Linear Algebra and Analytic Geometry

Linear Mappings, Matrices, Determinants, Eigenvalue Theory, and Euclidean and Unitary Vector Spaces

Lucien Sina

Linear Algebra and Analytic Geometry

Linear Mappings, Matrices, Determinants, Eigenvalue Theory,

and Euclidean and Unitary Vector Spaces

Lucien Sina

10.5.2026

Contents

Preface

Linear algebra is one of the central foundations of modern mathematics and at the same time an indispensable tool in the natural sciences and engineering. Its concepts and methods appear in many areas in ever new forms—from the solution of systems of linear equations and geometric questions to deep structures in abstract algebra and analysis.

This book aims to present linear algebra and analytic geometry in a clear, structured, and at the same time comprehensive manner. It deliberately follows an approach that does not merely state the classical results, but develops the underlying structures step by step. Starting from elementary concepts such as sets and mappings, the central algebraic structures—groups, rings, and fields—are introduced gradually. On this foundation, vector spaces emerge as the natural framework of linear algebra.

A particular emphasis is placed on the systematic development of the theory of linear mappings and matrices. Concepts such as basis, dimension, kernel, and image are not treated in isolation, but are presented within a unified structural context. Building on this, eigenvalue theory is developed, offering deep insight into the internal structure of linear mappings.

Another central component is the study of Euclidean and unitary vector spaces. Here, geometric aspects come to the foreground: inner products, orthogonality, norms, and orthonormal bases connect algebraic concepts with intuitive geometry. Results such as the spectral theorem illustrate in an exemplary way how closely algebra and geometry are intertwined.

The book is designed to serve both as a companion text for a lecture course and as a resource for self-study. Numerous examples, exercises, and sample solutions are intended to deepen understanding and encourage active engagement with the concepts discussed.

A central aim of this work is not only to teach computational techniques, but also to foster an understanding of the structures on which they are based. Linear algebra is therefore not presented as a collection of isolated methods, but as a coherent mathematical system that connects many areas of mathematics.

Chapter 1

Sets and Mappings

Sets and mappings form the foundation of linear algebra and of most areas of mathematics.

1.1 Sets

A *set* is a collection of well-distinguished objects, which are called its *elements*. In the following, we introduce several standard notions and notations that will be used regularly later on.

Finite sets: Finite sets can be described by listing all their elements. For example, one writes

$$M := \{x_1, x_2, \ldots, x_n\}.$$

The symbol $:=$ means "is defined as". The symbols x_i are called *elements* of M; one writes $x_i \in M$ for $1 \leq i \leq n$.

The order in which the elements are listed is irrelevant, and repetitions are not counted: the expression $\{a, b, a\}$ denotes the same set as $\{a, b\}$. If the listed elements are pairwise distinct, that is, if $x_i \neq x_j$ for all $i \neq j$, then n is exactly the number of elements of M. The number of elements, or cardinality, of a finite set M is denoted by $|M|$.

Empty set: The empty set contains no elements and is denoted by $\varnothing$ (or $\{\}$).

Subsets: A set M' is called a subset of M, written $M' \subseteq M$, if and only if

$$\forall x \; (x \in M' \Rightarrow x \in M).$$

If $M' \subseteq M$ and $M' \neq M$, one writes $M' \subsetneq M$ and calls M' a proper subset of M. Two sets are equal if and only if each is a subset of the other:

$$M = N \quad \Longleftrightarrow \quad M \subseteq N \;\text{ and }\; N \subseteq M.$$

Set-builder notation: Sets are often defined by means of a property:

$$\{\, x \in X \mid P(x) \,\}$$

This is read as "the set of all x in X for which the property $P(x)$ holds". For example: $\{n \in \mathbb{Z} \mid n \text{ is even}\}$.

Infinite sets and the natural numbers: The best-known simple infinite set is the set of natural numbers. Here we use the convention

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}.$$

The structure of $\mathbb{N}$ can be described axiomatically by the *Peano axioms* (in one common formulation):

1. $0 \in \mathbb{N}$.
2. There is a mapping $S : \mathbb{N} \to \mathbb{N}$, called the *successor map*, which assigns to each n its successor $S(n)$.
3. 0 is not a successor: $\forall n \in \mathbb{N} : \; S(n) \neq 0$.
4. The successor map is injective: $\forall m, n \in \mathbb{N} : S(m) = S(n) \Rightarrow m = n$.
5. (Induction axiom) If $K \subseteq \mathbb{N}$, $0 \in K$, and $\forall n \in K : S(n) \in K$, then $K = \mathbb{N}$.

The Peano axioms describe the basic structure of the natural numbers: there is a distinguished starting point 0, every number has a unique successor, and induction makes it possible to derive properties for all natural numbers. (Some authors let the natural numbers begin with 1 instead of 0; this changes some formulations, but not the underlying theory.)

Remark: The concepts and notations used here—set notation with braces, $\in$, $\subseteq$, $|M|$, $\varnothing$, and set-builder notation—occur constantly in linear algebra; becoming comfortable with them greatly facilitates later work.

1.1.1 Number Systems and Their Extensions

Starting from the natural numbers, one obtains further number systems that are important for analysis and linear algebra by means of systematic extensions.

Integers: The set of integers is defined by

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Intuitively, $\mathbb{Z}$ is obtained from $\mathbb{N}$ by adjoining, for each positive n, a negative element $-n$. Formally, one may interpret $\mathbb{Z}$ as a set of equivalence classes of pairs of natural numbers (a, b), where (a, b) represents the difference $a - b$.

Rational numbers: The rational numbers are the "fractions" of integers:

$$\mathbb{Q} := \{\, p/q \mid p, q \in \mathbb{Z},\ q \neq 0 \,\}.$$

Here, too, there is a formal construction by equivalence classes of pairs (p, q), with the equivalence relation $(p, q) \sim (p', q')$ precisely when $pq' = p'q$. The set $\mathbb{Q}$ is a field (that is, the usual arithmetic rules for $+, \cdot$ hold, except for division by 0) and is dense in $\mathbb{R}$: between any two real numbers there is always a rational number.

Real numbers: The real numbers $\mathbb{R}$ contain $\mathbb{Q}$ and provide the appropriate setting for limits, continuity, and classical analysis. There are several equivalent constructions of $\mathbb{R}$; two of the most common are

- *Dedekind cuts*: a real number is interpreted as a cut (partition) of the rational numbers into two nonempty sets A, B with $a < b$ for all $a \in A,\ b \in B$.

- *Completion by Cauchy sequences*: one considers Cauchy sequences of rational numbers and forms equivalence classes according to equality of limits.

Intuitively, real numbers appear through decimal expansions (for example $3{,}14159\ldots$ for π); not all such expansions are finite or periodic—those that are not are called *irrational* (for example $\sqrt{2}, \pi$). A central property of $\mathbb{R}$ is *completeness*: every nonempty subset of $\mathbb{R}$ that is bounded above has a least upper bound (supremum).

Complex numbers: The complex numbers are defined as

$$\mathbb{C} := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{R},\ \mathrm{i}^2 = -1\}$$

One may also regard $\mathbb{C}$ as pairs (a, b) equipped with suitable addition and multiplication. The set $\mathbb{C}$ is a field, but not an ordered field (there is no compatible total order relation that is compatible with addition and multiplication). An important result (stated here without proof) is the Fundamental Theorem of Algebra: every nonconstant polynomial with complex coefficients has at least one zero in $\mathbb{C}$; thus $\mathbb{C}$ is algebraically closed.

Chain of inclusions: These number systems are related by the following natural chain of embeddings:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Each inclusion is proper; for example, $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, and $\mathrm{i} \in \mathbb{C} \setminus \mathbb{R}$.

Algebraic and order-theoretic properties:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are closed under $+$ and $\cdot$; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
- $\mathbb{Q}$ is dense in $\mathbb{R}$: between any two real numbers one can find rational numbers.
- $\mathbb{R}$ is, up to isomorphism, the unique complete ordered field; this completeness explains why many analytic statements, such as the existence of limits, hold in $\mathbb{R}$ but not already in $\mathbb{Q}$.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countably infinite, whereas $\mathbb{R}$ and $\mathbb{C}$ have uncountable cardinality.

Didactic note: On a first reading, it is often helpful for students to keep the motivation for each extension clearly in view:

- $\mathbb{Z}$ is introduced so that subtraction can always be carried out;
- $\mathbb{Q}$ is introduced to make division possible, except by 0;
- $\mathbb{R}$ is introduced to complete limits and limiting processes, for instance limits of sequences;
- $\mathbb{C}$ is introduced to represent polynomial factors completely and to complete the algebraic structure.

Short examples, such as $2-5$, which requires $\mathbb{Z}$, the equation $2x = 1$, which requires $\mathbb{Q}$, or the sequence $1, 1.4, 1.41, 1.414, \ldots$, which leads to $\sqrt{2} \in \mathbb{R}$, make these transitions tangible for students.

1.1.2 Elementary Set Operations

Starting from a given set M, many subsets can be formed by selecting elements according to specified properties. The *power set* $\mathcal{P}(M)$ denotes the set of all subsets of M.

Subset defined by a property (set-builder notation): If M is a set and $E(x)$ is a property of x, one defines

$$M' := \{\, x \in M \mid E(x) \,\},$$

read as "the set of all x in M for which $E(x)$ holds". Example: $\{n \in \mathbb{N} \mid n \text{ is prime}\}$.

Union and intersection (finite and indexed forms): Let $M_1, \dots, M_n$ be sets. Their union and intersection are defined by

$$M_1 \cup \cdots \cup M_n := \{x \mid \exists i \in \{1, \dots, n\} : \; x \in M_i\},$$

$$M_1 \cap \cdots \cap M_n := \{x \mid \forall i \in \{1, \dots, n\} : \; x \in M_i\}.$$

For families $(X_i)_{i \in I}$ of sets indexed by an index set I, one uses the standard notation for indexed unions and intersections:

$$\bigcup_{i \in I} X_i := \{x \mid \exists i \in I : \; x \in X_i\},$$
$$\bigcap_{i \in I} X_i := \{x \mid \forall i \in I : \; x \in X_i\}.$$

Example with intervals: Let $I = \mathbb{N}$, using the convention introduced above that $\mathbb{N} = \{0, 1, 2, \dots\}$, and let $X_i := [-i, i] \subset \mathbb{R}$. Then

$$\bigcup_{i \in \mathbb{N}} [-i, i] = \mathbb{R},$$

because for every real number x there exists an i such that $|x| \leq i$. On the other hand,

$$\bigcap_{i \in \mathbb{N}} [-i, i] = [-0, 0] = \{0\},$$

because $X_0 = [0, 0] = \{0\}$ is already included in the intersection. (If one instead lets $\mathbb{N}$ begin with 1, that is, if $I = \{1, 2, \dots\}$, then $\bigcap_{i \geq 1} [-i, i] = [-1, 1]$.)

Difference and complement: If $X' \subseteq X$, then

$$X \setminus X' := \{\, x \in X \mid x \notin X' \,\}$$

is called the *difference* of X and X'. The *complement* of a set A is always taken with respect to a reference set, or universe, U; one writes

$$A^{\complement} := U \setminus A = \{\, x \in U \mid x \notin A \,\}.$$

Further useful operations: The *symmetrical difference* (or *symmetric difference*) of A and B is

$$A \triangle B := (A \setminus B) \cup (B \setminus A),$$

that is, the set of precisely those elements that belong to exactly one of the two sets, but not to both.

Basic algebraic rules for sets: For sets A, B, C, the following elementary laws hold and are useful for transformations and proofs:

- *Commutativity:* $A \cup B = B \cup A, \quad A \cap B = B \cap A.$
- *Associativity:* $(A \cup B) \cup C = A \cup (B \cup C)$, and analogously for $\cap$.
- *Idempotence:* $A \cup A = A, \quad A \cap A = A.$
- *Distributivity:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- *De Morgan's laws (also for indexed families):*

$$\Big(\bigcup_{i \in I} X_i\Big)^{\complement} = \bigcap_{i \in I} X_i^{\complement}, \qquad \Big(\bigcap_{i \in I} X_i\Big)^{\complement} = \bigcup_{i \in I} X_i^{\complement}.$$

- *Difference rules:* $A \setminus B = A \cap B^{\complement}$. Moreover, $(A \setminus B) \cup (B \setminus A) = A \triangle B$.

1.2 Mappings

Mappings are used to describe relations between sets.

Definition 1. *Let X and Y be sets. A* mapping *(or* function*) from X to Y is a rule f that assigns to each $x \in X$ exactly one element $f(x) \in Y$. We write*

$$f : X \to Y, \qquad x \mapsto f(x).$$

Here $\to$ connects sets (the domain and the codomain), whereas $\mapsto$ describes the assignment of an element x to $f(x)$.

Definition 2. *Two mappings $f, g : X \to Y$ are called equal, written $f = g$, if and only if*

$$\forall x \in X : \; f(x) = g(x).$$

The set of all mappings from X to Y is denoted by $\mathrm{Abb}(X, Y)$ *(one also writes* $\mathrm{Fun}(X, Y)$*).*

1.2.1 Image and Preimage

Mappings allow us to assign not only individual elements, but also subsets of one set to subsets of another.

Definition 3 (Image)**.** *Let $f : X \to Y$ be a mapping and let $M \subseteq X$ be a subset. The* image *of M under f is*

$$f(M) := \{\, y \in Y \mid \exists x \in M : \; y = f(x) \,\}.$$

In particular, $f(\{x\}) = \{f(x)\}$ for $x \in X$, and $f(X) \subseteq Y$ is also called the range *or* image *of f.*

Definition 4 (Preimage)**.** *Let $f : X \to Y$ be a mapping and let $N \subseteq Y$. The* preimage *of N is*

$$f^{-1}(N) := \{\, x \in X \mid f(x) \in N \,\} \subseteq X.$$

For a single element $y \in Y$, one often writes $f^{-1}(\{y\})$ or simply $f^{-1}(y)$ for the set of all $x \in X$ such that $f(x) = y$.

Important: Here f^{-1} denotes a mapping on subsets (an operation $\mathcal{P}(Y) \to \mathcal{P}(X)$), not necessarily a mapping in the sense $Y \to X$. The preimage of a one-element set may contain several elements or may be empty.

Examples:

- The identity mapping $\mathrm{id}_X : X \to X$, defined by $\mathrm{id}_X(x) = x$, has image $\mathrm{id}_X(M) = M$ and preimage $\mathrm{id}_X^{-1}(M) = M$ for every subset $M \subseteq X$.

- A constant mapping with $f(x) = y_0$ for all $x \in X$ has image $\{y_0\}$; the preimage of any $y \neq y_0$ is empty, and $f^{-1}(\{y_0\}) = X$.

- Example of strict inclusion for intersections and images: Let $X = \{1, 2\}$, $Y = \{a\}$, and $f(1) = f(2) = a$. Then $M_1 = \{1\}$ and $M_2 = \{2\}$ satisfy $f(M_1) \cap f(M_2) = \{a\}$, but $f(M_1 \cap M_2) = f(\varnothing) = \varnothing$. Hence, in general, one only has

  $$f(M_1 \cap M_2) \subseteq f(M_1) \cap f(M_2),$$

  and the inclusion can be strict.

Important Rules of Calculation: Let $f : X \to Y$ be a mapping, let $(M_i)_{i \in I}$ be a family of subsets of X, and let $(N_j)_{j \in J}$ be a family of subsets of Y. Then the following rules hold:

$$f\left(\bigcup_{i \in I} M_i\right) = \bigcup_{i \in I} f(M_i),$$

$$f\left(\bigcap_{i \in I} M_i\right) \subseteq \bigcap_{i \in I} f(M_i),$$

$$f^{-1}\left(\bigcup_{j\in J} N_j\right) = \bigcup_{j\in J} f^{-1}(N_j),$$
$$f^{-1}\left(\bigcap_{j\in J} N_j\right) = \bigcap_{j\in J} f^{-1}(N_j),$$
$$f^{-1}(Y \setminus N) = X \setminus f^{-1}(N),$$
$$f(\varnothing) = \varnothing.$$

The first identity shows that images are compatible with unions; for intersections, however, one generally only has the inclusion in the direction indicated by $\subseteq$ (with equality, for example, if f is injective). Preimages, on the other hand, commute with both unions and intersections. Thus preimages behave particularly well with respect to set operations: the preimage of a union is the union of the preimages, and the preimage of an intersection is the intersection of the preimages. By contrast, for images one generally obtains only an inclusion in the case of intersections.

1.2.2 Restriction and Extension

Definition 5 (Restriction)**.** *Let $f : X \to Y$ and let $M \subseteq X$. The* restriction *of f to M is the mapping*

$$f|_M : M \to Y, \qquad x \mapsto f(x).$$

Remark on extending the codomain: If $Y \subseteq Y'$ and $f : X \to Y$, then f may also be regarded as a mapping

$f : X \to Y'$ with the same values but with a larger codomain. In this sense, one speaks of an extension of the codomain.

1.2.3 Properties

Definition 6. *A mapping* $f\colon X \to Y$ *is called*

- injective *(or* one-to-one*) if*

$$\forall x, x' \in X : \quad f(x) = f(x') \implies x = x'.$$

- surjective *(or* onto*) if*

$$f(X) = Y \quad \iff \quad \forall y \in Y\ \exists x \in X :\ y = f(x).$$

- bijective *if f is both injective and surjective.*

1.2.4 Inverse Mapping

If $f\colon X \to Y$ is bijective, then for every $y \in Y$ there exists exactly one $x \in X$ such that $f(x) = y$. In this case, one defines the *inverse mapping*

$$f^{-1}\colon Y \to X, \qquad y \mapsto f^{-1}(y),$$

so that $f^{-1}(f(x)) = x$ for all $x \in X$ and $f(f^{-1}(y)) = y$ for all $y \in Y$.

Important: One must not confuse the two meanings of f^{-1}:

- For an arbitrary mapping f and a subset $N \subseteq Y$, the notation $f^{-1}(N)$ denotes the *preimage* of N, namely

$$f^{-1}(N) = \{x \in X \mid f(x) \in N\} \subseteq X.$$

  This is an operation $\mathcal{P}(Y) \to \mathcal{P}(X)$.

- If f is bijective, then f^{-1} additionally denotes the *inverse mapping* $Y \to X$. In this case, the preimage of a singleton is the singleton consisting of the corresponding inverse image:

$$f^{-1}(\{y\}) = \{\, f^{-1}(y) \,\} \qquad (y \in Y).$$

1.2.5 Theorem (Injectivity ⇔ Surjectivity on Finite Sets)

Theorem 7. *Let X be a finite set and let $f\colon X \to X$ be a mapping. Then the following statements are equivalent:*

1. *f is injective.*

2. *f is surjective.*

3. *f is bijective.*

Proof. Let $X = \{x_1, \ldots, x_n\}$, where the elements x_i are pairwise distinct and $n \in \mathbb{N}$.

$(\mathbf{1}) \Rightarrow (\mathbf{2})$: Suppose that f is injective. Then the images $f(x_1), \ldots, f(x_n)$ are pairwise distinct. Hence the set $f(X) = \{f(x_1), \ldots, f(x_n)\}$ has exactly n elements. Since

$f(X) \subseteq X$ and X also has n elements, it follows that $f(X) = X$. Thus f is surjective.

$(\mathbf{2}) \Rightarrow (\mathbf{1})$: Suppose that f is surjective, so that $f(X) = X$. If f were not injective, then there would exist $x_i \neq x_j$ with $f(x_i) = f(x_j)$. In that case the image would contain at most $n-1$ elements, that is, $|f(X)| \leq n-1$. This contradicts the assumption $f(X) = X$, since $|X| = n$. Therefore f must be injective.

The equivalence with (3) is now immediate, because bijectivity means precisely that both injectivity and surjectivity hold. Hence (1), (2), and (3) are equivalent. □

Remark: For infinite sets, this statement does not hold in general: on $\mathbb{N}$ there are injective but not surjective mappings, for example $n \mapsto n+1$, and there are also surjective but not injective mappings, depending on the construction. Finiteness is therefore the decisive assumption in this theorem. A short rule to remember is: *For finite sets, injectivity and surjectivity are equivalent.*

1.2.6 Composition

Definition 8. *Let X, Y, Z be sets and let $f\colon X \to Y$, $g\colon Y \to Z$ be mappings. The* composition *of f and g is the mapping*

$$g \circ f\colon X \longrightarrow Z, \qquad (g \circ f)(x) := g(f(x)).$$

One reads $g \circ f$ as "g composed with f"; first f is applied, then g. In diagrammatic notation:

$$X \xrightarrow{f} Y \xrightarrow{g} Z \qquad \textit{or equivalently} \qquad Z \xleftarrow{g} Y \xleftarrow{f} X.$$

Theorem 9 (Associativity of Composition)**.** *For mappings $f\colon X \to Y$, $g\colon Y \to Z$, and $h\colon Z \to W$, one has*

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

Proof. Let $x \in X$. Then

$$\begin{aligned}
\big((h \circ g) \circ f\big)(x) &= (h \circ g)(f(x)) \\
&= h\big(g(f(x))\big) \\
&= h\big((g \circ f)(x)\big) \\
&= \big(h \circ (g \circ f)\big)(x).
\end{aligned}$$

Since both sides agree for every $x \in X$, the two mappings are equal. □

Theorem 10 (Non-commutativity in General)**.** *The composition of mappings is, in general,* not *commutative; that is, one usually has $g \circ f \neq f \circ g$.*

Example. Consider $X = Y = Z = \mathbb{R}$ and the mappings

$$f(x) = x + 1, \qquad g(x) = 2x \quad (x \in \mathbb{R}).$$

Then, for all $x \in \mathbb{R}$,

$$(g \circ f)(x) = g(f(x)) = g(x + 1) = 2(x + 1) = 2x + 2,$$

whereas

$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 1.$$

Since $2x + 2 \neq 2x + 1$ (for instance, at $x = 0$), the mappings $g \circ f$ and $f \circ g$ are different. This proves the claim. $\square$

Remark 11.

- *Remember:* $\circ$ *is* associative *but not* commutative. *Hence the notation* $h \circ g \circ f$ *is unambiguous even without parentheses.*

- *The order of execution is important:* $g \circ f$ *means first* f*, then* g*. Practice this with simple computational examples until the order becomes intuitive.*

- *Later, we shall study the relationship between composition and identity/inverse mappings in more detail.*

1.2.7 Identity and Inverses

Definition 12. *For every set* X*, the* identity mapping *is the mapping*

$$\mathrm{id}_X \colon X \longrightarrow X, \qquad \mathrm{id}_X(x) := x \quad (x \in X).$$

Theorem 13. *Let* $f \colon X \to Y$ *be a mapping with* $X, Y \neq \varnothing$*. Then the following statements hold:*

1. f *is injective* $\Longleftrightarrow$ *there exists* $g \colon Y \to X$ *such that* $g \circ f = \mathrm{id}_X$*.*

2. *f is surjective $\iff$ there exists $g\colon Y \to X$ such that $f \circ g = \mathrm{id}_Y$.*

3. *f is bijective $\iff$ there exists $g\colon Y \to X$ such that*

$$g \circ f = \mathrm{id}_X \quad \textit{and} \quad f \circ g = \mathrm{id}_Y.$$

In this case, g is unique and is called the inverse mapping, *or simply the* inverse, *of f; one writes $g = f^{-1}$.*

Proof. **(1)** "$\Rightarrow$": Suppose that f is injective. Choose a fixed element $x_0 \in X$ (possible because $X \neq \varnothing$). Define $g\colon Y \to X$ by

$$g(y) := \begin{cases} \text{the unique } x \in X \text{ with } f(x) = y, & y \in f(X), \\ x_0, & y \notin f(X). \end{cases}$$

This definition is well-defined because, for $y \in f(X)$, injectivity implies that there is exactly one x with $f(x) = y$. For all $x \in X$, we then have

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

and hence $g \circ f = \mathrm{id}_X$.

"$\Leftarrow$": Suppose that $g\colon Y \to X$ satisfies $g \circ f = \mathrm{id}_X$. If $f(x) = f(x')$, then

$$x = \mathrm{id}_X(x) = g(f(x)) = g(f(x')) = \mathrm{id}_X(x') = x',$$

so $x = x'$. Thus f is injective.

(2) "$\Rightarrow$": Suppose that f is surjective. For each $y \in Y$, choose (once and for all) an element $x_y \in X$ with $f(x_y) = y$, and set $g(y) := x_y$. Then $f(g(y)) = y$ for all $y \in Y$, and hence $f \circ g = \mathrm{id}_Y$.

"$\Leftarrow$": Suppose that $g\colon Y \to X$ satisfies $f \circ g = \mathrm{id}_Y$. Then, for every $y \in Y$, we have $y = f(g(y))$, so $y \in f(X)$. Hence $f(X) = Y$, and f is surjective.

Remark on (2): Constructing such a g from a surjective mapping f means choosing, for each $y \in Y$, a preimage $x_y \in f^{-1}(\{y\})$. In finite or constructive situations this causes no difficulty; for arbitrary sets, however, the general statement that "every surjection has a right inverse" relies on a choice function and is therefore connected with the *axiom of choice*.

(3) If f is bijective, then the inverse mapping f^{-1} exists, and we immediately have

$$f^{-1} \circ f = \mathrm{id}_X, \qquad f \circ f^{-1} = \mathrm{id}_Y.$$

Conversely, the two identities, together with parts (1) and (2), imply that f is injective and surjective, hence bijective.

Uniqueness of the inverse: If $g, h\colon Y \to X$ both satisfy the two identities, then

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h,$$

so $g = h$. Thus the inverse is unique. $\square$

Remark 14.

- *The notions of a* left inverse *(for a map g with $g \circ f = \mathrm{id}_X$) and a* right inverse *(for a map g with $f \circ g = \mathrm{id}_Y$) are useful: injectivity $\iff$ existence of a left inverse, and surjectivity $\iff$ existence of a right inverse.*
- *The existence of a right inverse for a surjection requires choosing, for each y, one preimage; for infinite sets, this is a point at which the axiom of choice may become relevant.*
- *One should be careful with notation: in general, f^{-1} denotes the preimage operation on subsets. For bijections, f^{-1} is also used for the inverse function $Y \to X$.*

1.2.8 Further Concepts

Definition 15 (Ordered Tuples / Choice Functions)**.** *Let $X_1, \ldots, X_n$ be sets. An* ordered n-tuple *is an expression*

$$x = (x_1, \ldots, x_n)$$

with $x_i \in X_i$ for $i = 1, \ldots, n$. One may regard x as a function

$$x : \{1, \ldots, n\} \longrightarrow X_1 \cup \cdots \cup X_n, \qquad i \mapsto x(i) = x_i,$$

and in this sense, x is sometimes also called a choice function*, since for each label i an element x_i of X_i is selected. Often one also writes briefly $x_i := x(i)$, or informally $x = \{x_1, \ldots, x_n\}$ (the latter notation only informally).*

Remark 16. *Two tuples are equal if and only if all their components agree:*

$$(x_1, \dots, x_n) = (x'_1, \dots, x'_n) \iff x_1 = x'_1,\ \dots,\ x_n = x'_n.$$

Thus the order of the components is relevant, unlike for sets.

Definition 17 (Cartesian Product / Direct Product)**.** *The* Cartesian product*, or* direct product*, of the sets* $X_1, \dots, X_n$ *is*

$$X_1 \times \cdots \times X_n := \{(x_1, \dots, x_n) \mid x_i \in X_i \text{ for } i = 1, \dots, n\}.$$

In the special case $X_1 = \cdots = X_n = X$*, one writes* $X^n := X \times \cdots \times X$*.*

Proposition 18. *If n is finite, then*

$$X_1 \times \cdots \times X_n \neq \varnothing \iff X_i \neq \varnothing \text{ for all } i.$$

Remark 19. *For infinite families* $(X_i)_{i \in I}$*, the reverse implication* $\left(\prod_{i \in I} X_i \neq \varnothing \Rightarrow X_i \neq \varnothing\ \forall i\right)$ *always holds. The forward implication* $\left(X_i \neq \varnothing\ \forall i \Rightarrow \prod_{i \in I} X_i \neq \varnothing\right)$*, however, generally holds only by using the* axiom of choice*. This is an important, though often technical, distinction: finite products do not require the axiom of choice, whereas products with arbitrarily many factors generally do.*

Definition 20 (Projections)**.** *For each* $i \in \{1, \dots, n\}$*, the i-th* projection *is defined by*

$$\pi_i : X_1 \times \cdots \times X_n \longrightarrow X_i, \qquad \pi_i(x_1, \dots, x_n) := x_i.$$

Remark 21. *If $X_1 \times \cdots \times X_n \neq \varnothing$, then π_i is surjective onto X_i: for every $y \in X_i$, there exists a tuple in $X_1 \times \cdots \times X_n$ whose i-th component is y. For finite products, the remaining components can be chosen arbitrarily; for infinite products, constructing such tuples may require the axiom of choice.*

Definition 22 (Families and Sequences)**.** *Let I be an arbitrary set, called an index set. A mapping*

$$\varphi : I \longrightarrow X, \qquad i \mapsto x_i = \varphi(i),$$

is called a family *of elements of X. The family is usually denoted by $(x_i)_{i \in I}$. If $I = \mathbb{N}$, then $(x_i)_{i \in \mathbb{N}}$ is called a* sequence*.*

Remark 23. *In contrast to a subset $X' \subseteq X$, a family $(x_i)_{i \in I}$ also records the assignment of indices i to elements x_i:*

- *The same element may occur more than once, for example $x_i = x_j$ with $i \neq j$.*
- *The order, or more generally the labels i, are part of the data.*
- *The image $\varphi(I) = \{x_i \mid i \in I\}$ is a subset of X, but passing to this subset generally loses the information about the indexing.*

Definition 24 (Choice Function)**.** *Let $\mathcal{C}$ be a set of nonempty sets, for example $\mathcal{C} = \{X_i\}_{i \in I}$. A* choice function *is a mapping*

$$c : \mathcal{C} \longrightarrow \bigcup \mathcal{C}, \qquad C \mapsto c(C) \in C,$$

which assigns to each set $C \in \mathcal{C}$ an element $c(C) \in C$.

Remark 25. *The assertion that every family of nonempty sets admits a choice function is precisely the* axiom of choice. *This axiom has already appeared in the discussion of inverse mappings and products, and it plays a fundamental role in many areas of mathematics. For many practical purposes, however, especially in finite constructions, it is not needed.*

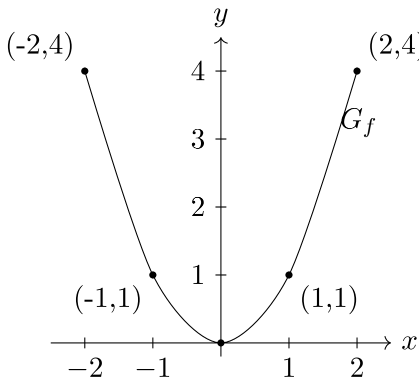
1.2.9 Graphs and Relations

Definition 26 (Graph of a mapping)**.** *Let $f : X \to Y$ be a mapping. The* graph *of f is the set*

$$G_f := \{\, (x, f(x)) \in X \times Y \mid x \in X \,\} \subseteq X \times Y.$$

Thus the graph G_f is precisely the set of all ordered pairs that indicate which element $y \in Y$ is assigned to each element $x \in X$. A mapping f can be described completely by its graph, and conversely.

Graphical representation: Typically, one draws the graph G_f in a coordinate system, marking each pair $(x, f(x))$ as a point in the (x, y)-plane. A simple example for visualization is the mapping $f(x) = x^2$, restricted to a small selection of x-values. The following example shows such a schematic representation:



Projection onto the first component: Consider the projection

$$\pi_X : X \times Y \longrightarrow X, \qquad \pi_X(x, y) := x.$$

The restriction $\pi_X|_{G_f} : G_f \to X$ is bijective:

- *Surjective:* For every $x \in X$, the pair $(x, f(x)) \in G_f$ belongs to the graph; hence $\pi_X|_{G_f}$ reaches every element x.

- *Injective:* If $\pi_X(x, f(x)) = \pi_X(x', f(x'))$, then $x = x'$. Since the pairs in the graph are uniquely determined by their first component, it follows that $(x, f(x)) = (x', f(x'))$.

Intuitively, the projection onto X "ignores" the second component; however, on the graph this produces a one-to-one correspondence between points of the graph and elements of X.

No overhang / vertical line test: The graph G_f of a mapping never has an "overhang" in the sense that several different y-values occur in the graph for the same x-value. Formally, for every $x \in X$ there exists exactly one $y \in Y$ such that $(x, y) \in G_f$. Geometrically, this means that no vertical line $x = \text{const}$ intersects the graph more than once; this is the familiar *vertical line test*.

Definition 27 (Relation)**.** *A* relation *on a set X is a subset $R \subseteq X \times X$. If $(x, y) \in R$, one often writes $x \sim_R y$, or simply $x \sim y$, and says that "x is related to y".*

Examples of relations: In each case, choose the set X appropriately.

1. The relation $\leq$ on $\mathbb{R}$: $(x, y) \in R$ if and only if $x \leq y$.
2. The divisibility relation $|$ on $\mathbb{N}$: $(a, b) \in R$ if and only if a divides b.
3. The relation "having the same length" on the set of all words over an alphabet: $(u, v) \in R$ if and only if $|u| = |v|$.

1.2.10 Equivalence Relations

Definition 28 (Equivalence relation)**.** *A relation $\sim$ on X is called an* equivalence relation *if, for all $x, y, z \in X$, the following properties hold:*

1. *(Reflexivity) $x \sim x$.*

2. *(Symmetry)* $x \sim y \Rightarrow y \sim x$.

3. *(Transitivity)* $x \sim y$ *and* $y \sim z \Rightarrow x \sim z$.

Examples of equivalence relations:

1. Equality $=$ on any set X.

2. Congruence modulo n on $\mathbb{Z}$: $a \equiv b \pmod{n}$ if and only if n divides $a - b$.

3. "Belonging to the same block of a partition": if X is partitioned into disjoint blocks (subsets), then two elements are equivalent if they lie in the same block.

1.2.11 Exercise

Let $X = \{1, 2, 3, 4\}$. For each of the following relations on X, determine whether it is an equivalence relation. Justify your answer.

1. $R_1 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1)\}$.

2. $R_2 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,3)\}$.

3. $R_3 = \{(a,b) \in X \times X \mid a \equiv b \pmod{2}\}$ ("same parity").

Sample solutions:

1. *Checking reflexivity, symmetry, and transitivity:* Reflexivity: All pairs (x, x) for $x \in X$ are present $\Rightarrow$ the relation is reflexive. Symmetry: $(1, 2)$ belongs to R_1, and $(2, 1)$ also belongs to R_1. For all other non-diagonal pairs, symmetry is satisfied as well, since the only non-diagonal pair is $1 \leftrightarrow 2$. Hence R_1 is symmetric. Transitivity: Consider the critical chains: $1 \sim 2$ and $2 \sim 1$ imply $1 \sim 1$, which is present. There is no chain such as $1 \sim 2$ and $2 \sim 3$, so no required pair is missing. Thus R_1 is transitive. $\Rightarrow$ R_1 is an equivalence relation; its equivalence classes are $\{1, 2\}$, $\{3\}$, and $\{4\}$.

2. Reflexivity: Yes, all pairs (x, x) are present. Symmetry: $(1, 2) \in R_2$, but $(2, 1) \notin R_2$. Hence R_2 is not symmetric $\Rightarrow$ it is not an equivalence relation. (Therefore, a complete check of the remaining properties is unnecessary.)

3. *Same parity (even/odd):* Reflexive: $a \equiv a \pmod 2$ for every a — yes. Symmetric: $a \equiv b \pmod 2 \Rightarrow b \equiv a \pmod 2$ — yes. Transitive: $a \equiv b \pmod 2$ and $b \equiv c \pmod 2 \Rightarrow a \equiv c \pmod 2$ — yes. $\Rightarrow$ R_3 is an equivalence relation. The two equivalence classes are $\{1, 3\}$ (odd) and $\{2, 4\}$ (even).

1.2.12 Equivalence Classes

If an equivalence relation $\sim$ is defined on a set X, then it allows one to collect "equivalent" elements into a single new object. In this way, one abstracts from differences that are irrelevant with respect to the relation.

Definition 29 (Equivalence class)**.** *Let $\sim$ be an equivalence relation on X. For $a \in X$, the* equivalence class *of a is defined by*

$$[a] := \{ x \in X \mid x \sim a \}.$$

A subset $A \subseteq X$ is called an equivalence class *with respect to $\sim$ if the following conditions hold:*

1. *$A \neq \varnothing$,*

2. *for all $x, y \in A$, one has $x \sim y$,*

3. *if $x \in A$ and $y \in X$ with $y \sim x$, then $y \in A$.*

Theorem 30. *The equivalence classes partition X: every $a \in X$ belongs to exactly one equivalence class. In particular, for any two equivalence classes A, A', either $A = A'$ or $A \cap A' = \varnothing$.*

Proof. Fix $a \in X$ and set $A := [a] = \{x \in X \mid x \sim a\}$. Since $\sim$ is reflexive, a belongs to A, and hence $A \neq \varnothing$. If $x, y \in A$, then $x \sim a$ and $y \sim a$; by symmetry and transitivity it follows that $x \sim y$. Thus A satisfies conditions (2) and (3) of the definition.

Now let A and A' be two equivalence classes with $A \cap A' \neq \varnothing$. Choose $z \in A \cap A'$. For $x \in A$, one has $x \sim z$ because $z \in A$; and since $z \in A'$, one also has $z \sim y$ for all $y \in A'$. By transitivity, it follows that

$x \sim y$ for all $y \in A'$, hence $x \in A'$, and therefore $A \subseteq A'$. Interchanging the roles of A and A' gives $A' = A$. Thus any two distinct equivalence classes are disjoint, and every $a \in X$ lies in the class $[a]$, hence in exactly one class. $\square$

Definition 31 (Quotient set and canonical projection)**.** *The set of all equivalence classes is called the* quotient set *and is denoted by*

$$X/\sim \quad \textit{or} \quad X/R$$

The mapping

$$\pi\colon X \longrightarrow X/\sim, \qquad \pi(a) := [a]$$

is called the canonical projection *(or quotient map). It is surjective, and the preimages of its values are precisely the equivalence classes:*

$$\pi^{-1}([a]) = [a].$$

Each element $a \in [a]$ is called a representative *of the class $[a]$.*

Example 32 (Congruence modulo n)**.** *On $\mathbb{Z}$, for a fixed $n \in \mathbb{N}_{\geq 1}$, one defines the relation*

$$a \equiv b \pmod{n} \quad :\Longleftrightarrow \quad n \mid (a-b).$$

This is an equivalence relation. The quotient set $\mathbb{Z}/n\mathbb{Z}$ consists of the n classes

$$[0], [1], \ldots, [n-1],$$

where, for example, $[3] = \{\ldots, -2, 1, 4, 7, \ldots\}$ for $n = 3$. These classes are typical examples of representatives and quotient sets.

1.3 Exercises with Sample Solutions

The following exercises cover the concepts introduced so far: sets and set operations, mappings (injectivity, surjectivity, bijectivity), composition, graphs, relations, equivalence relations, equivalence classes, and quotient sets. The sample solutions are kept concise; as an exercise, students should work out the proofs in full detail themselves.

Exercise 33 (Basic operations). *Let*

$$A = \{1, 2, 3\}, \qquad B = \{2, 3, 4\}, \qquad C = \{3, 4, 5\}.$$

Determine:

$$A \cup B, \quad A \cap B, \quad (A \cup B) \cap C, \quad A \setminus C.$$

Solution 34. $A \cup B = \{1, 2, 3, 4\}$. $A \cap B = \{2, 3\}$. $(A \cup B) \cap C = \{1, 2, 3, 4\} \cap \{3, 4, 5\} = \{3, 4\}$. $A \setminus C = \{1, 2, 3\} \setminus \{3, 4, 5\} = \{1, 2\}$.

Exercise 35 (Indexed sets). *For $I = \mathbb{N} = \{0, 1, 2, \dots\}$ and $X_i = [-i, i] \subset \mathbb{R}$ for $i \in I$, compute*

$$\bigcup_{i \in I} X_i, \qquad \bigcap_{i \in I} X_i.$$

Solution 36. *For every $x \in \mathbb{R}$ there exists an i such that $|x| \leq i$; hence $\bigcup_{i \in I} X_i = \mathbb{R}$. Since $X_0 = [0, 0] = \{0\}$ and $X_0 \subseteq X_i$ for all i, we have $\bigcap_{i \in I} X_i = \{0\}$.*

Exercise 37 (Properties of a mapping)**.** *Consider* $f\colon \{1,2,3\} \to \{a,b\}$ *with* $f(1) = a,\ f(2) = a,\ f(3) = b$. *Is* f *injective? surjective? bijective?*

Solution 38. f *is* not *injective, because* $f(1) = f(2) = a$ *although* $1 \neq 2$. f *is* surjective, *since* $f(\{1,2,3\}) = \{a,b\}$, *which is the codomain. Since it is not injective,* f *is not bijective either.*

Exercise 39 (Composition and identity)**.** *Give a concrete example of sets* X, Y *and mappings* $f\colon X \to Y$, $g\colon Y \to X$ *such that* $g \circ f = \mathrm{id}_X$, *but* $f \circ g \neq \mathrm{id}_Y$. *What follows from* $g \circ f = \mathrm{id}_X$ *about* f *(injective/surjective)?*

Solution 40. *Set* $X = \{1,2\}$ *and* $Y = \{a,b,c\}$. *Define* $f(1) = a$ *and* $f(2) = b$. *Choose* $g(a) = 1$, $g(b) = 2$, *and* $g(c) = 1$. *Then* $g \circ f = \mathrm{id}_X$, *since* $g(f(1)) = g(a) = 1$, *and similarly for the other element of* X. *However,* $f \circ g$ *maps* c *to* $f(1) = a$, *so* $f \circ g \neq \mathrm{id}_Y$. *From* $g \circ f = \mathrm{id}_X$ *it follows that* f *is injective (it has a left inverse) and* g *is surjective (it has a right inverse).*

Exercise 41 (Images, unions, and intersections)**.** *Prove that*

$$f\left(\bigcup_{i\in I} M_i\right) = \bigcup_{i\in I} f(M_i), \qquad f\left(\bigcap_{i\in I} M_i\right) \subseteq \bigcap_{i\in I} f(M_i).$$

Solution 42. *For the first equality, let $y \in f(\bigcup_i M_i)$. Then there is an element $x \in \bigcup_i M_i$ such that $y = f(x)$. Hence $x \in M_i$ for some i, and therefore $y \in f(M_i) \subseteq \bigcup_i f(M_i)$. Conversely, if $y \in \bigcup_i f(M_i)$, then for some i there exists $x \in M_i$ with $y = f(x)$. Thus $x \in \bigcup_i M_i$, so $y \in f(\bigcup_i M_i)$.*

For the second assertion, let $y \in f(\bigcap_i M_i)$. Then there exists $x \in \bigcap_i M_i$ with $y = f(x)$. Since $x \in M_i$ for every i, we have $y \in f(M_i)$ for every i. Therefore $y \in \bigcap_i f(M_i)$. The reverse inclusion need not hold in general, for example when f is not injective.

Exercise 43 (Preimages and set operations)**.** *Show that*

$$f^{-1}\left(\bigcup_{j\in J} N_j\right) = \bigcup_{j\in J} f^{-1}(N_j),$$
$$f^{-1}\left(\bigcap_{j\in J} N_j\right) = \bigcap_{j\in J} f^{-1}(N_j).$$

Solution 44. *Both directions in both identities follow directly from the definition $f^{-1}(N) = \{x \mid f(x) \in N\}$ and from the way $\exists$ and $\forall$ interact with $\vee$ and $\wedge$. Formally,*

$$f(x) \in \bigcup_j N_j \iff \exists j : f(x) \in N_j \iff \exists j : x \in f^{-1}(N_j).$$

The argument for intersections is analogous, with $\forall$ in place of $\exists$.

Exercise 45 (Graph of a mapping)**.** *Let $f\colon X \to Y$ be a mapping. Show that for every $x \in X$ there exists exactly one pair $(x, y) \in G_f$. Explain how this yields the vertical line test.*

Solution 46. *By definition, $G_f = \{(x, f(x)) \mid x \in X\}$. For a fixed x, the pair $(x, f(x))$ exists, and because the value $f(x)$ is unique, there cannot be another pair (x, y') in the graph with $y' \neq f(x)$. Geometrically, this means that to each x there belongs at most one, and by definition exactly one, value y. Hence no vertical line can meet the graph more than once.*

Exercise 47 (Relations and equivalence relations)**.** *For $X = \{1, 2, 3, 4\}$, decide whether the following relations are equivalence relations:*

1. $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1)\}$.
2. $R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3)\}$.

Solution 48. *For R_1, reflexivity holds. Symmetry also holds, since both $(1, 2)$ and $(2, 1)$ are present. Transitivity is checked in the remaining nontrivial cases; for instance, $1 \sim 2$ and $2 \sim 1$ imply $1 \sim 1$, which is included. Thus R_1 is an equivalence relation, with equivalence classes $\{1, 2\}, \{3\}, \{4\}$.*

For R_2, reflexivity holds, but symmetry fails: $(1, 2) \in R_2$, whereas $(2, 1) \notin R_2$. Hence R_2 is not an equivalence relation.

Exercise 49 (Equivalence classes and quotient set)**.** *On* $\mathbb{Z}$*, define* $a \sim b$ *if and only if* $a \equiv b \pmod 4$*. Determine the equivalence classes and the quotient set* $\mathbb{Z}/4\mathbb{Z}$*. Give three different systems of representatives.*

Solution 50. *The equivalence classes are* $[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$*,* $[1]$*,* $[2]$*, and* $[3]$*. Hence*

$$\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}.$$

Three possible systems of representatives are, for example, $\{0, 1, 2, 3\}$*,* $\{4, 5, 6, 7\}$*, and* $\{0, -3, -2, -1\}$*.*

Exercise 51 (Finite sets and the pigeonhole principle)**.** *Let* X *be a finite set with* $|X| = n$*, and let* $f\colon X \to X$*. Show that if* f *is injective, then* f *is surjective. Hint: use the pigeonhole principle.*

Solution 52. *If* f *is injective, then the* n *values* $f(x)$*, with* $x \in X$*, are pairwise distinct. Thus* $f(X)$ *has at least* n *elements. Since* $f(X) \subseteq X$ *and* X *has exactly* n *elements, it follows that* $f(X) = X$*. Therefore* f *is surjective. In pigeonhole terminology: placing* n *objects into* n *boxes without any collision forces every box to be occupied.*

Exercise 53 (Axiom of Choice)**.** *Let* $(X_i)_{i\in I}$ *be a family of nonempty sets. State, in words, the question answered by the axiom of choice, and indicate whether this issue arises when* I *is finite.*

Solution 54. *The question is:* Is there always a mapping $c\colon I \to \bigcup_{i\in I} X_i$ such that $c(i) \in X_i$ for every $i \in I$? *This is precisely the question of the existence of a choice function. If the index set I is finite, such a function can always be constructed by choosing one element from each set X_i. Thus the essential difficulty arises only for infinite families; in full generality, it is resolved by the axiom of choice (or, in models without this axiom, such a function need not always exist).*

Note for instructors: This collection may be used as an exercise sheet for a lecture course or tutorial. Exercises 1–4 are mostly direct computational or conceptual problems; Exercises 5–7 focus on proof techniques; Exercises 8–11 combine conceptual insight with more advanced observations concerning quotients and the axiom of choice. For homework, a mixture of elementary and intermediate problems is recommended; for examinations, variants of Exercises 3, 4, 5, and 10 are particularly suitable.

Chapter 2

Groups

2.1 Operation / Composition

Definition 55. *A* binary operation *(or* composition*) on a set G is a rule*

$$* : G \times G \longrightarrow G, \qquad (a, b) \mapsto a * b,$$

which assigns to each ordered pair $(a, b) \in G \times G$ a uniquely determined element $a * b \in G$.

Important remarks:

- The requirement $* : G \times G \to G$ is called *closure*: the result of combining two elements of G must again lie in G.

- For binary operations one often uses short infix notation such as $a * b$, ab, or standard symbols such as $a + b$, $a \cdot b$. Depending on the context, one may also write $a \circ b$ or $a \circledast b$.

- Some properties of operations that become important later in group theory are, for example, *associativity* $(a * b) * c = a * (b * c)$, the existence of an *identity* element, and the existence of *inverses*. These properties eventually lead to the definition of a group (see the next section).

Examples of binary operations:

1. *Addition* on the integers:

$$+ \; : \; \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \qquad (a, b) \mapsto a + b.$$

Closure, associativity, and commutativity hold.

2. *Multiplication* on the real numbers:

$$\cdot \; : \; \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \qquad (a, b) \mapsto a \cdot b.$$

Here, too, closure and associativity hold; multiplication is commutative.

3. *Matrix multiplication* on $M_n(\mathbb{R})$ (the set of all $n \times n$-matrices):

$$* \; : \; M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R}), \qquad (A, B) \mapsto A \cdot B.$$

This operation is closed and associative, but in general *not* commutative. It is an important example of a non-commutative structure.