $\varphi(m)$, as the number of integers a with $1 \leqslant a \leqslant m$ such that $\gcd(a,m) = 1$, i.e. $\varphi(m)$ is the number of units modulo m. Additionally, we define $\varphi(1) = 1$.

For example, when p is prime, $\varphi(p) = p - 1$, and $\varphi(p^2) = p^2 - p$. When p, q are distinct primes,

$$\varphi(p,q) = pq - p - q + 1$$

Next, let's take a look at behavior of a power of an integer modulo p.

Theorem 1.3.11. (*Fermat's Little Theorem*) Let p be a prime. Then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$. Equivalently,

$$a^{p-1} \equiv 1 \mod p$$

for all $a \not\equiv 0 \mod p$.

Proof. If $a \not\equiv 0 \mod p$, then a is a unit mod p. Thus $ax \equiv ay \mod p$ if and only if $x \equiv y \mod p$. Hence the numbers $a, 2a, \ldots, (p-1)a$ are pairwise incongruent (distinct) modulo p, and $\not\equiv 0 \mod p$, so they are $1, 2, 3, \ldots, p-1$ in some order. Hence

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \mod p$$

or

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

But $(p-1)!$ is a unit mod p (since it is a product of units), so we can cancel it to obtain $a^{p-1} \equiv 1 \mod p$. ■

Theorem 1.3.12. (*Fermat-Euler Theorem*) Let $\gcd(a,m)=1$. Then $a^{\varphi(m)} \equiv 1 \mod m$.

Proof. Let

$$U = \{x \in \mathbb{Z} \mid 0 < x < m, \gcd(x,m) = 1\}$$

be the $\varphi(m)$ numbers that are coprime to m. Label them $u_1, u_2, \ldots, u_{\varphi(m)}$. Then $au_1, au_2, \ldots, au_{\varphi}(m)$ are all distinct and invertible modulo m (since a is a unit), and hence they are $u_1, u_2, \ldots, u_{\varphi(m)}$ in some order. It follows that

$$au_1 \cdot au_2 \cdots au_{\varphi(m)} \equiv u_1 u_2 \cdots u_{\varphi(m)} \mod m$$

i.e.

$$a^{\varphi(m)} z \equiv z \mod m$$

where $z = u_1 u_2 \cdots u_{\varphi(m)}$ is a product of unit modulo m, whence itself a unit. Thus we may cancel it to obtain the theorem. ■

Lemma 1.3.13. Let p be prime. Then

$$x^2 \equiv 1 \mod p \equiv x \equiv 1 \text{ or } -1 \mod p$$

Proof.

$$\begin{aligned} x^2 \equiv 1 \mod p &\Leftrightarrow x^2 - 1 \equiv 0 \mod p \\ &\Leftrightarrow (x+1)(x-1) \equiv 0 \mod p \end{aligned}$$

But by Proposition 1.3.6, $x+1 \equiv 0 \mod p$ or $x-1 \equiv 0 \mod p$. Therefore, $x \equiv -1$ or $1 \mod p$. ■

More generally, a non-zero polynomial of degree k over $\mathbb{Z}_p$ has at most k roots in $\mathbb{Z}_p$.

Theorem 1.3.14. (*Wilson's Theorem*) Let p be prime. Then $(p-1)! \equiv -1 \mod p$.

Proof. It is true for $p = 2$. Now assume $p > 2$. Note that the units modulo p comes in pairs whose product is 1, together with some elements that are self-inverse, i.e. elements x such that $x^2 \equiv 1 \mod p$. By Lemma 1.3.13, the elements that are self-inverse are 1 and -1, so the remaining $p-3$ units of $\mathbb{Z}_p$ come in inverse pairs. Hence $(p-1)!$ is the product of $(p-3)/2$ pairs of inverses together with 1 and -1, giving $(p-1)! \equiv -1 \mod p$. ■

Proposition 1.3.15. Let p be an odd prime. Then -1 is a square modulo p, i.e. $\exists x \in \mathbb{Z}$ such that $x^2 \equiv -1 \mod p$, if and only if $p \equiv 1 \mod 4$.

Proof. Suppose $p \equiv 1 \mod 4$. By Wilson's theorem,

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1 \cdot 2 \cdot \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-3)(p-2)(p-1) \\ &\equiv 1 \cdot 2 \cdot \cdots \left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right) \cdots (-3)(-2)(-1) \\ &= (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2}\right)!\right)^2 \mod p \end{aligned}$$

But if $p = 4k + 1$ for some $k \in \mathbb{Z}$, then

$$-1 \equiv (-1)^{2k} \left(\left(\frac{p-1}{2} \right)! \right)^2 \mod p$$

so -1 is a square modulo p.

Suppose, on the other hand, that $p \equiv -1 \mod 4$, i.e. $p = 4k + 3$ for some $k \in \mathbb{Z}$. If -1 were a square modulo p, i.e. if there were $z \in \mathbb{Z}$ such that $z^2 \equiv -1 \mod p$, then by Fermat's little theorem,

$$1 \equiv z^{p-1} \equiv z^{4k+2} \equiv z^{2(2k+1)} \equiv (-1)^{2k+1} \equiv -1 \mod p$$

which is a contradiction. ■

Remark 1.3.7. When $p \equiv 1 \mod 4$, Wilson's theorem tells us a solution to

$$x^2 \equiv -1 \mod p$$

For example, when $p = 29 = 4 \cdot 7 + 1$, $x = (2 \cdot 7)!$ works.

1.3.3 Public Key Cryptography

In this subsection, we look into an example of practical application of the number theory, *public key cryptography*. Let us agree to write message as sequences of numbers. To send the message as encrypted form in such a way that only the reciever can decrypt them easily, we use the RSA (Rivest, Shamir, Adleman) scheme. To apply the RSA scheme, reciever do as follows.

- Think of two large primes p, q.
- Let $n = pq$, and pick an *encoding exponent* e, coprime to $\varphi(n) = (p-1)(q-1)$.
- Publish the pair (n, e), *encryption scheme* to public.

Now, to send an encrypted message,

- Sender chops the message into pieces/numbers $M < n$;
- and send $M^e \mod n$, computed quickly by repeated squaring $\mod n$.

Then, to decrypt it,

- Reciever work out the *decoding exponent* d, such that $ed \equiv 1 \mod \varphi(n)$;
- and compute
$$(M^e)^d = M^{k\varphi(n)+1} \equiv M \mod n$$
(consider both cases $M \equiv 0 \mod p$ and $M \not\equiv 0 \mod p$).

Note that in order to decrypt in this way, we require n and d, or n, e and $\varphi(n)$. Finding $\varphi(n)$ is as difficult as finding the prime factors of n, which is believed to be computationally hard.

1.4 The Real Numbers

1.4.1 Real Numbers

We have seen $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Now it is time to extend the boundaries of numbers once again.

Proposition 1.4.1. There is no rational x with $x^2 = 2$.

Proof. (*Method 1*) Suppose $x^2 = 2$. Note we may assume $x > 0$ since $(-x)^2 = x^2$. If x is rational, then $x = a/b$ for some $a, b \in \mathbb{N}$. Thus $a^2/b^2 = 2$, or

$$a^2 = 2b^2$$

But the exponent of 2 in the prime factorisation of a^2 is even while the exponent of 2 in the prime factorisation of $2b^2$ is odd, contradicting the Fundamental Theorem of Arithmetic. Thus $x \notin \mathbb{Q}$. ■

N.b. the same proof shows that if $\exists x \in \mathbb{Q}$ with $x^2 = n$ for some $n \in \mathbb{N}$, then n must be a square.

Proof. (*Method 2*) Suppose $x^2 = 2$ for some $x = a/b$ with $a, b \in \mathbb{N}$. Then for any $c, d \in \mathbb{Z}$, $cx + d$ is of the form e/b for some $e \in \mathbb{Z}$. Thus if $cx + d > 0$, then

$$cx + d \geqslant \frac{1}{b}$$

But $0 < x - 1 < 1$ as $1 < x < 2$ so if n is sufficiently large,

$$0 < (x-1)^n < \frac{1}{b}$$

But for any $n \in \mathbb{N}$, $(x-1)^n$ is of the form $cx + d$ for some $c, d \in \mathbb{Z}$, since $x^2 = 2$; and this is a contradiction. ■

So one may say $\mathbb{Q}$ has a gap. For example, consider set $A = \{x \mid x \in \mathbb{Q}, x^2 < 2\}$. 2 is an upper bound for the set A but so is 1.5, 1.42, etc. We observe that in $\mathbb{Q}$, there is no *least upper bound*. Then, what will be the set without any gaps?

The *real numbers*, written $\mathbb{R}$, is a set with elements 0 and 1 ($0 \neq 1$), equipped with operations $+$ and $\cdot$, and an ordering $<$ satisfying the following.

(1) $+$ is commutative and associative with identity 0, and every x has an inverse under $+$.

(2) $\cdot$ is commutative and associative with identity 1, and every $x \neq 0$ has an inverse under $\cdot$.

(3) $\cdot$ is distributive over addition, i.e. $\forall a, b, c$,

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

(4) For all a, b, exactly one of $a < b$ or $a = b$ or $a > b$ holds, and $\forall a, b, c$,

$$a < b \text{ and } a < c \Rightarrow a < c$$

(5) $\forall a, b, c$,

$$a < b \Rightarrow a + c < b + c$$

and

$$a < b \Rightarrow ac < bc \text{ if } c > 0$$

(6) Given any set S of reals that is non-empty and bounded above, S has a *least upper bound* (Theorem 3.1.2).

We say that a set S is *bounded above* if $\exists x \in \mathbb{R}$ such that $x \geqslant y$ for all $y \in S$. Such an x is an upper bound for S. For the definition of least upper bound (supremum), see Definition 3.1.2.

Remark 1.4.1.

(1) From (1)-(5), we can check, for example, $0 < 1$. If not, then $1 < 0$ so

$$0 = 1 - 1 < 0 - 1 = -1$$

and hence

$$0 = 0(-1) < (-1)(-1) = 1$$

which is a contradiction.

(2) We may consider $\mathbb{Q}$ as contained in $\mathbb{R}$, by identifying $a/b \in \mathbb{Q}$ with $ab^{-1} \in \mathbb{R}$, where b^{-1} is the multiplicative inverse of b.

(3) $\mathbb{Q}$ does not satisfy (6) as e.g. the set of x such that $x^2 < 2$ does not have a supremum.

(4) In (6), the conditions non-empty and bounded above are crucial: if S is empty, then every $x \in \mathbb{R}$ is an upper bound for S, so there is no least upper bound. If S is not bounded above, then it has no upper bound, and certainly no least upper bound.

(5) It is possible to construct $\mathbb{R}$ out of $\mathbb{Q}$ and check that (1)-(6) hold, but it takes effort.

(6) A structure obeying rules (1)-(3) is called a *field*. For example, $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$ with p prime are all fields, but $\mathbb{Z}$ is not.

Example 1.4.1. Consider

$$S = \{x \in \mathbb{R} : 0 \leqslant x \leqslant 1\} = [0, 1]$$

Is 2 an upper bound for S? – yes, since $\forall x \in S$, $x \leqslant 2$.
Is $3/4$ an upper bound for S? – no, since $7/8 \in S$ but $7/8 > 3/4$.
The least upper bound of S is 1 because 1 is an upper bound and every other upper bound is equal or greater than 1. Hence $\sup(S) = 1$.

Example 1.4.2. Consider

$$S = \{x \in \mathbb{R} : 0 < x < 1\} = (0, 1)$$

Is 2 an upper bound for S? – yes, since $\forall x \in S$, $x \leqslant 2$.
Is $3/4$ an upper bound for S? – no, since $7/8 \in S$ but $7/8 > 3/4$.

We still have $\sup(S) = 1$ because 1 is an upper bound, and there is no upper bound c such that $c < 1$; indeed, c is certainly greater than 0 so if $c < 1$, then $0 < c < 1$, so

$$\frac{c+1}{2} \in S$$

with $(c+1)/2 > c$.

Proposition 1.4.2. (*Axiom of Archimedes*) $\mathbb{N}$ is not bounded above in $\mathbb{R}$.

Proof. Suppose on the contrary that $\mathbb{N}$ is bounded above. Let $c = \sup\mathbb{N}$. By definition, $c-1$ is not an upper bound for $\mathbb{N}$, so $\exists n \in \mathbb{N}$ such that $n > c-1$. But then $n+1 \in \mathbb{N}$ with $n+1 > c$, contradicting the fact that c was an upper bound for $\mathbb{N}$. ■

Corollary 1.4.2.1. For any $t \in \mathbb{R}$ with $t > 0$, there exists $n \in \mathbb{N}$ with $1/n < t$.

Proof. Given $t > 0$, by Proposition 1.4.2, $\exists n \in \mathbb{N}$ such that $n > 1/t$. Hence $1/n < t$. ■

A set S is said to be *bounded below* if $\exists x$ such that $x \leqslant y$ for all $y \in S$. Such an x is called a lower bound for S. If S is non-empty and bounded below, then $-S = \{-y : y \in S\}$ is non-empty and bounded above, so it has a least upper bound, say c. Hence $-c$ is the greatest lower bound, i.e. *infimum* for S and we write $\inf(S)$. Corollarly 1.4.2.1 immediately implies that

$$\inf(\{1/n : n \in \mathbb{N}\}) = 0$$

Example 1.4.3. Consider

$$S = \{0, 1/2, 2/3, 3/4, \ldots\} = \{1 - 1/n : n \in \mathbb{N}\}$$

Clearly, 1 is an upper bound. Suppose $c < 1$ is an upper bound for S. Then

$$1 - \frac{1}{n} \leqslant c \quad \forall n \in \mathbb{N}$$

so $0 < 1 - c \leqslant 1/n$ for all $n \in \mathbb{N}$, contradicting Corollary 1.4.2.1. Thus $\sup(S) = 1$.

Theorem 1.4.3. There exists $x \in \mathbb{R}$ with $x^2 = 2$.

Proof. Let

$$S = \{x \in \mathbb{R} : x^2 < 2\}$$

Note that S is non-empty since e.g. $1 \in S$. It is also bounded above, e.g. by 2. Hence we may let $\sup(S) = c$. Observe that $1 < c < 2$. We claim that $c^2 = 2$. First, suppose $c^2 < 2$. For $0 < t < 1$,

$$(c+t)^2 = c^2 + 2ct + t^2 < c^2 + 4t + t = c^2 + 5t \leqslant 2$$

for sufficiently small t, e.g. $t \leqslant (2 - c^2)/5$. But this contradicts the assumption that c was an upper bound for S. Now suppose $c^2 > 2$. For $0 < t < 1$ we have

$$(c-t)^2 = c^2 - 2ct + t^2 > c^2 - 4t + 0 \geqslant 2$$

for sufficiently small t, e.g. $t \leqslant (c^2 - 2)/4$. This contradicts the assumption that c is the least upper bound for S. Hence $c^2 = 2$ by construction of real numbers. ■

N.b. the same proof shows that $\sqrt[n]{x}$ exists $\forall n \in \mathbb{N}$, $\forall x \in \mathbb{R}$, $n > 0$.

A real that is not rational is called *irrational*. For example, $\sqrt{2}, \sqrt{3}, \sqrt{4}$ are all irrational. Also, observe that $2+3\sqrt{5}$ is irrational, since if $2+3\sqrt{5} = a/b$ with $a, b \in \mathbb{N}$, then

$$\sqrt{5} = \frac{a-2b}{3b} \in \mathbb{Q}$$

The rationals are *dense* in $\mathbb{R}$, in a sense that $\forall a < b \in \mathbb{R}$, $\exists c \in \mathbb{Q}$ with $a < c < b$. To show the assetion above, assume that $a \geqslant 0$. By Corollary 1.4.2.1, $\exists n \in N$ with $1/n < b - a$. Let

$$T = \{k \in \mathbb{N} : k/n \geqslant b\}$$

By the Axiom of Archimedes, $\exists N \in \mathbb{N}$ such that $N > b$. Hence $Nn \in \mathbb{T}$, so $T \neq \varnothing$. By the well-ordering principle (Theorem 1.2.2), T has a least element m. Let's set $c = (m-1)/n$. Since $m - 1 \notin T$, $c < b$. If $c \leqslant a$, then

$$\frac{m}{n} = c + \frac{1}{n} < a + (b - a) = b$$

which is a contradiction. Therefore, $a < c < b$. Similarly, the irrationals are also dense in $\mathbb{R}$, i.e. $\forall a < b \in \mathbb{R}$, $\exists c \in \mathbb{R}\backslash\mathbb{Q}$ with $a < c < b$. For example, this can be constructed by taking a rational c with $a\sqrt{2} < c < b\sqrt{2}$ and then

$$a < \frac{c}{\sqrt{2}} < b$$

1.4.2 Decimal Expansions

We assume basic knowledge of sequences and series. Let (d_n) be a sequence with $d_n \in \{0, 1, \ldots, 9\}$. Then

$$\sum_{n=1}^{\infty} \frac{d_n}{10^n}$$

converges to some limit x, where $0 \leqslant x \leqslant 1$, because (by Theorem 3.1.1) the partial sums are increasing and bounded by

$$\sum_{n=1}^{\infty} \frac{9}{10^n} = 1$$

We say that

$$0.d_1 d_2 d_3 \ldots$$

is the *decimal expansion* of x. To show that any $x \in [0, 1)$ has a decimal expansion, pick $d_1 \in \mathbb{Z}$ maximal such that

$$\frac{d_1}{10} \leqslant x < 1$$

Then $0 \leqslant d_1 \leqslant 9$ because $0 \leqslant x < 1$, and

$$0 \leqslant x - \frac{d_1}{10} < \frac{1}{10}$$

because d_1 maximal. Now pick $d_2 \in \mathbb{Z}$ maximal such that

$$\frac{d_2}{100} \leqslant x - \frac{d_1}{10}$$

Then $0 \leqslant d_2 \leqslant 9$ because

$$0 \leqslant x - \frac{d_1}{10} < \frac{1}{10}$$

and

$$0 \leqslant x - \frac{d_1}{10} - \frac{d_2}{100} < \frac{1}{100}$$

because d_2 maximal. Inductively, pick $d_n \in \mathbb{Z}$ maximal such that

$$\frac{d_n}{10^n} \leqslant x - \sum_{j=1}^{n-1} \frac{d_j}{10^j}$$

so

$$0 \leqslant x - \sum_{j=1}^{n} \frac{d_j}{10^j} < \frac{1}{10^n}$$

Since $1/10^n \to 0$ as $n \to \infty$, $x - \sum_{j=1}^{n}(d_j/10^j) \to 0$, i.e.

$$x = \sum_{j=1}^{\infty} \frac{d_j}{10^j} = 0.d_1 d_2 d_3 \ldots$$

Remark 1.4.2.

(1) Decimal expansions need not be unique, e.g. $0.47999\ldots = 0.4800\ldots$.

(2) A decimal expansion is *periodic* if, aster a finite number of items, it repeats in blocks, of length k say. I.e. $\exists l, k$ such that $d_{n+k} = d_n$ for all $n > l$.

We can tell that a periodic decimal is rational, e.g. if

$$x = 0.7836147147147\ldots$$

then

$$10^4 x - 7836 = 0.147147\ldots = 147 \sum_{j=1}^{\infty} \frac{1}{10^{3j}} = 147 \frac{1}{10^3} \frac{1}{1 - 1/10^3}$$

so $x \in \mathbb{Q}$. Conversely, if $x \in \mathbb{Q}$, then it has a periodic decimal expansion. To see this, we write

$$x = \frac{p}{2^a 5^b q}$$

where $a, b, p, q \in \mathbb{Z}$, $a, b, q \geqslant 0$, $\gcd(q, 10) = 1$. Then,

$$10^{\max\{a,b\}} x = \frac{t}{q} = n + \frac{c}{q}$$

where $n, c \in \mathbb{Z}$, $0 \leqslant c < q$. By Fermat-Euler's theorem (Theorem 1.3.12), since $\gcd(q, 10) = 1$,

$$10^{\varphi(q)} \equiv 1 \mod q$$

or $10^{\varphi(q)} - 1 = kq$ for some $k \in \mathbb{N}$. Hence

$$\frac{c}{q} = \frac{kc}{kq} = \frac{kc}{10^{\varphi(q)} - 1} = kc \sum_{j=1}^{\infty} \frac{1}{(10^{\varphi(q)})^j}$$

Since $0 \leqslant kc < kq$, we can write kc as a $\varphi(q)$-digit number $d_1 d_2 \ldots d_{\varphi(q)}$. Then

$$\frac{c}{q} = 0.d_1 d_2 \ldots d_{\varphi(q)} d_1 d_2 \ldots d_{\varphi(q)}$$

and so x is periodic.

1.4.3 Algebraic and Transcendental Numbers

∗ Euler's Number

We define the *Euler's number*

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

Note that this series convergences by monotone convergence theorem, since it is increasing and bounded above by

$$1 + 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 3$$

If we define $0! = 1$, then

$$e = \sum_{j=0}^{\infty} \frac{1}{j!}$$

Proposition 1.4.4. e is irrational.

Proof. Suppose e were rational, say $e = p/q$ where $p, q \in \mathbb{N}$ and $q > 1$ (since $2 < e < 3$). Then $q!e \in \mathbb{N}$. But

$$\begin{aligned} q!e &= q! + \frac{q!}{1!} + \frac{q!}{2!} + \cdots + \frac{q!}{q!} + \frac{q!}{(q+1)!} + \frac{q!}{(q+2)!} + \cdots \\ &= N + x \end{aligned}$$

for some $N \in \mathbb{N}$, where

$$\begin{aligned} x &= \sum_{j=q+1}^{\infty} \frac{q!}{j!} = \sum_{j=1}^{\infty} \frac{q!}{(q+j)!} \\ &= \frac{1}{q+1} + \frac{q+1}{q+2} + \frac{1}{(q+1)(q+2)(q+3)} + \cdots \end{aligned}$$

and in general,

$$\frac{q!}{(q+j)!} \leqslant \frac{1}{(q+1)^j}$$

so

$$x \leqslant \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots = \frac{1}{q} < 1$$

as $q \geqslant 2$. Hence $0 < x < 1$, contradicting the fact that $q!e \in \mathbb{N}$. Thus e is irrational. ■

∗ Algebraic and transcendental numbers

We say a real number is *algebraic* if it is a root of a (non-zero) polynomial with integer coefficients (or rational coefficients).

Example 1.4.4.

(1) Every rational number is algebraic: $x = p/q \Rightarrow qx - p = 0$.

(2) $\sqrt{2}$ is algebraic: it satisfies $x^2 - 2 = 0$.

A real number is *transcendental* if it is not algebraic.

Theorem 1.4.5. (Liouville, 1851) The number

$$L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

is transcendental.

Proof. To prove the theorem, we first need two sublemmas about polynomials.

Lemma 1.4.6. For any polynomial p, there exists a constant K such that

$$|p(x) - q(x)| \leqslant K|x - y|$$

for all $0 \leqslant x, y \leqslant 1$.

Proof. Suppose $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. Then

$$\begin{aligned} p(x) - p(y) &= a_d(x^d - y^d) + a_{d-1}(x^{d-1} - y^{d-1}) + \cdots + a_1(x - y) \\ &= (x - y)\left[a_d(x^{d-1} + x^{d-2}y + \cdots + y^{d-1}) + \cdots + a_1\right] \end{aligned}$$

so clearly,

$$|p(x) - p(y)| \leqslant |x - y|\left[(|a_d| + |a_{d-1}| + \cdots + |a_1|)d\right]$$

■

Lemma 1.4.7. A non-zero polynomial of degree d has at most d roots.

Proof. Given a polynomial p of degree d, we may assume by induction that it holds for all polynomials of degree less than d, and that p has a root r (otherwise we are done). We may write $p(x) = (x - r)q(x)$ for some polynomial q of degree $d - 1$. So each root of p is either r, or a root of q. But by the induction hypothesis, q has at most $d - 1$ roots. ■

Now we are ready. Write

$$L_n = \sum_{k=1}^{n} \frac{1}{10^k}$$

so $L_n \to L$ as $n \to \infty$. Suppose there is a polynomial p of which L is a root. By Lemma 1.4.6, there exists K such that $|p(x) - p(y)| \leqslant K|x - y|$ for all $0 \leqslant x, y \leqslant 1$.

Suppose p has a degree d, i.e. $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$, $a_d \neq 0$. Notice that $L_n = s/10^{n!}$ for some $s \in \mathbb{N}$, so

$$p(L_n) = \frac{t}{10^{dn!}}$$

for some $t \in \mathbb{Z}$. By Lemma 1.4.7, for sufficiently large n, L_n is not a root of p. Hence $|p(L_n)| \geqslant 1/10^{dn!}$, i.e.

$$|p(L_n) - p(L)| \geqslant \frac{1}{10^{dn!}}$$

Therefore,

$$\frac{1}{10^{dn!}} \leqslant |p(L_n) - p(L)| \leqslant K|L_n - L| \leqslant K\frac{2}{10^{(n+1)!}}$$

Since

$$|L - L_n| = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} \leqslant \frac{2}{10^{(n+1)!}}$$

But $1/10^{dn!} \leqslant 2K/10^{(n+1)!}$ is a contradiction for sufficiently large n. ■

Remark 1.4.3.

(1) The same proof shows that any real number x such that $\forall x \in \mathbb{N}$, there exists rational p/q such that

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}$$

is transcendental, i.e. "x is transcendental if it has a very good rational approximation."

(2) Such x are known as *Liouville numbers*.

(3) This proof does not show that e is transcendental, but in fact it is.

1.4.4 Complex Numbers

Observe that some polynomials have no real roots, e.g. $x^2 + 1$. We will try and define x with $x^2 + 1 = 0$ into existence.

The *complex numbers*, written $\mathbb{C}$, consist of $\mathbb{R}^2$ (the set of all ordered pairs (a, b) with $a, b \in \mathbb{R}$) together with operations $+$ and $\cdot$ defined by

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

We can view $\mathbb{R}$ as contained in $\mathbb{C}$ by identifying $a \in \mathbb{R}$ with $(a, 0) \in \mathbb{C}$. Note that

$$(a, 0) + (b, 0) = (a + b, 0)$$

and

$$(a, 0) \cdot (b, 0) = (ab, 0)$$

Now let $i = (0, 1)$, with $i^2 = (-1, 0)$, corresponding to $-1 \in \mathbb{R}$. Then, for every $z \in \mathbb{C}$, we can write

$$z = (a, b) = a(1, 0) + b(0, 1) = a + bi$$

for some $a, b \in \mathbb{R}$.

Remark 1.4.4.

(1) $\mathbb{C}$ is a field, i.e. it obeys (1)-(3) from the definition of $\mathbb{R}$, including that for some $z \in \mathbb{C}$ $(z \neq 0)$, $\exists w$ such that $zw = 1$. Indeed, given $z = a + bi$, since

$$(a + bi)(a - bi) = a^2 + b^2$$

we have

$$(a + bi)\frac{a - bi}{a^2 + b^2} = 1$$

(2) Every non-zero polynomial (even allowing complex coefficients) has a root in $\mathbb{C}$. This is known as the *Fundamental Theorem of Algebra*.

1.5 Countability

We introduce the concept countability to obtain a deeper understanding of sizes of sets – in particular, infinite sets. We say a set X is *countable* if X is finite or there is a bijection $X \to \mathbb{N}$. That is, X is countable if and only if we can list the elements of X as $x_1, x_2, \ldots$.

Example 1.5.1.

(1) Any finite set is countable.

(2) $\mathbb{N}$ is countable.

(3) $\mathbb{Z}$ is countable, as we may list the elements of $\mathbb{Z}$ as $0, 1, -1, 2, -2, \ldots$, i.e.

$$x_n = \begin{cases} n/2 & 2|n \\ -(n-1)/2 & 2 \nmid n \end{cases}$$

Lemma 1.5.1. Any subset of $\mathbb{N}$ is countable.

Proof. If $S \subseteq \mathbb{N}$ is non-empty, by well-ordering principle, there is a least element $s_1 \in S$. If $S \backslash \{s_1\} \neq \varnothing$, by well-ordering principle, there is a least element $s_2 \in S \backslash \{s_1\}$. And if $S \backslash \{s_1, s_2\} \neq \varnothing$, we can repeat the process. If at some point this process ends, then

$$S = \{s_1, s_2, \ldots, s_m\}$$

is finite. If it goes on forever, then the map

$$g : \mathbb{N} \to S, \quad n \mapsto s_n$$

is well-defined, and is injective. It is also surjective because if $k \in S$, then $k \in \mathbb{N}$, and there are less than k elements of S less than k, so $k = s_n$ for some $n \leqslant k$. ■

Note that the idea used in the proof of Lemma 1.5.1 may not work for other sets. For example, in $\mathbb{R}$, let

$$S = \{1/2, 2/3, 3/4, \ldots\} \cup \{1\}$$

then S is countable as we can list it as

$$1, 1/2, 2/3, 3/4, \ldots$$

but if we had tried to list the elements in increasing order, then 1 would not be on the list.

Theorem 1.5.2. The following statements are equivalent:

(1) X is countable;

(2) there is an injection $X \to \mathbb{N}$;

(3) $X = \varnothing$ or there is surjection $\mathbb{N} \to X$.

Proof. ((1)⇒(2)) If X finite, it obviously injects into $\mathbb{N}$. Otherwise, if X infinite, X bijects with $\mathbb{N}$, and it injects into $\mathbb{N}$.
((2)⇒(1)) If there is an injection $f : X \to \mathbb{N}$, then f is a bijection between X and $S = f(X)$. If S is finite, then so is X. If S is infinite, then by Lemma 1.5.1, there is a bjiection $g : S \to \mathbb{N}$, and thus

$$X \xrightarrow{f} S = f(X) \xrightarrow{g} \mathbb{N}$$

is a bijection.
((3)⇒(2)) Suppose that $X \neq \varnothing$ and there is a surjection $f : \mathbb{N} \to X$. Now define g by

$$g(a) = \min f^{-1}(\{a\})$$

which exists by well-ordering principle. But by construction, g is injective. Hence (3) implies (2).
Finally, it is clear that (1) implies (3). Therefore, three statements are equivalent. ■

Corollary 1.5.2.1. Any subset of a countable set is countable.

Proof. If $Y \subseteq X$ and X is countable, then take the injection $X \to \mathbb{N}$ restricted to Y. ■

We may thus view "countable" as saying that a set is "at most as big as $\mathbb{N}$".[7]

Theorem 1.5.3. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof. (*Method 1*) Define $a_1 = (1,1)$, and a_n inductively, given $a_{n-1} = (p,q)$, by writing

$$a_n = \begin{cases} (p-1, q+1) & p \neq 1 \\ (p+q, 1) & p = 1 \end{cases}$$

This list includes every point $(x,y) \in \mathbb{N} \times \mathbb{N}$, hence there exists a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. ■

Proof. (*Method 2*) Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(x,y) \mapsto 2^x 3^y$. Then f is injective by the fundamental theorem of arithmetic (Theorem 1.3.7). Thus $\mathbb{N} \times \mathbb{N}$ is countable by Theorem 1.5.2. ■

Corollary 1.5.3.1. $\mathbb{Z} \times \mathbb{Z}$ is countable.

Proof. Since $\mathbb{Z}$ is countable, there is an injection $f : \mathbb{Z} \to \mathbb{N}$, and since $\mathbb{N} \times \mathbb{N}$ is countable, there is an injection $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Hence we have an injection

$$\mathbb{Z} \times \mathbb{Z} \xrightarrow{(f,f)} \mathbb{N} \times \mathbb{N} \xrightarrow{g} \mathbb{N}$$

■

By induction, we further can tell that $\mathbb{Z}^k$ is countable for any $k \in \mathbb{N}$.

Theorem 1.5.4. A countable union of countable sets is countable.

[7] Review definition if confused.

Proof. (*Method 1*) May assume that our countable sets are indexed by $\mathbb{N}$, so given countable sets $A_1, A_2, \ldots$, we wish to show

$$\bigcup_{n\in\mathbb{N}} A_n$$

is countable. For each $i \in \mathbb{N}$, since A_i is countable, we may list its elements as $a_1^{(i)}, a_2^{(i)}, \ldots$. Define

$$f : \bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N}, \quad x \mapsto 2^i 3^j$$

where $x = a_j^{(i)}$ for the least i such that $x \in A_i$. hen f is injective by the fundamental theorem of arithmetic (Theorem 1.3.7). ■

Proof. (*Method 2*) Let I be a countable index set, and for each $i \in I$, A_i is a countable set. Since I is countable, there is an injection $f : I \to \mathbb{N}$, and for each $i \in I$, since A_i is countable, there is an injection $g_i : A_i \to \mathbb{N}$. We construct an injection

$$h : \bigcup_{i\in I} A_i \to \mathbb{N} \times \mathbb{N}$$

as follows: for each $x \in \bigcup_{i\in I} A_i$, pick

$$m_x = \min\{j \in \mathbb{N} : x \in A_i, f(i) = j\}$$

which exists by well-ordering principle. Let $i_x \in I$ be such that $f(i_x) = m_x$ (i_x is unique because f is injective). Then

$$h(x) = (m_x, g_{i_x}(x))$$

defines an injection. ■

Example 1.5.2.

$$\mathbb{Q} = \bigcup_{n\in\mathbb{N}} \frac{1}{n}\mathbb{Z} = \bigcup_{n\in\mathbb{N}} \left\{ \frac{m}{n} : m \in \mathbb{Z} \right\}$$

so $\mathbb{Q}$ is a countable union of countable sets, hence countable.

Theorem 1.5.5. The set $\mathbb{A}$ of algebraic numbers is countable.

Proof. It suffices to show that the set of all polynomials with integer coefficients is countable, as then $\mathbb{A}$ is a countable union of finite sets, so by Theorem 1.5.4, is countable. In fact, it suffices to show that for each $d \in \mathbb{N}$, the set P_d of all integer polynomials of degree d is countable, again by Theorem 1.5.4. But the map $P_d \to \mathbb{Z}^{d+1}$,

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 \mapsto (a_d, a_{d-1}, \ldots, a_1, a_0)$$

is an injection, so since $\mathbb{Z}^{d+1}$ is countable, P_d is. ■

But certainly, not all sets are countable.

Theorem 1.5.6. $\mathbb{R}$ is uncountable.

Proof. (*Diagonal argument*, Cantor) If $\mathbb{R}$ were countable, we would be able to list all the reals as $r_1, r_2, r_3, \ldots$. Write each r_n in decimal form in some way:

$$r_1 = n_1.d_{11}d_{12}d_{13}d_{14}\ldots$$
$$r_2 = n_2.d_{21}d_{22}d_{23}d_{24}\ldots$$
$$r_3 = n_3.d_{31}d_{32}d_{33}d_{34}\ldots$$
$$\vdots$$

Now define

$$r = 0.d_1d_2d_3\ldots$$

by

$$d_n = \begin{cases} 1 & d_{nn} \neq 1 \\ 2 & d_{nn} = 1 \end{cases}$$

Note that r has only one decimal expansion, and is not on the list, since $\forall n \in \mathbb{N}$, $r \neq r_n$. This contradicts the assumption that $\mathbb{R}$ is countable. ■

N.b. it in fact shows that the interval $(0,1)$ is uncountable.

Corollary 1.5.6.1. There are uncountably many transcendental numbers.

Proof. If $\mathbb{R}\backslash\mathbb{A}$ were countable, then since $\mathbb{A}$ is countable by Theorem 1.5.5, $\mathbb{R} = (\mathbb{R}\backslash\mathbb{A}) \cup \mathbb{A}$ would also be countable, leading to contradiction. ■

Theorem 1.5.7. $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof. (*Method 1*) If $\mathcal{P}(\mathbb{N})$ were countable, we could just list it as $S_1, S_2, \ldots$. Let

$$S = \{n \in \mathbb{N} : n \notin S_n\}$$

Then S is not on our list since $\forall n \in \mathbb{N}$, $S \neq S_n$ (as S and S_n differ in the element n). This is a contradiction, and thus $\mathcal{P}(\mathbb{N})$ is uncountable. ■

Note that the proof above is similar as the diagonal argument by Cantor.

Proof. (*Method 2*) Note that there is an injection from $(0,1)$ into $\mathcal{P}(\mathbb{N})$: write $x \in (0,1)$ in binary

$$0.x_1x_2x_3\ldots$$

with $x_i \in \{0,1\}$, and set $f(x) = \{n \in N : x_n = 1\}$. Then, f is an injection. ■

Theorem 1.5.8. For any set X, there is no bijection between X and its power set $\mathcal{P}(X)$.

Proof. Given any $f : X \to \mathcal{P}(X)$, we shall show it is not a surjection. Let

$$S = \{x \in X : x \notin f(x)\}$$

Then S does not belong to the image of f, since $\forall x \in X$, S and $f(x)$ differ in the element x. Thus $S \neq f(x)$ for any $x \in X$. ■

Remark 1.5.1.

(1) This is reminiscent of Russell's paradox.

(2) In fact, it gives another proof that there is no universal set. Suppose we had such a universal set V, then we would have $\mathcal{V} \subseteq V$, in which case there would certainly be a surjection from V to $\mathcal{P}(V)$.

Example 1.5.3. Let $\{A_i : i \in I\}$ be a family of open pairwise disjoint intervals of $\mathbb{R}$. Such family is countable.

Each interval A_i contains a rational and $\mathbb{Q}$ is countable, so since the intervals are disjoint, we have an injection from I into $\mathbb{Q}$.

To summerise, to show that a set X is countable, we

(1) list its elements;

(2) inject it into $\mathbb{N}$;

(3) use the fact that a countable union of countable sets is countable;

(4) if the set is in or near $\mathbb{R}$, consider $\mathbb{Q}$.

To show that X is uncountable,

(1) run a diagonal argument on X;

(2) inject some uncountable set into X.

Intuitively, we think of "A bijects with B" as saying that "A and B are of the same size", "A injects into B" as saying that "A is at most as big as B", and "A surjects onto B" as saying that "A is at least as big as B" (for $B \neq \emptyset$). However, for these interpretations to make sense, we need that if "A is at most as big as B", then "B is at least as big as A", and conversely.

Lemma 1.5.9. Given non-empty sets A and B,

$$\exists \text{ injection } f : A \to B \Leftrightarrow \exists \text{ surjection } g : B \to A$$

Proof. Suppose $f : A \to B$ is injective. Fix $a_0 \in A$. Define $g : B \to A$ by

$$b \mapsto \begin{cases} \text{unique } a \in A \text{ such that } f(a) = b & \text{if it exists} \\ a_0 & \text{otherwise} \end{cases}$$

Then g is surjective. Conversely, suppose $g : B \to A$ is surjective. Let $f : A \to B$,

$$a \mapsto \text{some } b \in B \text{ such that } g(b) = a$$

Then f is injective. ∎

We also need that if "A is at most as big as B" and "B is at most as big as A", then "A and B have the same size".

Theorem 1.5.10. (*Schröder-Bernstein Theorem*) If $f : A \to B$ and $g : B \to A$ are injections, then there exists bijection $h : A \to B$.

Proof. For $a \in A$, write $g^{-1}(a)$ for the $b \in B$ (if it exists) such that $g(b) = a$. Similarly for B, write $f^{-1}(b)$ for the $a \in A$ (if it exists) such that $f(a) = b$. We call $g^{-1}(a), f^{-1}(g^{-1}(a)), g^{-1}(f^{-1}(g^{-1}(a))), \ldots$ the *ancestor sequence* of $a \in A$ (might terminate). Similarly, define the ancestor sequence of $b \in B$. Let

$A_0 = \{a \in A : \text{ancestor sequence of } a \text{ stops at an even time, i.e. the last point is in } A\}$

$A_1 = \{a \in A : \text{ancestor sequence of } a \text{ stops at an odd time, i.e. the last point is in } B\}$

and

$$A_\infty = \{a \in A : \text{ancestor sequence of } a \text{ does not stop}\}$$

Similarly, define B_0, B_1, B_∞. Note that f bijects A_0 bijects A_0 with B_1 (observing that every $b \in B_1$ has at least one ancestor, so is $f(a)$ for some $a \in A_0$), and similarly, g bijects B_0 with A_1. And f (or g) bijects A_∞ with B_∞. Then the function $h : A \to B$,

$$a \mapsto \begin{cases} f(a) & a \in A_0 \\ g^{-1}(a) & a \in A_1 \\ f(a) & a \in A_\infty \end{cases}$$

is a bijection. ■

Example 1.5.4. Is there a bijection from $[0,1]$ to $[0,1] \cup [2,3]$? Observe that we have an injection

$$f : [0,1] \to [0,1] \cup [2,3], \quad x \mapsto x$$

and an injection

$$g : [0,1] \cup [2,3] \to [0,1], \quad x \mapsto x/3$$

So by the Schröder-Bernstein theorem, ther is a bijection between $[0,1]$ and $[0,1] \cup [2,3]$.

It would be nice to be able to say that for any two sets A and B, either A injects into B or B injects into A. This is true, but proof is beyond the scope of this course.[8]

[8] See Part II Logic and Set Theory.

1.6 Example Sheets

1.6.1 Sheet 1

1. Impossible, since one is a multiple of 3 rather than 3 itself.

2. Note that the possible candidates are the quadrupoles of form $(10n+1, 10n+3, 10n+7, 10n+9)$. There are some examples: $(101, 103, 107, 109)$, $(191, 193, 197, 199)$, etc. However, it is currently unable to prove/disprove if there are infinitely many numbers of those quadrupoles – positive result will imply the *twin prime conjecture*.

3. With $a_1 = 41$, n^{th} term will take the form

$$a_n = a_1 + \sum_{j=1}^{n-1} 2j = a_1 + n(n-1) = n^2 - n + 41$$

   Then, $a_{41} = 41^2$ is clearly not a prime.

4. More generally, we claim that there exists a sequence of $n \in \mathbb{N}$ consequtive natural numbers containing no primes. If we let $x = (n+1)! + 2$, then, for all $0 \leqslant j \leqslant n-1$,

$$\begin{aligned} x + j &= 1 \cdot 2 \cdots j(j+1)(j+2) \cdots n(n+1) + 2 + j \\ &= (j+2)\left[1 \cdot 2 \cdots j(j+1)(j+3) \cdots n(n+1) + 1\right] \end{aligned}$$

   is clearly a composite number as required. Hence for $n = 100$,

$$101! + 2, 101! + 3, \ldots, 101! + 101$$

   are all not prime.

5. It can be translated as: "For any natural number m, there exists a natural number n such that n is greater than or equal to n, and for all natural numbers a and b, at least one of the following conditions holds: a is 1, b is 1, or the product of a and b is not equal to n." This statement is true, as we can choose n to be a least prime that is greater than m (because there are infinitely many primes). Meanwhile, negation will give

$$\exists m \forall n \exists a \exists b ((n < m) \vee [(a \neq 1) \wedge (b \neq 1) \wedge (ab = n)])$$

6. Firstly, $2^{19} + 5^{40} \equiv 2^{19} + 2^{40} \equiv (-1) + 1 \equiv 0 \mod 3$. Secondly, for $2^{91} - 1$, if we let $2^{13} = 1$,

$$2^{91} - 1 = x^7 - 1 = (x-1)(x^6 + x^5 + \cdots + 1)$$

   So $2^{13} - 1 \big| 2^{91} - 1$.

7. 3 is a factor of n^2, and this implies $3^2 | n^2$ and $3|n$.

8. $3^{3n+4} + 7^{2n+1} = 3^4(27)^n + 7(49)^7 \equiv 4 \cdot 5^n - 4 \cdot 5^n \equiv 0 \mod 11$.

9. Let $p_1, p_2, \ldots, p_k$ all the primes of the form $4n-1$. Now let $N = 4p_1p_2 \cdots p_k - 1$. By fundamental theorem of arithmetic, there exists a unique prime factorisation consisting of primes that are less than N. Claim that at least one of the prime factor of N is of the form $4n-1$. If all factors are of the form $4n+1$, $N \equiv 1 \mod 4$,

which is a contradiction. Hence at least one prime factor is of the form $4n+1$. But $p_i \nmid N$ for all $i = 1,\dots,k$, leading to contradiction. Therefore, there are infinitely many primes of the form $4n+1$.

However, for the primes of the form $4n+1$, the similar method will not work since all prime factors can be of the form $4n-1$.

10. Let $F_n = 2^{2^n}+1$ and $d = \gcd(F_n, F_m)$ where $n > m$. Then $d|F_m$ and $d|F_n$. But

$$2^{2^n} - 1 = (2^{2^{n-1}}+1)(2^{2^{n-1}}-1) = F_{n-1}F_{n-2}\cdots F_1F_0 \qquad (*)$$

So $d|F_nF_{n-1}\cdots F_0$ ($\because m \leqslant n-1$). Furthermore, $F_n - F_{n-1}F_{n-2}\cdots F_0 = 2$, so $d|2$. But since every term of F_n is odd, $d = 1$. Then, result follows from observing $(*)$.

11. Step-by-step calculation gives

    (a) $2*n = 1*(2*(n-1)) = 2*(n-1)+1$ and $2*1 = 1*2 = 3$. Hence $2*n = n+2$.

    (b) $3*n = 2*(3*(n-1)) = (3*(n-1))+2$ and $3*1 = 2*2 = 4$. Hence $3*n = 2n+2$.

    (c) $4*n = 3*(4*(n-1)) = 2(4*(n-1))+2$ and $4*1 = 3*2 = 6$. Hence $4*n = 2^{n+2}+2$.

    Then, from the fact that $5*1 = 4*2 = 14$,

$$5*5 = 2^{2^{2^{2^{16}}}} - 2$$

12. $a+b = 100$, $a,b \in \mathbb{N}$. $ab \leqslant (a+b)^2/4 = 5050$. Equality when $a = b = 50$.

13. Yes; repeat of 82644628100 gives

$$8264462810082644628100 = 90909090910^2$$

    Note that $10^{11}+1 = 11^2 \cdot 23 \cdot 4093 \cdot 8779$.

14. Consider sequence $n, n+1, \dots, n+b-1$. At least one is multiple of b, and at least two is multiple of a. If one of multiple of a is also multiple of b, then remaining one is not. Therefore, we can choose two distinct numbers whose product is a multiple of ab.

1.6.2 Sheet 2

1. $x = 16, y = 27$ by the Euclid's algorithm. Meanwhile, there is no integer solution for $3381x + 2646y = 21$ since $\gcd(3381, 2646) = 147 > 21$ (Bézout's theorem).

2. This need not be true. E.g. $(2,3) = (9,4) = 1$ but $(18,12) = 6$. However, it is true that $(a,b)(c,d)|(ac,bd)$. If we let $g_1 = (a,b), g_2 = (c,d)$ and $a = g_1a', b = g_1b', c = g_2c', d = g_2d'$, $(ac,bd) = g_1g_2(a'c', b'd')$; and clearly $g_1g_2|g_1g_2(a'c', b'd')$.

   Now suppose $(a,b) = (a,c) = 1$. Then, by Bézout's theorem, $ax+by = az+cw = 1$ for some $x,y,z,w \in \mathbb{Z}$. Hence,

$$(ax+by)(az+cw) = (axz+cxw+byz)a + yw(bc) = 1$$

   implies $(a,bc) = 1$. Note that reverse direction also holds since

$$ax + y(bc) = ax + (yb)c + ax + (yc)b = 1$$

   for some $x,y \in \mathbb{Z}$ if $(a,bc) = 1$.

3. First part is trivial since $10^n \equiv 1 \mod 9$. By Fermat-Euler theorem, we have $2^{\varphi(9)} = 2^6 \equiv 1 \mod 9$. Hence $2^{29} \equiv 2^5 \equiv 5 \mod 9$, and thus 4 is missing.

4. Inductively, it can be found that F_n is even if n is multiple of 3, and F_n is multiple of 3 if n is multiple of 4. Hence, F_{2023} is odd and not a multiple of 3.

5. We employ Euclid's algorithm to find inverses.

   (a) There is an unique solution modulo 40 since $\gcd(7,40) = 1$. From $17 \cdot 7 \equiv 1 \mod 40$, $x \equiv -11 \mod 40$.

   (b) $\gcd(12,54) = 6$ so we solve $2x \equiv 5 \mod 9$. Therefore, $x \equiv 7 \mod 9$.

   (c) Each congruence can be solved as $z \equiv 12 \mod 17$ and $z \equiv 15 \mod 19$. Then, since $\gcd(17,19) = 1$, by the chinese remainder theorem, the solution satisfying both congruences will be $z \equiv 148 \mod 323$.

6. Sender sends $M^2 = 35^7 \equiv 75 \mod 160$. With decoding exponent $d = 23$, reciever can obtain $75^{23} = 35 \mod 160$, the original message.

7. (*Divisor Sum*, Gauss) We simplify all the terms of fractions

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$$

   and note denominator of each fraction, d, will divide n, and numerator of that will be coprime with d. Hence, there are $\varphi(d)$ fractions with denominator d. Viz $n = \sum_{d|n} \varphi(d)$.

8. By Fermat's little theorem, $10^{22} \equiv 1 \mod 23$. Hence

$$10^{881} - 1 \equiv 10(10^{22})^{40} - 1 \equiv 9 \mod 23$$

9. By Fermat's little theorem, we have $x^{p-1} \equiv 1 \mod p$ and $x^p \equiv x \mod p$. Multiplying these, $x^{2p-1} \equiv x \mod p$. Put $p = 3k+2$ to find $x^{6k+3} \equiv x \mod p$. This gives

$$x \equiv (x^3)^{2k+1} \equiv 1 \mod p$$

   Moreover,

$$y \equiv (y^3)^{2k+1} \equiv a^{2k+1} \mod p$$

10. Note that all prime divisors of n^2+1 are of form $4k+1$, since

$$p | n^2+1 \Leftrightarrow n^2 \equiv -1 \mod p \Rightarrow n^4 \equiv 1 \mod p \Rightarrow 4 | p-1 \Leftrightarrow p \equiv 1 \mod 4$$

    by Fermat's little theorem. Now, assume $p_1, p_2, \ldots, p_k$ are all the primes of form $4m+1$. Then, if we consider $N = (2p_1p_2\cdots p_k)^2 + 1$, by fundamental theorem of arithmetic and the fact above, N will have a prime divisor of form $4k+1$. But $p_i \nmid N$ for all $i = 1, \ldots, k$, which is a contradiction. Hence there are infinitely many such primes.

11. Last 5 digits of$5^6, 5^7, \ldots 5^{14}$ are

$$03125, 15625, 78125, 90625, 53125, 65625, 28125, 40625, 30125$$

    respectively. Notice that they are periodic with period 8. Hence, we want to find $n = 5^{5^5}$ modulo 8. But $5^2 \equiv 1 \mod 8$ so $n \equiv 5 \mod 8$ and the 5^{th}-last digit will be 0 from 03125.

12. Observe Fibonacci sequence modulo 29 to find that they take values that are in

$$S = \{0, 1, 2, 3, 5, 8, 13, 21, 26, 28\}$$

However, with $(n^7)^4 \equiv 1 \mod 29$, possible values of n^7 modulo 29 are $\{0, 1, 12, 17, 28\}$, and $\{9, 10, 11, 22, 27\}$ for $n^7 - 77$. But $\{9, 10, 11, 22, 27\} \cap S = \varnothing$. Hence it is impossible for $n^7 - 77$ to be a Fibonacci number.

1.6.3 Sheet 3

1. Consider a set

$$A = \{x \in \mathbb{R} \mid x^3 < 2\}$$

Since $2^3 = 8 > 2$ and $x^3 > 2^3 > 2$ if $x > 2$, A is bounded above. Thus by least upper bound axiom, there exists $\sup(A) = a$. Observe that $1 < a < 2$. We claim that $a^3 = 2$. First, suppose $a^3 < 2$. For $0 < t < 1$ that is sufficiently small,

$$\begin{aligned}(a+t)^3 &= a^3 + 3a^2t + 3at^2 + t^3 \\ &< a^3 + 6t + 6t + t = a^3 + 13t \leqslant 2\end{aligned}$$

But this contradicts our assumption that a is an upper bound. Now suppose $a^3 > 2$. Similarly, for sufficiently small $0 < t < 1$,

$$\begin{aligned}(a-t)^3 &= a^3 - 3a^2t + 3at^2 - t^3 \\ &> a^3 - 6t - t = a^3 - 7t \geqslant 2\end{aligned}$$

and this contradicts our assumption that a is a least upper bound. Hence, $a^3 = 2$ by definition of real numbers.

We claim that there is no $x \in \mathbb{Q}$ such that $x^3 = 2$. Suppose $x \in \mathbb{Q}$. Let $x = p/q$ where $p, q \in \mathbb{N}$ and $\gcd(p, q) = 1$. Then, $N = p^3 = 2q^3$. By the fundamental theorem of arithmetic, there exists a unique prime factorisation of N. But the exponent of 2 of p^3 is multiple of 3 while that of $2q^3$ is 1 modulo 3, which is a contradiction. Hence we proved that a is irrational.

2. Let $\sqrt{2} + \sqrt{3} = a$. Then, $2\sqrt{6} = a^2 - 5$. Since $2\sqrt{6}$ is a root of $y^2 - 24 = 0$, put $y = x^2 - 5$ to find

$$(x^2 - 5)^2 - 24 = x^4 - 10x^2 + 1 = 0$$

with a as a root. Thus $\sqrt{2} + \sqrt{3}$ is algebraic.

Now suppose $\sqrt{2} + \sqrt{3} = p/q$ where $p, q \in \mathbb{N}$ and $\gcd(p, q) = 1$. Then

$$5 + 2\sqrt{6} = \frac{p^2}{q^2}, \quad \sqrt{6} = \frac{p^2 - 5q^2}{2q^2} \in \mathbb{Q}$$

which is a contradiction. Hence $\sqrt{2} + \sqrt{3}$ is irrational.

3. Suppose that $x = p/q$ where $p, q \in \mathbb{Z}, p \neq 0, \gcd(p, q) = 1$. If we let

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and $P(p/q) = 0$, then,

$$0 = q^n P(p/q) = p^n + q(a_{n-1}p^{n-1} + \cdots + a_0 q^{n-1})$$

Hence $q | p^n$ and consequently $q | p$, implying $|q| = 1$. Therefore, $p/q \in \mathbb{Z}$ as required. C.f. *rational root test*.

4. See Analysis I Lemma 3.1.3 (5).

5. This is not always true. For example, let $x_n = \sum_{j=1}^{n}(1/j)$. Then $x_n - x_{n-1} = 1/n \to 0$ but x_n diverges.

6. (i) $x_n \to 3$.
   (ii) It clearly diverges.
   (iii) Converges. We have
   $$x_n = \frac{n+1-n}{\sqrt{n+1}-\sqrt{n}} \to 0$$
   (iv) Note that
   $$(n!)^2 = (1\cdot n)(2\cdot(n-1))\cdots((n-1)\cdot 2)(n\cdot 1) \geqslant n^n$$
   So $(n!)^{1/n} \geqslant \sqrt{n}$. But $\sqrt{n} \to \infty$ as $n \to \infty$ so x_n also diverges.

7. (i) $1/(1+n^2) < 1/n^2$ so converges by comparison.
   (ii) We have
   $$\frac{n^n}{n!}\frac{(n+1)!}{(n+1)^{n+1}} = \frac{1}{\left(1+\frac{1}{n}\right)^n} \to \frac{1}{e}$$
   Hence it converges by ratio test.
   (iii) $1/\sqrt{n(n+1)} > 1/(\sqrt{2}n)$ so it diverges by comparison.

8. We claim that $x_n > x_{n+1} > 0$. Since it is clear that $x_{n+1} > 0$ if $x_n > 0$, and $x_1 = 1 > 0$, we have $x_n > 0$ for all n by induction. But
   $$x_n > x_{n+1} \Leftrightarrow x_n > \frac{x_n}{1+\sqrt{x_n}} \Leftrightarrow 1+\sqrt{x_n} > 1 \Leftrightarrow x_n > 0$$
   so $x_n > x_{n+1} > 0$ for all $n \geqslant 1$ as required. Then, since (x_n) is decreasing and bounded by 0, it converges by monotone convergence theorem. Now suppose $x_n \to a$. Then
   $$a = \frac{a}{1+\sqrt{a}}$$
   so $a = 0$.

9. Hmmm... it is trivial when it is rational (periodic). But what if not? I *will* return.

10. Since $x_n \to 0$, there exists N such that $n \geqslant N \Rightarrow x_n < 1$. Hence
    $$\sum_{n=1}^{\infty} x_n^2 = \sum_{n=1}^{N-1} x_n^2 + \sum_{N}^{\infty} x_n^2 \geqslant \sum_{n=1}^{N-1} x_n^2 + \sum_{N}^{\infty} x_n$$
    and thus convergent by comparison test.

    However, it is not quite true when x_n is not always positive. E.g. consider $x_n = (-1)^n/\sqrt{n}$.

11. No. For example, we may choose $a, b, c \in \mathbb{R}$ such that $a+b+c = 0$ and $a^3+b^3+c^3 > 0$ (e.g. $a = -1, b = -2, c = 3$). Then, let
    $$x_{3n} = \frac{a}{n^{1/3}}, \quad x_{3n+1} = \frac{b}{n^{1/3}}, \quad x_{3n+2} = \frac{c}{n^{1/3}}$$
    Notice that $\sum x_n$ converges but $\sum x_n^3$ does not.

12. First, we claim that if $z + 1/z \in \mathbb{Q}$, then $z^n + 1/z^n \in \mathbb{Q}$. We prove the claim by induction. Suppose $z^k + 1/z^k \in \mathbb{Q}$ for $k = 1, \ldots, n-1$. Then, since

$$z^n + \frac{1}{z^n} = \left(1 + \frac{1}{z}\right)\left(z^{n-1} + \frac{1}{z^n - 1}\right) - \left(z^{n-2} + \frac{1}{z^{n-2}}\right)$$

$z^n + 1/z^n \in \mathbb{Q}$ as required. Note that contrapositive states that if $z^n + 1/z^n$ is irrational, then $z + 1/z$ is also irrational.

Now let $z = \sqrt[100]{\sqrt{3} + \sqrt{2}}$. It follows from the claim above that because

$$z^{100} + \frac{1}{z^{100}} = 2\sqrt{3} \notin \mathbb{Q}$$

$z + 1/z$ is irrational.

13. It is convergent by the Dirichlet's test.

1.6.4 Sheet 4

1. $\binom{4}{0} + \binom{4}{2} + \binom{4}{4} = 8$. More generally,

$$\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{2\lfloor n/2 \rfloor} = 2^{n-1}$$

from the binomial theorem.

2. (i) This holds for $n \geqslant k$. Suppose we choose $k+1$ distinct numbers from $1, 2, \ldots n+1$. If the largest number we choose is $j+1$, the ways of choosing the numbers will be $\binom{j}{k}$. Therefore, since the largest number we choose can be $k, k+1, \ldots, n$,

$$\binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}$$

(ii) We choose n distinct numbers from $S = \{1, 2, \ldots, 2n\}$. Suppose $A = \{1, \ldots, n\}$ and $B = \{n+1, \ldots, 2n\}$. We may choose k items from set A and $n-k$ items from set B, and the total ways of doing this will be

$$\binom{n}{k}\binom{n}{n-k} = \binom{n}{k}^2$$

Since possible values of k are $k = 0, 1, \ldots, n$,

$$\binom{n}{0}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$$

3. Let $A, B \subseteq S$ and $A^c = S \backslash A$, $B^c = S \backslash B$. Then,

$$\begin{aligned} A \triangle B &= (A \backslash B) \cup (B \backslash A) = (A \cap B^c) \cup (B \cap A^c) \\ &= (A \cup B) \cap (A \cup A^c) \cap (B \cup B^c) \cap (B^c \cup A^c) \\ &= (A \cup B) \cap S \cap S \cap (B^c \cup A^c) \\ &= (A \cup B) \cap (A^c \cup B^c) \end{aligned}$$

Also,

$$(A \triangle B)^c = ((A \cap B^c) \cup (B \cap A^c))^c = (A^c \cup B) \cap (A \cup B^c)$$

Hence,

$$\begin{aligned}(A \triangle B) \triangle C &= ((A \triangle B) \cup C) \cap ((A \triangle B)^c \cup C^c) \\ &= (((A \cup B) \cap (A^c \cup B^c)) \cup C) \cap (((A^c \cup B) \cap (A \cup B^c)) \cup C^c) \\ &= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap (A^c \cup B \cup C^c) \cap (A \cup B^c \cup C^c) \\ &= A \triangle (B \triangle C)\end{aligned}$$

as required (n.b. $\triangle$ is also commutative).

4. By the inclusion-exclusion principle,

$$\varphi(p_1p_2p_3) = p_1p_2p_3 - p_1p_2 - p_2p_3 - p_3p_1 + p_1 + p_2 + p_3 - 1$$

Put $p_1 = 7, p_2 = 11, p_3 = 13$ to obtain $\varphi(1001) = 720$.

5. Yes. For example, consider $A_n = [n, \infty)$. Then $\bigcap_{i=1}^n A_i = A_n \neq \varnothing$. Now suppose $A = \bigcap_{i=1}^\infty A_i$ is non-empty. If we let $x \in A$, $x \geqslant n$ for all $n \in \mathbb{N}$, which is a contradiction. Hence $A = \varnothing$.

6. g is injective if $f \circ g$ is injective; and f is surjective if $f \circ g$ is surjective.

7. Because there exists a bijection between $\mathbb{R}$ and $(0,1)$, it is sufficent to show that there exists an injection $f : (0,1) \times (0,1) \to (0,1)$. For $(x,y) \in (0,1) \times (0,1)$ where

$$x = 0.x_1x_2\cdots \text{ and } y = 0.y_1y_2\cdots$$

let

$$f(x) = 0.x_1y_1x_2y_2\cdots$$

To make this well-defined, we avoid writing decimals that end with infinitely long tails of 9s. Furthermore, suppose $f(a,b) = f(c,d)$. This implies $0.a_1b_1a_2b_2\cdots = 0.c_1d_1c_2d_2\cdots$. Then $a_i = c_i, b_i = d_i$ so $(a,b) = (c,d)$ and f is injective.

8. By construction, it is reflective and symmetric. However, it is not transitive. E.g. $4R36$ and $36R9$ but $4 \nmid 9$. Thus R is not an equivalence relation.

9. Without loss of generality, let n elements $\{1, 2, \ldots, n\}$. First, note that, for R to be transitive, it should contain $(1,1), (2,2), \ldots, (n,n)$. Now, for the upper bound, we consider whether (x,y) is in R or not, with condition $x > y$ (because R symmetric). Since there are $n(n-1)/2$ such pairs, upper bound will be $2^{n(n-1)/2}$. For the lower bound, there are 2^{n-1} ways to choose elements that are not related with any other elements from $\{2, 3, \ldots, n\}$. This is a lower bound, since there will be at least one way, e.g. relating every pair, to relate the elements that are related with at least one another element.

   Meanwhile, clearly $2^{n(n-1)/2}$ is not the strongest upper bound since we did not account for transitivity. Recall that equivalence class forms partition, and there is a equivalence relation for a given partition. Hence, number of equivalence relations is the same as the ways of partitioning a set, i.e. *Bell numbers*. First few terms of Bell numbers are

$$B_1 = 1, B_2 = 2, B_3 = 5, B_4 = 15, B_5 = 52$$

and there also exists a summation formula

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

But there is no explicit formula to calculate it. However, we may give a rough estimate $B_n \leqslant n^n$, since n^n is a number of maps $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. n^n is a stronger upper bound than $2^{n(n-1)/2}$, since

$$\ln n \leqslant \frac{\ln 2}{2} n - \frac{\ln 2}{2}$$

(for sufficiently large n).

10. Each disc contains a point with rational coordinates, and so there exists an injection from family of discs $D \to \mathbb{Q} \times \mathbb{Q}$. But $\mathbb{Q} \times \mathbb{Q}$ is countable so such family is always countable.

    However, there exists an uncountable family of circles. Consider a family of all concentric circles, I. If we write $r(C) \in \mathbb{R}$ for radius of a circle $C \in I$, there exists a bijection $I \to \mathbb{R}_{>0}$, $C \mapsto r(C)$. Hence I is uncountable.

11. It is countable. There is a bijection $F \to \mathbb{N}$,

$$\{a_1, \ldots, a_n\} \mapsto 2^{a_1} + \cdots 2^{a_n}$$

12. Suppose set of increasing functions are countable. Then, we may number them as $f_1, f_2, f_3, \ldots$. Now define a new function recursively by $f(1) = 1$ and

$$f(n+1) = f(n) + f_n(n+1) - f_n(n) + 1$$

    If $f_n(n) = f(n)$, $f(n+1) = f_n(n+1) + 1 \neq f_n(n+1)$. So $f \neq f_n$ for all n, which is a contradiction. Hence set of increasing functions is uncountable.

    For decreasing functions, consider

$$S_N = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ is decreasing and } f(1) \leqslant N\}$$

    and $S = \bigcup_{N \in \mathbb{N}} S_N$. We claim that S_N is countable for all $N \in \mathbb{N}$. We prove by induction. Because $S_1 = \{f\}$ where $f(n) = 1 \quad \forall n \in \mathbb{N}$, it is clearly countable. Suppose S_N is countable. Note that a function in S_{N+1} is the constant function $f(n) = N + 1$ or it achieves some number $m = f(n_0) < N + 1$ after some point $n_0 \in \mathbb{N}$. After this point, the function can be considered as a function of S_N (by replacing $N + 1$ as N). Hence we may define a function in S_{N+1} by specifying n_0 and a function in S_N. Therefore, there is an injection from S_{N+1} to $\mathbb{N} \times S_N$, which is countable since S_N is countable (we may map $f(n) = N + 1 \mapsto (1, f(n) = N)$). Hence, S_{N+1} is countable, and thus S_N is countable for all $N \in \mathbb{N}$. Therefore, S is countable since it is a countable union of countable sets.

13. S is always countable because there exists an injection $S \mapsto \mathbb{N}$, $A \mapsto \max(A)$.

    For next part, let's consider a collection of all infinite bit strings, B, which is uncountable by diagonal argument. Then, consider a bijection $\phi : B \to \mathcal{P}(N)$ that maps elements by concatenating 1 in front of the bit string and identifying initial segments as binary expansions of the set elements. For example, for finite bit string,

$$00101 \mapsto \{1, 2, 4, 9, 18, 37\}$$

Note that all the associated integers are disjoint beyond the point at which two strings first differ. Hence, every intersection is finite and includes 1. So, we may define $T = \operatorname{im}\phi$.

14. Since both $\mathbb{Q}$ and $\mathbb{Q}\backslash\{0\}$ are dense, they are order isomorphic (requires further explanation).

CHAPTER 2

Groups

Lecture by Professor Henry Wilton. Michaelmas term 2023.

2.1 Groups

2.1.1 Introduction

Definition 2.1.1. A *binary operation* on a set X is a map

$$\cdot : X \times X \to X,\ (x, y) \mapsto x \cdot y$$

Definition 2.1.2. A *group* is a triple $(G, \cdot, e)$ where G is a set, $e \in G$, $\cdot$ is a binary operation, satisfying four axioms: for all $g_1, g_2, g_3 \in G$,

- Closure: $g_1 \cdot g_2 \in G$.
- Associativity: $(g_3 \cdot g_2) \cdot g_1 = g_3 \cdot (g_2 \cdot g_1)$.
- Identity: $\exists e \in G$ s.t. $g \cdot e = g \quad \forall g \in G$.
- Inverse: For each $a \in G$, $\exists b \in G$ s.t. $a \cdot b = e$.

We sometimes write only G for a group, if the operation and the identity element is clear enough.

Example 2.1.1. The symmetries of an equilateral triangle form a group.

Example 2.1.2. $(\mathbb{Z}, +, 0)$ forms a group.

Proposition 2.1.1. Let $(G, \cdot, e)$ be a group and $a, b, b', e \in G$. Then,

(1) if $a \cdot b = e$ then $b \cdot a = e$;

(2) $e \cdot a = a$;

(3) if $a \cdot b = e = a \cdot b'$, then $b = b'$;

(4) If $a \cdot e' = a$, $e' = e$.

Proof.

(1) $b = b \cdot e = b \cdot (a \cdot b) = (b \cdot a) \cdot b$. But there exists c such that $b \cdot c = e$. Hence

$$e = b \cdot c = ((b \cdot a) \cdot b) \cdot c = (b \cdot a) \cdot (b \cdot c) = (b \cdot a) \cdot e = b \cdot a$$

(2) There exists $b \in G$ such that $a \cdot b = e$. Hence

$$e \cdot a = (a \cdot b) \cdot a = a \cdot (b \cdot a) = a \cdot e = a$$

by identity.

(3) There exists $c \in G$ such that $b \cdot c = c \cdot b = e$. Then,

$$b' = e \cdot b' = (b \cdot a) \cdot b' = b \cdot (a \cdot b') = b \cdot e = b$$

(4) By inverse and part (1), there exists $b \in G$ such that $b \cdot a = e$. We are given $a = a \cdot e'$. Multiply on the left by b to obtain

$$e = b \cdot a = b \cdot (a \cdot e') = (b \cdot a) \cdot e' = e \cdot e' = e'$$

■

Part (3) of Proposition 2.1.1 says that inverses are unique. Therefore, if $a \cdot b = e$, then we can write $b = a^{-1}$; and by part (1), $a \cdot a' = e = a^{-1} \cdot a$. Hence $(a^{-1})^{-1} = a$. It now makes sense to write, for any $g \in G$, $g^0 = e$, $g^1 = g$, $g^2 = g \cdot g$, $\ldots$, $g^n = g^{n-1} \cdot g$ for any $n \in \mathbb{N}$, and $g^n = (g^{-1})^{-n}$ for $n = -1, -2, \ldots$.

Example 2.1.3. For any $g \in G$, $m, n \in \mathbb{Z}$, $g^m \cdot g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$.

Remark 2.1.1. Recall that $a \cdot b$ is not necessarily $b \cdot a$ in a group. Also, it is not necessarily true that $(a \cdot b)^{-1} = a^{-1}b^{-1}$. However,

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (a \cdot (b \cdot b^{-1})) \cdot a^{-1} = (a \cdot e) \cdot a^{-1} = a \cdot a^{-1} = e$$

and $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Definition 2.1.3. If G is a group, and furthermore, $a \cdot b = b \cdot a$ for all $a, b \in G$, then G is called *abelian*.[1]

For example, if $G = \{e\}$ and $e \cdot e = e$, $(G, \cdot, e)$ is called the *trivial group*. Moreover,

(1) $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ are all abelian groups;

(2) $(\mathbb{N}, +, 0)$ is not a group;

(3) $(\mathbb{Q}, \times, 1)$ is not a group but $(\mathbb{Q}\backslash\{0\}, \times, 1)$ is. Likewise, $(\mathbb{R}\backslash\{0\}, \times, 1)$, $(\mathbb{C}\backslash\{0\}, \times, 1)$ are also groups.

Definition 2.1.4. The *order* of a group $(G, \cdot, e)$ is the number of elements of G, denoted by $|G|$. If $|G| < \infty$, then $(G, \cdot, e)$ is finite.

Example 2.1.4.

(1) For any $n \in \mathbb{N}_{\geqslant 0}$, let

$$C_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

Then $(C_n, \times, 1)$ is an abelian group of order n.

(2) Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. For $a, b \in \mathbb{Z}_n$, let $a +_n b$ be the remainder when $a + b$ is divided by n. Then $(\mathbb{Z}_n, +_n, 0)$ is an abelian group of order n.

[1] You may capitalise.

∗ Matrix groups

There are lot more types of groups. For example, let $\mathrm{GL}_2(\mathbb{R})$ be the set of 2×2 matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \mathbb{R}$ and A invertible, i.e. there is B such that

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1} = 1$$

Now, $(\mathrm{GL}_2(\mathbb{R}), \cdot, 1)$ is a group. It is infinite because it contains

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

for all $t \in \mathbb{R}$ and non-abelian, e.g.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Matrix groups will be revisted later when we are talking physics.

∗ Symmetric groups

Let X be a set. Then a *permutation* of a set X is a bijection $X \to X$.

Definition 2.1.5. $\mathrm{Sym}(X)$ is defined to be a set of all permutations, i.e. bijections $X \to X$.

Lemma 2.1.2. (*Composition is associative*) Consider maps of sets

$$W \xrightarrow{f} X \xrightarrow{g} Y \xrightarrow{h} Z$$

Then

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

Proof. Let $w \in W$. Then

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

■

Proposition 2.1.3. For any set X, $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ is a group.

Proof. Associativity follows from Lemma 2.1.2. The identity map $\mathrm{id}_X : X \to X$, $x \mapsto x$ clearly produces an identity element for the group. Finally, inverse exists by definition. ■

We are especially interesed in the case when X is finite.

Definition 2.1.6. If $X = \{1, 2, \ldots, n\}$, we write $S_n = \mathrm{Sym}(X)$.

N.b. $|S_n| = n!$.

2.1.2 Subgroups

Definition 2.1.7. Let $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ be groups. If (1) $H \subseteq G$, (2) $e_H = e_G$, and (3) $a \cdot_H b = a \cdot_G b$ for all $a, b \in H$, then H is a *subgroup* of G and we write

$$H \leqslant G$$

Proposition 2.1.4. (*Subgroup Criterion*) Let G be a group and $H \subseteq G$ is a non-empty subset. If $a \cdot b^{-1} \in H$ for all $a, b \in H$, then $H \leqslant G$.

Proof. Since H is non-empty, there is $x \in H$. Therefore

$$e_G = x \cdot x^{-1} \in H$$

For any $a \in H$, $a^{-1} = e_G \cdot_G a^{-1} \in H$. Finally, for any $a, b \in H$, $b^{-1} \in H$ by above, so

$$a \cdot_G b = a \cdot_G (b^{-1})^{-1} \in H$$

Now, if we set $e_H = e_G$ and $\cdot_H$ as the restriction of $\cdot_G$ to H, then $H \leqslant G$. ■

Example 2.1.5.

(1) Every group G is a subgroup of itself.

(2) For any group G, $1_G = \{e_G\}$ is called the *trivial subgroup*. Other subgroups are called *proper*.

(3) $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$.

(4) If $H_i \leqslant G$ (for some sets of is), then

$$H = \bigcap_i H_i \leqslant G$$

(5) For any subset of $X \subseteq G$, define

$$\langle X \rangle = \bigcap_{X \subseteq H \leqslant G} H \leqslant G$$

This is the subgroup generated by X. If $\langle X \rangle = G$, then we say that X generates G.

Proposition 2.1.5. The subgroups of $\mathbb{Z}$ are exactly the subsets

$$n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$

for all $n = 0, 1, 2, \ldots$

Proof. First, note that each $n\mathbb{Z}$ really is a subgroup of $\mathbb{Z}$: if $a = nk, b = nl \in n\mathbb{Z}$,

$$a + (-b) = a - b = nk - nl = n(k - l) \in n\mathbb{Z}$$

so the result follows by the subgroup criterion.

Now suppose that $H \subseteq \mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$ and we are done. If $\{H\} \neq \{0\}$, then we may choose $n \in H \backslash \{0\}$ to be the smallest positive element of H.[2] Since H is closed under taking inverses, $-n \in H$. Moreover, since H is closed under addition,

[2] Well-ordering principle.

$n+n=2n\in H$, $n+2n=3n\in H$,...,$nk\in H$ for all $k\geqslant 1$. Similarly $-n-n=-2n\in H$ etc. So $n\mathbb{Z}\in H$. We want to show that $n\mathbb{Z}=H$. Suppose $n\mathbb{Z}\neq H$. Then there is $x\in H\backslash n\mathbb{Z}$. Dividing x by n and take remainders to find $x=nq+r$ for some $q\in\mathbb{Z}$ and $0<r<n$ ($r\neq 0$ since $x\notin n\mathbb{Z}$). But now

$$r=x-nq\in H$$

which is a contradiction to the definition of n. ■

2.1.3 Isometry

Let $\mathbb{C}$ be a complex plane, equipped with the notion of distance: $|z-w|$ for some $z,w\in\mathbb{C}$.

Definition 2.1.8. For any subsets $X\subseteq\mathbb{C}$, an *isometry* of X is a bijection $f:X\to X$ that preserves distance, i.e.

$$|f(x)-f(y)|=|x-y|$$

for all $x,y\in X$.

Proposition 2.1.6. Let $X\subseteq\mathbb{C}$. The sets of isometries of X,

$$\mathrm{Isom}(X)=\{f\ :\ X\to X \text{ is a bijection and } f \text{ is an isometry}\}$$

is a subgroup of $\mathrm{Sym}(X)$.

Proof. Since $\mathrm{id}_X\in\mathrm{Isom}(X)$, it is non-empty. By the subgroup criterion, it suffices to check that $f\cdot g^{-1}\in\mathrm{Isom}(X)$ where $f,g\in\mathrm{Isom}(X)$. Let $x,y\in X$. Then,

$$\begin{aligned}|(f\circ g^{-1})(x)-(f\circ g^{-1})(y)| &= |g^{-1}(x)-g^{-1}(y)|\\ &= |g\circ g^{-1}(x)-g\circ g^{-1}(y)|\\ &= |x-y|\end{aligned}$$

■

Definition 2.1.9. Let $X_n\subseteq\mathbb{C}$ be the n-gon with vertices

$$X_n=\{e^{2\pi ik/n}\mid k=0,1,\ldots,n-1\}$$

Then, we define the n^{th} *dihedral group* as

$$D_{2n}=\mathrm{Isom}(X_n)$$

Example 2.1.6. D_6 is the isometry group of the equilateral triangle.

Theorem 2.1.7. Order of n^{th} diherdral group, $|D_{2n}|$, is $2n$ and

$$D_{2n}=\{e,r,\ldots,r^{n-1},s,rs,\ldots,r^{n-1}s\}$$

where r and s are bijections $r,s:X_n\to X_n$ such that

$$r(z)=e^{2\pi i/n}z$$

i.e. *rotation*, and

$$s(z)=\bar{z}$$

i.e. *reflection*.

Proof. We first need some geometric facts.

Lemma 2.1.8. (*Kite lemma*) Let $x_1, x_2, y_1, y_2 \in \mathbb{C}$. If $|y_1 - x_1| = |y_2 - x_1|$ and $|y_1 - x_2| = |y_2 - x_2|$, then $x_2 - x_1$ is perpendicular to $y_2 - y_1$.

Lemma 2.1.9. (*Three Point lemma*) Let $X \subseteq \mathbb{C}$, $f \in \mathrm{Isom}(X)$. If there are x_1, x_2, x_3 in X, not colinear, such that $f(x_1) = x_1, f(x_2) = x_2, f(x_3) = x_3$, then $f = \mathrm{id}_X$.

Proof. We will only prove the three point lemma here. Suppose there is some $y \in X$ such that $f(y) \neq y$. Then since f is a isometry,

$$|f(y) - x_i| = |f(y) - f(x_i)| = |y - x_i|$$

where $i = 1, 2, 3$. Now let $y_1 = y$, $y_2 = f(y)$. Then, by the Lemma 2.1.8,

$$x_2 - x_1 \perp f(y) - y$$

Similarly, $x_3 - x_1 \perp f(y) - y$. Hence x_1, x_2, x_3 are colinear, which is a contradiction. ■

Returning to the original proof, we check that $r, s \in D_{2n}$. Indeed, for any $x, y \in \mathbb{C}$,

$$\begin{aligned} |r(x) - r(y)| &= |e^{2\pi i/n}x - e^{2\pi i/n}y| = |e^{2\pi i/n}(x - y)| = |e^{2\pi i/n}||x - y| \\ &= |x - y| \end{aligned}$$

so r is an isometry; and $r(e^{2\pi ik/n}) = e^{2\pi i(k+1)/n}$ so r preserves X_n. Similarly, for any $x, y \in \mathbb{C}$,

$$s(x) - s(y) = |\bar{x} - \bar{y}| = |\overline{(x - y)}| = |x - y|$$

so again, s is isometry; and $s(e^{2\pi ik/n}) = e^{-2\pi i/n} = e^{2\pi i(n-k)/n}$ so s also preserves X_n. Therefore, $r, s \in D_{2n}$. Consequently, we find out that

$$\{e, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\} \subseteq D_{2n}$$

To see that this is all of the elements of D_{2n}, let $f \in D_{2n}$, and consider its effects on $x = 1$, $y = e^{2\pi i/n}$, $z = e^{-2\pi i/n}$. Since $f \in D_{2n}$, it sends vertices to verticies, so

$$f(x) = e^{2\pi ik/n}$$

for some $k = 0, 1, \ldots, n - 1$. Hence,

$$r^k \circ f(x) = r^{-k}(e^{2\pi ik/n}) = 1 = x$$

Now since $r^{-k} \circ f \in D_{2n}$, $r^{-k} \circ f(y) \in \{y, z\}$ and $r^{-k} \circ f(z) \in \{y, z\}$ from isometry. There are two cases:

(1) $r^{-k} \circ f(y) = y$ and $r^{-k} \circ f(z) = z$;

(2) $r^{-k} \circ f(y) = z$ and $r^{-k} \circ f(z) = y$.

In case (1), $r^{-k} \circ f$ fixes x, y, z. Thus $r^{-1} \circ f = \mathrm{id}_X$ by the three point lemma. Hence $f = r^k$. In case (2), $r^{-k} \circ f(x) = x = s(x)$, $r^{-k} \circ f(y) = z = s(y)$, $r^{-k} \circ f(z) = y = s(z)$. So $s^{-1} \circ r^{-k} \circ f$ fixes x, y, z and again by the three point lemma, $f = r^k s$.

Finally, to show that $|D_{2n}| = 2n$, we need to check that all elements on the lists are distinct. First, if $0 \leqslant k, l < n$ such that $r^k = r^l$, then

$$e^{2\pi ik/n} = r^k(1) = r^l(1) = e^{2\pi il/n} \Rightarrow r = l$$

If $r^k = s$, then $e^{2\pi ik/n} = r^k(1) = s(1) = 1$ so $s = r^0 = e$, which is a contradiction; hence, $s \neq r^k$ for any k. If $r^k = r^l s$, then $s = r^{k-l}$, which is a contradiction. Lastly, if $0 \leqslant k, l < n$ such that $r^k s = r^l s$, then by multiplying s^{-1}, $r^k = r^l \Rightarrow k = l$ as above. ■

To multiply elements of D_{2n} with ease, we use the *dihedral relation*, stated below.

Lemma 2.1.10. (*Dihedral Relation*) For $r, s \in D_{2n}$ as above, $sr = r^{-1}s$.

Proof. We show that sr and rs^{-1} do the same thing to $\{x, y, z\}$ as above. (**Incomplete**) ■

Using the dihedral relation, algebra becomes easy in D_{2n}. For instance, $r^k r^l = r^{k+l}$, $r^k(r^l s) = r^{k+l}s$, $(r^k s)r^l = r^{k-l}s$, and $r^k s r^l s = r^{k-l}ss = r^{k-l}$.

2.1.4 Homomorphisms

∗ Homomorphisms and isomorphisms

Definition 2.1.10. A map between group $\phi : G \to H$ is called a *homomorphism* if

$$\phi(g \cdot g') = \phi(g) \cdot \phi(g')$$

for all $g, g' \in G$, i.e. it preserves group operation.

Example 2.1.7.

(1) For any group G, H, the map $\phi : G \to H$, $g \mapsto e_G$ is the *trivial homomorphism*.

(2) If $H \leqslant G$, then the map $i_H : H \to G$, $h \mapsto h$ is the *inclusion homomorphism*.

(3) Recall $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$. If $n|m$, $\phi : C_m \to C_n$, $z \mapsto z^{m/n}$ is a homomorphism.

Lemma 2.1.11. If $\phi : G \to H$ is a homomorphism, then

(1) $\phi(e_G) = e_H$;

(2) $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.

Proof.

(1) Calculation gives

$$\begin{aligned} e_H &= \phi(e_G)^{-1} \cdot \phi(e_G) = \phi(e_G)^{-1} \cdot \phi(e_G \cdot e_G) = \phi(e_G)^{-1} \cdot (\phi(e_G) \cdot \phi(e_G)) \\ &= (\phi(e_G)^{-1} \cdot \phi(e_G)) \cdot \phi(e_G) = e_H \cdot \phi(e_G) = \phi(e_G) \end{aligned}$$

(2) $\phi(g) \cdot \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(e_G) = e_H$ by (1). Hence $\phi(g^{-1}) = \phi(g)^{-1}$ by definition.

■

Definition 2.1.11. If a homomorphism $\phi : G \to H$ is also a bijection, we say that ϕ is an *isomorphism*, and write

$$G \cong H$$

i.e. G is isomorphic to H.

For example, consider two groups C_n and $\mathbb{Z}_n$. Then $\phi_n : \mathbb{Z}_n \to C_n$, $k \mapsto e^{2\pi i k/n}$ is a bijection. Furthermore, $k + l = pn + (k +_n l)$ for some $p \in \mathbb{Z}$, and

$$\begin{aligned} \phi(k +_n l) &= e^{2\pi i(k+_n l)/n} = e^{2\pi i(pn)/n} e^{2\pi i(k+_n l)/n} \\ &= e^{2\pi i(pn+k+_n l)/n} \\ &= e^{2\pi i(k+l)/n} = e^{2\pi i(k)/n} e^{2\pi i(l)/n} = \phi(k)\phi(l) \end{aligned}$$

Thus $\mathbb{Z}_n \cong C_n$

Lemma 2.1.12.

(1) If $\phi : G \to H$ is a homomorphism, so is ϕ^{-1}.

(2) If $G \xrightarrow{\phi} H \xrightarrow{\psi} K$ are both Homomorphisms, then so is $\psi \circ \phi$.

(3) $\cong$ is an equivalence relations.[3]

Definition 2.1.12. Let $\phi : G \to H$ be a homomorphism.

(1) The *image* of ϕ is

$$\mathrm{im}(\phi) = \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$$

(2) The *kernel* of ϕ is

$$\ker(\phi) = \{g \in G \mid \phi(g) = e\}$$

Proposition 2.1.13. If $\phi : G \to H$ is a homomorphism, then (1) $\mathrm{im}\,\phi \leqslant H$ and (2) $\ker\phi \leqslant G$.

Proof.

(1) $e_H = \phi(e_G) \in \mathrm{im}\,\phi$ so $\mathrm{im}\,\phi$ is non-empty. Also, for $h_1 = \phi(g_1), h_2 = \phi(g_2) \in \mathrm{im}\,\phi$, $h_1 h_2^{-1} = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1 g_2^{-1}) \in \mathrm{im}(\phi)$. So $\mathrm{im}\,\phi \leqslant H$ by the subgroup criterion.

(2) $e_H = \phi(e_G) \Rightarrow e_G \in \ker\phi$ so it is non-empty. Also, for $g_1, g_2 \in \ker\phi$, $\phi(g_1 g_2^{-1}) = e_H \cdot e_H^{-1} = e_H$ so $g_1 g_2^{-1} \in \ker\phi$. Hence $\ker\phi \leqslant G$ by the subgroup criterion.

■

Remark 2.1.2. Let $\phi : G \to H$ be a homomorphism.

(1) ϕ is surjective if and only if $\mathrm{im}\,\phi = H$.

(2) ϕ is injective if and only if $\ker\phi$ is the trivial subgroup, i.e. $\ker\phi = 1_G \leqslant G$. Indeed, if ϕ is injective, then $\ker\phi = \phi^{-1}(\{e_H\})$ has equal or less than one element. But $e_G \in \ker\phi$ so $\ker\phi = \{e_G\} = 1_G$.

Conversely, suppose $\ker\phi = 1_G$. If $\phi(g_1) = \phi(g_2)$, then

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = e_H \Rightarrow g_1 g_2^{-1} \in \ker\phi = \{e_G\}$$

so $g_1 g_2^{-1} = e_G \Rightarrow g_1 = g_2$. Thus ϕ is injective.

(3) Therefore, $\phi : G \to H$ is an isomorphism if and only if $\mathrm{im}\,\phi = H$ and $\ker\phi = 1_G$.

∗ Cyclic groups

Definition 2.1.13. A group G is *cyclic* if there is $g \in G$ such that

$$G = \{g^k \mid k \in \mathbb{Z}\}$$

where such element g is called the *generator* of G.

Example 2.1.8.

(1) $C_n \cong \mathbb{Z}_n$ are cyclic.

[3] Recall Numbers and Sets.

(2) $\mathbb{Z}$ is cyclic, with generator 1.

Theorem 2.1.14. If G is cyclic, then either $G \cong C_n$ for some n, or $G \cong \mathbb{Z}$.

Proof. Let G be a cyclic group, with generator g. Let

$$S = \{k \in \mathbb{N} \mid g^k = e\}$$

and let[4]

$$n = \begin{cases} \min S & S \neq \varnothing \\ \infty & S = \varnothing \end{cases}$$

If $n = \infty$, define $\phi : \mathbb{Z} \to G$ by $k \mapsto g^k$. We need to show that ϕ is an isomorphism. Since

$$\phi(k+l) = g^{k+l} = g^k g^l = \phi(g)\phi(k)$$

ϕ is a homomorphism. Also, it is surjective because it is cyclic. To prove that injectivity, suppose $\ker\phi \neq \{0\}$, and let $0 \neq k \in \ker\phi$. Since $\ker\phi \leqslant \mathbb{Z}$, we may replace k by $-k$ if necessary, and assume $k > 0$.[5] But now $k \in S$, so S is non-empty, which is a contradiction. Thus $\ker\phi$ is trivial, so ϕ is bijective, and $\mathbb{Z} \cong G$.

If $n < \infty$, define $\phi : \mathbb{Z}_n \to G$, $k \mapsto g^k$. It is easy to check ϕ is a homomorphism. To prove surjectivity, consider $g^k \in G$ for some $k \in \mathbb{Z}$. Using the division algorithm, write $k = nq + r$ for some $r \in \mathbb{Z}_n$, $q \in \mathbb{Z}$. So

$$g^k = (g^n)^q g^r = g^r = \phi(r)$$

as required. To prove injectivity, suppose that $\phi(k) = e$. Since n was minimal such that $\phi(n) = e$, and $0 \leqslant k < n$, it follows that $k = 0$. So $\ker\phi = \{0\} = 1_{\mathbb{Z}_n}$. Thus ϕ is injective, hence an isomorphism, and $G \cong \mathbb{Z}_n \cong C_n$. ∎

Because of Theorem 2.1.14, we will write C_n for any cyclic group of order n, and also $C_\infty = \mathbb{Z}$.

Definition 2.1.14. For any group G and element $g \in G$, let

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \leqslant G$$

Note that $\langle g \rangle$ is cyclic, so $\langle g \rangle \cong C_n$ for some $n \in \mathbb{N} \cup \{\infty\}$. This number n is called the *order* of g, denoted $o(g)$. Also, from the proof of Theorem 2.1.14, we have $g^{o(g)} = e$. N.b. this is different with the order of the group itself, $|G|$.

2.2 Group Actions

2.2.1 Actions

Definition 2.2.1. An *action* of a group G on a set X is a map

$$G \times X \to X, \quad (g, x) \mapsto gx \text{ or } g(x)$$

($g \in G$ and $x \in X$) such that

(1) $ex = x$ for all $x \in X$;

[4] ∞ is merely a symbol here.
[5] They are both in $\ker\phi$.

(2) $(g \cdot h)x = g(hx)$ for all $g, h \in G$, $x \in X$.

We write $G \curvearrowright X$ to indicate that G acts on X.

Example 2.2.1.

(1) For any group G and set X, $gx = x$ for all $g \in G$, $x \in X$ define the *trivial action*.

(2) The symmetric group $\mathrm{Sym}(X)$ acts on X via $fx = f(x)$.

(3) For any $X \subseteq \mathbb{C}$, $\mathrm{Isom}(X) \leqslant \mathrm{Sym}(X)$ acts on X.

(4) In particular, D_{2n} acts on the regular n-gon X_n.

(5) Every group G acts on itself, i.e. $X = G$, via $g \in G$, $\gamma \in G = X$, $g\gamma = g \cdot \gamma$. This is called the *regular action*.

Theorem 2.2.1. An action of a group G on a set X is the same as the homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. Suppose $G \curvearrowright X$. Gor any $g \in G$, consider $t_g : X \to X$, $x \mapsto gx$. Now

$$t_{g^{-1}}(t_g(x)) = t_{g^{-1}}(gx) = g^{-1}(gx) = (g^{-1} \cdot g)(x) = ex = x$$

So $t_{g^{-1}} = (t_g)^{-1}$. Hence t_g is a bijection. Therefore, we may define $\phi : G \to \mathrm{Sym}(X)$, $g \mapsto tg$. We need to check that ϕ is a homomorphism. For any $g, h \in G$, $x \in X$,

$$(t_g \circ t_h)(x) = t_g(hx) = g(hx) = (gh)(x) = t_{gh}(x)$$

so $t_g \circ t_h = t_{gh}$. Thus $\phi(g)\phi(h) = t_g \circ t_h = t_{gh} = \phi(gh)$ and ϕ is a homomorphism.

Conversely, given a homomorphism $\phi : G \to \mathrm{Sym}(X)$, we may define an action $G \curvearrowright X$ as follows: $gx = \phi(g)(x)$. Let's check that this is an action:

(1) $ex = \phi(e)(x) = \mathrm{id}_X(x) = x$

(2) $(gh)x = \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)(hx) = g(hx)$

■

Theorem 2.2.2. (*Cayley's Theorem*) Every group G is isomorphic to a subgroup of some symmetric group $\mathrm{Sym}(X)$. Furthermore, if $|G| < \infty$, X can be taken to be finite.

Proof. Let $X = G$. Consider the regular action $G \curvearrowright X$. By Theorem 2.2.1, this gives a homomorphism $\phi : G \to \mathrm{Sym}(X)$. Let $H = \mathrm{im}\,\phi$. Since we proved that $H \leqslant \mathrm{Sym}(X)$, we may think of ϕ as a surjective homomorphism $\phi : G \to H$. Now claim $\ker \phi = \{e\}$, indeed,

$$g \in \ker \phi \Leftrightarrow \phi(g) = \mathrm{id}_G \Leftrightarrow g\gamma = \gamma,\ \forall \gamma \in G \Rightarrow ge = e \Rightarrow g = e$$

Hence ϕ is an isomorphism, as required. Moreover, since $G = X$, if $|G| < \infty$, then X is certainly also finite. ■

Definition 2.2.2. Let $G \curvearrowright X$ and $x \in X$.

(1) The *orbit* of x is the set

$$Gx = \{y \in X \mid y = gx \text{ for some } g \in G\}$$

(2) The *stabiliser* of x is the set

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$$

If $Gx = X$ for all $x \in X$, the action is *transitive*. If every element $g \in G$ apart from e has $x \in X$ such that $gx \neq x$, then $G \curvearrowright X$ is called *faithful*. Note that $G \curvearrowright X$ is faithful if and only if the associated homomorphism $G \to \mathrm{Sym}(X)$ is injective.

Proposition 2.2.3. Suppose $G \curvearrowright X$.

(1) $\mathrm{Stab}_G(x) \leqslant G$ for any $x \in X$.

(2) The orbits $\{Gy \mid y \in X\}$ form a *partition* of X, i.e. every element is in exatly one orbit.

Proof.

(1) Let's check the subgroup criterion. Clearly, $e \in \mathrm{Stab}_G(x)$. If $g, h \in \mathrm{Stab}_G(x)$,

$$(gh^{-1})(x) = (gh^{-1})(hx) = ((gh^{-1})h)x = (g(h^{-1}h))x = gx = x$$

So $gh^{-1} \in \mathrm{Stab}_G(x)$ and $\mathrm{Stab}_G(x) \leqslant G$ as claimed.

(2) First, note that $x = ex \in Gx$. So every $x \in X$ is in at least one orbit. Suppose $x \in Gy \cap Gz$. Then there are two elements $g, h \in G$ such that $gy = x = hz$. We claim that $Gy \subseteq Gz$. To prove this, take an arbitrary element $ky \in Gy$ for some $k \in G$. Since $gy = hz$,

$$y = ey = (g^{-1}g)y = g^{-1}(gy) = g^{-1}(hz) = (g^{-1}h)z$$

So $ky = k((g^{-1}h)z) = (k(g^{-1}h))z \in Gz$. Hence, $Gy \subseteq Gz$. Similarly, $Gz \subseteq Gy$, and thus we obtain $Gy = Gz$. Therefore, $Gy = Gz$ if $x \in Gy$ and $x \in Gz$.

■

Example 2.2.2. By definition, $D_{2n} \curvearrowright X_n$. Let x be a vertex. Then, $\mathrm{Stab}_{D_{2n}}(x) = \{e, s\}$ so $|\mathrm{Stab}_{D_{2n}}(x)| = 2$, $|D_{2n}x| = n$, and $|D_{2n}| = 2n$.

2.2.2 Cosets

Recall that G acts on itself by the regular action $G \curvearrowright G$. For any subgroup $H \leqslant G$, we can restrict the action to H to get an action $H \curvearrowright G$, $h\gamma = h \cdot \gamma$ for $h \in H$, $\gamma \in G$.

Definition 2.2.3. Let $H \leqslant G$ and $\gamma \in G$. We form a *right coset* of H in G as

$$H\gamma = \{g \in G \mid g = h \cdot \gamma \text{ for some } h \in H\}$$

The sets of right cosets of H in G is denoted $H\backslash G$. The number of right cosets $|H\backslash G|$ is called the *index* of H in G, and is also denoted by $|G : H|$. Moreover, note that $H\gamma$ is the orbit of γ under the regular action of H on G.

Lemma 2.2.4. For any $H \leqslant G$, the right coset partitions G.

Proof. Right cosets are orbits, and orbits partition. ■

Theorem 2.2.5. (*Lagrange's Theorem*) Let $H \leqslant G$. If $|G| < \infty$, then

$$|G| = |H||G : H|$$

Proof. First, note that each coset $H\gamma$ is in bijection with H:

$$H \to H\gamma, \quad h \mapsto h\gamma$$

$$H\gamma \to H, \quad h\gamma \mapsto (h\gamma)\gamma^{-1} = h$$

Therefore, $|H\gamma| = |H|$ for all $\gamma \in G$. Since right cosets partition G into $|G : H|$ subsets of size $|H|$, the result follows. ■

Corollary 2.2.5.1. If $|G| < \infty$ and $g \in G$, then $o(g) \big| |G|$.

Proof. $o(g) = |\langle g \rangle| = |G|/|G : \langle g \rangle|$ by Lagrange's theorem. ■

Corollary 2.2.5.2. If $|G| < \infty$ and $g \in G$, $g^{|G|} = e$.

Proof. By Corollarly 2.2.5.1,

$$g^{|G|} = g^{o(g)|G:\langle g \rangle|} = (g^{o(g)})^{|G:\langle g \rangle|} = e^{|G:\langle g \rangle|} = e$$

■

Corollary 2.2.5.3. If $|G|$ is a prime, then G is cyclic, i.e. $G \cong C_p$, and any $g \neq e$ generates.

Proof. Choose any $g \neq e$ in G. Then, by Corollarly 2.2.5.1, $o(g) \big| |G| = p$. So either $o(g) = 1$ or $o(g) = p$. But $g \neq e$, so $o(g) \neq 1$, and

$$|\langle g \rangle| = o(g) = p = |G|$$

Hence, $\langle g \rangle = G$, and G is indeed cyclic. ■

Example 2.2.3. Lagrange's theorem can be also applied to number theory. Recall from Numbers and Sets that $x \in \mathbb{Z}_n$ has a multiplicative inverse modulo n if and only if $\gcd(x, n) = 1$. Hence, we define

$$\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$$

which is a group, with operation $\times_n$, denoting multiplication modulo n on $\mathbb{Z}_n$. Now we give a different proof for the Fermat-Euler theorem as follows.

Proof. By dividing modulo n, we may assume $x \in \mathbb{Z}_n$. Now, by Corollarly 2.2.5.2,

$$x^{\varphi(n)} = x^{|\mathbb{Z}_n^\times|} = 1$$

That is, $x^{\varphi(n)} \equiv 1 \mod n$. ■

Definition 2.2.4. Let $H \leqslant G$ and $\gamma \in G$. The subset

$$\gamma H = \{g \in G \mid g = \gamma \cdot h \text{ for some } h \in H\}$$

is called the *left coset* of H in G.

The notation G/H denotes the set of all left cosets of H in G.

Lemma 2.2.6. If $H \leqslant G$, the sets of left cosets

$$G/H = \{\gamma H \mid \gamma \in G\}$$

partitions G.

Proof. Since $g \in gH$, we need to show that each $g \in G$ is at most one γH. First, note that $g \in \gamma H \Leftrightarrow g = \gamma h \Leftrightarrow g^{-1} = h^{-1}\gamma^{-1} \Leftrightarrow g^{-1} = h'\gamma^{-1} \Leftrightarrow g^{-1} \in H\gamma^{-1}$ for some $h, h' \in H$. Therefore, since right cosets partition,

$$g \in \gamma H \cap \gamma' H \Rightarrow g^{-1} \in H\gamma^{-1} \cap H(\gamma')^{-1} \Rightarrow H\gamma^{-1} = H(\gamma')^{-1} \Rightarrow \gamma H = \gamma' H$$

■

In facts, there exists an action $H \curvearrowright G$ which can show that left coset is an orbit.

Lemma 2.2.7. If $|G| < \infty$ and $H \leqslant G$, $|G/H| = |H\backslash G| = |G : H|$.

Theorem 2.2.8. (*Orbit-Stabiliser Theorem*) Suppose $G \curvearrowright X$ and $x \in X$. The assignment

$$g\,\mathrm{Stab}_G(x) \mapsto gx$$

defines a well-defined bijection $G/\mathrm{Stab}_G(x) \to Gx$.

Proof. For brevity, write $S = \mathrm{Stab}_G(x)$, and $\Phi(gS) = gx$. We first check that Φ is well defined. Suppose $g_1 S = g_2 S$. Because $g_1 \in g_1 S = g_2 S$, there is $s \in S$ such that $g_1 = g_2 s$. Now[6]

$$\begin{aligned}\Phi(g_1 S) &= g_1 x = (g_2 s)x = g_2(sx)\\ &= g_2 x = \Phi(g_2 S)\end{aligned}$$

Hence Φ is well-defined.

Clearly, Φ is surjective since for any $gx \in Gx$, $\Phi(gS) = gx$.

Finally, to prove that Φ is injective, suppose $\Phi(g_1 S) = \Phi(g_2 S)$. This implies

$$g_1 x = g_2 x \Leftrightarrow (g_2^{-1} g_1)x = x \Leftrightarrow s = g_2^{-1} g_1 \in S$$

Thus $g_1 = (g_2 \cdot g_2^{-1}) \cdot g_1 = g_2 \cdot (g_2^{-1} g_1) = g_2 s \in g_2 S$. Because cosets partition, $g_1 S = g_2 S$ as required. ■

Corollary 2.2.8.1. For finite group G, if $G \curvearrowright X$ and $x \in X$, then $|G| = |Gx||\mathrm{Stab}_G(x)|$.

Proof. By Theorem 2.2.5 and Theorem 2.2.8,

$$|Gx| = |G/\mathrm{Stab}_G(x)| = |G|/|\mathrm{Stab}_G(x)|$$

■

Example 2.2.4. $D_{2n} \curvearrowright X_n$. Let $v \in X_n$ be a vertex. Then, $|D_{2n}v|$ = number of verticies $= n$, and $|\mathrm{Stab}_{D_{2n}}(v)| = 2$. So $|D_{2n}| = 2n$ by Corollarly 2.2.8.1 (recall Example 2.2.2).

Example 2.2.5. Let T a regular tetrahedron. Let $G \leqslant \mathrm{Isom}(T)$ be the group of rotational symmetries. Let $v \in T$ be a vertex. Then, size of the orbit $|Gv| = 4$, and $|\mathrm{Stab}_G(v)| = 3$. So by Corollarly 2.2.8.1, $|G| = 12$.

Example 2.2.6. Let G be a group of rotational isometries of a cube, C. Let $v \in C$ be a vertex. Then, $|Gv| = 8$ and $|\mathrm{Stab}_G(v)| = 3$. So $|G| = 24$.

Theorem 2.2.9. (*Cauchy's Theorem*) If $|G| < \infty$, p prime such that $p||G|$, then there is a $g \in G$ such that $o(g) = p$.

[6] Check if each operation is group operation or group action.

Proof. Consider the set X of p-tuples

$$X = \{(g_1, g_2, \ldots, g_p) \mid g_i \in G \ \forall i \text{ and } g_1 g_2 \cdots g_p = e\}$$

Define an action of $C_p \cong \langle t \rangle$ on X as

$$t^k(g_1, \ldots, g_p) = (g_{k+1}, \ldots, g_p, g_1, \ldots, g_k)$$

It is easy to see that e acts trivially and that $t^k(t^l(g_1, \ldots, g_p)) = t^{k+l}(g_1, \ldots, g_p)$. Most importantly, we need to check that $t^k(g_1, \ldots, g_p) \in X$. If we let $a = g_1 \cdots g_k$ and $b = g_{k+1} \cdots g_p$, we have $ab = e$ since $(g_1, \ldots, g_p) \in X$. Hence $ba = e$ and $t^k(g_1, \ldots, g_p) \in X$ as claimed. In conclusion, we have defined an action of C_p on X. Next, compute the size of X. Note that from $g_1 g_2 \cdots g_p = e$, we have

$$g_p = (g_1 g_2 \cdots g_{p-1})^{p-1}$$

Observe that we can arbitrarily choose $g_1, g_2, \ldots, g_{p-1}$, g_p is automatically decided. So

$$|X| = \underbrace{|G||G| \cdots |G|}_{p-1} 1 = |G|^{p-1}$$

Furthermore, by Proposition 2.2.3 (2), C_p action partitions X into orbits:

$$X = C_p x_1 \cup C_p x_2 \cup \cdots \cup C_p x_m$$

By orbit-stabiliser theorem (Corollarly 2.2.8.1), $|C_p x_j| \big| |C_p| = p$. So $|C_p x_j| = 1$ or $|C_p x_j| = p$ for each j. Let l be the number of size 1. Then

$$|X| = l + (m - l)p$$

But $|X| = |G|^{p-1} = l + (m-l)p$. Since $p \big| |G|$ by hypothesis, we have $p|l$. In particular, either $l = 0$ or $l \geqslant p$. Meanwhile, note that $|C_p X| = 1$ means that if we let $x = (g_1, \ldots, g_p)$, $t^k x = x$ for all k, implying $x = (g, \ldots, g)$ for some g. Because $\underbrace{e \cdots e}_{p} = e$, $(e, \ldots, e) \in X$ provides an orbit of size 1. Therefore there are at least $p \geqslant 2$ such orbits. So there is a $g \neq e$ such that $(g, g, \ldots, g) \in X$, i.e. $g^p = e$. This is our desired element of order p. ∎

2.2.3 Conjugations

Definition 2.2.5. Let G be a group, and $g \in G$. For any $h \in G$, the element $hgh^{-1} \in G$ is called the *conjugate* of g by h.

Example 2.2.7. If G is an abelian group, then, for any $g, h \in G$, $hgh^{-1} = ghh^{-1} = ge = g$; so the only conjugate of g is g itself.

Example 2.2.8. In D_{2n}, consider $g = s$, $h = r$. Recall the dihedral relation

$$r^{-1}s = sr \Rightarrow r^2(r^{-1}s)r^{-1} = r^2(sr)r^{-1} \Rightarrow rsr^{-1} = r^2 s$$

More generally,

$$\begin{aligned} r^k s r^{-k} &= (r^{k-1} r) s (r^{-1} r^{1-k}) \\ &= r^{k-1} (r s r^{-1}) r^{1-k} \\ &= r^{k-1} (r^2 s) r^{1-k} \\ &= (r^{k-1} r^2) s r^{1-k} \\ &= r^2 (r^{k-1} s r^{1-k}) = \cdots = r^{2k} s \end{aligned}$$

Note that these are all reflections. Consider $z_k = e^{2\pi i k/n} = r^k(z_0) \in X_n$. Then

$$(r^{2k}s)(z_k) = (r^k s r^{-k})(z_k) = ((r^k s r^{-k}) r^k)(z_0) = r^k s(z_0) = r^k(z_0) = z_k$$

So $r^{2k}s$ is the reflection in the line of symmetry through z_k.

Notice that G can acts on itself by conjugation. $G \curvearrowright G$, $g(\gamma) = g\gamma g^{-1}$. This is not the same with the regular action.

Definition 2.2.6. The orbit of γ under the conjugation action is called the *conjugacy class* of γ:

$$\mathrm{ccl}(\gamma) = \{g\gamma g^{-1} \mid g \in G\}$$

Definition 2.2.7. The stabiliser of γ inder the conjugation action is called the *centraliser* of γ:

$$C_G(\gamma) = \{g \in G \mid g\gamma g^{-1} = \gamma\}$$

Note that $g\gamma g^{-1} = \gamma \Leftrightarrow g\gamma = \gamma g$.

Definition 2.2.8. We define the *centre* of G as

$$Z(G) = \{h \in G \mid hg = gh \text{ for all } g \in G\} = \bigcap_{g \in G} C_G(g)$$

2.3 The Möbius Group

2.3.1 Möbius Transformation and Möbius Group

The Möbius group is almost a group of bijections of $\mathbb{C}$, but to make good sense of it, we need to add in one extra point.

Definition 2.3.1. We define the *Riemann Sphere* as $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$.

The reason we use the term 'sphere' to denote a complex plane is because 'stereographic projection' identifies the unit sphere with $\mathbb{C}$, except the north pole, which is what we call ∞.

Definition 2.3.2. Let $a, b, c, d \in \mathbb{C}$ such that $ad - bc \neq 0$. If $c \neq 0$, the corresponding *Möbius transformation* $\mu : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is defined by

$$z \mapsto \begin{cases} \frac{az+b}{cz+d} & z \in \mathbb{C} \backslash \{-d/c\} \\ \infty & z = -d/c \\ a/c & z = \infty \end{cases}$$

If $c = 0$, then μ is defined by

$$z \mapsto \begin{cases} \frac{az+b}{d} & z \in \mathbb{C} \\ \infty & z = \infty \end{cases}$$

Moreover, we define a set

$$\mathcal{M} = \{f : \mathbb{C}_\infty \to \mathbb{C}_\infty \mid f \text{ is a Möbius transformation}\}$$

Example 2.3.1. If

$$\mu_1(z) = \frac{a_1 z + b_1}{c_1 z + d_1}, \quad \mu_2(z) = \frac{a_2 z + b_2}{c_2 z + d_2}$$

then

$$\mu_1 \circ \mu_2(z) = \frac{(a_1 a_2 + b_1 b_2)z + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2)z + (c_1 b_2 + d_1 d_2)}$$

Cf. matrix multiplication.

Theorem 2.3.1. (*Möbius Group*) $(\mathcal{M}, \circ, \mathrm{id})$ is a group.

Proof. By Example 2.3.1 (nearly), a composition of Möbius transformation is again a Möbius transformation. Composition of function is associative, and $\mathrm{id} : z \mapsto z$ is clearly an identity. Finally, if

$$\mu(z) = \frac{az + b}{cz + d}$$

let

$$\nu(z) = \frac{dz - b}{-cz + a}$$

Then, by Example 2.3.1, $\mu \circ \nu(z) = z$ as required. ■

Before going further, we formally define a concept that we already know about.

Definition 2.3.3. If $f : X \to X$, any $x \in X$ is a *fixed point* if $f(x) = x$, and we may write $\mathrm{Fix}(f)$ to denote the set containing fixed points.

Lemma 2.3.2. (*Three-point Lemma for* $\mathcal{M}$) If $\mu \in \mathcal{M}$ has 3 different fixed points w_1, w_2, w_3 in $\mathbb{C}_\infty$, then $\mu = \mathrm{id}_{\mathbb{C}_\infty}$.

Proof. Let $\mu(z) = (az + b)/(cz + d)$. A fixed point w_i satisfies the equation

$$w_i = \frac{aw_i + b}{cw_i + d}$$

If $w_1 = \infty$, then $c = 0$. So w_2, w_3 satisfy $w_i = (aw_i + b)/d \Leftrightarrow (a - d)w_i + b = 0$. This is a linear equation in w_i with two roots, so $a = d$ and $b = 0$. Thus $\mu(z) = z$.

Now suppose $w_i \neq \infty$ for $i = 1, 2, 3$. Again,

$$w_i = \frac{aw_i + b}{cw_i + d} \Rightarrow cw_i^2 + dw_i = aw_i + b \Rightarrow cw_i^2 + (d - a)w_i - b = 0$$

For this quadratic equation to have three roots, $c = d - a = b = 0$. Hence $\mu(z) = z$ as required. ■

Example 2.3.2. Every $\mu \in \mathcal{M}$ has at least one fixed point in $\mathbb{C}_\infty$.

Example 2.3.3. If $\mu(z) = z + 1$, $\mathrm{Fix}(\mu) = \{\infty\}$. If $\mu(z) = 2z$, then $\mathrm{Fix}(\mu) = \{0, \infty\}$.

Lemma 2.3.3. (*Triple Transitivity*) For any triples of distinct points $z_1, z_2, z_3 \in \mathbb{C}_\infty$ and $w_1, w_2, w_3 \in \mathbb{C}_\infty$, there exists $\mu \in \mathcal{M}$ such that $\mu(z_i) = w_i$ for $i = 1, 2, 3$.

Proof. Let

$$\alpha(z) = \frac{z - z_1}{z - z_3}\frac{z_2 - z_3}{z_3 - z_1}, \quad \beta(z) = \frac{z - w_1}{z - w_3}\frac{w_2 - w_3}{w_2 - w_1}$$

Note that

$$\alpha : \begin{matrix} z_1 \mapsto 0 \\ z_2 \mapsto 1 \\ z_3 \mapsto \infty \end{matrix}, \qquad \beta : \begin{matrix} w_1 \mapsto 0 \\ w_2 \mapsto 1 \\ w_3 \mapsto \infty \end{matrix}$$

Now, since α and β are Möbius transformations, $\mu = \beta^{-1} \circ \alpha$ will work. ■

Remark 2.3.1. The 3-point lemma implies that the μ constructed is unique.[7] We say the action of $\mathcal{M}$ on $\mathbb{C}_\infty$ is "*sharply triply transitive*."

Definition 2.3.4. Let $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ be distinct. Because $\mathcal{M} \curvearrowright \mathbb{C}_\infty$ is sharply triply transitive, there is a unique $\alpha \in \mathcal{M}$ such that $\alpha(z_1) = 0, \alpha(z_2) = 1, \alpha(z_3) = \infty$, which is the same α from proof of Lemma 2.3.3. Then, the *cross-ratio* is defined as

$$[z_1, z_2, z_3, z_4] = \alpha(z_4) = \frac{(z_4 - z_1)(z_2 - z_3)}{(z_4 - z_3)(z_2 - z_1)}$$

Proposition 2.3.4. $\mathcal{M}$ is generated by the set of elements of the following three forms:

(1) $\alpha_a : z \mapsto az$, $a \neq 0$.

(2) $\beta_b : z \mapsto z + b$, $b \in \mathbb{C}$.

(3) $\gamma : z \mapsto 1/z$.

Proof. Let $\mu \in \mathcal{M}$ be arbitrary. Let $z_1 = \mu(0), z_2 = \mu(1), z_3 = \mu(\infty)$. First, we construct μ_1 such that $\mu_1(z_3) = \infty$: either $z_3 = \infty$ and $\mu_1 = \mathrm{id}$ or

$$\mu_1(z) = \frac{1}{z + b} = \gamma \circ \beta_b(z)$$

where $b = -z_3$. Let's write $z_1' = \mu_1(z_1)$ and $z_2' = \mu_1(z_2)$. Now let $b' = -z_1'$ and $\mu_2 = \beta_{b'}$. Then $\mu_2(\infty) = \infty$ and $\mu_2(z_1') = 0$. So by construction, $\mu_2 \circ \mu_1(z_3) = \infty$, $\mu_2 \circ \mu_1(z_1) = 0$, and $z_2'' = \mu_2 \circ \mu_1(z_2) \neq 0, \infty$. Finally, let $a = 1/z_2''$ and $\mu_3 = \alpha_a$ to find

$$\mu_3 \circ \mu_2 \circ \mu_1(z_1) = 0$$

$$\mu_3 \circ \mu_2 \circ \mu_1(z_2) = 1$$

$$\mu_3 \circ \mu_2 \circ \mu_1(z_3) = \infty$$

So $(\mu_3\mu_2 \circ \mu_1)^{-1} = \mu_1^{-1} \circ \mu_2^{-1} \circ \mu_3^{-1}$ sends $0 \mapsto z_1$, $1 \mapsto z_2$, and $\infty \mapsto z_3$. Thus μ and $\mu_1^{-1} \circ \mu_2^{-1} \circ \mu_3^{-1}$ agree on $0, 1, \infty$, and hence everywhere, by the 3-point lemma (Lemma 2.3.2). ■

[7] Suppose there exists another transformation.

2.3.2 Circles

Definition 2.3.5. A *circle* in $\mathbb{C}_\infty$ is:

(1) Either a Euclidean circle in $\mathbb{C}$;

(2) or $l \cup \{\infty\}$ where $l \subseteq \mathbb{C}$ is a Euclidean straight line.

Recall that Euclidean circles are defined by $|z-c| = r$ where $r > 0$, $c \in \mathbb{C}$, while Euclidean straight line can be written as $|z-a| = |z-b|$ ($a \neq b$, $a, b \in \mathbb{C}$).

Theorem 2.3.5. If $C \subseteq \mathbb{C}_\infty$ is a circle and $\mu \in \mathcal{M}$, then $\mu(C)$ is also a circle.

Proof. From Proposition 2.3.4, it is enough to check that $\alpha_a, \beta_b, \gamma$ send C to a circle. Since it is clear for α_a and β_b, we will only prove for γ. If C is an Euclidean circle with equation $|z-c| = r$, then $\gamma(c)$ has equation

$$\left|\frac{1}{z} - c\right| = r \Leftrightarrow \left|\frac{1}{z} - c\right|^2 = r^2 \Leftrightarrow \left(\frac{1}{z} - c\right)\left(\frac{1}{\bar{z}} - \bar{c}\right) = r^2$$

and

$$\frac{1}{|z|^2} - \frac{c}{\bar{z}} - \frac{\bar{c}}{z} + |c|^2 - r^2 = 0 \Leftrightarrow (|c|^2 - r^2)|z|^2 - cz - \bar{c}\bar{z} + 1 = 0$$

If $|c|^2 - r^2 = 0$, this becomes

$$cz + \bar{c}\bar{z} = 1 \Leftrightarrow \frac{z}{\bar{c}} + \frac{\bar{z}}{c} = \frac{1}{|c|^2} \Leftrightarrow |z|^2 = |z|^2 - \frac{z}{\bar{c}} - \frac{\bar{z}}{c} + \frac{1}{|c|^2} = \left|z - \frac{1}{c}\right|^2$$

which is a straight line. If $|c|^2 - r^2 \neq 0$, we divide by it and obtain

$$\begin{aligned} &|z|^2 - \frac{c}{(|c|^2 - r^2)}z - \frac{\bar{c}}{(|c|^2 - r^2)}\bar{z} + \frac{1}{(|c|^2 - r^2)} = 0 \\ \Leftrightarrow &\left|z - \frac{\bar{c}}{(|c|^2 - r^2)}\right|^2 = \frac{|c|^2}{(|c|^2 - r^2)^2} - \frac{1}{(|c|^2 - r^2)} = \frac{r^2}{(|c|^2 - r^2)^2} \end{aligned}$$

which is a circle.

The case when C is an Euclidean line is similar, and left as an exercise. ∎

Corollary 2.3.5.1. Four points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$ are on a circle if and only if

$$[z_1, z_2, z_3, z_4] \in \mathbb{R} \cup \{\infty\}$$

Proof. Recall that $[z_1, z_2, z_3, z_4] = \alpha(z_4)$ where $\alpha(z_1) = 0, \alpha(z_2) = 1, \alpha(z_3) = \infty$. Let $C \subseteq \mathbb{C}_\infty$ a circle. If $z_1, z_2, z_3, z_4 \in C$, then $0, 1, \infty, \alpha(z_4) \in \alpha(C)$ a circle. Since the only line through 0 and 1 is $\mathbb{R}$, we see that $\alpha(z_4) \in \mathbb{R} \cup \{\infty\}$.

Conversely, if $0, 1, \infty, \alpha(z_4) \in \mathbb{R} \cup \{\infty\}$, then $z_1, z_2, z_3, z_4 \in \alpha^{-1}(\mathbb{R} \cup \{\infty\})$, which is also a circle. ∎

2.4 Small Finite Groups

We will try to systematically list small groups, according to their order. First, following three are clear by Theorem 2.2.9 (Cauchy's theorem).

- $|G| = 1$, $G \cong 1$ (trivial group).

- $|G| = 2$, $G \cong C_2$.
- $|G| = 3$, $G \cong C_3$.

If $|G| = 4$, we have C_4. To check if there is another example, we introduce the following.

Definition 2.4.1. If G, H are group, the *direct product* of G, H is

$$G \times H = \{(g,h) \mid g \in g, h \in H\}$$

with operation

$$(g_1,h_1) \cdot (g_2,h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$$

Note that $e = (e_G, e_H)$ is an identity and $(g,h)^{-1} = (g^{-1}, h^{-1})$. Note also that $|G \times H| = |G||H|$.

Example 2.4.1. The group $K_4 = V_4 = C_2 \times C_2$ is often called the *Klein 4-group*. Note that, for $(a,b) \in C_2 \times C_2$,

$$(a,b)^2 = (a^2, b^2) = (e,e) = e$$

So every element is of order 1 or 2. In particular, no element has order 4. So $C_2 \times C_2 \ncong C_4$.

Theorem 2.4.1. (*Direct Product Theorem*) If $H_1, H_2 \leqslant G$ and

(1) $H_1 \cap H_2 = \{e\}$,

(2) $h_1 h_2 = h_2 h_1$ whenever $h_1 \in H_1$ and $h_2 \in H_2$,

(3) for each $g \in G$, there are $h_1 \in H_1, h_2 \in H_2$ such that $g = h_1 h_2$,

then, $G \cong H_1 \times H_2$.

Proof. Define $\Phi : H_1 \times H_2 \to G$, $(h_1, h_2) \mapsto h_1 h_2$. We need to show that Φ is an isomorphism. To show that Φ is a homomorphism,

$$\Phi(h_1,h_2)\Phi(h_1',h_2') = h_1 h_2 h_1' h_2' = h_1 h_1' h_2 h_2' = \Phi(h_1 h_1', h_2 h_2') = \Phi((h_1,h_2)(h_1',h_2'))$$

by part (2) of hypotheses. Also, surjectivity is immediate from hypotheses (3). To prove injectivity, suppose $h_1 h_2 = \Phi(h_1,h_2) = e$. But this implies

$$H_1 \ni h_1 = h_2^{-1} \in H_2 \Rightarrow h_1 = h_2^{-1} \in H_1 \cap H_2 = \{e\} \Rightarrow (h_1,h_2) = (e,e) = e$$

by part (1). So $\ker \Phi = e$ as required. ∎

Lemma 2.4.2. (*Groups of order four*) If $|G| = 4$, then $G \cong C_4$ or $G \cong C_2 \times C_2$.

Proof. By Lagrange's theorem, every non-trivial element has order of 2 or 4. If there is an element g of order 4, then $G = \langle g \rangle \cong C_4$. Otherwise, let $a \neq b$ be elments of order 2. Then, $\langle a \rangle \cap \langle b \rangle = \{e\}$, $G = \langle a \rangle \langle b \rangle$[8], and $ab = ba$ (from Example Sheet 1). Hence by the direct product theorem, $G \cong \langle a \rangle \times \langle b \rangle \cong C_2 \times C_2$. ∎

Another application of the direct product theorem is to product of cyclic groups.

Theorem 2.4.3. (*Chinese Remainder Theorem*) If $\gcd(m,n) = 1$, then $C_m \times C_n \cong C_{mn}$.

[8]This notation is same with (3) from Theorem 2.4.1

Proof. Let $C_{mn} = \langle g \rangle$ and set $H_1 = \langle g^n \rangle \cong C_m$, $H_2 = \langle g^m \rangle \cong C_n$. We will check the hypotheses of the direct product theorem.

(1) Note that $g^k \in H_1 \Leftrightarrow n|k$ and $g^k \in H_2 \Leftrightarrow m|k$; so

$$g^k \in H_1 \cap H_2 \Leftrightarrow m|k \text{ and } n|k \Leftrightarrow mn = \operatorname{lcm}(m,n)|k \Leftrightarrow g^k = e \text{ in } C_{mn}$$

Hence $H_1 \cap H_2 = \{e\}$ as required.

(2) Obvious because C_{mn} is abelian.

(3) Let $g^k \in C_{mn}$. Bézout's theorem (Corollarly 1.3.5.1) implies that there are $p, q \in \mathbb{Z}$ such that $k = pm + qn$. Hence $g^k = (g^m)^p (g^n)^q$ as required.

■

We continue our classification of groups of small order. If $|G| = 5$, $G \cong C_5$ since 5 is prime. If $|G| = 6$, we classify as follows.

Lemma 2.4.4. (*Groups of order six*) If $|G| = 6$, then $G \cong C_6$ or $G \cong D_6$.

Proof. By Cauchy's theorem (Theorem 2.2.9), there are elements $r, s \in G$ such that $o(r) = 3$ and $o(s) = 2$. Then $|\langle r \rangle| = 3 = 6/2$ so $|G : \langle r \rangle| = 2$ by the Lagrange's theorem (Theorem 2.2.5); and $s \notin \langle r \rangle$. Therefore $s\langle r \rangle$ and $\langle r \rangle$ partition G, and we may write

$$s\langle r \rangle = G \backslash \langle r \rangle = \langle r \rangle s$$

Hence $sr = r^i s$ for some $i = 0, 1, 2$ and we can analyse each cases:

- $i = 0$; $sr = r \Rightarrow r = e$, leading to contradiction.
- $i = 1$; $sr = rs$ so $\langle r \rangle$ and $\langle s \rangle$ commute, and by Theorem 2.4.1 and Theorem 2.4.3,
$$G \cong \langle r \rangle \times \langle s \rangle \cong C_3 \times C_2 \cong C_6$$
- $i = 2$; we have $sr = r^2 s = r^{-1} s$, which is the dihedral relation. Now we can list the elements
$$e, r, r^2, s, rs, r^2 s$$
and dihedral relation implies that $r^i r^j = r^{i+j}$, $r^i s r^j = r^{i-j} s$ etc. hold, so $G \cong D_6$.

■

Remark 2.4.1. S_3 is non-abelian group of order 6, so $S_3 \cong D_6$.

Continuing with our journey, $C \cong C_7$ if $|G| = 7$ since 7 is prime. If $|G| = 8$, we may think of groups $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8$, and the fact that they are all different. However, this is not all we have.

Example 2.4.2. (*The Quaternion Group*) Let

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with multiplication such that

- $i^2 = k^2 = j^2 = -1$,
- $(-1)i = -i, (-1)j = -j, (-1)k = -k$,

- $ij = k, jk = i, ki = j$,
- $ji = -k, kj = -i, ik = -j$,
- $(-1)^2 = 1$.

Note that Q_8 is non-abelian, so $Q_8 \ncong C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$. Also, Q_8 has only one element of order 2, so $Q_8 \ncong D_8$.

Lemma 2.4.5. (*Groups of order eight*) If $|G| = 8$, then $G \cong C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8$, or Q_8.

Proof. By Lagrange's theorem, every element is of order 1,2,4, or 8. First,

- if there is an element of order 8, then $G \cong C_8$;
- if every element is of order 2, then G is abelian by the Example Sheet, and we may choose $a, b \in G\backslash\{e\}$ such that $a \neq b$. Then by the direct product theorem $\langle a, b\rangle = \langle a\rangle \times \langle b\rangle$. Now let $c \notin \langle a, b\rangle$[9], and again by the direct product theorem, $G \cong \langle a, b, c\rangle \cong \langle a\rangle \times \langle b\rangle \times \langle c\rangle \cong C_2 \times C_2 \times C_2$.

So for the remaining cases, we assume there is element $a \in G$ such that $o(a) = 4$. Let $b \in G\backslash\langle a\rangle$. Because $|G : \langle a\rangle| = 2$, $b\langle a\rangle$ and $\langle a\rangle$ partition G and $b\langle a\rangle = G\backslash\langle a\rangle = \langle a\rangle b$. This means that $ba = a^i b$ for some $i = 0, 1, 2, 3$. If $i = 0$, $ba = b \Rightarrow a = e$, which is a contradiction. If $i = 2$, $ba = a^2 b \Rightarrow bab^{-1} = a^2$. But $o(a) = 4$ and $o(a^2) = 2$, which is a contradiction by Example Sheet 2, Question 1. Let's take a look at remaining two cases:

- $i = 1 \Rightarrow ba = ab \Rightarrow ba^j = a^j b\ \forall j \Rightarrow G$ abelian;
- $i = 3 \Rightarrow ba = a^3 b = a^{-1} b$.

Next, we think about b^2. If $b^2 = ba^j$ for some j, then $b = a^j \in \langle a\rangle$, leading to contradiction. So $b^2 \in \langle a\rangle \Rightarrow b^2 = a^j$ for some $j = 0, 1, 2, 3$.

- $j = 0$, $b^2 = e$;
- $j = 1$, $b^2 = a \Rightarrow o(b) = 8 \Rightarrow G \cong C_8$;
- $j = 2$, $b^2 = a^2$;
- $j = 3$, $b^2 = a^3 \Rightarrow o(b) = 8 \Rightarrow G \cong C_8$.

Thus we have four combination of cases left to analyse.

- $i = 1, j = 0$; G is abelian and $\langle a\rangle \cap \langle b\rangle = \{e\} \Rightarrow G \cong \langle a\rangle \times \langle b\rangle \cong C_4 \times C_2$ by direct product theorem.
- $i = 1, j = 2$; G is abelian and $b^2 = a^2 \Rightarrow a^2 b^{-2} = (ab^{-1})^2 = e$. So $o(ab^{-1}) = 2$, $\langle a\rangle \cap \langle ab^{-1}\rangle = \{e\}$, giving $G \cong \langle a\rangle \times \langle ab^{-1}\rangle \cong C_4 \times C_2$ by the direct product theorem.
- $i = 3, j = 0$; We have $o(a) = 4$, $o(b) = 2$, and $ba = a^{-1} b$. Setting $r = a$ and $s = b$, we have $sr = r^{-1} s$ dihedral relation. We can list all the elements:

  $$e, r, r^2, r^3, s, rs, r^2 s, r^3 s$$

  and dihedral relation implies that $r^i s r^j = r^{i-j} s$ etc. So $G \cong D_8$.

[9] Group generated by a and b.

- $i = 3, j = 2$; $o(a) = 4$, $b^2 = a^2$, and $ba = a^{-1}b$. If we set $i = a$, $j = b$, $k = ab$, and $-1 = a^2 = b^2$, we may think of the elements of the group

$$e, a, a^2, a^3, b, ab, a^2, a^3b$$

as

$$1, i, -1, -i, j, k, -j, -k$$

and check that these all multiply as needed. Thus $G \cong Q_8$.

■

2.5 Quotients

2.5.1 Normal Subgroups

Let $\phi : G \to H$ be a homomorphism. We saw earlier that

$$\ker \phi \leqslant G$$

In fact, more is true.

Definition 2.5.1. $H \leqslant G$ is *normal* if $ghg^{-1} \in H$ for every $h \in H, g \in G$. We write $H \lhd G$ to denote normal subgroup.

Example 2.5.1.

(1) $1 \lhd G$ and $G \lhd G$ for all groups G.

(2) If G is abelian, then any $H \leqslant G$ is normal.

(3) $\langle r \rangle \leqslant D_6$ since $sr = r^2 s \Rightarrow srs^{-1} = r^2$, $sr^2 = rs \Rightarrow sr^2 s^{-1} = r$. So $\langle r \rangle \lhd D_6$. But $\langle s \rangle$ is not normal, because $rsr^{-1} = sr^{-2} = sr \notin \langle s \rangle$.

(4) Suppose $\phi : G \to G'$ is a homomorphism. If $h \in \ker \phi$ and $g \in G$, then $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e$. So $ghg^{-1} \in \ker \phi$. Therefore, $\ker \phi \lhd G$.

Lemma 2.5.1. If $H \leqslant G$, then $H \lhd G$ if and only if $gH = Hg$ for all $g \in G$,

Proof. Suppose $H \lhd G$. For any $h \in H$, $h' = ghg^{-1} \in H$ for all g. Hence,

$$gh = (ghg^{-1})g = h'g \in Hg$$

So $gH \subseteq Hg$. Likewise, $g^{-1}H \subseteq Hg^{-1} \Rightarrow Hg = (g^{-1}H)^{-1} \subseteq (Hg^{-1})^{-1} = gH$.[10] Hence $gH = Hg$.

Conversely, suppose $gH = Hg$. This means that for any $h \in H$, $gh \in Hg$. So $gh = h'g$ for some $h' \in H$. Therefore, $ghg^{-1} = h' \in H$ as required to show that $H \lhd G$. ■

Theorem 2.5.2. (*Quotient Group*) If $H \lhd G$, then the set of left cosets G/H is a group, with operation

$$(g_1H)(g_2H) = (g_1g_2)H$$

[10] See proof of Lemma 2.2.6.

Proof. We need to check that the operation is well defined. Suppose $g_1H = g_1'H$ and $g_2H = g_2'H \Leftrightarrow Hg_2 = Hg_2'$ (because $H \lhd G$). That is, there are $h_1, h_2 \in H$ such that $g_1 = g_1'h_1$ and $g_2 = h_2g_2'$. Therefore, $g_1g_2 = g_1'(h_1h_2)g_2' = g_1'g_2'h_3$ for some $h_3 \in H$ (note $Hg_2' = g_2'H$). So $g_1g_2 \in g_1'g_2'H$, and because cosets partition, $g_1g_2H = g_1'g_2'H$ as required.

Associativity follows from the fact that G is associative, and $H \in G/H$ provides the identity. Meanwhile, since

$$(gH)(g^{-1}H) = gg^{-1}H = eH = H$$

we have inverse $(g^{-1}H) = (gH)^{-1}$. ∎

Definition 2.5.2. If $H \lhd G$, then G/H is called the *quotient* of G by H.

Example 2.5.2.

(1) $G/1 \cong G$, $G/G \cong 1$.

(2) Since $\mathbb{Z}$ is abelian, $n\mathbb{Z} \lhd \mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z}$ is generated by $1 + n\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z} \cong C_n$.[11]

(3) If $H \leqslant G$ and $|G : H| = 2$, then for any $g \notin H$, $gH = G/H = Hg$, and the remaining coset is H. Hence $H \lhd G$ and therefore G/H is a group of order 2, giving $G/H \cong C_2$.

(4) For instance, $C_n = \langle r \rangle \lhd D_{2n}$ and $D_{2n}/C_n \cong C_2$.

(5) N.b. quotients are not subgroups.

(6) Also note that $C_4/C_2 \cong C_2$ and $K_4/C_2 \cong C_2$ but $K_4 \ncong C_4$.

Theorem 2.5.3. (*Isomorphism Theorem*) If $\phi : G \to H$ is a homomorphism, then

$$G/\ker\phi \cong \operatorname{im}\phi$$

Proof. Since $\ker\phi \lhd G$, the quotient $G/\ker\phi$ is indeed a group. Define $\bar{\phi} : G/\ker\phi \to \operatorname{im}\phi$, $g\ker\phi \mapsto \phi(g)$. We need to show that $\bar{\phi}$ is a well-defined isomorphism. Suppose $g_1\ker\phi = g_2\ker\phi$. This means that $g_1 = g_2k$ for some $k \in \ker\phi$. Then

$$\bar{\phi}(g_1\ker\phi) = \phi(g_1) = \phi(g_2k) = \phi(g_2)\phi(k) = \phi(g_2)e = \phi(g_2) = \bar{\phi}(g_2\ker\phi)$$

Now, to prove that it is a homomorphism, let $g_1, g_2 \in G$. Then,

$$\begin{aligned}\bar{\phi}(g_1\ker\phi)\bar{\phi}(g_2\ker\phi) = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \bar{\phi}((g_1g_2)\ker\phi)\\ = \bar{\phi}((g_1\ker\phi)(g_2\ker\phi))\end{aligned}$$

by definition of group multiplication.

For injectivity, suppose $\bar{\phi}(g_1\ker\phi) = \bar{\phi}(g_2\ker\phi)$. Then $\phi(g_1) = \phi(g_2)$. This implies $g_2^{-1}g_1 \in \ker\phi$, and $g_1\ker\phi = g_2\ker\phi$ as required.

Clearly, $\bar{\phi}$ is surjective since an element of $\operatorname{im}\phi$ is of the form $\phi(g) = \bar{\phi}(g\ker\phi)$, and $\operatorname{im}\phi = \operatorname{im}\bar{\phi}$. ∎

Example 2.5.3.

[11] See Proposition 2.1.5.

(1) Because $\phi : \mathbb{Z} \to C_n$, $k \mapsto e^{2\pi ik/n}$ is a homomorphism with $\operatorname{im}\phi = C_n$, $\ker\phi = n\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \cong C_n$.

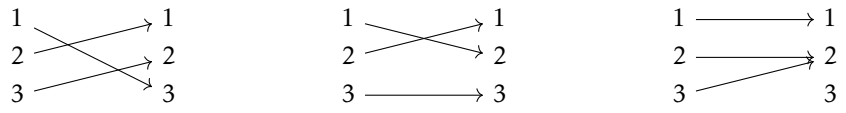
(2) Similarly, $\phi : \mathbb{R} \to C_\times = \mathbb{C}\backslash\{0\}$, $t \mapsto e^{2\pi it}$ is a homomorphism with $\operatorname{im}\phi = \{z \in \mathbb{C} : |z| = 1\} = S^1$, i.e. a one dimensional sphere, and $\ker\phi = \mathbb{Z}$. Hence $\mathbb{R}/\mathbb{Z} \cong S^1$.

Definition 2.5.3. G is *simple* if the only normal subgroups are 1 and G. Thus, every homomorphism $G \to H$ is either trivial or injective.

2.6 Permutations

Recall that a permutation of a set X is a bijection $X \to X$ and that $\mathrm{Sym}(X)$ is the group of all such permutations. Also, if $X = \{1, 2, \ldots, n\}$, $\mathrm{Sym}(X) = S_n$.

Example 2.6.1. Let $X = \{1, 2, 3\}$, S_3.



σ τ Not a permutation.

Notice that σ and τ are permutations. The obvious way to compute the product is to list:

$$1 \mapsto 3 \mapsto 3$$

$$2 \mapsto 1 \mapsto 2$$

$$\underbrace{3 \mapsto 2 \mapsto 1}_{\tau\circ\sigma}$$

Definition 2.6.1. Any list of k different elements $a_1, a_2, \ldots, a_k \in \{1, \ldots, n\}$ determines a *k-cycle* $\sigma = (a_1 a_2 \cdots a_k)$ as follows.

$$\sigma(b) = \begin{cases} a_{j+1} & b = a_j, j < k \\ a_1 & b = a_k \\ b & \text{otherwise} \end{cases}$$

With cycles, we can easily calculate the product of permutations.

Example 2.6.2. Consider $\sigma = (132) = (321)$, $\tau = (12)$. Then

$$\tau\sigma = (12)(132) = (13)(2) = (13)$$

Example 2.6.3. $(1432)(243) = (1423)$.

Remark 2.6.1. Note that $(a_1 a_2 \cdots a_k) = (a_2 a_3 \cdots a_k a_1)$. For example,

$$(123) = (231) = (312)$$

Definition 2.6.2. Cycles $(a_1 \cdots a_k)$ and $(b_1 \cdots b_k)$ are *disjoint* if $a_i \neq b_j$ for all i, j.

For example, $(123), (45) \in S_5$ are disjoint. N.b. disjoint cycles commute.

Theorem 2.6.1. Every $\sigma \in S_n$ can be written as a product of disjoint cycles. This expression is unique up to:

(1) Shifting the element of each cycle.

(2) Permuting the cycles.

Proof. The action of $\langle\sigma\rangle$ on $X = \{1,\dots,n\}$ partition X into orbits:

$$\langle\sigma\rangle i_1 \cup \langle\sigma\rangle i_2 \cup \cdots \cup \langle\sigma\rangle i_k$$

Setting $n_j = |\langle\sigma\rangle i_j|$ for $1 \leqslant j \leqslant k$, we see that

$$\sigma = (i_1\ \sigma(i_1)\cdots\sigma^{n_1-1}(i_1))(i_2\cdots\sigma^{n_2-1}(i_2))\cdots(i_k\cdots\sigma^{n_k-1}(i_k))$$

which proves existence. (These are all disjoint because orbits partition.) For uniqueness, note that the only choices we made were (1) orbit representative i_j, and (2) the order in which we wrote down the orbits. But changing (1) shifts the cycle, and changing (2) permutes the cycles. ■

Example 2.6.4. $(12)(34)(56)(123456) = (1)(246)(3)(5) = (246)$

Definition 2.6.3. If $\sigma = (a_1^1\cdots a_{k_1}^1)\cdots(a_1^l\cdots a_{k_l}^l)$ are disjoint cycles, then σ is called a $(k_1,\dots,k_l) - cycle$. The set of numbers $\{k_1,\dots,k_l\}$ is called the *cycle type* of σ.

For example, $(12)(34)(56)$ is a $(2,2,2)$-cycle. We usually omit singletons, so, e.g. $(12)(345)(6)$ is a $(2,3)$-cycle.

Remark 2.6.2. If $\sigma = (a_1\cdots a_k)$ is a k-cycle, then $o(\sigma) = k$. More generally, if σ is a $(k_1,\dots,k_l)$-cycle, then $o(\sigma) = \operatorname{lcm}\{k_1,\dots,k_l\}$.

Definition 2.6.4. A 2-cycle is called a *transposition*.

Theorem 2.6.2. The set of transposition in S_n generates S_n.

Proof. Note there is a copy of S_{n-1} sitting inside S_n as a subgroup: $S_{n-1} \cong \operatorname{Stab}_{S_n}(n)$. The proof is by induction on n.

For base case $n = 2$, $S_2 = \{e,(1,2)\} \cong C_2$ and the result is obvious. Now suppose S_{n-1} is generated by transposition, and let $\sigma \in S_n$. If $\sigma(n) = n$, then $\sigma \in \operatorname{Stab}_{S_n}(n) \cong S_{n-1}$ so σ is a product of transpositions by the inductive hypothesis. If not, let $\tau = (n\ \sigma(n))$. Then

$$\tau\sigma(n) = \tau(\sigma(n)) = n$$

So, as above,

$$\tau\sigma \in \operatorname{Stab}_{S_n}(n) \cong S_{n-1}$$

and $\tau\sigma$ is a product of transpositions. Thus σ is also a product of transpositions. ■

In fact, we can do slightly better. A transposition of the form $(i\ i+1)$ is for $1 \leqslant i < n$ is called *adjacent*. Then, we have the following.

Lemma 2.6.3. Any transposition is a product of odd numbers of adjacent transpositions.

Proof. Let (ij) be a transposition with $j > i$. We proceed by induction on $j - i$.

In the base case, $j = i + 1 \Rightarrow (ij) = (i\ i+1)$ is adjacent. Otherwise, if $j > i + 1$, then

$$(j-1\ j)(i\ j-1)(j-1\ j) = (ij)$$

and the result follows by induction. ■

Lemma 2.6.4. If $\tau_1, \ldots, \tau_k$ are all transpositions, and

$$\sigma = \tau_1 \cdots \tau_k = e$$

then k is even.

Proof. First, note that we may assume that all the τ_i are adjacent.[12] Also, we call a pair $\{i, j\} \subseteq \{1, \ldots, n\}$ an *inversion* if $i < j$ but $\sigma(i) > \sigma(j)$. The lemma follows from the claim:

$$k \equiv \#\text{ inversions of } \sigma \mod 2$$

We prove the claim by induction on k. Base case is when $k = 0$, numbers of inversion 0. Now suppose

$$\sigma = \tau_1 \tau_2 \cdots \tau_k = \tau \sigma'$$

with $\tau_1 = \tau = (l\, l+1)$, $\sigma' = \tau_2 \cdots \tau_k$. How many pairs $\{i, j\}$ $(i < j)$ are inversions of σ' but not σ, or vice versa? There are 10 cases to analyse, depending on where l and $l+1$ are, relative to $\sigma'(i)$, $\sigma'(j)$.

σ'	σ	order
✗	✗	$l < l+1 \leqslant \sigma'(i) < \sigma'(j)$
✓	✓	$l < l+1 \leqslant \sigma'(j) < \sigma'(i)$
✗	✗	$\sigma'(i) < \sigma'(j) \leqslant l < l+1$
✓	✓	$\sigma'(j) < \sigma'(i) \leqslant l < l+1$
✗	✗	$\sigma'(i) \leqslant l < l+1 < \sigma'(j)$
✓	✓	$\sigma'(j) \leqslant l < l+1 \leqslant \sigma'(i)$
✗	✗	$\sigma'(i) < l < l+1 \leqslant \sigma'(j)$
✓	✓	$\sigma'(j) < l < l+1 \leqslant \sigma'(i)$
✗	✓	$\sigma'(i) = l < l+1 = \sigma'(j)$
✓	✗	$\sigma'(j) = l < l+1 = \sigma'(i)$

Since the final two cases correspond to the unique pair $\{(\sigma')^{-1}(l), (\sigma')^{-1}(l+1)\}$,

$$\#\text{ inversions of } \sigma = (\#\text{ inversions of } \sigma') \pm 1$$

proving the claim. Now, if $\sigma = \tau_1 \cdots \tau_k = 2$, then σ has 0 inversions, so by the claim, $k \equiv 0 \mod 2$, i.e. k is even. ∎

Theorem 2.6.5. (*Sign Homomorphism*) The map

$$\operatorname{sgn} : S_n \to C_2 = \{\pm 1\}, \quad \tau_1 \cdots \tau_k \mapsto (-1)^k$$

is a well defined homomorphism.

Proof. To see that sgn is well defined, suppose τ_i, τ'_j are transpositions such that $\tau_1 \cdots \tau_k = \tau'_1 \cdots \tau'_l$. Then,

$$\tau_k \tau_{k-1} \cdots \tau_1 \tau'_1 \cdots \tau'_l = e$$

[12] Parity is conserved.

But by Lemma 2.6.4 above, $k+l$ is a multiple of 2. Hence, $k \equiv l \mod 2 \Rightarrow (-1)^k = (-1)^l$.

Now, to see that sgn is a homomorphism, note that

$$\begin{aligned}\operatorname{sgn}(\tau_1 \cdots \tau_k \tau_1' \cdots \tau_l') &= (-1)^{k+l} = (-1)^k(-l)^l \\ &= \operatorname{sgn}(\tau_1 \cdots \tau_k)\operatorname{sgn}(\tau_1' \cdots \tau_l')\end{aligned}$$

■

Definition 2.6.5. If $\operatorname{sgn}(\sigma) = 1$, then σ is *even*; otherwise, σ is called *odd*. The subgroup containing even permutations, i.e.

$$A_n = \ker(\operatorname{sgn}) \lhd S_n$$

is called the *alternating group* on n elements.

Example 2.6.5. $S_3 = \{e, (123), (321), (12), (23), (31)\}$. We have $(123) = (12)(23)$ and $(321) = (23)(12)$. Therefore,

$$A_3 = \{e, (123)(321)\} \cong C_3$$

Remark 2.6.3. The cycle type makes it easy to determine the sign of a permutation. Indeed,

$$(a_1 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$$

so $(a_1 \cdots a_k)$ is even if and only if k is odd. More generally, a $(k_1, \ldots, k_l)$-cycle is even if and only if $\#\{k_i \text{ even}\}$ is even.

Example 2.6.6. $(12)(34)$ is even but $(12)(34)(56)$ is odd.

Let's apply the facts to study conjugation in S_n and A_n. We will start with S_n.

Theorem 2.6.6. Two permutations $\sigma_1, \sigma_2 \in S_n$ are conjugate if and only if their cycle types are the same.

Proof. Suppose

$$\sigma_1 = (a_1^1 \cdots a_{l_1}^1) \cdots (a_1^k \cdots a_{l_k}^k)$$

is a product of disjoint cycles, so

$$\sigma_1(a_j^i) = a^i_{j+_{l_i} 1}$$

Since the cycle types are same, σ_2 will take the form $\sigma_2 = (b_1^1 \cdots b_{l_1}^1) \cdots (b_1^k \cdots b_{l_k}^k)$. Now, note that $\tau(a_j^i) = b_j^i$ defines a permutation of $\{1, \ldots, n\}$. Let's compute

$$\tau\sigma_1\tau^{-1}(b_j^i) = \tau\sigma_1(a_j^i) = \tau(a^i_{j+_{l_i}+1}) = b^i_{j+_{l_i}1}$$

Hence $\tau\sigma_1\tau^{-1} = \sigma_2$. So σ_1 and σ_2 are indeed conjugate.

Conversely, suppose $\sigma_2 = \tau\sigma\tau^{-1}$. The above argument says that if

$$\sigma_1 = (a_1^1 \cdots a_{l_1}^1) \cdots (a_1^k \cdots a_{l_k}^k)$$

then

$$\sigma_2 = (b_1^1 \cdots b_{l_1}^1) \cdots (b_1^k \cdots b_{l_k}^k)$$

where $b_j^i = \tau(a_j^i)$. Therefore, σ_1 and σ_2 have the same cycle type. ■

Example 2.6.7. $(12)(123)(12) = (213)$; and, more generally,

$$\sigma(12\cdots l)\sigma^{-1} = (\sigma(1)\,\sigma(2)\cdots\sigma(l))$$

We can use Theorem 2.6.6 to count conjugacy classes in S_n.

Example 2.6.8. $|\mathrm{ccl}_{S_3}(12)| = \binom{3}{2} = 3$, $|\mathrm{ccl}_{S_3}(123)| = 2$, and $|\mathrm{ccl}_{S_3}((12)(34))| = 3$.

Recall that orbit-stabiliser (Corollarly 2.2.8.1) tells us that

$$|C_{S_n}(\sigma)| = |S_n|/|\mathrm{ccl}_{S_n}(\sigma)| = n!/|\mathrm{ccl}_{S_n}(\sigma)|$$

Hence we can also compute the sizes of centralisers.

Example 2.6.9. Consider S_4.

$$|C_{S_4}((12)(34))| = \frac{|S_4|}{|\mathrm{ccl}_{S_4}((12)(34))|} = \frac{4!}{3} = 8$$

Indeed, we can list

$$C_{S_4}((12)(34)) = \{e, (12), (34), (12)(34), (13)(24), (14)(23), (1423), (1324)\}$$

Example 2.6.10. We can list all the conjugacy classes in S_4 as follows.

Typical element γ	$\lvert\mathrm{ccl}_{S_4}(\gamma)\rvert$	$\lvert C_{S_4}(\gamma)\rvert$
e	1	24
(12)	6	4
$(12)(34)$	3	8
(123)	8	3
(1234)	6	4

and check $|S_4| = 24$ if wanted.

Now, let's turn to conjugacy classes in A_n. Be careful, that conjugacy classes in S_n can split in A_n.

Example 2.6.11. $(123), (321)$ are conjugate in S_3. But $A_3 \cong C_3$ is abelian, so (123) is not conjugate in A_3 to (321), because they are not equal.[13]

Lemma 2.6.7. Let $\gamma \in A_n \subseteq S_n$.

(1) If some odd element of S_n commutes with γ, then $\mathrm{ccl}_{A_n}(\gamma) = \mathrm{ccl}_{S_n}(\gamma)$.

(2) If every element of S_n that commutes with γ is even, then $\mathrm{ccl}_{S_n}(\gamma)$ splits into two:
$$\mathrm{ccl}_{S_n}(\gamma) = \mathrm{ccl}_{A_n}(\gamma) \cup \mathrm{ccl}_{A_n}(\tau\gamma\tau)$$
where τ is any transposition.

Theorem 2.6.8. A_5 is simple.

[13] There is no permutation τ in A_n such that $\tau(123)\tau^{-1} = (321)$.

Proof. Suppose $N \lhd A_5$. We need to prove that $N = 1$ or $N = A_5$. By Example Sheet 3 Q5, N is an union of conjugacy classes of A_5. Since it has to contain e, the possible orders of N are: 1, 22, 37, 48, 33, 45, 16, 28, 40, 13, 25, 60. By Lagrange's theorem, only acceptable values are 1 and 60, which correspond to trivial subgroup and A_5 respectively. Hence, A_5 is indeed simple. (Also note that A_5 is the smallest example of a non-abelian simple group). ■

2.7 Matrix Groups

This section requires some knowledge from Vectors & Matrices.

2.7.1 General Linear Group

Groups of matrices provide some of the most important and fascinating examples of (infinite) groups. To begin, let

$$M_n(\mathbb{F}) = \{n \times n \text{ matrices with entries in } \mathbb{F}\}$$

where $\mathbb{F}$ a field, e.g. $\mathbb{R}, \mathbb{C}$. Matrix multiplication is well known to be associative, and there is an identity $I_n = I = \mathbb{1} = 1$. However, not all matrices are invertible.

Definition 2.7.1. A *general linear group* $\mathrm{GL}(n, \mathbb{F})$ is defined as a set of invertible $n \times n$ matrices over $\mathbb{F}$.[14]

Proposition 2.7.1. $\det : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}\backslash\{0\}$ is a surjective homomorphism.

Proof. We have $\det AB = \det A \det B$. Also, if A invertible, it has non-zero determinant and $\det A \in \mathbb{F}\backslash\{0\}$. Furthermore, to prove surjectivity, for any $x \in \mathbb{F}\backslash\{0\}$, we take I and replace I_{11} with x. Then the determinant of such matrix is x. ■

Definition 2.7.2. We define the *special linar group* as the kernal of $\det : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}\backslash\{0\}$:

$$\mathrm{SL}(n, \mathbb{F}) = \ker(\det) = \{A \in \mathrm{GL} \mid \det A = 1\}$$

It follows that $\mathrm{SL}(n, \mathbb{F}) \lhd \mathrm{GL}(n, \mathbb{F})$. Also note that $Q_8 \leqslant \mathrm{SL}(2, \mathbb{C})$.

2.7.2 Change of Basis and Action

One may think of a natural action by matrix conjugation:

$$\mathrm{GL}(n, \mathbb{R}) \curvearrowright M_n(\mathbb{R}), \quad P(A) = PAP^{-1}$$

where $P \in \mathrm{GL}(n, \mathbb{R})$ and $A \in M_n(\mathbb{R})$.

Proposition 2.7.2. Let V be a n-dimensional vector space and $\alpha : V \to V$ a linear map. If $A \in M_n(\mathbb{R})$ represents α in some basis, then the orbit

$$\mathrm{GL}(n, \mathbb{R})A = \{PAP^{-1} \mid P \in \mathrm{GL}(n, \mathbb{R})\}$$

consists of all matrices that represent α in any basis.

[14] Composition of invertible matrices are invertible.

Proof. A basis $\{\mathbf{v}_1,\dots,\mathbf{v}_n\}$ for V defines an isomorphisms of vector spaces $\phi:\mathbb{R}^n\to V$,

$$(\lambda_1,\dots,\lambda_n)\mapsto\sum_{i=1}^{n}\lambda_i\mathbf{v}_i$$

The hypothesis that A represents α in this basis means:

$$A=\phi^{-1}\circ\alpha\circ\phi\Rightarrow\alpha=\phi\circ A\circ\phi^{-1}$$

Likewise, another basis $\{u_1,\dots,u_n\}$ corresponds to an isomorphism $\psi:\mathbb{R}^n\to V$ and $B\in M_n(\mathbb{R})$ reprents α in this basis if

$$B=\psi^{-1}\circ\alpha\circ\psi=\psi^{-1}\circ(\phi\circ A\circ\phi^{-1})\circ\psi=(\psi^{-1}\circ\phi)\circ A\circ(\psi^{-1}\circ\phi)^{-1}$$

Thus, $B=PAP^{-1}$ where $P=\psi^{-1}\circ\phi\in\mathrm{GL}(n,\mathbb{R})$. We have shown that every matrix representing α is in $\mathrm{GL}(n,\mathbb{R})$. We still need to prove the reverse inclusion.

Conversely, suppose $B+PAP^{-1}$. Then, setting $\psi=\phi\circ P^{-1}$, it defines a basis

$$\{\mathbf{u}_i=\psi(\mathbf{e}_i)\}$$

for V with $\mathbf{e}_i$ as the standard i^{th} basis vector of $\mathbb{R}^n$. Then, B is the matrix for α in this basis. ∎

2.7.3 Möbius Transformation Revisited

Recall that multiplication in $\mathcal{M}$ looked similar to multiplication of 2×2 matrices. This is explained by the next result.

Proposition 2.7.3. Identitify

$$\mathbb{C}_\times=\left\{\begin{pmatrix}\lambda&0\\0&\lambda\end{pmatrix}\in\mathrm{GL}(2,\mathbb{C})\;\middle|\;\lambda\neq 0\right\}$$

Then $\mathbb{C}_\times\lhd\mathrm{GL}(2,\mathbb{C})$ and $\mathrm{GL}(2,\mathbb{C})/\mathbb{C}_\times\cong\mathcal{M}$.

Proof. Define $\Phi:\mathrm{GL}(2,\mathbb{C})\to\mathcal{M}$,

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\mapsto\left(z\mapsto\frac{az+b}{cz+d}\right)$$

By our computation of multiplication in $\mathcal{M}$, we see that Φ is a homomorphism, which is obviously surjective. A matrix

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\ker\Phi$$

if and only if it fixes $0,1,\infty$, i.e. $b=c$ and $a+b=c+d\Rightarrow a=d$. So $\ker\Phi=\mathbb{C}_\times$. The result follows from the isomorphism theorem (Theorem 2.5.3). ∎

2.7.4 Orthogonal Groups

Let's write $||\bullet||$ for the usual Euclidean notation of distance on $\mathbb{R}^n$:

$$||\mathbf{u}-\mathbf{v}|| = \sqrt{\sum_{i=1}^{n}(u_i - v_i)^2}$$

Definition 2.7.3. The n-dimensional *orthogonal group* is the subgroup of $\mathrm{GL}(n,\mathbb{R})$ that preserves distance in $\mathbb{R}^n$, i.e.

$$\mathrm{O}(n) = \{A \in \mathrm{GL}(n,\mathbb{R}) \,:\, ||A\mathbf{u} - A\mathbf{v}|| = ||\mathbf{u}-\mathbf{v}||, \quad \forall \mathbf{u},\mathbf{v} \in \mathbb{R}^n\}$$

Remark 2.7.1. This is same as saying that $||A\mathbf{x} = \mathbf{x}||$ for all $\mathbf{x} \in \mathbb{R}^n$. In fact, the *dot product*

$$\mathbf{u}\cdot\mathbf{v} = \sum_{i=1}^{n} u_i v_i$$

is often more convinient to work with the notion of distance.

Lemma 2.7.4. (*Polarisation Identity*) For $\mathbf{u},\mathbf{v} \in \mathbb{R}^n$,

$$2(\mathbf{u}\cdot\mathbf{v}) = ||\mathbf{u}||^2 + ||\mathbf{v}||^2 - ||\mathbf{u}-\mathbf{v}||^2$$

Proof. By definitions,

$$||\mathbf{u}-\mathbf{v}||^2 = (\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) = ||\mathbf{u}||^2 - 2(\mathbf{u}\cdot\mathbf{v}) + ||\mathbf{v}||^2$$

■

Hence, we can characterise $\mathrm{O}(n)$ using the dot product.

Lemma 2.7.5.

$$\mathrm{O}(n) = \{A \in \mathrm{GL}(n,\mathbb{R}) \mid (A\mathbf{x})\cdot(A\mathbf{y}) = \mathbf{x}\cdot\mathbf{y}, \quad \forall \mathbf{x},\mathbf{y} \in \mathbb{R}^n\}$$

Proof. If $(A\mathbf{x})\cdot(A\mathbf{y}) = \mathbf{x}\cdot\mathbf{y}$ for all $\mathbf{x},\mathbf{y} \in \mathbb{R}^n$, then, for any $\mathbf{u},\mathbf{v} \in \mathbb{R}^n$,

$$||A\mathbf{u} - A\mathbf{v}||^2 = ||A(\mathbf{u}-\mathbf{v})||^2 = (A(\mathbf{u}-\mathbf{v}))\cdot(A(\mathbf{u}-\mathbf{v})) = (\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) = ||\mathbf{u}-\mathbf{v}||^2$$

so $A \in \mathrm{O}(n)$.

Conversely, if $A \in \mathrm{O}(n)$, then for any $\mathbf{x},\mathbf{y} \in \mathbb{R}^n$,

$$\begin{aligned} 2(A\mathbf{x})\cdot(A\mathbf{y}) &= ||A\mathbf{x}||^2 + ||A\mathbf{y}||^2 - ||A\mathbf{x} - A\mathbf{y}||^2 \\ &= ||A\mathbf{x} - A0||^2 + ||A\mathbf{y} - A0||^2 - ||A\mathbf{x} - A\mathbf{y}||^2 \\ &= ||\mathbf{x}||^2 + ||\mathbf{y}||^2 - ||\mathbf{x}-\mathbf{y}||^2 = 2(\mathbf{x}\cdot\mathbf{y}) \end{aligned}$$

using the polarisation identity. ■

Lemma 2.7.6. Let $A \in M_n(\mathbb{R})$. Then following are equivalent:

(1) $A \in \mathrm{O}(n)$;

(2) The columns of A forms an orthonormal basis;

(3) $A^\intercal A = I$.

Proof. (1)⇒(2). Let $\{\mathbf{e}_1,\dots \mathbf{e}_n\}$ be the standard basis for $\mathbb{R}^n$. The i^{th} column of A is $A\mathbf{e}_i$. But

$$(A\mathbf{e}_i)\cdot(A\mathbf{e}_j) = \mathbf{e}_i\cdot\mathbf{e}_j = \delta_{ij}$$

so the columns form an orthonormal basis.

(2)⇒(3). Since $(A\mathbf{e}_i)\cdot(A\mathbf{e}_j) = \mathbf{e}_i\cdot\mathbf{e}_j = \delta_{ij}$, $\mathbf{u}\cdot\mathbf{v} = \mathbf{u}^\intercal\mathbf{v}$, this means that $e_i^\intercal A^\intercal A e_j = \delta_{ij}$. But $\mathbf{e}_i^\intercal M\mathbf{e}_j$ is the ij entry of M for any matrix M, so $A^\intercal A = I$ as required.

(3)⇒(1). Suppose $\mathbf{u},\mathbf{v}\in\mathbb{R}^n$. Then

$$(A\mathbf{u})\cdot(A\mathbf{v}) = (A\mathbf{u})^\intercal(A\mathbf{v}) = \mathbf{u}^\intercal A^\intercal A\mathbf{v} = \mathbf{u}^\intercal\mathbf{v} = \mathbf{u}\cdot\mathbf{v}$$

■

Recall that $\det(A^\intercal) = \det A$. Therefore, if $A\in \mathrm{O}(n)$,

$$1 = \det I = \det(A^\intercal A) = \det(A^\intercal)\det A = (\det A)^2$$

Hence $\det A = \pm 1$.

Definition 2.7.4. We define the *special orthogonal group* as

$$\mathrm{SO}(n) = \mathrm{O}(n)\cap\mathrm{SL}(n,\mathbb{R}) = \{A\in\mathrm{O}(n)\mid \det A = 1\}$$

Note that $\mathrm{SO}(n) = \ker(\det:\mathrm{O}(n)\to\{\pm 1\})$ so

$$|\mathrm{O}(n):\mathrm{SO}(n)| = 2$$

by the isomorphism theorem.

CHAPTER 3

Analysis I

Lecture by Professor Claude Warnick. Lent term 2024.

3.1 Limits and Convergence

3.1.1 Sequences

Consider a sequence of real numbers

$$a_1, a_2, a_3, \dots$$

(a_n) where $a_n \in \mathbb{R}$. We start by defining *limit*.

Definition 3.1.1. We say $a_n \to a$ as $n \to \infty$ for some $a \in \mathbb{R}$ if: given $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that

$$|a_n - a| < \epsilon \quad \forall n \geqslant N$$

If $a_n \leqslant a_{n+1}$ $\forall n$ we say (a_n) is *increasing*; and *decreasing*, *strictly increasing*, *strictly decreasing* for $a_n \geqslant a_{n+1}$, $a_n > a_{n+1}$, $a_n < a_{n+1}$ respectively. In all above cases, (a_n) is *monotone*.

Theorem 3.1.1. (*Monotone Convergence Theorem*) An increasing sequence of real numbers which is bounded above converges (i.e. it has a limit).

In other words, monotone convergence theorem says if $a_n \in \mathbb{R}$ $(n \geqslant 1)$, $A \in \mathbb{R}$ with

$$a_1 \geqslant a_2 \geqslant a_3 \geqslant \cdots \text{ and } a_n \geqslant A \quad \forall n$$

there exists $a \in \mathbb{R}$ such that $a_n \to a$ as $n \to \infty$. Equivalently, decreasing sequence bounded below has a limit. Theorem 3.1.1 is also equivalent with Theorem 3.1.2

Theorem 3.1.2. (*Least Upper Bound Axiom*) Every non-empty set bounded above has a *supremum*.

Definition 3.1.2. (Supremum) If $S \subset \mathbb{R}$,$S \neq \varnothing$ we say that

$$\sup S = K$$

if

(1) $x \leqslant K \quad \forall x \in S$ (K is upper bound for S).

(2) Given $\epsilon > 0$, $\exists x \in S$ such that $x > K - \epsilon$ (K is least upper bound).

Note that similar definition can be made for greatest lower bound and infimum. If $\sup S \in S$, we say $\sup S$ is the *maximum* of S, i.e. $\sup S = \max S$.

Lemma 3.1.3.

(1) The limit is unique, i.e. if $a_n \to a$ and $a_n \to b$ as $n \to \infty$ then $a = b$.

(2) Subsequences converge to the same limit, i.e. if $a_n \to a$ as $n \to \infty$ and $n_1 < n_2 < \cdots$, then $a_{n_j} \to a$ as $j \to \infty$.

(3) If $a_n = c \quad \forall n$, then $a_n \to c$ as $n \to \infty$.

(4) If $a_n \to a$ and $b_n \to b$ then $a_n + b_n \to a + b$.

(5) If $a_n \to a$ and $b_n \to b$ then $a_n b_n \to ab$.

(6) If $a_n \to a$, $a_n \neq 0$ and $a \neq 0$, then $1/a_n \to 1/a$.

(7) If $a_n \leqslant A \quad \forall n$ and $a_n \to a$, then $a \leqslant A$.

(8) If $a_n \to a$ and $c_n \to a$ as $n \to \infty$ and $a_n \leqslant b_n \leqslant c_n$, then $b_n \to a$.

Proof. We will only prove 1, 2, and 5 here.

(1) For any $\epsilon > 0$, we can find $N_1(\epsilon)$ and $N_2(\epsilon)$ such that

$$n \geqslant N_1(\epsilon) \Rightarrow |a_n - a| < \epsilon$$

$$n \geqslant N_2(\epsilon) \Rightarrow |a_n - b| < \epsilon$$

If $n \geqslant \max\{N_1(\epsilon), N_2(\epsilon)\}$, then

$$\begin{aligned} 0 \leqslant |b - a| &= |b - a_n + a_n - a| \\ &\leqslant |b - a_n| + |a_n - a| < 2\epsilon \end{aligned}$$

This implies |b-a|=0, otherwise we can set $\epsilon = |b - a|/3$ to find

$$0 \leqslant |b - a| < \frac{2}{3}|b - a|$$

■

(2) Since $n_j < n_{j+1} \Rightarrow n_{j+1} \geqslant n_j + 1$, by induction, we have $n_j \geqslant j$. As $a_n \to a$ as $n \to \infty$, given $\epsilon > 0$ there exists $N = N(\epsilon)$ such that

$$n \geqslant N(\epsilon) \Rightarrow |a_n - a| < \epsilon$$

So if $j \geqslant N(\epsilon)$, then $n_j \geqslant j \geqslant N(\epsilon)$ and

$$|a_{n_j} - a| < \epsilon$$

■

(3) As $a_n \to a$, $b_n \to b$ as $n \to \infty$, for any $\epsilon > 0$, we can find $N_1(\epsilon)$ and $N_2(\epsilon)$ such that

$$n \geqslant N_1(\epsilon) \Rightarrow |a_n - a| < \epsilon$$
$$n \geqslant N_2(\epsilon) \Rightarrow |b_n - b| < \epsilon$$

Now

$$\begin{aligned} |a_n b_n - ab| &= |a_n b_n - a_n b + a_n b - ab| \\ &\leqslant |a_n b_n - a_n b| + |a_n b - ab| \\ &= |a_n||b_n - b| + |b||a_n - a| \end{aligned}$$

If $n \geqslant N_1(1)$ then $|a_n - a| \leqslant 1$ and hence

$$|a_n| = |a_n - a + a| \leqslant |a_n - a| + |a| \leqslant 1 + |a|$$

Thus if $n \geqslant N_3(\epsilon) = \max\{N_1(1), N_1(\epsilon), N_2(\epsilon)\}$ then

$$|a_n b_n - ab| < (1 + |a|)\epsilon + |b|\epsilon = (1 + |a| + |b|)\epsilon$$

which can be made as small as we like.

■

Lemma 3.1.4.

(1) $1/n \to 0$ as $n \to \infty$.

Proof. $(1/n)$ is a decreasing sequence, bounded below by 0, so by monotone convergence theorem it has a limit L. Now,

$$\frac{1}{2n} = \left(\frac{1}{2}\right)\left(\frac{1}{n}\right) \to \frac{1}{2}L$$

(Lemma 3.1.3 (3), (5)). But $(1/2n)$ is a subsequence of $(1/n)$, so by Lemma 3.1.3 (2),

$$\frac{1}{2n} \to L$$

Then, by Lemma 3.1.3 (1),

$$\frac{1}{2}L = L$$

and $L = 0$. ■

(2) If $|x| < 1$, $x^n \to 0$ as $n \to \infty$.

Proof. Suppose $0 \leqslant x < 1$. Then (x^n) is a decreasing sequence bounded below by 0, and it converges by monotone convergence theorem to a limit L. Now,

$$x^{n+1} = xx^n \to xL$$

(Lemma 3.1.3 (5)). However, (x^{n+1}) is a subsequence of (x^n) so by Lemma 3.1.3 (2), $x^{n+1} \to L$; and consequently by Lemma 3.1.3 (1), $L = xL \Rightarrow L = 0$.

Suppose $-1 < x < 1$. Then,

$$-|x|^n \leqslant x^n \leqslant |x|^n$$

We know $|x|^n \to 0$ and $-|x|^n \to 0$ from above, so $x^n \to 0$ by Lemma 3.1.3 (8). ■

Note that when we talk about a sequence converging, we mean to a *finite* limit, while there is a notion of *tending to infinity*: $a_n \to \infty$ if $\forall M \in \mathbb{R}\ \exists N = N(M)$ such that $n \geqslant N \Rightarrow a_n > M$.

Meanwhile, we can see that our definition of convergence still works if $a_n, a \in \mathbb{C}$ (Definition 3.1.1). Furthermore, Lemma 3.1.3 (1) to (6) all apply for complex sequences, but (7), (8), and Theorem 3.1.1 use the *order relation* so do not carry over directly.

Lemma 3.1.5. If (z_n) is a complex sequence, then $z_n \to z$ if and only if $\mathrm{Re}(z_n) \to \mathrm{Re}(z)$ and $\mathrm{Im}(z_n) \to \mathrm{Im}(z)$.

Proof. Note if $\omega \in \mathbb{C}$,

$$\max\{|\mathrm{Re}(\omega)|, |\mathrm{Im}(\omega)|\} \leqslant |\omega| \leqslant |\mathrm{Re}(\omega)| + |\mathrm{Im}(\omega)|$$

($\Rightarrow$) Suppose $z_n \to z$. Then, $\forall \epsilon > 0$ there exists $N = N(\epsilon)$ such that

$$n \geqslant N \Rightarrow |z_n - z| < \epsilon \Rightarrow |\mathrm{Re}(z_n) - \mathrm{Re}(z)| < \epsilon \\ \text{and } |\mathrm{Im}(z_n) - \mathrm{Im}(z)| < \epsilon$$

Therefore $\mathrm{Re}(z_n) \to \mathrm{Re}(z)$ and $\mathrm{Im}(z_n) \to \mathrm{Im}(z)$.

($\Leftarrow$) Suppose $\mathrm{Re}(z_n) \to \mathrm{Re}(z)$ and $\mathrm{Im}(z_n) \to \mathrm{Im}(z)$. Then $\forall \epsilon > 0\ \exists N_1 = N_1(\epsilon), N_2 = N_2(\epsilon)$ such that

$$n \geqslant N_1 \Rightarrow |\mathrm{Re}(z_n) - \mathrm{Re}(z)| < \epsilon \\ n \geqslant N_2 \Rightarrow |\mathrm{Im}(z_n) - \mathrm{Im}(z)| < \epsilon$$

So if $n \geqslant \max\{N_1(\epsilon), N_2(\epsilon)\} = N_3(\epsilon)$, then

$$|z_n - z| \leqslant |\mathrm{Re}(z_n) - \mathrm{Re}(z)| + |\mathrm{Im}(z_n) - \mathrm{Im}(z)| < 2\epsilon$$

and therefore $z_n \to z$. ∎

Theorem 3.1.6. (*Bolzano-Weierstrass Theorem*) Every bounded sequence in $\mathbb{R}$ has a convergent subsequence, i.e. if $x_n \in \mathbb{R}$ and there exists $K > 0$ such that $|x_n| \leqslant K \quad \forall n$, we can find $n_1 < n_2 < n_3 < \cdots$ and $x \in \mathbb{R}$ such that $x_{n_j} \to x$ as $j \to \infty$. N.b. we do not assert uniqueness, e.g. if $x_n = (-1)^n$, $x_{2n} \to 1$ but $x_{2n+1} \to -1$.

Proof. Set $a_1 = -K$, $b_1 = K$ so that all terms of (x_n) lie in $[a_1, b_1]$. Let $c = (a_1 + b_1)/2$. Either

(1) There are infinitely many terms of (x_n) in $[a_1, c]$ or

(2) There are infinitely many terms of (x_n) in $[c, b_1]$.

If (1) holds, we set $a_2 = a_1$, $b_2 = c$; or if (1) does not hold, we set $a_2 = c$, $b_2 = b_1$. Continue inductively to construct a_k, b_k such that infinitely many terms of (x_n) lie in $[a_k, b_k]$, with

$$b_{k+1} - a_{k+1} = \frac{1}{2}(b_k - a_k)$$

and

$$a_k \leqslant a_{k+1} < b_{k+1} \leqslant b_k$$

By construction, (a_k) is increasing and bounded above by b_1. So, from the monotone convergence theorem,

$$a_k \to a \in [a_1, b_1] \text{ as } k \to \infty$$

Similarly, since (b_k) is decreasing and bounded below by a_1,

$$b_k \to b \in [a_1, b_1] \text{ as } k \to \infty$$

But

$$b_{k+1} - a_{k+1} = \frac{1}{2}(b_k - a_k) \Rightarrow b - a = \frac{1}{2}(b - a)$$

and $b = a$. Now construct n_j as follows.

- Pick $n_1 = 1$.
- Pick n_j to be the smallest integer greater than n_{j-1} such that $x_{n_j} \in [a_j, b_j]$.

We can do this as $[a_j, b_j]$ contains infinitely many terms of (x_n). Viz, $a_j \leqslant x_{n_j} \leqslant b_j$ and by Lemma 3.1.3 (8), $x_{n_j} \to a$. ■

Definition 3.1.3. A sequence (a_n) of real numbers is a *Cauchy sequence* (Cauchy) if for all $\epsilon > 0$ there exists $N = N(\epsilon)$ such that $n, m \geqslant N \Rightarrow |a_n - a_m| < \epsilon$.

Lemma 3.1.7. Every convergent sequence is a Cauchy sequence.

Proof. If $a_n \to a$, then given $\epsilon > 0$ $\exists N = N(\epsilon)$ such that if $n \geqslant N$, $|a_n - a| < \epsilon$. But if $m, n \geqslant N$,

$$|a_n - a_m| = |a_n - a + a - a_m| \leqslant |a_n - a| + |a_m - a| < 2\epsilon$$

■

Theorem 3.1.8. Every Cauchy sequence is convergent.

Proof. Suppose (a_n) is Cauchy. First we show (a_n) is bounded. Since (a_n) is Cauchy, given $\epsilon > 0$ $\exists N = N(\epsilon)$ such that

$$|a_n - a_m| < \epsilon \quad \forall n, m \geqslant N(\epsilon)$$

So if $n, m \geqslant N(1)$, then $|a_n - a_m| < 1$. Set $m = N(1)$ to see

$$|a_n| = |a_n - a_{N(1)} + a_{N(1)}| \leqslant |a_n - a_{N(1)}| + |a_{N(1)}| \leqslant 1 + |a_{N(1)}| \quad \forall n \geqslant N(1)$$

Thus if $K = 1 + \max\{|a_1|, \ldots, |a_{N(1)}|\}$,

$$|a_n| \leqslant K \quad \forall n$$

Now, by Bolzano-Weierstrass theorem (Theorem 3.1.6), there must be $a \in \mathbb{R}$ and $n_1 < n_2 < n_3 < \cdots$ such that $a_{n_j} \to a$ as $j \to \infty$. We claim, in fact, $a_n \to a$ as $n \to \infty$. To see this, write

$$|a_n - a| = |a_n - a_{n_j} + a_{n_j} - a| \leqslant |a_n - a_{n_j}| + |a_{n_j} - a|$$

and fix $\epsilon > 0$. Since (a_n) is Cauchy, $\exists N_1(\epsilon)$ such that if $n, n_j \geqslant N_1(\epsilon)$, $|a_n - a_{n_j}| < \epsilon$.

Since $a_{n_j} \to a$, $\exists N_2(\epsilon)$ such that if $j \geqslant N_2(\epsilon)$, $|a_{n_j} - a| < \epsilon$. Fix j such that $j \geqslant N_2(\epsilon)$ and $n_j \geqslant N_1(\epsilon)$. Then we have, for any $n \geqslant N_1(\epsilon)$,

$$|a_n - a| < 2\epsilon$$

i.e. $a_n \to a$. ■

We have shown a real sequence converges if and only if it is Cauchy (Lemma 3.1.7 and Theorem 3.1.8). This is called the *Cauchy's general principle of convergence*.

Corollary 3.1.8.1. A complex sequence converges if and only if it is Cauchy.

Proof. From estimate at start of proof of Lemma 3.1.5, it follows that (z_n) is Cauchy if and only if $(\mathrm{Re}(z_n))$ and $(\mathrm{Im}(z_n))$ are both Cauchy. ■

3.1.2 Series and Convergence Tests

Definition 3.1.4. Suppose $a_j \in \mathbb{R}(\text{ or } \mathbb{C})$. Define sequence of *partial sums* (S_N) where

$$S_N = \sum_{j=1}^{N} a_j$$

Then, if $S_N \to S$ as $N \to \infty$, we write

$$S = \sum_{j=1}^{\infty} a_j$$

and say $\sum_{j=1}^{\infty} a_j$ converges. Conversely, if S_N does not converge, we say $\sum_{j=1}^{\infty} a_j$ diverges.

Remark 3.1.1. Any problem on series is a problem about sequences, and vice versa.

Lemma 3.1.9.

(1) If $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ converge, then so does

$$\sum_{j=1}^{\infty} (\lambda a_j + \mu b_j)$$

for $\lambda, \mu \in \mathbb{R}(\text{ or } \mathbb{C})$; and

$$\sum_{j=1}^{\infty} (\lambda a_j + \mu b_j) = \lambda \sum_{j=1}^{\infty} a_j + \mu \sum_{j=1}^{\infty} b_j$$

(2) Suppose there exists N such that $a_j = b_j \ \forall j \geqslant N$. Then either $\sum_{j=1}^{\infty} a_j$ and $\sum_{j=1}^{\infty} b_j$ both converge, or both diverge.

Proof. Suppose $n \geqslant N$. Then,

$$S_n = \sum_{j=1}^{N-1} a_j + \sum_{j=N}^{n} a_j$$

and

$$\begin{aligned} D_n &= \sum_{j=1}^{N-1} b_j + \sum_{j=N}^{n} b_j \\ &= S_n + \left(\sum_{j=1}^{N-1} b_j - \sum_{j=1}^{N-1} a_j \right) \\ &= S_n + k \end{aligned}$$

where k finite constant. Thus, D_n converges if and only if S_n converges. ∎

An important example is the *geometric series*. Suppose $x \in \mathbb{R}$ and let $a_j = x^{j-1}$ for $j \geqslant 1$. Then,

$$S_n = \sum_{j=1}^{n} x^{j-1} = 1 + x + x^2 + \cdots + x^{n-1}$$

and

$$S_n = \begin{cases} \frac{1-x^n}{1-x} & x \neq 1 \\ n & x = 1 \end{cases}$$

We can check the convergence of S_n for different values of x:

- if $|x| < 1$, $x^n \to 0$ and $S_n \to 1/(1-x)$.
- if $x \geqslant 1$, write $x = 1 + \delta$ where $\delta \geqslant 0$. By expansion,

  $$x^n = 1 + \delta n + \cdots + \delta^n \geqslant 1 + \delta n$$

  Hence, $x^n \to \infty$ and $S_n \to \infty$ for $x > 1$.
- if $x = 1$, trivially $S_n = n \to \infty$.
- if $x < -1$, $x^n = (-1)^n |x|^n$ does not converge as $|x|^n \to \infty$. $|S_n| \to \infty$ but S_n may alternate in sign.
- if $x = -1$,

  $$S_n = \begin{cases} 1 & n \text{ odd} \\ 0 & n \text{ even} \end{cases}$$

  and hence it does not converge.

Therefore, we may conclude that $\sum_{j=1}^{\infty} x^{j-1}$ converges if and only if $|x| < 1$.

Let's take a further look into convergence tests. A simple, but useful result is the n^{th} *term test*.

Lemma 3.1.10. If $\sum_{j=1}^{\infty} a_j$ converges, then $a_j \to 0$ as $j \to \infty$.

Proof. If $S_n = \sum_{j=1}^{n} a_j$, $a_n = S_n - S_{n-1}$ but

$$S_n \to S \Rightarrow S_{n-1} \to S$$

so $a_n \to 0$. ■

Note that converse of Lemma 3.1.10 is false. For example, consider $\sum_{j=1}^{\infty} 1/j$, i.e. *harmonic series*. If we let $S_n = \sum_{j=1}^{n} 1/j$,

$$\begin{aligned} S_{2n} &= S_n + \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \\ &\geqslant S_n + \frac{1}{2n} + \frac{1}{2n+1} + \cdots + \frac{1}{2n} \end{aligned}$$

Thus $S_{2n} \geqslant S_n + 1/2$ and $S_{2n} - S_n \geqslant 1/2$. If $S_n \to S$, then $S_{2n} \to S$ and $0 \geqslant 1/2$, which is a contradiction. Therefore, $S_n = \sum_{j=1}^{n} 1/j$ diverges.

Moreover, Lemma 3.1.10 is often used to show a series does not converge.

∗ Series with non-negative terms

We consider, for the time being, series whose terms satisfy

$$a_j \geqslant 0 \quad \forall j$$

Theorem 3.1.11. (*Comparison Test*) Suppose $0 \leqslant b_n \leqslant a_n \quad \forall n$. Then if $\sum_{n=1}^{\infty} a_n$ converges, so does $\sum_{n=1}^{\infty} b_n$.

Proof. Let $S_N = \sum_{n=1}^{N} a_n$ and $D_N = \sum_{n=1}^{N} b_n$. Both S_N and D_N are monotonically increasing and $S_N \to S$. But

$$b_n \leqslant a_n \Rightarrow D_N \leqslant S_N \leqslant S$$

So, since (D_N) is increasing and bounded above, D_N converges (Theorem 3.1.1). ■

For example of the comparison test, consider $\sum_{n=1}^{\infty} 1/n^2$. We have

$$0 \leqslant \frac{1}{n^2} < \frac{1}{n(n-1)} = \underbrace{\frac{1}{n-1} - \frac{1}{n}}_{a_n}$$

for $n \geqslant 2$. Then,

$$\sum_{n=2}^{N} a_n = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \cdots + \left(\frac{1}{N-1} - \frac{1}{N}\right) = 1 - \frac{1}{N} \to 1$$

as $N \to \infty$. Hence, since $\sum_{n=2}^{\infty} 1/(n-1)n$ converges, $\sum_{n=2}^{\infty} 1/n^2$ and consequently $\sum_{n=1}^{\infty} 1/n^2$ converges by comparison test.

Theorem 3.1.12. (*Root Test*) Suppose $a_n \geqslant 0$ and $a_n^{1/n} \to a$ as $n \to \infty$. Then if $a < 1$, $\sum a_n$ converges; else if $a > 1$, $\sum a_n$ diverges. If $a = 1$, test is inconclusive.

Proof. If $a < 1$, choose r such that $a < r < 1$. From Definition 3.1.1, $\exists N$ such that $\forall n \geqslant N$[1]

$$a_n^{1/n} < r \Rightarrow a_n < r^n$$

Since $r < 1$, the series $\sum r^n$ converges, so by comparison test and Lemma 3.1.9 (2), we have that $\sum a_n$ converges.

If $a > 1$, $\exists N$ such that $\forall n \geqslant N$ $a_n^{1/n} > 1 \Rightarrow a_n > 1$. Hence, $\sum a_n$ diverges (Lemma 3.1.10). ■

Theorem 3.1.13. (*Ratio Test*) Suppose $a_n > 0$ and $a_{n+1}/a_n \to l$. If $l < 1$ $\sum a_n$ converge; else if $l > 1$ $\sum a_n$ diverge. If $l = 1$, test is inconclusive.

Proof. Suppose $l < 1$ and choose r with $l < r < 1$. Then from Definition 3.1.1, $\exists N$ such that $\forall n \geqslant N$ $a_{n+1}/a_n < r$. Hence, for $n > N$,

$$a_n = \frac{a_n}{a_{n-1}} \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_{N+1}}{a_N} a_N < a_N r^{n-N} \Rightarrow a_n < k r^n$$

where k is independent of n. But since $\sum kr^n$ converges, so does $\sum a_n$ (Lemma 3.1.9 (2)).

[1] Choose $\epsilon = r - a > 0$.

If $l > 1$, pick $r > 1$ such that $1 < r < l$. Then, $\exists N$ such that $\forall n \geqslant N$ $a_{n+1}/a_n > r$ and

$$a_n = \frac{a_n}{a_{n-1}} \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_{N+1}}{a_N} a_N > a_N r^{n-N}$$

But $r^{n-N} \to \infty$ as $n \to \infty$. Thus $a_n \to \infty$ and $\sum a_n$ diverges. ■

Here are some examples for the tests above.

- $\sum(n/2^n)$. Can show the covergence by both ratio and root test.
- $\sum 1/n$ diverges but ratio test and root test both yields 1 (inconclusive).
- $\sum 1/n^2$ converges but ratio test and root test both yields 1 (inconclusive).

Remark 3.1.2. To show $n^{1/n} \to 1$, write $n^{1/n} = 1 + \delta_n$ ($\delta_n > 0$). Then, binomial expansion gives

$$n = (1 + \delta_n)^n > \frac{n(n-1)}{2} \delta_n^2$$

and

$$0 < \delta_n^2 < \frac{2}{n+1} \Rightarrow \delta_n = 0$$

Theorem 3.1.14. (*Cauchy's Condensation Test*) Let (a_n) be a decreasing sequence of positive terms. Then $\sum_{n=1}^{\infty} a_n$ converges if and only if

$$\sum_{n=1}^{\infty} 2^n a_{2^n}$$

converges.

Proof. Since a_n is decreasing, note that

$$a_{2^k} \leqslant a_{2^{k-1}+i} \leqslant a_{2^{k-1}}$$

for $1 \leqslant i \leqslant 2^{k-1}$. Let us prove each direction seperately.

($\Rightarrow$) Suppose $\sum a_n$ converges. But

$$\begin{aligned} 2^{k-1} a_{2^k} &= a_{2^k} + \cdots + a_{2^k} \\ &\leqslant a_{2^{k-1}+1} + a_{2^{k-1}+2} + \cdots + a_{2^{k-1}+2^{k-1}} \\ &= \sum_{n=2^{k-1}+1}^{2^k} a_n \end{aligned}$$

Hence,

$$\sum_{k=1}^{K} 2^{k-1} a_{2^k} \leqslant \sum_{k=1}^{K} \left(\sum_{n=2^{k-1}+1}^{2^k} a_n \right) = \sum_{n=2}^{2^K} a_n \leqslant \sum_{n=1}^{\infty} a_n$$

and $\sum_{k=1}^{K} 2^k a_{2^k}$ converges since it is increasing in K and bounded above.

($\Leftarrow$) Suppose $\sum 2^n a_{2^n}$ converges. Then,

$$\begin{aligned} \sum_{n=2^{k-1}+1}^{2^k} a_n &= a_{2^{k-1}+1} + a_{2^{k-1}+2} + \cdots + a_{2^{k-1}+2^{k-1}} \\ &\leqslant a_{2^{k-1}} + \cdots + a_{2^{k-1}} \\ &= 2^{k-1} a_{2^{k-1}} \end{aligned}$$

This implies

$$\sum_{n=2}^{2^K} a_n = \sum_{k=1}^{K} \left(\sum_{n=2^{k-1}+1}^{2^k} a_n \right) \leqslant \sum_{k=1}^{K} 2^{k-1} a_{2^{k-1}} \leqslant \sum_{n=1}^{\infty} 2^{k-1} a_{2^{k-1}}$$

Thus for any N, if we pick K such that $2^K > N$,

$$\sum_{n=2}^{N} \leqslant \sum_{n=2}^{2^K} a_n \leqslant \sum_{n=1}^{\infty} 2^{k-1} a_{2^{k-1}}$$

Similarly, by monotone convergence theorem, $\sum_{n=2}^{N} a_n$ converges. ■

Corollary 3.1.14.1. (*p-series test*) $\sum_{n \geqslant 1} (1/n^p)$ (for $p > 0$) converges if and only if $p > 1$.

Proof. $a_n = 1/n^p$ is a decreasing sequence of positive numbers, since

$$\frac{n}{n+1} < 1 \Rightarrow \left(\frac{n}{n+1} \right)^p < 1 \Rightarrow \frac{1}{(n+1)^p} < \frac{1}{n^p}$$

Meanwhile,

$$2^n a_{2^n} = 2^n \left(\frac{1}{2^n} \right)^p = 2^{n-np} = \left(2^{1-p} \right)^n = r^n$$

We know that $\sum r^n$ converges if and only if $r < 1$, which is equivalent to $p > 1$. Hence, by Cauchy's condensation test, $\sum_{n \geqslant 1} (1/n^p)$ (for $p > 0$) converges if and only if $p > 1$. ■

∗ Alternating series

Theorem 3.1.15. (*Alternating Series Test*) Suppose (a_n) is a decreasing sequence, tending to 0 as $n \to \infty$. Then, the series

$$\sum_{n=1}^{\infty} (-1)^{n+1} a_n$$

converges.

Proof. Let

$$S_n = \sum_{k=1}^{n} (-1)^{k+1} a_k$$

Then we can find S_{2n} is increasing, since

$$S_{2n} = (a_1 - a_2) + (a_3 - a_4) + \cdots + (a_{2n-1} - a_{2n})$$

Similarly,

$$S_{2n+1} = a_1 - (a_2 - a_3) - (a_4 - a_5) - \cdots - (a_{2n} - a_{2n+1})$$

gives

$$S_{2n+1} \leqslant S_{2n-1} \leqslant \cdots \leqslant S_3 \leqslant S_1$$

Furthermore, $S_{2n+1} = S_{2n} + a_{2n+1} \leqslant S_{2n}$, so

$$S_2 \leqslant S_4 \leqslant \cdots \leqslant S_{2n} \leqslant S_{2n+1} \leqslant S_{2n-1} \leqslant \cdots \leqslant S_3 \leqslant S_1$$

See that (S_{2n}) is increasing, bounded above by S_1; so $S_{2n} \to S$; and (S_{2n+1}) is decreasing, bounded below by S_2, so $S_{2n+1} \to \tilde{S}$. But

$$S_{2n+1} = S_{2n} + a_{2n+1}$$

implies $\tilde{S} = S$. Thus, given $\epsilon > 0$ there exists N_1, N_2 such that

$$|S_{2n} - S| < \epsilon \quad \forall n \geqslant N_1$$

$$|S_{2n+1} - S| < \epsilon \quad \forall n \geqslant N_2$$

Therefore, if we choose $n \geqslant 2\max\{N_1, N_2\} + 1 = N$, $|S_n - S| < \epsilon \Rightarrow S_n \to S$. ■

One may easily see that $\sum(-1)^{n+1}/n$ converges using the alternating series test.

∗ Absolute and conditional convergence

Definition 3.1.5. Let $a_n \in \mathbb{C}$. If $\sum_{n=1}^{\infty} |a_n|$ converges, we say $\sum_{n=1}^{\infty} a_n$ is *absolutely convergent*.

Note that since $|a_n| \geqslant 0$, previous tests can be applied to show absolute convergence.

Theorem 3.1.16. If $\sum_{n=1}^{\infty} a_n$ is absolutely convergent, then it is convergent.

Proof. Let

$$S_n = \sum_{k=1}^{n} a_k, \quad \bar{S}_n = \sum_{k=1}^{n} |a_k|$$

Suppose that $n \leqslant m$. Then

$$|S_m - S_n| = \left| \sum_{k=n+1}^{m} a_k \right| \leqslant \sum_{k=n+1}^{m} |a_k| = |\bar{S}_m - \bar{S}_n|$$

$(\bar{S}_n)$ is convergent, hence Cauchy (Lemma 3.1.7), so given $\epsilon > 0$ $\exists N$ such that $\forall m \geqslant n \geqslant N$ we have

$$|\bar{S}_m - \bar{S}_n| < \epsilon \Rightarrow |S_m - S_n| < \epsilon$$

Thus (S_n) is Cauchy and it converges (Theorem 3.1.8). ■

For example of absolute convergence, consider $\sum_{n=1}^{\infty} a_n$ where $z \in \mathbb{C}$ and $a_n = (z^n/2^n)$. $|a_n| = (|z|/2)^n$ so $\sum |a_n|$ converges if and only if $|z|/2 < 1$. This gives absolute convergence for $|z| < 2$. If $|z| \geqslant 2$, $|a_n| \geqslant 1$ and there is no absolute convergence. Finally, note that coverse of Theorem 3.1.16 is false.

Definition 3.1.6. If $\sum a_n$ converges, but $\sum |a_n|$ does not, we say series is *conditionally convergent*.

N.b. order of terms matters. If rearranged, the sum may change. Consider the rearranged sequences below.

(1) $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$

(2) $1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} - \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \frac{1}{11} - \frac{1}{6} + \cdots$

If S_n is partial sum of (1), T_n partial sum of (2), then

$$S_n \to S > 0$$
$$T_n \to \frac{3S}{2} \neq S$$

Definition 3.1.7. Let $\sigma : \mathbb{N} \to \mathbb{N}$ be a bijection, then (a'_n) with $a'_n = a_{\sigma(n)}$ is a *rearrangement* of (a_n).

Theorem 3.1.17. If $a'_n = a_{\sigma(n)}$ is a rearrangement of (a_n), and $\sum_{n=1}^{\infty} a_n$ is absolutely convergent, then

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a'_n$$

Proof. Fix $\epsilon > 0$. Since $\sum_{n=1}^{\infty} |a_n|$ converges, $\exists N$ such that

$$\sum_{n=N+1}^{\infty} |a_n| < \epsilon$$

Pick M such that $\sigma^{-1}(k) < M$ for $k = 1, \ldots, N$. Then if $m \geqslant M$,

$$\sum_{n=1}^{\infty} a_n - \sum_{n=1}^{m} a_{\sigma(n)} = \sum_{n \in K_m} a_n$$

where $K_m = \{N+1, N+2, \ldots\} \backslash \{\text{finitely many points}\}$. So

$$\left| \sum_{n=1}^{\infty} a_n - \sum_{n=1}^{m} a'_n \right| \leqslant \sum_{n \in K_m} |a_n| \leqslant \sum_{n \geqslant N+1} |a_n| < \epsilon$$

i.e. $\sum_{n=1}^{m} a'_n \to \sum_{n=1}^{\infty} a_n$ as $m \to \infty$. ∎

3.2 Continuity

3.2.1 Continuity of a Function

Suppose $\mathrm{E} \subseteq \mathbb{C}$ is non-empty, and $f : \mathrm{E} \to \mathbb{C}$ is any function (includes case where $\mathrm{E} \subseteq \mathbb{R}$, $f : \mathrm{E} \to \mathbb{R}$).

Definition 3.2.1. f is *continuous* at $a \in \mathrm{E}$ if: given $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that

$$|f(z) - f(a)| < \epsilon$$

for all $z \in \mathrm{E}$ with $|z - a| < \delta$, i.e. *"Points close to a in the domain are mapped close to $f(a)$ in range."*

We say f is continuous on E if f is continuous at a for all $a \in \mathrm{E}$.

Theorem 3.2.1. $f : \mathrm{E} \to \mathbb{C}$ is continuous at $a \in \mathrm{E}$ if and only if

$$f(z_n) \to f(a)$$

for all sequences (z_n) with $z_n \in \mathrm{E}$, $z_n \to a$.

Proof. ($\Rightarrow$) Suppose f is continuous at a, and (z_n) is a sequence $z_n \in \mathrm{E}$ with $z_n \to a$. Let $\epsilon > 0$. Then $\exists \delta > 0$ such that

$$z \in \mathrm{E}, |z-a| < \delta \Rightarrow |f(z) - f(a)| < \epsilon$$

Since $z_n \to a$, there exists N such that

$$n \geqslant N \Rightarrow |z_n - a| < \delta \Rightarrow |f(z) - f(a)| < \epsilon$$

Therefore $f(z_n) \to f(a)$.

($\Leftarrow$) Suppose f is not continuous at a. Then, $\exists \epsilon > 0$ such that $\forall \delta > 0$, $\exists z \in \mathrm{E}$ with

$$|z-a| < \delta \text{ and } |f(z) - f(a)| \geqslant \epsilon$$

apply this with

$$\delta = 1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots$$

to find for each n and $z_n \in \mathrm{E}$ with

$$|z_n - a| < \frac{1}{n} \text{ and } |f(z_n) - f(a)| \geqslant \epsilon > 0$$

Then $z_n \to a$ as $n \to \infty$ but $f(z_n) \nrightarrow f(a)$, which is a contradiction. Hence f is continuous at a. ∎

This means we could alternatively take our definition of continuity as:

$$f(z_n) \to f(a)$$

for all sequences (z_n) with $z_n \in \mathrm{E}$, $z_n \to a$.

Lemma 3.2.2. Suppose $f, g : \mathrm{E} \to \mathbb{C}$ are continuous at $a \in \mathrm{E}$. Then so are the functions

(1) $f(z) + g(z)$,

(2) $f(z)g(z)$,

(3) $\lambda g(z)$ (constant $\lambda \in \mathbb{C}$),

(4) $1/f(z)$ provided $f(z) \neq 0$ $\forall z \in \mathrm{E}$.

Proof. Using the sequential characterisation of continuity, this follows easily from analogous results for sequences (Lemma 3.1.3). E.g. if $z_n \to a$,

$$f(z_n) \to f(a) \text{ and } g(z) \to g(a) \Rightarrow f(z_n) + g(z_n) \to f(a) + g(a)$$

etc. ∎

Note that Lemma 3.2.2 can also be directly proved from Definition 3.2.1. We now show that composition of continuous functions is continuous.

Theorem 3.2.3. Suppose $A, B \subseteq \mathbb{C}$, $f : A \to B$, $g : B \to C$ and that f is continuous at $a \in A$, g is continuous at $f(a) \in B$. Then $g \circ f : A \to \mathbb{C}$ is continuous at a.

Proof. Suppose (z_n) is any sequence with $z_n \in A$, $z_n \to a$. Then by continuity of f at a,

$$f(z_n) \to f(a)$$

By continuity of g at $f(a)$,

$$g(f(z_n)) \to g(f(a)) \Leftrightarrow g \circ f(z_n) \to g \circ f(a)$$

Hence $g \circ f$ is continuous at a. ■

Here are some examples of continuous (and discontinuous) functions.

(1) $f(z) = z$ is continuous at all points of $\mathbb{C}$.

(2) By Lemma 3.2.2 and Example (1) above, any polynomial in z is continuous at all points of $\mathbb{C}$.

(3) $f(z) = |z|$ is continuous at all points of $\mathbb{C}$.[2]

(4) $f : \mathbb{R} \to \mathbb{R}$,

$$x \mapsto \begin{cases} 0 & x < 0 \\ 1 & x \geqslant 0 \end{cases}$$

is not continuous at $x = 0$.

(5) $f : \mathbb{R} \to \mathbb{R}$,

$$f(x) = \begin{cases} \sin \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

$\sin x$ is continuous,[3] so if $x \neq 0$ then Theorem 3.2.3 and Lemma 3.2.2 imply f is continuous at x. However, f is discontinuous at $x = 0$. Choose x_n such that

$$\frac{1}{x_n} = \left(2n + \frac{1}{2}\right)\pi$$

which imply $f(x_n) = 1$, $x_n \to 0$, $f(0) = 0 \neq \lim_{n\to\infty} f(x_n)$.

(6) $f : \mathbb{R} \to \mathbb{R}$,

$$f(x) = \begin{cases} x \sin \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

f is continuous at $x \neq 0$ by same reasons as (5). But f is also continuous at 0 this time. Suppose $x_n \to 0$. Then

$$|f(x_n)| = |x_n| \left|\sin \frac{1}{x_n}\right| \leqslant |x_n|$$

So $|f(x_n)| \leqslant |x_n|$ and $f(x_n) \to 0 = f(0)$.

[2] See reverse triangle inequality.
[3] See later sections for proof.

(7) (*Dirichlet Function*) $f : \mathbb{R} \to \mathbb{R}$,

$$f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

is discontinuous at every point. If $x \in \mathbb{Q}$, take sequence $x_n \notin \mathbb{Q}$, then $x_n \to x$ but

$$f(x_n) = 0 \nrightarrow f(x) = 1$$

If $x \notin \mathbb{Q}$, take $x_n \in \mathbb{Q}$, $x_n \to x$ but

$$f(x_n) = 1 \nrightarrow f(x) = 0$$

3.2.2 Limit of a Function

Suppose $\mathrm{E} \subseteq \mathbb{C}$, $f : \mathrm{E} \to \mathbb{C}$. We want to define

$$\lim_{z \to a} f(z)$$

even when a may not belong to E. For instance, consider $f : \mathbb{C}\backslash\{0\} \to \mathbb{C}$,

$$z \mapsto \sin z/z$$

What is $\lim_{z\to 0} f(z)$? – However, this does not always make sense. If $\mathrm{E} = \{0\} \cup [1, 2]$, for $f : \mathrm{E} \to \mathbb{R}$ it is impossible to consider $\lim_{x\to 0} f(x)$, because there are no point near 0 except 0 itself.

Definition 3.2.2. Suppose $\mathrm{E} \subseteq \mathbb{C}$, $a \in \mathbb{C}$. We say that a is a *limit point* of E if for any $\delta > 0$ there exists $z \in \mathrm{E}$ such that

$$0 < |z - a| < \delta$$

N.b. a is a limit point of E if and only if there exists a sequence (z_n) such that $z_n \in \mathrm{E}$, $z_n \neq a$, and

$$z_n \to a$$

Definition 3.2.3. Suppose $\mathrm{E} \subseteq C$, $f : \mathrm{E} \to \mathbb{C}$ and let $a \in \mathbb{C}$ be a limit point of E. We say

$$\lim_{z \to a} f(z) = l$$

if: given $\epsilon > 0$, $\exists \delta > 0$ such that $\forall z \in \mathrm{E}$,

$$0 < |z - a| < \delta \Rightarrow |f(z) - l| < \epsilon$$

Lemma 3.2.4. If f, E, a as above, then

$$\lim_{z \to a} f(z) = l$$

if and only if $f(z_n) \to l$ for all sequences $z_n \in \mathrm{E}$, $z_n \neq a$, $z_n \to a$.

Observe that the definitions immediately tell us that if $a \in \mathrm{E}$ is a limit point then f is continuous at a if and only if

$$\lim_{z \to a} f(z) = f(a)$$

If $a \in \mathrm{E}$ is *isolated*, i.e. not a limit point, then f is always continuous at a.

Note that limit of functions behave similarly to limits of sequences.

Lemma 3.2.5. Suppose $\mathrm{E} \subseteq \mathbb{C}$, $a \in \mathbb{C}$ is a limit point, and $f, g : \mathrm{E} \to \mathbb{C}$

(1) The limit is unique, i.e. if $f(z) \to A$ and $f(z) \to B$ as $z \to a$, then $A = B$.

(2) If $f(z) \to l$, $g(z) \to k$, then$f(z) + g(z) = l + k$ as $z \to a$;

(3) $f(z)g(z) = lk$ as $z \to a$;

(4) $f(z)/g(z) = l/k$ as $z \to a$ (if $k \neq 0$).

Proof. (of (1))

$$|A - B| = |A - f(z) + f(z) - B| \leqslant |A - f(z)| + |f(z) - B|$$

for all $z \in \mathrm{E}$, $z \neq a$. Given $\epsilon > 0$, $\exists \delta_1 > 0$ such that

$$0 < |z - a| < \delta_1, z \in \mathrm{E} \Rightarrow |f(z) - A| < \epsilon,\ z \in \mathrm{E}$$

Also $\exists \delta_2 > 0$ such that

$$0 < |z - a| < \delta_2, z \in \mathrm{E} \Rightarrow |f(z) - B| < \epsilon,\ z \in \mathrm{E}$$

Since a is a limit point, $\exists z \in \mathrm{E}$ such that

$$0 < |z - a| < \min\{\delta_1, \delta_2\} \Rightarrow |A - B| < 2\epsilon$$

Because ϵ is arbitrary, $A = B$. ■

Theorem 3.2.6. (*Intermediate Value Theorem*) Suppose $f : [a, b] \to \mathbb{R}$ is continuous and $f(a) < f(b)$. Then for any η with $f(a) < \eta < f(b)$ there exists $c \in [a, b]$ such that $f(c) = \eta$.

Proof. Let

$$S = \{x \in [a, b] \mid f(x) < \eta\}$$

Clearly S is not empty as $a \in S$. S is bounded above by b. So S has a supremum, c (Theorem 3.1.2). We claim $f(c) = \eta$. From the definition of a supremum (Definition 3.1.2), for each $n \in \mathrm{N}$ there exists $x_n \in S$ with

$$c - \frac{1}{n} \leqslant x_n \leqslant c$$

Hence $x_n \to c$. But f is continuous so $f(x_n) \to f(c)$ and

$$f(x_n) < \eta \Rightarrow f(c) \leqslant \eta$$

In particular, $c \neq b$. Now let

$$\tilde{x}_n = c + \frac{1}{n}$$

For n large enough, $\tilde{x}_n \in [a,b]$, and $\tilde{x}_n \to c$. Furthermore, $f(\tilde{x}_n) \geqslant \eta$ since

$$\tilde{x}_n > c \Rightarrow \tilde{x}_n \notin S$$

Hence

$$f(c) = \lim_{n\to\infty} f(\tilde{x}_n) \geqslant \eta$$

and thus $f(c) = \eta$. ■

This theorem is useful to find roots of functions. For example, we can check existence of N^{th} roots. Suppose $y > 0$. Consider for $N \in \mathbb{N}$ the function $f : [0, 1+y] \to \mathbb{R}$,

$$x \mapsto x^N$$

Then since

$$(a+y)^N \geqslant 1 + Ny > y$$

we have

$$f(0) < y < f(1+y)$$

and there exists $c \in (0, 1+y)$ such that $f(c) = y$ by intermediate value theorem (IVT). c is a *positive* N^{th} *root* of y. In fact, since

$$y_1 < y_2 \Rightarrow f(y_1) < f(y_2)$$

c is unique.

Lemma 3.2.7. (*Bounds on Continuous Function*) Suppose $f : [a,b] \to \mathbb{R}$ is continuous. Then there exist K such that

$$|f(x)| \leqslant K \quad \forall x \in [a,b]$$

Proof. Suppose not. Then for each $n = 1, 2, \ldots$ we can find $x_n \in [a,b]$ with $|f(x_n)| > n$. By Bolzano-Weierstrass theorem (Theorem 3.1.6), (x_n) is a bounded sequence, and hence has a subsequence $x_{n_j} \to x$ for some x. Moreover, since

$$a \leqslant x_{n_j} \leqslant b \Rightarrow a \leqslant x \leqslant b$$

so $x \in [a,b]$. But

$$|f(x_{n_j})| > n_j \geqslant j$$

so $f(x_{n_j})$ cannot converge. This contradicts the assumption that f is continuous as $f(x_{n_j}) \nrightarrow f(x)$. ■

Theorem 3.2.8. (*Extreme Value Theorem*) Suppose $f : [a,b] \to \mathbb{R}$ is continuous. Then there exist $y, Y \in [a,b]$ such that

$$f(y) \leqslant f(x) \leqslant f(Y) \quad \forall x \in [a,b]$$

Proof. The set

$$A = \{f(x) \mid x \in [a,b]\}$$

is bounded by Lemma 3.2.7, so has a supremum $M = \sup A$. From Definition 3.1.2, $M - 1/n$ is not an upper bound of A for $n \in \mathbb{N}$. So $\exists y_n \in A$ with

$$M - \frac{1}{n} \leqslant y_n \leqslant M$$

From definition of A, there exists $x_n \in [a,b]$ with

$$y_n = f(x_n) \Rightarrow M - \frac{1}{n} \leqslant f(x_n) \leqslant M$$

(x_n) is a bounded sequence. So by Bolzano-Weierstrass theorem we can pick a subsequence (x_{n_j}) such that

$$x_{n_j} \to y$$

for some $y \in [a,b]$. Also $f(x_{n_j}) \to M$, so by continuity of f,

$$f(y) = \lim_{j\to\infty} f(x_{n_j}) = M$$

It follows immediately that

$$f(x) \leqslant f(y) \quad \forall x \in [a,b]$$

For lower bound, we can either consider $\inf A$ and argue similarly, or apply result already established to $-f$. ■

Note that, for Lemma 3.2.7 and Theorem 3.2.8, it is crucial that f is defined on a closed bounded interval: e.g. consider

- $f : (0,1] \to \mathbb{R}$, $x \mapsto 1/x$, continuous, but unbounded.
- $f : [0,\infty) \to \mathbb{R}$, $x \mapsto x$, continuous, but unbounded.

3.2.3 Inverse Function Theorem

Definition 3.2.4. Function $f : [a,b] \to \mathbb{R}$ is

- *increasing* if $a \leqslant x_1 < x_2 \leqslant b \Rightarrow f(x_1) \leqslant f(x_2)$;
- *strictly increasing* if $a \leqslant x_1 < x_2 \leqslant b \Rightarrow f(x_1) < f(x_2)$.

Decreasing and strictly decreasing are defined similarly.

Theorem 3.2.9. Suppose $f : [a,b] \to \mathbb{R}$ is continuous and strictly increasing. Let $c = f(a)$, $d = f(b)$. Then

$$f : [a,b] \to [c,d]$$

is a bijection and

$$f^{-1} : [c,d] \to [a,b]$$

is continuous and strictly increasing.

Proof. First we note that f is injective. If $x \neq y$, then without loss of generality

$$a \leqslant x < y \leqslant b \Rightarrow f(x) < f(y) \Rightarrow f(x) \neq f(y)$$

Next, f maps into $[c,d]$. If $a \leqslant x \leqslant b$, then

$$c = f(a) \leqslant f(x) \leqslant f(b) = d$$

Also, f is surjective by intermediate value theorem: if $\eta \in [c,d]$ then $\exists x \in [a,b]$ with $f(x) = \eta$.

To show f^{-1} is continuous, fix $z \in (c,d)$ and let $y = f^{-1}(z) \in (a,b)$. Let $\epsilon > 0$ to be sufficiently small that

$$a \leqslant y - \epsilon < y < y + \epsilon \leqslant b \Rightarrow c \leqslant f(y-\epsilon) < f(y) < f(y+\epsilon) \leqslant d$$

Pick $\delta > 0$ such that $(z-\delta, z+\delta) \subset (f(y-\epsilon), f(y+\epsilon))$. Since $f : (y-\epsilon, y+\epsilon) \to (f(y-\epsilon), f(y+\epsilon))$ is bijective, if $|z'-z| < \delta$, then

$$\begin{aligned} z' \in (f(y-\epsilon), f(y+\epsilon)) &\Rightarrow f^{-1}(z') \in (y-\epsilon, y+\epsilon) \\ &\Rightarrow |f^{-1}(z') - f^{-1}(z)| < \epsilon \end{aligned}$$

If $z = c$ or d similar argument works. Therefore f^{-1} is continuous.

To see f^{-1} is increasing, suppose not. Then $\exists c \leqslant z_1 < z_2 \leqslant d$ with $f^{-1}(z_1) \geqslant f^{-1}(z_2)$. But f is strictly increasing; this implies

$$f\left(f^{-1}(z_1)\right) \geqslant f\left(f^{-1}(z_2)\right) \Rightarrow z_1 \geqslant z_2$$

which is a contradiction. Thus f^{-1} is strictly increasing. ∎

3.3 Differentiability

In this section, let

$$f : \mathrm{E} \to \mathbb{C}$$

where $\mathrm{E} \subseteq \mathbb{C}$, while mostly E will be a real interval.

Definition 3.3.1. Let $x \in \mathrm{E}$ be a limit point. f is said to be *differentiable* at x, with derivative $f'(x)$ if

$$\lim_{y \to x} \frac{f(y) - f(x)}{y - x} = f'(x)$$

exists.

If f is differentiable at each $x \in \mathrm{E}$, we say f is differentiable on E. Also, we will assume from now on E has no isolated points (set is either interval or disc).

Remark 3.3.1.

(1) Other common notations are

$$\frac{df}{dx}, \frac{dy}{dx}$$

etc.

(2) We can equivalently write

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

(3) Another ways to phrase definition: let $\epsilon(h) = f(x+h) - f(x) - hf'(x)$; then

$$\lim_{h\to 0} \frac{\epsilon(h)}{h} = 0$$

We say, f has a *best affine approximation* near x.

(4) If f is differentiable at x, then f is continuous at x, since $\epsilon(h) \to 0$ as $h \to 0$ giving $f(x+h) \to f(x)$ as $h \to 0$.

Let's look at some examples.

(1) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x$ is differentiable at each x and $f'(x) = 1$, i.e.

$$f(x+h) = x + h = f(x) + h \cdot 1 + 0$$

where $1 = f'(x)$ and $0 = \epsilon(h)$.

(2) $f : \mathbb{R} \to \mathbb{R}$, $x \to |x|$ is differentiable for $x \neq 0$. At $x = 0$ consider

$$\frac{f(h) - f(0)}{h} = \frac{|h|}{h}$$

We have

$$\lim_{h_n \to 0+} \frac{f(h) - f(0)}{h} = 1$$

but

$$\lim_{h_n \to 0-} \frac{f(h) - f(0)}{h} = -1$$

hence the limit does not exist and f is not differentiable at $x = 0$.

3.3.1 Differentiation of Sums and Products

Proposition 3.3.1.

(1) If $f(x) = c \ \forall x \in \mathrm{E}$ then f is differentiable on E with $f'(x) = 0$.

(2) If f, g are differentiable at x, so is $f + g$ and

$$(f+g)'(x) = f'(x) + g'(x)$$

(3) If f, g are differentiable at x, so is fg and

$$(fg)'(x) = f(x)g'(x) + f'(x)g(x)$$

(4) If f is differentiable at x and $f(y) \neq 0 \ \forall y \in E$ then $1/f$ is differentiable at x and

$$\left(\frac{1}{f}\right)' = -\frac{f'(x)}{f(x)^2}$$

Proof.

(1) Can easily see

$$\lim_{h\to 0} \frac{c - c}{h} = 0$$

■

(2) By Lemma 3.2.5, and from

$$\frac{f(x+h)+g(x+h)-f(x)-g(x)}{h} = \frac{f(x+h)-f(x)}{h} + \frac{g(x+h)-g(x)}{h}$$

we have

$$\lim_{h\to 0} \frac{(f+g)(x+h)-(f+g)(x)}{h} = f'(x)+g'(x)$$

■

(3) Let $\phi(x) = f(x)g(x)$. Then for $h \neq 0$

$$\begin{aligned}\frac{\phi(x+h)-\phi(x)}{h} &= \frac{f(x+h)g(x+h)-f(x)g(x)}{h} \\ &= \frac{f(x+h)g(x+h)-f(x+h)g(x)+f(x+h)g(x)-f(x)g(x)}{h} \\ &= f(x+h)\left(\frac{g(x+h)-g(x)}{h}\right) + g(x)\left(\frac{f(x+h)-f(x)}{h}\right)\end{aligned}$$

implying

$$\frac{\phi(x+h)-\phi(x)}{h} \to f(x)g'(x)+f'(x)g(x)$$

■

(4) Let $\phi(x) = 1/f(x)$. Then,

$$\frac{\phi(x+h)-\phi(x)}{h} = \frac{\frac{1}{f(x+h)}-\frac{1}{f(x)}}{h} = \frac{f(x)-f(x+h)}{h}\frac{1}{f(x)f(x+h)}$$

Again, by Lemma 3.2.5,

$$\frac{\phi(x+h)-\phi(x)}{h} \to -\frac{f'(x)}{f(x)^2}$$

■

Note that (3) and (4) give the quotient rule:

$$\left(\frac{f}{g}\right)'(x) = \frac{f'(x)g(x)-g'(x)f(x)}{g(x)^2}$$

For example, consider $f_n(x) = x^n$ where $n \in \mathbb{N}$. Shown that $f_1(x)$ is differentiable and $f_1'(x) = 1$, we claim $f_n(x)$ is differentiable with $f_n'(x) = nx^{n-1}$ for all n. If the claim is true for f_{n-1}, observe that

$$f_n(x) = x^{n-1}x = f_{n-1}(x)f_1(x)$$

By Proposition 3.3.1 (3), f_n is differentiable, and

$$\begin{aligned}f_n'(x) &= f_1(x)f_{n-1}'(x) + f_1'(x)f_{n-1}(x) \\ &= x(n-1)x^{n-2} + x^{n-1} = nx^{n-2}\end{aligned}$$

Hence, by induction, $f_n'(x) = nx^{n-1}$ for all $n \in \mathbb{N}$.

Now consider $f_{-n}(x) = x^{-n}$ where $n \in \mathbb{N}$. If $x \neq 0$ $f_{-n}(x) = 1/f_n(x)$. So by Proposition 3.3.1 (4), $f_{-n}(x)$ is differentiable and

$$f'_{-n}(x) = -\frac{f'_n(x)}{f_n(x)^2} = -\frac{nx^{n-1}}{x^{2n}} = -nx^{-n-1}$$

Therefore $f'_n(x) = nx^{n-1}$ holds for all $n \in \mathbb{Z}$ (with condition $x \neq 0$ if $n < 0$).

Combining results above with Proposition 3.3.1, we see all polynomial functions are differentiable everywhere, and rational functions $f(x) = p(x)/q(x)$ (p, q coprime polynomials) are differentiable everywhere except the roots of q.

Theorem 3.3.2. (*Chain Rule*) Suppose $U, V \subset \mathbb{C}$ and $f : U \to V$, $g : V \to \mathbb{C}$ are such that f is differentiable at $a \in U$ and g is differentiable at $f(a) \in V$. Then, $g \circ f : U \to \mathbb{C}$ is differentiable at a and

$$(g \circ f)'(a) = g'(f(a))f'(a)$$

Proof. Let $f(a) = b$. We can restate the differentiability of f at a, g at b as:

$$f(x) = f(a) + (x-a)f'(a) + \epsilon_f(x)(x-a)$$

$$g(y) = g(b) + (y-b)g'(b) + \epsilon_g(y)(y-b)$$

with $\lim_{x\to a} \epsilon_f(x) = \lim_{y\to b} \epsilon_g(y) = 0$. Notice we can set $\epsilon_f(a) = 0$, $\epsilon_g(b) = 0$ to make ϵ_f, ϵ_g continuous at a, b respectively. Now set $y = f(x)$ and write

$$\begin{aligned} g(f(x)) &= g(f(a)) + (f(x) - f(a))g'(f(a)) + \epsilon_g(f(x))(f(x) - f(a)) \\ &= g(f(a)) + \big((x-a)f'(a) + \epsilon_f(x-a)\big)\, g'(f(a)) \\ &\quad + \epsilon_g(f(x))\big((x-a)f'(a) + \epsilon_f(x)(x-a)\big) \end{aligned}$$

Thus

$$\begin{aligned} g(f(x)) &= g(f(a)) + (x-a)f'(a)g'(f(a)) + (x-a)\left[g'(f(a))\epsilon_f(x) + f'(a)\epsilon_g(f(x)) + \epsilon_g(f(x))\epsilon_f(x)\right] \\ &= g(f(a)) + (x-a)f'(a)g'(f(a)) + (x-a)\sigma(x) \end{aligned}$$

where

$$\sigma(x) = g'(f(a))\epsilon_f(x) + f'(a)\epsilon_g(f(x)) + \epsilon_g(f(x))\epsilon_f(x)$$

Note that $\epsilon_f(x) \to 0$ as $x \to a$, and $\epsilon_g(f(x))$ is composition of continuous functions, so $\epsilon_g(f(x)) \to 0$ as $x \to a$. Hence $\sigma(x) \to 0$ as $x \to a$ and therefore $(g \circ f)'(a) = g'(f(a))f'(a)$ from definition of differentiation. ∎

Remark 3.3.2. Chain rule is often written as

$$\frac{dy}{dx} = \frac{dy}{dt}\frac{dt}{dx}$$

where $y(t(x))$.

3.3.2 The Mean Value Theorem

Theorem 3.3.3. (*Rolle's Theorem*) Let $f : [a,b] \to \mathbb{R}$ be continuous on $[a,b]$ and differentiable on (a,b). If $f(a) = f(b)$ then $\exists c \in (a,b)$ such that $f'(c) = 0$.

Proof. By Theorem 3.2.8 (EVT), $\exists y, Y \in [a,b]$ such that

$$m = f(y) \leqslant f(x) \leqslant f(Y) = M$$

$\forall x \in [a,b]$. If $m = M = f(a)$ then $f(x) = M$ and f constant, so we can take any $c \in (a,b)$.

Otherwise, either $M > f(a)$ or $m < f(a)$. If $M > f(a)$, then $Y \in (a,b)$. We claim $f'(Y) = 0$. To see this, suppose $h_n \to 0+$. Then

$$\frac{f(Y+h_n) - f(Y)}{h_n} \leqslant 0 \Rightarrow \lim_{h\to 0} \frac{f(Y+h) - f(Y)}{h} \leqslant 0$$

If $h_n \to 0-$,

$$\frac{f(Y+h_n) - f(Y)}{h_n} \geqslant 0 \Rightarrow \lim_{h\to 0} \frac{f(Y+h) - f(Y)}{h} \geqslant 0$$

Hence by uniqueness of limit, $f'(Y) = 0$. If $m < f(a)$ a similiar argument shows $y \in (a,b)$ and $f'(y) = 0$. Regardless $\exists c \in (a,b)$ such that $f'(c) = 0$. ■

Theorem 3.3.4. (*Mean Value Theorem*) Let $f : [a,b] \to \mathbb{R}$ be a continuous function, differentiable on (a,b). Then there exists $c \in (a,b)$ such that

$$f(b) - f(a) = f'(c)(b-a) \Leftrightarrow f'(c) = \frac{f(b) - f(a)}{b-a}$$

Proof. Consider

$$\phi(x) = (x-a)(f(b) - f(a)) - (b-a)(f(x) - f(a))$$

Clearly, ϕ satisfies conditions of Rolle's theorem, so $\exists c \in (a,b)$ such that

$$\phi'(c) = 0 \Rightarrow 0 = (f(b) - f(a)) - (b-a)f'(c)$$

■

If f is differentiable on an open interval I containing a, another way to state mean value theorem (MVT) is: given h such that $a + h \in I$, $\exists \Theta = \Theta(h) \in (0,1)$ such that

$$f(a+h) = f(a) + hf'(a + \Theta h)$$

The mean value theorem allows us to export local information about the derivative to global properties of the function.

Corollary 3.3.4.1. Let $f : [a,b] \to \mathbb{R}$ continuous, and differentiable on (a,b). Then,

(1) if $f'(x) > 0$ $\forall x \in (a,b)$, f is strictly increasing.

(2) if $f'(x) \geqslant 0$ $\forall x \in (a,b)$, f is increasing.

(3) if $f'(x) = 0$ $\forall x \in (a,b)$, f is constant on $[a,b]$

Proof.

(1) Let $a \leqslant x < y \leqslant b$. Hypotheses of mean value theorem apply to $f : [x, y] \to \mathbb{R}$ so $\exists c \in (x, y)$ such that
$$f(y) - f(x) = f'(c)(y - x) > 0$$

(2) Same as above, but use $f'(c) \geqslant 0$.

(3) Pick $x \in (a, b]$. Then, by applying mean value theorem on $[a, x]$, we deduce that there exists $c \in (a, x)$ such that
$$f(x) - f(a) = f'(c)(x - a) = 0$$
and f is constant.

■

Meanwhile, note that the mean value theorem is not necessarily true on general sets: e.g. $f : \mathbb{Q} \to \mathbb{Q}$,
$$x \mapsto \begin{cases} 0 & x^2 < 2 \\ 1 & x^2 > 2 \end{cases}$$

Now we revisit the inverse function theorem.

Theorem 3.3.5. Suppose $f : [a, b] \to \mathbb{R}$ is continuous and differentiable on (a, b), with $f'(x) > 0 \ \forall x \in (a, b)$. Let $f(a) = c$, $f(b) = d$. Then,
$$f : [a, b] \to [c, d]$$
is bijective and f^{-1} is differentiable on (c, d) with
$$(f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))}$$

Proof. By Corollary 3.3.4.1 f is strictly increasing on $[a, b]$. By Theorem 3.2.9,
$$f : [a, b] \to [c, d]$$
is bijective and
$$f^{-1} : [c, d] \to [a, b]$$
is continuous and strictly increasing. However, it remains to show f^{-1} is differentiable on (c, d).

Let $y \in (c, d)$ and set $x = f^{-1}(y)$. Given h such that $y + h \in (c, d)$, let k be such that $y + h = f(x + k)$. Then,
$$\frac{f^{-1}(y + h) - f^{-1}(y)}{h} = \frac{x + k - x}{f(x + k) - y} = \frac{k}{f(x + k) - f(x)}$$

Fix $\epsilon > 0$; then by differentiability of f and facts about limits, $\exists \delta > 0$ such that for all $0 < |k| < \delta$ we have
$$\left| \frac{k}{f(x + k) - f(x)} - \frac{1}{f'(x)} \right| < \epsilon$$

Since f^{-1} is continuous, there exists δ' such that

$$\begin{aligned} 0 < |h| < \delta' &\Rightarrow 0 < |f^{-1}(y+h) - x| < \delta \\ &\Rightarrow 0 < k < \delta \\ &\Rightarrow \left| \frac{f^{-1}(y+h) - f^{-1}(y)}{h} - \frac{1}{f'(x)} \right| < \epsilon \end{aligned}$$

Therefore f^{-1} is differentiable at y and

$$(f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))}$$

■

With fixed $R > 0$, consider $f : [0, R] \to \mathbb{R}$, $x \mapsto x^n$ for $n \in \mathbb{N}$. f is continuous on $[0, R]$, differentiable on $(0, R)$ with $f'(x) = nx^{n-1} > 0$ $(x \in (0, R))$. Hence by Theorem 3.3.5, f maps $[0, R]$ bijectively onto $[0, R^n]$ and the inverse $g(y) = f^{-1}(y) = y^{1/n}$ is differentiable with

$$g'(y) = \frac{1}{f'(f^{-1}(y))} = \frac{1}{n(y^{1/n})^{n-1}} = \frac{1}{n} y^{\frac{1}{n}-1}$$

More generally, let $h(x) = x^r$ where $r \in \mathbb{Q}$. Writing $r = m/n$ for $m \in \mathbb{Z}$, $n \in \mathbb{N}$ and defining

$$x^r = \left(x^{1/n}\right)^m$$

h is differentiable on $(0, \infty)$ and

$$h'(x) = m\left(x^{1/n}\right)^{m-1}\left(\frac{1}{n} x^{\frac{1}{n}-1}\right) = \frac{m}{n} x^{\frac{m}{n}-1} = r x^{r-1}$$

by chain rule.

Theorem 3.3.6. (*Cauchy's Mean Value Theorem*) Let $f, g : [a, b] \to \mathbb{R}$ be continuous on $[a, b]$ and differentiable on (a, b). Then there exists $c \in (a, b)$ such that

$$g'(f(a) - f(b)) = f'(c)(g(a) - g(b))$$

which can be also written as

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(c)}{g'(c)}$$

if both sides are well-defined.

Proof. Let

$$\phi(x) = (g(x) - g(a))(f(b) - f(a)) - (g(b) - g(a))(f(x) - f(a))$$

ϕ is continuous on $[a, b]$, differentiable on (a, b) and $\phi(a) = \phi(b) = 0$. Hence by Rolle's theorem, there exists $c \in (a, b)$ such that

$$\phi'(c) = 0 \Rightarrow g'(c)(f(a) - f(b)) - f'(c)(g(a) - g(b)) = 0$$

■

A famous application of Cauchy's mean value theorem is the *L'Hôpital's rule*. Consider

$$\frac{e^x - 1}{\sin x}$$

as $x \to 0$.[4] With noting that

$$\frac{e^x - 1}{\sin x} = \frac{e^x - e^0}{\sin x - \sin 0}$$

apply Cauchy's mean value theorem with $f(x) = e^x$, $g(x) = \sin x$ on interval $[x, 0]$ or $[0, x]$ to deduce that $\exists \theta_x \in (0, 1)$ such that

$$\frac{e^x - 1}{\sin x} = \frac{e^{\theta_x x}}{\cos(\theta_x x)}$$

Now $0 < |\theta_x x| < |x|$ so as $x \to 0$ $\theta_x x \to 0$. Further, because $e^y / \cos y$ is continuous, we have

$$\frac{e^{\theta_x x}}{\cos(\theta_x x)} \to 1$$

as $x \to 0$. Thus

$$\lim_{x \to 0} \frac{e^x - 1}{\sin x} = 1$$

3.3.3 Higher Derivatives and Taylor's Theorem

Suppose $f : (a, b) \to \mathbb{R}$ is differentiable on (a, b). Then we can consider the function

$$f' : (a, b) \to \mathbb{R}, \quad x \mapsto f'(x)$$

If this is differentiable at $x \in (a, b)$ we say f is twice differentiable at x and write

$$(f')'(x) = f''(x) = f^{(2)}(x)$$

We can iterate to define k-times differentiability and write

$$f^{(k)}(x) = \left(f^{(k-1)}\right)'(x)$$

Furthermore, function is said to be *smooth* if it is k-times differentiable on (a, b) for every k. We would like to extend mean value theorem for a function which is more differentiable to incorporate higher derivatives.

Theorem 3.3.7. (*Taylor's Theorem with Lagrange Remainder*) Suppose f and its derivatives to order $n - 1$ are continuous on $[a, a + h]$ and f is n times differentiable on $(a, a + h)$. Then there exists $\theta \in (0, 1)$ such that

$$f(a + h) = f(a) + hf'(a) + \frac{h^2}{2!} f''(a) + \cdots + \frac{h^{n-1}}{(n-1)!} f^{(n-1)}(a) + \frac{h^n}{n!} f^{(n)}(a + \theta h)$$

[4] We will formally define e and sin later.

N.b. for $n = 1$ Theorem 3.3.7 is mean value theorem, so Theorem 3.3.7 is a n^{th} order mean value theorem. We say

$$R_n = \frac{h^n}{n!} f^{(n)}(a + \theta h)$$

is *Lagrange's form of the remainder*.

Also, considering $g(x) = -f(x)$ and applying Theorem 3.3.7 at $x = -a$, we can show the result also holds if $h < 0$, provided conditions hold on $[a+h, a]$, $(a+h, a)$ etc. – which is able to be assured by stating f is n times differentiable on some interval (c, d) with $[a, a + h] \subset (c, d)$ (or $[a + h, a]$).

Proof. (*Method 1*) Observe we can choose $a = 0$ without loss of generality; if we prove the result for $a = 0$, applying it to $g(x) = f(a + x)$ gives general case.

For $0 \leqslant t \leqslant h$ let

$$\phi(t) = f(t) - f(0) - tf'(0) - \cdots - \frac{t^{n-1}}{(n-1)!} f^{(n-1)}(0) - \frac{t^n}{n!} B$$

where we choose B such that $\phi(h) = 0$, i.e.

$$\frac{h^n}{n!} B = f(h) - f(0) - tf'(0) - \cdots - \frac{t^{n-1}}{(n-1)!} f^{(n-1)}(0) \qquad (*)$$

Now repeatedly apply Rolle's theorem (Theorem 3.3.3) to find another expression for B. First observe ϕ and its first $n-1$ derivatives are continuous on $[0, h]$, and $\phi^{(n)}$ exists on $(0, h)$. Also note that $\phi^{(k)}(0) = 0$ for $0 \leqslant k \leqslant n-1$. Then

$$\phi(0) = \phi(h) = 0 \Rightarrow \exists \theta_1 \in (0,1) \text{ such that } \phi'(\theta_1 h) = 0$$

$$\phi'(0) = \phi'(\theta_1 h) = 0 \Rightarrow \exists \theta_2 \in (0,1) \text{ such that } \phi''(\theta_2 \theta_1 h) = 0$$

$$\vdots$$

$$\phi^{(n-1)}(0) = \phi^{(n-1)}(\theta_{n-1} \cdots \theta_1 h) = 0 \Rightarrow \exists \theta_n \in (0,1) \text{ such that } \phi^{(n)}(\theta_n \theta_{n-1} \cdots \theta_1 h) = 0$$

Let $\theta = \theta_1 \theta_2 \cdots \theta_n \in (0,1)$. Then

$$\phi^{(n)}(\theta h) = 0 \Rightarrow f^{(n)}(\theta h) - B = 0$$

i.e. $B = f^{(n)}(\theta h)$ for some $\theta \in (0,1)$. Rearranging equation $(*)$ gives us the desired result. ∎

Proof. (*Method 2*) Again, assume $a = 0$ without loss of generality. This time, for $0 \leqslant t \leqslant h$, let

$$F(t) = f(h) - f(t) - (h-t)f'(t) - \frac{(h-t)^2}{2!} f''(t) - \cdots - \frac{(h-t)^{n-1}}{(n-1)!} f^{(n-1)}(t)$$

F is continuous on $[0, h]$ and differentiable on $(0, h)$, and

$$\begin{aligned} F'(t) &= -f'(t) + f'(t) - (h-t)f''(t) + (h-t)f''(t) - \frac{(h-t)^2}{2!} f^{(3)}(t) + \cdots - \frac{(h-t)^{n-1}}{(n-1)!} f^{(n)}(t) \\ &= -\frac{(h-t)^{n-1}}{(n-1)!} f^{(n)}(t) \end{aligned}$$

Now set

$$\phi(t) = F(t) - \left(\frac{h-t}{h}\right)^p F(0)$$

with $1 \leqslant p \leqslant n$, $p \in \mathbb{N}$. Then $\phi(0) = 0 = \phi(h)$. So by Rolle's theorem there exists $\theta \in (0,1)$ such that $\phi'(\theta h) = 0$. But

$$\phi'(\theta h) = F'(\theta h) + \frac{p(1-\theta)^{p-1}}{h} F(0)$$

Hence

$$\begin{aligned} 0 = &-\frac{h^{n-1}(1-\theta)^{n-1}}{(n-1)!} f^{(n)}(\theta h) \\ &+ \frac{p(1-\theta)^{p-1}}{h}\left(f(h) - f(0) - hf'(0) - \frac{h^2}{2!}f''(0) - \cdots - \frac{h^{n-1}}{(n-1)!}f^{(n-1)}(0)\right) \end{aligned}$$

If $p = n$, we can rearrange to find Taylor's theorem with Lagrange remainder. Otherwise, if $p = 1$, we have proved the *Taylor's theorem with Cauchy remainder*. ■

Theorem 3.3.8. (*Taylor's Theorem with Cauchy Remainder*) With the same hypotheses as Theorem 3.3.7, we have

$$f(a+h) = f(a) + hf'(a) + \cdots + \frac{h^{n-1}}{(n-1)!} f^{(n-1)} f^{(n-1)}(a) + \tilde{R}_n$$

where

$$\tilde{R}_n = \frac{(1-\theta)^{n-1}h^n}{(n-1)!} f^{(n)}(a+\theta h)$$

for some $\theta \in (0,1)$.

Both versions of Taylor's theorem assert that

$$f(h) = P_{n-1}(h) + R_n(h)$$

where

$$P_{n-1}(h) = \sum_{i=0}^{n-1} \frac{h^i}{i!} f^{(i)}(0)$$

the *Taylor polynomial*, and

$$R_n(h) = \begin{cases} \frac{h^n}{n!} f^{(n)}(a+\theta h) & \text{(Lagrange)} \\ \frac{(1-\tilde{\theta})^{n-1}h^n}{(n-1)!} f^{(n)}(a+\tilde{\theta}h) & \text{(Cauchy)} \end{cases}$$

for some $\theta, \tilde{\theta} \in (0,1)$. Finally, be aware that Taylor's theorem does not say

$$f(h) = \sum_{i=0}^{\infty} \frac{h^i}{i!} f^{(i)}(0)$$

where the right hand side is called the *Taylor series*. In fact this is not always true, even if f is smooth and even if the series converges. To show a function is equal to its Taylor series, we need to show $R_n(h) \to 0$ as $n \to \infty$ for fixed h. For example, consider the binomial series $f(x) = (1+x)^r$ where $r \in \mathbb{Q}$. Claim that if $|x| < 1$, then

$$(1+x)^r = 1 + \binom{r}{1}x + \cdots + \binom{r}{n}x^n + \cdots$$

where we define

$$\binom{r}{n} = \frac{r(r-1)\cdots(r-n+1)}{n!}$$

where the series converges absolutely.

Proof. Clearly,

$$f^{(n)}(x) = r(r-1)\cdots(r-n+1)(1+x)^{r-n}$$

By Theorem 3.3.7, for $|x| < 1$ and $n \geqslant r$,

$$(1+x)^r = 1 + \binom{r}{1}x + \cdots + \binom{r}{n-1}x^{n-1} + \binom{r}{n}\frac{x^n}{(1+\theta x)^{n-r}}$$

for some $\theta \in (0,1)$, which can depend on both n and x. But if $x \geqslant 0$, $(1+\theta x)^{n-r} \geqslant 1$ so

$$0 \leqslant \frac{1}{(1+\theta x)^{n-r}} \leqslant 1 \Rightarrow |R_n(x)| = \left|\binom{r}{n}\frac{x^n}{(1+\theta x)^{n-r}}\right| \leqslant \left|\binom{r}{n}x^n\right|$$

Now observe that $\sum_{n\geqslant 0}\binom{r}{n}x^n$ converges absolutely for $|x| < 1$:

$$\left|\frac{a_{n+1}}{a_n}\right| = \left|\frac{r-n}{n+1}\right||x| \to |x| < 1 \quad \text{as } n \to \infty$$

So by ratio test and Theorem 3.1.16, $\sum_{n\geqslant 0}\binom{r}{n}x^n$ converges. This implies

$$\binom{r}{n}x^n \to 0 \quad \text{as } n \to \infty$$

Thus, $R_n(x) \to 0$ as $n \to \infty$ for $x \in [0,1)$.

However, if $-1 < x < 0$, the above approach does not work as $(1+\theta x)^{n-1} < 1$. Instead, we can use Cauchy's remainder

$$R_n = \frac{(1-\theta)^{n-1}x^n}{(n-1)!}r(r-1)\cdots(r-n+1)(1+\theta x)^{r-n} = r\binom{r-1}{n-1}\left(\frac{1-\theta}{1+\theta x}\right)^{n-1}(1+\theta x)^{r-1}x^n$$

for some $\theta \in (0,1)$. But $(1-\theta)/(1+\theta x) < 1$ for all $x \in (-1,1)$ as $1+\theta x = 1-\theta+\theta(x+1) \geqslant 1-\theta$. Hence

$$|R_n| \leqslant r|x|\left|\binom{r-1}{n-1}x^{n-1}\right|(1+\theta x)^{r-1}$$

Moreover, $(1+\theta x)^{r-1} \leqslant \max\{(1-|x|)^{r-1},(1+|x|)^{r-1}\}$, and

$$|R_n| \leqslant r|x|\max\{(1-|x|)^{r-1},(1+|x|)^{r-1}\}\left|\binom{r-1}{n-1}x^{n-1}\right| = K_{r,x}\left|\binom{r-1}{n-1}x^{n-1}\right| \to 0$$

as $n \to \infty$ since $K_{r,x}$ is independent of n. Therefore $R_n \to 0$ as $n \to \infty$ for x fixed in $(-1,1)$. ∎

3.4 Power Series

We want to consider functions defined by power series of the form

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

where $a_n, z, z_0 \in \mathbb{C}$. Obviously the series may not converge for every $z \in \mathbb{C}$. First thing to do is to find out the set of points for which it does converge.[5] By translation, we can assume $z_0 = 0$.

Lemma 3.4.1. If $\sum_{n=0}^{\infty} a_n z^n$ converges, and $|w| < |z|$, then $\sum_{n=0}^{\infty} a_n w^n$ converges absolutely.

Proof. Since $\sum_{n=0}^{\infty} a_n z^n$ converges, $a_n z^n \to 0$. Thus $\exists K > 0$ such that[6]

$$|a_n z^n| \leqslant K \quad \forall n$$

Now consider (note that $z > 0$ to define w)

$$|a_n w^n| = |a_n z^n| \left|\frac{w}{z}\right|^n \leqslant K\rho^n$$

where $\rho = |w/z| < 1$ by assumption. Thus $\sum_{n=0}^{\infty} |a_n w^n|$ converges by comparison to the geometric series $\sum_{n=0}^{\infty} K\rho^n$, which converges. ∎

We now use Lemma 3.4.1 to show every power series has a well-defined *radius of convergence*.

Theorem 3.4.2. Let $\sum_{n=0}^{\infty} a_n z^n$ be a power series. Then there exists $R \in [0, \infty]$, the radius of convergence, such that the series converges absolutely for $|z| < R$ and diverges for $|z| > R$.

Proof. Let

$$A = \left\{ r \geqslant 0 \;\middle|\; \exists z \in \mathbb{C} \text{ with } |z| = r \text{ such that } \sum_{n=0}^{\infty} a_n z^n \text{ converges} \right\}$$

Clearly, $0 \in A$, and A is non-empty. So let

$$R = \sup A$$

with noting that $\sup A = \infty$ meaning A is unbounded above. From definition of A, $\sum a_n z^n$ diverges for $|z| > R$. Suppose $|w| < R$. Then there exists $r \in \mathbb{A}$ with $|w| < r$ so $\exists z \in \mathbb{C}$ with $|z| = r$ and $\sum a_n z^n$ converging. $|w| < |z|$ so by Lemma 3.4.1 $\sum a_n w^n$ converges absolutely. ∎

Note that $R = 0$ means $\sum a_n z^n$ converges only for $z = 0$, and $R = \infty$ means $\sum a_n z^n$ converges absolutely for all $z \in \mathbb{C}$. When $0 < R < \infty$ theorem tells us nothing about convergence for $|z| = R$. Now we introduce a lemma that is useful at finding R:

Lemma 3.4.3. If $|a_{n+1}/a_n| \to l$ as $n \to \infty$, then $R = 1/l$.

[5] Note that set is always non-empty as it contains z_0.

[6] Recall that convergent series is bounded.

Proof. We use ratio test. Consider

$$\lim_{n\to\infty}\left|\frac{a_{n+1}z^{n+1}}{a_n z^n}\right| = \lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right||z| = l|z|$$

so if $l|z| < 1$ we get absolute convergence, and if $l|z| > 1$ we get divergence. ∎

Let's take a look at some examples.

- $\sum_{n=0}^{\infty} z^n/n!$ converges absolutely for all $z \in \mathbb{C}$, since

$$\left|\frac{a_{n+1}}{a_n}\right| = \frac{n!}{(n+1)!} = \frac{1}{n+1} \to 0 = l$$

and $R = \infty$.

- $\sum_{n=0}^{\infty} n!z^n$ converges only for $z = 0$, since $|a_{n+1}/a_n| = n+1 \to \infty$ for $R = 0$.
- $\sum_{n=0}^{\infty} z^n$ geometric series converges if and only if $|z| < 1$.
- $\sum_{n=0}^{\infty} z^n/n^2$ has radius of convergence $R = 1$; specifically, absolute convergence for $|z| \leqslant 1$ and divergence for $|z| > 1$.
- $\sum_{n=0}^{\infty} z^n/n$ has radius of convergence $R = 1$. For $z = 1$, it diverges (harmonic series). For $|z| = 1$, $z \neq 1$, consider

$$\begin{aligned}(1-z)\sum_{n=1}^{N}\frac{z^n}{n} &= \sum_{n=1}^{N}\left(\frac{z^n}{n} - \frac{z^{n+1}}{n}\right)\\ &= \sum_{n=1}^{N}\left(\frac{z^{n+1}}{n+1} - \frac{z^{n+1}}{n}\right) + z - \frac{z^{N+1}}{N+1}\\ &= z - z\sum_{n=1}^{N}\frac{1}{n(n+1)}z^n - \frac{z^{N+1}}{N+1}\end{aligned}$$

If $|z| \leqslant 1$,

$$\sum_{n=1}^{N}\frac{1}{n(n+1)}z^n$$

converges absolutely by comparison to $\sum 1/n(n+1)$, and

$$\left|\frac{z^{N+1}}{N+1}\right| \leqslant \frac{1}{N+1} \to 0$$

Therefore $\sum_{n=0}^{\infty} z^n/n$ converges for $|z| \leqslant 1$, $z \neq 1$.

We conclude that nothing can be said in general about convergence on $|z| = R$, and need to analyse case by case. We shall see that inside the radius of convergence, power series are very well behaved, and "can treated like polynomials."

Theorem 3.4.4. Suppose

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

has radius of convergence $R > 0$. Then f is differentiable at all points z with $|z| < R$, and

$$f'(z) = \sum_{n=1}^{\infty} n a_n z^{n-1}$$

Proof. We start by stating two auxillary lemmas:

Lemma 3.4.5. If $\sum_{n=0}^{\infty} a_n z^n$ has radius of convergence R, then so do $\sum_{n=1}^{\infty} n a_n z^{n-1}$ and $\sum_{n=2}^{\infty} n(n-1) a_n z^{n-2}$

Lemma 3.4.6.

(1) Let $n, r \in \mathbb{N}$. For all $2 \leqslant r \leqslant n$,

$$\binom{n}{r} \leqslant n(n-1)\binom{n-2}{r-2}$$

(2) Let $n \in \mathbb{N}$. For all $z, h \in \mathbb{C}$,

$$|(z+h)^n - z^n - nhz^{n-1}| \leqslant n(n-1)(|z| + |h|)^{n-2}|h|^2$$

Assume, for now, that these results hold. By Lemma 3.4.5, we may define

$$g(z) = \sum_{n=1}^{\infty} n a_n z^{n-1}$$

where $|z| < R$. We need to show

$$I = \frac{f(z+h) - f(z) - hg(z)}{h} \to 0$$

as $h \to 0$. Fix z with $|z| < R$, and assume $|z| + |h| < r < R$ for some r. All sums in I converge by Lemma 3.4.5, and

$$I = \frac{1}{h} \sum_{n=0}^{\infty} a_n [(z+h)^n - z^n - hnz^{n-1}]$$

Then by continuity of absolute value function,

$$\begin{aligned} |I| &= \frac{1}{|h|} \left| \lim_{N \to \infty} \sum_{n=0}^{N} a_n [(z+h)^n - z^n - hnz^{n-1}] \right| \\ &= \lim_{N \to \infty} \underbrace{\frac{1}{|h|} \left| \sum_{n=0}^{N} a_n [(z+h)^n - z^n - hnz^{n-1}] \right|}_{I_N} \end{aligned}$$

Now, using the triangle inequality and Lemma 3.4.6 (2),

$$\begin{aligned} |I_N| &\leqslant \frac{1}{|h|} \sum_{n=0}^{N} |a_n| |(z+h)^n - z^n - hnz^{n-1}| \\ &\leqslant \frac{1}{|h|} \sum_{n=0}^{N} |a_n| |n(n-1)(|z| + |h|)^{n-2}|h|^2| \\ &\leqslant |h| \sum_{n=0}^{N} n(n-1)|a_n| r^{n-2} \\ &\leqslant |h| \sum_{n=0}^{\infty} n(n-1)|a_n| r^{n-2} = |h| A_r \end{aligned}$$

where A_r converges by Lemma 3.4.5 plus the fact that $r < R$. We have shown that

$$|I| = \lim_{N\to\infty} |I_N| \leqslant |h|A_r \to 0$$

as $h \to 0$. ■

Here we proof two auxillary lemmas:

Proof. (Lemma 3.4.5) Suppose $0 < |z| < R$, then $\exists r$ such that $|z| < r < R$. We know $\sum_{n=0}^{\infty} a_n r^n$ converges so $a_n r^n \to 0$ as $n \to \infty$ and hence $\exists K$ such that

$$|a_n r^n| \leqslant K \quad \forall n \geqslant 0$$

Thus

$$|na_n z^{n-1}| = \frac{|a_n r^n|}{|z|} n \left|\frac{z}{r}\right|^n \leqslant \frac{K}{|z|} n\rho^n$$

where K is independent of n and $\rho = |z|/r < 1$. But $\sum_{n=1}^{\infty} n\rho^n$ converges by ratio test:

$$\left|\frac{(n+1)\rho^{n+1}}{n\rho^n}\right| = \rho\left(1 + \frac{1}{n}\right) \to \rho < 1$$

Therefore, $\sum_{n=1}^{\infty} na_n z^{n-1}$ converges absolutely by comparison.

If $|z| > R$, then

$$|na_n z^{n-1}| \geqslant \frac{1}{|z|}|a_n z^n|$$

If $\sum_{n=1}^{\infty} na_n w^{n-1}$ converges for some $|w| > R$, then taking $|w| > |z| > R$ we have $\sum_{n=1}^{\infty} na_n z^{n-1}$ converging absolutely by Lemma 3.4.1. This implies that $\sum a_n z^n$ converges absolutely (by comparison), contradicting R being radius of convergence of $\sum a_n z^n$. Therefore $\sum_{n=1}^{\infty} na_n w^{n-1}$ diverges, and $\sum_{n=1}^{\infty} na_n z^{n-1}$ has radius of convergence R.

For the series $\sum_{n=2}^{\infty} n(n-1)a_n z^{n-2}$, apply result above, starting with $\sum_{n=1}^{\infty} na_n z^{n-1}$. ■

Proof. (Lemma 3.4.6)

(1) Simple manipulation gives

$$\binom{n}{r}\Big/\binom{n-2}{r-2} = \frac{n!}{(n-r)!r!}\frac{(n-r)!(r-2)!}{(n-2)!} = \frac{n(n-1)}{r(r-1)} \geqslant n(n-1)$$

since $r \in \mathbb{N}$, $r \geqslant 2$.

(2) By binomial expansion, (1), and triangle inequality, we have

$$\begin{aligned}
|(z+h)^n - z^n - nhz^{n-1}| &= \left|\sum_{r=2}^{n}\binom{n}{r} z^{n-r}h^r\right| \\
&\leqslant \sum_{r=2}^{n} n(n-1)\binom{n-2}{r-2}|z|^{n-r}|h|^r \\
&= n(n-1)|h|^2\sum_{r=2}^{n}\binom{n-2}{r-2}|z|^{n-r} \\
&= n(n-1)|h|^2(|z|+|h|)^{n-2}
\end{aligned}$$

■

N.b. Theorem 3.4.4 can be iterated: power series are smooth inside the radius of convergence.

3.4.1 The Standard Functions

∗ Exponentials and logarithms

We saw in previous example that $\sum_{n=0}^{\infty} z^n/n!$ has $R = \infty$, i.e. it converges at all $z \in \mathbb{C}$. With this fact, we define the *exponential function* as follows.

Definition 3.4.1. (*Exponential Function*) Let $\exp : \mathbb{C} \to \mathbb{C}$,

$$z \mapsto \exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

We immediately have from Theorem 3.4.4 that exp is differentiable and

$$\exp'(z) = \exp(z)$$

Nextly, we claim $\exp(a+b) = \exp(a)\exp(b)$. To show this, we need the following fact: if $F : \mathbb{C} \to \mathbb{C}$ satisfies $F'(z) = 0$ for all $z \in \mathbb{C}$, then F is constant.[7]

Proof. Consider $g : \mathbb{R} \to \mathbb{C}$, $g(t) = F(tz)$ for some fixed $z \in \mathbb{C}$. By chain rule,

$$g'(t) = zF'(tz) = 0$$

We can write

$$g(t) = u(t) + iv(t)$$

with u, v real, and then

$$g'(t) = u'(t) + iv'(t)$$

giving

$$u'(t) = v'(t) = 0 \Rightarrow u, v \text{ constant}$$

by Corollary 3.3.4.1. Therefore $F(z) = F(0)$ (put $t = 0$ and $t = 1$). But since z is arbitrary, F is constant. ■

Now for $a, b \in \mathbb{C}$ consider

$$F(z) = \exp(a+b-z)\exp(z)$$

We compute

$$F'(z) = -\exp'(a+b-z)\exp(z) + \exp(a+b-z)\exp'(z) = 0$$

to find out that $F(0) = F(b)$. Hence $\exp(a+b)\exp(0) = \exp(a)\exp(b)$, but

$$\exp(0) = \sum_{n=0}^{\infty} \frac{0^n}{n!} = 1$$

Therefore, $\exp(a+b) = \exp(a)\exp(b)$ for all $a, b \in \mathbb{C}$.

From now on we restrict to $\mathbb{R}$.

Theorem 3.4.7. Consider $\exp : \mathbb{R} \to \mathbb{R}$.

(1) exp is everywhere differentiable and $\exp'(x) = \exp(x)$.

[7] Note the difference with Corollary 3.3.4.1 – range is now $\mathbb{C}$.

(2) $\exp(x+y) = \exp(x)\exp(y)$ for all $x, y \in \mathbb{R}$.

(3) $\exp(x) > 0$ for all $x \in \mathbb{R}$.

(4) exp is strictly increasing.

(5) $\exp(x) \to \infty$ as $x \to \infty$; and $\exp \to 0$ as $x \to -\infty$.

(6) $\exp : \mathbb{R} \to (0, \infty)$ is a bijection.

Proof. (1) and (2) are done. We prove the remainings.

(3) If $x > 0$, clearly

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \geqslant 1 > 0$$

Also, $\exp(0) = 1$ and $\exp(x-x) = \exp(x)\exp(-x) = 1$. Thus $\exp(-x) > 0$ for all $x > 0$.

(4) $\exp'(x) = \exp(x) > 0$. Hence exp is strictly increasing by Corollary 3.3.4.1.

(5) $\exp(x) \geqslant 1 + x$ for $x \geqslant 0$ so if $x \to \infty$, $\exp(x) \to \infty$. Meanwhile, for $x \geqslant 0$,

$$\exp(-x) = \frac{1}{\exp(x)}$$

so $\exp(-x) \to 0$ as $x \to \infty$, i.e. $\exp(x) \to 0$ as $x \to -\infty$.

(6) Injectivity is immediate from being strictly increasing. For surjectivity, suppose $y \in (0, \infty)$. Then from (4), there exists $a, b \in \mathbb{R}$ such that

$$\exp(a) < y < \exp(b)$$

Applying intermediate value theorem (Theorem 3.2.6) to $\exp : [a, b] \to \mathbb{R}$ gives $\exists x \in \mathbb{R}$ such that $\exp(x) = y$. Hence exp is surjective.

■

Notice that $\exp : (\mathbb{R}, +) \to ((0, \infty), \times)$ is a group isomorphism. And since exp is a bijection, it has an inverse function

$$\ln : (0, \infty) \to \mathbb{R}$$

which is called the *logarithmic function*.

Theorem 3.4.8.

(1) $\ln : (0, \infty) \to \mathbb{R}$ is a bijection, and

$$\ln(\exp(x)) = x \quad \forall x \in \mathbb{R},$$

$$\exp(\ln(t)) = t \quad \forall t \in (0, \infty)$$

(2) ln is differentiable and monotone, with

$$\ln'(t) = \frac{1}{t}$$

(3) $\ln(st) = \ln(s) + \ln(t)$ where $s, t > 0$.

(4) $\ln(x) \to \infty$ as $x \to \infty$; and $\ln(x) \to -\infty$ as $x \to 0$.

Proof.

(1) Trivial from construction (ln is the inverse of exp).

(2) Inverse function theorem (Theorem 3.3.5) gives that ln is differentiable and

$$\ln'(t) = \frac{1}{\exp'(\ln(t))} = \frac{1}{\exp(\ln t)} = \frac{1}{t}$$

for all $t > 0$.

(3) Because e is an isomorphism, so is its inverse.

■

Now define for $\alpha \in \mathbb{R}$ and $x > 0$,

$$\Gamma_\alpha(x) = \exp(\alpha \ln(x))$$

Theorem 3.4.9. Suppose $x, y > 0$ and $\alpha, \beta \in \mathbb{R}$. Then

(1) $\Gamma_\alpha(x, y) = \Gamma_\alpha(x)\Gamma_\alpha(y)$.

(2) $\Gamma_{\alpha+\beta}(x) = \Gamma_\alpha(x)\Gamma_\beta(x)$.

(3) $\Gamma_\alpha(\Gamma_\beta(x)) = \Gamma_{\alpha\beta}(x)$.

(4) $\Gamma_1(x) = x$, $\Gamma_0(x) = 1$.

Proof.

(1) $\Gamma_\alpha(xy) = \exp(\alpha \ln(xy)) = \exp(\alpha \ln(x) + \alpha \ln(y)) = \exp(\alpha \ln(x)) \exp(\alpha \ln(y)) = \Gamma_\alpha(x)\Gamma_\alpha(y)$.

(2) $\Gamma_{\alpha+\beta}(x) = \exp((\alpha + \beta)\ln(x)) = \exp(\alpha \ln(x) + \beta \ln(x))$
$= \exp(\alpha \ln(x)) \exp(\beta(\ln(x))) = \Gamma_\alpha(x)\Gamma_\beta(x)$.

(3) $\Gamma_\alpha(\Gamma_\beta(x)) = \exp(\alpha \ln(\exp(\beta \ln(x)))) = \exp(\alpha\beta \ln(x)) = \Gamma_{\alpha\beta}(x)$.

(4) $\Gamma_1(x) = \exp(\ln(x)) = x$, $\Gamma_0(x) = \exp(0) = 1$.

■

Now suppose $p, q \in \mathbb{Z}$, $p, q \geqslant 1$. Then,

$$\Gamma_p(x) = \Gamma_{1+1+\cdots+1}(x) = \Gamma_1(x)\Gamma_1(x)\cdots\Gamma_1(x) = x^p$$

and

$$\Gamma_p(x)\Gamma_{-p}(x) = \Gamma_0(x) = 1 \Rightarrow \Gamma_{-p}(x) = \frac{1}{x^p}$$

Further,

$$\left(\Gamma_{1/q}(x)\right)^q = \Gamma_{1/q}(x)\cdots\Gamma_{1/q}(x) = \Gamma_{1/q+\cdots+1/q}(x) = \Gamma_1(x) = x$$

gives $\Gamma_{1/q}(x) = x^{1/q}$. Finally,

$$\Gamma_{p/q}(x) = \Gamma_{\underbrace{1/q + \cdots + 1/q}_{p \text{ times}}}(x) = \left(\Gamma_{1/q}(x)\right)^p = (x^1/q)^p = x^{p/q}$$

. Thus $\Gamma_\alpha(x)$ agrees with x^α for $x \in \mathbb{Q}$ as previously defined. Hence we can extend the definition of x^α into $x \in \mathbb{R}$ and write

$$x^\alpha = \Gamma_\alpha(x)$$

for $\alpha \in \mathbb{R}$, $x \in (0, \infty)$. We also introduce *Euler's number*

$$e = \exp(1) = \sum_{n=1}^{\infty} \frac{1}{n!}$$

and write exp as a power:

$$\exp(x) = \exp(x \ln e) = \Gamma_x(e) = e^x$$

Now we can generalise as follows.

$$(x^\alpha)' = (e^{\alpha \ln x})' = \frac{\alpha}{x} e^{\alpha \ln x} = \alpha x^{\alpha - 1}$$

for all $x > 0$, $\alpha \in \mathbb{R}$. Meanwhile, for $f(x) = a^x$ ($a > 0$, $x \in \mathbb{R}$),

$$f'(x) = (e^{x \ln a})' = e^{x \ln a} \ln a = a^x \ln a$$

In particular, $f'(x) > 0$ for $a > 1$ and $f'(x) < 0$ for $a < 1$.

Lemma 3.4.10. For any $r > 0$ we have

(1) $x^r e^{-x} \to 0$ as $x \to \infty$.

(2) $x^{-r} \ln x \to 0$ as $x \to \infty$.

(3) $x^r \ln x \to 0$ as $x \to 0+$.

Proof.

(1) For $x > 0$,

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots > \frac{x^n}{n!}$$

for any $n \in \mathbb{N}$. Pick n such that $n - r \geqslant 1$. Then,

$$0 \leqslant \frac{x^r}{e^x} \leqslant \frac{n!}{x^{n-r}} \leqslant \frac{n!}{x}$$

so $x^r e^- x \to 0$ as $x \to \infty$.

(2) Pick m such that $m \geqslant 2/r$. For $x > 1$,

$$0 \leqslant \frac{x^{1/r}}{e^x} \leqslant \frac{m!}{x^{m-1/r}} \leqslant \frac{m!}{x^{1/r}}$$

Let $x = \ln y$ and write

$$0 \leqslant \frac{(\ln y)^{1/r}}{r} \leqslant \frac{m!}{(\ln y)^{1/r}}$$

giving

$$0 \leqslant \frac{\ln y}{y^r} \leqslant \frac{(m!)^r}{\ln y}$$

But $\ln y \to \infty$ as $y \to \infty$; thus $\ln y / y^r \to 0$.

(3) Set $z = 1/y$ where y is from above. We have

$$0 \leqslant -z^r \ln z \leqslant \frac{(m!)^r}{-\ln z}$$

Since $\ln z \to -\infty$ as $z \to 0+$, $z^r \ln z \to 0$.

■

∗ Trigonometric functions

Definition 3.4.2. (*Trigonometric Functions*) We define

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k z^{2k}}{(2k)!}$$

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k z^{2k+1}}{(2k+1)!}$$

We can check that, like the exponential function, both series have infinite radius of convergence by ratio test. Hence,

$$\cos' z = -\sin z \text{ and } \sin' z = \cos z$$

by Theorem 3.4.4. Also observe that

$$\begin{aligned} e^{iz} &= \lim_{N\to\infty} \left(\sum_{k=0}^{2N+1} \frac{(iz)^k}{k!} \right) \\ &= \lim_{N\to\infty} \left(\sum_{k=0}^{N} \frac{(iz)^{2k}}{(2k)!} + \sum_{k=0}^{N} \frac{(iz)^{2k+1}}{(2k+1)!} \right) \\ &= \lim_{N\to\infty} \left(\sum_{k=0}^{N} (-1)^k \frac{z^{2k}}{(2k)!} \right) + i \sum_{k=0}^{N} (-1)^k \frac{z^{2k+1}}{(2k+1)!} \\ &= \cos z + i \sin z \end{aligned}$$

Similarly, $e^{-iz} = \cos z - i \sin z$. Hence,

$$\cos z = \frac{1}{2}(e^{iz} + e^{-iz})$$

and

$$\sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$$

These formulae give many trigonometric identities, e.g. $\cos z = \cos(-z)$, $\sin(z) = -\sin(-z)$, $\cos(0) = 1$, $\sin(0) = 0$ etc. Employing $e^{a+b} = e^a e^b$, we also find

$$\sin(z+w) = \sin z \sin w + \cos z \sin w$$

and

$$\cos(z+w) = \cos z \cos w - \sin z \sin w$$

for all $z, w \in \mathbb{C}$. Furthermore, set $w = -z$ to deduce

$$\cos^2 + \sin^2 = \cos(0) = 1 \qquad (*)$$

Now, if $x \in \mathbb{R}$ then $\sin x, \cos x \in \mathbb{R}$ and $(*)$ implies $|\cos x|, |\sin x| \leqslant 1$. N.b. this need not be true away from real axis, e.g. if $y \in \mathbb{R}$,

$$\cos iy = \frac{1}{2}(e^{-y} + e^{y}) \to \infty$$

as $y \to \pm\infty$.

$*$ Periodicity of trigonometric functions

Proposition 3.4.11. There is a smallest positive number ω (where $\sqrt{2} < \omega/2 < \sqrt{3}$) such that

$$\cos\frac{\omega}{2} = 0$$

Proof. Suppose $0 \leqslant x \leqslant 2$.

$$\sin x = \left(x - \frac{x^3}{3!}\right) + \left(\frac{x^5}{5!} - \frac{x^7}{7!}\right) + \cdots + \frac{x^{2n-1}}{(2n-1)!}\left(1 - \frac{x^2}{2n(2n+1)}\right) + \cdots$$

Since each term in parenthesis are positive, $\sin x \geqslant 0$, and if $0 < x \leqslant 2$, $\sin x > 0$. So $\cos' x = -\sin x < 0$ for $0 < x < 2$. Hence $\cos x$ is strictly decreasing in this interval, hence it has at most one root in $[0, 2]$. To complete the proof we show $\cos\sqrt{2} > 0 > \cos\sqrt{3}$, then intermediate valuable theorem implies a root exists in $[\sqrt{2}, \sqrt{3}]$. But

$$\cos\sqrt{2} = 1 - \underbrace{\frac{(\sqrt{2})^2}{2!}}_{=0} + \underbrace{\frac{(\sqrt{2})^4}{4!} - \frac{(\sqrt{2})^6}{6!}}_{>0} + \cdots + \underbrace{\frac{(\sqrt{2})^{2n}}{(2n)!}\left(1 - \frac{2}{(2n+1)(2n+2)}\right)}_{>0} + \cdots$$

so $\cos\sqrt{2} > 0$, and

$$\cos\sqrt{3} = \underbrace{1 - \frac{(\sqrt{3})^2}{2!} + \frac{(\sqrt{3})^4}{4!}}_{-1/8} - \left(\underbrace{\frac{(\sqrt{3})^6}{6!} - \frac{(\sqrt{3})^8}{8!}}_{>0}\right) - \cdots - \frac{(\sqrt{3})^{2n}}{(2n)!}\left(\underbrace{1 - \frac{3}{(2n+1)(2n+2)}}_{>0}\right) - \cdots$$

implies $\cos\sqrt{3}$, completing the proof. ∎

Corollary 3.4.11.1. $\sin\omega/2$=1.

Proof. From

$$\sin^2\frac{\omega}{2} + \cos^2\frac{\omega}{2} = 1$$

we have $\sin^2\omega/2 = 1 \Rightarrow \sin\omega/2 = \pm 1$. But $\omega/2 \in (0, 2)$ so $\sin\omega/2 > 0$. Therefore $\sin\omega/2 = 1$. ∎

Since we established some properties, we now define $\pi = \omega$. Periodic properties of the
trigonometric functions follows.

Theorem 3.4.12.

(1) $\sin(z + \pi/2) = \cos z$; $\cos(z + \pi/2) = -\sin z$.

(2) $\sin(z + \pi) = -\sin z$; $\cos(z + \pi) = -\cos z$.

(3) $\sin(z+2\pi) = \sin z$; $\cos(z+2\pi) = \cos z$.

Proof. (1) Follows from addition formulae plus $\cos(\pi/2) = 0$, $\sin(\pi/2) = 1$. (2) and (3) follow by iterating. ■

It follows that

$$e^{iz+2\pi i} = \cos(z+2\pi) + i\sin(z+2\pi) = \cos z + i\sin z = e^{iz}$$

and hence e^{ω} is periodic with period $2\pi i$. Also

$$e^{i\pi} = \cos\pi + i\sin\pi = -\cos 0 + i(-\sin 0) = -1$$

giving the *Euler's identity*:

$$e^{i\pi} + 1 = 0$$

∗ Trigonometric functions and geometry

Given $\mathbf{x}, \mathbf{y} \in \mathbb{R}^2$, define $\mathbf{x}\cdot\mathbf{y}$ as usual. We set $\|\mathbf{x}\| = \sqrt{\mathbf{x}\cdot\mathbf{x}}$. Cauchy-Schwarz shows that

$$|\mathbf{x}\cdot\mathbf{y}| \leqslant \|\mathbf{x}\|\|\mathbf{y}\|$$

Hence for $\mathbf{x} \neq 0$, $\mathbf{y} \neq 0$,

$$-1 \leqslant \frac{\mathbf{x}\cdot\mathbf{y}}{\|\mathbf{x}\|\|\mathbf{y}\|} \leqslant 1$$

Thus we can define the angle between $\mathbf{x}$ and $\mathbf{y}$ as the unique $\theta \in [0,\pi]$ with

$$\cos\theta = \frac{\mathbf{x}\cdot\mathbf{y}}{\|\mathbf{x}\|\|\mathbf{y}\|}$$

∗ Hyperbolic functions

Definition 3.4.3. (*Hyperbolic Functions*) Define

$$\cosh z = \frac{1}{2}(e^z + e^{-z})$$

$$\sinh z = \frac{1}{2}(e^z - e^{-z})$$

where $z \in \mathbb{C}$.

It follows that

$$\cosh z = \cos(iz) \text{ and } \sinh z = -i\sin(iz)$$

Also,

$$\cosh' z = \sinh z, \quad \sinh' z = \cosh z$$

and

$$\cosh^2 z - \sinh^2 z = 1$$

3.5 Integration

3.5.1 Riemann Integral

Informally, we define

$$\int_a^b f(x)dx$$

as the (signed) area under the graph of $f(x)$. To find the area, we approximate graph from above and below by rectangles. If f is 'nice', estimates from above and below will be close for a suitably fine dissection of $[a,b]$. We assume $f:[a,b]\to\mathbb{R}$ is bounded, i.e. $\exists K$ such that $|f(x)|\leqslant K$ for all $x\in[a,b]$.

Definition 3.5.1. A *dissection* $\mathcal{D}$ of $[a,b]$ is a finite subset of $[a,b]$ containing the end points a, b. We write

$$\mathcal{D}=\{x_0,x_1,\dots,x_n\}$$

with

$$a=x_0<x_1<\cdots<x_n=b$$

Associated to a dissection are the *upper* and *lower sums*, given by

$$U(f,\mathcal{D})=\sum_{j=1}^{n}(x_j-x_{j-1})\sup_{x\in[x_{j-1},x_j]}f(x)$$

and

$$L(f,\mathcal{D})=\sum_{j=1}^{n}(x_j-x_{j-1})\inf_{x\in[x_{j-1},x_j]}f(x)$$

respectively. Clearly, for any dissection, $L(f,\mathcal{D})\leqslant U(f,\mathcal{D})$.

Lemma 3.5.1. Suppose $\mathcal{D}',\mathcal{D}$ are dissections with $\mathcal{D}'\supseteq\mathcal{D}$. Then,

$$L(f,\mathcal{D})\leqslant L(f,\mathcal{D}')\leqslant U(f,\mathcal{D}')\leqslant U(f,\mathcal{D})$$

We say $\mathcal{D}'$ is a refinement of $\mathcal{D}$.

Proof. Let $\mathcal{D}=\{x_0,\dots,x_n\}$ with $x_0<x_1<\cdots<x_n$. First, consider the case where $\mathcal{D}'=\mathcal{D}\cup\{y\}$. Then, $y\in(x_{r-1},x_r)$ for some r. Clearly,

$$\sup_{[x_{r-1},y]}f(x)\leqslant\sup_{[x_{r-1},x_r]}f(x)$$

and

$$\sup_{[y,x_r]}f(x)\leqslant\sup_{[x_{r-1},x_r]}f(x)$$

Combining these,

$$\begin{aligned}(y-x_{r-1})\sup_{[x_{r-1},y]}f(x)+(x_r-y)\sup_{[y,x_r]}f(x)&\leqslant(y-x_{r-1})\sup_{[x_{r-1},x_r]}f(x)+(x_r-y)\sup_{[x_{r-1},x_r]}f(x)\\&=(x_r-x_{r-1})\sup_{[x_{r-1},x_r]}f(x)\end{aligned}$$

Hence $U(f,\mathcal{D}')\leqslant U(f,\mathcal{D})$. Similarly,

$$\inf_{[x_{r-1},y]}f,\ \inf_{[y,x_r]}f\geqslant\inf_{[x_{r-1},x_r]}f$$

and $L(f,\mathcal{D}')\geqslant U(f,\mathcal{D})$. Now if $\mathcal{D}'$ has more extra points, we add them one at a time and use the result recursively. ∎

Lemma 3.5.2. Suppose $\mathcal{D}_1$ and $\mathcal{D}_2$ are two dissections. Then,

$$L(f,\mathcal{D}_1) \leqslant U(f,\mathcal{D}_2)$$

Proof. Since $\mathcal{D}_1 \subseteq \mathcal{D}_1 \cup \mathcal{D}_2$ and $\mathcal{D}_2 \subseteq \mathcal{D}_1 \cup \mathcal{D}_2$, we have, from Lemma 3.5.1,

$$L(f,\mathcal{D}_1) \leqslant L(f,\mathcal{D}_1 \cup \mathcal{D}_2) \leqslant U(f,\mathcal{D}_1 \cup \mathcal{D}_2) \leqslant U(f,\mathcal{D}_2)$$

■

Note that if $\mathcal{D}_0 = \{a,b\}$,

$$L(f,\mathcal{D}_0) = (b-a)\inf_{[a,b]} f \geqslant -(b-a)K$$

and

$$U(f,\mathcal{D}_0) = (b-a)\sup_{[a,b]} f \leqslant (b-a)K$$

Since $\mathcal{D}_0 \subseteq \mathcal{D}$ for any $\mathcal{D}$, we deduce

$$\{U(f,\mathcal{D}) \mid \mathcal{D} \text{ dissections}\}$$

and

$$\{L(f,\mathcal{D}) \mid \mathcal{D} \text{ dissections}\}$$

are bounded above by $(b-a)K$, and below by $-(b-a)K$; and both sets are non-empty. We can define the *upper* and *lower integra*l now.

Definition 3.5.2. The *upper integral* of f is

$$I^*(f) = \overline{\int_a^b} f(x)dx = \inf_{\mathcal{D}} U(f,\mathcal{D})$$

and the *lower integral* of f is

$$I_*(f) = \underline{\int_a^b} f(x)dx = \sup_{\mathcal{D}} L(f,\mathcal{D})$$

Also notice that from Lemma 3.5.2,

$$L(f,\mathcal{D}_1) \leqslant U(f,\mathcal{D}_2) \Rightarrow L(f,\mathcal{D}_1) \leqslant \inf_{\mathcal{D}_2} U(f,\mathcal{D}_2) \Rightarrow \sup_{\mathcal{D}_1} L(f,\mathcal{D}_1) \leqslant \inf_{\mathcal{D}_2} U(f,\mathcal{D}_2) \Rightarrow I_*(f) \leqslant I^*(f)$$

Hence,

$$(b-a)\inf_{[a,b]} f(x) \leqslant I_*(f) \leqslant I^*(f) \leqslant (b-a)\sup_{[a,b]} f(x)$$

Now we formally define the integral as follows.

Definition 3.5.3. A bounded function $f : [a,b] \to \mathbb{R}$ is *Riemann integrable* (integrable) if

$$I^*(f) = I_*(f)$$

Then we define

$$\int_a^b f(x)dx = I^*(f) = I_*(f) = \int_a^b f$$

Example 3.5.1. Consider function $f : [0,1] \to \mathbb{R}$, $x \mapsto x$. Let

$$\mathcal{D}_k = \left\{0, \frac{1}{k}, \ldots, \frac{k-1}{k}, 1\right\}$$

(uniform dissection). Then,

$$U(f, \mathcal{D}_k) = \sum_{j=1}^{k} \left(\frac{j}{k} - \frac{(j-1)}{k}\right) \sup_{\left[\frac{j-1}{k}, \frac{j}{k}\right]} x = \sum_{j=1}^{k} \frac{1}{k}\frac{j}{k} = \frac{1}{k^2}\frac{1}{2}k(k+1) = \frac{1}{2} + \frac{1}{2k}$$

Similarly,

$$L(f, \mathcal{D}_k) = \frac{1}{2} - \frac{1}{2k}$$

Therefore,

$$I^*(f) = \inf_{\mathcal{D}} U(f, \mathcal{D}) \leqslant \inf_{\mathcal{D}_k} U(f, \mathcal{D}_k) = \frac{1}{2}$$

and

$$I_*(f) = \sup \mathcal{D} L(f, \mathcal{D}) \geqslant \sup_{\mathcal{D}_k} L(f, \mathcal{D}_k) = \frac{1}{2}$$

But $I_*(f) \leqslant I^*(f)$ so $I_*(f) = I^*(f) = 1/2$. Thus f is integrable and

$$\int_0^1 x dx = \frac{1}{2}$$

Example 3.5.2. Consider $f : [0,1] \to \mathbb{R}$,

$$x \mapsto \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

This time, f is not Riemann integrable. For any dissection $\mathcal{D}$,

$$U(f, \mathcal{D}) = \sum_{j=1}^{n} (x_j - x_{j-1}) \sup_{[x_{j-1}, x_j]} f = \sum_{j=1}^{n} (x_j - x_{j-1}) = 1$$

and

$$L(f, \mathcal{D}) = \sum_{j=1}^{n} (x_j - x_{j-1}) \inf_{[x_{j-1}, x_j]} f = 0$$

Thus, $I_*(f) \neq I^*(f)$ and f is not Riemann integrable.

Theorem 3.5.3. (*Cauchy Criterion for Integrability*) A bounded function $f : [a,b] \to \mathbb{R}$ is integrable if and only if for all $\epsilon > 0$ there exists a dissection $\mathcal{D}$ with

$$U(f, \mathcal{D}) - L(f, \mathcal{D}) < \epsilon$$

Proof. For any dissection, we have

$$0 \leqslant I^*(f) - I_*(f) \leqslant U(f, \mathcal{D}) - L(f, \mathcal{D}) < \epsilon$$

If the criterion holds, then

$$0 \leqslant I^*(f) - I_*(f) < \epsilon$$

for all $\epsilon > 0$. So $I^*(f) = I_*(f)$ and f is integrable.

Conversely, suppose f is integrable and fix $\epsilon > 0$. It follows from definition of supremum and infimum that there exist $\mathcal{D}_1$, $\mathcal{D}_2$ with

$$U(f, \mathcal{D}_1) \leqslant I^*(f) + \epsilon/2$$

and

$$L(f, \mathcal{D}_2) \geqslant I_*(f) - \epsilon/2$$

Let $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$. Then,

$$U(f, \mathcal{D}) \leqslant U(f, \mathcal{D}_1),$$
$$L(f, \mathcal{D}) \geqslant L(f, \mathcal{D}_2)$$

and we can find

$$\begin{aligned} 0 \leqslant U(f, \mathcal{D}) - L(f, \mathcal{D}) &\leqslant U(f, \mathcal{D}_1) - L(f, \mathcal{D}_2) \\ &\leqslant I^*(f) + \epsilon/2 - I_*(f) + \epsilon/2 = \epsilon \end{aligned}$$

■

This criterion (Theorem 3.5.3) can be used to show monotone functions and continuous functions are integrable.

Observe that if $f : [a, b] \to \mathbb{R}$ is monotone, it is bounded by $f(a)$ and $f(b)$.

Theorem 3.5.4. Suppose $f : [a, b] \to \mathbb{R}$ is monotone. Then f is integrable.

Proof. Suppose f is increasing. Then $\sup_{[x_{j-1}, x_j]} f = f(x_j)$ and $\inf_{[x_{j-1}, x_j]} f = f(x_{j-1})$. Thus for any dissection $\mathcal{D}$,

$$U(f, \mathcal{D}) - L(f, \mathcal{D}) = \sum_{j=1}^{n} (x_j - x_{j-1})[f(x_j) - f(x_{j-1})]$$

Now choose a uniform dissection into n pieces, i.e.

$$\mathcal{D}_n = \left\{ a, a + \frac{(b-a)}{n} + a + \frac{2(b-a)}{n}, \ldots, a + \frac{n-1}{n}(b-a), b \right\}$$

Then,

$$\begin{aligned} U(f, \mathcal{D}_n) - L(f, \mathcal{D}_n) &= \sum_{j=1}^{n} \frac{(b-a)}{n} \left[f\left(a + \frac{j(b-a)}{b} \right) - f\left(a + \frac{(j-1)}{n}(b-a) \right) \right] \\ &= \frac{(b-a)}{n}(f(b) - f(a)) \end{aligned}$$

Taking n sufficiently large, for any $\epsilon > 0$, we can find $\mathcal{D} = \mathcal{D}_n$ such that

$$U(f, \mathcal{D}) - L(f, \mathcal{D}) < \epsilon$$

Hence f is integrable by Theorem 3.5.3. ■

If $f : [a, b] \to \mathbb{R}$ is continuous, then f is bounded by the extreme value theorem (Theorem 3.2.8).

Theorem 3.5.5. Suppose $f : [a, b] \to \mathbb{R}$ is continuous. Then f is integrable.

Proof. We prove the contrapositive, i.e. if f is not integrable, then f is not continuous. Suppose f is not integrable; then by Theorem 3.5.3, there exists $\epsilon_0 > 0$ such that, for all dissections $\mathcal{D}$,

$$U(f,\mathcal{D}) - L(f,\mathcal{D}) > \epsilon_0$$

Since

$$U(f,\mathcal{D}) - L(f,\mathcal{D}) = \sum_{j=1}^{n} (x_j - x_{j-1})[f(x_j) - f(x_{j-1})]$$

it follows that for any dissection there is a j with

$$\sup_{[x_{j-1},x_j]} f - \inf_{[x_{j-1},x_j]} f > \frac{\epsilon_0}{b-a}$$

otherwise

$$U(f,\mathcal{D}) - L(f,\mathcal{D}) \leqslant \sum_{j=1}^{n} (x_j - x_{j-1}) \frac{\epsilon_0}{b-a} = \epsilon_0$$

In particular, we can find $y, z \in [x_{j-1}, x_j]$ with

$$f(y) - f(z) > \frac{\epsilon_0}{b-a}$$

Now let $\mathcal{D}_n$ be the uniform dissection into n equal intervals:

$$\mathcal{D}_n = \left\{ a, a + \frac{(b-a)}{n} + a + \frac{2(b-a)}{n}, \ldots, a + \frac{n-1}{n}(b-a), b \right\}$$

Applying the argument above to $\mathcal{D}_n$, there must exist y_n, z_n in the same subinterval so that $|y_n - z_n| < (b-a)/n$, with

$$f(y_n) - f(z_n) > \frac{\epsilon_0}{b-a}$$

(y_n) is bounded by construction, so by Bolzano-Weierstrass theorem we can take a convergent subsequence $y_{n_k} \to \eta$ for some $\eta \in [a,b]$. Moreover, since

$$|y_{n_k} - z_{n_k}| < \frac{b-a}{n_k} \leqslant \frac{b-a}{k}$$

we have $z_{n_k} \to \eta$ also. But

$$f(y_{n_k}) - f(z_{n_k}) > \frac{\epsilon_0}{b-a} > 0$$

implies $f(y_{n_k})$ and $f(z_{n_k})$ cannot both converges to the same limit. So f is not continuous at η (Theorem 3.2.1). ■

However, a function not being continuous nor monotone does not suggest that function is not integrable. Between monotone and continuous functions, we have a large class of integrable functions, e.g. *Thomae's function*.[8]

[8] Moreover, this function is continuous at each irrational, and discontinuous at each rational.

3.5.2 Elementary Properties of the Integral

Before establishing various properties of the integral, we first give some properties of infimum and supremum.

Lemma 3.5.6. Suppose $I = [a,b]$ and $f, g : I \to \mathbb{R}$ are bounded. Then,

(1) If $f(x) \leqslant g(x)$ for all $x \in I$,

$$\sup_I f \leqslant \sup_I g \text{ and } \inf_I f \leqslant \inf_I g$$

(2) $\sup_I(-f) = -\inf_I f$.

(3) If $\lambda > 0$, then

$$\sup_I(\lambda f) = \lambda \sup_I f \text{ and } \inf_I(\lambda f) = \lambda \inf_I f$$

(4)

$$\sup_I(f+g) \leqslant \sup_I f + \sup_I g$$
$$\inf_I(f+g) \geqslant \inf_I f + \inf_I g$$

(5) $\sup_I |f| - \inf_I |f| \leqslant \sup_I f - \inf_I f$.

(6) $\sup_I f^2 - \inf_I f^2 \leqslant 2\sup_I |f|(\sup_I f - \inf_I f)$.

Proof. We will only prove (4)-(6).

(4) We have $f(x) \leqslant \sup_I f$, $g(x) \leqslant \sup_I g$ for all $x \in I$. Hence

$$f(x) + g(x) \leqslant \sup_I f + \sup_I g \quad \forall x \in I$$

and

$$\sup_I(f+g) \leqslant \sup_I f + \sup_I g$$

Proof is similar for inf.

(5)
- If $f(x) \geqslant 0$ for all x, then $|f| = f$ and

$$\sup_I |f| - \inf_I |f| = \sup_I f - \inf_I f$$

- If $f(x) \leqslant 0$ for all x, then $|f| = -f$ and

$$\sup_I |f| - \inf_I |f| = \sup_I(-f) - \inf_I(-f) = -\inf_I f + \sup_I f$$

by (2).

- If $\inf_I f < 0 < \sup_I f$, then

$$\begin{aligned}\sup_I |f| - \inf_I |f| &= \sup_I |f| = \max\{\sup_I f, \sup_I(-f)\} \\ &\leqslant \sup_I f + \sup_I(-f) \\ &= \sup_I f - \inf_I f\end{aligned}$$

(6) From

$$f(x)^2 - f(y)^2 = (f(x) + f(y))(f(x) - f(y)) \leqslant 2 \sup_I |f| (\sup_I f - \inf_I f)$$

we take supremum over x and y for the result.

■

Corollary 3.5.6.1. For any dissection $\mathcal{D}$ of $[a,b]$, and bounded functions $f, g : [a,b] \to \mathbb{R}$,

(1) If $f(x) \leqslant g(x)$ for all $x \in [a,b]$,

$$U(f,\mathcal{D}) \leqslant U(g,\mathcal{D}) \text{ and } L(f,\mathcal{D}) \leqslant L(g,\mathcal{D})$$

(2) $L(-f,\mathcal{D}) = -U(f,\mathcal{D})$.

(3) If $\lambda > 0$,

$$U(\lambda f,\mathcal{D}) = \lambda U(f,\mathcal{D}) \text{ and } L(\lambda f,\mathcal{D}) = \lambda L(f,\mathcal{D})$$

(4)

$$U(f+g,\mathcal{D}) \leqslant U(f,\mathcal{D}) + U(g,\mathcal{D})$$
$$L(f+g,\mathcal{D}) \leqslant L(f,\mathcal{D}) + L(g,\mathcal{D})$$

(5) $U(|f|,\mathcal{D}) - L(|f|,\mathcal{D}) \leqslant U(f,\mathcal{D}) - L(f,\mathcal{D})$.

(6) $U(f^2,\mathcal{D}) - L(f^2,\mathcal{D}) \leqslant 2\sup_{[a,b]} |f| (U(f,\mathcal{D}) - L(f,\mathcal{D}))$.

Proof. Recall the definition of upper/lower sum and results follow from Lemma 3.5.6. For (6) we additionally need that

$$\sup_{[x_{j-1},x_j]} |f| \leqslant \sup_{[a,b]} |f|$$

■

Theorem 3.5.7. Let f, g be bounded and integrable on $[a,b]$. Then,

(1) If $f(x) \leqslant g(x)$ for all $x \in [a,b]$,

$$\int_a^b f(x)dx \leqslant \int_a^b g(x)dx$$

(2) If $\lambda \in \mathbb{R}$, λf is integrable, and

$$\int_a^b \lambda f(x)dx = \lambda \int_a^b f(x)dx$$

(3) $f + g$ is integrable, and

$$\int_a^b (f+g)(x)dx = \int_a^b f(x)dx + \int_a^b g(x)dx$$

(4) $|f|$ is integrable, and
$$\left|\int_a^b f(x)dx\right| \leqslant \int_a^b |f(x)|dx$$

(5) The product fg is integrable.

Proof.

(1) For any dissection $\mathcal{D}$, we have
$$L(f,\mathcal{D}) \leqslant L(g,\mathcal{D}) \leqslant I_*(g)$$
Hence $I_*(f) \leqslant I_*(g)$. But f, g integrable, so
$$\int_a^b f(x)dx \leqslant \int_a^b g(x)dx$$

(2) First consider $\lambda > 0$. Since f is integrable, $\forall \epsilon > 0$, $\exists \mathcal{D}$ such that
$$U(f,\mathcal{D}) \leqslant \int_a^b f(x)dx + \epsilon, \quad L(f,\mathcal{D}) \geqslant \int_a^b f(x)dx - \epsilon$$
Then, by Corollary 3.5.6.1 (3),
$$\begin{aligned}\lambda \int_a^b f(x)dx - \lambda\epsilon \leqslant \lambda L(f,\mathcal{D}) = L(\lambda f,\mathcal{D}) \leqslant I_*(\lambda f)\\ \leqslant I^*(\lambda f) \leqslant U(\lambda f,\mathcal{D}) = \lambda U(f,\mathcal{D}) \leqslant \lambda \int_a^b f(x)dx + \lambda\epsilon\end{aligned}$$
But ϵ is arbitrary so
$$I_*(\lambda f) = I^*(\lambda f) = \lambda \int_a^b f(x)dx$$
Now consider $\lambda = -1$, $\mathcal{D}$ as above. Then,
$$\int_a^b f(x)dx - \epsilon \leqslant L(f,\mathcal{D}) = -U(-f,\mathcal{D})$$
and
$$\int_a^b f(x)dx + \epsilon \geqslant U(f,\mathcal{D}) = -L(-f,\mathcal{D})$$
Therefore
$$-\int_a^b f(x)dx - \epsilon \leqslant L(-f,\mathcal{D}) \leqslant I_*(-f) \leqslant I^*(-f) \leqslant U(-f,\mathcal{D}) \leqslant -\int_a^b f(x)dx + \epsilon$$
and
$$I_*(-f) = I^*(-f) = -\int_a^b f(x)dx$$
since ϵ arbitrary. And we can combine the two results above to get desired for all $\lambda \in \mathbb{R}$.

(3) Since f, g integrable, $\forall \epsilon > 0$ there exist $\mathcal{D}_1, \mathcal{D}_2$ such that

$$\int_a^b f(x)dx - \epsilon \leqslant L(f, \mathcal{D}_1) \leqslant U(f, \mathcal{D}_1) \leqslant \int_a^b f(x)dx + \epsilon$$

$$\int_a^b g(x)dx - \epsilon \leqslant L(g, \mathcal{D}_2) \leqslant U(g, \mathcal{D}_2) \leqslant \int_a^b g(x)dx + \epsilon$$

Now let $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$. Then, by Corollary 3.5.6.1 (4),

$$\begin{aligned} \int_a^b f(x)dx + \int_a^b g(x)dx - 2\epsilon &\leqslant L(f, \mathcal{D}_1) + L(g, \mathcal{D}_2) \\ &\leqslant L(f, \mathcal{D}) + L(g, \mathcal{D}) \\ &\leqslant L(f + g, \mathcal{D}) \end{aligned}$$

Similarly,

$$\begin{aligned} \int_a^b f(x)dx + \int_a^b g(x)dx + 2\epsilon &\geqslant U(f, \mathcal{D}_1) + U(g, \mathcal{D}_2) \\ &\geqslant U(f, \mathcal{D}) + U(g, \mathcal{D}) \\ &\geqslant U(f + g, \mathcal{D}) \end{aligned}$$

Combining two, we obtain

$$\int_a^b f(x)dx + \int_a^b g(x)dx - 2\epsilon \leqslant I_*(f+g) \leqslant I^*(f+g) \leqslant \int_a^b f(x)dx + \int_a^b g(x)dx + 2\epsilon$$

Since ϵ arbitrary, $f + g$ is integrable and

$$\int_a^b f(x)dx + \int_a^b g(x)dx = \int_a^b (f + g)(x)dx$$

(4) By Theorem 3.5.3 and Corollary 3.5.6.1 (5), $\forall \epsilon > 0$ $\exists \mathcal{D}$ such that

$$\epsilon > U(f, \mathcal{D}) - L(f, \mathcal{D}) \geqslant U(|f|, \mathcal{D}) - L(|f|, \mathcal{D})$$

We immediately see that $|f|$ is integrable by Theorem 3.5.3. Also,

$$-|f(x)| \leqslant f(x) \leqslant |f(x)| \quad \forall x$$

so by (1),

$$-\int_a^b |f(x)|dx \leqslant \int_a^b f(x)dx \leqslant \int_a^b |f(x)|dx$$

(5) Noting

$$fg = \frac{1}{4}\left[(f+g)^2 - (f-g)^2\right] \tag{†}$$

it is sufficient to show f^2 is integrable. Suppose $|f(x)| \leqslant K$ $\forall x \in [a, b]$. Then given $\epsilon > 0$, there exists $\mathcal{D}$ such that

$$U(f, \mathcal{D}) - L(f, \mathcal{D}) < \frac{\epsilon}{2K}$$

By Corollary 3.5.6.1 (6),

$$U(f^2,\mathcal{D}) - L(f^2,\mathcal{D}) \leqslant 2\sup_{[a,b]}|f|(U(f,\mathcal{D}) - L(f,\mathcal{D})) < \epsilon$$

Hence f^2 is integrable, and consequently fg is integrable by (†).

■

Theorem 3.5.8. (*Additivity of the Integral*) Suppose $f : [a,b] \to \mathbb{R}$ and let $c \in (a,b)$. Then f is integrable if and only if $f|_{[a,c]}$ and $f|_{[c,b]}$ are integrable, and

$$\int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx$$

Proof. First, suppose $f : [a,b] \to \mathbb{R}$ is integrable. Let $\epsilon > 0$. By Theorem 3.5.3, $\exists\mathcal{D}$, a dissection of $[a,b]$, such that

$$U(f,\mathcal{D}) - L(f,\mathcal{D}) < \epsilon$$

By considering $\mathcal{D} \cup \{c\}$ if necessary, we can assume $\mathcal{D} = \{x_0,\dots,x_n\}$ and $x_l = c$ for some l. Let $\mathcal{D}_L = \{x_0,\dots,x_l\}$ and $\mathcal{D}_R = \{x_l,\dots,x_n\}$, which are dissections of $[a,c]$ and $[c,b]$ respectively. Then, from

$$L(f,\mathcal{D}) = L(f|_{[a,c]},\mathcal{D}_L) + L(f|_{[c,b]},\mathcal{D}_R)$$

$$U(f,\mathcal{D}) = U(f|_{[a,c]},\mathcal{D}_L) + U(f|_{[c,b]},\mathcal{D}_R)$$

we have

$$\Big[U(f|_{[a,c]},\mathcal{D}_R) - L(f|_{[a,c]},\mathcal{D}_R)\Big] + \Big[U(f|_{[c,b]},\mathcal{D}_R) - L(f|_{[c,b]},\mathcal{D}_R)\Big] < \epsilon$$

Both terms in square brackets are non-negative, so

$$U(f|_{[a,c]},\mathcal{D}_R) - L(f|_{[a,c]},\mathcal{D}_R) < \epsilon$$

and

$$U(f|_{[c,b]},\mathcal{D}_R) - L(f|_{[c,b]},\mathcal{D}_R) < \epsilon$$

Therefore $f|_{[a,c]}$ and $f|_{[c,b]}$ are integrable.

Conversely, suppose $f|_{[a,c]}$ and $f|_{[c,b]}$ are integrable. Theorem 3.5.3 says that $\exists\mathcal{D}_L,\mathcal{D}_R$ such that

$$U(f|_{[a,c]},\mathcal{D}_R) - L(f|_{[a,c]},\mathcal{D}_R) < \epsilon$$

$$U(f|_{[c,b]},\mathcal{D}_R) - L(f|_{[c,b]},\mathcal{D}_R) < \epsilon$$

But if we let $\mathcal{D} = \mathcal{D}_L \cup \mathcal{D}_R$, we have

$$U(f,\mathcal{D}) - L(f,\mathcal{D}) < 2\epsilon$$

Hence f is integrable.

Finally, we deduce that

$$\int_a^b f(x)dx \geqslant L(f,\mathcal{D}) = L(f|_{[a,c]},\mathcal{D}_L) + L(f|_{[c,b]},\mathcal{D}_R) \geqslant \int_a^c f(x)dx - \epsilon + \int_c^b f(x)dx - \epsilon$$

Similarly,

$$\int_a^b f(x)dx \leqslant U(f,\mathcal{D}) = U(f|_{[a,c]},\mathcal{D}_L)+U(f|_{[c,b]},\mathcal{D}_R) \leqslant \int_a^c f(x)dx+\epsilon+\int_c^b f(x)dx+\epsilon$$

Therefore,

$$\left|\int_a^b f(x)dx - \int_a^c f(x)dx - \int_c^b f(x)dx\right| \leqslant 2\epsilon$$

for arbitrary ϵ, completing the proof. ■

Finally, we introduce a convention that if $a > b$,

$$\int_a^b f(x)dx = -\int_b^a f(x)dx$$

and if $a = b$

$$\int_a^a f = 0$$

With this convention, it follows that if $|f| \leqslant K$,

$$\left|\int_a^b f(x)dx\right| \leqslant K|b-a|$$

3.5.3 Piecewise Continuous Functions

Definition 3.5.4. A bounded function $f : [a,b] \to \mathbb{R}$ is *piecewise continuous* if ther exists a dissection $\mathcal{D}$ of $[a,b]$ such that for each $i = 1,2,\ldots,n$, if we define $f_i : (x_{i-1},x_i) \to \mathbb{R}$, $x \mapsto f(x)$, then f_i is continuous and has a limit as $x \to x_{i-1}$ and $x \to x_i$. I.e. the function $\bar{f}_i : [x_{i-1},x_i] \to \mathbb{R}$ given by

$$\bar{f}_i(x) = \begin{cases} \lim_{x\to x_{i-1}} f_i(x) & x = x_{i-1} \\ f_i(x) & x \in (x_{i-1},x_i) \\ \lim_{x\to x_i} f_i(x) & x = x_{i+1} \end{cases}$$

is continuous (hence integrable).

Consequently, from the observation obove, together with Theorem 3.5.8, piecewise continuous function is integrable. Furthermore,[9] if $f : [a,b] \to \mathbb{R}$ is integrable, and $g : [a,b] \to \mathbb{R}$ is bounded, with $g(x) = f(x)\ \forall x \in [a,b]\backslash\{y_1,\ldots,y_N\}$, then g is integrable and

$$\int_a^b f(x)dx = \int_a^b g(x)dx$$

3.5.4 The Fundamental Theorem of Calculus

Suppose $f : [a,b] \to \mathbb{R}$ is integrable (hence bounded). Let

$$F(x) = \int_a^x f(t)dt$$

for $x \in [a,b]$.

[9] Left as an exercise.

Theorem 3.5.9. F is continuous.

Proof. Suppose $|f| \leqslant K$ and assume $x, x+h \in [a,b]$. Then

$$F(x+h) - F(x) = \int_x^{x+h} f(t)dt$$

gives

$$|F(x+h) - F(x)| = \left| \int_x^{x+h} f(t)dt \right| \leqslant K|h| \to 0$$

as $h \to 0$. Therefore, $\lim_{h\to 0}(F(x+h) - F(x)) = 0 \Rightarrow \lim_{h\to 0} F(x+h) = F(x)$ and F is continuous. ■

Theorem 3.5.10. (*Fundamental Theorem of Calculus I*, FTC 1) If in addition f is continuous at x, then F is differentiable at x, and

$$F'(x) = f(x)$$

Proof. We need to estimate

$$\left| \frac{F(x+h) - F(x)}{h} - f(x) \right| = \left| \frac{1}{h} \int_x^{x+h} f(t)dt - f(x) \right| = \frac{1}{|h|} \left| \int_x^{x+h} (f(t) - f(x))dt \right|$$

Now, given $\epsilon > 0$ $\exists \delta > 0$ such that

$$|t - x| < \delta \Rightarrow |f(t) - f(x)| < \epsilon$$

since f is continuous. Suppose $|h| < \delta$. Then $|f(t) - f(x)| < \epsilon$ for all t between x and $x+h$. Therefore,

$$\left| \frac{F(x+h) - F(x)}{h} - f(x) \right| \leqslant \frac{1}{|h|} \epsilon |h| = \epsilon$$

i.e.

$$\lim_{h\to 0} \frac{F(x+h) - F(x)}{h} = f(x)$$

■

Note that for Theorem 3.5.10 to hold, the condition f is continuous is necessary. For instance, consider

$$f(x) = \begin{cases} -1 & x \in [-1, 0] \\ 1 & x \in (0, 1] \end{cases}$$

Although f is montone and thus integrable,

$$F(x) = \begin{cases} -x - 1 & x \leqslant 0 \\ x - 1 & x \geqslant 0 \end{cases}$$

i.e. $F(x) = -1 + |x|$ is not differentiable at $x = 0$.

Corollary 3.5.10.1. (*Integration is Inverse of Differentiation*) If $f = g'$ is continuous on $[a,b]$, then

$$F(x) = \int_a^x f(t)dt = g(x) - g(a)$$

Proof. $F - g$ has zero derivative on $[a,b]$ by Theorem 3.5.10, and $F(a) = 0$. Hence $(F-g)(a) = -g(a)$. So by Corollary 3.3.4.1,

$$(F-g)(x) = -g(a) \quad \forall x$$

and $F(x) = g(x) - g(a)$. ■

Note that all continuous functions have an *indefinite integral*, or *anti-derivative*:

$$\int f(x)dx = \int_a^x f(t)dt$$

where a arbitrary.

Theorem 3.5.11. (*Fundamental Theorem of Calculus II*, FTC 2) Suppose that $f : [a,b] \to \mathbb{R}$ is continuous on $[a,b]$, differentiable on (a,b) and that f' is integrable. Then

$$\int_a^b f'(x)dx = f(b) - f(a)$$

N.b. Theorem 3.5.11 is stronger than Corollary 3.5.10.1 since it does not require f' from Theorem 3.5.11 to be continuous.

Proof. Let $\mathcal{D}$ be any dissection of $[a,b]$. Applying the mean value theorem (Theorem 3.3.4) to f on $[x_{j-1}, x_j]$, $\exists \xi_j \in (x_{j-1}, x_j)$ such that

$$f'(\xi_j)(x_j - x_{j-1}) = f(x_j) - f(x_{j-1})$$

This gives

$$\sum_{j=1}^{n} f'(\xi_j)(x_j - x_{j-1}) = f(b) - f(a)$$

But

$$\sum_{j=1}^{n}(x_j - x_{j-1}) \inf_{[x_{j-1},x_j]} f' \leqslant \sum_{j=1}^{n}(x_j - x_{j-1})f'(\xi_j) \leqslant \sum_{j=1}^{n}(x_j - x_{j-1}) \sup_{[x_{j-1},x_j]} f'$$

So

$$L(f', \mathcal{D}) \leqslant f(b) - f(a) \leqslant U(f', \mathcal{D}) \Rightarrow I_*(f') \leqslant f(b) - f(a) \leqslant I^*(f')$$

But because f' is integrable,

$$I_*(f') = I^*(f') = \int_a^b f'(x)dx = f(b) - f(a)$$

■

Following are the important corollarys of fundamental theorem of calculus.

Corollary 3.5.11.1. (*Integration by Parts*) Suppose f' and g' exist and are continuous on $[a,b]$. Then

$$\int_a^b f'(x)g(x)dx = f(b)g(b) - f(a)g(a) - \int_a^b f(x)g'(x)dx$$

Proof. By the product rule and Corollary 3.5.10.1,

$$\begin{aligned}\int_a^b f'(x)g(x)dx &= \int_a^b ((fg)'(x) - f(x)g'(x))dx = \int_a^b (fg)'(x)dx - \int_a^b f(x)g'(x)dx \\ &= f(b)g(b) - f(a)g(a) - \int_a^b f(x)g'(x)dx\end{aligned}$$

■

Corollary 3.5.11.2. (*Integration by Substitution*) Let $g : [\alpha, \beta] \to [a, b]$ with $g(\alpha) = a$, $g(\beta) = b$ and suppose g' exists and is continuous on $[\alpha, \beta]$. Let $f : [a, b] \to \mathbb{R}$ be continuous. Then

$$\int_a^b f(x)dx = \int_\alpha^\beta f(g(t))g'(t)dt$$

Proof. Set $F(x) = \int_a^x f(t)dt$ as before. Let $h(t) = F(g(t))$ which is well defined for $t \in [\alpha, \beta]$ as g takes value in $[a, b]$. Then,

$$\begin{aligned}\int_\alpha^\beta f(g(t))g'(t)dt &= \int_\alpha^\beta F'(g(t))g'(t)dt \\ &= \int_\alpha^\beta h'(t)dt \\ &= h(\beta) - h(\alpha) \\ &= F(g(\beta)) - F(g(\alpha)) \\ &= F(b) - F(a) = \int_a^b f(t)dt\end{aligned}$$

■

Theorem 3.5.12. (*Taylor's Theorem with Integral Remainder*) Suppose f and its first n derivatives exist, and are continuous for $x \in [0, h]$. Then,

$$f(h) = f(0) + hf'(0) + \cdots + \frac{h^{n-1}f^{(n-1)}(0)}{(n-1)!} + R_n$$

where

$$R_n = \frac{h^n}{(n-1)!}\int_0^1 (1-t)^{n-1}f^{(n)}(th)dt$$

Proof. By Theorem 3.5.11,

$$\begin{aligned}f(h) &= f(0) + \int_0^h f'(u)du \\ &= f(0) - \left[(h-u)f'(u)\right]_0^h + \int_0^h (h-u)f''(u)du \\ &= f(0) + hf'(0) + \int_0^h \left(-\frac{d}{du}\frac{(h-u)^2}{2}\right)f''(u)du\end{aligned}$$

Keep integrating by parts to get

$$f(h) = f(0) + hf'(0) + \cdots + \frac{h^{n-1}f^{(n-1)}(0)}{(n-1)!} + \underbrace{\int_0^h \frac{(h-u)^{n-1}}{(n-1)!} f^{(n)}(u)du}_{R_n}$$

Substitution $u = th$ gives the desired

$$R_n = \frac{h^n}{(n-1)!}\int_0^1 (1-t)^{n-1} f^{(n)}(th)dt$$

■

Remark 3.5.1. Note we assume $f^{(n)}$ is continuous but in previous versions of the Taylor's theorem we just assumed $f^{(n)}$ exists. If we make this additional assumption, we can recover Cauchy and Lagrange form of remainder.

Theorem 3.5.13. Suppose $f, g : [a,b] \to \mathbb{R}$ are continuous and $g(x) \neq 0$ for all $x \in (a,b)$. Then $\exists c \in (a,b)$ such that

$$\int_a^b f(x)g(x)dx = f(c)\int_a^b g(x)dx$$

N.b. if $g(x) = 1$, we get $\int_a^b f(x)dx = f(c)(b-a)$.

Proof. Apply Cauchy's mean value theorem (Theorem 3.3.6) to

$$F(x) = \int_a^x (fg)(x)dx \text{ and } G(x) = \int_a^x g(x)dx$$

to deduce that there exists $c \in (a,b)$ such that

$$(F(b)-F(a))G'(c) = F'(c)(G(b)-G(a)) \Rightarrow \left(\int_a^b (fg)(x)dx\right) g(c) = f(c)g(c)\int_a^b g(x)dx$$

$g(c) \neq 0$ so we can cancel out $g(c)$ to obtain the desired result. ■

Now consider

$$R_n = \frac{h^n}{(n-1)!}\int_0^1 (1-t)^{n-1} f^{(n)}(th)dt$$

To obtain the Cauchy remainder, apply Theorem 3.5.13 with $\tilde{g} = 1$ and $\tilde{f}(t) = (1-t)^{n-1}f^{(n)}(th)$ to get $\exists \theta \in (0,1)$ such that

$$\int_0^1 \tilde{f}(t)dt = \tilde{f}(\theta) \Rightarrow R_n = \frac{h^n}{(n-1)!}(1-\theta)^{n-1}f^{(n)}(\theta h)$$

Alternatively, split integrands as

$$\underbrace{\left((1-t)^{n-1}\right)}_{\tilde{g}}\underbrace{\left(f^{(n)}(th)\right)}_{\tilde{f}}$$

to find

$$\int_0^1 (1-t)^{n-1} f^{(n)}(th)dt = f^{(n)}(\theta h)\int_0^1 (1-t)^{n-1}dt$$

for some $\theta \in (0,1)$, by theorem 3.5.13. But $\int_0^1 (1-t)^{n-1}dt = 1/n$, so we obtain the Lagrange remainder

$$R_n = \frac{h^n}{n!} f^{(n)}(\theta h)$$

Finally, we will point out that it is necessary to include the assumption that f' is integrable in the hypotheses of Theorem 3.5.11. For example, consider $f : [-1,1] \to \mathbb{R}$, given by

$$f(x) = \begin{cases} |x|^{3/2} \sin \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

satisfies that f is continuous on $[-1,1]$, differentiable on $(-1,1)$, but f' is unbounded hence not integrable.

3.5.5 Improper Integrals

The theory of integration we have developed so far applies to bounded functions defined on bounded intervals. For a full treatment for functions whose domain or image is unbounded, we have to wait for the Lebesgue integral.[10] Note that content of this subsection, Riemann integral, is a partial resolution.

∗ Integrals on an infinite domain

Suppose $f : [a,\infty) \to \mathbb{R}$ is integrable on each interval $[a,R]$ $(R > a)$ and

$$\int_a^R f(x)dx \to l$$

as $R \to \infty$. Then we say $\int_a^\infty f(x)dx$ exists, or converges, and

$$\int_a^\infty f(x)dx = l$$

Otherwise, if $\int_a^R f(x)dx$ has no limit, we say $\int_a^\infty f(x)dx$ *diverges*. A similar definition applies to $\int_{-\infty}^a f(x)dx$ for $f : (-\infty, a] \to \mathbb{R}$.

Furthermore, if $\int_{-\infty}^a f(x)dx = l_1$ and $\int_a^\infty f(x)dx = l_2$ we say $\int_{-\infty}^\infty f(x)dx$ exists, and

$$\int_{-\infty}^\infty f(x)dx = \int_{-\infty}^a f(x)dx + \int_a^\infty f(x)dx$$

independent of a.[11] Be careful that this is not the same as

$$\int_{-R}^R f(x)dx$$

converging. For instance, $\int_{-R}^R xdx = 0$ but $\int_0^\infty xdx$ does not converge.

[10] See Probability and Measure, Part II.
[11] This needs check.

∗ Integrands with an isolated singularity

Suppose $f : (b, c] \to \mathbb{R}$ is integrable on each $[b + \delta, c]$ for $0 < \delta < c - b$. Then if

$$\int_{b+\delta}^{c} f(x)dx \to l$$

as $\delta \to 0$, we say $\int_b^c f(x)dx$ exists or converges and equals l; and it is similarly defined for $f : [a, b) \to \mathbb{R}$ integrable on $[a, b - \delta]$ $(0 < \delta < b - a)$.

If $f : [a, c]\backslash\{b\} \to \mathbb{R}$ and

$$\int_a^b f(x)dx, \quad \int_b^c f(x)dx$$

exist, we say $\int_a^c f(x)dx$ exists, and

$$\int_a^c f(x)dx = \int_a^b f(x)dx + \int_b^c f(x)dx$$

∗ Properties and examples of improper integral

For example,

$$\int_1^\infty \frac{dx}{x^k}$$

converges if and only if $k > 1$, and

$$\int_0^1 \frac{dx}{x^k}$$

converges if and only if $k < 1$, since $(k \neq 1)$

$$\int_0^R \frac{dx}{x^k} = \left[\frac{x^{1-k}}{1-k}\right]_1^R = \frac{R^{1-k} - 1}{1-k}$$

- converges as $R \to \infty$ if $1 - k < 0$, not if $1 - k > 0$;
- converges as $R \to 0$ if $1 - k > 0$, not if $1 - k < 0$;

and because if $k = 1$,

$$\int_1^R \frac{dx}{x} = [\ln x]_1^R = \ln R$$

does not converge as $R \to \infty$ or $R \to 0$.

Lemma 3.5.14. Suppose $f, g : [a, \infty) \to \mathbb{R}$ are integrable on each $[a, R]$, $R > a$. If $0 \leqslant f(x) \leqslant g(x)$ for all $x \geqslant a$, then

$$\int_a^\infty g(x)dx \text{ converges } \Rightarrow \int_a^\infty f(x)dx \text{ converges}$$

Proof. Note that

$$R \mapsto \int_a^R f(x)dx$$

is increasing as $f(x) \geqslant 0$, and

$$\int_a^R f(x)dx \leqslant \int_a^R g(x)dx \leqslant \int_a^\infty g(x)dx$$

Hence $R \mapsto \int_a^R f(x)dx$ is increasing and bounded above. Let

$$l = \sup_{R \geqslant a} \int_a^R f(x)dx$$

and claim

$$l = \lim_{R \to \infty} \int_a^R f(x)dx$$

To see this, let $\epsilon > 0$. Then from definition of supremum, $\exists R_0$ such that

$$\int_a^{R_0} f(x)dx \geqslant l - \epsilon$$

So if $R \geqslant R_0$,

$$l - \epsilon \leqslant \int_a^{R_0} f(x)dx \leqslant \int_a^R f(x)dx \leqslant l$$

■

Example 3.5.3. Consider

$$\int_0^\infty e^{-x^2/2}dx$$

For $x > 1$, $e^{-x^2/2} \leqslant e^{-x/2}$, and

$$\int_1^R e^{-x/2}dx = 2(e^{-1/2} - e^{-R/2}) \to 2e^{-1/2}$$

as $R \to \infty$. Hence $\int_1^\infty e^{-x^2/2}dx$ converges, and therefore

$$\int_0^\infty e^{-x^2/2}dx$$

converges because from

$$\int_0^R e^{-x^2/2}dx = \int_0^1 e^{-x^2/2}dx + \int_1^R e^{-x^2/2}dx$$

left hand side converges as $R \to \infty$ if and only if $\int_1^R e^{-x^2/2}dx$ does.

However, be careful that, unlike the situation with series,

$$\int_0^\infty f(x)dx \text{ converges } \not\Rightarrow f(x) \to 0 \text{ as } x \to \infty$$

∗ Integral test

Theorem 3.5.15. (*Integral Test*) Suppose $f : [1, \infty) \to \mathbb{R}$ is positive and decreasing. Then,

(1) the integral $\int_1^\infty f(x)dx$ converges if and only if the sum $\sum_{n=1}^\infty f(n)$ converges.

(2) as $n \to \infty$,
$$\sum_{r=1}^{n} f(r) - \int_1^n f(x)dx \to l$$
for some l with $0 \leqslant l \leqslant f(1)$.

Note that (2) of Theorem 3.5.15 implies (1) of that. Also f decreasing from the hypotheses of that implies f integrable on $[1, R]$ $(R > 1)$ by Theorem 3.5.4.

Proof. If $n - 1 \leqslant x \leqslant n$,
$$f(n-1) \geqslant f(x) \geqslant f(n) \Rightarrow f(n-1) \geqslant \int_{n-1}^n f(x)dx \geqslant f(n)$$
Adding, we have
$$\sum_{r=1}^{n-1} f(r) \geqslant \int_1^n f(x)dx \geqslant \sum_{r=2}^{n} f(r)$$
From here, claim (1) is clear since $\int_1^R f(x)dx$ is monotonically increasing, as is $\sum_{r=1}^n f(r)$.

Let
$$\phi(n) = \sum_{r=1}^{n} f(r) - \int_1^n f(x)dx$$
Then,
$$\phi(n) - \phi(n-1) = f(n) - \int_{n-1}^n f(x)dx \leqslant 0$$
and
$$\phi(n) = f(n) + \sum_{r=1}^{n-1} f(r) - \int_1^n f(x)dx \geqslant f(n) \geqslant 0$$
So $\phi(n)$ is decreasing and bounded below. Hence, from monotone convergence theorem, $\phi(n) \to l$ with $0 \leqslant l \leqslant \phi(1) = f(1)$. ■

Example 3.5.4.

(1) $\sum_{n=1}^\infty 1/n^k$ converges if $k > 1$. We saw $\int_1^\infty (dx/x^k)$ converges if $k > 1$. So integral test gives result.

(2) Consider
$$\sum_{n=2}^{\infty} \frac{1}{n \ln n}$$
Let $f(x) = 1/x \ln x$ for $x \geqslant 2$. Then,
$$\int_2^R \frac{dx}{x \ln x} = [\ln(\ln x)]_2^R = \ln(\ln R) - \ln(\ln 2) \to \infty$$
as $R \to \infty$, and the corresponding sum diverges by integral test.

Corollary 3.5.15.1. (*Euler-Mascheroni Constant*) As $n \to \infty$,

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \ln n \to \gamma$$

with $0 \leqslant \gamma \leqslant 1$.[12]

Proof. Set $f(x) = 1/x$ in Theorem 3.5.15 (2). ■

3.5.6 Lebesgue's Criterion for Riemann Integrability

Theorem 3.5.16. (*Lebesgue's Criterion*) If $f : [a, b] \to \mathbb{R}$ is bounded, then f is Riemann integral if and only if

$$\{x \mid f \text{ discontinuous at } x\}$$

has *measure zero*.

Definition 3.5.5. For an interval I, let $|I|$ denote its length. A subset $A \subset \mathbb{R}$ has *measure zero* if $\forall \epsilon > 0$ there exists a countable collection of intervals I_j such that

$$A \subset \bigcup_{j=1}^{\infty} I_j \text{ and } \sum_{j=1}^{\infty} |I_j| < \epsilon$$

i.e. "can cover A with countable numbers of infinitesimal intervals."

Lemma 3.5.17.

(1) If B has measure zero and $A \subset B$, then A has measure zero.

(2) If A_k has measure zero for each $k \in \mathbb{N}$, then $\bigcup_{k\in\mathbb{N}} A_k$ has measure zero.

Proof.

(1) Obvious from definition.

(2) Fix $\epsilon > 0$. For each k, pick I_j^k $(j = 1, 2, \ldots)$ such that

$$A_k \subset \bigcup_{j=1}^{\infty} I_j^k \text{ and } \sum_{j=1}^{\infty} |I_j^k| < \epsilon 2^{-k}$$

Then consider $\{I_j^k\}_{j,h=1}^{\infty}$. We have

$$\bigcup_{k\in\mathbb{N}} A_k \subset \bigcup_{j,k=1}^{\infty} I_k^j$$

and

$$\sum_{k=1}^{\infty} \sum_{j=1}^{\infty} |I_j^k| < \sum_{k=1}^{\infty} \epsilon 2^{-k} = \epsilon$$

■

Since $\{x\}$ is clearly measure zero, this implies countable sets have measure zero.

[12] Question: is γ irrational?

∗ Oscillation of function

For an interval I, define the *oscillation* of a bounded function f defined on I as

$$\omega_f(I) = \sup_I f - \inf_I f \geqslant 0$$

We have that if $I' \subset I$, then $\omega_f(I') \leqslant \omega_f(I)$. Now define

$$\omega_f(x) = \lim_{\epsilon \to 0} \omega_f((x-\epsilon, x+\epsilon))$$

Lemma 3.5.18. f is continuous at x if and only if $\omega_f(x) = 0$.

∗ Proof of necessity of Lebesgue's criterion

Note that

$$D = \{x \in [a,b] \mid f \text{ discontinuous at } x\} = \{x : \omega_f(x) > 0\}$$

If $N(\alpha) = \{x : \omega_f(x) \geqslant \alpha\}$, then

$$D = \bigcup_{k=1}^{\infty} N(1/k)$$

It is sufficient to show that $N(\alpha)$ has measure zero, for $f : [a,b] \to \mathbb{R}$ integrable function. Fix $\epsilon > 0$, then there exists a dissection $\mathcal{D}$ such that

$$U(f,\mathcal{D}) - L(f,\mathcal{D}) = \sum_{j=1}^{n} (x_j - x_{j-1}) \omega_f([x_{j-1}, x_j]) < \alpha\epsilon/2$$

from Cauchy criterion for integrability. Let

$$F = \{j : (x_{j-1}, x_j) \cap N(\alpha) \neq \varnothing\}$$

Then for each $j \in F$, $\omega_f([x_{j-1}, x_j]) \geqslant \alpha$. This implies

$$\alpha \sum_{j \in F} (x_j - x_{j-1}) \leqslant \sum_{j \in F} \omega_f([x_{j-1}, x_j])(x_j - x_{j-1}) < \epsilon\alpha/2 \Rightarrow \sum_{j \in F} (x_j - x_{j-1}) < \epsilon/2$$

These cover $N(\alpha)$, except for possibly $\{x_0, \ldots, x_n\}$ which can be covered by a finite number of intervals of total length $\epsilon/2$. Therefore, $N(\alpha)$ has measure zero and consequently D has measure zero.

3.6 Example Sheets

3.6.1 Sheet 1

1. Straightforward.

2. Converges for $a_1 = 0, 1$, diverges for $a_1 = 2$.

3. $a_1 > b_1 > 0$ by construction. Let $a_n > b_n > 0$. Then

$$a_{n+1} > b_{n+1} \Leftrightarrow \frac{a_n + b_n}{2} > \frac{a_n b_n}{a_n + b_n} \Leftrightarrow (a_n + b_n)^2 > 2a_n b_n \Leftrightarrow a_n^2 + b_n^2 > 0$$

   Thus $a_{n+1} > b_{n+1}$. Now since

$$b_{n+1} = \frac{2a_n b_n}{a_n + b_n} > b_n \Leftrightarrow a_n > b_n$$

   we have $b_{n+1} > 0$. Therefore, by induction, $a_n > b_n > 0$ for all $n \geqslant 1$. Finally, we also have

$$a_n > a_{n+1} = \frac{a_n + b_n}{2} \Leftrightarrow a_n > b_n$$

   Combining all, $a_n \geqslant a_{n+1} \geqslant b_{n+1} \geqslant b_n$.

   Now we find the common limit. (a_n) is decreasing and bounded by b_1, so $a_n \to a$ by monotone convergence theorem. Similarly $b_n \to b$. Then, limit on both sides of $a_{n+1} = (a_n + b_n)/2$ gives

$$a = \frac{a + b}{2}$$

   i.e. $a = b$ – the limit is common. Also note that

$$a_{n+1} b_{n+1} = a_n b_n = a_1 b_1$$

   Therefore, $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \sqrt{a_1 b_1}$.

4. a_n is not converging, hence it is not Cauchy, and there exists $\epsilon > 0$ such that $|a_n - a_m| \geqslant \epsilon$ for any n, m. Without loss of generality, let $a_1 - a_2 = \epsilon$. Now suppose

$$A = \{a_i \mid a_i \geqslant a_1\}$$

$$B = \{a_i \mid a_i \leqslant a_2\}$$

   We may order members of set A to construct a increasing subsequence (a_{n_j}), which is bounded above. Thus, by monotone convergence theorem, $a_{n_j} \to a < \infty$. Similarly, we reorder members of B to construct a decreasing subsequence a_{m_j} with $a_{m_j} \to b$. But $a \neq b$ since $a \geqslant a_1 > a_2 \geqslant b$.

5. Converges, converges for $|z| < 5$, converges absolutely, converges for $|z| < 1$. Boundaries are not checked.

6. Integral test.

7. We calculate as follows.

$$s_{2n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots = \overbrace{\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots\right)}^{2n} - 2\overbrace{\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \cdots\right)}^{n}$$
$$= h_{2n} - h_n$$

Meanwhile,

$$t_{3n} = \overbrace{\frac{1}{1} + \frac{1}{3} + \cdots + \frac{1}{4n-1}}^{2n} - \overbrace{\frac{1}{2} - \frac{1}{4} - \cdots - \frac{1}{2n}}^{n}$$
$$= h_{4n} - \left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{4n}\right) - \left(\frac{1}{2} - \frac{1}{4} - \cdots - \frac{1}{2n}\right)$$
$$= h_{4n} - \frac{1}{2}h_{2n} - \frac{1}{2}h_n = s_{4n} + \frac{1}{2}s_{2n}$$

By alternating series test, s_n converges to a finite value, say s. Then, $t_{3n} = s_{4n} + s_{2n}/2 \to 3s/2$ so $t_n \to 3s/2$ as $n \to \infty$.

8. Firstly, $a_n > 0$ for all n since

$$a_n = \frac{1}{\sqrt{n}} + \frac{(-1)^{n-1}}{n} \geqslant \frac{1}{\sqrt{n}} - \frac{1}{n} > 0$$

for $n \geqslant 2$ and $a_1 = 2 > 0$. Also, clearly $\lim_{n\to\infty} a_n = 0$ since both $1/\sqrt{n} \to 0$ and $1/n \to 0$ as $n \to \infty$. Now consider

$$\sum_{n=1}^{\infty} (-1)^{n-1} a_n = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{\sqrt{n}} + \sum_{n=1}^{\infty} \frac{1}{n}$$

The first sum converges by alternating series test, but second sum diverges; hence, $\sum_{n=1}^{\infty}(-1)^{n-1}a_n$ also diverges.

9. (*Dirichlet's test*) Simplify to obtain

$$S_n b_n - S_{m-1} b_m + \sum_{j=m}^{n-1} S_j b_j - \sum_{j=m}^{n-1} S_j b_{j+1} = \sum_{j=m}^{n} S_j b_j - \sum_{j=m-1}^{n-1} S_j b_{j+1}$$
$$= \sum_{j=m}^{n} S_j b_j - \sum_{j=m}^{n} S_{j-1} b_j$$
$$= \sum_{j=m}^{n} (S_j - S_{j-1}) b_j = \sum_{j=m}^{n} a_j b_j$$

Now since S_n is a bounded sequence, i.e. $|S_n| \leqslant K$, for each term

$$\left|S_j(b_j - b_{j-1})\right| \leqslant K(b_j - b_{j-1})$$

But series

$$\sum_{j=1}^{n-1} K(b_j - b_{j-1}) = K(b_1 - b_n) \to K b_1$$

as $n \to \infty$ so series $\sum_{j=1}^{n-1} S_j(b_j - b_{j+1})$ absolutely converges, and hence converges. Also, because $b_n \to 0$ and S_n is bounded,

$$S_n b_n, S_{n-1} b_n \to 0$$

as $n \to \infty$. Therefore, $\sum_{j=1}^{\infty} a_j b_j$ converges.

Alternating series test can be easily obtained by setting $a_n = (-1)^n$.

Now consider $\sum_{n=1}^{\infty} \cos n/n$. Let $a_n = \cos n$ and $b_n = 1/n$. To apply the Dirichlet's test, we need to show $\sum \cos n$ is bounded. Let $S_n = \sum_{n=1}^{\infty} \cos n$ and $S_0 = 0$. Then,

$$\begin{aligned} S_n \sin 1 &= \cos 1 \sin 1 + \cos 2 \sin 1 + \cdots + \cos n \sin 1 \\ &= -\frac{1}{2}(\sin 2 - \sin 0 + \sin 3 - \sin 1 + \cdots + \sin(n+1) - \sin(n-1)) \\ &= \frac{\sin 1 - \sin(n+1)}{2} \end{aligned}$$

gives

$$S_n = \frac{\sin 1 - \sin(n+1)}{2 \sin 1}$$

which is bounded. Thus by Dirichlet's test, $\sum_{n=1}^{\infty} \cos n/n$ converges.

10. Q10.

11. Note that

$$\frac{1}{1-z} - \frac{z}{1-z^2} = \frac{1+z-z}{1-z^2} = \frac{1}{1-z^2}$$

One can find out that by telescoping sums,

$$\sum_{j=1}^{n} \frac{z^{2^{j-1}}}{1-z^{2^j}} = \frac{1}{1-z} - \frac{1}{1-z^{2^n}}$$

Then, if $|z| < 1$, $z^{2^n} \to 0$ as $n \to \infty$ so the series converges to

$$\frac{1}{1-z} - 1 = \frac{z}{1-z}$$

If $|z| > 1$, $z^{2^n} \to \infty$ as $n \to \infty$ so series simply converges to $1/1 - z$. Finally, if $|z| = 1$,

$$\left| \frac{z^{2^{j-1}}}{1-z^{2^j}} \right| = \frac{1}{|1-z^{2^j}|} > \frac{1}{2}$$

so

$$\sum_{j=1}^{n} \frac{z^{2^{j-1}}}{1-z^{2^j}} > \frac{1}{2} n$$

diverges as $n \to \infty$.

12. Consider sequence (a_n), $a_n \in \mathbb{R}$. We can easily construct monotonic subsequence (a_{n_j}) by choosing $n_1 = 1$, and then n_i as the least greatest j such that $a_j \geqslant a_{n_{i-1}}$, $j \geqslant n_{i-1}$ inductively.

Now assume the sequence is bounded. The subsequence we found above, (a_{n_j}) will also be bounded and by the monotone convergence theorem, (a_{n_j}) will converge. Thus we proved the Bolzano-Weierstrass theorem.

13. Since (x_n) converges, it is bounded. Now sequence $(|x_n|)$. Because it is bounded, we can rearrange terms to make $(|x_n|)$ decreasing. Then, by alternating series test, $\sum(-1)^n|x_n|$ converges. ϵ_n will follow based on the original signs of x_n.

14. No. It is impossible.

3.6.2 Sheet 2

1. If $x \notin \mathbb{Q}$, take sequence $x_n \in \mathbb{Q}$. Then $x_n \to x$ but

$$f(x_n) = x_n \to x \neq 1 - x = f(x)$$

so f is discontinuous. If $x \in \mathbb{Q}$, take sequence $x_n \notin \mathbb{Q}$. Then $x_n \to x$. Now

$$f(x_n) = 1 - x_n \to 1 - x \neq x = f(x)$$

for all x that is not $1/2$. Therefore, f is discontinuous for all $x \in \mathbb{R}$, $x \neq 1/2$. However, for $x = 1/2$, f is indeed continuous. Hence the required set will be $\{1/2\}$.

2. We say $f(x) \to \infty$ as $x \to \infty$ if for given $M > 0$, there exists $\delta(M) > 0$ such that

$$\forall x \in \mathbb{R}, x > \delta \Rightarrow f(x) > M$$

Now let's solve the second part of the question.
($\Rightarrow$) Suppose $f \to \infty$ as $x \to \infty$, and x_n is a sequence with $x_n \to \infty$. Let $M > 0$. Then $\exists \delta > 0$ such that

$$\forall x \in \mathbb{R}, x > \delta \Rightarrow f(x) > M$$

But since $x_n \to \infty$, there exists N such that

$$n \geqslant N \Rightarrow x_n > \delta \Rightarrow f(x_n) > M$$

Therefore, $f(x_n) \to \infty$.
($\Leftarrow$) Suppose f is not continuous at a. Then, $\exists M > 0$ such that for all $\delta > 0$, $\exists x \in \mathbb{R}$ with $x > \delta$ and $f(x) \leqslant M$. Now consider

$$\delta = 1, 2, \ldots, n, \ldots$$

for $x_1, x_2, \ldots, x_n, \ldots$ respectively. Then, $x_n > n$ and $f(x_n) \leqslant M$. Then $x_n \to \infty$ as $n \to \infty$ but $f(x_n) \nrightarrow \infty$, which is a contradiction. Hence $f \to \infty$ as $x \to \infty$.

3. No. For example, consider

$$f(x) = 0 \text{ for all } x \in \mathbb{R}$$

$$g(x) = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$$

Then $\lim_{x\to 0} f(x) = 0$ and $\lim_{x\to 0} g(x) = 1$. However,

$$\lim_{x \to 0} g(f(x)) = 0$$

instead of expected 1. Note that g is not continuous at $x = 0$.

4. We only need to check if h_n is continuous at a point $a \in [0,1]$ such that $f_i(a) = f_j(a)$, and $f_i(x) - f_j(x)$ decreasing at a (without loss of generality) for some $i, j \in \{1, 2, \ldots, n\}$. Then,

$$\lim_{x \to a-} h_n(x) = \lim_{x \to a-} f_i(x) = f_i(a)$$

$$\lim_{x \to a+} h_n(x) = \lim_{x \to a+} f_j(x) = f_j(a)$$

But $f_i(a) = f_j(a)$ so the limit exists and $\lim_{x \to a} h_n(x) = f_i(a) = f_j(a)$. Hence h_n is continuous at a, and consequently at any $x \in [0,1]$.

5. Let $g(x) = f(x) - x$, which is also continuous at $[0,1]$. If $g(0) = 0$, $f(0) = 0$, done. Now if $g(0) > 0$, consider $g(1)$. If $g(1) = 0$, done. Otherwise, we have $g(1) < 0$. Then, by intermediate value theorem, there exists $c \in (0,1)$ such that

$$g(c) = f(c) - c = 0 \Leftrightarrow f(c) = c$$

However, a continuous bijection $h : (0,1) \to (0,1)$ need not to have a fixed point. E.g. consider $h(x) = x^2$. With such idea, we may construct a bijection of $[0,1]$ with no fixed point:

$$x \mapsto \begin{cases} 1 & x = 0 \\ x^2 & 0 < x < 1 \\ 0 & x = 1 \end{cases}$$

6. We assume the familiar features of sin and cos. For instance, $f(x)$ is periodic with period 2π. Thus we only consider $f(x) : [0, 2\pi] \to [0,2]$. Since f continuous, there exists $y \in [0, 2\pi]$ such that $f(y) \leqslant f(x)$ for all $x \in [0, 2\pi]$, by the extreme value theorem. Now we only need to show that $f(y) \neq 0$, or furthermore, $f(x) > 0$ $\forall x \in [0, 2\pi]$. Note that $f(x) = 0$ if and only if $\sin^2 x = 0$ and $\sin^2(x + \cos^7 x) = 0$. Suppose there is a point $c \in [0, 2\pi]$ with $f(x) = 0$. Then, we have

$$c = n\pi, \quad c + \cos^7 c = m\pi$$

for some $n, m \in \mathbb{Z}$. Simplification gives

$$(-1)^m = \cos^7(m\pi) = (n - m)\pi$$

which is a contradiction. Thus $f(x) > 0$ for all $x \in [0, 2\pi]$.

7. Q7.

8. Let $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x^5 + 3x^4 + 2x + 16$. Differentiate to find

$$f'(x) = 10x^4 + 12x^3 + 2$$

and

$$f''(x) = 40x^3 + 36x^2 = 4x^2(10x + 9)$$

Since $f''(x) < 0$ for $x < -9/10$, we know that f' is strictly decreasing at $[-2, -1]$. Furthermore, because $f'(-1) = 0$, $f'(x) > 0$ for $x \in [-2, -1)$, and f is strictly increasing at $[-2, -1)$.

Now, since $f(-2) = -4 < 0$ and $f(-1) = 15 > 0$, there exists $c \in (-2, -1)$ such that $f(c) = 0$ (by intermediate value theorem); and such point is unique since f is strictly increasing at $(-2, -1)$.

Moreover, there is no root for $x \leqslant -2$ since $f(-2) < 0$ and $f'(x)$ is strictly decreasing for $x \leqslant -2$. Similarly, there is no root for $x \geqslant 0$ since $f(x) \geqslant f(0) = 16 > 0$.

We only need to check for $(-1, 0)$. In this interval,

$$f(x) > 2x + 3x^4 + 2x + 16 = 3x^4 + 4x + 16 > 3x^4 + 12 > 12$$

so there is no root.

9. (2) (4) is true (see lecture note). (1) is also true. However, (3) is false, e.g. consider $f(x) = x^3$ at $x = 0$.

10. Note that $f(0) < \infty$ since f is differentiable for all x. By the mean value theorem, there exists $c \in (0, x)$ such that

$$\frac{f(x) - f(0)}{x} = f'(c)$$

Taking limits of both sides,

$$\lim_{x\to\infty} \frac{f(x) - f(0)}{x} = \lim_{x\to\infty} f'(c) = l$$

and

$$\lim_{x\to\infty} \frac{f(x)}{x} = l + \lim_{x\to\infty} \frac{f(0)}{x} = l$$

However, converse is not necessarily true, e.g. consider $f(x) = \sin x$.

11. If $x \neq 0$, simple calculation gives

$$f'(x) = 1 + 4x \sin \frac{1}{x} - 2\cos \frac{1}{x}$$

If $x = 0$,

$$f'(0) = \lim_{x\to 0} \frac{f(x) - f(0)}{x} = \lim_{x\to 0} \left(1 + 2x \sin \frac{1}{x}\right) = 1$$

since $h \to 0$ but $|\sin(1/h)| \leqslant 1$. Now consider an arbitrary interval $[-\delta, \delta]$. Let $x = 2/(2n+1)\pi$ with $n \in \mathbb{N}$, $x < \delta$. Then,

$$f(x) = x - 2x^2 < 0$$

since $x < 1/2$. Therefore, because $f(x) < f(0) = 0$ while $x > 0$, f(x) is not increasing in the interval $[-\delta, \delta]$. Since δ was arbitrary, we are done.

3.6.3 Sheet 3

1. Put $y = x + h$ where $h \neq 0$. Then,

$$\left|\frac{f(x+h) - f(x)}{h}\right| \leqslant |h|$$

Since it holds for all h,

$$\lim_{h\to 0} \frac{f(x+h) - f(x)}{h} = 0$$

Thus f is constant.

2. Note that $-1 \leqslant \sin(1/x) \leqslant 1$. With this fact, claim that f_α is bounded if and only if $0 \leqslant \alpha \leqslant 1$. One may easily proof this.

   Meanwhile, It is clear that f_α is continuous at all points except $x = 0$. We only need to check for $x = 0$: f_α is continuous if and only if $\alpha > 0$ and differentiable if and only if $\alpha > 1$. These give the table as follows.

$\alpha =$	$-1/2$	0	$1/2$	1	$3/2$	2	$5/2$	3	$7/2$
f_α bounded	✗	✓	✓	✓	✗	✗	✗	✗	✗
f_α cont.	✗	✗	✓	✓	✓	✓	✓	✓	✓
f_α diffable	✗	✗	✗	✗	✓	✓	✓	✓	✓
f'_α bounded	-	-	-	-	✗	✓	✗	✗	✗
f'_α cont.	-	-	-	-	✗	✗	✓	✓	✓
f'_α diffable	-	-	-	-	✗	✗	✗	✗	✓

3. $\log(1+x)$ is continuous on $[0, a/n]$ and differentiable on $(0, a/n)$. Hence, by mean value theorem, there exists $c \in (0, a/n)$ such that

$$\frac{\ln(1+a/n)}{a/n} = \frac{1}{1+c}$$

   Rearrange to find

$$\ln\left(\left(1+\frac{a}{n}\right)^n\right) = \frac{a}{1+c}$$

   Since ln is inverse of exp,

$$\left(1+\frac{a}{n}\right)^n = e^{a/(1+c)} \to e^a$$

   as $n \to \infty$ (Note that both limits exist).

4. Let $1/n = m$. Then

$$\lim_{n\to\infty} n(a^{1/n}-1) = \lim_{m\to 0}\frac{a^m-1}{m} = \lim_{m\to 0}\frac{e^{m\ln a}-1}{m\ln a}\ln a = \ln a$$

5. $f_{3/2}$ and f_2 from Question 2 shows the argument is false at $x = 0$. Note that $\lim_{h\to 0} f'(c+\theta h)$ may not exist.

6. It is clearly differentiable for $x \neq 0$. For $x = 0$, we can tell that f is infinitely differentiable since $x^r e^{-x} \to 0$ as $x \to \infty$ for any $r > 0$. Taylor's theorem states that

$$f(x) = \frac{x^n}{n!} f^{(n)}(\theta x)$$

   However,

$$f(x) \neq \sum_{i=}^{\infty} \frac{x^i}{i!} f^{(i)}(0) = 0$$

   Taylor series, since

$$R_n(x) = \frac{x^n}{n!} f^{(n)}(\theta x) \neq 0$$

   as $n \to \infty$.

7. $3/2$, $2^{1/3}$, $1/e$, 1.

8. By Cauchy's mean value theorem,

$$\frac{f(x)}{g(x)} = \frac{f(x)-f(a)}{g(x)-g(a)} = \frac{f'(c)}{g'(c)}$$

for some $c \in (a,x)$. Hence

$$\lim_{x\to a}\frac{f(x)}{g(x)} = \lim_{x\to a}\frac{f'(c)}{g'(c)} = l$$

Put $g(x) = x - a$. Then,

$$\lim_{x\to a}\frac{f(x)-f(a)}{x-a} = \lim_{x\to a} f'(x) = l$$

So f is also differentiable at a (with limit l).

Meanwhile, consider $g(x) = x$,

$$f(x) = \begin{cases} x^2 \sin\frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

and $a = 0$. Then

$$f'(x) = 2x\sin\frac{1}{x} - \cos\frac{1}{x}$$

and $g'(x) = 1$. We have

$$\lim_{x\to 0}\frac{f(x)}{g(x)} = \lim_{x\to 0} x\sin\frac{1}{x} = 0$$

but $\lim_{x\to 0} f'(x)/g'(x)$ is not defined.

For the final part, let $f(x) = x - (n+1)x^{n+1} + nx^{n+2}$, and $g(x) = (1-x)^2$. Then $f'(x) = 1 - (n+1)^2x^n + n(n+2)x^{n+1}$, $g'(x) = 2x - 2$. Thus the limit will be

$$\frac{n(n+1)}{2}$$

9. We have $\tan' x = \sec^2 x$ for $x \in (-\pi/2, \pi/2)$. Now consider $\tan x : [-a,a] \to [-c,c]$ for some $0 < a < \pi/2$, with $c = \tan a$. Then by inverse function theorem, $\tan^{-1}$ is differentiable on $(-c,c)$ with

$$(\tan^{-1} x)' = \frac{1}{1+x^2}$$

Moreover, since $c \to \infty$ as $a \to \pi/2$, it is differentiable for $x \in \mathbb{R}$.

By ratio test, we can check the power series

$$g(x) = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{2n+1}$$

has a radius of convergence of 1. Hence g is differentiable for $|x| < 1$ and

$$g'(x) = \sum_{n=0}^{\infty}(-1)^n x^{2n} = \frac{1}{1+x^2} = (\tan^{-1} x)'$$

Integrate both sides to obtain that $\tan^{-1} = g(x)$ ($g(0) = \tan 0$).

10. Clearly,
$$p_n = (1+a_1)\cdots(1+a_n) = 1 + (a_1 + \cdots + a_n) + (\cdots) \geqslant s_n$$
Now since ln is increasing,
$$\begin{aligned} p_n \leqslant e^{s_n} &\Leftrightarrow \ln p_n \leqslant s_n \\ &\Leftrightarrow \ln(1+a_1) + \cdots + \ln(1+a_n) \leqslant a_1 + \cdots + a_n \end{aligned}$$
Claim that $\ln(1+x) \leqslant x$ for $x \geqslant 0$. Let $f(x) = \ln(1+x) - x$. But
$$f'(x) = 1 - \frac{1}{1+x} = \frac{x}{1+x} \geqslant$$
and $f(0) = 0$. So $\ln(1+x) \leqslant x$ for $x \geqslant 0$. Thus
$$\ln\left(1+a_j\right) \leqslant a_j$$
for all $j = 1, 2, \ldots, n$ and
$$s_n \leqslant p_n \leqslant e^{s_n}$$
First suppose $p_n \to p$ as $n \to \infty$. Then, s_n is bounded by p and it is increasing ($a_n \geqslant 0$). Therefore it converges.

Suppose $s_n \to s$ as $n \to \infty$. Then, p_n is bounded by e^s and it is increasing ($(1+a_n) \geqslant 1$). Therefore it converges. Thus $\prod_{n=1}^{\infty}(1+a_n)$ converges if and only if $\sum_{n=1}^{\infty} a_n$ converges.

Let $a_n = 1/(n^2-1)$. Then,
$$s_n = \sum_{j=2}^{n} a_n = \sum_{j=2}^{n} \frac{1}{2}\left(\frac{1}{j-1} - \frac{1}{j+1}\right) = \frac{3}{4} - \frac{1}{2}\left(\frac{1}{n} + \frac{1}{n+1}\right) \to \frac{3}{4}$$
Thus by above, p_n converges. Now,
$$\begin{aligned} \ln p_n &= \sum_{j=2}^{n} \ln(1+a_n) = \sum_{j=2}^{n} \ln\left(\frac{j^2}{j^2-1}\right) = \sum_{j=2}^{n} \left[\ln\left(j^2\right) - \ln\left(j^2-1\right)\right] \\ &= \sum_{j=2}^{n} \left[2\ln j - \ln(j-1) - \ln(j+1)\right] \\ &= \sum_{j=2}^{n} \left[(\ln j - \ln(j-1)) - (\ln(j+1) - \ln j)\right] \\ &= \ln 2 + \ln\frac{n}{n+1} \to \ln 2 \end{aligned}$$
as $n \to \infty$. Thus $p_n \to 2$ as $n \to \infty$.

11. Q11.

12. (*Theorem of Darboux*) Let $d = (a+b)/2$. For $a \leqslant x \leqslant d$, define $\alpha(x) = a$ and $\beta(x) = 2x - a$, and for $d \leqslant x \leqslant b$, define $\alpha(x) = 2x - b$ and $\beta(x) = b$. Then for $x \in (a,b)$, we have $a \leqslant \alpha < \beta \leqslant b$. Now, define
$$g(x) = \frac{(f\circ\beta)(x) - (f\circ\alpha)(x)}{\beta(x) - \alpha(x)}$$

with $a < x < b$. Furthermore, $g(x) \to f'(a)$ as $x \to a$ and $g(x) \to f'(b)$ as $x \to b$. Hence, by the intermediate value theorem, there exists $m \in (a,b)$ such that $g(m) = y$. Then, by the mean value theorem, there exists $c \in (\alpha(m), \beta(m))$ such that

$$f'(c) = g(m) = y$$

13. We consider

$$f(x) = \exp\left(\frac{1}{(x-a)(x-b)}\right)$$

(See Rudin.)

3.6.4 Sheet 4

1. Let $f : [0,a] \to [0,a^2]$, $x \mapsto x^2$. Consider a dissection

$$\mathcal{D}_k = \left\{0, \frac{a}{k}, \frac{2a}{k}, \ldots, \frac{ak}{k}\right\}$$

Then,

$$U(f,\mathcal{D}_k) = \sum_{j=1}^{k} \frac{a}{k}\frac{j^2a^2}{k^2} = \frac{a^3}{k^3}\sum_{j=1}^{k} j^2 = \frac{a^3(k+1)(2k+1)}{6k^2}$$

and

$$I^* = \inf_{\mathcal{D}} U(f,\mathcal{D}) \leqslant \inf_{k} U(f,\mathcal{D}_k) = \frac{a^3}{3}$$

Similarly,

$$L(f,\mathcal{D}_k) = \frac{a^3(k-1)(2k-1)}{6k^2}$$

and

$$I_* = \sup_{\mathcal{D}} L(f,\mathcal{D}) \geqslant \sup_{k} L(f,\mathcal{D}_k) = \frac{a^3}{3}$$

But since $I^* \geqslant I_*$,

$$I^* = I_* = \int_0^a x^2 dx = \frac{a^3}{3}$$

2. Claim that such integral exists. Given $\epsilon > 0$, consider two intervals $[0,\delta]$ and $[\delta,1]$ where $\delta = \epsilon/4$. Since $f(x) = \sin(1/x)$ continuous on $[\delta,1]$, there exists a dissection $\mathcal{D}_2$ such that $U(f,\mathcal{D}_2) - L(f,\mathcal{D}_1) \leqslant \epsilon/2$ by the Cauchy criterion for integrability. For interval $[0,\delta]$, consider dissection $\mathcal{D}_1 = \{0,\delta\}$. Then, $U(f,\mathcal{D}_1) \leqslant \delta$ and $L(f,\mathcal{D}_1) \geqslant -\delta$. Hence

$$U(f,\mathcal{D}_1) - L(f,\mathcal{D}_1) \leqslant 2\delta = \epsilon/2$$

Thus if we let $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$, we are done by the Cauchy criterion for integrability.

3. Consider

$$f(x) = x^{-1/2}e^{-x}$$

This is unbounded since $f(x) \to \infty$ as $x \to 0+$. However, $\int_0^\infty f(x)dx = \sqrt{\pi} < \infty$.

4. Consider

$$f(x) = \begin{cases} 1 & x = 0 \\ 0 & \text{otherwise} \end{cases}$$

f is integrable with $\int_0^1 f(x)dx = 0$. For the next part, suppose there exists a function $f(x)$ such that $\int_0^1 f(x)dx = 0$, $f(a) > 0$ for some $a \in [0,1]$, and f continuous. Since f continuous, there exists $\delta > 0$ such that

$$|x - a| < \delta \Rightarrow |f(x) - f(a)| < \frac{f(a)}{2}$$

Now, we have

$$\int_{a-\delta}^{a+\delta} f(x)dx \geqslant 2\delta\left(\frac{f(a)}{2}\right) = \delta f(a) > 0$$

which is a contradiction. Hence f cannot be continuous.

5. Let D denote the set of discontinuities. For each $x \in D$, the left and right limits differ since f monotonic, and thus the two limit values can be the endpoints of an interval I_x. Now consider the set

$$\{I_d : d \in D\}$$

Because each interval is disjoint, contains a rational, and $\mathbb{Q}$ is countable, there exists an injection from D to $\mathbb{Q}$. Hence D is countable. (Recall Numbers and Sets.)

For the next part, we know

$$\frac{f_n(x)}{2^n} \leqslant \frac{1}{2^n}$$

for all $n \in \mathbb{N}$ and $x \in [0,1]$ but $\sum_{n=1}^{\infty}(1/2^n) = 1 < \infty$. Hence $f(x)$ converges for every $x \in [0,1]$ by the comparison test. For given m, $f_m(y) \geqslant f_m(x)$ if $y \geqslant x$. Hence it immediately follows that f is increasing, and thus f in integrable. Now consider

$$f(x_m) = \sum_{n=1}^{\infty} 2^{-n} f_n(x_m)$$

Since

$$\lim_{x \to x_m -} f(x) = f(x_m) - \frac{f_m(x_m)}{2^m} \neq f(x_m)$$

$f(x)$ is discontinuous at x_m.

6. By the mean value theorem, there exists $c \in (0,x)$ such that

$$\frac{f(x)}{x} = \frac{2c}{c^2 - 1}$$

Then,

$$|f(x)| = \left|\frac{2c}{c^2-1}x\right| \leqslant \frac{2}{1-c^2}x^2 \leqslant \frac{8}{3}x^2$$

Meanwhile,

$$\begin{aligned} I_n = \int_{n-1/2}^{n+1/2} \ln x dx - \ln n &= \int_{n-1/2}^{n+1/2} \ln \frac{x}{n} dx \\ &= \int_{n-1/2}^{n} \ln \frac{x}{n} dx + \int_{n}^{n+1/2} \ln \frac{x}{n} dx \\ &= \int_0^{1/2} \left(\ln\left(1 - \frac{t}{n}\right) + \ln\left(1 + \frac{t}{n}\right) \right) dt \\ &= \int_0^{1/2} f(t/n) dt \end{aligned}$$

So

$$|I_n| = \left| \int_0^{1/2} f(t/n) dt \right| \leqslant \int_0^{1/2} |f(t/n)| dt \leqslant \int_0^{1/2} \frac{8}{3} \frac{t^2}{n^2} dt = \frac{1}{9n^2}$$

Finally, calculate to find

$$\sum_{j=1}^{n} I_j = \sum_{j=1}^{n} \left(\int_{j-1/2}^{j+1/2} \ln x dx - \ln j \right) = \int_{1/2}^{n+1/2} \ln x dx - \sum_{j=1}^{n} \ln j = \ln \frac{(n+1/2)^{n+1/2}}{e^n n!} + \frac{1}{2} \ln 2$$

But since $\sum |I_j|$ converges by comparison test, $\sum I_j$, and consequently

$$\frac{n!}{(n+1/2)^{n+1/2} e^{-n}}$$

converges. Moreover,

$$\left(\frac{n+1/2}{n} \right)^{n+1/2} \to \sqrt{e} < \infty$$

as $n \to \infty$; so $n!/n^{n+1/2}e^{-n} \to \ell$ as required.

7. (*Wallis's Product & Stirling's Formula*) Calculation gives

$$\begin{aligned} I_n = \int_0^{\pi/2} \cos^n x dx &= \int_0^{\pi/2} \cos x \cos^{n-1} x dx \\ &= \left[\sin x \cos^{n-1} x \right]_0^{\pi/2} + (n-1) \int_0^{\pi/2} \cos^{n-2} x \sin^2 x dx \\ &= (n-1) I_{n-2} - (n-1) I_n \end{aligned}$$

Hence $nI_n = (n-1)I_{n-2}$. Furthermore, since $0 \leqslant \cos x \leqslant 1$ if $x \in [0, \pi/2]$, $\cos^{n+2} x \leqslant \cos^{n+1} x \leqslant \cos^n x$. Thus $I_{2n+1} \leqslant I_{2n} \leqslant I_{2n-1}$. Divide by I_{2n+1} to obtain

$$1 \leqslant \frac{I_{2n}}{I_{2n+1}} \leqslant \frac{I_{2n-1}}{I_{2n+1}} = \frac{2n+1}{2n}$$

Now, since $2n/2n+1 \to 1$,

$$1 = \lim_{n\to\infty} \frac{I_{2n+1}}{I_{2n}} = \lim_{n\to\infty} \frac{2 \cdot 2 \cdot 4 \cdot 4 \cdots 2n \cdot 2n}{1 \cdot 3 \cdot 3 \cdot 5 \cdots (2n-1) \cdot (2n+1)} \frac{I_1}{I_0}$$

Therefore,

$$\frac{\pi}{2} = \lim_{n\to\infty} \frac{2^{4n}}{2n+1} \binom{2n}{n}^{-2}$$

($I_1 = 1, I_0 = \pi/2$.) Recall from question six

$$\ell = \lim_{n\to\infty} \frac{n!}{n^{n+1/2}e^{-n}}$$

Then, by manipulating limits,

$$\begin{aligned}\frac{\pi}{2} &= \lim_{n\to\infty} \frac{2^{4n}(n!)^4}{(2n+1)((2n)!)^2} = \lim_{n\to\infty} \frac{2^{4n}(\ell n^{n+1/2}e^{-n})^4}{(2n+1)(\ell(2n)^{2n+1/2}e^{-2n})^2} \\ &= \lim_{n\to\infty} \frac{2^{4n}\ell^2}{2n+1}\frac{n^{4n+2}}{2^{4n+1}n^{4n+1}} = \frac{\ell^2}{4}\end{aligned}$$

Hence we find $\ell = \sqrt{2\pi}$.

8. They both converge.

   (a) For $\int_1^\infty \sin^2(1/x)dx$, note that $\sin x \leqslant x$ for $0 \leqslant x$. So $\sin^2(1/x) \leqslant 1/x^2$ and

   $$\int_1^\infty \sin^2\frac{1}{x}dx \leqslant \int_1^\infty \frac{dx}{x^2} = 1$$

   Thus it converges.

   (b) For $\int_0^\infty x^p e^{-x^q}dx$, we may substitute $x^q = t$ and consider $\int_0^\infty x^p e^{-x}dx$ without loss of generality. Firstly, $\int_0^1 x^p e^{-x}$ clearly converges. Now, for $\int_1^\infty x^p e^{-x}dx$, consider

   $$\lim_{x\to\infty} \frac{x^p e^{-x}}{1/x^2} = \lim_{x\to\infty} \left(\frac{x}{e^{x^{1/p+2}}}\right)^{p+2} = 0$$

   Thus $x^p/e^x < 1/x^2$ for sufficiently large x. Therefore, since $\int_1^\infty (dx/x^2) = 1 < \infty$, we are done.

9. By definition,

$$\lim_{n\to\infty} \sum_{j=n+1}^{2n} \frac{1}{j/n}\frac{1}{n} = \int_1^2 \frac{dx}{x} = \ln 2$$

For the second part, consider

$$I_n = \int_0^1 \frac{x^n}{1+x}dx$$

Note that

$$I_k + I_{k-1} = \int_0^1 \frac{x^{k-1}(1+x)}{(1+x)}dx = \frac{1}{k}$$

Hence the sum

$$\begin{aligned}\frac{1}{n+1} - \frac{1}{n+2} + \cdots &= (I_n + I_{n+1}) - (I_{n+1} + I_{n+2}) + \cdots + (-1)^{n-1}(I_{2n-1} + I_{2n}) \\ &= I_n + (-1)^{n-1}I_{2n} \to 0\end{aligned}$$

10. Q10.

11. By the fundamental theorem of calculus,

$$\begin{aligned} g(x) &= x\int_0^1 tf(t)dt - \int_0^x t(t)dt - x\int_x^1 f(t)dt \\ g'(x) &= \int_0^1 tf(t)dt - \int_x^1 f(t)dt \\ g''(x) &= f(x) \end{aligned}$$

12. Integration by parts gives

$$\begin{aligned} I_n(\theta) &= \int_{-1}^1 (1-x^2)^n \cos(\theta x)dx \\ &= \frac{1}{\theta}\left[(1-x^2)^n \sin(\theta x)\right]_{-1}^1 + \frac{n}{\theta}\int_{-1}^1 2x(1-x^2)^{n-1}\sin(\theta x)dx \\ &= \left[-\frac{2n}{\theta^2}\int_{-1}^1 x(1-x^2)^{n-1}\cos(\theta x)\right]_{-1}^1 \\ &+ \frac{2n}{\theta^2}\int_{-1}^1 \Big((1-x^2)^{n-1} + (n-1)x(-2x)(1-x^2)^{n-2}\Big)\cos(\theta x)dx \\ &= \frac{2n}{\theta^2}((2n-1)I_{n-1} - 2(n-1)I_{n-2}) \end{aligned}$$

Note that $\theta I_0(\theta) = 2\sin\theta$ and $\theta^3 I_1(\theta) = 4\sin\theta - 4\theta\cos\theta$. Suppose that

$$\theta^{2n+1} I_n(\theta) = n!(P_n(\theta)\sin\theta + Q_n(\theta)\cos\theta)$$

for $n = 0, 1, 2, \ldots, k$ where P_n and Q_n are polynomials of degree at most n with integer coefficients. Then,

$$\begin{aligned} \theta^{2n+3} I_{n+1} &= \theta^{2n+1}(2n+2)(2n+1)I_n - \theta^{2n+1}(4n+4)nI_{n-1} \\ &= 2(2n+1)(n+1)n!(P_n(\theta)\sin\theta + Q_n(\theta)\cos\theta) \\ &- 4(n+1)n(n-1)!\theta^2(P_{n-1}(\theta)\sin\theta + Q_{n-1}(\theta)\cos\theta) \\ &= (n+1)!(((4n+2)P_n(\theta) - 4\theta^2 P_{n-1}(\theta))\sin\theta \\ &+ ((4n+2)Q_n(\theta) - 4\theta^2 Q_{n-1}(\theta))\cos\theta) \end{aligned}$$

Therefore, by induction,

$$\theta^{2n+1} I_n(\theta) = n!(P_n(\theta)\sin\theta + Q_n(\theta)\cos\theta)$$

for all $n \in \mathbb{N}_{\geqslant 0}$ where P_n and Q_n are polynomials of degree at most n with integer coefficients.

Now, put $\theta = \pi/2$ to find $(\pi/2)^{2n+1} I_n(\pi/2) = n!P_n(\pi/2)$. Suppose $\pi/2 = p/q$ where $p, q \in \mathbb{N}$. Then, since P_n is a polynomial of degree at most n,

$$N = p^{2n+1}P_n(\pi/2) = \frac{q^{n+1}}{n!}I_n(\pi/2)$$

where $N \in \mathbb{N}$. But $0 < I_n(\pi/2) < 2$ and $q^{n+1}/n! \to 0$ as $n \to \infty$. Hence, for sufficiently large n,

$$0 < N < 1$$

which is a contradiction. Therefore π is irrational.

13. Note that

$$\begin{aligned}|g(x_j)-g(x_{j-1})| &= |(f_1(x_j)-f_1(x_{j-1}))-(f_2(x_j)-f_2(x_{j-1}))|\\ &\leqslant |f_1(x_j)-f_1(x_{j-1})|+|f_2(x_j)-f_2(x_{j-1})|\end{aligned}$$

But since f_i $(i=1,2)$ is increasing,

$$\sum_{j=1}^{n}|f_i(x_j)-f_i(j-1)| = \sum_{j=1}^{n}(f_i(x_j)-f_i(j-1)) = f_i(x_n)-f_i(x_0)$$

Hence

$$S(\mathcal{D}) = \sum_{j=1}^{n}|g(x_j)-g(x_{j-1})| \leqslant (f_1(x_n)+f_2(x_n))-(f_1(x_0)+f_2(x_0)) = K$$

Now for given $g(x)$, it is integrable since continuous. However, if we choose dissection

$$\mathcal{D}_n = \left\{-1,-\frac{2}{\pi},-\frac{2}{3\pi},\dots,-\frac{2}{(2n+1)\pi},\frac{2}{(2n+1)\pi},\dots,\frac{2}{3\pi},\frac{2}{\pi},1\right\}$$

with $x_0=1, x_j = 2/(2j+1)\pi, x_{n+1}=-1$,

$$\sum_{j=1}^{n-1}|g(x_{j+1})-g(x_j)| = \sum_{j=1}^{n-1}\left|\frac{(-1)^{j+1}}{(j+1)\pi}-\frac{(-1)^j}{j\pi}\right| = \frac{1}{\pi}\sum_{j=1}^{n-1}\left(\frac{1}{j}+\frac{1}{j+1}\right)$$

and

$$S(\mathcal{D}_n) = 2\frac{1}{\pi}\sum_{j=1}^{n-1}\left(\frac{1}{j}+\frac{1}{j+1}\right)+\frac{4}{(2n+1)\pi}+2\left(\sin 1-\frac{2}{\pi}\right)\to\infty$$

So S is not bounded and therefore it is not the difference of two increasing functions.