Math 300

Course Notes

Contents

1 Sets and quantifiers

1.1 Introduction to set notation

Informal definition. A *set* is a collection of objects.

Conventions.
- Sets are frequently denoted by uppercase letters (e.g. A, B, C).
- If x is in A, then we say that x is an *element* of A or that A *contains* x, and we write $x \in A$.
- Otherwise, we write $x \notin A$.
- If the elements of A are precisely $a_1, \ldots, a_n$, then we write $A = \{a_1, \ldots, a_n\}$.

Examples.
i. natural numbers $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$[1]
ii. integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
iii. rational numbers $\mathbb{Q}$
iv. real numbers $\mathbb{R}$
v. complex numbers $\mathbb{C}$

Convention. If the elements of A are precisely those of B that satisfy a condition P, then we write

$$A = \{x \in B \,|\, x \text{ satisfies the condition } P\}.$$

Examples.
i. $\mathbb{N} = \{n \in \mathbb{Z} \,|\, n \geq 0\}$
ii. $\mathbb{Q} = \left\{\frac{n}{m} \,\middle|\, n, m \in \mathbb{Z}, m \neq 0\right\}$

Definition. The *empty set* $\varnothing$ is the set that contains no elements.

That is, $\varnothing = \{\}$.

1.2 Quantifiers

Informal definition. If there is an element $x \in A$ that satisfies the condition P, then we write

$$\exists\, x \in A : x \text{ satisfies the condition } P.$$

The symbol $\exists$ is called the *existential quantifier*.

Convention. There are a few ways this can be read. Examples include,

- "There exists an x in A such that x satisfies P."
- "There is an x in A such that…"
- "There is an x in A that satisfies the condition P."

Examples. The following statements are true:

i. $\exists\, n \in \mathbb{Z} : n$ is even
ii. $\exists\, x \in \mathbb{R} : x > 3$
iii. $\exists\, n \in \mathbb{N} : n > 3$ and n is even

[1] There is an alternative convention that $\mathbb{N} = \{1, 2, 3, \ldots\}$.

The following are false:

iv. $\exists\, n \in \mathbb{N} : n < 0$

v. $\exists\, n \in \mathbb{Z} : n > 3$ and $n < 1$

vi. $\exists\, x \in \mathbb{R} : x^2 = -1$

Informal definition. If every $x \in A$ satisfies the condition P, then we write

$$\forall\, x \in A : x \text{ satisfies the condition } P.$$

The symbol $\forall$ is called the *universal quantifier*.

Convention. This may be read as, for example,

- "For all/every/any x in A, x satisfies the condition P"
- "All x in A satisfy..."
- "Every/Any x in A satisfies..."

Examples. True statements:

i. $\forall n \in \mathbb{N} : n \geq 0$

ii. $\forall k \in \mathbb{N} : k \in \mathbb{Z}$

iii. $\forall x \in \mathbb{R} : x^2 \geq 0$

False statements:

iv. $\forall x \in \mathbb{R} : x \in \mathbb{N}$

v. $\forall m \in \mathbb{Z} : m$ is even

vi. $\forall n \in \mathbb{N} : \sqrt{n} \in \mathbb{N}$

Remark. Note that

$$\text{If } x \in A, \text{ then } P(x)$$

may also be formalized as

$$\forall x \in A : P(x).$$

Examples. Quantifiers can be strung together:

i. $\forall m \in \mathbb{Z} : \exists n \in \mathbb{N} : m < n$

ii. $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : x - y = 2$

iii. $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : \forall z \in \mathbb{R} : (x - y)z = 0$

Convention. When introducing new variables of the same type, it is convenient to do so alphabetically (e.g. a, b, c, or x, y, z).

1.3 Proofs with quantifiers

To prove a claim of the form

$$\exists x \in A : P(x),$$

we have simply to exhibit an $x \in A$ that satisfies the condition P.

Consider the following example:

Claim. *There is a $k \in \mathbb{Z}$ such that $k^2 = k$.*

Proof. We have $0 \in \mathbb{Z}$ and $0^2 = 0$. □

Remark. We could have just as well chosen $k = 1$. Only a single $k \in \mathbb{Z}$ satisfying $k^2 = k$ is required to prove the claim.

Convention. A proof should consist of grammatically correct English sentences. It is considered undesirable to begin a sentence with a mathematical symbol. To adhere to this rule, it is often convenient to preface an otherwise-bare mathematical formula with a brief phrase such as

- "We have. . . "
- "Observe that. . . "
- "Note that. . . "

To prove a claim of the form

$$\forall x \in A : P(x),$$

there are two steps:

1. Introduce an arbitrary $x \in A$.
2. Show that x satisfies P.

The first step is accomplished by means of a statement such as

- "Let $x \in A$."
- "Fix $x \in A$."
- "Suppose that $x \in A$."

Claim. *If $q \in \mathbb{Q}$, then $\frac{q}{2} \in \mathbb{Q}$.*

Proof. Fix $q \in \mathbb{Q}$. By the definition of $\mathbb{Q}$, there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $q = \frac{m}{n}$. Thus,

$$\frac{q}{2} = \frac{m}{2n} \in \mathbb{Q}.$$

□

Convention. Common prefaces to a conclusion include

- "Thus,"
- "Hence,"
- "Therefore,"
- "It follows that,"

Claim. *For every $m \in \mathbb{Z}$, there is an $n \in \mathbb{Z}$ with $m < n$.*

Proof. Fix $m \in \mathbb{Z}$ and let $n = m + 1$. It follows that $m < n$. $\square$

Convention. The following phrases have similar meanings:

- "such that"
- "with"
- "subject to the condition that"
- "satisfying"
- "for which"

2 Logical connectives

2.1 Negation

Informal definition. The *negation* of a statement S is the statement that *it is not the case that* S, written $\neg S$.

Convention. The symbol $\neg$ is read "not".

Examples.

i. The negation of
$$\exists\, x \in \mathbb{R} : x^2 = -1$$
is
$$\neg\exists\, x \in \mathbb{R} : x^2 = -1,$$
which states that *it is not the case that* there is a real number that squares to -1.

ii. The negation of
$$\forall n \in \mathbb{Z} : n \geq 0$$
is
$$\neg\forall n \in \mathbb{Z} : n \geq 0,$$
which asserts that *it is not the case that* every integer is positive.

Informal definition. To *disprove* a statement S is to prove that S is false. This is equivalent to proving $\neg S$.

It is useful to note that
$$\neg\forall x \in A : P(x) \qquad \text{is equivalent to} \qquad \exists x \in A : \neg P(x)$$
and
$$\neg\exists x \in A : P(x) \qquad \text{is equivalent to} \qquad \forall x \in A : \neg P(x).$$

Examples.

i. The negation of
$$\exists x \in \mathbb{R} : \forall y \in \mathbb{R} : x = y$$
is
$$\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : x \neq y$$

ii. The negation of
$$\forall m \in \mathbb{Z} : \exists n \in \mathbb{N} : m + n < 0$$
is
$$\exists m \in \mathbb{Z} : \forall n \in \mathbb{N} : m + n \geq 0$$

Proof of i. Fix $x \in \mathbb{R}$. If $y = x + 1$, then $x \neq y$. $\square$

Proof of ii. Put $m = 0$ and let $n \in \mathbb{N}$. Since $n \geq 0$, it follows that $m + n \geq 0$. $\square$

2.2 Logical connectives

Informal definition. We implement the following shorthand.

symbol	meaning
$\wedge$	and
$\vee$	or
$\rightarrow$, $\implies$	if ... then
$\leftrightarrow$, $\iff$	if and only if (precisely if, precisely when,...)

Examples. The following statements are true,

i. $(3 = 3) \wedge (5 = 5)$

ii. $(1 = 1) \vee (2 > 3)$

iii. $(5 < 6) \vee (5 < 7)$

iv. $\forall x \in \mathbb{R} : (x > 3) \rightarrow (x > 0)$

v. $(1 = 2) \rightarrow (7 \geq 5)$

vi. $\forall k \in \mathbb{N} : (k^2 = 4) \leftrightarrow (k = 2)$

and the following are false,

vii. $\forall x \in \mathbb{R} : (x^2 = 4) \leftrightarrow (x = 2)$

viii. $\forall k \in \mathbb{Z} : (k > 5) \rightarrow (k > 8)$

To prove a

- *conjunction* $P \wedge Q$, you must prove both P and Q.
- *disjunction* $P \vee Q$, suppose that P is *false* and prove Q.
- *implication* $P \rightarrow Q$, supoose that P is *true* and prove Q.

Remark. When proving an implication $P \rightarrow Q$, the assumption P is often left unstated.

Claim. *For every $x \in \mathbb{R}$ there is a $y \in \mathbb{R}$ such that $y < x$ and $y < 0$.*

Proof. Fix $x \in \mathbb{R}$ and let y be the minimum of $x - 1$ and -1. It follows that $y < x$ and $y < 0$. $\square$

Claim. *Let $x \in \mathbb{R}$. If $x^2 = x$, then $x = 0$ or $x = 1$.*

Proof. Suppose that $x^2 = x$ and $x \neq 0$. Dividing both sides of $x^2 = x$ by $x \neq 0$ yields $x = 1$. $\square$

Alternative proof. Suppose that $x^2 = x$ and $x \neq 1$. Dividing both sides of $x(x-1) = 0$ by $x - 1 \neq 0$ provides $x = 0$. $\square$

Claim. *Let $x \in \mathbb{R}$. If $xy = y$ for all $y \in \mathbb{R}$, then $x = 1$.*

Proof. From the condition that $xy = y$ for all $y \in \mathbb{R}$, we conclude that $x = x \cdot 1 = 1$. $\square$

Informal definition. We write

$$\exists!\, x \in A : P(x)$$

when there exists a *unique* $x \in A$ that satisfies the property P.

This is equivalent to

$$\exists\, x \in A : P(x) \wedge \Big(\forall y \in A : P(y) \to x = y\Big).$$

Examples. We have

i. $\exists! x \in \mathbb{R} : x^3 = 8$

ii. $\forall x \in \mathbb{R} : \exists! k \in \mathbb{Z} : k \leq x < k + 1$

Claim. *There is a unique $m \in \mathbb{N}$ satisfying the property that $m \leq n$ for all $n \in \mathbb{N}$.*

Proof. Put $m = 0$. For all $n \in \mathbb{N}$, we have $m \leq n$. Now suppose that $m' \in \mathbb{N}$ satisfies $m' \leq n$ for all $n \in \mathbb{N}$. In particular, $m' \leq 0$ and $0 \leq m'$. Thus, $m = 0$. □

Remark. The expression

$$\forall x \in A : P(x)$$

is shorthand for

$$\forall x : \big(x \in A \to P(x)\big)$$

3 Set operations and functions

3.1 Assorted abbreviations

abbr.	Latin	meaning
e.g.	*exempli gratia*	for example
i.e.	*id est*	that is
viz.	*videlicet*	namely
cf.	*confer*	compare (*erroneously:* see)
ff.	*foliis*	following
ibid.	*ibidem*	in the same place (followed by page number)
op. cit.	*opere citato*	in the work cited (in the same work)
loc. cit.	*loco citato*	in the place cited (on the same page)
QED	*quod erat demonstrandum*	that which was to be shown

3.2 Union, intersection, containment, and complement

Let A and B be sets.

Definition. The *union* of A and B is

$$A \cup B = \big\{x \,|\, x \in A \text{ or } x \in B\big\}.$$

Example. If A and B are the sets of even and odd integers, respectively, then $A \cup B = \mathbb{Z}$.

Definition. The *intersection* of A and B is

$$A \cap B = \big\{x \,|\, x \in A \text{ and } x \in B\big\}.$$

Example. We have

$$\mathbb{N} = \mathbb{Z} \cap \mathbb{R}_{\geq 0}$$

where $R_{\geq 0} = \{x \in \mathbb{R} \,|\, x \geq 0\}$ is the set of nonnegative real numbers.

Definition. We say that A and B are *disjoint* when $A \cap B = \varnothing$.

Example. Every set A is disjoint from the empty set $\varnothing$.

Definition. We say that A is a *subset* of B if

$$\forall x : \big(x \in A \to x \in B\big).$$

In this case, we write $A \subseteq B$.

Examples. We have

i. $\varnothing \subseteq A$ for every set A,

ii. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Definition. The *difference* of A and B is

$$B \backslash A = \{x \in B \,|\, x \notin A\}.$$

Example. The set of irrational numbers is $\mathbb{R} \backslash \mathbb{Q}$.

Definition. If $A \subseteq B$, then the *complement* of A in B is $A^c = B \backslash A$.

Example. The complement of the set of even integers is the set of odd integers.

Claim. *Let A, B, and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

To prove this, we will assume that $A \subseteq B$ and $B \subseteq C$, and we must deduce that $A \subseteq C$.

Proof. Fix $x \in A$. From $A \subseteq B$ we obtain $x \in B$, and from $B \subseteq C$ we conclude that $x \in C$. $\square$

3.3 First definitions and examples

Let A and B be sets.

Informal definition. A *function* $f : A \to B$ is a rule that assigns to each $x \in A$ a unique $f(x) \in B$.

$$\forall x \in A : \exists! y \in B : y = f(x)$$

Remark. We sometimes write $x \mapsto f(x)$ to

Examples. i. Consider

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ k &\mapsto 2k. \end{aligned}$$

ii. The *identity function* on A is

$$\begin{aligned} f : A &\to A \\ x &\mapsto x. \end{aligned}$$

iii. The *constant function* $f : A \to B$ with value $b \in B$ is

$$\begin{aligned} f : A &\to B \\ x &\mapsto b. \end{aligned}$$

iv. The *empty function* $f : \varnothing \to B$ is completely determined by the value it assigns each element in $\varnothing$.

v. If $A \subseteq B$ then the associated *inclusion function* is

$$\begin{aligned} f : A &\to B \\ x &\mapsto x. \end{aligned}$$

vi. We may consider a property $P(x)$ that elements $x \in A$ can satisfy as a function

$$\begin{aligned} P : A &\to \mathbb{B} \\ x &\mapsto P(x) \end{aligned}$$

where $\mathbb{B} = \{\top, \bot\}$ is the Boolean domain, comprising the *truth values* true $\top$ and false $\bot$.

Definition. The *composition* of $f : A \to B$ and $g : B \to C$ is

$$\begin{aligned} g \circ f : A &\to C \\ x &\mapsto g(f(x)). \end{aligned}$$

4 Injective and surjective functions

4.1 Shortening proofs

Claim. *Let $x \in \mathbb{R}$. If $x > 0$, then there is a $y \in \mathbb{R}$ such that $0 < y < x$.*

Formally, this is

$$\forall x \in \mathbb{R} : \exists y \in \mathbb{R} : 0 < y < x$$

Proof. Fix $x \in \mathbb{R}$. Suppose that $x > 0$. Put $y = \frac{x}{2}$ and observe that $0 < y < x$. $\square$

Informal definition. We will say that a *fully explicit proof* is a proof that explicitly

i. states every assumption and introduces every variable,

ii. validates every statement.

Actual proofs in the mathematical literature are hardly ever fully explicit. In particular, actual proofs will often refrain from

i. stating every assumption or introducing every variable. This is particularly common when the assumptions would be stated at the opening of a proof.

   Proof. Put $y = \frac{x}{2}$ and observe that $0 < y < x$. $\square$

ii. validates every statement. When a statement is obvious, it is often omitted.

   Proof. Fix $x \in \mathbb{R}$. Suppose that $x > 0$ and put $y = \frac{x}{2}$. $\square$

Taken together, we have

Proof. Put $y = \frac{x}{2}$. $\square$

The balance between what to make explicit and what to keep implicit in a proof depends on the intended audience. A guiding principle is that

Given your proof, the intended reader should be able to easily write a fully explicit proof.

Remark. In general, when a statement is obvious, it does not need to be proved. Be aware that the word *obvious* (or its synonyms *clear*, *apparent*, *trivial*, *elementary*,…) mean "obvious how to prove" and not "obvious that it is true".

4.2 Injectivity and surjectivity

Definition. The function $f : A \to B$ is said to be *injective* if $f(x) = f(y)$ implies $x = y$.

$$\forall x, y \in A : \big(f(x) = f(y)\big) \implies (x = y)$$

Claim. *The function $f : \mathbb{N} \to \mathbb{N}$ given by $f(k) = 2k$ is injective.*

Proof. Let $k, \ell \in \mathbb{N}$ and suppose that $f(k) = f(\ell)$. Dividing both sides of $2k = 2\ell$ by 2 yields $k = \ell$. $\square$

Claim. *The constant function $f : \mathbb{R} \to \mathbb{Z}$ with value 0 is not injective.*

We must show that

$$\exists x, y \in \mathbb{R} : \big(f(x) = f(y)\big) \wedge (x \neq y).$$

Proof. We have $f(1) = 0 = f(2)$ but $1 \neq 2$. $\square$

Definition. The function $f : A \to B$ is called *surjective* when for every $y \in B$ there is an $x \in A$ with $f(x) = y$.

$$\forall y \in B : \exists x \in A : f(x) = y$$

Claim. *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not surjective.*

We must show that
$$\exists y \in \mathbb{R} : \forall x \in \mathbb{R} : f(x) \neq y$$

Proof. From $x^2 \geq 0$ for all $x \in \mathbb{R}$, it follows that $f(x) \neq -1$ for any $x \in \mathbb{R}$. $\square$

Definition. We say that $f : A \to B$ is *bijective* when it is both injective and surjective.

Claim. *The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is bijective.*

Proof. If $x, y \in \mathbb{R}$ satisfy $2x = 2y$, then division by 2 yields $x = y$. This proves injectivity.
To establish surjectivity, fix $y \in \mathbb{R}$ and observe that $2(\frac{y}{2}) = y$. $\square$

4.3 More proofs with functions

Let A, B, and C be sets and let $S \subseteq A$ be a subset.

Claim. *If $f : A \to B$ and $g : B \to C$ are injective, then $g \circ f : A \to C$ is injective.*

We must show that
$$\forall x, y \in A : g \circ f(x) = g \circ f(y) \implies x = y$$

Proof. Suppose that $g\big(f(x)\big) = g\big(f(y)\big)$. From the injectivity of g we have $f(x) = f(y)$, and from the injectivity of f we conclude that $x = y$. $\square$

Claim. *If $f : A \to B$ and $g : B \to C$ are surjective, then $g \circ f : A \to C$ is surjective.*

Now we must show that
$$\forall c \in C : \exists a \in A : g \circ f(a) = c$$

Proof. From the surjectivity of g there is a $b \in B$ such that $g(b) = c$, and from the surjectivity of f there is an $a \in A$ with $f(a) = b$. Thus, $g(f(a)) = g(b) = c$. $\square$

Claim. *If $f : A \to B$ and $g : B \to A$ satisfy $g \circ f = \mathrm{id}_A$, then f is injective and g is surjective.*

Proof. Suppose that $f(a) = f(a')$. Applying g to each side, we obtain $a = g(f(a)) = g(f(a')) = a'$. This establishes the injectivity of f.
Now fix $a \in A$ and observe that $g(f(a)) = a$. This proves the surjectivity of g. $\square$

Definition. The *restriction* of $f : A \to B$ to S is the function

$$\begin{aligned} f|_S : S \to\ & B \\ x \mapsto\ & f(x). \end{aligned}$$

Claim. *If $f : A \to B$ is injective, then $f|_S : S \to B$ is injective.*

Proof. Let $x, y \in S$ with $f(x) = f(y)$. By the injectivity of f, we have $x = y$. $\square$

Claim. *If $f : A \to B$ is surjective, then it is not necessarily true that $f|_S : S \to B$ is surjective.*

Proof. Suppose that B is nonempty, put $S = \varnothing \subseteq A$, and observe that $f|_S : S \to B$ is not surjective. $\square$

5 Limits

5.1 The hierarchy of results

type	description
theorem	a primary result
proposition	a result of lesser significance than a theorem
lemma	an intermediate result needed to prove another result
corollary	a result that follows quickly from a theorem or proposition

Let $f : A \to B$ and $g : B \to C$ be functions.

Lemma. *If f and g are injective, then $g \circ f$ is injective.*

Lemma. *If f and g are surjective, then $g \circ f$ is surjective.*

Theorem. *If the functions $f : A \to B$ and $g : B \to C$ are bijective, then $g \circ f : A \to C$ is bijective.*

Corollary. *If $f : A \to A$ is bijective, then $f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}} : A \to A$ is bijective for all $n \geq 1$.*

5.2 Proof by contradiction

A standard way to prove that P is true is to show that $\neg P$ entails a contradiction.

$$\begin{aligned} P &\equiv P \vee \bot \\ &\equiv \neg(\neg P) \vee \bot \\ &\equiv \neg P \to \bot \end{aligned}$$

To prove P by contradiction, first suppose that P is true and then obtain a contradiction.

Proposition. *There are infinitely many prime numbers.*

Proof. Suppose for a contradiction that $p_1, \ldots, p_k$ is a finite enumeration of all prime numbers and put $n = p_1 \cdots p_k + 1$. Since n is not divisible by any of the p_i, it follows that n is prime. This yields the desired contradiction. □

Remark. When you prove a statement by contradiction, it is conventional to explicitly inform the reader at the outset. For example, you can write "Suppose not.", "Assume for a contradiction that…", "Assume for the sake of a contradiction that…", "Assume with the aim of reaching a contradiction…", etc. When the contradiction is obtained, authors will occasionally indicate this by writing "This yields the desired contradiction," "This provides the desired contradiction," etc.

5.3 Limits at infinity

Let $f : \mathbb{R} \to \mathbb{R}$ be a function.

Definition. We say that $f(x) \to \infty$ as $x \to \infty$, or that $\lim\limits_{x\to\infty} f(x) = \infty$, when

$$\forall M > 0 : \exists N > 0 : \forall x > N : f(x) > M.$$

In this case, we write $\lim\limits_{x\to\infty} f(x) = \infty$.

Proposition. *We have*

$$\lim_{x\to\infty} 2x = \infty$$

Proof. Fix $M > 0$, put $N = \frac{M}{2}$, and let $x > \frac{N}{2}$. It follows that

$$f(x) = 2x > 2N = M.$$

$\square$

Proposition. *We have*

$$\lim_{x\to\infty} \frac{1}{x} \neq \infty.$$

We must show that

$$\exists M > 0 : \forall N > 0 : \exists x > N : f(x) \leq M$$

Proof. Put $M = 1$, let $N > 0$, and put $x = \max(1, N)$. If $N \geq 1$, then $f(x) = \frac{1}{N} \leq 1$. Otherwise, $x = 1$ and $f(x) = 1$. $\square$

Definition. Fix $L \in \mathbb{R}$. We say that $f(x) \to L$ as $x \to \infty$, or that $\lim_{x\to\infty} f(x) = L$, when

$$\forall \varepsilon > 0 : \exists N > 0 : \forall x > N : |f(x) - L| < \varepsilon.$$

Proposition. *We have*

$$\lim_{x\to\infty} \frac{1}{x} = 0.$$

We must show that

$$\forall \varepsilon > 0 : \exists N > 0 : \forall x > N : \left|\frac{1}{x}\right| < \varepsilon.$$

Proof. Let $\varepsilon > 0$, choose $N = \frac{1}{\varepsilon}$, and let $x > N$. From $x > \frac{1}{\varepsilon}$, we obtain $\left|\frac{1}{x}\right| = \frac{1}{x} < \varepsilon$. $\square$

Proposition. *We have*

$$\lim_{x\to\infty} x \neq 0.$$

We will show that

$$\exists \varepsilon > 0 : \forall N > 0 : \exists x > N : |x| > \varepsilon.$$

Proof. Put $\varepsilon = 1$, let $N \geq 0$, and let $x = \max(1, N)$. If $N \geq 1$, then $x = N$ and thus $|x| = x \geq \varepsilon$. Otherwise, $x = 1$ and $|x| \geq \varepsilon$. $\square$

5.4 Limits at points

Definition. Fix $x_0 \in \mathbb{R}$. We say that $f(x) \to \infty$ as $x \to x_0$, or that $\lim_{x\to x_0} f(x) = \infty$, when

$$\forall M > 0 : \exists \delta > 0 : \forall x \in \mathbb{R} : |x - x_0| < \delta \implies f(x) > M.$$

Proposition. *We have*

$$\lim_{x\to 0} \frac{1}{x} \neq \infty.$$

We want to show that

$$\exists M > 0 : \forall \delta > 0 : \exists x \in \mathbb{R} : |x| < \delta \ \wedge \ \frac{1}{x} \leq M.$$

Proof. Put $M = 1$, let $\delta > 0$, and put $x = -\frac{\delta}{2}$. It follows that $|x| = \frac{\delta}{2} < \delta$ and that $\frac{1}{x} = -\frac{2}{\delta} \leq 1$. $\square$

Definition. Fix $x_0 \in \mathbb{R}$ and $L \in \mathbb{R}$. We say that $f(x) \to L$ as $x \to x_0$, or that $\lim_{x \to \infty} f(x) = L$, when

$$\forall \varepsilon > 0 : \exists \delta > 0 : \forall x \in \mathbb{R} : |x - x_0| < \delta \implies |f(x) - L| < \varepsilon$$

Proposition. *We have*

$$\lim_{x \to 0} 3x = 0.$$

We will show that

$$\forall \varepsilon > 0 : \exists \delta > 0 : \forall x \in \mathbb{R} : |x| < \delta \implies |3x| < \varepsilon$$

Proof. Let $\varepsilon > 0$, choose $\delta = \frac{\varepsilon}{3}$, and let $x \in \mathbb{R}$ with $|x| < \delta$. From $|x| < \frac{\varepsilon}{3}$, we conclude that $|3x| < \varepsilon$. $\square$

6 Relations

6.1 The word "respectively"

Examples.

i. The integers 2 and 7 are even and odd, respectively.

ii. Paris, Rome, and Berlin are the respective capitals of France, Italy, and Germany.

iii. The TGV, the Shanghai maglev, and the Acela are the fastest trains in Europe, Asia, and North America, respectively.

iv. The cats sat on their respective mats.

v. The largest and the smallest breed of dogs are, respectively, the English Mastiff and the Chihuahua.

6.2 The phrase "in general"

In nonmathematical contexts, the phrase "in general" can mean that something is usually or typically the case. In mathematics, it means that it is *always* the case. Similarly, in mathematics, to say that P is "not generally true" is to say that P is not always true.

Examples.

i. In general, if $x, y \in \mathbb{R}$ are distinct, then $(x-y)^2 > 0$.

ii. Let $x \in \mathbb{R}$. It is not generally true that $x^2 > 9$.

6.3 Cartesian products

Definition. The *Cartesian product* of A and B is the set of ordered pairs

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Remark. When $A = B$, we also write A^2 for $A \times A$.

Example.

i. If $A = \{a\}$ and $B = \{b\}$, then $A \times B = \{(a, b)\}$.

ii. If $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$, then

$$\begin{aligned} A \times B = \big\{&(a,1),(a,2),(a,3),\\ &(b,1),(b,2),(b,3),\\ &(c,1),(c,2),(c,3)\big\}. \end{aligned}$$

iii. The set $\mathbb{R}$ is a line, $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ is a plane, and $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ is a three-dimensional space.

iv. We have

$$\varnothing \times \varnothing = \varnothing.$$

v. More generally, for any set A,

$$\varnothing \times A = \varnothing = A \times \varnothing.$$

Remark. Suppose that A and B are finite sets, and write $|A|$ and $|B|$ for their sizes. Observe that

$$|A \times B| = |A| \times |B|,$$

where the $\times$ on the left is the Cartesian product and that on the right is multiplication in $\mathbb{N}$.

6.4 Relations

Definition. A *relation* from A to B is a subset $R \subseteq A \times B$.

Conventions. i. We ususually write $(a, b) \in R$ as aRb.

ii. When $A = B$, we call R a *relation on* A.

Examples. i. $A = B = \mathbb{R}$, $R = \{(x, y) \in \mathbb{R}^2 \mid x < y\}$.

ii. $A = B = \mathbb{N}$, $R = \{(m, n) \in \mathbb{N}^2 \mid m|n\}$.

iii. $A = B$, the *identity relation* $I_A = \{(a, a') \in A^2 \mid a = a'\}$.

iv. the *empty relation* $R = \varnothing \subseteq A \times B$.

v. $A \times B \subseteq A \times B$.

Definition. The *domain* of $R \subseteq A \times B$ is the subset

$$\operatorname{Dom} R = \{a \in A \mid \exists b \in B : aRb\},$$

and the *range* is

$$\operatorname{Rng} R = \{b \in B \mid \exists a \in A : aRb\}.$$

Definition. A *function* from A to B is a relation $f \subseteq A \times B$ such that

$$\forall a \in A : \exists!\, b \in B : (a, b) \in f.$$

We usually write $(a, b) \in f$ as $f(a) = b$.

Remark. When we consider a function $f : A \to B$ as a subset of the cartesian product $A \times B$, we typically do so by refering to its *graph*,

$$\operatorname{graph} f = \{(a, b) \in A \times B \mid f(a) = b\}.$$

Definition. If $R \subseteq A \times B$ is a relation from A to B, then the *inverse* of R is the relation $R^{-1} \subseteq B \times A$ given by

$$bR^{-1}a \iff aRb.$$

Definition. If R is a relation from A to B, and if S is a relation from B to C, then the *composition* of R and S is

$$S \circ R = \{(a, c) \mid \exists b \in B : aRb \wedge bSc\}.$$

Examples. i. $I_A \circ I_A = I_A$.

ii. Consider the relations $\leq$ and $<$ on $\mathbb{N}$. We have $(\leq \circ <) = <$.

iii. Observe that $m(< \circ <)n \iff m + 1 < n$.

7 Equivalence relations and partial orders

7.1 Proving that two sets are equal

Given two sets A and B, the standard way to prove that $A = B$ is

i. prove that $A \subseteq B$,

ii. prove that $B \subseteq A$.

Definition. The *symmetric difference* of A and B is $A \,\Delta\, B = A\backslash B \cup B\backslash A$.

Proposition. *We have* $A \,\Delta\, B = (A \cup B)\backslash(A \cap B)$.

Proof. ($\subseteq$). Fix $x \in A \,\Delta\, B$. We have $x \in A\backslash B$ or $x \in B\backslash A$. Suppose that $x \in A\backslash B$. From $x \in A$ it follows that $x \in A \cup B$, and from $x \notin B$ we deduce that $x \notin A \cap B$. Therefore, $x \in (A \cup B)\backslash(A \cap B)$. The case that $x \in B\backslash A$ is similar.

($\supseteq$). Now suppose that $y \in (A \cup B)\backslash(A \cap B)$. From $y \in A \cup B$ we have $y \in A$ or $y \in B$, and from $y \notin A \cap B$ we obtain $y \notin A$ or $y \notin B$. Thus, if $y \in A$ then $y \notin B$ and we conclude that $y \in A\backslash B$. The case that $y \in B$ is similar. $\square$

7.2 Proving that two relations are equal

Suppose that R and S are relations from A to B. The standard way to prove that $R = S$ is to prove that

$$\forall a \in A : \forall b \in B : aRb \iff aSb.$$

Proposition. *If R and S are the relations on $\mathbb{N}$ given by*

$$\begin{aligned} mRn &\iff m \leq n \\ mSn &\iff 2m \leq 2n, \end{aligned}$$

then $R = S$.

Proof 1. First suppose that mRn. Multiplying each side of $m \leq n$ by 2 yields $2m \leq 2n$, from which we conclude that mSn.

Now suppose that mSn. Dividing $2m \leq 2n$ through by 2 provides $m \leq n$, whence mRn. $\square$

Proof 2. We have

$$\begin{aligned} mRn &\iff m \leq n \\ &\iff 2m \leq 2n \\ &\iff mSn. \end{aligned}$$

$\square$

7.3 Properties of relations

Definition. We say that the relation R on A is

- *reflexive* when $\forall a \in A : aRa$
- *transitive* when $\forall a, b, c \in A : (aRb \wedge bRc) \implies aRc$
- *symmetric* when $\forall a, b \in A : aRb \implies bRa$
- *antisymmetric* when $\forall a, b \in A : (aRb \wedge bRa) \implies a = b$

Definition. The relation R on A is

- an *equivalence relation* when it is reflexive, transitive, and symmetric;
- a *partial order* when it is reflexive, transitive, and antisymmetric.

Examples. Equivalence relations include

i. $I_A \subseteq A^2$

ii. $\varnothing \subseteq A^2$ precisely when $A = \varnothing$

iii. $A^2 \subseteq A^2$

iv. the relation $\equiv_k$ on $\mathbb{Z}$, given by $a \equiv_k b \iff \exists \ell \in \mathbb{Z} : a = b + k\ell \iff k \mid (a - b)$.

Examples. Partial orders include

i. $\leq$ on $\mathbb{Z}$

ii. $\mid$ on $\mathbb{Z}$

iii. $\subseteq$ on $\mathcal{P}(X)$, where X is a set and
$$\mathcal{P}(X) = \{Y \mid Y \subseteq X\}$$
is the *powerset* of X.

Definition. A set A equipped with a partial order R is called a *partially ordered set* or a *poset*.

7.4 Proofs with relations

Let R be a relation from A to B.

Proposition. *We have* $\operatorname{Dom} R^{-1} = \operatorname{Rng} R$.

Proof 1. ($\subseteq$). Let $b \in \operatorname{Dom} R^{-1}$. Thus, there is an $a \in A$ such that $bR^{-1}a$. It follows that aRb, from which $b \in \operatorname{Rng} R$.

($\supseteq$). Now fix $b \in \operatorname{Rng} R$ and let $a \in A$ with aRb. From $bR^{-1}a$ we conclude that $b \in \operatorname{Dom} R$. □

Proof 2. Fix $a \in A$ and $b \in B$ and observe that

$$\begin{aligned} b \in \operatorname{Dom} R^{-1} &\iff \exists\, a \in A : bR^{-1}a \\ &\iff \exists\, a \in A : aRb \\ &\iff b \in \operatorname{Rng} R. \end{aligned}$$

□

Proposition. *We have* $I_A \circ R = R$.

Proof 1. Let $a \in A$ and $b \in B$.

First suppose that $a(I_A \circ R)b$. Thus, there is an $a' \in A$ with $a = a'$ and $a'Rb$, and we deduce that aRb.

Now suppose that aRb. From $a = a$ and aRb, we obtain $a(I_A \circ R)b$. □

Proof 2. Let $a \in A$ and $b \in B$. It is readily seen that

$$\begin{aligned} a(I_A \circ R)b &\iff \exists\, a' \in A : a = a' \,\wedge\, a'Rb \\ &\iff aRb. \end{aligned}$$

□

8 Quotients

8.1 The words “natural” and “canonical”

While there is a certain amount of subtlety here, very roughly speaking, “canonical” and “natural” mean “standard”.

Examples. i. There is a canonical function $f : A \to A$ (viz. the identity map).

ii. The inclusion map

$$\begin{aligned} i : A &\to B \\ a &\mapsto a \end{aligned}$$

is a natural map from $A \subseteq B$ to B.

iii. There are canonical *projection maps*

$$\begin{aligned} p_A : A \times B \to A \\ p_B : A \times B \to B \end{aligned}$$

given by

$$\begin{aligned} p_A(a, b) = a \\ p_B(a, b) = b. \end{aligned}$$

Remark. At a slightly deeper level, a property or construction is *natural* or *canonical* for a class of structures (e.g. sets) if can be described without knowing anything further about the particular instance of the structure under consideration. For example, if you tell me that you have a set A, then—without any information about your set—I can describe the identity function $\mathrm{id} : A \to A$.

8.2 The word “conversely”

You can shorten a proof of $A = B$ or $P \iff Q$ by using the keyword “conversely”, which signals that you are about to establish the opposite inclusion or implication.

Proposition. *For all $m, n \in \mathbb{Z}$, we have $m \geq n$ if and only if $2m \geq 2n$.*

Proof 1. ($\Rightarrow$). Multiplying both sides of $m \geq n$ by 2 yields $2m \geq 2n$.
($\Leftarrow$). Dividing each side of $2m \geq 2n$ by 2 provides $m \geq n$. □

Proof 2. Multiplying both sides of $m \geq n$ by 2 yields $2m \geq 2n$. Conversely, dividing each side of $2m \geq 2n$ by 2 provides $m \geq n$. □

8.3 Operations on sets

Let A be a set.

Definition. A *binary operation* on A is a function

$$\bullet : A \times A \to A.$$

Remark. i. We typically write $\bullet(a, b)$ as $a \bullet b$.

ii. More generally, an *n-ary operation* on A is a function $\bullet : A^n \to A$.

Examples. Examples $(A, \bullet)$ of sets with binary operations include

i. $(\mathbb{Z}, +)$

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (m, n) &\mapsto m + n \end{aligned}$$

ii. $(\mathbb{Z}, -)$

iii. $(\mathbb{Z}, \times)$

iv. *non*example: $(\mathbb{R}, \div)$, since we cannot divide by zero

v. $(\mathcal{P}(A), \cap)$

vi. $(\mathcal{P}(A), \cup)$

8.4 Quotients

Let $\sim$ be an equivalence relation on A.

Definition. The $\sim$-*equivalence class* of $a \in A$ is the subset

$$[a]_\sim = \{b \in A \mid a \sim b\} \subseteq A.$$

The *quotient* of A by $\sim$ is the set

$$A/\!\sim\; = \big\{[a]_\sim \,\big|\, a \in A\big\}.$$

Examples. i. (A, I_A). If $a \in A$, then

$$[a]_{I_A} = \{b \in A \mid a = b\} = \{a\}.$$

Thus,

$$A/I_A \; = \big\{\{a\} \,\big|\, a \in A\big\}.$$

There is a natural bijection

$$\begin{aligned} f : A &\to A/I_A \\ a &\mapsto \{a\}. \end{aligned}$$

i. (A, A^2). Suppose $\sim = A^2$. For each $a \in A$, we have

$$[a]_\sim = \{b \in A \mid a \sim b\} = A.$$

Hence,

$$A/\!\sim = \{A\}.$$

i. $(\mathbb{Z}, \equiv_k)$. Fix $k \in \mathbb{N}_+$. Given $m \in \mathbb{Z}$, we have

$$\begin{aligned} [m]_{\equiv_k} &= \{n \in \mathbb{Z} \mid n \equiv_k m\} \\ &= \{n \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z} : n = m + k\ell\} \\ &= \{\ldots, m - k, m, m + k, m + 2k, \ldots\}. \end{aligned}$$

The quotient is

$$\mathbb{Z}/\!\equiv_k \; = \big\{[0], [1], \ldots, [k-1]\big\}.$$

We call this set the *integers modulo k*. It is usually denoted $\mathbb{Z}_k$.

Definition. The *quotient map* associated to $(A, \sim)$ is the function

$$\begin{aligned} q : A &\to A/\!\sim \\ a &\mapsto [a]. \end{aligned}$$

9 Constructions of number systems

9.1 The complex numbers $\mathbb{C}$

Definition. The *complex numbers* $(\mathbb{C}, +, \times)$ comprise

1. the set $\mathbb{C} = \mathbb{R}^2$,
2. the binary operation
$$\begin{aligned} + : \quad \mathbb{C}^2 &\longrightarrow \mathbb{C} \\ ((a,b),(a',b')) &\longmapsto (a+a', b+b'), \end{aligned}$$
3. the binary operation
$$\begin{aligned} \times : \quad \mathbb{C}^2 &\longrightarrow \mathbb{C} \\ ((a,b),(a',b')) &\longmapsto (aa'-bb', ab'+a'b). \end{aligned}$$

Remarks. i. We usually write (a,b) as $a+bi$.

ii. The value $i = (0,1)$ is called the *imaginary unit*.

Proposition. *We have $i^2 = -1$.*

Proof. A straightforward computation yields

$$\begin{aligned} (0,1)\cdot(0,1) &= (0\cdot 0 - 1\cdot 1, 0\cdot 1 - 1\cdot 0) \\ &= (0,-1). \end{aligned}$$

□

9.2 The rational numbers $\mathbb{Q}$

Let $\sim$ be the relation on $\{(p,q) \in \mathbb{Z}^2 \mid q \neq 0\} \subseteq \mathbb{Z}^2$ given by

$$(p,q) \sim (p',q') \iff pq' = p'q.$$

Proposition. *The relation $\sim$ is an equivalence relation on $\{(p,q) \in \mathbb{Z}^2 \mid q \neq 0\}$.*

Proof. Let $(p,q) \in \mathbb{Z}^2$. From $pq = pq$ it follows that $(p,q) \sim (p,q)$, whence $\sim$ is reflexive.

Suppose that $(p,q) \sim (p',q')$ and $(p',q') \sim (p'',q'')$. If $p' = 0$. Thus,

$$pq' = p'q \qquad \text{and} \qquad p'q'' = p''q'.$$

If $p' = 0$, then it immediately follows that $p = p'' = 0$ and consequently that $(p,q) \sim (p'',q'')$. Hence suppose that $p \neq 0$. Multiplying the preceding equalities together provides

$$pp'q'q'' = p'p''qq'.$$

and dividing through by $p'q'$ yields $pq'' = p''q$, so that $(p,q) \sim (p'',q'')$. Therefore, $\sim$ is transitive.

Finally, the symmetry of $\sim$ follows directly from that of the relation $=$ on $\mathbb{Z}$. □

Definition. The *rational numbers* $(\mathbb{Q}, +, \times)$ consist of

1. the set $\mathbb{Q} = \{(p,q) \in \mathbb{Z}^2 \mid q \neq 0\} / \sim$,

2. the binary operation

$$\begin{aligned} + : \quad \mathbb{Q}^2 &\longrightarrow \mathbb{Q} \\ \big([(p,q)], [(p',q')]\big) &\longmapsto \big[(pq' + p'q, qq')\big], \end{aligned}$$

3. the binary operation

$$\begin{aligned} \times : \quad \mathbb{Q}^2 &\longrightarrow \mathbb{Q} \\ \big([(p,q), (p',q')]\big) &\longmapsto \big[(pp', qq')\big]. \end{aligned}$$

Remarks. i. We typically write $\big[(p,q)\big] \in \mathbb{Q}$ as $\frac{p}{q}$.

ii. In our definition, we have assumed that the operations $+$ and $\times$ are *well-defined*, that is, that they do not depend on the choice of *representatives* (p,q) and (p',q'). Well-definedness will be a topic of a later lecture.

9.3 The integers $\mathbb{Z}$

Define the relation $\sim$ on $\mathbb{N}$ by

$$(m,n) \sim (m',n') \iff m + n' = m' + n.$$

Proposition. *The relation $\sim$ is an equivalence relation on $\mathbb{N}^2$.*

Proof. Symmetry and reflexivity are clear.

Suppose that $(m,n) \sim (m',n')$ and $(m',n') \sim (m'',n'')$. Adding the equalities

$$m + n' = m' + n \qquad \text{and} \qquad m' + n'' = m'' + n'$$

and subtracting $m' + n'$ yields

$$m + n'' = m'' + n.$$

We conclude that $\sim$ is transitive. $\square$

Definition. The *integers* $(\mathbb{Z}, +, \times)$ consist of

i. the set $\mathbb{Z} = \mathbb{N}^2$,

ii. the binary operation

$$\begin{aligned} + : \quad \mathbb{Z}^2 &\longrightarrow \mathbb{Z} \\ ((m,n), (m',n')) &\longmapsto (m + m', n + n'), \end{aligned}$$

iii. the binary operation

$$\begin{aligned} \times : \quad \mathbb{Z}^2 &\longrightarrow \mathbb{Z} \\ ((m,n), (m',n')) &\longmapsto (mm' + nn', mn' + m'n). \end{aligned}$$

Remark. i. We usually write $\big[(m,n)\big] \in \mathbb{Z}$ as $m - n$ when $m \geq n$, and as $-(n-m)$ when $m < n$.

ii. As with $\mathbb{Q}$, we have not yet shown that the operations $+$ and $\times$ are well-defined.

10 Binary operations

Definition. A *magma* $(A, *)$ is a set A equipped with a binary operation $* : A \times A \to A$.

10.1 Properties of operations

Let $* : A \times A \to A$ be a binary operation on A.

Definition. We say that $*$ is

- *commutative* when
$$\forall a, b \in A : a * b = b * a$$
- *associative* when
$$\forall a, b, c \in A : (a * b) * c = a * (b * c)$$

Examples. i. Addition $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is commutative and associative.

ii. Multiplication $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is commutative and associative.

iii. Subtraction $- : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is neither commutative nor associative.

iv. The *partial operation* division $\div : \mathbb{R} \times (\mathbb{R} \backslash \{0\}) \to \mathbb{R}$ is neither commutative nor associative.

v. The cross product $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ is neither commutative nor associative.

vi. Union, intersection, and symmetric difference $\cup, \cap, \Delta : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A)$ are commutative and associative for any set A.

vii. When $n \geq 2$, we have that $n \times n$ matrix multiplication $\mathrm{Mat}_{n,n}(\mathbb{R}) \times \mathrm{Mat}_{n,n}(\mathbb{R}) \to \mathrm{Mat}_{n,n}(\mathbb{R})$ is associative but *not* commutative.

viii. The midpoint operator $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by
$$x * y = \frac{x + y}{2}$$
is commutative but not associative.

Definition. We say that $(A, *)$ is a *semigroup* when $*$ is associative. If $*$ is additionally commutative, then $(A, *)$ is called a *commutative semigroup*.

10.2 Identity elements

Definition. We say that $e \in A$ is an *identity element* for $* : A \times A \to A$ when
$$\forall a \in A : a * e = a = e * a.$$

Remarks. i. The element e is also called a *neutral element*, or simply an *identity*.

ii. When $*$ is considered as a multiplication opperation, e is sometimes written $1 \in A$. When it is considered as an addition operation, it is sometimes written $0 \in A$.

iii. If e satisfies
$$\forall a \in A : a * e = a,$$
then it is called a *right identity*. Likewise, if it satisfies
$$\forall a \in A : e * a = a,$$
then it is called a *left identity*.

Examples. i. $0 \in \mathbb{R}$ is an identity for $(\mathbb{R}, +)$

ii. $1 \in \mathbb{R}$ is an identity for $(\mathbb{R}, \cdot)$

iii. Subtraction $- : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ does not admit an identity element $e \in \mathbb{R}$

iv. $\varnothing \in \mathcal{P}(A)$ is an identity for $(\mathcal{P}(A), \cup)$

v. $\varnothing \in \mathcal{P}(A)$ is also an identity for $(\mathcal{P}(A), \Delta)$

vi. $A \in \mathcal{P}(A)$ is an identity for $(\mathcal{P}(A), \cap)$

vii. The $n \times n$ identity matrix $I_n \in \mathrm{Mat}_{n,n}(\mathbb{R})$ is an identity for $(\mathrm{Mat}_{n,n}(\mathbb{R}), \cdot)$

viii. The midpoint operator on $\mathbb{R}$ does not admit an identity element $e \in \mathbb{R}$

Proposition. *If $e \in A$ is an identity element for a binary operation $* : A \times A \to A$, then it is unique with this property.*

Proof. If $e, e' \in A$ are both identities for $*$, then

$$e = e * e' = e'.$$

□

Definition. A semigroup $(A, *)$ that admits an identity element $e \in A$ is called a *monoid*.

10.3 Inverse elements

Let $*$ be a binary operation on A, and let $e \in A$ be an identity element.

Definition. Fix an element $a \in A$. If $b \in A$ satisfies

$$a * b = e = b * a$$

then b is called an *inverse element* of a, and we write $b = a^{-1}$.

Proposition. *If b satisfies $a * b = e$ (resp. $b * a = e$), then b is called a* right (resp. left) inverse *of a.*

Remark. Let $(A, *)$ be a semigroup. If $b \in A$ is an inverse of $a \in A$, then b is unique with this property.

Proof. If $b, b' \in A$ are inverses of a, then

$$\begin{aligned} b &= e * b \\ &= (b' * a) * b \\ &= b' * (a * b) \\ &= b' * e \\ &= b'. \end{aligned}$$

□

Examples. i. In $(\mathbb{R}, +)$, the inverse of $x \in \mathbb{R}$ is $-x$.

ii. In $(\mathbb{R}, \cdot)$, the inverse of $x \in \mathbb{R}\backslash\{0\}$ is $\frac{1}{x}$. The element $0 \in \mathbb{R}$ does not have an inverse.

iii. In $(\mathcal{P}(A), \cup)$, only $\varnothing \in \mathcal{P}(A)$ has an inverse.

iv. Likewise, in $(\mathcal{P}(A), \cap)$, only $A \in \mathcal{P}(A)$ has an inverse.

v. In $(\mathcal{P}(A), \Delta)$, the inverse of $S \in \mathcal{P}(A)$ is itself.

Definition. A semigroup $(A, *)$ is called a *group* when every $a \in A$ has an inverse $a^{-1} \in A$.

Definition. A group $(A, *)$ is an *abelian group* when $*$ is commutative.

Examples. The following are abelian groups.

i. $(A, +)$ for $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

ii. $(A \backslash \{0\}, \cdot)$ for $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

iii. $(\mathcal{P}(A), \Delta)$ for any set A

11 More algebraic structures

11.1 Rings

Definition. A *ring* $(R,+,\cdot)$ comprises a set R and two binary operations $+,\cdot : R \times R \to R$, such that

i. $(R,+)$ is an abelian group,

ii. $(R,\cdot)$ is a monoid,

iii. the operation $\cdot$ *distributes* over $+$, that is, for all $a,b,c \in R$,

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

Remarks. i. We typically call $+$ *addition* and $\cdot$ *multiplication.*

ii. The additive identity of R is conventionally denoted $0 \in R$ and called *zero, and the multiplicative identity by* $1 \in R$ *and called* one.

iii. If the multiplication $\cdot$ *is commutative, then* $(R,+,\cdot)$ *is called a* commutative ring.

iv. If $(R,+,\cdot)$ *satisfies all the conditions of a ring except for the existence of a multiplicative identity* $1 \in R$*, then it is called a* rng.

Examples. The following are rings:

i. $(R,+,\cdot)$ for $R = \mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$.

ii. $\big(\{0\},+,\cdot\big)$

iii. $(\mathbb{Z}_n,+,\cdot)$

iv. $\big(\mathrm{Mat}_{n,n}(\mathbb{R}),+,\cdot\big)$

v. Fix a set X. Equip the set

$$\mathrm{Fun}(X,\mathbb{R}) = \{f \mid f : X \to \mathbb{R}\}$$

of functions from X to $\mathbb{R}$ with the operations $+$ and $\cdot$ given by

$$(f+g)(x) = f(x) +_{\mathbb{R}} g(x)$$
$$(f \cdot g)(x) = f(x) \cdot_{\mathbb{R}} g(x).$$

The following are *not* rings:

iv. $(\mathbb{N},+,\cdot)$

v. $(2\mathbb{Z},+,\cdot)$

vi. $(\mathbb{R},+,+)$

Definition. A *zero divisor* in a commutative ring $(A,+,\cdot)$ is an element $a \in A$ for which there exists a nonzero $b \in A$ with $ab = 0$.

Definition. A commutative ring $(R,+,\cdot)$ is called an *integral domain* when

i. it does not contain any nonzero zero divisor,

ii. $0 \neq 1$.

Examples. i. $(R,+,\cdot)$ for $R = \mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$

Nonexamples. ii. $\big(\{0\},+,\cdot\big)$

iii. $\big(\mathbb{Z}_4,+,\cdot\big)$

11.2 Fields

Definition. An integral domain $(R, +, \cdot)$ is called a *field* when every nonzero element $a \in R\backslash\{0\}$ has a multiplicative inverse $a^{-1} \in R$,

Examples. i. $(A, +, \cdot)$ for $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

ii. $(\mathbb{Z}_2, +, \cdot)$

iii. $(\mathbb{Z}_p, +, \cdot)$ for prime $p \in \mathbb{N}$

Nonexamples. iv. $(\mathbb{Z}, +, \cdot)$

v. $(\{0\}, +, \cdot)$

vi. $(\mathbb{Z}_n, +, \cdot)$ for $n \in \mathbb{N}$ composite

11.3 Vector spaces

Fix a field k.

Definition. A *k-vector space* $(V, +, \cdot)$ comprises a set V together with operations

$$+ : V \times V \to V$$

and

$$\cdot : k \times V \to V$$

such that

i. $(V, +)$ is an abelian group

ii. *scalar multiplication* $\cdot$ and *vector addition* $+$ satisfy

$$\begin{aligned} 1 \cdot u &= u \\ (a + b) \cdot u &= (a \cdot u) + (b \cdot u) \\ a \cdot (b \cdot u) &= (a \cdot b) \cdot u \\ a \cdot (u + v) &= (a \cdot u) + (a \cdot v) \end{aligned}$$

Remark. We call elements of k *scalars* and those of V *vectors*.

Examples. i. $k = \mathbb{R}$, $V = \mathbb{R}$

ii. $k = \mathbb{R}$, $V = \mathbb{C}$

iii. $k = \mathbb{Q}$, $V = \{0\}$

Nonexamples. iv. $k = \mathbb{Z}$, $V = \mathbb{Z}$

v. $k = \{0\}$, $V = \mathbb{R}$

11.4 Modules

Fix a ring R.

Definition. An *R-module* $(V, +, \cdot)$ comprises a set V together with operations

$$+ : V \times V \to V$$

and

$$\cdot : k \times V \to V$$

that together satisfy the familiar vector space conditions.

Remark. That is, an R-module is a vector space with a ring of scalars R rather than a field of scalars k.

Examples.

i. Every k-vector space $(V, +, \cdot)$ is a k-module, since every field k is a ring.

ii. $R = \mathbb{Z}$, $V = \mathbb{Z}^n$

iii. $R = \{0\}$, $V = \{0\}$

Nonexamples.

iv. $R = \mathbb{N}$, $V = \mathbb{Z}$

12 Homomorphisms

12.1 Informal idea

Informal definition. A *homomorphism* from a structured set X to a structured set Y is a structure-preserving function $f : X \to Y$.

False definition. A homomorphism $f : X \to Y$ is called a

i. *monomorphism* if it is injective,

ii. *epimorphism* if it is surjective,

iii. *isomorphism* if it is bijective.

Definition. i. A homomorphism $f : X \to X$ is called an *endomorphism*.

ii. An isomorphism $f : X \to X$ is called an *automorphism*.

	$f : X \to Y$	$f : X \to X$
—	*homo-*	*endo-*
bijection	*iso-*	*auto-*
injection	*mono-*	—
surjection	*epi-*	—

Remark. Monomorphisms are occasionally denoted $f : X \hookrightarrow Y$, epimorphisms $f : X \twoheadrightarrow Y$, and isomorphisms $f : X \xrightarrow{\sim} Y$.

Definition. We say that X and Y are *isomorphic* if there exists an isomorphism $f : X \xrightarrow{\sim} Y$.

Examples. i. The identity map $\mathrm{id} : X \xrightarrow{\sim} X$ for any structured set X

ii. The inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{R}, +)$

iii. The inclusion $(\mathbb{Q}, +, \cdot) \hookrightarrow (\mathbb{R}, +, \cdot)$

iv. The projection $(\mathbb{Z}, +, \cdot) \twoheadrightarrow (\mathbb{Z}_n, +, \cdot)$

v. The inclusion $(0, +, \cdot) \hookrightarrow (\mathbb{R}, +, \cdot)$

vi.

$$\begin{aligned} f : (\mathbb{Z}, +) &\xrightarrow{\sim} (\mathbb{Z}, +) \\ k &\longmapsto -k \end{aligned}$$

vii. Fix $n \in \mathbb{Z}$ and let

$$\begin{aligned} f_n : (\mathbb{Z}, +) &\xrightarrow{\sim} (\mathbb{Z}, +) \\ k &\longmapsto n \cdot k \end{aligned}$$

viii. $(\mathbb{N}, \leq) \hookrightarrow (\mathbb{Z}, \leq)$

ix.

$$\begin{aligned} f : (\mathbb{R}, \leq) &\xrightarrow{\sim} (\mathbb{R}, \geq) \\ x &\longmapsto -x \end{aligned}$$

x.

$$\begin{aligned} f : (\mathbb{Z}, I) &\longrightarrow (\mathbb{Z}, \cong_2) \\ k &\longmapsto k \end{aligned}$$

Nonexamples. i.

$$\begin{aligned} f : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}, +) \\ x &\longmapsto 1 \end{aligned}$$

ii.

$$\begin{aligned} f : (\mathbb{Z}, +, \cdot) &\longrightarrow (\mathbb{Z}, +, \cdot) \\ k &\longmapsto -k \end{aligned}$$

iii.

$$\begin{aligned} f : (\mathbb{Z}, \cong_2) &\longrightarrow (\mathbb{Z}, I) \\ k &\longmapsto k \end{aligned}$$

iv.

$$\begin{aligned} f : (\mathbb{R}, \leq) &\longrightarrow (\mathbb{R}, \leq) \\ x &\longmapsto x^2 \end{aligned}$$

12.2 Formal definitions

The definition of *homomorphism* depends on the context. However, it should always be the case that

i. the identity $\mathrm{id} : X \to X$ is a homomorphism,

ii. if $f : X \to Y$ and $g : Y \to Z$ are homomorphisms, then $g \circ f : X \to Z$ is a homomorphism.

Definition. A homomorphism $f : X \to Y$ is called a

i. *monomorphism* if
$$\forall (g, g' : Z \to X) : (f \circ g = f \circ g') \implies g = g',$$
that is, f is *left-cancellative*,

ii. *epimorphism* if
$$\exists (h : Y \to X) : (h \circ f = h' \circ f) \implies h = h',$$
that is, f is *right-cancellative*,

iii. *isomorphism* if
$$\exists (k : Y \to X) : (f \circ k = \mathrm{id}_Y) \wedge (k \circ f = \mathrm{id}_X),$$
that is, f has an *inverse* k.

	homomorphism	isomorphism
set	function	bijection
group, ring, field	(group, ...) homomorphism	(group, ...) isomorphism
vector space, module	linear map	linear isomorphism
partial order	monotone map	order isomorphism
topological space	continuous map	homeomorphism
metric space	cont. map	homeo.
alternatively	isometric embedding	isometry

Definition. A *group homomorphism* from $(G, \cdot)$ to $(H, *)$ is a function $f : G \to H$ such that

$$\forall g, g' \in G \ : \ f(g \cdot g') = f(g) * f(g').$$

Example. Fix $n \in \mathbb{N}_+$. The map

$$\begin{aligned} f : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_n, +) \\ k &\longmapsto k \mod n \end{aligned}$$

is a group homomorphism.

Definition. A *ring homomorphism* from $(R, +, \cdot)$ to $(S, \oplus, *)$ is a function $f : R \to S$ such that for all $r, r' \in R$,

i. $f(r + r') = f(r) \oplus f(r')$,

ii. $f(r \cdot r') = f(r) * f(r')$,

iii. $f(1_R) = 1_S$.

Remarks. i. A *field homomorphism* is a ring homomorphism between fields.

ii. If we omit the condition that $f(1_R) = 1_S$, then we have the definition of a *nonunital ring homomorphism* (or a *rng homomorphism*).

Example. The map $f : \mathbb{Z} \to \mathbb{Z}_2$ given by

$$f(k) = \begin{cases} 0 & \text{if } k \text{ is even,} \\ 1 & \text{if } k \text{ is odd.} \end{cases}$$

is a ring homomorphism.

Example. The map

$$\begin{aligned} f(k) : \mathbb{Z} &\to \mathbb{Z} \\ k &\mapsto 2k \end{aligned}$$

is not a ring homomorphism, but is a nonunital ring homomorphism.

Definition. A *monotone map* of posets from $(A, \leq)$ to $(B, \preccurlyeq)$ is a function $f : A \to B$ such that

$$\forall a, a' \in A : a \leq a' \implies f(a) \preccurlyeq f(a').$$

An *order embedding* is an injective monotone map, and an *order isomorphism* is a bijective monotone map.

Example. Let $A = \{0\}$ and $B = \{0, 1\}$, and let $\leq$ and $\preccurlyeq$ be the usual partial orders on A and B, respectively. The map

$$\begin{aligned} f : (A, \leq) &\longrightarrow (B, \preccurlyeq) \\ 0 &\longmapsto 0 \end{aligned}$$

is an order embedding but not an order isomorphism.

Definition. A *linear map* of k-vector spaces from U to V is a function $f : U \to V$ such that

i. $f(u + u') = f(u) + f(u')$ for all $u, u' \in U$, and

ii. $f(su) = sf(u)$ for all $u \in U$ and $s \in k$.

Remark. Equivalently, $f(u + su') = f(u) + f(su')$ for all $u, u' \in U$ and $s \in k$.

Example. The map $f : \mathbb{R}^3 \to \mathbb{R}^2$ where

$$f(x_1, x_2, x_3) = (2x_1 + x_2, x_2)$$

is linear.

Example. Fix a set A with at least two elements. Let $I \subseteq A \times A$ be the identity relation on A and define the equivalence relation $R = A \times A$. The function

$$\begin{aligned} f : (A, I) &\longrightarrow (A, R) \\ a &\longmapsto a \end{aligned}$$

is both a monomorphism and an epimorphism, but not an isomorphism.

12.3 Proofs with group homomorphisms

Proposition. *If $\phi : G \to H$ is a group homomorphism, then $\phi(1_G) = 1_H$.*

Proof. We have

$$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1).$$

The result follows by multiplying each side by $\phi(1)^{-1}$. □

Proposition. *If $\phi : G \to H$ is a group homomorphism, then $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.*

Proof. Multiply each side of

$$\phi(g) \cdot \phi(g^{-1}) = \phi(g \cdot g^{-1}) = \phi(1) = 1$$

on the left by $\phi(g)^{-1}$. □