Fundamentals of mathematics

1 | Introduction

Axiom 1.1 (Peano axioms).

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

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

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

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

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

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

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

2 | Set theory

Definitions and basic operations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

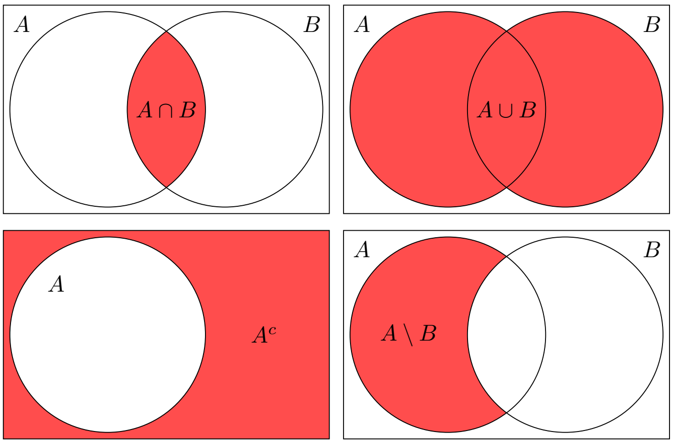

Figure 1: Venn diagrams

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

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

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

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

Functions between sets

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 | Logic and propositional calculus

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

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

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

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

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

4 | Symmetric group

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Corollary 1.58. The function

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

is a group morphism[3].

5 | Equivalence relations and order relations

Equivalence relations

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

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

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

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

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

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

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

[2] See definition ??.
[3] See definition ??.

Order relations

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

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

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

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

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

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

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

Theorem 1.68. All sets can be well-ordered.

6 | Cardinality and combinatorics

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

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

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

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

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

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

Corollary 1.74. There is no set containing all sets.

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

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

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

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

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

Proposition 1.79 (Binomial coefficient formulas).

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

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

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

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

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

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

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

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

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

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

7 | Arithmetic

Integer numbers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Modular arithmetic

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

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

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

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

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

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

is a ring morphism.

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

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

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

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

is ring isomorphism.

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

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

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

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

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

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

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

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

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

8 | Polynomials

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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