uc3m | Universidad Carlos III de Madrid

ESCUELA POLITÉCNICA SUPERIOR
UNIVERSIDAD CARLOS III DE MADRID

Discrete Mathematics Lecture Notes

Grado en Ingeniería en Informática

Doble Grado en Ingeniería en Informática y Administración de Empresas

Academic Year 2021–2022

Departamento de Matemáticas
Universidad Carlos III de Madrid
Avda. de la Universidad, 30
28911 Leganés

v1: January 2022

Important warning

These notes are meant to be a mere **rough draft** to help the students to follow the Discrete Mathematics course. By any means, they are not intended to be a substitute of the basic bibliography. Students are expected to read (at least some of) these books in order to learn and fully understand the contents of the course. This bibliography can be found in the *Guía de la asignatura* (in Spanish) or in the corresponding *Reina* file (in English); both sources have links in the main *Aula Global* web page.

Discrete Mathematics

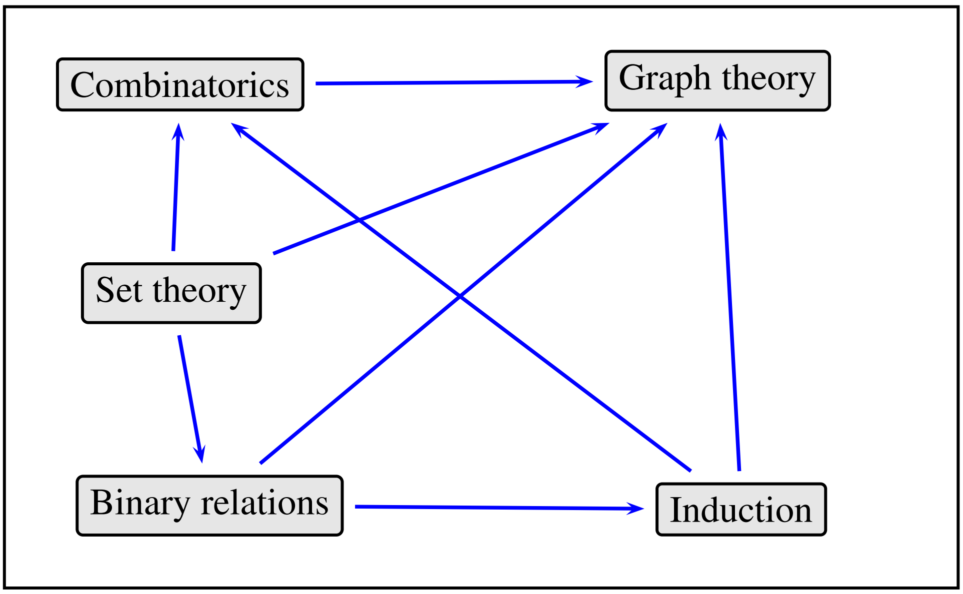
Academic Year 2021–2022

Grado en Ingeniería en Informática

Doble Grado en Ingeniería en Informática y Administración de Empresas

Universidad Carlos III de Madrid

Discrete mathematics course map



Chapter 1: Set theory and functions

1. Elementary set theory:
   - Definitions and operations.
   - Natural numbers.
2. Functions:
   - Definitions and operations.
   - Function types.
3. Integers and division:
   - The division algorithm.
   - Greatest common divisor and least common multiple.
   - Prime numbers. The fundamental theorem of Arithmetic.

Set theory

Definition 1
A **set** X *is a well-defined collection of objects, each of which is called an* **element** *of the set:*

$$X = \{x_1, x_2, x_3, \ldots\} .$$

Given a set X and a certain object x one (and only one) of the following statements is true:

- *the object x belongs to the set X: $x \in X$, or*
- *the object x does not belong to X: $x \notin X$.*

The order of the elements in a set is irrelevant, as well as the number of occurrences of an element in the list.

Definition 2
Two sets are **equal** *if and only if they have the same elements.*

Definition 3
The **empty set** $\emptyset$ *is the set with no elements: $\emptyset = \{\ \}$. The* **universal set** S *is the set containing all objects under consideration.*

How to describe a set?

- By using a roster (when it is possible to list all the elements of the set):

$$X = \{1, 2, 3, 4, 5, 6\}.$$

- By using a defining predicate:

$$Y = \{y\colon P(y)\},$$

  where $P(y)$ is a predicate containing the free variable y. Then Y is the set of all objects y such that $P(y)$ is true.
- By using set operations to build a new set from already existing sets:

$$Z = \{1, 2\} \cup \{x\colon x \in [4, 5]\}.$$

- By using a recursive description of the set C in terms of another set D and some operations on the elements of D:

$$C = \{n^3\colon n \in \mathbb{N}\} = \{m \in \mathbb{N}\colon \exists k \in \mathbb{N} \text{ such that } m = k^3\}.$$

- Venn diagrams are very useful to represent sets.

Subsets

Definition 4
*The set A is s **subset** of the set B ($A \subseteq B$) if and only if every element of A is also an element of B. The set A is a **proper subset** of B ($A \subset B$) if A is a subset of B, and B contains at least an element not in A.*

- Every set A satisfies $A \subseteq A \subseteq S$.
- The empty set $\emptyset$ is a subset of every set A: $\emptyset \subseteq A$.

Definition 5
*The **power set** of the set A, denoted as $\mathcal{P}(A)$, is the set of all subsets of A:*

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

Set operation

Given two sets A and B we can define the following operations:

- Union: $A \cup B = \{x\colon (x \in B) \vee (x \in A)\}$.
- Intersection: $A \cap B = \{x\colon (x \in B) \wedge (x \in A)\}$.
- Complement: $\overline{A} = \{x\colon x \notin A\}$, and it satisfies that $\overline{(\overline{A})} = A$.
- Difference: $A \setminus B = \{x\colon (x \in A) \wedge (x \notin B)\}$.
- Symmetric difference: $A \triangle B = \{x\colon (x \in A \cup B) \wedge (x \notin A \cap B)\}$.

Some properties:

- Distributive laws
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- De Morgan's laws
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Cartesian product

Definition 6
Given two sets X and Y, the Cartesian product $X \times Y$ is the set of all ordered pairs of the form:

$$X \times Y = \{(x, y)\colon (x \in X) \wedge (y \in Y)\}.$$

Remark: $\{\ \}$ is not the same as $(\ )$. In particular, $\{1, 2\}$ is a set and therefore, $\{1, 2\} = \{2, 1\}$. However, $(1, 2)$ is an ordered pair and therefore, $(1, 2) \neq (2, 1)$.

Definition 7
Two sets A and B are disjoint if $A \cap B = \emptyset$.

Natural numbers

Definition 8
The set of natural numbers $\mathbb{N}$ is defined by the following conditions:

(1) $1 \in \mathbb{N}$.

(2) If $n \in \mathbb{N}$, then the successor of n (i.e., the number $n+1$) belongs to $\mathbb{N}$.

(3) Every $n \in \mathbb{N}$ except 1 is the successor of some number in $\mathbb{N}$.

(4) Every non-empty subset of $\mathbb{N}$ has a minimum element (Well-ordering property).

- Note that $0 \notin \mathbb{N}$.
- The non-negative integers are defined as $\mathbb{Z}_+ = \{0\} \cup \mathbb{N}$.
- We can informally "define" the following sets of numbers:
  - Integer numbers: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.
  - Rational numbers: $\mathbb{Q} = \left\{ \frac{p}{q} \colon p, q \in \mathbb{Z}\,, q \neq 0 \right\}$. Actually, each rational number $\frac{p}{q}$ can be represented in infinitely many ways: $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$.

Functions

Definition 9 (Spivak)
*A **function** $f \subset X \times Y$ from a set X onto a set Y is a subset of the Cartesian product $X \times Y$ such that for every $x \in X$, f contains exactly one pair of the form (x, y). The set X is called the **domain** of f and it is denoted as Dom(f). The set Y is called the **codomain** of f. The **image** of f is the set*

$$\mathrm{Im}(f) = \{y \colon \exists\, x \in X \text{ such that } (x, y) \in f\}\,.$$

- Given two sets X and Y, a function is an object that assigns to each element $x \in X$ a unique element $y \in Y$, which is denoted as $y = f(x)$. Usually, functions are denoted as $f \colon X \to Y$.
- When the sets X and Y are known, the notation for a function f is usually relaxed to $x \to f(x)$ or $y = f(x)$.

Function types

Definition 10
Given a function $f\colon X \to Y$, we say that

- f *is* ***injective*** *if $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$.*
- f *is* ***surjective*** *if for every $y \in Y$, there exists at least an element $x \in X$ such that $y = f(x)$.*
- f *is* ***bijective*** *if it is injective and surjective.*

If $f : X \to Y$ is bijective, we can define its **inverse function** $f^{-1}\colon Y \to X$ by the following well-defined rule:

$$f^{-1}(y) = x \quad \Leftrightarrow \quad y = f(x)\,.$$

Given two functions $f\colon X \to Y$, $g\colon Y \to Z$, we can define a new function $g \circ f\colon X \to Z$ by the following rule:

$$\big(g \circ f\big)(x) = g(f(x))\,.$$

The function $g \circ f$ is the **composition** of f and g.

Integer divisibility

The set of integers $\mathbb{Z}$ is *closed* with respect to the operations of sum, subtraction, and product. In other words, for every $a, b \in \mathbb{Z}$, $a \pm b \in \mathbb{Z}$ and $a \cdot b \in \mathbb{Z}$. They also satisfy:

- 0 is the identity with respect to the sum: $a + 0 = a$ for every $a \in \mathbb{Z}$.
- 1 is the identity with respect to the product: $a \cdot 1 = a$ for every $a \in \mathbb{Z}$.
- For every $a \in \mathbb{Z}$, there exists a unique inverse element $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.

However, the result of dividing two integers might not be an integer.

Definition 11
Given two integers $a \neq 0$ and b, we say that ***a divides b*** *if there is an integer $q \in \mathbb{Z}$ such that $b = a \cdot q$. If a divides b, we say that a is a* **factor** *of b and that b is a* **multiple** *of a. We denote* $\boldsymbol{a \mid b}$ *when a divides b, and we write* $\boldsymbol{a \nmid b}$ *when a does not divide b.*

Remarks:

- Every non-zero integer $a \in \mathbb{Z} \setminus \{0\}$ divides 0: $\quad 0 = a \cdot 0 \quad (q = 0)$.
- 1 divides any $a \in \mathbb{Z}$: $\quad a = 1 \cdot a \quad (q = a)$.
- Any nonzero integer $a \in \mathbb{Z} \setminus \{0\}$ divides itself: $\quad a = a \cdot 1$ $(q = 1)$.

The division algorithm

Theorem 12 (The division algorithm) *Let a and $b \neq 0$ be two integers. Then there exists a **unique** pair of integers q and r such that*

$$a = q \cdot b + r \quad \text{with} \quad 0 \leq r < |b|\,.$$

- The numbers a and b are called **dividend** and **divisor**, respectively.
- The number r is the **remainder**: $r = a \bmod b$.
- The number q is the **quotient**:

$$q = a \operatorname{div} b = \begin{cases} \lfloor a/b \rfloor & \text{if } b > 0, \\ \lceil a/b \rceil & \text{if } b < 0, \end{cases}$$

where

- The function **floor** assigns to each real number x the **largest** integer $\lfloor x \rfloor \leq x$.
- The function **ceiling** assigns to each real number x the **smallest** integer $\lceil x \rceil \geq x$.

Greatest common divisor

Definition 13
*Let a, b be integers, not both simultaneously zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** of a and b. It is denoted by $\gcd(a, b)$.*

Remark: The case $a = b = 0$ is excluded because any integer divides 0.

Theorem 14 *The greatest common divisor of two numbers is unique.*

Definition 15
*The **least common multiple** of two natural numbers a, b is the least natural number m such that $a \mid m$ and $b \mid m$. It is denoted by $\operatorname{lcm}(a, b)$.*

Theorem 16 *If a, b are two natural numbers, then*

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

Definition 17
*Two integers a and b are **relatively prime** if $\gcd(a, b) = 1$. The integers $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ for any $1 \leq i < j \leq n$.*

The fundamental theorem of Arithmetic

Definition 18
A natural number $p > 1$ is called a **prime number** *if the only positive factors of p are 1 and p. A natural number $p > 1$ that is not prime is called* **composite***.*

Remark: The natural number 1 is **not** prime. The first prime number is 2, and the other prime numbers are odd natural numbers $(3, 5, 7, 11, \ldots)$.

Theorem 19 (Euclid) *There are infinite prime numbers.*

Prime numbers are very important as they constitute the building "blocks" for the set of natural numbers.

Theorem 20 (The fundamental theorem of Arithmetic) *Every natural number $n > 1$ can be written uniquely as a product of* **primes**

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \ldots \cdot p_k^{n_k} ,$$

where the p_i are distinct prime numbers written in increasing order, and the exponents n_i are natural numbers $n_i \geq 1$.

Chapter 2: Elementary combinatorics I

Definition 21
Let S be a set. If there are exactly $n \in \mathbb{N}$ distinct elements in S, we say that S is a finite set, and that n is the cardinality of S. The cardinality of S is denoted by $|S|$.

Definition 22
Two sets A and B have the same cardinality if and only if there exists a bijective function $f\colon A \to B$.

Definition 23
A set that is either finite or has the same cardinality as the set $\mathbb{N}$ is called countable.

The goal of combinatorics is to compute the cardinal of certain finite sets.

Elementary combinatorics I

1. The sum rule: if $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$.
2. The product rule: $|A \times B| = |A| \cdot |B|$.
   - Permutations.
   - Ordered subsets.
   - Subsets.
3. The inclusion-exclusion principle: $|A \cup B| = |A| + |B| - |A \cap B|$.
4. The pigeonhole principle. (see Problem set).

The sum principle

Proposition 24 (The sum principle v1) *If A and B are two finite and disjoint sets $A \cap B = \emptyset$, then*

$$|A \cup B| \;=\; |A| + |B|\,.$$

Proposition 25 (The sum principle v2) *If $A_1, A_2, \ldots, A_m$ are a sequence of finite and pairwise disjoint sets $A_i \cap A_j = \emptyset$ for all $i \neq j$, then*

$$|A_1 \cup A_2 \cup \cdots \cup A_m| \;=\; |A_1| + |A_2| + \cdots + |A_m| \;=\; \sum_{j=1}^{m} |A_j|\,.$$

Proposition 26 (The sum principle v3) *If a first task can be done in n_1 ways, and a second task in n_2 ways, and if these tasks cannot be done at the same time, then there are $n_1 + n_2$ ways to do either task.*

The product principle

Proposition 27 (The product principle v1) *If A and B are two finite sets, then*

$$|A \times B| \;=\; |A| \cdot |B| \,.$$

Proposition 28 (The product principle v2) *If $A_1, A_2, \ldots, A_m$ are finite sets, then*

$$|A_1 \times A_2 \times \ldots \times A_m| \;=\; |A_1| \cdot |A_2| \cdots |A_m| \;=\; \prod_{k=1}^{m} |A_k| \,.$$

Proposition 29 (The product principle v3) *Suppose that a procedure can be broken down into two tasks. If there are n_1 ways to perform the first task, and n_2 ways to perform the second task after the first task has been done, then there are $n_1 \cdot n_2$ ways to do the procedure.*

Permutations

Definition 30
For each positive integer $n \in \mathbb{N}$, we define the **factorial of n** *as*

$$n! \;=\; n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 \,.$$

Proposition 31 (Permutations of n distinct objects) *Given n distinct objects, there are $n!$ distinct ordered arrangements (= permutations) of these objects.*

Proposition 32 (Permutations with repetition) *Given n objects that can classified into k groups of identical objects, and such that the first group contains n_1 identical elements, the second group contains n_2 identical elements, etc, then the number of distinct ordered arrangements of these objects is*

$$\binom{n}{n_1, n_2, \ldots, n_k} \;\equiv\; \frac{n!}{n_1! n_2! \cdots n_k!} \,, \qquad \text{with} \quad \sum_{i=1}^{k} n_i \;=\; n \,.$$

Ordered subsets

Proposition 33 (r-permutations of a set of n elements) *Given a set of n distinct elements we can form*

$$n(n-1)(n-2)\dots(n-r+1) \;=\; \frac{n!}{(n-r)!}$$

ordered subsets containing r elements.

Remark: If $r = n$, the first formula implies that there are $n!$ n-permutations of a set of n elements (= permutations of a set of n elements). The second formula only makes sense if we define $0! = 1$.

Proposition 34 *The number of r-permutations of a set of n distinct objects with repetition allowed is n^r.*

Subsets

Proposition 35 *The number of distinct subsets with r elements that can be extracted from a set of n distinct elements is given by: es*

$$\binom{n}{r} \;=\; \frac{n!}{r!\,(n-r)!}\,.$$

The symbol $\binom{n}{r}$ is read "n choose k".

Definition 36 (Binomial coefficients)
For all non-negative integers $n, r \in \mathbb{Z}_+$ such that $0 \le r \le n$ we define the binomial coefficient $\binom{n}{r}$ as follows:

$$\binom{n}{r} \;=\; \frac{n!}{r!\,(n-r)!}\,,$$

where we define $0! = 1$.

Binomial coefficients: Pascal's triangle

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

$$\binom{n}{r} \equiv \binom{\text{row}}{\text{column}}$$

$$
\begin{tikzcd}
a \arrow[dr] & & b \arrow[dl] \\
 & a+b &
\end{tikzcd}
$$

Theorem 37 (Symmetry)

$$\binom{n}{r} = \binom{n}{n-r} = \frac{n!}{r!\,(n-r)!}\,, \quad n \geq 0\,, \quad 0 \leq r \leq n\,.$$

Theorem 38 (Pascal's identity)

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}\,, \quad n \geq 0\,, \quad 0 < r \leq n\,.$$

Newton's binomial theorem

Theorem 39 (Newton's binomial theorem)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k\, y^{n-k}\,, \quad n \geq 0\,.$$

Corollary 40

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k\,, \quad n \geq 0\,.$$

Corollary 41 *For every* $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n\,,$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0\,.$$

Binomial coefficients

Corollary 42 *Given a finite set A, then*

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

Theorem 43 (Vandermonde's identity) *Given any $n, m \geq 0$ and $0 \leq k \leq m+n$, the following equation holds:*

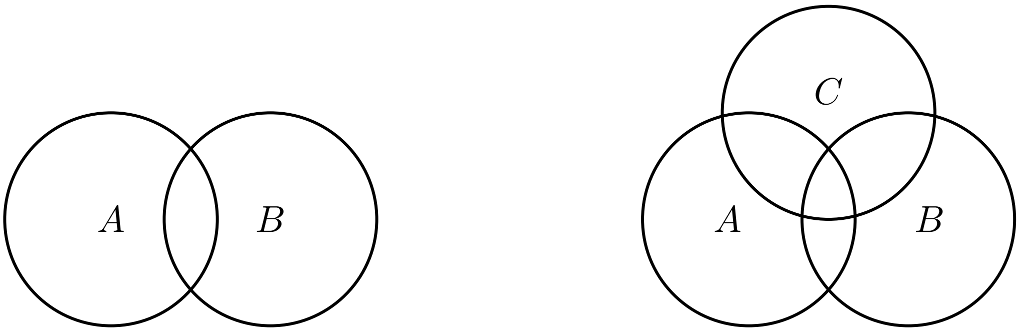
$$\binom{m+n}{k} = \sum_{q=0}^{k} \binom{m}{k-q}\binom{n}{q}.$$

Remark: $\binom{n}{k} = 0$ whenever $k < 0$ or $k > n$.

The inclusion-exclusion principle

Proposition 44 (The inclusion-exclusion principle v1)

$$|A \cup B| = |A| + |B| - |A \cap B|.$$



Proposition 45 (The inclusion-exclusion principle v2)

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

The inclusion-exclusion principle (2)

Proposition 46 (The inclusion-exclusion principle v3)

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots \cup A_n| &= \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| \\ &+ \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \cdots \\ &+ (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|\,.\end{aligned}$$

Proposition 47 (The inclusion-exclusion principle v4) *Given sets $A_i \subset S$ with $1 \le i \le n$, then*

$$\begin{aligned}|\overline{A_1 \cup A_2 \cup \cdots \cup A_n}| &= |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| \\ &= |S| - |A_1 \cup A_2 \cup \cdots \cup A_n|\,.\end{aligned}$$

Remarks:

- $\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n} = \{x \colon x \notin A_1\,, x \notin A_2\,, \ldots\,, x \notin A_n\}$.
- $\overline{A} = S \setminus A \;\Rightarrow\; |\overline{A}| = |S| - |A|$.

Chapter 3: Graph theory I

1. Undirected graphs:
   - Basic notation and definitions.
   - Graph representation.
   - Graph isomorphism.
   - Walks in a graph.
   - Trees.
   - Planar graphs.
2. Algorithms in graph theory.
3. Combinatorial problems on graphs.

Undirected graphs

Definition 48
A **pseudograph** $G = (V, E, \gamma)$ *consists of a nonempty vertex set* V*, an edge set* E*, and a function* $\gamma\colon E \to \{\{u, v\}\colon u, v \in V\}$

- The function γ encodes the graph connectivities.
- If $e \in E$ satisfies $\gamma(e) = \{u, v\}$ with $u \neq v$, we say that u and v are adjacent, and that e is incident with u and v.
- If there two distinct edges $e_1, e_2 \in E$ such that $\gamma(e_1) = \gamma(e_2) = \{a, b\}$, then we say that e_1 and e_2 are multiple edges.
- If there exists $e \in E$ such that $\gamma(e) = \{v, v\} = \{v\}$, then e is a loop incident with v.
- Hereafter, if we do not say it explicitly, we will assume that $G = (V, E)$ is undirected.

Definition 49
A **multigraph** $G = (V, E, \gamma)$ *is a pseudograph in which multiple edges are allowed, but loops are not allowed. A* **simple graph** $G = (V, E, \gamma)$ *is a pseudograph in which loops and multiple edges are not allowed.*

More definitions

Definition 50
The **degree** *(or valence) of a vertex* $v \in V$ *in a graph* $G = (V, E)$ *is the number of edges incident with it, except that a loop contributes twice to the degree of that vertex. The degree of a vertex* v *is denoted by* $d(v)$ *(or by* $\deg(v)$*).*

Remark: Given a vertex $v \in V$, its degree $d(v)$ is equal to

$$d(v) \;=\; |\{\{v, y\} \in E\colon y \neq v\}| + 2 \times \text{Number of loops}\,.$$

Definition 51
A vertex of degree 1 *is called a* **terminal** *(or a pendant vertex). A vertex of degree* 0 *is called an* **isolated** *vertex. A graph with no edges is called* **trivial**.

Definition 52
A **regular** *graph is a graph such that all vertices have the same degree.*

The Handshaking Theorem

Theorem 53 (The Handshaking Theorem) *In any undirected graph $G = (V, E)$, we have that*

$$\sum_{v \in V} d(v) \;=\; 2|E|\,.$$

Corollary 54 *For any graph G, the sum of all vertex degrees is an even number.*

Theorem 55 *Any graph has an even number of vertices of odd degree.*

Corollary 56 *For any graph G with an odd number of vertices, there is an odd number of vertices of even degree.*

More definitions

Definition 57
A graph $G = (V, E)$ is **bipartite** *if its vertex set V can be partitioned into two disjoint nonempty subsets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 with a vertex in V_2.*

Simple graph families:

- The complete graph of n vertices K_n.
- The path P_n of n vertices.
- The cycle C_n of n vertices.
- The wheel graph of $n+1$ vertices W_n.
- The complete bipartite graph with n and m vertices $K_{n,m}$.
- The n-cube graphs Q_n are defined as follows: each vertex represents a bit string of length n, and two vertices u and v are adjacent if and only if the corresponding bit strings differ in exactly one bit.

Complementary graph and subgraphs. Representing graphs.

Definition 58
The **complementary graph** $\overline{G} = (V, \overline{E})$ *of a simple graph* $G = (V, E)$ *has the same vertex set as* G*, and two vertices are adjacent in* $\overline{G}$ *if and only if they are not adjacent in* G*.*

Definition 59
The graph $H = (W, F)$ *is a* **subgraph** *of* $G = (V, E)$ *if* $W \subseteq V$ *and* $F \subseteq E$*.*

Definition 60
Given a graph $G = (V, E)$*, a* **spanning subgraph** *of* G *is any subgraph* $H = (V, F)$ *of* G *(hence,* $F \subseteq E$*).*

Definition 61
Let $G = (V, E)$ *be a graph, and* $v_1, v_2, \ldots, v_{|V|}$ *be a fixed ordering of its vertex set* V*. The* **adjacency matrix** *of* G *associated to that particular vertex ordering is the matrix of dimensions* $|V| \times |V|$ *such that its entry* A_{ij} *counts the number of edges joining the vertices* v_i *and* v_j*.*

Isomorphism of graphs

Remark: Do not confuse a graph with its graphical representation!

Definition 62
The simple graphs $G_1 = (V_1, E_1)$ *and* $G_2 = (V_2, E_2)$ *are* **isomorphic** *if and only if there exist a bijective function* $f : V_1 \to V_2$ *with the following property:* a *and* b *are adjacent in* G *if and only if* $f(a)$ *and* $f(b)$ *are adjacent in* G_2*. The function* f *is called an* **isomorphism***.*

Remark: Given two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, then

1. If $|V_1| \neq |V_2|$, then G_1 and G_2 are **not** isomorphic.
2. If $|E_1| \neq |E_2|$, then G_1 and G_2 are **not** isomorphic.
3. If S_i is the degree sequence of the graph G_i, and $S_1 \neq S_2$, then G_1 and G_2 are **not** isomorphic.
4. Other methods ...

Remark: G_1 and G_2 isomorphic if there exists an invertible linear map (a permutation of the basis vectors) $\pi : V_1 \to V_2$ such that $A_2 = P^{-1} \cdot A_1 \cdot P$. There are $|V_1|! = |V_2|!$ maps of this type!

Walks in a graph

Definition 63
A **walk** *in a graph* $G = (V, E)$ *is an alternating sequence of vertices and edges of the form* $v_0, \{v_0, v_1\}, v_1, \{v_1, v_2\}, v_2, \ldots, v_{\ell-1}, \{v_{\ell-1}, v_\ell\}, v_\ell$. *The* **length** *of the walk is equal to the number of edges in the walk. There is an implicit direction in every walk:* v_0 *is the* **initial vertex**, *and* v_ℓ *is the* **final vertex**.

Definition 64
A **trail** *is a walk in which no edge occurs more than once. A closed trail is called a* **circuit**. *A* **path** *is a trail in which all of its vertices are different, except that the initial and final vertices can be the same. A* **cycle** *is a closed path of positive length.*

Remark. **Circuit** can be also used as a synonym of closed walk, or closed path (cycle).

Number of walks between two vertices

Theorem 65 *Let* G *be a graph with adjacency matrix* A *with respect to the ordering* $\{v_1, v_2, \ldots, v_{|V|}\}$ *of its vertex set. The number of distinct oriented walks of length* $n \geq 1$ *that start at* v_i *and end at* v_j *is given by the entry* (i, j) *of the matrix* A^n.

Corollary 66 *Let* G *be a simple graph with adjacency matrix* A, *then*

- $A^2_{ii} = d(i)$ *for every* $1 \leq i \leq |V|$.
- *tr* $A^2 = 2|E|$.
- *tr* $A^3 = 6 \times$ *Number of unoriented triangles in* G.

Connected graphs

Definition 67
An undirected graph is **connected** *if there is a path between every pair of distinct vertices of G. A disconnected graph is formed by the disjoint union of several connected subgraphs called the* **connected components** *of the graph.*

Remark: If two vertices of a graph can be connected by a walk, then there is at least one path connecting them. These paths correspond to the walks of minimum length connecting these two vertices.

Definition 68
An **articulation point or cut vertex** *of a graph G is a vertex whose removal (together with those edges incident with it) produces a graph with more connected components than in G.*

A **cut edge or bridge** *of a graph G is an edge whose removal produces a graph with more connected components than in G.*

Chapter 4: Graph theory II

1. Undirected graphs:
   - Basic notation and definitions.
   - Graph representation.
   - Graph isomorphism.
   - Walks in a graph.
   - Trees.
   - Planar graphs.
2. Algorithms in graph theory.
3. Combinatorial problems on graphs.

Trees

Definition 69
*A **tree** is a simple connected graph with no cycles. A **forest** is a simple graph with no cycles. Each connected component of a forest is a tree.*

Remark: Trees may be rooted trees. A rooted tree is a tree with one distinguished vertex (the root). Hereafter, we will assume that all trees are rootless, unless specified.

Theorem 70

(a) *The simple graph G is a tree if and only if it is connected and, if we remove any edge, we obtain a disconnected graph.*

(b) *The simple graph G is a tree if and only if it does not contain any cycles and, if we add any edge, we create a cycle.*

Theorem 71 *A graph $G = (V, E)$ is a tree if and only if there exists a unique path between any pair of vertices.*

Theorem 72 *Any tree with at least two vertices contains at least two vertices of degree one.*

Properties of trees

Definition 73
How to grow a tree?:

1. *Start from the trivial tree $G = (\{r\}, \emptyset)$, where r is the root vertex.*
2. *Given $G = (V, E)$, add a new vertex u and a new edge $\{u, v\}$ where $v \in V$.*

Theorem 74 *Any graph obtained by using the preceding procedure is a tree, and any tree can be obtained in this way.*

Theorem 75 *Any tree with n vertices has $n - 1$ edges.*

Theorem 76 *If G is a graph with n vertices, then the following statements are equivalent:*

1. *G is a tree.*
2. *G is connected and has $n - 1$ edges.*
3. *G has $n - 1$ edges and does not contain any cycle.*

Planar graphs

Definition 77
*A **planar** graph is a graph that can be embedded in the plane: i.e., it can be drawn on the plane in such a way that their edges do not cross each other. A **plane** graph is a graphical representation of a planar graph such that their edges do not cross each other.*

Definition 78
*A **subdivision** of an edge results from inserting a new vertex into that edge. The subdivision of a graph G is obtained by subdividing one or more edges in G.*

Theorem 79 (Kuratowsky, 1930) *A graph is planar if and only if it does not contain a subgraph that is a subdivision of K_5 or $K_{3,3}$.*

Planar and dual graphs

Theorem 80 (Euler's formula, 1752) *A plane and connected graph $G = (V, E)$ divides the plane into R regions, such that*

$$|V| - |E| + R = 2\,.$$

A plane graph (not necessarily connected) divides the plane into R regions, such that

$$|V| - |E| + R = 1 + \text{Number of connected components of } G.$$

Definition 81
*Given a plane connected graph $G = (V, E)$, we can define its **dual graph** $G^\star = (V^\star, E^\star)$ in the following way: To each region f of G we associate a dual vertex $f^* \in V^*$, and to each edge $e \in E$, there corresponds a unique dual edge $e^* \in E^*$. If the original edge e is the intersection of two faces f, h (possibly, $f = h$), then the corresponding dual edge e^* is incident with the dual vertices $f^*, g^* \in V^*$.*

- Notice that $(G^*)^* = G$.

Some corollaries about graph planarity

Definition 82
Given a plane graph, the **degree of a region** r *is the degree of the dual vertex* $r \in V^\star$ *associated with it in the dual graph* G^*. *We denote the degree of the region* r *as* d_r.

Theorem 83 *Given a plane connected graph* G, *then*

$$2|E| = \sum_{r \in R} d_r ,$$

where R *is the set of regions defined on the plane by* G.

Corollary 84 *If* G *is a simple, connected, and planar graph with* $|V| \geq 3$, *then* $|E| \leq 3|V| - 6$.

Corollary 85 *If* G *is a simple, connected, and planar graph with* $|V| \geq 3$ *and without cycles of length* 3, *then* $|E| \leq 2|V| - 4$.

Chapter 5: Graph theory III

1. Undirected graphs.
2. Algorithms in graph theory:
   - Minimum-weight spanning tree: Prim's and Kruskal's algorithms.
   - Shortest path: Dijkstra's algorithm.
   - Graph colorings.
   - Eulerian and Hamiltonian graphs. Fleury's algorithm.
3. Combinatorial problems on graphs.

Minimum-weight spanning tree

Definition 86
A **spanning tree** *of a connected graph G is a subgraph of G that is a tree and contains all vertices of G.*

Definition 87
A **weighted graph** *$G = (V, E, \omega)$ is a graph such that every edge $e \in E$ is associated to a weight $\omega(e) \in \mathbb{R}$.*

Definition 88
A **minimum-weight spanning tree** *of a connected weighted graph $G = (V, E, \omega)$ is a spanning tree $T = (V, A)$ of G such that $\omega(A) = \sum_{e \in A} \omega(e)$ takes the minimum possible value.*

Problem 1
Find a minimum-weight spanning tree of a connected weighted graph $G = (V, E, \omega)$.

Remark: The number of trees with n vertices grows very rapidly with n.

Definition 89
A **greedy algorithm** *to solve a given problem is an algorithm such that at every step, it always takes, among all the choices allowed by the problem, the optimum one.*

Prim's algorithm, 1957

Algorithm 90 (Prim's algorithm)
procedure *Prim(G: connected weighted graph with n vertices)*
$T_1 = (V_1, E_1)$ *where* $E_1 = \{e_1\}$, $e_1 = \{x_0, x_1\}$ *is one edge with minimum weight* ω_{min},
    and $V_1 = \{x_0, x_1\}$.
for $i = 1$ **to** $n - 2$
begin
  $e_{i+1} = \{x_i, x_{i+1}\}$ *edge of minimum weight that is incident with a vertex* x_j *of*
    $T_i = (V_i, E_i)$, *and such that it does not form a cycle when added to* T_i
  $T_{i+1} = (V_i \cup \{x_{i+1}\}, E_i \cup \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$
end

Remarks:

- The edge e_i $(i = 1, \ldots, n - 1)$ might not be unique.
- The minimum-weight spanning tree might not be unique.
- At each step, T_i is a tree $(1 \leq i \leq n - 1)$.

Theorem 91 *Given a connected weighted graph $G = (V, E, \omega)$, Prim's algorithm produces a minimum-weight spanning tree of G.*

Kruskal's algorithm, 1957

Algorithm 92 (Kruskal's algorithm)
procedure *Kruskal(G: connected weighted graph with n vertices)*
$T_0 = (V, E_0)$ *with* $E_0 = \emptyset$
for $i = 1$ **to** $n - 1$
begin
$e_i =$ *edge of minimum weight such that it does not form a cycle when added to*
$T_{i-1} = (V, E_{i-1})$
$T_i = (V, E_{i-1} \cup \{e_i\}) = (V, E_i)$
end

Remarks:

- The edge e_i $(i = 1, \ldots, n-1)$ might not be unique.
- At each step, T_i is a forest $(1 \leq i \leq n-1)$.

Theorem 93 *Given a connected weighted graph $G = (V, E, \omega)$, Kruskal's algorithm produces a minimum-weight spanning tree of G.*

Shortest path between two vertices: Dijkstra's algorithm, 1959

Problem 2
Find the shortest path that joins an initial vertex s to a final vertex t belonging to a simple, connected, and weighted graph $G = (V, E, \omega)$ such that all wights are positive ($\omega_e > 0$ for every edge $e \in E$).

Theorem 94 *Dijkstra's algorithm finds the length of the shortest path between two vertices of a simple, connected, and weighted graph $G = (V, E, \omega)$ with all its weights being positive.*

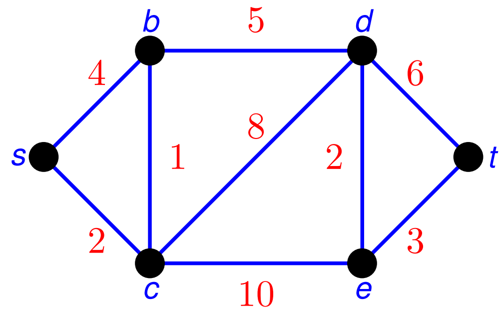
The basic idea:
In each iteration, we assign to each vertex j two labels, that might be either temporary (δ_j, P_j) or permanent $\boxed{(\delta_j, P_j)}$.

- The label δ_j is an estimate of the length of the path going from the initial vertex s to the vertex j.
- The label P_j is an estimate of the predecessor of the vertex j along the above path.

We will denote the weight of the edge $\{i, j\} \in E$ as $\omega_{ij} > 0$.

Dijkstra's algorithm

Problem 3
Compute the shortest path between vertices s and t in the following graph:



Dijkstra's algorithm (2)

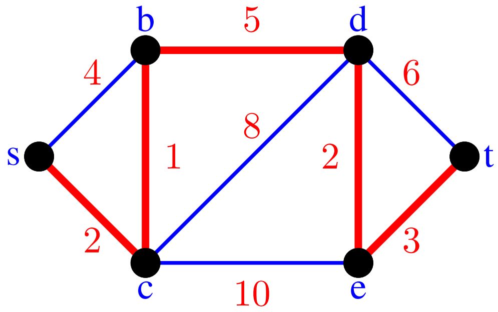
(1) Initial Step: We mark the origin s with the permanent label $\boxed{(0, s)}$.
All the other vertices $j \in V$ ($j \neq s$) are marked with temporary labels:
- If $\{j, s\} \in E$, we assign the label $(\omega_{s,j}, s)$ to j.
- If $\{j, s\} \notin E$, we assign to j the label $(\infty, -)$.

(2) Let $v \in V$ be the last vertex that has become permanent. For each temporary vertex j, we compare the temporary label δ_j to the new value $\delta_v + \omega_{v,j}$:
- If $\delta_v + \omega_{v,j} < \delta_j$, the old label (δ_j, P_j) is replaced by $(\delta_v + \omega_{v,j}, v)$.
- If $\delta_v + \omega_{v,j} \geq \delta_j$, the label remains the same.

(3) Among all temporary vertices j, we choose one $j_0$with the minimum label $\delta_{j_0} = \delta_{\min}$:
- If $\delta_{\min} = \infty$, the algorithm ends: there is no path between s and t.
- If $\delta_{\min} < \infty$, we mark such vertex with the permanent label $\boxed{(\delta_{\min}, P_{j_0})}$.

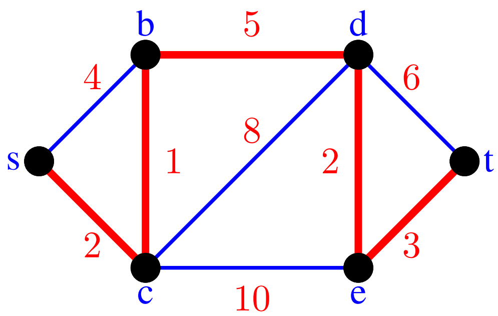
(4) If t is the vertex whose label $\boxed{(\delta_t, P_t)}$ has become permanent, the algorithm ends.
The length of the shortest path between s and t is δ_t and such a path is obtained by following the permanent labels in reverse order $t \to P_t \to \cdots \to s$. If such vertex is not t, go back to Step (2).

Dijkstra's algorithm: An example



Vertex	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
s	$\boxed{(0, s)}$	$\star$	$\star$	$\star$	$\star$	$\star$
b	$(4, s)$	$(3, c)$	$\boxed{(3, c)}$	$\star$	$\star$	$\star$
c	$(2, s)$	$\boxed{(2, s)}$	$\star$	$\star$	$\star$	$\star$
d	∞	$(10, c)$	$(8, b)$	$\boxed{(8, b)}$	$\star$	$\star$
e	∞	$(12, c)$	$(12, c)$	$(10, d)$	$\boxed{(10, d)}$	$\star$
t	∞	∞	∞	$(14, d)$	$(13, e)$	$\boxed{(13, e)}$

Dijkstra's algorithm (2)



Remarks:

- If at a given step there are several options, we can choose any of them.
- The shortest path between two vertices may not be unique; but the shortest length does not depend on such a choice.
- The final output of Dijkstra's algorithm (when all vertices have been marked permanent) is a rooted spanning tree T, such that the root is the initial vertex s, and the distance between s and any other vertex j of the graph is the sum of all the weights of the **unique** path between s and j on T.

Directed graphs or digraphs

Definition 95
A **directed graph** $G = (V, E)$ *consists in a nonempty set of* **vertices** V *and an* **edge** *set* E*, such that each edge* $e \in E$ *is an* ordered *pair of vertices* $e = (x, y)$ *with* $x, y \in V$.

Definition 96
Let G *be a directed graph* $G = (V, E)$*, and let* $v \in V$ *be a vertex of* G*. The* **indegree** $d_i(v)$ *(or* $\deg^-(v)$*) of* v *is the number of edges whose second entry is* v*. The* **outdegree** $d_o(v)$ *(or* $\deg^+(v)$*) of* v *is the number of edges whose first entry is* v.

Proposition 97 *In any directed graph* $G = (V, E)$:

$$\sum_{v \in V} d_i(v) = \sum_{v \in V} d_o(v) = |E| .$$

Definition 98
Let $G = (V, E)$ *be a directed graph, and we consider the ordering* $v_1, v_2, \ldots, v_{|V|}$ *of its vertex set* V*. The* **adjacency matrix** *of* G associated to that ordering *is the* $|V| \times |V|$ *matrix whose entries* A_{ij} *count the number of edges* (v_i, v_j) *that start at* v_i *and end at* v_j.

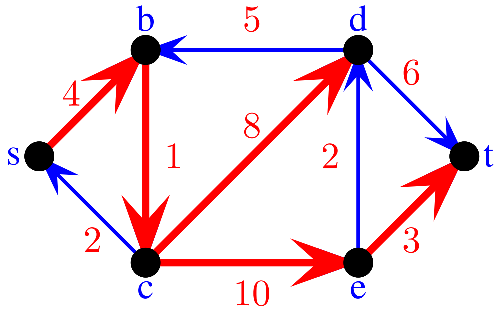
Directed graphs (2)

Definition 99
A **walk** *of length* ℓ *in a directed graph* $G = (V, E)$ *is a sequence of* ℓ *edges of the form* $(v_0, v_1), (v_1, v_2), \ldots, (v_{\ell-1}, v_\ell)$.

The definitions of trail, path, closed walk, circuit, and cycle are the natural generalization of those given for undirected graphs in Chapter 3.

We can also define weighted directed graphs $G = (V, E, \omega)$ in an analogous way.

Dijkstra's algorithm for directed graphs



Vertex	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
s	$\boxed{(0, s)}$	$\star$	$\star$	$\star$	$\star$	$\star$
b	$(4, s)$	$\boxed{(4, s)}$	$\star$	$\star$	$\star$	$\star$
c	∞	$(5, b)$	$\boxed{(5, b)}$	$\star$	$\star$	$\star$
d	∞	∞	$(13, c)$	$\boxed{(13, c)}$	$\star$	$\star$
e	∞	∞	$(15, c)$	$(15, c)$	$\boxed{(15, c)}$	$\star$
t	∞	∞	∞	$(19, d)$	$(18, e)$	$\boxed{(18, e)}$

Chapter 6: Graph theory IV

1. Undirected graphs.
2. Algorithms in graph theory:
   - Minimum-weight spanning tree: Prim's and Kruskal's algorithms.
   - Shortest path: Dijkstra's algorithm.
   - Graph colorings.
   - Eulerian and Hamiltonian graphs. Fleury's algorithm.
3. Combinatorial problems on graphs.

Proper colorings of a graph

Definition 100
A **proper coloring** *(with q colors) of a graph $G = (V, E)$ is a function $c : V \to \{1, 2, \ldots, q\}$ such that $c(u) \neq c(w)$ whenever u and w are adjacent.*

- Given a graph $G = (V, E)$, the total number of vertex colorings (including both proper and improper colorings) with q colors is $q^{|V|}$.
- Hereafter, we will consider **proper colorings**.
- Two difficult questions:
  1. How many distinct colorings with q colors $P_G(q)$ can be obtained from a graph G?
  2. Which is the minimum number of colors q needed to color a given graph G?

Definition 101
The **chromatic number** *$\chi(G)$ of a graph G is the minimum positive integer q such that there is at least one coloring of G with q colors; i.e., $P_G(q) > 0$ for every $q \geq \chi(G) \in \mathbb{N}$.*

Proposition 102 *Given an arbitrary graph G, deciding whether the vertices of G can be colored or not with $k \geq 3$ colors is a hard problem.*

Greedy algorithm for coloring a graph

Algorithm 103 (Greedy algorithm)
procedure *(G: simple and connected graph with n vertices)*
We order the vertices of V: $(v_1, v_2, \ldots, v_n)$
$c(v_1) = 1$
for $i = 2$ **to** n
begin
  $S_i = \{q\colon c(v_k) = q$ *, for every v_k that is adjacent to v_i with $k < i$*$\}$
  $c(v_i) =$ *min*$(\overline{S_i} \cap \mathbb{N}) =$ *the smallest color not in S_i*
end

Remarks:

- This algorithm does not compute $\chi(G)$, but an upper bound of $\chi(G)$ which depends (strongly) on the chosen vertex ordering.
- To compute the value of $\chi(G)$, we should consider the $n!$ possible orderings of the n vertices of G (= exponential time!).

Some theorems

Theorem 104 *If G is a graph with maximum degree k, then $\chi(G) \leq k+1$.*

Theorem 105 (Brooks, 1941) *If G is a connected non-complete graph with maximum degree $k \geq 3$, then $\chi(G) \leq k$.*

Proposition 106 *A graph G is bipartite if and only if $\chi(G) = 2$.*

Theorem 107 *A graph is bipartite if and only if it does not contain any cycle of odd length.*

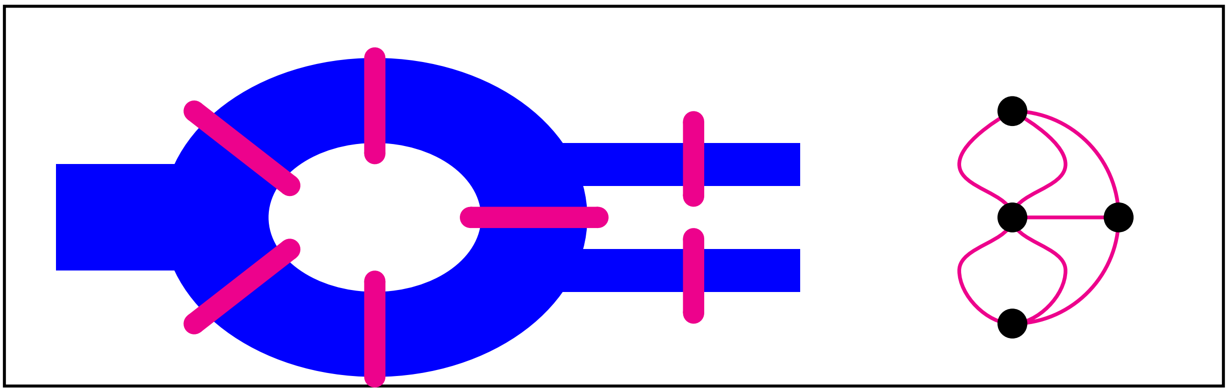
Corollary 108 *Any tree is bipartite.*

Theorem 109 (The four-color theorem, Appel and Haken, 1976) *For any planar graph G, $P_G(4) > 0$.*

- The original proof was **computer assisted** and required more than 1200h of CPU.
- An analytic proof is not yet known.
- There is no three-color theorem: there are planar graphs G with chromatic number $\chi(G) = 4$: e.g. K_4.

Eulerian graphs

Problem 4 (Euler)
The old city of Königsberg was crossed by a river and there were seven bridges. Was it possible to start walking at some point and get back to the same place by crossing every bridge exactly once?



Problem 5
Given a graph $G = (V, E)$, is there any circuit containing every edge $e \in E$? (If it is a circuit, then each edge is visited exactly once).

Eulerian graphs

Definition 110
*An **Euler tour** is a circuit containing every edge of the graph. A graph admitting an Euler tour is an **Eulerian graph**.*
*An **Euler trail** is an open trail that contains all the edges of the graph.*

Theorem 111 *A connected graph is Eulerian if and only if the degree of all its vertices is even. A connected graph contains an Euler trail if and only if it contains exactly two vertices of odd degree.*
A connected and directed graph is Eulerian if and only if for every vertex $v \in V$, $d_i(v) = d_o(v)$.

Therefore, the problem of the bridges of Königsberg does **not** have any solution: the corresponding graph does not admit any Euler tour/trail.

Fleury's algorithm

Let $G = (V, E)$ be a connected graph with all its vertices of even degree:

(1) Initial step: We choose any vertex v_0 as the initial vertex of the Euler tour $C_0 = (v_0)$ and we define $G_0 = (V_0, E_0) = G$. The algorithm sequentially increases the tour C_0 while it drops elements from G_0.

(2) How to extend the tour?: Le $C_i = (v_0, e_1, v_1, \ldots, e_i, v_i)$ be the tour corresponding to the graph $G_i = (V_i, E_i) \subseteq G_0$.

- If there exits a unique edge incident with v_i, $e_{i+1} = \{v_i, w\} \in E_i = E \setminus \{e_1, e_2, \ldots, e_i\}$:
  - $C_{i+1} = (v_0, e_1, v_1, \ldots, e_i, v_i, e_{i+1}, w)$.
  - $G_{i+1} = (V_i \setminus \{v_i\}, E_i \setminus \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$.
- If there are several edges in E_i incident with v_i, we choose any of these edges such that it is **not** a **bridge**. If we choose $e_{i+1} = \{v_i, w\} \in E_i$:
  - $C_{i+1} = (v_0, e_1, v_1, \ldots, e_i, v_i, e_{i+1}, w)$.
  - $G_{i+1} = (V_i, E_i \setminus \{e_{i+1}\}) = (V_{i+1}, E_{i+1})$.

(3) We repeat Step (2) $|E|$ times until $G_{|E|} = (\emptyset, \emptyset)$. Then $C_{|E|}$ is the Euler tour we were looking for.

Hamiltonian graphs

Problem 6
Is it possible to find a cycle on a graph G such that it contains all vertices of G exactly once?

Definition 112
A **Hamilton cycle** *of a graph G is a cycle that contains all the vertices of G. A graph admitting one Hamilton graph is a* **Hamiltonian graph**.
A **Hamilton path** *of a graph G is an open path that contains all vertices of G.*

The problem of deciding that a given graph is Hamiltonian or not is hard.

Theorem 113 (Dirac, 1950) *If G is a simple graph with $n \geq 3$ vertices and each vertex has a degree $\geq n/2$, then G is a Hamiltonian graph.*

Remark: Not every Hamiltonian graph satisfies the above condition: e.g. C_n with $n \geq 5$.

Chapter 7: Elementary combinatorics II

1. The sum rule: if $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$.
2. The product rule: $|A \times B| = |A| \cdot |B|$.
3. The inclusion-exclusion principle: $|A \cup B| = |A| + |B| - |A \cap B|$.
4. The pigeonhole principle.
5. Other standard counting problems:
   - Distributions.
   - Partitions.

Distributions

Proposition 114 (Distributions) *The number of distributions of a given set of identical r objects into n (distinct) groups, and such that each group contains at least one object, is given by*

$$\binom{r-1}{n-1}.$$

Proposition 115 *The number of distributions of a given set of identical r objects into n (distinct) groups is given by*

$$\binom{n+r-1}{r}.$$

Set partitions

Definition 116
Let S be a finite set of cardinality n. A **partition** *of S of type $(n_1, n_2, \ldots, n_k)$ with $n_i \in \mathbb{N}$ is the set $\{S_i\}_{i=1}^{k}$, where the subsets S_i satisfy: (1) $|S_i| = n_i$ for all $1 \leq i \leq k$, (2) are pairwise disjoint: $S_i \cap S_j = \emptyset$ for all $i \neq j$; and (3) their union is S (therefore, $\sum_{i=1}^{k} n_i = n$).*

Proposition 117 *Let S be a set of cardinality $m \cdot n$. Then, there exist*

$$\frac{(m \cdot n)!}{(m!)^n \, n!}$$

distinct partitions of S into n subsets S_i of type $(m, m, \ldots, m)$.

Proposition 118 *The number of distinct partitions of a set of cardinality m of type $(m_1, m_2, \ldots, m_n)$ is given by:*

$$\binom{m}{m_1, m_2, \ldots, m_n} \prod_{k \geq 1} \frac{1}{r_k!},$$

where r_k if the number of subsets of cardinality k.

Chapter 8: Advanced methods in combinatorics.

1. Recurrence relations:
   - Definitions.
   - Solution of a linear homogeneous recurrence relation.
   - Solution of a linear nonhomogeneous recurrence relation.
2. Generating functions.

Recurrence relation

Definition 119
A **recurrence relation** *for the sequence $(a_n)_{n\in\mathbb{N}}$ is an equation that expresses a_n in terms of one or more terms in the recurrence; i.e., it is, for any fixed $k \geq 1$, an equation of the type*

$$F(n; a_n, a_{n-1}, a_{n-2}, \ldots, a_{n-k}) = 0,$$

which is valid for all $n \geq k+1$. The initial conditions are the first k terms in the sequence: $(a_1, \ldots, a_k)$.

Definition 120
A recurrence relation is of k-th order if a_n can be expressed in terms of $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$. A recurrence relation is **linear** *if it expresses a_n as a linear function for a fixed number of the preceding terms. Otherwise, the relation is* **nonlinear***. A recurrence relation is* **homogeneous** *if the zero sequence $a_n = a_{n-1} = \ldots = a_{n-k} = 0$ satisfies the relation. Otherwise, it is* **nonhomogeneous**.

Solution of a linear homogeneous recurrence relation

Theorem 121 (Solution of a homogeneous first-order recurrence relation) *Let us suppose that the sequence $(a_n)_{n\in\mathbb{N}}$ satisfies the recurrence relation*

$$a_n \;=\; A\,a_{n-1}\,, \quad n \geq 2\,,$$

where A is a real number, and we know the initial condition a_1. Then, the solution of this relation is given by:

$$a_n \;=\; a_1\,A^{n-1}\,, \quad n \geq 1\,.$$

Remark: In this course, we will only consider linear recurrence relations with constant coefficients.

Solution of a linear homogeneous recurrence relation

Theorem 122 (Solution of a homogeneous Fibonacci-type recurrence relation) *Let us suppose that the sequence $(a_n)_{n\in\mathbb{N}}$ satisfies the recurrence relation*

$$a_n \;=\; A\,a_{n-1} \;+\; B\,a_{n-2}\,, \quad n \geq 3\,,$$

with real numbers A, B, and known initial conditions (a_1, a_2). If the characteristic equation associated to this relation

$$x^2 \;=\; A\,x + B$$

has characteristic roots α and β, then the solution of the recurrence relation is given for all $n \geq 1$ by

$$a_n \;=\; \begin{cases} K_1\,\alpha^n + K_2\,\beta^n & \text{if } \alpha \neq \beta, \\ (K_1 + nK_2)\,\alpha^n & \text{if } \alpha = \beta, \end{cases}$$

where the constants K_1 and K_2 can be obtained using the initial conditions (a_1, a_2).

Solution of a linear homogeneous recurrence relation

- Let us suppose that the sequence $(a_n)_{n\in\mathbb{N}}$ satisfies the linear recursion:

$$a_n \;=\; c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}\,, \qquad n \geq k+1\,,$$

  with real numbers $c_1, c_2, \ldots, c_k$. We assume that the k initial conditions $(a_1, a_2, \ldots, a_k)$ are known.
- If we look for a solution of the form

$$a_n = K_i x^n\,,$$

  then the amplitude K_i cancels out, and the indeterminate x should satisfy the characteristic equation:

$$x^k \;=\; c_1 x^{k-1} + c_2 x^{k-2} + \ldots + c_k\,.$$

- If a_n and b_n are two solutions of a given linear homogeneous recurrence relation, then any linear combination $\alpha a_n + \beta b_n$ will be also a solution of that recursion.

Solution of a linear homogeneous recurrence relation (2)

- To each distinct characteristic root x_i, there corresponds a solution $a_n^{(i)}$, whose structure depends on the multiplicity of x_i:
  - If the root x_i is simple, then $a_n^{(i)} = K_i x_i^n$.
  - If the root x_i is double, then $a_n^{(i)} = (K_i + K_i' n) x_i^n$.
  - If the root x_i is triple, then $a_n^{(i)} = (K_i + K_i' n + K_i'' n^2) x_i^n$, etc.
- If the characteristic equation has r distinct roots x_i with multiplicities k_i (such that $\sum_{i=1}^r k_i = k$), then the general solution for this recursion has the form:

$$a_n \;=\; \sum_{i=1}^{r} \left[\sum_{j=1}^{k_i} K_i^{(j)} n^{j-1} \right] x_i^n\,, \qquad n \geq 1\,,$$

  where the k constants $K_i^{(j)}$ are determined using the k initial conditions.

Solution of a linear nonhomogeneous recurrence relation

Theorem 123 (Solution of a linear nonhomogeneous recurrence relation) *Let us assume that the sequence $(a_n)_{n\in\mathbb{N}}$ satisfies the linear nonhomogeneous recurrence relation with constant coefficients:*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + t_n\,, \quad n \geq k+1\,,$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and the initial conditions $(a_1, \ldots, a_k)$ are known. The function $t_n : \mathbb{N} \to \mathbb{R}$ is a given known function of n. Then, the general solution of this linear nonhomogeneous recurrence is equal to the sum of the general solution for the linear homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}\,, \quad n \geq k+1\,,$$

plus any particular solution of the full recurrence.

Solution of a linear nonhomogeneous recurrence relation

Theorem 124 (Solution of a linear nonhomogeneous recurrence relation) *Let us suppose that the sequence $(a_n)_{n\in\mathbb{N}}$ satisfies the linear nonhomogeneous recurrence*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + t_n\,, \quad n \geq k+1\,,$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and the initial conditions $(a_1, a_2, \ldots, a_k)$ are known. Let us further assume that the function $t_n : \mathbb{N} \to \mathbb{R}$ is of the form

$$t_n = s^n \left[b_0 + b_1 n + \ldots + b_t n^t\right]\,,$$

with real numbers $b_0, b_1, \ldots, b_t, s$. If s is not a characteristic root of the associated linear homogeneous recurrence, then there exists a particular solution of the form

$$a_{n,p} = s^n \left[p_0 + p_1 n + \ldots + p_t n^t\right]\,.$$

If s is a characteristic root with multiplicity m of the associated linear homogeneous recurrence, then there exists a particular solution of the form

$$a_{n,p} = n^m \cdot s^n \left[p_0 + p_1 n + \ldots + p_t n^t\right]\,.$$

- The particular solution $a_{n,p}$ has **no** free parameters: there is only a unique choice for the coefficients $\{p_k\}_{k=1}^{t}$ such that $a_{n,p}$ is actually a solution.

Chapter 9: Advanced methods in combinatorics.

1. Recurrence relations.
2. Generating functions:
   - Definitions.
   - How to efficiently encode combinatorial problems?
   - Solution of recurrence relations.

Generating functions

Definition 125
The **generating function** *associated to the sequence* $(a_0, a_1, a_2, \dots, a_n, \dots)$ *is the following formal power series:*

$$F(x) \;=\; a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots \;=\; \sum_{n=0}^{\infty} a_n\, x^n\,.$$

- $(1+x)^k = \sum_{n=0}^{k} \binom{k}{n} x^n$ is the g.f. of $\left(\binom{k}{0}, \binom{k}{1}, \dots, \binom{k}{k}, 0, 0, \dots\right)$.
- $1 + x + x^2 + \dots + x^{k-1} = \sum_{n=0}^{k-1} x^n = \frac{1-x^k}{1-x}$ is the g.f. of $(\underbrace{1, 1, \dots, 1}_{k}, 0, 0, \dots)$.
- $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots = \sum_{n=0}^{\infty} x^n$ is the g.f. of $(1, 1, 1, \dots)$.
- $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ is the g.f. of $(1, 1, \frac{1}{2!}, \frac{1}{3!}, \dots)$.

Basic operations with generating functions

- The g.f. for the sequence $(1, 2, 3, \ldots)$ is given by
  $$\sum_{n=0}^{\infty}(n+1)x^n = \frac{d}{dx}\sum_{n=0}^{\infty}x^{n+1} = \frac{d}{dx}\frac{x}{1-x} = \frac{1}{(1-x)^2}.$$
- If $F(x) = \sum_{n=0}^{\infty} a_n x^n$ and $G(x) = \sum_{n=0}^{\infty} b_n x^n$, then $(F+G)(x) = \sum_{n=0}^{\infty}(a_n + b_n)x^n$.
- If F is the g.f. of the sequence $\{a_n\}$, then the g.f. of the sequence $(\underbrace{0, 0, \ldots, 0}_{k}, a_0, a_1, \ldots)$ is $G(x) = x^k F(x)$.

Integer partitions

Problem 7

Count the number of distinct partitions of the positive integer N*. For example, if* $N = 4$*, there are 5 partitions:* $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$.

1. The sum principle allows us to compute the generating function associated to use the positive integer k in the partition:
   - The generating function for using 1 in the partition is $f_1 = 1 + x + x^2 + x^3 + \ldots = \frac{1}{1-x}$.
   - The generating function for using 2 in the partition is $f_2 = 1 + x^2 + x^4 + x^6 + \ldots = \frac{1}{1-x^2}$.
   - The generating function for using $p \geq 1$ in the partition is $f_p = 1 + x^p + x^{2p} + x^{3p} + \ldots = \frac{1}{1-x^p}$.
2. Because writing up a partition is a sequential process, the generating function that encodes Problem 7 is given by the product principle:

$$f(x) = \prod_{k=1}^{\infty} f_k(x) = \prod_{k=1}^{\infty}\frac{1}{1-x^k} = 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + \cdots$$

Practical procedure

- Encoding of a combinatorial problem:
  1. Compute the generating function F by using the sum/product principles and other operations.
  2. Compute the coefficients a_n by computing the Taylor power-series expansion of F around $x = 0$.
- Solving a recurrence relation:
  1. Rewrite the recurrence relation for a_n in terms of an equation that only involves the generating function F.
  2. Solve this equation and obtain a closed form for F in terms of x.
  3. Compute the coefficients a_n by computing the Taylor power-series expansion of F around $x = 0$.

Example: the Fibonacci recursion

We want to solve the recurrence relation

$$a_n = a_{n-1} + a_{n-2}\,, \quad n \geq 2\,, \quad a_0 = 0\,, \quad a_1 = 1\,,$$

by using the generating function

$$F(x) = \sum_{n=0}^{\infty} a_n\, x^n = a_0 + a_1\, x + \sum_{n=2}^{\infty} a_n\, x^n\,.$$

Algorithm:

1. Multiply the recurrence relation by x^n and sum over all values of n for which this recursion is valid (in our case, $n \geq 2$):

$$\sum_{n=2}^{\infty} a_n\, x^n = \sum_{n=2}^{\infty} a_{n-1}\, x^n + \sum_{n=2}^{\infty} a_{n-2}\, x^n\,.$$

Example: the Fibonacci recursion

2. Manipulate the sums so that they can be expressed in terms of F and the initial conditions:
   - $\sum_{n=2}^{\infty} a_n\, x^n = F - a_0 - a_1\, x = F - x.$
   - $\sum_{n=2}^{\infty} a_{n-1}\, x^n = x \sum_{n=2}^{\infty} a_{n-1}\, x^{n-1} = x \sum_{m=1}^{\infty} a_m\, x^m = x(F - a_0) = x\, F.$
   - $\sum_{n=2}^{\infty} a_{n-2}\, x^n = x^2 \sum_{n=2}^{\infty} a_{n-2}\, x^{n-2} = x^2 \sum_{m=0}^{\infty} a_m\, x^m = x^2\, F.$

   The Fibonacci recursion now becomes the equation

$$F - x \;=\; x\, F + x^2\, F\,.$$

3. We solve this equation for F:

$$F(x) \;=\; \frac{x}{1 - x - x^2} \;=\; \sum_{n=0}^{\infty} a_n\, x^n\,.$$

Example: the Fibonacci recursion

4. We compute the Taylor power-series expansion of F and we read the coefficient of x^n:

$$F(x) \;=\; \frac{x}{1 - x - x^2} \;=\; x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + \dots$$

   We can obtain all coefficients with a little algebra:

$$\begin{aligned}
F(x) \;&=\; \frac{\alpha}{x + (1+\sqrt{5})/2} + \frac{\beta}{x + (1-\sqrt{5})/2} \\
&=\; \frac{1}{\sqrt{5}} \left[\frac{1}{1 - x(1+\sqrt{5})/2} - \frac{1}{1 - x(1-\sqrt{5})/2} \right] \\
&=\; \sum_{n=0}^{\infty} \frac{x^n}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]. \\
F_n \;&=\; \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].
\end{aligned}$$

Generalized binomial theorem

Theorem 126 *Let k be a fixed positive integer, then we have formally that*

$$\frac{1}{(1+x)^k} = \sum_{n=0}^{\infty} \binom{-k}{n} x^n ,$$

where for all $n \geq 0$ the above binomial coefficient is defined as

$$\binom{-k}{n} = \frac{-k(-k-1)(-k-2)\ldots(-k-n+1)}{n!} = (-1)^n \binom{n+k-1}{n} .$$

Chapter 10: Graph theory V

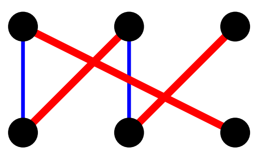
1. Undirected graphs.
2. Algorithms in graph theory.
3. Combinatorial problems on graphs:
   - Perfect matchings.
   - Proper colorings.

Perfect matchings

Definition 127
A **perfect matching** *of a simple graph with $2n$ vertices is a spanning subgraph composed by n disjoint edges.*

Remarks:

- All the vertices of G belong to the matching.
- Each vertex of G is incident with a single edge belonging to the matching.
- If G is bipartite, then we can prove more theorems.



Theorem 128 *If G is a bipartite and regular graph with degree $d \geq 1$, then G contains a perfect matching.*

Proper colorings: chromatic polynomial

Definition 129
Let $G = (V, E)$ be a simple graph and let $q \geq 2$ be a natural number. The chromatic polynomial P_G is a polynomial such that $P_G(q)$ gives the number of distinct proper colorings of G with $q \in \mathbb{N}$ colors.

Theorem 130 *If $G = (V, E)$ is a simple graph, $P_G(q)$ is a polynomial in q.*

The proof is based on these two facts:

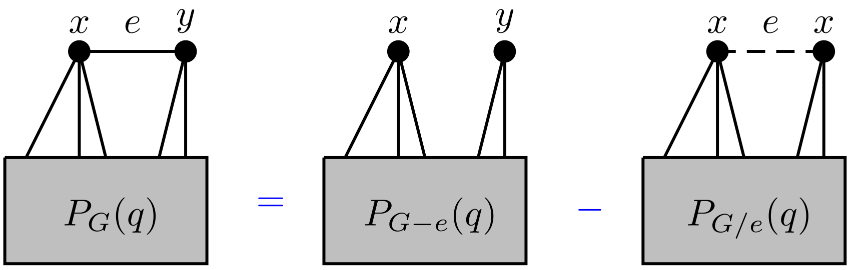
- If $G = (\{v\}, \emptyset)$, $P_G(q) = q$.
- The contraction-deletion theorem holds:

Theorem 131 (The contraction-deletion theorem) *If $G = (V, E)$ is a simple graph, and $e = \{x, y\} \in E$ with $x, y \in V$, then*

$$P_G(q) = P_{G-e}(q) - P_{G/e}(q) \,,$$

where $G - e$ is the graph obtained from G by deleting the edge e, and G/e is the graph obtained from G by contracting the edge e (i.e., by identifying vertices x and y, and by eliminating possible multiple edges).

Proof of the contraction-deletion theorem



> **Theorem 132** *If G is a disconnected graph with $k \geq 1$ connected components G_j, then* $P_G(q) = \prod_{j=1}^{k} P_{G_j}(q)$.

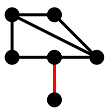
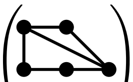
> **Theorem 133** *If G is a graph that can be split into two parts G_1 and G_2 such that $G_1 \cap G_2 = K_n$ for some $n \geq 1$, then*
> $$P_G(q) \;=\; \frac{P_{G_1}(q) \times P_{G_2}(q)}{P_{K_n}(q)}\,.$$

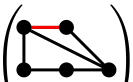
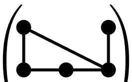
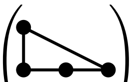
1. If $G = K_n$, then $P_{K_n}(q) = q(q-1)\ldots(q-n+1)$.
2. If G is a tree with n vertices T_n, then $P_{T_n}(q) = q(q-1)^{n-1}$.

Example

Problem 8
In the Lattice'06 Symposium there were six one-hour parallel lectures scheduled for the first day $\{c_1, \ldots, c_6\}$. There were groups interested in attending to lectures $\{c_1, c_2\}$, $\{c_1, c_4\}$, $\{c_3, c_5\}$, $\{c_2, c_6\}$, $\{c_4, c_5\}$, $\{c_5, c_6\}$, and $\{c_1, c_6\}$. If lectures cannot overlap, which is the minimum number of hours needed to allocate all the lectures in such a way that everyone could attend the lectures he/she was interested in?

Use a recursive application of the contraction-deletion theorem:

$P\Big($  $\Big) \;=\; (q-1) \times P\Big($  $\Big)$

$P\Big($  $\Big) \;=\; P\Big($  $\Big) - P\Big($  $\Big) \;=\; (q-2)P_{C_4}(q)$

$$\begin{aligned} P_G(q) &= (q-1)(q-2)P_{C_4}(q) \quad [P_{C_4}(q) = q(q-1)(q^2-3q+3)] \\ &= q(q-1)^2(q-2)(q^2-3q+3) \quad \Rightarrow \quad \chi(G) = 3\,. \end{aligned}$$

Chapter 11. Binary relation. Equivalence relations

1. Binary relations:
   - Definitions.
   - Graphical representation of a relation.
   - Operations with relations.
   - Properties.
2. Equivalence relations:
   - Equivalence classes.
   - Quotient set.
3. Order relations.
4. Lattices and Boolean algebras.

Binary relations between two sets

Definition 134
A **binary relation** $\mathcal{R}$ *between the sets* V *and* W *is a subset of the Cartesian product* $V \times W$*:*

$$V \times W = \{(v, w) \colon (v \in V) \wedge (w \in W)\}\,.$$

Therefore, $\mathcal{R} \subseteq V \times W$. *The* **domain** *of* $\mathcal{R}$ *is the set:*

$$\mathit{Dom}\,\mathcal{R} = \{v \in V \colon (v, w) \in \mathcal{R} \quad \textit{for some } w \in W\}\,.$$

and the **image** *of* $\mathcal{R}$ *is the set:*

$$\mathit{Im}\,\mathcal{R} = \{w \in W \colon (v, w) \in \mathcal{R} \quad \textit{for some } v \in V\}\,.$$

Notation: If $(v, w) \in \mathcal{R}$, we denote it as $v\mathcal{R}w$.

Binary relations on a set

Definition 135
A **binary relation** $\mathcal{R}$ *on the set* V *is a subset of the Cartesian product* $V \times V$ *Hence,* $\mathcal{R} \subseteq V \times V$. *The* **domain** *of* $\mathcal{R}$ *is the set:*

$$\text{Dom}\,\mathcal{R} \;=\; \{v \in V : (v, w) \in \mathcal{R} \quad \text{for some } w \in V\}$$

and the **image** *of* $\mathcal{R}$ *is the set:*

$$\text{Im}\,\mathcal{R} \;=\; \{w \in V : (v, w) \in \mathcal{R} \quad \text{for some } v \in V\}\,.$$

Important remark: A function $f : A \to B$ is a relation between the sets A and B and such that to each element $x \in \text{Dom}(f)$ there corresponds a unique element of B (i.e., $f(x)$).

Graphical representation of a relation

- Cartesian representation.
- Venn's diagrams.
- Adjacency matrix of $\mathcal{R}$:
  Let V and W be the sets $V = \{v_1, v_2, \ldots, v_{|V|}\}$ and $W = \{w_1, w_2, \ldots, w_{|W|}\}$. Then entry (i, j) of $A_\mathcal{R}$ is equal to 1 if $v_i \mathcal{R} w_j$, and it is equal to 0 otherwise.
- Directed graph $G_\mathcal{R}$ associated to $\mathcal{R}$:
  The vertices of $G_\mathcal{R}$ are the elements of the set V where the relation $\mathcal{R}$ is defined. The set of (directed) edges is the set of ordered pairs:

$$E \;=\; \{(v_i, v_j) \in V \times V : v_i \mathcal{R} v_j\}\,.$$

Operations with relations

Definition 136
Given the relation $\mathcal{R}$ on V, we define its **inverse relation** $\mathcal{R}^{-1}$ *as the relation on V defined as $(v_1, v_2) \in \mathcal{R}^{-1} \;\Leftrightarrow\; (v_2, v_1) \in \mathcal{R}$, or in other words, $v_1 \mathcal{R}^{-1} v_2 \;\Leftrightarrow\; v_2 \mathcal{R} v_1$.*

Given any relation $\mathcal{R}$, there always exists its inverse relation $\mathcal{R}^{-1}$. This is in contradiction to what happens with functions: the inverse function f^{-1} exists if and only if f is bijective.

Definition 137
Given a relation $\mathcal{R}$ on V, we define its **complementary relation** $\overline{\mathcal{R}}$ *as the relation on V such that $(v_1, v_2) \in \overline{\mathcal{R}} \;\Leftrightarrow\; (v_1, v_2) \notin \mathcal{R}$.*

Binary relations are subsets of $V \times W$, therefore, set operations can be interpreted as operations with relations.

Composition of relations

Definition 138
Let $\mathcal{R}$ be a relation between the sets V and W, and let $\mathcal{S}$ be a relation between the sets W and Y. The **composition of the relation** $\mathcal{S}$ *and $\mathcal{R}$ is a relation between the sets V and Y denoted as $\mathcal{S} \circ \mathcal{R}$. In particular, $\mathcal{S} \circ \mathcal{R}$ is a subset of the Cartesian product $V \times Y$ such that, given any $v \in V$ and $y \in Y$, $v(\mathcal{S} \circ \mathcal{R})y$ if and only if there exists some $w \in W$ satisfying $v\mathcal{R}w$ and $w\mathcal{S}y$.*

Proposition 139 *Let $A_{\mathcal{R}}$ be the adjacency matrix of the relation $\mathcal{R}$ between V and W, and let $A_{\mathcal{S}}$ be the adjacency matrix of the relation $\mathcal{S}$ between W and Y. Then, the adjacency matrix $A_{\mathcal{S}\circ\mathcal{R}}$ of the composition of the relations $\mathcal{S} \circ \mathcal{R}$ between V and Y is given by:*

$$A_{\mathcal{S}\circ\mathcal{R}} \;=\; A_{\mathcal{R}} \odot A_{\mathcal{S}} \,,$$

where the product $\odot$ is the **Booolean product** *of matrices.*

Using Boolean operations (instead of regular ones) guaranties that $A_{\mathcal{S}\circ\mathcal{R}}$ is an adjacency matrix associated to a binary relation.

Properties of relations on a set V

Definition 140
A relation $\mathcal{R}$ es **reflexive** *if for every $v \in V$, $v\mathcal{R}v$.*

Definition 141
A relation $\mathcal{R}$ is **irreflexive** *if for every $v \in V$, $v\overline{\mathcal{R}}v$.*

Definition 142
A relation $\mathcal{R}$ is **symmetric** *if $\mathcal{R} = \mathcal{R}^{-1}$, i.e., if $v\mathcal{R}w \;\Rightarrow\; w\mathcal{R}v$.*

Definition 143
A relation $\mathcal{R}$ is **antisymmetric** *if $(v_1\mathcal{R}v_2) \wedge (v_2\mathcal{R}v_1) \;\Rightarrow\; v_1 = v_2$.*

Transitive relations

Definition 144
A relation $\mathcal{R}$ is **transitive** *if $(v_1\mathcal{R}v_2) \wedge (v_2\mathcal{R}v_3) \;\Rightarrow\; v_1\mathcal{R}v_3$.*

Proposition 145 *A relation $\mathcal{R}$ is transitive if and only if $\mathcal{R}^n \subseteq \mathcal{R}$ for all $n \in \mathbb{N}$. The* **n-th power** *$\mathcal{R}^n$ of the relation $\mathcal{R}$ is recursively defined as follows:*

$$\mathcal{R}^1 = \mathcal{R}\,, \qquad \mathcal{R}^n = \mathcal{R} \circ \mathcal{R}^{n-1}\,.$$

Corollary 146 *A relation $\mathcal{R}$ is transitive if and only $\mathcal{R}^2 \subseteq \mathcal{R}$. In other words, $\mathcal{R}$ is transitive if and only if for each nonzero entry $(A_{\mathcal{R}^2})_{i,j} = 1$ of the adjacency matrix of $\mathcal{R}^2$, the corresponding entry of the adjacency matrix of $\mathcal{R}$ is also nonzero $(A_{\mathcal{R}})_{i,j} = 1$.*

Equivalence relations

Definition 147
A relation $\mathcal{R}$ on a set V is an **equivalence relation** *if it is reflexive, symmetric and transitive.*

Notation: If $\mathcal{R}$ is an equivalence relation, $a\mathcal{R}b$ is usually denoted as

$$a \equiv b \pmod{\mathcal{R}}.$$

Definition 148
Let $\mathcal{R}$ be an equivalence relation on a set V. The set of all the elements of V related to a certain element $v \in V$ is called the **equivalence class determined by v**, *and it is denoted as $[v]_{\mathcal{R}}$, or simply as $[v]$. Therefore,*

$$[v]_{\mathcal{R}} = \{w \in V : v\mathcal{R}w\} .$$

Any element $w \in [v]_{\mathcal{R}}$ (in particular, v) is a **representative** *of the equivalence class $[v]_{\mathcal{R}}$.*

Quotient set

Theorem 149 *Let $\mathcal{R}$ be an equivalence relation on V. Then,*

(1) $[a]_{\mathcal{R}}$ is non-empty for all $a \in V$.

(2) For any two elements $a, b \in V$, either $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ (and $a\mathcal{R}b$), or $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$.

(3) The equivalence classes determine the relation uniquely.

Theorem 150 *Let $\mathcal{R}$ be an equivalence relation on V. Then the set of all equivalence classes of $\mathcal{R}$ form a partition of V. Conversely, given a partition $\{V_1, V_2, \ldots\}$ of V, there exists an equivalence relation $\mathcal{R}$ such that its equivalence classes are the sets V_i.*

Definition 151
Let $\mathcal{R}$ be an equivalence relation on V. The set of all the equivalence classes of $\mathcal{R}$ is called the **quotient set of V by $\mathcal{R}$**, *and it is denoted by $V/\mathcal{R}$:*

$$V/\mathcal{R} = \{[v]_{\mathcal{R}} : v \in V\} .$$

Chapter 12: Modular arithmetic

1. Integer arithmetic:
   - Integer divisibility (reminder).
   - Euclid's algorithm.
   - Bezout's identity.
   - Linear Diophantine equations.
2. Modular arithmetic:
   - Linear congruences.
   - Arithmetic on $\mathbb{Z}_p$.
   - Euler's ϕ function. Euler's theorem.

Integer arithmetic: reminder from Chapter 1

Definition 152
Given two integers $a \neq 0$ and b, we say that $\boldsymbol{a}$ **divides** $\boldsymbol{b}$ *if there is an integer $q \in \mathbb{Z}$ such that $b = a \cdot q$. If a divides b, we say that a is a* **factor** *of b and that b is a* **multiple** *of a. We denote* $\boldsymbol{a \mid b}$ *when a divides b, and we write* $\boldsymbol{a \nmid b}$ *when a does not divide b.*

Remarks:

- Every non-zero integer $a \in \mathbb{Z}$ divides 0: $\quad 0 = a \cdot 0$.
- 1 divides any $a \in \mathbb{Z}$: $\quad a = 1 \cdot a$.
- Any integer $a \in \mathbb{Z}$ divides itself: $\quad a = a \cdot 1$.

Theorem 153 (The division algorithm) *Let a and $b \neq 0$ be two integers. Then there exists a* **unique** *pair of integers q and r such that*

$$a \;=\; q \cdot b + r \qquad \text{with} \quad 0 \leq r < |b|\,.$$

Properties of integer division

Theorem 154 *Let a, b, c be integers. Then:*

1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*
2. *If $a \mid b$, then $a \mid (b \cdot c)$ for every $c \in \mathbb{Z}$.*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*
4. *If $c \neq 0$, then $a \mid b$ if and only if $(c \cdot a) \mid (c \cdot b)$.*
5. *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*
6. *If $a \mid b$ and $b \mid a$, then $a = \pm b$.*

Theorem 155 *If $a \mid b_i$ for $i = 1, \ldots, N$, then $a \mid \sum_{i=1}^{N} u_i \cdot b_i$ for every $u_i \in \mathbb{Z}$.*

Greatest common divisor. Euclid's lemma (IIIrd century BC)

Definition 156
Let a, b be integers, not both simultaneously zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** *of a and b. It is denoted by $\gcd(a, b)$.*

Remarks:

- The case $a = b = 0$ is excluded because any integer divides 0.
- $\gcd(0, a) = |a|$ for every nonzero integer a.

Theorem 157 *The greatest common divisor of two numbers is unique.*

Lemma 158 (Euclid) *Given the integers a, $b \neq 0$, q and r, such that $a = q \cdot b + r$ with $0 \leq r < |b|$, then $\gcd(a, b) = \gcd(b, r)$.*

Euclid's algorithm

Problem 9
Apply recursively Euclid's lemma to compute $\gcd(662, 414)$.

$$\begin{aligned}
a &= b \cdot q + r\,,\\
662 &= 414 \cdot 1 + 248\,,\\
414 &= 248 \cdot 1 + 166\,,\\
248 &= 166 \cdot 1 + 82\,,\\
166 &= 82 \cdot 2 + \boxed{2}\,,\\
82 &= 2 \cdot 41 + 0\,.
\end{aligned}$$

$$\begin{aligned}
\gcd(662, 414) &= \gcd(414, 248) = \gcd(248, 166) = \gcd(166, 82)\\
&= \gcd(82, 2) = \boxed{2}\,.
\end{aligned}$$

In general, $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-2}, r_{n-1})$, where r_{n-1} is the last nonzero remainder ($r_n = 0$). In the last step: $r_{n-2} = q_n \cdot r_{n-1} \Rightarrow r_{n-1} \mid r_{n-2}$. Therefore, $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$.

Theorem 159 *In Euclid's algorithm,* $\gcd(a, b) = r_{n-1}$ *(= the last nonzero remainder).*

Bezout's identity

Theorem 160 (Bezout's identity, 1730-1783) *If* a *and* b *are two integers not simultaneously zero, then there exist integers* u, w *such that*

$$\gcd(a, b) = a \cdot u + b \cdot w\,.$$

DEMOSTRACIÓN. If we write the steps of Euclid's algorithm:

$$\begin{array}{rclcrcll}
a &=& q_1 \cdot b + r_1 & \Rightarrow & r_1 &=& a - q_1 \cdot b & P_1\\
b &=& q_2 \cdot r_1 + r_2 & \Rightarrow & r_2 &=& b - q_2 \cdot r_1 & P_2\\
r_1 &=& q_3 \cdot r_2 + r_3 & \Rightarrow & r_3 &=& r_1 - q_3 \cdot r_2 & P_3\\
\vdots &&&& \vdots &&&\\
r_{n-4} &=& q_{n-2} \cdot r_{n-3} + r_{n-2} & \Rightarrow & r_{n-2} &=& r_{n-4} - q_{n-2} \cdot r_{n-3} & P_{n-2}\\
r_{n-3} &=& q_{n-1} \cdot r_{n-2} + r_{n-1} & \Rightarrow & r_{n-1} &=& r_{n-3} - q_{n-1} \cdot r_{n-2} & P_{n-1}\\
r_{n-2} &=& q_n \cdot r_{n-1} + (r_n = 0) & \Rightarrow & r_{n-1} &=& \gcd(a, b) & P_n
\end{array}$$

Then, $\gcd(a, b) = r_{n-1} = \alpha_{n-1} r_{n-3} + \beta_{n-1} r_{n-2} = \alpha_{n-2} r_{n-4} + \beta_{n-2} r_{n-3} = \ldots = \alpha_3 r_1 + \beta_3 r_2 = \alpha_2 b + \beta_2 r_1 = \alpha_1 a + \beta_1 b$.

Bezout's identity (2)

Important remark: Bezout's identity does **not** imply that the integers u, v are unique.

Theorem 161 *Let a and b be two integers not simultaneously zero with $\gcd(a, b) = d$. An integer c can be written in the form $a \cdot x + b \cdot y$ for some integers x, y if and only if c is a multiple of d. In particular, d is the smallest positive integer of the form $a \cdot x + b \cdot y$ with $x, y \in \mathbb{Z}$.*

Corollary 162 *Two integers are relatively prime if and only if there exist integers x, y such that $a \cdot x + b \cdot y = 1$.*

Corollary 163 *If $\gcd(a, b) = d$, then*

1. $\gcd(m \cdot a, m \cdot b) = m \cdot d$ *for every* $m \in \mathbb{N}$.
2. $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Corollary 164 *If a, b are two relatively-prime integers, then:*

1. *If $a \mid c$ and $b \mid c$, then $(a \cdot b) \mid c$.*
2. *If $a \mid (b \cdot c)$, then $a \mid c$.*

Least common multiple

Definition 165
The **least common multiple** *of two natural numbers a, b is the* <u>*least natural number*</u> *m such that $a \mid m$ and $b \mid m$. It is denoted by $\operatorname{lcm}(a, b)$.*

Remark: This number exists because the set of natural numbers $\mathbb{N}$ is a well-ordered set (see next chapter).

Theorem 166 *If a, b are two natural numbers, then*

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) \;=\; a \cdot b\,.$$

Some results on prime numbers:

Theorem 167 *The positive integer n is a composite number if and only if n can be divided by some prime number $p \leq \sqrt{n}$.*

Lemma 168 *Let p be a prime number, and let a, b be integers. Then:*

(a) *Either $p \mid a$, or p and a are relatively prime.*

(b) *If $p \mid (a \cdot b)$, then either $p \mid a$ or $p \mid b$.*

Linear Diophantine equations [Diophantus of Alexandria, IIIrd century]

Definition 169
A **Diophantine equation** *is an equation of one or several variables such that we are only interested in their integer solutions.*

Theorem 170 (Brahmagupta, VIIth century) *The linear equation*

$$a \cdot x + b \cdot y \;=\; c\,,$$

where a, b, c are integers (and a, b not simultaneously zero), admits integer solutions if and only if $d = \gcd(a, b)$ divides c. In this case, there exist infinite integer solutions (x_k, y_k) with $k \in \mathbb{Z}$ given by

$$\begin{aligned} x_k &= u \cdot p + \frac{b \cdot k}{d}\,, \\ y_k &= w \cdot p - \frac{a \cdot k}{d}\,, \end{aligned}$$

where $p = c/d \in \mathbb{Z}$ and u, w are given by

$$d \;=\; u \cdot a + w \cdot b\,.$$

Modular arithmetic

Modular arithmetic allows us to perform algebraic operations using, instead of a given set of numbers, their respective remainders with respect to some fixed positive number called the **modulus**. The modulus is 12 or 24 when we count hours with a clock, 7 when we count days in a week, etc.

Definition 171
Let a, b be integers, and let m be a natural number. Then $\boldsymbol{a, b}$ **are congruent** <u>**modulo**</u> $\boldsymbol{m}$ *if $m \mid (a - b)$. This relation is denoted as $a \equiv b \pmod{m}$.*

Proposition 172

1. *$a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.*
2. *$a \equiv b \pmod{m}$ is and only if $a = b + k \cdot m$ for some $k \in \mathbb{Z}$.*

Theorem 173 *For each positive integer m, the binary relation $\equiv \pmod{m}$ is an equivalence relation.*

The quotient set $\mathbb{Z}_m$

The equivalence classes (or congruence classes) modulo m

$$[a]_m = \{b \in \mathbb{Z} : a \equiv b \pmod{m}\} = \{a + mk : k \in \mathbb{Z}\}$$

form a partition of $\mathbb{Z}$. There are m distinct equivalence classes corresponding to the m possible remainders obtained by dividing an integer by m.

Theorem 174 *The quotient set $\mathbb{Z}_m = \mathbb{Z}/\equiv \pmod{m}$ is given by*

$$\mathbb{Z}_m = \{[a]_m : 0 \le a \le m-1\} .$$

Remark: Usually, the notation for $\mathbb{Z}_m$ is a bit looser:

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\} .$$

Modular arithmetic

Theorem 175 *Let m be a positive integer. If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then:*

- $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$.
- $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$.

Corollary 176 *Let m, k be positive integers. If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.*

Theorem 177 *Let m be a positive integer, and let a, b, c be integers. If $a \cdot c \equiv b \cdot c \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.*

Remarks:

- This theorem allows us to divide by a common factor c both sides of the sign $\equiv$ whenever c and the modulus m are relatively primes.
- If c and m are not relatively primes, then the correct result is: Let us write $m = p \cdot c$ for positive integers p, c, and let a, b be integers. If $a \cdot c \equiv b \cdot c \pmod{p \cdot c}$, then $a \equiv b \pmod{p}$.

Modular division: linear congruence equations

Definition 178
A congruence modulo m of the form

$$a \cdot x \equiv b \pmod{m},$$

where m is a positive integer, a, b are integers, and x is a variable is called a **linear congruence equation**.

Remark: If there exists a unique solution of the linear congruence equation $a \cdot x \equiv 1 \pmod{m}$, then solving this equation is equivalent to obtain the multiplicative inverse of a modulo m.

Remark: If x is a solution of a linear congruence equation, and $x' \equiv x \pmod{m}$, then x' is also a solution of that equation:

$$a \cdot x' \equiv a \cdot x \pmod{m} \equiv b \pmod{m}.$$

Therefore, the solutions of a linear congruence equation (if any) form classes of congruence modulo m: i.e., they are elements of $\mathbb{Z}_m$.

Linear congruence equations

Theorem 179 *If $d = \gcd(a, m)$, then the linear congruence equation*

$$a \cdot x \equiv b \pmod{m}$$

has a solution if and only if $d \mid b$. In this case and if x_0 is a particular solution of the linear congruence equation, the general solution is given by

$$x_k = x_0 + \frac{m \cdot k}{d}, \qquad k \in \mathbb{Z}.$$

In particular, these solutions form d congruence classes modulo m with representatives:

$$\left\{ x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{m(d-1)}{d} \right\}.$$

Corollary 180 *If $\gcd(a, m) = 1$, the solutions x of the linear congruence equation $a \cdot x \equiv b \pmod{m}$ form a unique congruence class modulo m.*

Corollary 181 *If $\gcd(a, m) = 1$ with $m > 1$, then there exists a multiplicative inverse of a modulo m. This multiplicative inverse is unique modulo m.*

Arithmetic with $\mathbb{Z}_m$

The elements of $\mathbb{Z}_m$ with $m \in \mathbb{N}$ are equivalence classes modulo m. For the sake of simplicity, $x \in \mathbb{Z}_m$ represents that $x \in [x]_m$.
The **sum** and the **multiplication** on $\mathbb{Z}_m$ are defined as:

$$\begin{aligned} x + y &= [x]_m + [y]_m = [x+y]_m , \\ x \cdot y &= [x]_m \cdot [y]_m = [x \cdot y]_m , \end{aligned}$$

and they verify the usual properties: for every $x, y, z \in \mathbb{Z}_m$,

- Closure: $x + y \in \mathbb{Z}_m$ and $x \cdot y \in \mathbb{Z}_m$.
- Associativity: $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Commutativity: $x + y = y + x$ and $x \cdot y = y \cdot x$.
- Distributivity: $x \cdot (y + z) = x \cdot y + x \cdot z$.
- Identity element (sum): $\exists\, 0 \in \mathbb{Z}_m$ such that $0 + x = x, \forall\, x \in \mathbb{Z}_m$.
- Identity element (product): $\exists\, 1 \in \mathbb{Z}_m$ such that $1 \cdot x = x, \forall\, x \in \mathbb{Z}_m$.
- Inverse element (sum): $\forall\, x \in \mathbb{Z}_m, \exists - x \in \mathbb{Z}_m$ such that $x + (-x) = 0$.

Remark: These properties are those characterizing a **field** (like $(\mathbb{R}, +, \cdot)$), except for the existence of a multiplicative inverse.

Arithmetic with $\mathbb{Z}_m$ (2)

In $\mathbb{Z}$ there does not exist in general the multiplicative inverse of an integer x: y is the multiplicative inverse of x if and only if $x \cdot y = 1$. However, two properties hold:

1. Cancellation law: If $x \neq 0$ and $x \cdot y = x \cdot z$, then $y = z$.
2. If $x \cdot y = 0$, then either $x = 0$ or $y = 0$.

None of these two properties holds in general in $\mathbb{Z}_m$.

Definition 182
An element $x \not\equiv 0 \pmod{m}$ of $\mathbb{Z}_m$ is a **divisor of zero** *if there exists an element $y \not\equiv 0 \pmod{m}$ such that $x \cdot y \equiv 0 \pmod{m}$.*

Remark: in some books, the condition $x \not\equiv 0 \pmod{m}$ is dropped.

Definition 183
An element $x \in \mathbb{Z}_m$ is a **unit modulo m** *if it has a multiplicative inverse modulo m; i.e., if there is an element $s \in \mathbb{Z}_m$ such that $x \cdot s \equiv 1 \pmod{m}$.*

Theorem 184 *The multiplicative inverse of a unit modulo m is unique.*

Remark: As the inverse of a unit r modulo m is unique, it will be denoted by r^{-1}.

Arithmetic with $\mathbb{Z}_m$ (3)

Theorem 185 *An element $r \in \mathbb{Z}_m$ is invertible (i.e., it has a multiplicative inverse) if and only if r and m are relatively primes.*

Definition 186
The set of invertible elements in $\mathbb{Z}_m$ will be denoted as U_m.

Corollary 187 *If p is a prime number, every nonzero element of $\mathbb{Z}_p$ is invertible.*

- If p is prime, then $(\mathbb{Z}_p, +, \cdot)$ is a **field** like $(\mathbb{R}, +, \cdot)$ or $(\mathbb{Q}, +, \cdot)$.
- If $m = p \cdot q$ is composite, then there are divisors of zero in $\mathbb{Z}_m$: $p \cdot q \equiv 0 \pmod{m}$ with $p, q \not\equiv 0 \pmod{m}$. In this case, $(\mathbb{Z}_m, +, \cdot)$ is a **ring with divisors of zero**.

Definition 188
Euler's (totient) function $\phi \colon \mathbb{N} \to \mathbb{N}$ *is defined as $\phi(m) = |U_m|$. In words, the value of Euler's function at a positive integer m is equal to the number of invertible elements of $\mathbb{Z}_m$.*

Lemma 189 *If p is a prime number, then $\phi(p) = p - 1$.*

Euler's theorem

Theorem 190 (Euler, 1790) *If y is invertible in $\mathbb{Z}_m$ (i.e., if $\gcd(y, m) = 1$), then*

$$y^{\phi(m)} \equiv 1 \pmod{m}.$$

Corollary 191 (Fermat's little theorem) *If p is a prime number and if $y \not\equiv 0 \pmod{p}$, then*

$$y^{p-1} \equiv 1 \pmod{p}.$$

Corollary 192 *If p is a prime number, then $y^p \equiv y \pmod{p}$ for any integer y.*

Theorem 193

1. *If p is a prime, then $\phi(p^k) = p^{k-1}(p-1)$ for every $k \in \mathbb{N}$.*
2. *If $\gcd(m, n) = 1$, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.*
3. *If $n \geq 2$ has the following decomposition in prime factors $n = \prod_{k=1}^{r} p_k^{n_k}$ with $n_k \geq 1$, then $\phi(n) = n \cdot \prod_{k=1}^{r}(1 - 1/p_k)$.*

Chapter 13. Order relations

1. Binary relations.
2. Equivalence relations.
3. Order relations:
   - Partially ordered sets.
   - Hasse diagrams.
   - Maximal elements.
   - Totally ordered sets.
   - Well-ordered sets and mathematical induction.
4. Lattices and Boolean algebras.

Partial order relation

Definition 194
A binary relation on a set V is a **partial order** *(or an* **order relation***) if it is reflexive, antisymmetric, and transitive.*

Notation: Order relations are usually denoted by the symbol $\preceq$.

Definition 195
A set V equipped with an order relation $\preceq$ is called a **partially ordered set** *$(V, \preceq)$ (or poset).*

Definition 196
Let $(V, \preceq)$ be a partially ordered set. Two elements $a, b \in V$ are **comparable** *if either $a \preceq b$ or $b \preceq a$. If none of these conditions holds, such elements are* **incomparable**.

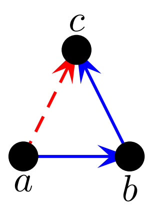
Definition 197
A partially ordered set $(V, \preceq)$ is **totally ordered** *when any pair of elements $a, b \in V$ are comparable. In this case, $(V, \preceq)$ is a* **totally ordered** *set (or* **linear order** *or* **chain***).*

Hasse diagrams, 1926

The directed graph associated to an order relation $\preceq$ can be simplified by eliminating redundant elements.

Algorithm to obtain the Hasse diagram for a partial order $\preceq$:

1. As $\preceq$ is reflexive, there is a loop incident with each vertex. We eliminate all these loops.
2. The transitivity of $\preceq$ implies the existence of subgraphs of the following type:

   If $a \preceq b$ and $b \preceq c$, we eliminate the superfluous edge associated to $a \preceq c$.
3. We choose that all the oriented edges point upwards. Then, we eliminate all the arrows.

Extremal elements

Definition 198
*Let $(V, \preceq)$ be a partially ordered set. $M \in V$ is a **maximal element** if for all $v \in V$, $M \preceq v$ implies that $M = v$. $m \in V$ is a **minimal element** if for all $v \in V$, $v \preceq m$ implies that $m = v$. In other words, in the Hasse diagram associated to $(V, \preceq)$, there is no element above M, and no element below m.*

Definition 199
*Let $(V, \preceq)$ be a partially ordered set. $M^\star \in V$ is a **maximum** (or **greatest element**) if $v \preceq M^\star$ for all $v \in V$. $m^\star \in V$ is a **minimum** (or **least element**) if $m^\star \preceq v$ for all $v \in V$. In other words, in the Hasse diagram associated to $(V, \preceq)$, $M^\star$ is above all the elements of V, and $m^\star$ is below all elements of V. The maximum and minimum of $(V, \preceq)$ are denoted by $\max(V)$ and min(V), respectively.*

Remark: The maximal, minimal, greatest, and/or least elements of $(V, \preceq)$ might not exist.

Theorem 200 *The maximum $M^\star$ of a partially ordered set $(A, \preceq)$, <u>if it exists</u>, is unique. In addition, the maximum of $(A, \preceq)$ is also a maximal element of it.*

Extremal elements (2)

Remark: The subsets of a partially ordered set $(V, \preceq)$ inherit the order $\preceq$.

Definition 201
*Let $(V, \preceq)$ a partially ordered set, and $B \subset V$. $u \in V$ is an **upper bound** of B if $b \preceq u$ for all $b \in B$. The set of the upper bounds of B is denoted by major(B).*
*$u^\star \in V$ is the **supremum** of B if it is the least upper bound of B: $u^\star =$ min(major(B)).*

*$d \in V$ is a **lower bound** of B if $d \preceq b$ for all $b \in B$. The set of all the lower bounds of B is denoted by minor(B).*
*$d^\star \in V$ is the **infimum** of B if it is the greatest lower bound of B: $d^\star = \max($minor$(B))$.*

Remark: It may happen that major$(B) = \emptyset$, minor$(B) = \emptyset$ and/or $\sup(B)$ and $\inf(B)$ do not exist.

Total order compatible with a partial order

Definition 202
*A total order $(V, \preceq_T)$ is **compatible** with the partial order $(V, \preceq_P)$ if for all $v, w \in V$, $v \preceq_P w$ implies that $v \preceq_T w$.*

Algorithm 203 (Topological sort)
procedure *TotalOrder($(V, \preceq_P)$: finite partially ordered set)*
$k = 1$
while $V \neq \emptyset$
begin
  v_k = *a minimal element of* $(V, \preceq_P)$
  $V \to V \setminus \{v_k\}$
  $k \to k + 1$
end

$v_1 \preceq_T v_2 \preceq_T \ldots \preceq_T v_n$ is a total order compatible with $(V, \preceq_P)$.

Well-ordered set

Definition 204
$(V, \preceq)$ is a **well-ordered set** *if $(V, \preceq)$ is a total order and any nonempty subset of V always has a minimum.*

Remarks:

- The set of natural numbers with the usual order $(\mathbb{N}, \leq)$ is a well-ordered set. This property is equivalent to the induction principle.
- The totally-ordered set $(\mathbb{Z}, \leq)$ is not a well-ordered set; but as $\mathbb{Z}$ is isomorphic to $\mathbb{N}$, we can choose another order $\preceq$ such that $(\mathbb{Z}, \preceq)$ is a well-ordered set.

The induction principle for the natural numbers

Definition 205 (Induction principle: weak version)
Let P be some property that satisfies the following conditions:

(1) Base step: $P(1)$ is true.

(2) Inductive step: If $P(k)$ is true for an arbitrary and fixed k, then $P(k+1)$ is true.

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

Remark: The hypothesis in the inductive step ($P(k)$ is true) is called the **induction hypothesis**. To perform the inductive step, one assumes the induction hypothesis, and then uses this assumption to prove that $P(k+1)$ is true.

Definition 206 (Induction principle: strong version)
Let P be some property that satisfies the following conditions:

(1) Base step: $P(1)$ is true.

(2) Inductive step: Given an arbitrary fixed k, if $P(m)$ is true for any $1 \leq m \leq k$, then $P(k+1)$ is true.

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

The induction principle for well-ordered sets

Proposition 207 (Strong induction principle for well-ordered sets) *Let $(V, \preceq)$ be a well-ordered set, and P be some property that satisfies the following conditions:*

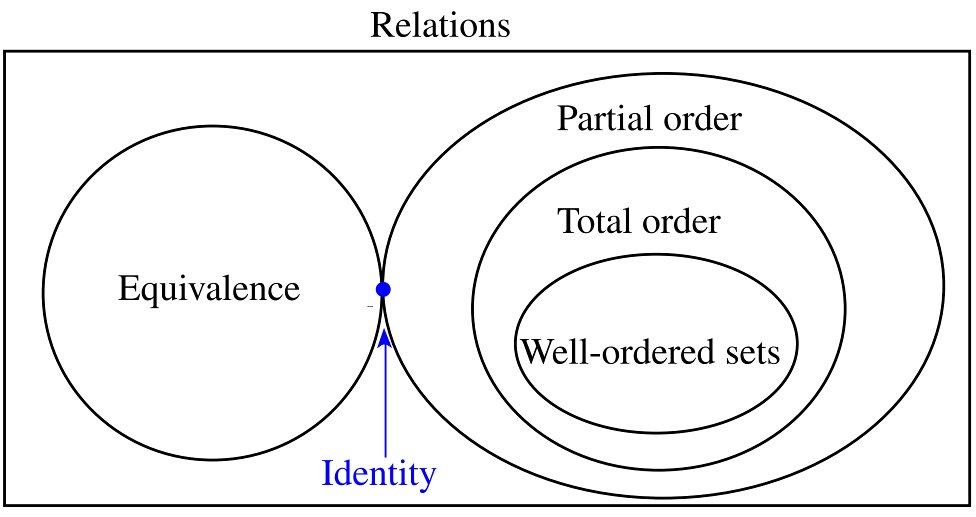
(1) Base step: $P(v_0)$ is true for $v_0 =$ min(V).

(2) Inductive step: Let w be an arbitrary fixed element of V, and let v be its successor. If $P(x)$ is true for all $v_0 \preceq x \preceq w$, then $P(v)$ is true.

Then, $P(v)$ is true for every $v \in V$.

Summary: types of relations

Relation	Reflexive	Symmetric	Antisymmetric	Transitive	
Equivalence	YES	YES	NO	YES	
Order	YES	NO	YES	YES	
Total order	YES	NO	YES	YES	Every pair is comparable
Well-ordered set	YES	NO	YES	YES	Every nonempty subset has a minimum



Chapter 14. Lattices and Boolean algebras

1. Binary relations.
2. Equivalence relations.
3. Order relations.
4. Lattices and Boolean algebras:
    - Definitions and properties.
    - Bounded lattices.
    - Distributive lattices.
    - Complemented lattices.
    - Boolean algebras.

Lattices

Definition 208
*A **lattice** is a nonempty partially ordered set* $(A, \preceq)$ *in which* $\sup(\{a, b\})$ *and* $\inf(\{a, b\})$ *exist for all* $a, b \in A$.

- If $\sup(a, b)$ and $\inf(a, b)$ exist, they are unique.
- If $(A, \preceq)$ is a lattice, both operations can be considered as binary operations on A: if $a, b \in A$
    - Their supremum is denoted by $\sup(a, b) = a \vee b \in A$.
    - Their infimum is denoted by $\inf(a, b) = a \wedge b \in A$.
- Not every partially ordered set is a lattice.
- A totally-ordered set is a lattice with $\sup(a, b) = \max(a, b)$ and $\inf(a, b) = \min(a, b)$.

Duality

- If $(A, \preceq)$ is a partially ordered set, then $(A, \succeq)$ is also a partially ordered set. The Hasse diagram of $(A, \succeq)$ is obtained by inverting the Hasse diagram of $(A, \preceq)$.
- If $(A, \preceq)$ is a lattice, then $(A, \succeq)$ is also a lattice, with the interchange $\sup \leftrightarrow \inf$.

Corollary 209 (Duality principle) *Any statement about a lattice $(A, \preceq)$ is still valid if we make the interchanges $\preceq \leftrightarrow \succeq$, $\sup \leftrightarrow \inf$, and $\vee \leftrightarrow \wedge$.*

- The lattices $(A, \preceq)$ and $(A, \succeq)$ are dual.
- The order relations $\preceq$ and $\succeq$ are dual.
- The operations $\vee$ and $\wedge$ are dual.

Lattice properties

Proposition 210 *If $(A, \preceq)$ is a lattice, then for any $a, b, c \in A$:*

1. $\sup(a, a) = a \vee a = a$ *[idempotent law]*
2. $\sup(a, b) = a \vee b = b \vee a = \sup(b, a)$ *[commutativity law]*
3. $\sup(a, \sup(b, c)) = a \vee (b \vee c) = (a \vee b) \vee c = \sup(\sup(a, b), c)$ *[associativity law]*
4. $\sup(a, \inf(a, b)) = a \vee (a \wedge b) = a$ *[absortion law]*

By duality, one obtains

Corollary 211 *If $(A, \preceq)$ is a lattice, then for any $a, b, c \in A$:*

1. $\inf(a, a) = a \wedge a = a$ *[idempotent law]*
2. $\inf(a, b) = a \wedge b = b \wedge a = \inf(b, a)$ *[commutativity law]*
3. $\inf(a, \inf(b, c)) = a \wedge (b \wedge c) = (a \wedge b) \wedge c = \inf(\inf(a, b), c)$ *[associativity law]*
4. $\inf(a, \sup(a, b)) = a \wedge (a \vee b) = a$ *[absortion law]*

Lattice properties (2)

Proposition 212 *If $(A, \preceq)$ is a lattice, then the following statements are equivalent for any $a, b \in A$:*

1. $a \preceq b$
2. $\sup(a, b) = a \vee b = b$
3. $\inf(a, b) = a \wedge b = a$

Proposition 213 (Distributive inequatities) *If $(A, \preceq)$ is a lattice, then for any $a, b, c \in A$:*

1. $\inf(a, \sup(b, c)) = a \wedge (b \vee c) \succeq (a \wedge b) \vee (a \wedge c) = \sup(\inf(a, b), \inf(a, c))$
2. $\sup(a, \inf(b, c)) = a \vee (b \wedge c) \preceq (a \vee b) \wedge (a \vee c) = \inf(\sup(a, b), \sup(a, c))$

Lattices as algebraic structures

Definition 214
A lattice is an algebraic structure $(A, \vee, \wedge)$ with two binary operations $\vee$ and $\wedge$ that satisfy the commutative, associative, and absorption laws.

- The absorption law implies the idempotent law.
- Even though we do not assume the existence of any order relation on A, there is one order relation induced by the properties of the operations $\vee$ and $\wedge$. In particular, for any $a, b \in A$,

$$a \preceq b \;\Leftrightarrow\; a \vee b = b\,.$$

  - $a \preceq a$ because $a \vee a = a$ (idempotent law).
  - If $a \preceq b \Leftrightarrow a \vee b = b$. If $b \preceq a \Leftrightarrow b \vee a = a$. Therefore, $a = b$.
  - If $a \preceq b \Leftrightarrow a \vee b = b$ and $b \preceq c \Leftrightarrow b \vee c = c$, then $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$. Therefore $a \preceq c$.
- In summary, $\preceq$ is a partial order relation and $(A, \preceq)$ is a partially ordered set.

Sublattices

Definition 215
Given a lattice $(A, \vee, \wedge)$, a **sublattice** $(M, \vee, \wedge)$ *of* $(A, \vee, \wedge)$ *is given by a nonempty subset $M \subseteq A$ such that $(M, \vee, \wedge)$ is also a lattice using the same operations as those used in $(A, \vee, \wedge)$. (In other words, $(M, \vee, \wedge)$ should be closed under the binary operations $\vee$ and $\wedge$.)*

- Any lattice is a sublattice of itself.

Bounded lattices

Definition 216
A lattice $(A, \preceq)$ has a **lower bound**, *denoted by 0, if $0 \preceq a$ for all $a \in A$. A lattice has an* **upper bound** *denoted by 1, if $a \preceq 1$ for all $a \in A$. A lattice is* **bounded** *if it contains a lower bound 0 and an upper bound 1.*

- The bounds 0 and 1 satisfy the following properties for all $a \in A$:
  - $\sup(a, 1) = a \vee 1 = 1$.
  - $\inf(a, 1) = a \wedge 1 = a$.
  - $\sup(a, 0) = a \vee 0 = a$.
  - $\inf(a, 0) = a \wedge 0 = 0$.
- The upper bound 1 is the identity element for $\wedge$: $a \wedge 1 = a$, and it satisfies $a \vee 1 = 1$.
- The lower bound 0 is the identity element for $\vee$: $a \vee 0 = a$, and it satisfies $a \wedge 0 = 0$.
- In a bounded lattice, we can extend the duality principle by considering the interchange $0 \leftrightarrow 1$.
- Any finite lattice A is bounded: $1 = \sup(A)$ and $0 = \inf(A)$.

Distributive lattices

Definition 217
A lattice $(A, \preceq)$ is a **distributive lattice** *if for all $a, b, c \in A$,*

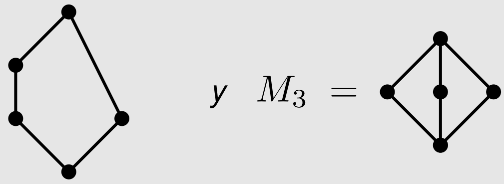
$$\begin{aligned}
\inf(a, \sup(b,c)) = a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) = \sup(\inf(a,b), \inf(a,c)) \\
\sup(a, \inf(b,c)) = a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) = \inf(\sup(a,b), \sup(a,c))
\end{aligned}$$

- This property is stronger than the distributive laws:

$$\begin{aligned}
\inf(a, \sup(b,c)) = a \wedge (b \vee c) &\succeq (a \wedge b) \vee (a \wedge c) = \sup(\inf(a,b), \inf(a,c)) \\
\sup(a, \inf(b,c)) = a \vee (b \wedge c) &\preceq (a \vee b) \wedge (a \vee c) = \inf(\sup(a,b), \sup(a,c))
\end{aligned}$$

Theorem 218 *A lattice is distributive if and only if it does* **not** *contain a sublattice that is isomorphic to any of the following two lattices:*

N_5 = *y* M_3 =



where N_5 is called the "pentagonal lattice", and M_3 is called the "diamond lattice".

Complemented lattices

Definition 219
Let $(A, \vee, \wedge, 0, 1)$ be a bounded lattice. An element $a \in A$ has a **complement** *$b \in A$ if $\sup(a,b) = a \vee b = 1$ and $\inf(a,b) = a \wedge b = 0$.*

- The bounds 0 and 1 are complements of each other.
- If a is a complement of b, then b is a complement of a.
- An element $a \in A$ may have no complements, or it may have several ones.
- The unique complement of 1 is 0, and vice versa.

Definition 220
A bounded lattice $(A, \vee, \wedge, 0, 1)$ is **complemented** *if for each $a \in A$ there is at least one complement.*

Proposition 221 *Let $(A, \vee, \wedge)$ be a distributive lattice. If an element $a \in A$ has a complement, this this elemenent is unique.*

- If $(A, \vee, \wedge)$ is a distributive and complemented lattice, then each element $a \in A$ has a **unique** complement. This element will be denoted by $\overline{a}$.

Boolean algebras

Definition 222 (Definition 1)
A **Boolean algebra** *is a bounded, distributive and complemented lattice* $(A, \vee, \wedge, ^{-}, 0, 1)$.

Definition 223 (Definition 2)
Let B be a nonempty set with at least two distinct elements $0, 1$. We define on B the following operations:

- *The (binary) Boolean sum $(a, b) \to a + b \in B$.*
- *The (binary) Boolean multiplication $(a, b) \to a \cdot b \in B$.*
- *The (unary) complementation $a \to \overline{a} \in B$.*

Then B is a **Boolean algebra** *if the following properties hold for all $a, b, c \in B$:*

1. $a + 0 = a$ *[identity w.r.t. the sum]*
2. $a \cdot 1 = a$ *[identity w.r.t. the multiplication]*
3. $a + b = b + a$, $a \cdot b = b \cdot a$ *[commutativity laws]*
4. $a + (b + c) = (a + b) + c$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *[associativity laws]*
5. $a + (b \cdot c) = (a + b) \cdot (a + c)$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *[distributive laws]*
6. $a + \overline{a} = 1$, $a \cdot \overline{a} = 0$ *[complement laws]*

Simple Boolean algebra

- We can drop the symbol $\cdot$ in the Boolean multiplication $a \cdot b = ab$ whenever there is no confusion.
- The elements $0, 1 \in A$ do **not** have to be equal to the numbers $0, 1 \in \mathbb{Z}$.
- The Boolean operations $+$ and $\cdot$ do **not** have to coincide with the sum and multiplication of real numbers.

Let $(B, +, \cdot, ^{-}, 0, 1)$ be an algebra with $B = \{0, 1\}$ and the operations $+$, $\cdot$, and $^{-}$ defined on B as follows:

$$
\begin{aligned}
1 \cdot 0 &= 0 \cdot 1 = 0 \cdot 0 = 0\,, \\
1 \cdot 1 &= 1\,, \\
1 + 1 &= 1 + 0 = 0 + 1 = 1\,, \\
0 + 0 &= 0\,, \\
\overline{1} &= 0\,, \\
\overline{0} &= 1\,.
\end{aligned}
$$

Then $(B, +, \cdot, ^{-}, 0, 1)$ is a Boolean algebra, and it is the simplest one that exists: the **Boolean algebra of two elements**.

General non-trivial Boolean algebras

Let A be a nonempty set. We now consider the power set $\mathcal{P}(A)$ with the order relation for every pair $B, C \subseteq A$.

$$B \preceq C \quad \Leftrightarrow \quad B \subseteq C\,.$$

- The set $(\mathcal{P}(A), \preceq)$ is a partially ordered set.
- The set $(\mathcal{P}(A), \preceq)$ is a lattice. Given $B, C \subseteq A$, then
  - $\sup(B, C) = B \cup C \subseteq A$ ($\vee \Rightarrow \cup$).
  - $\inf(B, C) = B \cap C \subseteq A$ ($\wedge \Rightarrow \cap$).
- The identities are
  - $1 = A$.
  - $0 = \emptyset$
- The set $(\mathcal{P}(A), \cup, \cap, \emptyset, A)$ is a distributive lattice.
- Each $B \subseteq A$ has a unique complement $\overline{B} = A \setminus B \subseteq A$.
- The set $(\mathcal{P}(A), \cup, \cap, \setminus, \emptyset, A)$ is a Boolean algebra.
- Practical use in probability theory.

Properties of a Boolean algebra

Proposition 224 *Let $(B, +, \cdot, \overline{}, 0, 1)$ be a Boolean algebra. Then, for all $a, b \in B$:*

1. *Idempotent laws: $a + a = a$ and $a \cdot a = a$.*
2. *Dominance laws: $a + 1 = 1$ and $a \cdot 0 = 0$.*
3. *Absortion laws: $a \cdot (a + b) = a$ and $a + a \cdot b = a$.*
4. *De Morgan laws: $\overline{(a + b)} = \overline{a} \cdot \overline{b}$ and $\overline{(a \cdot b)} = \overline{a} + \overline{b}$.*
5. *Involution law: $\overline{\overline{a}} = a$.*
6. *$\overline{1} = 0$ and $\overline{0} = 1$.*

Definition 225
Given a statement in a Boolean algebra, its **dual statement** *is obtained by interchanging $+ \leftrightarrow \cdot$ and $0 \leftrightarrow 1$ in the original statement.*

Proposition 226 *If a theorem is the consequences of the definitions of Boolean algebra, then the dual of the theorem is also a theorem.*

Definition 227
Let $(B, +, \cdot, \overline{}, 0, 1)$ be a Boolean algebra. Then a subset $C \subseteq B$ is a **Boolean subalgebra** *if $0, 1 \in C$, and it is closed under the same operations $+, \cdot, \overline{}$.*