JKU: Mathematics for AI 1

Niels Lubbes

October 30, 2023

§1.5: An introduction to proof

Understanding a proposition

- **Goldbach Conjecture:**
  An even natural number is equal to either 2 or the sum of two prime numbers.

Understanding a proposition

- **Goldbach Conjecture:**
  An even natural number is equal to either 2 or the sum of two prime numbers.
- First steps to understand the statement:

  1. What are the **definitions** of the concepts that are used?

  A natural number is an element of $\mathbb{N} := \{1, 2, 3, \ldots\}$.
  The even natural numbers are $\{2n : n \in \mathbb{N}\}$.
  A prime number in $\mathbb{N} \setminus \{1\}$ is not a product of two elements in $\mathbb{N} \setminus \{1\}$.

Understanding a proposition

- **Goldbach Conjecture:**
  An even natural number is equal to either 2 or the sum of two prime numbers.
- First steps to understand the statement:

  1. What are the **definitions** of the concepts that are used?
  A natural number is an element of $\mathbb{N} := \{1, 2, 3, \ldots\}$.
  The even natural numbers are $\{2n : n \in \mathbb{N}\}$.
  A prime number in $\mathbb{N} \setminus \{1\}$ is not a product of two elements in $\mathbb{N} \setminus \{1\}$.

  2. Write down some **examples** in order to obtain intuition.

$$
\begin{aligned}
4 &= 2 + 2 \\
6 &= 3 + 3 \\
8 &= 3 + 5 \\
10 &= 5 + 5 \\
&\vdots
\end{aligned}
$$

Understanding a proposition

- **Goldbach Conjecture:**
  An even natural number is equal to either 2 or the sum of two prime numbers.
- First steps to understand the statement:

  1. What are the **definitions** of the concepts that are used?
  A natural number is an element of $\mathbb{N} := \{1, 2, 3, \ldots\}$.
  The even natural numbers are $\{2n : n \in \mathbb{N}\}$.
  A prime number in $\mathbb{N} \setminus \{1\}$ is not a product of two elements in $\mathbb{N} \setminus \{1\}$.

  2. Write down some **examples** in order to obtain intuition.

$$\begin{aligned} 4 &= 2 + 2 \\ 6 &= 3 + 3 \\ 8 &= 3 + 5 \\ 10 &= 5 + 5 \\ &\vdots \end{aligned}$$

- The conjecture has been computationally verified for $n \leq 4 \cdot 10^{18}$.
  This is however *evidence* for the conjecture but not a *proof*!

Some common structure in proofs

- Recall that $A \iff B$ is defined as

$$(A \implies B) \wedge (A \impliedby B).$$

- Recall that $A \implies B$ is logically equivalent to its contrapositive statement:

$$\neg B \implies \neg A.$$

- A Lemma is usually an intermediate result for some main result called Theorem.

Proof by definition

- We call $n \in \mathbb{N}$ even if $n \in \{2k : k \in \mathbb{N}\}$ and odd otherwise.
- **Lemma.** Let $n \in \mathbb{N}$. Then n is even $\iff$ n^2 is even.

Proof by definition

- We call $n \in \mathbb{N}$ even if $n \in \{2k : k \in \mathbb{N}\}$ and odd otherwise.
- **Lemma.** Let $n \in \mathbb{N}$. Then n is even $\iff$ n^2 is even.

  Proof.
  First, we prove the $\Longrightarrow$ direction:

$$\begin{aligned} n \text{ is even} \quad &\Longrightarrow \quad n = 2k \text{ for some } k \in \mathbb{N} \\ \Longrightarrow \quad n^2 = (2k)^2 = 4k^2 = 2(2k)^2 \quad &\Longrightarrow \quad n^2 \text{ is even.} \end{aligned}$$

Proof by definition

- We call $n \in \mathbb{N}$ even if $n \in \{2k : k \in \mathbb{N}\}$ and odd otherwise.
- **Lemma.** Let $n \in \mathbb{N}$. Then n is even $\iff$ n^2 is even.

  Proof.
  First, we prove the $\Longrightarrow$ direction:

  $$\begin{aligned} n \text{ is even} \quad &\Longrightarrow \quad n = 2k \text{ for some } k \in \mathbb{N} \\ \Longrightarrow \quad n^2 = (2k)^2 = 4k^2 = 2(2k)^2 \quad &\Longrightarrow \quad n^2 \text{ is even.} \end{aligned}$$

  Next, we prove the $\Longleftarrow$ direction by proving its equivalent contrapositive[†] statement: n is odd $\Longrightarrow$ n^2 is odd.

  $$\begin{aligned} n \text{ is odd} \quad &\Longrightarrow \quad n = 2k+1 \text{ for some } k \in \mathbb{N}_0 \\ \Longrightarrow \quad n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \quad &\Longrightarrow \quad n^2 \text{ is odd.} \end{aligned}$$

  Recall.[†] $(A \Longrightarrow B) \iff (\neg B \Longrightarrow \neg A)$.

Proof by definition

- We call $n \in \mathbb{N}$ even if $n \in \{2k : k \in \mathbb{N}\}$ and odd otherwise.
- **Lemma.** Let $n \in \mathbb{N}$. Then n is even $\iff$ n^2 is even.

Proof.
First, we prove the $\implies$ direction:

$$\begin{aligned} n \text{ is even} \quad &\implies \quad n = 2k \text{ for some } k \in \mathbb{N} \\ \implies \quad n^2 = (2k)^2 = 4k^2 = 2(2k)^2 \quad &\implies \quad n^2 \text{ is even.} \end{aligned}$$

Next, we prove the $\impliedby$ direction by proving its equivalent contrapositive[†] statement: n is odd $\implies n^2$ is odd.

$$\begin{aligned} n \text{ is odd} \quad &\implies \quad n = 2k + 1 \text{ for some } k \in \mathbb{N}_0 \\ \implies \quad n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \quad &\implies \quad n^2 \text{ is odd.} \end{aligned}$$

Recall.[†] $(A \implies B) \iff (\neg B \implies \neg A)$.

We showed both the $\implies$ and $\impliedby$ directions and therefore concluded the proof of the lemma.

Proof by definition: Exercise

- **Exercise.**
  Prove that the sum of two odd natural numbers is even.

Proof by definition: another example

- **Theorem.** *Let $f : M \to N$ be a function.*
  Then f is invertible $\iff$ f is bijective.

Proof by definition: another example

- **Theorem.** *Let $f : M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- First recall the definitions!

Proof by definition: another example

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- First recall the definitions!
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that

$$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$

Proof by definition: another example

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*

- First recall the definitions!
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that

  $$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$

  We call f bijective iff f is both surjective and injective.

Proof by definition: another example

- **Theorem.** *Let $f\colon M \to N$ be a function.*
  Then f is invertible $\iff$ f is bijective.

- First recall the definitions!
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that

$$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$

  We call f bijective iff f is both surjective and injective.
  We call f surjective iff $\forall y \in N, \exists x \in M\colon f(x) = y$.

Proof by definition: another example

- **Theorem.** *Let $f\colon M \to N$ be a function.*
  Then f is invertible $\iff$ f is bijective.

- First recall the definitions!
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that

$$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$

  We call f bijective iff f is both surjective and injective.
  We call f surjective iff $\forall y \in N, \exists x \in M\colon f(x) = y$.
  We call f injective iff $\forall x_1, x_2 \in M\colon f(x_1) = f(x_2) \implies x_1 = x_2$.

Proof by definition: another example

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- First recall the definitions!
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that
  $$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$
  We call f bijective iff f is both surjective and injective.
  We call f surjective iff $\forall y \in N, \exists x \in M\colon f(x) = y$.
  We call f injective iff $\forall x_1, x_2 \in M\colon f(x_1) = f(x_2) \implies x_1 = x_2$.
- Try easy but complicated enough examples for understanding.

Proof by definition: another example

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- First recall the definitions!
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that
  $$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$
  We call f bijective iff f is both surjective and injective.
  We call f surjective iff $\forall y \in N, \exists x \in M\colon f(x) = y$.
  We call f injective iff $\forall x_1, x_2 \in M\colon f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$.
- Try easy but complicated enough examples for understanding.
  $f\colon \{1,2\} \to \{a,b\}$, $f(1) := a$ and $f(2) := b$.
  (f is bijective, $f^{-1}(a) = 1$ and $f^{-1}(b) = 2$).
  $g\colon \{1,2\} \to \{a,b,c\}$, $g(1) := a$ and $g(2) := b$.
  (g is not surjective and $g^{-1}(c)$ is not defined).
  $h\colon \{1,2\} \to \{a,b\}$ and $h(1) := h(2) := a$.
  (h is not injective and $h^{-1}(b)$ is not defined).

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- Definitions:
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that
  $$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$
  We call f bijective iff f is both surjective and injective.
  We call f surjective iff $\forall y \in N, \exists x \in M\colon f(x) = y$.
  We call f injective iff $\forall x_1, x_2 \in M\colon f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$.
- **Proof.** Let us first prove the $\Longrightarrow$ direction:

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- Definitions:
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that
  $$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$
  We call f bijective iff f is both surjective and injective.
  We call f surjective iff $\forall y \in N, \exists x \in M\colon f(x) = y$.
  We call f injective iff $\forall x_1, x_2 \in M\colon f(x_1) = f(x_2) \implies x_1 = x_2$.
- **Proof.** Let us first prove the $\implies$ direction:
  $$f \text{ is invertible } \implies \forall y \in N\colon f(f^{-1}(y)) = y$$
  $$\implies \forall y \in N, \exists x \in M\colon f(x) = y \implies f \text{ is surjective.}$$

  $$f \text{ is invertible} \implies$$
  $$\left(\forall x_1, x_2 \in M\colon f(x_1) = f(x_2) \Rightarrow x_1 = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = x_2\right)$$
  $$\implies f \text{ is injective.}$$

  Since f is surjective and injective, we conclude that f is bijective.

- **Theorem.** *Let $f\colon M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- Definitions.
  We call f invertible iff there exists $f^{-1}\colon N \to M$ such that
  $$\forall x \in M\colon f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N\colon f(f^{-1}(y)) = y.$$
  The function f is bijective iff $\forall y \in N, \exists! x \in M\colon f(x) = y$.
- **Proof continued.** Next, we prove the $\Longleftarrow$ direction and thus we assume that the function f is bijective.

- **Theorem.** *Let $f: M \to N$ be a function.*
  Then f is invertible $\iff$ f is bijective.

- Definitions.
  We call f invertible iff there exists $f^{-1}: N \to M$ such that

  $$\forall x \in M: f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N: f(f^{-1}(y)) = y.$$

  The function f is bijective iff $\forall y \in N, \exists! x \in M: f(x) = y$.

- **Proof continued.** Next, we prove the $\Longleftarrow$ direction and thus we assume that the function f is bijective.

  Let $g: N \to M$ be the function that sends $y \in N$ to
  the unique element $x \in M$ such that $f(x) = y$.

  We observe that
  $\forall x \in M: g(f(x)) = g(y) = x$ and
  $\forall y \in N: f(g(y)) = f(x) = y$.

  We conclude that f is invertible with $f^{-1} = g$.

- **Theorem.** *Let $f: M \to N$ be a function. Then f is invertible $\iff$ f is bijective.*
- Definitions.
  We call f invertible iff there exists $f^{-1}: N \to M$ such that
  $$\forall x \in M: f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in N: f(f^{-1}(y)) = y.$$
  The function f is bijective iff $\forall y \in N, \exists! x \in M: f(x) = y$.
- **Proof continued.** Next, we prove the $\Longleftarrow$ direction and thus we assume that the function f is bijective.

  Let $g: N \to M$ be the function that sends $y \in N$ to the unique element $x \in M$ such that $f(x) = y$.

  We observe that
  $\forall x \in M: g(f(x)) = g(y) = x$ and
  $\forall y \in N: f(g(y)) = f(x) = y$.

  We conclude that f is invertible with $f^{-1} = g$.

  As we showed both the $\Longrightarrow$ and $\Longleftarrow$ directions, we concluded the proof of the theorem.

More exercises for proof by definition.

- **Exercise.** Let $f\colon M \to N$ be a function.
  Let $\mathrm{id}_M\colon M \to M$ and $\mathrm{id}_N\colon N \to N$ be the identity functions.
  Prove that $f \circ \mathrm{id}_M = f$ and $\mathrm{id}_N \circ f = f$.

More exercises for proof by definition.

- **Exercise.** Let $f\colon M \to N$ be a function.
  Let $\mathrm{id}_M\colon M \to M$ and $\mathrm{id}_N\colon N \to N$ be the identity functions.
  Prove that $f \circ \mathrm{id}_M = f$ and $\mathrm{id}_N \circ f = f$.

- **Exercise.**
  Proof that the inverse f^{-1} of a function $f\colon M \to N$ is unique.

Some common proof techniques

- When proving the proposition

  $$A \iff B \iff C$$

  it is sufficient to prove

  $$A \Longrightarrow B \Longrightarrow C \Longrightarrow A.$$

  Example. See Theorem 1.26 in lecture notes.

Some common proof techniques

- When proving the proposition

  $$A \iff B \iff C$$

  it is sufficient to prove

  $$A \Longrightarrow B \Longrightarrow C \Longrightarrow A.$$

  Example. See Theorem 1.26 in lecture notes.

- When proving that two sets X and Y are equal:

  Step 1. Take an arbitrary (but fixed) element $x \in X$ and show that $x \in Y$.
  Step 2. Take an arbitrary (but fixed) element $y \in Y$ and show that $y \in X$.

  Exercise. Let $f: M \to N$ be an invertible function and $S \subset N$.
  Prove the following proposition:

  $$\left\{ f^{-1}(y) : y \in S \right\} = \{ x \in M : f(x) \in S \}.$$

  Hint. $x \in \left\{ f^{-1}(y) : y \in S \right\} \Longrightarrow \exists y \in S : x = f^{-1}(y) \Longrightarrow \ldots$

Proof by contradiction

- **Theorem.**
  There does not exist $x \in \mathbb{Q}$ *such that* $x^2 = 2$.

Proof by contradiction

- **Theorem.**
  There does not exist $x \in \mathbb{Q}$ *such that* $x^2 = 2$.

- **Proof.**
  Assume by contradiction that there exists $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof by contradiction

- **Theorem.**
  There does not exist $x \in \mathbb{Q}$ such that $x^2 = 2$.

- **Proof.**
  Assume by contradiction that there exists $x \in \mathbb{Q}$ such that $x^2 = 2$.
  This implies that $x = \frac{m}{n}$ with either m or n being odd
  (otherwise we divide both the numerator and denominator by two).

Proof by contradiction

- **Theorem.**
  There does not exist $x \in \mathbb{Q}$ such that $x^2 = 2$.

- **Proof.**
  Assume by contradiction that there exists $x \in \mathbb{Q}$ such that $x^2 = 2$.
  This implies that $x = \frac{m}{n}$ with either m or n being odd
  (otherwise we divide both the numerator and denominator by two).
  This leads to the following sequence of implications:

$$2 = x^2 = \frac{m^2}{n^2} \Longrightarrow m^2 = 2n^2 \Longrightarrow m^2 \text{ is even}$$

$$\overset{\text{previous lemma}}{\Longrightarrow} m \text{ is even}$$

$$\Longrightarrow \exists k \in \mathbb{Z}\colon 2n^2 = m^2 = (2k)^2 = 4k^2 \Longrightarrow n^2 \text{ is even}$$

$$\overset{\text{previous lemma}}{\Longrightarrow} n \text{ is even.}$$

Proof by contradiction

- **Theorem.**
  There does not exist $x \in \mathbb{Q}$ such that $x^2 = 2$.

- **Proof.**
  Assume by contradiction that there exists $x \in \mathbb{Q}$ such that $x^2 = 2$.
  This implies that $x = \frac{m}{n}$ with either m or n being odd
  (otherwise we divide both the numerator and denominator by two).
  This leads to the following sequence of implications:

$$2 = x^2 = \frac{m^2}{n^2} \implies m^2 = 2n^2 \implies m^2 \text{ is even}$$

$$\overset{\text{previous lemma}}{\implies} m \text{ is even}$$

$$\implies \exists k \in \mathbb{Z}\colon 2n^2 = m^2 = (2k)^2 = 4k^2 \implies n^2 \text{ is even}$$

$$\overset{\text{previous lemma}}{\implies} n \text{ is even.}$$

We arrived at a contradiction as n must be odd.
Hence, we conclude the proof of the theorem.

Proof by induction

- Recall that a predicate $P(n)$ is a proposition depending on a variable n.

- **Induction basis:**
  $P(1)$ is true.

  Induction step:
  If $P(n)$ is true for some $n \in \mathbb{N}$, then $P(n+1)$ is true.

- To prove ($\forall n \in \mathbb{N}\colon P(n)$ is true) it is sufficient to prove both the induction basis and induction step:

$$P(1) \text{ is true} \Longrightarrow P(2) \text{ is true} \Longrightarrow P(3) \text{ is true} \Longrightarrow \dots$$

- **Induction hypothesis:**
  $P(n)$ is true for some $n \in \mathbb{N}$.

Proof by induction

- **Recall.** Induction basis: $P(1)$ is true.
  Induction step: If $P(n)$ is true for some $n \in \mathbb{N}$, then $P(n+1)$ is true.
  Induction hypothesis: $P(n)$ is true for some $n \in \mathbb{N}$.
- **Theorem.** For all $n \in \mathbb{N}$, we have

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Proof by induction

- **Recall.** Induction basis: $P(1)$ is true.
  Induction step: If $P(n)$ is true for some $n \in \mathbb{N}$, then $P(n+1)$ is true.
  Induction hypothesis: $P(n)$ is true for some $n \in \mathbb{N}$.
- **Theorem.** For all $n \in \mathbb{N}$, we have
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$
  Proof. Induction basis:
$$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}.$$
  Induction step: We observe that
$$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + n + 1.$$
  By the induction hypothesis, we have $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ and thus
$$\sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$
  We concluded the proof as we showed both
  the induction basis and induction step. (Recall previous lecture.)

Proof by strong induction

- Let $k \geq 1$ be an integer.
  A predictate $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq k$ if the following holds:
  Induction basis: $P(k)$ is true, and
  Induction step: If $P(i)$ is true for all $k \leq i \leq n$, then $P(n+1)$ is true.

Proof by strong induction

- Let $k \geq 1$ be an integer.
  A predictate $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq k$ if the following holds:
  Induction basis: $P(k)$ is true, and
  Induction step: If $P(i)$ is true for all $k \leq i \leq n$, then $P(n+1)$ is true.
- **Theorem.** For all $n \in \mathbb{N}$ such that $n \geq 2$ there exists $i \in \mathbb{N}$ and prime numbers $p_1, \ldots, p_i$ such that $n = p_1 \cdot p_2 \cdots p_i$.

Proof by strong induction

- Let $k \geq 1$ be an integer.
  A predictate $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq k$ if the following holds:
  Induction basis: $P(k)$ is true, and
  Induction step: If $P(i)$ is true for all $k \leq i \leq n$, then $P(n+1)$ is true.
- **Theorem.** For all $n \in \mathbb{N}$ such that $n \geq 2$ there exists $i \in \mathbb{N}$ and prime numbers $p_1, \ldots, p_i$ such that $n = p_1 \cdot p_2 \cdots p_i$.

  Proof. Induction basis:
  $n = 2$ is a prime number and thus the proposition is true with $i = 1$.

  Induction step:
  We make a case distinction on whether $n + 1$ is prime.

  case 1: If $n + 1$ is prime, then the proposition is true with $i = 1$.

Proof by strong induction

- Let $k \geq 1$ be an integer.
  A predictate $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq k$ if the following holds:
  Induction basis: $P(k)$ is true, and
  Induction step: If $P(i)$ is true for all $k \leq i \leq n$, then $P(n+1)$ is true.
- **Theorem.** For all $n \in \mathbb{N}$ such that $n \geq 2$ there exists $i \in \mathbb{N}$ and prime numbers $p_1, \ldots, p_i$ such that $n = p_1 \cdot p_2 \cdots p_i$.

  Proof. Induction basis:
  $n = 2$ is a prime number and thus the proposition is true with $i = 1$.

  Induction step:
  We make a case distinction on whether $n+1$ is prime.

  case 1: If $n+1$ is prime, then the proposition is true with $i = 1$.

  case 2: Suppose that $n+1$ is not prime. In this case, $n+1 = a \cdot b$ for some $a, b \in \mathbb{N}$ such that $2 \leq a, b \leq n$. By the induction hypothesis there exists finitely many prime numbers $p_1, \ldots, p_i$ and $q_1, \ldots, q_j$ such that

  $$a = p_1 \cdots p_i \quad \text{and} \quad b = q_1 \cdots q_j.$$

  Thus $n+1 = a \cdot b$ is indeed a product of finitely many prime numbers.
  We conclude the proof as we considered both cases for the induction step.

Proof by strong induction: exercise.

- **Exercise.**

  Prove that $2^n > 2n + 1$ for all natural numbers $n \geq 3$.
  Hint. use induction.

§1.6: Bounded sets, infimum and supremum

Upper bound, maximum and supremum

- Suppose that $A \subset \mathbb{R}$.

Upper bound, maximum and supremum

- Suppose that $A \subset \mathbb{R}$.
- A upper bound for A is (if it exists) defined as $c \in \mathbb{R}$ such that $a \leq c$ for all $a \in A$.

  Examples. The closed interval $[-1, 3]$ has 3 and 4.1 as upper bounds.
  We say that $[-1, 3]$ is bounded from above.
  Similarly, the half open interval $[-2, 4)$ is bounded from above.
  The set $\mathbb{N} = \{1, 2, \ldots\}$ is not bounded from above.

Upper bound, maximum and supremum

- Suppose that $A \subset \mathbb{R}$.
- A upper bound for A is (if it exists) defined as $c \in \mathbb{R}$ such that $a \leq c$ for all $a \in A$.

  Examples. The closed interval $[-1, 3]$ has 3 and 4.1 as upper bounds. We say that $[-1, 3]$ is bounded from above.
  Similarly, the half open interval $[-2, 4)$ is bounded from above.
  The set $\mathbb{N} = \{1, 2, \ldots\}$ is not bounded from above.
- The maximum $\max A$ for A is (if it exists) defined as the element $c \in A$ such that $a \leq c$ for all $a \in A$.

  Examples. $\max\{1, 2, 5\} = 5$, $\max[-1, 3] = 3$ and $\max(-1, 5] = 5$.
  However, the maximum of the open interval $(-1, 5)$ does not exist.

Upper bound, maximum and supremum

- Suppose that $A \subset \mathbb{R}$.
- A upper bound for A is (if it exists) defined as $c \in \mathbb{R}$ such that $a \le c$ for all $a \in A$.

  Examples. The closed interval $[-1, 3]$ has 3 and 4.1 as upper bounds.
  We say that $[-1, 3]$ is bounded from above.
  Similarly, the half open interval $[-2, 4)$ is bounded from above.
  The set $\mathbb{N} = \{1, 2, \ldots\}$ is not bounded from above.
- The maximum $\max A$ for A is (if it exists) defined as the element $c \in A$ such that $a \le c$ for all $a \in A$.

  Examples. $\max\{1, 2, 5\} = 5$, $\max[-1, 3] = 3$ and $\max(-1, 5] = 5$.
  However, the maximum of the open interval $(-1, 5)$ does not exist.
- The supremum $\sup A$ for A is (if it exists) defined as $c \in \mathbb{R}$ such that $a \le c$ for all $a \in A$ and
  for all $\epsilon > 0$ there exists $b \in A$ such that $b > c - \epsilon$.

  Examples. $\sup(-1, 5) = 5$ and $\sup\{1, 2, 5\} = \max\{1, 2, 5\} = 5$.
  The supremum is a least upper bound.

Lower bound, minimum and infimum

- Suppose that $A \subset \mathbb{R}$.

Lower bound, minimum and infimum

- Suppose that $A \subset \mathbb{R}$.
- A lower bound for A is (if it exists) defined as $c \in \mathbb{R}$ such that $c \leq a$ for all $a \in A$.

  Examples.
  The closed interval $[-1, 3]$ has -1, -2 and -1.1 as lower bounds.
  We say that $[-1, 3]$ is bounded from below.
  The set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is not bounded from below.

Lower bound, minimum and infimum

- Suppose that $A \subset \mathbb{R}$.
- A lower bound for A is (if it exists) defined as $c \in \mathbb{R}$ such that $c \leq a$ for all $a \in A$.

  Examples.
  The closed interval $[-1, 3]$ has -1, -2 and -1.1 as lower bounds.
  We say that $[-1, 3]$ is bounded from below.
  The set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is not bounded from below.
- The minimum $\min A$ for A is (if it exists) defined as the element $c \in A$ such that $c \leq a$ for all $a \in A$.

  Examples. $\min\{1, 2, 5\} = 1$, $\min[-1, 3] = -1$ and $\min[-1, 5) = -1$.
  However, the minimum of the open interval $(-1, 5)$ does not exist.

Lower bound, minimum and infimum

- Suppose that $A \subset \mathbb{R}$.
- A lower bound for A is (if it exists) defined as $c \in \mathbb{R}$ such that $c \leq a$ for all $a \in A$.

  Examples.
  The closed interval $[-1, 3]$ has -1, -2 and -1.1 as lower bounds.
  We say that $[-1, 3]$ is bounded from below.
  The set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is not bounded from below.
- The minimum $\min A$ for A is (if it exists) defined as the element $c \in A$ such that $c \leq a$ for all $a \in A$.

  Examples. $\min\{1, 2, 5\} = 1$, $\min[-1, 3] = -1$ and $\min[-1, 5) = -1$.
  However, the minimum of the open interval $(-1, 5)$ does not exist.
- The infimum $\inf A$ for A is (if it exists) defined as $c \in \mathbb{R}$ such that $c \leq a$ for all $a \in A$ and for all $\epsilon > 0$ there exists $b \in A$ such that $c + \epsilon > b$.

  Examples. $\inf(-1, 5) = -1$ and $\inf\{1, 2, 5\} = \min\{1, 2, 5\} = 1$. The infimum is a greatest lower bound.

- **Completeness Axiom for the real numbers $\mathbb{R}$.**
  If $A \subset \mathbb{R}$ is a non-empty set that is bounded from above,
  then $\sup A$ exists.
- This axiom does not hold for the rational numbers $\mathbb{Q}$. For example,
  $$\sup\left\{x \in \mathbb{Q} : x \leq \sqrt{2}\right\} = \sqrt{2} \notin \mathbb{Q}.$$
  Indeed, for all $q \in \mathbb{Q}$ such that $\sqrt{2} < q$, there exists $r \in \mathbb{Q}$ such that
  $$\sqrt{2} < r < q.$$

- **Completeness Axiom for the real numbers $\mathbb{R}$.**
  If $A \subset \mathbb{R}$ is a non-empty set that is bounded from above, then $\sup A$ exists.
- This axiom does not hold for the rational numbers $\mathbb{Q}$. For example,
  $$\sup \left\{x \in \mathbb{Q} : x \leq \sqrt{2}\right\} = \sqrt{2} \notin \mathbb{Q}.$$
  Indeed, for all $q \in \mathbb{Q}$ such that $\sqrt{2} < q$, there exists $r \in \mathbb{Q}$ such that
  $$\sqrt{2} < r < q.$$
- **Exercise.** Let $A \subset \mathbb{R}$ and $-A := \{-a : a \in A\}$.
  Prove that if A is a non-empty set that is bounded from above, then $\sup A$ exists and $\sup A = -\inf(-A)$.

Completeness Axiom

- **Completeness Axiom for the real numbers $\mathbb{R}$.**
  If $A \subset \mathbb{R}$ is a non-empty set that is bounded from above, then $\sup A$ exists.

- This axiom does not hold for the rational numbers $\mathbb{Q}$. For example,
  $$\sup\left\{x \in \mathbb{Q} : x \leq \sqrt{2}\right\} = \sqrt{2} \notin \mathbb{Q}.$$
  Indeed, for all $q \in \mathbb{Q}$ such that $\sqrt{2} < q$, there exists $r \in \mathbb{Q}$ such that
  $$\sqrt{2} < r < q.$$

- **Exercise.** Let $A \subset \mathbb{R}$ and $-A := \{-a : a \in A\}$.
  Prove that if A is a non-empty set that is bounded from above, then $\sup A$ exists and $\sup A = -\inf(-A)$.

- **Exercise.**
  Prove that if $A \subset \mathbb{R}$ is a non-empty set that is bounded from below, then $\inf A$ exists.
  Hint. Use the completeness axiom and the previous exercise

Determining the infimum of some set

- **Theorem.**
  For all $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

  Proof. See lecture notes.

Determining the infimum of some set

- **Theorem.**
  For all $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

  Proof. See lecture notes.

- **Proposition.** $\inf\left\{\frac{1}{n} : n \in \mathbb{N}\right\} = 0$.

Determining the infimum of some set

- **Theorem.**
  For all $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

  Proof. See lecture notes.

- **Proposition.** $\inf \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = 0$.

  Proof. We observe that 0 is a lower bound.
  Now suppose by contradiction that there exists $\epsilon > 0$ such that

  $$\inf \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = \epsilon.$$

  We arrive at a contradiction with the Theorem as $\frac{1}{n} < \epsilon$ for some $n \in \mathbb{N}$ and thus ϵ is not a lower bound of the set.

Determining the infimum of some set

- **Theorem.**
  For all $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

  Proof. See lecture notes.

- **Proposition.** $\inf \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = 0.$

  Proof. We observe that 0 is a lower bound.
  Now suppose by contradiction that there exists $\epsilon > 0$ such that

  $$\inf \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = \epsilon.$$

  We arrive at a contradiction with the Theorem as $\frac{1}{n} < \epsilon$ for some $n \in \mathbb{N}$ and thus ϵ is not a lower bound of the set.

- **Proposition.** $\max \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = 1.$

Determining the infimum of some set

- **Theorem.**
  For all $\epsilon > 0$ there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

  Proof. See lecture notes.

- **Proposition.** $\inf \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = 0$.

  Proof. We observe that 0 is a lower bound.
  Now suppose by contradiction that there exists $\epsilon > 0$ such that
  $$\inf \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = \epsilon.$$
  We arrive at a contradiction with the Theorem as $\frac{1}{n} < \epsilon$ for some $n \in \mathbb{N}$ and thus ϵ is not a lower bound of the set.

- **Proposition.** $\max \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} = 1$.

  Proof. Follows from the fact that $1 \in \left\{ \frac{1}{n} : n \in \mathbb{N} \right\}$ and $\frac{1}{n} \leq 1$ for all $n \in \mathbb{N}$.

- **Exercise.** Let
$$A = \left\{ \frac{1}{n^2 - n - 3} : n \in \mathbb{N} \right\}.$$
Compute, if it exists, the following quantities:
$$\inf A, \qquad \sup A, \qquad \min A, \qquad \max A.$$

§1.7: Some basic combinatorial objects, identities and inequalities

Factorial

- The factorial of $n \in \mathbb{N}$ is defined as

$$n! := 1 \cdot 2 \cdots n.$$

  We define $0! := 1$.

- **Examples.** $3! = 1 \cdot 2 \cdot 3 = 6$ and $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

- The factorial $n!$ is equal to the number of ways to put n distinct balls into n distinct boxes.

- **Problem.** In how many ways can we put 3 distinct balls into 3 distinct boxes?

Factorial

- The factorial of $n \in \mathbb{N}$ is defined as

$$n! := 1 \cdot 2 \cdots n.$$

  We define $0! := 1$.

- **Examples.** $3! = 1 \cdot 2 \cdot 3 = 6$ and $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

- The factorial $n!$ is equal to the number of ways to put n distinct balls into n distinct boxes.

- **Problem.** In how many ways can we put 3 distinct balls into 3 distinct boxes?

  Answer. For the first ball we have 3 choices, for the second ball 2 choices and for the third ball only 1 choice. Thus, there are $3!$ ways.

Factorial

- The factorial of $n \in \mathbb{N}$ is defined as

$$n! := 1 \cdot 2 \cdots n.$$

  We define $0! := 1$.

- **Examples.** $3! = 1 \cdot 2 \cdot 3 = 6$ and $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

- The factorial $n!$ is equal to the number of ways to put n distinct balls into n distinct boxes.

- **Problem.** In how many ways can we put 3 distinct balls into 3 distinct boxes?

  Answer. For the first ball we have 3 choices, for the second ball 2 choices and for the third ball only 1 choice. Thus, there are 3! ways.

- **Exercise.** In how many ways can you write a 9-digit number that contains each digit in $\{1, \ldots, 9\}$?

Binomial coefficient

- For $n, k \in \mathbb{N}_0$ the binomial coefficient is defined as
$$\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}.$$
- The binomial coefficient $\binom{n}{k}$ shows in how many ways we can put k identical balls into n distinct boxes such that each box receives at most one ball.
- With a k-element set we mean a set that consists of k elements.
- **Problem.**
In how many ways can we choose a 2-element subset from $\{1, 2, 3\}$?

Binomial coefficient

- For $n, k \in \mathbb{N}_0$ the binomial coefficient is defined as

$$\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}.$$

- The binomial coefficient $\binom{n}{k}$ shows in how many ways we can put k identical balls into n distinct boxes such that each box receives at most one ball.
- With a k-element set we mean a set that consists of k elements.
- **Problem.**
  In how many ways can we choose a 2-element subset from $\{1, 2, 3\}$?

  Answer. There are three boxes (labeled 1, 2 or 3) and there are two identical balls: $\binom{3}{2} = \frac{3!}{2! \cdot 1!} = 3$.

Binomial coefficient

- For $n, k \in \mathbb{N}_0$ the binomial coefficient is defined as

$$\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}.$$

- The binomial coefficient $\binom{n}{k}$ shows in how many ways we can put k identical balls into n distinct boxes such that each box receives at most one ball.
- With a k-element set we mean a set that consists of k elements.
- **Problem.**
  In how many ways can we choose a 2-element subset from $\{1, 2, 3\}$?

  Answer. There are three boxes (labeled 1, 2 or 3) and there are two identical balls: $\binom{3}{2} = \frac{3!}{2! \cdot 1!} = 3$.
- More generally, the number of k-element subsets of an n-element set is equal to $\binom{n}{k}$.

- **Lemma.** For all $n, k \in \mathbb{N}$ such that $k \leq n-1$, we have
$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$
- **Proof.** Let

  $A :=$ set of $(k+1)$-element subsets of $S := \{1, \ldots, n+1\}$,
  $B :=$ set of k-element subsets of $\{1, \ldots, n\}$,
  $C :=$ set of $(k+1)$-element subsets of $\{1, \ldots, n\}$,

  and recall that
$$|A| = \binom{n+1}{k+1}, \qquad |B| = \binom{n}{k}, \qquad |C| = \binom{n}{k+1}.$$
- We observe that
$$|A| = |U| + |V|,$$
  where

  $U :=$ set of $(k+1)$-element subsets of S containing $n+1$,
  $V :=$ set of $(k+1)$-element subsets of S not containing $n+1$.
- The function $B \to U$ that sends $\{b_1, \ldots, b_k\}$ to $\{b_1, \ldots, b_k, n+1\}$ is a bijection and thus $|B| = |U|$. (See exercise on next slide.)
- We observe that $C = V$ and thus $|C| = |V|$.
- We concluded the proof since $|A| = |B| + |C|$.

Exercises related to the lemma

- **Exercise.** Suppose that $n, k \in \mathbb{N}$.
  Let B be the set of k-element subsets of $\{1, \ldots, n\}$.
  Let U be the set of $(k+1)$-element subsets of $\{1, \ldots, n+1\}$ containing the element $n+1$.
    - Determine the sets B and U and construct a bijection $B \to U$ under the assumption that $n = 4$ and $k = 2$.
    - Next, construct a bijection $B \to U$ for all $n, k \in \mathbb{N}$.
    - Express the cardinality $|U|$ in terms of n and k.

- **Exercise.** Suppose that $n, k \in \mathbb{N}$.
  Let B be the set of k-element subsets of $\{1, \ldots, n\}$.
  Let U be the set of $(k+1)$-element subsets of $\{1, \ldots, n+1\}$ containing the element $n+1$.
  - Determine the sets B and U and construct a bijection $B \to U$ under the assumption that $n = 4$ and $k = 2$.
  - Next, construct a bijection $B \to U$ for all $n, k \in \mathbb{N}$.
  - Express the cardinality $|U|$ in terms of n and k.

- **Exercise.** Determine the following numbers for all $0 \leq k \leq 6$:
  - The number of k-element subsets of $\{1, \ldots, 6\}$.
  - The number of all subsets of $\{1, \ldots, 6\}$.

  Conclude from these countings the following numbers for all $0 \leq k \leq 7$:
  - The number of k-element subsets of $\{1, \ldots, 7\}$ that contain 7.
  - The number of k-element subsets of $\{1, \ldots, 7\}$ that do not contain 7.
  - The number of all subsets of $\{1, \ldots, 7\}$.

- **Exercise.** Prove the following identity for all $r, m, n \in \mathbb{N}_0$ such that $r \leq m + n$:
$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}.$$
Hint. Let A and B be sets such that $|A| = m$, $|B| = n$ and $|A \cup B| = m + n$. For all r-element subsets $U \subset A \cup B$ we have that $A \cap U$ is an k-element subset of A and $B \cap U$ is an $(r-k)$-element subset of B where $k = |A \cap U|$.

- **Proposition.** For all $n \in \mathbb{N}$, we have
$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

- **Exercise.** Prove this proposition by induction.
  Hint: Use the previous lemma for the induction step.

- **Proposition.** For all $n \in \mathbb{N}$, we have
$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

- **Exercise.** Prove this proposition by induction.
Hint: Use the previous lemma for the induction step.

- **Alternative Proof.**
Let P be the set of subsets of an n-element set S.

For each subset $U \in P$ and element $e \in S$ the are two choices: either $e \in U$ or $e \notin U$ and thus
$$|P| = 2^{|S|} = 2^n.$$

On the other hand, P contains k-element subsets of S for all $0 \leq k \leq n$ and thus
$$|P| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}.$$

Binomial Theorem

- **Binomial Theorem.** For all $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$, we have

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

- **Example.**

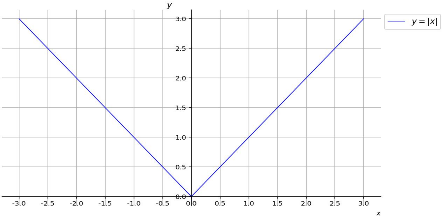
$$\begin{aligned}(x+y)^4 &= (x+y)\cdot(x+y)\cdot(x+y)\cdot(x+y)\\ &= \binom{4}{0}y^4 + \binom{4}{1}xy^3 + \binom{4}{2}x^2y^2 + \binom{4}{3}x^3y + \binom{4}{4}x^4\\ &= y^4 + 4xy^3 + 6y^2x^2 + 4x^3y + x^4\end{aligned}$$

§1.8: Some important functions

- The absolute value of $x \in \mathbb{R}$ is defined as

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

The graph of this function for $x \in [-3, 3]$ is as follows:



Solving inequalities

- **Problem.** Determine the set

$$L := \{x \in \mathbb{R} : |x - 1| < 2\}.$$

- **Problem.** Determine the set

$$L := \{x \in \mathbb{R} : |x - 1| < 2\} .$$

Solution. We make a case distinction:

Solving inequalities

- **Problem.** Determine the set

$$L := \{x \in \mathbb{R} : |x - 1| < 2\}.$$

Solution. We make a case distinction:

- First, suppose that $x - 1 \geq 0$ so that $1 \leq x$.
In this case $|x - 1| = x - 1$ and thus

$$\begin{aligned} L_1 := \{x \in \mathbb{R} : |x - 1| < 2 \ \& \ 1 \leq x\} &= \{x \in \mathbb{R} : x - 1 < 2 \ \& \ 1 \leq x\} \\ &= \{x \in \mathbb{R} : 1 \leq x < 3\}. \end{aligned}$$

- **Problem.** Determine the set

$$L := \{x \in \mathbb{R} : |x-1| < 2\}.$$

Solution. We make a case distinction:

- First, suppose that $x - 1 \geq 0$ so that $1 \leq x$.
  In this case $|x-1| = x-1$ and thus

$$\begin{aligned} L_1 := \{x \in \mathbb{R} : |x-1| < 2 \;\&\; 1 \leq x\} &= \{x \in \mathbb{R} : x-1 < 2 \;\&\; 1 \leq x\} \\ &= \{x \in \mathbb{R} : 1 \leq x < 3\}. \end{aligned}$$

- Next, suppose that $x - 1 < 0$ so that $x < 1$.
  In this case $|x-1| = -(x-1) = 1-x$ and thus

$$\begin{aligned} L_2 := \{x \in \mathbb{R} : |x-1| < 2 \;\&\; x < 1\} &= \{x \in \mathbb{R} : 1-x < 2 \;\&\; x < 1\} \\ &= \{x \in \mathbb{R} : -1 < x < 1\}. \end{aligned}$$

Solving inequalities

- **Problem.** Determine the set

$$L := \{x \in \mathbb{R} : |x-1| < 2\}.$$

Solution. We make a case distinction:

- First, suppose that $x - 1 \geq 0$ so that $1 \leq x$.
  In this case $|x-1| = x-1$ and thus

$$\begin{aligned} L_1 := \{x \in \mathbb{R} : |x-1| < 2 \;\&\; 1 \leq x\} &= \{x \in \mathbb{R} : x-1 < 2 \;\&\; 1 \leq x\} \\ &= \{x \in \mathbb{R} : 1 \leq x < 3\}. \end{aligned}$$

- Next, suppose that $x - 1 < 0$ so that $x < 1$.
  In this case $|x-1| = -(x-1) = 1-x$ and thus

$$\begin{aligned} L_2 := \{x \in \mathbb{R} : |x-1| < 2 \;\&\; x < 1\} &= \{x \in \mathbb{R} : 1-x < 2 \;\&\; x < 1\} \\ &= \{x \in \mathbb{R} : -1 < x < 1\}. \end{aligned}$$

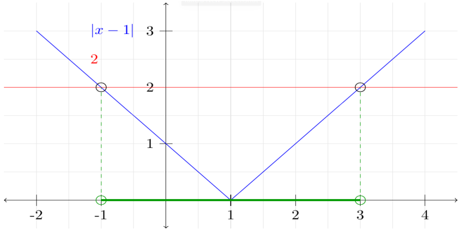
- We conclude that

$$L = L_1 \cup L_2 = \{x \in \mathbb{R} : -1 < x < 3\} = (-1, 3).$$

Solving inequalities

- The graphs of the functions $f(x) := |x-1|$ and $g(x) := 2$ illustrate the solution set

$$\{x \in \mathbb{R} : |x-1| < 2\} = (-1, 3).$$



- **Remark.** Notice that the inequality changes when multiplying both sides with a negative real number.
For example $-6x \geq 8$ implies that $x \leq -\frac{8}{6} = -\frac{4}{3}$.

Solving inequalities

Problem. Determine the set

$$L := \{x \in \mathbb{R} : 2|x+3| - 4|x-1| \geq 8x - 2\}\,.$$

Solution. We make a case distinction:

Case 1. $x+3 \geq 0$ and $x-1 \geq 0$:

$$L_1 := \{x \in \mathbb{R} : 2(x+3) - 4(x-1) \geq 8x-2,\ x+3 \geq 0,\ x-1 \geq 0\} = [1, \tfrac{6}{5}].$$

Case 2. $x+3 \geq 0$ and $x-1 < 0$.

$$L_2 := \{x \in \mathbb{R} : 2(x+3) - 4(-x+1) \geq 8x-2,\ x+3 \geq 0,\ x-1 < 0\} = [-3, 1).$$

Case 3. $x+3 < 0$ and $x-1 \geq 0$.

$$\begin{aligned} L_3 &:= \{x \in \mathbb{R} : 2(-x-3) - 4(x-1) \geq 8x-2,\ x+3 < 0,\ x-1 \geq 0\} \\ &= \{x \in \mathbb{R} : x < -3\ \&\ x \geq 1\} = \varnothing. \end{aligned}$$

Case 4. $x+3 < 0$ and $x-1 < 0$.

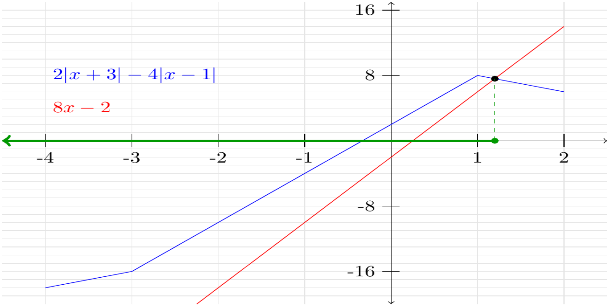
$$L_4 := \{x \in \mathbb{R} : 2(-x-3) - 4(-x+1) \geq 8x-2,\ x+3 < 0,\ x-1 < 0\} = (-\infty, -3).$$

We conclude that

$$L := L_1 \cup L_2 \cup L_3 \cup L_4 = (-\infty, -3) \cup [-3, 1) \cup [1, \tfrac{6}{5}] = (-\infty, \tfrac{6}{5}]$$

- The graphs of the functions $f(x) := 2|x+3| - 4|x-1|$ and $g(x) := 8x - 2$ illustrating the solution set

$$\{x \in \mathbb{R} : 2|x+3| - 4|x-1| \geq 8x - 2\} = (-\infty, \tfrac{6}{5}].$$



- **Exercise.** Determine the set

$$\{x \in \mathbb{R} : 3|x+2| - 4x + 3 \leq 5|x-1|\} .$$

- **Exercise.** Determine the set

$$\{x \in \mathbb{R} : 3|x+2| - 4x + 3 \leq 5|x-1|\}\,.$$

- **Exercise.** Prove that the following three identities hold for all $x \in \mathbb{R}$ and $z \in [0, \infty)$:
  - $|-x| = |x|$.
  - $|x| \leq z \iff -z \leq x \leq z$.
  - $|x| < z \iff -z < x < z$.

  Hint. Use case distinctions.

Triangle inequality

- **Triangle Inequality.** For all $x, y \in \mathbb{R}$ we have

$$|x + y| \leq |x| + |y|.$$

Triangle inequality

- **Triangle Inequality.** For all $x, y \in \mathbb{R}$ we have
$$|x+y| \leq |x| + |y|.$$

- **Proof.** Since $z \leq |z|$ and $-z \leq |z|$ for all $z \in \mathbb{R}$, we have
$$x + y \leq |x| + |y| \quad \text{and} \quad -x - y \leq |x| + |y|.$$
Since $|x+y|$ is equal to either $x+y$ or $-(x+y) = -x-y$, we concluded the proof.

Triangle inequality

- **Triangle Inequality.** For all $x, y \in \mathbb{R}$ we have
$$|x + y| \leq |x| + |y|.$$

- **Proof.** Since $z \leq |z|$ and $-z \leq |z|$ for all $z \in \mathbb{R}$, we have
$$x + y \leq |x| + |y| \quad \text{and} \quad -x - y \leq |x| + |y|.$$
Since $|x + y|$ is equal to either $x + y$ or $-(x + y) = -x - y$, we concluded the proof.

- **Exercise.** Let $x_i \in \mathbb{R}$ for all $1 \leq i \leq n$. Prove the generalized triangle inequality
$$|\sum_i^n x_i| \leq \sum_i^n |x_i|.$$
Hint. Use induction.

Examples of elementary functions

Examples and non-examples of real elementary functions $D \subset \mathbb{R} \to \mathbb{R}$:

function name	examples	non-example
affine linear	$2x + 3, \qquad -3x + \pi$	x^2
constant	$1, \qquad \pi$	x
linear	$2\,x, \qquad -\pi\,x$	$x + 1$
polynomial	$x^2 + \sqrt{2}\,x + 1, \qquad (x+1)^4$	x^π
power	$x^2, \qquad \lvert x\rvert^\pi, \qquad \lvert x\rvert^{-\frac{1}{2}}$	$x^{\frac{1}{2}}$ when $x < 0$
exponential	$2^x, \qquad e^x$	
logarithmic	$\ln\lvert x\rvert, \qquad \log_2\lvert x\rvert$	$\ln x$ when $x < 0$
trigoniometric	$\sin x, \qquad \cos x, \qquad \tan x$	

Exponential and logarithmic function

The exponential function $\exp\colon \mathbb{R} \to (0, \infty)$ is defined as

$$\exp(x) := e^x := \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + \frac{x}{1} + \frac{x^2}{1 \cdot 2} + \frac{x^3}{1 \cdot 2 \cdot 3} + \dots .$$

Euler's number is defined as $e := e^1 \approx 2.7$. For all $x_1, x_2 \in \mathbb{R}$ we have

$$e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2}.$$

Exponential and logarithmic function

The exponential function $\exp\colon \mathbb{R} \to (0,\infty)$ is defined as

$$\exp(x) := e^x := \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + \frac{x}{1} + \frac{x^2}{1\cdot 2} + \frac{x^3}{1\cdot 2\cdot 3} + \dots.$$

Euler's number is defined as $e := e^1 \approx 2.7$. For all $x_1, x_2 \in \mathbb{R}$ we have

$$e^{x_1+x_2} = e^{x_1} \cdot e^{x_2}.$$

The logarithm function $\ln\colon (0,\infty) \to \mathbb{R}$ is defined as the inverse of exp:

$$\ln y := \exp^{-1}(y).$$

For all $y_1, y_2, y \in (0,\infty)$ and $x \in \mathbb{R}$ we have

$$\ln(y_1 \cdot y_2) = \ln(y_1) + \ln(y_2), \qquad e^{\ln y} = y, \qquad \ln(e^x) = x.$$

Exponential and logarithmic function

The exponential function $\exp\colon \mathbb{R} \to (0,\infty)$ is defined as

$$\exp(x) := e^x := \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + \frac{x}{1} + \frac{x^2}{1\cdot 2} + \frac{x^3}{1\cdot 2\cdot 3} + \dots.$$

Euler's number is defined as $e := e^1 \approx 2.7$. For all $x_1, x_2 \in \mathbb{R}$ we have

$$e^{x_1+x_2} = e^{x_1} \cdot e^{x_2}.$$

The logarithm function $\ln\colon (0,\infty) \to \mathbb{R}$ is defined as the inverse of exp:

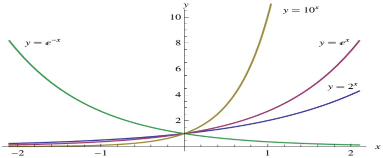
$$\ln y := \exp^{-1}(y).$$

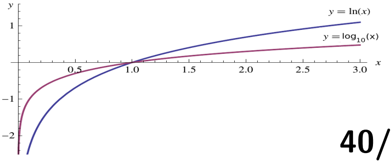
For all $y_1, y_2, y \in (0,\infty)$ and $x \in \mathbb{R}$ we have

$$\ln(y_1 \cdot y_2) = \ln(y_1) + \ln(y_2), \qquad e^{\ln y} = y, \qquad \ln(e^x) = x.$$

We define for all $b \in (0,\infty)$ such that $b \neq 1$:

$$\log_b x := \frac{\ln x}{\ln b}$$





- **Recall.** For all $x, y \in (0, \infty)$ we have

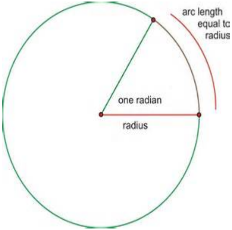
$$\ln(x \cdot y) = \ln(x) + \ln(y), \qquad e^{\ln x} = x, \qquad \ln(e^x) = x.$$

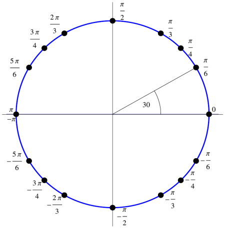
In particular, for all $t > 0$ and constant $c \in (0, \infty)$ we have

$$c^t = e^{\ln(c^t)} = e^{t \ln c}.$$

- **Exercise.** Determine the following sets:
  - $\left\{x \in (4, \infty) : 4\, a^{2x-1}\, b^{4x+3} = 3\, c^{x-4}\right\}$ where $a, b, c > 0$ are constants.
  - $\{x \in (0, \infty) : \log_3 x = 5\}$.
  - $\{x \in (-1, \infty) : 2 \ln(x + 3) - 3 \ln(x + 2) + \ln(x + 1)\}$.

- One radian defines the angle that *subtends* an arc on a circle, so that the length of the arc is equal to the radius of the circle:





An angle of α degrees corresponds to $\frac{\alpha}{180}\pi$ radians.

degrees	0°	30°	45°	60°	90°	180°	270°	360°
radians	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π

Cos, sin and tan functions

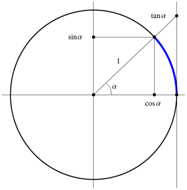
The unit circle is defined as

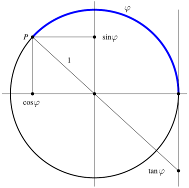
$$\left\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0\right\}.$$

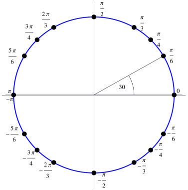
The cosine and sine are the functions $\mathbb{R} \to \mathbb{R}$ such that

$$(\cos\alpha, \sin\alpha)$$

is the end point on the unit-circle of an arc with length α:



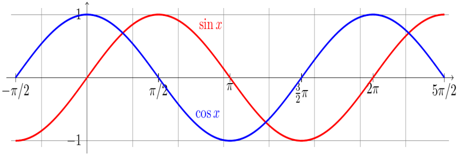


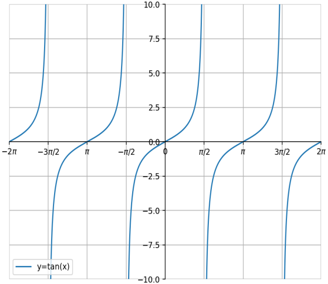


The tangent is the function $\mathbb{R} \setminus \left\{\frac{\pi}{2} + k\pi : k \in \mathbb{Z}\right\} \to \mathbb{R}$ such that

$$\tan\alpha := \frac{\sin\alpha}{\cos\alpha}.$$

Graphs of trigonometric functions:





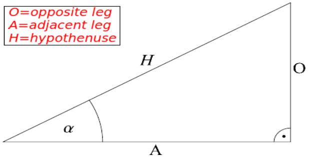
The arccos, arcsin and arctan are defined by the inverses of the following bijective functions respectively

$$\cos\colon [0,\pi] \to [-1,1], \quad \sin\colon [-\tfrac{\pi}{2},\tfrac{\pi}{2}] \to [-1,1], \quad \tan\colon (-\tfrac{\pi}{2},\tfrac{\pi}{2}) \to \mathbb{R}.$$

Formulas for right triangles

Trigoniometric formulas for angles in a right triangle:

$$\sin\alpha = \frac{O}{H}, \quad \cos\alpha = \frac{A}{H}, \quad \tan\alpha = \frac{O}{A}.$$



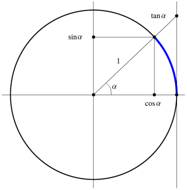
Exercise. Compute without a calculator the points $(\cos\alpha, \sin\alpha)$ for all

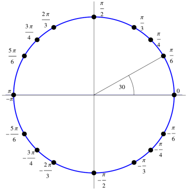
$$\alpha \in \{0, \tfrac{\pi}{6}, \tfrac{\pi}{4}, \tfrac{\pi}{3}, \tfrac{\pi}{2}\}.$$

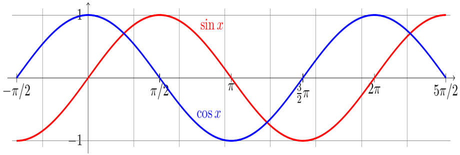
Hint. Consider the triangles with side lengths $(1,1,1)$ and $(1,1,\sqrt{2})$ and use the fact that the angles in a triangle add up to π.

Some trigoniometric identities for cos and sin

Recall that $(\cos\alpha, \sin\alpha)$ is the end point on the unit-circle of an arc with length α:







As a direct consequence, we observe the following identities for all $x \in \mathbb{R}$:

$$\cos^2 x + \sin^2 x = 1$$

$$\begin{aligned}
\cos(x + 2\pi) &= \cos x & \sin(x + 2\pi) &= \sin x \\
\cos(x + \pi) &= -\cos x & \sin(x + \pi) &= -\sin x \\
\cos(x + \tfrac{\pi}{2}) &= -\sin x & \sin(x + \tfrac{\pi}{2}) &= \cos x \\
\cos(-x) &= \cos x & \sin(-x) &= -\sin x
\end{aligned}$$

Applying the trigoniometric identities

- **Exercise.** Compute without calculator the values $\cos \alpha$ and $\sin \beta$ for all
$$\alpha \in \left\{ \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3} \right\} \quad \text{and} \quad \beta \in \left\{ \frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6} \right\},$$
by using the following facts for all $x \in \mathbb{R}$:
    - $\sin \frac{\pi}{6} = \frac{1}{2}$, $\sin \frac{\pi}{4} = \frac{1}{\sqrt{2}}$, $\sin \frac{\pi}{3} = \frac{\sqrt{3}}{2}$, and
    - $\sin(-x) = -\sin x$, $\sin(x + \frac{\pi}{2}) = \cos x$, $\cos(x + \frac{\pi}{2}) = -\sin x$.

Applying the trigoniometric identities

- **Exercise.** Compute without calculator the values $\cos\alpha$ and $\sin\beta$ for all

$$\alpha \in \left\{\tfrac{\pi}{6}, \tfrac{\pi}{4}, \tfrac{\pi}{3}\right\} \quad \text{and} \quad \beta \in \left\{\tfrac{2\pi}{3}, \tfrac{3\pi}{4}, \tfrac{5\pi}{6}\right\},$$

  by using the following facts for all $x \in \mathbb{R}$:
  - $\sin\frac{\pi}{6} = \frac{1}{2}$, $\sin\frac{\pi}{4} = \frac{1}{\sqrt{2}}$, $\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$, and
  - $\sin(-x) = -\sin x$, $\sin(x + \frac{\pi}{2}) = \cos x$, $\cos(x + \frac{\pi}{2}) = -\sin x$.

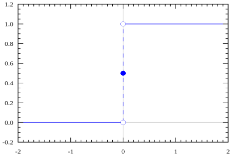
- **Exercise.** Compute

$$\left\{x \in [-\pi, \pi] : \cos x = \tfrac{\sqrt{3}}{2}\right\} \quad \text{and} \quad \left\{x \in [-\pi, \pi] : \sin^2 x = \tfrac{1}{2}\right\}.$$

The Heaviside step and ReLu functions

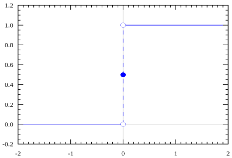
The Heaviside step function $H\colon \mathbb{R} \to \mathbb{R}$ is defined as

$$H(x) := \begin{cases} 1 & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases}$$



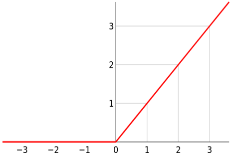
The Heaviside step function $H\colon \mathbb{R} \to \mathbb{R}$ is defined as

$$H(x) := \begin{cases} 1 & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases}$$



The ramp function $r\colon \mathbb{R} \to \mathbb{R}$ is defined as

$$r(x) := \begin{cases} x & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases}$$



In the context of artificial neural networks the ramp function is called a ReLU activation function, where ReLu stands for “rectified linear unit”.

§1.9: Complex numbers

Complex numbers

The set of complex numbers with imaginary unit i is defined as

$$\mathbb{C} := \{x + \mathrm{i}\, y : x, y \in \mathbb{R}\} \quad \text{where} \quad \mathrm{i}^2 = -1.$$

Let $z = x + \mathrm{i}\, y$ be a complex number.

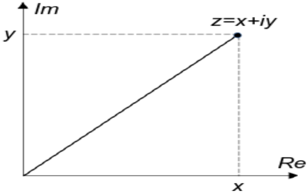
$$\begin{aligned} \mathrm{Re}(z) &:= x \quad \text{(real part)} \\ \mathrm{Im}(z) &:= y \quad \text{(imaginary part)} \end{aligned}$$

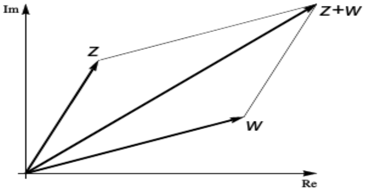
Addition and multiplication of the complex numbers $z = x + \mathrm{i}\, y$ and $w = u + \mathrm{i}\, v$:

$$z + w = (x + \mathrm{i}\, y) + (u + \mathrm{i}\, v) = (x + u) + \mathrm{i}\,(y + v).$$

$$z \cdot w = (x + \mathrm{i}\, y) \cdot (u + \mathrm{i}\, v) = (xu + \mathrm{i}^2 yv) + \mathrm{i}\,(xv + yu) = (xu - yv) + \mathrm{i}\,(xv + yu).$$

We can identify the complex numbers with the complex plane.
Geometrically, the sum $z + w$ is the corner of a parallelogram:





Question. What does multiplication geometrically mean?

The complex conjugate of a complex number $z = x + \imath\, y$ is defined as

$$\overline{z} := x - \imath\, y.$$

We observe that

$$z \cdot \overline{z} = (x + \imath\, y) \cdot (x - \imath\, y) = x^2 + y^2.$$

We can use this to compute the multiplicative inverse of z:

$$z^{-1} = \frac{1}{z} = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{x - \imath\, y}{x^2 + y^2} = \frac{x}{x^2 + y^2} - \imath\, \frac{y}{x^2 + y^2}.$$

Complex numbers form a field

The complex conjugate of a complex number $z = x + \imath\, y$ is defined as

$$\overline{z} := x - \imath\, y.$$

We observe that

$$z \cdot \overline{z} = (x + \imath\, y) \cdot (x - \imath\, y) = x^2 + y^2.$$

We can use this to compute the multiplicative inverse of z:

$$z^{-1} = \frac{1}{z} = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{x - \imath\, y}{x^2 + y^2} = \frac{x}{x^2 + y^2} - \imath\, \frac{y}{x^2 + y^2}.$$

Exercise. Show that $\mathbb{C}$ is a field.
Hint.
Notice that $-z = -x - \imath\, y$ and 0 are the additive inverse and identity, resp.
Moreover, z^{-1} and 1 are the multiplicative inverse and identity, resp.
It remains to show that
complex multiplication and addition are commutative and associative,
and that multiplication distributes over addition.

Problem. Compute the real and imaginary part of

$$\frac{2-3i}{1+5i}.$$

Problem. Compute the real and imaginary part of

$$\frac{2-3\imath}{1+5\imath}.$$

Answer.

$$\frac{2-\imath\,3}{1+\imath\,5}=\frac{(2-\imath\,3)\cdot(1-\imath\,5)}{(1+\imath\,5)\cdot(1-\imath\,5)}=\frac{(2-\imath\,3)\cdot(1-\imath\,5)}{1^2+5^2}=\frac{-13-\imath\,13}{26}=-\tfrac{1}{2}-\imath\,\tfrac{1}{2}.$$

Problem. Compute the real and imaginary part of

$$\sqrt{i}.$$

Problem. Compute the real and imaginary part of

$$\frac{2-3\mathrm{i}}{1+5\mathrm{i}}.$$

Answer.

$$\frac{2-\mathrm{i}\,3}{1+\mathrm{i}\,5} = \frac{(2-\mathrm{i}\,3)\cdot(1-\mathrm{i}\,5)}{(1+\mathrm{i}\,5)\cdot(1-\mathrm{i}\,5)} = \frac{(2-\mathrm{i}\,3)\cdot(1-\mathrm{i}\,5)}{1^2+5^2} = \frac{-13-\mathrm{i}\,13}{26} = -\tfrac{1}{2}-\mathrm{i}\,\tfrac{1}{2}.$$

Problem. Compute the real and imaginary part of

$$\sqrt{i}.$$

Answer. Suppose that $z = x + \mathrm{i}\,y$ with $x, y \in \mathbb{R}$ such that $z^2 = \mathrm{i}$.
By comparing the real and complex part of

$$z^2 = {\color{blue}x^2 - y^2} + \mathrm{i}\,{\color{red}2xy} = {\color{blue}0} + \mathrm{i}\,{\color{red}1} = \mathrm{i},$$

we find that

$$x^2 - y^2 = (x+y)(x-y) = 0 \quad \text{and} \quad 2xy = 1.$$

As $xy > 0$ we deduce that $x + y \neq 0$ and thus $x - y = 0$.
It follows $2x^2 = 1$ so that $x = y = \pm\frac{1}{\sqrt{2}}$ and thus

$$z = \pm\left(\tfrac{1}{\sqrt{2}} + \mathrm{i}\,\tfrac{1}{\sqrt{2}}\right).$$

Problem. Compute the real and imaginary part of

$$\frac{2-3\mathrm{i}}{1+5\mathrm{i}}.$$

Answer.

$$\frac{2-\mathrm{i}\,3}{1+\mathrm{i}\,5}=\frac{(2-\mathrm{i}\,3)\cdot(1-\mathrm{i}\,5)}{(1+\mathrm{i}\,5)\cdot(1-\mathrm{i}\,5)}=\frac{(2-\mathrm{i}\,3)\cdot(1-\mathrm{i}\,5)}{1^2+5^2}=\frac{-13-\mathrm{i}\,13}{26}=-\tfrac{1}{2}-\mathrm{i}\,\tfrac{1}{2}.$$

Problem. Compute the real and imaginary part of

$$\sqrt{i}.$$

Answer. Suppose that $z=x+\mathrm{i}\,y$ with $x,y\in\mathbb{R}$ such that $z^2=\mathrm{i}$.
By comparing the real and complex part of

$$z^2=x^2-y^2+\mathrm{i}\,2xy=0+\mathrm{i}\,1=\mathrm{i},$$

we find that

$$x^2-y^2=(x+y)(x-y)=0 \quad \text{and} \quad 2xy=1.$$

As $xy>0$ we deduce that $x+y\neq 0$ and thus $x-y=0$.
It follows $2x^2=1$ so that $x=y=\pm\frac{1}{\sqrt{2}}$ and thus

$$z=\pm\left(\tfrac{1}{\sqrt{2}}+\mathrm{i}\,\tfrac{1}{\sqrt{2}}\right).$$

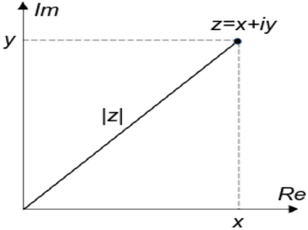
Exercise. What are the possible values of i^n for $n\in\mathbb{N}_0$?

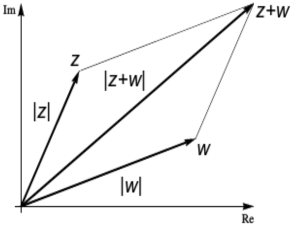
The absolute value of complex numbers

The absolute value of the complex number $z = x + \imath\, y$ is defined as

$$|z| := \sqrt{x^2 + y^2}.$$

The absolute value is equal to the distance between 0 and z in the complex plane:





We see in these examples that

$$\mathrm{Im}(z) = y \leq |z|, \qquad \mathrm{Re}(z) = x \leq |z|, \qquad |z + w| \leq |z| + |w|.$$

The latter is called the triangle inequality for complex numbers.

Triangle inequality

Lemma. For all $a, b \in \mathbb{C}$, we have

$$|a|^2 = \overline{a} \cdot a, \quad \overline{a+b} = \overline{a} + \overline{b}, \quad a + \overline{a} = 2\,\mathrm{Re}(a), \quad \mathrm{Re}(a) \leq |a|, \quad |a \cdot b| = |a| \cdot |b|, \quad |a| = |\overline{a}|.$$

Proof. Exercise.

Theorem (triangle inequality). For all $z, w \in \mathbb{C}$ we have

$$|z+w| \leq |z| + |w|.$$

Proof. As both sides are positive real numbers it suffices to prove that

$$|z+w|^2 \leq (|z| + |w|)^2.$$

We use the above lemma to show this inequality:

$$\begin{gathered}
|z+w|^2 = (z+w) \cdot (\overline{z+w}) = (z+w) \cdot (\overline{z} + \overline{w}) \\
= |z|^2 + (z\overline{w} + \overline{z}w) + |w|^2 = |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 \\
\leq \\
|z|^2 + 2\,|z \cdot \overline{w}| + |w|^2 = |z|^2 + 2\,|z| \cdot |\overline{w}| + |w|^2 \\
= |z|^2 + 2\,|z| \cdot |w| + |w|^2 = (|z| + |w|)^2.
\end{gathered}$$

This completes the proof.

Representations of complex numbers

We consider two equivalent representations of z

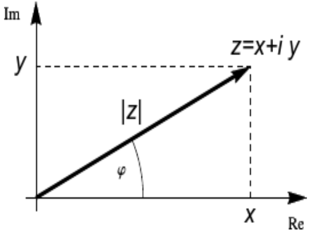
- canonical representation:

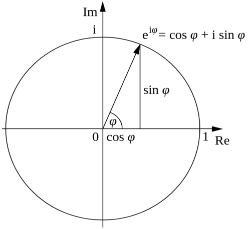
$$z = x + \mathrm{i}\, y.$$

- Euler's formula:

$$z = r \cdot e^{\mathrm{i}\varphi} = r \cdot (\cos\varphi + \mathrm{i}\,\sin\varphi),$$

where $r = |z|$ and $\varphi \in [0, 2\pi)$ is the argument of z.





We call (r, φ) the polar coordinate of z.

Exercise. Show for all $z, w \in \mathbb{C}$ that $|z + w| = |z| + |w|$ if and only if z and w have the same argument.

Convert from polar to canonical representations

Problem. Suppose that z has polar coordinates $(r, \phi) = (2, \frac{\pi}{4})$. Determine the canonical representation of z.

Convert from polar to canonical representations

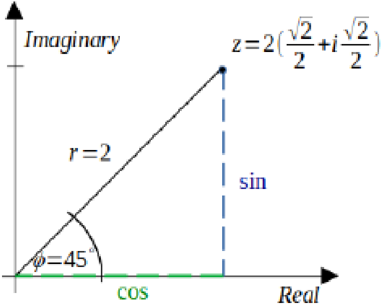
Problem. Suppose that z has polar coordinates $(r, \phi) = (2, \frac{\pi}{4})$. Determine the canonical representation of z.

Answer. We know that

$$\cos\frac{\pi}{4} = \sin\frac{\pi}{4} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$

and thus the canonical representation of z is

$$z = 2 \cdot (\cos\frac{\pi}{4} + \mathrm{i}\,\sin\frac{\pi}{4}) = \sqrt{2} + \mathrm{i}\,\sqrt{2}.$$



Real and imaginary parts using Euler's formula

Problem. Compute the real and imaginary part of

$$e^{\mathrm{i}\varphi} \qquad \text{for all} \qquad \varphi \in \left\{\tfrac{\pi}{2}, \pi, \tfrac{3\pi}{2}, 2\pi\right\}.$$

Real and imaginary parts using Euler's formula

Problem. Compute the real and imaginary part of

$$e^{\mathrm{i}\,\varphi} \qquad \text{for all} \qquad \varphi \in \left\{\tfrac{\pi}{2}, \pi, \tfrac{3\pi}{2}, 2\pi\right\}.$$

Answer. We can read the real and imaginary parts from their canonical representations:

$$\begin{aligned}
e^{\mathrm{i}\,\frac{\pi}{2}} &= \cos\tfrac{\pi}{2} + \mathrm{i}\,\sin\tfrac{\pi}{2} = \mathrm{i},\\
e^{\mathrm{i}\,\pi} &= \cos\pi + \mathrm{i}\,\sin\pi = -1,\\
e^{\mathrm{i}\,\frac{3\pi}{2}} &= \cos\tfrac{3\pi}{2} + \mathrm{i}\,\sin\tfrac{3\pi}{2} = -\mathrm{i},\\
e^{\mathrm{i}\,2\pi} &= \cos 2\pi + \mathrm{i}\,\sin 2\pi = 1.
\end{aligned}$$

Euler's identity is considered to be an exemplar of mathematical beauty as it shows a profound connection between the most fundamental numbers in mathematics:

$$e^{\mathrm{i}\,\pi} + 1 = 0$$

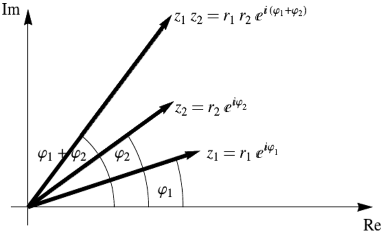
Multiplication and division using exponential representation

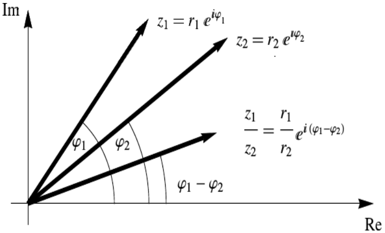
We can use Euler's formula to compute the product, quotient and powers of the complex numbers $z_1 = r_1 e^{\mathrm{i}\,\varphi_1}$, $z_2 = r_2 e^{\mathrm{i}\,\varphi_2}$ and $z = r\, e^{\mathrm{i}\,\varphi}$:

$$z_1 \cdot z_2 = \left(r_1\, e^{\mathrm{i}\varphi_1}\right) \cdot \left(r_2\, e^{\mathrm{i}\varphi_2}\right) = r_1 r_2 e^{\mathrm{i}(\varphi_1+\varphi_2)}.$$

$$\frac{z_1}{z_2} = \frac{r_1\, e^{\mathrm{i}\varphi_1}}{r_2\, e^{\mathrm{i}\varphi_2}} = \frac{r_1}{r_2} e^{\mathrm{i}(\varphi_1-\varphi_2)}.$$

$$z^n = \left(r\, e^{\mathrm{i}\varphi}\right)^n = r^n\, e^{\mathrm{i}n\varphi}.$$





de Moivre's formula: $z^n = r^n\, e^{\mathrm{i}n\varphi} = r^n\left(cos(n\,\varphi) + \mathrm{i}\,\sin(n\,\varphi)\right)$.

Computing powers and quotients of complex numbers

Problem. Compute the arithmetic representations of

$$(1+\mathrm{i})^{12} \qquad \text{and} \qquad \frac{1+\mathrm{i}}{3e^{-\mathrm{i}\frac{\pi}{4}}}.$$

Computing powers and quotients of complex numbers

Problem. Compute the arithmetic representations of

$$(1+\mathrm{i})^{12} \qquad \text{and} \qquad \frac{1+\mathrm{i}}{3e^{-\mathrm{i}\frac{\pi}{4}}}.$$

Answer.

$$(1+\mathrm{i})^{12} = \left(\sqrt{2}\, e^{\mathrm{i}\frac{\pi}{4}}\right)^{12} = 2^6\, e^{\mathrm{i}3\pi} = 64\, e^{\mathrm{i}\pi} = -64.$$

Computing powers and quotients of complex numbers

Problem. Compute the arithmetic representations of

$$(1+\mathfrak{i})^{12} \qquad \text{and} \qquad \frac{1+\mathfrak{i}}{3e^{-\mathfrak{i}\frac{\pi}{4}}}.$$

Answer.

$$(1+\mathfrak{i})^{12} = \left(\sqrt{2}\, e^{\mathfrak{i}\frac{\pi}{4}}\right)^{12} = 2^6\, e^{\mathfrak{i}3\pi} = 64\, e^{\mathfrak{i}\pi} = -64.$$

$$\frac{1+\mathfrak{i}}{3\, e^{-\mathfrak{i}\frac{\pi}{4}}} = \frac{\sqrt{2}\, e^{\mathfrak{i}\,\frac{\pi}{4}}}{3\, e^{-\mathfrak{i}\frac{\pi}{4}}} = \tfrac{\sqrt{2}}{3}\, e^{\mathfrak{i}\,\frac{\pi}{2}} = \tfrac{\sqrt{2}}{3}\, \mathfrak{i}.$$

Problem. Compute the arithmetic representations of

$$(1+\mathrm{i})^{12} \qquad \text{and} \qquad \frac{1+\mathrm{i}}{3e^{-\mathrm{i}\frac{\pi}{4}}}.$$

Answer.

$$(1+\mathrm{i})^{12} = \left(\sqrt{2}\, e^{\mathrm{i}\frac{\pi}{4}}\right)^{12} = 2^6\, e^{\mathrm{i}3\pi} = 64\, e^{\mathrm{i}\pi} = -64.$$

$$\frac{1+\mathrm{i}}{3\, e^{-\mathrm{i}\frac{\pi}{4}}} = \frac{\sqrt{2}\, e^{\mathrm{i}\,\frac{\pi}{4}}}{3\, e^{-\mathrm{i}\frac{\pi}{4}}} = \tfrac{\sqrt{2}}{3}\, e^{\mathrm{i}\,\frac{\pi}{2}} = \tfrac{\sqrt{2}}{3}\,\mathrm{i}.$$

Alternative.

$$\frac{1+\mathrm{i}}{3\, e^{-\mathrm{i}\frac{\pi}{4}}} = \frac{1}{3} \cdot \frac{1+\mathrm{i}}{\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\,\mathrm{i}} \cdot \frac{\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\,\mathrm{i}}{\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\,\mathrm{i}}$$

$$=$$

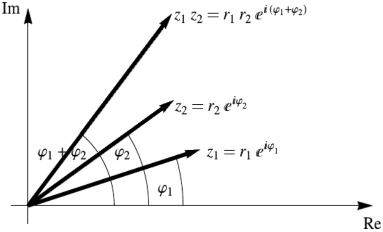
$$\frac{1}{3} \cdot \frac{\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\,\mathrm{i} + \frac{1}{\sqrt{2}}\,\mathrm{i} - \frac{1}{\sqrt{2}}}{\frac{1}{2} + \frac{1}{2}} = \tfrac{\sqrt{2}}{3}\,\mathrm{i}.$$

Multiplication and absolute value

Recall that multiplication of the complex numbers

$$z_1 = r_1 e^{i\varphi_1} \quad \text{and} \quad z_2 = r_2 e^{i\varphi_2}$$

has the following geometric interpretation:



Since $r_1 = |z_1|$ and $r_2 = |z_2|$, we observe that the following identity holds

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|.$$

Quadratic formula

Quadratic-formula. Let $a, b, c \in \mathbb{C}$ and $a \neq 0$.

$$q(x) := a\,x^2 + b\,x + c = 0 \quad \iff \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

If $a, b, c \in \mathbb{R}$, then the following holds:

- If $b^2 - 4ac > 0$, then $q(x)$ has two real zeros.
- If $b^2 - 4ac = 0$, then $q(x)$ has one real zero of multiplicity 2.
- If $b^2 - 4ac < 0$, then $q(x)$ has two nonreal zeros.

Example.

$$x^2 - 3x + 1 = 0 \quad \iff \quad x = \frac{3 \pm \sqrt{5}}{2}.$$

$$x^2 - 2x + 1 = (x-1)^2 = 0 \quad \iff \quad x = 1 \text{ with multiplicity } 2.$$

$$x^2 - x + 1 = 0 \quad \iff \quad x = \frac{1 \pm \mathrm{i}\sqrt{3}}{2}.$$

Remark. For all $u \in R$, we have

$$\sqrt{-u} = \mathrm{i}\sqrt{u}.$$

Roots of complex polynomials

Problem. Determine the following set of solutions

$$\left\{x \in \mathbb{C} : x^2 + (1-\mathrm{i})x - \mathrm{i} = 0\right\}.$$

Answer. We apply the quadratic formula:

$$x = \frac{\mathrm{i} - 1 \pm \sqrt{(1-\mathrm{i})^2 + 4\mathrm{i}}}{2} = \frac{\mathrm{i} - 1 \pm \sqrt{2\mathrm{i}}}{2} = \frac{\mathrm{i} - 1 \pm \sqrt{2}\sqrt{\mathrm{i}}}{2}.$$

We recall that

$$\sqrt{\mathrm{i}} = \tfrac{1}{\sqrt{2}} + \mathrm{i}\,\tfrac{1}{\sqrt{2}},$$

and conclude that the solutions to our equation are

$$x = \frac{\mathrm{i} - 1 + \sqrt{2}\left(\frac{1}{\sqrt{2}} + \mathrm{i}\frac{1}{\sqrt{2}}\right)}{2} = \mathrm{i}$$

and

$$x = \frac{\mathrm{i} - 1 + \sqrt{2}\left(-\frac{1}{\sqrt{2}} - \mathrm{i}\frac{1}{\sqrt{2}}\right)}{2} = -1.$$

This implies that $\left\{x \in \mathbb{C} : x^2 + (1-\mathrm{i})x - \mathrm{i} = 0\right\} = \{\mathrm{i}, -1\}$.

§1.10: Vectors and norms

Addition and scalar multiplication of vectors

A vector $\mathbf{v}$ and the zero vector $\mathbf{0}$ both in $\mathbb{C}^d$ and of dimension $d \in \mathbb{N}$:

$$\mathbf{v} = (v_i)_{i=1}^d = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} \quad \text{and} \quad \mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The addition and scalar multiplication of vectors is for all scalars $\lambda \in \mathbb{C}$ defined as

$$\mathbf{u} + \mathbf{v} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_d \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_d + v_d \end{pmatrix} \quad \text{and} \quad \lambda \cdot \mathbf{u} = \begin{pmatrix} \lambda \cdot u_1 \\ \lambda \cdot u_2 \\ \vdots \\ \lambda \cdot u_d \end{pmatrix}.$$

Euclidean norm and inner product

The Euclidean norm of $\mathbf{v}(v_i)_{i=1}^d \in \mathbb{C}^d$ is a real number:

$$\|\mathbf{v}\|_2 := \sqrt{\sum_{i=1}^{d} |v_i|^2}.$$

The inner product of the vectors $\mathbf{u} = (u_i)_{i=1}^d$ and $\mathbf{v} = (v_i)_{i=1}^d \in \mathbb{C}^d$:

$$\langle \mathbf{u}, \mathbf{v} \rangle := \sum_{i=1}^{d} u_i \bar{v}_i.$$

We observe the following equality:

$$\|\mathbf{v}\|_2 = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}.$$

Remark. If $d = 1$, then the Euclidean norm is the absolute value.

Lemma. The inner product is formally a mapping

$$\langle \cdot, \cdot \rangle \colon \mathbb{C}^d \times \mathbb{C}^d \to \mathbb{C}$$

that satisfies the following properties:

Positive definiteness:
For all $\mathbf{u} \in \mathbb{C}^d$, where $\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} : x > 0\}$:

$$\langle \mathbf{u}, \mathbf{u} \rangle \in \mathbb{R}_{\geq 0} \qquad \text{and} \qquad \langle \mathbf{u}, \mathbf{u} \rangle = 0 \iff \mathbf{u} = \mathbf{0}.$$

Linearity in the first argument:
For all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^d$ and $\lambda \in \mathbb{C}$,

$$\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle \qquad \text{and} \qquad \langle \lambda \cdot \mathbf{u}, \mathbf{v} \rangle = \lambda \cdot \langle \mathbf{u}, \mathbf{v} \rangle.$$

Conjugate symmetry:
For all $\mathbf{u}, \mathbf{v} \in \mathbb{C}^d$,

$$\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$$

Proof. Exercise.

Linearity of inner product

Lemma. For all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^d$ and $\lambda, \mu \in \mathbb{C}$ we have

$\langle \lambda \cdot \mathbf{u} + \mu \cdot \mathbf{v}, \mathbf{w} \rangle = \lambda \cdot \langle \mathbf{u}, \mathbf{w} \rangle + \mu \cdot \langle \mathbf{v}, \mathbf{w} \rangle$ and $\langle \mathbf{u}, \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{w} \rangle = \overline{\lambda} \cdot \langle \mathbf{u}, \mathbf{v} \rangle + \overline{\mu} \cdot \langle \mathbf{v}, \mathbf{w} \rangle$.

Proof. By linearity in the first argument,

$$\langle \lambda \cdot \mathbf{u} + \mu \cdot \mathbf{v}, \mathbf{w} \rangle = \langle \lambda \cdot \mathbf{u}, \mathbf{w} \rangle + \langle \mu \cdot \mathbf{v}, \mathbf{w} \rangle = \lambda \cdot \langle \mathbf{u}, \mathbf{w} \rangle + \mu \cdot \langle \mathbf{v}, \mathbf{w} \rangle.$$

We apply conjugate symmetry and properties of the complex conjugate:

$$\langle \mathbf{u}, \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{w} \rangle = \overline{\langle \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{w}, \mathbf{u} \rangle} = \overline{\lambda \cdot \langle \mathbf{v}, \mathbf{u} \rangle + \mu \cdot \langle \mathbf{w}, \mathbf{u} \rangle} = \overline{\lambda} \cdot \overline{\langle \mathbf{v}, \mathbf{u} \rangle} + \overline{\mu} \cdot \overline{\langle \mathbf{w}, \mathbf{u} \rangle}.$$

We again apply conjugate symmetry and the fact that $\overline{(\bar{z})} = z$:

$$\overline{\lambda} \cdot \overline{\langle \mathbf{v}, \mathbf{u} \rangle} + \overline{\mu} \cdot \overline{\langle \mathbf{w}, \mathbf{u} \rangle} = \overline{\lambda} \cdot \langle \mathbf{u}, \mathbf{v} \rangle + \overline{\mu} \cdot \langle \mathbf{u}, \mathbf{w} \rangle.$$

Lemma (semilinearity in the second argument).
For all $\lambda \in \mathbb{C}$ and $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{C}^d$, we have

$$\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle \quad \text{and} \quad \langle \mathbf{u}, \lambda \cdot \mathbf{v} \rangle = \overline{\lambda} \cdot \langle \mathbf{u}, \mathbf{v} \rangle.$$

Proof. Exercise.

Exercise. Prove that for all $\lambda \in \mathbb{C}$ and $\mathbf{v} \in \mathbb{C}^d$, we have

$$\|\lambda \cdot \mathbf{v}\|_2 = |\lambda| \cdot |\mathbf{v}\|_2.$$

Cauchy-Schwarz inequality

Theorem (Cauchy-Schwarz inequality). For all $\mathbf{u}, \mathbf{v} \in \mathbb{C}^d$,

$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\|_2 \|\mathbf{v}\|_2.$$

Proof. We observe that

$$|\langle \mathbf{u}, \mathbf{v} \rangle| = \left| \sum_{i=1}^{d} u_i \bar{v}_i \right| \leq \sum_{i=1}^{d} |u_i \bar{v}_i| = \sum_{i=1}^{d} |u_i||v_i| = \|\mathbf{u}\|_2 \|\mathbf{v}\|_2 \sum_{i=1}^{d} \frac{|u_i|}{\|\mathbf{u}\|_2} \frac{|v_i|}{\|\mathbf{v}\|_2}.$$

Since $(a-b)^2 = a^2 + b^2 - 2ab \geq 0$ we have $a \cdot b \leq \frac{1}{2}(a^2 + b^2)$ and thus

$$\|\mathbf{u}\|_2 \|\mathbf{v}\|_2 \sum_{i=1}^{d} \frac{|u_i|}{\|\mathbf{u}\|_2} \frac{|v_i|}{\|\mathbf{v}\|_2} \leq \|\mathbf{u}\|_2 \|\mathbf{v}\|_2 \sum_{i=1}^{d} \frac{1}{2} \left(\frac{|u_i|^2}{\|\mathbf{u}\|_2^2} + \frac{|v_i|^2}{\|\mathbf{v}\|_2^2} \right).$$

The proof is concluded as $\|\mathbf{w}\|_2 = \sqrt{\sum_{i=1}^{d} |w_i|^2}$ for all $\mathbf{w} \in \mathbb{C}^d$ and thus

$$\sum_{i=1}^{d} \frac{1}{2} \left(\frac{|u_i|^2}{\|\mathbf{u}\|_2^2} + \frac{|v_i|^2}{\|\mathbf{v}\|_2^2} \right) = \frac{1}{2} \left(\frac{1}{\|\mathbf{u}\|_2^2} \sum_{i=1}^{d} |u_i|^2 + \frac{1}{\|\mathbf{v}\|_2^2} \sum_{i=1}^{d} |v_i|^2 \right) = 1.$$

Triangle inequality

Theorem (Triangle inequality). For all $\mathbf{u}, \mathbf{v} \in \mathbb{C}^d$,

$$\|\mathbf{u} + \mathbf{v}\|_2 \leq \|\mathbf{u}\|_2 + \|\mathbf{v}\|_2.$$

Proof. See lecture notes: uses Cauchy-Schwarz inequality.

Unit vectors and standard basis

The **unit vectors** are defined as

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \;\; \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \;\; \dots \;\; , \mathbf{e}_d = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Any vector $\mathbf{v} = (v_i)_{i=1}^d \in \mathbb{C}^d$ can be uniquely represented in terms of unit vectors:

$$\mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \sum_{i=1}^{d} v_i \mathbf{e}_i.$$

The **standard basis** for $\mathbb{C}^d$ is defined as the set

$$\{\mathbf{e}_1, \dots, \mathbf{e}_d\}.$$

Notice that $\|\mathbf{e}_i\| = 1$ for all $i = 1, \dots, d$.

§2.1: Matrices

A real $m \times n$ matrix A is an array of entries in $\mathbb{R}$ arranged in m rows and n columns:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Notation. We write $A = (a_{ij})_{i,j=1}^{m,n}$.

Names for matrices:

$$D := \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix} \qquad \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix} \qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} \end{pmatrix} \qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}$$

diagonal matrix	column vector	row vector	upper triangular matrix

Notation. We write $D = \mathbf{diag}(a_{11}, a_{22}, a_{33})$.

Scalar multiplication of a matrix $A := (a_{ij})_{i,j=1}^{m,n}$ with scalar $\lambda \in \mathbb{R}$:

$$\lambda \cdot A = \begin{pmatrix} \lambda \cdot a_{11} & \lambda \cdot a_{12} & \dots & \lambda \cdot a_{1n} \\ \lambda \cdot a_{21} & \lambda \cdot a_{22} & \dots & \lambda \cdot a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda \cdot a_{m1} & \lambda \cdot a_{m2} & \dots & \lambda \cdot a_{mn} \end{pmatrix}.$$

Example.

$$3 \cdot \begin{pmatrix} 1 & -2 & 3 \\ 0 & 2 & -4 \end{pmatrix} = \begin{pmatrix} 3 \cdot 1 & 3 \cdot (-2) & 3 \cdot 3 \\ 3 \cdot 0 & 3 \cdot 2 & 3 \cdot (-4) \end{pmatrix} = \begin{pmatrix} 3 & -6 & 9 \\ 0 & 6 & -12 \end{pmatrix}$$

Matrix sum

The matrix sum of $m \times n$ matrices $A := (a_{ij})_{i,j=1}^{m,n}$ and $B := (b_{ij})_{i,j=1}^{m,n}$ is defined as the matrix

$$A + B = (a_{ij} + b_{ij})_{i,j=1}^{m,n}.$$

Example.

$$\begin{pmatrix} 3 & -6 & 9 \\ 0 & 6 & -12 \end{pmatrix} + \begin{pmatrix} 2 & -2 & 0 \\ 2 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 3+2 & -6-2 & 9+0 \\ 0+2 & 6+6 & -12+2 \end{pmatrix} = \begin{pmatrix} 5 & -8 & 9 \\ 2 & 12 & -10 \end{pmatrix}$$

The matrix product of an $m \times p$ matrix $A := (a_{ij})_{i,j=1}^{m,p}$ with an $p \times n$ matrix $B := (b_{ij})_{i,j=1}^{p,n}$ is defined as

$$A \cdot B = \left(\sum_{k=1}^{p} a_{ik} \cdot b_{kj} \right)_{i,j=1}^{m,n}$$

Example. $m = 3$, $p = 4$ and $n = 2$:

$$\begin{pmatrix} 2 & 1 & -3 & 0 \\ 1 & 0 & 1 & 2 \\ -1 & 1 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 2 \\ 2 & 1 \\ 3 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 2\cdot1+1\cdot-1+(-3)\cdot2+0\cdot3 & 2\cdot0+1\cdot2+(-3)\cdot1+0\cdot1 \\ 1\cdot1+0\cdot-1+\quad 1\cdot2+2\cdot3 & 1\cdot0+0\cdot2+\quad 1\cdot1+2\cdot1 \\ -1\cdot1+1\cdot-1+\quad 3\cdot2+1\cdot3 & -1\cdot0+1\cdot2+\quad 3\cdot1+1\cdot1 \end{pmatrix} = \begin{pmatrix} -5 & -1 \\ 9 & 3 \\ 7 & 6 \end{pmatrix}.$$

Remarks. If the number of columns of A is not equal to the number of rows of B, then $A \cdot B$ is not defined!
Matrix multiplication is associative:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

However, matrix multiplication is not commutative:

$$A \cdot B \neq B \cdot A.$$

Matrix-vector product

Let $\mathbf{a}_i$ denote the ith row of a matrix $A \in \mathbb{R}^{m\times n}$ and let $\mathbf{x} \in \mathbb{R}^n$ be a vector:

$$A = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_m \end{pmatrix} \quad \text{and} \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix}$$

The matrix-vector product $\langle \mathbf{a}_i, \mathbf{x} \rangle$ is defined as the i-th row of the following matrix product

$$A \cdot \mathbf{x} := \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} \langle \mathbf{a}_1, \mathbf{x} \rangle \\ \langle \mathbf{a}_2, \mathbf{x} \rangle \\ \vdots \\ \langle \mathbf{a}_m, \mathbf{x} \rangle \end{pmatrix}.$$

Example.

$$A = \begin{pmatrix} 1 & 6 \\ 2 & 5 \\ 3 & 4 \end{pmatrix} \text{ and } \mathbf{x} = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \quad \Longrightarrow \quad A \cdot \mathbf{x} = \begin{pmatrix} 1\cdot 3 + 6 \cdot 4 \\ 2 \cdot 3 + 5 \cdot 4 \\ 3 \cdot 3 + 4 \cdot 4 \end{pmatrix} = \begin{pmatrix} 27 \\ 26 \\ 25 \end{pmatrix}.$$

Calculation rules for matrices

Theorem.

- For all $A, B \in \mathbb{R}^{m \times n}$ and $\lambda \in \mathbb{R}$,
$$\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B.$$
- For all $A \in \mathbb{R}^{m \times p}$, $B \in \mathbb{R}^{p \times n}$ and $\lambda \in \mathbb{R}$,
$$A \cdot (\lambda \cdot B) = \lambda \cdot A \cdot B.$$
- For all $A \in \mathbb{R}^{m \times p}$ and $B, C \in \mathbb{R}^{p \times n}$,
$$A \cdot (B + C) = A \cdot B + A \cdot C.$$
- For all $A \in \mathbb{R}^{m \times n}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,
$$A \cdot (\mathbf{x} + \mathbf{y}) = A \cdot \mathbf{x} + A \cdot \mathbf{y}.$$
- For all $A \in \mathbb{R}^{m \times n}$, $\mathbf{x} \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$,
$$A \cdot (\lambda \cdot \mathbf{x}) = \lambda \cdot A \cdot \mathbf{x}.$$

Proof. Exercise.

Additive and multiplicative identities

The zero matrix $0_{mn} \in \mathbb{R}^{m\times n}$ and identity matrix $I_n \in \mathbb{R}^{n\times n}$ are defined as

$$0_{mn} := \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad I_n := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Exercise. Prove that for all $A \in \mathbb{R}^{m\times n}$ we have

$$A + 0_{mn} = 0_{mn} + A = A, \qquad A \cdot I_n = A \qquad \text{and} \qquad I_m \cdot A = A.$$

Remark.
A square matrix $A \in \mathbb{R}^{n\times n}$ is invertible if there exists a matrix $A^{-1} \in \mathbb{R}^{n\times n}$ such that

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n.$$

In this case, we call A^{-1} the inverse of A.

Matrix transpose

The matrix transpose of $A := (a_{ij})_{ij}$ is obtained by reflecting the entries along the diagonal:

$$A^\top = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}^\top = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}$$

Example.

$$\begin{pmatrix} 1 & 2 & -1 \\ 3 & -5 & 6 \end{pmatrix}^\top = \begin{pmatrix} 1 & 3 \\ 2 & -5 \\ -1 & 6 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & -1 & 3 \\ 0 & 4 & -5 \\ 1 & 2 & 8 \end{pmatrix}^\top = \begin{pmatrix} 2 & 0 & 1 \\ -1 & 4 & 2 \\ 3 & -5 & 8 \end{pmatrix}$$

Transpose and multiplication

Let $(M)_{ij}$ denote the entry in the ith row and jth column of a matrix $M \in \mathbb{R}^{n\times m}$.
We observe that for all $1 \leq i \leq n$ and $1 \leq j \leq m$,

$$(M^\top)_{ij} = (M)_{ji}.$$

Lemma. If $A \in \mathbb{R}^{m\times p}$ and $B \in \mathbb{R}^{p\times n}$, then

$$(A \cdot B)^\top = B^\top \cdot A^\top.$$

Proof. Notice that $B^\top \cdot A^\top$ exists as $B^\top \in \mathbb{R}^{n\times p}$ and $A^\top \in \mathbb{R}^{p\times m}$.
Hence, for all $1 \leq i \leq n$ and $1 \leq j \leq m$,

$$((A \cdot B)^\top)_{ij} = (A \cdot B)_{ji} = \sum_{k=1}^{p} (A)_{jk}(B)_{ki}$$

and

$$(B^\top \cdot A^\top)_{ij} = \sum_{k=1}^{p} (B^\top)_{ik}(A^\top)_{kj} = \sum_{k=1}^{p} (B)_{ki}(A)_{jk}.$$

We concluded the proof, since for all $1 \leq k \leq p$,

$$(A)_{jk}(B)_{ki} = (B)_{ki}(A)_{jk}$$

and thus for all $1 \leq i \leq n$ and $1 \leq j \leq m$,

$$((A \cdot B)^\top)_{ij} = (B^\top \cdot A^\top)_{ij}.$$

Transpose and addition

Exercise. Prove that for all $A, B \in \mathbb{R}^{m \times n}$,

$$(A + B)^\top = A^\top + B^\top.$$

§2.2: Systems of linear equations

Problem. Determine all solutions $(x_1, x_2) \in \mathbb{R}$ that satisfy the following system of linear equations, for all $(\alpha, \beta) \in \{(6,2),\ (6,3),\ (4,2)\}$:

$$\begin{aligned} 2x_1 + x_2 &= 1 \\ \alpha\, x_1 + \beta\, x_2 &= 2. \end{aligned}$$

Answer.

If $(\alpha, \beta) = (6,2)$, then there exists 1 solution: $(x_1, x_2) = (0,1)$.

If $(\alpha, \beta) = (6,3)$, then there exists no solutions for (x_1, x_2).

If $(\alpha, \beta) = (4,2)$, then there exists ∞ many solutions for (x_1, x_2):

$$\big\{(x_1, x_2) \in \mathbb{R}^2 : 2x_1 + x_2 = 1 \text{ and } 4x_1 + 2x_2 = 2\big\}$$

$$=$$

$$\left\{ \begin{pmatrix} 1-\lambda \\ 2\lambda \end{pmatrix} : \lambda \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -2 \end{pmatrix} : \lambda \in \mathbb{R} \right\}.$$

Coefficient matrix and RHS

Let $m, n \in \mathbb{N}$ and $a_{ij}, b_i \in \mathbb{R}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$.

A system of linear equations in n variables is given by

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m. \end{aligned}$$

The coeffient matrix A and right hand side (RHS) $\mathbf{b}$ are defined as

$$A = (a_{ij})_{i,j=1}^{m,n} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

The set of solutions is $L(A, \mathbf{b}) := \{\mathbf{x} \in \mathbb{R}^n : A \cdot \mathbf{x} = \mathbf{b}\}$, since

$$A \cdot \mathbf{x} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} = \mathbf{b}.$$

Set of solutions

Problem. Determine all solutions $(x_1, x_2) \in \mathbb{R}$ that satisfy the following system of linear equations, for all $(\alpha, \beta) \in \{(6,2),\ (6,3),\ (4,2)\}$:

$$\begin{aligned} 2x_1 + x_2 &= 1 \\ \alpha\, x_1 + \beta\, x_2 &= 2. \end{aligned}$$

Answer.

If $(\alpha, \beta) = (6,2)$, then there exists 1 solution:

$$L\left(\begin{pmatrix} 2 & 1 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = \left\{\mathbf{x} \in \mathbb{R}^2 : \begin{pmatrix} 2 & 1 \\ 6 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right\} = \left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}.$$

If $(\alpha, \beta) = (6,3)$, then there exists no solutions:

$$L\left(\begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = \emptyset.$$

If $(\alpha, \beta) = (4,2)$, then there exists ∞ many solutions:

$$L\left(\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -2 \end{pmatrix} : \lambda \in \mathbb{R}\right\}.$$

Homogeneous system

Let us consider the following system of equations:

$$
\begin{aligned}
2\,x_1 + x_2 &= 1\\
4\,x_1 + 2\,x_2 &= 2.
\end{aligned}
$$

Recall that its coefficient matrix A and RHS $\mathbf{b}$ are

$$
A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.
$$

Recall that its solution set is a follows

$$
L\left(\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -2 \end{pmatrix} : \lambda \in \mathbb{R} \right\}.
$$

The solution set of its corresponding homogeneous system is $A \cdot \mathbf{x} = \mathbf{0}$:

$$
L\left(\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) = \left\{ \lambda \cdot \begin{pmatrix} 1 \\ -2 \end{pmatrix} : \lambda \in \mathbb{R} \right\}.
$$

Existence of infinitely many solutions

Suppose that $A \in \mathbb{R}^{m \times n}$ and $\mathbf{b} \in \mathbb{R}^m$.

Lemma. If $L(A, \mathbf{b}) \neq \varnothing$ and $L(A, \mathbf{0}) \neq \{\mathbf{0}\}$, then

$$|L(A, \mathbf{b})| = \infty.$$

Proof. By assumption, there exist non-zero vectors $\mathbf{y} \in L(A, \mathbf{b})$ and $\mathbf{z} \in L(A, \mathbf{0})$ such that $A \cdot \mathbf{y} = \mathbf{b}$ and $A \cdot \mathbf{z} = \mathbf{0}$.

This implies that for all $\lambda \in \mathbb{R}$,

$$A \cdot (\mathbf{y} + \lambda \cdot \mathbf{z}) = A \cdot \mathbf{y} + \lambda \cdot A \cdot \mathbf{z} = \mathbf{b} + \lambda \cdot \mathbf{0} = \mathbf{b}.$$

This concludes the proof as $\mathbf{y} + \lambda \cdot \mathbf{z}$ is a solution for each $\lambda \in \mathbb{R}$.

Lemma. If $L(A, \mathbf{0}) = \{\mathbf{0}\}$, then $|L(A, \mathbf{b})| \leq 1$.

Proof. Exercise.

§2.3: Gaussian elimination

Row echelon form

The leading coefficient of a row is the first nonzero coefficient from the left.

A matrix is in row echelon form if

- nonzero rows are above zero rows, and
- the leading coefficient of a row is strictly right of the leading coefficient of the row above.

A matrix is in reduced row echelon form if it is in row echelon form, and

- the leading coefficients are 1 and the only nonzero entry in their column.

Example.

row echelon form

$$\begin{pmatrix} 1 & 5 & 7 & 11 & 3 \\ 0 & 0 & 2 & 4 & 5 \\ 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

reduced row echelon form

$$\begin{pmatrix} 1 & 0 & 3 & 0 & 11 \\ 0 & 1 & 5 & 0 & 2 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

The leading coefficients of the left matrix are 1, 2 and 1.

Quizzing row echelon forms

Problem. Which of the following matrices are in row echelon form or reduced row echelon form?

$$A = \begin{pmatrix} 1 & 0 & 2 & 5 \\ 0 & 0 & -3 & \frac{1}{2} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -2 & 0 & 2 & 3 & -1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 8 & \pi \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$E = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad F = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Quizzing row echelon forms

Problem. Which of the following matrices are in row echelon form or reduced row echelon form?

$$A = \begin{pmatrix} 1 & 0 & 2 & 5 \\ 0 & 0 & -3 & \frac{1}{2} \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -2 & 0 & 2 & 3 & -1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 8 & \pi \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$E = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad F = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Answer.
Row echelon form: A, B, C, D.
Reduced row echelon form: C, D.
NOT in row echelon form: E, F.

Solving systems in row echelon form

Problem. Determine the solution set

$$L(A, \mathbf{b}),$$

where

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Solving systems in row echelon form

Problem. Determine the solution set

$$L(A, \mathbf{b}),$$

where

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Answer. We convert to a system of linear equations:

$$\begin{aligned} x_1 + 2x_2 &= 2 \\ x_3 &= 1 \\ 0 &= 0 \\ 0 &= 1. \end{aligned}$$

Since the last equation is never valid, there are no solutions to this system:

$$L(A, \mathbf{b}) = \varnothing.$$

Solving systems in row echelon form

Problem. Determine the solution set

$$L(A, \mathbf{b}) \qquad \text{where} \qquad A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Solving systems in row echelon form

Problem. Determine the solution set

$$L(A, \mathbf{b}) \qquad \text{where} \qquad A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Answer. We convert to a system of linear equations in three variables:

$$\begin{aligned} x_1 + 2x_2 &= 2 \\ x_3 &= 1 \\ 0 &= 0 \\ 0 &= 0. \end{aligned}$$

We find that $x_3 = 1$ and treat either x_2 or x_1 as a *free variable*:

$$L(A, \mathbf{b}) = \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} : x_2 \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + x_1 \cdot \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} : x_1 \in \mathbb{R} \right\}.$$

Exercise. Show that both sets are really equal.

Gaussian elimination and rank

The row operations on a matrix are defined as follows

1. Interchanging two rows.
2. Multiplication of a row with a non-zero scalar $\lambda \in \mathbb{R}$.
3. Addition of multiple of row to another row.

Gaussian elimination is a sequence of elementary row operations applied to a matrix A until the output matrix C is in row echelon form.

We define $\operatorname{rank} A$ as the number of non-zero rows of C.

Exercise. Prove that the number of non-zero rows of E does not depend on the sequence of row operations.

Exercise. Show that $\operatorname{rank} A \leq \min\{m, n\}$.

Computing the rank

Problem. Compute $\operatorname{rank} A$, where

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Answer.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \xrightarrow[R_2 = R_2 - 4R_1]{} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 9 \end{pmatrix}$$

$$\xrightarrow[R_3 = R_3 - 7R_1]{} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}$$

$$\xrightarrow[R_3 = R_3 - 2R_2]{} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} := C$$

We find that $\operatorname{rank} A = 2$, since the output matrix C in row echelon form and has two non-zero rows.

Equivalent matrices

Recall that a relation $R \subset M \times M$ for some non-empty set M is called an equivalence relation if for all $x, y, z \in M$ the following holds:

- reflexive: $(x, x) \in R$,
- symmetric: $(x, y) \in R \implies (y, x) \in R$, and
- transitive: $(x, y), (y, z) \in R \implies (x, z) \in R$.

Exercise. Let $M := \mathbb{R}^{m \times n}$ and suppose that $R \subset M \times M$ is the relation such that $(A, B) \in R$ if and only if the matrices A and B are related by a sequence of row operations. Show that R is an equivalence relation.

Matrix concatenation

The matrix concatenation $(A|B)$ of an $m \times n$ matrix A and $m \times p$ matrix B is obtained by appending the columns of B to the columns of A.
Example.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{a} := \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix}, \quad \mathbf{b} := \begin{pmatrix} 8 \\ 9 \\ 10 \end{pmatrix} \quad \mathbf{c} := \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix},$$

$$(A|\mathbf{b}) = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 8 \\ 1 & 1 & 1 & 9 \\ 1 & 0 & 1 & 10 \end{array}\right),$$

$$(A|I) = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right),$$

$$(\mathbf{a} \,|\, \mathbf{b} \,|\, \mathbf{c}) = \begin{pmatrix} 2 & 8 & 0 \\ 3 & 9 & 1 \\ 5 & 10 & 2 \end{pmatrix}.$$

Solving linear systems using Gaussian elimination

Theorem. Let $A \in \mathbb{R}^{m \times n}$ and $\mathbf{b} \in \mathbb{R}^n$. If the matrix $(C|\mathbf{d})$ is obtained from $(A|\mathbf{b})$ using row operations, then

$$L(A, \mathbf{b}) = L(C, \mathbf{d}).$$

Proof. Recall that the row operations are:

- Interchanging two rows.
- Multiplication of a row with a non-zero scalar $\lambda \in \mathbb{R}$.
- Addition of multiple of row to another row.

We observe that the row operations applied the matrix $(A|\mathbf{b})$ correspond to the following operations applied to the system of linear equations defined by $A \cdot \mathbf{b} = \mathbf{x}$:

- Interchanging two equations.
- Multiplying both sides of an equation with a non-zero scalar $\lambda \in \mathbb{R}$.
- Adding a multiple of an equation to another equation.

We conclude the proof as the latter three operations do not change the solution set.

Example Gaussian elimination

Problem. Determine the solution set

$$L(A, \mathbf{b}) \qquad \text{where} \qquad A = \begin{pmatrix} 3 & 5 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 42 \\ 6 \end{pmatrix}.$$

Answer.

$$\left(\begin{array}{cc|c} 3 & 5 & 42 \\ 1 & -1 & 6 \end{array}\right) \xrightarrow[R_1 \leftrightarrow R_2]{} \left(\begin{array}{cc|c} 1 & -1 & 6 \\ 3 & 5 & 42 \end{array}\right)$$

$$\xrightarrow[R_2 = R_2 - 3R_1]{} \left(\begin{array}{cc|c} 1 & -1 & 6 \\ 0 & 8 & 24 \end{array}\right)$$

$$\xrightarrow[R_2 = \frac{1}{8} R_2]{} \left(\begin{array}{cc|c} 1 & -1 & 6 \\ 0 & 1 & 3 \end{array}\right)$$

$$\xrightarrow[R_1 = R_1 + R_2]{} \left(\begin{array}{cc|c} 1 & 0 & 9 \\ 0 & 1 & 3 \end{array}\right) =: (C|\mathbf{d}).$$

The matrix $(C|\mathbf{d})$ corresponds to the system $C \cdot \mathbf{x} = \mathbf{d}$:

$$x_1 + 0x_2 = 9$$

$$0x_1 + x_2 = 3.$$

It follows from the previous theorem that $L(A, \mathbf{b}) = L(C, \mathbf{d}) = \left\{ \begin{pmatrix} 9 \\ 3 \end{pmatrix} \right\}$.

Problem. Determine the solution set

$$L(A, \mathbf{b}) \qquad \text{where} \qquad A = \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 6 \\ 2 & 0 & -4 \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} 5 \\ 3 \\ 4 \end{pmatrix}.$$

Answer.

$$\left(\begin{array}{ccc|c} 2 & 1 & -2 & 5 \\ 0 & 3 & 6 & 3 \\ 2 & 0 & -4 & 4 \end{array}\right) \xrightarrow[R_3 = R_3 - R_1]{} \left(\begin{array}{ccc|c} 2 & 1 & -2 & 5 \\ 0 & 3 & 6 & 3 \\ 0 & -1 & -2 & -1 \end{array}\right)$$

$$\xrightarrow[R_3 = -R_3]{} \left(\begin{array}{ccc|c} 2 & 1 & -2 & 5 \\ 0 & 3 & 6 & 3 \\ 0 & 1 & 2 & 1 \end{array}\right)$$

$$\xrightarrow[R_2 \leftrightarrow R_3]{} \left(\begin{array}{ccc|c} 2 & 1 & -2 & 5 \\ 0 & 1 & 2 & 1 \\ 0 & 3 & 6 & 3 \end{array}\right)$$

$$\xrightarrow[R_3 = R_3 - 3R_2]{} \left(\begin{array}{ccc|c} 2 & 1 & -2 & 5 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\xrightarrow[R_1 = R_1 - R_2]{} \left(\begin{array}{ccc|c} 2 & 0 & -4 & 4 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\xrightarrow[R_1 = \frac{1}{2} R_1]{} \left(\begin{array}{ccc|c} 1 & 0 & -2 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) =: (C, \mathbf{d}).$$

$$\begin{aligned} x_1 - 2x_3 &= 2 \\ x_2 + 2x_3 &= 1. \end{aligned}$$

$$L(A, \mathbf{b}) = L(C, \mathbf{d}) = \left\{ \begin{pmatrix} 2 + 2x_3 \\ 1 - 2x_3 \\ x_3 \end{pmatrix} : x_3 \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} : \lambda \in \mathbb{R} \right\}.$$

Example. Let $A \in \mathbb{R}^{4\times 3}$ and $\mathbf{b} \in \mathbb{R}^4$.
Suppose that $(C, \mathbf{d})$ is the reduced row echelon form of $(A, \mathbf{b})$ for some $\alpha \in \mathbb{R}$, where

$$C = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathbf{d} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ \alpha \end{pmatrix}$$

Let consider the system of linear equations $C \cdot \mathbf{x} = \mathbf{d}$:

$$\begin{aligned} x_1 + 2x_2 &= 2 \\ x_3 &= 1 \\ 0 &= 0 \\ 0 &= \alpha. \end{aligned}$$

Notice that

$$\operatorname{rank} A = 2 \quad \text{and} \quad L(A, \mathbf{b}) = L(C, \mathbf{d}).$$

If $\alpha = 0$, then

$$|L(A, \mathbf{b})| = \infty.$$

If $\alpha \neq 0$, then

$$L(A, \mathbf{b}) = \varnothing.$$

Rank and reduced echelon form

Theorem. Suppose that $A \in \mathbb{R}^{m \times n}$. Then:

$$\operatorname{rank} A = n = m \iff |L(A, \mathbf{b})| = 1 \text{ for all } \mathbf{b} \in \mathbb{R}^n.$$

Proof. Let $(C, \mathbf{d})$ be the reduced row echelon form of $(A|\mathbf{b})$ so that

$$L(A, \mathbf{b}) = L(C, \mathbf{d}).$$

$(\Longrightarrow)$ Notice that $C = I_n$ as a direct consequence of the definitions of "rank" and "reduced row echelon form".
Since $|L(I_n, \mathbf{d})| = 1$ for all $\mathbf{d} \in \mathbb{R}^n$ and $L(A, \mathbf{b}) = L(C, \mathbf{d})$,
we concluded the proof.

$(\Longleftarrow)$ We find that $|L(A, \mathbf{d})| = |L(C, \mathbf{d})| = 1$ for all $\mathbf{d} \in \mathbb{R}^n$.
Suppose by contradiction that $C \neq I_n$. In this case one of the variables for the system $C \cdot \mathbf{x} = \mathbf{d}$ is a free variable and thus either

$$|L(C, \mathbf{d})| = \infty \quad \text{or} \quad L(C, \mathbf{d}) = \varnothing \qquad \text{(see example previous slide).}$$

We arrived at a contradiction and thus $C = I_n$.
Hence, $\operatorname{rank} A = n = m$ as was to be shown.

Elementary matrices

An elementary matrix is a matrix that can be obtained from the identity matrix by a single row operation.

Example. Elementary 3×3 matrices for the row operations $R_2 \leftrightarrow R_1$, $\quad R_2 = 3R_2 \quad$ and $\quad R_3 = R_3 + 4R_1$:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}.$$

The row operation $R_2 = R_2 + 3R_1$ on a matrix can be realized by multiplying with an elementary matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -2 \\ -3 & 1 & 4 \\ 2 & -3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -2 \\ 2 & -3 & 4 \end{pmatrix}.$$

Elementary matrices

An elementary matrix is a matrix that can be obtained from the identity matrix by a single row operation.

Example. Elementary 3×3 matrices for the row operations $R_2 \leftrightarrow R_1$, $\quad R_2 = 3R_2 \quad$ and $\quad R_3 = R_3 + 4R_1$:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}.$$

The row operation $R_2 = R_2 + 3R_1$ on a matrix can be realized by multiplying with an elementary matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -2 \\ -3 & 1 & 4 \\ 2 & -3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & -2 \\ 2 & -3 & 4 \end{pmatrix}.$$

Remark. If $A \in \mathbb{R}^{m \times n}$ is a matrix and C its reduced row echelon form, then by definition there exists elementary matrices $E_1, \ldots, E_k$ such that

$$C = E_k \cdots E_1 \cdot A.$$

Exercise. Show that elementary matrices $E \in \mathbb{R}^{n \times n}$ are invertible and that the inverse E^{-1} is also an elementary matrix.

§2.4: Matrices as linear transformations

The matrix transformation $T_A \colon \mathbb{R}^n \to \mathbb{R}^m$ of a matrix $A \in \mathbb{R}^{m\times n}$ is defined as

$$T_A(\mathbf{x}) = A \cdot \mathbf{x}.$$

Example.

$$\text{if} \quad A = \begin{pmatrix} 1 & -3 \\ 3 & 5 \\ -1 & 7 \end{pmatrix} \in \mathbb{R}^{3\times 2} \quad \text{and} \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2$$

then

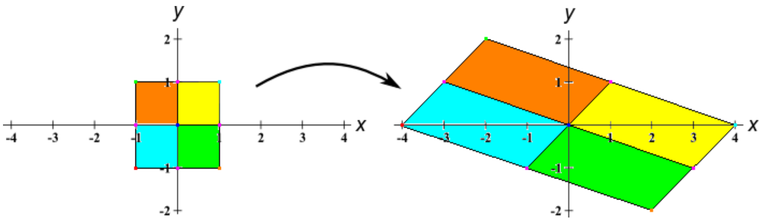
$$T_A(\mathbf{x}) = A \cdot \mathbf{x} = \begin{pmatrix} 1 & -3 \\ 3 & 5 \\ -1 & 7 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 - 3x_2 \\ 3x_1 + 5x_2 \\ -x_1 + 7x_2 \end{pmatrix}.$$

Example. Let the function $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be defined as

$$T\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} 3x_1 + x_2 \\ -x_1 + x_2 \end{pmatrix}.$$

The function T is a matrix transformation:

$$\begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3x_1 + x_2 \\ -x_1 + x_2 \end{pmatrix}.$$



Composition of linear maps

Recall that if $f\colon \mathbb{R}^n \to \mathbb{R}^m$ and $g\colon \mathbb{R}^m \to \mathbb{R}^k$ are functions, then their composition is defined as the function

$$g \circ f\colon \mathbb{R}^n \to \mathbb{R}^k, \quad x \mapsto g(f(x)).$$

Problem. Suppose that A is an $m \times n$ matrix and B and $k \times m$ matrix with matrix transformations

$$T_A\colon \mathbb{R}^n \to \mathbb{R}^m \quad \text{and} \quad T_B\colon \mathbb{R}^m \to \mathbb{R}^k.$$

Determine the matrix M such that :

$$T_M = T_B \circ T_A\colon \mathbb{R}^n \to \mathbb{R}^k.$$

Composition of linear maps

Recall that if $f\colon \mathbb{R}^n \to \mathbb{R}^m$ and $g\colon \mathbb{R}^m \to \mathbb{R}^k$ are functions, then their composition is defined as the function

$$g \circ f\colon \mathbb{R}^n \to \mathbb{R}^k, \quad x \mapsto g(f(x)).$$

Problem. Suppose that A is an $m \times n$ matrix and B and $k \times m$ matrix with matrix transformations

$$T_A\colon \mathbb{R}^n \to \mathbb{R}^m \quad \text{and} \quad T_B\colon \mathbb{R}^m \to \mathbb{R}^k.$$

Determine the matrix M such that :

$$T_M = T_B \circ T_A\colon \mathbb{R}^n \to \mathbb{R}^k.$$

Answer. The $k \times n$ matrix

$$M = B \cdot A.$$

A function $T\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation if the following holds:

- For all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,
$$T(\mathbf{x} + \mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y}).$$
- For all $\mathbf{x} \in \mathbb{R}^n$ and all $\lambda \in \mathbb{R}$,
$$T(\lambda \cdot \mathbf{x}) = \lambda \cdot T(\mathbf{x}).$$

Theorem. A function $T\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation if and only if there exists a matrix $A \in \mathbb{R}^{m \times n}$ with $T = T_A$.

Proof. Exercise.
Hint. For the $\Longleftarrow$ direction show that

$$A = \begin{pmatrix} T(\mathbf{e}_1) & \cdots & T(\mathbf{e}_n) \end{pmatrix}$$

for some linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^m$.

Lemma for invertible linear transformations

Lemma. If $A \in \mathbb{R}^{n \times n}$ is an invertible matrix,
then T_A is an invertible function.

Proof. By definition

$$A \cdot A^{-1} = I_n = A^{-1} \cdot A$$

and thus

$$T_A \circ T_{A^{-1}} = T_{A \cdot A^{-1}} = T_{I_n} = \mathrm{id} \quad \text{and} \quad T_{A^{-1}} \circ T_A = T_{A^{-1} \cdot A} = T_{I_n} = \mathrm{id}\,.$$

Lemma. If $A \in \mathbb{R}^{n \times n}$ is a matrix such that T_A is invertible, then its inverse $T := T_A^{-1}$ is a linear transformation.

Proof. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$ be arbitrary.
By definition of the inverse,

$$(T_A \circ T)(\mathbf{x}) = \mathbf{x} = (T \circ T_A)(\mathbf{x}) \qquad \text{and} \qquad (T_A \circ T)(\mathbf{y}) = \mathbf{y} = (T \circ T_A)(\mathbf{y}).$$

Therefore,

$$\begin{aligned} T(\mathbf{x} + \mathbf{y}) &= T((T_A \circ T)(\mathbf{x}) + (T_A \circ T)(\mathbf{y})) \\ &= T(\ \ A \cdot T(\mathbf{x}) + A \cdot T(\mathbf{y}) \ \ ) \\ &= T(\ \ A \cdot (T(\mathbf{x}) + T(\mathbf{y})) \ \ ) \\ &= (T \circ T_A)(T(\mathbf{x}) + T(\mathbf{y})) \\ &= T(\mathbf{x}) + T(\mathbf{y}). \end{aligned}$$

Similarly,

$$\begin{aligned} T(\lambda \cdot \mathbf{x}) &= T(\lambda \cdot (T_A \circ T)(\mathbf{x})) \\ &= T(\lambda \cdot A \cdot T(\mathbf{x})) \\ &= T(A \cdot \lambda \cdot T(\mathbf{x})) \\ &= (T \circ T_A)(\lambda \cdot T(\mathbf{x})) \\ &= \lambda \cdot T(\mathbf{x}). \end{aligned}$$

Hence, T is a linear transformation and thus we concluded the proof.

Lemma. If $A \in \mathbb{R}^{n\times n}$ is a matrix such that $T_A \colon \mathbb{R}^n \to \mathbb{R}^n$ is invertible, then A is an invertible matrix.

Proof. By definition of the inverse, there exists a function $T \colon \mathbb{R}^n \to \mathbb{R}^n$ such that

$$T_A \circ T = \mathrm{id} = T \circ T_A.$$

It follows from the previous lemma that T is a linear transformation. By the previous theorem, there exists a matrix $B \in \mathbb{R}^{n\times n}$ such that

$$T = T_B.$$

Therefore,

$$\mathrm{id} = T_A \circ T_B = T_{A\cdot B} = T_{I_n} \quad \text{and} \quad \mathrm{id} = T_B \circ T_A = T_{B\cdot A} = T_{I_n}.$$

Hence,

$$A \cdot B = I_n = B \cdot A$$

and thus

$$A^{-1} = B.$$

The following theorem summarizes the previous three lemma's:

Theorem. Let $A \in \mathbb{R}^{n \times n}$ be a square matrix. Then

$$T_A \text{ is invertible} \iff A \text{ is invertible.}$$

§2.5: Determinants

Matrix determinant

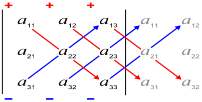
The determinant $\det M$ of a $n \times n$ matrix M is defined as follows if $n \leq 3$,

$$\det(a) = a$$

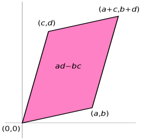
$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$$

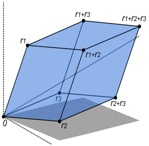
$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{31} \cdot a_{22} \cdot a_{13} - a_{32} \cdot a_{23} \cdot a_{11} - a_{33} \cdot a_{21} \cdot a_{12}.$$

The determinant for 3×3 matrices can be remembered using Sarrus rule:



Proposition. The absolute value of the determinant is equal to the volume of the area of a parallelogram (left) or volume of a parallelepiped (right):





$|\det(r_1|r_2|r_3)|$

Computing determinant

Problem. Compute the following determinant using expansion along the first row

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 6 & 7 & 8 \\ 1 & -1 & -1 \end{pmatrix}.$$

Answer.

$$\det \begin{pmatrix} 3 & 2 & 1 \\ 6 & 7 & 8 \\ 1 & -1 & -1 \end{pmatrix} = 3 \cdot \det \begin{pmatrix} 7 & 8 \\ -1 & -1 \end{pmatrix} - 2 \cdot \det \begin{pmatrix} 6 & 8 \\ 1 & -1 \end{pmatrix} + 1 \cdot \det \begin{pmatrix} 6 & 7 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$3 \cdot [7 \cdot (-1) - 8 \cdot (-1)] - 2 \cdot [6 \cdot (-1) - 8 \cdot 1] + 1 \cdot [6 \cdot (-1) - 7 \cdot 1]$$

$$=$$

$$3 \cdot 1 - 2 \cdot (-14) + 1 \cdot (-13) = 18.$$

We may compute the determinant by expanding along any column or row:

Theorem. If $A \in \mathbb{R}^{n \times n}$ with $n \geq 2$, then for any $1 \leq i, j \leq n$,

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det A_{ij} \quad \text{and} \quad \det A = \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det A_{ij},$$

where the matrix A_{ij} is the matrix A with the ith row and jth column removed.

Example.

$$\det \begin{pmatrix} 1 & 2 & 100 \\ 3 & 5 & \sqrt{2} \\ 0 & 0 & 1 \end{pmatrix} = 0 \cdot \det A_{31} - 0 \cdot \det A_{32} + 1 \cdot \det A_{33}$$

$$= 1 \cdot (1 \cdot 5 - 2 \cdot 3) = -1.$$

Exercise. Show that for all $n \times n$ matrices A,

$$\det A^{\top} = A.$$

Determinant of a matrix

Example. Computing determinant of 4×4 matrix by expanding along the first column:

$$\det \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} = a \cdot \det A_{11} - e \cdot \det A_{21} + i \cdot \det A_{31} - m \cdot \det A_{41}$$

$$=$$

$$a \cdot \det \begin{pmatrix} f & g & h \\ j & k & l \\ n & o & p \end{pmatrix} - e \cdot \det \begin{pmatrix} b & c & d \\ j & k & l \\ n & o & p \end{pmatrix} + i \cdot \det \begin{pmatrix} b & c & d \\ f & g & h \\ n & o & p \end{pmatrix} - m \cdot \det \begin{pmatrix} b & c & d \\ f & g & h \\ j & k & l \end{pmatrix}$$

$$\det A_{11} = \det \begin{pmatrix} f & g & h \\ j & k & l \\ n & o & p \end{pmatrix} = f \cdot \det \begin{pmatrix} k & l \\ o & p \end{pmatrix} - j \cdot \det \begin{pmatrix} g & h \\ o & p \end{pmatrix} + n \cdot \det \begin{pmatrix} g & h \\ k & l \end{pmatrix}$$

$$\det \begin{pmatrix} k & l \\ o & p \end{pmatrix} = k \cdot \det \left(p\right) - o \cdot \det \left(l\right)$$

$$\det \left(p\right) = p$$

Computing determinant

Problem. Compute the determinant of the following matrix

$$A := \begin{pmatrix} 3 & -7 & 8 & 9 & -6 \\ 0 & 2 & -5 & 7 & 3 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 2 & 4 & -1 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix}.$$

Computing determinant

Problem. Compute the determinant of the following matrix

$$A := \begin{pmatrix} 3 & -7 & 8 & 9 & -6 \\ 0 & 2 & -5 & 7 & 3 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 2 & 4 & -1 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix}.$$

Answer.

$$\det \begin{pmatrix} 3 & -7 & 8 & 9 & -6 \\ 0 & 2 & -5 & 7 & 3 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 2 & 4 & -1 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix} = 3 \cdot \det \begin{pmatrix} 2 & -5 & 7 & 3 \\ 0 & 1 & 5 & 0 \\ 0 & 2 & 4 & -1 \\ 0 & 0 & -2 & 0 \end{pmatrix}$$

$$= 3 \cdot 2 \cdot \det \begin{pmatrix} 1 & 5 & 0 \\ 2 & 4 & -1 \\ 0 & -2 & 0 \end{pmatrix} = 3 \cdot 2 \cdot (-1 \cdot -1) \cdot \det \begin{pmatrix} 1 & 5 \\ 0 & -2 \end{pmatrix}$$

$$= 3 \cdot 2 \cdot (-1 \cdot -1) \cdot (-2) = -12.$$

Upper and lower triangular matrix

An $m \times n$ matrix is triangular if all the entries either below or above the main diagonal are zero.

Example. Determinant of an upper triangular matrix:

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} = a_{11} \cdot a_{22} \cdot a_{33}.$$

Lemma. If $A = (a_{ij})$ is an $n \times n$ triangular matrix, then

$$\det A = a_{11} \cdot a_{22} \cdots a_{nn}.$$

Proof. Exercise.

Determinant and multiplying row by scalar

Lemma. If the matrix B is obtained from $A \in \mathbb{R}^{n\times n}$ by multiplying a row with $\lambda \in \mathbb{R}^n$ such that $n \geq 2$, then

$$\det B = \lambda \cdot \det A.$$

Proof. Suppose the ith row of A is multiplied with λ so that for all $1 \leq j \leq n$:

$$b_{ij} = \lambda \cdot a_{ij} \qquad \text{and} \qquad \det B_{ij} = \det A_{ij}.$$

By expanding along the ith row, we obtain,

$$\begin{aligned}
\det B &= \sum_{j=1}^{n} (-1)^{i+j} \cdot b_{ij} \cdot \det B_{ij} \\
&= \sum_{j=1}^{n} (-1)^{i+j} \cdot \lambda \cdot a_{ij} \cdot \det B_{ij} \\
&= \sum_{j=1}^{n} (-1)^{i+j} \cdot \lambda \cdot a_{ij} \cdot \det A_{ij} \\
&= \lambda \cdot \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det A_{ij} \\
&= \lambda \cdot \det A.
\end{aligned}$$

Determinant and interchanging rows

Lemma. If B is obtained by interchanging two rows of a matrix $A \in \mathbb{R}^{n \times n}$ such that $n \geq 2$, then

$$\det B = -\det A.$$

Proof. We apply induction on n.
Induction basis: If $n = 2$, then $\det A = -\det B$ (**Exercise**).
Induction step: Let $n \geq 3$. There exists $1 \leq i \leq n$ such that the ith row of A is equal to the ith row of B. This implies that for all $1 \leq j \leq n$,

$$b_{ij} = a_{ij}.$$

Moreover, $B_{ij} \in \mathbb{R}^{(n-1)\times(n-1)}$ is for all $1 \leq j \leq n$ obtained from the matrix A_{ij} by interchanging two rows. Hence, by the induction hypothesis,

$$\det B_{ij} = -\det A_{ij}.$$

By expanding along the ith row, we obtain,

$$\det B = \sum_{j=1}^{n} (-1)^{i+j} \cdot b_{ij} \cdot \det B_{ij} = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det B_{ij}$$

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

Determinant and row operations

Lemma.

- If the matrix B is obtained from $A \in \mathbb{R}^{n\times n}$ by multiplying a row with $\lambda \in \mathbb{R}^n$ such that $n \geq 2$, then
$$\det B = \lambda \cdot \det A.$$
- If B is obtained by interchanging two rows of a matrix $A \in \mathbb{R}^{n\times n}$ such that $n \geq 2$, then
$$\det B = -\det A.$$
- If the matrix B is obtained from A by adding a multiple of one row of A to another row, then
$$\det B = \det A.$$

Proof for 3th item. Exercise. Hint: use induction.

Corollary. If the matrix B is obtained from $A \in \mathbb{R}^{n\times n}$ using row operations, then
$$\det A = 0 \iff \det B = 0.$$

Computing determinant using row operations

Example. Computing the determinant using Gaussian elimination:

$$\begin{aligned}
&\det\begin{pmatrix} 1 & -4 & 2 \\ -2 & 8 & -9 \\ -1 & 7 & 0 \end{pmatrix} \\
&= \det\begin{pmatrix} 1 & -4 & 2 \\ 0 & 0 & -5 \\ 0 & 3 & 2 \end{pmatrix} \\
&= -\det\begin{pmatrix} 1 & -4 & 2 \\ 0 & 3 & 2 \\ 0 & 0 & -5 \end{pmatrix} \\
&= (-1)\cdot 1\cdot 3\cdot(-5) = 15.
\end{aligned}$$

Notice that we applied the row operations

$$R_2 = R_2 + 2R_1, \qquad R_3 = R_3 + R_1 \quad \text{and} \quad R_2 \leftrightarrow R_3.$$

Determinant and invertible matrices

Theorem. If $A \in \mathbb{R}^{n\times n}$ is a square matrix, then the following are equivalent

- A is invertible.
- $\det A \neq 0$.
- $\operatorname{rank} A = n$.
- The linear system $A \cdot \mathbf{x} = \mathbf{b}$ has a unique solution for all $\mathbf{b} \in \mathbb{R}^n$.
- A is equivalent via row operations to the identity matrix I_n.

Proof. See lecture notes.

Determining whether a matrix is invertible

Problem. Determine whether the following matrix is invertible:

$$A := \begin{pmatrix} 3 & -7 & 8 & 9 & -6 \\ 0 & 2 & -5 & 7 & 3 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 2 & 4 & -1 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix}$$

Determining whether a matrix is invertible

Problem. Determine whether the following matrix is invertible:

$$A := \begin{pmatrix} 3 & -7 & 8 & 9 & -6 \\ 0 & 2 & -5 & 7 & 3 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 2 & 4 & -1 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix}$$

Answer. We already computed $\det A = -12$ and thus by the previous theorem this matrix must be invertible.

Multiplying with elementary matrices

Lemma. If $E \in \mathbb{R}^{n \times n}$ is an elementary matrix and $B \in \mathbb{R}^{n \times n}$ any matrix, then

$$\det(E \cdot B) = \det(E) \cdot \det(B)$$

Proof. By definition, E is obtained from the identity matrix I_n via a single row operation. Moreover, if we apply this row operation to B, then we obtain the matrix $E \cdot B$.

We make a case distinction on the type of row operation.

- If E is obtained from I_n by interchanging two rows, then by a previous lemma

$$\det(E \cdot B) = -\det B \qquad \text{and} \qquad \det E = -\det I_n = -1.$$

- If E is obtained from I_n by a row dilation λ, then by a previous lemma

$$\det(E \cdot B) = \lambda \cdot \det B \qquad \text{and} \qquad \det(E) = \lambda \cdot \det I_n = \lambda.$$

- If E is obtained from I_n by adding a multiple of a row to another row, then by a previous lemma

$$\det(E \cdot B) = \det B \quad \text{and} \quad \det E = \det I_n = 1.$$

This concludes the proof as we showed the equality in each of the three cases.

The determinant is compatible with multiplication

Theorem. For all square matrices $A, B \in \mathbb{R}^{n\times n}$,

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Proof. By properties of Gaussian elimination, there exists elementary matrices $E_j, \dots, E_1, F_k \cdots F_1$ and unique reduced echelon forms C_A and C_B such that

$$A = E_j \cdots E_1 \cdot C_A \qquad \text{and} \qquad B = F_k \cdots F_1 \cdot C_B.$$

By the repeated applications of the previous lemma, we have

$$\det A = \det(E_j) \cdot \det(E_{j-1} \cdots E_1 \cdot C_A) = \ldots = \det(E_j) \cdots \det(E_1) \cdot \det(C_A),$$
$$\det B = \det(F_k) \cdot \det(F_{k-1} \cdots F_1 \cdot C_B) = \ldots = \det(F_k) \cdots \det(F_1) \cdot \det(C_B),$$

and thus

$$\begin{aligned} &\det(A \cdot B) \\ &= \det(E_j \cdots E_1 \cdot C_A \cdot F_k \cdots F_1 \cdot C_B) \\ &= \det(E_j) \cdots \det(E_1) \cdot \det(C_A) \cdot \det(F_k) \cdots \det(F_1) \cdot \det(C_B) \\ &= \det(A) \cdot \det(B). \end{aligned}$$

Remark. Notice that $\det(A) = det(C_A) = 0$ or $\det(B) = \det(C_B) = 0$ if and only if $\det(A \cdot B) = 0$.

Computing the determinant of a matrix product

Problem. Compute $\det A$, where

$$A = \begin{pmatrix} 15 & 10 & 24 \\ 15 & 22 & 12 \\ 12 & 4 & 33 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 0 \\ 2 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 0 \\ 2 & 0 & 5 \end{pmatrix}.$$

Computing the determinant of a matrix product

Problem. Compute $\det A$, where

$$A = \begin{pmatrix} 15 & 10 & 24 \\ 15 & 22 & 12 \\ 12 & 4 & 33 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 0 \\ 2 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 0 \\ 2 & 0 & 5 \end{pmatrix}.$$

Answer. By the previous theorem,

$$\det A = \left(\det \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 0 \\ 2 & 0 & 5 \end{pmatrix} \right)^2$$

By expansion along the third row, we find that

$$\det \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 0 \\ 2 & 0 & 5 \end{pmatrix} = 2 \cdot \det \begin{pmatrix} 2 & 4 \\ 4 & 0 \end{pmatrix} + 5 \cdot \det \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 2 \cdot (-16) + 5 \cdot (-2) = -42.$$

Therefore,

$$\det A = (-42)^2 = 1764.$$

§2.6: Inverse matrices

Computing the inverse via Gaussian elimination

Theorem. If $A \in \mathbb{R}^{n \times n}$ is a matrix with inverse A^{-1}, then the reduced row echelon form of $(A|I_n)$ is equal to $(I_n|A^{-1})$.

Proof. Let $\mathbf{c}_i$ denote the ith column of A^{-1}, so that

$$A^{-1} = (\mathbf{c}_1|\cdots|\mathbf{c}_n) \quad \text{and} \quad \mathbf{c}_i = A^{-1} \cdot \mathbf{e}_i.$$

Hence,

$$A \cdot \mathbf{c}_i = \mathbf{e}_i$$

and thus $\mathbf{c}_i$ is the unique solution to the system

$$A \cdot \mathbf{x} = \mathbf{e}_i.$$

This implies that $(I_n|\mathbf{c}_i)$ is the reduced row echelon form of

$$(A|\mathbf{e}_i).$$

Instead of computing the reduced row echelon form of $(A|\mathbf{e}_i)$ separately for all $1 \leq i \leq n$, we compute in one go the reduced row echelon form of the matrix

$$(A|\mathbf{e}_1|\cdots|\mathbf{e}_n) = (A|I_n),$$

which is

$$(I_n|\mathbf{c}_1|\cdots|\mathbf{c}_n) = (I_n|A^{-1}).$$

Computing a matrix inverse

Problem. Compute the inverse of
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Computing a matrix inverse

Problem. Compute the inverse of

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Answer. By Gaussian elimination

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right) \xrightarrow[R_2 = R_2 - 3R_1]{} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array}\right)$$

$$\xrightarrow[R_1 = R_1 + R_2]{} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & -2 & -3 & 1 \end{array}\right)$$

$$\xrightarrow[R_2 = (-1/2)R_2]{} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & 3/2 & -1/2 \end{array}\right).$$

It therefore follows from the previous theorem that

$$A^{-1} = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}.$$

Computing a matrix inverse

Problem. Compute the inverse of

$$\begin{pmatrix} 1 & 0 & 2 \\ 4 & 1 & 8 \\ 0 & 1 & 1 \end{pmatrix}.$$

Computing a matrix inverse

Problem. Compute the inverse of

$$\begin{pmatrix} 1 & 0 & 2 \\ 4 & 1 & 8 \\ 0 & 1 & 1 \end{pmatrix}.$$

Answer. By Gaussian elimination

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 4 & 1 & 8 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow[R_2 = R_2 - 4R_1]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -4 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[R_3 = R_3 - R_2]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -4 & 1 & 0 \\ 0 & 0 & 1 & 4 & -1 & 1 \end{array}\right)$$

$$\xrightarrow[R_1 = R_1 - 2R_3]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -7 & 2 & -2 \\ 0 & 1 & 0 & -4 & 1 & 0 \\ 0 & 0 & 1 & 4 & -1 & 1 \end{array}\right).$$

It therefore follows from the previous theorem that

$$A^{-1} = \begin{pmatrix} -7 & 2 & -2 \\ -4 & 1 & 0 \\ 4 & -1 & 1 \end{pmatrix}.$$

Last slide