Summaries of Mathematics and Physics

Version: September 11, 2021

Contents

Part I

Mathematics

Chapter 1.1

First year

1.1.1 Fundamentals of mathematics

1.1.1.1 | Introduction

Axiom 1.1 (Peano axioms).

1. $1 \in \mathbb{N}$.
2. $\forall n \in \mathbb{N}$, exists a "successor" $S(n) \in \mathbb{N}$ of n.
3. $\forall n \in \mathbb{N}$, $S(n) \neq 1$.
4. $\forall n, m \in \mathbb{N}$, $n = m \iff S(n) = S(m)$.
5. *(Induction axiom)* If $K \subseteq \mathbb{N}$ is a set such that:
   i) $1 \in K$.
   ii) $\forall k \in K$, $S(k) \in K$.

   Then, $K = \mathbb{N}$.

Axiom 1.2 (Induction axiom). Peano's 5th axiom can be stated in the following way: Let ϕ be a predicate[1] such that:

1. $\phi(1)$ is true.
2. $\forall n \in \mathbb{N}$, $\phi(n)$ being true implies that $\phi(S(n))$ is true.

Then, $\phi(n)$ is true for all $n \in \mathbb{N}$.

Proposition 1.3. All non-empty subsets of $\mathbb{N}$ have a first element.

Proposition 1.4. If a set A satisfies the first four Peano's axioms and has the property that all non-empty subsets of it have a first element, then A satisfies the induction axiom.

1.1.1.2 | Set theory

Definitions and basic operations

Definition 1.5. A *set* is a collection of distinct elements.

Definition 1.6. Let A be a finite set. The *cardinal of* A, $|A|$, is the number of elements in A.

Definition 1.7. Let A be a set. We say a set B is a *subset* of A, denoted by $B \subseteq A$, if and only if all elements of B are also elements of A

Definition 1.8 (Axiom of extensionality). Let A, B be two sets. We say that A and B are *equal*, $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.

Definition 1.9. Let A be set. The subset $\mathcal{P}(A)$, called *power set*, is the set of all subsets of A.

Definition 1.10. We define the *empty set* $\varnothing$ as the unique set having no elements.

Definition 1.11. Let A, B be two sets. The *intersection of A and B*, $A \cap B$, is the set of all elements of both A and B. That is,

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

Proposition 1.12. Let A, B, C be three sets. Then:

1. $A \cap B = B \cap A$.
2. $A \cap (B \cap C) = (A \cap B) \cap C$.
3. $A \cap B \subseteq A$.
4. $A \cap \varnothing = \varnothing$.
5. $A \subseteq B \iff A \cap B = B$.
6. If $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cap B$.

Definition 1.13. Let A, B be two sets. The *union of A and B*, $A \cup B$, is the set of all elements of either A or B. That is,

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

Proposition 1.14. Let A, B, C be three sets. Then:

1. $A \cup B = B \cup A$.
2. $A \cup (B \cup C) = (A \cup B) \cup C$.
3. $A \subseteq A \cup B$.
4. $A \cup \varnothing = A$.
5. $A \subseteq B \iff A \cup B = B$.
6. If $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

Proposition 1.15. Let A, B, C be three sets. Then:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Definition 1.16. Let U be a set and $A \subseteq U$ be a subset of U. The *complement of A in U* is the set of elements not in A. That is,

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

Proposition 1.17 (De Morgan's laws). Let U be a set and A, B be two subsets of U. Then:

1. $(A \cup B)^c = A^c \cap B^c$.
2. $(A \cap B)^c = A^c \cup B^c$.

Definition 1.18. Let U be a set and A, B be two subsets of U. The *set difference of A and B*, $A \setminus B$, is the set of elements in A but not in B. That is,

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

Proposition 1.19. Let A, B, C be three sets. Then:

1. $A \setminus B = A \cap B^c$.
2. $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$.
3. $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

[1] A *predicate* is a formula that can be evaluated to true or false in function of the values of the variables that occur in it.

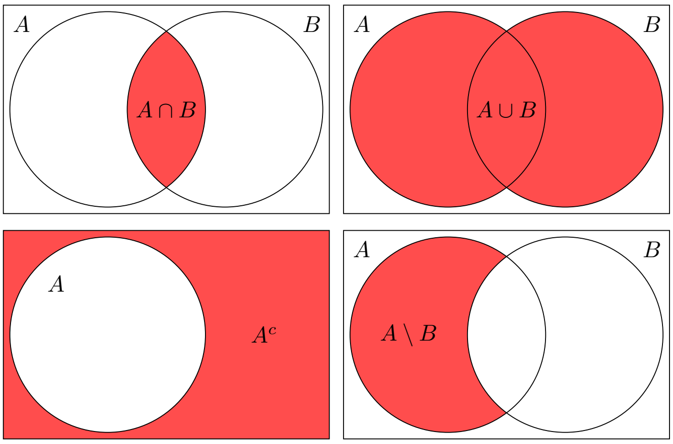


Figure 1.1.1: Venn diagrams

Definition 1.20. Let A, B be two sets. The *Cartesian product*, $A \times B$, is the set

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

Proposition 1.21. Let A, B, C be three sets. Then:

1. $A \times \varnothing = \varnothing \times A = \varnothing$.
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Functions between sets

Definition 1.22. Let A, B be two sets. A *function from A to B* is a binary relation between A and B that associates to each element of A exactly one element of B.

Definition 1.23. Let A, B, C be three sets and $f : A \to B$, $g : B \to C$ be two functions. The *composition* $g \circ f$ is:

$$\begin{aligned} g \circ f : A &\longrightarrow \quad B \quad \longrightarrow \quad C \\ a &\longmapsto f(a) \longmapsto g[f(a)] \end{aligned}$$

Definition 1.24. Let $f : A \to B$ be a function and $U \subseteq A$ be a subset. The *image of U* is the subset of B defined by $f(U) = \{f(u) : u \in U\}$. If $U = A$, $f(U) = f(A) =: \operatorname{im} f$ is the *image of f*.

Definition 1.25. Let $f : A \to B$ be a function and $b \in B$. The *preimage of b* is the set of elements $a \in A$ such that $f(a) = b$. More generally, if $V \subseteq B$, the *preimage of V* is the subset of A defined by:

$$f^{-1}(V) = \{a \in A : f(a) = v \in V\}.$$

Proposition 1.26. Let $f : A \to B$ be a function and $U \subseteq A$ be a subset of A. Then,

1. $f\left(\bigcup_{i \in I} U_i\right) \subseteq \bigcup_{i \in I} f(U_i)$.
2. $f\left(\bigcap_{i \in I} U_i\right) \subseteq \bigcap_{i \in I} f(U_i)$.
3. $f(U^c) \subseteq f(U)^c$.

Definition 1.27. Let $f : A \to B$ be a function. The following statements are equivalent:

1. $\forall b \in B$, $f^{-1}(b)$ has no more than one element.
2. $\forall a_1, a_2 \in A$, if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.
3. $\forall a_1, a_2 \in A$, if $f(a_1) = f(a_2)$, then $a_1 = a_2$.

If f satisfies one of these conditions, then it satisfies the other two and we say that f is *injective*.

Proposition 1.28. Let $f : A \to B$, $g : B \to C$ be two functions.

1. If f and g are injective, then $g \circ f$ is injective.
2. If $g \circ f$ is injective, then f is injective.

Definition 1.29. Let $f : A \to B$ be a function. The following statements are equivalent:

1. The preimage of each element of B has at least one element.
2. $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$.
3. $\operatorname{im} f = B$.

If f satisfies one of these conditions, then it satisfies the other two and we say that f is *surjective*.

Proposition 1.30. Let $f : A \to B$, $g : B \to C$ be two functions.

1. If f and g are surjective, then $g \circ f$ is surjective.
2. If $g \circ f$ is surjective, then g is surjective.

Definition 1.31. Let $f : A \to B$ be a function. We say that f is *bijective* if it is both injective and surjective. Bijective functions $f^{-1} : B \to A$.

Proposition 1.32. Let $f : A \to B$ be a bijective function. The f has an associated inverse function $f^{-1} : B \to A$ defined as:

$$\begin{aligned} f^{-1} : B &\longrightarrow A \\ b &\longmapsto f^{-1}(b) \end{aligned}$$

Theorem 1.33. Let $f : A \to B$ be a function. f is invertible (that is admits and inverse function) if and only if f is bijective.

1.1.1.3 | Logic and propositional calculus

Definition 1.34. Let P be a proposition. Then, $\neg P$ expresses the *negation of P*.

Definition 1.35. Let P, Q be propositions. Then, $P \wedge Q$ expresses that *P and Q are both true.*

Definition 1.36. Let P, Q be propositions. Then, $P \vee Q$ expresses that *either P or Q are true.*

Definition 1.37. Let P, Q be propositions. Then, $P \Rightarrow Q$ expresses that *Q is true whenever P is true.* Note that $P \Rightarrow Q = Q \vee \neg P$.

Definition 1.38. Let P, Q be propositions. Then, $P \Leftrightarrow Q$ expresses that *P and Q have the same truth-value.* Note that $P \Leftrightarrow Q = (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

1.1.1.4 | Symmetric group

Definition 1.39. Let $n \in \mathbb{N}$. We denote by S_n the set of all the bijections $\{1, 2, \ldots, n\}$ to itself. An element of S_n is a permutation of $\{1, \ldots, n\}$.

Proposition 1.40. The pair $(S_n, \circ)$, where

$$\begin{aligned} \circ : S_n \times S_n &\longrightarrow S_n \\ (\sigma, \tau) &\longmapsto \sigma \circ \tau \end{aligned}$$

is a group[2] called *symmetric group*.

Theorem 1.41. The cardinal of S_n is $n!$.

Definition 1.42. Let $\sigma \in S_n$. The set $\{m \in \mathbb{N} : \sigma^m = \mathrm{id}\}$ is non-empty. Hence, it contains a minimal element $\mathrm{ord}(\sigma)$. The integer $\mathrm{ord}(\sigma)$ is called the *order of* σ.

Definition 1.43. Let $\sigma \in S_n$. The *support of* σ is:

$$\mathrm{supp}(\sigma) = \{k \in \{1, \ldots, n\} : \sigma(k) \neq k\}.$$

Lemma 1.44. Let $\sigma \in S_n$. Then:

1. $p \in \mathrm{supp}(\sigma) \implies \sigma(p) \in \mathrm{supp}(\sigma)$.
2. $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$.

Lemma 1.45. Let $\sigma, \tau \in S_n$. If $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$, then $\sigma \circ \tau = \tau \circ \sigma$.

Definition 1.46. Let $\sigma \in S_n$ and $k \in \{1, \ldots, n\}$. The *orbit of* k is the finite set $\{k, \sigma(k), \sigma^2(k), \ldots\}$.

Theorem 1.47 (Orbit structure). Let $\sigma \in S_n$ and $\Omega = \{\omega_1, \ldots, \omega_k\}$ be the set of all the orbits of σ. Then:

1. $\bigcup_{j=1}^{k} \omega_j = \{1, \ldots, n\}$.
2. If $\omega_i, \omega_j \in \Omega$ and $\omega_i \cap \omega_j \neq \varnothing$, then $\omega_i = \omega_j$.
3. All orbits are non-empty.

Theorem 1.48 (Orbit linear structure). Let $\sigma \in S_n$, ω be one of its orbits and $a \in \omega$. If $k = |\omega|$, then $\omega = \{a, \sigma(a), \ldots, \sigma^{k-1}(a)\}$ and $\sigma^k(a) = a$.

Definition 1.49. If $\sigma \in S_n$ has a unique orbit with $k > 1$ elements, then we say that σ is a *cycle of length* k.

Definition 1.50. A *transposition* $\tau \in S_n$ is a cycle of length 2.

Theorem 1.51. Let $\sigma \in S_n$, then σ can be written uniquely (except for the order) as a product of cycles with pairwise disjoint supports.

Corollary 1.52. Let $\sigma \in S_n$ and $\sigma = \sigma_1 \cdots \sigma_\ell$ be its decomposition as product of disjoint cycles. Then, $\mathrm{ord}(\sigma) = \mathrm{lcm}(\sigma_1, \ldots, \sigma_\ell)$.

Corollary 1.53. Let $\sigma \in S_n$. Then, σ is a product of transpositions.

Definition 1.54. Let $\sigma \in S_n$. The *sign of* σ is $\varepsilon(\sigma) = (-1)^{n-r}$, where r is the number of orbits of σ.

Theorem 1.55. Let $\sigma \in S_n$ be a permutation and $\tau \in S_n$ be a transposition. Then, $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = -\varepsilon(\sigma)$.

Corollary 1.56. Let $\sigma \in S_n$ be such that $\sigma = \tau_1 \cdots \tau_\ell$, where $\tau_i \in S_n$ are transpositions for $i = 1, \ldots, \ell$. Then, $\varepsilon(\sigma) = (-1)^\ell$.

Corollary 1.57. The parity of the number of transpositions in which $\sigma \in S_n$ can be written is invariant.

Corollary 1.58. The function

$$\begin{aligned} \varepsilon : S_n &\longrightarrow \{+1, -1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$$

is a group morphism[3].

1.1.1.5 | Equivalence relations and order relations

Equivalence relations

Definition 1.59. Let A be a set and $\sim$ be a binary relation on A. We say that $\sim$ is an *equivalence relation* if and only if the following properties are satisfied:

1. Reflexivity:
$$a \sim a, \quad \forall a \in A.$$
2. Symmetry:
$$\text{If } a \sim b, \text{ then } b \sim a, \quad \forall a, b \in A.$$
3. Transitivity:
$$\text{If } a \sim b \text{ and } b \sim c, \text{ then } a \sim c, \quad \forall a, b, c \in A.$$

Definition 1.60. Let $\sim$ be an equivalence relation on a set A and $a \in A$. The *equivalence class of* a under $\sim$ is the subset of A:

$$[a] = \bar{a} = \{b \in A : a \sim b\}.$$

Theorem 1.61. Let $\sim$ be an equivalence relation on a set A. The equivalence classes $\sim$ form a partition of A. That is, if $\{\omega_i\}$ are the equivalence classes, then:

1. $\bigcup_{i \in I} \omega_i = A$.
2. If $i, j \in I$ and $\omega_i \cap \omega_j \neq \varnothing$, then $\omega_i = \omega_j$.
3. If $i \in I \implies \omega_i \neq \varnothing$.

Definition 1.62. Let $\sim$ be an equivalence relation on a set A. We define the quotient set, $A/\sim$, as the set of all equivalence classes of $\sim$.

[2] See definition 1.1.
[3] See definition 1.20.

Order relations

Definition 1.63. Let A be a set and $\leq$ be a binary relation on A. We say $\leq$ is a *partial order relation* if and only if the following properties are satisfied:

1. Reflexivity:
$$a \leq a, \quad \forall a \in A.$$
2. Antisymmetry:
$$\text{If } a \leq b \text{ and } b \leq a, \text{ then } a = b, \quad \forall a, b \in A.$$
3. Transitivity:
$$\text{If } a \leq b \text{ and } b \leq c, \text{ then } a \leq c, \quad \forall a, b, c \in A.$$

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

Definition 1.64. Let $(A, \leq)$ be a partially ordered set. We say that $a \in A$ is a *minimal element* if and only if $b \leq a \implies b = a$, $\forall b \in A$. Futhermore, a is a *least element* if and only if $a \leq b$, $\forall b \in A$. Analogously, we say that $a \in A$ is a *maximal element* if and only if $b \geq a \implies b = a$, $\forall b \in A$. We say that $a \in A$ is a greatest element if and only if $a \geq b$, $\forall b \in A$.

Lemma 1.65. Let $(A, \leq)$ be a partially ordered set. If $(A, \leq)$ admits a minimum, this is unique.

Definition 1.66. Let A be a set. A *total order relation* on A is a partial order relation in which any two elements of A are comparable. That is, a total order is a binary relation $\leq$ satisfying the properties of a partial order relation and such that $\forall a, b \in A$, we have $a \leq b$ or $b \leq a$.

Definition 1.67. Let A be a set. A *well-order relation* on A is a total order on A with the property that every nonempty subset of A has a least element. A set A together with a well-order relation is a *well-ordered set*.

Theorem 1.68. All sets can be well-ordered.

1.1.1.6 | Cardinality and combinatorics

Definition 1.69. Let A, B be two sets. We say that A and B have the same cardinal if and only if there exists a bijection $A \to B$.

Definition 1.70. Let A, B be two sets. We say that $|A| \leq |B|$ if and only if there exists an injection function $A \hookrightarrow B$.

Theorem 1.71 (Cantor-Bernstein theorem). Let A, B be two sets. If there is an injection $A \hookrightarrow B$ and an injection $B \hookrightarrow A$, then there is a bijection $A \to B$. Comparative of cardinals is an order relation.

Proposition 1.72. Let A, B be two subsets of a set U. Then,

1. Inclusion–exclusion principle:
$$|A \cup B| = |A| + |B| - |A \cap B|$$
2. $|A \times B| = |A||B|$
3. $|A^c| + |A| = |U|$
4. $|\mathcal{P}(A)| = 2^{|A|}$

Theorem 1.73 (Cantor's theorem). Let A un set, then $|\mathcal{P}(A)| > |A|$.

Corollary 1.74. There is no set containing all sets.

Corollary 1.75. There are infinitely many sets with infinite cardinal:
$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots$$
We denote this cardinals by:
$$\aleph_0 = |\mathbb{N}| \quad \aleph_1 = |\mathcal{P}(\mathbb{N})| \quad \aleph_2 = |\mathcal{P}(\mathcal{P}(\mathbb{N}))| \quad \cdots$$

Proposition 1.76. Let A, B be two finite sets. The set of functions $f : A \to B$ has cardinal $|B|^{|A|}$.

Definition 1.77. Let U be a set and $A \in \mathcal{P}(U)$. We define the *characteristic function of* A as:
$$\begin{aligned} \chi_A : U &\longrightarrow \{0, 1\} \\ r &\longmapsto \begin{cases} 1 & \text{if} \quad r \in A \\ 0 & \text{if} \quad r \notin A \end{cases} \end{aligned}$$

Proposition 1.78. Let U be a set and $A, B \in \mathcal{P}(U)$. Then:

1. $\chi_U = 1$
2. $\chi_{A^c} = 1 - \chi_A$
3. $\chi_{A \cap B} = \chi_A \chi_B$
4. $\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \chi_B$

Proposition 1.79 (Binomial coefficient formulas).

1. $\binom{n}{k} = \frac{n!}{(n-k)!k!}$
2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$
3. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
4. $k\binom{n}{k} = n\binom{n-1}{k-1}$
5. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Proposition 1.80. Let $f : A \to B$ be a function between two sets of the same finite cardinal. The following statements are equivalent:

1. f is injective.
2. f is surjective.
3. f is bijective.

Corollary 1.81. Let $f : A \to B$ be a function between finite sets. Then:

1. If f is injective, then $|A| \leq |B|$.
2. If f is surjective, then $|A| \geq |B|$.

Theorem 1.82 (Pigeonhole principle). Let A, B be two sets such that $|A| = n$ and $|B| = m$ and $f : A \to B$ be a function. If $n > m$, then $\exists a, b \in A$ such that $a \neq b$ $f(a) = f(b)$.

Proposition 1.83 (Combinations without repetition). A combination without repetition is a subset with m elements of a set with n elements. The number of such combinations is $\binom{n}{m}$.

Proposition 1.84 (Combinations with repetition). A combination with repetition is an unordered list with m elements (allowing repetitions) of a set with n elements. The number of such combinations is $\binom{n+m-1}{m}$.

Proposition 1.85 (Variations without repetition). A variation without repetition is an ordered list of length m elements (without repeating them) taken from a set with n elements. The number of such variations is $\frac{n!}{(n-m)!}$.

Proposition 1.86 (Variacions with repetition). A variation with repetition is an ordered list of length m elements (allowing repetitions) taken from a set with n elements. The number of such variations is n^m.

1.1.1.7 | Arithmetic

Integer numbers

For some basic definitions in group and ring theory you might need to refer to sections 1.2.1.1 and 1.2.1.2.

Definition 1.87. Let $a, b \in \mathbb{Z}$. We say that *a is a multiple of b* if there exists $c \in \mathbb{Z}$ such that $a = cb$.

Theorem 1.88. Let $D, d \in \mathbb{Z}$, $d \neq 0$. Then, there are unique $q, r \in \mathbb{Z}$ such that $D = qd + r$ and $0 \leq r \leq |d|$.

Proposition 1.89. Let $a, b \in \mathbb{Z}$. $a\mathbb{Z} \subseteq b\mathbb{Z} \iff b \mid a$.

Corollary 1.90. Let $a, b \in \mathbb{Z}$. $a\mathbb{Z} = b\mathbb{Z} \iff a = \pm b$.

Proposition 1.91. Let $a\mathbb{Z}$, $b\mathbb{Z}$ be two ideals of $\mathbb{Z}$. Then, $\exists! m \in \mathbb{N}$ such that $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. This integer m is called the *least common multiple of a and b*.

Proposition 1.92. Let $a\mathbb{Z}$, $b\mathbb{Z}$ be two ideals of $\mathbb{Z}$. Then, $\exists! d \in \mathbb{N}^*$ such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. This integer d is called the *greatest common divisor of a and b*.

Proposition 1.93. Let $a, b, m, d \in \mathbb{Z}$.

1. If $a \mid m$ and $b \mid m$, then $\operatorname{lcm}(a, b) \mid m$.
2. If $d \mid a$ and $d \mid b$, then $d \mid \gcd(a, b)$.

Definition 1.94. Let $a, b \in \mathbb{Z}$. We say that a and b are *coprime* or *relatively prime* if and only if $\gcd(a, b) = 1$.

Definition 1.95. We say that $p \in \mathbb{Z}$ is *prime* if and only if $p\mathbb{Z}$ is a maximal ideal. The set of prime numbers is denoted by $\mathbb{P}$.

Proposition 1.96. Let $a \in \mathbb{Z}$. Then, $a \in \mathbb{P}$ if and only if a has exactly 4 divisors: a, $-a$, 1 and -1.

Lemma 1.97. Let $a, b, k \in \mathbb{Z}$ such that $a \geq b > 0$. Then, common divisors of a and b are the same as common divisors of $a + kb$ and b.

Theorem 1.98 (Bézout's theorem). Let $a, b \in \mathbb{Z}$, then there exists $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$. Moreover, $\gcd(a, b) = 1 \iff \exists u, v \in \mathbb{Z}$ such that $au + bv = 1$.

Theorem 1.99 (Gauß' theorem). Let $a, b \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

Corollary 1.100. Let $a, b, c \in \mathbb{Z}$ be integers such that a and b are relatively prime. If $a \mid c$ and $b \mid c$, then $ab \mid c$.

Theorem 1.101 (Prime number theorem). Let $x \in \mathbb{R}$. If $\pi(x)$ is the number of prime number less than or equal to x, then $\pi(x) \sim \frac{x}{\log(x)}$.

Theorem 1.102. Let $a, b \in \mathbb{Z}$. Then,

$$\gcd(a, b) \operatorname{lcm}(a, b) = |ab|.$$

Lemma 1.103. Let $p \in \mathbb{P}$ and $a \in \mathbb{Z}$. Then, $p \mid a$ or $\gcd(a, p) = 1$.

Corollary 1.104. Let $a, b \in \mathbb{Z}$ and $p \in \mathbb{P}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Corollary 1.105. Let $p, q \in \mathbb{P}$. If $p \mid q$, then $p = \pm q$.

Theorem 1.106 (Fundamental theorem of arithmetic). Let $n \in \mathbb{N}$ such that $n > 1$. Then, n can be represented uniquely (except for the order) as the product of prime numbers.

Theorem 1.107 (Euclid's theorem). The set $\mathbb{P}$ is infinite.

Theorem 1.108. Let $a, b, c, x, y \in \mathbb{Z}$. The equation $ax + by = c$ has at least a solution if and only if $\gcd(a, b) \mid c$. In this case, if $d = \gcd(a, b)$, $a = a'd$ and $b = b'd$, the set $\mathcal{S}$ of solutions of the equation $ax + by = c$ is

$$S = \{(x_0, y_0) + \lambda(-b', a') : \lambda \in \mathbb{Z}\},$$

where (x_0, y_0) is a particular solution of the equation.

Modular arithmetic

Definition 1.109. Let $n, x, y \in \mathbb{Z}$. We say $x \sim y \iff x - y \in n\mathbb{Z}$. A commonly used notation for this is $x \equiv y \mod n$. The set of equivalence classes under $\sim$ is denoted by $\mathbb{Z}/n\mathbb{Z}$ and its elements are denoted by $\bar{x}$.

Lemma 1.110. $\mathbb{Z}/n\mathbb{Z}$ té n elements.

Proposition 1.111. Addition and multiplication are well-defined in $\mathbb{Z}/n\mathbb{Z}$ if we do it in the following way:

$$\begin{aligned} + : {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} &\longrightarrow {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \\ (\bar{a}, \bar{b}) &\longmapsto \overline{a + b} \end{aligned} \qquad \begin{aligned} \cdot : {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} &\longrightarrow {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \\ (\bar{a}, \bar{b}) &\longmapsto \overline{a \cdot b} \end{aligned}$$

Theorem 1.112. Since $(\mathbb{Z}, +, \cdot)$ is a ring, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring and the projection

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \\ a &\longmapsto \bar{a} \end{aligned}$$

is a ring morphism.

Lemma 1.113. Let $n \in \mathbb{Z}$. Then, $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ has multiplicative inverse if and only if $\gcd(a,n) = 1$.

Corollary 1.114. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a field if and only if $n \in \mathbb{P}$.

Theorem 1.115 (Chinese remainder theorem). Let $m, n \in \mathbb{Z}$ be relatively prime. Then, the function

$$\begin{aligned}\psi : \mathbb{Z}/_{nm\mathbb{Z}} &\longrightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \\ \overline{a}^{mn} &\longmapsto (\overline{a}^{m}, \overline{a}^{n})\end{aligned}$$

is ring isomorphism.

Definition 1.116 (Euler's totient function). Let $n \in \mathbb{N}$. We define the function $\varphi : \mathbb{N} \to \mathbb{N}$ as:

$$\begin{aligned}\varphi(n) = |\{\alpha \in \mathbb{Z}/n\mathbb{Z} : \alpha \text{ is invertible}\}| &= \\ = |\{0 < r \le n : \gcd(r,n) = 1\}|.\end{aligned}$$

Lemma 1.117. Let $m, n \in \mathbb{Z}$ be relatively prime. Then, $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Theorem 1.118 (Euler's theorem). Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $\gcd(a,n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

In particular, $a^{-1} \equiv a^{\varphi(n)-1} \mod n$.

Theorem 1.119 (Fermat's little theorem). Let $p \in \mathbb{P}$. Then, $\varphi(p) = p - 1$ and

$$a^p \equiv a \mod p.$$

In particular, if $\gcd(a,p) = 1$, $a^{p-1} \equiv 1 \mod p$.

1.1.1.8 | Polynomials

Definition 1.120. Let R be a ring. A *polynomial p with coefficients in R* is an expression of the form

$$p = p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

where x is a *variable* or an *indeterminate* and $a_i \in R$ are the *coefficients*. The term a_0 is called *constant term*, and the term a_n, *leading coefficient*. Finally, the set of all polynomials in the variable x and coefficients in R is denoted by $R[x]$.

Definition 1.121. Let $p(x) = \sum_{i=0}^n a_i x^i \in R[x]$ be a polynomial such that $a_n \neq 0$. Then, we define the *degree of $p(x)$* as $\deg p(x) = n$[4].

Definition 1.122. Let $p(x), q(x) \in R[x]$ such that $p(x) = \sum_{i=0}^n a_i x^i \in R[x]$ and $q(x) = \sum_{i=0}^n n_i x^i \in R[x]$. We define the *sum of $p(x)$ and $q(x)$* as:

$$p(x) + q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

We define the *product of $p(x)$ and $q(x)$* as:

$$p(x) \cdot q(x) = \sum_{i=0}^{n} c_i x^i, \quad c_i = \sum_{j=0}^{i} a_i b_{j-i}.$$

Proposition 1.123. Let K be a field. If $p(x), q(x) \in K[x]$ and $p(x), q(x) \neq 0$, then $p(x) \cdot q(x) \neq 0$.

Theorem 1.124 (Euclidian division). Let K be a field. Let $p(x), s(x) \in K[x]$ with $s(x) \neq 0$. Then, $\exists! q(x), r(x) \in K[x]$ such that $p(x) = q(x) \cdot s(x) + r(x)$ and $0 \le \deg(r(x)) < \deg(s(x))$.

Theorem 1.125. Let K be a field. Then, $K[x]$ is a principal ideal, that is, if $I \subset K[x]$ is an ideal, then $\exists p(x) \in K[x]$ such that $I = p(x) \cdot K[x]$.

Definition 1.126. Let K be a field. Let $p(x), q(x) \in K[x]$. Then, $\gcd(p(x), q(x))$ is a generator of the ideal $p(x) \cdot K[x] + q(x) \cdot K[x]$ and $\operatorname{lcm}(p(x), q(x))$ is a generator of the ideal $p(x) \cdot K[x] \cap q(x) \cdot K[x]$.

Definition 1.127. We say that a polynomial $p(x) = \sum_{i=0}^n a_i x^i$ is *monic* if $a_n = 1$.

Theorem 1.128 (Bézout's theorem). Let K be a field and $p(x), q(x) \in K[x]$. Then, $\exists u(x), v(x) \in K[x]$ such that $p(x) \cdot u(x) + q(x) \cdot v(x) = \gcd(p(x), q(x))$.

Definition 1.129. Two polynomials $p(x)$, $q(x)$ are *coprime* or *relatively prime* if and only if $\gcd(p(x), q(x)) = 1$.

Theorem 1.130 (Gauß' theorem). Let K be a field and $p(x), a(x), b(x) \in K[x]$. If $p(x) \mid a(x) \cdot b(x)$ and $\gcd(a(x), p(x)) = 1$, then $p(x) \mid b(x)$.

Definition 1.131. Let K be a field. A polynomial $p(x) \in K[x]$ is *prime* if and only if its ideal $p(x) \cdot K[x]$ is maximal, that is, for all ideals $I \subseteq K[x]$ if $p(x) \cdot K[x] \subset I$, then $I = K[x]$.

Definition 1.132. Let K be a field and $a \in K$. The *evaluation in a* is a function ϕ_a defined as:

$$\begin{aligned}\phi_a : K[x] &\longrightarrow K \\ p(x) &\longmapsto p(a)\end{aligned}$$

Definition 1.133. Let K be a field and $a \in K$. a is a *root of* $p(x)$ if and only if $\phi_a(p(x)) = p(a) = 0$.

Theorem 1.134 (Ruffini's rule). Let K be a field, $p(x) \in K[x]$ and $a \in K$. Then, $x - a \mid p(x) \iff p(a) = 0$.

Definition 1.135. Let K be a field and $p(x) \in K[x]$. Then, $p(x)$ is *irreducible* if and only if $p(x) \cdot K[x]$ is maximal.

Theorem 1.136. Let K be a field and $p(x) \in K[x]$. Then, $p(x)$ has at most $\deg(p(x))$ roots.

Theorem 1.137 (D'Alembert theorem). All non-constant polynomials $p(x) \in \mathbb{C}[x]$ has exactly $\deg(p(x))$ roots.

Corollary 1.138. Let $p(x) \in \mathbb{C}[x]$ be such that $\deg(p(x)) > 1$. Then, $\exists! \alpha, r_1, \ldots, r_n \in \mathbb{C}$ such that

$$p(x) = \alpha(x - r_1) \cdots (x - r_n),$$

where r_i are the roots of $p(x)$ and α is the leading coefficient of $p(x)$.

Corollary 1.139. Let $p(x) \in \mathbb{C}[x]$. The roots of $p(x)$ in $\mathbb{C} \setminus \mathbb{R}$ come in pairs $(r, \overline{r})$, where $\overline{r}$ is the complex conjugate of r.

Theorem 1.140. In $\mathbb{R}[x]$ irreducible polynomials are of degree 1 or degree 2.

[4]To see properties relating degrees of polynomials see proposition 1.127.

1.1.2 Linear algebra

1.1.2.1 | Matrices

Linear systems

Definition 2.1. A *linear equation* is an equation of the form

$$a_1x_1 + \cdots + a_nx_n = b$$

where $x_1, \ldots, x_n$ are the *variables* or *unknowns* and $a_i, b \in \mathbb{R}$, $i = 1, \ldots, n$, are the coefficients of the equation. The term b is usually called *constant term*.

Definition 2.2. A *system of linear equations* is a collection of one or more linear equations involving the same set of variables.

Definition 2.3. Let

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad\vdots \qquad\quad \vdots \qquad\quad \vdots \qquad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

be a system of linear equations. A *solution of a system of equations* is a set of numbers $c_1, \ldots, c_n$ such that

$$a_{i1}c_1 + \cdots + a_{in}c_n = b_i$$

for $i = 1, \ldots, m$. A linear system may behave in three possible ways:

1. The system has a unique solution.
2. The system has infinitely many solutions.
3. The system has no solution.

Definition 2.4. Two systems of equations are *equivalent* if they have the same solutions.

Matrices

Definition 2.5 (Matrix). A *matrix* $\mathbf{A}$ *with coefficients in* $\mathbb{R}$ is a table of real numbers arranged in rows and columns. That is, $\mathbf{A}$ is of the form:

$$\mathbf{A} = (a_{ij}) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

for some values $a_{ij} \in \mathbb{R}$, $i = 1, \ldots, m$ and $j = 1, \ldots, n$. The set of $m \times n$ matrices with real coefficients is denoted by $\mathcal{M}_{m\times n}(\mathbb{R})$[5].

Definition 2.6. Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and $\alpha \in \mathbb{R}$. If $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$, we define the *sum* $\mathbf{A} + \mathbf{B}$ as:

$$\mathbf{A} + \mathbf{B} = (a_{ij} + b_{ij})$$

We define the *product* $\alpha\mathbf{A}$ as:

$$\alpha\mathbf{A} = (\alpha a_{ij})$$

Proposition 2.7 (Properties of addition and scalar multiplication of matrices). The following properties are satisfied:

1. Commutativity:
$$\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$$
for all $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{R})$.
2. Associativity:
$$(\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$$
for all $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathcal{M}_{m\times n}(\mathbb{R})$.
3. Additive identity element: $\exists \mathbf{0} \in \mathcal{M}_{m\times n}(\mathbb{R})$ such that
$$\mathbf{A} + \mathbf{0} = \mathbf{A}$$
for all $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$.
4. Additive inverse element: $\forall \mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})\ \exists(-\mathbf{A}) \in \mathcal{M}_{m\times n}(\mathbb{R})$ such that
$$\mathbf{A} + (-\mathbf{A}) = \mathbf{0}$$
5. Distributivity:
$$(\alpha + \beta)\mathbf{A} = \alpha\mathbf{A} + \beta\mathbf{A}$$
for all $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and all $\alpha, \beta \in \mathbb{R}$.

Definition 2.8. Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and $\mathbf{B} \in \mathcal{M}_{n\times p}(\mathbb{R})$. We define the *product* $\mathbf{AB}$ as

$$\mathbf{AB} = (c_{ij}) \quad \text{where } c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

Proposition 2.9 (Properties of matrix product). The following properties are satisfied:

1. Associativity:
$$(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$$
for all $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$, $\mathbf{B} \in \mathcal{M}_{n\times p}(\mathbb{R})$ and $\mathbf{C} \in \mathcal{M}_{p\times q}(\mathbb{R})$.
2. Multiplicative identity element: $\exists \mathbf{I}_n \in \mathcal{M}_n(\mathbb{R})$ such that
$$\begin{aligned} \mathbf{A}\mathbf{I}_n &= \mathbf{A} \quad \forall \mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R}) \text{ and} \\ \mathbf{I}_n\mathbf{A} &= \mathbf{A} \quad \forall \mathbf{A} \in \mathcal{M}_{n\times p}(\mathbb{R}) \end{aligned}$$
3. Distributivity:
$$(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC},$$
for all $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and $\mathbf{C} \in \mathcal{M}_{n\times p}(\mathbb{R})$.

Definition 2.10. We say that a matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ is *invertible* if there is a matrix $\mathbf{B} \in \mathcal{M}_n(\mathbb{R})$ satisfying

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n$$

The set of invertible matrices of size n over $\mathbb{R}$ is denoted by $\mathrm{GL}_n(\mathbb{R})$[6].

Lemma 2.11. The product of invertible matrices is invertible.

[5] In the case when $m = n$ we will denote $\mathcal{M}_{n\times n}(\mathbb{R})$ by $\mathcal{M}_n(\mathbb{R})$.
[6] Or more generally, the set of invertible matrices of size n over a field (see definition 1.86) K is denoted by $\mathrm{GL}_n(K)$.

Echelon form of a matrix

Definition 2.12. Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. The *i-th pivot of* $\mathbf{A}$ is the first nonzero element in the i-th row of $\mathbf{A}$.

Definition 2.13 (Row echelon form). A matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ is in *row echelon form* if:

- All rows consisting of only zeros are at the bottom.
- The pivot of a nonzero row is always strictly to the right of the pivot of the row above it.

Definition 2.14 (Reduced row echelon form). A matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ is in *reduced row echelon form* if:

- It is in row echelon form.
- Pivots are equal to 1.
- Each column containing a pivot has zeros in all its other entries.

Theorem 2.15 (Gauß' theorem). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. Then, there is a matrix $\mathbf{P} \in \mathrm{GL}_m(\mathbb{R})$ such that $\mathbf{PA} = \mathbf{A}'$ is in reduced row echelon form. Moreover, $\mathbf{A}'$ is uniquely determined by $\mathbf{A}$.

Theorem 2.16 (PAQ reduction theorem). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. Then, there exist matrices $\mathbf{P} \in \mathrm{GL}_m(\mathbb{R})$ and $\mathbf{Q} \in \mathrm{GL}_n(\mathbb{R})$ such that

$$\mathbf{PAQ} = \left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right).$$

The number r is uniquely determined by $\mathbf{A}$.

Rank of a matrix

Definition 2.17 (Rank). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix and suppose

$$\mathbf{PAQ} = \left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right)$$

for some matrices $\mathbf{P} \in \mathcal{M}_m(\mathbb{R})$ and $\mathbf{Q} \in \mathcal{M}_n(\mathbb{R})$. We define the *rank of* $\mathbf{A}$, denoted by $\operatorname{rank}\mathbf{A}$, as the number ones in the matrix $\mathbf{PAQ}$, that is, $\operatorname{rank}\mathbf{A} := r$.

Proposition 2.18. Let $\mathbf{A}, \mathbf{A}' \in \mathcal{M}_{m\times n}(\mathbb{R})$, $\mathbf{B}, \mathbf{B}' \in \mathcal{M}_{1\times n}(\mathbb{R})$ and $\mathbf{P} \in \mathrm{GL}_m(\mathbb{R})$ be matrices. Suppose we have a system of linear equations $\mathbf{Ax} = \mathbf{B}$. If $\mathbf{P}(\mathbf{A} \mid \mathbf{B}) = (\mathbf{A}' \mid \mathbf{B}')$[7], then the systems $\mathbf{Ax} = \mathbf{B}$ and $\mathbf{A}'\mathbf{x} = \mathbf{B}'$ are equivalent.

Corollary 2.19. The reduced row echelon form of an invertible matrix is the identity matrix.

Definition 2.20 (Transposition). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. If $\mathbf{A} = (a_{ij})$, we define the *transpose* $\mathbf{A}^{\mathrm{T}}$ *of* $\mathbf{A}$ as the matrix $\mathbf{A}^{\mathrm{T}} = (b_{ij})$, where $b_{ij} = a_{ji}$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

Proposition 2.21. Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. Then, $\operatorname{rank}\mathbf{A} = \operatorname{rank}\mathbf{A}^{\mathrm{T}}$.

Theorem 2.22 (Rouché-Frobenius theorem). Let $\mathbf{Ax} = \mathbf{B}$ be a system of equations with n variables. The system is:

- *determined and consistent* if and only if
$$\operatorname{rank}\mathbf{A} = \operatorname{rank}(\mathbf{A} \mid \mathbf{B}) = n$$
- *indeterminate with s free variables* if and only if
$$\operatorname{rank}\mathbf{A} = \operatorname{rank}(\mathbf{A} \mid \mathbf{B}) = n - s$$
- *inconsistent* if and only if
$$\operatorname{rank}\mathbf{A} \neq \operatorname{rank}(\mathbf{A} \mid \mathbf{B})$$

Determinant of a matrix

Definition 2.23 (Determinant). A determinant is a function $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ satisfying the following properties:

1. If $\mathbf{A} = (\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_n)$, where $\mathbf{a}_i$ are column vectors in $\mathbb{R}^n$ for $i = 1, \ldots, n$ and $\mathbf{a}_j = \lambda\mathbf{u} + \mu\mathbf{v}$ for some other column vectors $\mathbf{u}$ and $\mathbf{v}$, then:
$$\begin{aligned} \det\mathbf{A} &= \det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_j \mid \cdots \mid \mathbf{a}_n) = \\ &= \det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_{j-1} \mid \lambda\mathbf{u} + \mu\mathbf{v} \mid \mathbf{a}_{j+1} \mid \cdots \mid \mathbf{a}_n) = \\ &= \lambda\det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_{j-1} \mid \mathbf{u} \mid \mathbf{a}_{j+1} \mid \cdots \mid \mathbf{a}_n) + \\ &\quad + \mu\det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_{j-1} \mid \mathbf{v} \mid \mathbf{a}_{j+1} \mid \cdots \mid \mathbf{a}_n) \end{aligned}$$
2. The determinant changes its sign whenever two columns are swapped.
3. $\det\mathbf{I}_n = 1$ for all $n \in \mathbb{N}$.

Lemma 2.24. Whenever two columns of a matrix are identical, the determinant is 0.

Proposition 2.25. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a matrix in its row echelon form. If $\mathbf{A} = (a_{ij})$, then:

$$\det\mathbf{A} = \prod_{i=1}^{n} a_{ii}$$

Proposition 2.26. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a matrix. The following are equivalent:

1. $\mathbf{A}$ is not invertible.
2. $\operatorname{rank}\mathbf{A} < n$.
3. $\det\mathbf{A} = 0$.

Theorem 2.27. Let $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ be a determinant. Then, for all matrices $\mathbf{A}, \mathbf{B} \in \mathcal{M}_n(\mathbb{R})$:

$$\det(\mathbf{AB}) = \det\mathbf{A}\det\mathbf{B}.$$

Corollary 2.28. Let $\det, \det' : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ be two determinants. Then, for all matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$:

$$\det\mathbf{A} = \det{}'\mathbf{A}$$

[7] Here $(\mathbf{A} \mid \mathbf{B})$ denotes the augmented matrix obtained by appending the columns of $\mathbf{B}$ to the columns of $\mathbf{A}$.

Proposition 2.29. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. Then:

$$\det \mathbf{A} = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

Proposition 2.30. For all matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$:

$$\det \mathbf{A} = \det \mathbf{A}^{\mathrm{T}}$$

Proposition 2.31. Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$. We denote by $\mathbf{A}_{ij}$ the square matrix obtained from $\mathbf{A}$ by removing the i-th row and j-th column. Then, for every $i \in \{1, \ldots, n\}$,

$$\det \mathbf{A} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ij}.$$

Definition 2.32. Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$. We define the *cofactor matrix* $\mathbf{C}$ *of* $\mathbf{A}$ as:

$$\mathbf{C} = (b_{ij}), \quad \text{where } b_{ij} = (-1)^{i+j} \det \mathbf{A}_{ij}\text{[8]}.$$

We define the *adjugate matrix* $\operatorname{adj} \mathbf{A}$ *of* $\mathbf{A}$ as:

$$\operatorname{adj} \mathbf{A} = \mathbf{C}^{\mathrm{T}}.$$

Theorem 2.33. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. Then:

$$\mathbf{A} \operatorname{adj} \mathbf{A} = (\det \mathbf{A}) \mathbf{I}_n$$

Moreover if $\det \mathbf{A} \neq 0$, then:

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \operatorname{adj} \mathbf{A}$$

1.1.2.2 | Vector spaces

Introduction and basic definitions

Definition 2.34. A *vector space over a field*[9] K is a set V together with two operations

$$\begin{aligned} + : V \times V &\longrightarrow V \\ (\mathbf{v}_1, \mathbf{v}_2) &\longmapsto \mathbf{v}_1 + \mathbf{v}_2 \end{aligned} \qquad \begin{aligned} \cdot : K \times V &\longrightarrow V \\ (\lambda, \mathbf{v}) &\longmapsto \lambda \cdot \mathbf{v} \end{aligned}$$

that satisfy the following properties:

1. $\mathbf{v}_1 + (\mathbf{v}_2 + \mathbf{v}_3) = (\mathbf{v}_1 + \mathbf{v}_2) + \mathbf{v}_3 \quad \forall \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V$.
2. $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_2 + \mathbf{v}_1 \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$.
3. $\exists \mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v} \quad \forall \mathbf{v} \in V$.
4. $\forall \mathbf{v} \in V$ there exists $-\mathbf{v} \in V$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.
5. $\lambda \cdot (\mu \cdot \mathbf{v}) = (\lambda\mu) \cdot \mathbf{v} \quad \forall \mathbf{v} \in V$ and $\forall \lambda, \mu \in K$.
6. $1 \cdot \mathbf{v} = \mathbf{v} \quad \forall \mathbf{v} \in V$, where 1 denotes the multiplicative identity element in K.
7. $\lambda \cdot (\mathbf{v}_1 + \mathbf{v}_2) = \lambda \cdot \mathbf{v}_1 + \lambda \cdot \mathbf{v}_2 \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$ and $\forall \lambda \in K$.
8. $(\lambda + \mu) \cdot \mathbf{v} = \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{v} \quad \forall \mathbf{v} \in V$ and $\forall \lambda, \mu \in K$.

In these conditions, we say that $(V, +, \cdot)$ is a vector space[10].

Definition 2.35. Let V be a vector space over a field K and $U \subseteq V$ be a subset of V. Then, U is a vector space over K if the following property is satisfied:

$$\lambda \mathbf{u}_1 + \mu \mathbf{u}_2 \in U \quad \forall \mathbf{u}_1, \mathbf{u}_2 \in U \text{ and } \forall \lambda, \mu \in K$$

Definition 2.36. Let V be a vector space and $U \subseteq V$. U is a *vector subspace of* V if it's itself a vector space with the operations defined in V.

Definition 2.37. Let V be a vector space over a field K. A *linear combination of the vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ is a vector of the form

$$a_1 \mathbf{v}_1 + \cdots + a_n \mathbf{v}_n$$

where $a_i \in K$, $i = 1, \ldots, n$.

Definition 2.38. Let V be a vector space over a field K and $U \subseteq V$. The set

$$\langle U \rangle = \{a_1 \mathbf{u}_1 + \cdots + a_n \mathbf{u}_n : a_i \in K, \mathbf{u}_i \in U, i = 1, \ldots, n\}$$

is called *subspace generated by* U.

Lemma 2.39. Let V be a vector space and $U \subseteq V$. Then, $\langle U \rangle$ is a vector subspace of V. Moreover, $\langle U \rangle$ is the smallest subspace containing U.

Definition 2.40. Let V be a vector space and $U \subseteq V$. We say that U is a *generating set of* V if $\langle U \rangle = V$.

Linear independence

Definition 2.41. Let V be a vector space over a field K. The vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ are *linearly independent* if the unique solution of the equation

$$a_1 \mathbf{v}_1 + \cdots + a_n \mathbf{v}_n = 0$$

for $a_i \in K$, $i = 1, \ldots, n$, is $a_1 = \cdots = a_n = 0$. Otherwise we say that the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are *linearly dependent*.

Lemma 2.42. Let V be a vector space. The vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly dependent if and only if one of them is a linear combination of the others.

Definition 2.43. Let V be a vector space. A *basis of* V is an ordered set $\mathfrak{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ of vectors of V such that:

1. $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle = V$.
2. $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent.

Lemma 2.44 (Steinitz exchange lemma). Let V be a vector space, $\mathfrak{B}$ be bases of V be and $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$ be linearly independent vectors of V. Then, we can exchange k appropriate vectors of $\mathfrak{B}$ by $\mathbf{v}_1, \ldots, \mathbf{v}_k$ to define a new basis.

[8] $\mathbf{C}$ is usually denoted as cof $\mathbf{A}$.

[9] See definition 1.86.

[10] For simplicity we will denote the vector space only by V and if the context is clear we won't refer to its associated field. Moreover sometimes we will also omit the product $\cdot$ between a scalar and a vector.

Corollary 2.45. Let V be a vector space that has a finite basis $\mathfrak{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$. Then, all basis of V be are finite and they have the same number (n) of vectors.

Lemma 2.46. Let V be a vector space. Suppose we have a generating set $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ of V. Then, V be admits a basis formed with a subset of S.

Definition 2.47. Let V be a finite vector space. The *dimension of* V, denoted by $\dim V$, is the number of vectors in any basis of V.

Definition 2.48. Let V be a finite vector space over a field K, $\mathfrak{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be a basis of V be and $\mathbf{v} \in V$. Suppose

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$$

for some $a_i \in K$, $i = 1, \dots, n$. We call $(a_1, \dots, a_n) \in K^n$ *coordinates of* $\mathbf{v}$ *on the basis* $\mathfrak{B}$ and we denote it by $[\mathbf{v}]_{\mathfrak{B}}$.

Proposition 2.49. Let V be a vector space. If $\dim V < \infty$, the maximum number of linearly independent vectors is equal to $\dim V$. If $\dim V = \infty$, there is no such maximum.

Proposition 2.50. Let V be a vector space of dimension n. Then, n is de minimum size of a generating set of V.

Proposition 2.51. Let V be a finite vector space and U be a vector subspace of V. Then, $\dim U \leq \dim V$ and

$$\dim U = \dim V \iff U = V$$

Sum of subspaces

Lemma 2.52. Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. Then, the intersection $U \cap W$ is a vector subspace of V.

Definition 2.53. Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. The *sum of* U *and* W is:

$$U + W = \langle U \cup W \rangle = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \mathbf{w} \in W\}$$

Proposition 2.54 (Graßmann formula). Let V be a finite vector space and $U, W \subseteq V$ be two vector subspace of V. Then:

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$$

Lemma 2.55. Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. Then, $U \cap W = \{0\}$ if and only if all vectors $\mathbf{v} \in U + W$ can be written uniquely as $\mathbf{v} = \mathbf{u} + \mathbf{w}$, with $\mathbf{u} \in U$ and $\mathbf{w} \in W$.

Definition 2.56 (Direct sum). Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. Then, the sum $U + W$ is *direct* if $U \cap W = \{0\}$. In this case we denote the sum as $U \oplus W$. More generally, if $U_1, \dots, U_n \subseteq V$ are vector subspaces of V, the sum $U = U_1 + \cdots + U_n$ is direct if all vector $\mathbf{u} \in U$ can be written uniquely as $\mathbf{u} = \mathbf{u}_1 + \cdots + \mathbf{u}_n$, where $\mathbf{u}_i \in U_i$ for $i = 1, \dots, n$. In this case we denote the sum by $U_1 \oplus \cdots \oplus U_n$.

Rank of a matrix

Definition 2.57. Let $\mathbf{A} \in \mathcal{M}_{n\times m}(\mathbb{R})$. The *row rank of* $\mathbf{A}$ is the dimension of the subspace generated by the rows of $\mathbf{A}$ in $\mathbb{R}^m$. Analogously, the *column rank of* $\mathbf{A}$ is the dimension of the subspace generated by the columns of $\mathbf{A}$ in $\mathbb{R}^n$.

Proposition 2.58. Let $\mathbf{A} \in \mathcal{M}_{n\times m}(\mathbb{R})$. Then, the row rank of $\mathbf{A}$ is equal to the column rank of $\mathbf{A}$. Therefore, we refer to it simply as *rank of* $\mathbf{A}$ or $\operatorname{rank} \mathbf{A}$.

Definition 2.59. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. A *minor of order* k *of* $\mathbf{A}$ is a submatrix $\mathbf{A}' \in \mathcal{M}_k(\mathbb{R})$ obtained from $\mathbf{A}$ selecting k rows and k columns of $\mathbf{A}$.

Proposition 2.60. Let $\mathbf{A} \in \mathcal{M}_{n\times m}(\mathbb{R})$. Then:

$$\operatorname{rank} \mathbf{A} = \max\{k : \mathbf{A} \text{ has an invertible minor of order } k\}$$

Quotient vector space

Definition 2.61. Let V be a vector space and $U \subseteq V$ be a vector subspace. We say that $W \subseteq V$ is a *complementary subspace of* U if $U \oplus W = V$.

Definition 2.62. Let V be a finite vector space of dimension n and $U \subseteq V$ be a vector subspace of dimension m. Then, there exists a complementary subspace of U and its dimension is $n - m$.

Definition 2.63. Let V be a vector space and $U \subseteq V$ be a vector subspace. We say the vectors $\mathbf{v}_1, \mathbf{v}_2 \in V$ are *equivalent modulo* U, $\mathbf{v}_1 \sim_U \mathbf{v}_2$, if $\mathbf{v}_1 - \mathbf{v}_2 \in U$.

Lemma 2.64. Let V be a vector space and $U \subseteq V$ be a vector subspace. Then, $\sim_U$ is an equivalence relation and, moreover, if $\mathbf{v} \in V$ the *equivalence class* $[\mathbf{v}]$ *of* $\mathbf{v}$ is:

$$[\mathbf{v}] = \mathbf{v} + U := \{\mathbf{v} + \mathbf{u} : \mathbf{u} \in U\}$$

Definition 2.65. Let V be a vector space over a field K and $U \subseteq V$ be a vector subspace. We define the *quotient space* V/U *under* $\sim_U$ as the set of equivalence classes with the operations defined as:

$$[\mathbf{v}_1] + [\mathbf{v}_2] = [\mathbf{v}_1 + \mathbf{v}_2] \qquad \lambda[\mathbf{v}_1] = [\lambda\mathbf{v}_1]$$

for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and all $\lambda \in K$.

Proposition 2.66. Let V be a vector space over a field K and $U \subseteq V$ be a vector subspace. The set V/U together with the two operations defined above is a vector space over K.

Proposition 2.67. Let V be a finite vector space of dimension n and $U \subseteq V$ be a vector subspace. Then:

$$\dim \left({}^{V}\!/_{U} \right) = \dim V - \dim U$$

1.1.2.3 | Linear maps

Definition 2.68. Let U, V be two vector spaces over a field K. A function $f : U \to V$ is a *linear map* if $\forall \mathbf{u}_1, \mathbf{u}_2 \in U$ and $\forall \lambda \in K$ the following two conditions are satisfied:

1. $f(\mathbf{u}_1 + \mathbf{u}_2) = f(\mathbf{u}_1) + f(\mathbf{u}_2)$.
2. $f(\lambda \mathbf{u}_1) = \lambda f(\mathbf{u}_1)$.

Proposition 2.69. Let U, V be two vector spaces over a field K. Then, if $f : U \to V$ is a linear map, $\forall \mathbf{u}_1, \mathbf{u}_2 \in U$ and $\forall \lambda, \mu \in K$ we have:

1. $f(\mathbf{0}) = \mathbf{0}$.
2. $f(-\mathbf{u}_1) = -f(\mathbf{u}_1)$.
3. $f(\lambda \mathbf{u}_1 + \mu \mathbf{u}_2) = \lambda f(\mathbf{u}_1) + \mu f(\mathbf{u}_2)$.

Proposition 2.70. Let U, V, W be three vector spaces. If $f : U \to V$ and $g : V \to W$ are linear maps, then $g \circ f : U \to W$ is a linear map.

Proposition 2.71. Let U, V be two vector spaces. If $f : U \to V$ is a bijective linear map, then $f^{-1} : U \to V$ is a linear map.

Proposition 2.72. Let U, V be two vector spaces, $f : U \to V$ be a linear map and $W \subseteq U$ and $Z \subseteq V$ be vector subspaces. Then:

1. $f(W) = \{f(\mathbf{w}) : \mathbf{w} \in W\} \subseteq V$ is a vector subspace.
2. $f^{-1}(Z) = \{\mathbf{u} \in U : f(\mathbf{u}) \in Z\} \subseteq U$ is a vector subspace.

In particular, $f(V)$ is denoted by $\operatorname{im} f$ and $f^{-1}(\{0\})$ is denoted by $\ker f$ and these subspaces are called *image of* f and *kernel of* f, respectively. More precisely, their definitions are:

$$\operatorname{im} f = \{f(\mathbf{u}) : \mathbf{u} \in U\} \qquad \ker f = \{\mathbf{u} \in U : f(\mathbf{u}) = 0\}$$

Proposition 2.73. Let U, V be two vector spaces and $f : U \to V$ be a linear map. Then:

1. f is injective if and only if $\ker f = \{0\}$
2. f is surjective if and only if $\operatorname{im} f = V$.

Corollary 2.74. Let U, V be two finite vector spaces and $f : U \to V$ be a linear map. Then:

1. f is injective if and only if $\dim(\ker f) = 0$
2. f is surjective if and only if $\dim(\operatorname{im} f) = \dim V$.

Definition 2.75.

- A monomorphism is an injective linear map.
- An epimorphism is a surjective linear map.
- An isomorphism is a bijective linear map.
- An endomorphism is a linear map from a vector space to itself.
- An automorphism is a bijective endomorphism.

Definition 2.76. We say that two vector spaces U and V are *isomorphic*, $V \cong U$, if there exists an isomorphism between them.

Proposition 2.77. Let U, V be two vector spaces and $f : U \to V$ be a monomorphism. If $\mathbf{u}_1, \ldots, \mathbf{u}_n \in U$ are linearly independent vectors, then $f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n)$ are linearly independent.

Lemma 2.78. Let U, V be two vector spaces and $f : U \to V$ be a linear map. If $\mathbf{u}_1, \ldots, \mathbf{u}_n \in U$, then:

$$\langle f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n) \rangle = f(\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle)$$

Corollary 2.79. Let U, V be two vector spaces and $f : U \to V$ be an epimorphism. If $\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle = U$, then $\langle f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n) \rangle = V$.

Corollary 2.80. Let U, V be two vector spaces and $f : U \to V$ be an isomorphism. If $(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ is a basis of U, then $(f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n))$ is a basis of V.

Theorem 2.81 (Coordination theorem). Let V be a finite vector space over a field K of dimension n and $\mathfrak{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V. Then, the function $f : K^n \to V$ defined by

$$f(a_1, \ldots, a_n) = a_1 \mathbf{v}_1 + \cdots a_n \mathbf{v}_n$$

is a isomorphism.

Corollary 2.82. Two finite vector spaces are isomorphic if and only if they have the same dimension.

Isomorphism theorems

Theorem 2.83 (First isomorphism theorem). Let U, V be two vector spaces and $f : U \to V$ be a linear map. Then, there exists an isomorphism $\tilde{f} : U/\ker f \to \operatorname{im} f$ satisfying $f = \tilde{f} \circ \pi$, where $\pi : U \to U/\ker f$, $\pi(\mathbf{u}) = [\mathbf{u}]$.

$$\begin{tikzcd}
U \arrow[r, "f"] \arrow[d, "\pi"'] & \operatorname{im} f \\
U/\ker f \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$

Figure 1.1.2

Corollary 2.84. Let U, V be two vector spaces such that $\dim U = n$ and let $f : U \to V$ be a linear map. Then:

$$\dim(\ker f) + \dim(\operatorname{im} f) = n$$

Corollary 2.85. Let U, V be two finite vector spaces of dimensions n and $f : U \to V$ be a linear map. Then:

$$f \text{ is injective} \iff f \text{ is surjective} \iff f \text{ is bijective}$$

Theorem 2.86 (Second isomorphism theorem). Let V be a vector space and $U, W \subseteq V$ be two vector subspaces. Then, there exists an isomorphism

$$U/_{U \cap W} \cong U + W/_{W}$$

Theorem 2.87 (Third isomorphism theorem). Let U, V, W be three vector spaces such that $W \subseteq U \subseteq V$. Then, there exists an isomorphism

$$\left.{}^{(V/W)}\middle/_{(U/W)}\right. \cong \left.{}^{V}\middle/_{U}\right.$$

Theorem 2.88. Let U, V be two vector spaces over a field K, $\mathfrak{B} = (\mathbf{u}_1, \dots, \mathbf{u}_n)$ be a basis of U and $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ be any vectors of V. Then, there exists a unique linear map $f : U \to V$ such that $f(\mathbf{u}_i) = \mathbf{v}_i$, $i = 1, \dots, n$.

Matrix of a linear map

Proposition 2.89. Let U, V be two finite vector spaces over a field K with $\dim U = n$ and $\dim V = m$, $\mathfrak{B}$ and $\mathfrak{B}'$ be bases of U be and V respectively and $f : U \to V$ be a linear map. Then, there exists a matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(K)$ such that $\forall \mathbf{u} \in U$:

$$[f(\mathbf{u})]_{\mathfrak{B}'} = \mathbf{A}[\mathbf{u}]_{\mathfrak{B}}$$

The matrix $\mathbf{A}$ is called *matrix of f in the basis $\mathfrak{B}$ and $\mathfrak{B}'$* and it is denoted by $[f]_{\mathfrak{B},\mathfrak{B}'}$[11].

Corollary 2.90. Let V be a finite vector space, $\mathfrak{B}$ and $\mathfrak{B}'$ be two basis of V respectively and $\mathrm{id} : V \to V$ be the identity linear map. Then, $\forall \mathbf{u} \in V$ we have:

$$[\mathbf{u}]_{\mathfrak{B}'} = [\mathrm{id}]_{\mathfrak{B},\mathfrak{B}'}[\mathbf{u}]_{\mathfrak{B}}$$

The matrix $[\mathrm{id}]_{\mathfrak{B},\mathfrak{B}'}$ is called *change-of-basis matrix*.

Proposition 2.91. Let U, V, W be three vector spaces, $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ be bases of U, V and W respectively and $f : U \to V$ and $g : V \to W$ be linear maps. Then, $g \circ f : U \to W$ has the following matrix in the basis $\mathfrak{B}$ and $\mathfrak{B}''$:

$$[g \circ f]_{\mathfrak{B},\mathfrak{B}''} = [g]_{\mathfrak{B}',\mathfrak{B}''}[f]_{\mathfrak{B},\mathfrak{B}'}$$

Corollary 2.92. Let V be a finite vector space, $\mathfrak{B}$ and $\mathfrak{B}'$ be two basis of V. Then, the matrix $[id]_{\mathfrak{B},\mathfrak{B}'}$ is invertible and

$$([\mathrm{id}]_{\mathfrak{B},\mathfrak{B}'})^{-1} = [\mathrm{id}]_{\mathfrak{B}',\mathfrak{B}}$$

Corollary 2.93. Let U, V be two finite vector spaces, $\mathfrak{B}$ and $\mathfrak{B}'$ be bases of U and V respectively and $f : U \to V$ be a linear map. Then:

1. f is injective $\iff \operatorname{rank}[f]_{\mathfrak{B},\mathfrak{B}'} = \dim U$.
2. f is surjective $\iff \operatorname{rank}[f]_{\mathfrak{B},\mathfrak{B}'} = \dim V$.

Corollary 2.94. Let U, V be two finite vector spaces. A linear map $f : U \to V$ is an isomorphism if and only if there exist basis $\mathfrak{B}$ and $\mathfrak{B}'$ of U and V respectively such that $[f]_{\mathfrak{B},\mathfrak{B}'}$ is invertible.

Proposition 2.95 (Change of basis formula). Let U, V be two finite vector spaces, $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be bases of U, $\mathfrak{B}_1'$ and $\mathfrak{B}_2'$ be bases of V and $f : U \to V$ be a linear map. Then:

$$[f]_{\mathfrak{B}_2,\mathfrak{B}_2'} = [\mathrm{id}]_{\mathfrak{B}_1',\mathfrak{B}_2'}[f]_{\mathfrak{B}_1,\mathfrak{B}_1'}[\mathrm{id}]_{\mathfrak{B}_2,\mathfrak{B}_1}$$

Lemma 2.96. Let U, V be two finite vector spaces over a field K with $\dim U = n$ and $\dim V = m$ and $\mathfrak{B}$ and $\mathfrak{B}'$ be bases of U be and V respectively. Then, any matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(K)$ determines a linear map $f : U \to V$ with $[f]_{\mathfrak{B},\mathfrak{B}'} = \mathbf{A}$.

Theorem 2.97. Let U, V be two finite vector spaces and $f : U \to V$ be a linear map. Then, there exist basis $\mathfrak{B}$ of U and $\mathfrak{B}'$ of V such that:

$$[f]_{\mathfrak{B},\mathfrak{B}'} = \left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right)$$

where $r = \dim(\operatorname{im} f)$.

Dual space

Lemma 2.98. Let U, V be two finite vector spaces over a field K. Then, the set

$$\mathcal{L}(U, V) := \{f : f \text{ is a linear map from } U \text{ to } V\}^{12}$$

is a vector space over K with the operations defined as:

1. $(f + g)(\mathbf{u}) = f(\mathbf{u}) + f(\mathbf{u}) \quad \forall f, g \in \mathcal{L}(U, V)$ and $\forall \mathbf{u} \in U$.
2. $(f\lambda)(\mathbf{u}) = \lambda f(\mathbf{u}) \quad \forall f, g \in \mathcal{L}(U, V)$, $\forall \mathbf{u} \in U$ and $\forall \lambda \in K$.

Proposition 2.99. Let U, V be two finite vector spaces over a field K with $\dim U = n$ and $\dim V = m$. Then, for all basis $\mathfrak{B}$ of U be and $\mathfrak{B}'$ of V, the function

$$\begin{aligned} \mathcal{L}(U, V) &\longrightarrow \mathcal{M}_{m\times n}(K) \\ f &\longmapsto [f]_{\mathfrak{B},\mathfrak{B}'} \end{aligned}$$

is a isomorphism.

Corollary 2.100. Let U, V be two finite vector spaces with $\dim U = n$, $\dim V = m$. Then, $\dim \mathcal{L}(U, V) = nm$.

Definition 2.101. Let V be a vector space over a field K. We define the *dual space V^* of V* as:

$$V^* := \mathcal{L}(V, K)$$

Proposition 2.102. Let V be a finite vector space over a field K with $\dim V = n$ and $\mathfrak{B}$ be a basis of V. Then, the function

$$\begin{aligned} V^* &\longrightarrow \mathcal{M}_{1\times n}(K) \\ \omega &\longmapsto [\omega]_{\mathfrak{B},1} \end{aligned}$$

is a isomorphism. Therefore, $\dim V^* = \dim V$.

Definition 2.103. We define the *Kronecker delta δ_{ij}* as the function:

$$\delta_{ij} = \begin{cases} 0 & \text{if} \quad i \neq j \\ 1 & \text{if} \quad i = j \end{cases}$$

Definition 2.104. Let V be a finite vector space and $\mathfrak{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be a basis of V. We define the *dual basis $\mathfrak{B}^*$ of $\mathfrak{B}$* as the basis of V^* formed by $(\eta_1, \dots, \eta_n)$ where

$$\eta_i(\mathbf{v}_j) = \delta_{ij}$$

[11] If $U = V$ and $\mathfrak{B} = \mathfrak{B}'$, we denote $[f]_{\mathfrak{B},\mathfrak{B}}$ simply by $[f]_{\mathfrak{B}}$.
[12] If $U = V$, we denote $\mathcal{L}(V, V)$ simply as $\mathcal{L}(V)$.

Lemma 2.105. Let V be a vector space over a field K, $\mathfrak{B}$ be a basis of V and $(\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*)$ be the dual basis of $\mathfrak{B}$. Then, $\forall \mathbf{v} \in V$:

$$[\mathbf{v}]_{\mathfrak{B}} = (\mathbf{v}_1^*(\mathbf{v}), \ldots, \mathbf{v}_n^*(\mathbf{v})) \in K^n$$

Lemma 2.106. Let V be a vector space over a field K, $\mathfrak{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\mathfrak{B}^*$ be the dual basis of $\mathfrak{B}$. Then, $\forall \omega \in V^*$:

$$[\omega]_{\mathfrak{B}^*} = (\omega(\mathbf{v}_1), \ldots, \omega(\mathbf{v}_n)) \in K^n$$

Definition 2.107 (Dual map). Let U, V be two vector spaces over a field K and $f \in \mathcal{L}(U, V)$. The function f^* defined by

$$\begin{aligned} f^* : U^* &\longrightarrow V^* \\ \omega &\longmapsto \omega \circ f \end{aligned}$$

is a linear map and it's called *dual map of f*.

Theorem 2.108. Let U, V be two finite vector spaces, $\mathfrak{B}$ and $\mathfrak{B}'$ be bases of U and V respectively and $f \in \mathcal{L}(U, V)$. Then:

$$[f^*]_{\mathfrak{B}'^*, \mathfrak{B}^*} = \left([f]_{\mathfrak{B}, \mathfrak{B}'}\right)^{\mathrm{T}}$$

Double dual space

Definition 2.109 (Double dual space). Let V be a vector space over a field K. The *double dual space V^{**} of V* is defined as:

$$V^{**} := (V^*)^* = \mathcal{L}(V^*, K)$$

Proposition 2.110. Let V be a vector space over a field K and $\mathbf{v} \in V$. We define the function:

$$\begin{aligned} \phi_{\mathbf{v}} : V^* &\longrightarrow K \\ \omega &\longmapsto \omega(\mathbf{v}) \end{aligned}$$

which is linear. This map induces an injective linear map Φ defined by:

$$\begin{aligned} \Phi : V &\longrightarrow V^{**} \\ \mathbf{v} &\longmapsto \phi_{\mathbf{v}} \end{aligned}$$

Moreover, if $\dim V < \infty$, Φ is a natural isomorphism[13].

Annihilator space

Definition 2.111. Let V be a vector space and $U \subseteq V^*$ be a vector subspace of V^*. We define the *annihilator of U* as:

$$U^0 = \{\mathbf{v} \in V : \omega(\mathbf{v}) = 0 \ \forall \omega \in U\}$$

Lemma 2.112. Let V be a vector space and $U \subseteq V^*$ be a vector subspace of V^*. If $U = \langle \omega_1, \ldots, \omega_n \rangle$, then U^0 is the set of solutions of the system:

$$\begin{cases} \omega_1(\mathbf{v}) = 0 \\ \quad\vdots \\ \omega_n(\mathbf{v}) = 0 \end{cases}$$

[13] This means that the definition of Φ does not depend on a choice of basis.

Lemma 2.113. Let V be a vector space and $U \subseteq V^*$ be a vector subspace of V^*. Then, U^0 is a vector subspace of V^*.

Theorem 2.114. Let V be a finite vector space and $U \subseteq V^*$ be a vector subspace of V^*. Then:

$$\dim U^0 + \dim U = \dim V$$

Definition 2.115. Let V be a vector space and $U \subseteq V$ be a vector subspace of V. We define the *annihilator of U* as:

$$U^0 = \{\omega \in V^* : \omega(\mathbf{v}) = 0 \ \forall \mathbf{v} \in U\}$$

Lemma 2.116. Let V be a vector space and $U \subseteq V$ be a vector subspace of V. If $U = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, then:

$$U^0 = \{\omega \in V^* : \omega(\mathbf{v}_1) = \cdots = \omega(\mathbf{v}_n) = 0\}$$

Proposition 2.117. Let V be a vector space. Then, whether $U \subseteq V$ or $U \subseteq V^*$, we have:

$$\left(U^0\right)^0 = U$$

1.1.2.4 | Classification of endomorphisms

Definition 2.118. Let V be a vector space over a field K and $\lambda \in K$. A *homothety of ratio λ* is a linear map $f : V \to V$ such that $f(\mathbf{v}) = \lambda \mathbf{v} \ \forall \mathbf{v} \in V$.

Similarity

Definition 2.119. Let V be a vector space and $f, g \in \mathcal{L}(V)$. We say that f and g are *similar* if there are basis $\mathfrak{B}$ and $\mathfrak{B}'$ of V such that $[f]_{\mathfrak{B}} = [g]_{\mathfrak{B}'}$.

Lemma 2.120. Let V be a vector space, $\mathfrak{B}$ and $\mathfrak{B}'$ basis of V and $f \in \mathcal{L}(V)$. If $\mathbf{M} = [f]_{\mathfrak{B}}$, $\mathbf{N} = [f]_{\mathfrak{B}'}$ and $\mathbf{P} = [\mathrm{id}]_{\mathfrak{B}, \mathfrak{B}'}$, then:

$$\mathbf{M} = \mathbf{P}^{-1} \mathbf{N} \mathbf{P}$$

Definition 2.121. Let K be a field. Two matrices $\mathbf{M}, \mathbf{N} \in \mathcal{M}_n(K)$ are *similar* if there exists a matrix $\mathbf{P} \in \mathrm{GL}_n(K)$ such that $\mathbf{M} = \mathbf{P}^{-1} \mathbf{N} \mathbf{P}$.

Proposition 2.122. Let V be a finite vector space and $f, g \in \mathcal{L}(V)$.

1. f and g are similar if and only if for all basis $\mathfrak{B}$ of V the matrices $[f]_{\mathfrak{B}}$ and $[g]_{\mathfrak{B}}$ are similar.

2. f and g are similar if and only if there is an automorphism $h \in \mathcal{L}(V)$ such that $g = h^{-1} f h$.

Diagonalization

Definition 2.123. Let K be a field. A matrix $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(K)$ is *diagonal* if $a_{ij} = 0$ whenever $i \neq j$. That is, $\mathbf{A}$ is of the form:

$$\mathbf{A} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

Definition 2.124. Let K be a field. A matrix $\mathbf{A} \in \mathcal{M}_n(K)$ is *diagonalizable* if it is similar to diagonal matrix.

Definition 2.125. An endomorphism is *diagonalizable* if its associated matrix in some basis is diagonalizable.

Definition 2.126. Let V be a vector space over a field K and $f \in \mathcal{L}(V)$. We say that a nonzero vector $\mathbf{v} \in V$ is an *eigenvector of f with eigenvalue* $\lambda \in K$ if $f(\mathbf{v}) = \lambda \mathbf{v}$.

Lemma 2.127. Let V be a vector space over a field K, $f \in \mathcal{L}(V)$ and $\lambda \in K$. The eigenvectors of f of eigenvalue λ are the nonzero vectors of the subspace $\ker(f - \lambda \mathrm{id})$, called *eigenspace corresponding to* λ.

Lemma 2.128. Let V be a vector space over a field K with $\dim V = n$, $\mathfrak{B}$ be a basis of V and $f \in \mathcal{L}(V)$. Then, $\det([f - x\mathrm{id}]_{\mathfrak{B}})$ is a polynomial on the variable x of degree n and with coefficients in K. Moreover, the dominant coefficient is $(-1)^n$ and the constant term is $\det([f]_{\mathfrak{B}})$.

Corollary 2.129. Let V be a vector space of dimension n and $f \in \mathcal{L}(V)$. Then, f has at most n distinct eigenvalues.

Corollary 2.130. Let V be a vector space over $\mathbb{C}$ and $f \in \mathcal{L}(V)$. Then, f has at least one eigenvalue.

Definition 2.131. Let K be a field and $\mathbf{A} \in \mathcal{M}_n(K)$. The polynomial $p_{\mathbf{A}}(\lambda) = \det(\mathbf{A} - \lambda \mathbf{I}_n)$ is called *characteristic polynomial of* $\mathbf{A}$.

Proposition 2.132. Let V be a vector space and $f \in \mathcal{L}(V)$. For all basis $\mathfrak{B}$ of V, the characteristic polynomial of $[f]_{\mathfrak{B}}$ is the same. Therefore, we denote it $p_f(\lambda)$ and we refer to it as *characteristic polynomial of f*.

Proposition 2.133. Let V be a vector space and $f \in \mathcal{L}(V)$. Then, eigenvectors of f of distinct eigenvalues are linearly independent.

Corollary 2.134. Let V be a vector space and $f \in \mathcal{L}(V)$. Suppose $\lambda_1, \ldots, \lambda_n$ are the distinct eigenvalues of f and $V_{\lambda_1}, \ldots, V_{\lambda_n}$ are their corresponded eigenspaces. Then,

$$V_{\lambda_1} + \cdots + V_{\lambda_n}$$

is a direct sum.

Proposition 2.135. Let V be a finite vector space of dimension n, $f \in \mathcal{L}(V)$ and λ be a root of multiplicity m of the characteristic polynomial $p_f(x)$. Then:

$$1 \leq \dim(\ker(f - \lambda \mathrm{id})) \leq m$$

Theorem 2.136 (Diagonalization theorem). Let V be a finite vector space and $f \in \mathcal{L}(V)$. f is diagonalizable if and only if:

1. $p_f(x) = (-1)^n (x - \lambda_1)^{m_1} \cdots (x - \lambda_k)^{m_k}$ with distinct $\lambda_1, \ldots, \lambda_k \in K$.
2. $\dim(\ker(f - \lambda_i \mathrm{id})) = m_i$, $i = 1, \ldots, k$.

Corollary 2.137. Let V be a finite vector space with $\dim V = n$ and $f \in \mathcal{L}(V)$. If f has n distinct eigenvalues, f is diagonalizable.

Proposition 2.138. Let V be a finite vector space and $f, g \in \mathcal{L}(V)$ such that f and g are similar. Then:

$$f \text{ is diagonalizable} \iff g \text{ is diagonalizable}$$

Lemma 2.139. Let K be a field and $\mathbf{A}, \mathbf{B} \in \mathcal{M}_n(K)$ be similar matrices. Then, $\forall k \in \mathbb{N}$, $\mathbf{A}^k$ and $\mathbf{B}^k$ are similar.

Lemma 2.140. Let V be a finite vector space over a field K with $\dim V = n$ and $f \in \mathcal{L}(V)$. Then, the function $\phi_f : K[x] \to \mathcal{L}(V)$ defined by

$$\phi_f(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 f + \cdots + a_n f^n$$

is linear and satisfies:

$$\phi_f((pq)(x)) = \phi_f(p(x)) \phi_f(q(x)) \quad \forall p(x), q(x) \in K[x]$$

Definition 2.141. Let V be a finite vector space with $\dim V = n$ and $f \in \mathcal{L}(V)$. The *minimal polynomial* $m_f(x) \in K[x]$ *of f* is the unique a polynomial satisfying:

- $m_f(f) = 0$.
- m_f is monic.
- m_f is of minimum degree.

Proposition 2.142. Let V be a vector space over a field K and $f \in \mathcal{L}(V)$. If $p(x) \in K[x]$ is such that $p(f) = 0$, then $m_f(x) \mid p(x)$.

Cayley-Hamilton theorem

Theorem 2.143 (Cayley-Hamilton theorem). Let K be a field, $n \geq 1$ and $\mathbf{A} \in \mathcal{M}_n(K)$. Then:

$$m_{\mathbf{A}}(x) \mid p_{\mathbf{A}}(x) \mid m_{\mathbf{A}}(x)^n$$

Therefore $p_{\mathbf{A}}(\mathbf{A}) = 0$ and $m_{\mathbf{A}}(x)$ and $p_{\mathbf{A}}(x)$ have the same irreducible factors.

Corollary 2.144. Let K be a field and $\mathbf{A} \in \mathrm{GL}_n(K)$ be a matrix with $p_{\mathbf{A}}(x) = a_0 + a_1 x + \cdots + (-1)^n x^n$. Then:

$$\mathbf{A}^{-1} = -\frac{1}{a_0} \left(\mathbf{A}^{n-1} + a_{n-1} \mathbf{A}^{n-2} + \cdots + a_2 \mathbf{A} + a_1 \mathbf{I}_n \right)$$

Lemma 2.145. Let V be a finite vector space over a field K, $\mathfrak{B}$ be a basis of V and $f \in \mathcal{L}(V)$. Then $\forall \lambda, \mu \in K$ and $\forall r, s \in \mathbb{N}$:

1. $[f^r]_{\mathfrak{B}} = ([f]_{\mathfrak{B}})^r$.
2. $[\lambda f]_{\mathfrak{B}} = \lambda [f]_{\mathfrak{B}}$.
3. $[\lambda f^r + \mu f^s]_{\mathfrak{B}} = [\lambda f^r]_{\mathfrak{B}} + [\mu f^s]_{\mathfrak{B}}$.

Lemma 2.146. Let V be a finite vector space over a field K, $f \in \mathcal{L}(V)$ and $\mathbf{v}$ be an eigenvector of f of eigenvalue λ. Then, $\forall p(x) \in K[x]$ we have:

$$p(f)(\mathbf{v}) = p(\lambda)\mathbf{v}$$

Theorem 2.147 (Cayley-Hamilton theorem). Let V be a finite vector space over a field K such that $\dim V = n$ and $f \in \mathcal{L}(V)$. Then:

$$m_f(x) \mid p_f(x) \mid m_f(x)^n$$

Definition 2.148. A field K satisfying that all polynomial with coefficient in K of degree greater o equal to 1 factorizes as a product of linear factors is called an *algebraically closed field*.

Definition 2.149. Let V be a vector space and $f \in \mathcal{L}(V)$. We say that $U \subseteq V$ is an *invariant subspace of V under f* if $f(U) \subseteq U$.

Lemma 2.150. Let V be a vector space and $f \in \mathcal{L}(V)$.

1. If $U \subseteq V$ is an invariant subspace of V under f, then:
$$p_{f_{|U}}(x) \mid p_f(x)^{14}$$
2. If U_1 and U_2 are invariant subspaces of V under f such that $V = U_1 \oplus U_2$, then:
   - $p_f(x) = p_{f_{|U_1}}(x) \cdot p_{f_{|U_2}}(x)$.
   - $m_f(x) = \mathrm{lcm}(m_{f_{|U_1}}(x), m_{f_{|U_2}}(x))$.

Lemma 2.151. Let V be a vector space, $f \in \mathcal{L}(V)$ and $a(x), b(x) \in K[x]$. Suppose $m(x) = \mathrm{lcm}(a(x), b(x))$ and $d(x) = \gcd(a(x), b(x))$. Then:

1. $\ker(a(f)) + \ker(b(f)) = \ker(m(f))$.
2. $\ker(a(f)) \cap \ker(b(f)) = \ker(d(f))$.

In particular, if $a(x)$ and $b(x)$ are coprime and $a(f)b(f) = 0$, then:

$$V = \ker(a(x)) \oplus \ker(b(x))$$

Theorem 2.152. Let V be a finite vector space such that $\dim V = n$ and $f \in \mathcal{L}(V)$. If $p_f(x) = q_1(x)^{n_1} \cdots q_r(x)^{n_r}$ and $m_f(x) = q_1(x)^{m_1} \cdots q_r(x)^{m_r}$ with $q_i(x)$ distinct irreducible factors, then:

$$V = \ker(q_1(f)^{m_1}) \oplus \cdots \oplus \ker(q_r(f)^{m_r})$$

Moreover, $\dim(\ker(q_i(f)^{m_i})) = n_i \deg(q_i(x))$.

Jordan form

Definition 2.153. Let K be a field and $\mathbf{A} \in \mathcal{M}_n(K)$. A *jordan bloc of* $\mathbf{A}$ is a square submatrix composed by a value $\lambda \in K$ on the principal diagonal, ones on the diagonal just below the principal diagonal and zeros elsewhere. That is, a Jordan bloc is a matrix of the form:

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \ddots & \vdots \\ 0 & 1 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}$$

[14] Here $f_{|U}$ is the function f restricted to the subspace U.

Proposition 2.154. Let V be a finite vector space over a field K with $\dim V = n$ and $f \in \mathcal{L}(V)$. If $p_f(x) = \pm(x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$, there exists a basis $\mathfrak{B}$ of V such that

$$[f]_{\mathfrak{B}} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{J}_r \end{pmatrix}$$

where $\mathbf{J}_1, \ldots, \mathbf{J}_r$ are Jordan blocs associated with eigenvalues $\lambda_1, \ldots, \lambda_k$ satisfying:

1. For $i = 1, \ldots, k$, the sum of the sizes of Jordan blocs associated with the eigenvalue λ_i is n_i.
2. The sizes of Jordan blocs are determined by $\dim(\ker((f - \lambda_i \mathrm{id})^r))$, $r = 1, \ldots, n_i - 1$.

Proposition 2.155. Let V be a finite vector space over a field K with $\dim V = n$ and $\mathbf{A} \in \mathcal{M}_n(K)$. If $p_{\mathbf{A}}(x) = \pm(x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$, there exist a matrix $\mathbf{P} \in \mathrm{GL}_n(K)$ such that:

$$\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{J}_r \end{pmatrix}$$

where $\mathbf{J}_1, \ldots, \mathbf{J}_r$ are Jordan blocs associated with eigenvalues $\lambda_1, \ldots, \lambda_k$ satisfying properties 1 and 2.

Theorem 2.156. Let V be a vector space and $f, g \in \mathcal{L}(V)$ be such that $p_f(x) = (x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$. If g satisfies:

1. $p_f(x) = p_g(x)$
2. $m_f(x) = m_g(x)$
3. $\dim(\ker((f - \lambda \mathrm{id})^r)) = \dim(\ker((g - \lambda \mathrm{id})^r))$ $\forall \lambda \in K$ $\forall r \geq 1$

then f is similar to g.

1.1.2.5 | Symmetric bilinear forms

First definitions

Definition 2.157. Let U, V, W be three vector spaces over a field K. We say that a function $\varphi : U \times V \to W$ is *bilinear* if $\forall \mathbf{u}_1, \mathbf{u}_2, \mathbf{u} \in U$, $\forall \mathbf{v}_1, \mathbf{v}_2, \mathbf{v} \in V$ and $\forall \lambda \in K$ we have:

1. $\varphi(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}) = \varphi(\mathbf{u}_1, \mathbf{v}) + \varphi(\mathbf{u}_2, \mathbf{v})$.
2. $\varphi(\lambda\mathbf{u}, \mathbf{v}) = \lambda\varphi(\mathbf{u}, \mathbf{v})$.
3. $\varphi(\mathbf{u}, \mathbf{v}_1 + \mathbf{v}_2) = \varphi(\mathbf{u}, \mathbf{v}_1) + \varphi(\mathbf{u}, \mathbf{v}_2)$.
4. $\varphi(\mathbf{u}, \lambda\mathbf{v}) = \lambda\varphi(\mathbf{u}, \mathbf{v})$.

Definition 2.158. Let V be a vector space over a field K. A *bilinear form from V onto K* is a bilinear map $\varphi : V \times V \to K$.

Definition 2.159. Let V be a vector space over a field K. A bilinear form $\varphi : V \times V \to K$ is *symmetric* if

$$\varphi(\mathbf{v}_1, \mathbf{v}_2) = \varphi(\mathbf{v}_2, \mathbf{v}_1) \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

Matrix associated with a bilinear form

Definition 2.160. Let V be a finite vector space over a field K, $\mathfrak{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. We define the *matrix of the bilinear form φ with respect to the basis* $\mathfrak{B}$ as the matrix $[\varphi]_{\mathfrak{B}} \in \mathcal{M}_n(K)$ defined as:

$$[\varphi]_{\mathfrak{B}} = \begin{pmatrix} \varphi(\mathbf{v}_1, \mathbf{v}_1) & \varphi(\mathbf{v}_1, \mathbf{v}_2) & \cdots & \varphi(\mathbf{v}_1, \mathbf{v}_n) \\ \varphi(\mathbf{v}_2, \mathbf{v}_1) & \varphi(\mathbf{v}_2, \mathbf{v}_2) & \cdots & \varphi(\mathbf{v}_2, \mathbf{v}_n) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi(\mathbf{v}_n, \mathbf{v}_1) & \varphi(\mathbf{v}_n, \mathbf{v}_2) & \cdots & \varphi(\mathbf{v}_n, \mathbf{v}_n) \end{pmatrix}$$

Lemma 2.161. Let V be a finite vector space over a field K, $\mathfrak{B}$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then:

$$\varphi(\mathbf{v}_1, \mathbf{v}) = ([\mathbf{v}_1]_{\mathfrak{B}})^{\mathrm{T}} [\varphi]_{\mathfrak{B}} [\mathbf{v}]_{\mathfrak{B}} \quad \forall \mathbf{v}_1, \mathbf{v} \in V$$

Proposition 2.162. Let V be a finite vector space over a field K, $\mathfrak{B}$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then:

$$\varphi \text{ is symmetric} \iff [\varphi]_{\mathfrak{B}} \text{ is symmetric}$$

Proposition 2.163. Let V be a finite vector space over a field K, $\mathfrak{B}$ and $\mathfrak{B}'$ be bases of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then:

$$[\varphi]_{\mathfrak{B}'} = ([\mathrm{id}]_{\mathfrak{B}',\mathfrak{B}})^{\mathrm{T}} [\varphi]_{\mathfrak{B}} [\mathrm{id}]_{\mathfrak{B}',\mathfrak{B}}$$

Orthogonal basis

Definition 2.164. Let V be a finite vector space over a field K, $\varphi : V \times V \to K$ be a symmetric bilinear form and $\mathbf{v}_1, \mathbf{v}_2 \in V$.

- We say that $\mathbf{v}_1$ and $\mathbf{v}_2$ are *orthogonal* if $\varphi(\mathbf{v}_1, \mathbf{v}_2) = 0$.
- If $\mathbf{v}_1 \neq 0$, we say that $\mathbf{v}_1$ is *isotropic* if $\varphi(\mathbf{v}_1, \mathbf{v}_1) = 0$.

Definition 2.165. Let V be a finite vector space over a field K, $\mathfrak{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form.

- We say that $\mathfrak{B}$ is *orthogonal with respect to* φ if $\varphi(\mathbf{v}_i, \mathbf{v}_j) = 0 \ \forall i \neq j$.
- We say that $\mathfrak{B}$ is *orthonormal with respect to* φ if $\varphi(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij}$.

Theorem 2.166. Let V be a finite vector space over a field K, $\mathfrak{B}$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then, V has an orthogonal basis with respect to φ and an orthonormal basis with respect to φ.

Corollary 2.167. Let K be a field with $\operatorname{char} K \neq 2$ and $\mathbf{A} \in \mathcal{M}_n(K)$ be a symmetric matrix. Then, there exists a matrix $\mathbf{P} \in \mathrm{GL}_n(K)$ such that $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P}$ is diagonal.

Orthogonal decompositions

Definition 2.168. Let V be a finite vector space over a field K, $U \subseteq V$ be a vector subspace of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. We define the *orthogonal complement of* U as:

$$U^{\perp} = \{\mathbf{v} \in V : \varphi(\mathbf{v}, \mathbf{u}) = 0 \ \forall \mathbf{u} \in U\}$$

Definition 2.169. Let V be a finite vector space over a field K and $\varphi : V \times V \to K$ be a symmetric bilinear form. We define the *radical of* φ as:

$$\operatorname{rad} \varphi = V^{\perp}$$

We say that φ is *nonsingular* if $\operatorname{rad} \varphi = \{0\}$.

Definition 2.170. Let V be a finite vector space over a field K, $\varphi : V \times V \to K$ be a nonsingular symmetric bilinear form and $\mathbf{v}_0 \in V$. We define $\varphi_{\mathbf{v}_0} : V \to K$, $\varphi_{\mathbf{v}_0}(\mathbf{v}) = \varphi(\mathbf{v}_0, \mathbf{v})$. Then, the function

$$\begin{aligned} V &\longrightarrow V^* \\ \mathbf{v}_0 &\longmapsto \varphi_{\mathbf{v}_0} \end{aligned}$$

is a isomorphism.

Definition 2.171. Let V be a finite vector space over a field K, $U \subseteq V$ be a vector subspace of V and $\varphi : V \times V \to K$ be a nonsingular symmetric bilinear form. Then:

1. $\dim V = \dim U + \dim U^{\perp}$.
2. $(U^{\perp})^{\perp} = U$.
3. If $\varphi_{|U}$ is nonsingular, then $V = U \oplus U^{\perp}$.

Definition 2.172. Let V be a finite vector space over a field K, $U_1, U_2 \subseteq V$ be vector subspaces of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. We say that the sum $U_1 + U_2$ is *orthogonal* if it is direct and $\varphi(\mathbf{u}_1, \mathbf{u}_2) = 0 \ \forall \mathbf{u}_1 \in U_1$ and $\mathbf{u}_2 \in U_2$. In this case, we denote $U_1 + U_2$ by $U_1 \perp U_2$.

Proposition 2.173. Let V be a finite vector space over a field K, $U_1, U_2 \subseteq V$ be vector subspaces of V such that $V = U_1 \perp U_2$ and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then, $\forall \mathbf{v} \in V$ there exist unique $\mathbf{u}_1 \in U_1$ and $\mathbf{u}_2 \in U_2$ such that $\mathbf{v} = \mathbf{u}_1 + \mathbf{u}_2$.

Definition 2.174. Let V be a finite vector space over a field K, $U_1, U_2 \subseteq V$ be vector subspaces of V such that $V = U_1 \perp U_2$ and $\varphi : V \times V \to K$ be a symmetric bilinear form. The function

$$\begin{aligned} \pi : V = U_1 \perp U_2 &\longrightarrow U_i \\ \mathbf{v} = \mathbf{u}_1 + \mathbf{u}_2 &\longmapsto \mathbf{u}_i \end{aligned}$$

for $i = 1, 2$ is called *orthogonal projection of V onto U_i according to the decomposition $V = U_1 \perp U_2$*.

Method 2.175 (Gram-Schmidt process). Let V be a finite vector space over a field K, $\mathfrak{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. $\forall \mathbf{u}, \mathbf{v} \in V$, we define

$$\operatorname{proj}_{\mathbf{u}}(\mathbf{v}) = \frac{\varphi(\mathbf{u}, \mathbf{v})}{\varphi(\mathbf{u}, \mathbf{u})} \mathbf{u}$$

We will create an orthogonal basis $(\mathbf{u}_1,\ldots,\mathbf{u}_n)$ of V from $\mathfrak{B}$. We define $\mathbf{u}_i$, $i=1,\ldots,n$ to be:

$$\begin{aligned}\mathbf{u}_1 &= \mathbf{v}_1\\ \mathbf{u}_2 &= \mathbf{v}_2 - \operatorname{proj}_{\mathbf{u}_1}(\mathbf{v}_2)\\ \mathbf{u}_3 &= \mathbf{v}_3 - \operatorname{proj}_{\mathbf{u}_1}(\mathbf{v}_3) - \operatorname{proj}_{\mathbf{u}_2}(\mathbf{v}_3)\\ &\vdots\\ \mathbf{u}_n &= \mathbf{v}_n - \sum_{i=1}^{n-1}\operatorname{proj}_{\mathbf{u}_i}(\mathbf{v}_n)\end{aligned}$$

To obtain an orthogonal basis $(\mathbf{e}_1,\ldots,\mathbf{e}_n)$ of V from $\mathfrak{B}$, define $\mathbf{e}_i$, $i=1,\ldots,n$ to be:

$$\mathbf{e}_i = \frac{\mathbf{u}_i}{\sqrt{\varphi(\mathbf{u}_i,\mathbf{u}_i)}}$$

Sylvester's law of inertia

Definition 2.176. An *orthogonal geometry over a field* K is a pair (V,φ), where V is a vector space over K and φ is a symmetric bilinear form over V.

Definition 2.177. Let (V_1,φ_1), (V_2,φ_2) be two orthogonal geometries over a field K. An *isometry from* (V_1,φ_1) *to* (V_2,φ_2) is an isomorphism $f: V_1\to V_2$ such that

$$\varphi_2(f(\mathbf{u}),f(\mathbf{v})) = \varphi_1(\mathbf{u},\mathbf{v})\quad \forall \mathbf{u},\mathbf{v}\in V_1$$

We say that (V_1,φ_1) and (V_2,φ_2) are *isometric* if there exists an isometry between them.

Definition 2.178. Let V be a vector space over a field K and φ_1, φ_2 be symmetric bilinear forms. We say that φ_1 and φ_2 are *equivalent* if and only if (V,φ_1) and (V,φ_2) are isometric.

Definition 2.179. Let $\mathbf{A},\mathbf{B}\in\mathcal{M}_n(\mathbb{R})$. We say that $\mathbf{A}$ and $\mathfrak{B}$ are congruent if there exists a matrix $\mathbf{P}\in\mathrm{GL}_n(\mathbb{R})$ such that

$$\mathbf{A} = \mathbf{P}^{\mathrm{T}}\mathbf{B}\mathbf{P}$$

Proposition 2.180. Let V be a finite vector space over a field K, $\mathfrak{B}_1$ be a basis of V and φ_1, φ_2 be symmetric bilinear forms. Then the following statements are equivalent:

1. The orthogonal geometries (V,φ_1) and (V,φ_2) are isometric.
2. There exists a basis $\mathfrak{B}_2$ of V such that $[\varphi_1]_{\mathfrak{B}_1} = [\varphi_2]_{\mathfrak{B}_2}$.
3. The matrices $[\varphi_1]_{\mathfrak{B}_1}$ and $[\varphi_2]_{\mathfrak{B}_2}$ are congruent.

Theorem 2.181 (Sylvester's law of inertia). Let V be a finite vector space over $\mathbb{R}$ and φ be a symmetric bilinear form over V. Then, there exists a basis $\mathfrak{B}$ of V such that:

$$[\varphi]_{\mathfrak{B}} = \begin{pmatrix} 0 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 0 & & & & \text{\huge 0} & & \\ & & & 1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & & & \\ & \text{\huge 0} & & & & & -1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & -1 \end{pmatrix}$$

where in the diagonal there are r_0 zeros, r_+ ones and r_- minus ones and the triplet (r_0,r_+,r_-) doesn't depend on the basis $\mathfrak{B}$.

Definition 2.182. Let V be a finite vector space over $\mathbb{R}$ and φ be a symmetric bilinear form over V. Let $\mathfrak{B}$ be an orthogonal basis of V with respect to φ. We define the *rank of* φ as:

$$\operatorname{rank}\varphi = \operatorname{rank}([\varphi]_{\mathfrak{B}})$$

We define the *signature of* φ as:

$$\operatorname{sig}\varphi = (r_+,r_-)$$

where r_+ is el number of positive real numbers on the diagonal of $[\varphi]_{\mathfrak{B}}$ and r_- is el number of negative real numbers on the diagonal of $[\varphi]_{\mathfrak{B}}$.

Theorem 2.183. Let (V_1,φ_1), (V_2,φ_2) be two orthogonal geometries over $\mathbb{R}$ of finite dimension. Then, (V_1,φ_1) and (V_2,φ_2) are isometric if and only if $\dim V_1 = \dim V_2$ and $\operatorname{sig}\varphi_1 = \operatorname{sig}\varphi_2$.

Inner products

Definition 2.184. Let V be a finite vector space over $\mathbb{R}$ and φ be a symmetric bilinear form over V. We say that φ is *positive-definite* if

$$\varphi(\mathbf{v},\mathbf{v}) > 0\quad \forall\mathbf{v}\in V\setminus\{0\}$$

We say that φ is *negative-definite* if

$$\varphi(\mathbf{v},\mathbf{v}) < 0\quad \forall\mathbf{v}\in V\setminus\{0\}$$ [15]

Definition 2.185. Let V be a vector space over $\mathbb{R}$. An *inner product over* V is a positive-definite symmetric bilinear form over V.

Definition 2.186. An *Euclidean vector space* is a pair (V,φ), where V is a vector space over $\mathbb{R}$ and φ is an inner product over V.

Theorem 2.187 (Cauchy-Schwartz inequality). Let (V,φ) be an Euclidean vector space. Then:

$$\varphi(\mathbf{v}_1,\mathbf{v}_2)^2 \leq \varphi(\mathbf{v}_1,\mathbf{v}_1)\varphi(\mathbf{v}_2,\mathbf{v}_2)\quad \forall\mathbf{v}_1,\mathbf{v}_2\in V$$

Definition 2.188. Let V be a vector space over $\mathbb{R}$. A *norm on* V is a function

$$\begin{aligned}\|\cdot\|: V &\longrightarrow \mathbb{R}\\ \mathbf{v} &\longmapsto \|\mathbf{v}\|\end{aligned}$$

such that:

1. $\|\mathbf{v}\| = 0 \iff \mathbf{v} = \mathbf{0}\ \forall\mathbf{v}\in V$.

[15] The terms *positive-semidefinite* and *negative-semidefinite* are used when $\forall\mathbf{v}\in V\setminus\{0\}$, $\varphi(\mathbf{v},\mathbf{v})\geq 0$ or $\varphi(\mathbf{v},\mathbf{v})\leq 0$, respectively.

2. $\|\lambda\mathbf{v}\| = |\lambda|\|\mathbf{v}\|$, $\forall \mathbf{v} \in V$, $\lambda \in \mathbb{R}$.
3. $\|\mathbf{v}_1 + \mathbf{v}_2\| \leq \|\mathbf{v}_1\| + \|\mathbf{v}_2\|$, $\forall \mathbf{v}_1, \mathbf{v}_2 \in V$[16].

Proposition 2.189. Let (V, φ) be an Euclidean vector space. Then, the function

$$\begin{aligned} \|\cdot\|_\varphi : V &\longrightarrow \mathbb{R} \\ \mathbf{v} &\longmapsto \|\mathbf{v}\|_\varphi = \sqrt{\varphi(\mathbf{v}, \mathbf{v})} \end{aligned}$$

is a norm called *norm associated with the inner product* φ.

Definition 2.190. Let (V, φ) be an Euclidean vector space and $\mathbf{v}_1, \mathbf{v}_2 \in V \setminus \{0\}$. We define the *angle with respect to* φ *between* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ as the unique $\theta \in [0, \pi]$ such that:

$$\cos\theta = \frac{\varphi(\mathbf{v}_1, \mathbf{v}_2)}{\|\mathbf{v}_1\|_\varphi \|\mathbf{v}_2\|_\varphi}$$

Spectral theorem

Definition 2.191. Let (V, φ) be a finite Euclidean vector space and $f \in \mathcal{L}(V)$. Then, there exists a unique $f' \in \mathcal{L}(V)$ such that

$$\varphi(f(\mathbf{v}_1), \mathbf{v}_2) = \varphi(\mathbf{v}_1, f'(\mathbf{v}_2)) \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

This f' is called *adjoint of* f.

Definition 2.192. Let (V, φ) be a finite Euclidean vector space and $f \in \mathcal{L}(V)$. f is called *auto-adjoint* if $f = f'$.

Lemma 2.193. Let (V, φ) be a finite Euclidean vector space of dimension n and $f \in \mathcal{L}(V)$ be auto-adjoint. Then, there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that

$$p_f(x) = (x - \lambda_1) \cdots (x - \lambda_n)$$

Definition 2.194. Let K be a field and $A \in \mathrm{GL}_n(K)$ be a matrix. We say that A is *orthogonal* if and only if

$$\mathbf{P}\mathbf{P}^\mathrm{T} = \mathbf{P}^\mathrm{T}\mathbf{P} = \mathbf{I}_n$$

The set of orthogonal matrices of size n over K is denoted by $\mathcal{O}_n(K)$.

Theorem 2.195 (Spectral theorem). Let (V, φ) be a a finite Euclidean vector space and $f \in \mathcal{L}(V)$ be auto-adjoint. Then, V has an orthonormal basis of eigenvectors of f. In particular, f diagonalizes.

Corollary 2.196. Let K be a field. All symmetric matrices $A \in \mathcal{M}_n(K)$ are diagonalizable. More precisely, there exists $\mathbf{P} \in \mathcal{O}_n(K)$ such that $\mathbf{P}^\mathrm{T}\mathbf{A}\mathbf{P}$ is diagonal.

Definition 2.197. Let $A = (a_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{C})$. We define the *complex conjugate* $\overline{\mathbf{A}}$ *of* $\mathbf{A}$ as $\overline{\mathbf{A}} = (\overline{a_{ij}})$.

Proposition 2.198. Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{C})$, $\mathbf{C} \in \mathcal{M}_{n\times p}(\mathbb{C})$ and $\lambda \in \mathbb{C}$. Then:

1. $\overline{\mathbf{A} + \mathbf{B}} = \overline{\mathbf{A}} + \overline{\mathbf{B}}$.
2. $\overline{\mathbf{AC}} = \overline{\mathbf{A}} \cdot \overline{\mathbf{C}}$.
3. $\overline{\lambda \cdot \mathbf{A}} = \overline{\lambda} \cdot \overline{\mathbf{A}}$.

Corollary 2.199. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a symmetric matrix. Then, there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that

$$p_\mathbf{A}(x) = (x - \lambda_1) \cdots (x - \lambda_n)$$

Theorem 2.200 (Descartes' rule of signs). Let $P(x) = a_0 + \cdots + a_n x^n \in \mathbb{R}[x]$:

1. The number of positive roots of $P(x)$ is at most equal to the number of sign variations in the sequence $[a_d, a_{d-1}, \ldots, a_1, a_0]$.
2. If $P(x) = a_n(x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$, then the number of positive roots of $P(x)$ is equal to the number of sign variations in the sequence (having in account multiplicity).

[16] Note that $\forall \mathbf{v} \in V$ we have: $0 = \|\mathbf{v} + (-\mathbf{v})\| \leq \|\mathbf{v}\| + \|-\mathbf{v}\| = 2\|\mathbf{v}\| \implies \|\mathbf{v}\| \geq 0$.

1.1.3 Real-valued functions

1.1.3.1 | The real line

Definition 3.1. Let $(K, +, \cdot)$ be a field. We say that K, together with a total order relation $\leq$[17], is an *ordered field* if the following properties are satisfied:

1. If $x, y, z \in K$ are such that $x \leq y$, then $x + z \leq y + z$.
2. If $x, y \in K$ are such that $x \geq 0$ and $y \geq 0$, then $x \cdot y \geq 0$.

Definition 3.2. Let K be an ordered field and $A \subset K$. We say that A is *bounded from above* if $\exists M \in K$ (called *upper bound of* A) such that $x \leq M\ \forall x \in A$. Analogously, we say that A is *bounded from below* if $\exists m \in K$ (called *lower bound of* A) such that $x \geq m\ \forall x \in A$.

Definition 3.3. Let K be an ordered field and $A \subset K$ be a set bounded from above. We say that an upper bound α of A is the *supremum of* A, denoted by $\sup A$, if any other upper bound α' satisfies $\alpha' \geq \alpha$. Analogously if $B \subset K$ is a set bounded from below, we say that a lower bound β of B is the *infimum of* B, denoted by $\inf B$, if any other lower bound β' satisfies $\beta' \leq \beta$.

Proposition 3.4. Let K be an ordered field and $A \subset K$. If M is an upper bound of A, then $-M$ is a lower bound of $-A$. Similarly, if m is an lower bound of A, then $-m$ is a upper bound of $-A$

Proposition 3.5. Let K be an ordered field and $A, B \subset K$. If $\alpha = \sup A$ and $\beta = \inf B$, then:

$$-\alpha = \inf(-A) \qquad -\beta = \sup(-B)$$

Proposition 3.6. The supremum of a set, if exists, is unique.

Theorem 3.7 (Supremum axiom). There exists a unique field with the property that any bounded set from above has a supremum: the field of real numbers $\mathbb{R}$.

Proposition 3.8. Natural numbers are not bounded from above in $\mathbb{R}$.

Corollary 3.9 (Archimedean property). Let $\alpha \in \mathbb{R}$. Then, $\exists n \in \mathbb{N}$ such that $\alpha < n$.

Corollary 3.10. Let $\alpha \in \mathbb{R}_{>0}$. Then, $\exists n \in \mathbb{N}$ such that $0 < \frac{1}{n} < \alpha$.

Proposition 3.11. Let $x, y \in \mathbb{R}$ such that $x < y$. Then, there exist numbers $z \in \mathbb{R} \setminus \mathbb{Q}$ and $q \in \mathbb{Q}$ such that $x < z < y$ and $x < q < y$.

Definition 3.12. Given $x, y \in \mathbb{R}$ such that $x < y$ we define:

- $(x, y) = \{z \in \mathbb{R} : x < z < y\}$.
- $[x, y) = \{z \in \mathbb{R} : x \leq z < y\}$.
- $(x, y] = \{z \in \mathbb{R} : x < z \leq y\}$.
- $[x, y] = \{z \in \mathbb{R} : x \leq z \leq y\}$.

[17] See definition 1.63

Lemma 3.13. Let K be an ordered field and $A \subset K$ be a set. If $\alpha = \sup A$, then $\forall \varepsilon > 0$ the interval $(\alpha - \varepsilon, \alpha]$ contains points of A.

Definition 3.14. Let $x \in \mathbb{R}$. We define the *absolute values* $|x|$ *of* x as:

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

Lemma 3.15. Let $x, y \in \mathbb{R}$. Then:

1. $|x| \geq 0$.
2. $|x| = 0 \iff x = 0$.
3. $|xy| = |x||y|$.
4. $|x + y| \leq |x| + |y|$. *(Triangular inequality)*

Definition 3.16. Let $x \in \mathbb{R}$. A *neighbourhood of* x is any open interval containing x.

Infinite and countable sets

Definition 3.17. A $X \neq \varnothing$ is *infinite* if there exist $\varnothing \neq A \subset X$ and $\phi : X \to A$ such that ϕ is a bijection. If no such A and ϕ exist, X is *finite.*

Proposition 3.18. Let X, Y be sets such that $X \subseteq Y$. If X is infinite, Y is infinite.

Proposition 3.19. Let $X \subset \mathbb{N}$. X is finite if and only if X is bounded.

Definition 3.20. Let A be a set. We say that A is *countable* if there exists a bijective function from A to $\mathbb{N}$. We say that A is *uncountable* if there is no such bijection.

Proposition 3.21. Any infinite subset of $\mathbb{N}$ is countable.

Corollary 3.22. Any subset of a countable set is either finite or countable.

Corollary 3.23. Let A be an infinite set. A is countable if and only if there exists an injective function from A to $\mathbb{N}$.

Proposition 3.24. If A and B are countable sets, then $A \times B$ is also countable.

Theorem 3.25. $\mathbb{Q}$ is countable.

Theorem 3.26. $\mathbb{R}$ is uncountable.

1.1.3.2 | Sequences

Limit notion

Definition 3.27. A *sequence of real numbers* is an enumerated collection of real numbers. More formally, a sequence is a function $a : \mathbb{N} \to \mathbb{R}$. The number $a(n)$ is usually denoted by a_n and the whole sequence by (a_n).

Definition 3.28. A sequence (a_n) is *bounded from above* if there is a real number M such that $a_n \leq M\ \forall n \in \mathbb{N}$. Analogously, (a_n) is *bounded from below* if there is a real number m such that $a_n \geq m\ \forall n \in \mathbb{N}$. Finally, we say that (a_n) is *bounded* if there exist $m, M \in \mathbb{R}$ such that $m \leq a_n \leq M\ \forall n \in \mathbb{N}$.

Definition 3.29 (Limit). Let (a_n) be a sequence of real numbers and $\ell \in \mathbb{R}$. We say that

$$\lim_{n\to\infty} a_n = \ell \text{ if } \forall \varepsilon > 0\ \exists n_0 : |a_n - \ell| < \varepsilon \quad \forall n > n_0.$$

We say that

$$\lim_{n\to\infty} a_n = \pm\infty \text{ if } \forall M > 0\ \exists n_0 : \pm a_n > M\ \forall n > n_0.$$

Definition 3.30. We say a sequence is *convergent* if it has a limit, and *divergent* otherwise.

Lemma 3.31. The limit of a convergent sequence is unique.

Lemma 3.32. Let (a_n) be a convergent sequence. Then (a_n) is bounded. Moreover, if $m \leq a_n \leq M\ \forall n \in \mathbb{N}$, then $m \leq \lim_{n\to\infty} a_n \leq M$.

Lemma 3.33. Let (a_n) and (b_n) be convergent sequences with respective limits α and β. Then:

1. The sequences $(a_n + b_n)$ and $(a_n b_n)$ are convergents and
$$\lim_{n\to\infty} a_n + b_n = \alpha + \beta \qquad \lim_{n\to\infty} a_n \cdot b_n = \alpha \cdot \beta$$
2. If $\alpha \neq 0$, then $a_n \neq 0$ for n sufficiently large, the sequence $\left(\frac{b_n}{a_n}\right)$ is convergent and
$$\lim_{n\to\infty} \frac{b_n}{a_n} = \frac{\beta}{\alpha}$$

Definition 3.34. Let (a_n) be a sequence. We say (a_n) is *monotonically increasing* if $a_n \leq a_{n+1}\ \forall n \in \mathbb{N}$. Analogously, we say (a_n) is *monotonically decreasing* if $a_n \geq a_{n+1}\ \forall n \in \mathbb{N}$[18]. Finally, we say (a_n) is *monotonic* if it is either monotonically increasing or monotonically decreasing.

Theorem 3.35. All monotonic and bounded sequences are convergent.

Lemma 3.36. Let (a_n) and (b_n) be two sequences verifying $a_n \leq b_n\ \forall n \in \mathbb{N}$. Then, $\lim_{n\to\infty} a_n \leq \lim_{n\to\infty} b_n$.

Proposition 3.37 (Squeeze theorem). Let (a_n), (b_n) and (c_n) be three sequences verifying $a_n \leq b_n \leq c_n\ \forall n \in \mathbb{N}$ and such that (a_n) and (c_n) are convergent. Suppose that $\lim_{n\to\infty} a_n = \lim_{n\to\infty} c_n = \ell$. Then, (b_n) is convergent and $\lim_{n\to\infty} b_n = \ell$.

Lemma 3.38. Let $p \in \mathbb{R}_{>0}$ and $\alpha, x \in \mathbb{R}$. Then:

1. $\lim_{n\to\infty} \frac{1}{n^p} = 0$.
2. $\lim_{n\to\infty} \sqrt[n]{p} = 1$.
3. $\lim_{n\to\infty} \sqrt[n]{n} = 1$.
4. If $x > 1$, $\lim_{n\to\infty} \frac{n^\alpha}{x^n} = 0$.
5. If $x < 1$, $\lim_{n\to\infty} x^n = 0$.

Theorem 3.39 (Root test). Let $(a_n) \geq 0$ be a sequence. Suppose that the limit $\ell = \lim_{n\to\infty} \sqrt[n]{a_n}$ exists.

1. If $\ell < 1 \implies \lim_{n\to\infty} a_n = 0$.
2. If $\ell > 1 \implies \lim_{n\to\infty} a_n = +\infty$.

Theorem 3.40 (Ratio test). Let $(a_n) \geq 0$ be a sequence. Suppose that the limit $\ell = \lim_{n\to\infty} \frac{a_{n+1}}{a_n}$ exists.

1. If $\ell < 1 \implies \lim_{n\to\infty} a_n = 0$.
2. If $\ell > 1 \implies \lim_{n\to\infty} a_n = +\infty$.

Theorem 3.41. Let $(a_n) \geq 0$ be a sequence. If $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \ell$, then $\lim_{n\to\infty} \sqrt[n]{a_n} = \ell$.

The number e

Definition 3.42. We define the sequences (S_n) and (T_n) as:

$$S_n = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} \qquad T_n = \left(1 + \frac{1}{n}\right)^n$$

Proposition 3.43. The sequences (S_n) and (T_n) are convergent and have the same limit. This limit is denoted by e and it's equal to $\mathrm{e} = 2.71828\ldots$

Theorem 3.44. The number e is irrational.

[18] If the inequalities are strict, we say that (a_n) is *strictly increasing* or *strictly decreasing*, respectively.

Subsequences

Definition 3.45 (Subsequence). Let (a_n) be a sequence of real numbers and (k_n) be an increasing sequence of natural numbers. The sequence (a_{k_n}) is called a *subsequence of* (a_n).

Lemma 3.46. Let (a_n) be a sequence. If $\lim_{n\to\infty} a_n = \ell$, then any subsequence of (a_n) has limit ℓ.

Definition 3.47. Let (a_n) be a sequence. We say p is an *accumulation point of* (a_n) if $\forall\varepsilon > 0$ and $\forall n_0 \in \mathbb{N}\ \exists n > n_0$ such that $|a_n - p| < \varepsilon$.

Proposition 3.48. Let (a_n) be a sequence. p is an accumulation point of (a_n) if and only if there is a subsequence (a_{k_n}) of (a_n) with $\lim_{n\to\infty} a_{k_n} = p$.

Corollary 3.49. A convergent sequence has its limit as the unique accumulation point.

Proposition 3.50. All sequences have a monotonic subsequence.

Theorem 3.51 (Bolzano-Weierstraß theorem). All bounded sequences have a convergent subsequence.

Proposition 3.52. Let (a_n) be a bounded sequence. Then, (a_n) is convergent if and only if it has a unique accumulation point.

Definition 3.53. Let (a_n) be a sequence. We define the *limit superior of* (a_n) as:

$$\limsup_{n\to\infty} a_n := \inf\{\sup\{x_m : m \geq n\} : n \geq 0\}$$

We define the *limit inferior of* (a_n) as:

$$\liminf_{n\to\infty} a_n := \sup\{\inf\{x_m : m \geq n\} : n \geq 0\}$$

Proposition 3.54. Let (a_n) be a sequence. Then $\limsup_{n\to\infty} a_n$ and $\liminf_{n\to\infty} a_n$ always exist and

$$\liminf_{n\to\infty} a_n \leq \limsup_{n\to\infty} a_n$$

If, moreover, (a_n) is bounded, then for all accumulation point $p \in \mathbb{R}$ of (a_n) we have:

$$\liminf_{n\to\infty} a_n \leq p \leq \limsup_{n\to\infty} a_n$$

Proposition 3.55. Let (a_n) be a bounded sequence. Then:

$$(a_n) \text{ is convergent } \iff \liminf_{n\to\infty} a_n = \limsup_{n\to\infty} a_n$$

In this case we have:

$$\lim_{n\to\infty} a_n = \limsup_{n\to\infty} a_n = \liminf_{n\to\infty} a_n$$

Cauchy condition

Definition 3.56 (Cauchy sequence). We say that a sequence (a_n) is a *Cauchy sequence* if $\forall\varepsilon > 0\ \exists n_0$ such that $|a_n - a_m| < \varepsilon\ \forall n, m > n_0$.

Theorem 3.57. A sequence is convergent if and only if it's a Cauchy sequence.

Theorem 3.58 (Stolz-Cesàro theorem). Let (a_n) be a strictly increasing sequence and (b_n) be any other sequence. Suppose that

$$\lim_{n\to\infty} \frac{b_n - b_{n-1}}{a_n - a_{n-1}} = \ell \in \mathbb{R} \cup \{\pm\infty\}$$

Then:

1. If $\lim_{n\to\infty} a_n = \pm\infty$, $\lim_{n\to\infty} \frac{b_n}{a_n} = \ell$.
2. If $\lim_{n\to\infty} b_n = \lim_{n\to\infty} a_n = 0$, $\lim_{n\to\infty} \frac{b_n}{a_n} = \ell$.

1.1.3.3 | Continuity

Limit of a function

Definition 3.59. Let $f : [a, b] \to \mathbb{R}$ be a function and $x_0 \in (a, b)$. We say that ℓ is *the limit of the function f at the point x_0*, denoted by $\lim_{x\to x_0} f(x) = \ell$, if $\forall\varepsilon > 0\ \exists\delta > 0$ such that $|f(x) - \ell| < \varepsilon$ whenever $|x - x_0| < \delta$.

Lemma 3.60. Let $f : (a, b) \to \mathbb{R}$ be a function and $x_0 \in (a, b)$. Then, $\lim_{x\to x_0} f(x) = \ell$ if and only if for any sequence $(a_n) \subset (a, b) \setminus \{x_0\}$ with $\lim_{n\to\infty} a_n = x_0$ we have $\lim_{n\to\infty} f(a_n) = \ell$.

Lemma 3.61. The limit of a function at a point, if exists, is unique.

Proposition 3.62. Let $f, g : (a, b) \to \mathbb{R}$, $x_0 \in (a, b)$ and suppose that $\lim_{x\to x_0} f(x) = \ell_1$ and $\lim_{x\to x_0} g(x) = \ell_2$. Then, the following properties are satisfied:

1. $\lim_{x\to x_0} (f + g)(x) = \ell_1 + \ell_2$.
2. $\lim_{x\to x_0} (f \cdot g)(x) = \ell_1 \cdot \ell_2$.
3. If $\ell_1 > 0$, then $f(x) > 0$ on a neighbourhood of x_0. And if $\ell_1 < 0$, then $f(x) < 0$ on a neighbourhood of x_0. Moreover in both cases $\lim_{x\to x_0} \left(\frac{1}{f}\right)(x) = \frac{1}{\ell_1}$.

Definition 3.63. Let $I \subset \mathbb{R}$ be an interval and $f : I \to \mathbb{R}$. We say that f is *bounded on I* if there are $m, M \in \mathbb{R}$ such that

$$m \leq f(x) \leq M \quad \forall x \in I$$

Lemma 3.64. Let $I \subset \mathbb{R}$ be an interval, $f : I \to \mathbb{R}$ and $x_0 \in I$. If the limit of f at x_0 exists, then f is bounded on a neighbourhood of x_0.

Definition 3.65. Let $I \subset \mathbb{R}$ be an interval, $f : I \to \mathbb{R}$ and $x_0 \in I$. We say that the limit of f at x_0 is infinite, denoted by $\lim_{x\to x_0} f(x) = \pm\infty$, if $\forall\varepsilon > 0\ \exists\delta > 0$ such that $\pm f(x) > \varepsilon$ whenever $|x - x_0| < \delta$.

Lemma 3.66. Let $f : (a,b) \to \mathbb{R}$ be a function and $x_0 \in (a,b)$. Then, $\lim\limits_{x \to x_0} f(x) = \pm\infty$ if and only if for all sequence $(a_n) \subset (a,b) \setminus \{x_0\}$ with $\lim\limits_{n\to\infty} a_n = x_0$, we have $\lim\limits_{n\to\infty} f(a_n) = \pm\infty$.

Definition 3.67. Let $I \subset \mathbb{R}$ be an interval, $f : I \to \mathbb{R}$ and $x_0 \in I$. We say that ℓ is the *right-sided limit of f at x_0*, denoted by $\lim\limits_{x\to x_0^+} f(x) = \ell$, if $\forall \varepsilon > 0\ \exists \delta > 0$ such that $|f(x) - \ell| < \varepsilon$ whenever $x - x_0 < \delta$. Analogously, we say that ℓ is the *left-sided limit of f at x_0*, denoted by $\lim\limits_{x\to x_0^-} f(x) = \ell$, if $\forall\varepsilon > 0\ \exists\delta > 0$ such that $|f(x) - \ell| < \varepsilon$ whenever $x_0 - x < \delta$.

Lemma 3.68. Let $f : (a,b) \to \mathbb{R}$ and $x_0 \in (a,b)$. Then:

$$\lim_{x\to x_0} f(x) = \ell \iff \lim_{x\to x_0^+} f(x) = \lim_{x\to x_0^-} f(x) = \ell$$

Definition 3.69. Let $f : (a,\infty) \to \mathbb{R}$. We say that ℓ is the *limit of f at infinity*, denoted by $\lim\limits_{x\to\infty} f(x) = \ell$, if $\forall\varepsilon > 0\ \exists K > a$ such that $|f(x) - \ell| < \varepsilon$ for all $x > K$.

Definition 3.70. Let $f : (a,\infty) \to \mathbb{R}$. We say that the limit of f at infinity is infinity, denoted by $\lim\limits_{x\to\infty} f(x) = \pm\infty$, if $\forall K > 0\ \exists M > a$ such that $\pm f(x) > K$ for all $x > M$.

Continuity

Definition 3.71. Let $I \subset \mathbb{R}$ be an interval, $f : I \to \mathbb{R}$ and $x_0 \in I$. We say that f is *continuous at x_0* if the limit of f at x_0 exists and it's equal to $f(x_0)$[19]. We say that f is *continuous on I* if it's continuous at all points of I.

Lemma 3.72. Let $I \subset \mathbb{R}$ be an interval and $f : I \to \mathbb{R}$. f is continuous at $x_0 \in I$ if and only if for all sequence $(a_n) \subset I$ with $\lim\limits_{n\to\infty} a_n = x_0$ we have that $\lim\limits_{n\to\infty} f(a_n) = f(x_0)$.

Proposition 3.73. Let $I \subset \mathbb{R}$ be an interval and $f, g : I \to \mathbb{R}$ be continuous functions at $x_0 \in I$. Then:

1. $f + g$ and $f \cdot g$ are continuous at x_0.
2. If $f(x_0) > 0$, then $f(x) > 0$ on a neighbourhood of x_0. And if $f(x_0) < 0$, then $f(x) < 0$ on a neighbourhood of x_0. Moreover, in both cases, $\frac{1}{f}$ is continuous at x_0.

Proposition 3.74. Let $I, J \subset \mathbb{R}$ be intervals, $f : I \to \mathbb{R}$ and $g : J \to \mathbb{R}$. Let $x_0 \in I$ with $f(x_0) \in J$ and suppose that f is continuous at x_0 and g is continuous at $f(x_0)$. Then, $g \circ f$ is continuous at x_0.

Theorem 3.75 (Weierstraß theorem). Let $f : [a,b] \to \mathbb{R}$ be a continuous function. Then, f is bounded on $[a,b]$. Moreover, $\exists m, M \in [a,b]$ such that:

$$f(m) \leq f(x) \leq f(M) \quad \forall x \in [a,b]$$

Theorem 3.76 (Bolzano's theorem). Let $f : [a,b] \to \mathbb{R}$ be a continuous function. If $f(a) \cdot f(b) < 0$, then $\exists c \in (a,b)$ such that $f(c) = 0$.

Corollary 3.77 (Intermediate value theorem). Let $f : [a,b] \to \mathbb{R}$ be a continuous function and $c \in \langle f(a), f(b)\rangle$[20]. Then, $\exists z \in (a,b)$ such that $f(z) = c$.

Corollary 3.78. All real numbers have a unique positive n-th root.

Continuity of inverse function

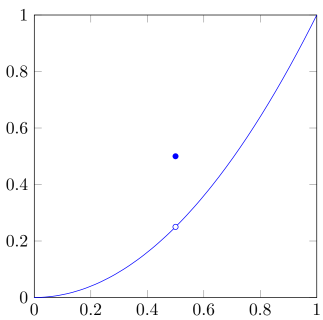
Definition 3.79. Let $I \subset \mathbb{R}$ be an interval and $f : I \to \mathbb{R}$. We say that f is *increasing on I* if $f(x) \leq f(y)$ whenever $x \leq y$. We say that f is *decreasing on I* if $f(x) \geq f(y)$ whenever $x \leq y$[21]. We say that f is *monotonic* if it is either increasing or decreasing.

Theorem 3.80. Let $f : (a,b) \to \mathbb{R}$ be a continuous function. If f is injective and continuous, then f is monotonic. Moreover, f^{-1} is also continuous on $f((a,b))$.

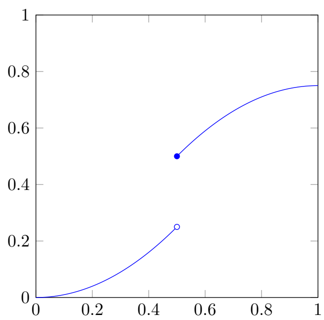
Classification of discontinuities

Definition 3.81. Let $I \subset \mathbb{R}$ be an interval and $f : I \to \mathbb{R}$. Suppose f is not continuous at $x_0 \in I$. There are mainly four types of discontinuities:

1. *Removable discontinuity*: The limit $\lim\limits_{x\to x_0} f(x)$ exists but
$$\lim_{x\to x_0} f(x) \neq f(x_0)$$
2. *Jump discontinuity*: The one-sided limits $\lim\limits_{x\to x_0^+} f(x)$ and $\lim\limits_{x\to x_0^-} f(x)$ exist but
$$\lim_{x\to x_0^+} f(x) \neq \lim_{x\to x_0^-} f(x)$$
3. *Discontinuity of the first kind*:
$$\text{Either } \lim_{x\to x_0^+} f(x) = \pm\infty \text{ or } \lim_{x\to x_0^-} f(x) = \pm\infty$$
4. *Discontinuity of the second kind*: One one-sided limit does not exist.

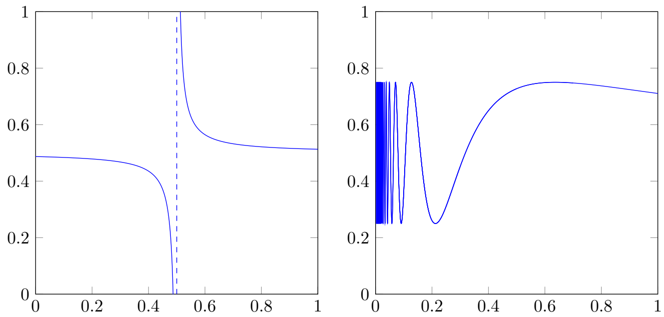


Removable discontinuity



Jump discontinuity

[19] If I contains one of its endpoints, the continuity in these points must be defined with the notion of one-sided limit.
[20] The interval $\langle a, b\rangle$ is defined as $\langle a,b\rangle := (\min(a,b), \max(a,b))$.
[21] If the inequalities are strict, we say that f is *strictly increasing* or *strictly decreasing*, respectively.



Discontinuity of the first kind

Discontinuity of the second kind

Figure 1.1.3: Types of discontinuities

1.1.3.4 | Exponential and logarithmic functions

Lemma 3.82. Let $a \in \mathbb{R}_{>0}$ and $f : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ defined by $f(x) = a^x$. The function f has the following properties:

1. $f(x+y) = f(x)f(y)$.
2. If $a > 1$, f is increasing. If $a < 1$, f is decreasing.
3. If $(a_n) \subset \mathbb{Q}$ is a sequence with $\lim_{n\to\infty} a_n = 0$, then $\lim_{n\to\infty} f(a_n) = 1$.

Lemma 3.83. Let $a, x \in \mathbb{R}$ be such that $a > 0$ and $(x_n) \subset \mathbb{Q}$ be a sequence with $\lim_{n\to\infty} x_n = x$. Then, $\lim_{n\to\infty} a^{x_n}$ exists and does not depend on the sequence (x_n). That is, if $(y_n) \subset \mathbb{Q}$ is another sequence with $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = x$, then $\lim_{n\to\infty} a^{x_n} = \lim_{n\to\infty} a^{y_n}$.

Definition 3.84. Let $a \in \mathbb{R}_{>0}$. We define the *exponential function with base* a as the function $\tilde{f} : \mathbb{R} \to \mathbb{R}$ defined by $\tilde{f}(x) = \lim_{n\to\infty} a^{x_n}$, where (x_n) is any sequence of rational numbers $\lim_{n\to\infty} x_n = x$.

Proposition 3.85. The function g has the following properties:

1. If $x \in \mathbb{Q}$, $\tilde{f}(x) = a^x$.
2. $\tilde{f}(x+y) = \tilde{f}(x)\tilde{f}(y)$.
3. If $a > 1$, $\tilde{f}$ is increasing. If $a < 1$, $\tilde{f}$ is decreasing.
4. $\tilde{f}(x) > 0$ $\forall x \in \mathbb{R}$.
5. $\tilde{f}$ is continuous.
6. If $a > 1$, $\lim_{x\to\infty} \tilde{f}(x) = \infty$ and $\lim_{x\to-\infty} \tilde{f}(x) = 0$.

   If $a < 1$, $\lim_{x\to\infty} \tilde{f}(x) = 0$ and $\lim_{x\to-\infty} \tilde{f}(x) = \infty$[22].

Proposition 3.86. Let $a, x, y \in \mathbb{R}$ be such that $a > 0$. Then, $(a^x)^y = a^{xy}$.

Definition 3.87. Let $a \in \mathbb{R}_{>0}$. Since a^x is continuous and monotonic and its image is $(0, \infty)$, it has an associated inverse defined in $(0, \infty)$. This function is denoted by $\log_a(x)$ and it is called *logarithm with base* a[23].

Proposition 3.88. The logarithm with base $a \in \mathbb{R}_{>0}$ has the following properties:

1. $\log_a$ is continuous.
2. If $a > 1$, $\log_a$ is increasing. If $a < 1$, $\log_a$ is decreasing.
3. If $a > 1$, $\lim_{x\to 0} \log_a(x) = -\infty$ and $\lim_{x\to\infty} \log_a(x) = \infty$.

   If $a < 1$, $\lim_{x\to 0} \log_a(x) = \infty$ and $\lim_{x\to\infty} \log_a(x) = -\infty$.
4. $\log_a(xy) = \log_a(x) + \log_a(y)$.
5. $\log_a(x^y) = y \log_a(x)$.

Proposition 3.89. Let (a_n) be a sequence such that $\lim_{n\to\infty} a_n = \infty$. Then:

$$\mathrm{e} = \lim_{n\to\infty} \left(1 + \frac{1}{a_n}\right)^{a_n}$$

Corollary 3.90. Let (a_n) be a sequence such that $\lim_{n\to\infty} a_n = \infty$ and $x \in \mathbb{R}$. Then:

$$\mathrm{e}^x = \lim_{n\to\infty} \left(1 + \frac{x}{a_n}\right)^{a_n}$$

Proposition 3.91. For all $x \in \mathbb{R}_{\geq 0}$ we have:

$$1 + x \leq \mathrm{e}^x \leq 1 + x\mathrm{e}^x$$

1.1.3.5 | Differentiation

Definition of derivative and elementary properties

Definition 3.92. Let $f : (a, b) \to \mathbb{R}$. We say that f is *differentiable at* $x_0 \in (a, b)$ if the following limit exists:

$$\lim_{x\to x_0} \frac{f(x) - f(x_0)}{x - x_0} = \lim_{h\to 0} \frac{f(x_0 + h) - f(x_0)}{h}$$

In this case, we denote this limit by $f'(x_0)$ and we refer to it as the *derivative of* f *at* x_0. We say f is *differentiable on* (a, b) if it is differentiable at each point of (a, b).

Proposition 3.93. Let $I \subset \mathbb{R}$ be an interval and $f : I \to \mathbb{R}$ be a differentiable function at $x_0 \in I$. The *tangent line to the graph at the point* $(x_0, f(x_0))$ is:

$$y(x) = f(x_0) + f'(x_0)(x - x_0)$$

That is, the derivative of f at x_0 is precisely the slope of the tangent line at the point x_0.

Lemma 3.94. Let $I \subset \mathbb{R}$ be an interval and $f : I \to \mathbb{R}$ be a differentiable function at $x_0 \in I$. Then, f is continuous at x_0.

[22] From now on, we will denote $\tilde{f}(x)$ simply as a^x $\forall x \in \mathbb{R}$.

[23] If the base of the logarithm is the number e, it is common to denote $\log_{\mathrm{e}}(x)$ by $\ln(x)$.

Differentiation rules

Proposition 3.95. Let f, g be two functions defined on a neighbourhood of a and differentiable at a. Then, $f+g$ and fg are differentiable at a and

1. $(f+a)'(a) = f'(a) + g'(a)$.
2. $(f \cdot g)'(a) = f'(a)g(a) + f(a)g'(a)$.

If, moreover, $f(a) \neq 0$, then $\frac{1}{f}$ is defined on a neighbourhood of a, it is differentiable at a and

3. $\left(\frac{1}{f}\right)'(a) = -\frac{f'(a)}{f(a)^2}$.

Proposition 3.96 (Chain rule). Let $g : (a, b) \to (c, d)$ and $f : (c, d) \to \mathbb{R}$. Suppose that g is differentiable at $x \in (a, b)$ and f is differentiable at $g(x) \in (c, d)$. Then, $f \circ g$ is differentiable at x and

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

Proposition 3.97 (Inverse function rule). Let $f : (a, b) \to \mathbb{R}$ be an injective and continuous function on (a, b) and differentiable at $c \in (a, b)$ with $f'(c) \neq 0$. Then, f^{-1} is differentiable at $f(c)$ and

$$(f^{-1})'(f(c)) = \frac{1}{f'(c)}$$

$f(x)$	$f'(x)$
x^α	$\alpha x^{\alpha-1}$
a^x	$a^x \ln a$
$\log_a x$	$\frac{1}{x \ln a}$
$\sin(x)$	$\cos(x)$
$\cos(x)$	$-\sin(x)$
$\tan(x)$	$1 + \tan^2(x) = \frac{1}{\cos^2(x)}$
$\cot(x)$	$-1 - \cot^2(x) = -\frac{1}{\sin^2(x)}$
$\arcsin(x)$	$\frac{1}{\sqrt{1-x^2}}$
$\arccos(x)$	$-\frac{1}{\sqrt{1-x^2}}$
$\arctan(x)$	$\frac{1}{1+x^2}$
$\text{arccot}(x)$	$-\frac{1}{1+x^2}$

Table 1.1.1: Table of derivatives of elementary functions

Basic differentiation theorems

Definition 3.98. Let $I \subset \mathbb{R}$ be an interval, $f : I \to \mathbb{R}$ and $c \in I$. We say that c is a *local maximum of f* if exists an open interval $J \subset I$ with $c \in J$ such that $f(x) \leq f(c)$ $\forall x \in J$. We say that c is a *local minimum of f* if exists an open interval $J \subset I$ with $c \in J$ such that $f(x) \geq f(c)$ $\forall x \in J$. Finally, a *local extremum* is either a local maximum or a local minimum.

Proposition 3.99. Let $I \subset \mathbb{R}$ be an interval, $f : I \to \mathbb{R}$ and $c \in I$ be a local extremum of f. If f is differentiable at c, then $f'(c) = 0$.

Theorem 3.100 (Rolle's theorem). Let $f : [a, b] \to \mathbb{R}$ be a continuous and differentiable function on (a, b). Suppose $f(a) = f(b)$. Then, there exists a point $c \in (a, b)$ such that $f'(c) = 0$.

Theorem 3.101 (Mean value theorem). Let $f : [a, b] \to \mathbb{R}$ be a continuous function on $[a, b]$ and differentiable on (a, b). Then, there exists a point $c \in (a, b)$ such that

$$f(b) - f(a) = f'(c)(b - a)$$

Corollary 3.102. Let f be a differentiable function on (a, b) verifying that $f'(x) = 0$ $\forall x \in (a, b)$. Then, f is constant in (a, b).

Corollary 3.103. Let f be a differentiable function on (a, b). If $f'(x) > 0$ $\forall x \in (a, b)$, then f is strictly increasing on (a, b). Similarly, if $f'(x) < 0$ $\forall x \in (a, b)$, then f is strictly decreasing on (a, b).

Corollary 3.104. Let f be a differentiable function on a neighbourhood of a and such that f' is continuous on this neighbourhood. Suppose that $f'(a) \neq 0$. Then, exists another neighbourhood of a on which f is invertible.

Theorem 3.105 (Cauchy's mean value theorem). Let $f, g : [a, b] \to \mathbb{R}$ be continuous functions on $[a, b]$ and differentiable on (a, b). Then, there exists a point $c \in (a, b)$ such that

$$g'(c)(f(b) - f(a)) = f'(c)(g(b) - g(a))$$

Theorem 3.106 (L'Hôpital's rule). Let f, g be two functions defined on a neighbourhood of $a \in \mathbb{R} \cup \{\pm\infty\}$ and such that either $\lim_{x\to a} f(x) = \lim_{x\to a} g(x) = 0$ or $\lim_{x\to a} g(x) = \infty$. Suppose, moreover, that the limit $\lim_{x\to a} \frac{f'(x)}{g'(x)}$ exists. Then, the limit $\lim_{x\to a} \frac{f(x)}{g(x)}$ exists too and

$$\lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}$$

Theorem 3.107 (Darboux's theorem). Let $f : (a, b) \to \mathbb{R}$ be a differentiable function and suppose that there exist $x, y \in (a, b)$, $x < y$, with $f'(x)f'(y) < 0$. Then, there exists $z \in (x, y)$ such that $f'(z) = 0$.

1.1.3.6 | Convexity and concavity

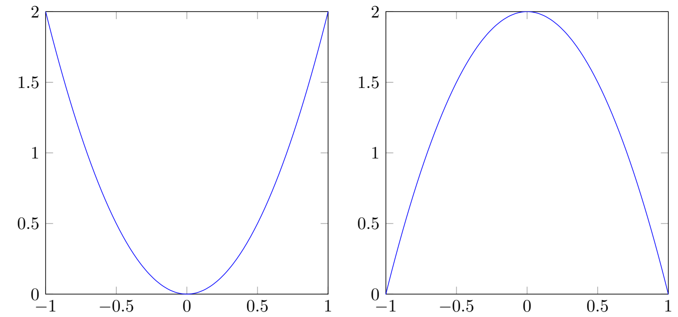
Definition 3.108. We say that $f : I \to \mathbb{R}$ is *convex* if given any two points $a, b \in I$, $a < b$, the segment between $(a, f(a))$ and $(b, f(b))$ lies above the graph on (a, b). That is:

$$f(bt + (1-t)a) \leq tf(b) + (1-t)f(a) \quad \forall t \in [0, 1]$$

We say that f is *concave* if given any two points $a, b \in I$, $a < b$, the segment between $(a, f(a))$ and $(b, f(b))$ lies below the graph on (a, b). That is:

$$f(bt + (1-t)a) \geq tf(b) + (1-t)f(a) \quad \forall t \in [0, 1]^{24}$$

[24] If the inequalities are strict, we say that f is *strictly convex* or *strictly concave*, respectively.



Convex function   Concave function

Figure 1.1.4

Lemma 3.109. A function f is convex on an interval I is and only if $-f$ if concave on I.

Lemma 3.110. Let $f : I \to \mathbb{R}$. f is convex on I if and only if $\forall a, x, b \in I$ with $a < x < b$ we have:

$$\frac{f(x) - f(a)}{x - a} \leq \frac{f(b) - f(a)}{b - a}$$

Or, equivalently:

$$\frac{f(b) - f(a)}{b - a} \leq \frac{f(b) - f(x)}{b - x}.$$

Similarly, f is concave on I if and only if $\forall a, x, b \in I$ with $a < x < b$ we have:

$$\frac{f(x) - f(a)}{x - a} \geq \frac{f(b) - f(a)}{b - a}$$

Or, equivalently:

$$\frac{f(b) - f(a)}{b - a} \geq \frac{f(b) - f(x)}{b - x}.$$

Proposition 3.111. Let f be a convex or concave function on an interval I. Then, f is continuous on I.

Lemma 3.112. Let f be a differentiable function and $a < b$ be such that $f(a) = f(b)$. Then:

- If f' is increasing, $f(x) \leq f(a)\ \forall x \in (a, b)$.
- If f' is decreasing, $f(x) \geq f(a)\ \forall x \in (a, b)$.

Theorem 3.113. Let f be a differentiable function on an interval I. Then:

- f is (strictly) convex if and only if f' is (strictly) increasing.
- f is (strictly) concave if and only if f' is (strictly) decreasing.

Theorem 3.114. Let f be a differentiable function on an interval I. Then, f is convex if and only if the graph lies above all its tangent lines. And similarly, f is concave if and only if the graph lies below all its tangent lines.

Definition 3.115. Let f be a differentiable function on an interval I. If the function $f' : I \to \mathbb{R}$ is differentiable at $a \in I$, we say that f is *two times differentiable at a*. If this happens in all points of I, we say that f is *two times differentiable on I*. In this case we denote the derivative of f' at the point a, $(f')'(a)$, by $f''(a)$ and we refer to it as *second derivative of f at a*.

Theorem 3.116. Let f be a function two times differentiable on I. Then:

1. f is convex on I if and only if $f''(x) \geq 0\ \forall x \in I$.
2. f is concave on I if and only if $f''(x) \leq 0\ \forall x \in I$.

Definition 3.117. Let $f : I \to \mathbb{R}$. We say that f is convex at $x \in I$ if exists a neighbourhood $J \subset I$ of x on which f is convex. Analogously, we say that f is concave at $x \in I$ if exists a neighbourhood $J \subset I$ of x on which f is concave.

Definition 3.118. Let f be a continuous function on I. We say $x \in I$ is an *inflection point* if exists $\delta > 0$ such that f is convex (or concave) on $(x - \delta, x]$ and concave (or convex) on $[x, x + \delta)$.

Proposition 3.119. Let f be a function two times differentiable on I. Then:

1. If a is an inflection point, $f''(a) = 0$.
2. Suppose that f'' is continuous at $a \in I$. Then:
   - If $f''(a) \geq 0$, f is convex at a.
   - If $f''(a) \leq 0$, f is concave at a.

1.1.3.7 | Polynomial approximation

Definition 3.120. Let f, g be two functions defined on a neighbourhood of $a \in \mathbb{R}$. We say that f and g have *contact of order $\geq n$ at a* if

$$\lim_{x \to a} \frac{f(x) - g(x)}{(x - a)^n} = 0$$

Definition 3.121. Let f be a function. Iterating the process in definition 3.115, one can define the notion of the *n-th derivative of f at the point $a \in \mathbb{R}$*, denoted by $f^{(n)}(a)$.

Definition 3.122. We say that a function f is of *class $\mathcal{C}^n$ at a point $a \in \mathbb{R}$, $n \in \mathbb{N}$*, if f is n times differentiable at a neighbourhood of a and $f^{(n)}$ is continuous in this neighbourhood. We say that f is of *class $\mathcal{C}^\infty$ at a* if f is of class $\mathcal{C}^n$ at $a\ \forall n \in \mathbb{N}$. Finally, if $p \in \mathbb{N} \cup \{\infty\}$, we say that f is of *class $\mathcal{C}^p$, or $\mathcal{C}^p(I)$, on an interval I* it it is of class $\mathcal{C}^p$ at all points of I.

Lemma 3.123. Let f, g be functions n times differentiable at $a \in \mathbb{R}$. Then:

1. If $f^{(i)}(a) = g^{(i)}(a)$, $i = 0, 1, \ldots, n$, and $f^{(n)}$ and $g^{(n)}$ are continuous at a, then f and g have contact of order $\geq n$.
2. If f and g have contact of order $\geq n$, then $f^{(i)}(a) = g^{(i)}(a)$, $i = 0, 1, \ldots, n$.

Theorem 3.124. Let f be a function n times differentiable at $a \in \mathbb{R}$. Then, the polynomial

$$P_{n,f,a}(x) = f(a) + f'(a)(x - a) + \frac{f''(a)}{2!}(x - a)^2 + \\ + \frac{f^{(3)}(a)}{3!}(x - a)^3 + \cdots + \frac{f^{(n)}(a)}{n!}(x - a)^n$$

has contact with f of order $\geq n$ at a. This polynomial is called *Taylor polynomial of order n of f centered at a*.

Proposition 3.125. Let P and Q be polynomials of degree $\leq n$ with order of contact $\geq n$ at a point $a \in \mathbb{R}$. Then $P = Q$[25].

Theorem 3.126. Let f be a function n times differentiable at $a \in \mathbb{R}$. If $f'(a) = f''(a) = \cdots = f^{(n-1)}(a) = 0$ and $f^{(n)}(a) \neq 0$ then:

1. If n is odd, a isn't a local extremum of f.
2. If n is even and $f^{(n)}(a) > 0$, a is a local minimum of f.
3. If n is even and $f^{(n)}(a) < 0$, a is a local maximum of f.

Theorem 3.127. Let f be a function $n+1$ times differentiable on a neighbourhood I of $a \in \mathbb{R}$. Let $P = P_{n,f,a}$, $R_n := f - P$ and $x \in I$. Then:

1. Cauchy's formula:
$$R_n(x) = \frac{f^{(n+1)}(\xi)}{n!}(x-\xi)^n(x-a)$$
for some $\xi \in \langle a, x \rangle$.
2. Lagrange's formula:
$$R_n(x) = \frac{f^{(n+1)}(\eta)}{(n+1)!}(x-a)^{n+1}$$
for some $\eta \in \langle a, x \rangle$.
3. Integral formula: If $f^{(n+1)}$ is integrable[26] on $[a, x]$:
$$R_n(x) = \int_a^x \frac{f^{(n+1)}(t)}{n!}(x-t)^n \mathrm{d}t$$

Definition 3.128. We say that f is *analytic at a* if it's of class $\mathcal{C}^\infty$ on a neighbourhood I of a and $\lim_{n\to\infty} R_n(x) = 0$ $\forall x \in I$.

$f(x)$	Taylor polynomials
e^x	$1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!}$
$\ln(1+x)$	$x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots + (-1)^{n+1}\frac{x^n}{n}$
$\sin(x)$	$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!}$
$\cos(x)$	$1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots + (-1)^n \frac{x^{2n}}{(2n)!}$
$\frac{1}{1-x}$	$1 + x + x^2 + x^3 + \cdots + x^n$
$(1+x)^\alpha$	$1 + \alpha x + \cdots + \frac{\alpha(\alpha-1)\cdots(\alpha-(n-1))}{n!}x^n$
$\arctan(x)$	$x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots + (-1)^n \frac{x^{2n+1}}{2n+1}$

Table 1.1.2: Taylor polynomials centered at 0 of some elementary functions

1.1.3.8 | Riemann integral

Construction of Riemann integral

Definition 3.129. Let $I = [a, b]$ be an interval. A *partition $\mathcal{P}$ of I* is a finite collection of points $a = t_0 < t_1 < \cdots < t_n = b$ of I. We denote by $\mathrm{P}(I)$ the set of all partitions of the interval I.

Definition 3.130. Let $f : I \to \mathbb{R}$ be a bounded function and $\mathcal{P} = \{t_i\}_{i=0}^n \in \mathrm{P}(I)$. We define the respective *lower sum and upper sum of f associated with $\mathcal{P}$* as:
$$L(f, \mathcal{P}) = \sum_{i=1}^n m_i(t_i - t_{i-1}) \quad U(f, \mathcal{P}) = \sum_{i=1}^n M_i(t_i - t_{i-1})$$
where $m_i = \inf\{f(x_i) : x_i \in [t_{i-1}, t_i]\}$ and $M_i = \sup\{f(x_i) : x_i \in [t_{i-1}, t_i]\}$.

Definition 3.131. Let $\mathcal{P}, \mathcal{Q} \in \mathrm{P}(I)$ be two partitions. We say that *$\mathcal{P}$ is finer than $\mathcal{Q}$*, $\mathcal{Q} \prec \mathcal{P}$, if $\mathcal{Q} \subset \mathcal{P}$.

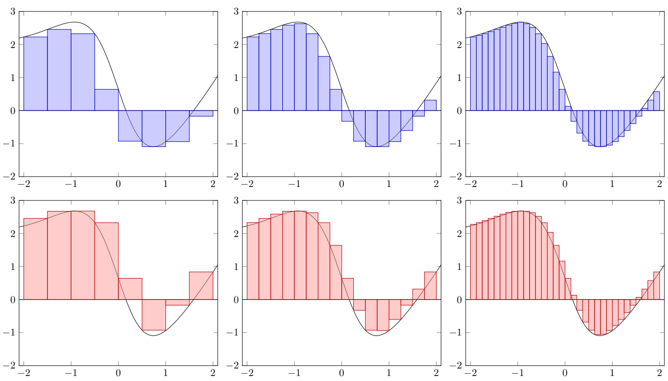


Figure 1.1.5: Lower (blue) and upper (red) sums of a function with three different partitions, each one finer than the previous one.

Proposition 3.132. Let $f : I \to \mathbb{R}$ be a bounded function and $\mathcal{P}, \mathcal{Q} \in \mathrm{P}(I)$ with $\mathcal{Q} \prec \mathcal{P}$. Then:
$$L(f, \mathcal{Q}) \leq L(f, \mathcal{P}) \leq U(f, \mathcal{P}) \leq U(f, \mathcal{Q})$$

Definition 3.133. Let $I = [a, b]$ and $f : I \to \mathbb{R}$ be a bounded function. We define the *lower integral of f on I* as:
$$\underline{\int_a^b} f(x)\mathrm{d}x = \sup\{L(f, \mathcal{P}) : \mathcal{P} \in \mathrm{P}(I)\}$$
Analogously, we define the *upper integral of f on I* as:
$$\overline{\int_a^b} f(x)\mathrm{d}x = \inf\{U(f, \mathcal{P}) : \mathcal{P} \in \mathrm{P}(I)\}$$

Definition 3.134. Let $I = [a, b]$ and $f : I \to \mathbb{R}$ be a bounded function. We say that *f is integrable on I* if
$$\underline{\int_a^b} f(x)\mathrm{d}x = \overline{\int_a^b} f(x)\mathrm{d}x$$
In this case, we denote the integral of f on I by $\displaystyle\int_a^b f(x)\mathrm{d}x$.

[25] This means that the Taylor polynomial $P_{n,f,a}(x)$ is the unique polynomial which has contact with a function f of order $\geq n$ at a point a.

[26] See definition 3.134.

Lemma 3.135. Let $I = [a, b]$ and $f : I \to \mathbb{R}$ be a bounded function. Then, f is integrable on I if and only if $\forall\varepsilon > 0$ $\exists\mathcal{P} \in \mathrm{P}(I)$ such that:

$$U(f, \mathcal{P}) - L(f, \mathcal{P}) < \varepsilon$$

Theorem 3.136. Let $I = [a, b]$ and $f : I \to \mathbb{R}$ be a monotonic and bounded function. Then, f is integrable on I.

Definition 3.137. Let $f : I \to \mathbb{R}$ be a function. We say that f *is uniformly continuous on* I if $\forall\varepsilon > 0$ $\exists\delta > 0$ such that $|f(x) - f(y)| < \varepsilon$ whenever $|x - y| < \delta$.

Theorem 3.138. Let $I = [a, b]$ and $f : I \to \mathbb{R}$ be a continuous function. Then, f is uniformly continuous at I.

Theorem 3.139. Let $I = [a, b]$ and $f : I \to \mathbb{R}$ be a continuous function. Then, f is integrable on I.

Properties of the integral

Proposition 3.140. Let f, g be integrable functions on $[a, b]$ and $c \in \mathbb{R}$. Then, $f + g$ and cf are integrable on I and

$$\int_a^b [f(x) + g(x)]\mathrm{d}x = \int_a^b f(x)\mathrm{d}x + \int_a^b g(x)\mathrm{d}x$$
$$\int_a^b cf(x)\mathrm{d}x = c\int_a^b f(x)\mathrm{d}x$$

Theorem 3.141. Let f be an integrable function on $[a, b]$ with $f([a, b]) \subseteq [c, d]$ and g be a continuous function on $[c, d]$. Then, $g \circ f$ is integrable on $[a, b]$.

Corollary 3.142. Let f be an integrable function on $[a, b]$. Then, f^2 is integrable on $[a, b]$. And if there exists $\delta > 0$ with $f(x) > \delta$ $\forall x \in [a, b]$, then $\frac{1}{f}$ is integrable on $[a, b]$.

Corollary 3.143. Let f, g be integrable functions on $[a, b]$. Then, fg is integrable on $[a, b]$.

Inequalities involving integrals

Proposition 3.144. Let f, g be integrable functions on $[a, b]$ with $f(x) \leq g(x)$ $\forall x \in [a, b]$. Then:

$$\int_a^b f(x)\mathrm{d}x \leq \int_a^b g(x)\mathrm{d}x$$

Corollary 3.145. Let f be an integrable function on $[a, b]$ with $m \leq f(x) \leq M$ $\forall x \in [a, b]$. Then:

$$m(b - a) \leq \int_a^b f(x)\mathrm{d}x \leq M(b - a)$$

If, moreover, f is continuous, there exists $c \in [a, b]$ such that:

$$\int_a^b f(x)\mathrm{d}x = f(c)(b - a)$$

Proposition 3.146. Let f be an integrable function on $[a, b]$. Then, $|f|$ is integrable on $[a, b]$ and

$$\left|\int_a^b f(x)\mathrm{d}x\right| \leq \int_a^b |f(x)|\mathrm{d}x$$

Proposition 3.147. Let f be an integrable function on $[a, b]$ and g be a function defined on $[a, b]$ distinct to f on a finite number points. Then, g is integrable on $[a, b]$ and

$$\int_a^b g(x)\mathrm{d}x = \int_a^b f(x)\mathrm{d}x$$

Fundamental theorem of calculus

Proposition 3.148. Let $f : [a, b] \to \mathbb{R}$ and $b \in (a, c)$. f is integrable on $[a, c]$ if and only if f is integrable on $[a, b]$ and on $[b, c]$. Moreover:

$$\int_a^c f(x)\mathrm{d}x = \int_a^b f(x)\mathrm{d}x + \int_b^c f(x)\mathrm{d}x$$

Theorem 3.149 (Fundamental theorem of calculus). Let f be an integrable function on $[a, b]$. Then,

$$F(t) = \int_a^t f(x)\mathrm{d}x$$

is a continuous function on $[a, b]$. If, moreover, f is continuous at $c \in [a, b]$, then F is differentiable at c and $F'(c) = f(c)$. Finally, if f is continuous on $[a, b]$, then F is differentiable on $[a, b]$ and $F' = f$. In this last case, the function F is called *primitive function of* f.

Theorem 3.150. Let f be an integrable function on $[a, b]$ which has primitives. Then, these primitives are of the form:

$$F(t) = k + \int_a^t f(x)\mathrm{d}x$$

where $k \in \mathbb{R}$. Moreover they satisfy $F' = f$ and

$$\int_a^b f(x)\mathrm{d}x = F(b) - F(a)$$

Corollary 3.151 (Integration by parts). Let f, g be integrable functions on $[a, b]$ with primitives F and G, respectively. Then:

$$\int_a^b F(x)g(x)\mathrm{d}x = F(b)G(b) - F(a)G(a) - \int_a^b f(x)G(x)\mathrm{d}x$$

Corollary 3.152 (Integration by substitution). Let $\varphi : [c, d] \to [a, b]$ be a function of class $\mathcal{C}^1$ such that $\varphi(c) = a$ and $\varphi(d) = b$ and f be a continuous function on $[a, b]$. Then:

$$\int_a^b f(x)\mathrm{d}x = \int_c^d (f \circ \varphi)(x)\varphi'(x)\mathrm{d}x$$

Riemann sums

Definition 3.153. Let $\mathcal{P} = \{t_i\}_{i=0}^n \in \mathrm{P}([a,b])$. A *Riemann sum of f associated with $\mathcal{P}$, $S(f,\mathcal{P})$*, is:

$$S(f,\mathcal{P}) = \sum_{i=1}^n f(x_i)(t_i - t_{i-1})$$

where $x_i \in [t_{i-1}, t_i]$.

Theorem 3.154. Let f be a continuous function on $[a,b]$. Then, $\forall \varepsilon > 0$ $\exists \delta > 0$ such that if $\mathcal{P} = \{t_i\}_{i=0}^n \in \mathrm{P}([a,b])$ with $t_i - t_{i-1} < \delta$, then:

$$\left| \int_a^b f(x)\mathrm{d}x - S(f,\mathcal{P}) \right| < \varepsilon$$

for all Riemann sums associated with $\mathcal{P}$.

Corollary 3.155. Let f be a continuous function on $[a,b]$ and let $\mathcal{P}_n = \{t_i\}_{i=0}^n \in \mathrm{P}([a,b])$ be a sequence de partitions of $[a,b]$ such that $t_i - t_{i-1} < 1/n$. Then, for all Riemann sums $S(f,\mathcal{P}_n)$ we have:

$$\int_a^b f(x)\mathrm{d}x = \lim_{n\to\infty} S(f,\mathcal{P}_n)$$

Geometric applications

Definition 3.156. Let $f : [a,b] \to \mathbb{R}$ and $\mathcal{P} = \{t_i\}_{i=0}^n \in \mathrm{P}([a,b])$. We define the *length of the polygonal approximating the arc length of f on* $[a,b]$ as:

$$\ell(f,\mathcal{P}) = \sum_{i=1}^n \sqrt{(t_i - t_{i-1})^2 + (f(t_i) - f(t_{i-1}))^2}$$

Lemma 3.157. Let $f : I \to \mathbb{R}$ and $\mathcal{P}, \mathcal{Q} \in \mathrm{P}(I)$ with $\mathcal{Q} \prec \mathcal{P}$. Then, $\ell(f,\mathcal{P}) \geq \ell(f,\mathcal{Q})$.

Definition 3.158. Let $f : I \to \mathbb{R}$. If the set $\mathcal{L} := \{\ell(f,\mathcal{P}) : \mathcal{P} \in \mathrm{P}([a,b])\}$ is bounded from above, we say that the graph is *rectifiable* and we define its length $\ell(f,[a,b])$ as:

$$\ell(f,[a,b]) = \sup \mathcal{L}$$

Proposition 3.159. Let f be a function of class $\mathcal{C}^1([a,b])$. Then, f is rectifiable on $[a,b]$ and

$$\ell(f,[a,b]) = \int_a^b \sqrt{1 + f'(x)^2}\mathrm{d}x$$

Definition 3.160. Let $\varphi : [a,b] \to \mathbb{R}^2$ with $\varphi(t) = (x(t), y(t))$ and $\mathcal{P} = \{t_i\}_{i=0}^n \in \mathrm{P}([a,b])$. We define the *length of the polygonal approximating the arc length of φ on* $[a,b]$ as:

$$\ell(\varphi,\mathcal{P}) = \sum_{i=1}^n \sqrt{[x(t_i) - x(t_{i-1})]^2 + [y(t_i) - y(t_{i-1})]^2}$$

Proposition 3.161. Let $\varphi : [a,b] \to \mathbb{R}^2$ with $\varphi(t) = (x(t), y(t))$. Suppose that the functions $x(t)$, $y(t)$ are of class $\mathcal{C}^1([a,b])$. Then, the curve φ is rectifiable on $[a,b]$ and

$$\ell(\varphi,[a,b]) = \int_a^b \sqrt{[x'(t)]^2 + [y'(t)]^2}\mathrm{d}x$$

Lemma 3.162. Let f, g be continuous functions on $[a,b]$. Then, $\forall \varepsilon > 0$, $\exists \delta > 0$ such that if $\mathcal{P} = \{t_i\}_{i=0}^n$ with $t_i - t_{i-1} < \delta$, then:

$$\left| \int_a^b \sqrt{f(x)^2 + g(x)^2}\mathrm{d}x - \sum_{i=1}^n (t_i - t_{i-1})\sqrt{f(c_i)^2 + g(d_i)^2} \right| < \varepsilon$$

for any $c_i, d_i \in [t_{i-1}, t_i]$, $i = 1, \ldots, n$.

Lemma 3.163. Let f, g be continuous functions on $[a,b]$. Then, $\forall \varepsilon > 0$, $\exists \delta > 0$ such that if $\mathcal{P} = \{t_i\}_{i=0}^n$ with $t_i - t_{i-1} < \delta$, then:

$$\left| \int_a^b f(x)g(x)\mathrm{d}x - \sum_{i=1}^n (t_i - t_{i-1}) f(c_i) g(d_i) \right| < \varepsilon$$

for any $c_i, d_i \in [t_{i-1}, t_i]$, $i = 1, \ldots, n$.

Proposition 3.164 (Surface of revolution). Let $f : [a,b] \to \mathbb{R}_{>0}$ be a function of class $\mathcal{C}^1$. Then, the surface of the solid formed by rotating the area below the function $f(x)$ and between the lines $x = a$ and $x = b$ about the x-axis is given by:

$$S_x = 2\pi \int_a^b f(x)\sqrt{1 + f'(x)^2}\mathrm{d}x$$

Proposition 3.165 (Surface of revolution). Let $a > 0$ and $f : [a,b] \to \mathbb{R}$ be a function of class $\mathcal{C}^1$. Then, the surface of the solid formed by rotating the area below the function $f(x)$ and between the lines $x = a$ and $x = b$ about the y-axis is given by:

$$S_y = 2\pi \int_a^b x\sqrt{1 + f'(x)^2}\mathrm{d}x$$

Proposition 3.166 (Volume of revolution). Let $f, g : [a,b] \to \mathbb{R}_{>0}$ be bounded and integrable functions. Then, the volume of the solid formed by rotating the area between the curves of $f(x)$ and $g(x)$ and the lines $x = a$ and $x = b$ about the x-axis is given by:

$$V_x = \pi \int_a^b \left| f(x)^2 - g(x)^2 \right| \mathrm{d}x$$

Proposition 3.167 (Volume of revolution). Let $a > 0$ and $f, g : [a,b] \to \mathbb{R}$ be bounded and integrable functions. Then, the volume of the solid formed by rotating the area between the curves of $f(x)$ and $g(x)$ and the lines $x = a$ and $x = b$ about the y-axis is given by:

$$V_y = \pi \int_a^b x \left| f(x) - g(x) \right| \mathrm{d}x$$

Proposition 3.168 (Center of masses). The *center of masses (x_0, y_0) of a thin plate with uniformly density ρ* is:

$$x_0 = \frac{\displaystyle\int_a^b x\sqrt{1 + f'(x)^2}dx}{\displaystyle\int_a^b \sqrt{1 + f'(x)^2}dx} \qquad y_0 = \frac{\displaystyle\int_a^b f(x)\sqrt{1 + f'(x)^2}dx}{\displaystyle\int_a^b \sqrt{1 + f'(x)^2}dx}$$

Calculation of primitives

Lemma 3.169. Let $P(x), Q(x) \in \mathbb{R}[x]$ be polynomials with $\deg P(x) < \deg Q(x)$. Suppose $Q(x)$ factorises as:

$$Q(x) = \prod_{i=1}^{n} (x - a_i)^{r_i} \prod_{i=1}^{m} (x^2 + b_i x + c_i)^{s_i}$$

with $b_i^2 - 4c_i < 0$ for $i = 1, \ldots, m$. Then, the function $\frac{P(x)}{Q(x)}$ can be expressed as:

$$\frac{P(x)}{Q(x)} = \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{A_i^j}{(x - a_i)^j} + \sum_{i=1}^{m} \sum_{j=1}^{s_i} \frac{M_i^j x + N_i^j}{(x^2 + b_i x + c_i)^j}$$

where $A_i^j, M_i^j, N_i^j \in \mathbb{R}\ \forall i, j$.

Proposition 3.170. Let $P(x), Q(x) \in \mathbb{R}[x]$ be polynomials. If $P(x) = C(x)Q(x) + R(x)$, then:

$$\int \frac{P(x)}{Q(x)} \mathrm{d}x = \int C(x) \mathrm{d}x + \int \frac{R(x)}{Q(x)} \mathrm{d}x$$

where $\deg R(x) < \deg Q(x)$.

Lemma 3.171. Let $P(x), Q(x) \in \mathbb{R}[x]$ be polynomials with $\deg P(x) < \deg Q(x)$. Suppose $Q(x)$ factorises as:

$$Q(x) = \prod_{i=1}^{n} (x - a_i)^{r_i} \prod_{i=1}^{m} (x^2 + b_i x + c_i)^{s_i}$$

with $b_i^2 - 4c_i < 0$ for $i = 1, \ldots, m$. Then, the function $\frac{P(x)}{Q(x)}$ can be expressed as:

$$\frac{P(x)}{Q(x)} = \left(\frac{A_1(x)}{Q_1(x)}\right)' + \frac{A_2(x)}{Q_2(x)}$$

where $Q_2(x) = \prod_{i=1}^{n}(x - a_i) \prod_{i=1}^{m}(x^2 + b_i x + c_i)$, $Q_1(x) = \frac{Q(x)}{Q_2(x)}$ and $A_i \in \mathbb{R}[x]$ with $\deg A_i(x) < \deg Q_i(x)$, $i = 1, 2$.

Theorem 3.172 (Hermite reduction method). Let $P(x), Q(x) \in \mathbb{R}[x]$ be polynomials. Suppose

$$\frac{P(x)}{Q(x)} = \left(\frac{A_1(x)}{Q_1(x)}\right)' + \frac{A_2(x)}{Q_2(x)}$$

for some polynomials $Q_i(x), A_i(x) \in \mathbb{R}[x]$. Then:

$$\int \frac{P(x)}{Q(x)} \mathrm{d}x = \frac{A_1(x)}{Q_1(x)} + \int \frac{A_2(x)}{Q_2(x)} \mathrm{d}x$$

Chapter 1.2

Second year

1.2.1 Algebraic structures

1.2.1.1 | Groups

Groups and subgroups

Definition 1.1 (Group). A *group* is a non-empty set G together with a binary operation

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1 \cdot g_2 \end{aligned}$$

satisfying the following properties:

1. Associativity:
$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad \forall g_1, g_2, g_3 \in G$$
2. Identity element:
$$\exists e \in G : e \cdot g = g \cdot e = g \quad \forall g \in G$$[1]
3. Inverse element:
$$\forall g \in G, \exists h \in G : g \cdot h = h \cdot g = e$$
We denote h by g^{-1}.

In this context we say $(G \cdot)$ is a group. If, moreover, we have $g_1 \cdot g_2 = g_2 \cdot g_1 \ \forall g_1, g_2 \in G$, we say that the group $(G, \cdot)$ is *commutative* or *abelian*[2].

Lemma 1.2. Let $(G, \cdot)$ be a group. Then:

1. The identity element is unique.
2. Given an element $g \in G$, $\exists! h \in G$ such that $g \cdot h = h \cdot g = e$.
3. Given $g, h \in G$ such that $g \cdot h = e$, we have $h = g^{-1}$.

Definition 1.3 (Subgroup). Let $(G, \cdot)$ be a group and H be a subset of G. $(H, \cdot)$ is called a *subgroup* of $(G, \cdot)$[3] if satisfies:

1. If $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$.
2. $e \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Proposition 1.4. Let $(G, \cdot)$ be a group and $H \neq \varnothing$ be a subset of G. Then:

$$(H, \cdot) \text{ is a subgroup} \iff h_1 \cdot h_2^{-1} \in H \quad \forall h_1, h_2 \in H$$

Proposition 1.5. If $(H, +)$ is a subgroup of $(\mathbb{Z}, +)$, then $\exists n \in \mathbb{Z}$ such that $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

Proposition 1.6. Let $(G_i, *_i)$, $i = 1, \ldots, n$, be groups. Then the product

$$(G_1, *_1) \times \cdots \times (G_n, *_n)$$

induces a group with the operation $\cdot$ defined as

$$(g_1, \ldots, g_n) \cdot (g_1', \ldots, g_n') = (g_1 *_1 g_1', \ldots, g_n *_n g_n'),$$

where $g_i, g_i' \in G_i$.

Definition 1.7. The *order of a group* $(G, \cdot)$ is the number of elements in its set, that is, $|G|$.

Lemma 1.8. Let $(G, \cdot)$ be a group and $\{(H_i, \cdot) : i \in I\}$ be a set of subgroups of $(G, \cdot)$. Then if

$$H = \bigcap_{i \in I} H_i,$$

we have that $(H, \cdot)$ is also a subgroup of $(G, \cdot)$.

Definition 1.9. Let $(G, \cdot)$ be a group and $X \subseteq G$ be a subset of G. The *subgroup of* $(G, \cdot)$ *generated by* X, $(\langle X \rangle, \cdot)$, is the smallest subgroup of $(G, \cdot)$ containing X, that is,

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

Definition 1.10. Let $(G, *)$ be a group, $g \in G$ and $n \in \mathbb{Z}$. We define g^n as:

$$g^n = \begin{cases} g * \overset{(n)}{\cdots} * g & \text{if} \quad n > 0 \\ 1 & \text{if} \quad n = 0 \\ (g^{-1}) * \overset{(|n|)}{\cdots} * (g^{-1}) & \text{if} \quad n < 0 \end{cases}$$

Lemma 1.11. Let $(G, \cdot)$ be a group and $g \in G$. Then for all $n, m \in \mathbb{Z}$ we have:

1. $g^n \cdot g^m = g^{n+m} = g^m \cdot g^n$.
2. $(g^n)^m = g^{nm} = (g^m)^n$.

Proposition 1.12. Let $(G, *)$ be a group and $X \subseteq G$ be a subset of G. Then:

$$\langle X \rangle = \{e\} \cup \{g_1^{\alpha_1} * \cdots * g_n^{\alpha_n} : n \in \mathbb{N}, \alpha_i \in \mathbb{Z}, g_i \in X\}$$

Corollary 1.13. Let $(G, \cdot)$ be a group and $g \in G$. Then:

$$\langle g \rangle = \{g^i : i \in \mathbb{Z}\}$$

Definition 1.14. Let $(G, \cdot)$ be a group and $g \in G$. A subgroup $(\langle g \rangle, \cdot)$ of $(G, \cdot)$ generated by a single element g is called a *cyclic group*.

Definition 1.15. Let $(G, \cdot)$ be a group and $g \in G$. The *order of* g is $\operatorname{ord}(g) := |\langle g \rangle|$.

Proposition 1.16. Let $(G, \cdot)$ be a group and $g \in G$. Then:

$$\operatorname{ord}(g) = \min\{i \in \mathbb{N} : g^i = e\}$$

If no such i exists, we say $\operatorname{ord}(g) = \infty$.

Corollary 1.17. Let $n \in \mathbb{N}$ such that $n > 1$ and $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Then:

$$\operatorname{ord}(\bar{a}) = \frac{n}{\gcd(a, n)}$$

[1] From now on, we will denote e or e_G the identity element of the group $(G, \cdot)$.
[2] Sometimes to simplify the notation and if the context is clear, we will refer to G directly as the group as well as the set.
[3] Sometimes we will denote that $(H, \cdot)$ is a subgroup of $(G, \cdot)$ by $H \leq G$.

Lemma 1.18. Let $(G,\cdot)$ be a group and $g\in G$ such that $\mathrm{ord}(g)=n$. Then:

1. $g^m=e \iff n\mid m$.
2. $g^m=g^{m'} \iff m=m' \mod n$.
3. If $0\le i\le n$, then $g^{-i}=(g^i)^{-1}=g^{n-i}$.

Corollary 1.19. Let $(G_i,*_i)$, $i=1,\dots,n$, be groups. For $i=1,\dots,n$, let $g_i\in G_i$ and consider the element $g=(g_1,\dots,g_n)\in(G_1,*_1)\times\cdots\times(G_n,*_n)$. Then:

$$\mathrm{ord}(g)=\mathrm{lcm}(\mathrm{ord}(g_1),\dots,\mathrm{ord}(g_n))$$

Group morphisms

Definition 1.20 (Group morphism). Let $(G,*)$, $(H,\cdot)$ be two groups. A *group morphism from* $(G,*)$ *to* $(H,\cdot)$ is a function $\phi:G\to H$ such that:

$$\phi(g_1*g_2)=\phi(g_1)\cdot\phi(g_2)\quad\forall g_1,g_2\in G$$

Lemma 1.21. Let $\phi:G_1\to G_2$ be a morphism between $(G_1,*)$ and $(G_2,\cdot)$. Then,

1. $\phi(e_1)=e_2$.
2. $\phi(g^{-1})=\phi(g)^{-1}\quad\forall g\in G_1$.
3. $\phi(g^n)=\phi(g)^n\quad\forall g\in G_1$ and $\forall n\in\mathbb{Z}$.

Definition 1.22. We say a subgroup $(H,\cdot)$ of a group $(G,\cdot)$ is *normal*, $H\lhd G$, if and only if $\forall h\in H$ and $\forall g\in G$, we have $g\cdot h\cdot g^{-1}\in H$.

Definition 1.23. Let $(G_1,*)$, $(G_2,\cdot)$ be two groups and $\phi:G_1\to G_2$ be a group morphism. The *kernel of* ϕ is:

$$\ker\phi=\{g\in G_1:\phi(g)=e_2\}$$

The *image of* ϕ is:

$$\mathrm{im}\,\phi=\{h\in G_2:\phi(g)=h \text{ for some } g\in G_1\}$$

Proposition 1.24. Let $(G_1,*)$, $(G_2,\cdot)$ be two groups and $\phi:G_1\to G_2$ be a group morphism. Then:

1. $(\ker\phi,*)$ is a normal subgroup of $(G_1,*)$ and $(\mathrm{im}\,\phi,\cdot)$ is a subgroup of $(G_2,\cdot)$.
2. Let $g,g'\in G_1$. The following statements are equivalent:
   i) $\phi(g)=\phi(g')$.
   ii) $g*g'^{-1}\in\ker\phi$.
   iii) $g'^{-1}*g\in\ker\phi$.
3. ϕ is injective if and only if $\ker\phi=\{e_1\}$.
4. ϕ is surjective if and only if $\mathrm{im}\,\phi=G_2$.

Definition 1.25. Let $(G,*)$, $(H,\cdot)$ be two groups. An *isomorphism between* $(G,*)$ *and* $(H,\cdot)$ is a bijective morphism between these groups. In this case, we say that $(G,*)$, $(H,\cdot)$ are *isomorphic*: $G\cong H$.

Proposition 1.26. Let $(G_1,\cdot_1)$, $(G_2,\cdot_2)$, $(G_3,\cdot_3)$ be three groups and $\phi:G_1\to G_2$, $\psi:G_2\to G_3$ be two group morphisms. Then the composition $\psi\circ\phi$ is also a group morphism.

Proposition 1.27. Let $(G_1,*)$, $(G_2,\cdot)$ be groups and let $\phi:G_1\to G_2$ be an isomorphism. Then $\phi^{-1}:G_2\to G_1$ is also an isomorphism.

Theorem 1.28 (Classification of cyclic groups). Let $(G,\cdot)$ be a group and $g\in G$ be an element such that $\langle g\rangle=G$.

- If $|G|=\infty$, then $G\cong\mathbb{Z}$. We can define the isomorphism as follows:

$$\begin{aligned}\phi:\mathbb{Z}&\longrightarrow G\\ k&\longmapsto g^k\end{aligned}$$

- If $|G|=n$, then $G\cong\mathbb{Z}/n\mathbb{Z}$. We can define the isomorphism as follows:

$$\begin{aligned}\phi:\mathbb{Z}/n\mathbb{Z}&\longrightarrow G\\ \bar{k}&\longmapsto g^k\end{aligned}$$

Corollary 1.29. Let $(G,\cdot)$ be a group and $g\in G$ be such that $\langle g\rangle=G$. Then all subgroups of G are cyclic. Moreover:

- If $|G|=\infty$, subgroups of $(G,\cdot)$ are of the form $\langle g^n\rangle$, $n\in\mathbb{N}\cup\{0\}$.
- If $|G|=n$, then there is a unique subgroup $(H,\cdot)$ of $(G,\cdot)$ for every divisor $d>0$ of n. In fact, if $n=dq$, then $H=\langle g^q\rangle$ and $|H|=d$.

Definition 1.30. Let X be a set. We define the *symmetric group* $(S(X),\circ)$ as:

$$S(X)=\{f:X\to X: f \text{ is bijective}\}^4$$

Definition 1.31. Let $(G,\cdot)$ be a group. We define the functions:

$$\begin{aligned}\ell_g:G&\longrightarrow G\\ x&\longmapsto g\cdot x\end{aligned}\qquad\qquad \begin{aligned}r_g:G&\longrightarrow G\\ x&\longmapsto x\cdot g\end{aligned}$$

Lemma 1.32. Let $(G,\cdot)$ be a group. The functions ℓ_g, r_g are bijective and its inverses are $\ell_{g^{-1}}$, $r_{g^{-1}}$, respectively.

Proposition 1.33. Let $(G,\cdot)$ be a group. We define the functions:

$$\begin{aligned}\phi:G&\longrightarrow S(G)\\ g&\longmapsto \ell_g\end{aligned}\qquad\qquad \begin{aligned}\psi:G&\longrightarrow S(G)\\ g&\longmapsto r_{g^{-1}}\end{aligned}$$

Then, ϕ and ψ are injective group morphisms.

Theorem 1.34 (Cayley's theorem). Let $(G,\cdot)$ be a group. Then, there is an injective morphism:

$$\phi:G\longrightarrow S(G)$$

Corollary 1.35. If $(G,\cdot)$ is a group with $|G|=n$, then $(G,\cdot)$ is isomorphic to a subgroup of $(S_n,\circ)$.

[4] Observe that if $X=\{1,\dots,n\}$, then $S(X)=S_n$.

Cosets

Definition 1.36. Let $(G,\cdot)$ be a finite group, $(H,\cdot)$ be a subgroup of $(G,\cdot)$ and $g_1,g_2\in G$.

- We say $g_1\sim g_2 \iff g_1\cdot g_2^{-1}\in H$.
- We say $g_1\approx g_2 \iff g_2^{-1}\cdot g_1\in H$.

Lemma 1.37. Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. Then:

1. $\sim$ and $\approx$ are equivalence relations.
2. If $g\in G$, then:
$$\begin{aligned}[g]_\sim &= H\cdot g=\{h\cdot g : h\in H\}\\ [g]_\approx &= g\cdot H=\{g\cdot h' : h'\in H\}\end{aligned}$$
Usually we say that $H\cdot g$ are the *right cosets in* G and $g\cdot H$, the *left cosets in* G.

Definition 1.38. Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. We define the *set of right cosets* and the *set of left cosets*, respectively, as follows:
$$G/_{\sim}=\{H\cdot g: g\in G\}\quad G/_{\approx}=\{g\cdot H : g\in G\}$$

Proposition 1.39. Let $(G,\cdot)$ be a group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. The following statements are equivalent:

1. $H\lhd G$.
2. $g\cdot H=H\cdot g\quad \forall g\in G$.

Theorem 1.40 (Lagrange's theorem). Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. Then:
$$|H|\mid |G|$$

Definition 1.41. Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. We define the *index of* $(H,\cdot)$ *in* $(G,\cdot)$ as:
$$[G:H]:=\frac{|G|}{|H|}$$

Corollary 1.42. Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. Then:
$$[G:H]=\left|G/_{\sim}\right|=\left|G/_{\approx}\right|$$

Corollary 1.43. Let $(G,\cdot)$ be a finite group.

1. If $g\in G$, then $\operatorname{ord}(g)\mid |G|$.
2. If $|G|$ is prime, then $(G,\cdot)$ is cyclic.
3. If $(H,\cdot)$ and $(K,\cdot)$ are subgroups of $(G,\cdot)$ and $\gcd(|H|,|K|)=1$, then $H\cap K=\{e\}$.

Definition 1.44 (Quotient group). Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$ such that $H\lhd G$. We define the *quotient group* $(G/H,*)$ as
$$G/_{H}=G/_{\sim}=G/_{\approx}$$
and
$$\begin{aligned} *: G/_H\times G/_H &\longrightarrow G/_H\\ (g_1\cdot H, g_2\cdot H)&\longmapsto (g_1\cdot g_2)\cdot H\end{aligned}$$

Lemma 1.45. Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$ such that $H\lhd G$. The projection
$$\begin{aligned}\pi: G&\longrightarrow G/_H\\ g&\longmapsto [g]=g\cdot H\end{aligned}$$
is a group morphism.

Isomorphism theorems

Theorem 1.46 (First isomorphism theorem). Let $(G_1,*)$, $(G_2,\cdot)$ be groups, $\phi: G_1\to G_2$ be a group morphism and $(H,*)$ be a subgroup of $(G_1,*)$ such that $H\lhd G_1$. If $(H,*)$ is a subgroup of $(\ker\phi,*)$, then there exists a unique group morphism $\psi: G_1/H\to G_2$ such that the diagram of figure 1.2.1 is commutative, that is, $\phi=\psi\circ\pi$.

$$\begin{tikzcd} G_1 \arrow[r, "\phi"] \arrow[d, "\pi"'] & G_2 \\ G_1/_H \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 1.2.1

The definition of ψ is $\psi([g])=\phi(g)\ \forall g\in G_1$. In particular, if $H=\ker\phi$, then ψ is injective and therefore there is an isomorphism $\psi: G_1/\ker\phi\to \operatorname{im}\phi$.

Theorem 1.47. Let
$$\begin{aligned}\phi:\mathbb{Z}&\longrightarrow \mathbb{Z}/_{n\mathbb{Z}}\times\mathbb{Z}/_{m\mathbb{Z}}\\ 1&\longmapsto (\bar{1},\bar{1})\end{aligned}$$
be a group morphism. Then, ϕ induces a morphism $\psi:\mathbb{Z}/nm\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. Moreover, ψ is injective if and only if $\gcd(n,m)=1$ and in this case ψ is an isomorphism.

Corollary 1.48. Let $n,m\in\mathbb{Z}$ be two coprime integers and $a,b\in\mathbb{Z}$. The system of congruences
$$\begin{cases} x\equiv a \mod n\\ x\equiv b\mod m\end{cases}$$
has solutions and these are of the form $x\equiv c\mod nm$, where $c\equiv a\mod n$ and $c\equiv b\mod m$.

Definition 1.49. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$. We define the *products of group subsets* K, H as the sets:
$$\begin{aligned}H\cdot K&=\{h\cdot k: h\in H, k\in K\}\\ K\cdot H&=\{k\cdot h : k\in K, h\in H\}\end{aligned}$$

Proposition 1.50. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\lhd G$. Then, $(H\cdot K,\cdot)$ is a subgroup of $(G,\cdot)$ and $H\cdot K=K\cdot H$.

Proposition 1.51. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\cap K=\{e\}$. If $H,K\lhd G$, then the function

$$\begin{aligned}\phi : H\times K &\longrightarrow H\cdot K\\ (h,k)&\longmapsto h\cdot k\end{aligned}$$

is an isomorphism. In particular, $\forall h\in H$ and $\forall k\in K$, $h\cdot k=k\cdot h$.

Theorem 1.52 (Second isomorphism theorem). Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\lhd G$. Then $H\cap K\lhd K$ and

$$K/_{H\cap K}\cong H\cdot K/_{H}$$

Corollary 1.53. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$. Then:

$$|H||K|=|H\cap K||H\cdot K|$$

Lemma 1.54. Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H\lhd G$ and $H\subseteq K$. Then $H\lhd K$, $(K/H,*)$ is a subgroup of $(G/H,*)$ and moreover

$$K/_{H}\lhd G/_{H}\iff K\lhd G$$

Theorem 1.55 (Correspondence theorem). Let $(G,\cdot)$ be a group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$ such that $H\lhd G$. Then, there is a bijection ϕ from the set $\mathcal{G}$ of all subgroups $(K,\cdot)$ of $(G,\cdot)$ such that $H\subseteq K$ onto the set $\mathcal{H}$ of all subgroups $(K/H,*)$ of $(G/H,*)$. More precisely, the bijection is:

$$\begin{aligned}\phi:\mathcal{G}&\longrightarrow\mathcal{H}\\ K&\longmapsto K/H\end{aligned}$$

Theorem 1.56 (Third isomorphism theorem). Let $(G,\cdot)$ be a group and $(H,\cdot)$, $(K,\cdot)$ be subgroups of $(G,\cdot)$ such that $H,K\lhd G$ and $H\subseteq K$. Then $K/H\lhd G/H$ and

$$\left(G/_{H}\right)/\left(K/_{H}\right)\cong G/_{K}$$

Group actions

Definition 1.57. Let X be a set and $(G,\cdot)$ be a group. A *(left) group action of* $(G,\cdot)$ *on* X is a function

$$\begin{aligned}*:G\times X&\longrightarrow X\\ (g,x)&\longmapsto g*x\end{aligned}$$

satisfying the following properties:

1. $e*x=x$, $\forall x\in X$.
2. $(g_1\cdot g_2)*x=g_1*(g_2*x)$, $\forall x\in X$ and $\forall g_1,g_2\in G$.

A set X together with an action $*$ of $(G,\cdot)$ is usually called a *(left) G-set*.

Lemma 1.58. Let $(G,\cdot)$ be a group and X be a G-set. For all $g\in G$ the function

$$\begin{aligned}\ell_g:X&\longrightarrow X\\ x&\longmapsto g*x\end{aligned}$$

is bijective an its inverse is $\ell_{g^{-1}}$.

Definition 1.59. Let $(G,\cdot)$ be a group and X be a G-set. For all $x,y\in X$, we say $x\backsim y\iff\exists g\in G:y=g*x$.

Lemma 1.60. The relation $\backsim$ is an equivalence relation.

Definition 1.61. Let $(G,\cdot)$ be a group and X be a G-set. If $x\in X$, we define the *orbit of x* as:

$$\mathcal{O}_x=[x]_\backsim=\{g*x:g\in G\}$$

Definition 1.62. Let $(G,\cdot)$ be a group and X be a G-set. For $x\in X$, we define the *stabilizer of* $(G,\cdot)$ *with respect to* x as the set:

$$G_x=\{g\in G:g*x=x\}$$

Proposition 1.63. Let $(G,\cdot)$ be a group and X be a G-set. For all $x\in X$, $(G_x,\cdot)$ is a subgroup of $(G,\cdot)$.

Theorem 1.64 (Orbit-stabilizer theorem). Let $(G,\cdot)$ be a group, X be a G-set and $x\in X$. The surjective function

$$\begin{aligned}\phi:G&\longrightarrow\mathcal{O}_x\\ g&\longmapsto g*x\end{aligned}$$

induces a bijective function $\psi:G/{\approx}\to\mathcal{O}_x$, where $\approx$ is the equivalence relation $g_1\approx g_2\iff g_2^{-1}\cdot g_1\in G_x$ $\forall g_1,g_2\in G$[5]. In particular, if G is finite:

$$|\mathcal{O}_x|=|[G:G_x]|$$

Corollary 1.65 (Orbits formula). Let $(G,\cdot)$ be a finite group and X be a finite G-set. If $x_1,\ldots,x_m$ are the elements of X and $|\mathcal{O}_{x_i}|=1$ for $i=1,\ldots,r$, then:

$$|X|=r+\sum_{i=r+1}^{m}|\mathcal{O}_{x_i}|=r+\sum_{i=r+1}^{m}|[G:G_{x_i}]| \tag{1.2.1}$$

Applications of orbits formula

Theorem 1.66 (Cauchy's theorem). Let $(G,\cdot)$ be a finite group of order n and $p\in\mathbb{P}$. If $p\mid n$, then $(G,\cdot)$ has an element of order p.

Corollary 1.67. Let p be an odd prime number. Then groups of order $2p$ are isomorphic to $(\mathbb{Z}/2p\mathbb{Z},+)$ or $(\mathrm{D}_{2p},\circ)$[6].

Proposition 1.68. Let $(G,\cdot)$ be a group. The function

$$\begin{aligned}G\times G&\longrightarrow G\\ (g,x)&\longmapsto g\cdot x\cdot g^{-1}\end{aligned}$$

is an action of $(G,\cdot)$ over itself. It is called the *conjugation action*.

[5]Note that the notation $\approx$ for the equivalence relation correspond with the one defined in definition 1.36.

[6]See section 1.2.1.1.

Definition 1.69 (Center of a group). Let $(G,\cdot)$ be a group. We define the *center of* $(G,\cdot)$ as:

$$Z(G)=\{z\in G:z\cdot g=g\cdot z\ \forall g\in G\}$$[7]

Proposition 1.70. Let $p\in\mathbb{P}$ and $(G,\cdot)$ be a finite group of order p^n for some $n\geq 1$. Then, $|Z(G)|>1$.

Lemma 1.71. Let $(G,\cdot)$ be a group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. Consider the application

$$\begin{aligned}H\times {}^{G}\!/_{\approx}&\longrightarrow {}^{G}\!/_{\approx}\\(h,g\cdot H)&\longmapsto(h\cdot g)\cdot H\end{aligned}$$

This application defines an action of the subgroup $(H,\cdot)$ over the set $G/{\approx}$.

Definition 1.72. Let $(G,\cdot)$ be a group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. The *normalizer of* $(H,\cdot)$ *in* $(G,\cdot)$ is

$$N_G(H)=\{g\in G:g\cdot h\cdot g^{-1}\in H\ \forall h\in H\}$$

Lemma 1.73. Let $(G,\cdot)$ be a group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. Then, $(N_G(H),\cdot)$ is a subgroup of $(G,\cdot)$ containing H and, moreover, $H\lhd N_G(H)$.

Corollary 1.74. Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ be a subgroup of $(G,\cdot)$. Then, by orbits formula applied to action defined on lemma 1.71, we have:

$$[G:H]=[N_G(H):H]+\sum_{|\mathcal{O}_x|>1}|\mathcal{O}_x|$$

Proposition 1.75. Let $(G,\cdot)$ be a group of order $n\in\mathbb{N}$, $p\in\mathbb{P}$ such that $p\mid n$ and $(H,\cdot)$ be a subgroup of $(G,\cdot)$ of order p^i, $i\geq 1$. Suppose $p\mid[G:H]$. Then, $p\mid[N_G(H):H]$.

Sylow's theorems

Corollary 1.76. Let $(G,\cdot)$ be a group of order $n\in\mathbb{N}$, $p\in\mathbb{P}$ and $(H,\cdot)$ be a subgroup of $(G,\cdot)$ such that $|H|=p^i$, $i\geq 0$. Suppose $p\mid[G:H]$. Then, there is a subgroup $(H',\cdot)$ of $(G,\cdot)$ such that $H\subset H'$ and $|H'|=p^{i+1}$. Moreover, $H\lhd H'$ and $H'/H\cong\mathbb{Z}/p\mathbb{Z}$.

Theorem 1.77 (First Sylow theorem). Let $(G,\cdot)$ be a finite group and $p\in\mathbb{P}$. Suppose $|G|=p^rm$, where $r\geq 0$ and $\gcd(p,m)=1$. Then, there is a subgroup $(K,\cdot)$ of $(G,\cdot)$ of order p^r. Moreover there is a chain of subgroups $(H_i,\cdot)$ satisfying:

$$\{e\}=H_0\lhd H_1\lhd\cdots\lhd H_r=K,$$

such that $H_{i+1}/H_i\cong\mathbb{Z}/p\mathbb{Z}$ for $0\leq i<r$.

Definition 1.78. Let $p\in\mathbb{P}$. A group $(G,\cdot)$ is a *p-group* if $|G|=p^r$, for some $r\in\mathbb{N}$.

Definition 1.79. Let $p\in\mathbb{P}$ and $(G,\cdot)$ be a group. A *Sylow p-subgroup* is a p-subgroup of $(G,\cdot)$ of maximum order.

Definition 1.80. Let $(G,\cdot)$ be a finite group. We say $(G,\cdot)$ is *soluble* if there is a chain of subgroups $(H_i,\cdot)$ of $(G,\cdot)$ satisfying:

$$\{e\}=H_0\lhd H_1\lhd\cdots\lhd H_r=K,$$

and such that the subgroups $(H_{i+1}/H_i,*)$, $0\leq i<r$, are cyclic.

Theorem 1.81 (Second Sylow theorem). Let $(G,\cdot)$ be a finite group and $p\in\mathbb{P}$. Suppose $|G|=p^rm$, where $r\geq 0$ and $\gcd(p,m)=1$. Let $(K,\cdot)$ be a Sylow p-subgroup of $(G,\cdot)$. Then, if $(H,\cdot)$ is a subgroup of $(G,\cdot)$ of order p^i, $\exists g\in G$ such that $g\cdot H\cdot g^{-1}\subseteq K$. In particular two different Sylow p-subgroups $(K_1,\cdot)$ and $(K_2,\cdot)$ are conjugate, that is, there exists an element $g\in G$ such that $g\cdot K_1\cdot g^{-1}=K_2$.

Theorem 1.82 (Third Sylow theorem). Let $(G,\cdot)$ be a finite group and $p\in\mathbb{P}$. Suppose $|G|=p^rm$, where $r\geq 0$ and $\gcd(p,m)=1$. Let $(K,\cdot)$ be a Sylow p-subgroup of $(G,\cdot)$ and n_p be the number of different Sylow p-subgroups of $(G,\cdot)$. Then, $n_p=[G:N_G(K)]$, $n_p\mid m$ and $n_p\equiv 1\mod p$.

Corollary 1.83. Let $p,q\in\mathbb{P}$ be such that $p<q$ and $q\not\equiv 1\mod p$. If $(G,\cdot)$ is a group of order pq, then $G\cong\mathbb{Z}/pq\mathbb{Z}$.

Examples of groups

Let $n\in\mathbb{N}$ and $p\in\mathbb{P}$.

- $(\mathbb{Z},+)$, $(\mathbb{Z}/n\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$
- $((\mathbb{Z}/p\mathbb{Z})^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$
- $(S_n,\circ)$
- $(A_n,\circ)$, where $A_n=\{\sigma\in S_n:\varepsilon(\sigma)=1\}$. Note that $|A_n|=\frac{S_n}{2}=\frac{n!}{2}$.
- $(\mathrm{GL}_n(\mathbb{A}),\cdot)$, where $\mathrm{GL}_n(\mathbb{A})=\{\mathbf{M}\in\mathcal{M}_n(\mathbb{A}):\mathbf{M}\text{ is invertible}\}$ and $\mathbb{A}=\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.
- $(\mathrm{SL}_n(\mathbb{A}),\cdot)$, where $\mathrm{SL}_n(\mathbb{A})=\{\mathbf{M}\in\mathrm{GL}_n(\mathbb{A}):\det\mathbf{M}=1\}$ and $\mathbb{A}=\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.
- $(\mathrm{D}_{2n},\circ)$, where D_{2n} is the set of rotations and reflections that leave invariant the regular polygon of n vertices centered at origin. It can be seen that $\mathrm{D}_{2n}=\langle r,s:\mathrm{ord}(r)=n,\mathrm{ord}(s)=2,r\circ s=s\circ r^{-1}\rangle$. This group is called the *dihedral group*. Note that $|\mathrm{D}_{2n}|=2n$.
- $(\mathrm{Q}_8,\cdot)$, where $\mathrm{Q}_8=\langle a,b:\mathrm{ord}(a)=\mathrm{ord}(b)=4,b\cdot a=a^{-1}\cdot b\rangle$. This group is called the *quaternion group*. Note that $|\mathrm{Q}_8|=8$.
- $(\mathrm{Dic}_n,\cdot)$, where $\mathrm{Dic}_n=\langle a,b:\mathrm{ord}(a)=2n,b^2=a^n,b^{-1}\cdot a\cdot b=a^{-1}\rangle$. This group is called the *dicyclic group*. Note that $|\mathrm{Dic}_n|=4n$.

[7]Note that, by orbits formula (1.2.1), if we consider the conjugation action we have:

$$|G|=|Z(G)|+\sum_{|\mathcal{O}_x|>1}|\mathcal{O}_x|$$

Classification of groups of small order

$\|G\|$	Non-isomorphic groups
1	$\{e\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, S_3
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, $\mathrm{D}_{2\cdot 4}$, Q_8
9	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$
10	$\mathbb{Z}/10\mathbb{Z}$, $\mathrm{D}_{2\cdot 5}$
11	$\mathbb{Z}/11\mathbb{Z}$
12	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathrm{D}_{2\cdot 6}$, A_4, Dic_3
13	$\mathbb{Z}/13\mathbb{Z}$
14	$\mathbb{Z}/14\mathbb{Z}$, $\mathrm{D}_{2\cdot 7}$
15	$\mathbb{Z}/15\mathbb{Z}$

1.2.1.2 | Rings and fields

Rings, subrings and ring morphisms

Definition 1.84 (Ring). A *ring* is a set R equipped with two binary operations (called addition and multiplication):

$$\begin{aligned} +: R\times R &\longrightarrow R & \cdot: R\times R &\longrightarrow R\\ (r_1,r_2) &\longmapsto r_1+r_2 & (r_1,r_2) &\longmapsto r_1\cdot r_2\end{aligned}$$

satisfying the following properties:

1. $(R,+)$ is an abelian group.
2. $(R,\cdot)$ satisfies[8]:
   i) Associativity:
   $$(r_1\cdot r_2)\cdot r_3 = r_1\cdot(r_2\cdot r_3)\quad \forall r_1,r_2,r_3\in R.$$
   ii) Identity element[9]:
   $$\exists 1\in R: 1\cdot r = r\cdot 1 = r\quad \forall r\in R.$$
   iii) Commutativity:
   $$r_1\cdot r_2 = r_2\cdot r_1\quad \forall r_1,r_2\in R.$$
3. Multiplication is distributive with respect to addition:
   $$(r_1+r_2)\cdot r_3 = r_1\cdot r_3 + r_2\cdot r_3\quad \forall r_1,r_2,r_3\in R.$$

In this context we say $(R,+,\cdot)$ is a ring.

Definition 1.85. A *noncommutative ring* is a ring whose multiplication is not commutative.

Definition 1.86 (Field). Let $(R,+,\cdot)$ be a ring. If every nonzero element of R has a multiplicative inverse (that is, $(R,\cdot)$ is an abelian group), we say that R is a *field*.

Proposition 1.87. Let $(R_i,+_i,\cdot_i)$, $i=1,\ldots,n$, be rings. Then the product

$$(R_1,+_1,\cdot_1)\times\cdots\times(R_n,+_n,\cdot_n)$$

induces a ring with operations $+$ and $\cdot$ defined as

$$\begin{aligned}(r_1,\ldots,r_n)+(r_1',\ldots,r_n') &= (r_1+_1 r_1',\ldots,r_n+_n r_n'),\\ (r_1,\ldots,r_n)\cdot(r_1',\ldots,r_n') &= (r_1\cdot_1 r_1',\ldots,r_n\cdot_n r_n'),\end{aligned}$$

where $r_i,r_i'\in R_i$.

Proposition 1.88. Let $(R,+,\cdot)$ be a ring. We define the *set of polynomials over the ring* $(R,+,\cdot)$ as:

$$R[x] := \{r_0 + r_1\cdot x+\cdots+r_n\cdot x^n : r_i\in R\ \forall i \text{ and } n\geq 0\}.$$

Moreover, $(R[x],+,\cdot)$ is a ring.

Definition 1.89. A ring $(R,+,\cdot)$ is a *Boolean ring* if $r^2=r$ $\forall r\in R$.

Lemma 1.90. Let $(R,+,\cdot)$ be a ring. Then:

1. The multiplicative identity element is unique.
2. $\forall r\in R$, $0\cdot r=0$.
3. $\forall r\in R$, $(-1)\cdot r=-r$, where -1 is the additive inverse of 1.
4. $\forall r,s\in R$, $(-r)\cdot s = -(r\cdot s)$ and $(-r)\cdot(-s)=r\cdot s$.

Definition 1.91 (Subring). Let $(R,+,\cdot)$ be a ring and $S\subseteq R$ be a subset of R. $(S,+,\cdot)$ is called a *subring* of $(R,+,\cdot)$ if satisfies:

1. $(S,+)$ is a subgroup of $(R,+)$.
2. $\forall s_1,s_2\in S$, $s_1\cdot s_2\in S$.
3. $1\in S$.

Definition 1.92 (Ring morphism). Let $(R,+,\cdot)$, $(S,\oplus,\odot)$ be two rings. A *ring morphism from* $(R,+,\cdot)$ *to* $(S,\oplus,\odot)$ is a function $\phi: R\to S$ such that:

1. $\phi(r_1+r_2)=\phi(r_1)\oplus\phi(r_2)\quad \forall r_1,r_2\in R$[10].
2. $\phi(r_1\cdot r_2)=\phi(r_1)\odot\phi(r_2)\quad \forall r_1,r_2\in R$.
3. $\phi(1_R)=1_S$.

Lemma 1.93. Let $(R,+,\cdot)$, $(S,\oplus,\odot)$ be two rings and $\phi: R\to S$ be a ring morphism. Then, knowing that $\ker\phi=\{r\in R: f(r)=0\}$, then:

1. $(\ker\phi,+)$ is a subgroup of $(R,+)$.
2. $\forall k\in\ker\phi$ and $\forall r\in R$, $k\cdot r\in\ker\phi$.

Proposition 1.94. Let $(R,+,\cdot)$, $(S,\oplus,\odot)$ be two rings and $\phi: R\to S$ be a ring morphism. Then:

1. $f(0)=0$.

[8]Some definitions state that the commutative property is not necessary to define a ring. However, in these notes we will take the definition given.
[9]It is common to denote the additive identity element as 0 and the multiplicative identity element as 1.
[10]That is, ϕ is a group morphism between groups $(R,+)$ and $(S,\oplus)$.

2. $f(-r) = -f(r)\ \forall r \in R$.
3. If $r \in R$ has a multiplicative inverse, then $f(r)$ so it has and, moreover, $f(r^{-1}) = f(r)^{-1}$.

Proposition 1.95. Let $(R_1, +_1, \cdot_1)$, $(R_2, +_2, \cdot_2)$ and $(R_3, +_3, \cdot_3)$ be rings and $\phi : R_1 \to R_2$, $\psi : R_2 \to R_3$ be two ring morphisms. Then, the composition $\psi \circ \phi$ is also a ring morphism.

Proposition 1.96. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be rings and let $\phi : R \to S$ be a bijective ring morphism. Then $\phi^{-1} : S \to R$ is also a bijective ring morphism.

Ideals

Definition 1.97 (Ideal). Let $(R, +, \cdot)$ be a ring. A subgroup $(I, +)$ of $(R, +)$ is an *ideal* if $\forall x \in I$ and $\forall r \in R$, $x \cdot r \in I$.

Lemma 1.98 (Principal ideal). Let $(R, +, \cdot)$ be a ring and $a \in R$. The set

$$(a) := a \cdot R = \{a \cdot r : r \in R\}$$

is an ideal of $(R, +, \cdot)$ and it is called *principal ideal generated by a*.

Proposition 1.99. Let $(R, +, \cdot)$ be a nonzero ring. R is a field if and only if $(R, +, \cdot)$ has only two ideals: $\{0\}$ and R.

Definition 1.100. Let $(R, +, \cdot)$ be a ring. An element $r \in R$ is a *unit* if it has a multiplicative inverse. The set of units in $(R, +, \cdot)$ is denoted by R^* or $U(R)$. Moreover, $(R^*, \cdot)$ is a group called *multiplicative group of* $(R, +, \cdot)$.

Lemma 1.101. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be rings and $u \in R^*$. Then:

1. If $r \in R$, then $r \cdot R = r \cdot u \cdot R$.
2. If $f : R \to S$ is a ring morphism, then $f : R^* \to S^*$ is a group morphism.

Proposition 1.102. Let K be a field. Then, all ideals of $K[x]$ are principal. Moreover if $I \neq \{0\}$ is an ideal of $K[x]$, there exists a monic polynomial $p(x) \in K[x]$ such that $I = p(x) \cdot K[x]$.

Proposition 1.103. Let $(R, +, \cdot)$ be a ring and I, J be a ideals of $(R, +, \cdot)$. Then the sets

$$I \cap J := \{x : x \in I,\ x \in J\}$$
$$I + J := \{x + y : x \in I,\ y \in J\}$$
$$I \cdot J := \left\{ \sum_{i=1}^{n} x_i y_i : n \geq 0,\ x_i \in I,\ y_i \in J \right\}$$

are all ideals. In particular $I \cap J$ is the largest ideal contained in I and J, and $I + J$ is the smallest ideal containing I and J.

Definition 1.104. Let $(R, +, \cdot)$ be a ring and I, J be a ideals of $(R, +, \cdot)$. If $I = (a)$ and $J = (b)$ for some $a, b \in R$, then we define (a, b) as:

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

Proposition 1.105. Let $a, b \in \mathbb{Z}$, $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Then:

$$(a) + (b) = (d) \qquad (a) \cap (b) = (m)$$

Definition 1.106. A ring is *Noetherian* if all its ideals are finitely generated.

Theorem 1.107 (Hilbert's basis theorem). If $(R, +, \cdot)$ is a Noetherian ring, then $(R[x_1, \ldots, x_n], +, \cdot)$ is a Noetherian ring.

Lemma 1.108. Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be two rings and $\phi : R \to S$ be a ring morphism. Then:

1. $\ker \phi$ is an ideal of $(R, +, \cdot)$.
2. $\operatorname{im} \phi$ is a subring of $(S, \oplus, \odot)$.

Ideal quotient

Definition 1.109. Let $(R, +, \cdot)$ be a ring and I be an ideal of $(R, +, \cdot)$. For all $r_1, r_2 \in R$, we say $r_1 \sim r_2 \iff r_1 - r_2 \in I$. Since $(I, +)$ is a subgroup of $(R, +)$, $\sim$ is an equivalence relation and we denote by

$$R/I := \{x + I : x \in R\}$$

the set of equivalence classes.

Proposition 1.110. Let $(R, +, \cdot)$ be a ring and I be an ideal of $(R, +, \cdot)$. Then R/I is a ring with operations defined as:

- $\forall r_1, r_2 \in R$, $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$. $\overline{0}$ is the identity element with respect to this operation.
- $\forall r_1, r_2 \in R$, $\overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2}$. $\overline{1}$ is the identity element with respect to this operation.

Moreover the projection:

$$\begin{aligned} \pi : R &\longrightarrow R/I \\ r &\longmapsto \overline{r} \end{aligned}$$

is a surjective ring morphism with $\ker \pi = I$.

Corollary 1.111. Let $(R, +, \cdot)$ be a ring and I be an ideal of $(R, +, \cdot)$. Ideals of R/I are of the form J/I, where J is an ideal of $(R, +, \cdot)$ containing I.

Isomorphism theorems

Theorem 1.112 (First isomorphism theorem). Let $(R, +, \cdot)$, $(S, \oplus, \odot)$ be two rings, $\phi : R \to S$ be a ring morphism and I be an ideal such that I is a subgroup of $(\ker \phi, +)$. Then there exists a unique ring morphism $\psi : R/I \to S$ such that the diagram of figure 1.2.2 is commutative, that is, $\phi = \psi \circ \pi$.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 1.2.2

The definition of ψ is $\psi([r]) = \phi(r)\ \forall r \in R$. In particular, if $I = \ker\phi$, then ψ is injective and therefore there is an isomorphism $\psi : R/\ker\phi \to \operatorname{im}\phi$.

Theorem 1.113 (Second isomorphism theorem). Let $(R, +, \cdot)$ be a ring and I, J be ideals of $(R, +, \cdot)$. Then, $(I + J)/I$ is an ideal of R/I and there is a group isomorphism

$$\phi : {}^{(I+J)}\!\big/_{I} \longrightarrow {}^{J}\!\big/_{(I \cap J)},$$

such that $\phi(a \cdot b) = \phi(a) \cdot \phi(b)\ \forall a, b \in J$.

Theorem 1.114 (Third isomorphism theorem). Let $(R, +, \cdot)$ be a ring and I, J be ideals of $(R, +, \cdot)$ such that $I \subseteq J$. Then, there is a ring isomorphism:

$$\left({}^{R}\!\big/_{I}\right)\Big/\left({}^{J}\!\big/_{I}\right) \cong {}^{R}\!\big/_{J}$$

Theorem 1.115 (Correspondence theorem). Let $(R, +, \cdot)$ be ring and I be an ideal of $(R, +, \cdot)$. Then there is a bijection ϕ from the set $\mathcal{R}$ of all ideals J of $(R, +, \cdot)$ such that $I \subseteq J$ onto the set $\mathcal{I}$ of all ideals J/I of R/I. More precisely, the bijection is:

$$\begin{aligned}\phi : \mathcal{R} &\longrightarrow \mathcal{I}\\ J &\longmapsto {}^{J}\!\big/_{I}\end{aligned}$$

Special rings and ideals

Definition 1.116. A ring $R \neq \{0\}$[11] is an *integral domain* if the product of any two nonzero elements is nonzero.

Definition 1.117. Let R be a ring. We say $r \in R$ is a *zero divisor* if $\exists s \in R \setminus \{0\}$ such that $r \cdot s = 0$. We say $r \in R$ is *not* a *zero divisor* if $r \cdot s = 0 \implies s = 0$.

Definition 1.118. Let R be an integral domain. We say R is a *principal ideal domain* (*PID*) if every ideal of R is principal.

Definition 1.119. Let R be a ring and $P \neq R$ be an ideal of R. We say P is *prime* if $\forall a, b \in R$, we have $a \cdot b \in P \iff a \in P$ or $b \in P$.

Definition 1.120. Let R be a ring and $M \neq R$ be an ideal of R. We say M is *maximal* if for any ideal I of R with $M \subseteq I$, either $I = R$ or $I = M$.

Proposition 1.121. Let R be a ring. Then:

1. An ideal P of R is prime if and only if R/P is an integral domain.
2. An ideal M of R is maximal if and only if R/M is a field.

In particular, all maximal ideals are prime.

Definition 1.122. Let R be an integral domain and $a \in R \setminus \{0\}$ be a non-unit element. We say a is *irreducible* if every factorization of a contains at least one unit.

Definition 1.123. Let R be an integral domain and $a \in R \setminus \{0\}$ be a non-unit element. We say a is *prime* if and only if (a) is a prime ideal or, equivalently, if $b, c \in R$ are such that $a \mid b \cdot c$, then $a \mid b$ or $a \mid c$.

Proposition 1.124. Let R be an integral domain and $a \in R \setminus \{0\}$ be a non-unit element.

1. If a is prime, then a is irreducible.
2. If R is a PID, the following statements are equivalent:
   i) a is irreducible.
   ii) (a) is maximal.
   iii) a is prime.

Theorem 1.125. Let R be a ring. All ideals $I \neq R$ are contained in a maximal ideal.

Polynomial ring

Definition 1.126. Let R be a ring and $p(x) \in R[x]$. If $p(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_n \neq 0$, we define the *degree of* $p(x)$ as:

$$\deg p(x) = \begin{cases} n & \text{if} \quad p(x) \neq 0 \\ -\infty & \text{if} \quad p(x) = 0 \end{cases}$$

Proposition 1.127. Let R be a ring and $p(x), q(x) \in R[x]$ be polynomials with leading coefficients p_n and q_n respectively. Then:

1. $\deg(p(x) + q(x)) \leq \max\{\deg p(x), \deg q(x)\}$ and the equality holds when $\deg p(x) \neq \deg q(x)$.
2. $\deg(p(x) \cdot q(x)) \leq \deg p(x) + \deg q(x)$ and the equality holds when either p_n or q_n is not a zero divisor.

Proposition 1.128. Let R be a ring and $b(x), a(x) \in R[x]$ such that the leading coefficient of $b(x)$ is a unit. Then, $\exists! q(x), r(x) \in R[x]$ such that $a(x) = b(x)q(x) + r(x)$ with $\deg r(x) < \deg b(x)$.

Proposition 1.129 (Universal property of polynomials). Let R, S be two rings, $\phi : R \to S$ be a ring morphism and $s \in S$. Then $\exists! \psi : R[x] \to S$ such that ψ is a ring morphism, $\psi(r) = \phi(r)\ \forall r \in R$ and $\psi(x) = s$. That is, the diagram of figure 1.2.3 is commutative and $\psi(x) = s$.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, hook, "i"'] & S \\ R[x] \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 1.2.3

Proposition 1.130 (Universal property of polynomials in several variables). Let R, S be two rings, $\phi : R \to S$ be a ring morphism and $s_1, \ldots, s_n \in S$ be not necessarily distinct elements of S. Then $\exists! \psi : R[x_1, \ldots, x_n] \to S$ such that ψ is a ring morphism, $\psi(r) = \phi(r)\ \forall r \in R$ and $\psi(x_i) = s_i$ for $i = 1, \ldots, n$.

[11] From now on, for simplicity, we will denote the ring $(R, +, \cdot)$ as R.

Corollary 1.131. Let R be a ring and $r \in R$. Then, the function

$$\begin{aligned} \phi_r : R[x] &\longrightarrow R \\ p(x) &\longmapsto p(r) \end{aligned}$$

is a ring morphism. Moreover $\ker \phi_r = (x-r) \cdot R[x]$ and for all $p(x) \in R[x]$ $\exists q(x) \in R[x]$ such that:

$$p(x) = (x-r) \cdot q(x) + p(r)$$

Corollary 1.132. Let R be a ring and $r_1, \ldots, r_n \in R$. Then, the function

$$\begin{aligned} \phi : R[x_1, \ldots, x_n] &\longrightarrow R \\ p(x_1, \ldots, x_n) &\longmapsto p(r_1, \ldots, r_n) \end{aligned}$$

is a ring morphism. Moreover for all $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ $\exists q_i(x_1, \ldots, x_n) \in R[x]$ for $i = 1, \ldots, n$ such that:

$$p(x_1, \ldots, x_n) = p(r_1, \ldots, r_n) + \sum_{i=1}^{n} (x_i - r_i) \cdot q_i(x_1, \ldots, x_n)$$

Therefore, $\ker \phi = (x_1 - r_1, \ldots, x_n - r_n)$ and consequently:

$$R[x_1, \ldots, x_n] \big/ (x_1 - r_1, \ldots, x_n - r_n) \cong R$$

Corollary 1.133. Let K be a field and $r_1, \ldots, r_n \in K$. Then, the ideal $(x_1 - r_1, \ldots, x_n - r_n)$ is maximal in $K[x_1, \ldots, x_n]$ and

$$K[x_1, \ldots, x_n] \big/ (x_1 - r_1, \ldots, x_n - r_n) \cong K$$

Theorem 1.134 (Fundamental theorem of algebra). Ideals of $\mathbb{C}[x]$ are of the form $(x-z)$, where $z \in \mathbb{C}$. That is, irreducible polynomials in $\mathbb{C}[x]$ have degree 1.

Theorem 1.135 (Hilbert's Nullstellensatz). Maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ are of the form $(x_1 - z_1, \ldots, x_n - z_n)$, where $z_1, \ldots, z_n \in \mathbb{C}$.

Theorem 1.136 (Eisenstein's criterion). Let $a(x) \in \mathbb{Z}[x] \setminus \{0\}$ be such that $a(x) = \sum_{i=0}^{n} a_i x^i$ with $\gcd(a_0, \ldots, a_n) = 1$. If $\exists p \in \mathbb{P}$ such that:

- $p \mid a_i$, $i = 0, 1, \ldots, n-1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

then $a(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Theorem 1.137 (General Eisenstein's criterion). Let R be an integral domain, $a(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$ and p be a prime element in R such that:

- $p \mid a_i$, $i = 0, 1, \ldots, n-1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$.

Then, if $a(x) = b(x) \cdot c(x)$, either $\deg b(x) = 0$ or $\deg c(x) = 0$.

Unique factorization domains

Definition 1.138. Let R be an integral domain. We say that two elements $a, b \in R \setminus \{0\}$ are *associated* if $\exists u \in R^*$ such that $a = b \cdot u$.

Definition 1.139. Let R be an integral domain. We say that R is a *unique factorization domain* (*UFD*) if $\forall a \in R \setminus \{0\}$:

1. $$a = u p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$
   where $u \in R^*$, p_i are irreducible elements of R and $\alpha_i \in \mathbb{N}$ $\forall i$.
2. Such representation is unique in the sense that if $a = v q_1^{\beta_1} \cdots q_s^{\beta_s}$, where $v \in R^*$, q_i are irreducible elements of R and $\beta_i \in \mathbb{N}$ $\forall i$, then $r = s$ and $\exists \sigma \in S_n$ such that p_i and $q_{\sigma(i)}$ are associated and $\alpha_i = \beta_{\sigma(i)}$ for $i = 1, \ldots, r$[12].

Definition 1.140. Let R be an integral domain and $a, b \in R$ be such that at least one of them is nonzero. A *greatest common divisor of a and b* is an element $d \in R$ such that:

1. $d \mid a$ and $d \mid b$.
2. If d' is a common divisor of a and b, then $d' \mid d$.

Proposition 1.141. Let R be a UFD. Then, $\forall a, b \in R \setminus \{0\}$ there exists a greatest common divisor of a and b. Moreover such element is unique.

Proposition 1.142. Let R be an integral domain. Then:

1. If R is a UFD, all irreducible elements are prime.
2. If
   $$u p_1 \cdots p_r = v q_1 \cdots q_s,$$
   where $u, v \in R^*$ and both p_i and q_i are prime elements $\forall i$, then $r = s$ and $\exists \sigma \in S_r$ such that p_i is associated with $q_{\sigma(i)}$ for $i = 1, \ldots, r$.

Proposition 1.143. Let R be an integral domain.

1. If R is a UFD, then R satisfies the *ascending chain condition on principal ideals* (*ACCP*):
   If
   $$a_1 \cdot R \subseteq \cdots \subseteq a_n \cdot R$$
   is an ascending chain of principal ideals, then $\exists n_0 \in \mathbb{N}$ such that $a_{n_0} \cdot R = a_i \cdot R$ for $i \geq n_0$.
2. If R satisfies the ACCP, then all elements in R are product of irreducible factors.

Theorem 1.144. Let R be an integral domain. Then, R is UFD if and only if:

1. All irreducible elements in R are prime.
2. ACCP is satisfied.

[12] Equivalently, such representation is unique in the sense that if $a = u p_1 \cdots p_r = v q_1 \cdots q_s$, where $u, v \in R^*$ and p_i, q_i are irreducible elements of R $\forall i$, then $r = s$ and $\exists \sigma \in S_n$ such that p_i and $q_{\sigma(i)}$ are associated for $i = 1, \ldots, r$.

Lemma 1.145. Let R be an integral domain. Let

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

be a chain of ideals of R. Then,

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

is an ideal of R.

Theorem 1.146. Let R be a PID. Then, R is a UFD.

Corollary 1.147. Let $d \in \mathbb{Z} \setminus \{0\}$ such that d is square-free. Then, $\mathbb{Z}[\sqrt{d}]$ satisfies the ACCP.

Proposition 1.148. Let R be a integral domain. If R satisfies the ACCP, then $R[x]$ also satisfies the ACCP.

Corollary 1.149. Let R be a UFD. Then, $\forall n \geq 0$, all nonzero elements of $R[x_1, \ldots, x_n]$ are product of irreducible elements.

Field of fractions

Definition 1.150. Let R be an integral domain. Consider the set:

$$R \times (R \setminus \{0\}) = \{(a, b) : a, b \in R, b \neq 0\}$$

We define the relation $\sim$ in the following way:

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = a_2 b_1,$$

for all $(a_1, b_1), (a_2, b_2) \in R \times (R \setminus \{0\})$.

Lemma 1.151. The relation $\sim$ is an equivalence relation. We denote by $\mathrm{Frac}(R)$ the set of equivalence classes $R \times (R \setminus \{0\})/\sim$ and by $\frac{a}{b}$ the equivalence class $\overline{(a,b)} \in \mathrm{Frac}(R)$. $\mathrm{Frac}(R)$ is called *field of fractions of R*.

Definition 1.152. Let R be an integral domain. We define the sum and multiplication in $\mathrm{Frac}(R)$ as follows:

1. $\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$, $\forall \frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathrm{Frac}(R)$
2. $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$, $\forall \frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathrm{Frac}(R)$

Theorem 1.153. Let R be an integral domain and consider $(\mathrm{Frac}(R), +, \cdot)$ with the operations $+$ and $\cdot$ defined above. Then:

1. $(\mathrm{Frac}(R), +, \cdot)$ is a field.
2. The function

$$\begin{aligned} i : R &\longrightarrow \mathrm{Frac}(R) \\ r &\longmapsto \frac{r}{1} \end{aligned}$$

is an injective ring morphism and satisfies the following property: If K is a field and $\phi : R \to K$ is an injective ring morphism, then $\exists! \psi : \mathrm{Frac}(R) \to K$ such that ψ is a ring morphism, and the diagram of figure 1.2.4 is commutative.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, hook, "i"'] & K \\ \mathrm{Frac}(R) \arrow[ur, "\psi"'] & \end{tikzcd}$$

Figure 1.2.4

Irreducible and prime elements in $R[X]$

Proposition 1.154. Let R be a UFD and $p \in R$. The following statements are equivalent:

1. p is irreducible in R.
2. p is irreducible in $R[x]$.
3. p is prime in R.
4. p is prime in $R[x]$.

Definition 1.155. Let R be a UFD and $a(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$. We say $p(x)$ is a *primitive polynomial* if 1 is a greatest common divisor of $a_0, \ldots, a_n$.

Lemma 1.156 (Gauß' lemma). Let R be a UFD and $a(x), b(x) \in R[x] \setminus \{0\}$ be primitive polynomials. Then, $a(x) \cdot b(x)$ is primitive.

Lemma 1.157. Let R be a UFD. Then:

1. If $c_1 \cdot a(x) = c_2 \cdot b(x)$, where $c_1, c_2 \in R$, $a(x), b(x) \in R[x]$ and $b(x)$ is primitive, then $c_1 \mid c_2$.
2. If moreover $a(x)$ is also primitive, then $\exists u \in R^*$ such that $c_1 = u \cdot c_2$.

Proposition 1.158. Let R be a UFD and $p(x) \in R[x]$ be a primitive polynomial. The following statements are equivalent:

1. $p(x)$ is irreducible in $R[x]$.
2. $p(x)$ is irreducible in $\mathrm{Frac}(R[x])$.
3. $p(x)$ is prime in $R[x]$.
4. $p(x)$ is prime in $\mathrm{Frac}(R[x])$.

Theorem 1.159. Let R be a UFD. Then, $R[x]$ is a UFD.

Corollary 1.160. $\mathbb{Z}[x_1, \ldots, x_n]$ and $K[x_1, \ldots, x_n]$, where K is a field, are both UFD.

Examples of rings

Let $n \in \mathbb{N}$ and $d \in \mathbb{Z}$ such that d is square-free.

- $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $R[x]$, where R is a ring[13].
- $\mathcal{M}_n(K)$, where K is a field. Note that this is a non-commutative ring.

[13]Note that if $R = R[y]$, then $R[x] = (R[y])[x] = R[x, y]$. So the set of polynomials with several variables over a ring R is also a ring with the same operations as R.

- $\mathbb{Z}[\sqrt{d}]$, where $Z[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. In particular, the set $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[\mathrm{i}]$ is called the set of *Gaußian integers*.
- $\mathbb{Q}(\sqrt{d})$, where $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$.

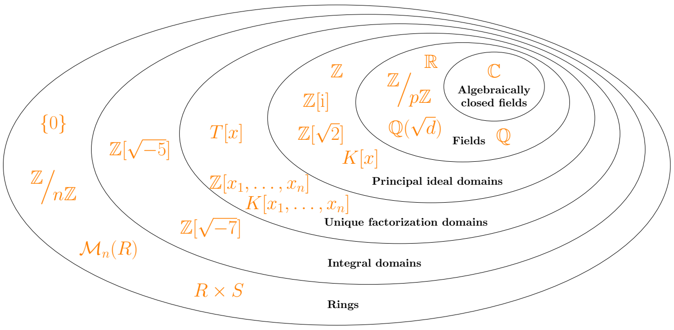


Figure 1.2.5: Inclusions of algebraic structures. Here R and S are nonzero rings, T is a UFD, K is a field, $d \in \mathbb{Z}$ such that d is square-free, $n \in \mathbb{N}$ and $p \in \mathbb{P}$.

1.2.2 Discrete mathematics

1.2.2.1 | Generating functions and recurrence relations

Generating functions

Definition 2.1. Let (a_n) be a sequence of real numbers. We define its *ordinary generating function* as the following formal power series:

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots = \sum_{n=0}^{\infty} a_nx^n.$$

Proposition 2.2. Let $\sum_{n=0}^{\infty} a_nx^n, \sum_{n=0}^{\infty} b_nx^n$ be two formal power series. Then:

- $\sum_{n=0}^{\infty} a_nx^n + \sum_{n=0}^{\infty} b_nx^n = \sum_{n=0}^{\infty}(a_n + b_n)x^n.$
- $\lambda \sum_{n=0}^{\infty} a_nx^n = \sum_{n=0}^{\infty} \lambda a_nx^n.$
- $\left(\sum_{n=0}^{\infty} a_nx^n\right)\left(\sum_{n=0}^{\infty} b_nx^n\right) = \sum_{n=0}^{\infty}(a_0b_n + a_1b_{n-1} + \cdots + a_nb_0)x^n.$
- $\left(\sum_{n=0}^{\infty} a_nx^n\right)' = \sum_{n=1}^{\infty} na_nx^{n-1}.$

Proposition 2.3 (Closed forms). We can write the following ordinary generating functions with their corresponding closed forms:

- $\sum_{n=0}^{N} x^n = \frac{1 - x^{N+1}}{1 - x}.$
- $\sum_{n=0}^{\infty} x^n = \frac{1}{1 - x}.$
- $\sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n = \left(\frac{1}{1 - x}\right)^k.$

Proposition 2.4. Suppose A and B are two finite disjoint sets. We set some restrictions for the non-ordered selection of elements of $A \cup B$. For every $n \geq 0$, let:

- a_n be the number of non-ordered selection of n elements of A satisfying the restrictions,
- b_n be the number of non-ordered selection of n elements of B satisfying the restrictions,
- c_n be the number of non-ordered selection of n elements of $A \cup B$ satisfying the restrictions.

And let $f(x)$, $g(x)$, $h(x)$ be the ordinary generating functions of (a_n), (b_n), (c_n), respectively. Then we have:

$$h(x) = f(x)g(x).$$

Definition 2.5. Let (a_n) be a sequence of real numbers. We define its *exponential generating function* as the following formal power series:

$$a_0 + a_1x + a_2\frac{x^2}{2!} + a_3\frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} a_n\frac{x^n}{n!}.$$

Definition 2.6. Let (a_n) be a sequence of real numbers such that $a_i = 1\ \forall i$. Then its exponential generating function associated is the so called *exponential series*:

$$\mathrm{e}^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Proposition 2.7. The exponential series has the following properties:

1. $\mathrm{e}^{x+y} = \mathrm{e}^x\mathrm{e}^y\ \forall x, y \in \mathbb{R}.$
2. $(\mathrm{e}^x)^n = \mathrm{e}^{nx}\ \forall x, n \in \mathbb{R}.$

Proposition 2.8. Suppose A and B are two finite disjoint sets. We set some restrictions for the ordered selection of elements of $A \cup B$. For every $n \geq 0$, let:

- a_n be the number of ordered selection of n elements of A satisfying the restrictions,
- b_n be the number of ordered selection of n elements of B satisfying the restrictions,
- c_n be the number of ordered selection of n elements of $A \cup B$ satisfying the restrictions.

And let $f(x)$, $g(x)$, $h(x)$ be the exponential generating functions of (a_n), (b_n), (c_n), respectively. Then we have:

$$h(x) = f(x)g(x).$$

Recurrence relations

Definition 2.9. Let (a_n) be a sequence of real numbers. A *recurrence relation of order k for (a_n)* is an expression that express a_n in terms of k consecutive terms of the sequence, $a_{n-1}, \ldots, a_{n-k}$, for $k \leq n$. We say a sequence is *recurrent* if it satisfies a recurrence relation or, equivalently, if it's a solution of the recurrence relation.

Definition 2.10. The *initial values* of a recurrence relation of order k are the values of the first k terms for which the recurrence relation is still not valid, that is, the values $a_0, a_1, \ldots, a_{k-1}$.

Lemma 2.11. The solution of a recurrence relation of order k with k initial conditions is unique.

Definition 2.12. A *linear recurrence relation of order k* is a recurrence relation that can be written as the form

$$a_n + c_1a_{n-1} + \cdots c_ka_{n-k} = g(n)$$

where $c_1, \ldots c_k \in \mathbb{R}, c_k \neq 0$ and $g : \mathbb{N} \to \mathbb{N}$ is an arbitrary function.

Definition 2.13. We say a linear recurrence relation is *homogeneous* if $g(n) = 0$, that is, if it's of the form:

$$a_n + c_1 a_{n-1} + \cdots c_k a_{n-k} = 0, \quad \text{with } c_k \neq 0.$$

Proposition 2.14. The general solution to a recurrence relation

$$a_n + c_1 a_{n-1} + \cdots c_k a_{n-k} = g(n)$$

can be expressed as

$$(a_n^{\text{part}}) + (a_n^{\text{hom}}),$$

where (a_n^{part}) is a particular solution of the recurrence relation and (a_n^{hom}) is the general solution of its associated homogeneous recurrence relation.

Proposition 2.15. Given $c_1, \ldots, c_k \in \mathbb{R}$, the set of sequences that are solution of the homogeneous linear recurrence relation $a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = 0$ form a real vector space.

Definition 2.16. Let $a_n + c_1 a_{n-1} + \cdots + c_k a_{n-k} = 0$ be a homogeneous linear recurrence relation of order k. The *characteristic polynomial* of the recurrence is:

$$x^k + c_1 x^{k-1} + \cdots + c_k = 0.$$

Proposition 2.17. Consider an homogeneous linear recurrence relation with characteristic polynomial

$$(x - r_1)(x - r_2) \cdots (x - r_k) = 0$$

where $r_1, \ldots, r_k \in \mathbb{C}$ are different complex numbers. Then the general term of the sequences that satisfy the recurrence relation is

$$a_n = \lambda_1 r_1^n + \cdots + \lambda_k r_k^n$$

for arbitrary numbers $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$.

1.2.2.2 | Graph theory

Definition 2.18. A *graph* G is an structure based on a set $V(G)$ of vertices and a set $E(G)$ of edges, which are non-ordered pairs of vertices.

Definition 2.19. Let G be a graph. The *order of* G is $n = |V(G)|$ and the *size of* G is $m = |E(G)|$.

Definition 2.20. Let G be a graph. Two vertices $a, b \in V(G)$ are said to be *adjacent* to one another if exists an edge $e \in E(G)$ that connects them. In this case we say the edge e is *incident* on vertices a and b.

Definition 2.21. An edge that connects a vertex with itself is called a *loop*.

Definition 2.22. Two or more edges incidents with the same vertices are called *multiple edges*.

Definition 2.23. A graph G is *finite* if $V(G)$ and $E(G)$ are finite.

Definition 2.24. A graph is *simple* if it has neither multiples edges nor loops.

Definition 2.25. A *complete graph* is a graph in which each pair of different vertices is joined by an edge. We denote by K_n the complete graph of order n.

Definition 2.26. Let G be a finite graph. The *degree of a vertex* is the number of edges that are incident to it. If $v \in V(G)$ we denote the degree of v by $\deg v$ or $\deg_G v$[14].

Lemma 2.27 (Handshaking lemma). For every graph G we have:

$$\sum_{v \in V(G)} \deg v = 2|E(G)|.$$

Corollary 2.28. In any graph, the number of odd-degree vertices is even.

Definition 2.29. Let G be a graph with $V(G) = \{v_1, \ldots, v_n\}$. The *degree sequence of* G is the decreasing sequence

$$(\deg v_{i_1}, \ldots, \deg v_{i_n}).$$

Definition 2.30. We say a graph G is k*-regular* if $\deg v = k\ \forall v \in V(G)$.

Definition 2.31. Let G be a graph. A graph F is an *induced subgraph of* G if $V(F) \subseteq V(G)$ and $E(F) \subseteq E(G)$.

Definition 2.32. A *walk of length* k in a graph G is a sequence of vertices $(u_1, \ldots, u_k)$ where $u_i u_{i+1} \in E(G)$ for $i = 1, \ldots, k-1$.

Definition 2.33. A walk in a graph is *closed* if it starts and ends in the same vertex.

Definition 2.34. A walk in a graph is a *trail* if all the edges of the walk are distinct.

Definition 2.35. A walk in a graph is a *path* if all the vertices (and therefore the edges) of the walk are distinct.

Definition 2.36. A closed walk in a graph is a *closed trail* if all the edges of the closed walk are distinct.

Definition 2.37. A closed path is called a *cycle*.

Proposition 2.38. Let G be a graph. Given $u, v \in V(G)$, there exists a walk between u and v if and only if there exists a path between u and v.

Definition 2.39. Let G be a graph. Given $u, v \in V(G)$, we say that u and v are connected if there is a path in G between u and v.

Proposition 2.40. The relation $u \sim v$ if and only if u and v are connected is an equivalence relation. The equivalent classes are the *connected components of* G.

Definition 2.41. A graph G is *connected* if $\forall u, v \in V(G)$, u and v are connected.

Definition 2.42. A graph G is *bipartite* if $V(G) = X \sqcup Y$ and $\forall e \in E(G)$ we have $e = xy$ with $x \in X$ and $y \in Y$.

Definition 2.43. Let G be a graph such that $E(G) \neq \varnothing$. Take an edge $e \in E(G)$. We denote by $G - e$ the induced graph of G such that

$$V(G - e) = V(G) \qquad E(G - e) = E(G) \setminus \{e\}.$$

[14] Observe that with this definition every loop counts as two edges.

Definition 2.44. Given a connected graph G, we say that $e \in E(G)$ is a *bridge of* G if $G - e$ is non-connected.

Proposition 2.45. Let G be a connected graph. $e \in E(G)$ is a bridge if and only if e doesn't belong to any cycle of G.

Definition 2.46. Let G be a connected graph. An *Eulerian trail* in G is a trail that contain all the edges of G. An *Eulerian circuit* in G is a closed Eulerian trail. G is called *Eulerian* if it admits an eulerian circuit.

Theorem 2.47 (Euler theorem). Let G be a connected graph. G is Eulerian $\iff \deg v = 2k \ \forall v \in V(G)$, $k \in \mathbb{N}$.

Definition 2.48. Let G be a graph of order n with $V(G) = \{v_1, \ldots, v_n\}$. We define the *adjacency matrix of* G, $\mathbf{A}(G) \in \mathcal{M}_n(\mathbb{R})$, as a_{ij} to be the number of edges incident with v_i and v_j.

Proposition 2.49. Let G be a graph of order n with $V(G) = \{v_1, \ldots, v_n\}$ and let $\mathbf{A}(G) = (a_{ij})$ be the adjacency matrix of G. Then:

1. $\mathbf{A}(G)$ is symmetric.
2. $\displaystyle\sum_{j=1}^{n} a_{jk} = \sum_{j=1}^{n} a_{kj} = \deg v_k, \quad k = 1, \ldots, n.$
3. For $k \in \mathbb{N}$, consider $\mathbf{A}(G)^k = (b_{ij}^k)$. Then b_{ij}^k is equal to the number of walks of length k between vertices v_i and v_j.

Definition 2.50. A *tree* is an acyclic connected graph, that is, a connected graph that has no cycles.

Definition 2.51. Let T be a tree. A *leave* of T is a vertex of degree 1.

Definition 2.52. Let G be a graph. A *generator tree* is a induced subgraph T of G such that $|V(G)| = |V(T)|$ and T is a tree.

Proposition 2.53. Let G be a graph such that $|V(G)| = n \geq 2$. The following are equivalent:

1. G is a tree.
2. G is connected and every edge of G is a bridge.
3. G is connected and $|E(G)| = n - 1$.
4. G is acyclic and $|E(G)| = n - 1$.
5. For $v_i, v_j \in V(G)$, $i \neq j$, there exists a unique path between v_i, v_j.
6. G is acyclic but adding a new edge creates exactly one cycle.

Definition 2.54. Let G be a connected graph. G is called *traversable* if admits an Eulerian trail.

Theorem 2.55. Let G be a connected graph. G is traversable if and only if G has exactly to odd-degree vertices.

Definition 2.56. Two graphs G, H are said to be *isomorphic* if exists a bijective map $f : V(G) \to V(H)$ such that $vv' \in E(G) \iff f(v)f(v') \in E(H)$.

Proposition 2.57. Two finite isomorphic graphs have the same order, size and degree sequence.

Theorem 2.58. Two graphs G, H are isomorphic if and only if exists a permutation matrix $\mathbf{P}$ such that

$$\mathbf{P}\mathbf{A}(G)\mathbf{P}^{\mathrm{T}} = \mathbf{A}(H)$$

where $\mathbf{A}(G)$, $\mathbf{A}(H)$ are adjacency matrices of G, H, respectively.

1.2.2.3 | Linear programming

Definition 2.59. Given vectors $\mathbf{c}, \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{b} \in \mathbb{R}^m$ and a matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$, we define the *linear programming to maximize*[15] as

$$\mathrm{LP} = \begin{cases} \text{max}: & z = \mathbf{c}^{\mathrm{T}}x & \textit{(objective function)} \\ \text{subject to}: & \mathbf{A}x \lesseqqgtr \mathbf{b} & \textit{(restrictions)} \\ & \mathbf{u} \leq x \leq \mathbf{v} & \end{cases}$$

Definition 2.60. Given vectors $\mathbf{c}, \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{b} \in \mathbb{R}^m$ and a matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$, we define the *canonical form of a linear programming to maximize* as

$$\mathrm{LP} = \begin{cases} \text{max}: & z = \mathbf{c}^{\mathrm{T}}x & \textit{(objective function)} \\ \text{subject to}: & \mathbf{A}x \leq \mathbf{b} & \textit{(restrictions)} \\ & \mathbf{u} \leq x \leq \mathbf{v} & \end{cases}$$

Analogously we define the *canonical form of a linear programming to minimize* as

$$\mathrm{LP} = \begin{cases} \text{min}: & z = \mathbf{c}^{\mathrm{T}}x \\ \text{subject to}: & \mathbf{A}x \geq \mathbf{b} \\ & \mathbf{u} \leq x \leq \mathbf{v} \end{cases}$$

Definition 2.61. Given a linear program, the *feasible region* of the program is the set

$$\mathfrak{F} = \{x \in \mathbb{R}^n : \mathbf{A}x \lesseqqgtr \mathbf{b}, \mathbf{u} \leq x \leq \mathbf{v}\}.$$

That is, the set of the points that satisfy the conditions of the problem.

Proposition 2.62. Given an $x \in \mathbb{R}^n$, x is a *feasible solution* of the linear program if and only if $x \in \mathfrak{F}$.

Definition 2.63. A *polyhedron* P is a set of $\mathbb{R}^n$ that can be expressed as an intersection of a finite collection of half-spaces, that is

$$P = \{x \in \mathbb{R}^n : \mathbf{A}x \geq \mathbf{b}, \mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R}), \mathbf{b} \in \mathbb{R}^m\}.$$

A *polytope* is a non-empty and bounded polyhedron. The feasible region of any linear program is a polyhedron.

Definition 2.64. Let $P \subset \mathbb{R}^n$ be a polyhedron. A point $x \in \mathbb{R}^n$ is an extreme point of P if there is neither a pair of points $y, z \in P$, nor a scalar $\lambda \in [0, 1]$ such that $x = \lambda y + (1 - \lambda)z$.

[15] Analogously we can define a *linear programming to minimize* changing the objective function to a minimize function.

Definition 2.65. Let LP be a linear program. We define the *standard form of LP* as

$$\text{LP} = \begin{cases} \text{min}: & z = \mathbf{c}^{\mathrm{T}}x \\ \text{subject to}: & \mathbf{A}x = \mathbf{b} \\ & x \geq 0 \end{cases}$$

Definition 2.66. Let $\text{LP} = \min\limits_{x \in \mathbb{R}^n} \{\mathbf{c}^{\mathrm{T}}x : \mathbf{A}x = \mathbf{b}, x \geq 0\}$. Feasible solution in which free variables or non-basic variable equal zero with respect to basis of basic variables are called *basic feasible solutions*.

Proposition 2.67. If a linear program admits feasible solutions, exists a basic feasible solution. If a linear program admits an optimal solution, exists an optimal basic feasible solution.

Theorem 2.68. Let P be a non-empty polyhedron of a linear program in standard form with maximum rank and let $x \in P$. Then x is an extreme point of P if and only if x is a basic feasible solution.

Definition 2.69 (Simplex method: Phase I). Given a linear program in standard form

$$\text{LP} = \begin{cases} \text{min}: & z = \mathbf{c}^{\mathrm{T}}x \\ \text{subject to}: & \mathbf{A}x = \mathbf{b} \\ & x \geq 0 \end{cases}$$

its associated problem in phase I (LP_1) is

$$\text{LP}_1 = \begin{cases} \text{min}: & w = \displaystyle\sum_{i=1}^{m} y_i \\ \text{subject to}: & \mathbf{A}x + \mathbf{I}_m y = \mathbf{b} \\ & x, y \geq 0 \end{cases}$$

A condition necessary for LP having basic feasible solutions is that the optimal solution of LP_1 must be $w = 0$. In fact, if $w \neq 0$, then the original linear program has no feasible solutions[16].

Proposition 2.70 (Simplex method: Phase II). Suppose in a simplex table with positive pivots and therefore independent-terms vector $\mathbf{d} \geq 0$, there is a coefficient $c_j < 0$.

$$\left(\begin{array}{c|c} * & \mathbf{d}^{\mathrm{T}} \\ \hline \mathbf{c} & z - z_0 \end{array}\right).$$

To find a basic feasible solution with lower cost, we make the following change of variable:

1. The variable in column j becomes a basic variable.
2. The variable in row i such that
$$\frac{d_i}{a_{ij}} = \min\left\{\frac{d_k}{a_{kj}} : a_{kj} > 0\right\}$$
becomes a non-basic variable. If this variable does not exists, that is, $a_{kj} \leq 0\ \forall k$ then the linear program is not bounded.

Definition 2.71 (Dual program). Let $\text{LP} = \min\limits_{x \in \mathbb{R}^n} \{\mathbf{c}^{\mathrm{T}}x : \mathbf{A}x \geq \mathbf{b}, x \geq 0\}$. We define the *dual program of LP* as

$$\text{LP}^* = \begin{cases} \text{max}: & z = \mathbf{b}^{\mathrm{T}}y \\ \text{subject to}: & \mathbf{A}^{\mathrm{T}}y \leq \mathbf{c} \\ & y \geq 0 \end{cases}$$

The linear program LP is called *primal*.

Theorem 2.72 (Weak duality theorem). Let x be a feasible solution of the primal linear program and y a feasible solution of the dual linear program. Then we have:

- $\mathbf{c}^{\mathrm{T}}x \leq \mathbf{d}^{\mathrm{T}}y$ if the primal linear program is in canonical form to maximize.
- $\mathbf{c}^{\mathrm{T}}x \geq \mathbf{d}^{\mathrm{T}}y$ if the primal linear program is in canonical form to minimize.

Corollary 2.73. Let x, y be feasible solutions of the primal and dual linear programs respectively such that $\mathbf{c}^{\mathrm{T}}x = \mathbf{d}^{\mathrm{T}}y$. Then x and y are optimal solutions.

Theorem 2.74 (Strong duality theorem). Any linear program has an optimal solution if and only if its dual linear program does, and in this case, the values coincide.

Theorem 2.75 (Complementary property). Suppose that the optimal table of the primal linear program is of the form

$$\left(\begin{array}{c|c} * & \mathbf{d}^{\mathrm{T}} \\ \hline \mathbf{c} & z - z_0 \end{array}\right),$$

where $\mathbf{c} = (c_1, \ldots, c_{n+m})$ and $\mathbf{d} = (d_1, \ldots, d_m)$ with $c_i \geq 0$, $i = 1, \ldots, n+m$. If $(y_1, \ldots y_m, t_1^*, \ldots, t_n^*)$ is the optimal solution of the dual linear program, expressed in standard form, then

$$c_1 = t_1^*, \ldots, c_n = t_n^*, c_{n+1} = y_1, \ldots, c_{n+m} = y_m.$$

[16]This phase is useful to find, if there is, an initial basic feasible solution.

1.2.3 Functions of several variables

1.2.3.1 | Topology of $\mathbb{R}^n$

Definition 3.1. Let M be a set. A *distance in* M is a function $d : M \times M \to \mathbb{R}$ such that $\forall x, y, x \in M$ the following properties are satisfied:

1. $d(x, y) \geq 0$.
2. $d(x, y) = 0 \iff x = y$.
3. $d(x, y) = d(y, x)$.
4. $d(x, y) \leq d(x, z) + d(z, y)$ *(triangular inequality).*

We define a *metric space* as a pair (M, d) that satisfy the previous properties.

Definition 3.2. Let V be a real vector space. A *norm* on V is a function $\|\cdot\| : V \to \mathbb{R}$ such that $\forall \mathbf{u}, \mathbf{v} \in V$ and $\forall \lambda \in \mathbb{R}$ the following properties are satisfied:

1. $\|\mathbf{u}\| \geq 0$.
2. $\|\mathbf{u}\| = 0 \iff \mathbf{u} = 0$.
3. $\|\lambda \mathbf{u}\| = |\lambda| \|\mathbf{u}\|$.
4. $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ *(triangular inequality).*

We define a *normed vector space* as a pair $(V, \|\cdot\|)$ that satisfy the previous properties.

Proposition 3.3. Let $(V, \|\cdot\|)$ be a normed vector space. Then (V, d) is a metric space with associated distance $d(\mathbf{u}, \mathbf{v}) := \|\mathbf{u} - \mathbf{v}\|$, $\forall \mathbf{u}, \mathbf{v} \in V$.

Definition 3.4. Let V be a real vector space. A *dot product* on V is a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ such that $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and $\forall \alpha, \beta \in \mathbb{R}$ the following properties are satisfied:

1. $\langle \alpha \mathbf{u} + \beta \mathbf{w}, \mathbf{v} \rangle = \alpha \langle \mathbf{u}, \mathbf{v} \rangle + \beta \langle \mathbf{u}, \mathbf{v} \rangle$,
   $\langle \mathbf{u}, \alpha \mathbf{v} + \beta \mathbf{w} \rangle = \alpha \langle \mathbf{u}, \mathbf{v} \rangle + \beta \langle \mathbf{u}, \mathbf{w} \rangle$.
2. $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$.
3. $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$.
4. $\langle \mathbf{u}, \mathbf{u} \rangle = 0 \iff \mathbf{u} = 0$.

We define an *Euclidean space* as a pair $(V, \langle \cdot, \cdot \rangle)$ that satisfy the previous properties[17].

Proposition 3.5. Let $(V, \langle \cdot, \cdot \rangle)$ be an Euclidean space. Then $(V, \|\cdot\|)$ is a normed space with associated norm $\|\mathbf{u}\| := \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$, $\forall \mathbf{u} \in V$. .

Proposition 3.6. Let $\langle \cdot, \cdot \rangle_2 : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ be a map defined by

$$\langle \mathbf{u}, \mathbf{v} \rangle_2 = \sum_{i=1}^{n} u_i v_i$$

$\forall \mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, being $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$. Then, the pair $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_2)$ is an Euclidean space.

Corollary 3.7. Consider the norm $\|\cdot\|_2$ and distance d_2 in $\mathbb{R}^n$ defined as follows:

$$\|\mathbf{u}\|_2 = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle_2} = \sqrt{\sum_{i=1}^{n} u_i^2},$$

$$d_2(\mathbf{u}, \mathbf{v}) = \|\mathbf{u} - \mathbf{v}\| = \sqrt{\sum_{i=1}^{n} (u_i - v_i)^2}.$$

Then, $(\mathbb{R}^n, \|\cdot\|_2)$ is a normed space and $(\mathbb{R}^n, d_2)$ is a metric space.

Proposition 3.8. Let $(V, \langle \cdot, \cdot \rangle)$ be an Euclidean space with the norm defined as $\|\mathbf{u}\| := \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$. Then for all $\mathbf{u}, \mathbf{v} \in V$ the following properties are satisfied:

1. $\langle \mathbf{u}, \mathbf{v} \rangle \leq \|\mathbf{u}\| \|\mathbf{v}\|$ *(Cauchy-Schwarz inequality).*
2. $\|\mathbf{u} - \mathbf{v}\| \geq \|\mathbf{u}\| - \|\mathbf{v}\|$.
3. $\|\mathbf{u} + \mathbf{v}\|^2 + \|\mathbf{u} - \mathbf{v}\|^2 = 2(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2)$ *(Parallelogram law).*
4. $\|\mathbf{u} + \mathbf{v}\|^2 - \|\mathbf{u} - \mathbf{v}\|^2 = 4 \langle \mathbf{u}, \mathbf{v} \rangle$.
5. On $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_2)$, if $\mathbf{u} = (u_1, \ldots, u_n)$, then:

$$|u_i| \leq \|\mathbf{u}\| \leq \sum_{i=1}^{n} |u_i|.$$

Definition 3.9. Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be a linear map. We define the *norm of* L as

$$\|L\| = \sup\{\|L(x)\| : \|x\| = 1\}.$$

Lemma 3.10. Let $\Phi : \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m) \to \mathbb{R}$ be a map defined as $\Phi(L) = \|L\|$. Then, Φ is a norm on the vector space $\mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$.

Proposition 3.11. Let $L \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$. Then:

$$\|L\| = \inf\{C : \|L(x)\| \leq C \|x\|\}.$$

Corollary 3.12. Let $L, M \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$ be linear maps with associated matrices $L = (a_{ij})$, $M = (b_{ij})$ respectively. The following properties are satisfied:

1. $\|L(x)\| \leq \|L\| \|x\|$.
2. $\|L\| \leq \left(\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}^2 \right)^{1/2}$.
3. $|a_{ij} - b_{ij}| < \varepsilon, \forall i, j \iff \|L - M\| < \varepsilon'$.

Definition 3.13. Let (M, d) be a metric space. The *sphere with center* p *and radius* $r \in \mathbb{R}^+$ is the set $S(p, r) = \{x \in M : d(x, p) = r\}$.

Definition 3.14. Let (M, d) be a metric space. The *open ball with center* p *and radius* $r \in \mathbb{R}^+$ is the set $B(p, r) = \{x \in M : d(x, p) < r\}$.

[17] Sometimes the notation $\mathbf{u} \cdot \mathbf{v}$ is used, instead of $\langle \mathbf{u}, \mathbf{v} \rangle$, to denote the dot product between $\mathbf{u}$ and $\mathbf{v}$.

Definition 3.15. Let (M, d) be a metric space. The *closed ball with center* p *and radius* $r \in \mathbb{R}^+$ is the set $\overline{B}(p, r) = \{x \in M : d(x, p) \leq r\}$.

Definition 3.16. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. A is a *bounded set* if exists a ball containing it.

Definition 3.17. Let (M, d) be a metric space. A *neighborhood of* p is a bounded set $E(p) \subset M$ such that $\exists r \in \mathbb{R}^+$ satisfying $B(p, r) \subset E(p)$.

Definition 3.18. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. p is an *interior point of* A if $\exists r \in \mathbb{R}^+$ such that $B(p, r) \subset A$. The *interior of* A is the set $\mathring{A}$ containing all interior points of A.

Definition 3.19. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. p is an *exterior point of* A if $\exists r \in \mathbb{R}^+$ such that $B(p, r) \cap A = \varnothing$. The *exterior of* A is the set $\mathring{A}$ containing all exterior points of A.

Definition 3.20. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. p is an *adherent point* of A if $\forall r \in \mathbb{R}^+$, $B(p, r) \cap A \neq \varnothing$. The *adherence* of A is the set $\overline{A}$ containing all adherent points of A.

Definition 3.21. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. p is a *limit point* of A if $\forall r \in \mathbb{R}^+$, $B(p, r) \setminus \{p\} \cap A \neq \varnothing$. The *limit set* of A is the set A' containing all limit points of A.

Definition 3.22. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. p is an *isolated point* of A if it is an adherent but not limit point, that is, if $p \in A$ and $\exists r \in \mathbb{R}^+$ such that $B(p, r) \setminus \{p\} \cap A = \varnothing$.

Definition 3.23. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. p is a *boundary point* of A if $\forall r \in \mathbb{R}^+$, $B(p, r) \cap A \neq \varnothing$ and $B(p, r) \cap A^c \neq \varnothing$. The *boundary* of A is the set ∂A containing all boundary points of A.

Proposition 3.24. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. If p is a limit point of A, then $B(p, r)$ has infinity many point of A, $\forall r \in \mathbb{R}^+$.

Theorem 3.25 (Bolzano-Weierstraß theorem). Let $B \subset \mathbb{R}^n$ be a set. If B has infinity many points and it is bounded, then it has at least a limit point.

Definition 3.26. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. A is *open* if $\forall p \in A$, $\exists r \in \mathbb{R}^+$ such that $B(p, r) \subset A$.

Definition 3.27. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. A is *closed* if its complementary A^c is open.

Proposition 3.28. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. A is closed $\iff A = \overline{A} \iff \partial A \subset A \iff A' \subset A$.

Proposition 3.29. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M. A is open $\iff A = \mathring{A}$.

Proposition 3.30. Let (M, d) be a metric space and $A \subseteq M$ be a subset of M.

- $\mathring{A}$ is the biggest open set contained in A, that is, if $B \subset A$ is open, $B \subset \operatorname{Int} A$.
- $\overline{A}$ is the smallest set contained in A, that is, if $B \supset A$ is closed, $\overline{A} \supset B$.

Proposition 3.31.

- Union of open sets is open.
- Intersection of a finite number of open sets is open.
- Union of a finite number of closed sets is closed.
- Intersection of closed sets is closed.

Definition 3.32. We say a set A is *connected* if there are no open sets $U, V \neq \varnothing$ such that:

$$A \subseteq U \cup V, \quad A \cap U \cap V = \varnothing, \quad A \cap U \neq \varnothing, \quad A \cap V \neq \varnothing.$$

Definition 3.33. Let (M, d) be a metric space. A *sequence* (x_n) in M is a map

$$\begin{aligned} \mathbb{N} &\longrightarrow M \\ n &\longmapsto x_n \end{aligned}$$

Definition 3.34. Let (M, d) be a metric space. We say $(x_n) \subset M$ is *convergent* to $p \in M$ if

$$\forall \varepsilon \in \mathbb{R}^+, \ \exists n_0 \in \mathbb{N} : d(x_n, p) < \varepsilon \text{ if } n > n_0.$$

Definition 3.35. Let (M, d) be a metric space. We say a sequence (x_n) is a *Cauchy sequence* if $\forall \varepsilon > 0$ $\exists n_0$ such that $d(x_n, x_m) < \varepsilon$, for all $m, n \geq n_0$.

Definition 3.36. A metric space (M, d) is *complete* if every Cauchy sequence in M converges in M.

Definition 3.37. A subset $K \subset \mathbb{R}^n$ is *compact* if it is closed and bounded.

Theorem 3.38. Let $K \subset \mathbb{R}^n$ be an arbitrary set and $(x_m) \in K$ be a sequence. Then K is compact if and only if there exists a partial sequence (x_{m_k}) and $x \in K$ such that $\lim_{k \to \infty} x_{m_k} = x$.

1.2.3.2 | Continuity

Definition 3.39 (Graph of a function). Let $f : U \subseteq \mathbb{R}^n \to \mathbb{R}$. We define the *graph of* f as the following subset of $\mathbb{R}^{n+1}$:

$$\operatorname{graph}(f) = \{(x, f(x)) \in \mathbb{R}^{n+1} : x \in U\}.$$

Definition 3.40. Given a function $f : U \subseteq \mathbb{R}^n \to \mathbb{R}$, we define the *level set* $C_k(f)$ as $C_k(f) = \{x \in \mathbb{R}^n : f(x) = k\}$.

Definition 3.41. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ and $p \in U'$. We say $\lim_{x \to p} \mathbf{f}(x) = L$ if $\forall \varepsilon > 0$, $\exists \delta > 0$ such that $\|\mathbf{f}(x) - L\| < \varepsilon$ if $\|x - p\| < \delta$.

Proposition 3.42. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$, $\mathbf{f} = (f_1, \ldots, f_m)$, and $p \in U'$.

1. The limit of $\mathbf{f}$ at point p, if exists, is unique.
2. $\lim_{x \to p} \mathbf{f}(x) = L \iff \lim_{x \to p} f_j(x) = L_j \quad \forall j = 1, \ldots, m.$

Lemma 3.43. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ and $\ell \in U'$. $\exists \lim_{x\to\ell} \mathbf{f}(x) = L \iff \forall (x_n) \in \mathbb{R}^n : \lim_{n\to\infty} x_n = \ell$ and $x_n \neq \ell$ for all n we have $\lim_{n\to\infty} \mathbf{f}(x_n) = L$.

Definition 3.44. We say that $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ is *continuous* at $p \in U'$ if exists $\lim_{x\to p} \mathbf{f}(x) = \mathbf{f}(p)$. We say that $\mathbf{f}$ is continuous on U, if it is at each point $p \in U$.

Definition 3.45. We say that $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ is *uniformly continuous* on U if $\forall \varepsilon > 0$, $\exists \delta > 0 : \|\mathbf{f}(x) - \mathbf{f}(y)\| < \varepsilon$, $\forall x, y \in U : \|x - y\| < \delta$.

Corollary 3.46. A uniformly continuous function is continuous.

Theorem 3.47 (Heine's theorem). Let $\mathbf{f} : K \subset \mathbb{R}^n \to \mathbb{R}^m$ be continuous function and K a compact set. Then $\mathbf{f}$ is uniformly continuous on K.

Theorem 3.48. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ be an uniformly continuous function and $(x_n) \in U$ be a Cauchy sequence. Then $(\mathbf{f}(x_n)) \in \mathbb{R}^m$ is a Cauchy sequence.

Theorem 3.49. Let $\mathbf{f} : K \subset \mathbb{R}^n \to \mathbb{R}^m$ be a continuous function and K be a compact set. Then $\mathbf{f}(K)$ is a compact set.

Theorem 3.50 (Weierstraß' theorem). Let $f : K \subset \mathbb{R}^n \to \mathbb{R}$ be a continuous function and K a compact set. Then f attains a maximum and a minimum on K.

Theorem 3.51 (Intermediate value theorem). Let $f : U \subseteq \mathbb{R}^n \to \mathbb{R}$ be a continuous function and U be a connected set. Then $\forall x, y \in U$ and $\forall c \in [f(x), f(y)]$, $\exists z \in U : f(z) = c$.

Definition 3.52. A function $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ is called *Lipschitz continuous* if $\exists k > 0$ such that

$$\|\mathbf{f}(x) - \mathbf{f}(y)\| \leq k\|x - y\|$$

$\forall x, y \in U$. If $0 \leq k < 1$ we say that $\mathbf{f}$ is a *contraction*.

Proposition 3.53. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ be a locally Lipschitz continuous function at $p \in U$. Then $\mathbf{f}$ is continuous at p.

Definition 3.54. Let (M, d) be a metric space and $f : M \to \mathbb{R}$ a function. We define the *modulus of continuity of* f as the function $\omega_f : (0, \infty) \to [0, \infty]$ defined as

$$\omega_f(\delta) := \sup\{|f(x) - f(y)| : d(x, y) < \delta, x, y \in M\}.$$

1.2.3.3 | Differential calculus

Differential of a function

Definition 3.55. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ and $a \in U$. The function $\mathbf{f}$ is *differentiable at* a if there exists a linear map $D\mathbf{f}(a) : \mathbb{R}^n \to \mathbb{R}^m$ such that

$$\lim_{x\to a} \frac{\|\mathbf{f}(x) - \mathbf{f}(a) - D\mathbf{f}(a)(x - a)\|}{\|x - a\|} = \lim_{h\to 0} \frac{\|\mathbf{f}(a + h) - \mathbf{f}(a) - D\mathbf{f}(a)h\|}{\|h\|} = 0.$$

$D\mathbf{f}(a)$ is called the *differential of* $\mathbf{f}$ *at point* a. Furthermore, we say $\mathbf{f}$ is differentiable on $B \subseteq U$ if it is differentiable at each point of B.

Proposition 3.56. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ and $a \in U$. $\mathbf{f} = (f_1, \ldots, f_m)$ is differentiable at a if and only if every component function $f_j : U \subseteq \mathbb{R}^n \to \mathbb{R}$ is differentiable at a.

Definition 3.57. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}$, $a \in U$ and $\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v}\| = 1$. The *directional derivative of* $\mathbf{f}$ *at* a in the direction of $\mathbf{v}$ is

$$D_{\mathbf{v}}\mathbf{f}(a) = \lim_{t\to 0} \frac{\mathbf{f}(a + t\mathbf{v}) - \mathbf{f}(a)}{t}.$$

Definition 3.58. Let $U \subseteq \mathbb{R}^n$ be an open set, $\mathbf{f} : U \to \mathbb{R}$ and $a \in U$. If the following limit exists, we define the *partial derivative with respect to* x_j *of* $\mathbf{f}$ *at* a as

$$\frac{\partial \mathbf{f}}{\partial x_j}(a) = \lim_{h\to 0} \frac{\mathbf{f}(a + h\mathbf{e}_j) - \mathbf{f}(a)}{h}\text{[18]}.$$

Definition 3.59. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ and $a \in U$. If all partial derivatives of $\mathbf{f}$ at a exist, we call *Jacobian matrix of* $\mathbf{f}$ *at* a the matrix associated with $D\mathbf{f}(a)$ (with respect to the canonical basis of $\mathbb{R}^n$ and $\mathbb{R}^m$):

$$D\mathbf{f}(a) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & \cdots & \frac{\partial f_1}{\partial x_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(a) & \cdots & \frac{\partial f_m}{\partial x_n}(a) \end{pmatrix}.$$

If $n = m$, we define the *Jacobian determinant* as $J\mathbf{f}(a) = \det D\mathbf{f}(a)$.

Definition 3.60. Let $U \subseteq \mathbb{R}^n$ be an open set, $f : U \to \mathbb{R}$ and $a \in U$ such that f is differentiable at $a \in U$. The *gradient of* f *at* a is

$$\boldsymbol{\nabla} f(a) := Df(a) = \left(\frac{\partial f}{\partial x_1}(a), \ldots, \frac{\partial f}{\partial x_n}(a)\right).$$

Proposition 3.61. Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$ be a differentiable function at $a \in U$. Then there exists the tangent hyperplane to the graph of f at a and has the equation

$$x_{n+1} = f(a) + \boldsymbol{\nabla} f(a) \cdot (x - a)\text{[19]}.$$

Theorem 3.62. Let $U \subseteq \mathbb{R}^n$ be an open set, $f : U \to \mathbb{R}$, $a \in U$ and $\mathbf{v} \in \mathbb{R}^n$ such that $\|\mathbf{v}\| = 1$. If f is differentiable at a, then $D_{\mathbf{v}} f(a)$ exists and

$$D_{\mathbf{v}} f(a) = \boldsymbol{\nabla} f(a) \cdot \mathbf{v}.$$

[18] Here $\mathbf{e}_j$ is the j-th vector of the canonical basis of $\mathbb{R}^n$, that is, $\mathbf{e}_j = (0, \ldots, 0, \overset{(j)}{1}, 0, \ldots, 0)$.

[19] In general (not only the case of the graph of a function) the tangent hyperplane to function f at a point a is given by the equation

$$\boldsymbol{\nabla} f(a) \cdot (x - a) = 0.$$

Proposition 3.63. Let $U \subseteq \mathbb{R}^n$ be an open set, $f : U \to \mathbb{R}$ be a differentiable function on U and C_k be the level set of value $k \in \mathbb{R}$. Then $\boldsymbol{\nabla} f(a) \perp C_k$ at $a \in C_k$.

Proposition 3.64. Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$ a differentiable function at $a \in U$ and $\mathbf{v} \in \mathbb{R}^n$. Then:

- $\max\{D_{\mathbf{v}} f(a) : \|\mathbf{v}\| = 1\} = \|\boldsymbol{\nabla} f(a)\|$ and it is attained when $\mathbf{v} = \dfrac{\boldsymbol{\nabla} f(a)}{\|\boldsymbol{\nabla} f(a)\|}$.
- $\min\{D_{\mathbf{v}} f(a) : \|\mathbf{v}\| = 1\} = -\|\boldsymbol{\nabla} f(a)\|$ and it is attained when $\mathbf{v} = -\dfrac{\boldsymbol{\nabla} f(a)}{\|\boldsymbol{\nabla} f(a)\|}$.

Theorem 3.65. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ be a differentiable function at $a \in U$. Then $\mathbf{f}$ is locally Lipschitz continuous at a.

Theorem 3.66. Let $\mathbf{f}, \boldsymbol{g} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ be two differentiable functions at a point $a \in U$ and let $c \in \mathbb{R}$. Then:

1. $\mathbf{f} + \boldsymbol{g}$ is differentiable at a and
$$D(\mathbf{f} + \boldsymbol{g})(a) = D\mathbf{f}(a) + D\boldsymbol{g}(a).$$
2. $c\mathbf{f}$ is differentiable at a and
$$D(c\mathbf{f})(a) = cD\mathbf{f}(a).$$
3. If $m = 1$, then $(fg)(x) = f(x)g(x)$ is differentiable at a and
$$D(fg)(a) = g(a)Df(a) + f(a)Dg(a).$$
4. If $m = 1$ and $g(a) \neq 0$, then $\left(\dfrac{f}{g}\right)(x) = \dfrac{f(x)}{g(x)}$ is differentiable at a and
$$D\left(\frac{f}{g}\right)(a) = \frac{g(a)Df(a) - f(a)Dg(a)}{[g(a)]^2}.$$

Theorem 3.67 (Chain rule). Let $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^m$ be open sets. Let $\mathbf{f} : U \to \mathbb{R}^m$ and $\boldsymbol{g} : V \to \mathbb{R}^p$. Suppose that $\mathbf{f}(U) \subset V$, $\mathbf{f}$ is differentiable at $a \in U$ and $\boldsymbol{g}$ is differentiable at $\mathbf{f}(a)$. Then $\boldsymbol{g} \circ \mathbf{f}$ is differentiable at a and
$$D(\boldsymbol{g} \circ \mathbf{f})(a) = D\boldsymbol{g}(\mathbf{f}(a)) \circ D\mathbf{f}(a).$$

Definition 3.68. Let $U \subseteq \mathbb{R}^n$ be an open set and $\mathbf{f} : U \to \mathbb{R}^m$. We say that $\mathbf{f}$ is a *function of class $\mathcal{C}^k(U)$*, $k \in \mathbb{N}$, if all partial derivatives of order k exists and are continuous on U. We say that $\mathbf{f}$ is *function of class $\mathcal{C}^\infty(U)$* if it is of class $\mathcal{C}^k(U)$, $\forall k \in \mathbb{N}$.

Theorem 3.69 (Differentiability criterion). Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$, $\mathbf{f}(x) = (f_1(x), \ldots, f_m(x))$. If all partial derivatives $\dfrac{\partial f_i(x)}{\partial x_j}$ exists in a neighborhood of $a \in U$ and are continuous at a, then $\mathbf{f}$ is differentiable at $a \in U$.

Proposition 3.70. Let $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^m$ and $A \subseteq U$. If all partial derivatives of $\mathbf{f}$ exist on A and are bounded functions on A, then $\mathbf{f}$ is uniformly continuous on A.

Theorem 3.71 (Mean value theorem). Let $f : B \to \mathbb{R}$ be a function of class $\mathcal{C}^1$ in an open connected set B. Let $x, y \in B$. Then,
$$f(x) - f(y) = \boldsymbol{\nabla} f(z) \cdot (x - y),$$
for some $z \in [x, y]$.

Theorem 3.72 (Mean value theorem for vector-valued functions). Let $\mathbf{f} : B \to \mathbb{R}^m$ be a function of class $\mathcal{C}^1$ in an open connected set B. Let $x, y \in B$. Then,
$$\|\mathbf{f}(x) - \mathbf{f}(y)\| \leq \|Df(z)\|\|x - y\|,$$
for some $z \in [x, y]$.

Higher order derivatives

Definition 3.73. Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$. We denote the *partial derivative of f of order k with respect to the variables $x_{i_1}, \ldots, x_{i_k}$* as
$$\frac{\partial^k f}{\partial x_{i_k} \cdots \partial x_{i_1}}.$$

Definition 3.74. Let $U \subseteq \mathbb{R}^n$ be an open set. If $f : U \to \mathbb{R}$ has second order partial derivatives at $a \in U$, we define the *hessian matrix of f at a point a* as
$$Hf(a) = \begin{pmatrix} \dfrac{\partial^2 f}{\partial x_1^2}(a) & \cdots & \dfrac{\partial^2 f}{\partial x_n x_1}(a) \\ \vdots & \ddots & \vdots \\ \dfrac{\partial^2 f}{\partial x_1 x_n}(a) & \cdots & \dfrac{\partial^2 f}{\partial x_n^2}(a) \end{pmatrix}.$$

Theorem 3.75 (Schwarz's theorem). Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$. If f has mixed partial derivatives of order k and are continuous functions on $A \subseteq U$, then for any permutation $\sigma \in S_k$ we have
$$\frac{\partial^k f}{\partial x_{i_k} \cdots \partial x_{i_1}}(a) = \frac{\partial^k f}{\partial x_{\sigma(i_k)} \cdots \partial x_{\sigma(i_1)}}(a), \quad \forall a \in A.$$

Inverse and implicit function theorems

Lemma 3.76. Let $U \subseteq \mathbb{R}^n$ be an open set and $\mathbf{f} : U \to \mathbb{R}^m$ with $\mathbf{f} \in \mathcal{C}^1(U)$. Given an $a \in U$ and $\varepsilon > 0$, $\exists B(a, r) \subset U$ such that
$$\|\mathbf{f}(x) - \mathbf{f}(y)\| \leq (\|D\mathbf{f}(a)\| + \varepsilon)\|x - y\|, \quad \forall x, y \in B(a, r).$$

Lemma 3.77. Let $U \subseteq \mathbb{R}^n$ be an open set and $\mathbf{f} : U \to \mathbb{R}^n$ with $\mathbf{f} \in \mathcal{C}^1(U)$. Suppose that for some $a \in U$, $J\mathbf{f}(a) \neq 0$. Then $\exists B(a, r) \subset U$ and $c > 0$ such that
$$\|\mathbf{f}(y) - \mathbf{f}(x)\| \geq c\|y - x\|, \quad \forall x, y \in B(a, r).$$
In particular, $\mathbf{f}$ is injective on $B(a, r)$.

Theorem 3.78 (Inverse function theorem). Let $U \subseteq \mathbb{R}^n$ be an open set, $\mathbf{f} : U \to \mathbb{R}^n$ with $\mathbf{f} \in \mathcal{C}^1(U)$ and $a \in U$ such that $J\mathbf{f}(a) \neq 0$. Then $\exists B = B(a, r) \subset U$ such that:

1. $\mathbf{f}$ is injective on B.
2. $\mathbf{f}(B) = V$ is an open set of $\mathbb{R}^n$.
3. $\mathbf{f}^{-1} : V \to B$ is of class $\mathcal{C}^1$ on V.

Moreover, it is satisfied that $D\mathbf{f}^{-1}(\mathbf{f}(a)) = D\mathbf{f}(a)^{-1}$

Definition 3.79. A function $\mathbf{f} : U \subseteq \mathbb{R}^n \to \mathbb{R}^n$ is a *diffeomorphism of class* $\mathcal{C}^k$ if it is bijective and both $\mathbf{f}$ and $\mathbf{f}^{-1}$ are of class $\mathcal{C}^k$.

Theorem 3.80 (Implicit function theorem). Let $U \subseteq \mathbb{R}^{n+m}$ be an open set, $\mathbf{f} : U \to \mathbb{R}^m$ with $\mathbf{f} \in \mathcal{C}^1(U)$ and $(a, b) = (a_1, \ldots, a_n, b_1, \ldots, b_m) \in U$ such that $\mathbf{f}(a, b) = 0$. If $D\mathbf{f}(x) = (Df_1(x) \mid Df_2(x))$ with $Df_1(x) \in \mathcal{M}_{m\times n}(\mathbb{R})$, $Df_2(x) \in \mathcal{M}_m(\mathbb{R})$ and $\det Df_2(x) \neq 0$ (i.e. rang $D\mathbf{f}(a, b) = m$), then exists an open set $W \subseteq \mathbb{R}^n$ such that $a \in W$ and a function $\boldsymbol{g} : W \to \mathbb{R}^m$ with $\boldsymbol{g} \in \mathcal{C}^1(W)$, such that

$$\boldsymbol{g}(a) = b \quad \text{and} \quad \mathbf{f}(x, \boldsymbol{g}(x)) = 0 \quad \forall x \in W.$$

Moreover, is is satisfied that

$$D\boldsymbol{g}(a) = -Df_2(a, \boldsymbol{g}(a))^{-1} \circ Df_1(a, \boldsymbol{g}(a)).$$

Taylor's polynomial and maxima and minima

Theorem 3.81 (Taylor's theorem). Let $U \subseteq \mathbb{R}^n$ be an open set, $f : U \to \mathbb{R}$, $a \in U$ and $f \in \mathcal{C}^{k+1}(U)$. Then:

$$\begin{aligned} f(x) &= f(a) + \\ &+ \sum_{m=1}^{k} \frac{1}{m!} \left(\sum_{i_m,\ldots,i_1=1}^{n} \frac{\partial^m f}{\partial x_{i_m} \cdots \partial x_{i_1}}(a) \prod_{j=1}^{m} (x_{i_j} - a_{i_j}) \right) + \\ &\qquad + R_k(f, a), \end{aligned}$$

where

$$\begin{aligned} R_k(f, a) &= \\ &= \frac{1}{(k+1)!} \sum_{i_{k+1},\ldots,i_1=1}^{n} \frac{\partial^{k+1} f}{\partial x_{i_{k+1}} \cdots \partial x_{i_1}}(\xi) \prod_{j=1}^{k+1} (x_{i_j} - a_{i_j}) = \\ &= o(\|x - a\|^k) \end{aligned}$$

for some $\xi \in [a, x]$. In particular, for $k = 2$ we have:

$$\begin{aligned} f(x) = f(a) + Df(a)(x - a) + \frac{1}{2} Hf(a)(x - a, x - a) + \\ + R_2(f, a), \end{aligned}$$

where $R_2(f, a) = o(\|x - a\|^2)$.

Definition 3.82. Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$. We say that f has a *local maximum at* $a \in U$ if $\exists B(a, r) \subset U : f(x) \leq f(a)$, $\forall x \in B(a, r)$. Analogously, we say that f has a *local minimum at* $a \in U$ if $\exists B(a, r) \subset U : f(x) \geq f(a)$, $\forall x \in B(a, r)$. A *local extremum* is either a local maximum or a local minimum. Moreover, if $f(x) \leq f(a)$ $\forall x \in U$, we say that f has a *global maximum at* $a \in U$. Similarly if $f(x) \geq f(a)$ $\forall x \in U$, we say that f has a *global minimum at* $a \in U$.

Proposition 3.83. Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$ be a differentiable function at $a \in U$. If f has a local extremum at a, then $\boldsymbol{\nabla} f(a) = 0$.

Definition 3.84. Let $U \subseteq \mathbb{R}^n$ be an open set and $f : U \to \mathbb{R}$. We say that $a \in U$ is a *critical point of* f if $\boldsymbol{\nabla} f(a) = 0$. We say that $a \in U$ is a *saddle point* if a is a critical point but not a local extremum.

Theorem 3.85. Let $\mathcal{Q}$ be a quadratic form. Then for all $x \neq 0$ we have:

$$\mathcal{Q} \text{ is defined positive} \iff \exists \lambda \in \mathbb{R}^+ : \mathcal{Q}(x) \geq \lambda \|x\|^2.$$
$$\mathcal{Q} \text{ is defined negative} \iff \exists \lambda \in \mathbb{R}^- : \mathcal{Q}(x) \leq \lambda \|x\|^2.$$

Proposition 3.86 (Sylvester's criterion). Let $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$ be a symmetric matrix. A is defined positive if and only if all its principal minors are positive, that is:

$$a_{11} > 0, \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0, \ldots, \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} > 0.$$

A is defined negative if and only if its principal minor of order k have sign $(-1)^k$, that is:

$$a_{11} < 0, \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0, \ldots, (-1)^n \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} > 0.$$

Theorem 3.87. Let $U \subseteq \mathbb{R}^2$ be an open set, $f : U \to \mathbb{R}$ a function of class $\mathcal{C}^2(U)$ and $a \in U : \boldsymbol{\nabla} f(a) = 0$. Let $Hf(a)$ be the hessian matrix of f at a and $\mathcal{H}f(a)$ be its associated quadratic form. Then:

1. If $\mathcal{H}f(a)$ is defined positive $\implies$ f has a local minimum at a.
2. If $\mathcal{H}f(a)$ is defined negative $\implies$ f has a local maximum at a.
3. If $\mathcal{H}f(a)$ is undefined $\implies$ f has a saddle point at a.

Theorem 3.88 (Lagrange multipliers theorem). Let $f, g_i : U \subseteq \mathbb{R}^n \to \mathbb{R}$ be functions of class $\mathcal{C}^1(U)$ for $i = 1, \ldots, k$ and $1 \leq k < n$. Let $S = \{x \in U : g_i(x) = 0, \forall i\}$ and $a \in S$ such that $f_{|S}(a)$ is a local extremum. If the vectors $\boldsymbol{\nabla} g_1(a), \ldots, \boldsymbol{\nabla} g_k(a)$ are linearly independents, then $\exists \lambda_1, \ldots, \lambda_k \in \mathbb{R}$ such that:

$$\boldsymbol{\nabla} f(a) = \sum_{i=1}^{k} \lambda_i \boldsymbol{\nabla} g_i(a).$$

1.2.3.4 | Integral calculus

Integration over compact rectangles

Definition 3.89. A *rectangle* R of $\mathbb{R}^n$ is a product $R = I_1 \times \cdots \times I_n$ where $I_j \in \mathbb{R}$ are bounded and non-degenerate[20] intervals.

Definition 3.90. The n*-dimensional volume* (*surface* if $n = 2$ or *length* if $n = 1$) of a bounded rectangle $R = I_1 \times \cdots \times I_n$, $I_i = [a_i, b_i]$ is:

$$\mathrm{vol}(R) = \prod_{i=1}^{n} (b_i - a_i).$$

[20] That is, non-empty intervals with more than one point.

Definition 3.91. Given a rectangle $R = I_1 \times \cdots \times I_n$, a *partition of* R is the product $\mathcal{P} = \mathcal{P}_1 \times \cdots \times \mathcal{P}_n$ where $\mathcal{P}_j$ is a partition of the interval I_j. A partition $\mathcal{P}$ is *regular* if for all j, $\mathcal{P}_j$ is regular, that is, all subintervals in $\mathcal{P}_j$ have the same size. We denote by $\mathbf{P}(R)$ the set of all partitions of R.

Definition 3.92. Given two partitions $\mathcal{P} = I_1 \times \cdots \times I_n$ and $\mathcal{P}' = I_1' \times \cdots \times I_n'$ of a rectangle R, we say that $\mathcal{P}'$ is *finer than* $\mathcal{P}$ if each $\mathcal{P}_j'$ is finer than $\mathcal{P}_j$.

Definition 3.93. Let $R \subset \mathbb{R}^n$ be a compact rectangle, $f : R \to \mathbb{R}$ be a bounded function and $\mathcal{P} \in \mathbf{P}(R)$. For each subrectangle R_j, $j = 1, \ldots, m$, determined by $\mathcal{P}$ let

$$m_j = \inf\{f(x) : x \in R_j\} \quad \text{i} \quad M_j = \sup\{f(x) : x \in R_j\}.$$

We define the *lower sum* and the *upper sum of* f *with respect to* $\mathcal{P}$ as:

$$L(f, \mathcal{P}) = \sum_{j=1}^{m} m_j \mathrm{vol}(R), \qquad U(f, \mathcal{P}) = \sum_{j=1}^{m} M_j \mathrm{vol}(R)^{21}.$$

Definition 3.94. Let $R \subset \mathbb{R}^n$ be a compact rectangle and $f : R \to \mathbb{R}$ be a bounded function. We define the *lower integral* and *upper integral of* f *on* R as

$$\underline{\int_R} f = \sup\{L(f, \mathcal{P}) : \mathcal{P} \in \mathbf{P}\},$$
$$\overline{\int_R} f = \inf\{U(f, \mathcal{P}) : \mathcal{P} \in \mathbf{P}\}.$$

We say that f is *Riemann-integrable on* R if $\underline{\int_R} f = \overline{\int_R} f$.

Proposition 3.95. Let $R \subset \mathbb{R}^n$ be a compact rectangle and $f : R \to \mathbb{R}$ be a bounded function. f is Riemann-integrable if and only if $\forall \varepsilon\ \exists \mathcal{P} \in \mathbf{P}(R)$ such that $U(f, \mathcal{P}) - L(f, \mathcal{P}) < \varepsilon$.

Definition 3.96. Let $R \subset \mathbb{R}^n$ be a compact rectangle; $f : R \to \mathbb{R}$, a bounded function; $\mathcal{P} \in \mathbf{P}(R)$, and ξ_j, an arbitrary point of the subrectangle R_j, $j = 1, \ldots, m$. Then we define the *Riemann sum of* f *associated to* $\mathcal{P}$ as:

$$S(f, \mathcal{P}) = \sum_{j=1}^{m} f(\xi_j) \mathrm{vol}(R_j).$$

Theorem 3.97. Let $R \subset \mathbb{R}^n$ be a compact rectangle and $f : R \to \mathbb{R}$ be a bounded function. f is Riemann-integrable over R if and only if $\forall \varepsilon > 0\ \exists \mathcal{P}_\varepsilon \in \mathbf{P}(R)$ such that

$$\left| S(f, \mathcal{P}) - \int_R f \right| = \left| \sum_{j=1}^{m} f(\xi_j) \mathrm{vol}(R_j) - \int_R f \right| < \varepsilon,$$

for any $\mathcal{P} \in \mathbf{P}(R)$ finer than $\mathcal{P}_\varepsilon$ and for any $\xi_j \in R_j$.

Fubini's theorem

Theorem 3.98 (Fubini's theorem). Let $R_1 \subset \mathbb{R}^n$ and $R_2 \subset \mathbb{R}^m$ be closed rectangles and $f : R_1 \times R_2 \to \mathbb{R}$ be an integrable[22] function. Suppose for every $x_0 \in R_1$, $f(x_0, y)$ is integrable over R_2. Then the function $g(x) = \int_{R_2} f(x, y) \mathrm{d}y$ is integrable over R_1 and

$$\int_{R_1 \times R_2} f(x, y) = \int_{R_1} \mathrm{d}x \int_{R_2} f(x, y) \mathrm{d}y.$$

Similarly if for every $y_0 \in R_2$, $f(x, y_0)$ is integrable over R_1, then the function $h(y) = \int_{R_1} f(x, y) \mathrm{d}x$ is integrable over R_2 and

$$\int_{R_1 \times R_2} f(x, y) = \int_{R_2} \mathrm{d}y \int_{R_1} f(x, y) \mathrm{d}x.$$

Corollary 3.99. Let $R_1 \subset \mathbb{R}^n$ and $R_2 \subset \mathbb{R}^m$ be closed rectangles and let $f : R_1 \times R_2 \to \mathbb{R}$ be a continuous function on $R_1 \times R_2$. Then,

$$\int_{R_1 \times R_2} f = \int_{R_1} \mathrm{d}x \int_{R_2} f(x, y) \mathrm{d}y = \int_{R_2} \mathrm{d}y \int_{R_1} f(x, y) \mathrm{d}x.$$

Corollary 3.100. Let $R = [a_1, b_1] \times \cdots \times [a_n, b_n] \subset \mathbb{R}^n$ be a rectangle. If $f : R \to \mathbb{R}$ is a continuous function, then

$$\int_R f = \int_{a_n}^{b_n} \mathrm{d}x_n \int_{a_{n-1}}^{b_{n-1}} \mathrm{d}x_{n-1} \cdots \int_{a_1}^{b_1} f(x_1, \ldots, x_n) \mathrm{d}x_1.$$

Definition 3.101. Let $D \subset \mathbb{R}^{n-1}$ be a compact set and $\varphi_1, \varphi_2 : D \to \mathbb{R}$ be continuous functions such that $\varphi_1(x) \leq \varphi_2(x)\ \forall x \in D$. The set

$$S = \{(x, y) \subset \mathbb{R}^n : x \in D, \varphi_1(x) \leq y \leq \varphi_2(x)\}$$

is called an *elementary region in* $\mathbb{R}^n$. In particular, if $n = 2$, we say S is x*-simple*. An elementary region in $V \subset \mathbb{R}^3$ is called xy*-simple* if it is of the form

$$V = \{(x, y, z) \in \mathbb{R}^3 : (x, y) \in U, \phi_1(x, y) \leq z \leq \phi_2(x, y)\},$$

where U is an elementary region in $\mathbb{R}^2$ and ϕ_1, ϕ_2 are continuous functions on U[23].

Theorem 3.102 (Fubini's theorem for elementary regions). Let $S = \{(x, y) \subset \mathbb{R}^n : x \in D, \varphi_1(x) \leq y \leq \varphi_2(x)\}$ be an elementary region in $\mathbb{R}^n$ and $f : S \to \mathbb{R}$. If f is integrable over S and for all $x_0 \in D$ the function $f(x_0, y)$ is integrable over $[-M, M]$, $M \in \mathbb{R}$, then

$$\int_S f = \int_D \mathrm{d}x \int_{\varphi_1(x)}^{\varphi_2(x)} f(x, y) \mathrm{d}y.$$

Definition 3.103. Let $D \subset \mathbb{R}^{n-1}$ be a compact set and $S = \{(x, y) \subset \mathbb{R}^n : x \in D, \varphi_1(x) \leq y \leq \varphi_2(x)\}$ an elementary region. We define the n*-dimensional volume of* S as

$$\mathrm{vol}(S) := \int_S \mathrm{d}x = \int_D \mathrm{d}x \int_{\varphi_1(x)}^{\varphi_2(x)} \mathrm{d}y^{24}.$$

[21] We will omit the results related to these definitions because of they are a natural extension of results of single-variable functions course and can be deduced easily. That's why we only expose the most important ones here.

[22] As we only have defined Riemann-integration, it goes without saying that an *integrable function* means a *Riemann-integrable function*.

[23] Analogously we define y*-simple* regions in $\mathbb{R}^2$ and yz*-simple* or xz*-simple* regions in $\mathbb{R}^3$.

[24] In particular, we define the area of a region $S \subset \mathbb{R}^2$ as $\mathrm{area}(S) = \iint_S \mathrm{d}x\mathrm{d}y$ and the volume of a region $\Omega \subset \mathbb{R}^3$ as $\mathrm{vol}(\Omega) = \iiint_\Omega \mathrm{d}x\mathrm{d}y\mathrm{d}z$.

Corollary 3.104 (Cavalieri's principle). Let $\Omega \subset R \times [a,b]$ be a set in $\mathbb{R}^n$ where $R \subset \mathbb{R}^{n-1}$ is a rectangle. For every $t \in [a,b]$ let

$$\Omega_t = \{(x,y) \in \Omega : y = t\} \subset \mathbb{R}^n$$

be the section of Ω corresponding to the hyperplane $y = t$. If $\nu(\Omega_t)$ is the $(n-1)$-dimensional volume (area if $n = 3$ or length if $n = 2$) of Ω_t, then

$$\mathrm{vol}(\Omega) = \int_a^b \nu(\Omega_t)\mathrm{d}t.$$

Definition 3.105 (Center of mass). The *center of mass of an object with mass density* $\rho(x,y,z)$ occupying a region $\Omega \subset \mathbb{R}^3$ is the point $(\overline{x}, \overline{y}, \overline{z}) \in \mathbb{R}^3$ whose coordinates are:

$$\overline{x} = \frac{1}{m}\iiint_\Omega x\rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z,$$
$$\overline{y} = \frac{1}{m}\iiint_\Omega y\rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z,$$
$$\overline{z} = \frac{1}{m}\iiint_\Omega z\rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z,$$

where $m = \displaystyle\iiint_\Omega \rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z$ is the total mass of the object.

Definition 3.106 (Moment of inertia). Given a body with mass density $\rho(x,y,z)$ occupying a region $\Omega \subset \mathbb{R}^3$ and a line $L \subset \mathbb{R}^3$, the *moment of inertia of the body about the line* L is

$$I_L = \iiint_\Omega d(x,y,z)^2\rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z,$$

where $d(x,y,z)$ denotes the distance from (x,y,z) to the line L. In particular, when L is the z-axis, then

$$I_z = \iiint_\Omega (x^2+y^2)\rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z,$$

and similarly for I_x and I_y. The moment of inertia of the body about the xy-plane is defined by

$$I_{xy} = \iiint_\Omega z^2\rho(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z,$$

and similarly for I_{yz} and I_{zx}.

Change of variable

Theorem 3.107 (Change of variable theorem). Let $U \subseteq \mathbb{R}^n$ be an open set and let $\varphi : U \to \mathbb{R}^n$ be a diffeomorphism. If $f : \varphi(U) \to \mathbb{R}$ is integrable on $\varphi(U)$, then

$$\int_{\varphi(U)} f = \int_U (f \circ \varphi)|J\varphi|.$$

Corollary 3.108 (Integral in polar coordinates). Let $\varphi : [0,\infty) \times [0,2\pi) \to \mathbb{R}$ be such that

$$\varphi(r,\theta) \longmapsto (r\cos\theta, r\sin\theta).$$

Then we have $|J\varphi| = r$ and therefore:

$$\int_{\varphi(U)} f(x,y)\mathrm{d}x\mathrm{d}y = \int_U f(r\cos\theta, r\sin\theta)r\mathrm{d}r\mathrm{d}\theta.$$

Corollary 3.109 (Integral in cylindrical coordinates). Let $\varphi : [0,\infty) \times [0,2\pi) \times \mathbb{R} \to \mathbb{R}$ be such that

$$\varphi(r,\theta,z) \longmapsto (r\cos\theta, r\sin\theta, z).$$

Then we have $|J\varphi| = r$ and therefore:

$$\int_{\varphi(U)} f(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z = \int_U f(r\cos\theta, r\sin\theta, z)r\mathrm{d}r\mathrm{d}\theta\mathrm{d}z.$$

Corollary 3.110 (Integral in spherical coordinates). Let $\varphi : [0,\infty) \times [0,2\pi) \times [0,\pi] \to \mathbb{R}$ be such that

$$\varphi(\rho,\theta,\phi) \longmapsto (\rho\sin\phi\cos\theta, \rho\sin\phi\sin\theta, \rho\cos\phi).$$

Then we have $|J\varphi| = \rho^2\sin\phi$ and therefore:

$$\int_{\varphi(U)} f(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z =$$
$$= \int_U f(\rho\sin\phi\cos\theta, \rho\sin\phi\sin\theta, \rho\cos\phi)\rho^2\sin\phi\mathrm{d}\rho\mathrm{d}\theta\mathrm{d}\phi.$$

1.2.3.5 | Vector calculus

Arc-length and line integrals

Definition 3.111. Let $\boldsymbol{\gamma} : [a,b] \to \mathbb{R}^n$ be a parametrization of a curve and $\mathcal{P} = \{t_0, \ldots, t_n\}$ be a partition of $[a,b]$. Then, the *length of the polygonal* created from the vertices $\boldsymbol{\gamma}(t_i)$ is

$$L(\boldsymbol{\gamma}, \mathcal{P}) = \sum_{i=1}^n \|\boldsymbol{\gamma}(t_i) - \boldsymbol{\gamma}(t_{i-1})\|.$$

Definition 3.112. Let $\boldsymbol{\gamma} : [a,b] \to \mathbb{R}^n$ be a parametrization of a curve c. The *arc length of* c is

$$L(c) = \sup\{L(\boldsymbol{\gamma}, \mathcal{P}) : \mathcal{P} \in \mathbf{P}([a,b])\} \in [0,\infty].$$

Definition 3.113. We say that a curve c is *rectifiable* if it has a finite arc length, that is, if $L(c) < \infty$.

Proposition 3.114. Let $\boldsymbol{\gamma} : [a,b] \to \mathbb{R}^n$ be a parametrization of class $\mathcal{C}^1$ of a curve c. Then c is rectifiable and

$$L(c) = \int_a^b \|\boldsymbol{\gamma}'(t)\|\mathrm{d}t\text{[25]}.$$

Definition 3.115. Let $\boldsymbol{F} : U \subset \mathbb{R}^m \to \mathbb{R}^n$ be a vector field[26]. If all its component functions F_i are integrable, we define

$$\int_U \boldsymbol{F} = \left(\int_U F_1, \ldots, \int_U F_n\right) \in \mathbb{R}^n.$$

[25] It can be seen that the arc length of a curve does not depend on its parametrization.
[26] A *vector field* is nothing more than a vector-valued function.

Definition 3.116. Let c be a curve in $\mathbb{R}^2$ parametrized by $\boldsymbol{\gamma} = (x(t), y(t))$. The unit tangent vector to the curve at time t is

$$\mathbf{T} = \frac{\boldsymbol{\gamma}'(t)}{\|\boldsymbol{\gamma}'(t)\|}.$$

The normal vector to the curve is $N(t) = (y'(t), -x'(t))$ and the unit normal vector to the curve is

$$\mathbf{n} = \frac{N(t)}{\|N(t)\|}\text{[27]}.$$

Definition 3.117. Let c be a curve parametrized by $\boldsymbol{\gamma} : [a, b] \to \mathbb{R}^n$ and $\varphi : [c, d] \to [a, b]$ be a diffeomorphism. The composition $\boldsymbol{\gamma} \circ \varphi : [c, d] \to \mathbb{R}^n$ is called a *reparametrization of* c.

Definition 3.118. Let c be a curve of class $\mathcal{C}^1$ parametrized by $\boldsymbol{\gamma} : [a, b] \to \mathbb{R}^n$ an L be its arc length. We define the *arc length parameter* as

$$s(t) = \int_a^t \|\boldsymbol{\gamma}'(t)\|\mathrm{d}t.$$

We reparametrize c by $\rho(s) = \boldsymbol{\gamma}(t(s))$, $0 \le s \le L$. Then $\rho'(s)$ is a unit tangent vector to c and $\rho''(s)$ is perpendicular to c at the point $\rho(s)$.

Definition 3.119. Let c be a curve of class $\mathcal{C}^2$ and s be its arc length parameter. We define the *curvature* of c at the point $\rho(s)$ as

$$\kappa(\rho(s)) = \|\rho''(s)\|.$$

Definition 3.120. Let $c = \{\boldsymbol{\gamma}(t) : t \in [a, b]\} \subset \mathbb{R}^n$ be a curve of class $\mathcal{C}^1$ and $f : \mathbb{R}^n \to \mathbb{R}$ be continuous function. We define the *line integral of f along* c as

$$\int_c f\mathrm{d}s = \int_a^b f(\boldsymbol{\gamma}(t))\|\boldsymbol{\gamma}'(t)\|\mathrm{d}t\text{[28]}.$$

Definition 3.121. Let $c = \{\boldsymbol{\gamma}(t) : t \in [a, b]\} \subset \mathbb{R}^n$ be a curve of class $\mathcal{C}^1$ and $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$ be a continuous vector field. We define the *line integral of* $\mathbf{f}$ *along* c as

$$\int_c \mathbf{f} \cdot \mathrm{d}\mathbf{s} = \int_c \mathbf{f} \cdot \mathbf{T}\mathrm{d}s = \int_a^b \mathbf{f}(\boldsymbol{\gamma}(t)) \cdot \boldsymbol{\gamma}'(t)\mathrm{d}t,$$

where $\mathbf{T}$ is the unit tangent vector c[29]. If c is closed, then this integral is called the *circulation of* $\mathbf{f}$ *around* c.

Definition 3.122. A *Jordan arc* is the image of an injective continuous map $\boldsymbol{\gamma} : [a, b] \to \mathbb{R}^n$. A *Jordan closed curve* is the image of an injective continuous map $\boldsymbol{\gamma} : [a, b] \to \mathbb{R}^n$ such that $\boldsymbol{\gamma}(a) = \boldsymbol{\gamma}(b)$.

Conservative vector fields

Definition 3.123. Let $U \subseteq \mathbb{R}^n$ be a domain and $f : U \to \mathbb{R}$ be a function of class $\mathcal{C}^1$. We say that $\mathbf{f} : U \to \mathbb{R}^n$ is a *conservative* or a *gradient vector field* if

$$\mathbf{f}(x) = \boldsymbol{\nabla} f(x), \quad \forall x \in U.$$

The function f is called the *potential* of $\mathbf{f}$.

Theorem 3.124. Let $\mathbf{f} = \boldsymbol{\nabla} f$ be a conservative vector field on $U \subseteq \mathbb{R}^n$ and c be a closed curve that admits a parametrization $\boldsymbol{\gamma}(t) : [a, b] \to \mathbb{R}^n$ of class $\mathcal{C}^1(U)$. Then

$$\int_c \mathbf{f} \cdot \mathrm{d}\mathbf{s} = f(\boldsymbol{\gamma}(b)) - f(\boldsymbol{\gamma}(a)).$$

Corollary 3.125. Let $\mathbf{f}$ be a conservative vector field on U and c be a closed curve that admits a parametrization of class $\mathcal{C}^1(U)$. Then $\displaystyle\int_c \mathbf{f} \cdot \mathrm{d}\mathbf{s} = 0$.

Divergence, curl and Laplacian

Definition 3.126. Let $\mathbf{f} = (F_1, \ldots, F_n)$ be a vector field of class $\mathcal{C}^1(U)$, $U \subseteq \mathbb{R}^n$. The *divergence of* $\mathbf{f}$ is

$$\mathbf{div}\,\mathbf{f} = \boldsymbol{\nabla} \cdot \mathbf{f} = \sum_{i=1}^n \frac{\partial F_j}{\partial x_j}.$$

Definition 3.127. Let $\mathbf{f} = (F_1, F_2, F_3)$ be a vector field of class $\mathcal{C}^1(U)$, $U \subseteq \mathbb{R}^3$. The *curl de* $\mathbf{f}$ is

$$\mathbf{rot}\,\mathbf{f} = \boldsymbol{\nabla} \times \mathbf{f} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ \frac{\partial}{\partial x} & \frac{\partial}{\partial y} & \frac{\partial}{\partial z} \\ F_1 & F_2 & F_3 \end{vmatrix} =$$

$$= \left(\frac{\partial F_3}{\partial y} - \frac{\partial F_2}{\partial z}, \frac{\partial F_1}{\partial z} - \frac{\partial F_3}{\partial x}, \frac{\partial F_2}{\partial x} - \frac{\partial F_1}{\partial y}\right).$$

Definition 3.128. Let $f : U \subseteq \mathbb{R}^n \to \mathbb{R}$ be a function of class $\mathcal{C}^2(U)$, $U \subseteq \mathbb{R}^3$. The *Laplacian of* f is

$$\nabla^2 f = \Delta f = \sum_{i=1}^n \frac{\partial^2 f}{\partial x_j^2}.$$

Proposition 3.129. Let U be an open set of $\mathbb{R}^3$ and $f : U \to \mathbb{R}$, $\mathbf{f} : U \to \mathbb{R}^3$ be functions of class $\mathcal{C}^2(U)$. Then for all $x \in U$ we have:

$$\mathbf{rot}(\boldsymbol{\nabla} f) = 0, \qquad \mathbf{div}(\mathbf{rot}\,\mathbf{f}) = 0 \quad \text{i} \quad \mathbf{div}(\boldsymbol{\nabla} f) = \nabla^2 f.$$

Surface area and surface integrals

Proposition 3.130. Let S be the graph of a function $z = \Phi(x, y)$ of class $\mathcal{C}^1(U)$, $U \subseteq \mathbb{R}^2$. Then

$$\text{area}\,(S) = \iint_U \sqrt{1 + \left(\frac{\partial \Phi}{\partial x}\right)^2 + \left(\frac{\partial \Phi}{\partial y}\right)^2}\mathrm{d}x\mathrm{d}y.$$

Definition 3.131. A *parametrized surface* $S \subset \mathbb{R}^3$ is the image of a map $\Phi : U \subseteq \mathbb{R}^2 \to \mathbb{R}^3$ of class $\mathcal{C}^1(U)$ defined by $\Phi(u, v) = (x(u, v), y(u, v), z(u, v))$.

[27] Observe that $-N(t)$ is also a normal vector to the curve but, by agreement, we take the one pointing to the right of the curve or, if the curve is closed, the one pointing outwards from the curve.

[28] It can be seen that this integral is independent of the parametrization of c.

[29] It can be seen that the latter integral is independent of the parametrization of c except for a factor of -1 that depends on the orientation of the parametrization.

Proposition 3.132. Let $S = \Phi(U)$ be a surface in $\mathbb{R}^3$ parametrized by $\Phi \in \mathcal{C}^1(U)$. Then the unit normal vector to S at the point $\Phi(u,v)$ is

$$\mathbf{n}(u,v) = \frac{\frac{\partial \Phi}{\partial u} \wedge \frac{\partial \Phi}{\partial v}}{\left\| \frac{\partial \Phi}{\partial u} \wedge \frac{\partial \Phi}{\partial v} \right\|}.$$

Proposition 3.133. Let $S = \Phi(U)$ be a surface in $\mathbb{R}^3$ parametrized by $\Phi \in \mathcal{C}^1(U)$. Then,

$$\operatorname{area}(S) = \iint_U \left\| \frac{\partial \Phi}{\partial u} \wedge \frac{\partial \Phi}{\partial v} \right\| \mathrm{d}u\mathrm{d}v.$$

Definition 3.134. Let $S = \Phi(U)$ be a surface in $\mathbb{R}^3$ parametrized by $\Phi \in \mathcal{C}^1(U)$ and $f : \mathbb{R}^3 \to \mathbb{R}$ be a continuous function whose domain contain S. We define the *surface integral f over S* as

$$\iint_S f \mathrm{d}S = \iint_U f(\Phi(u,v)) \left\| \frac{\partial \Phi}{\partial u} \wedge \frac{\partial \Phi}{\partial v} \right\| \mathrm{d}u\mathrm{d}v^{30}.$$

Definition 3.135. Let $S = \Phi(U)$ be a surface in $\mathbb{R}^3$ parametrized by $\Phi \in \mathcal{C}^1(U)$ and $\mathbf{f} : \mathbb{R}^3 \to \mathbb{R}^3$ be a continuous vector field whose domain contain S. We define the *surface integral* $\mathbf{f}$ *over* S or the *flux of* $\mathbf{f}$ *across* S as

$$\iint_S \mathbf{f} \cdot \mathrm{d}\mathbf{S} = \iint_S \mathbf{f} \cdot \mathbf{n} \mathrm{d}S = \\ = \iint_U \mathbf{f}(\Phi(u,v)) \cdot \left(\frac{\partial \Phi}{\partial u} \wedge \frac{\partial \Phi}{\partial v} \right) \mathrm{d}u\mathrm{d}v,$$

where $\mathbf{n}$ is the unit normal vector to S[31].

Theorems of vector calculus on $\mathbb{R}^2$

Definition 3.136. Let $U \subseteq \mathbb{R}^3$ be an open set. A *differential 1-form on U* is an expression of the form

$$\omega = F_1 \mathrm{d}x + F_2 \mathrm{d}y + F_3 \mathrm{d}z,$$

where F_1, F_2, F_3 are scalar functions defined on U[32].

Theorem 3.137 (Green's theorem). Let $\mathbf{f} = (f_1, f_2)$ be a vector field of class $\mathcal{C}^1(U)$, $U \subseteq \mathbb{R}^2$, and $c = \partial U$ be the curve formed from the boundary of U[33]. Then

$$\int_{\partial U} \mathbf{f} \cdot \mathrm{d}\mathbf{s} = \iint_U \mathbf{rot}\, \mathbf{f} \mathrm{d}x\mathrm{d}y^{34}.$$

Corollary 3.138. Let U be a region in $\mathbb{R}^2$ and ∂U be its boundary. Then,

$$\operatorname{area}(U) = \int_{\partial U} x\mathrm{d}y = -\int_{\partial U} y\mathrm{d}x = \frac{1}{2}\int_{\partial U} (x\mathrm{d}y - y\mathrm{d}x).$$

Theorem 3.139 (Divergence theorem on $\mathbb{R}^2$). Let $\mathbf{f} = (f_1, f_2)$ be a vector field of class $\mathcal{C}^1(U)$, $U \subseteq \mathbb{R}^2$ with boundary ∂U. Then,

$$\int_{\partial U} \mathbf{f} \cdot \mathbf{n} \mathrm{d}s = \iint_U \mathbf{div}\, \mathbf{f} \mathrm{d}x\mathrm{d}y^{35}.$$

Theorems of vector calculus on $\mathbb{R}^3$

Theorem 3.140 (Stokes' theorem). Let S be a parametrized surface of class $\mathcal{C}^1$ and ∂S be its boundary. Let $\mathbf{f} = (f_1, f_2, f_3)$ be a vector field of class $\mathcal{C}^1$ in a domain containing $S \cup \partial S$. Then

$$\int_{\partial S} \mathbf{f} \cdot \mathrm{d}\mathbf{s} = \iint_S \mathbf{rot}\, \mathbf{f} \cdot \mathbf{n} \mathrm{d}S.$$

Corollary 3.141. Let $a \in \mathbb{R}^3$ and $\mathbf{n}$ be a unit vector. Suppose $D_r = D(a,r)$ is a disk of radius r centered at a and perpendicular to $\mathbf{n}$. Let $\mathbf{f}$ be a vector field of class $\mathcal{C}^1(D_r)$. Then

$$\mathbf{rot}\, \mathbf{f}(a) \cdot \mathbf{n} = \lim_{r \to 0} \frac{1}{\operatorname{area}(D_r)} \int_{\partial D_r} \mathbf{f} \cdot \mathrm{d}\mathbf{s}.$$

Therefore, the $\mathbf{n}$-th component of $\mathbf{rot}\, \mathbf{f}(a)$ is the circulation of $\mathbf{f}$ in a small circular surface perpendicular to $\mathbf{n}$, per unit of area.

Theorem 3.142 (Gauß' or divergence theorem on $\mathbb{R}^3$). Let $\mathbf{f} = (f_1, f_2, f_3)$ be a vector field of class $\mathcal{C}^1$ on a symmetric region[36] $V \subset \mathbb{R}^3$ with boundary ∂V. Then,

$$\iint_{\partial V} \mathbf{f} \cdot \mathbf{n} \mathrm{d}S = \iiint_V \mathbf{div}\, \mathbf{f} \mathrm{d}x\mathrm{d}y\mathrm{d}z$$

[30] It can be seen that this integral is independent of the parametrization of S.

[31] It can be seen that the latter integral is independent of the parametrization of S except for a factor of -1 that depends on the orientation of the normal vector $\mathbf{n}$.

[32] Extending this notion, we can define 2-forms and 3-forms as:

$$\begin{aligned} \omega &= F_1 \mathrm{d}x\mathrm{d}y + F_2 \mathrm{d}y\mathrm{d}z + F_3 \mathrm{d}z\mathrm{d}y && \text{2-form,} \\ \omega &= F \mathrm{d}x\mathrm{d}y\mathrm{d}z && \text{3-form.} \end{aligned}$$

[33] It goes without saying that the orientation is chosen positive, that is counterclockwise.

[34] Alternatively, using differential forms, we get

$$\int_{\partial U} (F_1 \mathrm{d}x + F_2 \mathrm{d}y) = \iint_U \left(\frac{\partial F_2}{\partial x} - \frac{\partial F_1}{\partial y} \right) \mathrm{d}x\mathrm{d}y.$$

[35] The first integral represents the flux of $\mathbf{f}$ across the curve ∂U.

[36] A region on $\mathbb{R}^3$ is *symmetric* if is xy-simple, yz-simple and xz-simple.

Corollary 3.143. Let $B_r = B(a, r)$ be a ball of radius r centered at $a \in \mathbb{R}^3$ and $\mathbf{f}$ be a vector field of class $\mathcal{C}^1(B_r)$. Then

$$\mathbf{div}\,\mathbf{f}(a) = \lim_{r\to 0} \frac{1}{\mathrm{vol}(B_r)} \iint_{\partial B_r} \mathbf{f}\cdot\mathbf{n}\mathrm{d}S.$$

Therefore, $\mathbf{div}\,\mathbf{f}(a)$ is the flux of $\mathbf{f}$ outward form a, in the normal direction across the surface of a small ball centered on a, per unit of volume.

1.2.4 Linear geometry

1.2.4.1 | The foundations of geometry

In this section we will only study geometry in the plane.

Euclidean geometry

Axiom 4.1 (Euclid's axioms).

1. It is possible to draw, from any point to any point, a straight line.
2. It is possible to extend any segment by either of its two ends.
3. With center at any point it is possible to draw a circle that passes through any other point.
4. All right angles are equal.
5. If a line segment intersects two straight lines forming two interior angles on the same side that sum to less than two right angles, then the two lines, if extended indefinitely, meet on the side on which the angles sum to less than two right angles.

5′. *(Playfair's axiom)* Given a line and a point not on it, at most one line parallel to the given line can be drawn through the point.

Hilbert's axioms

Definition 4.2. In elementary plane geometry[37], there are two types of objects, *points* and *lines*, which can have three types of relationships between them:

- An *incidence relation*. We say, for example, that a point lies on a line or a line passes through a point.
- An *order relation*. We say, for example, that a point lies between two other points.
- A *congruence relation*. We say, for example, that a segment is congruent to another or an angle is congruent to another[38].

Axiom 4.3 (Incidence axioms).

1. For every two points there exists no more than one line containing both.
2. There exist at least two points on a line.
3. There exist at least three points that do not lie on the same line.

Axiom 4.4 (Order axioms).

1. If a point B lies between A and C, then B lies between C and A and there exists a line containing the distinct points A, B, C.
2. If A and B are two points, there exists at least one point C such that B lies between A and C.
3. Given three point on a line, there is no more than one which lies between the other two.
4. *(Pasch's axiom)* Let A, B, C be three points notlying in the same line and let r be a line not passing through any of the points A, B, C and passing through a point of the segment AB. Then it also passes through either a point of the segment BC or a point of the segment AC.

Definition 4.5. A *ray* or *half-line* is a point A, called vertex, and all the points of a line passing through A lying on the same side with respect to A.

Definition 4.6. A *half-plane* is a straight line r and all the points lying on the same side with respect to r.

Definition 4.7. An *angle* is a non-ordered pair of rays with same vertices that belong to different straight lines.

Axiom 4.8 (Congruence axioms).

1. Congruence of angles and congruence of rays are equivalence relations.
2. Let a and b be two lines not necessarily different, A and B be points on a and A' be a point on b. We fix a side of the line b with respect to A'. Then, there exists a point B' lying on this side of b such that $AB \equiv A'B'$.
3. Let a, a' be two lines not necessarily different. Let AB, BC be segments on a that intersect only in one point and $A'B', B'C'$ be segments on a' that also intersect only in one point. If $AB \equiv A'B'$ and $BC \equiv B'C'$, then $AC \equiv A'C'$.
4. Let $\angle hk$ be an angle, k' be a ray and H be one of the two half-planes that k' defines. Then, there is one and only one angle $\angle h'k'$ such that $\angle hk \equiv \angle h'k'$ and h' belongs to H.
5. *(SAS criterion)* Consider two triangles[39] ABC and $A'B'C'$ (not necessarily different). If $AC \equiv A'C'$, $AB \equiv A'B'$ and $\alpha \equiv \alpha'$, then $\beta \equiv \beta'$.

Axiom 4.9 (Continuity axioms).

1. *(Axiom of Archimedes)* If AB and CD are any segments, then there exists a number n such that n segments CD constructed contiguously from A, along the ray from A to B, will pass beyond the point B.
2. *(Axiom of completeness)* An extension of a set of points on a line with order and congruence relations that would preserve the relations existing among the original elements as well as the rest of the axioms is impossible.

[37] In this section we only study the geometry in the plane.
[38] We will use the notation $\equiv$ to say that two angles or segments are congruent.
[39] We will use the following notation with respect to the angles of a triangle ABC: $\alpha = \angle CAB$, $\beta = \angle ABC$ and $\gamma = \angle BCA$.

3. *(RC)* If a straight line passes through a point inside a circle, it intersects the circle in two points.
4. *(CC)* If a circle passes through points inside and outside another circle, the two circle intersect in two points.

Axiom 4.10 (Axiom of Parallels). Let a be any line and A be a point not on it. Then there is at most one line that passes through A and does not intersect a.

Definition 4.11. Different types of geometry:

- A *Hilbert plane* is a geometry where axioms 4.3, 4.4 and 4.8 are satisfied.
- A *Pythagorean plane* is a Hilbert plane in which axiom of Parallels is satisfied.
- An *Euclidean plane* is a Pythagorean plane in which axioms RC and CC are satisfied.
- The *Cartesian geometry of* $\mathbb{R}^2$ is the unique geometry satisfying all Hilbert's axioms.

Absolute geometry

Definition 4.12. *Absolute geometry* is the part of Euclidean geometry that only uses axioms 4.3, 4.4 and 4.8.

Theorem 4.13. In an isosceles triangles, the angles opposite the congruent sides are congruent.

Theorem 4.14 (SAS criterion). If two sides of a triangle and the angle between them are congruent to the corresponding sides and angle of a second triangle, then the two triangles are congruent.

Theorem 4.15. Adjacent angles of congruent angles are congruent.

Theorem 4.16. Opposite angles[40] are congruent.

Theorem 4.17. If A and B are each on one of the sides of an angle with vertex O, any ray with vertex O that passes through an interior point of the angle intersects the segment AB.

Theorem 4.18. There exist right angles.

Theorem 4.19. Let $\alpha, \alpha', \beta, \beta'$ be angles. If $\alpha \equiv \alpha'$ and $\beta \equiv \beta'$, then $\alpha + \beta \equiv \alpha' + \beta'$.

Theorem 4.20 (SSS criterion). If two triangles have all its sides congruent, they have all its angles congruent.

Theorem 4.21. Right angles are congruent.

Theorem 4.22 (Exterior angle theorem). An exterior angle of a triangle is greater than any of the non-adjacent interior angles.

Theorem 4.23. If ℓ is a line and P is a point not lying on ℓ, there exists a line L passing through P and such that not intersects ℓ.

Theorem 4.24 (ASA criterion). If two triangles have a side and the two angles of this side congruent, the triangles are congruent.

Theorem 4.25 (SAA criterion). If two triangles have a side, an angle of this side and the angle opposite to this side congruent, the triangles are congruent.

Theorem 4.26. In any triangle the greater side is opposite to the greater angle.

Theorem 4.27. If a triangle has two congruent angles, it is isosceles.

Theorem 4.28. Every segment has a midpoint.

Theorem 4.29. Every angle has an angle bisector.

Theorem 4.30. Every segment has a perpendicular bisector.

Theorem 4.31 (Saccheri–Legendre theorem). The sum of the angles of a triangle is at most two right angles.

Cartesian geometry

Definition 4.32. An *ordered field* K is a field together with a total order of its elements, satisfying:

- $x \leq y \implies x + z \leq y + z \quad \forall x, y, z \in K.$
- $x, y \geq 0 \implies xy \geq 0 \quad \forall x, y \in K.$

Definition 4.33. We say a field K is *Pythagorean* if $\forall a \in K$, $1 + a^2 = b^2$ for some $b \in K$.

Theorem 4.34. K^2 is a Pythagorean plane if and only if K is an ordered Pythagorean field.

Definition 4.35. An ordered field K is *Archimedean* if axiom of Archimedes is valid in K.

Definition 4.36. An ordered field K is *Euclidean* if $\forall a \in K$, $a > 0$, there exists a $b \in K$ such that $b^2 = a$.

Theorem 4.37. K^2 is a Euclidean plane if and only if K is an ordered Euclidean field.

Definition 4.38. The smallest Pythagorean field is called *Hilbert field* (Ω) and it can be defined as the intersection of all Pythagorean fields of $\mathbb{R}$. Alternatively, it can be defined as the field whose elements are the real numbers obtained from rational numbers with the operations of addition, subtraction, multiplication, multiplicative inverse and the operation $a \mapsto \sqrt{1 + a^2}$.

Definition 4.39. The smallest Euclidean field is called *constructible field* ($\mathbb{K}$) and it can be defined as the intersection of all Euclidean fields of $\mathbb{R}$. Alternatively, it can be defined as the field whose elements are the real numbers obtained from rational numbers with the operations of addition, subtraction, multiplication, multiplicative inverse and the square root of positive numbers.

[40] Opposite angles are angles that are opposite each other when two lines intersect.

Non-Euclidean geometries

Definition 4.40 (Hyperbolic geometry). *Hyperbolic geometry* is the non-Euclidean geometry where axiom of Parallels fails.

Proposition 4.41. Properties of hyperbolic geometry:

- There are infinity lines parallel to a given line ℓ that pass through a point not lying on ℓ.
- There are lines inside an angle that do not intersect the sides of the angle.
- The sum of the angles of any triangle is less than two right angles.

Definition 4.42. Hyperbolic geometry models:

- Beltrami-Klein model:
  - Points: $\mathcal{K} := \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$.
  - Lines: Lines of $\mathbb{R}^2$ that intersect with $\mathcal{K}$.
  - Incidence and order relations are the same as in ordinary Euclidean geometry of $\mathbb{R}^2$.
  - Two segments $AB, A'B' \in \mathcal{K}$ are congruent if and only if there is an Euclidean motion[41] f such that $f(A) = A'$ and $f(B) = B'$. Two angles $hk, h'k' \in \mathcal{K}$ are congruent if and only if there is an Euclidean motion f such that $f(h) = h'$ and $f(k) = k'$.

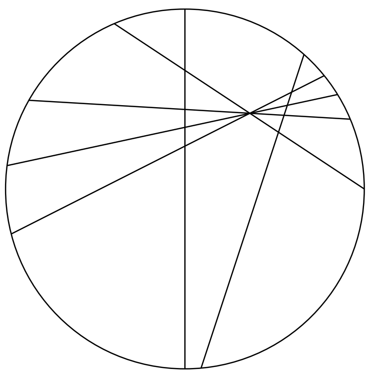


Figure 1.2.6: Beltrami–Klein model

- Poincaré disk model:
  - Points: $\mathcal{D} := \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$.
  - Lines:
    1. Lines of $\mathbb{R}^2$ that pass through the origin.
    2. Circles of $\mathbb{R}^2$ that intersect orthogonally the circle $\mathcal{C} = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.
  - Incidence and order relations are the same as in ordinary Euclidean geometry of $\mathbb{R}^2$.
  - Is a conformal model: The hyperbolic measure of an angle coincides with the Euclidean measure of it whereas the distance between two points $A, B \in \mathcal{D}$ is measured using the following formula:
  $$d_h(A,B) := -\ln \frac{d(A,P)d(B,Q)}{d(A,Q)d(B,P)}.$$
  where $P, Q \in \mathcal{C}$ are the boundary points of $\mathcal{D}$ on the line passing through A and B so that A lies between P and B.

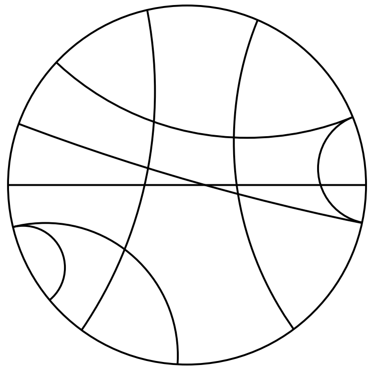


Figure 1.2.7: Poincaré disk model

- Poincaré half-plane model:
  - Points: $\mathcal{H} := \{(x,y) \in \mathbb{R}^2 : y > 0\}$.
  - Lines:
    1. Vertical straight lines of $\mathbb{R}^2$.
    2. Circles of $\mathbb{R}^2$ with center on the x-axis.
  - Incidence and order relations are the same as in ordinary Euclidean geometry of $\mathbb{R}^2$.
  - Is a conformal model. The distance between two points $A, B \in \mathcal{D}$ is measured using the following formula:
  $$d_h(A,B) := -\ln \frac{d(A,P)d(B,Q)}{d(A,Q)d(B,P)}.$$
  where $P, Q \in \{(x,y) \in \mathbb{R}^2 : y = 0\}$ are the points where the semicircle meet the boundary line $y = 0$.

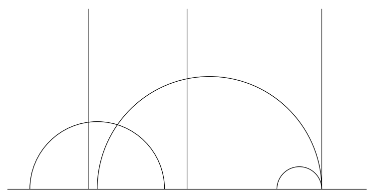


Figure 1.2.8: Poincaré half-plane model

Definition 4.43 (Non-Paschian geometry). *Non-Paschian geometry* is the non-Euclidean geometry where axiom of Archimedes fails.

Proposition 4.44 (Construction of a non-Paschian geometry). Suppose we have a total order relation $\trianglelefteq$ on $\mathbb{R}$ such that:

1. $x \trianglelefteq y \implies x + z \trianglelefteq y + z \ \forall x, y, z \in \mathbb{R}$.
2. $\exists a, b \in \mathbb{R}$ such that $a \trianglerighteq 0$, $b \trianglerighteq 1$ and $ab \trianglelefteq 0$.

Then, the ordinary affine geometry of $\mathbb{R}^2$ together with $\trianglelefteq$, satisfy all Hilbert's axioms except Pasch's axiom.

[41] See section 1.2.4.3.

Definition 4.45 (Non-SAS geometry). *Non-SAS geometry* is the non-Euclidean geometry where SAS criterion fails.

Proposition 4.46 (Construction of a non-SAS geometry).

- Points: $\mathcal{S} = \{(x, y, z) \in \mathbb{R}^3 : x + z = 0\} = \{(x, y, -x) \in \mathbb{R}^3\}$.
- Lines: Ordinary straight lines of $\mathbb{R}^2$ contained in $\mathcal{S}$.
- Incidence and order relations are the same as in ordinary Euclidean geometry of $\mathbb{R}^2$.
- Congruence of angles is the same as in the ordinary geometry of $\mathbb{R}^3$. Congruence of segments is based in the following distance:

  $$d'((x, y, -x), (x', y' - x'))^2 = (x - x')^2 + (y - y')^2.$$

  That is, two segments are congruent if so are their projections to the plane $z = 0$.

Definition 4.47 (Non-Archimedean geometry). *Non-Archimedean geometry* is the non-Euclidean geometry where SAS criterion fails.

Axiomatic projective space

Definition 4.48. An *axiomatic projective space* is a system of points and lines with an incidence relation that satisfy:

1. Every line contains at least 3 points
2. Any two distinct points lie on a unique line.
3. *(Projective axiom)* If A, B, C, D are four different points and lines AB and CD intersect, then lines AC and BD also intersect.

Definition 4.49. Let X be a projective space. A *projective subvariety of* X is a set $Z \neq \varnothing$ of points of X such that if $x, y \in Z$ are different points, then all the points lying on the line passing through x and y belong to Z. Thus, Z is also a projective space.

Proposition 4.50. Let X be a projective space. The intersection of subvarieties of X is also a subvariety of X.

Proposition 4.51. If A and B are subvarieties of a projective space X, we define its sum $A+B$ as the intersection of all subvarieties containing $A \cup B$. As a consequence, $A + B$ is a subvariety of X.

Definition 4.52. Let X, Y be a projective spaces. A *collineation between* X *and* Y is a bijection map $f : X \to Y$ such that $A, B, C \in X$ are three collinear points if and only if $f(A), f(B), f(C) \in Y$ are also collinear.

Definition 4.53. If X is a projective space, the *dimension of* X is the maximum n such that there is a chain of inclusions

$$X_0 \subset X_1 \subset X_2 \subset \cdots \subset X_n,$$

where each X_i is a non-empty subvariety of X. If this n doesn't exist, we say X has infinite dimension.

Definition 4.54. A *projective plane* is a projective space of dimension 2 that satisfies the following axioms:

1. Any two distinct points lie on a unique line.
2. Any two distinct lines meet on a unique point.
3. There exist at least four points of which no three are collinear.

Theorem 4.55. X is a projective space of dimension 2 if and only if X satisfies axioms 4.54.

Theorem 4.56 (Duality principle). If a statement $\mathcal{P}$ (which only involves points and lines) is true in any projective plane, then the statement obtained from $\mathcal{P}$ exchanging points by lines (and correctly changing all the connectors to make a consistent statement) is also true in any projective plane.

Affine and projective spaces

Definition 4.57. An *affine plane* is a set of points and lines satisfying the following axioms:

1. Any two distinct points lie on a unique line.
2. If r is a line and $P \notin r$ is a point, there exists a unique line s such that $P \in s$ and r and s does not intersect.
3. Any line has at least two distinct points.
4. There exist at least two distinct lines.

Proposition 4.58 (Passage from the projective plane to the affine plane). Suppose X is a projective plane and $r \in X$ is an arbitrary line of X. Let $\mathbb{A} := X - r$. Then, $\mathbb{A}$ is an affine plane.

Proposition 4.59 (Passage from the affine plane to the projective plane). Suppose $\mathbb{A}$ is an affine plane. Let $\mathcal{R}$ be the set of all lines of $\mathbb{A}$. We define

$$L = {}^{\mathcal{R}}\!/\!_{\sim} \quad \text{where } r \sim s \iff r \parallel s.$$

Construction of a projective plane X:

1. The points of X are the points of $\mathbb{A}$ and L.
2. The lines of X are the lines of $\mathbb{A}$ an another line ℓ.
3. Incidence relation on X: Let $P \in X$ be a point and $r \in X$ a line. Then:
   - If $P \in \mathbb{A}$ and $r \in \mathbb{A}$, then $P \in r$ has the same meaning on X and A.
   - If $P \in \mathbb{A}$ and $r = \ell$, then $P \notin r$.
   - If $P \in X \setminus \mathbb{A} = L$, then $P \in \ell$.
   - If $P \in X \setminus \mathbb{A} \neq L$, then P is an equivalence class of lines of $\mathbb{A}$ and, if $r \in \mathbb{A}$, we say $P \in r$ if $r \in X$.

1.2.4.2 | Projective geometry

Projective space

Definition 4.60. Let V be a $n+1$-dimensional vector space over a field K. We define the *n-dimensional projective space $\mathcal{P}(V)$ of V* in either of these two equivalent ways:

- $\mathcal{P}(V) := \{$1-dimensional vector subspaces of $V\}$.
- $\mathcal{P}(V) := (V\backslash\{0\})/\sim$ where the relation $\sim$ is defined $\forall \mathbf{v}, \mathbf{u} \in V$ as $\mathbf{v} \sim \mathbf{u} \iff \mathbf{v} = \lambda\mathbf{u}$, $\lambda \neq 0$[42].

Definition 4.61. Let V, W be two vector spaces over a field K and $\mathcal{P}(V)$, $\mathcal{P}(W)$ be their associated projective spaces. If $\phi : V \to W$ is an isomorphism, we can consider the map:

$$\begin{aligned} \mathcal{P}(\phi) : \mathcal{P}(V) &\to \mathcal{P}(W) \\ [\mathbf{v}] &\mapsto [\phi(\mathbf{v})] \end{aligned}$$

We say $\mathcal{P}(\phi)$ is an *homography between $\mathcal{P}(V)$ and $\mathcal{P}(W)$*.

Definition 4.62. Let V be a vector space over a field K and W be a vector space over a field K'. An *semilinear isomorphism* $\phi : V \to W$ is a bijective map associated with a field isomorphism $r : K \to K'$ such that

$$\begin{aligned} \phi(\mathbf{u}+\mathbf{v}) &= \phi(\mathbf{u}) + \phi(\mathbf{v}) \quad \forall \mathbf{u}, \mathbf{v} \in V. \\ \phi(\lambda\mathbf{v}) &= r(\lambda)\phi(\mathbf{v}) \quad \forall \mathbf{v} \in V,\ \forall \lambda \in K. \end{aligned}$$

Definition 4.63. Let V be a vector space over a field K, W be a vector space over a field K' and $\phi : V \to W$ a semilinear isomorphism. We say $\mathcal{P}(\phi) : \mathcal{P}(V) \to \mathcal{P}(W)$ is an *isomorphism between projective spaces* and we write $\mathcal{P}(V) \cong \mathcal{P}(W)$ to denote that $\mathcal{P}(V), \mathcal{P}(W)$ are isomorphic.

Proposition 4.64. Let V be a $n+1$-dimensional vector space over a field K. Then there is an homography $\mathcal{P}(V) \cong \mathcal{P}(K^{n+1})$[43].

Definition 4.65. Let V be a $n+1$-dimensional vector space over a field K and $E \subseteq V$ be a $m+1$-dimensional vector subspace. Consider the natural inclusion $\mathcal{P}(E) \subseteq \mathcal{P}(V)$. We say $\mathcal{P}(E)$ is a *m-dimensional projective subvariety of $\mathcal{P}(V)$*. In particular, we call *line of $\mathcal{P}(V)$* any 1-dimensional projective subvariety and we call *hyperplane of $\mathcal{P}(V)$* any $n-1$-dimensional projective subvariety.

Homogeneous coordinates and Graßmann formula

Definition 4.66. Let V be a $n+1$-dimensional vector space over a field K, $(\mathbf{v}_0, \ldots, \mathbf{v}_n)$ be a basis of V and $\mathcal{P}(V)$ be a projective space. Given $x \in \mathcal{P}(V)$ such that $x = [\mathbf{v}]$ for some $\mathbf{v} \in V$, $\mathbf{v} = \lambda_0\mathbf{v}_0 + \cdots + \lambda_n\mathbf{v}_n$, we define the *homogeneous coordinates of x* as

$$x = \{\lambda_0, \ldots, \lambda_n\}.$$

Definition 4.67. Let $\mathcal{P}(V)$ be a n-dimensional projective space. A *projective frame on $\mathcal{P}(V)$* is a tuple of $n+2$ points of $\mathcal{P}(V)$, such that any $n+1$ points of the tuple are not contained in a hyperplane.

Theorem 4.68. Let $\mathcal{P}(V)$ be a n-dimensional projective space. If $U_0, \ldots, U_n, U$ is a projective frame of $\mathcal{P}(V)$, there exists a basis $(\mathbf{v}_0, \ldots, \mathbf{v}_n)$ of V such that

$$U_i = [\mathbf{v}_i] \text{ for } i = 0, \ldots, n \text{ and } U = [\mathbf{v}_1 + \cdots + \mathbf{v}_n].$$

If $(\mathbf{u}_0, \ldots, \mathbf{u}_n)$ is another basis of V that satisfies the same property, then $\exists \tau \neq 0 : \mathbf{u}_i = \tau\mathbf{v}_i$, for $i = 0, \ldots, n$.

Definition 4.69. Let $\mathcal{P}(V)$ be a n-dimensional projective space and let $H \subset \mathcal{P}(V)$ be a hyperplane. The *equation of the hyperplane* is

$$x_0a_0 + \ldots + x_na_n = 0.$$

Definition 4.70. Let $\mathcal{P}(V)$ be a projective space and let $Y_1 = \mathcal{P}(E_1)$ and $Y_2 = \mathcal{P}(E_2)$ be two projective subvarieties of $\mathcal{P}(V)$. Then

- $Y_1 \cap Y_2 = \mathcal{P}(E_1 \cap E_2)$.
- $Y_1 + Y_2 = \mathcal{P}(E_1 + E_2)$.

Theorem 4.71 (Graßmann formula). Let $\mathcal{P}(V)$ be a projective space and $Y_1 = \mathcal{P}(E_1)$, $Y_2 = \mathcal{P}(E_2)$ be two projective subvarieties of $\mathcal{P}(V)$. Then:

$$\dim(Y_1 \cap Y_2) + \dim(Y_1 + Y_2) = \dim Y_1 + \dim Y_2$$[44].

Fano and Pappus configurations

Definition 4.72. A *configuration* is a finite set of points and lines satisfying the following axioms:

1. There are four points such that no three of them are collinear.
2. Two distinct points lie on at most one line.

Definition 4.73. Let X be a projective geometry and $\mathcal{C}$ be a configuration. We say $\mathcal{C} \subseteq X$ if there exists injective maps i_p, i_ℓ from the points and lines of $\mathcal{C}$ to the points and lines of X, respectively, such that if A is a point and s is a line satisfying $A \in s$, then $i_p(A) \in i_\ell(s)$.

Definition 4.74. Let X be a projective geometry and $\mathcal{C}$ be a configuration. We say $\mathcal{C}$ is *realizable on X* if there is an inclusion $\mathcal{C} \subseteq X$.

Definition 4.75. Let X be a projective geometry and $\mathcal{C}$ be a configuration. We say $\mathcal{C}$ is a *theorem in X* if satisfies that for any line $r \in \mathcal{C}$, the inclusion $\mathcal{C} - r \subseteq X$ can be extended to an inclusion $\mathcal{C} \subseteq X$.

Definition 4.76. *Fano configuration* is a configuration of 7 points and 7 lines defined in either of the following ways:

- It's the configuration described in figure 1.2.9.

[42] Observe that $\sim$ is an equivalence relation.
[43] From now on we will use the notation $P_n(K) := \mathcal{P}(K^{n+1})$.
[44] The formula is also valid for the case $Y_1 \cap Y_2 = \varnothing$ if we consider, by agreement, $\dim \varnothing := -1$.

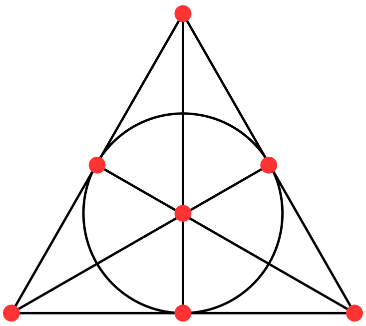


Figure 1.2.9: Fano configuration

- It's the unique projective plane of order 2[45].
- It's the projective plane $P_2(\mathbb{F}_2)$.

Theorem 4.77. If $n \geq 2$, Fano configuration is a theorem in $P_n(K)$ if and only if $\operatorname{char} K = 2$.

Definition 4.78. *Pappus configuration* is a configuration of 9 points and 9 lines defined in either of the following ways:

- It's the configuration described in figure 1.2.10.

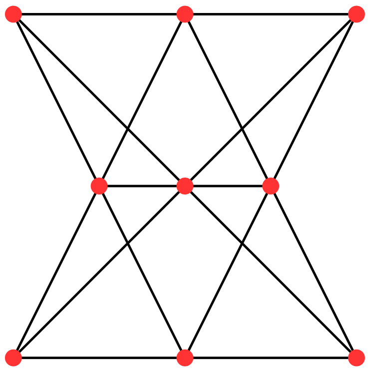


Figure 1.2.10: Pappus configuration

- It's the configuration whose points are the elements of the group $(\mathbb{Z}/9\mathbb{Z}, +)$ and whose lines are triples $\{i, j, k\}$ such that $i + j + k = 0$ where i, j, k are different modulo 3.
- It's the configuration obtained from the affine plane over $\mathbb{F}_3$ eliminating three parallel lines.

Theorem 4.79. Let K be a division ring. Pappus configuration is a theorem in $P_n(K)$ if and only if K is a field.

Desargues configuration

Definition 4.80. Two triangles ABC and $A'B'C'$ are said to be in *perspective with respect to a point* if lines AA', BB' and CC' intersect at the point P. This point is called *centre of perspectivity*.

Definition 4.81. Two triangles ABC and $A'B'C'$ of sides a, b, c and a', b', c' respectively are said to be in *perspective with respect to a line* if points $a \cap a'$, $b \cap b'$ and $c \cap c'$ lie on the same line r. This line is called *axis of perspectivity*.

Theorem 4.82 (Desargues' theorem). If two triangles are in perspective with respect to a point, so are in perspective with respect to a line[46].

Definition 4.83. *Desargues configuration* is a configuration of 10 points and 10 lines defined in either of the following ways:

- It's the configuration described in figure 1.2.11.

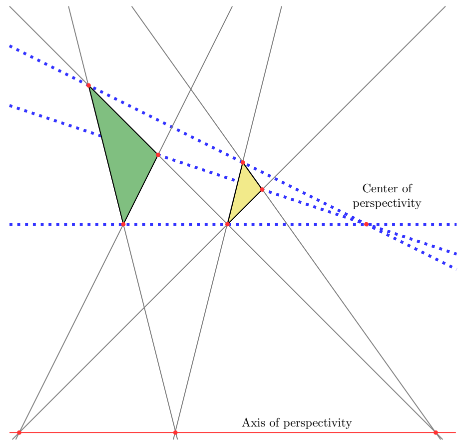


Figure 1.2.11: Desargues configuration

- It's the configuration whose points are the elements of the set $S = \{1, 2, 3, 4, 5\}$ and whose lines are the subsets of cardinal 3 of S.
- It's the configuration created from two triangles that are simultaneously in perspective with respect to a point and in perspective with respect to a line.

Definition 4.84. Projective planes in which Desargues' theorem is not satisfied are called *non-Desarguesian planes*.

Theorem 4.85 (Coordination theorem). Let X be an axiomatic projective space of finite dimension $n > 1$ where Pappus' theorem is valid. Then there exist a field K and an isomorphism $X \cong P_n(K)$[47].

Fundamental theorem of projective geometry and cross ratio

Theorem 4.86 (Fundamental theorem of projective geometry). Let $f : \mathcal{P}(V) \to \mathcal{P}(W)$ be a collineation between projective spaces of finite dimension greater than 1. Then, there exists a semilinear isomorphism $\phi : V \to W$ such that $f = P(\phi)$.

Definition 4.87 (Cross ratio). Let $A, B, C, D \in \mathcal{P}(V)$ be four collinear points lying on a line $L \in \mathcal{P}(V)$ with A, B, C different. As we have $A = [\mathbf{v}_1]$, $B = [\mathbf{v}_2]$,

[45] A finite projective plane of order n is a projective plane in which every line has $n+1$ points and every point lies on $n+1$ lines.

[46] Desargues' theorem is valid in any axiomatic projective space of dimension 3 and, generally, in any axiomatic projective space that is a subvariety of an axiomatic projective space of dimension 3. In particular, it is valid in $P_n(K)$ for any division ring K and $n \geq 2$.

[47] If Pappus theorem is not valid but Desargues' theorem is, then $X \cong P_n(K)$ for some division ring K.

$C = [\mathbf{v}_3]$ and $D = [\mathbf{v}_4]$ for some vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4 \in V$ then $L = \langle \mathbf{v}_1, \mathbf{v}_2 \rangle$. Therefore, $\mathbf{v}_3 = \lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2$ and $\mathbf{v}_4 = \mu_1 \mathbf{v}_1 + \mu_2 \mathbf{v}_2$, for some $\lambda_1, \lambda_2, \mu_1, \mu_2 \in K$. We define the *cross ratio between* A, B, C, D as

$$(A, B, C, D) := \begin{cases} \dfrac{\lambda_2 \mu_1}{\lambda_1 \mu_2} & \text{if} \quad \lambda_1 \mu_2 \neq 0, \\ \infty & \text{if} \quad \lambda_1 \mu_2 = 0. \end{cases}$$

Definition 4.88. Let $A, B, C, D \in \mathcal{P}(V)$ be four collinear points. If $(A, B, C, D) = -1$ we say the points A, B, C, D form an *harmonic ratio.*

Definition 4.89. Let a, b, c, d be four lines on a plane (with a, b, c different) intersecting at the point P. Let r be a different line such that $P \notin r$ and let $A := a \cap r$, $B := b \cap r$, $C := c \cap r$, $D := d \cap r$. We define the *cross ratio between* a, b, c, d as

$$(a, b, c, d) := (A, B, C, D).$$

Definition 4.90. Let X be a projective space such that $\dim X \geq 2$. Let $L_1, L_2 \in X$ be two lines intersecting at the point $P \in X$ and $f : L_1 \to L_2$ be a function such that $f(A) = L_2 \cap PA$. We say f is a *perspectivity.* The composition of perspectivities is called a *projectivity.*

Theorem 4.91. If $f : L_1 \to L_2$ is a projectivity, then f preserves cross ratio, that is:

$$(f(A), f(B), f(C), f(D)) = (A, B, C, D).$$

Theorem 4.92. Let V be a 2-dimensional vector space and $f : \mathcal{P}(V) \to \mathcal{P}(V)$ be a bijection. There exists linear function $\phi : V \to V$ such that $f = P(\phi)$ if and only if f preserves cross ratio.

Plücker coordinates

Proposition 4.93. Let $r \in \mathcal{P}_3(K)$ be a line and $A, B \in r$ two points with coordinates $A = \{a_0, a_1, a_2, a_3\}$ and $B = \{b_0, b_1, b_2, b_3\}$. Consider the matrix:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$$

Now consider the six minors of A:

$$p_{01} = \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}, \quad p_{02} = \begin{vmatrix} a_0 & a_2 \\ b_0 & b_2 \end{vmatrix}, \quad p_{03} = \begin{vmatrix} a_0 & a_3 \\ b_0 & b_3 \end{vmatrix},$$
$$p_{23} = \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \quad p_{31} = \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}, \quad p_{12} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}.$$

The coordinates $\{p_{01}, p_{02}, p_{03}, p_{23}, p_{31}, p_{12}\}$ doesn't depend on the points A, B on the line r. We define the *Plücker coordinates of* r as the coordinates $\{p_{01}, p_{02}, p_{03}, p_{23}, p_{31}, p_{12}\}$

Proposition 4.94. Two lines are equal if and only if they have the same Plücker coordinates.

Proposition 4.95. Let r be a line with Plücker coordinates $\{p_{01}, p_{02}, p_{03}, p_{23}, p_{31}, p_{12}\}$. Then the points $x = \{x_0, x_1, x_2, x_3\} \in r$ satisfy

$$\begin{pmatrix} p_{12} & -p_{02} & p_{01} & 0 \\ -p_{31} & -p_{03} & 0 & p_{01} \\ p_{23} & 0 & -p_{03} & p_{02} \\ 0 & p_{23} & p_{31} & p_{12} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

1.2.4.3 | Affine geometry

Affine space

Definition 4.96. Let V be a vector space over a field K. An *affine space over* V is a set $\mathbb{A}$ together with a map:

$$\begin{aligned} \mathbb{A} \times V &\to \mathbb{A} \\ (P, \mathbf{v}) &\mapsto P + \mathbf{v} \end{aligned}$$

such that:

1. $P + \mathbf{0} = P \ \forall P \in X$.
2. $P + (\mathbf{v} + \mathbf{w}) = (P + \mathbf{v}) + \mathbf{w} \ \forall P \in X$ and $\forall \mathbf{v}, \mathbf{w} \in V$.
3. For all $P, Q \in X \ \exists! \mathbf{v} \in V : Q = P + \mathbf{v}$. We denote the vector $\mathbf{v}$ by $\overrightarrow{PQ}$.

Definition 4.97. Let $\mathbb{A}$ be an affine space associated to a vector space V over a field K[48]. We define the *dimension of* $\mathbb{A}$ as $\dim \mathbb{A} = \dim V$.

Proposition 4.98. Let $\mathbb{A}$ be an affine space, $P, Q, R, S \in \mathbb{A}$. Then, the following properties are satisfied:

1. $\overrightarrow{PQ} = \mathbf{0} \iff P = Q$.
2. $\overrightarrow{PQ} = -\overrightarrow{QP}$.
3. $\overrightarrow{PQ} + \overrightarrow{QR} = \overrightarrow{PR}$.
4. $\overrightarrow{PQ} = \overrightarrow{RS} \implies \overrightarrow{PR} = \overrightarrow{QS}$.

Definition 4.99. Let $\mathbb{A}$ be an affine space, $P_1, \ldots, P_n \in \mathbb{A}$ and $\lambda_1, \ldots, \lambda_n \in K$ such that $\lambda_1 + \cdots + \lambda_n = 1$. Given an arbitrary point $O \in \mathbb{A}$, we define the *affine combination of* $P_1, \ldots, P_n$ as

$$\lambda_1 P_1 + \cdots + \lambda_n P_n := O + (\lambda_1 \overrightarrow{OP_1} + \cdots + \lambda_n \overrightarrow{OP_n}).$$

We say the points $P_1, \ldots, P_n$ are *affinely independents* if the vectors $\overrightarrow{P_1 P_2}, \ldots, \overrightarrow{P_1 P_n}$ are linearly independent.

Definition 4.100. Let $\mathbb{A}$ be an affine space and $P_1, \ldots, P_r \in \mathbb{A}$. The *barycenter of the points* $P_1, \ldots, P_r$ is

$$B := \frac{1}{r} (P_1 + \cdots + P_n).$$

[48]From now on, for simplicity, we will only refer to the affine space by mentioning the set $\mathbb{A}$ without mentioning the associated vector space V over a field K.

Subvarieties and Graßmann formula

Definition 4.101. Let $\mathbb{A}$ be an affine space. If $P \in \mathbb{A}$ and F is a vector subspace of V, then an *affine subvariety of* $\mathbb{A}$ is the set:

$$P + F := \{P + \mathbf{v} \in \mathbb{A} : \mathbf{v} \in F\} = \{Q \in \mathbb{A} : \overrightarrow{PQ} \in F\}.$$

We say F is the *director subspace of the subvariety* $P+F$. If $\dim F = m$, then $\dim(P+F) = m$. If $m = 1$, we say the subvariety is *line*. If $m = \dim \mathbb{A} - 1$, we say la subvariety is a *hyperplane*.

Proposition 4.102. Let $P + F$ be an affine subvariety of an affine space $\mathbb{A}$. Then if $Q \in P + F$, we have $P + F = Q + F$.

Definition 4.103. Two subvarieties $P+F$ and $Q+G$ are said to be *parallel* if $F \subseteq G$ or $G \subseteq F$.

Definition 4.104. Let Y, Z be two subvarieties of an affine space $\mathbb{A}$ such that $Y \cap Z \neq \varnothing$ and let F, G be their director subspaces, respectively. Then if $P \in Y \cap Z$, we have that $Y \cap Z$ is a subvariety of $\mathbb{A}$ and $Y \cap Z = P + F \cap G$.

Definition 4.105. Let $Y = P + F$, $Z = Q + G$ be two subvarieties of an affine space $\mathbb{A}$. We define its *sum* as the subvariety

$$Y + Z := P + (F + G + \langle \overrightarrow{PQ} \rangle)$$ [49].

Theorem 4.106 (Affine Graßmann formulas). Let $L_1 = P_1 + F_1$, $L_2 = P_2 + F_2$ be two subvarieties of an affine space $\mathbb{A}$. Then:

- If $L_1 \cap L_2 \neq \varnothing$,
  $$\dim(L_1 + L_2) = \dim L_1 + \dim L_2 - \dim(L_1 \cap L_2).$$
- If $L_1 \cap L_2 = \varnothing$,
  $$\dim(L_1 + L_2) = \dim L_1 + \dim L_2 - \dim(F_1 \cap F_2) + 1.$$

Coordinates and equations

Definition 4.107. An affine frame in an affine space $\mathbb{A}$ is a pair $\mathcal{R} = \{P; \mathcal{B}\}$ formed by a point $P \in \mathbb{A}$ and a basis $\mathcal{B}$ of V. The point P is called the *origin* of this affine frame.

Definition 4.108. Let $\mathcal{R} = \{P; \mathcal{B}\}$, $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$, be an affine frame in an affine space $\mathbb{A}$ and let $Q \in \mathbb{A}$. We define *affine coordinates of* Q as

$$Q = (\lambda_1, \ldots, \lambda_n) \iff \overrightarrow{PQ} = \lambda_1 \mathbf{v}_1 + \cdots + \lambda_n \mathbf{v}_n.$$

Proposition 4.109. Let $\mathbb{A}$ be an affine space and $P_0, \ldots, P_n \in \mathbb{A}$ be points satisfying the following equivalent properties:

1. The points are affinely independent.
2. There is no proper subvariety[50] containing all of them.
3. $P_0 + \cdots + P_n = \mathbb{A}$.
4. The vectors $\overrightarrow{P_0P_1}, \ldots, \overrightarrow{P_0P_n} \in V$ are linearly independent.

Then $\mathcal{R} = \{A_0; \overrightarrow{P_0P_1}, \ldots, \overrightarrow{P_0P_n}\}$ is an affine frame in $\mathbb{A}$.

Definition 4.110. Let $\{\lambda_0, \ldots, \lambda_n\}$ be homogeneous coordinates of a projective space $\mathcal{P}(V)$ and $(\mu_1, \ldots, \mu_n)$ affine coordinates of an affine space $\mathbb{A}$. We call *homogenization* the transformation of affine coordinates to homogeneous coordinates as follows:

$$(\mu_1, \ldots, \mu_n) \mapsto \{\mu_1, \ldots, \mu_n, 1\}.$$

Similarly, we call *dehomogenization* the transformation of homogeneous coordinates to affine coordinates as follows:

$$\{\lambda_0, \ldots, \lambda_n\} \mapsto \left(\frac{\lambda_0}{\lambda_n}, \ldots, \frac{\lambda_{n-1}}{\lambda_n}\right).$$

Definition 4.111. Let $\mathcal{R} = \{P; \mathcal{B}\}$, $\mathcal{B} = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$, be an affine frame in an affine space $\mathbb{A}$ and $L = Q + F$ be a subvariety of $\mathbb{A}$. Let $Q = (q_1, \ldots, q_n)$ be a point of $\mathbb{A}$ and $(\mathbf{v}_1, \ldots, \mathbf{v}_r)$ be a basis of F. We call *parametric equations of* L the equations

$$(x_1, \ldots, x_n) = (q_1, \ldots, q_n) + \sum_{i=1}^{r} \lambda_i \mathbf{v}_i.$$

If $\lambda_1, \ldots, \lambda_r \in K$ we get the coordinates of $(x_1, \ldots, x_n)$. If $\mathbf{v}_j = \sum_{i=1}^{n} \alpha_{ij} \mathbf{u}_i$, $j = 1, \ldots, r$ we can rearrange the parametric equations to get:

$$\begin{pmatrix} x_1 - q_1 \\ \vdots \\ x_n - q_n \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1r} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nr} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_r \end{pmatrix}.$$

The *Cartesian equations of* L are those obtained by equating to zero the minors of size $(r+1) \times (r+1)$ of the augmented matrix $(\alpha_{ij} \mid x_i - q_i)$.

Affinities

Definition 4.112. A function $f : \mathbb{A}_1 \to \mathbb{A}_2$ between two affine space over vector spaces V_1, V_2 is an *affinity* if there exists a linear function $\phi : V_1 \to V_2$ such that for all $P \in X$, $\mathbf{v} \in V_1$

$$f(P + \mathbf{v}) = f(P) + \phi(\mathbf{v})$$ [51].

We call the *differential of* f, denoted by $\mathrm{d}f$, the function ϕ.

Proposition 4.113. Let $f : \mathbb{A}_1 \to \mathbb{A}_2$ and $g : \mathbb{A}_2 \to \mathbb{A}_3$ be affinities. Then $g \circ f : \mathbb{A}_1 \to \mathbb{A}_3$ is an affinity and $\mathrm{d}(g \circ f) = \mathrm{d}g \circ \mathrm{d}f$.

Proposition 4.114. Let $f : \mathbb{A}_1 \to \mathbb{A}_2$ be an affinity and $P, Q \in \mathbb{A}_1$. Then

$$\mathrm{d}f(\overrightarrow{PQ}) = \overrightarrow{f(P)f(Q)}.$$

[49] As expected, $Y + F$ is the smallest subvariety containing $Y \cup Z$.
[50] A proper subvariety Y of $\mathbb{A}$ is a subvariety such that $Y \neq \varnothing$ and $Y \neq \mathbb{A}$.
[51] If ϕ is a semilinear map, then we say f is a *semiaffinity*.

Proposition 4.115. Let $f, g : \mathbb{A}_1 \to \mathbb{A}_2$ be affinities such that $f(P) = g(P)$ for some $P \in \mathbb{A}_1$ and $\mathrm{d}f = \mathrm{d}g$. Then, $f = g$.

Proposition 4.116. Let $f : \mathbb{A}_1 \to \mathbb{A}_2$ be an affinity and $\lambda_1, \ldots, \lambda_r$ such that $\lambda_1 + \cdots + \lambda_r = 1$. Then

$$f(\lambda_1 P_1 + \cdots + \lambda_r P_r) = \lambda_1 f(P_1) + \cdots + \lambda_r f(P_r).$$

Proposition 4.117. Let $f : \mathbb{A}_1 \to \mathbb{A}_2$ be an affinity and $L = P + F$ be a subvariety of $\mathbb{A}$. Then $f(P + F)$ is a subvariety of $\mathbb{A}$ and

$$f(P + F) = f(P) + \mathrm{d}f(F).$$

Proposition 4.118. Let $f : \mathbb{A}_1 \to \mathbb{A}_2$ be an affinity and $\mathcal{R}_1 = \{P_1; (\mathbf{u}_1, \ldots, \mathbf{u}_n)\}$, $\mathcal{R}_2 = \{P_2; (\mathbf{v}_1, \ldots, \mathbf{v}_m)\}$ be affine frames of $\mathbb{A}_1$, $\mathbb{A}_2$, respectively. If $x = (x_1, \ldots, x_n) \in \mathbb{A}_1$ and $y = (y_1, \ldots, y_n) \in \mathbb{A}_2$ then

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} \rho_1 \\ \vdots \\ \rho_m \end{pmatrix} + \mathbf{M} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

o, equivalently,

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \\ 1 \end{pmatrix} = \left(\begin{array}{ccc|c} & & & \rho_1 \\ & \mathbf{M} & & \vdots \\ & & & \rho_m \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbf{M}_{\mathcal{R}_1, \mathcal{R}_2}(f) \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}$$

where $\mathbf{M}$ is the matrix associated with $\mathrm{d}f$ and $(\rho_1, \ldots, \rho_m)$ are the coordinates of $\overrightarrow{P_2 f(P_1)}$ in the basis $(\mathbf{v}_1, \ldots, \mathbf{v}_m)$. Here, $\mathbf{M}_{\mathcal{R}_1, \mathcal{R}_2}(f)$ denote the matrix of f with respect to affine frames $\mathcal{R}_1$, $\mathcal{R}_2$.

Examples of affinities

Definition 4.119. Two affinities $f, g : \mathbb{A} \to \mathbb{A}$ are *similar* if there exist a bijective affinity $h : \mathbb{A} \to \mathbb{A}$ such that $h^{-1} f h = g$.

Proposition 4.120. Two affinities f, g are similar if there exist affine frames $\mathcal{R}$, $\mathcal{R}'$ such that $\mathbf{M}_{\mathcal{R}}(f) = \mathbf{M}_{\mathcal{R}'}(g)$.

Definition 4.121. A point $P \in \mathbb{A}$ is a *fixed point of* $f : \mathbb{A} \to \mathbb{A}$ if $f(P) = P$.

Definition 4.122. A linear subvariety $L = P + F \subset \mathbb{A}$ is *invariant under an affinity* $f : \mathbb{A} \to \mathbb{A}$ if $f(L) \subset L$.

Proposition 4.123. A linear subvariety $L = P + F \subset \mathbb{A}$ is invariant under an affinity $f : \mathbb{A} \to \mathbb{A}$ if and only if

1. $\mathrm{d}f(F) \subset F$.
2. $\overrightarrow{Pf(P)} \in F$.

In particular, a line $r = P + \langle \mathbf{v} \rangle$ is invariant under f if and only if

1. $\mathbf{v}$ is an eigenvector of $\mathrm{d}f$.
2. $\overrightarrow{Pf(P)} \in \langle \mathbf{v} \rangle$.

Proposition 4.124. If the set of fixed points of an affinity f, $\mathrm{Fix}(f)$, is non-empty, then $\mathrm{Fix}(f)$ is a subvariety.

Definition 4.125. Let f be an affinity. We define the *invariance level of* f, $\rho(f)$, as

$$\rho(f) = \min\{\dim L : f(L) \subset L \subset \mathbb{A}\} \in \{0, \ldots, \dim \mathbb{A}\}.$$

Definition 4.126 (Translations). Let $\mathbb{A}$ be an affine space and $\mathbf{v} \neq 0$. A *translation* with translation vector $\mathbf{v}$ is an affinity $T_{\mathbf{v}} : \mathbb{A} \to \mathbb{A}$ defined by $T_{\mathbf{v}} = P + \mathbf{v}$.

Proposition 4.127 (Properties of translations). Let $T_{\mathbf{v}}$ be a translation. Then:

1. $\mathrm{Fix}(T_{\mathbf{v}}) = \varnothing$.
2. Invariant lines are those with director subspace $\langle \mathbf{v} \rangle$.
3. If $\mathcal{R} = \{P; (\mathbf{v}_1, \ldots, \mathbf{v}_n)\}$ is an affine frame, then

$$\mathbf{M}_{\mathcal{R}}(T_{\mathbf{v}}) = \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & 1 \\ 0 & \ddots & \ddots & \vdots & 0 \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ \hline 0 & \cdots & 0 & 0 & 1 \end{array}\right).$$

4. All translations are similar and $\rho(T_{\mathbf{v}}) = 1$.

Definition 4.128 (Reflections). Let $\mathbb{A}$ be an affine space and suppose $\operatorname{char} K \neq 2$. Let $H = P + E$ be a hyperplane of $\mathbb{A}$ and let $\mathbf{v} \notin E$. The *reflection of* $\mathbf{v}$ *with respect to* H is the unique affinity $f : \mathbb{A} \to \mathbb{A}$ such that $f(P) = P$ for all $P \in H$ and $\mathrm{d}f(\mathbf{v}) = -\mathbf{v}$. Usually H is called the *mirror of the reflection* and $\mathbf{v}$ the *root of the reflection*.

Proposition 4.129 (Properties of reflections). Let f be a reflection with root $\mathbf{v}$ and mirror $H = P + E$. Then:

1. $\mathrm{Fix}(f) = H$.
2. Invariant lines are those contained on H and those with director subspace $\langle \mathbf{v} \rangle$.
3. If $\mathcal{R} = \{P; (\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}, \mathbf{v})\}$ is an affine frame such that $P \in H$ and $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1} \in E$, then

$$\mathbf{M}_{\mathcal{R}}(f) = \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & 0 \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & -1 & 0 \\ \hline 0 & \cdots & 0 & 0 & 1 \end{array}\right)$$

4. All reflections are similar and $\rho(f) = 0$.

Definition 4.130 (Projections). Let $\mathbb{A}$ be an affine space and H a hyperplane of $\mathbb{A}$ with director subspace E and let $\mathbf{v} \notin E$. The *projection over* H *in the direction of* $\mathbf{v}$ is the affinity $f : \mathbb{A} \to \mathbb{A}$ such that $f(P) = P$ for all $P \in H$ and $\mathrm{d}f(\mathbf{v}) = 0$.

Proposition 4.131 (Properties of projections). Let f be a projection over $H = P + E$ in the direction of $\mathbf{v}$. Then:

1. $\mathrm{Fix}(f) = H$.

2. Invariant lines are those contained on H.

3. If $\mathcal{R} = \{P; (\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}, \mathbf{v})\}$ is an affine frame such that $P \in H$ and $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1} \in E$, then

$$\mathbf{M}_{\mathcal{R}}(f) = \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & 0 \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & 0 & 0 \\ \hline 0 & \cdots & 0 & 0 & 1 \end{array}\right)$$

4. All projections are similar and $\rho(f) = 0$.

Definition 4.132 (Homotheties). An *homothety* is an affinity $f : \mathbb{A} \to \mathbb{A}$ such that $\mathrm{d}f = \lambda \mathrm{id}$, $\lambda \neq 0, 1$. This λ is called the *similitude ratio of the homothety.*

Proposition 4.133 (Properties of homotheties). Let f be an homothety of similitude ratio λ. Then:

1. f has a unique fixed.

2. If $\mathcal{R} = \{P; \mathcal{B}\}$ is an affine frame with $P \in \mathrm{Fix}(f)$ and $\mathcal{B}$ an arbitrary basis, then

$$\mathbf{M}_{\mathcal{R}}(f) = \left(\begin{array}{ccc|c} & & & 0 \\ & \lambda\mathbf{I} & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 1 \end{array}\right)$$

3. Two homotheties are similar if and only if they have the same similitude ratio. Moreover, $\rho(f) = 0$.

Proposition 4.134. Let $T_{\mathbf{w}}$ be a translation and R a reflection with root $\mathbf{v}$ with respect to the hyperplane $H = P + E$. Let $f = T_{\mathbf{w}} \circ R$. We take an affine frame $\mathcal{R} = \{P; (\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}, \mathbf{v})\}$ such that $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1} \in E$. Then if $\mathbf{w} = (w_1, \ldots, w_n)$ in this frame we have,

$$\mathbf{M}_{\mathcal{R}}(f) = \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & w_1 \\ 0 & \ddots & \ddots & \vdots & w_2 \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & -1 & w_n \\ \hline 0 & \cdots & 0 & 0 & 1 \end{array}\right)$$

1. If $\mathbf{w} \in \langle \mathbf{v} \rangle \implies w_1 = \cdots = w_{n-1} = 0$ and therefore f is a reflection with mirror the hyperplane $2x_n = w_n$.

2. If $\mathbf{w} \notin \langle \mathbf{v} \rangle$ we say f is a *glide reflection*. In this case, if $\mathbf{w} = w_n\mathbf{v} + \mathbf{u}$ with $\mathbf{u} \in E$ and we take $\mathcal{R} = (P + \frac{w_n}{2}\mathbf{v}; (\mathbf{u}, \mathbf{u}_2 \ldots, \mathbf{u}_{n-1}, \mathbf{v}))$, then

$$\mathbf{M}_{\mathcal{R}}(f) = \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & 1 \\ 0 & \ddots & \ddots & \vdots & 0 \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & -1 & 0 \\ \hline 0 & \cdots & 0 & 0 & 1 \end{array}\right).$$

The invariance level of glide reflections is $\rho(f) = 1$.

Fundamental theorem of affine geometry

Definition 4.135 (Simple ratio). Let $A, B, C \in \mathbb{A}$ be three different collinear points. The *simple ratio of* A, B, C is the unique scalar $\lambda := (A, B, C) \in K$ such that

$$\overrightarrow{AB} = \lambda \overrightarrow{AC}.$$

Theorem 4.136 (Fundamental theorem of affine geometry). Let $f : \mathbb{A} \to \mathbb{A}$ be a collineation of an affine space of dimension $n \geq 2$ over the field K with more than two elements. Then f is a semiaffinity.

Proposition 4.137. Two affinities $f, g : \mathbb{A} \to \mathbb{A}$ are similar if and only if

1. $\mathrm{d}f$ and $\mathrm{d}g$ are similar.

2. $\rho(f) = \rho(g)$.

Theorem 4.138. Let $f : \mathbb{A} \to \mathbb{A}$ be an affinity and $P \in \mathbb{A}$ a point. Let $\mathbf{v} := \overrightarrow{Pf(P)}$. Then

$$\rho(f) = \min\{r : (\mathrm{d}f - \mathrm{id})^r(\mathbf{v}) \in \mathrm{im}(\mathrm{d}f - \mathrm{id})^{r+1}\}.$$

Corollary 4.139. If f is a affinity and 1 is not an eigenvector of $\mathrm{d}f$, then $\rho(f) = 0$.

Euclidean affine spaces

Definition 4.140. An *Euclidean affine space* is an affine space such that the associated vector space is an Euclidean vector space[52].

Definition 4.141. Let $\mathbb{A}$ be an Euclidean affine space. We define the *distance between two points* $P, Q \in \mathbb{A}$ as

$$d(A, B) := \|\overrightarrow{AB}\|.$$

We define the *segment delimited by* A *and* B as

$$\{P \in \mathbb{A} : P = \lambda A + (1 - \lambda)B, \lambda \in [0, 1]\}.$$

Proposition 4.142. Let $\mathbb{A}$ be an Euclidean affine space. Then the following properties are satisfied:

1. $d(A, C) \leq d(A, B) + d(B, C)$ *(Triangular inequality).*

If ABC is a right triangle with right angle at A, then:

2. $d(B, C)^2 = d(A, B)^2 + d(A, C)^2$ *(Pythagorean theorem).*

Definition 4.143. Two subvarieties $L_1 = P_1 + F_1$, $L_2 = P_2 + F_2$ of an Euclidean affine space $\mathbb{A}$ are *orthogonal*, $L_1 \perp L_2$, if $F_1 \perp F_2$[53].

Definition 4.144. Let $L_1 = P_1 + F_1$, $L_2 = P_2 + F_2$ be two subvarieties of an Euclidean affine space $\mathbb{A}$. We define the *distance between two affine subvarieties* as

$$d(L_1, L_2) := \inf\{d(A_1, A_2) : A_1 \in L_1, A_2 \in L_2\}.$$

Theorem 4.145. Let $L_1 = P_1 + F_1$, $L_2 = P_2 + F_2$ be two subvarieties of an Euclidean affine space $\mathbb{A}$. Let $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2 \in F_1 + F_2$, with $\mathbf{u}_i \in F_i$, and $\mathbf{v} \in (F_1 + F_2)^{\perp}$ such that $\overrightarrow{P_1P_2} = \mathbf{u} + \mathbf{v}$. Then we have

$$d(L_1, L_2) = \|\mathbf{v}\| = d(P_1 + \mathbf{u}_1, P_2 - \mathbf{u}_2).$$

[52] Remember definition 2.186.
[53] Remember definition 2.174.

Euclidean motions

Definition 4.146. Let $\mathbb{A}$ be an Euclidean affine space. A function $f : \mathbb{A} \to \mathbb{A}$ is an *Euclidean motion* if

$$d(f(A), f(B)) = d(A, B) \quad \forall P, Q \in \mathbb{A}.$$

Proposition 4.147. Let $\mathbb{A}$ be an Euclidean affine space. $f : \mathbb{A} \to \mathbb{A}$ is an Euclidean motion if and only if f is a affinity and $\mathrm{d}f$ is a isometry[54].

Proposition 4.148 (Examples of Euclidean motions).

- Any translation $T_{\mathbf{v}}$ is an Euclidean motion. Moreover, $T_{\mathbf{u}} \sim T_{\mathbf{v}}$ (as Euclidean motions) if and only if $\|\mathbf{u}\| = \|\mathbf{v}\|$.
- An homothety f of similitude ratio λ is an Euclidean motion if and only if $\lambda = -1$. Moreover, all homotheties are similar as Euclidean motions.
- A reflection f of mirror $H = Q + E$ and root $\mathbf{v}$ is an Euclidean motion if and only if $\langle \mathbf{v} \rangle \perp E$. These reflections are called *orthogonal reflections*. If $\mathbf{n}$ is a unit normal vector to the mirror, then the orthogonal reflection is given by
$$f(P) = P - 2\langle \overrightarrow{QP}, \mathbf{n} \rangle \mathbf{n}.$$
- *Glide orthogonal reflections* are Euclidean motions.
- A rotation on the affine plane is an Euclidean motion, whose differential is a rotation of an angle other than zero. This affinity has a unique fixed point and if we take this point as a reference, its matrix in this frame will be
$$\begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Classification of Euclidean motions

Theorem 4.149 (Classification of isometries).

1. Two isometries are similar if and only if they have the same characteristic polynomial.
2. For any isometry, there exists an orthonormal basis in which the matrix associated with the isometry is of the form
$$\begin{pmatrix} I_r & & & & \\ & -I_s & & & \\ & & R_1 & & \\ & & & \ddots & \\ & & & & R_t \end{pmatrix}$$
where $r, s, t \geq 0$, I_m denote the identity matrix of size $m \times m$ and each R_i is a rotation with matrix
$$R_i = \begin{pmatrix} \cos\alpha_i & -\sin\alpha_i \\ \sin\alpha_i & \cos\alpha_i \end{pmatrix}.$$
with $\alpha_i \neq 0, \pi$ for $i = 1, \ldots, t$.

Definition 4.150. Let $P \in \mathbb{A}$ be a point of an Euclidean affine space and $f : \mathbb{A} \to \mathbb{A}$ be an Euclidean motion. Express the vector $\overrightarrow{Pf(P)}$ as

$$\overrightarrow{Pf(P)} = \mathbf{u} + \mathbf{v} \quad \mathbf{u} \in \ker(\mathrm{d}f - \mathrm{id}), \mathbf{v} \in \mathrm{im}(\mathrm{d}f - \mathrm{id}).$$

Then $\mathbf{u}_f := \mathbf{u}$ is the *glide vector of* f.

Proposition 4.151. The glide vector $\mathbf{u}_f$ has the following properties:

- $\mathrm{d}f(\mathbf{u}_f) = \mathbf{u}_f$.
- $\mathbf{u}_f$ does not depend on the point P.
- If $\mathbf{u}_f = 0 \implies \rho(f) = 0$. Otherwise, $\rho(f) = 1$.

Theorem 4.152 (Classification of Euclidean motions). Two Euclidean motions $f, g : \mathbb{A} \to \mathbb{A}$ are similar (as Euclidean motions) if and only if $\mathrm{d}f \sim \mathrm{d}g$ (as isometries) and $\|\mathbf{u}_f\| = \|\mathbf{u}_g\|$.

1.2.4.4 | Quadrics

Quadrics

Definition 4.153. Let $\mathbb{A}$ an affine space of dimension n over a field K. A *quadric in* $\mathbb{A}$ is a polynomial of degree 2 with n variables, $p(x_1, \ldots, x_n)$, and coefficients in the field K modulo the equivalence relation

$$p(x_1, \ldots, x_n) \sim \lambda p(x_1, \ldots, x_n) \quad \text{if } \lambda \in K, \lambda \neq 0.$$

The *points of the quadric* $p(x_1, \ldots, x_n)$ are

$$\{(a_1, \ldots, a_n) \in \mathbb{A} : p(a_1, \ldots, a_n) = 0\}.$$

Definition 4.154. A *conic* is a quadric in a 2-dimensional space.

Definition 4.155. Two quadrics p, q of an affine space $\mathbb{A}$ are *equivalent* if there exists a bijective affinity $f : \mathbb{A} \to \mathbb{A}$ such that $f(p) = q$.

Definition 4.156. Let $\mathcal{P}_n(K)$ be a projective space of dimension n over a field K. A *quadric in* $\mathcal{P}_n(K)$ is a homogeneous polynomial of degree 2 with $n+1$ variables, $p(x_1, \ldots, x_{n+1})$, and coefficients in the field K modulo the equivalence relation

$$p(x_1, \ldots, x_{n+1}) \sim \lambda p(x_1, \ldots, x_{n+1}) \quad \text{if } \lambda \in K, \lambda \neq 0.$$

The *points of the quadric* $p(x_1, \ldots, x_{n+1})$ are

$$\{(a_1, \ldots, a_{n+1}) \in \mathcal{P}_n(K) : p(a_1, \ldots, a_{n+1}) = 0\}.$$

Definition 4.157. Two quadrics p, q in $\mathcal{P}_n(K)$ are *equivalent* if there exists a homography $f : \mathcal{P}_n(K) \to \mathcal{P}_n(K)$ such that $f(p) = q$.

Theorem 4.158. There is a bijective correspondence between quadrics of K^n and quadrics of $\mathcal{P}_n(K)$ not divisible by x_{n+1}. Thus, the points of the affine quadric are the points of the projective quadric that are in the affine space[55].

[54] Remember definition 2.177. From this we deduce that if $\mathbf{A} \in \mathcal{M}_n(K)$ is the matrix associated with an isometry, then $\mathbf{A}\mathbf{A}^{\mathrm{T}} = \mathbf{I}_n$.

[55] Nevertheless, observe that two equivalent projective quadrics as projective quadrics may not be equivalent as affine quadrics.

Proposition 4.159. Let $\mathbb{A}$ be an affine space and $\mathcal{P}_n(K)$ a projective space, both of dimension n and over a field K. Let p be a quadric.

- *Homogenization*: If $p(x_1,\ldots,x_n)\in\mathbb{A}$, then:
$$p(x_1,\ldots,x_n)\mapsto x_{n+1}^2 p\left(\frac{x_1}{x_{n+1}},\ldots,\frac{x_n}{x_{n+1}}\right)\in\mathcal{P}_n(K)$$
- *Dehomogenization*: If $p(x_1,\ldots,x_{n+1})\in\mathcal{P}_n(K)$, then:
$$p(x_1,\ldots,x_{n+1})\mapsto p(x_1,\ldots,x_n,1)\in\mathbb{A}$$

Four points of view of quadrics

Definition 4.160. We say a bilinear form is *anisotropic* or *elliptic* if the unique isotropic vector[56] is the null vector.

Theorem 4.161. There is, expect for equivalence, only one symmetric bilinear form of dimension 2 such that it is non-singular[57] and non-elliptic. We call this bilinear form *hyperbolic plane.*

Definition 4.162. Let $\varphi: V\times V\to K$ a symmetric bilinear form. We define the *quadratic form associated with* φ as
$$\begin{aligned} q: V &\longrightarrow K\\ \mathbf{u} &\longmapsto \varphi(\mathbf{u},\mathbf{u})\end{aligned}$$
This function clearly satisfies:

1. $q(\lambda\mathbf{u})=\lambda^2\mathbf{u}$.
2. $\varphi(\mathbf{u},\mathbf{v})=\dfrac{1}{2}\left(q(\mathbf{u}+\mathbf{v})-q(\mathbf{u})-q(\mathbf{v})\right)$.

Proposition 4.163. Two symmetric bilinear forms φ_1, φ_2 over V are equivalent if there exists an isomorphism $\phi: V\to V$ such that $\varphi_1(\mathbf{u},\mathbf{v})=\varphi_2(\phi(\mathbf{u}),\phi(\mathbf{v}))\ \forall\mathbf{u},\mathbf{v}\in V$. Two quadratic forms q_1,q_2 over V are equivalent if there exists an isomorphism $\phi: V\to V$ such that $q_1(\mathbf{u})=q_2(\phi(\mathbf{u}))\ \forall\mathbf{u}\in V$.

Theorem 4.164. Symmetric bilinear forms, quadratic forms, symmetric matrices and homogeneous polynomials of degree 2 are equivalents ways to study quadrics.

Definition 4.165. A quadric is *non-degenerate* if its associated quadratic form is non-singular.

Classification of quadratic forms and quadrics

Definition 4.166. A *quadratic space* is a pair (V,q) where V is a vector space over a field K and q is a quadratic form.

Definition 4.167. Let $E_1=(V_1,q_1)$ and $E_2=(V_2,q_2)$ be two quadratic spaces. An *isometry between* E_1 *and* E_2, $E_1\cong E_2$, is an isomorphism $\phi: V_1\to V_2$ such that $q_1(\mathbf{v})=q_2(\phi(\mathbf{v}))\ \forall\mathbf{v}\in V$.

Definition 4.168. Let (V,q) be a quadratic space. (V,q) is *totally isotropic* if all its vectors are isotropic.

Definition 4.169. Let (V,q) be a quadratic space. We define the *rank of* (V,q) as
$$\rho(V):=\dim V-\dim\operatorname{Rad}(V)^{58}.$$

Theorem 4.170 (Witt's theorem). Let E be a quadratic space and suppose that $E=E_1\perp F_1=E_2\perp F_2$. If $E_1\cong E_2$, then $F_1\cong F_2$.

Definition 4.171. Let (V,q) be a quadratic space. We define the *index of* (V,q) as
$$\iota(V):=\max\{\dim F: F\subseteq V\text{ and }F\text{ is totally isotropic}\}.$$

Theorem 4.172. Let $E\subseteq V$ a totally isotropic subspace of maximum dimension and $(\mathbf{u}_1,\ldots,\mathbf{u}_r)$ a basis of E (therefore, $r=\iota(V)$). Then, there exist vectors $\mathbf{v}_1,\ldots,\mathbf{v}_r\in V$ such that each $H_i:=\langle\mathbf{u}_i,\mathbf{v}_i\rangle$ is an hyperbolic plane and $V=H_1\perp\cdots\perp H_r\perp F$, where F is anisotropic.

Proposition 4.173. Let (V,q) be a quadratic space and M be the associated matrix of q. Then $\dim V$, $\rho(V)$, $\iota(V)$ and $\det M$ modulo squares[59] are invariant under isometries.

Theorem 4.174 (Classification of quadratic forms in $\mathbb{C}$). If $K=\mathbb{C}$, two quadratic forms are equivalent if and only if they have the same rank. All quadratic forms of rank r are equivalent to
$$x_1^2+\cdots+x_r^2.$$

Theorem 4.175 (Classification of quadratic forms in $\mathbb{F}_q$). If $K=\mathbb{F}_q$ with q odd, all quadratic form of rank n are equivalent to either of these two diagonal forms:
$$\begin{gathered}x_1^2+\cdots+x_n^2,\\ x_1^2+\cdots+x_{n-1}^2+\nu x_n^2,\end{gathered}$$
where ν in not a square. Moreover, two quadratic forms are equivalent if and only if they have the same rank and determinant (modulo squares).

Theorem 4.176 (Classification of quadratic forms in $\mathbb{R}$). If $K=\mathbb{R}$, all quadratic forms of rang r are equivalent to the diagonal form
$$\pm x_1^2\pm\cdots\pm x_r^2.$$
If we denote by r^+ the number of positive signs and by r^- the number of negative signs, then two quadratic forms are equivalents if and only if they have the same values (r^+,r^-).

Theorem 4.177 (Classification of projective quadrics in $\mathbb{C}$). If $K=\mathbb{C}$, two projective quadrics are equivalents if and only if they have the same rank.

[56] Remember definition 2.164.
[57] Remember definition 2.168.
[58] If A is the associated matrix of q, we have $\operatorname{rank}A=\rho(V)$.
[59] That is, if (V_1,q_1), (V_1,q_1) are two quadratic spaces and $\mathbf{M}_i$, $i=1,2$, are the associated matrices to q_1, q_2, respectively, we have $\det\mathbf{M}_1=a^2\det\mathbf{M}_2$, for some $a\in K$.

Theorem 4.178 (Classification of projective quadrics in $\mathbb{F}_q$). If $K = \mathbb{F}_q$, there are (except of equivalence) this projective quadrics in each rank n:

- If n is odd:
$$x_1^2 + \cdots + x_n^2.$$
- If n is even:
$$x_1^2 + \cdots + x_n^2,$$
$$x_1^2 + \cdots + x_{n-1}^2 + \nu x_n^2,$$
where ν in not a square.

Theorem 4.179 (Classification of projective quadrics in $\mathbb{R}$). If $K = \mathbb{R}$, two projective quadrics are equivalents if they have the same rank and index.

Theorem 4.180 (Classification of affine quadrics). Let q_1, q_2 be two affine quadrics and for $i = 1, 2$ let q_i^∞ be the quadric q_i restricted to the hyperplane "at infinity" H, that is, restricted to the hyperplane $x_{n+1} = 0$. In these conditions, $q_1 \sim q_2$ if and only if:

1. $q_1 \sim q_2$ as projective quadrics, that is, in $P_n(K)$.
2. $q_1^\infty \sim q_2^\infty$ as quadrics in $H \cong P_{n-1}(K)$.

1.2.5 Mathematical analysis

1.2.5.1 | Numeric series

Series convergence

Definition 5.1. Let (a_n) be a sequence of real numbers. A *numeric series* is an expression of the form

$$\sum_{n=1}^{\infty} a_n.$$

We call a_n *general term of the series* and $S_N = \sum_{n=1}^{N} a_n$, for all $N \in \mathbb{N}$, *N-th partial sum of the series*[60].

Definition 5.2. We say the series $\sum a_n$ is *convergent* if the sequence of partial sums is convergent, that is, if $S = \lim_{N\to\infty} S_N$ exist and it's finite. In that case, S is called the *sum of the series*. If the previous limit doesn't exists or it is infinite we say the series is *divergent*[61].

Proposition 5.3. Let (a_n) be a sequence such that $\sum a_n < \infty$. Then $\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}$ such that

$$\left|\sum_{n=1}^{N} a_n - \sum_{n=1}^{\infty} a_n\right| < \varepsilon$$

if $N \geq n_0$.

Theorem 5.4 (Cauchy's test). Let (a_n) be a sequence. $\sum a_n < \infty$ if and only if $\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N}$ such that

$$\left|\sum_{n=N}^{M} a_n\right| < \varepsilon$$

if $M \geq N \geq n_0$.

Corollary 5.5. Changing a finite number of terms in a series has no effect on the convergence or divergence of the series.

Corollary 5.6. If $\sum a_n < \infty$, then $\lim_{n\to\infty} a_n = 0$.

Theorem 5.7 (Linearity). Let $\sum a_n, \sum b_n$ be two convergent series with sums A and B respectively and let λ be a real number. The series

$$\sum_{n=1}^{\infty} (a_n + \lambda b_n)$$

is convergent and has sum $A + \lambda B$.

Theorem 5.8 (Associative property). Let $\sum a_n$ be a convergent series with sum A. Suppose (n_k) is a strictly increasing sequence of natural numbers. The series $\sum b_n$, with $b_k = a_{n_{k-1}+1} + \cdots + a_{n_k}$ for all $i \in \mathbb{N}$, is convergent and its sum is A.

Non-negative terms series

Theorem 5.9. Let $\sum a_n$ be a series of non-negative terms $a_n \geq 0$[62]. The series converges if and only if the sequence (S_N) of partial sums is bounded.

Theorem 5.10 (Comparison test). Let $(a_n), (b_n) \geq 0$ be two sequences of real numbers. Suppose that exists a constant $C > 0$ and a number $n_0 \in \mathbb{N}$ such that $a_n \leq C b_n$ for all $n \geq n_0$.

1. If $\sum b_n < \infty \implies \sum a_n < \infty$.
2. If $\sum a_n = +\infty \implies \sum b_n = +\infty$.

Theorem 5.11 (Limit comparison test). Let (a_n), $(b_n) \geq 0$ be two sequences of real numbers. Suppose that the limit $\ell = \lim_{n\to\infty} \frac{a_n}{b_n}$ exists.

1. If $0 < \ell < \infty \implies \sum a_n < \infty \iff \sum b_n < \infty$.
2. If $\ell = 0$ and $\sum b_n < \infty \implies \sum a_n < \infty$.
3. If $\ell = \infty$ and $\sum a_n < \infty \implies \sum b_n < \infty$.

Theorem 5.12 (Root test). Let $(a_n) \geq 0$. Suppose that the limit $\ell = \lim_{n\to\infty} \sqrt[n]{a_n}$ exists.

1. If $\ell < 1 \implies \sum a_n < \infty$.
2. If $\ell > 1 \implies \sum a_n = +\infty$.

Theorem 5.13 (Ratio test). Let $(a_n) \geq 0$. Suppose that the limit $\ell = \lim_{n\to\infty} \frac{a_{n+1}}{a_n}$ exists.

1. If $\ell < 1 \implies \sum a_n < \infty$.
2. If $\ell > 1 \implies \sum a_n = +\infty$.

Theorem 5.14 (Raabe's test). Let $(a_n) \geq 0$. Suppose that the limit $\ell = \lim_{n\to\infty} n\left(1 - \frac{a_{n+1}}{a_n}\right)$ exists.

1. If $\ell > 1 \implies \sum a_n < \infty$.
2. If $\ell < 1 \implies \sum a_n = +\infty$.

Theorem 5.15 (Condensation test). Let $(a_n) \geq 0$ be a decreasing sequence. Then:

$$\sum a_n < \infty \iff \sum 2^n a_{2^n} < \infty.$$

Theorem 5.16 (Logarithmic test). Let $(a_n) \geq 0$. Suppose that the limit $\ell = \lim_{n\to\infty} \frac{\log \frac{1}{a_n}}{\log n}$ exists.

1. If $\ell > 1 \implies \sum a_n < \infty$.
2. If $\ell < 1 \implies \sum a_n = +\infty$.

[60] From now on we will write $\sum a_n$ to refer $\sum_{n=1}^{\infty} a_n$.

[61] We will use the notation $\sum a_n < \infty$ or $\sum a_n = +\infty$ to express that the series converges or diverges, respectively.

[62] Obviously the following results are also valid if the series is of non-positive terms or has a finite number of negative or positive terms.

Theorem 5.17 (Integral test). Let $f : [1, \infty) \to (0, \infty)$ be a decreasing function. Then:

$$\sum f(n) < \infty \iff$$
$$\iff \exists C > 0 \text{ such that } \int_1^n f(x)\mathrm{d}x \le C \ \forall n.$$

Alternating series

Definition 5.18. An *alternating series* is a series of the form $\sum (-1)^n a_n$, with $(a_n) \ge 0$.

Theorem 5.19 (Leibnitz's test). Let $(a_n) \ge 0$ be a decreasing sequence such that $\lim_{n\to\infty} a_n = 0$. Then, $\sum (-1)^n a_n$ is convergent.

Theorem 5.20 (Abel's summation formula). Let $(a_n), (b_n)$ be two sequences of real numbers. Then,

$$\sum_{n=N}^{M} a_n(b_{n+1} - b_n) = a_{M+1}b_{M+1} - a_N b_N -$$
$$- \sum_{n=N}^{M} b_{n+1}(a_{n+1} - a_n).$$

Theorem 5.21 (Dirichlet's test). Let $(a_n), (b_n)$ be two sequences of real numbers such that:

1. $\exists C > 0$ such that $\left|\sum_{n=1}^{N} a_n\right| \le C$ for all $N \in \mathbb{N}$.
2. (b_n) is monotone and $\lim_{n\to\infty} b_n = 0$.

Then, $\sum a_n b_n$ is convergent.

Theorem 5.22 (Abel's test). Let $(a_n), (b_n)$ be two sequences of real numbers such that:

1. The series $\sum a_n$ is convergent.
2. (b_n) is monotone and bounded.

Then, $\sum a_n b_n$ is convergent.

Absolute convergence and rearrangement of series

Definition 5.23. We say a series $\sum a_n$ is *absolutely convergent* if $\sum |a_n|$ is convergent.

Theorem 5.24. If a series converges absolutely, it converges.

Definition 5.25. We say a sequence (b_n) is a *rearrangement of the sequence* (a_n) if exists a bijective map $\sigma : \mathbb{N} \to \mathbb{N}$ such that $b_n = a_{\sigma(n)}$. A *rearrangement of the series* $\sum a_n$ is the series $\sum a_{\sigma(n)}$ for some bijection $\sigma : \mathbb{N} \to \mathbb{N}$.

Definition 5.26. Let $x \in \mathbb{R}$. We define the *positive part of* x as

$$x^+ = \begin{cases} x & \text{si } x \ge 0 \\ 0 & \text{si } x < 0 \end{cases}$$

Analogously, we define the *negative part of* x as

$$x^- = \begin{cases} 0 & \text{si } x \ge 0 \\ -x & \text{si } x < 0 \end{cases}$$

Note that we can write $x = x^+ - x^-$ and $|x| = x^+ + x^-$.

Theorem 5.27. A series $\sum a_n$ is absolutely convergent if and only if positive and negative terms series, $\sum a_n^+$ and $\sum a_n^-$, converge. In this case,

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} a_n^+ - \sum_{n=1}^{\infty} a_n^-.$$

Theorem 5.28. Let $\sum a_n$ be an absolutely convergent series. Then, for all bijection $\sigma : \mathbb{N} \to \mathbb{N}$, the rearranged series $\sum a_{\sigma(n)}$ is absolutely convergent and $\sum a_n = \sum a_{\sigma(n)}$.

Theorem 5.29 (Riemann's theorem). Let $\sum a_n$ be a convergent series but not absolutely convergent. Then, $\forall \alpha \in \mathbb{R} \cup \{\infty\}$, there exists a bijective map $\sigma : \mathbb{N} \to \mathbb{N}$ such that $\sum a_{\sigma(n)}$ converges and $\sum a_{\sigma(n)} = \alpha$.

Theorem 5.30. A series $\sum a_n$ is absolutely convergent if and only if any rearranged series converges to the same value of $\sum a_n$.

1.2.5.2 | Sequences and series of functions

Sequences of functions

Definition 5.31. Let $D \subseteq \mathbb{R}$. A set

$$(f_n(x)) = \{f_1(x), f_2(x), \ldots, f_n(x), \ldots\}$$

is a *sequence of real functions* if $f_i : D \to \mathbb{R}$ is a real-valued function. In this case we say the sequence $(f_n(x))$, or simply (f_n), is well-defined on D.

Definition 5.32. Let (f_n) be a sequence of functions defined on $D \subseteq \mathbb{R}$ and $f : D \to \mathbb{R}$. We say (f_n) *converges pointwise to* f *on* D if $\forall x \in D$, $\lim_{n\to\infty} f_n(x) = f(x)$

Definition 5.33. Let (f_n) be a sequence of functions defined on $D \subseteq \mathbb{R}$ and $f : D \to \mathbb{R}$. We say (f_n) *converges uniformly to* f *on* D if $\forall \varepsilon > 0$, $\exists n_0 : |f_n(x) - f(x)| < \varepsilon$ $\forall n \ge n_0$ and $\forall x \in D$.

Lemma 5.34. Let (f_n) be an uniform convergent sequence of functions defined on $D \subseteq \mathbb{R}$ and let f be a function such that (f_n) converges pointwise to f. Then, (f_n) converges uniformly f on D.

Lemma 5.35. Let (f_n) be a sequence of functions defined on $D \subseteq \mathbb{R}$. (f_n) converges uniformly a f en D if and only if $\lim_{n\to\infty} \sup\{|f_n(x) - f(x)| : x \in D\} = 0$.

Corollary 5.36. A sequence of functions (f_n) converges uniformly to f on $D \subseteq \mathbb{R}$ if and only if there is a sequence (a_n), with $a_n \ge 0$ and $\lim_{n\to\infty} a_n = 0$, and a number $n_0 \in \mathbb{N}$ such that $\sup\{|f_n(x) - f(x)| : x \in D\} \le a_n$, $\forall n \ge n_0$.

Theorem 5.37 (Cauchy's test). A sequence of functions (f_n) converges uniformly to f on $D \subseteq \mathbb{R}$ if and only if $\forall \varepsilon > 0$ $\exists n_0 : \sup\{|f_n(x) - f_m(x)| : x \in D\} < \varepsilon$ if $n, m \ge n_0$.

Theorem 5.38. Let (f_n) be a sequence of continuous functions defined on $D \subseteq \mathbb{R}$. If (f_n) converges uniformly to f on D, then f is continuous on D, that is, for any $x_0 \in D$, it satisfies:

$$\lim_{n\to\infty}\left(\lim_{x\to x_0} f_n(x)\right) = \lim_{x\to x_0} f(x).$$

Theorem 5.39. Let (f_n) be a sequence of functions defined on $I = [a, b] \subseteq \mathbb{R}$. If (f_n) are Riemann-integrable on I and (f_n) converges uniformly to f on I, then f is Riemann-integrable on I and

$$\int_a^b \lim_{n\to\infty} f_n(x)\mathrm{d}x = \lim_{n\to\infty}\int_a^b f_n(x)\mathrm{d}x.$$

Theorem 5.40. Let (f_n) be a sequence of functions defined on $I = (a, b) \subset \mathbb{R}$. If (f_n) are derivable on I, $(f_n'(x))$ converges uniformly on I and $\exists x_0 \in I : \lim\limits_{n\to\infty} f_n(x_0) \in \mathbb{R}$, then there is a function f such that (f_n) converges uniformly to f on I, f is derivable on I and $(f_n'(x))$ converges uniformly to f' on I.

Series of functions

Definition 5.41. Let (f_n) be a sequence of functions defined on $D \subseteq \mathbb{R}$. The expression

$$\sum_{n=1}^{\infty} f_n(x)$$

is the *series of functions associated with* (f_n).

Definition 5.42. A series of functions $\sum f_n(x)$ defined on $D \subseteq \mathbb{R}$ *converges pointwise on* D if the sequence of partials sums

$$F_N(x) = \sum_{n=1}^{N} f_n(x)$$

converges pointwise. If the pointwise limit of (F_N) is $F(x)$, we say F is the *sum of the series in a pointwise sense.*

Definition 5.43. A series of functions $\sum f_n(x)$ defined on $D \subseteq \mathbb{R}$ *converges uniformly on* D if the sequence of partials sums

$$F_N(x) = \sum_{n=1}^{N} f_n(x)$$

converges uniformly. If the uniform limit of (F_N) is $F(x)$, we say F is the *sum of the series in an uniform sense.*

Theorem 5.44 (Cauchy's test). A series of functions $\sum f_n(x)$ defined on $D \subseteq \mathbb{R}$ converges uniformly if and only if $\forall \varepsilon > 0\ \exists n_0$ such that

$$\sup\left\{\left|\sum_{n=N}^{M} f_n(x)\right| : x \in D\right\} < \varepsilon$$

if $M \geq N \geq n_0$.

Corollary 5.45. If $\sum f_n(x)$ is a series of continuous functions on $D \subseteq \mathbb{R}$, then (f_n) converges uniformly to zero on D.

Theorem 5.46. If $\sum f_n(x)$ is uniformly convergent series of functions on $D \subseteq \mathbb{R}$, then its sum function is also continuous on D.

Theorem 5.47. Let (f_n) be a sequence of functions defined on $I = [a, b] \subseteq \mathbb{R}$. If (f_n) are Riemann-integrable on I and $\sum f_n(x)$ converges uniformly on I, then $\sum f_n(x)$ is Riemann-integrable on I and

$$\int_a^b \sum_{n=1}^{\infty} f_n(x)\mathrm{d}x = \sum_{n=1}^{\infty}\int_a^b f_n(x)\mathrm{d}x.$$

Theorem 5.48. Let (f_n) be a sequence of functions defined on $I = (a, b) \subset \mathbb{R}$. If (f_n) are derivable on I, $\sum f_n'(x)$ converges uniformly on I and $\exists c \in I : \sum f_n(c) < \infty$, then $\sum f_n(x)$ converges uniformly on I, $\sum f_n(x)$ is derivable on I and

$$\left(\sum_{n=1}^{\infty} f_n(x)\right)' = \sum_{n=1}^{\infty} f_n'(x).$$

Theorem 5.49 (Weierstraß M-test). Let (f_n) be a sequence of functions defined on $D \subseteq \mathbb{R}$ such that $|f_n(x)| \leq M_n\ \forall x \in D$ and suppose that $\sum M_n$ is a convergent numeric series. Then, $\sum f_n(x)$ is converges uniformly on D.

Theorem 5.50 (Dirichlet's test). Let $(f_n), (g_n)$ be two sequences of functions defined on $D \subseteq \mathbb{R}$. Suppose:

1. $\exists C > 0 : \sup\left\{\left|\sum_{n=1}^{N} f_n(x)\right| : x \in D\right\} \leq C,\ \forall N.$
2. $(g_n(x))$ is a monotone sequence for all $x \in D$ and $\lim\limits_{n\to\infty} \sup\{|g_n(x)| : x \in D\} = 0$.

Then, $\sum f_n(x)g_n(x)$ converges uniformly on D.

Theorem 5.51 (Abel's test). Let $(f_n), (g_n)$ be two sequences of functions defined on $D \subseteq \mathbb{R}$. Suppose:

1. The series $\sum f_n(x)$ converges uniformly on D.
2. $(g_n(x))$ is a monotone and bounded sequence for all $x \in D$.

Then, $\sum f_n(x)g_n(x)$ converges uniformly on D.

Power series

Definition 5.52. Let (a_n) be a sequence of real numbers and $x_0 \in \mathbb{R}$. A *power series centred on* x_0 is a series of functions of the form

$$\sum_{n=0}^{\infty} a_n(x - x_0)^n.$$

Proposition 5.53. Let $\sum a_n(x - x_0)^n$ be a power series. Suppose there exists an $x_1 \in \mathbb{R}$ such that $\sum a_n(x_1 - x_0)^n < \infty$. Then, $\sum a_n(x - x_0)^n$ converges uniformly on any closed interval $I \subset A = \{x \in \mathbb{R} : |x - x_0| < |x_1 - x_0|\}$.

Theorem 5.54. Let $\sum a_n(x - x_0)^n$ be a power series and consider

$$R = \left(\limsup_{n\to\infty} \sqrt[n]{|a_n|}\right)^{-1} \in [0, \infty].$$

Then:

1. If $|x-x_0|<R \implies \sum a_n(x-x_0)^n$ converges absolutely.
2. If $0 \le r < R \implies \sum a_n(x-x_0)^n$ converges uniformly on $[x_0-r, x_0+r]$.
3. If $|x-x_0|>R \implies \sum a_n(x-x_0)^n$ diverges.

The number R is called *radius of convergence of the power series.*

Theorem 5.55 (Abel's theorem). Let $\sum a_n x^n$ be a power series[63] with radius of convergence R satisfying $\sum a_n R^n < \infty$. Then the series $\sum a_n x^n$ converges uniformly on $[0,R]$. In particular, if $f(x)=\sum a_n x^n$,

$$\lim_{x\to R^-} f(x) = \sum_{n=0}^{\infty} a_n R^n.$$

Corollary 5.56. Let f be the sum function of a power series $\sum a_n x^n$. Then f is continuous on the domain of convergence of the series.

Corollary 5.57. If the series $\sum a_n x^n$ has radius of convergence $R \neq 0$ and f is its sum function, then f is Riemann-integrable on any closed subinterval on the domain of convergence of the series. In particular, for $|x|<R$,

$$\int_0^x f(t)\mathrm{d}t = \sum_{n=0}^{\infty} a_n \frac{x^{n+1}}{n+1}\text{[64]}.$$

Corollary 5.58. Let f be the sum function of the power series $\sum a_n x^n$. Then f is derivable within the domain of convergence of the series and

$$f'(x) = \sum_{n=0}^{\infty} n a_n x^{n-1}.$$

Corollary 5.59. Any function f defined as a sum of a power series $\sum a_n x^n$ is indefinitely derivable within the domain of convergence of the series and

$$f^{(k)}(x) = \sum_{n=k}^{\infty} n(n-1)\cdots(n-k+1)a_n x^{n-k},$$

for all $k \in \mathbb{N}\cup\{0\}$. In particular $f^{(k)}(0)=k!a_k$.

Definition 5.60. A function is *analytic* if it can be expressed locally as a power series.

Stone-Weierstraß approximation theorem

Definition 5.61. Let f be a real-valued function. We say f has *compact support*[65] if exists an $M>0$ such that $f(x)=0$ for all $x \in \mathbb{R}\setminus[-M,M]$.

Definition 5.62. Let f,g be real-valued functions with compact support. We define the convolution of f with g as

$$(f*g)(x) = \int_{\mathbb{R}} f(t)g(x-t)\mathrm{d}t\text{[66]}.$$

Definition 5.63. We sap a sequence of functions (ϕ_ε) with compact support is an *approximation of unity* if

1. $\phi_\varepsilon \ge 0$.
2. $\displaystyle\int_{\mathbb{R}} \phi_\varepsilon = 1$.
3. For all $\delta>0$, $\phi_\varepsilon(t)$ converges uniformly to zero when $\varepsilon \to 0$ if $|t|>\delta$.

Lemma 5.64. Let $f:\mathbb{R}\to\mathbb{R}$ be a continuous function with compact support. Let (ϕ_ε) be an approximation of unity. Then $(f*\phi_\varepsilon)$ converges uniformly to f on $\mathbb{R}$ when $\varepsilon\to 0$.

Theorem 5.65 (Stone-Weierstraß theorem). Let $f:[a,b]\to\mathbb{R}$ be a continuous function. Then, there exists polynomials $p_n \in \mathbb{R}[x]$ such that the sequence (p_n) converge uniformly to f on $[a,b]$.

1.2.5.3 | Improper integrals

Locally integrable functions

Definition 5.66. Let $f:[a,b)\to\mathbb{R}$, with $b\in\mathbb{R}\cup\{\infty\}$. We say f is *locally integrable on* $[a,b)$ if f is Riemann-integrable on $[a,x]$ for all $a\le x<b$.

Definition 5.67. Let $f:[a,b)\to\mathbb{R}$ be a locally integrable function. If there exists

$$\lim_{x\to b^-}\int_a^x f$$

and it's finite, we say that the *improper integral of f on* $[a,b)$, $\displaystyle\int_a^b f$, is *convergent.*

Theorem 5.68 (Cauchy's test). Let $f:[a,b)\to\mathbb{R}$ be a locally integrable function. The improper integral $\displaystyle\int_a^b f$ is convergent if and only if $\forall\varepsilon>0\ \exists b_0$, $a<b_0<b$, such that

$$\left|\int_{x_1}^{x_2} f\right| < \varepsilon$$

if $b_0<x_1<x_2<b$.

[63] From now on we will suppose, for simplicity, $x_0=0$.
[64] The formula is also valid for $|x|=R$ if the series $\sum a_n R^n$ (or $\sum a_n(-R)^n$) is convergent.
[65] In general, the support of a function is the adherence of the set of points which are not mapped to zero.
[66] Alternatively if f,g are Riemann-integrable functions on $[a,b]$ we can define the convolution of f and g as

$$(f*g)(x) = \int_a^b f(t)g(x-t)\mathrm{d}t.$$

Improper integrals of non-negative functions

Theorem 5.69. Let $f:[a,b)\to\mathbb{R}$ be a locally integrable non-negative function. A necessary and sufficient condition for $\displaystyle\int_a^b f$ to be convergent is that the function

$$F(x)=\int_a^x f(t)\mathrm{d}t$$

must be bounded for all $x<b$.

Theorem 5.70 (Comparison test). Let $f,g:[a,b)\to[0,+\infty)$ be two locally integrable non-negative functions. Then:

1. If $\exists C>0$ such that $f(x)\le Cg(x)$ $\forall x$ on a neighborhood of b and $\displaystyle\int_a^b g<\infty \implies \int_a^b f<\infty$.
2. Suppose the limit $\ell=\lim\limits_{x\to b}\dfrac{f(x)}{g(x)}$ exists. Then,
   i) If $\ell\in(0,\infty)\implies \displaystyle\int_a^b f<\infty \iff \int_a^b g<\infty$.
   ii) If $\ell=0$ and $\displaystyle\int_a^b g<\infty\implies\int_a^b f<\infty$.
   iii) If $\ell=\infty$ and $\displaystyle\int_a^b f<\infty\implies\int_a^b g<\infty$.

Theorem 5.71 (Integral test). Let $f:[1,\infty)\to(0,\infty)$ be a locally integrable decreasing function. Then:

$$\sum f(n)<\infty\iff\int_1^\infty f(x)\mathrm{d}x<\infty\text{[67]}.$$

Absolute convergence of improper integrals

Definition 5.72. Let $f:[a,b)\to(0,\infty)$ be a locally integrable function. We say $\displaystyle\int_a^b f$ *converges absolutely* if $\displaystyle\int_a^b |f|$ is convergent.

Theorem 5.73 (Dirichlet's test). Let $f,g:[a,b)\to\mathbb{R}$ be two locally integrable functions Suppose:

1. $\exists C>0$ such that $\left|\int_a^x f(t)\mathrm{d}t\right|\le C$ for all $x\in[a,b)$.
2. g is monotone and $\lim\limits_{x\to b}g(x)=0$.

Then, $\displaystyle\int_a^b fg$ is convergent.

Theorem 5.74 (Abel's test). Let $f,g:[a,b)\to\mathbb{R}$ be two locally integrable functions. Suppose:

1. $\displaystyle\int_a^b f$ is convergent.
2. g is monotone and bounded.

Then, $\displaystyle\int_a^b fg$ is convergent.

[67] This is another way of formulating theorem 5.17.

Differentiation under integral sign

Theorem 5.75. Let $f:[a,b]\times[c,d]\to\mathbb{R}$ be a continuous function on $[a,b]\times[c,d]$. Consider the function $F(y)=\displaystyle\int_a^b f(x,y)\mathrm{d}x$ defined on $[c,d]$. Then, F is continuous, that is, if $c<y_0<d$,

$$\lim_{y\to y_0}F(y)=\lim_{y\to y_0}\int_a^b f(x,y)\mathrm{d}x=\int_a^b\lim_{y\to y_0}f(x,y)\mathrm{d}x==\int_a^b f(x,y_0)\mathrm{d}x=F(y_0).$$

Theorem 5.76. Let $f:[a,b]\times[c,d]\to\mathbb{R}$ be a Riemann-integrable function and let $F(y)=\displaystyle\int_a^b f(x,y)\mathrm{d}x$. If f is differentiable with respect to y and $\partial f/\partial y$ is continuous on $[a,b]\times[c,d]$, then $F(y)$ is derivable on (c,d) and its derivative is

$$F'(y)=\int_a^b\frac{\partial f}{\partial y}(x,y)\mathrm{d}x,$$

for all $y\in(c,d)$.

Theorem 5.77. Let $f:[a,b]\times[c,d]\to\mathbb{R}$ be a continuous function on $[a,b]\times[c,d]$. Let $a,b:[c,d]\to\mathbb{R}$ be to differentiable functions satisfying $a\le a(y)\le b(y)\le b$ for every $y\in[c,d]$. Suppose that $\partial f/\partial y$ is continuous on $\{(x,y)\in\mathbb{R}^2: a(y)\le x\le b(y),\ c\le y\le d\}$. Then $F(y)=\displaystyle\int_{a(y)}^{b(y)}f(x,y)\mathrm{d}x$ is derivable on (c,d) and its derivative is

$$F'(y)=b'(y)f(b(y),y)-a'(y)f(a(y),y)++\int_{a(y)}^{b(y)}\frac{\partial f}{\partial y}(x,y)\mathrm{d}x,$$

for all $y\in(c,d)$.

Theorem 5.78. Let $f:[a,b)\times[c,d]\to\mathbb{R}$ be a continuous function on $[a,b)\times[c,d]$. We consider $F(y)=\displaystyle\int_a^b f(x,y)\mathrm{d}x$. Suppose that:

1. $\dfrac{\partial f}{\partial y}$ is continuous on $[a,b)\times[c,d]$.
2. Given $y_0\in[c,d]$, $\exists\delta>0$ such that the integral
$$\int_a^b\sup\left\{\left|\frac{\partial f}{\partial y}(x,y)\right|:y\in(y_0-\delta,y_0+\delta)\right\}\mathrm{d}x$$
exists and it's finite on $[a,b)$.

Then, $F(y)$ is derivable at y_0 and

$$F'(y_0)=\int_a^b\frac{\partial f}{\partial y}(x,y_0)\mathrm{d}x.$$

Theorem 5.79. Let $f : [a, b) \times [c, d] \to \mathbb{R}$ be a continuous function on $[a, b) \times [c, d]$. Let $a, b : [c, d] \to \mathbb{R}$ be two differentiable functions satisfying $a \leq a(y) \leq b(y) \leq b$ for every $y \in [c, d]$. We consider $F(y) = \displaystyle\int_{a(y)}^{b(y)} f(x, y)\mathrm{d}x$. Suppose that:

1. $\dfrac{\partial f}{\partial y}$ is continuous on $\{(x, y) \in \mathbb{R}^2 : a(y) \leq x \leq b(y),\ c \leq y \leq d\}$.
2. Given $y_0 \in [c, d]$, $\exists \delta > 0$ such that the integral
$$\int_{a(y)}^{b(y)} \sup\left\{\left|\frac{\partial f}{\partial y}(x, y)\right| : y \in (y_0 - \delta, y_0 + \delta)\right\} \mathrm{d}x$$
exists and it's finite on $[a, b)$.

The, $F(y)$ is derivable at y_0 and

$$F'(y_0) = b'(y_0)f(b(y_0), y_0) - a'(y_0)f(a(y_0), y_0) + \\ + \int_{a(y_0)}^{b(y_0)} \frac{\partial f}{\partial y}(x, y_0)\mathrm{d}x.$$

Gamma function

Definition 5.80. For $x > 0$, *Gamma function* is defined as

$$\Gamma(x) = \int_0^\infty t^{x-1}\mathrm{e}^{-t}\mathrm{d}t.$$

Theorem 5.81. Gamma function is a generalization of the factorial. In fact, for $x > 0$ we have

$$\Gamma(x + 1) = x\Gamma(x).$$

In particular, $\Gamma(n + 1) = n!$ for all $n \in \mathbb{N}$.

Theorem 5.82. Gamma function satisfies:

$$\lim_{x\to\infty} \frac{\Gamma(x + 1)}{(x/e)^x\sqrt{2\pi x}} = 1.$$

Corollary 5.83 (Stirling's formula).

$$\lim_{n\to\infty} \frac{n!}{n^n\mathrm{e}^{-n}\sqrt{2\pi n}} = 1.$$

1.2.5.4 | Fourier series

Periodic functions

Definition 5.84. Let $f : \mathbb{R} \to \mathbb{C}$ be a function. We say that f is *T-periodic*, or is *periodic with period T*, being $T > 0$, if $f(x + T) = f(x)$ for all $x \in \mathbb{R}$.

Lemma 5.85. Let $f : \mathbb{R} \to \mathbb{C}$ be a T-periodic function. Then $f(x+T') = f(x)$ for all $x \in \mathbb{R}$ if and only if $T' = kT$ for some $k \in \mathbb{Z}$.

Proposition 5.86. Let $f : \mathbb{R} \to \mathbb{C}$ be a T-periodic function. Then

$$\int_a^{a+T} f(x)\mathrm{d}x = \int_0^T f(x)\mathrm{d}x,$$

where $a \in \mathbb{R}$. In particular,

$$\int_a^{a+kT} f(x)\mathrm{d}x = k\int_0^T f(x)\mathrm{d}x.$$

Lemma 5.87. Let $f : \mathbb{R} \to \mathbb{C}$ be a T-periodic continuous function. Then, $|f|$ is bounded.

Proposition 5.88. Given a T-periodic function f, there is no power series uniformly convergent to f on $\mathbb{R}$.

Orthogonal systems

Definition 5.89. Let $f : \mathbb{R} \to \mathbb{C}$ be a function. Then $f \in L^p(I)$, $p \geq 1$, if

$$\|f\|_p := \left(\int_I |f(t)|^p\mathrm{d}t\right)^{1/p} < \infty.$$

Definition 5.90. Let $f, g : [a, b] \to \mathbb{C}$ be Riemann-integrable functions. We define the *inner product of f and g* as

$$\langle f, g\rangle := \int_a^b f(x)\overline{g(x)}\mathrm{d}x,$$

where $\overline{g}$ is the complex conjugate of g. Now, it's natural to define the *norm of f* as

$$\|f\| := \langle f, f\rangle^{1/2} = \left(\int_a^b |f(x)|^2\mathrm{d}x\right)^{1/2} = \|f\|_2.$$

And the *distance between f and g* as

$$d(f, g) := \|f - g\|.$$

Proposition 5.91. Let $f, g : [a, b] \to \mathbb{C}$ be Riemann-integrable functions and let $\alpha \in \mathbb{C}$. Then we have:

1. $\langle f, f\rangle \geq 0$.
2. $\langle f + h, g\rangle = \langle f, g\rangle + \langle h, g\rangle$ and $\langle f, g + h\rangle = \langle f, g\rangle + \langle f, h\rangle$.
3. $\langle f, g\rangle = \overline{\langle g, f\rangle}$.
4. $\langle \alpha f, g\rangle = \alpha\langle f, g\rangle$ and $\langle f, \alpha g\rangle = \overline{\alpha}\langle f, g\rangle$.

Theorem 5.92 (Cauchy–Schwarz inequality). Let $f, g : [a, b] \to \mathbb{C}$ be Riemann-integrable functions. Then,

$$|\langle f, g\rangle| \leq \|f\| \cdot \|g\|,$$

which can be written as

$$\int_a^b f\overline{g} \leq \left(\int_a^b |f|^2\right)^{1/2} \left(\int_a^b |g|^2\right)^{1/2}.$$

Theorem 5.93 (Minkowski inequality). Let $f, g : [a, b] \to \mathbb{C}$ be Riemann-integrable functions. Then,

$$\|f + g\| \leq \|f\| + \|g\|.$$

Definition 5.94. Let $f, g : [a, b] \to \mathbb{C}$ be Riemann-integrable functions with $f \neq g$. We say f and g are *orthogonal* if $\langle f, g\rangle = 0$. We say f and g are *orthonormal* if they are orthogonal and $\|f\| = \|g\| = 1$.

Definition 5.95. Let $S=\{\phi_0,\phi_1,\ldots\}$ be a collection of Riemann-integrable functions on $[a,b]$. We say S is an *orthonormal system* if $\|\phi_n\|=1$ $\forall n$ and $\langle\phi_n,\phi_m\rangle=0$ $\forall n\neq m$.

Proposition 5.96. Let

$$S_1=\left\{\frac{1}{T}\mathrm{e}^{\frac{2\pi i n x}{T}}, n\in\mathbb{Z}\right\},$$

$$S_2=\left\{\frac{1}{\sqrt{T}},\frac{\cos\left(\frac{2\pi n x}{T}\right)}{\sqrt{T/2}},\frac{\sin\left(\frac{2\pi m x}{T}\right)}{\sqrt{T/2}}, n,m\in\mathbb{N}\right\}.$$

Then S_1 and S_2 orthonormal systems on $[-T/2,T/2]$.

Definition 5.97. A collection of functions $S=\{\phi_0,\phi_1,\ldots,\phi_n\}$ is *linearly dependent* on $[a,b]$ if there exist $c_0,c_1,\ldots,c_n\in\mathbb{R}$ not all zero, such that

$$c_0\phi_0+c_1\phi_1+\cdots+c_n\phi_n=0,\quad\forall x\in[a,b].$$

Otherwise we say S is *linearly independent*. If the collection S has an infinity number of functions, we say S is linearly independent on $[a,b]$ if any finite subset of S is linearly independent on $[a,b]$.

Theorem 5.98. Let $S=\{\phi_0,\phi_1,\ldots\}$ be an orthonormal system on $[a,b]$. Suppose that $\sum c_n\phi_n(x)$ converges uniformly to a function f on $[a,b]$. Then, f is Riemann-integrable on $[a,b]$ and, moreover,

$$c_n=\langle f,\phi_n\rangle=\int_a^b f(x)\overline{\phi_n(x)}\mathrm{d}x,\quad\forall n\geq 0.$$

Fourier coefficients and Fourier series

Definition 5.99. Let $S=\left\{\frac{1}{T}\mathrm{e}^{\frac{2\pi i n x}{T}}, n\in\mathbb{Z}\right\}$ be an orthonormal system on $[-T/2,T/2]$ and let $f\in L^1([-T/2,T/2])$[68] be a T-periodic function[69]. We define the *n-th Fourier coefficient of f* as

$$\widehat{f}(n)=\left\langle f,\frac{1}{T}\mathrm{e}^{\frac{2\pi i n x}{T}}\right\rangle=\frac{1}{T}\int_{-T/2}^{T/2}f(x)\mathrm{e}^{-\frac{2\pi i n x}{T}}\mathrm{d}x,$$

for all $n\in\mathbb{Z}$.

Proposition 5.100. Let $f,g\in L^1([-T/2,T/2])$. The following properties are satisfied:

1. For all $\lambda,\mu\in\mathbb{C}$,
$$\widehat{\lambda f+\mu g}(n)=\lambda\widehat{f}(n)+\mu\widehat{g}(n).$$
2. Let $\tau\in\mathbb{R}$. We define $f_\tau(x)=f(x-\tau)$. Then,
$$\widehat{f_\tau}(n)=\mathrm{e}^{-\frac{2\pi i n\tau}{T}}\widehat{f}(n).$$
3. If f is even, then $\widehat{f}(n)=\widehat{f}(-n)$, $\forall n\in\mathbb{Z}$.
If f is odd, then $\widehat{f}(n)=-\widehat{f}(-n)$, $\forall n\in\mathbb{Z}$.
4. If $f\in\mathcal{C}^k$, then
$$\widehat{f^{(k)}}(n)=\left(\frac{2\pi i n}{T}\right)^k\widehat{f}(n).$$
5. $\widehat{(f*g)}(n)=\widehat{f}(n)\widehat{g}(n)$.

Definition 5.101. Let $f\in L^1([-T/2,T/2])$. We define the *Fourier series of f* as

$$Sf(x)=\sum_{n\in\mathbb{Z}}\widehat{f}(n)\mathrm{e}^{\frac{2\pi i n x}{T}}.$$

Definition 5.102. Let $f\in L^1([-T/2,T/2])$ and Sf be the Fourier series of f. The *N-th partial sum of Sf* is

$$S_Nf(x)=\sum_{n=-N}^{N}\widehat{f}(n)\mathrm{e}^{\frac{2\pi i n x}{T}}.$$

Proposition 5.103. Let $f\in L^1([-T/2,T/2])$. Then

$$Sf(x)=\frac{a_0}{2}+\sum_{n=1}^{\infty}a_n\cos\left(\frac{2\pi n x}{T}\right)+b_n\sin\left(\frac{2\pi n x}{T}\right),$$

where

$$a_n=\frac{2}{T}\int_{-T/2}^{T/2}f(x)\cos\left(\frac{2\pi n x}{T}\right)\mathrm{d}x,$$
$$b_n=\frac{2}{T}\int_{-T/2}^{T/2}f(x)\sin\left(\frac{2\pi n x}{T}\right)\mathrm{d}x,$$

for $n\geq 0$[70]. In particular, if f is even we have

$$Sf(x)=\frac{a_0}{2}+\sum_{n=1}^{\infty}a_n\cos\left(\frac{2\pi n x}{T}\right),$$

and if f is odd we have

$$Sf(x)=\sum_{n=1}^{\infty}b_n\sin\left(\frac{2\pi n x}{T}\right).$$

Definition 5.104. Let $f:(0,L)\to\mathbb{C}$ be a function. We define the *even extension of f* as

$$\tilde{f}(x)=\begin{cases} f(x) & \text{si}\quad x\in(0,L)\\ f(-x) & \text{si}\quad x\in(-L,0)\end{cases}$$

Analogously, we define the *odd extension of f* as

$$\hat{f}(x)=\begin{cases} f(x) & \text{si}\quad x\in(0,L)\\ -f(-x) & \text{si}\quad x\in(-L,0)\end{cases}$$

[68]Saying that $f\in L^1([-T/2,T/2])$ is equivalent to say that f is integrable on $[-T/2,T/2]$.
[69]From now on, we will work only with functions defined on $[-T/2,T/2]$ and extended periodically on $\mathbb{R}$.
[70]The relation between a_n,b_n and $\widehat{f}(n)$ is given by:

$$a_n=\widehat{f}(n)+\widehat{f}(-n)\quad\text{and}\quad b_n=\mathrm{i}\left[\widehat{f}(n)-\widehat{f}(-n)\right],\quad\forall n\in\mathbb{N}\cup\{0\}.$$

Proposition 5.105. Let $f \in L^1([0,T/2])$. If we make the even extension of f[71], then

$$Sf(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos\left(\frac{2\pi n x}{T}\right),$$

where $a_n = \frac{4}{T}\int_0^{T/2} f(x)\cos\left(\frac{2\pi n x}{T}\right)\mathrm{d}x$ for $n \geq 0$. If we make the odd extension of f, then

$$Sf(x) = \sum_{n=1}^{\infty} b_n \sin\left(\frac{2\pi n x}{T}\right),$$

where $b_n = \frac{4}{T}\int_0^{T/2} f(x)\sin\left(\frac{2\pi n x}{T}\right)\mathrm{d}x$ for $n \geq 1$.

Pointwise convergence

Definition 5.106 (Dirichlet kernel). We define the *Dirichlet kernel of order N* as

$$D_N(t) = \frac{1}{T}\sum_{n=-N}^{N} \mathrm{e}^{\frac{2\pi i n t}{T}} = \frac{1}{T}\frac{\sin\left(\frac{(2N+1)\pi t}{T}\right)}{\sin\left(\frac{\pi t}{T}\right)}.$$

Proposition 5.107. The Dirichlet kernel has the following properties:

1. D_N is a T-periodic and even function.
2. $\int_0^T D_N(t)\mathrm{d}t = 1,\ \forall N$.

Proposition 5.108. Let $f \in L^1([-T/2,T/2])$. Then

$$S_N f(x) = (f * D_N)(x) = \int_{-T/2}^{T/2} f(x-t)D_N(t)\mathrm{d}t = \\ = \int_0^{T/2} [f(x+t)+f(x-t)]D_N(t)\mathrm{d}t.$$

Lemma 5.109 (Riemann-Lebesgue lemma). Let $f \in L^1([-T/2,T/2])$ and $\lambda \in \mathbb{R}$. Then:

$$\lim_{\lambda\to\infty}\int_{-T/2}^{T/2} f(t)\sin(\lambda t)\mathrm{d}t = \lim_{\lambda\to\infty}\int_{-T/2}^{T/2} f(t)\cos(\lambda t)\mathrm{d}t = 0.$$

In particular, $\lim_{|n|\to\infty}\widehat{f}(n) = 0$.

Theorem 5.110. Let $f \in L^1([-T/2,T/2])$ be a function left and right differentiable at x_0, that is, there exists the following limits

$$f'(x_0^+) = \lim_{t\to 0^+}\frac{f(x_0+t)-f(x_0^+)}{t},$$
$$f'(x_0^-) = \lim_{t\to 0^-}\frac{f(x_0+t)-f(x_0^-)}{t},$$

(supposing the existence of left- and right-sided limits). Then,

$$\lim_{N\to\infty} S_N f(x_0) = \frac{f(x_0^+)+f(x_0^-)}{2}.$$

Theorem 5.111 (Dini's theorem). Let $f \in L^1([-T/2,T/2])$, $x_0 \in (-T/2,T/2)$ and $\ell \in \mathbb{R}$ such that

$$\int_0^\delta \frac{|f(x_0+t)+f(x_0-t)-2\ell|}{t}\mathrm{d}t < \infty$$

for some $\delta > 0$. Then $\lim_{N\to\infty} S_N f(x_0) = \ell$.

Theorem 5.112 (Lipschitz's theorem). Let $f \in L^1([-T/2,T/2])$ such that at a point $x_0 \in (-T/2,T/2)$ it satisfies

$$|f(x_0+t)-f(x_0)| \leq k|t|$$

for some constant $k \in \mathbb{R}$ and for $|t| < \delta$. Then $\lim_{N\to\infty} S_N f(x_0) = f(x_0)$.

Uniform convergence

Definition 5.113. Let $\sum a_n$ be a series with partial sums S_k. The series $\sum a_n$ is called *Cesàro summable* with sum S if

$$\lim_{N\to\infty}\frac{S_1+\cdots+S_N}{N} = S.$$

Definition 5.114 (Fejer kernel). We define the *Fejer kernel of order N* as

$$K_N(t) = \frac{1}{N+1}\sum_{k=0}^{N} D_k(t) = \frac{1}{T(N+1)}\frac{\sin^2\left(\frac{(N+1)\pi t}{T}\right)}{\sin^2\left(\frac{\pi t}{T}\right)},$$

being $D_k(t)$ the Dirichlet kernel of order k, $0 \leq k \leq N$.

Proposition 5.115. The Fejer kernel has the following properties:

1. K_N is a T-periodic, even and non-negative function.
2. $\int_{-T/2}^{T/2} K_N(t)\mathrm{d}t = 1,\ \forall N$.
3. $\forall\delta > 0,\ \lim_{N\to\infty}\sup\{|K_N(t)| : \delta \leq |t| \leq T/2\} = 0$.

Definition 5.116. Let $f \in L^1([-T/2,T/2])$. We define the *Fejér means* $\sigma_N f$, for all $N \in \mathbb{N}$, as

$$\sigma_N f(x) = \frac{S_0 f(x)+\cdots+S_N f(x)}{N+1}.$$

Proposition 5.117. Let $f \in L^1([-T/2,T/2])$. Then

$$\sigma_N f(x) = (f * K_N)(x) = \int_{-T/2}^{T/2} f(x-t)K_N(t)\mathrm{d}t = \\ = \int_0^{T/2} [f(x+t)+f(x-t)]K_N(t)\mathrm{d}t.$$

Theorem 5.118 (Fejér's theorem). Let $f \in L^1([-T/2,T/2])$ be a function having left- and right-sided limits at point x_0. Then,

$$\lim_{N\to\infty}\sigma_N f(x_0) = \frac{f(x_0^+)+f(x_0^-)}{2}.$$

In particular, if f is continuous at x_0, $\lim_{N\to\infty}\sigma_N f(x_0) = f(x_0)$.

[71] For simplicity, when we have a function f and make its even or odd extension, we will still call its even or odd extension f instead of $\tilde{f}$ or $\hat{f}$.

Theorem 5.119 (Fejér's theorem). Let f be a continuous function on $[-T/2, T/2]$. Then $\sigma_N f$ converges uniformly to f on $[-T/2, T/2]$.

Corollary 5.120. Let f be a continuous function on $[-T/2, T/2]$. Then there exists a sequence of trigonometric polynomials that converge uniformly to f on $[-T/2, T/2]$. In fact,

$$\sigma_N f(x) = \sum_{k=-N}^{N} \left(1 - \frac{|k|}{N+1}\right) \widehat{f}(k) \mathrm{e}^{2\pi \mathrm{i} k x}.$$

Corollary 5.121. Let f and g be continuous functions on $[-T/2, T/2]$ such that $Sf(x) = Sg(x)$. Then $f = g$.

Convergence in norm

Definition 5.122. We say a sequence (f_N) *converge to f in norm L^p* if $\lim_{N\to\infty} \|f_N - f\|_p = 0$.

Theorem 5.123. Let $f \in L^2([-T/2, T/2])$. Then, $\lim_{N\to\infty} \|\sigma_N f - f\| = 0$.

Corollary 5.124. Let $f \in L^1([-T/2, T/2])$. Then $\lim_{N\to\infty} \|\sigma_N f - f\|_1 = 0$.

Corollary 5.125. Let $f, g \in L^1([-T/2, T/2])$ be functions such that $Sf(x) = Sg(x)$. Then $\lim_{N\to\infty} \|g - f\|_1 = 0$.

Theorem 5.126 (Bessel's inequality). Let $f \in L^2(I)$, where I is any interval on the real line. Then:

$$T \sum_{n=-N}^{N} |\widehat{f}(n)|^2 \leq \|f\|^2,$$

$$\frac{T}{2}\left(\frac{|a_0|^2}{2} + \sum_{n=1}^{N} |a_n|^2 + |b_n|^2\right) \leq \|f\|^2,$$

for all $N \in \mathbb{N}$.

Theorem 5.127. $S_N f$ is the trigonometric polynomial of degree N that best approximates f in norm L^2.

Corollary 5.128. Let $f \in L^2([-T/2, T/2])$. Then, $\lim_{N\to\infty} \|S_N f - f\| = 0$.

Theorem 5.129 (Parseval's identity). Let $f, g \in L^2([-T/2, T/2])$ be bounded functions. Then

$$\langle f, g\rangle = T \sum_{n\in\mathbb{Z}} \widehat{f}(n)\overline{\widehat{g}(n)}.$$

In particular, if $f = g$:

$$\|f\|^2 = T \sum_{n\in\mathbb{Z}} |\widehat{f}(n)|^2,$$

$$\|f\|^2 = \frac{T}{2}\left(\frac{|a_0|^2}{2} + \sum_{n=1}^{\infty} |a_n|^2 + |b_n|^2\right).$$

Applications of Fourier series

Theorem 5.130 (Wirtinger's inequality). Let f be a function such that $f(0) = f(T)$, $f' \in L^2([0, T])$ and $\int_a^b f(t)\mathrm{d}t = 0$. Then,

$$\int_0^T |f(x)|^2 \mathrm{d}x \leq \frac{T^2}{4\pi^2} \int_0^T |f'(x)|^2 \mathrm{d}x,$$

with equality if and only if

$$f(x) = A\cos\left(\frac{2\pi x}{T}\right) + B\sin\left(\frac{2\pi x}{T}\right).$$

Theorem 5.131 (Wirtinger's inequality). Let $f \in \mathcal{C}^1([a, b])$ with $f(a) = f(b) = 0$. Then,

$$\int_a^b |f(x)|^2 \mathrm{d}x \leq \frac{(b-a)^2}{\pi^2} \int_a^b |f'(x)|^2 \mathrm{d}x.$$

Theorem 5.132 (Isoperimetric inequality). Let c be a simple and closed curve of class $\mathcal{C}^1$ whose length is L. If A_c is the area enclosed by c, then

$$A_c \leq \frac{L^2}{4\pi},$$

with equality if and only if c is a circle.

1.2.6 Numerical methods

1.2.6.1 | Errors

Floating-point representation

Theorem 6.1. Let $b \in \mathbb{N}$, $b \geq 2$. Any real number $x \in \mathbb{R}$ can be represented of the form

$$x = s\left(\sum_{i=1}^{\infty} \alpha_i b^{-i}\right) b^q$$

where $s \in \{-1, 1\}$, $q \in \mathbb{Z}$ and $\alpha_i \in \{0, 1, \ldots, b-1\}$. Moreover, this representation is unique if $\alpha_1 \neq 0$ and $\forall i_0 \in \mathbb{N}$, $\exists i \geq i_0 : \alpha_i \neq b-1$. We will write

$$x = s(0.\alpha_1\alpha_2\cdots)_b b^q$$

where the subscript b in the parenthesis indicates that the number $0.\alpha_1\alpha_2\alpha_3\cdots$ is in base b.

Definition 6.2 (Floating-point representation). Let x be a real number. Then, the *floating-point representation of x* is:

$$x = s\left(\sum_{i=1}^{t} \alpha_i b^{-i}\right) b^q$$

Here s is called the *sign*; $\sum_{i=1}^{t} \alpha_i b^{-i}$, the *significant* or *mantissa*, and q, the *exponent*, limited to a prefixed range $q_{\min} \leq q \leq q_{\max}$. Therefore, the floating-point representation of x can be expressed as:

$$x = smb^q = s(0.\alpha_1\alpha_2\cdots\alpha_t)_b b^q$$

Finally, we say a floating-point number is *normalized* if $\alpha_1 \neq 0$.

Format	b	t	$q_{\min}$	$q_{\max}$	bits
IEEE simple	2	24	-126	127	32
IEEE double	2	53	-1022	1023	64

Table 1.2.1: Parameters of IEEE simple and IEEE double formats.

Definition 6.3. Let $x \in \mathbb{R}$ be such that $x = s(0.\alpha_1\alpha_2\cdots)_b b^q$ with $q_{\min} \leq q \leq q_{\max}$. We say the *floating-point representation by truncation of x* is:

$$fl_T(x) = s(0.\alpha_1\alpha_2\cdots\alpha_t)_b b^q$$

We say the *floating-point representation by rounding of x* is:

$$fl_R(x) = \\ = \begin{cases} s(0.\alpha_1\cdots\alpha_t)_b b^q & \text{if } 0 \leq \alpha_{t+1} < \frac{b}{2} \\ s(0.\alpha_1\cdots\alpha_{t-1}(\alpha_t{+}1))_b b^q & \text{if } \frac{b}{2} \leq \alpha_{t+1} \leq b-1 \end{cases}$$

Definition 6.4. Given a value $x \in \mathbb{R}$ and an approximation $\tilde{x}$ of x, the *absolute error* is:

$$\Delta x := |x - \tilde{x}|$$

If $x \neq 0$, the *relative error* is:

$$\delta x := \frac{|x - \tilde{x}|}{x}$$

If x is unknown, we take:

$$\delta x \approx \frac{|x - \tilde{x}|}{\tilde{x}}$$

Definition 6.5. Let $\tilde{x}$ be an approximation of x. If $\Delta x \leq \frac{1}{2}10^{-t}$, we say $\tilde{x}$ *has t correct decimal digits*. If $x = sm10^q$ with $0.1 \leq m < 1$, $\tilde{x} = s\tilde{m}10^q$ and

$$u := \max\{i \in \mathbb{Z} : |m - \tilde{m}| \leq \frac{1}{2}10^{-i}\}$$

then we say that $\tilde{x}$ *has u significant digits*.

Proposition 6.6. Let $x \in \mathbb{R}$ be such that $x = s(0.\alpha_1\alpha_2\cdots)_b b^q$ with $\alpha_1 \neq 0$ and $q_{\min} \leq q \leq q_{\max}$. Then, its floating-point representation in base b and with t digits satisfy:

$$|fl_T(x) - x| \leq b^{q-t} \qquad |fl_R(x) - x| \leq \frac{1}{2}b^{q-t}$$
$$\left|\frac{fl_T(x) - x}{x}\right| \leq b^{1-t} \qquad \left|\frac{fl_R(x) - x}{x}\right| \leq \frac{1}{2}b^{1-t}$$

Definition 6.7. The *machine epsilon* ϵ is defined as:

$$\epsilon := \min\{\varepsilon > 0 : fl(1+\varepsilon) \neq 1\}$$

Proposition 6.8. For a machine working by truncation, $\epsilon = b^{1-t}$. For a machine working by rounding, $\epsilon = \frac{1}{2}b^{1-t}$.

Propagation of errors

Proposition 6.9 (Propagation of absolute errors). Let $f : \mathbb{R}^n \to \mathbb{R}$ be a function of class $\mathcal{C}^2$. If Δx_j is the absolute error of the variable x_j and $\Delta f(x)$ is the absolute error of the function f evaluated at the point $x = (x_1, \ldots, x_n)$, we have:

$$|\Delta f(x)| \lesssim \sum_{j=1}^{n} \left|\frac{\partial f}{\partial x_j}(x)\right| |\Delta x_j|$$[72]

The coefficients $\left|\frac{\partial f}{\partial x_j}(x)\right|$ are called *absolute condition numbers of the problem.*

Proposition 6.10 (Propagation of relative errors). Let $f : \mathbb{R}^n \to \mathbb{R}$ be a function of class $\mathcal{C}^2$. If δx_j is the relative error of the variable x_j and $\delta f(x)$ is the relative error of the function f evaluated at the point $x = (x_1, \ldots, x_n)$, we have:

$$|\delta f(x)| \lesssim \sum_{j=1}^{n} \frac{\left|\frac{\partial f}{\partial x_j}(x)\right| |x_j|}{|f(x)|} |\delta x_j|$$

The coefficients $\frac{\left|\frac{\partial f}{\partial x_j}(x)\right| |x_j|}{|f(x)|}$ are called *relative condition numbers of the problem.*

[72] The symbol $\lesssim$ means that we are omitting terms of order $\Delta x_j \Delta x_k$ and higher.

Numerical stability of algorithms

Definition 6.11. An algorithm is said to be *numerically stable* if errors in the input lessen in significance as the algorithm executes, having little effect on the final output. On the other hand, an algorithm is said to be *numerically unstable* if errors in the input cause a considerably larger error in the final output.

Definition 6.12. A problem with a low condition number is said to be *well-conditioned*. Conversely, a problem with a high condition number is said to be *ill-conditioned*.

1.2.6.2 | Zeros of functions

Definition 6.13. Let $f:\mathbb{R}\to\mathbb{R}$ be a function. We say α is a *zero* or a *solution to the equation* $f(x)=0$ if $f(\alpha)=0$.

Definition 6.14. Let $f:\mathbb{R}\to\mathbb{R}$ be a sufficiently differentiable function. We say α is a *zero of multiplicity* $m\in\mathbb{N}$ if

$$f(\alpha)=f'(\alpha)=\cdots=f^{(m-1)}(\alpha)=0 \quad\text{and}\quad f^{(m)}(\alpha)\neq 0$$

If $m=1$, the zero is called *simple*; if $m=2$, *double*; if $m=3$, *triple*...

Root-finding methods

For the following methods consider a continuous function $f:I\subseteq\mathbb{R}\to\mathbb{R}$ with an unknown zero $\alpha\in I$. Given $\varepsilon>0$, we want to approximate α with $\tilde{\alpha}$ such that $|\alpha-\tilde{\alpha}|<\varepsilon$.

Method 6.15 (Bisection method). Suppose $I=[a_0,b_0]$. For each step $n\geq 0$ of the algorithm we will approximate α by

$$c_n=\frac{a_n+b_n}{2}$$

If $f(c_n)=0$ we are done. If not, let

$$[a_{n+1},b_{n+1}]=\begin{cases}[a_n,c_n] & \text{if}\quad f(a_n)f(c_n)<0\\ [c_n,b_n] & \text{if}\quad f(a_n)f(c_n)>0\end{cases}$$

and iterate the process again[73]. The length of the interval $[a_n,b_n]$ is $\frac{b_0-a_0}{2^n}$ and therefore:

$$|\alpha-c_n|<\frac{b_0-a_0}{2^{n+1}}<\varepsilon \iff n>\frac{\log\left(\frac{b_0-a_0}{\varepsilon}\right)}{\log 2}-1$$

Method 6.16 (*Regula falsi* method). Suppose $I=[a_0,b_0]$. For each step $n\geq 0$ of the algorithm we will approximate α by

$$c_n=b_n-f(b_n)\frac{b_n-a_n}{f(b_n)-f(a_n)}=\frac{a_nf(b_n)-b_nf(a_n)}{f(b_n)-f(a_n)}.$$

If $f(c_n)=0$ we are done. If not, let

$$[a_{n+1},b_{n+1}]=\begin{cases}[a_n,c_n] & \text{if}\quad f(a_n)f(c_n)<0\\ [c_n,b_n] & \text{if}\quad f(a_n)f(c_n)>0\end{cases}$$

and iterate the process again.

Method 6.17 (Secant method). Suppose $I=\mathbb{R}$ and that we have two different initial approximations x_0, x_1. Then, for each step $n\geq 0$ of the algorithm we obtain a new approximation x_{n+2}, given by:

$$x_{n+2}=x_{n+1}-f(x_{n+1})\frac{x_{n+1}-x_n}{f(x_{n+1})-f(x_n)}$$

Method 6.18 (Newton-Raphson method). Suppose $I=\mathbb{R}$, $f\in\mathcal{C}^1$ and that we have an initial approximation x_0. Then, for each step $n\geq 0$ we obtain a new approximation x_{n+1}, given by:

$$x_{n+1}=x_n-\frac{f(x_n)}{f'(x_n)}$$

Method 6.19 (Newton-Raphson modified method). Suppose $I=\mathbb{R}$, $f\in\mathcal{C}^1$ and that we have an initial approximation x_0 of a zero α of multiplicity m. Then, for each step $n\geq 0$ we obtain a new approximation x_{n+1}, given by:

$$x_{n+1}=x_n-m\frac{f(x_n)}{f'(x_n)}$$

Method 6.20 (Chebyshev method). Suppose $I=\mathbb{R}$, $f\in\mathcal{C}^2$ and that we have an initial approximation x_0. Then, for each step $n\geq 0$ we obtain a new approximation x_{n+1}, given by:

$$x_{n+1}=x_n-\frac{f(x_n)}{f'(x_n)}-\frac{1}{2}\frac{f(x_n)^2f''(x_n)}{f'(x_n)^3}$$

Fixed-point iterations

Definition 6.21. Let $g:[a,b]\to[a,b]\subset\mathbb{R}$ be a function. A point $\alpha\in[a,b]$ is *n-periodic* if $g^n(\alpha)=\alpha$ and $g^j(\alpha)\neq\alpha$ for $j=1,\ldots,n-1$[74].

Theorem 6.22 (Fixed-point theorem). Let (M,d) be a complete metric space and $g:M\to M$ be a contraction[75]. Then, g has a unique fixed point $\alpha\in M$ and for every $x_0\in M$,

$$\lim_{n\to\infty}x_n=\alpha,\quad\text{where } x_n=g(x_{n-1})\quad\forall n\in\mathbb{N}$$

Proposition 6.23. Let (M,d) be a metric space and $g:M\to M$ be a contraction of constant k. Then, if we want to approximate a fixed point α by the iteration $x_n=g(x_{n-1})$, we have:

$$d(x_n,\alpha)\leq\frac{k^n}{1-k}d(x_1,x_0)\qquad\text{(a priori estimation)}$$
$$d(x_n,\alpha)\leq\frac{k}{1-k}d(x_n,x_{n-1})\qquad\text{(a posteriori estimation)}$$

Corollary 6.24. Let $g:\mathbb{R}\to\mathbb{R}$ be a function of class $\mathcal{C}^1$. Suppose α is a fixed point of g and $|g'(\alpha)|<1$. Then, there exists $\varepsilon>0$ and $I_\varepsilon:=[\alpha-\varepsilon,\alpha+\varepsilon]$ such that $g(I_\varepsilon)\subseteq I_\varepsilon$ and g is a contraction on I_ε. In particular, if $x_0\in I_\varepsilon$, the iteration $x_{n+1}=g(x_n)$ converges to α.

[73] Note that bisection method only works for zeros of odd multiplicity.
[74] Note that 1-periodic points are the fixed points of f.
[75] Remember definitions 3.1, 3.36 and 3.52.

Definition 6.25. Let $g : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^1$ and α be a fixed point of g. We say α is an *attractor fixed point* if $|g'(\alpha)| < 1$. In this case, any iteration $x_{n+1} = g(x_n)$ in I_ε converges to α. If $|g'(\alpha)| > 1$, we say α is a *repulsor fixed point*. In this case, $\forall x_0 \in I_\varepsilon$ the iteration $x_{n+1} = g(x_n)$ doesn't converge to α.

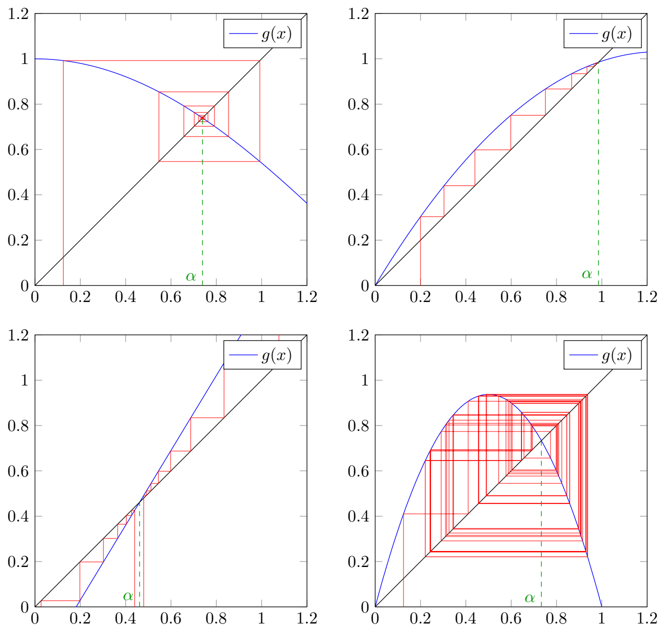


Figure 1.2.12: Cobweb diagrams. In the figures at the top, α is a attractor point, that is, $|g'(\alpha)| < 1$. More precisely, the figure at the top left occurs when $-1 < g'(\alpha) \leq 0$ and the figure at the top right when $0 \leq g'(\alpha) < 1$. In the figure at bottom left, α is a repulsor point. Finally, in the figure at bottom right the iteration $x_{n+1} = g(x_n)$ has no limit. It is said to have a *chaotic behavior*.

Order of convergence

Definition 6.26 (Order of convergence). Let (x_n) be a sequence of real numbers that converges to $\alpha \in \mathbb{R}$. We say (x_n) has *order of convergence* $p \in \mathbb{R}^+$ if exists $C > 0$ such that:

$$\lim_{n\to\infty} \frac{|x_{n+1} - \alpha|}{|x_n - \alpha|^p} = C$$

The constant C is called *asymptotic error constant*. For the case $p = 1$, we need $C < 1$. In this case the convergence is called *linear convergence*; for $p = 2$, is called *quadratic convergence*; for $p = 3$, *cubic convergence*... If it's satisfied that

$$\lim_{n\to\infty} \frac{|x_{n+1} - \alpha|}{|x_n - \alpha|^p} = 0$$

for some $p \in \mathbb{R}^+$, we say the sequence has *order of convergence at least* p.

Theorem 6.27. Let $g : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^p$ and let α be a fixed point of g. Suppose

$$g'(\alpha) = g''(\alpha) = \cdots = g^{(p-1)}(\alpha) = 0$$

with $|g'(\alpha)| < 1$ if $p = 1$. Then, the iteration $x_{n+1} = g(x_n)$, with x_0 sufficiently close to α, has order of convergence at least p. If, moreover, $g^{(p)}(\alpha) \neq 0$, then the previous iteration has order of convergence p with asymptotic error constant $C = \frac{|g^{(p)}(\alpha)|}{p!}$.

Theorem 6.28. Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^3$ and α be a simple zero of f. If $f''(\alpha) \neq 0$, then Newton-Raphson method for finding α has quadratic convergence with asymptotic error constant $C = \frac{1}{2}\left|\frac{f''(\alpha)}{f'(\alpha)}\right|$.
If $f \in \mathcal{C}^{m+2}$, and α is a zero of multiplicity $m > 1$, then Newton-Raphson method has linear convergence but Newton-Raphson modified method has at least quadratic convergence.

Theorem 6.29. Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^3$ and let α be a simple zero of f. Then, Chebyshev's method for finding α has at least cubic convergence.

Definition 6.30. We define the *computational efficiency of an algorithm* as a function $E(p,t)$, where t is the time taken for each iteration of the method and p is the order of convergence of the method. $E(p,t)$ must satisfy the following properties:

1. $E(p,t)$ is increasing with respect to the variable p and decreasing with respect to t.
2. $E(p,t) = E(p^m, mt)$ $\forall m \in \mathbb{R}$.

Examples of such functions are the following:

$$E(p,t) = \frac{\log p}{t} \qquad E(p,t) = p^{1/t}$$

Sequence acceleration

Method 6.31 (Aitken's Δ^2 method). Let (x_n) be a sequence of real numbers. We denote:

$$\Delta x_n := x_{n+1} - x_n$$
$$\Delta^2 x_n := \Delta x_{n+1} - \Delta x_n = x_{n+2} - 2x_{n+1} + x_n$$

Aitken's Δ^2 method is the transformation of the sequence (x_n) into a sequence y_n, defined as:

$$y_n := x_n - \frac{(\Delta x_n)^2}{\Delta^2 x_n} = x_n - \frac{(x_{n+1} - x_n)^2}{x_{n+2} - 2x_{n+1} + x_n}$$

with $y_0 = x_0$.

Theorem 6.32. Let (x_n) be a sequence of real numbers such that $\lim\limits_{n\to\infty} x_n = \alpha$, $x_n \neq \alpha$ $\forall n \in \mathbb{N}$ and $\exists C$, $|C| < 1$, satisfying

$$x_{n+1} - \alpha = (C + \delta_n)(x_n - \alpha) \quad \text{with} \quad \lim_{n\to\infty} \delta_n = 0$$

Then, the sequence (y_n) obtained from Aitken's Δ^2 process is well-defined and

$$\lim_{n\to\infty} \frac{y_n - \alpha}{x_n - \alpha} = 0^{[76]}$$

[76] This means that Aitken's Δ^2 method produces an acceleration of the convergence of the sequence (x_n).

Method 6.33 (Steffensen's method). Let $g : \mathbb{R} \to \mathbb{R}$ be a continuous function and suppose we have an iterative method $x_{n+1} = g(x_n)$. Then, for each step n we can consider a new iteration y_{n+1}, with $y_0 = x_0$, given by:

$$y_{n+1} = y_n - \frac{(g(y_n) - y_n)^2}{g(g(y_n)) - 2g(y_n) + y_n}$$

Proposition 6.34. Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^2$ and α be a simple zero of f. Then, Steffensen's method for finding α has at least quadratic convergence[77].

Zeros of polynomials

Lemma 6.35. Let $p(z) = a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{C}[x]$ with $a_n \neq 0$. We define

$$\lambda := \max\left\{\left|\frac{a_i}{a_n}\right| : i = 0, 1, \ldots, n-1\right\}$$

Then, if $p(\alpha) = 0$ for some $\alpha \in \mathbb{C}$, $|\alpha| \leq \lambda + 1$.

Definition 6.36 (Strum's sequence). Let (f_i), $i = 0, \ldots, n$, be a sequence of continuous functions defined on $[a, b] \subset \mathbb{R}$ and $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^1$ such that $f(a)f(b) \neq 0$. We say (f_n) is a *Sturm's sequence* if:

1. $f_0 = f$.
2. If $\alpha \in [a, b]$ satisfies $f_0(\alpha) = 0 \implies f_0'(\alpha) f_1(\alpha) > 0$.
3. For $i = 1, \ldots, n-1$, if $\alpha \in [a, b]$ satisfies $f_i(\alpha) = 0 \implies f_{i-1}(\alpha) f_{i+1}(\alpha) < 0$.
4. $f_n(x) \neq 0 \ \forall x \in [a, b]$.

Definition 6.37. Let (a_i), $i = 0, \ldots, n$, be a sequence. We define $\nu(a_i)$ as the number of sign variations of the sequence

$$\{a_0, a_1, \ldots, a_n\}$$

without taking into account null values.

Theorem 6.38 (Sturm's theorem). Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^1$ such that $f(a)f(b) \neq 0$ and with a finite number of zeros. Let (f_i), $i = 0, \ldots, n$, be a Sturm sequence defined on $[a, b]$. Then, the number of zeros of f on $[a, b]$ is

$$\nu(f_i(a)) - \nu(f_i(b))$$

Lemma 6.39. Let $p \in \mathbb{C}[x]$ be a polynomial. Then, the polynomial $q = \dfrac{p}{\gcd(p, p')}$ has the same roots as p but all of them are simple.

Proposition 6.40. Let $p \in \mathbb{R}[x]$ be a polynomial with $\deg p = m$. We define $f_0 = \dfrac{p}{\gcd(p, p')}$ and $f_1 = f_0'$. If $\deg f_0 = n$, then for $i = 0, 1, \ldots, n-2$, we define f_{i+2} as:

$$f_i(x) = q_{i+1}(x) f_{i+1}(x) - f_{i+2}(x)$$

(similarly to the euclidean division between f_i and f_{i+1}). Then, f_n is constant and hence the sequence (f_i), $i = 0, \ldots, n$, is a Sturm sequence.

Theorem 6.41 (Budan-Fourier theorem). Let $p \in \mathbb{R}[x]$ be a polynomial with $\deg p = n$. Consider the sequence $(p^{(i)})$, $i = 0, \ldots, n$. If $p(a)p(b) \neq 0$, the number of zeros of p on $[a, b]$ is:

$$\nu\left(p^{(i)}(a)\right) - \nu\left(p^{(i)}(b)\right) - 2k, \quad \text{for some } k \in \mathbb{N} \cup \{0\}$$

Corollary 6.42 (Descartes' rule of signs). Let $p = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{R}[x]$ be a polynomial. If $p(0) \neq 0$, the number of zeros of p on $[0, \infty)$ is:

$$\nu(a_i) - 2k, \quad \text{for some } k \in \mathbb{N} \cup \{0\}$$ [78]

Theorem 6.43 (Gershgorin circle theorem). Let $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{C})$ be a complex matrix and λ be an eigenvalue of A. For all $i, j \in \{1, 2, \ldots, n\}$ we define:

$$r_i = \sum_{\substack{k=1 \\ k \neq i}}^{n} |a_{ik}| \qquad R_i = \{z \in \mathbb{C} : |z - a_{ii}| \leq r_i\}$$

$$c_j = \sum_{\substack{k=1 \\ k \neq j}}^{n} |a_{kj}| \qquad C_j = \{z \in \mathbb{C} : |z - a_{jj}| \leq c_j\}$$

Then, $\lambda \in \bigcup_{i=1}^n R_i$ and $\lambda \in \bigcup_{j=1}^n C_j$. Moreover in each connected component of $\bigcup_{i=1}^n R_i$ or $\bigcup_{j=1}^n C_j$ there are as many eigenvalues (taking into account the multiplicity) as disks R_i or C_j, respectively.

Corollary 6.44. Let $p(z) = a_0 + a_1 z + \cdots + a_n z^n + z^{n+1} \in \mathbb{C}[x]$. We define

$$r = \sum_{i=1}^{n-1} |a_i| \quad c = \max\{|a_0|, |a_1| + 1, \ldots, |a_{n-1}| + 1\}$$

Then, if $p(\alpha) = 0$ for some $\alpha \in \mathbb{C}$,

$$\alpha \in (B(0,1) \cup B(-a_n, r)) \cap (B(-a_n, 1) \cup B(0, c))$$

1.2.6.3 | Interpolation

Definition 6.45. We denote by Π_n the *vector space of polynomials with real coefficients and degree less than or equal to n.*

Definition 6.46. Suppose we have a family of real valued functions $\mathfrak{C}$ and a set of points $\{(x_i, y_i)\}_{i=0}^n := \{(x_i, y_i) \in \mathbb{R}^2 : i = 0, \ldots, n \text{ and } x_j \neq x_k \iff j \neq k\}$. These points $\{(x_i, y_i)\}_{i=0}^n$ are called *support points*. The *interpolation problem* consists in finding a function $f \in \mathfrak{C}$ such that $f(x_i) = y_i$ for $i = 0, \ldots, n$[79].

[77] Note that the advantage of Steffensen's method over Newton-Raphson method is that in the former we don't need the differentiability of the function whereas in the latter we do.

[78] Note that making the change of variable $t = -x$ one can obtain the number of zeros on $(-\infty, 0]$ of p by considering the polynomial $p(t)$.

[79] Types of interpolation are for example polynomial interpolation, trigonometric interpolation, Padé interpolation, Hermite interpolation and spline interpolation.

Polynomial interpolation

Definition 6.47. Given a set of support points $\{(x_i, y_i)\}_{i=0}^n$, *Lagrange's interpolation problem* consists in finding a polynomial $p_n \in \Pi_n$ such that $p_n(x_i) = y_i$ for $i = 0, 1, \ldots, n$.

Definition 6.48. Let $\{(x_i, y_i)\}_{i=0}^n$ be a set of support points. We define $\omega_n(x) \in \mathbb{R}[x]$ as:

$$\omega_n(x) = \prod_{i=0}^{n}(x - x_i)$$

We define *Lagrange basis polynomials* $\ell_i(x) \in \mathbb{R}[x]$ as:

$$\ell_i(x) = \frac{\omega_n(x)}{(x - x_i)\omega_n(x_i)} = \prod_{\substack{j=0\\j\neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

Proposition 6.49. Let $\{(x_i, y_i)\}_{i=0}^n$ be a set of support points. Then, Lagrange's interpolation problem has a unique solution and this is:

$$p_n(x) = \sum_{i=0}^{n} y_i \ell_i(x)$$

Method 6.50 (Neville's algorithm). Let $\{(x_i, y_i)\}_{i=0}^n$ be a set of support points, $\{i_0, \ldots, i_k\} \subset \{0, \ldots, n\}$ and $P_{i_0,\ldots,i_k}(x) \in \Pi_k$ be such that $P_{i_0,\ldots,i_k}(x_{i_j}) = y_{i_j}$ for $j = 0, \ldots, k$. Then, it is satisfied that:

1. $P_i(x) = y_i$.
2. $P_{i_0,\ldots,i_k}(x) = \dfrac{\begin{vmatrix} P_{i_1,\ldots,i_k}(x) & x - x_{i_k} \\ P_{i_0,\ldots,i_{k-1}}(x) & x - x_{i_0}\end{vmatrix}}{x_{i_k} - x_{i_0}}$.

Definition 6.51. Let $f : \mathbb{R} \to \mathbb{R}$ be a function and $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be pairwise distinct points. We define the *divided difference of order k of f applied to* $\{x_i\}_{i=0}^k$, denoted by $f[x_0, \ldots, x_k]$, as the coefficient of x^k of the interpolating polynomial with support points $\{(x_i, f(x_i))\}_{i=0}^k$.

Proposition 6.52. Let $f : \mathbb{R} \to \mathbb{R}$ be a function and $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be pairwise distinct points. Lagrange interpolating polynomial with support points $\{(x_i, f(x_i))\}_{i=0}^n$ is:

$$p_n(x) = f[x_0] + \sum_{j=1}^{n} f[x_0, \ldots, x_j]\omega_{j-1}(x)$$

Method 6.53 (Newton's divided differences method). Let $f : \mathbb{R} \to \mathbb{R}$ be a function. For $x \in \mathbb{R}$, we have $f[x] = f(x)$. And if $\{x_i\}_{i=0}^n \subset \mathbb{R}$ are different points, then

$$f[x_0, \ldots, x_n] = \frac{f[x_1, \ldots, x_n] - f[x_0, \ldots, x_{n-1}]}{x_n - x_0}$$

Theorem 6.54. Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^{n+1}$, $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be pairwise distinct points and $p_n \in \mathbb{R}[x]$ be the interpolating polynomial with support points $\{(x_i, f(x_i))\}_{i=0}^n$. Then, $\forall x \in [a, b]$,

$$f(x) - p_n(x) = \frac{f^{(n+1)}(\xi_x)}{(n+1)!}\omega_n(x)$$

where $\xi_x \in \langle x_0, \ldots, x_n, x\rangle$[80].

[80]The interval $\langle a_1, \ldots, a_k\rangle$ is defined as $\langle a_1, \ldots, a_k\rangle := (\min(a_1, \ldots, a_k), \max(a_1, \ldots, a_k))$.

Lemma 6.55. Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^{n+1}$ and $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be pairwise distinct points. Then: $\exists \xi \in \langle x_0, \ldots, x_n\rangle$ such that:

$$f[x_0, \ldots, x_n] = \frac{f^{(n)}(\xi)}{n!}$$

Proposition 6.56. Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^{n+1}$, $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be pairwise distinct points and $\sigma \in S_n$. Then,

$$f[x_0, \ldots, x_n] = f[x_{\sigma(0)}, \ldots, x_{\sigma(n)}]$$

Definition 6.57. Let $\{(x_i, y_i)\}_{i=0}^n$ be support points. The points $\{x_i\}_{i=0}^n$ are *equally-spaced* if

$$x_i = x_0 + ih, \quad \text{for } i = 0, \ldots, n \text{ and with } h := \frac{x_n - x_0}{n}$$

Proposition 6.58. Let $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be equally-spaced points such that $x_i = x_0 + ih$, where $h = \frac{x_n - x_0}{n}$. Then:

$$\max\{|\omega_n(x)| : x \in [x_0, x_n]\} \leq \frac{h^{n+1}n!}{4}$$

Definition 6.59. Let $f : [a, b] \to \mathbb{R}$ be a function and $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be equally-spaced points. We define:

$$\Delta f(x) := f(x + h) - f(x)$$
$$\Delta^{n+1} f(x) := \Delta(\Delta^n f(x))$$

Lemma 6.60. Let $f : [a, b] \to \mathbb{R}$ be a function and $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be equally-spaced points. Then:

$$\Delta^n f(x_0) = n!h^n f[x_0, \ldots, x_n]$$

Corollary 6.61. Let $f \in \mathbb{R}[x]$ with $\deg f = n$. Suppose we interpolate f with equally-spaced nodes. Then, $\Delta^n f(x) \equiv$ constant.

Hermite interpolation

Definition 6.62. Given sets of points $\{x_i\}_{i=0}^m \subset \mathbb{R}$, $\{n_i\}_{i=0}^m \subset \mathbb{N}$ and $\{y_i^{(k)} : k = 0, \ldots, n_i - 1\}_{i=0}^m \subset \mathbb{R}$, *Hermite interpolation problem* consists in finding a polynomial $h_n \in \Pi_n$ such that $\sum_{i=0}^m n_i = n + 1$ and

$$h_n^{(k)}(x_i) = y_i^{(k)} \text{ for } i = 0, \ldots, m \text{ and } k = 0, \ldots, n_i - 1$$

Proposition 6.63. Hermite interpolation problem has a unique solution.

Definition 6.64. Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^n$ and $\{x_i\}_{i=0}^n \subset \mathbb{R}$ be points. We define $f[x_i, \overset{(n+1)}{\ldots}, x_i]$ as:

$$f[x_i, \overset{(n+1)}{\ldots}, x_i] = \frac{f^{(n)}(x_i)}{n!}$$

Theorem 6.65. Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^{n+1}$, $\{x_i\}_{i=0}^m \subset \mathbb{R}$ be pairwise distinct points and $\{n_i\}_{i=0}^m \subset \mathbb{N}$ be such that $\sum_{i=0}^m n_i = n + 1$. Let h_n be the Hermite interpolating polynomial of f with nodes $\{x_i\}_{i=0}^m \subset \mathbb{R}$, that is,

$$h_n^{(k)}(x_i) = f^{(k)}(x_i) \text{ for } i = 0, \ldots, m \text{ and } k = 0, \ldots, n_i - 1.$$

Then, $\forall x \in [a, b]$ $\exists \xi_x \in \langle x_0, \ldots, x_n, x\rangle$ such that:

$$f(x) - h_n(x) = \frac{f^{(n+1)}(\xi_x)}{(n+1)!}(x - x_0)^{n_0} \cdots (x - x_m)^{n_m}$$

Spline interpolation

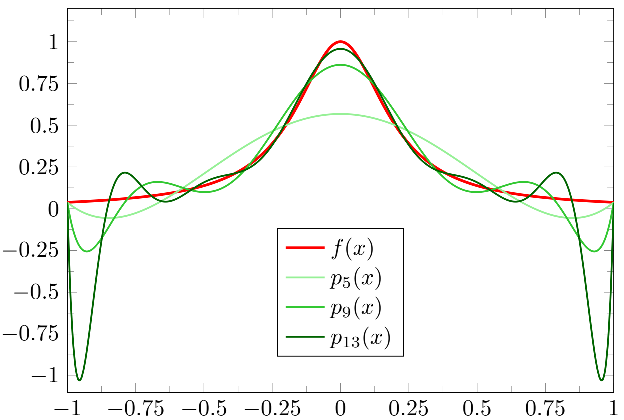


Figure 1.2.13: Runge's phenomenon. In this case $f(x) = \frac{1}{1+25x^2}$. $p_5(x)$ is the 5th-order Lagrange interpolating polynomial with equally-spaced interpolating points; $p_9(x)$, the 9th-order Lagrange interpolating polynomial with equally-spaced interpolating points, and $p_{13}(x)$, the 13th-order Lagrange interpolating polynomial with equally-spaced interpolating points.

Definition 6.66 (Spline). Let $\{(x_i, y_i)\}_{i=0}^n$ be support points of an interval $[a, b]$. A *spline of degree* p is a function $s : [a, b] \to \mathbb{R}$ of class $\mathcal{C}^{p-1}$ satisfying:

$$s_{|_{[x_i,x_{i+1}]}} \in \mathbb{R}[x] \quad \text{and} \quad \deg s_{|_{[x_i,x_{i+1}]}} = p$$

for $i = 0, \ldots, n-1$ and $s(x_i) = y_i$ for $i = 0, \ldots, n$. The most common case are splines of degree $p = 3$ or *cubic splines*. In this case we can impose two more conditions on their definition in one of the following ways:

1. *Natural cubic spline*:
$$s''(x_0) = s''(x_n) = 0$$
2. *Cubic Hermite spline*: Given $y_0', y_n' \in \mathbb{R}$,
$$s'(x_0) = y_0', \quad s'(x_n) = y_n'$$
3. *Cubic periodic spline*:
$$s'(x_0) = s'(x_n), \quad s''(x_0) = s''(x_n)$$

Definition 6.67. Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^2$. We define the *seminorm*[81] *of* f as:

$$\|f\|^2 = \int_a^b (f''(x))^2 \mathrm{d}x$$

Proposition 6.68. Let $f : [a, b] \to \mathbb{R}$ be a function of class $\mathcal{C}^2$ interpolating the support points $\{(x_i, y_i)\}_{i=0}^n \subset \mathbb{R}^2$, $a \leq x_0 < \cdots < x_n \leq b$. If s a spline associated with $\{(x_i, y_i)\}_{i=0}^n$, then:

$$\|f-s\|^2 = \|f\|^2 - \|s\|^2 - 2(f'-s)s''\Big|_{x_0}^{x_n} + 2\sum_{i=1}^n (f-s)s'''\Big|_{x_{i-1}^+}^{x_i^-}$$

Theorem 6.69. Let $f : [a, b] \to \mathbb{R}$ a function of class $\mathcal{C}^2$ interpolating the support points $\{(x_i, y_i)\}_{i=0}^n \subset \mathbb{R}^2$, $a \leq x_0 < \cdots < x_n \leq b$. If s is the natural cubic spline associated with $\{(x_i, y_i)\}_{i=0}^n$, then:

$$\|s\| \leq \|f\|$$[82]

1.2.6.4 | Numerical differentiation and integration

Differentiation

Theorem 6.70 (Intermediate value theorem). Let $f : [a, b] \to \mathbb{R}$ be a continuous function, $x_0, \ldots, x_n \in [a, b]$ and $\alpha_0, \ldots, \alpha_n \geq 0$. Then, $\exists \xi \in [a, b]$ such that:

$$\sum_{i=0}^n \alpha_i f(x_i) = \left(\sum_{i=0}^n \alpha_i\right) f(\xi)$$

Theorem 6.71 (Forward and backward difference formula of order 1). Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^2$. Then, the forward difference formula of order 1 is:

$$f'(a) = \frac{f(a+h) - f(a)}{h} - \frac{f''(\xi)}{2}h$$

where $\xi \in \langle a, a+h\rangle$. Analogously, the backward difference formula of order 1 is:

$$f'(a) = \frac{f(a) - f(a-h)}{h} + \frac{f''(\eta)}{2}h$$

where $\eta \in \langle a-h, a\rangle$.

Theorem 6.72 (Symmetric difference formula of order 1). Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^3$. Then, the symmetric difference formula of order 1 is:

$$f'(a) = \frac{f(a+h) - f(a-h)}{2h} - \frac{f^{(3)}(\xi)}{6}h^2$$

where $\xi \in \langle a-h, a+h\rangle$.

Theorem 6.73 (Symmetric difference formula of order 2). Let $f : \mathbb{R} \to \mathbb{R}$ be a function of class $\mathcal{C}^4$. Then, the symmetric difference formula of order 2 is:

$$f''(a) = \frac{f(a+h) - 2f(a) + f(a-h)}{h^2} - \frac{f^{(4)}(\xi)}{12}h^2$$

where $\xi \in \langle a-h, a, a+h\rangle$.

Richardson extrapolation

Theorem 6.74 (Richardson extrapolation). Suppose we have a function f that approximate a value α with an error that depends on a small quantity h. That is:

$$\alpha = f(h) + a_1 h^{k_1} + a_2 h^{k_2} + \cdots$$

with $k_1 < k_2 < \cdots$ and a_i are unknown constants. Given $q > 0$, we define:

$$D_1(h) = f(h) \quad \text{and} \quad D_{n+1}(h) = \frac{q^{k_n} D_n(h/q) - D_n(h)}{q^{k_n} - 1}$$

And we can observe that $\alpha = D_{n+1}(h) + O(h^{k_{n+1}})$.

[81] The term *seminorm* has been used instead of *norm* to emphasize that not all properties of a norm are satisfied with this definition.
[82] We can interpret this result as the natural cubic spline being the configuration that require the least "energy" to be "constructed".

Integration

Definition 6.75. Let $f : [a,b] \to \mathbb{R}$ be a continuous function, $\{x_i\}_{i=0}^n \subset [a,b]$ be a set of nodes and p_n be the Lagrange interpolating polynomial with support points $\{(x_i, f(x_i))\}_{i=0}^n$. We define the *quadrature formula* as:

$$\int_a^b f(x)\mathrm{d}x \approx \int_a^b p_n(x)\mathrm{d}x$$

Lemma 6.76. Let $f : [a,b] \to \mathbb{R}$ be a continuous function $\{x_i\}_{i=0}^n \subset [a,b]$ be a set of nodes. Then:

$$\int_a^b f(x)\mathrm{d}x \approx \sum_{i=1}^n a_i f(x_i) \quad \text{where } a_i := \int_a^b \ell_i(x)\mathrm{d}x$$

Definition 6.77. The *degree of precision* of a quadrature formula is the largest $m \in \mathbb{N}$ such that the formula is exact for x^k $\forall k = 0, 1, \ldots, m$.

Lemma 6.78. Let $p \in \Pi_n$ be a polynomial and $\{x_i\}_{i=0}^n \subset [a,b]$ be a set of nodes. Then:

$$\int_a^b p(x)\mathrm{d}x = \sum_{i=0}^n a_i p(x_i)$$

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

Newton-Cotes formulas

Theorem 6.79 (Mean value theorem for integrals). Let $f, g : [a,b] \to \mathbb{R}$ be such that f is continuous and g integrable. Suppose that g does not change the sign on $[a,b]$. Then, $\exists \xi \in [a,b]$ such that:

$$\int_a^b f(x)g(x)\mathrm{d}x = f(\xi)\int_a^b g(x)\mathrm{d}x$$

Theorem 6.80 (Closed Newton-Cotes Formulas). Let $f : [a,b] \to \mathbb{R}$ be a function and $\{x_i\}_{i=0}^n \subset [a,b]$ be a set of equally-spaced points. If $I = \int_a^b f(x)\mathrm{d}x$ and $h = \frac{b-a}{n}$, then $\exists \xi \in [a,b]$ such that:

- If n is even and $f \in \mathcal{C}^{n+2}$:
$$I = \sum_{i=0}^n a_i f(x_i) + \frac{h^{n+3} f^{n+2}(\xi)}{(n+2)!}\int_0^n t\prod_{i=0}^n (t-i)\mathrm{d}t$$
- If n is odd and $f \in \mathcal{C}^{n+1}$:
$$I = \sum_{i=0}^n a_i f(x_i) + \frac{h^{n+2} f^{n+1}(\xi)}{(n+1)!}\int_0^n \prod_{i=0}^n (t-i)\mathrm{d}t$$ [83]

Corollary 6.81 (Trapezoidal rule). Let $f : [a,b] \to \mathbb{R}$ be a function of class $\mathcal{C}^2$. Then, $\exists \xi \in [a,b]$ such that:

$$\int_a^b f(x)\mathrm{d}x = \frac{h}{2}(f(a) + f(b)) - \frac{f''(\xi)}{12}h^3$$

where $h = b - a$. This is the case $n = 1$ of closed Newton-Cotes formulas.

Corollary 6.82 (Simpson's rule). Let $f : [a,b] \to \mathbb{R}$ be a function of class $\mathcal{C}^4$. Then, $\exists \xi \in [a,b]$ such that:

$$\int_a^b f(x)\mathrm{d}x = \frac{h}{3}\left(f(a) + 4f\left(\frac{a+b}{2}\right) + f(b)\right) - \frac{f^{(4)}(\xi)}{90}h^5$$

where $h = \frac{b-a}{2}$. This is the case $n = 2$ of closed Newton-Cotes formulas.

Theorem 6.83 (Composite Trapezoidal rule). Let $f : [a,b] \to \mathbb{R}$ be a function of class $\mathcal{C}^4$, $h = \frac{b-a}{n}$ and $x_j = a + jh$ for each $j = 0, 1, \ldots, n$. Then, $\exists \xi \in [a,b]$ such that:

$$I = \int_a^b f(x)\mathrm{d}x = \frac{h}{2}\left[f(a) + 2\sum_{j=1}^{n-1} f(x_j) + f(b)\right] - \\ - \frac{f''(\xi)(b-a)}{12}h^2$$

We denote by $T(f, a, b, h)$ the approximation of I by trapezoidal rule.

Theorem 6.84 (Composite Simpson's rule). Let $f : [a,b] \to \mathbb{R}$ be a function of class $\mathcal{C}^4$, n be an even number, $h = \frac{b-a}{n}$ and $x_j = a + jh$ for each $j = 0, 1, \ldots, n$. Then, $\exists \xi \in [a,b]$ such that:

$$I = \int_a^b f(x)\mathrm{d}x = \frac{h}{3}\left[f(a) + 2\sum_{j=1}^{n/2-1} f(x_{2j}) + \right. \\ \left. + 4\sum_{j=1}^{n/2} f(x_{2j-1}) + f(b)\right] - \frac{f^{(4)}(\xi)(b-a)}{180}h^4$$

We denote by $S(f, a, b, h)$ the approximation of I by Simpson's rule.

Romberg method

Definition 6.85. We define *Bernoulli polynomials* $B_n(x)$ as $B_0(x) = 1$, $B_1(x) = x - \frac{1}{2}$ and

$$B'_{k+1} = (k+1)B_k \quad \text{for } k \geq 1$$

Bernoulli numbers are $B_n = B_n(0)$, $\forall n \geq 0$[84].

Theorem 6.86 (Euler-Maclaurin formula). Let $f \in \mathcal{C}^{2m+2}([a,b])$ be a function. Then:

$$T(f, a, b, h) = \int_a^b f(t)\mathrm{d}t + \sum_{k=1}^m \frac{B_{2k}h^{2k}}{(2k)!}\left(f^{(2k-1)}(b) - \right. \\ \left. - f^{(2k-1)}(a)\right) + \frac{(b-a)B_{2m+2}h^{2m+1}}{(2m+2)!}f^{(2m+2)}(\xi)$$

where $h = \frac{b-a}{n}$, B_n are the Bernoulli numbers and $\xi \in [a,b]$.

[83] Note that when n is even, the degree of precision is $n+1$, although the interpolation polynomial is of degree at most n. When n is odd, the degree of precision is only n.

[84] Exponential generating function of the sequence (B_n) of Bernoulli numbers is $\frac{x}{\mathrm{e}^x - 1} = \sum_{n=1}^\infty \frac{B_n}{n!}x^n$.

Theorem 6.87 (Romberg method). Let $f \in \mathcal{C}^{2m+2}([a,b])$ be a function. Then, by Euler-Maclaurin formula, we obtain:

$$T(f,a,b,h)=\int_a^b f(t)\mathrm{d}t+\beta_1 h^2+\beta_2 h^4+\cdots$$

where $h=\frac{b-a}{n}$. For $n=1,2,\ldots$ we define:

$$T_{n,1}=T\left(f,a,b,\frac{b-a}{2^n}\right)\quad T_{n,m+1}=\frac{4^m T_{n+1,m}-T_{n,m}}{4^m-1}$$

for $m\leq n$. Then, we can observe that:

$$T_{n,m}=\int_a^b f(t)\mathrm{d}t+O\left(\left(\frac{b-a}{2^n}\right)^{2m}\right)$$

Orthogonal polynomials

Definition 6.88. Let $f,g:[a,b]\to\mathbb{R}$ be continuous function and $\omega(x):[a,b]\to\mathbb{R}^+$ be a weight function. The expression

$$\langle f,g\rangle=\int_a^b\omega(x)f(x)g(x)\mathrm{d}x$$

defines a positive semidefinite dot product in the vector space of bounded functions on $[a,b]$.

Definition 6.89 (Orthogonal polynomials). Let $\mathfrak{P}=\{\phi_i(x)\in\mathbb{R}[x]:\deg\phi_i(x)=i,i\in\mathbb{N}\cup\{0\}\}$ be a family of polynomials and $\omega(x):[a,b]\to\mathbb{R}^+$ be a weight function. We say $\mathfrak{P}$ is *orthogonal with respect to the weight $\omega(x)$ on an interval $[a,b]$* if

$$\langle\phi_i,\phi_j\rangle=\int_a^b\omega(x)\phi_i(x)\phi_j(x)\mathrm{d}x=0\iff i\neq j$$

Note that $\langle\phi_i,\phi_i\rangle>0$ for each $i\in\mathbb{N}\cup\{0\}$.

Lemma 6.90. We define $\mathfrak{P}_n$ as $\mathfrak{P}_n=\{\phi_i(x)\in\Pi_n:\deg\phi_i(x)=i \text{ and } \langle\phi_i,\phi_j\rangle=0\iff i\neq j, i=0,\ldots,n\}$. Then, $\mathfrak{P}_n$ is an *orthogonal basis of* Π_n.

Lemma 6.91. Let $\phi_k\in\mathfrak{P}_k$ and $q\in\Pi_n$. Then, $\langle q,\phi_k\rangle=0$ for each $k>n$.

Lemma 6.92. Let $\phi_n\in\mathfrak{P}_n$. Then, $\forall n\in\mathbb{N}\cup\{0\}$, all roots of ϕ_n are real, simple and contained in the interval (a,b), where the associated weight function $\omega(x)$ is defined.

Theorem 6.93 (Existence of orthogonal polynomials). For each $n\in\mathbb{N}\cup\{0\}$ there exists a unique monic orthogonal polynomial ϕ_n with $\deg\phi_n=n$, associated with the weight function $\omega(x)$, defined by:

$$\phi_0=1\quad\phi_1(x)=x-\alpha_0$$
$$\phi_{n+1}(x)=(x-\alpha_n)\phi_n(x)-\beta_n\phi_{n-1}(x)$$

with $\alpha_n=\frac{\langle\phi_n,x\phi_n\rangle}{\langle\phi_n,\phi_n\rangle}$ $\forall n\in\mathbb{N}\cup\{0\}$ and $\beta_n=\frac{\langle\phi_n,\phi_n\rangle}{\langle\phi_{n-1},\phi_{n-1}\rangle}$ $\forall n\in\mathbb{N}$.

Definition 6.94 (Chebyshev polynomials). *Chebyshev polynomials T_n* are the orthogonal polynomials defined on $[-1,1]$ with the weight $\omega(x)=\frac{1}{\sqrt{1-x^2}}$. These can be defined recursively as:

$$T_0(x)=1\quad T_1(x)=x$$
$$T_{n+1}(x)=2xT_n(x)-T_{n-1}(x)$$

for $n=1,2,\ldots$ Moreover $T_n(x)=\cos(n\arccos(x))$ which implies that the roots of $T_n(x)$ are:

$$x_k=\cos\left(\frac{2k-1}{2n}\pi\right)\quad\text{for } k=1,\ldots,n$$

Definition 6.95 (Laguerre polynomials). *Laguerre polynomials L_n* are the orthogonal polynomials defined on $[0,\infty)$ with the weight $\omega(x)=\mathrm{e}^{-x}$. These can be defined recursively as:

$$L_0(x)=1\quad L_1(x)=1-x$$
$$L_{n+1}(x)=\frac{(2n+1-x)L_n(x)-nL_{n-1}(x)}{n+1}$$

for $n=1,2,\ldots$ The closed form of these polynomials is:

$$L_n(x)=\sum_{k=0}^n\binom{n}{k}\frac{(-1)^k}{k!}x^k$$

Definition 6.96 (Legendre polynomials). *Legendre polynomials P_n* are the orthogonal polynomials defined on $[-1,1]$ with the weight $\omega(x)=1$. These can be defined recursively as:

$$P_0(x)=1\quad P_1(x)=x$$
$$P_{n+1}(x)=\frac{(2n+1)xP_n(x)-nP_{n-1}(x)}{n+1}$$

for $n=1,2,\ldots$ The closed form of these polynomials is:

$$P_n(x)=\frac{1}{2^n}\sum_{k=0}^n\binom{n}{k}^2(x-1)^{n-k}(x+1)^k$$

Gaußian quadrature

Definition 6.97. Let $f:[a,b]\to\mathbb{R}$ be a function and $\omega(x):[a,b]\to\mathbb{R}^+$ be a weight function. Given a set of nodes $\{x_i\}_{i=1}^n\subset[a,b]$, the *quadrature formula with weight $\omega(x)$ of a function f* is

$$\int_a^b\omega(x)f(x)\mathrm{d}x\approx\sum_{i=1}^n\omega_i f(x_i)\quad\text{with } \omega_i=\int_a^b\omega(x)\ell_i(x)\mathrm{d}x$$

Lemma 6.98. Let $f:[a,b]\to\mathbb{R}$ be a function and $\{x_i\}_{i=1}^n$ be the zeros of the orthogonal polynomial $\phi_n\in\mathfrak{P}_n$ with weight $\omega(x)$ on the interval $[a,b]$. Then, the formula

$$\int_a^b\omega(x)f(x)\mathrm{d}x\approx\sum_{i=1}^n\omega_i f(x_i)\quad\text{with } \omega_i=\int_a^b\omega(x)\ell_i(x)\mathrm{d}x$$

is exact for all polynomials in Π_{2n-1}.

Proposition 6.99. Let $f:[a,b]\to\mathbb{R}$ be a function and $\{x_i\}_{i=1}^n$ be the zeros of the orthogonal polynomial $\phi_n\in\mathfrak{P}_n$ with weight $\omega(x)$ on the interval $[a,b]$. Then, in the formula

$$\int_a^b\omega(x)f(x)\mathrm{d}x\approx\sum_{i=1}^n\omega_i f(x_i)$$

the values ω_i are positive and real for $i=1,\ldots,n$.

Theorem 6.100. Let $f:[a,b]\to\mathbb{R}$ be a function of class $\mathcal{C}^{2n}$ and $\{x_i\}_{i=1}^n$ be the zeros of the orthogonal polynomial $\phi_n\in\mathfrak{P}_n$ with weight $\omega(x)$ on the interval $[a,b]$. Then:

$$\int_a^b \omega(x)f(x)\mathrm{d}x-\sum_{i=1}^n\omega_i f(x_i)=\frac{f^{2n}(\xi)}{(2n)!}\langle\phi_n,\phi_n\rangle$$

where $\xi\in[a,b]$.

1.2.6.5 | Numerical linear algebra

Triangular matrices

Definition 6.101. A matrix $\mathbf{A}=(a_{ij})\in\mathcal{M}_n(\mathbb{C})$ is *upper triangular* if $a_{ij}=0$ whenever $i>j$. That is, $\mathbf{A}$ is of the form:

$$\mathbf{A}=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ 0 & a_{22} & \ddots & \vdots\\ \vdots & \ddots & \ddots & a_{(n-1)n}\\ 0 & \cdots & 0 & a_{nn}\end{pmatrix}$$

Definition 6.102. A matrix $\mathbf{A}=(a_{ij})\in\mathcal{M}_n(\mathbb{C})$ is *lower triangular* if $a_{ij}=0$ whenever $j>i$. That is, $\mathbf{A}$ is of the form:

$$\mathbf{A}=\begin{pmatrix}a_{11} & 0 & \cdots & 0\\ a_{21} & a_{22} & \ddots & \vdots\\ \vdots & \ddots & \ddots & 0\\ a_{n1} & \cdots & a_{n(n-1)} & a_{nn}\end{pmatrix}$$

Definition 6.103. A linear system with a triangular matrix associated is called a *triangular system*.

Matrix norms

Definition 6.104. A *matrix norm* on the vector space $\mathcal{M}_n(\mathbb{R})$ is a function $\|\cdot\|:\mathcal{M}_n(\mathbb{R})\to\mathbb{R}$ satisfying all properties of a norm[85] and that:

$$\|\mathbf{AB}\|\leq\|\mathbf{A}\|\|\mathbf{B}\|,\quad\forall\mathbf{AB}\in\mathcal{M}_n(\mathbb{R})$$

Definition 6.105. Let $\|\cdot\|_\alpha$ be a vector norm. We say a matrix norm $\|\cdot\|_\beta$ is *compatible with* $\|\cdot\|_\alpha$ if

$$\|\mathbf{Av}\|_\alpha\leq\|\mathbf{A}\|_\beta\|\mathbf{v}\|_\alpha\quad\forall\mathbf{A}\in\mathcal{M}_n(\mathbb{R})\text{ and }\forall\mathbf{v}\in\mathbb{R}^n$$

Definition 6.106. Let $\|\cdot\|$ be a vector norm and $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$. We define a *subordinated matrix norm* $\|\cdot\|$ as:

$$\|\mathbf{A}\|=\max\{\|\mathbf{Av}\|:\mathbf{v}\in\mathbb{R}^n\text{ such that }\|\mathbf{v}\|=1\}=$$
$$=\sup\left\{\frac{\|\mathbf{Av}\|}{\|\mathbf{v}\|}:\mathbf{v}\in\mathbb{R}^n\text{ such that }\mathbf{v}\neq 0\right\}$$

Lemma 6.107. All subordinated matrix norms are compatible.

Lemma 6.108. For all subordinated matrix norm $\|\cdot\|$, we have $\|\mathbf{I}\|=1$.

Definition 6.109. Let $\mathbf{A}\in\mathcal{M}_n(\mathbb{C})$ be a matrix. We define the *spectrum* $\sigma(\mathbf{A})$ *of* $\mathbf{A}$ as:

$$\sigma(\mathbf{A})=\{\lambda\in\mathbb{C}:\lambda\text{ is and eigenvalue of }\mathbf{A}\}$$

[85] See definition 3.2.

Definition 6.110. Let $\mathbf{A}\in\mathcal{M}_n(\mathbb{C})$ be a matrix. We define the *spectral radius* $\rho(\mathbf{A})$ *of* $\mathbf{A}$ as:

$$\rho(\mathbf{A})=\max\{|\lambda|\in\mathbb{C}:\lambda\in\sigma(\mathbf{A})\}$$

Proposition 6.111. Let $\mathbf{v}=(v_1,\ldots,v_n)\in\mathbb{R}^n$ and $\mathbf{A}=(a_{ij})\in\mathcal{M}_n(\mathbb{R})$. Given the vector norms:

$$\|\mathbf{v}\|_1=\sum_{i=1}^n|v_i|$$
$$\|\mathbf{v}\|_2=\sqrt{\sum_{i=1}^n v_i^2}$$
$$\|\mathbf{v}\|_\infty=\max\{|v_i|:i=1,\ldots,n\}$$

their subordinated matrix norms are respectively:

$$\|\mathbf{A}\|_1=\max\left\{\sum_{i=1}^n|a_{ij}|:j=1,\ldots,n\right\}$$
$$\|\mathbf{A}\|_2=\sqrt{\rho(\mathbf{A}^\mathrm{T}\mathbf{A})}$$
$$\|\mathbf{A}\|_\infty=\max\left\{\sum_{j=1}^n|a_{ij}|:i=1,\ldots,n\right\}$$

Proposition 6.112 (Properties of matrix norms).

1. Matrix norms are continuous functions.
2. Given two matrix norms $\|\cdot\|_\alpha$ and $\|\cdot\|_\beta$, there exist $\ell,L\in\mathbb{R}^+$ such that:
$$\ell\|\mathbf{A}\|_\beta\leq\|\mathbf{A}\|_\alpha\leq L\|\mathbf{A}\|_\beta\quad\forall\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$$
3. For all subordinated matrix norm $\|\cdot\|$ and for all $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$:
$$\rho(\mathbf{A})\leq\|\mathbf{A}\|$$
4. Given a matrix $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$ and $\varepsilon>0$, there exist a matrix norm $\|\cdot\|_{\mathbf{A},\varepsilon}$ such that:
$$\rho(\mathbf{A})\leq\|\mathbf{A}\|_{\mathbf{A},\varepsilon}\leq\rho(\mathbf{A})+\varepsilon$$

Definition 6.113. A matrix $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$ is *convergent* if $\displaystyle\lim_{k\to\infty}\mathbf{A}^k=\mathbf{0}$.

Theorem 6.114. Let $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$. The following statements are equivalent:

1. $\mathbf{A}$ is convergent.
2. $\displaystyle\lim_{k\to\infty}\|\mathbf{A}^k\|=\mathbf{0}$ for some matrix norm $\|\cdot\|$.
3. $\rho(\mathbf{A})<1$.

Corollary 6.115. Let $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$. If there is a matrix norm $\|\cdot\|$ satisfying $\|\mathbf{A}\|<1$, then $\mathbf{A}$ converges.

Theorem 6.116. Let $\mathbf{A}\in\mathcal{M}_n(\mathbb{R})$.

1. The series $\sum_{k=0}^\infty\mathbf{A}^k$ converges if and only if $\mathbf{A}$ converge.

2. If $\mathbf{A}$ is convergent, then $\mathbf{I}_n - \mathbf{A}$ is non-singular and moreover:
$$(\mathbf{I}_n - \mathbf{A})^{-1} = \sum_{k=0}^{\infty} \mathbf{A}^k$$

Corollary 6.117. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. If there is a subordinated matrix norm $\|\cdot\|$ satisfying $\|\mathbf{A}\| < 1$, then $\mathbf{I}_n - \mathbf{A}$ is non-singular and moreover:
$$\frac{1}{1+\|\mathbf{A}\|} \leq \|(\mathbf{I}_n - \mathbf{A})^{-1}\| \leq \frac{1}{1-\|\mathbf{A}\|}$$

Matrix condition number

Definition 6.118. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$. We define the *condition number $\kappa(\mathbf{A})$ of* $\mathbf{A}$ as:
$$\kappa(\mathbf{A}) = \|\mathbf{A}\|\|\mathbf{A}^{-1}\|$$

Theorem 6.119. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$, $\mathbf{Ax} = \mathbf{b}$ be a system of linear equations and $\|\cdot\|$ be a subordinated matrix norm. Suppose we know $\mathbf{A}$ and $\mathbf{b}$ with absolute errors $\Delta\mathbf{A}$ and $\Delta\mathbf{b}$, respectively. Therefore, we actually have to solve the system:
$$(\mathbf{A} + \Delta\mathbf{A})(\mathbf{x} + \Delta\mathbf{x}) = (\mathbf{b} + \Delta\mathbf{b})$$
If $\|\Delta\mathbf{A}\| < \frac{1}{\|\mathbf{A}^{-1}\|}$, then:
$$\frac{\|\Delta\mathbf{x}\|}{\|\mathbf{x}\|} \leq \frac{\kappa(\mathbf{A})}{1 - \|\mathbf{A}^{-1}\|\|\Delta\mathbf{A}\|}\left(\frac{\|\Delta\mathbf{b}\|}{\|\mathbf{b}\|} + \frac{\|\Delta\mathbf{A}\|}{\|\mathbf{A}\|}\right)$$

Theorem 6.120. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$ and $\|\cdot\|$ be a subordinated matrix norm. Then:

1. $\kappa(\mathbf{A}) \geq \rho(\mathbf{A})\rho(\mathbf{A}^{-1})$.
2. If $\mathbf{b}, \mathbf{z} \in \mathbb{R}^n$ are such that $\mathbf{Az} = \mathbf{b}$, then:
$$\|\mathbf{A}^{-1}\| \geq \frac{\|\mathbf{z}\|}{\|\mathbf{b}\|}$$
3. If $\mathbf{B} \in \mathcal{M}_n(\mathbb{R})$ is a singular matrix, then:
$$\kappa(\mathbf{A}) \geq \frac{\|\mathbf{A}\|}{\|\mathbf{A} - \mathbf{B}\|}$$

Iterative methods

Definition 6.121. Suppose we want to solve the system $\mathbf{Ax} = \mathbf{b}$, where $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ and $\mathbf{b} \in \mathbb{R}^n$. We choose a matrix $\mathbf{N} \in \mathrm{GL}_n(\mathbb{R})$ and define $\mathbf{P} := \mathbf{N} - \mathbf{A}$. Then:
$$\mathbf{Ax} = \mathbf{b} \iff \mathbf{x} = \mathbf{N}^{-1}\mathbf{Px} + \mathbf{N}^{-1}\mathbf{b} =: \mathbf{Mx} + \mathbf{N}^{-1}\mathbf{b}$$
The matrix $\mathbf{M}$ is called the *iteration matrix*. This defines a fixed-point iteration in the following way:
$$\begin{cases} \mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b} \\ \mathbf{x}^{(0)} \quad \text{(initial approximation)} \end{cases}$$

Theorem 6.122. The iterative method $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ is convergent if and only if $\mathbf{M}$ is convergent and if and only if $\rho(\mathbf{M}) < 1$.

Corollary 6.123. If $\|\mathbf{M}\| < 1$ for some matrix norm, then the iterative method $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ is convergent.

Definition 6.124. We define the *rate of convergence R* of an iterative method $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ as:
$$R = -\log(\rho(\mathbf{M}))$$

Proposition 6.125. Let $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ be an iterative method to approximate the solution $\mathbf{x}$ of a system of equations $\mathbf{Ax} = \mathbf{b}$. Then, we have the following estimations:
$$\|\mathbf{x}^{(k)} - \mathbf{x}\| \leq \frac{\|\mathbf{M}\|^k}{1 - \|\mathbf{M}\|}\|\mathbf{x}^{(1)} - \mathbf{x}^{(0)}\| \qquad \text{(a priori)}$$
$$\|\mathbf{x}^{(k)} - \mathbf{x}\| \leq \frac{\|\mathbf{M}\|}{1 - \|\mathbf{M}\|}\|\mathbf{x}^{(k)} - \mathbf{x}^{(k-1)}\| \qquad \text{(a posteriori)}$$

Definition 6.126. Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$. We say A is *strictly diagonally dominant by rows* if
$$|a_{ii}| > \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}|$$
We say A is *strictly diagonally dominant by columns* if
$$|a_{jj}| > \sum_{\substack{i=1 \\ i \neq j}}^{n} |a_{ij}|$$

Definition 6.127 (Jacobi method). Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$ be such that $\prod_{i=1}^n a_{ii} \neq 0$, $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{Ax} = \mathbf{b}$ be a system of equations. *Jacobi method* consists in defining a matrix $\mathbf{N}$ (and consequently matrices $\mathbf{P}$ and $\mathbf{M}$ as defined above) in the following way:
$$\mathbf{N} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$
$$\mathbf{P} = \mathbf{N} - \mathbf{A} = \begin{pmatrix} 0 & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -a_{(n-1)n} \\ -a_{n1} & \cdots & -a_{n(n-1)} & 0 \end{pmatrix}$$
$$\mathbf{M} = \mathbf{N}^{-1}\mathbf{P} = \begin{pmatrix} 0 & \frac{-a_{12}}{a_{11}} & \cdots & \frac{-a_{1n}}{a_{11}} \\ \frac{-a_{21}}{a_{22}} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{-a_{(n-1)n}}{a_{(n-1)(n-1)}} \\ \frac{-a_{n1}}{a_{nn}} & \cdots & \frac{-a_{n(n-1)}}{a_{nn}} & 0 \end{pmatrix}$$
Note that the iterative method $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ can also be written as:
$$x_i^{(k+1)} = \frac{1}{a_{ii}}\left(b_i - \sum_{\substack{j=1 \\ j \neq i}}^{n} a_{ij}x_j^{(k)}\right) \qquad \text{for } i = 1, \ldots, n.$$

Theorem 6.128. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be such that $\prod_{i=1}^n a_{ii} \neq 0$ and $\mathbf{b} \in \mathbb{R}^n$. If $\mathbf{A}$ is strictly diagonally dominant by rows or columns, then Jacobi method applied to solve the system $\mathbf{Ax} = \mathbf{b}$ is convergent.

Definition 6.129 (Gauß-Seidel method). Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$ be such that $\prod_{i=1}^n a_{ii} \neq 0$, $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{Ax} = \mathbf{b}$ be a system of equations. *Gauß-Seidel method* consists in defining a matrix $\mathbf{N}$ (and consequently matrices $\mathbf{P}$ and $\mathbf{M}$ as defined above) in the following way:

$$\mathbf{N} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_{n1} & \cdots & a_{n(n-1)} & a_{nn} \end{pmatrix}$$

$$\mathbf{P} = \mathbf{N} - \mathbf{A} = \begin{pmatrix} 0 & -a_{12} & \cdots & -a_{1n} \\ 0 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -a_{(n-1)n} \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$\mathbf{M} = \mathbf{N}^{-1}\mathbf{P}$$

Note that the iterative method $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ can also be written as:

$$x_i^{(k+1)} = \frac{1}{a_{ii}}\left(b_i - \sum_{j=i+1}^{n} a_{ij}x_j^{(k)} - \sum_{j=1}^{i-1} a_{ij}x_j^{(k+1)}\right)$$

for $i = 1, \ldots, n$.

Theorem 6.130. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be such that $\prod_{i=1}^n a_{ii} \neq 0$ and $\mathbf{b} \in \mathbb{R}^n$. If $\mathbf{A}$ is strictly diagonally dominant by rows, then Gauß-Seidel method applied to solve the system $\mathbf{Ax} = \mathbf{b}$ is convergent.

Method 6.131 (Over-relaxation methods). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$, $\mathbf{Ax} = \mathbf{b}$ be a system of equations and $\alpha \in \mathbb{R}$ be a parameter (called *relaxation factor*). *Over-relaxation methods* consist in defining matrices $\mathbf{N}(\alpha)$, $\mathbf{P}(\alpha)$ and $\mathbf{M}(\alpha)$ as follows:

$$\mathbf{P}(\alpha) = \mathbf{N}(\alpha) - \mathbf{A} \qquad \mathbf{M}(\alpha) = \mathbf{N}(\alpha)^{-1}\mathbf{P}(\alpha)$$

Then, the iterative method can be written as:

$$\mathbf{x}^{(k+1)} = \mathbf{M}(\alpha)\mathbf{x}^{(k)} + \mathbf{N}(\alpha)^{-1}\mathbf{b}$$

Method 6.132 (Successive over-relaxation method). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$ be such that $\alpha \neq -1$ and $\mathbf{x}^{(k+1)} = \mathbf{N}^{-1}\mathbf{Px}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ be an iterative method. *Successive over-relaxation method (SOR)* consists in defining

$$\mathbf{N}(\alpha) = (1+\alpha)\mathbf{N} \quad \text{and} \quad \mathbf{P}(\alpha) = \mathbf{P} + \alpha\mathbf{N}$$

because it must be true that $\mathbf{A} = \mathbf{N}(\alpha) - \mathbf{P}(\alpha)$. Then, the previous iteration becomes:

$$\mathbf{x}^{(k+1)} = \mathbf{N}(\alpha)^{-1}\mathbf{P}(\alpha)\mathbf{x}^{(k)} + \mathbf{N}(\alpha)^{-1}\mathbf{b}$$

Definition 6.133. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$ be such that $\alpha \neq -1$ and $\mathbf{x}^{(k+1)} = \mathbf{N}(\alpha)^{-1}\mathbf{P}(\alpha)\mathbf{x}^{(k)} + \mathbf{N}(\alpha)^{-1}\mathbf{b}$ be a SOR method. Since $\mathbf{M}(\alpha) = \mathbf{N}(\alpha)^{-1}\mathbf{P}(\alpha)$, we have that

$$\mathbf{M}(\alpha) = \frac{1}{1+\alpha}(\mathbf{M} + \alpha\mathbf{I}_n)$$

and therefore:

$$\sigma(\mathbf{M}(\alpha)) = \left\{\frac{\lambda+\alpha}{1+\alpha} : \lambda \in \sigma(\mathbf{M})\right\}$$

Theorem 6.134. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{x}^{(k+1)} = \mathbf{Mx}^{(k)} + \mathbf{N}^{-1}\mathbf{b}$ be an iterative method. Suppose that the eigenvalues λ_i, $i = 1, \ldots, n$, of $\mathbf{M}$ are all real and satisfy:

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n < 1$$

Then, the associated SOR method given by $\mathbf{N}(\alpha) = (1+\alpha)\mathbf{N}$ and $\mathbf{P}(\alpha) = \mathbf{P} + \alpha\mathbf{N}$ converges for $\alpha > -\frac{1+\lambda_1}{2}$. Moreover, $\rho(\mathbf{M}(\alpha))$ is minimum whenever $\alpha = -\frac{\lambda_1+\lambda_n}{2}$.

Eigenvalues and eigenvectors

Definition 6.135. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a matrix whose eigenvalues are $\lambda_1, \ldots, \lambda_n$. λ_1 is called *dominant eigenvalue of* $\mathbf{A}$ if $|\lambda_1| > |\lambda_i|$ for $i = 2, \ldots, n$. The associated eigenvector to λ_1 is called *dominant eigenvector of* $\mathbf{A}$.

Definition 6.136. We say a matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ is *reducible* if $\exists \mathbf{P} \in \mathcal{M}_n(\mathbb{R})$ a permutation matrix, such that

$$\mathbf{PAP}^{-1} = \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{F} & \mathbf{G} \end{pmatrix}$$

for some square matrices $\mathbf{E}$ and $\mathbf{G}$ and for some other matrix $\mathbf{F}$. A matrix is *irreducible* if it is not reducible.

Theorem 6.137 (Perron-Frobenius theorem). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a non-negative irreducible matrix. Then, $\rho(\mathbf{A})$ is a real number and it is the dominant eigenvalue.

Method 6.138 (Power method). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. For simplicity, suppose $\mathbf{A}$ is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_n$ and eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Suppose $|\lambda_1| > |\lambda_2| \geq \cdots \geq |\lambda_n|$. The *power method* consists in finding an approximation of the dominant eigenvalue λ_1 starting from an initial approximation $\mathbf{x}^{(0)}$ of $\mathbf{v}_1$. We define:

$$\mathbf{x}^{(k+1)} = \mathbf{Ax}^{(k)} \qquad k \geq 0$$

Suppose $\mathbf{x}^{(0)} = \sum_{i=1}^n \alpha_i\mathbf{v}_i$. If we denote by $\mathbf{v}_{i,m}$ the m-th component of the vector $\mathbf{v}_i$ and choose ℓ such that $\mathbf{v}_{1,\ell} \neq 0$. Then:

$$\lim_{k\to\infty} \frac{\mathbf{x}^{(k)}}{\lambda_1^k} = \mathbf{v}_1 \qquad \lim_{k\to\infty} \frac{\mathbf{x}_\ell^{(k+1)}}{\mathbf{x}_\ell^{(k)}} = \lambda_1$$

provided that $\alpha_1 \neq 0$. More precisely we have:

$$\frac{\mathbf{x}_\ell^{(k+1)}}{\mathbf{x}_\ell^{(k)}} = \lambda_1 + O\left(\left|\frac{\lambda_2}{\lambda_1}\right|^k\right)$$

Method 6.139 (Normalized power method). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ and $\|\cdot\|$ be a vector norm[86]. For simplicity suppose $\mathbf{A}$ is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_n$ and eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Suppose $|\lambda_1| > |\lambda_2| \geq \cdots \geq |\lambda_n|$. The *normalized power method* consists in defining

$$\mathbf{y}^{(k)} = \frac{\mathbf{x}^{(k)}}{\|\mathbf{x}^{(k)}\|} \quad \mathbf{x}^{(k+1)} = \mathbf{A}\mathbf{y}^{(k)} \quad \text{for } k \geq 0$$

Suppose $\mathbf{x}^{(0)} = \sum_{i=1}^n \alpha_i \mathbf{v}_i$ such that $\alpha_1 \neq 0$. If we choose ℓ such that $\mathbf{v}_{1,\ell} \neq 0$. Then:

$$\lim_{k\to\infty} \mathbf{x}^{(k)} = \mathbf{v}_1 \qquad \lim_{k\to\infty} \frac{\mathbf{x}_\ell^{(k+1)}}{\mathbf{y}_\ell^{(k)}} = \lambda_1$$

More precisely we have:

$$\frac{\mathbf{x}_\ell^{(k+1)}}{\mathbf{y}_\ell^{(k)}} = \lambda_1 + O\left(\left|\frac{\lambda_2}{\lambda_1}\right|^k\right)$$

Method 6.140 (Rayleigh quotient). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. Suppose we have a power method $\mathbf{x}^{(k+1)} = \mathbf{A}\mathbf{x}^{(k)}$ to approximate the dominant eigenvalue λ_1 of $\mathbf{A}$. Then *Rayleigh quotient* approximates λ_1 as follows:

$$\lim_{k\to\infty} \frac{\left(\mathbf{x}^{(k+1)}\right)^{\mathrm{T}} \cdot \mathbf{x}^{(k)}}{\left(\mathbf{x}^{(k)}\right)^{\mathrm{T}} \cdot \mathbf{x}^{(k)}} = \lambda_1$$

More precisely:

$$\frac{\left(\mathbf{x}^{(k+1)}\right)^{\mathrm{T}} \cdot \mathbf{x}^{(k)}}{\left(\mathbf{x}^{(k)}\right)^{\mathrm{T}} \cdot \mathbf{x}^{(k)}} = \lambda_1 + O\left(\left|\frac{\lambda_2}{\lambda_1}\right|^{2k}\right)$$

If instead of a power method, we have a normalized power method $\mathbf{y}^{(k)} = \frac{\mathbf{x}^{(k)}}{\|\mathbf{x}^{(k)}\|}$, $\mathbf{x}^{(k+1)} = \mathbf{A}\mathbf{y}^{(k)}$, then:

$$\lim_{k\to\infty} \frac{\left(\mathbf{x}^{(k+1)}\right)^{\mathrm{T}} \cdot \mathbf{y}^{(k)}}{\left(\mathbf{y}^{(k)}\right)^{\mathrm{T}} \cdot \mathbf{y}^{(k)}} = \lambda_1$$

Method 6.141 (Inverse power method). Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ and $\mu \in \mathbb{C}$. The *inverse power method* consists in finding an approximation of the eigenvalue λ closest to μ starting from an initial approximation $\mathbf{x}^{(0)}$ of its associated eigenvector $\mathbf{v}$. So we applied the power method to the matrix $(\mathbf{A} - \mu\mathbf{I}_n)^{-1}$. That is, we have the recurrence:

$$\mathbf{y}^{(k)} = \frac{\mathbf{x}^{(k)}}{\|\mathbf{x}^{(k)}\|} \quad \mathbf{x}^{(k+1)} = (\mathbf{A} - \mu\mathbf{I}_n)^{-1}\mathbf{y}^{(k)} \quad \text{for } k \geq 0$$

Or, equivalently,

$$\mathbf{y}^{(k)} = \frac{\mathbf{x}^{(k)}}{\|\mathbf{x}^{(k)}\|} \quad (\mathbf{A} - \mu\mathbf{I}_n)\mathbf{x}^{(k+1)} = \mathbf{y}^{(k)} \quad \text{for } k \geq 0$$

Therefore, in each step we have to solve a system of equations to obtain $\mathbf{x}^{(k+1)}$. Finally[87], if we choose ℓ such that $\mathbf{v}_\ell \neq 0$, then:

$$\lim_{k\to\infty} \mathbf{x}^{(k)} = \mathbf{v} \qquad \lim_{k\to\infty} \frac{\mathbf{x}_\ell^{(k+1)}}{\mathbf{y}_\ell^{(k)}} = \frac{1}{\lambda - \mu}$$ [88]

Exact methods

Method 6.142 (Gaussian elimination). Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{C})$. We define $a_{ij}^{(1)} := a_{ij}$ for $i, j = 1, \ldots, n$ and

$$\mathbf{A}^{(1)} := \begin{pmatrix} a_{11}^{(1)} & a_{12}^{(1)} & \cdots & a_{1n}^{(1)} \\ a_{21}^{(1)} & a_{22}^{(1)} & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{(n-1)n}^{(1)} \\ a_{n1}^{(1)} & \cdots & a_{n(n-1)}^{(1)} & a_{nn}^{(1)} \end{pmatrix}$$

For $i = 2, \ldots, n$ we define $m_{i1} = \frac{a_{i1}^{(1)}}{a_{11}^{(1)}}$ to transform the matrix $\mathbf{A}^{(1)}$ into a matrix $\mathbf{A}^{(2)}$ defined by $a_{ij}^{(2)} = a_{ij}^{(1)} - m_{i1}a_{1j}^{(1)}$ for $i = 2, \ldots, n$ and by $a_{ij}^{(1)}$ for $i = 1$. That is, we obtain a matrix of the form:

$$\mathbf{A}^{(1)} \sim \begin{pmatrix} a_{11}^{(1)} & a_{12}^{(1)} & a_{13}^{(1)} & \cdots & a_{1n}^{(1)} \\ 0 & a_{22}^{(2)} & a_{23}^{(2)} & \cdots & a_{2n}^{(2)} \\ 0 & a_{32}^{(2)} & a_{33}^{(2)} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & a_{(n-1)n}^{(2)} \\ 0 & a_{n2}^{(2)} & \cdots & a_{n(n-1)}^{(2)} & a_{nn}^{(2)} \end{pmatrix} =: \mathbf{A}^{(2)}$$

Proceeding analogously creating multipliers m_{ij}, $i > j$, to echelon the matrix $\mathbf{A}$, at the end we will obtain an upper triangular matrix $\mathbf{A}^{(n)}$ of the form:

$$\mathbf{A}^{(n)} = \begin{pmatrix} a_{11}^{(1)} & a_{12}^{(1)} & a_{13}^{(1)} & a_{14}^{(1)} & \cdots & a_{1n}^{(1)} \\ 0 & a_{22}^{(2)} & a_{23}^{(2)} & a_{24}^{(2)} & \cdots & a_{2n}^{(2)} \\ 0 & 0 & a_{33}^{(3)} & a_{34}^{(3)} & \cdots & a_{3n}^{(3)} \\ 0 & 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & a_{(n-1)(n-1)}^{(n-1)} & a_{(n-1)n}^{(n-1)} \\ 0 & 0 & 0 & \cdots & 0 & a_{nn}^{(n)} \end{pmatrix}$$

Method 6.143. *Partial pivoting* method in gaussian elimination consists in selecting as the pivot element the entry with largest absolute value from the column of the matrix that is being considered.

Method 6.144. *Complete pivoting* method in gaussian elimination interchanges both rows and columns in order to use the largest element (by absolute value) in the matrix as the pivot.

Definition 6.145 (LU descompostion). Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$ be a matrix. A *LU decomposition of* $\mathbf{A}$ is an expression $\mathbf{A} = \mathbf{L}\mathbf{U}$, where $\mathbf{L} = (\ell_{ij}), \mathbf{U} = (u_{ij}) \in \mathcal{M}_n(\mathbb{R})$

[86] For power method it is recommended to use $\|\cdot\|_\infty$.

[87] Alternatively, here we could have applied the Rayleigh quotient.

[88] There's another method that applies power method to the matrix $\mathbf{A} - \mu\mathbf{I}_n$ with the same purpose as the inverse power method but without having to solve a system of equations in each iteration. In this case, this method gives the farthest eigenvalue of $\mathbf{A}$ from μ.

are matrices of the form:

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \ell_{21} & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \ell_{n1} & \cdots & \ell_{n(n-1)} & 1 \end{pmatrix} \tag{1.2.2}$$

$$\mathbf{U} = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & u_{(n-1)n} \\ 0 & \cdots & 0 & u_{nn} \end{pmatrix} \tag{1.2.3}$$

Lemma 6.146. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{Ax} = \mathbf{b}$ be a system of linear equations. Suppose $\mathbf{A} = \mathbf{LU}$ for some matrices $\mathbf{L}, \mathbf{U} \in \mathcal{M}_n(\mathbb{R})$ of the form of (1.2.2) and (1.2.3), respectively. Then, to solve the system $\mathbf{Ax} = \mathbf{b}$ we can proceed in the following way:

1. Solve the triangular system $\mathbf{Ly} = \mathbf{b}$.
2. Solve the triangular system $\mathbf{Ux} = \mathbf{y}$.

Proposition 6.147. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$. Then:

1. If LU decomposition exists, it is unique.
2. If we can make the gaussian elimination without pivoting rows, then[89]:

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ m_{21} & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ m_{n1} & \cdots & m_{n(n-1)} & 1 \end{pmatrix} \qquad \mathbf{U} = \mathbf{A}^{(n)}$$

Definition 6.148. A *permutation matrix* is a square binary matrix that has exactly one entry of 1 in each row and each column and 0 elsewhere.

Proposition 6.149. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$. Then, there exist a permutation matrix $\mathbf{P} \in \mathcal{M}_n(\mathbb{R})$ and matrices $\mathbf{L}, \mathbf{U} \in \mathcal{M}_n(\mathbb{R})$ of the form of (1.2.2) and (1.2.3), respectively, such that:

$$\mathbf{PA} = \mathbf{LU}$$

Definition 6.150 (QR descompostion). Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$ be a matrix. A *QR decomposition of* $\mathbf{A}$ is an expression $\mathbf{A} = \mathbf{QR}$, where $\mathbf{Q}, \mathbf{R} \in \mathcal{M}(\mathbb{R})$ are such that $\mathbf{Q}$ is orthogonal and $\mathbf{R}$ is upper triangular.

Lemma 6.151. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$, $\mathbf{b} \in \mathbb{R}^n$ and $\mathbf{Ax} = \mathbf{b}$ be a system of linear equations. Suppose $\mathbf{A} = \mathbf{QR}$ for some orthogonal matrix $\mathbf{Q}$ and some upper triangular matrix $\mathbf{R}$, both of size n. Then, solve the system $\mathbf{Ax} = \mathbf{b}$ is equivalent to solve the triangular system $\mathbf{Rx} = \mathbf{Q}^{\mathrm{T}}\mathbf{b}$.

Lemma 6.152. Let $\mathbf{Q}$ be an orthogonal matrix. Then:

1. $\det \mathbf{Q} = \pm 1$.
2. $\|\mathbf{Q}\|_2 = 1$.

[89] In practice, LU decomposition is implemented making gaussian elimination and storing the values m_{ij} in the position ij of the matrix $\mathbf{A}^{(k)}$, where there should be a 0.

Chapter 1.3

Third year

1.3.1 Complex analysis and Fourier analysis

1.3.2 Differential equations

1.3.3 Differential geometry

1.3.4 Galois theory

1.3.5 Probability

1.3.6 Statistics

1.3.7 Topology

Part II

Physics

2.0.8 Physical constants

Quantity	Symbol	Value
Avogadro constant	N_A	6.02214×10^{23} mol^{-1}
Boltzmann constant	k_B	1.38065×10^{-23} J $\cdot$ K^{-1}
Coulomb constant	k	8.98755×10^{9} N $\cdot$ m^2 $\cdot$ C^{-2}
Electron mass	m_e	9.10939×10^{-31} kg
Elementary charge	e	1.60218×10^{-19} C
Gravitational constant	G	6.67430×10^{-11} m^3 $\cdot$ kg^{-1} $\cdot$ s^{-2}
Neutron mass	m_{n}	1.67493×10^{-27} kg
Planck constant	h	6.62607×10^{-34} J $\cdot$ Hz^{-1}
Proton mass	m_{p}	1.67262×10^{-27} kg
Reduced Planck constant	$\hbar$	1.05457×10^{-34} J $\cdot$ s
Rydberg constant	R_H	1.09737×10^{7} m^{-1}
Speed of light in vacuum	c	299792458 m $\cdot$ s^{-1}
Stefan-Boltzmann constant	σ	5.67037×10^{-8} W $\cdot$ m^{-2} $\cdot$ K^{-4}
Surface gravity	g	9.80665 m $\cdot$ s^{-2}
Universal gas constant	R	8.31446 J $\cdot$ K^{-1} $\cdot$ mol^{-1}
Vacuum electric permittivity	ε_0	8.85419×10^{-12} F $\cdot$ m^{-1}
Vacuum magnetic permeability	μ_0	1.25664×10^{-6} N $\cdot$ A^{-2}
Wien's displacement constant	b	2.89777×10^{-3} m $\cdot$ K

Chapter 2.1

First year

2.1.1 Electricity and magnetism

2.1.1.1 | Vector calculus

	Formula (in Cartesian coordinates)
Gradient	$\boldsymbol{\nabla} f := \frac{\partial f}{\partial x}\mathbf{e}_x + \frac{\partial f}{\partial y}\mathbf{e}_y + \frac{\partial f}{\partial z}\mathbf{e}_z$
Divergence	$\mathbf{div}\,\mathbf{A} := \boldsymbol{\nabla}\cdot\mathbf{A} = \frac{\partial A_x}{\partial x} + \frac{\partial A_z}{\partial z} + \frac{\partial A_z}{\partial z}$
Curl	$\mathbf{rot}\,\mathbf{A} := \boldsymbol{\nabla}\times\mathbf{A} = \begin{vmatrix} \mathbf{e}_x & \mathbf{e}_y & \mathbf{e}_z \\ \frac{\partial}{\partial x} & \frac{\partial}{\partial y} & \frac{\partial}{\partial z} \\ A_x & A_y & A_z \end{vmatrix} = \left(\frac{\partial A_z}{\partial z} - \frac{\partial A_y}{\partial y}\right)\mathbf{e}_x + \left(\frac{\partial A_x}{\partial x} - \frac{\partial A_z}{\partial z}\right)\mathbf{e}_y + \left(\frac{\partial A_y}{\partial y} - \frac{\partial A_x}{\partial x}\right)\mathbf{e}_z$
Laplacian	$\nabla^2 f := \boldsymbol{\nabla}\cdot\boldsymbol{\nabla} f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} + \frac{\partial^2 f}{\partial z^2}$

2.1.1.2 | Electrostatics

Electric force

Proposition 1.1. The charge of any object is a multiple of the elementary charge e.

Law 1.2 (Charge conservation). The total electric charge in an isolated system never changes.

Law 1.3 (Coulomb's law). The force applied by a point charge q_1 over another point charge q_2 along a straight line is:

$$\mathbf{F}_1 = K\frac{q_1 q_2}{\|\mathbf{r}_{12}\|^2}\hat{\mathbf{r}}_{12}$$

where $\mathbf{r}_{12}$ is the vectorial distance between the charges, $\hat{\mathbf{r}}_{12} = \frac{\mathbf{r}_{12}}{\|\mathbf{r}_{12}\|}$ is the unit vector pointing from q_2 to q_1 and K is the Coulomb constant.

Principle 1.4 (Superposition principle). Consider a set of N point charges q_i which are at a distance $\mathbf{r}_i$ from another point charge Q. Then, the net force exerted by the N point charges to the charge Q is:

$$\mathbf{F}_Q = \sum_{i=1}^{N} K\frac{q_i Q}{\|\mathbf{r}_i\|^2}\hat{\mathbf{r}}_i$$

where $\hat{\mathbf{r}}_i$ is the unit vector pointing from q_i to Q.

Electric field

Definition 1.5. Given a point charge Q, the *electric field* created by this charge at a distance $\mathbf{r}$ from it is given by:

$$\mathbf{E} = K\frac{Q}{\|\mathbf{r}\|^2}\hat{\mathbf{r}}$$

Principle 1.6 (Superposition principle). Consider a set of N point charges q_i which are at a distance $\mathbf{r}_i$ from a point A. Then, the net electric field created by the N point charges at point A is:

$$\mathbf{E}_A = \sum_{i=1}^{N} K\frac{q_i}{\|\mathbf{r}_i\|^2}\hat{\mathbf{r}}_i$$

where $\hat{\mathbf{r}}_i$ is the unit vector pointing from q_i to A. In the case of a continuous distribution of charge we will have:

$$\mathbf{E} = \int \mathrm{d}\mathbf{E} = \int K\frac{\mathrm{d}q}{r^2}\hat{\mathbf{r}}$$

Note that $\mathrm{d}q = \lambda \mathrm{d}\ell$, $\mathrm{d}q = \sigma \mathrm{d}S$ or $\mathrm{d}q = \rho \mathrm{d}V$ depending on whether the distribution of charge is linear, superficial or volumetric. In each respective case, λ, σ and ρ represent the charge densities.

Electric flux and Gauß' law

Definition 1.7. Let $\mathbf{A}$ be a vectorial field and $\mathrm{d}\mathbf{S}$ be a small surface area. The *flux* $\mathrm{d}\Phi$ of $\mathbf{A}$ through $\mathrm{d}\mathbf{S}$ is:

$$\mathrm{d}\Phi = \mathbf{A}\cdot \mathrm{d}\mathbf{S}$$

And the flux through a surface S will be:

$$\Phi = \iint_S \mathrm{d}\Phi = \iint_S \mathbf{A}\cdot \mathrm{d}\mathbf{S}$$

Corollary 1.8. The electric flux of a field $\mathbf{E}$ through a surface S is:

$$\Phi_E = \iint_S \mathbf{E}\cdot \mathrm{d}\mathbf{S}$$

Law 1.9 (Gauß' law). The net electric flux through a closed surface S is equal to $\frac{1}{\varepsilon_0}$ times the net electric charge Q_{int} within that closed surface.

$$\Phi_E = \oiint_S \mathbf{E}\cdot \mathrm{d}\mathbf{S} = \frac{Q_{\text{int}}}{\varepsilon_0}$$

Electric potential

Proposition 1.10. The variation of the electrostatic potential energy that undergoes a point charge q when moving a distance $\mathrm{d}\boldsymbol{\ell}$ is:

$$\mathrm{d}U = -\mathbf{F}\cdot \mathrm{d}\boldsymbol{\ell} = -q\mathbf{E}\cdot \mathrm{d}\boldsymbol{\ell}$$

Therefore:

$$\Delta U = U(b) - U(a) = \int_a^b \mathrm{d}U = -\int_a^b q\mathbf{E}\cdot \mathrm{d}\boldsymbol{\ell}$$

Proposition 1.11. The work done by the electric field on a particle between two points a and b is $-\Delta U = U_a - U_b$, while the work done by the external forces on that particle in that interval is $\Delta U = U_b - U_a$.

Definition 1.12. The *potential difference* between two points a and b over a point charge q when an electric field $\mathbf{E}$ is applied to it is:

$$\mathrm{d}V := \frac{\mathrm{d}U}{q} = -\mathbf{E}\cdot \mathrm{d}\boldsymbol{\ell} \implies \Delta V = \frac{\Delta U}{q} = -\int_a^b \mathbf{E}\cdot \mathrm{d}\boldsymbol{\ell}$$

Definition 1.13. If we choose the infinite as an origin of potential (that is, $V = 0$ when $r = \infty$), we can define the *electric potential* at a distance r from a point charge q as:

$$V = K\frac{q}{r}$$

Principle 1.14 (Superposition principle). Consider a set of N point charges q_i which are at a distance $\mathbf{r}_i$ from a point A. Then, the total electric potential exerted by the N point charges on the point A is:

$$V_A = \sum_{i=1}^{N} K\frac{q_i}{\|\mathbf{r}_i\|}$$

In the case of a continuous distribution of charge we have:

$$\Delta V = V(b) - V(a) = -\int_a^b \mathbf{E}\cdot \mathrm{d}\boldsymbol{\ell}$$

Electrostatic energy

Definition 1.15. The *electrostatic energy* between two charges q_1 and q_2 separated a distance r is:

$$U = K\frac{q_1 q_2}{r} = q_2 V_1 = q_1 V_2$$

where V_i is the electric potential created by the charge q_i at a distance r.

Proposition 1.16. Consider a set of N point charges q_i. Let r_{ij} be the distance between the charge q_i and q_j. Then, the total electrostatic energy of the set will be:

$$U = \sum_{i=1}^{N}\sum_{j=i+1}^{N} K\frac{q_i q_j}{r_{ij}} = \frac{1}{2}\sum_{\substack{i,j=1\\ i\neq j}}^{N} K\frac{q_i q_j}{r_{ij}}$$

Conductors

Proposition 1.17. In a conductor, charges can move freely. In particular, if an external electric field is acting on a conductor, the charges move until they reach an electrostatic equilibrium.

Proposition 1.18. When a conductor is in electrostatic equilibrium:

- All the charges are in the surface and the total electric field inside the conductor is zero.
- The electric field just outside is perpendicular to the surface of the conductor and equal to σ/ε_0, where σ is the surface charge density.
- The volume enclosed in the conductor is an equipotential volume and its surface is an equipotential surface.

Capacitance and capacitors

Definition 1.19 (Capacitance). Consider a conductor with an electric charge Q. Then, if its potential is V, the *capacitance* of the conductor is defined as:

$$C := \frac{Q}{V}$$

The SI unit of the capacitance is the Farad ($1\ \mathrm{F} = \mathrm{C}\cdot\mathrm{V}^{-1}$).

Definition 1.20 (Capacitor). A *capacitor* is a device that stores electric charge and electrical energy. It consists in two conductors close to each other and with equal and opposite charge.

Proposition 1.21. Consider a capacitor whose conductors are parallel plates of surface area S and are separated a distance d. If Q is the charge stored in one plate and the potential difference between the plates is ΔV, we have that the capacitance of the capacitor is:

$$C = \frac{Q}{\Delta V} = \varepsilon_0\frac{S}{d}$$

Definition 1.22. Consider two opposite point charges of charge q separated a distance $\mathbf{d}$ (electric dipole). We define the *electric dipole moment* as:

$$\mathbf{p} = q\mathbf{d}$$

Proposition 1.23. Consider an electric dipole of moment $\mathbf{p}$ that is immersed in an electric field $\mathbf{E}$. Then, the electric force creates a torque $\boldsymbol{\tau}$ on the dipole given by:

$$\boldsymbol{\tau} = \mathbf{p}\times\mathbf{E}$$

This torque tends to line up the dipole with the magnetic field $\mathbf{B}$, so that it takes its lowest energy configuration. The potential energy associated with the electric dipole moment is:

$$U = -\boldsymbol{\mu}\cdot\mathbf{E}$$

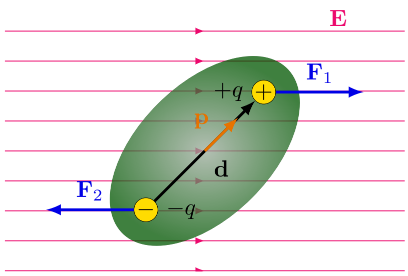


Figure 2.1.1: Electric dipole

Proposition 1.24. Consider a dielectric material with permittivity $\varepsilon = \kappa\varepsilon_0$ with $\kappa > 1$. Then, the capacitance of the capacitor with this material between their plates is:

$$C = \kappa C_0$$

where C_0 is the capacitance of the capacitor with no dielectric material (that is, in the vacuum).

Proposition 1.25. Consider a capacitor of capacitance C, charge Q and potential difference ΔV. Then, the potential energy stored in the capacitor is:

$$U = \frac{1}{2}\frac{Q^2}{C} = \frac{1}{2}CV^2 = \frac{1}{2}QV$$

Proposition 1.26. Consider a capacitor with a dielectric material inside it of permittivity ε. If E is the magnitude of the electric field between the plates of the capacitor, the energy density η of the electric field will be:

$$\eta = \frac{1}{2}\varepsilon E^2$$

Proposition 1.27. Consider N capacitors of capacitance C_i. We can associate the capacitors in two ways:

- in series:
$$\frac{1}{C_{\text{total}}} = \sum_{i=1}^{N} \frac{1}{C_i}$$
- in parallel:
$$C_{\text{total}} = \sum_{i=1}^{N} C_i$$

Electric current

Definition 1.28. An *electric current* is a stream of charged particles moving through an electrical conductor or space. Mathematically, the electric current is:

$$I = \frac{\mathrm{d}Q}{\mathrm{d}t}$$

By agreement, the direction of the electric current is the one of the positive charges.

Definition 1.29. The current density $\mathbf{J}$ is the amount of charge per unit of time that flows through a unit area of a chosen cross section. Mathematically, we have the following relation:

$$I = \iint_S \mathbf{J} \cdot \mathrm{d}\mathbf{S}$$

Proposition 1.30. Let n be the number of charge carriers per unit of volume (charge carrier density) of a conductor, q be the charge of these carriers, S be the section of the conductor and $\mathbf{v}_d$ be the drift velocity (average velocity attained by charged particles in a material due to an electric field). Then, we have:

$$I = \frac{\Delta Q}{\Delta t} = qn\|\mathbf{v}_d\|S$$

Moreover:

$$\mathbf{J} = qn\mathbf{v}_d$$

Law 1.31 (Microscopic Ohm's law). Let n be the charge carrier density of a conductor, τ be the average time between collisions of electrons and $\mathbf{E}$ be the electric field at which electrons are accelerated. Then:

$$\mathbf{J} = \frac{ne^2\tau}{m_e}\mathbf{E} =: \sigma\mathbf{E}$$

Here, σ is called *conductivity.*

Law 1.32 (Macroscopic Ohm's law). Suppose a conductor has a resistance R and carries an electric current I. If the conductor is subjected to a potential difference ΔV, then:

$$I = \frac{\Delta V}{R}$$

Definition 1.33 (Resistivity). Consider a conductor with conductivity σ that has length ℓ, section S and electric resistance R. Then, the *resistivity* of the conductor is:

$$\rho = R\frac{S}{\ell} = \frac{1}{\sigma}$$

Moreover, this resistivity varies with the temperature in the following way:

$$\rho(T) = \rho_0 \left[1 + \alpha(T - T_0)\right]$$

where ρ_0 is the resistivity of the material at temperature T_0 and α is the *temperature coefficient of resistivity.*

Proposition 1.34 (Joule effect). Suppose that a conductor of resistance R carries an electric current I. If it is subjected to a potential difference ΔV, then the power dissipated by heat is:

$$P = IV = RI^2 = \frac{V^2}{R}$$

Proposition 1.35. Consider N resistors of resistance R_i. We can associate the resistors in two ways:

- in series:
$$R_{\text{total}} = \sum_{i=1}^{N} R_i$$
- in parallel:
$$\frac{1}{R_{\text{total}}} = \sum_{i=1}^{N} \frac{1}{R_i}$$

Kirchhoff's laws and RC circuits

Definition 1.36. A battery is a device that maintains a constant potential difference while charges move along the circuit. The *electromotive force (emf)* ξ of a battery describes the work done per unit of charge. Generally, batteries have an internal resistance r and therefore the potential difference between their terminals is:

$$\Delta V = \xi - Ir$$

where I is the electric current passing through it. Finally, the total energy stored in the battery is:

$$W = Q\xi$$

where Q is the charge of the battery.

Law 1.37 (Kirchhoff's laws).

1. Kirchhoff's junction rule: In a node (junction), the sum of currents flowing into that node is equal to the sum of currents flowing out of that node.
2. Kirchhoff's loop rule: The directed sum of the potential differences around any closed loop is zero.

[1]Sometimes RC is denoted by τ and it is called the *RC time constant.*

Proposition 1.38 (Capacitor discharging). Suppose we have a circuit consisting of a resistor of resistance R and a charged capacitor of capacitance C and charge Q. Then, the charge of the capacitor as a function of time will be:

$$q(t) = Q\mathrm{e}^{-\frac{t}{RC}}$$

And, therefore, the electric current will be:

$$i(t) = I_0\mathrm{e}^{-\frac{t}{RC}}$$

where I_0 is the electric current at $t = 0$[1].

Proposition 1.39 (Capacitor charging). Suppose we have a circuit consisting of a battery of emf ξ, a resistor of resistance R and a discharged capacitor of capacitance C. Then, the charge of the capacitor as a function of time will be:

$$q(t) = Q_f(1 - \mathrm{e}^{-\frac{t}{RC}})$$

where Q_f is the final charge of the capacitor. Therefore the electric current will be:

$$i(t) = \frac{\xi}{R}\mathrm{e}^{-\frac{t}{RC}}$$

2.1.1.3 | Magnetostatics

Magnetic force

Proposition 1.40. Consider a point charge q moving at a velocity $\mathbf{v}$. If we apply a magnetic field $\mathbf{B}$ to it, a magnetic force acting on the particle is created:

$$\mathbf{F} = q(\mathbf{v} \times \mathbf{B})$$

The SI unit of the magnetic field is the Tesla ($1\ \mathrm{T} = 1\ \mathrm{N} \cdot \mathrm{A}^{-1} \cdot \mathrm{m}^{-1}$).

Proposition 1.41. Consider a wire of length $\boldsymbol{\ell}$ transporting an electric current I. If we apply a magnetic field $\mathbf{B}$ to the wire and $\boldsymbol{\ell}$ is the vector pointing at the direction of the current and whose magnitude is ℓ, then the magnetic force created by the wire is:

$$\mathbf{F} = I(\boldsymbol{\ell} \times \mathbf{B})$$

If the we take a differential element of length $\mathrm{d}\boldsymbol{\ell}$, then:

$$\mathrm{d}\mathbf{F} = I(\mathrm{d}\boldsymbol{\ell} \times \mathbf{B})$$

Lemma 1.42. The work done by the magnetic field on a particle is zero.

Proposition 1.43. Consider a particle of mass m, charge q and velocity $\mathbf{v}$. If there is a magnetic field $\mathbf{B}$ applied to it, we have two possibilities for its trajectory:

- If $\mathbf{v} \perp \mathbf{B}$, the trajectory will be circular with radius:

$$r = \frac{mv}{qB}$$

- If $\mathbf{v} \not\perp \mathbf{B}$, then $\mathbf{v} = \mathbf{v}_\perp + \mathbf{v}_\parallel$ (where $\mathbf{v}_\perp \perp \mathbf{B}$ and $\mathbf{v}_\parallel \parallel \mathbf{B}$) and the trajectory will be an helicoidal with radius:

$$r = \frac{mv_\perp}{qB}$$

Proposition 1.44. If there is a charge particle q moving at a velocity $\mathbf{v}$ in a region where there is an electric field $\mathbf{E}$ and a magnetic field $\mathbf{B}$, the particle experiences a force called *Lorentz force*:

$$\mathbf{F} = q(\mathbf{E} + \mathbf{v} \times \mathbf{B})$$

Magnetic moment

Definition 1.45. We define the *magnetic moment* of a coil as:

$$\boldsymbol{\mu} = I\mathbf{S}$$

where I is the electric current passing through it and $\mathbf{S}$ is the surface vector. The magnetic moment of a solenoid of N turns (each of are S) is:

$$\boldsymbol{\mu} = NI\mathbf{S}$$

Proposition 1.46. The torque done when a magnetic field $\mathbf{B}$ is applied to an object of magnetic moment $\boldsymbol{\mu}$ is:

$$\boldsymbol{\tau} = \boldsymbol{\mu} \times \mathbf{B}$$

This torque tends to line up the magnetic moment with the magnetic field $\mathbf{B}$, so that it takes its lowest energy configuration. The potential energy associated with the magnetic moment is:

$$U = -\boldsymbol{\mu} \cdot \mathbf{B}$$

Proposition 1.47. Consider a magnetic dipole of magnetic moment $\boldsymbol{\mu}$ that cannot rotate over itself within a magnetic field $\mathbf{B}$. The external force necessary to move the dipole a distance $\mathrm{d}y$ is:

$$F_{\text{ext}} = \frac{\mathrm{d}(\boldsymbol{\mu} \cdot \mathbf{B})}{\mathrm{d}y}$$

Proposition 1.48 (Hall effect). The *Hall effect* is the production of a voltage difference V_H across an electrical conductor of width d that is transverse to an electric current I in the conductor and to an applied magnetic field B perpendicular to the current. It is used for:

- determine the density n of charge carriers:

$$n = \frac{IB}{qdV_\mathrm{H}}$$

  where q is the charge of the charge carriers.

- measure the magnitude of the magnetic field:

$$B = \frac{nqd}{I}V_\mathrm{H}$$

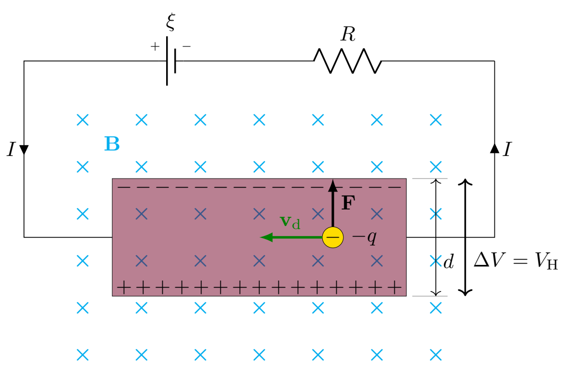


Figure 2.1.2: Hall effect when negative charge carriers are flowing through the circuit

Biot-Savart law

Proposition 1.49. The magnetic field created by a point charge q moving at velocity $\mathbf{v}$ at a distance $\mathbf{r}$ from it is:

$$\mathbf{B} = \frac{\mu_0}{4\pi}\frac{q\mathbf{v}\times\hat{\mathbf{r}}}{\|\mathbf{r}\|^2}$$

where μ_0 is the *vacuum permeability* and $\hat{\mathbf{r}}$ is the unit vector pointing from the charge to the point where we calculate the magnetic field.

Law 1.50 (Biot-Savart law). The magnetic field created by a wire of length $\mathrm{d}\boldsymbol{\ell}$ carrying an electric current I at a distance $\mathbf{r}$ from the wire is:

$$\mathrm{d}\mathbf{B} = \frac{\mu_0}{4\pi}\frac{I\mathrm{d}\boldsymbol{\ell}\times\hat{\mathbf{r}}}{\|\mathbf{r}\|^2}$$

Proposition 1.51. Magnetic field created by:

- a coil of radius R when it carries a current I:
  - on its center:
  $$\mathbf{B} = \frac{\mu_0 I}{2R}\mathbf{e}_x$$
  - at a distance x from its center in the same axis:
  $$\mathbf{B} = \frac{\mu_0}{2}\frac{R^2 I}{(x^2+R^2)^{3/2}}\mathbf{e}_x$$
- a solenoid of N turns, length ℓ and radius R when it carries a current I:
  - at a distance x from its center and over its axis:
  $$\mathbf{B} = \frac{\mu_0}{2}nI\left(\frac{x-a}{\sqrt{(x-a)^2+R^2}}-\right.$$
  $$\left.-\frac{x-b}{\sqrt{(x-b)^2+R^2}}\right)\mathbf{e}_x$$

  where $n = \frac{N}{\ell}$.

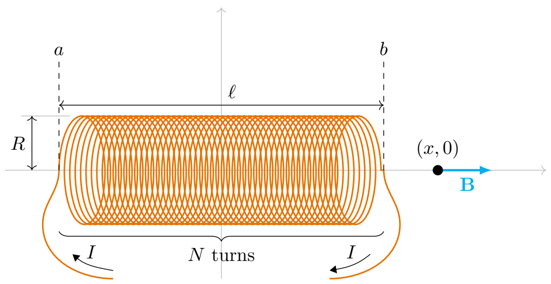


Figure 2.1.3

  - inside the solenoid ($|a|, |b| \gg R$) and far from its ends:
  $$\mathbf{B} = \mu_0 n I\mathbf{e}_x$$
- a finite wire at a point P situated at distance R from the axis of the wire and angles θ_1 and θ_2 from the point to the ends of the wire:
  $$B = \frac{\mu_0 I}{4\pi R}(\sin\theta_1+\sin\theta_2)$$

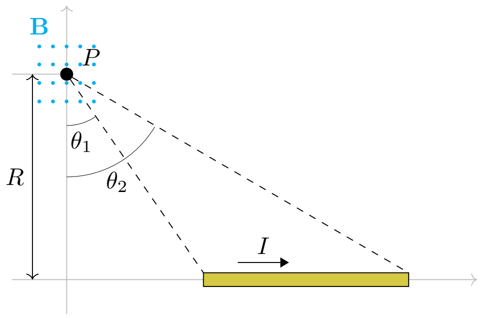


Figure 2.1.4

- an infinite wire at a distance R from it:
  $$B = \frac{\mu_0 I}{2\pi R}$$

Gauß' law and Ampère's law

Proposition 1.52. The magnetic force per unit of length ℓ between two straight parallel conductors carrying electric currents I_1 and I_2 and separated a distance r from each other is:

$$\frac{F}{\ell} = \frac{\mu_0}{2\pi}\frac{I_1 I_2}{r}$$

Law 1.53 (Gauß' law for magnetism). The magnetic flux through any closed surface S is zero.

$$\oiint_S \mathbf{B}\cdot\mathrm{d}\mathbf{S} = 0$$

Law 1.54 (Ampère's law). The line integral of a magnetic field $\mathbf{B}$ around a closed curve C is proportional to the total current I_{enc} passing through a surface S enclosed by C.

$$\oint_C \mathbf{B}\cdot\mathrm{d}\boldsymbol{\ell} = \mu_0 I_{\mathrm{enc}}$$

Magnetism of the matter

Proposition 1.55. Consider a particle of mass m, charge q, angular momentum $\mathbf{L}$ and magnetic moment $\boldsymbol{\mu}$. The relation between $\mathbf{L}$ and $\boldsymbol{\mu}$ is:

$$\boldsymbol{\mu} = \frac{q}{2m}\mathbf{L}$$

Proposition 1.56. The angular momentum is quantized. For an electron the quantum unit of the magnetic moment is called *Bohr magneton* and has a value of:

$$\mu_{\mathrm{B}} = \frac{e\hbar}{2m_e}$$

Therefore:

$$\boldsymbol{\mu}_L = -\mu_{\mathrm{B}}\frac{\mathbf{L}}{\hbar} \quad \text{and} \quad \boldsymbol{\mu}_S = -2\mu_{\mathrm{B}}\frac{\mathbf{S}}{\hbar}$$

where $\boldsymbol{\mu}_L$ is the magnetic moment due to the orbital angular momentum and $\boldsymbol{\mu}_S$ is the magnetic moment due to the spin. The total angular momentum is: $\mathbf{j} = \mathbf{L}+\mathbf{S}$

Definition 1.57. The *magnetization* $\mathbf{M}$ is defined as:

$$\mathbf{M} = \frac{\mathrm{d}\boldsymbol{\mu}}{\mathrm{d}V}$$

where $\mathrm{d}V$ is the volume element. Moreover if a section of a cylinder of length $\mathrm{d}\ell$ carries a current $\mathrm{d}i$, then:

$$M = \frac{\mathrm{d}i}{\mathrm{d}\ell}$$

Proposition 1.58. Suppose we place a cylinder of magnetic material inside a long solenoid that has n turns per unit of length and carries a current I. Then, the applied field of the solenoid $\mathbf{B}_{\text{app}}$ ($B_{\text{app}} = \mu_0 nI$) magnetizes the material so that it acquires a magnetization $\mathbf{M}$. The resultant magnetic field at a point inside the solenoid is:

$$\mathbf{B} = \mathbf{B}_{\text{app}} + \mu_0\mathbf{M}$$

Proposition 1.59. The magnetization $\mathbf{M}$ of a material is found to be proportional to the applied magnetic field that produces the alignment of the magnetic dipoles in the material. So, using the previous notation, we can write:

$$\mathbf{M} = \chi_{\text{m}}\frac{\mathbf{B}_{\text{app}}}{\mu_0}$$

where the constant χ_{m} is called *magnetic susceptibility*. Based on the value of χ_{m}, materials can be classified in three groups: *ferromagnetic*, *paramagnetic* and *diamagnetic*.

Material	χ_{m}	Attraction
Ferromagnetic	$(10^2, 10^5)$	Strong attraction
Paramagnetic	$(10^{-5}, 10^{-2})$	Weak attraction
Diamagnetic	$(-10^{-6}, -10^{-4})$	Weak repulsion

Definition 1.60. The permeability μ of a material is defined as:

$$\mu = (1 + \chi_{\text{m}})\mu_0$$

Electromagnetic induction

Definition 1.61. We define the *magnetic flux* as:

$$\Phi_B = \iint_S \mathbf{B} \cdot \mathrm{d}\mathbf{S}$$

Law 1.62 (Faraday's law). The emf ξ induced on a circuit is equal to the time rate of change of the magnetic flux Φ_B through the circuit.

$$\xi = \oint \mathbf{E} \cdot \mathrm{d}\boldsymbol{\ell} = -\frac{\mathrm{d}\Phi_B}{\mathrm{d}t}$$

Law 1.63 (Lenz's law). The emf and induced electric current tend to oppose the change in flux and to exert a mechanical force which opposes the motion.

Proposition 1.64. Consider a coil of radius r and a magnetic field B applied to it. Then, this induces an electric field of magnitude:

$$E = -\frac{r}{2}\frac{\mathrm{d}B}{\mathrm{d}t}$$

Proposition 1.65. The emf induced on a circuit by the relative motion between a magnetic field B and a segment of length ℓ of electric current is:

$$\xi = -B\ell v$$

where v is the velocity of the segment relative to the magnetic field.

Proposition 1.66. Due to the rotation at angular velocity ω of a solenoid of N turns and section S in a magnetic field B, the potential difference induced between the ends of the solenoid is:

$$V = NBS\omega\sin(\omega t) =: V_0\sin(\omega t)$$ [2]

Moreover if we connect the solenoid to a circuit of resistance R, we will produce an intensity I given by:

$$I = \frac{V_0}{R}\sin(\omega t)$$

Definition 1.67 (Eddy current). *Eddy currents* are loops of electrical current induced within conductors by a changing magnetic field. These currents induce a magnetic force that opposes the movement.

Inductance

Definition 1.68. Consider a solenoid of N turns, length ℓ and section S carrying an electric current I. Then, the magnetic flux Φ_B that passes through it is

$$\Phi_B = LI$$

where $L = \mu_0 n^2 S\ell$ and $n = \frac{N}{\ell}$. The coefficient L is called inductance. The SI unit of the inductance is the Henry ($1\text{ H} = \text{Wb}\cdot\text{A}^{-1}$).

Definition 1.69. An *inductor* is a solenoid with many turns.

Proposition 1.70. Consider a solenoid of inductance L and internal resistance r carrying an electric current I. Then, Faraday-Lenz law can be written as:

$$\xi = -L\frac{\mathrm{d}I}{\mathrm{d}t}$$

Therefore, the potential difference between the two ends of the solenoid is:

$$\Delta V = -L\frac{\mathrm{d}I}{\mathrm{d}t} - Ir$$

Definition 1.71. Consider two circuits close to each other so that the magnetic flux across a circuit depends also on the electric current that carries the other circuit. This dependance is given by:

$$\Phi_{B,1} = L_1I_1 + M_{12}I_2 \qquad \Phi_{B,2} = L_2I_2 + M_{21}I_1$$

where $\Phi_{B,i}$ is the flux that passes across the circuit i, I_i is the electric current flowing in the circuit i, L_i is the inductance coefficient of the circuit i and M_{ij} is the *mutual inductance* between the circuit i and j. Relating to the latter point, in general we have $M_{12} = M_{21}$.

Proposition 1.72. Consider an inductor of inductance L carrying an electric current I. Then, the potential energy stored in the inductor is:

$$U = \frac{1}{2}LI^2$$

Proposition 1.73. Consider an inductor that produces a magnetic field B inside it. Then, the energy density η of the magnetic field will be:

$$\eta = \frac{1}{2}\frac{B^2}{\mu_0}$$

[2] With this method, the energy isn't used at all. To solve this, three-phase electric power are used instead. This method consist in three coils separated by 120° between them.

Generalized Ampère's law

Definition 1.74. The *displacement current* is defined as:

$$I_\mathrm{d} = \varepsilon_0 \frac{\mathrm{d}\Phi_E}{\mathrm{d}t}$$

where Φ_E is the flux of the electric field through the surface where the current is flowing.

Law 1.75. The generalized Ampère's law (Ampère-Maxwell law) which takes into account displacement currents is:

$$\oint_C \mathbf{B} \cdot \mathrm{d}\boldsymbol{\ell} = \mu_0 I + \mu_0 \varepsilon_0 \frac{\mathrm{d}}{\mathrm{d}t} \iint_S \mathbf{E} \cdot \mathrm{d}\mathbf{S}$$

Definition 1.76. The speed of the electromagnetic waves in the vacuum is:

$$v = \frac{1}{\sqrt{\varepsilon_0 \mu_0}} =: c$$

Law	**Differential form**	**Integral form**
Gauß' law	$\boldsymbol{\nabla} \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0}$	$\oiint_S \mathbf{E} \cdot d\mathbf{S} = \frac{Q_\mathrm{int}}{\varepsilon_0}$
Gauß' law for magnetism	$\boldsymbol{\nabla} \cdot \mathbf{B} = 0$	$\oiint_S \mathbf{B} \cdot d\mathbf{S} = 0$
Faraday-Lenz law	$\boldsymbol{\nabla} \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$	$\oint_C \mathbf{E} \cdot \mathrm{d}\boldsymbol{\ell} = -\frac{\mathrm{d}}{\mathrm{d}t} \iint_S \mathbf{B} \cdot d\mathbf{S}$
Ampère-Maxwell law	$\boldsymbol{\nabla} \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t}$	$\oint_C \mathbf{B} \cdot \mathrm{d}\boldsymbol{\ell} = \mu_0 I + \mu_0 \varepsilon_0 \frac{\mathrm{d}}{\mathrm{d}t} \iint_S \mathbf{E} \cdot d\mathbf{S}$

Figure 2.1.5: Maxwell equations

2.1.2 Mechanics and special relativity

2.1.2.1 | Mechanics

Kinematics

Definition 2.1. The *equation of movement* of any particle is of the form:

$$\mathbf{r}(t) = x(t)\mathbf{e}_x + y(t)\mathbf{e}_y + z(t)\mathbf{e}_z$$

where $x(t)$, $y(t)$, $z(t)$ are the movements equations of the particle along x-, y- and z-axis, respectively.

Definition 2.2. Consider a particle with movement equation $\mathbf{r}(t)$. Then, the *average velocity over any time interval* $\Delta t = t_2 - t_1$ is:

$$\mathbf{v}_{\text{avg}} = \frac{\Delta \mathbf{r}(t)}{\Delta t} = \frac{\mathbf{r}(t_2) - \mathbf{r}(t_1)}{t_2 - t_1}$$

If we take the limit when $\Delta t \to 0$ (or $t_2 \to t_1$), we get the *instantaneous velocity at time* t_1:

$$\mathbf{v}(t_1) = \lim_{\Delta t \to 0} \frac{\Delta \mathbf{r}(t)}{\Delta t} = \dot{\mathbf{r}}(t_1) = \dot{x}(t_1)\mathbf{e}_x + \dot{y}(t_1)\mathbf{e}_y + \dot{z}(t_1)\mathbf{e}_z$$

Definition 2.3. The *speed* of a particle moving at a velocity $\mathbf{v}(t)$ is:

$$v(t) = \|\mathbf{v}(t)\|$$

Definition 2.4. Consider a particle moving at a velocity $\mathbf{v}(t)$. Then the *average acceleration over any time interval* $\Delta t = t_2 - t_1$ is:

$$\mathbf{a}_{\text{avg}} = \frac{\Delta \mathbf{v}(t)}{\Delta t} = \frac{\mathbf{v}(t_2) - \mathbf{v}(t_1)}{t_2 - t_1}$$

If we take the limit when $\Delta t \to 0$ (or $t_2 \to t_1$), we get the *instantaneous acceleration at time* t_1:

$$\mathbf{a}(t_1) = \lim_{\Delta t \to 0} \frac{\Delta \mathbf{v}(t)}{\Delta t} = \ddot{\mathbf{r}}(t_1) = \ddot{x}(t_1)\mathbf{e}_x + \ddot{y}(t_1)\mathbf{e}_y + \ddot{z}(t_1)\mathbf{e}_z$$

Proposition 2.5 (Uniform linear motion). Consider a particle moving at a constant speed v along a straight line. If at time $t = 0$ it is in the position x_0, then:

$$x(t) = x_0 + vt$$

Proposition 2.6 (Accelerated linear motion). Consider a particle moving at a constant acceleration a along a straight line. If at time $t = 0$ it is in the position x_0 with velocity v_0, then:

$$\dot{x}(t) = v_0 + at \qquad x(t) = x_0 + v_0 t + \frac{1}{2}at^2$$

Definition 2.7. Suppose a particle is at Cartesian coordinates (x, y) and at polar coordinates (r, φ). Then, polar unit vectors are defined as:

$$\begin{aligned} \mathbf{e}_r &= \cos\varphi\mathbf{e}_x + \sin\varphi\mathbf{e}_y \\ \mathbf{e}_\varphi &= -\sin\varphi\mathbf{e}_x + \cos\varphi\mathbf{e}_y \end{aligned}$$

Definition 2.8. The equations of the circular movement are the following:

$$\mathbf{r}(t) = r\mathbf{e}_r \quad \dot{\mathbf{r}}(t) = r\dot{\varphi}(t)\mathbf{e}_\varphi \quad \ddot{\mathbf{r}}(t) = r\ddot{\varphi}(t)\mathbf{e}_\varphi - r\dot{\varphi}(t)^2\mathbf{e}_r$$

where we have supposed that r is constant. We define the *angular velocity* $\omega(t)$ as $\omega(t) := \dot{\varphi}(t)$ and the *angular acceleration* $\alpha(t)$ as $\alpha(t) := \ddot{\varphi}(t)$. The first term of $\ddot{\mathbf{r}}(t)$ is called *tangential acceleration* and its magnitude is $a_t := r\alpha$. The second term is called *normal acceleration* and its magnitude is $a_n := r\omega^2$.

Definition 2.9. Consider a particle moving along the trajectory $\mathbf{r}(t)$. We define Frenet vectors as:

1. First Frenet vector: $\mathbf{e}_1(t) = \dfrac{\dot{\mathbf{r}}(t)}{\|\dot{\mathbf{r}}(t)\|}$
2. Second Frenet vector: $\mathbf{e}_2(t) = \dfrac{\dot{\mathbf{e}}_1(t)}{\|\dot{\mathbf{e}}_1(t)\|}$

Note that the first vector is tangent to the trajectory at each point and the second one is normal to the trajectory at each point.
From this definition we have:

$$\dot{\mathbf{r}}(t) = v(t)\mathbf{e}_1 \qquad \ddot{\mathbf{r}}(t) = a_t(t)\mathbf{e}_1 + a_n(t)\mathbf{e}_2(t)$$

We also define the *curvature* $\kappa(t)$ and *radius of curvature* $R(t)$ as:

$$\frac{1}{\kappa(t)} = R(t) := \frac{\|\dot{\mathbf{r}}(t)\|}{\|\dot{\mathbf{e}}_1(t)\|}$$

Finally, the normal acceleration is:

$$a_n(t) = \frac{v(t)^2}{R(t)}$$

Proposition 2.10 (Curvature). Consider a particle moving along a two-dimensional trajectory and let $\Delta\varphi$ be the angle the trajectory has curved when traveling a distance Δs. Then the *average curvature along* Δs is:

$$\kappa_{\text{avg}} = \frac{\Delta\varphi}{\Delta s}$$

If we take the limit when $\Delta s \to 0$ we have:

$$\kappa = \lim_{\Delta s \to 0} \frac{\Delta\varphi}{\Delta s} = \frac{\mathrm{d}\varphi}{\mathrm{d}s}$$

Proposition 2.11 (Arc length). The total distance traveled by a particle moving along a curve $\mathbf{r}(t)$ between the instants t_1 and t_2 is:

$$\int_{t_1}^{t_2} \|\dot{\mathbf{r}}(t)\|\mathrm{d}t$$

Proposition 2.12 (Projectile motion). The equations of a projectile motion like the one in figure 2.1.6 are:

$$\begin{aligned} x(t) &= x_0 + v_0\cos\theta t \qquad & y(t) &= y_0 + v_0\sin\theta t - \frac{1}{2}gt^2 \\ v_x(t) &= v_0\cos\theta \qquad & v_y(t) &= v_0\sin\theta - gt \end{aligned}$$

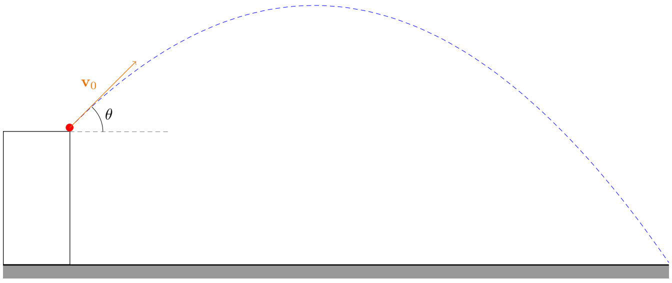


Figure 2.1.6

Dynamics

Law 2.13 (Newton's laws).

1. An object at rest will stay at rest and an object in motion will stay in motion unless acted on by a net external force. That is:

$$\sum \mathbf{F} = 0 \iff \frac{\mathrm{d}\mathbf{v}}{\mathrm{d}t} = 0$$

2. The rate of change of momentum of a body over time is directly proportional to the force applied, and occurs in the same direction as the applied force. That is:

$$\mathbf{F} = \frac{\mathrm{d}\mathbf{p}}{\mathrm{d}t}$$

3. If one object A exerts a force $\mathbf{F}_A$ on a second object B, then B simultaneously exerts a force $\mathbf{F}_B$ on A and the two forces are equal in magnitude and opposite in direction:

$$\mathbf{F}_A = -\mathbf{F}_B$$

Proposition 2.14 (Gravity force). Any two object with mass m_1 and m_2 exerts an attracting force called *gravity*:

$$\mathbf{F}_{21} = -G\frac{m_1 m_2}{|\mathbf{r}_{12}|^3}\mathbf{r}_{12}$$

where $\mathbf{F}_{21}$ is the force applied on object 2 exerted by object 1, $\mathbf{r}_{12}$ is the vector distance from object 1 to object 2.

Proposition 2.15 (Elastic force). Consider an object attached to a string of natural length x_0 as shown in the figure 2.1.7.

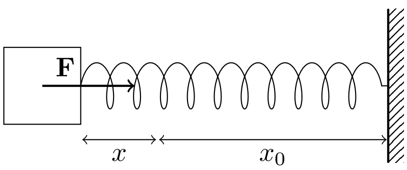


Figure 2.1.7

If we displace the object a distance of x from its equilibrium position, the resulting elastic force is:

$$\mathbf{F} = -k\mathbf{x}$$

where k is the spring constant. Moreover, ignoring the friction, the mass starts to oscillate and this oscillation have the following equations:

$$\begin{gathered} x(t) = A\cos(\omega t + \phi) \\ \dot{x}(t) = -\omega A\sin(\omega t + \phi) \\ \ddot{x}(t) = -\omega^2 A\cos(\omega t + \phi) = -\omega^2 x(t) \\ \omega = \sqrt{\frac{k}{m}} \qquad T = \frac{2\pi}{\omega} \qquad \nu = \frac{1}{T} \end{gathered}$$

where A is the amplitude, ϕ is the initial phase, ω is the angular frequency, T is the period and ν is the frequency.

Proposition 2.16. Consider an object on a surface that undergo a normal force $\mathbf{F}_N$ and it is pulled by a net force of magnitude F. Then the magnitude of the frictional force is:

$$F_f = \begin{cases} F & \text{if} \quad F \le \mu_s F_N \\ \mu_k F_N & \text{if} \quad F > \mu_s F_N \end{cases}$$

where μ_s is the *static coefficient of friction* and μ_k is the *kinetic coefficient of friction*.

Proposition 2.17 (Inertial forces). Consider two general reference frames $\mathcal{R}$ and $\mathcal{R}'$ (separated by $\mathbf{R}(t)$) and suppose that we observe a particle of mass m at position $\mathbf{r}(t)$ from $\mathcal{R}$ and at position $\mathbf{r}'(t)$ from $\mathcal{R}'$, as shown in the figure:

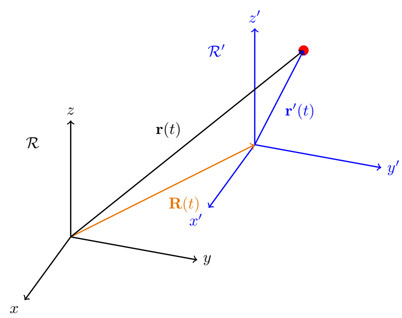


Figure 2.1.8

Then for a general $\mathbf{R}(t)$ we have $\mathbf{r}'(t) = \mathbf{r}(t) - \mathbf{R}(t)$ and therefore $\ddot{\mathbf{r}}'(t) = \ddot{\mathbf{r}}(t) - \ddot{\mathbf{R}}(t)$. If we assume that $\mathcal{R}$ is inertial, then

$$\mathbf{F}(t) - m\ddot{\mathbf{R}}(t) = m\ddot{\mathbf{r}}'(t)$$

If $\mathcal{R}'$ is not inertial, Newton's second law is not satisfied. In this case, we denote the term $-m\ddot{\mathbf{R}}(t)$ as an *inertial force* or *fictitious force*: $\mathbf{F}_{\text{iner}}(t) := -m\ddot{\mathbf{R}}(t)$[3].

Proposition 2.18 (Galilean transformation). Consider two reference frames $\mathcal{R}$ and $\mathcal{R}'$. Using the previous notation, suppose $\mathbf{R}(t) = Vt\mathbf{e}_x$. Then:

$$\begin{aligned} x' &= x - Vt & \qquad v_x' &= v_x - V \\ y' &= y & v_y' &= v_y \\ z' &= z & v_z' &= v_z \end{aligned}$$
$$t' = t$$

[3]Note that if $\mathcal{R}'$ is inertial, Newton's second law is still satisfied because $\mathbf{R}(t) = \mathbf{V}t$ and therefore $-m\ddot{\mathbf{R}}(t) = 0$.

Statics

Definition 2.19 (Linear momentum of a particle). Consider a particle of mass m moving at a velocity of $\mathbf{v}$. We define its *linear momentum* as:

$$\mathbf{p} = m\mathbf{v}$$

Proposition 2.20 (Linear momentum of a system of particles). Consider a system of N particles which interact with themselves (internal forces) and also with external forces. The *linear momentum of the system* is:

$$\mathbf{P} = \sum_{a=1}^{N} \mathbf{p}_a$$

Moreover if the net external force is $\mathbf{F}_{\text{ext}}$ we have:

$$\frac{\mathrm{d}\mathbf{P}}{\mathrm{d}t} = \mathbf{F}_{\text{ext}}$$

Proposition 2.21 (Center of masses). The *center of masses* (CM) of a system of N particles is:

$$\mathbf{R} = \frac{1}{M}\sum_{i=1}^{N} m_i\mathbf{r}_i$$

where $M = \displaystyle\sum_{i=1}^{N} m_i$. Differentiating the last equality we get

$$M\dot{\mathbf{R}} = \mathbf{P} \qquad M\ddot{\mathbf{R}} = \dot{\mathbf{P}} = \mathbf{F}_{\text{ext}}$$

If the mass distribution is continuous with the density $\rho(\mathbf{r})$ within a solid Ω, the center of mass is:

$$\mathbf{R} = \frac{1}{M}\iiint_{\Omega} \rho(\mathbf{r})\mathbf{r}\mathrm{d}V$$

where $M = \displaystyle\iiint_{\Omega} \rho(\mathbf{r})\mathrm{d}V$.

Proposition 2.22 (Angular momentum). Consider a particle with linear momentum $\mathbf{p}$ situated at position $\mathbf{r}$ with respect to the origin O. We define its *angular momentum* as:

$$\mathbf{L} = \mathbf{r} \times \mathbf{p}$$

The angular momentum of a system of N particles is:

$$\mathbf{L}_{\text{sys}} = \sum_{i=1}^{N} \mathbf{L}_i$$

Proposition 2.23 (Torque). Consider a particle at position $\mathbf{r}$ with respect to the origin O and let $\mathbf{F}$ be a force acting on the particle. We define the *torque* as:

$$\boldsymbol{\tau} = \mathbf{r} \times \mathbf{F}$$

The torque of a system of N particles is:

$$\boldsymbol{\tau}_{\text{ext}} = \sum_{i=1}^{N} \boldsymbol{\tau}_i$$

Proposition 2.24. Relating the torque and angular momentum of a particle and a system of particles we have:

$$\dot{\mathbf{L}} = \boldsymbol{\tau} \qquad \dot{\mathbf{L}}_{\text{sys}} = \boldsymbol{\tau}_{\text{ext}}$$

Therefore, if $\boldsymbol{\tau}_{\text{ext}} = 0$, then $\mathbf{L}_{\text{sys}} = \text{const.}$

Definition 2.25 (Mechanical equilibrium). The conditions of mechanical equilibrium are:

$$\mathbf{F}_{\text{ext}} = 0 \quad \text{and} \quad \boldsymbol{\tau}_{\text{ext}} = 0$$

Work and energy

Definition 2.26 (Work). The *work* of a constant force $\mathbf{F}$ acting on a particle that moves throughout a straight distance $\Delta\mathbf{r}$ is:

$$W = \mathbf{F} \cdot \Delta\mathbf{r}$$

If the force is not necessary constant and the particle moves along a curve c, we have:

$$W = \int_c \mathbf{F} \cdot \mathrm{d}\mathbf{r}$$

Definition 2.27 (Power). The *power* is defined as

$$P = \frac{\mathrm{d}W}{\mathrm{d}t}$$

If ΔW is the amount of work performed during a period of time of duration Δt, the *average power* is:

$$P = \frac{\Delta W}{\Delta t}$$

From the first definition we can deduce the following general formula:

$$P = \mathbf{F} \cdot \mathbf{v}$$

Definition 2.28 (Kinetic energy). The *kinetic energy* of a particle of mass m moving at a speed v is:

$$K = \frac{1}{2}mv^2$$

Theorem 2.29. The total work done on a particle is:

$$W = \Delta K$$

Definition 2.30 (Conservative forces). A force is *conservative* if for any path c connecting points A and B, the work necessary to move a particle from A to B does not depend on c.

Proposition 2.31. The work done by a conservative force can be expressed as a variation of a function called *potential energy*.

Proposition 2.32 (Potential energy). If a force $\mathbf{F}$ is conservative, we define the potential energy as:

$$U(\mathbf{r}) = -\int_{\mathbf{r}_0}^{\mathbf{r}} \mathbf{F} \cdot d\mathbf{r}$$

where $\mathbf{r}_0$ is a reference point and can be chosen arbitrarily. It can be easily seen that:

$$W = -\Delta U$$

Proposition 2.33 (Mechanical energy). The mechanical energy of a particle (with kinetic energy K) subjected to a conservative force of potential energy U is:

$$E = K + U$$

Theorem 2.34 (Conservation of mechanical energy). For a particle subjected to a conservative force we have:

$$\Delta E = 0$$

That is, E is constant. If there are non-conservative forces acting on the particle we have:

$$\Delta E = W_{\text{nc}}$$

where W_{nc} is the work done by non-conservative forces.

Proposition 2.35 (Examples of potential energies).

1. Elastic potential energy of a spring:

$$U = \frac{1}{2}kx^2$$

where x is the distance the spring has been stretched.

2. Gravitational potential energy of a solid of mass m:

$$U = -\frac{GM_T m}{r}$$

where M_T is the Earth mass, r is the distance form the center of the earth to the position of the solid and G is the gravitational constant. Note that if $r = R_T + h$, $h > 0$ and $\frac{r}{R_T} = 1 + \frac{h}{R_T} \approx 1$, then:

$$U = mgh$$

where R_T is the radius of earth and g is the surface gravity.

Rotation

Definition 2.36. Consider a system of N particles that spin around a reference axis at an angular velocity $\boldsymbol{\omega}$. The *moment of inertia* I with respect to the axis is:

$$I = \sum_{i=1}^{N} m_i {r_i}^2$$

where m_i is the mass of the i-th particle and r_i is the distance between that particle and the axis. Moreover we have:

$$\mathbf{L}_{\text{sys}} = I\boldsymbol{\omega}$$

Proposition 2.37. For a rigid body of moment of inertia I that spins around a reference axis at an angular velocity $\boldsymbol{\omega}$ we have:

$$\boldsymbol{\tau}_{\text{ext}} = I\dot{\boldsymbol{\omega}} = I\boldsymbol{\alpha}$$

Proposition 2.38. Consider a system of particles whose CM is at a distance $\mathbf{R}(t)$ from a fixed point O. If $\mathbf{P}$ is the linear momentum of the CM, we have:

$$\mathbf{L}_O = \mathbf{L}_{\text{CM}} + \mathbf{R} \times \mathbf{P}$$

where $\mathbf{L}_O$ is the angular momentum of the system with respect to the point O and $\mathbf{L}_{\text{CM}}$ is the angular momentum of the system with respect to the CM. Moreover if $\mathbf{F}_{\text{ext}}$ is the total external force applied onto the system, $\boldsymbol{\tau}_{\text{O,ext}}$ is the torque done by the forces with respect to the point O and $\boldsymbol{\tau}_{\text{CM,ext}}$ is the torque done by the forces with respect to the CM, we have:

$$\boldsymbol{\tau}_{\text{O,ext}} = \boldsymbol{\tau}_{\text{CM,ext}} + \mathbf{R} \times \mathbf{F}_{\text{ext}}$$

Finally, we deduce:

$$\dot{\mathbf{L}}_{CM} = \boldsymbol{\tau}_{\text{CM,ext}}$$

Proposition 2.39. Consider a system of particles with total mass M. Suppose the moment of inertia of the system with respect to the CM is I_{CM} and that the speed of the CM is V. If the angular velocity of the system around the CM is ω, the kinetic energy of rotation will be:

$$K = \frac{1}{2}MV^2 + \frac{1}{2}I_{\text{CM}}\omega^2$$

Theorem 2.40 (Parallel axis theorem). Consider a body of mass m that is rotating around an axis that passes through the body's center of mass. Let I_{CM} be the moment of inertia with respect of that axis. Suppose there is another axis parallel to the previous one and separated each other a distance of d. Then, the moment of inertia of the body with respect to this latter axis I will be:

$$I = I_{\text{CM}} + md^2$$

2.1.2.2 | Special relativity

Definition 2.41. A *inertial frame of reference* is a frame of reference in which a particle remains at rest or in uniform linear motion.

Principle 2.42 (First postulate). The laws of physics take the same form in all inertial frames of reference.

Principle 2.43 (Second postulate). The speed of light, c, is a constant, independent of the relative motion of the source.

Definition 2.44 (Lorentz factor). For an object moving at speed v, *Lorentz factor* is defined as:

$$\gamma = \frac{1}{\sqrt{1-\beta^2}}$$

where $\beta = v/c$.

Proposition 2.45 (Time dilation). Consider two frames of reference in uniform relative motion with velocity v such that one of them has a clock. If Δt_0 is the time interval between two events made in the same location and measured in the frame in which the clock is at rest (*proper time*), then the time measured by the other frame is:

$$\Delta t = \gamma \Delta t_0$$

Proposition 2.46 (Length contraction). Consider two frames of reference in uniform relative motion with velocity v such that one of them has an object. If L_0 is length of the object measured instantaneously in the frame in which the object is at rest (*proper length*), then the length measured by the other frame is:

$$L = \frac{L_0}{\gamma}$$

Proposition 2.47 (Lorentz transformations). Consider coordinates (x, y, z, t) and (x', y', z', t') of a single arbitrary event measured in two coordinate systems S and S', in uniform relative motion (S' is moving at velocity $\mathbf{v} = (v, 0, 0)$ with respect to S) in their common x and x' directions and with their spatial origins coinciding at time $t = t' = 0$. Then:

$$\begin{aligned} x' &= \gamma(x - \beta ct) & x &= \gamma(x' + \beta ct') \\ y' &= y & y &= y' \\ z' &= z & z &= z' \\ ct' &= \gamma(ct - \beta x) & ct &= \gamma(ct' + \beta x') \end{aligned}$$

Proposition 2.48 (Lorentz transformations of velocities). In a situation similar to the previous one, if an object is moving at a velocity $\mathbf{u} = (u_x, u_y, u_z)$ in S and $\mathbf{u}' = (u'_x, u'_y, u'_z)$ in S', we have:

$$\begin{aligned} u'_x &= \frac{u_x - v}{1 - u_x v/c^2} & u_x &= \frac{u'_x + v}{1 + u'_x v/c^2} \\ u'_y &= \frac{u_y}{\gamma\left(1 - u_x v/c^2\right)} & u_y &= \frac{u'_y}{\gamma\left(1 + u_x v/c^2\right)} \\ u'_z &= \frac{u_z}{\gamma\left(1 - u_x v/c^2\right)} & u_z &= \frac{u'_z}{\gamma\left(1 + u_x v/c^2\right)} \end{aligned}$$

Proposition 2.49 (Matrix form of Lorentz transformations). We can write the Lorentz transformations as:

$$\begin{pmatrix} x' \\ ct' \end{pmatrix} = \begin{pmatrix} \gamma & -\beta\gamma \\ -\beta\gamma & \gamma \end{pmatrix} \begin{pmatrix} x \\ ct \end{pmatrix}$$

If

$$\Lambda := \begin{pmatrix} \gamma & -\beta\gamma \\ -\beta\gamma & \gamma \end{pmatrix}, \text{ then } \Lambda^{-1} = \begin{pmatrix} \gamma & \beta\gamma \\ \beta\gamma & \gamma \end{pmatrix}$$

and we obtain the inverse transformations.

Proposition 2.50 (Lorentz invariant). The factor s^2, defined as follows, is invariant in any inertial frame of reference.

$$s^2 = c^2t^2 - x^2 - y^2 - z^2$$

Proposition 2.51 (Types of events). There are three types of events: *timelike*, *lightlike* and *spacelike*.

- $s^2 > 0 \implies$ *timelike*
- $s^2 = 0 \implies$ *lightlike*
- $s^2 < 0 \implies$ *spacelike*

Timelike and lightlike events are in causal relation with the origin (that is, it is possible to send a light signal from the origin to the point or vice versa), while *spacelike* events are not.

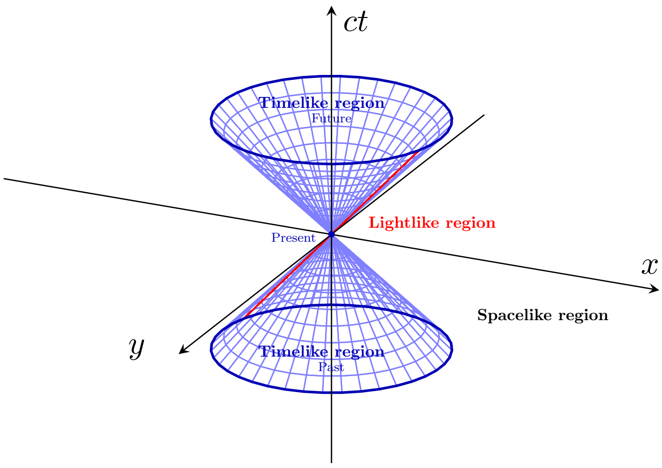


Figure 2.1.9: Minkowski diagram

Proposition 2.52 (Relativistic Doppler effect). Suppose a frame of reference where the receiver is at rest and the source is moving at speed β forming an angle ϕ with the light direction (measured in receiver frame). Then:

$$\nu_R = \frac{\nu_S}{\gamma(1 - \beta\cos\phi)} \tag{2.1.1}$$

$$\lambda_R = \gamma\lambda_S(1 - \beta\cos\phi) \tag{2.1.2}$$

where ν_S is the frequency measured by the source and ν_R is the frequency measured by the receiver, and analogously with wavelengths λ_S and λ_R.
Relation between the angles ϕ and ϕ', where ϕ' is the angle between the velocity and the light direction measured in source frame:

$$\tan\frac{\phi'}{2} = \sqrt{\frac{1+\beta}{1-\beta}}\tan\frac{\phi}{2}$$

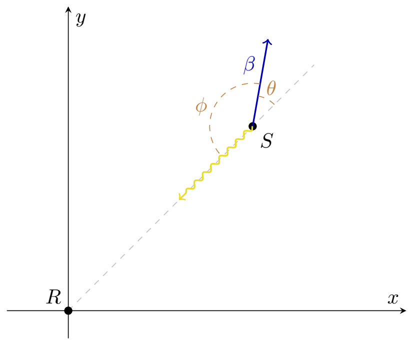


Figure 2.1.10: General case of Doppler effect

Corollary 2.53. There are three important cases to consider:

- The source moves away, that is making $\phi = \pi$ in equation (2.1.1) (*Redshift*):

$$\nu_R = \nu_S\sqrt{\frac{1-\beta}{1+\beta}}$$

- The source gets close, that is making $\phi = 0$ in equation (2.1.1) (*Blueshift*):

$$\nu_R = \nu_S\sqrt{\frac{1+\beta}{1-\beta}}$$

- The source moves transversely, that is making $\phi = \pi/2$ in equation (2.1.1):

$$\nu_R = \nu_S/\gamma$$

Proposition 2.54 (Relativistic mass). If m_0 is the mass of an object at rest, then the mass of an object at a velocity β is:

$$m = \gamma m_0$$

The mass m_0 is invariant.

Proposition 2.55 (Relativistic momentum). The relativistic momentum for a particle with mass at rest m_0 and moving at a velocity of $\mathbf{v}$ is given by:

$$\mathbf{p} = \gamma m_0 \mathbf{v}$$

Proposition 2.56 (Relativistic energy). The relativistic energy of a particle is:

$$E = mc^2 = \gamma m_0 c^2$$

On the other hand, $E = K + m_0c^2$, where K is the kinetic energy of a particle and m_0c^2 its rest energy. Moreover we can express the energy of a particle in terms of its momentum:

$$E = mc^2 = \sqrt{p^2c^2 + m_0^2c^4}$$

Proposition 2.57 (Photon energy and momentum). For a photon of frequency ν, energy E and linear momentum p, we have:

$$E = h\nu \qquad p = \frac{h\nu}{c}$$

Proposition 2.58 (Lorentz transformations of energy and momentum). Consider a particle that have energy E and momentum $\mathbf{p} = (p_x, p_y, p_z)$ in a frame of reference S and have energy E' and momentum $\mathbf{p}' = (p'_x, p'_y, p'_z)$ in frame of reference S'. These frames are in uniform relative motion (S' is moving at velocity $\mathbf{v} = (v, 0, 0)$ with respect to S) and their spatial origins coincide at time $t = t' = 0$. Then:

$$\begin{aligned} E' &= \gamma(E - \beta c p_x) & E &= \gamma(E' + \beta c p'_x) \\ cp'_x &= \gamma(cp_x - \beta E) & cp_x &= \gamma(cp'_x + \beta E') \\ p'_y &= p_y & p_y &= p'_y \\ p'_z &= p_z & p_z &= p'_z \end{aligned}$$

Proposition 2.59 (Compton scattering). Consider a photon with wavelength λ colliding with a particle at rest of mass m_0 (usually an electron). As a result of the collision, the photon energy decrease and therefore its wavelength increase (let's say the scattered photon has wavelength λ'). If the scattered photon is moving at an angle θ with respect to initial direction, we have:

$$\lambda' - \lambda = \frac{h}{m_0 c}(1 - \cos\theta)$$

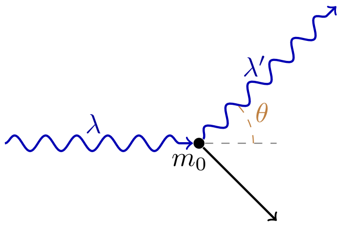


Figure 2.1.11: Compton scattering

2.1.2.3 | Fluids

Definition 2.60. A *fluid* is a substance that continually flows under an applied external force.

Definition 2.61. The *viscosity* of a fluid is a measure of its resistance to deformation at a given rate. We say a fluid is *ideal* if we don't consider viscosity.

Proposition 2.62 (Density). The density of a fluid of mass m that occupies a volume V is:

$$\rho = \frac{m}{V}$$

The density depends on temperature and pressure[4].

Definition 2.63. A fluid is said to be *incompressible* if its density doesn't varies with the pressure.

Proposition 2.64 (Pressure). Consider a point x and a small sphere centered at x. Then, the pressure $p(x)$ at point x is:

$$p(x) = \frac{\sum F_N}{S}$$

where $\sum F_N$ is the sum of normal forces and S is the surface which the forces are applied to. The SI unit of pressure is the Pascal: 1 Pa = 1 N/m^2.

Proposition 2.65 (Hydrostatic pressure). Consider a static fluid with constant density ρ and let p_0 be the pressure on its surface. Then, the pressure p on a depth h is

$$p = p_0 + \rho g h$$

Proposition 2.66 (Pascal's principle). Any pressure applied to the surface of a fluid is transmitted uniformly throughout the fluid in all directions, in such a way that initial variations in pressure are not changed.

$$p_1 = \frac{F_1}{S_1} = \frac{F_2}{S_2} = p_2$$

Proposition 2.67 (Archimedes' principle). Any object (of mass m), totally or partially immersed in a fluid of density ρ, is buoyed up by a force equal to the weight of the fluid displaced by the object, that is:

$$F_B := \rho g V_{\text{dis}}$$

where F_E is called the *buoyancy* and V_{dis} is the volume of the liquid displaced[5].

[4] This variation is typically small for solids and liquids but much greater for gases.

[5] Note that if $F_B - mg > 0$, the object rises to the surface of the liquid; if $F_B - mg < 0$, the object sinks, and if $F_B - mg = 0$, the object is neutrally buoyant, that is, it remains in place without either rising or sinking.

Definition 2.68. We define the *discharge of a fluid* as:

$$Q = Sv$$

where S is the cross-sectional area of the portion of the channel occupied by the flow and v is the average flow velocity. If the velocity is not constant, then:

$$Q = \iint_S \mathbf{v} \cdot d\mathbf{S}$$

Proposition 2.69 (Continuity equation). Consider an incompressible fluid moving throughout a channel. Then, the volume per unit of time is conserved, that is, the discharge is conserved. Mathematically:

$$Q_1 = S_1 v_1 = S_2 v_2 = Q_2$$

Definition 2.70. *Laminar flow* is a fluid motion that occurs when a fluid flows in parallel layers, with no disruption between those layers. *Turbulent flow* is a fluid motion characterized by chaotic changes in pressure and flow velocity.

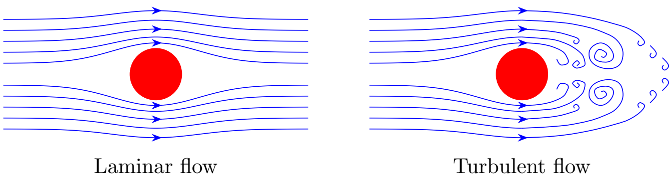


Figure 2.1.12

Proposition 2.71 (Bernolli's principle). Consider an incompressible and ideal fluid of density ρ with steady laminar flow. Then:

$$p + \rho g h + \frac{1}{2}\rho v^2 = \text{const.}$$

where p is the pressure at a point on a streamline; h, the elevation of the point from a reference frame, and v, the fluid flow speed at the chosen point.

Proposition 2.72 (Lift force). If the air has density ρ and an object of cross-sectional area S is moving at a velocity of v relative to the air, then the lift force is:

$$F_L = \frac{1}{2} C_L \rho S v^2$$

where C_L is the *lift coefficient*. From that we deduce that the minimum velocity for lifting is:

$$F_L = mg \implies v_{\min} = \sqrt{\frac{2mg}{C_L \rho S}}$$

Proposition 2.73 (Viscosity). Consider a fluid trapped between two plates of area S, one fixed and the other one in parallel motion at constant speed v. If we suppose a laminar flow, each layer of fluid moves faster than the one just below it and so this creates a friction force resisting their relative motion. An external force F is therefore required in order to keep the top plate moving at constant speed. This force is given by:

$$F = \eta \frac{vS}{z}$$

where z is the separation between the plates and η is the viscosity of the fluid ($[\eta] = \text{Pa} \cdot \text{s}$).

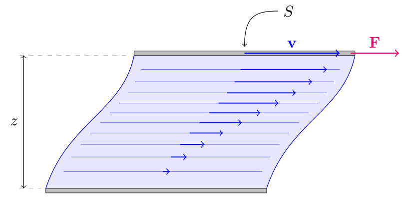


Figure 2.1.13

Proposition 2.74 (Velocity of a fluid in a channel). Consider a fluid with viscosity η in laminar flow so that the layer in contact with the wall of the channel (of radius r) is at rest. Let p_1 be the pressure at one point of the channel and p_2 be the pressure at another point separated a distance L along the x-axis from the previous point. Then, the speed of each layer of fluid at a distance x from the center of the channel is:

$$v(y) = \frac{p_1 - p_2}{4\eta L}(r^2 - y^2)$$

The average speed and maximal speed of the fluid are:

$$v_{\text{avg}} = \frac{p_1 - p_2}{8\eta L} r^2 \qquad v_{\max} = \frac{p_1 - p_2}{4\eta L} r^2 \tag{2.1.3}$$

Proposition 2.75 (Poiseuille's law). In conditions of the equation (2.1.3), we have:

$$Q = S v_{\text{avg}} = \frac{\pi}{8\eta} \frac{p_1 - p_2}{L} r^4 \implies \Delta p = \frac{8\eta}{\pi} \frac{L}{r^4} Q$$

If we denote $R_f := \frac{8\eta}{\pi} \frac{L}{r^4}$ the hydrodynamic resistance, we can write Poiseuille's law as follows:

$$\Delta p = R_f Q,$$

which is an analogy of Ohm's law[6].

Proposition 2.76 (Resistance in fluids). Consider n channels each of resistance R_i. The total resistance will be:

- Connected in series:

$$R_T = \sum_{i=1}^{n} R_i$$

- Connected in parallel:

$$\frac{1}{R_T} = \sum_{i=1}^{n} \frac{1}{R_i}$$

Proposition 2.77 (Dissipated power). Consider a fluid that passes throughout a channel of resistance R_f. If the discharge of the fluid is Q in a section where the pressure difference is Δp, the *dissipated power* will be:

$$P = \Delta p Q = R_f Q^2$$

[6] In that case, R_f would play the role of electric resistance; Q, the role of intensity of the current, and Δp, the role of electric potential difference.

Proposition 2.78 (Drag forces). An object moving at a velocity v in a fluid of density ρ and viscosity η creates drag forces:

- For low speeds and high viscosity, viscous forces predominate:
$$F = k\eta vr$$
where $k = 6\pi$ if the object is an sphere and r is its radius.
- For high speeds and low viscosity, inertial forces predominate:
$$F = \frac{1}{2} C_a \rho S v^2$$
where C_a is the aerodynamic coefficient and S the cross-sectional area.

Proposition 2.79 (Terminal velocity). An object falling (by gravity) inside a fluid attains a maximum velocity (terminal velocity) when its weight equals the drag force. We have two cases to consider:

- For viscous forces:
$$v_t = \frac{mg}{k\eta r}$$
- For inertial forces:
$$v_t = \sqrt{\frac{2mg}{C_a \rho S}}$$

Proposition 2.80 (Reynolds number). The Reynolds number helps to predict flow patterns in different fluid flow situations.
$$\mathrm{Re} = \frac{\rho v D}{\eta} \approx \frac{F_{\text{inertial}}}{F_{\text{viscous}}}$$
where v is the flow speed and D is the diameter of the object.
$$\begin{aligned} \mathrm{Re} < 2000 &\implies \text{laminar flow} \\ \mathrm{Re} > 3000 &\implies \text{turbulent flow} \end{aligned}$$

Chapter 2.2

Second year

2.2.1 Structure of matter and thermodynamics

2.2.1.1 | Structure of the matter

Kinetic theory of gases

Definition 1.1. A gas is constituted by large amount of particles moving at higher velocities and satisfying Newton's laws. Hence, we may consider the following assumptions:

- We can underestimate the gravity acting on the particles.
- The collisions between particles and between a particle and a wall of the container (perfectly rigid and with infinite mass) are completely elastic.
- The particles are point-particles.
- There is no interaction between particles (a part from the momentum of a collision).
- There is no preferred position and direction for the particles.

Proposition 1.2 (Molecular pressure). Consider a container of volume V that contains N molecules, each of mass m, of a gas. Then, the pressure P of the gas is:

$$P = \frac{N}{V} m \langle {v_x}^2 \rangle$$

where $\langle {v_x}^2 \rangle$ is the mean of the squares of the x-components of the velocities of all particles.

Proposition 1.3 (Molecular kinetic energy). Consider a gas at a temperature T. The average kinetic energy of a particle associated with x-axis movement of it is:

$$\langle K_x \rangle = \frac{1}{2} k_B T$$

where k_B is the Boltzmann constant. Since, by one of the initial hypothesis, $\langle {v_x}^2 \rangle = \langle {v_y}^2 \rangle = \langle {v_z}^2 \rangle$, then $\langle v^2 \rangle = 3\langle {v_x}^2 \rangle$ and therefore the mean kinetic energy $\langle K \rangle$ of a molecule is:

$$\langle K \rangle = \frac{3}{2} k_B T$$

Proposition 1.4 (Molecular velocities). Consider a gas of molar mass M constituted by molecules of mass m at a temperature T. Then, the *mean-square speed of the particles* is:

$$\langle v^2 \rangle = \frac{3k_B T}{m} = \frac{3RT}{M}$$

The *root-mean-square speed* is defined as $v_{\mathrm{rms}} = \sqrt{\langle v^2 \rangle}$

Proposition 1.5 (Boltzmann distribution). Consider a system at a temperature T in thermodynamic equilibrium. Then, the probability $P(E)$ to find a particle with energy E is proportional to *Boltzmann factor*. That is:

$$P(E) \propto \mathrm{e}^{-\frac{E}{k_B T}}$$

Proposition 1.6 (Maxwell-Boltzmann distribution). The number of molecules (from a total of N) of mass m in a gas moving at velocities between v and $v + \mathrm{d}v$ and at a temperature T is:

$$\mathrm{d}N = N f(v) \mathrm{d}v$$

where $f(v)$ is:

$$f(v) = \frac{4}{\sqrt{\pi}} \left(\frac{m}{2k_B T} \right)^{3/2} v^2 \mathrm{e}^{-\frac{mv^2}{2k_B T}}$$

Proposition 1.7 (Distribution of molecular velocities). Consider a gas constituted of molecules of mass m moving at a velocity v at a temperature T. If $v_{\max}$, $\langle v \rangle$ and v_{rms} are the maximum speed, mean speed and root-mean-square speed respectively, then:

$$\frac{\mathrm{d}f(v)}{\mathrm{d}v} = 0 \implies v_{\max} = \sqrt{\frac{2k_B T}{m}}$$

$$\langle v \rangle = \int_0^\infty v f(v) \mathrm{d}v = \sqrt{\frac{8k_B T}{\pi m}}$$

$$v_{\mathrm{rms}} = \sqrt{\langle v^2 \rangle} = \sqrt{\int_0^\infty v^2 f(v) \mathrm{d}v} = \sqrt{\frac{3k_B T}{m}}$$

Specific heat and equipartition theorem

Definition 1.8. When we heat up a substance, we transfer energy to it resulting in an increase of its internal energy U. The amount of heat Q necessary to increase the temperature of a substance is proportional to the variation of the temperature and its mass m. That is:

$$Q = C\Delta T = cm\Delta T$$

Definition 1.9. *Heat capacity* C is defined as the amount of heat to be supplied to an object to increase its temperature by one degree.

Definition 1.10. *Specific heat* c is defined as the heat capacity per unit of mass:

$$c = \frac{C}{m}$$

where m is the mass of the object to heat.

Definition 1.11. *Molar heat capacity* c_m is defined as the heat capacity per unit of mole:

$$c_{\mathrm{m}} = \frac{C}{n} = \frac{mc}{n} = \frac{M}{n}$$

where n is the number of moles of the object to heat, m its mass and M its molar mass.

Definition 1.12. The *adiabatic index* γ is defined as:

$$\gamma = \frac{C_P}{C_V}$$

where C_P is the heat capacity at constant pressure and C_V is the heat capacity at constant volume[1].

[1] In liquids and solids we have $C_p \approx C_V =: C$.

Definition 1.13 (Internal energy). The internal energy U of an ideal gas constituted of monoatomic particles is:

$$U = N\langle K_{\text{trans}}\rangle = \frac{3}{2}nRT$$

where N is the number of particles in the gas on it; n, the number of moles, and T, its the temperature.

Proposition 1.14 (Mayer's relation). Consider a substance constituted by n moles of an ideal gas. Then:

$$C_P = C_V + nR$$

Proposition 1.15 (Heat capacities in gases). Consider a substance constituted by n moles of an ideal gas. Since $C_V = \frac{\mathrm{d}U}{\mathrm{d}T}$, we have:

$$C_V = \frac{3}{2}nR \qquad C_P = \frac{5}{2}nR$$

Therefore, $\gamma = \frac{5}{3}$.

Theorem 1.16 (Equipartition theorem). Consider a substance at a temperature T in thermodynamic equilibrium. Then, the energy behave equally in each quadratic degree of freedom associated at each component of the kinetic or potential energy. Thus, there exists an average energy of $\frac{1}{2}k_BT$ per molecule or an average energy of $\frac{1}{2}RT$ per mole associated with each degree of freedom[2].

Corollary 1.17 (Equipartition theorem on diatomic molecules). Consider a diatomic molecule of mass m rotating around x and y axis. Then, its energy will be of the form:

$$E = \frac{1}{2}m\left({v_x}^2 + {v_y}^2 + {v_z}^2\right) + \frac{1}{2}I_x{\omega_x}^2 + \frac{1}{2}I_y{\omega_y}^2$$

Since we have 5 quadratic degrees of freedom, the total energy E will be $E = \frac{5}{2}k_BT$. If a gas in constituted by N diatomic molecules, then:

$$U = NE = \frac{5}{2}Nk_BT = \frac{5}{2}nN_Ak_BT = \frac{5}{2}nRT$$

where N_A is the Avogadro constant and n is the number of moles of the gas. Therefore, we will have $C_V = \frac{5}{2}nR$, $C_P = \frac{7}{2}nR$ and $\gamma = \frac{7}{5}$.

Corollary 1.18 (Dulong-Petit law). Consider a solid and suppose its atoms are connected with springs with effective constant k_{eff}. Then:

$$E = \frac{1}{2}m\left({v_x}^2 + {v_y}^2 + {v_z}^2\right) + \frac{1}{2}k_{\text{eff}}\left(x^2 + y^2 + z^2\right)$$

Since we have 6 quadratic degrees of freedom, the total energy E will be $E = \frac{6}{2}k_BT$. If a gas in constituted by N atoms, then:

$$U = NE = \frac{6}{2}Nk_BT = 3nN_Ak_BT = 3nRT$$

where n is the number of moles of the solid. Therefore, we will have $C = 3nR$.

Black-body radiation

Definition 1.19 (Thermal radiation). *Thermal radiation* is the electromagnetic radiation emitted by a body as a consequence of its temperature. All bodies emit this radiation and absorb the one emitted by its surroundings. In thermal equilibrium the emission and absorption are equal.

Proposition 1.20 (Black body). A *black body* is an object that absorbs all electromagnetic radiation incident on it.

Proposition 1.21 (Stefan-Boltzmann law). The energy radiated by a black body at a temperature T per unit of area and time (called *radiance*) is:

$$I = \sigma T^4$$

where σ is the Stefan-Boltzmann constant.

Proposition 1.22 (Wien's displacement law). The radiance does not distribute uniformly along all wavelengths (*spectral radiance* $I(\lambda)$). The maximum of this function is taken when

$$\lambda_{\max} =: \frac{b}{T}$$

where b is the *Wien's displacement constant* and T is the temperature of the body.

Proposition 1.23 (Rayleigh-Jeans law). *Rayleigh-Jeans law* is an approximation to the spectral radiance of electromagnetic radiation of a black body at a given temperature T as a function of the wavelength through classical arguments:

$$I(\lambda) = \frac{2\pi ck_BT}{\lambda^4}$$ [3]

Proposition 1.24 (Planck's law). To solve the ultraviolet catastrophe, Planck deduced the following formula for the spectral radiance:

$$I(\lambda) = \frac{2\pi hc^2}{\lambda^5\left(\mathrm{e}^{\frac{hc}{\lambda k_BT}} - 1\right)}$$ [4]

[2] The equipartition theorem fails when temperatures are very high or very low due to the discretization of the energy postulated by quantum physics.

[3] The Rayleigh-Jeans law agrees with experimental results at large wavelengths (low frequencies) but strongly disagrees at short wavelengths (high frequencies). This inconsistency between observations and the predictions of classical physics is commonly known as the *ultraviolet catastrophe*.

[4] Note that from here we can deduced Stefan-Boltzmann and Wien's displacement laws as follows:

$$I = \int_0^\infty I(\lambda)\mathrm{d}\lambda = \frac{2\pi^5{k_B}^4}{15c^2h^3}T^4 =: \sigma T^4 \qquad \frac{\mathrm{d}I(\lambda)}{\mathrm{d}\lambda} = 0 \implies \lambda = \frac{hc}{4.965}\cdot\frac{1}{T} =: \frac{b}{T}$$

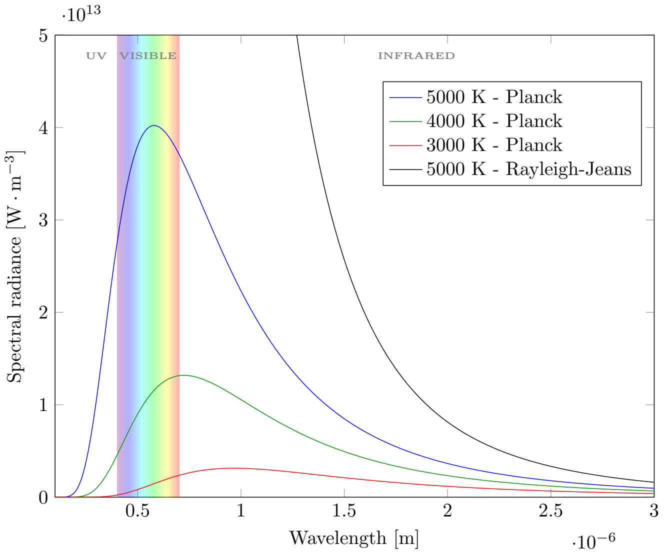


Figure 2.2.1: Graphical illustration of the ultraviolet catastrophe

Photoelectric effect

Definition 1.25 (Photoelectric effect). The *photoelectric effect* consists in the emission of electrons when electromagnetic radiation hits a material. Electrons emitted in this manner are called *photoelectrons*. Moreover we have the following properties:

- Photoelectric effect only occurs when the incident light is of frequency greater than or equal to a *threshold frequency* ν_0.
- Kinetic energy of the electrons increase proportionally to the frequency of the incident light.
- Increasing the intensity of the incident light does not increase the energy of photoelectrons, but the number of photoelectrons.

Proposition 1.26 (Stopping potential). Let ϕ be the energy required to remove an electron from the surface of a material. If we hit this surface with photons of frequency ν, then:

$$\frac{1}{2}m_e{v_{\max}}^2 = h\nu - \phi$$

Moreover, if we connect a potential difference V contrary to the movement of the electrons, then:

$$eV = h\nu - \phi$$

The electrons with lower energy than $\phi = h\nu_0$ won't have enough energy to remove an electron of the material.

Proposition 1.27 (Planck-Einstein relation). Relating the energy E of a photon of frequency ν and wavelength λ we have:

$$E = h\nu = \frac{hc}{\lambda}$$

Proposition 1.28 (De Broglie relation). The momentum p of photons of energy E and wavelength λ is:

$$p = \frac{E}{c} = \frac{h}{\lambda}$$

Light

Definition 1.29 (Light). We can think the light as a particle or as a wave. In particular, when it propagates, it behave like an electromagnetic wave and travels at a velocity

$$c = \frac{1}{\sqrt{\varepsilon_0\mu_0}}$$

where ε_0 is the vacuum permittivity and μ_0 vacuum permeability. Moreover the oscillating directions of the electric and magnetic field are perpendicular to each other and to the direction of propagation.

Definition 1.30 (Compton scattering). The *compton scattering* occurs when a photon of wavelength λ_1 collides with an electron and as a consequence the collision produces another photon of wavelength $\lambda_2 > \lambda_1$ (with less energy than the pervious one) deflected an angle θ from the original trajectory of the photon. Moreover, we have:

$$\lambda_2 - \lambda_1 = \frac{h}{m_e c}(1 - \cos\theta)$$[5]

where m_e is the mass of the electron.

Matter wave

Proposition 1.31 (Bohr's complementary principle). There are experiments in which bodies behave like particles and other ones in which they behave like waves.

Definition 1.32 (Wavelenth of a particle). Consider a particle of mass m, kinetic energy K and momentum p. Then its wavelength is:

$$\lambda = \frac{h}{p} = \frac{hc}{2mc^2K}$$

As a consequence, all elementary particles propagate like waves an exchange energy like particles.

Proposition 1.33 (Heisenberg's uncertainty principle). Let ΔY be the uncertainty of the magnitude Y of a particle. Then, for all particles we have:

$$\Delta x \Delta p \geq \frac{\hbar}{2} \qquad \Delta E \Delta t \geq \frac{\hbar}{2}$$

Wave function

Definition 1.34 (Schrödinger equation). Given that we cannot know the position and velocity of a particle with unlimited precision, a particle of mass m is described with a *wave function* $\Psi(x,t)$[6] which is a solution to *Schrödinger equation*:

$$\frac{-\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + U(x,t)\Psi(x,t) = i\hbar\frac{\partial\Psi(x,t)}{\partial t}$$

where $U(x,t)$ is the potential energy that the particle is subject to. More generally, the Schrödinger equation in three dimensions is:

$$\frac{-\hbar^2}{2m}\nabla^2\Psi(\mathbf{r},t) + U(\mathbf{r},t)\Psi(\mathbf{r},t) = i\hbar\frac{\partial\Psi(\mathbf{r},t)}{\partial t}$$

where $\mathbf{r} = x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$.

[5] This is deduced taking into account the conservation of energy and momentum.
[6] It is important that the function $\Psi(x,t)$ must be continuous.

Proposition 1.35 (Properties of Schrödinger equation). Consider a particle whose wave function is $\Psi(x,t)$. Then:

- The probability to find the particle between x and $x+\mathrm{d}x$ is:
$$|\Psi(x,t)|^2\mathrm{d}x$$
- *Probability density*:
$$P(x,t) = |\Psi(x,t)|^2 = \Psi(x,t)\Psi^*(x,t)$$
- *Normalization condition*:
$$\int_{-\infty}^{\infty} |\Psi(x,t)|^2\mathrm{d}x = 1$$
- *Expectation value of* x:
$$\langle x \rangle = \int_{-\infty}^{\infty} x\Psi(x,t)\Psi^*(x,t)\mathrm{d}x = 1$$

Here $\Psi^*(x,t)$ denotes the complex conjugate of $\Psi(x,t)$.

Definition 1.36 (Time-independent Schrödinger equation). Consider a stationary solution of the Schrödinger equation of the form:

$$\Psi(x,t) = \Phi(x)\mathrm{e}^{\frac{-\mathrm{i}Et}{\hbar}}$$

Then, if the potential energy $U(x,t)$ to which the particle is subject does not depend on time, that is $U(x,t) = U(x)$, we get the *time-independent Schrödinger equation*:

$$\frac{-\hbar^2}{2m}\frac{\mathrm{d}^2\Phi(x)}{\mathrm{d}x^2} + U(x)\Phi(x) = E\Phi(x) \tag{2.2.1}$$

Proposition 1.37 (Particle in a box-1D). Consider a particle of mass m confined to a one-dimensional box of length L. We can think that it is subjected to a potential

$$U(x) = \begin{cases} \infty & \text{if} \quad x \leq 0 \\ 0 & \text{if} \quad 0 < x < L \\ \infty & \text{if} \quad x \geq L \end{cases}$$

Since the particle cannot leave the region $(0,L)$, we have that $\Phi(x) = 0$ for $x \leq 0$ and $x \geq L$. Therefore, by equation (2.2.1):

$$\frac{-\hbar^2}{2m}\frac{\mathrm{d}^2\Phi(x,t)}{\mathrm{d}x^2} = E\Phi(x) \qquad \text{for } 0 \leq x \leq L$$

If we define $k^2 = \frac{2mE}{\hbar^2}$, we have

$$\frac{\mathrm{d}^2\Phi(x,t)}{\mathrm{d}x^2} + k^2\Phi(x) = 0 \qquad \text{for } 0 \leq x \leq L$$

which is the equation of a simple harmonic oscillator with solution $\Phi(x) = A\sin(kx) + B\cos(kx)$. Taking into account boundary conditions, we have that:

$$\Phi(x) = \Phi_n(x) = \sqrt{\frac{2}{L}}\sin\left(\frac{n\pi}{L}x\right)$$

where the number $n \in \mathbb{N}$ is called *quantum number*. In particular, $k = k_n = \frac{n\pi}{L}$ and therefore:

$$E_n = \frac{\hbar^2 k_n^2}{2m} = n^2\left(\frac{h^2}{8mL^2}\right) = n^2 E_1$$

And we observe that the energy is discretized in different levels.

Proposition 1.38 (Particle in a box-3D). If the particle of mass m is now confined to a three-dimensional box of edges a, b and c, we get:

$$\Phi_{n_x n_y n_z}(\mathbf{r}) = \sqrt{\frac{8}{abc}}\sin\left(\frac{n_x\pi}{a}x\right)\sin\left(\frac{n_y\pi}{b}x\right)\sin\left(\frac{n_z\pi}{c}x\right)$$

where n_x, n_y and n_z are independent quantum numbers[7]. Moreover:

$$E_{n_x n_y n_z} = {n_x}^2\left(\frac{h^2}{8ma^2}\right) + {n_y}^2\left(\frac{h^2}{8mb^2}\right) + {n_z}^2\left(\frac{h^2}{8mc^2}\right)$$

Definition 1.39. An energy level is *degenerate* if it corresponds to two or more different measurable states of a quantum system. For example, if a particle is contained in a cube, then:

$$E_{112} = E_{121} = E_{211} = 6E_1$$

where E_1 is the ground-state energy of the particle contained in a one-dimensional box.

Proposition 1.40 (Bohr's correspondence principle). In the limit of very large quantum numbers, the classical calculation and the quantum calculation must yield the same results.

Atoms

Definition 1.41 (Bohr model). The Bohr model[8] of an atom can be sum up with three postulates:

1. The electrons can move only in certain non-radiating circular orbits called stationary states.
2. If E_i and E_f are the initial and final energies of the atom, the frequency of the emitted radiation during a transition is given by
$$\nu = \frac{E_i - E_f}{h}$$
3. The angular momentum is quantized:
$$m_e v_n r_n = n\hbar \qquad n \in \mathbb{N}$$
where v_n and r_n are the speed of the electron and the radius of the orbit respectively in the state n.

Proposition 1.42 (Radii of Bohr orbits). The radius r_n of the n-th Bohr orbit of a monoelectronic atom with atomic number Z is:

$$r_n = n^2\frac{\hbar^2}{m_e k Z e^2} =: n^2\frac{a_0}{Z}$$

where k is the Coulomb constant. $a_0 = 0.0529$ nm is called *first Bohr radius*.

[7] This is obtained from the fact that the solutions $\Phi n_x n_y n_z(\mathbf{r})$ of the Schrödinger equation in three dimensions are of the form: $\Phi n_x n_y n_z(\mathbf{r}) = \Phi_{n_x}(x)\Phi_{n_y}(y)\Phi_{n_z}(z)$

[8] Bohr model only works for monoelectronic atoms, that is, atoms with only one electron.

Proposition 1.43 (Energy levels). The total energy E_n of the n-th orbit of a monoelectronic atom with atomic number Z is:

$$E_n = -Z^2 \frac{E_0}{n^2} \tag{2.2.2}$$

where $E_0 = \frac{m_e k^2 e^4}{2\hbar^2} = 13.6$ eV.

Proposition 1.44 (Rydberg-Ritz law). An electron that goes from an energy level n_i to a lower one $n_f < n_i$ emits a photon whose wavelength is:

$$\frac{1}{\lambda} = \frac{k^2 m_e e^4}{4\pi c\hbar^3} Z^2 \left(\frac{1}{{n_f}^2} - \frac{1}{{n_i}^2} \right) =: R_H Z^2 \left(\frac{1}{{n_f}^2} - \frac{1}{{n_i}^2} \right)$$

where R_H is the *Rydberg constant*.

Quantum theory of atoms

Definition 1.45 (Quantum numbers in spherical coordinates). Consider an atom with a single electron. Then, the potential energy for the electron depends only on the radial component and so we can make a change of variable to spherical coordinates (r, θ, ϕ)[9]. Hence, the independent quantum numbers n_x, n_y and n_z obtained from cartesian coordinates will become the quantum numbers n (associated with r), ℓ (associated with θ) and m_ℓ[10] (associated with ϕ), which in this case, are not independent. More precisely we have:

- *Principal quantum number*: $n = 1, 2, 3, \ldots$

  The energy, as seen in (2.2.2), is given by:

  $$E_n = -Z^2 \frac{13.6 \text{ eV}}{n^2}$$

- *Orbital quantum number*: $\ell = 0, 1, 2, \ldots, n-1$

  Moreover the magnitude $\|\mathbf{L}\|$ of the orbital angular momentum $\mathbf{L}$ is related to the orbital quantum number ℓ by:

  $$\|\mathbf{L}\| = \sqrt{\ell(\ell+1)}\hbar$$

- *Magnetic quantum number*: $m_\ell = 0, \pm 1, \pm 2, \ldots, \pm \ell$

  Moreover the z component L_z of the orbital angular momentum $\mathbf{L}$ is given by the quantum condition

  $$L_z = m_\ell \hbar$$

Therefore are n^2 degenerate states for the energy E_n. In terms of wave function we can write

$$\Psi_{n\ell m_\ell}(\mathbf{r}) = R_{n\ell}(\mathbf{r}) Y_{\ell m_\ell}(\mathbf{r})$$

Definition 1.46 (Spin). An electron has a *intrinsic orbital angular momentum* or simply *spin* $\mathbf{S}$ such that:

$$\|\mathbf{S}\| = \sqrt{s(s+1)}\hbar \qquad S_z = s\hbar$$

where $s = \pm\frac{1}{2}$ is another quantum number to be considered in the wave function and it is called *spin quantum number*. This fact result in $2n^2$ possible states for the energy E_n of a electron.

[9] Here ϕ denotes the azimuthal angle.

[10] Sometimes for simplicity the subindex ℓ is omitted.

n	ℓ	Type of orbital	m_ℓ
1	0	s	0
2	0	s	0
2	1	p	$-1, 0, 1$
3	0	s	0
3	1	p	$-1, 0, 1$
3	2	d	$-2, -1, 0, 1, 2$
4	0	s	0
4	1	p	$-1, 0, 1$
4	2	d	$-2, -1, 0, 1, 2$
4	3	f	$-3, -2, -1, 0, 1, 2, 3$
5	0	s	0
5	1	p	$-1, 0, 1$
5	2	d	$-2, -1, 0, 1, 2$
5	3	f	$-3, -2, -1, 0, 1, 2, 3$
5	4	g	$-4, -3, -2, -1, 0, 1, 2, 3, 4$

Table 2.2.1: Atomic orbitals in terms of quantum numbers n, ℓ and m_ℓ. Moreover for each configuration we have two possible values for the spin: $-\frac{1}{2}$ and $\frac{1}{2}$.

Polyelectronic atoms

Proposition 1.47 (Schrödinger equation). Consider an atom with N electrons. The Schrödinger equation becomes:

$$\left\{ \frac{-\hbar}{2\mu} \sum_{i=1}^{N} {\boldsymbol{\nabla}_i}^2 - \sum_{i=1}^{N} \frac{Ze^2}{4\pi\varepsilon_0 r_i} + \sum_{\substack{i,j=1 \\ i>j}}^{N} \frac{e^2}{4\pi\varepsilon_0 r_{ij}} \right\} \cdot \Phi(\mathbf{r}_1, \ldots, \mathbf{r}_N) = E\Phi(\mathbf{r}_1, \ldots, \mathbf{r}_N)$$

where $\mu = \dfrac{m_{\text{nuc}} m_e}{m_{\text{nuc}} + m_e}$ is the reduced mass of the electron (m_e) and the nucleus (m_{nuc}), $\mathbf{r}_i = x_i\mathbf{i} + y_i\mathbf{j} + z_i\mathbf{k}$ and ${\boldsymbol{\nabla}_i}^2 = \dfrac{\partial^2}{\partial x_i^2} + \dfrac{\partial^2}{\partial y_i^2} + \dfrac{\partial^2}{\partial z_i^2}$. This equation cannot be solved exactly but we can find approximations to it if we suppose:

- We neglect the interactions between electrons.
- We consider that the particles are identic and we cannot distinguish them.

Definition 1.48 (Fermions). A *fermion* is a particle that follows Fermi-Dirac statistics and has half integer spin.

Definition 1.49 (Boson). A *boson* is a particle that follows Bose-Einstein statistics and has integer spin.

Proposition 1.50 (Pauli exclusion principle). Two or more identical fermions cannot occupy simultaneously the same quantum state.

Proposition 1.51 (Symmetry of the wave function). Consider two non-interacting identical particles. The probability density of the two particles with wave function $\Psi(\mathbf{r}_1, \mathbf{r}_2)$ must be identical to that with wave function $\Psi(\mathbf{r}_2, \mathbf{r}_1)$. Therefore,

$$|\Psi(\mathbf{r}_1, \mathbf{r}_2)|^2 = |\Psi(\mathbf{r}_2, \mathbf{r}_1)|^2$$

and hence Ψ has to be necessary symmetric ($\Psi(\mathbf{r}_1, \mathbf{r}_2) = \Psi(\mathbf{r}_2, \mathbf{r}_1)$) or antisymmetric ($\Psi(\mathbf{r}_1, \mathbf{r}_2) = -\Psi(\mathbf{r}_2, \mathbf{r}_1)$). Moreover we have:

1. Φ is symmetric if and only if the particles are bosons.
2. Φ is antisymmetric if and only if the particles are fermions.

Nuclear physics

Definition 1.52 (Atom). An atom X formed by Z protons and N neutrons is denoted as ${}_{\mathrm{Z}}^{\mathrm{A}}\mathrm{X}$ where $A := Z+N$[11]. The number Z is called *atomic number* and the number A, *mass number*.

Definition 1.53. Two nuclides are

- *isotopes* if they have the same Z but different N and A.
- *isobars* if they have the same N but different Z and A.
- *isotones* if they have the same A but different Z and N.
- *isomers* if they have the same Z, N and A. They differ in the grouping structure.

Proposition 1.54 (Radii of nucleus). The stable nucleus has approximately constant density and therefore the nuclear radius R can be approximated by the following formula:

$$R = R_0 A^{1/3}$$

where $R_0 \approx 1.2$ fm.

Proposition 1.55 (Nucleus mass). The mass of a nucleus $M_{\mathrm{nuc}}(Z, A)$ of atomic number Z and mass number A satisfies:

$$M_{\mathrm{nuc}}(Z, A)c^2 = Zm_{\mathrm{p}}c^2 + (A - Z)m_{\mathrm{n}}c^2 - E_{\mathrm{b}}(Z, A)$$

where $E_{\mathrm{b}}(Z, A)$ is the *binding energy*, that is, the energy required to break up the nucleus into Z protons and $A-Z$ neutrons. If we take into account the mass of the electrons on the atomic mass $M_{\mathrm{at}}(Z, A)$ we get:

$$\begin{aligned} M_{\mathrm{at}}(Z, A)c^2 &= M_{\mathrm{nuc}}(Z, A)c^2 + Zm_e c^2 - E_e(Ze) \approx \\ &\approx ZM_{\mathrm{at}}({}_1^1\mathrm{H})c^2 + (A - Z)m_{\mathrm{n}}c^2 - E_{\mathrm{b}}(Z, A) \end{aligned}$$

where $E_e(Ze)$ is the *electron binding energy* and $E_e(Ze) \ll E_{\mathrm{b}}(Z, A)$ so it can be neglected, and $M_{\mathrm{at}}({}_1^1\mathrm{H})$ is the mass of hydrogen atom ${}_1^1\mathrm{H}$. From this, we can define the *mass defect* Δm:

$$\Delta m = M_{\mathrm{at}}(Z, A) - A$$

where $M_{\mathrm{at}}(Z, A)$ is expressed in u[12].

[11] Sometimes if the atom ${}_{\mathrm{Z}}^{\mathrm{A}}\mathrm{X}$ is well-known, we simply refer to it as ${}^{\mathrm{A}}\mathrm{X}$.

[12] Unified atomic mass unit.

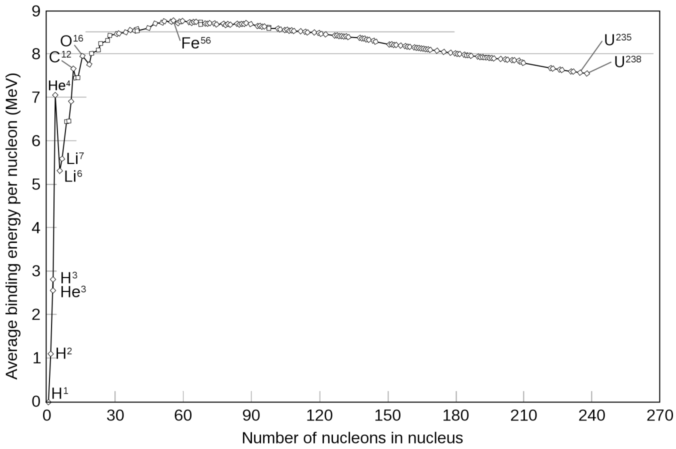


Figure 2.2.2: Binding energy curve

Proposition 1.56 (Semi-empirical mass formula). For a nucleus of atomic number Z and mass number A, we have:

$$\begin{aligned} E_{\mathrm{b}}(Z, A) = c_1 A - c_2 A^{2/3} - c_3 \frac{Z(Z-1)}{A^{1/3}} - \\ - c_4 \frac{(2Z - A)^2}{A} + \delta(Z, A) \end{aligned}$$

where

$$\delta(Z, A) = \begin{cases} -c_5 A^{-1/2} & \text{if} \quad N, Z \text{ are odd} \\ 0 & \text{if} \quad A \text{ is odd} \\ +c_5 A^{-1/2} & \text{if} \quad N, Z \text{ are even} \end{cases}$$

empirically, it can be seen that $c_1 \approx 15.56$ MeV, $c_2 \approx 17.23$ MeV, $c_3 \approx 0.697$ MeV, $c_4 \approx 23.285$ MeV and $c_1 \approx 12.00$ MeV.

Definition 1.57 (Q value). The Q *value* for a reaction is defined as:

$$Q = (m_i - m_f)c^2$$

where m_i is the sum of the reactant masses and m_f is the sum of the product masses. The decay will be spontaneous if $Q > 0$ and in this case, the decay will have a net release of energy.

Definition 1.58 (α-decay). An α particle is a nucleus of ${}_2^4\mathrm{He}$, which has a short range. The decay is:

$${}_Z^A\mathrm{X} \to {}_{Z-2}^{A-4}\mathrm{Y} + \alpha$$

In this case:

$$\begin{aligned} Q &= \left[M_{\mathrm{nuc}}\left({}_Z^A\mathrm{X}\right) - M_{\mathrm{nuc}}\left({}_{Z-2}^{A-4}\mathrm{Y}\right) - M_{\mathrm{nuc}}\left({}_2^4\mathrm{He}\right)\right]c^2 = \\ &= \left[M_{\mathrm{at}}\left({}_Z^A\mathrm{X}\right) - M_{\mathrm{at}}\left({}_{Z-2}^{A-4}\mathrm{Y}\right) - M_{\mathrm{at}}\left({}_2^4\mathrm{He}\right)\right]c^2 = \\ &= K_Y + K_\alpha \end{aligned}$$

where $M_{\mathrm{at}}\left({}_Z^A\mathrm{X}\right)$ is the mass of the atom ${}_2^4\mathrm{X}$, $M_{\mathrm{nuc}}\left({}_Z^A\mathrm{X}\right)$ is the mass of its nucleus (and the same for the atom Y), K_{Y} is the kinetic energy of the particle Y and K_α is the kinetic energy of the α particle. Moreover we have:

$$K_{\mathrm{Y}} \approx \frac{4}{A}Q \qquad K_\alpha \approx \frac{A-4}{A}Q$$

Definition 1.59 (β-decay).

1. β^- *decay*: $\mathrm{n} \to \mathrm{p} + e^- + \bar{\nu}_e$

   The decay:

   $$ {}^A_Z\mathrm{X} \to {}_{Z+1}^{A}\mathrm{Y} + e^- + \bar{\nu}_e $$

   Q factor[13]:

   $$ Q = \left[M_{\mathrm{at}}\left({}^A_Z\mathrm{X}\right) - M_{\mathrm{at}}\left({}_{Z+1}^{A}\mathrm{Y}\right)\right]c^2 $$

2. β^+ *decay*: $\mathrm{p} \to \mathrm{n} + e^+ + \nu_e$

   The decay:

   $$ {}^A_Z\mathrm{X} \to {}_{Z-1}^{A}\mathrm{Y} + e^+ + \nu_e $$

   Q factor:

   $$ Q = \left[M_{\mathrm{at}}\left({}^A_Z\mathrm{X}\right) - M_{\mathrm{at}}\left({}_{Z-1}^{A}\mathrm{Y}\right) - 2m_e\right]c^2 $$

3. *Electron capture*: $\mathrm{p} + e^- \to \mathrm{n} + \nu_e$

   The decay:

   $$ {}^A_Z\mathrm{X} + e^- \to {}_{Z-1}^{A}\mathrm{Y} + \nu_e $$

   Q factor:

   $$ Q = \left[M_{\mathrm{at}}\left({}^A_Z\mathrm{X}\right) - M_{\mathrm{at}}\left({}_{Z-1}^{A}\mathrm{Y}\right)\right]c^2 - B_n $$

   where B_n is the ionization energy at the shell n where the electron is captured.

Definition 1.60 (γ-decay). A γ particle is a photon which has long range. The decay is produced when the nucleus goes from an excited state to a less excited state. The decay is:

$$ {}^A_Z\mathrm{X}^* \to {}^A_Z\mathrm{X} + \gamma $$

Definition 1.61 (Radioactive activity). The *radioactive activity* of a substance is defined as the number of decays it has per unit of time. Its unit in the SI is the Bq ($[\mathrm{Bq}] = [\mathrm{s}^{-1}]$). The probability for a radionuclide to decay per unit of time is constant and unique for each radionuclide. This constant λ is called *decay constant*. Moreover if $N(t)$ is the number of radionuclide to decay at time t and $A(t)$ is the activity of the substance at time t, we have:

$$ A(t) = \lambda N(t) = -\frac{\mathrm{d}N(t)}{\mathrm{d}t} $$

And therefore:

$$ N(t) = N_0\mathrm{e}^{-\lambda t} \qquad A(t) = A_0\mathrm{e}^{-\lambda t} $$

where N_0 is the initial number of radionuclides and $A_0 = \lambda N_0$ is the initial activity of the substance.

Definition 1.62 (Half-time). We define the *half-time* $t_{1/2}$ as the time in which the number of radionuclide has reduced by half.

[13]Since neutrino's mass is around 2 eV, we can neglect it.

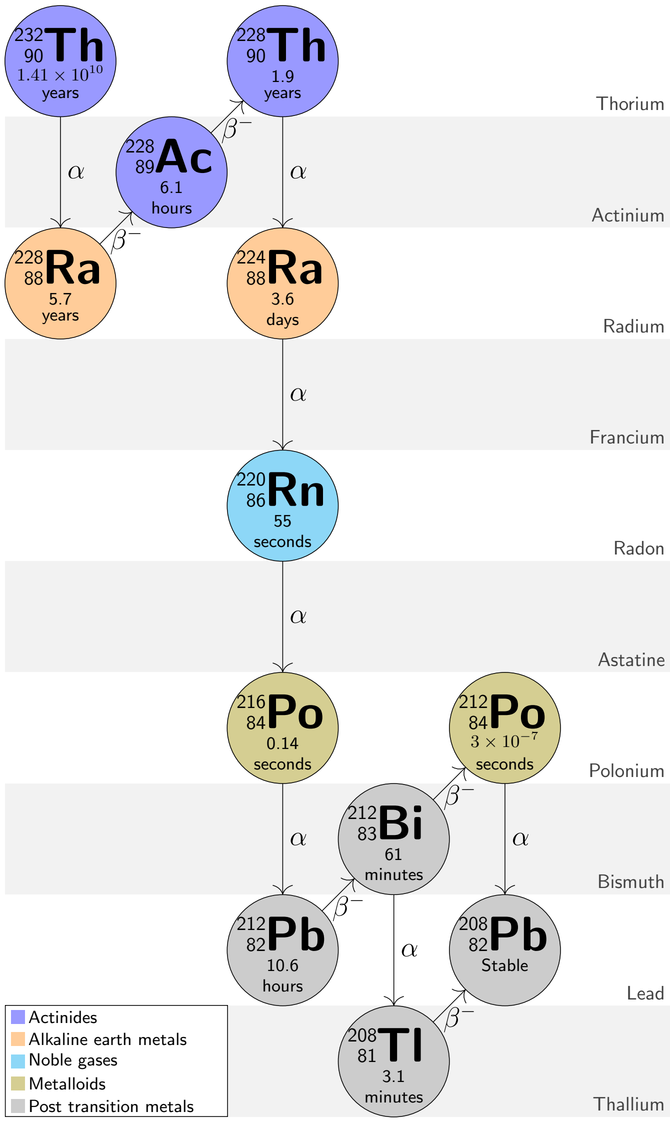


Figure 2.2.3: Decay chain of Thorium or *Thorium series* corresponding to nuclei with $A = 4n$, $n \in \mathbb{N}$.

Proposition 1.63 (Decay chain). Consider the decay chain:

$$ 1 \longrightarrow 2 \longrightarrow 3 $$

where the third nucleus is stable. Let $N_i(t)$ be the number of radionuclides of the substance i at time t, $A_i(t)$ be the activity of the substance i at time t and λ_i be the decay constance of the substance i, all of this for $i = 1, 2$. Then, if $N_1(0) = N_0$ and $N_2(0) = N_3(0) = 0$, we have:

$$ N_1(t) = N_0\mathrm{e}^{-\lambda_1 t} \quad N_2(t) = N_0\frac{\lambda_1}{\lambda_2 - \lambda_1}\left(\mathrm{e}^{-\lambda_1 t} - \mathrm{e}^{-\lambda_2 t}\right) $$

$$ A_1(t) = N_0\lambda_1\mathrm{e}^{-\lambda_1 t} \quad A_2(t) = N_0\frac{\lambda_1\lambda_2}{\lambda_2 - \lambda_1}\left(\mathrm{e}^{-\lambda_1 t} - \mathrm{e}^{-\lambda_2 t}\right) $$

We may have three possible situations:

1. *Secular equilibrium*: $\lambda_1 \ll \lambda_2$. This implies that over short time (compared to the half-life time of the substance 1),

   $$ \mathrm{e}^{-\lambda_1 t} \approx 1 \implies A_2(t) \approx N_0\lambda_1(1 - \mathrm{e}^{-\lambda_2 t}) $$

2. *Transient equilibrium*: $\lambda_1 < \lambda_2$.

$$\frac{A_2(t)}{A_1(t)} = \frac{\lambda_2}{\lambda_2 - \lambda_1}\left(1 - \mathrm{e}^{-(\lambda_2-\lambda_1)t}\right)$$

3. If $\lambda_1 > \lambda_2$, there is no equilibrium.

Definition 1.64 (Nuclear reactions). A nuclear reaction is a reaction of the form:

$$\mathrm{a} + \mathrm{X} \to \mathrm{Y} + \mathrm{b}$$

It is sometimes abbreviated as X(a,b)Y. The Q value of the reaction may behave in two ways:

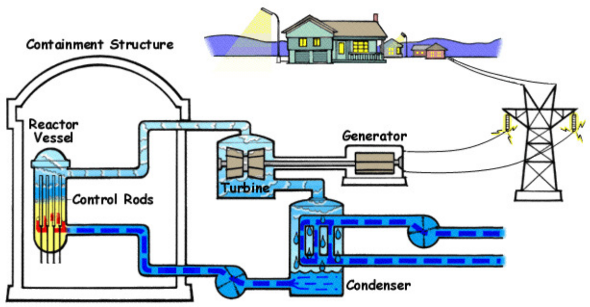
1. *Exothermic reaction ($Q > 0$)*: kinetic energy may be released during the course of a reaction.
2. *Endothermic reaction ($Q < 0$)*: kinetic energy may have to be supplied for the reaction to take place.

Definition 1.65 (Nuclear fission). *Nuclear fission* is a reaction in which the nucleus of an atom splits into two or more smaller nuclei. Nuclear fissions are usually initialized hitting an stable atom with a neutron, turning the atom excited. In fact, nuclear fissions involve a few neutrons which play an important role. The *reproduction factor* k is the number of neutrons produced from a nuclear fission.

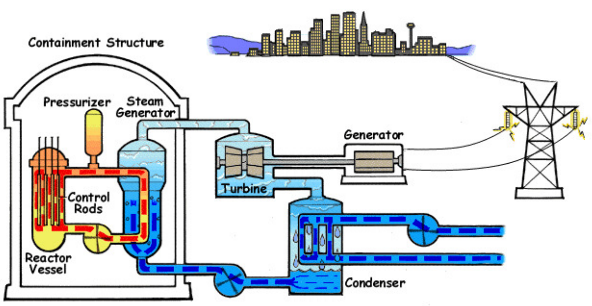
- If $k < 1$, the reaction will stop itself.
- If $k = 1$, the reaction is self-sustained.
- If $k > 1$, the reaction can be uncontrolled[14].

Definition 1.66 (Nuclear reactors). There are mainly two types of nuclear reactors:

1. BWR (*Boiling Water Reactor*):



2. PWR (*Pressurized Water Reactor*):



Definition 1.67 (Nuclear fusion). *Nuclear fusion* is a reaction in which two or more atomic nuclei are combined to form one or more different atomic nuclei and subatomic particles (neutrons or protons)[15]. The most interesting fusion reactions are:

$$\begin{aligned}
&{}^2\mathrm{H} + {}^2\mathrm{H} \to \mathrm{n} + {}^3\mathrm{He} && (Q = 3.3\ \mathrm{MeV})\\
&{}^2\mathrm{H} + {}^2\mathrm{H} \to \mathrm{p} + {}^3\mathrm{H} && (Q = 4.0\ \mathrm{MeV})\\
&{}^2\mathrm{H} + {}^1\mathrm{H} \to {}^3\mathrm{He} + \gamma && (Q = 5.49\ \mathrm{MeV})\\
&{}^2\mathrm{H} + {}^3\mathrm{H} \to \mathrm{n} + {}^4\mathrm{He} && (Q = 17.6\ \mathrm{MeV})
\end{aligned}$$

Elementary particles

Definition 1.68 (Elementary particles). All the matter is composed by 12 fermions (6 quarks and 6 leptons) and all of these have an associated antiparticle. Quarks and Leptons can interact with each other by exchanging Gauge bosons which are carriers of the 4 fundamental forces.

Definition 1.69 (Antimatter). Each elementary particle has an associated *antiparticle* which has the same properties as the initial particle but has different sign on all the charges.

Definition 1.70 (Quark). A *quark* is a fermion with fractional electric charge by 1/3. There are 6 types of quarks, known as *flavors*: *up* u and *down* d (first generation); *charm* c and *strange* s (second generation), and *top* t and *bottom* b (third generation)[16].

Definition 1.71 (Lepton). A *lepton* is a fermion which does not undergo strong interaction. There are 6 types of leptons, known as *flavors*: *electron* e^- and *electron neutrino* ν_e (first generation); *muon* μ^- and *muon neutrino* ν_μ (second generation), and *tau* τ^- and *tau neutrino* ν_τ (third generation).

Definition 1.72 (Lepton number). *Lepton number* L is a quantum number that is conserved in all interactions. It is defined as:

$$L = n_\ell - n_{\bar{\ell}}$$

where where n_ℓ is the number of leptons and $n_{\bar{\ell}}$ is the number of antileptons in a reaction. In addition to lepton number, *lepton family numbers* are defined as:

- *Electron number* L_e: for the electron and electron neutrino.
- *Electron number* L_μ: for the muon and muon neutrino.
- *Electron number* L_τ: for the tau and tau neutrino.

These numbers are also preserved during collisions.

[14] Because of that, in nuclear reactors there are *control roads* of some metal that absorbs neutrons. Therefore, if at any time $k > 1$, the control rods are introduced causing a decrease of the value of k.

[15] Even that nuclear fusion is still being the energetic promise of the future, its production is very costly. Indeed, we have to put together the nuclei in the way that the strong interaction overcome the electrostatic force, that is, put the nuclei together at a distance of $\sim 10^{-15}$ m.

[16] An important fact of quarks is that they cannot be isolated due to the *color confinement* property (see definition 1.74).

	L_e	L_μ	L_τ
e^-	$+1$	0	0
ν_e	$+1$	0	0
e^+	-1	0	0
$\bar{\nu}_e$	-1	0	0
μ^-	0	$+1$	0
ν_μ	0	$+1$	0
μ^+	0	-1	0
$\bar{\nu}_\mu$	0	-1	0
τ^-	0	0	$+1$
ν_τ	0	0	$+1$
τ^+	0	0	-1
$\bar{\nu}_\tau$	0	0	-1

Table 2.2.2: Lepton family numbers

Definition 1.73 (Hadron). A *hadron* is a subatomic particle made of two or three quarks held together by the strong force. There are two types of hadrons:

- Baryons: made of three quarks.
- Mesons: made of two quarks.

Definition 1.74 (Color charge). The *color charge*[17] is a property of quarks and gluons (see definition 1.75) that is related to the particles' strong interactions. There are three types of colors (*red*, *green* and *blue*) and three types of anticolors (*antired*, *antigreen* and *antiblue*). This two families of colors mixed together, or one color with its anticolor, produces the color *white* or, equivalently, has a net color charge of zero.

Definition 1.75 (Fundamental interactions). Fundamental interactions are characterized by the exchange of bosons. The 4 fundamental interactions are:

- Electromagnetic interaction: Based on emission and absorption of photons. The particles with which it interacts have nonzero electric charge. This interaction is described by quantum electrodynamics (QED).
- Strong interaction: It is transported by gluons. The particles with which it interacts have nonzero color charge. This interaction is described by quantum chromodynamics (QCD)[18].
- Weak interaction: It is transported by bosons W^+, W^- and Z^0. It modifies the flavour of a particle.
- Gravity: Te particles wit which it interacts have nonzero mass. The carrier particle of this forces is the graviton, which hasn't been observed yet.

Interaction	Relative intensity	Boson
Strong	1	Gluon g
Electromagnetic	10^{-2}	Photon γ
Weak	10^{-7}	W^+ W^- Z^0
Gravitational	10^{-39}	Graviton G

Table 2.2.3: Relative intensity of fundamental forces

Definition 1.76 (Grand Unified Theory). Electromagnetic and weak forces join together in a unique *electroweak theory* for energies $\gg 100$ GeV. This one join with strong force in the *Grand Unified Theory* for energies $\sim 10^{15}$ GeV. And finally, the 4 interaction join together at energies $> 10^{20}$ GeV or distances $\sim 10^{-34}$ m.

Solids

Definition 1.77. A solid is *crystalline* if atoms form a regular and structured patron. A solid is *amorphous* if the arrangement of atoms is not regular.

Proposition 1.78 (Classical interpretation of resistivity). Consider a metal of resistivity ρ with n_e electrons per unit of volume moving at an average speed of v_{av}. Then:

$$\rho = \frac{m_e v_{\text{av}}}{n_e e^2 \lambda}$$

where $\lambda = v_{\text{av}}\tau$ is the mean free path of electrons between collisions with the lattice ions and τ is the average time between these collisions[19].

Proposition 1.79 (Quantum interpretation of resistivity). Free electrons do not interact neither with ions nor with themselves. Indeed they behave as a particles in a gas (*fermi gas*). Moreover by Pauli exclusion principle, there can only be two electrons in each energy state. At $T = 0$ K the energy E_F of the last filled (or half-filled) energy state is called *Fermi energy*:

$$E_F = \frac{h^2}{8m_e}\left(\frac{3N}{\pi V}\right)^{2/3}$$

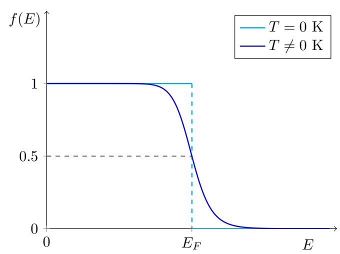
where N is the number of free electrons and V is the volume they occupy. That is, $\frac{N}{V}$ is the density of free electrons. The average energy E_{av} at $T = 0$ K is:

$$E_{\text{av}} = \frac{3}{5}E_F$$

Definition 1.80. The *Fermi factor* $f(E)$ is defined as the probability of a state being occupied. At $T = 0$ K we have:

$$f(E) = \begin{cases} 1 & \text{if} \quad E < E_F \\ 0 & \text{if} \quad E > E_F \end{cases}$$

If $T \neq 0$ K some electrons gain enough energy to level up and therefore we should redefine E_F in the following way: energy in which the probability of its corresponding state being occupied is $1/2$. Therefore the Fermi factor becomes:



[17] The color charge of quarks and gluons is completely unrelated to the everyday meaning of color.

[18] In particular, strong interaction is the responsible of maintaining the atomic nucleus unified: since protons have charge $+e$, they experience an electric force that tends to push them apart, but at short range ($\sim 10^{-15}$ m) the attractive nuclear force is strong enough to overcome the electromagnetic force.

[19] We know that $\rho \propto v_{\text{av}} \propto \sqrt{T}$ but empirically it is observed that $\rho \propto T$. The classical model is, therefore, inconsistent.

Proposition 1.81 (Band Theory of Solids). When many atoms are brought together to form a solid, the individual energy levels are split into bands of allowed energies. The splitting depends on the type of bonding and the lattice separation. The highest energy band that contains electrons is called the *valence band (VB)*. The lowest energy band that is not filled with electrons is called the *conduction band (CB)*.

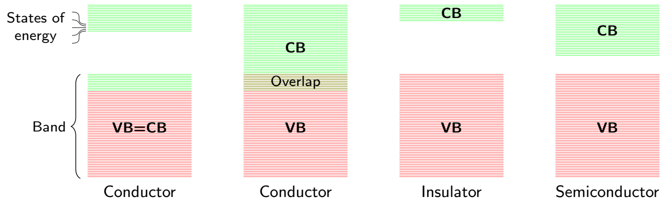
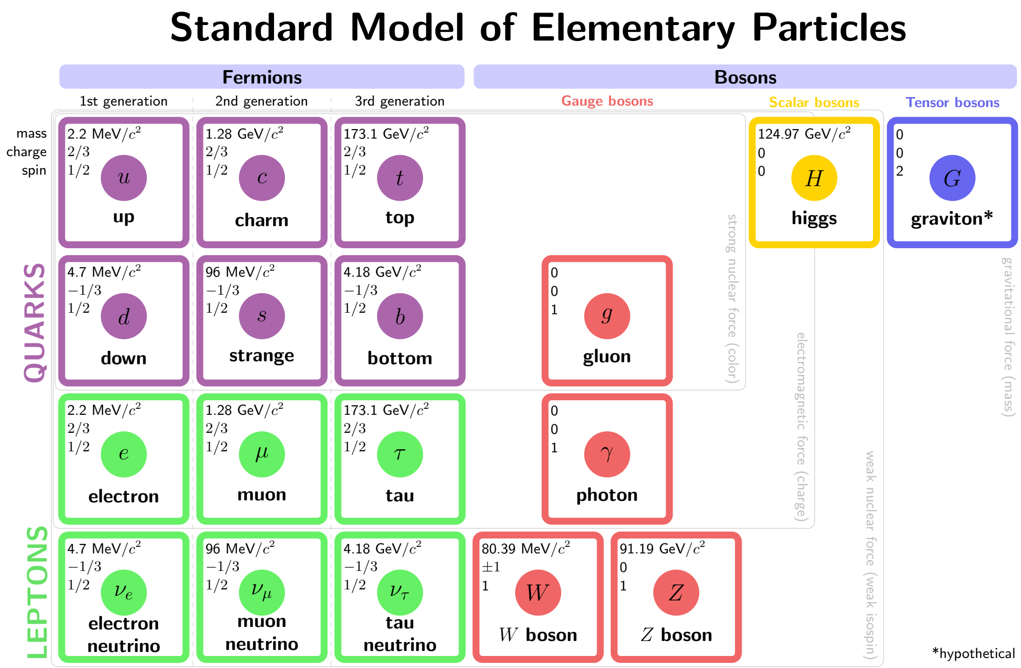


Figure 2.2.4: Band of levels on a conductor, insulator and semiconductor. In red there are the levels occupied by electrons and in green the levels empty.

- In a conductor, the valence band is only partially filled, so there are many available empty energy states for excited electrons which can move freely through these states.
- In an insulator, the valence band is completely filled and there is a large energy gap between it and the next allowed band, the conduction band. Therefore, the electrons can barely move.
- In a semi-conductor, the energy gap between the filled valence band and the empty conduction band is small; so, at ordinary temperatures, an appreciable number of electrons are thermally excited into the conduction band.



2.2.1.2 | Heat transfer

Definition 1.82 (Heat). The *heat* is the transport of thermal energy due to the temperature difference. The fundamental modes of heat transfer are: *conduction*, *convection* and *radiation*.

Conduction

Definition 1.83 (Conduction). *Thermal conduction* is the heat transfer produced by the contact of two object at different temperatures in the absence of matter transfer. Microscopically, energy is transferred throughout the material due to collisions of particles and the movement of electrons within the body.

Law 1.84 (Fourier's law). The law of heat conduction states that

$$\boldsymbol{\nabla}\boldsymbol{\Phi}_q = -\lambda \boldsymbol{\nabla} T$$

where $\boldsymbol{\Phi}_q$ is the heat flux density (energy transferred per unit of surface and time) and λ is the material's *thermal conductivity* ($[\lambda] = \mathrm{W} \cdot \mathrm{m}^{-1} \cdot \mathrm{K}^{-1}$).

Proposition 1.85 (Heat equation). For a medium at a temperature $T(\mathbf{r}, t)$ we have:

$$\frac{\partial T}{\partial t} = \frac{\lambda}{\rho c_s} \nabla^2 T =: \alpha \nabla^2 T$$

where ρ is the density of the material; c_s, its specific heat capacity; λ, its thermal conductivity, and α its *thermal diffusivity*.

Law 1.86 (Fick's law). The solute in a solvent at rest will move from a region of high concentration to a region of low concentration across a concentration gradient. Mathematically, if $\mathbf{J}$ is the diffusion flux; D, the diffusion coefficient, and c, the concentration, then:

$$\mathbf{J} = -D \boldsymbol{\nabla} c$$

Proposition 1.87 (Diffusion equation). The diffusion equation is:

$$\frac{\partial c}{\partial t} = D\nabla^2 c$$

Proposition 1.88. Suppose that inside a material there is a source of heat which generates an amount of heat $\dot{q}$ per unit of volume and time. Then:

$$\rho c_s \frac{\partial T}{\partial t} = \lambda \nabla^2 T + \dot{q}$$

where ρ is the density of the material; c_s, its specific heat capacity, and λ, its thermal conductivity. For the case of creating matter instead of energy and measuring the solute c of the solvent we have:

$$\frac{\partial c}{\partial t} = D\nabla^2 c + f(c,t)$$

where D is the diffusion coefficient and $f(c,t)$ is the function that measures the net solute created and destructed per unit of volume and time.

Convection

Definition 1.89 (Convection). *Thermal convection* is the heat transfer from one place to another due to the movement of fluid.

Proposition 1.90 (Newton's law of cooling). A body subjected to a forced convection exchanges heat with its surroundings as:

$$\frac{\mathrm{d}q}{\mathrm{d}t} = hA(T - T_0)$$

where h is the *heat transfer coefficient*; A, the heat transfer surface area; T, the temperature of the body on its surface, and T_0, the temperature of the environment.

Radiation

Definition 1.91 (Radiation). *Thermal radiation* is the emission of electromagnetic waves from all matter that has a temperature greater than absolute zero. Moreover, the power radiated from an object in a vacuum is:

$$P = \varepsilon\sigma T^4$$

where $0 < \varepsilon < 1$ is the emissivity of the object;σ, the Stefan-Boltzmann constant, and T, the temperature of the object.

2.2.1.3 | Thermodynamics

Basic definitions

Definition 1.92 (Thermodynamic system). A *thermodynamic system* is a region of the universe confined by walls. There are three types of systems:

- *Open system*: can exchange energy and matter with its surroundings (made of permeable and diathermic walls).
- *Closed system*: can exchange energy with its surroundings but not matter (made of impermeable and diathermic walls).
- *Isolated system*: can exchange neither energy nor matter with its surroundings (made of impermeable and adiabatic walls).

Definition 1.93. Variables which measure the macroscopic measurable properties of the state of a system are called *state variables* and can be of two types:

1. *Extensive*: are additive and scale the size of the system. Examples of such variables are: mass, volume, energy...
2. *Intensive*: do not depend on the system size or the amount of material in the system. Examples of such variables are: temperature, density, pressure...

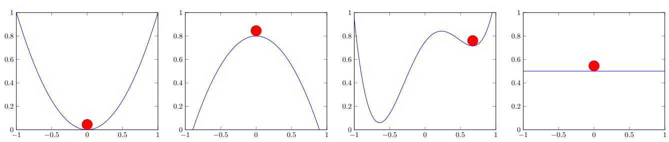
Moreover, *specific variables* are those created from an extensive variable and divided by the volume, number of moles, mass... Examples of such variables are: specific volume, density, specific heat capacity...

Definition 1.94. A system is in

1. *mechanical equilibrium* if the net force acting on the system is zero.
2. *thermal equilibrium* if there is no net flow of thermal energy inside it or between it and its surroundings.
3. *chemical equilibrium* if there are no chemical reactions on the system.
4. *thermodynamical equilibrium* if it is in mechanical, thermal and chemical equilibrium simultaneously.

Definition 1.95. There are different types of equilibrium:

- *Stable*: after a slight disturbance, the system returns to the equilibrium.
- *Unstable*: after a slight disturbance, the system get away from the equilibrium.
- *Metastable*: after a slight disturbance, the system returns to the equilibrium but if the disturbance is strong enough the system may get away from the equilibrium.
- *Neutral*: a slight disturbance does not displace the system from the equilibrium.



Stable Unstable Metastable Neutral

Definition 1.96 (Thermodynamic process). A *thermodynamic process* is the passage between two states of equilibrium. We distinguish the following types of processes:

- *Quasi-static process*: the system passes through states infinitely close to the equilibrium.

- *Reversible process*: the system can be inverted in each infinitesimally step by changing the sign of the external parameters.
- *Irreversible process*: the system cannot be inverted in each infinitesimally step by changing the sign of the external parameters.

- *Non-quasi-static process*: the system passes through non-equilibrium states.

Zeroth law of thermodynamics

Definition 1.97. We say that two systems are in *thermal contact* if they are separated by a diathermic wall.

Law 1.98 (Zeroth law of thermodynamics). If two systems are both in thermal equilibrium with a third system, then they are in thermal equilibrium with each other.

Corollary 1.99. Being in thermal equilibrium is an equivalence relation.

Definition 1.100. The *empirical temperature* is a common state variable between the systems that are in thermal equilibrium.

Proposition 1.101. The conversions between Celsius, Fahrenheit and Kelvin scales are:

$$T(^\circ\mathrm{C}) = \frac{5}{9}\left(T(^\circ\mathrm{F}) - 32\right) \qquad T(^\circ\mathrm{C}) = T(^\circ\mathrm{K}) - 273.15$$

Proposition 1.102. Let $z = z(x, y)$ be a function. Then:

$$\left(\frac{\partial z}{\partial y}\right)_x = \frac{1}{\left(\frac{\partial y}{\partial z}\right)_x} \qquad \left(\frac{\partial z}{\partial x}\right)_y = -\left(\frac{\partial z}{\partial y}\right)_x \left(\frac{\partial y}{\partial x}\right)_z$$

Definition 1.103 (Thermal expansion). The *volumetric (not linear) coefficient of thermal expansion* is given by

$$\alpha := \alpha_{\mathrm{V}} = \frac{1}{V}\left(\frac{\partial V}{\partial T}\right)_p$$

where the subscript p indicates that the pressure is held constant during the process.

Definition 1.104 (Compressibility). *Isothermal compressibility* is defined as

$$\kappa_T = -\frac{1}{V}\left(\frac{\partial V}{\partial p}\right)_T$$

where the subscript T indicates that the temperature is held constant during the process.

Definition 1.105 (Thermal pressure). The *thermal pressure coefficient* is defined as:

$$\beta = \left(\frac{\partial P}{\partial T}\right)_V = \frac{\alpha}{\kappa_T}$$

where the subscript V indicates that the volume is held constant during the process.

Work

Definition 1.106. The work done by a hydrostatic system is:

$$\mathrm{d}W = -p\mathrm{d}V \implies W = -\int_{V_{\mathrm{i}}}^{V_{\mathrm{f}}} p\mathrm{d}V$$

where V_{i} and V_{f} are the initial and final volumes of the system, respectively.

Lemma 1.107 (Sign convention of work). Given a system we have:

- $W > 0$, if the surroundings of the system do work on the system.
- $W < 0$, if the system do work on its surroundings.

Proposition 1.108. Depending on the type of process, we get different values for the total work done on the process:

- Isochoric process ($V = \text{const.}$):
$$\mathrm{d}V = 0 \implies W = 0$$
- Isobaric process ($p = \text{const.}$):
$$W = -p\Delta V$$
where p is the pressure of the system and ΔV is the difference of volume between the initial and final states.
- Isothermal process ($T = \text{const.}$):
$$W = -nRT\ln\left(\frac{V_{\mathrm{f}}}{V_{\mathrm{i}}}\right)$$
where n is the number of moles of present gas, R is the ideal gas constant, T is the temperature of the system and V_{i} and V_{f} are the initial and final volumes of the system, respectively.

First law of thermodynamics

Law 1.109 (First law of thermodynamics in isolated systems). In an isolated system, the work done by a process between two arbitrary states is independent of that process and depends only on the initial and final states.

Corollary 1.110. We define the *internal energy U_B of the state B* as:

$$U_B = U_A + W_{A\to B}^{\mathrm{ad}} \implies \Delta U = W_{A\to B}^{\mathrm{ad}}$$

where U_A is the internal energy of the state A, and $W_{A\to B}^{\mathrm{ad}}$ is the work done to go form A to B through an adiabatic process.

Law 1.111 (First law of thermodynamics in closed systems). In a closed system, the work done to go from an initial state to a final state does depend on the process followed and not only on the initial and final states.

Corollary 1.112. In a closed system, we define the *heat supplied to the system* Q in a process between two states A and B as:

$$Q_{A\to B} = \Delta U - W_{A\to B}$$

Or in differential form:

$$\delta Q = \mathrm{d}U - \delta W$$

where δ is not exactly the differential of a function.

Lemma 1.113 (Sign convention of heat). Given a system we have:

- $Q > 0$, if the heat is added to the system.
- $Q < 0$, if the heat is rejected from the system.

Definition 1.114. Relating the heat capacity of a substance we have:

$$C_X = \frac{\mathrm{d}Q_X}{\mathrm{d}T}$$

where the subscript X indicates that the variable X is held constant during the expansion.

Definition 1.115. *Latent heat* is the amount of heat required to completely change the phase of a kilogram of a substance.

Definition 1.116 (Enthalpy). We define the *enthalpy* H of a system as:

$$H = U + pV$$

where U is the internal energy, p is the pressure and V is the volume.

Proposition 1.117. Relating the heat capacities C_V and C_p holding constant the volume and the pressure, respectively, we have:

$$C_V = \left(\frac{\partial U}{\partial T}\right)_V \qquad C_p = \left(\frac{\partial H}{\partial T}\right)_p$$

And in general:

$$C_p = C_V + \left[\left(\frac{\partial U}{\partial V}\right)_T + p\right]\left(\frac{\mathrm{d}V}{\mathrm{d}T}\right)_p$$

Proposition 1.118 (Reversible adiabatic equation for an ideal gas). The equation for an ideal gas undergoing a reversible adiabatic process is:

$$\mathrm{d}U + p\mathrm{d}V = 0 \implies nc_V\mathrm{d}T + \frac{nRT}{V}\mathrm{d}V = 0 \implies$$
$$\implies \begin{cases} pV^\gamma = \text{const.} \\ V^{\gamma-1}T = \text{const.} \\ p^{1-\gamma}T^\gamma = \text{const.} \end{cases}$$

Second law of thermodynamics

Law 1.119 (Second law of thermodynamics). No system can absorb heat from a single reservoir and convert it entirely into work without additional net changes in the system or its surroundings.

Definition 1.120. A *heat engine* is a cyclic device whose purpose is to convert as much heat into work as possible. Heat engines contain a working substance (water in a steam engine) that absorbs a quantity of heat Q_h (hot) from a high temperature reservoir, does work W on its surroundings, and releases heat Q_c (cool) as it returns to its initial state. Its efficiency η is given by:

$$\eta = \frac{W}{Q_\mathrm{h}} = 1 - \frac{Q_\mathrm{c}}{Q_\mathrm{h}}$$

Definition 1.121. A *refrigerator engine* absorbs heat Q_c (cold) from the interior of a refrigerator and releases heat Q_h (hot) to the surroundings. This process requires work W to be done on the refrigerator. Its efficiency η is given by:

$$\eta = \frac{Q_\mathrm{c}}{W}$$

Definition 1.122. A *heat pump* is a refrigerator with a different objective. It absorbs heat Q_c from the outside (cold reservoir) and releases heat Q_h into the object or region of interest. This process requires work W to be done on the heat pump. Its efficiency η is given by:

$$\eta = \frac{Q_\mathrm{h}}{W}$$

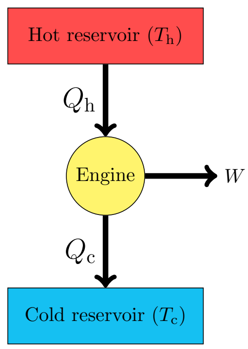


Figure 2.2.5: Heat engine

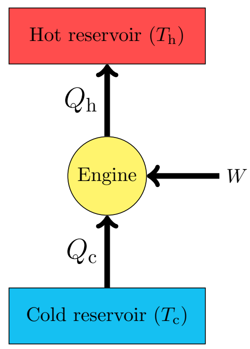


Figure 2.2.6: Heat pump

Definition 1.123 (Carnot cylce). *Carnot cycle* is a reversible thermodynamic process that consists of the following steps:

1. Isothermal expansion
2. Adiabatic expansion
3. Isothermal compression
4. Adiabatic compression

The efficiency η_C of Carnot cycle is:

$$\eta_\mathrm{C} = 1 - \frac{T_\mathrm{c}}{T_\mathrm{h}}$$

where T_h and T_c are the temperatures at the isothermal processes (see figure 2.2.7). Moreover it is satisfied that:

$$\frac{Q_\mathrm{c}}{Q_\mathrm{h}} = \frac{T_\mathrm{c}}{T_\mathrm{h}}$$

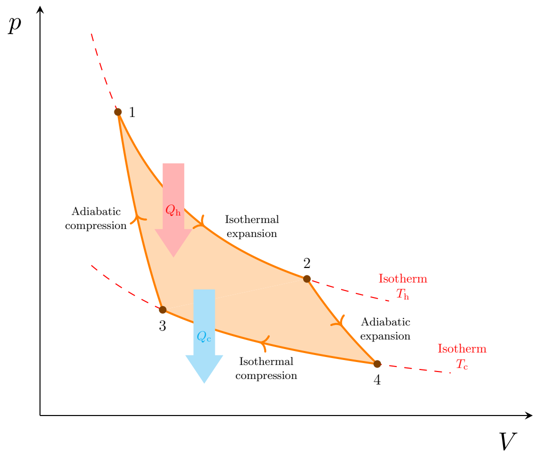


Figure 2.2.7: Carnot cycle

Theorem 1.124 (Carnot's theorem). All heat engines between two heat reservoirs are less or equally efficient than a Carnot heat engine operating between the same reservoirs.

Corollary 1.125. All reversible machines working between two heat reservoirs has the same efficiency.

Proposition 1.126. Consider a machine that realizes a Carnot cycle. Let T_1 and T_2 be the temperatures of the two reservoirs and $T_{1,\mathrm{w}}$ and $T_{2,\mathrm{w}}$ the temperatures of the machine when it is in touch with reservoirs of temperatures T_1 and T_2, respectively. Then, the power of this cycle[20] is:

$$P = \lambda \frac{(T_1 - T_{1,\mathrm{w}})(T_{2,\mathrm{w}} - T_2)(T_{1,\mathrm{w}} - T_{2,\mathrm{w}})}{T_1(T_1 - T_{1,\mathrm{w}}) + T_2(T_{2,\mathrm{w}} - T_2)}$$

where λ is the material's conductivity. The efficiency when the power is maximum is:

$$\eta = 1 - \sqrt{\frac{T_2}{T_1}} < \eta_{\mathrm{C}}$$

Entropy

Theorem 1.127 (Clausius theorem). For a thermodynamic system exchanging heat with external reservoirs and undergoing a thermodynamic cycle we have:

$$\oint \frac{\delta Q}{T} \leq 0$$

where δQ is the heat exchange with a reservoir at a temperature T. Moreover if the cycle is reversible, we have:

$$\oint \frac{\delta Q_{\mathrm{rev}}}{T} = 0$$

Definition 1.128 (Entropy). There exists a new state function, called *entropy* S, such that:

$$S(B) - S(A) = \int_A^B \frac{\delta Q_{\mathrm{rev}}}{T} \quad \text{or} \quad \mathrm{d}S = \frac{\delta Q_{\mathrm{rev}}}{T}$$

Law 1.129 (Second law of thermodynamics in terms of entropy). In an isolated system, the entropy cannot decrease: $\Delta S \geq 0$. Moreover:

$$\Delta S_{\mathrm{universe}} = \Delta S_{\mathrm{system}} + \Delta S_{\mathrm{surroundings}} \geq 0$$

Proposition 1.130. Entropy in different processes:

- Cyclic process:
$$\Delta S = 0$$
- Reversible adiabatic process:
$$\Delta S = 0$$
- Reversible isothermal process at temperature T:
$$\Delta S = \frac{Q}{T}$$
where Q is the heat exchanged on the process.
- Thermal contact between two reservoirs at temperatures T_1 and T_2:
$$\Delta S = Q\left(\frac{1}{T_2} - \frac{1}{T_1}\right)$$
where Q is the heat exchanged on the process.
- Change on temperature at constant volume:
$$\Delta S = C_V \ln \frac{T_2}{T_1}$$
where T_1 is the initial temperature and T_2 the final temperature.
- Change on temperature at constant pressure:
$$\Delta S = C_p \ln \frac{T_2}{T_1}$$
where T_1 is the initial temperature and T_2 the final temperature.
- Free adiabatic expansion of an ideal gas:
$$\Delta S = nRT \ln \frac{V_2}{V_1}$$
where V_1 is the initial volume and V_2 the final volume.
- Arbitrary process of an ideal gas:
$$\Delta S = nRT \ln \frac{V_2}{V_1} + nc_p \ln \frac{T_2}{T_1}$$

Definition 1.131. We define the *Helmholtz free energy* F as:

$$F = U - TS$$

At equilibrium, Helmholtz free energy is minimized.

Definition 1.132. We define the *Gibbs free energy* G as:

$$G = H - TS$$

[20] In a reversible cycle the efficiency is maximum but because of it is extremely slow the power is null.

Proposition 1.133. 2nd law of thermodynamics applied to non-isolated systems:

$$\Delta G = \Delta U + p\Delta V - T\Delta S \leq 0$$

Proposition 1.134. For a non-isolated system, we have different criteria to know whether or not a the system is spontaneous.

- If $T, p = \text{const.}$, then $\Delta G \leq 0$.
- If $T, V = \text{const.}$, then $\Delta F \leq 0$.
- If $S, p = \text{const.}$, then $\Delta H \leq 0$.
- If $S, V = \text{const.}$, then $\Delta U \leq 0$.
- If $U, V = \text{const.}$, then $\Delta S \geq 0$.

Proposition 1.135. The maximum amount of work that the system can perform in a thermodynamic process in which temperature is held constant is $|\Delta F|$.

Proposition 1.136 (Gibbs equation). For a closed system we have:

$$\mathrm{d}U = T\mathrm{d}S - p\mathrm{d}V$$

For an open system we have:

$$\mathrm{d}U = T\mathrm{d}S - p\mathrm{d}V + \mu\mathrm{d}N$$

where μ is the chemical potential and N is the number of particles in the system.