Chapter 1

Real and Complex Numbers

Basics

Notations

$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\mathbb{Q}$	Rational numbers
$\mathbb{N} = \{1, 2, \dots\}$	positive integers (natural numbers)
$\mathbb{Z}$	Integers

We know that $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. We write $\mathbb{R}_+$, $\mathbb{Q}_+$ and $\mathbb{Z}_+$ for the non-negative real, rational, and integer numbers $x \geq 0$, respectively. The notions $A \subset B$ and $A \subseteq B$ are equivalent. If we want to point out that B is strictly bigger than A we write $A \subsetneqq B$.

We use the following symbols

$:=$	defining equation
$\curvearrowright$, $\Rightarrow$	implication, "if ... , then ... "
$\Longleftrightarrow$	"if and only if", equivalence
$\forall$	for all
$\exists$	there exists

Let $a < b$ fixed real numbers. We denote the *intervals* as follows

$[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$	closed interval
$(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$	open interval
$[a, b) := \{x \in \mathbb{R} \mid a \leq x < b\}$	half-open interval
$(a, b] := \{x \in \mathbb{R} \mid a < x \leq b\}$	half-open interval
$[a, \infty) := \{x \in \mathbb{R} \mid a \leq x\}$	closed half-line
$(a, \infty) := \{x \in \mathbb{R} \mid a < x\}$	open half-line
$(-\infty, b] := \{x \in \mathbb{R} \mid x \leq b\}$	closed half-line
$(-\infty, b) := \{x \in \mathbb{R} \mid x < b\}$	open half-line

Mathematical Induction

Mathematical induction is a powerful method to prove theorems about natural numbers.

Theorem 1.1 (Principle of Mathematical Induction) *Let $n_0 \in \mathbb{Z}$ be an integer. To prove a statement $A(n)$ for all integers $n \geq n_0$ it is sufficient to show:*

(I) *$A(n_0)$ is true.*
(II) *For any $n \geq n_0$: If $A(n)$ is true, so is $A(n+1)$* (Induction step).

It is easy to see how the principle works: First, $A(n_0)$ is true. Apply (II) to $n = n_0$ we obtain that $A(n_0+1)$ is true. Successive application of (II) yields $A(n_0+2)$, $A(n_0+3)$ are true and so on.
Let us recall the meaning of the sum sign $\sum$ and the product sign $\prod$. Suppose $m \leq n$ are integers, and a_k, $k = m, \dots, n$ are real numbers. Then we set

$$\sum_{k=m}^{n} a_k := a_m + a_{m+1} + \cdots + a_n, \qquad \prod_{k=m}^{n} a_k := a_m a_{m+1} \cdots a_n.$$

In case $m = n$ the sum and the product consist of one summand and one factor only, respectively. In case $n < m$ it is customary to set

$$\sum_{k=m}^{n} a_k := 0, \text{(empty sum)} \qquad \prod_{k=m}^{n} a_k := 1 \quad \text{(empty product)}.$$

The following rules are obvious: If $m \leq n \leq p$ and $d \in \mathbb{Z}$ are integers then

$$\sum_{k=m}^{n} a_k + \sum_{k=n+1}^{p} a_k = \sum_{k=m}^{p} a_k, \qquad \sum_{k=m}^{n} a_k = \sum_{k=m+d}^{n+d} a_{k-d} \quad \text{(index shift)}.$$

We have for $a \in \mathbb{R}$, $\displaystyle\sum_{k=m}^{n} a = (n-m+1)a$.

Example 1.1 (a) For all nonnegative integers n we have $\displaystyle\sum_{k=1}^{n}(2k-1) = n^2$.

Proof. We use induction over n. In case $n = 0$ we have an empty sum on the left hand side (lhs) and $0^2 = 0$ on the right hand side (rhs). Hence, the statement is true for $n = 0$. Suppose it is true for some fixed n. We shall prove it for $n+1$. By the definition of the sum and by induction hypothesis, $\sum_{k=1}^{n}(2k-1) = n^2$, we have

$$\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1) + 2(n+1) - 1 \underset{\text{ind. hyp.}}{=} n^2 + 2n + 1 = (n+1)^2.$$

This proves the claim for $n+1$. ∎

(b) For all positive integers $n \geq 8$ we have $2^n > 3n^2$.
Proof. In case $n = 8$ we have

$$2^n = 2^8 = 256 > 192 = 3 \cdot 64 = 3 \cdot 8^2 = 3n^2;$$

and the statement is true in this case.
Suppose it is true for some fixed $n \geq 8$, i.e. $2^n > 3n^2$ (induction hypothesis). We will show that the statement is true for $n+1$, i.e. $2^{n+1} > 3(n+1)^2$ (induction assertion). Note that $n \geq 8$ implies

$$\begin{aligned}
n-1 \geq 7 > 2 \quad & \Longrightarrow (n-1)^2 > 4 > 2 && \Longrightarrow n^2-2n-1>0\\
\Longrightarrow 3(n^2-2n-1)>0 \quad & \Longrightarrow 3n^2-6n-3>0 && \mid +3n^2+6n+3\\
\Longrightarrow 6n^2 > 3n^2+6n+3 \quad & \Longrightarrow 2\cdot 3n^2 > 3(n^2+2n+1) &&\\
\Longrightarrow 2\cdot 3n^2 > 3(n+1)^2. & && \qquad (1.1)
\end{aligned}$$

By induction assumption, $2^{n+1} = 2\cdot 2^n > 2\cdot 3n^2$. This together with (1.1) yields $2^{n+1} > 3(n+1)^2$. Thus, we have shown the induction assertion. Hence the statement is true for all positive integers $n \geq 8$. ∎

For a positive integer $n \in \mathbb{N}$ we set

$$n! := \prod_{k=1}^{n} k, \qquad \text{read: "}n\text{ factorial,"} \quad 0! = 1! = 1.$$

For non-negative integers $n, k \in \mathbb{Z}_+$ we define

$$\binom{n}{k} := \prod_{i=1}^{k} \frac{n-i+1}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 2\cdot 1}.$$

The numbers $\binom{n}{k}$ are called *binomial coefficients* since they appear in the binomial theorem, see Proposition 1.4 below. It just follows from the definition that

$$\begin{aligned}
\binom{n}{k} &= 0 \quad \text{for } k > n,\\
\binom{n}{k} &= \frac{n!}{k!(n-k)!} = \binom{n}{n-k} \quad \text{for } 0 \leq k \leq n.
\end{aligned}$$

Lemma 1.2 *For $0 \leq k \leq n$ we have:*

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$$

Proof. For $k = n$ the formula is obvious. For $0 \leq k \leq n-1$ we have

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!}\\
&= \frac{(k+1)n! + (n-k)n!}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!} = \binom{n+1}{k+1}.
\end{aligned}$$

∎

We say that X is an n-set if X has exactly n elements. We write $\operatorname{Card} X = n$ (from "cardinality") to denote the number of elements in X.

Lemma 1.3 *The number of k-subsets of an n-set is $\binom{n}{k}$.*

The Lemma in particular shows that $\binom{n}{k}$ is always an integer (which is not obvious by its definition).

Proof. We denote the number of k-subsets of an n set X_n by C_k^n. It is clear that $C_0^n = C_n^n = 1$ since $\varnothing$ is the only 0-subset of X_n and X_n itself is the only n-subset of X_n. We use induction over n. The case $n = 1$ is obvious since $C_0^1 = C_1^1 = \binom{1}{0} = \binom{1}{1} = 1$. Suppose that the claim is true for some fixed n. We will show the statement for the $(n+1)$-set $X = \{1, \dots, n+1\}$ and all k with $1 \le k \le n$. The family of $(k+1)$-subsets of X splits into two disjoint classes. In the first class $\mathcal{A}_1$ every subset contains $n+1$; in the second class $\mathcal{A}_2$, not. To form a subset in $\mathcal{A}_1$ one has to choose another k elements out of $\{1, \dots, n\}$. By induction assumption the number is $\operatorname{Card} \mathcal{A}_1 = C_k^n = \binom{n}{k}$. To form a subset in $\mathcal{A}_2$ one has to choose $k+1$ elements out of $\{1, \dots, n\}$. By induction assumption this number is $\operatorname{Card} \mathcal{A}_2 = C_{k+1}^n = \binom{n}{k+1}$. By Lemma 1.2 we obtain

$$C_{k+1}^{n+1} = \operatorname{Card} \mathcal{A}_1 + \operatorname{Card} \mathcal{A}_2 = \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

which proves the induction assertion. ∎

Proposition 1.4 (Binomial Theorem) *Let $x, y \in R$ and $n \in \mathbb{N}$. Then we have*

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

Proof. We give a direct proof. Using the distributive law we find that each of the 2^n summands of product $(x+y)^n$ has the form $x^{n-k}\,y^k$ for some $k = 0, \dots, n$. We number the n factors as $(x+y)^n = f_1 \cdot f_2 \cdots f_n$, $f_1 = f_2 = \cdots = f_n = x + y$. Let us count how often the summand $x^{n-k}\,y^k$ appears. We have to choose k factors y out of the n factors $f_1, \dots, f_n$. The remaining $n - k$ factors must be x. This gives a 1-1-correspondence between the k-subsets of $\{f_1, \dots, f_n\}$ and the different summands of the form $x^{n-k}\,y^k$. Hence, by Lemma 1.3 their number is $C_k^n = \binom{n}{k}$. This proves the proposition. ∎

Q 1. Prove that for $x \neq 1$ and $n \in \mathbb{N}$ we have

$$\sum_{k=0}^{n} x^k = \frac{1 - x^{n+1}}{1 - x}.$$

Q 2. Prove that

$$\sum_{m=k}^{n} \binom{m}{k} = \binom{n+1}{k+1}, \quad (n \ge k).$$

Q 3. Prove that

$$\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6, \quad \sum_{k=1}^{n} k^3 = n^2(n+1)^2/4.$$

Q 4. Let r be a positive integer. Prove that there exist rational numbers $a_{r1}, a_{r2}, \dots a_{rr}$ such that for all $n \in \mathbb{N}$

$$\sum_{k=1}^{n} k^r = \frac{1}{r+1} n^{r+1} + a_{rr} n^r + \cdots + a_{r1} n.$$

1.1 Real Numbers

In this lecture course we ***assume the system of real numbers to be given***.
A satisfactory discussion of the main concepts of analysis such as convergence, continuity, differentiation and integration must be based on an accurately defined number concept.
An existence proof for the real numbers is given in [7, Appendix to Chapter 1]. The author explicitly constructs the real numbers $\mathbb{R}$ starting from the rational numbers $\mathbb{Q}$.
The aim of the following two sections is to formulate the axioms which are sufficient to derive all properties and theorems of the real number system.
The rational numbers are inadequate for many purposes, both as a field and an ordered set. For instance, there is no rational x with $x^2 = 2$. This leads to the introduction of irrational numbers which are often written as infinite decimal expansions and are considered to be "approximated" by the corresponding finite decimals. Thus the sequence

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ \dots$$

"tends to $\sqrt{2}$." But unless the irrational number $\sqrt{2}$ has been clearly defined, the question must arise: What is it that this sequence "tends to"?
This sort of question can be answered as soon as the so-called "real number system" is constructed.

Example 1.2 We now show that the equation

$$x^2 = 2 \tag{1.2}$$

is not satisfied by any rational number x. Suppose to the contrary that there were such an x, we could write $x = m/n$ with integers m and n, $n \neq 0$ that are not both even. Then (1.2) implies

$$m^2 = 2n^2. \tag{1.3}$$

This shows that m^2 is even and hence m is even. Therefore m^2 is divisible by 4. It follows that the right hand side of (1.3) is divisible by 4, so that n^2 is even, which implies that n

is even. But this contradicts our choice of m and n. Hence (1.2) is impossible for rational x.

Let us examine the situation a little more closely. Set

$$A = \{x \in \mathbb{Q}_+ \,|\, x^2 < 2\} \quad \text{and} \quad B = \{x \in \mathbb{Q}_+ \mid x^2 > 2\}.$$

We shall show that A contains no largest element and B contains no smallest. That is for every $p \in A$ we can find a rational $q \in A$ with $p < q$ and for every $p \in B$ we can find a rational $q \in B$ such that $q < p$.

Suppose that p is in A. We associate with $p > 0$ the rational number

$$q = p + \frac{2 - p^2}{p+2} = \frac{2p+2}{p+2}. \tag{1.4}$$

Then

$$q^2 - 2 = \frac{4p^2 + 8p + 4 - 2p^2 - 8p - 8}{(p+2)^2} = \frac{2(p^2-2)}{(p+2)^2}. \tag{1.5}$$

If p is in A then $2 - p^2 > 0$, (1.4) shows that $q > p$, and (1.5) shows that $q^2 < 2$. If p is in B then $2 < p^2$, (1.4) shows that $q < p$, and (1.5) shows that $q^2 > 2$.

The purpose of this example has been to show that the system of rational numbers has certain gaps in spite of the fact that between any two rationals there is another: If $r < s$ then $r < (r+s)/2 < s$. The real number system fills these gaps. This is the principal reason for the fundamental role which it plays in analysis.

Q 5. If r, $r \neq 0$, is rational and x is irrational prove that $r + x$ and rx are irrational!

Q 6. Prove that $\sqrt{12}$ is irrational!

We start with the brief discussion of the general concepts of *ordered set* and *field*.

1.1.1 Ordered Sets

Definition 1.1 Let S be a set. An *order* (or *total order*) on S is a relation, denoted by $<$, with the following properties. Let $x, y, z \in S$.

(i) One and only one of the following statements

$$x < y, \quad x = y, \quad y < x$$

is true.

(ii) $x < y$ and $y < z$ implies $x < z$ (transitivity of $<$).

In this case S is called an *ordered set*.

The statement $x < y$ may be read as "x is less than y" or "x precedes y". It is convenient to write $y > x$ instead of $x < y$. The notation $x \leq y$ indicates $x < y$ or $x = y$. In other words, $x \leq y$ is the negation of $x > y$. For example, $\mathbb{R}$ is an ordered set if $r < s$ is defined to mean that $s - r > 0$ is a positive real number. Let

$$\mathbb{R}^2 := \{(x, y) \mid x, y \in \mathbb{R}\}$$

be the set of ordered pairs of real numbers (Caution: We use the notation (a,b) for the open interval as well as for ordered pairs!). Then $\mathbb{R}^2$ becomes a ordered set defining

$$(x,y) < (x',y') \iff (x < x' \quad \text{or} \quad (x = x' \quad \text{and} \quad y < y')).$$

Definition 1.2 Suppose $(S, <)$ is an ordered set, and $E \subseteq S$. If there exists a $\beta \in S$ such that $x \le \beta$ for all $x \in E$, we say that E is *bounded above*, and call β an *upper bound* of E. *Lower bounds* are defined in the same way with $\ge$ in place of $\le$.
If S is both bounded above and below, we say that S is *bounded*.

Example 1.3 (a) The intervals $[a,b]$, $(a,b]$, $[a,b)$, (a,b), $(-\infty,b)$, and $(-\infty,b]$ are bounded above by b and all numbers greater than b.
(b) $E := \{1/n \,|\, n \in \mathbb{N}\} = \{1, 1/2, 1/3, \dots\}$ is bounded above by any $\alpha \ge 1$. It is bounded below by 0. But we need another axiom tho show that 0 is the greatest lower bound.

Q 7. Let E be a nonempty subset of an ordered set; suppose α is a lower bound and β is an upper bound of E. Prove that $\alpha \le \beta$!

Definition 1.3 Suppose S is an ordered set and $E \subseteq S$. If there is an $\alpha \in E$ such that

$$\alpha \ge x \quad \text{for all } x \text{ in } E$$

then α is called the *maximum of* E and is denoted by $\alpha = \max E$.
Similarly, $\beta \in E$ is called the *minimum* of E if $\beta \le x$ for all $x \in E$; $\beta = \min E$.

Example 1.4 (a) $E := [0,1)$, $0 = \min E$, E has no maximum.
(b) $E := \{1/n \,|\, n \in \mathbb{N}\}$, $\max E = 1$, E has no minimum.

Q 8. Give the proofs of the statements in Example 1.4.

Remarks 1.1 1. If E has a maximum it is unique.
2. If E is a finite set it has always a maximum and a minimum.
3. $\max E$ is an upper bound of E.

More important than maximum and minimum are the following more general notions:

Definition 1.4 Suppose S is an ordered set, $E \subseteq S$, an E is bounded above. Suppose there exists an $\alpha \in S$ such that

(i) α is an upper bound of E.
(ii) If β is an upper bound of E then $\alpha \le \beta$.

Then α is called the *least upper bound of* E or *supremum of* E (it is clear from (ii) that there is at most one such α), and we write

$$\alpha = \sup E.$$

The *greatest lower bound* or *infimum* of a set E which is bounded below is defined in the same manner: The statement

$$\alpha = \inf E$$

means that α is a lower bound of E and for all lower bounds β of E we have $\beta \le \alpha$.

An equivalent formulation of (ii) is the following: (ii') If $\beta < \alpha$ then β is not an upper bound of E.

Example 1.5 (a) Consider the sets A and B of Example 1.2 as subsets of the ordered set $\mathbb{Q}$. Since $A \cup B = \mathbb{Q}_+$ (there is no rational number with $x^2 = 2$) the upper bounds of A are exactly the elements of B. Since B contains no smallest member, *A has no least upper bound in $\mathbb{Q}_+$*.
Similarly, B is bounded below by A and all negative rational numbers. Since A has no largest member, *B has no greatest lower bound in $\mathbb{Q}$*.
(b) If $\alpha = \sup E$ exists, then α may or may not belong to E. For instance consider $[0,1)$ and $[0,1]$. Then

$$1 = \sup[0,1) = \sup[0,1],$$

and $1 \notin [0,1)$, $1 \in [0,1]$. We shall show that $\sup[0,1) = 1$. Obviously, 1 is an upper bound of this interval. Suppose that $\beta < 1$. Then $\beta < (\beta+1)/2 < 1$. Since $(\beta+1)/2 \in [0,1)$, β is not an upper bound. Consequently, 1 is the supremum of $[0,1)$. If $\max E$ exists then $\sup E$ also exists and $\max E = \sup E$. Indeed, $\max E$ is an upper bound for E and if β is another upper bound we have $\max E \le \beta$ since $\max E \in E$. The converse direction is also true and easy to see: If $\sup E$ exists *in* E then it equals $\max E$.

1.1.2 Fields

Definition 1.5 A *field* is a set F with two operations, called *addition* and *multiplication* which satisfy the following so-called "field axioms" (A),(M), and (D):

(A) Axioms for addition

(A1) If $x \in F$ and $y \in F$ then their sum $x + y$ is in F.
(A2) Addition is commutative: $x + y = y + x$ for all $x, y \in F$.
(A3) Addition is associative: $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$.
(A4) F contains an element 0 such that $0 + x = x$ for all $x \in F$.
(A5) To every $x \in F$ there exists an element $-x \in F$ such that $x + (-x) = 0$.

(M) Axioms for multiplication

(M1) If $x \in F$ and $y \in F$ then their product xy is in F.
(M2) Multiplication is commutative: $xy = yx$ for all $x, y \in F$.
(M3) Multiplication is associative: $(xy)z = x(yz)$ for all $x, y, z \in F$.
(M4) F contains an element 1 such that $1x = x$ for all $x \in F$.
(M5) If $x \in F$ and $x \neq 0$ then there exists an element $1/x \in F$ such that $x \cdot (1/x) = 1$.

(D) The distributive law

$$x(y + z) = xy + xz$$

holds for all $x, y, z \in F$.

Remarks 1.2 (a) One usually writes

$$x - y,\ \frac{x}{y},\ x + y + z,\ xyz,\ x^2,\ x^3,\ 2x, \dots$$

in place of

$$x + (-y),\ x \cdot \frac{1}{y},\ (x + y) + z,\ (xy)z,\ x \cdot x,\ x \cdot x \cdot x,\ 2x, \dots$$

(b) The field axioms clearly hold in $\mathbb{Q}$ if addition and multiplication have their customary meaning. Thus $\mathbb{Q}$ is a field. The integers $\mathbb{Z}$ form *not* a field since $2 \in \mathbb{Z}$ has no multiplicative inverse (axiom (M5) is not fulfilled).
(c) The smallest field is $\mathbb{F}_2 = \{0, 1\}$ consisting of the neutral element 0 for addition and the neutral element 1 for multiplication. Multiplication and addition are defined as follows $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$. It is easy to check the field axioms (A), (M), and (D) directly. Since $1 + 1 = 0$ one can see that the field axioms alone are not enough to detect the positive integers inside the real numbers. We need additional axioms namely ordering properties.
(d) Although it is not our purpose to study fields (or any other algebraic structures) in detail, it is worthwhile to prove that some familiar properties of $\mathbb{Q}$ are consequences of the field axioms; once we do this, we will not need to do it again for the real numbers and for the complex numbers.
(e) (A1) to (A5) and (M1) to (M5) mean that both $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are *commutative (or abelian) groups*, respectively.

Proposition 1.5 *The axioms of addition imply the following statements.*
(a) *If $x + y = x + z$ then $y = z$ (Cancellation law).*
(b) *If $x + y = x$ then $y = 0$ (The element 0 is unique).*
(c) *If $x + y = 0$ the $y = -x$ (The inverse $-x$ is unique).*
(d) $-(-x) = x$.

Proof. If $x + y = x + z$, the axioms (A) give

$$y = 0 + y = (-x + x) + y = -x + (x + y) = -x + (x + z) = (-x + x) + z = 0 + z = z.$$

This proves (a). Take $z = 0$ in (a) to obtain (b). Take $z = -x$ in (a) to obtain (c). Since $-x + x = 0$, (c) with $-x$ in place of x gives (d). ■

Proposition 1.6 *The axioms for multiplication imply the following statements.*
(a) *If $x \neq 0$ and $xy = xz$ then $y = z$ (Cancellation law).*
(b) *If $x \neq 0$ and $xy = x$ then $y = 1$ (The element 1 is unique).*
(c) *If $x \neq 0$ and $xy = 1$ then $y = 1/x$ (The inverse $1/x$ is unique).*
(d) *If $x \neq 0$ then $1/(1/x) = x$.*

The proof is so similar to that of Proposition 1.5 that we omit it.

Proposition 1.7 *The field axioms imply the following statements, for any $x, y, z \in F$*
(a) $0x = 0$.
(b) *If* $xy = 0$ *then* $x = 0$ *or* $y = 0$.
(c) $(-x)y = -(xy) = x(-y)$.
(d) $(-x)(-y) = xy$.

Proof. $0x + 0x = (0 + 0)x = 0x$. Hence 1.5 (b) implies that $0x = 0$, and (a) holds. Suppose to the contrary that both $x \neq 0$ and $y \neq 0$ then (a) gives

$$1 = \frac{1}{y} \cdot \frac{1}{x} xy = \frac{1}{y} \cdot \frac{1}{x} 0 = 0,$$

a contradiction. Thus (b) holds.
The first equality in (c) comes from

$$(-x)y + xy = (-x + x)y = 0y = 0,$$

combined with 1.5 (b); the other half of (c) is proved in the same way. Finally,

$$(-x)(-y) = -[x(-y)] = -[-xy] = xy$$

by (c) and 1.5 (d). ∎

Q 9. Prove the laws of fractions ($a, b, c, d \in \mathbb{R}$, $b \neq 0$, $d \neq 0$):
(a) $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.
(b) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$.
(c) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

1.1.3 Ordered Fields

In analysis dealing with equations is as important as dealing with inequalities. Calculations with inequalities are based on the ordering axioms. It turns out that all can be reduced to the notion of positivity.
In F there are distinguished positive elements ($x > 0$) such that the following axioms are valid.

Definition 1.6 An *ordered field* is a field F which is also an ordered set, such that for all $x, y, z \in F$

(O) Axioms for ordered fields

(O1) $x > 0$ and $y > 0$ implies $x + y > 0$,
(O2) $x > 0$ and $y > 0$ implies $xy > 0$.

If $x > 0$ we call x *positive*; if $x < 0$, x is *negative*.

For example $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields, if $x > y$ is defined to mean that $x - y$ is positive.

Proposition 1.8 *The following statements are true in every ordered field F.*
(a) *If $x < y$ and $a \in F$ then $a + x < a + y$.*
(b) *If $x < y$ and $x' < y'$ then $x + x' < y + y'$.*

Proof. (a) By assumption $(a + y) - (a + x) = y - x > 0$. Hence $a + x < a + y$.
(b) By assumption an by (a) we have $x+x' < y+x'$ and $y+x' < y+y'$. Using transitivity (Definition 1.1 (ii)) we have $x + x' < y + y'$. ■

Proposition 1.9 *The following statements are true in every ordered field.*
(a) *If $x > 0$ then $-x < 0$, and if $x < 0$ then $-x > 0$.*
(b) *If $x > 0$ and $y < z$ then $xy < xz$.*
(c) *If $x < 0$ and $y < z$ then $xy > xz$.*
(d) *If $x \neq 0$ then $x^2 > 0$. In particular, $1 > 0$.*
(e) *If $0 < x < y$ then $0 < 1/y < 1/x$.*

Proof. (a) If $x > 0$ then $0 = -x + x > -x + 0 = -x$, so that $-x < 0$. If $x < 0$ then $0 = -x + x < -x + 0 = -x$ so that $-x > 0$. This proves (a).
(b) Since $z > y$, we have $z - y > 0$, hence $x(z - y) > 0$ by axiom (O2), and therefore

$$xz = x(z - y) + xy \underset{Prp.\,1.8}{>} 0 + xy = xy.$$

(c) By (a), (b) and Proposition 1.7 (c)

$$-[x(z - y)] = (-x)(z - y) > 0,$$

so that $x(z - y) < 0$, hence $xz < xy$.
(d) If $x > 0$ axiom 1.6 (ii) gives $x^2 > 0$. If $x < 0$ then $-x > 0$, hence $(-x)^2 > 0$ But $x^2 = (-x)^2$ by Proposition 1.7 (d). Since $1^2 = 1$, $1 > 0$.
(e) If $y > 0$ and $v \leq 0$ then $yv \leq 0$. But $y\cdot(1/y) = 1 > 0$. Hence $1/y > 0$, likewise $1/x > 0$. If we multiply $x < y$ by the the positive quantity $(1/x)(1/y)$, we obtain $1/y < 1/x$. ■

Remark 1.3 The finite field $\mathbb{F}_2 = \{0, 1\}$, see Remarks 1.2, is not an ordered field since $1 + 1 = 0$ which contradicts $1 > 0$.
The field of complex numbers $\mathbb{C}$ (see below) is not an ordered field since $\mathrm{i}^2 = -1$ contradicts Proposition 1.9 (d).

Q 10. Show that the transitivity of $<$ is a consequence of (O1), (O2), and (A)!

1.1.4 Embedding of natural numbers into the real numbers

Let F be an ordered field. In order to distinguish 0 and 1 in F from the integers 0 and 1 we temporarily write 0_F and 1_F. For a positive integer $n \in \mathbb{N}$, $n \geq 2$ we define

$$n_F := 1_F + 1_F + \cdots + 1_F \quad (n \text{ times}).$$

Lemma 1.10 *We have $n_F > 0_F$ for all $n \in \mathbb{N}$.*

Proof. We use induction over n. By Proposition 1.9 (d) the statement is true for $n = 1$. Suppose it is true for a fixed n, i. e. $n_F > 0_F$. Moreover $1_F > 0_F$. Using axiom (O2) we obtain $(n+1)1_F = n_F + 1_F > 0$. ∎

From Lemma 1.10 it follows that $m \neq n$ implies $n_F \neq m_F$. Indeed, let n be greater than m, say $n = m + k$ for some $k \in \mathbb{N}$, then $n_F + k_F = m_F$. Since $k_F > 0$ it follows from 1.8 (a) that $n_F > m_F$. In particular, $n_F \neq m_F$. Hence, the mapping

$$\mathbb{N} \to F, \qquad n \mapsto n_F$$

is injective. In this way the positive integers are embedded into the real numbers. Addition and multiplication of natural numbers and of its embeddings are the same:

$$n_F + m_F = (n+m)_F, \qquad n_F\, m_F = (nm)_F.$$

From now on we identify a natural number with the associated real number. We write n for n_F.

Definition 1.7 (The Archimedean Axiom) An ordered field F is called *Archimedean* if for all $x, y \in F$ with $x > 0$ and $y > 0$ there exists $n \in \mathbb{N}$ such that $nx > y$.

An equivalent formulation is: The subset $\mathbb{N} \subset F$ of positive integers is not bounded above. Choose $x = 1$ in the above definition, then for any $y \in F$ there in an $n \in \mathbb{N}$ such that $n > y$; hence $\mathbb{N}$ is not bounded above.
Suppose $\mathbb{N}$ is not bounded and $x > 0, y > 0$ are given. Then y/x is not an upper bound for $\mathbb{N}$, that is there is some $n \in \mathbb{N}$ with $n > y/x$ or $nx > y$.

Remark 1.4 The fields $\mathbb{Q}$ and $\mathbb{R}$ are Archimedean, see below. But there exist ordered fields without this property. Let $F := \mathbb{R}(t)$ the field of rational functions $f(t) = p(t)/q(t)$ where p and q are polynomials with real coefficients. Since p and q have only finitely many zeros, for large t, $f(t)$ is either positive or negative. In the first case we set $f > 0$. In this way $\mathbb{R}(t)$ becomes an ordered field. But $t > n$ for all $n \in \mathbb{N}$ since the polynomial $f(t) = t - n$ becomes positive for large t (and fixed n).

1.1.5 The completeness of $\mathbb{R}$

Using the axioms so far we are not yet able to prove the existence of irrational numbers. We need the completeness axiom.

Definition 1.8 (Order Completeness) An ordered set S is said to be *order complete* if for every non-empty subset $E \subset S$ which is bounded above, there exists the least upper bound $\sup E$ in S.

(C) Completeness

The real numbers are order complete, i. e. every subset $E \subset \mathbb{R}$ which is bounded above has a least upper bound.

The set $\mathbb{Q}$ of rational numbers is not order complete since, for example, the bounded set $A = \{x \in \mathbb{Q}_+ \mid x^2 < 2\}$ has no least upper bound in $\mathbb{Q}$.
Later we will define the square root of 2 as $\sqrt{2} := \sup A$. The existence of $\sqrt{2}$ in $\mathbb{R}$ is furnished by the completeness axiom (C).
The axiom (C) implies that every subset $E \subset \mathbb{R}$ which is bounded below has a greatest lower bound. This is an easy consequence of Homework 1.4 (a).
We will see that an order complete field is always Archimedean.

Proposition 1.11 (a) $\mathbb{R}$ *is Archimedean.*
(b) *If* $x, y \in \mathbb{R}$, *and* $x < y$ *then there is a* $p \in \mathbb{Q}$ *with* $x < p < y$.

Part (b) may be stated by saying that $\mathbb{Q}$ *is dense in* $\mathbb{R}$.
Proof. (a) Let $x, y > 0$ be real numbers which do not fulfill the Archimedean property. That is, if $A := \{nx \mid n \in \mathbb{N}\}$, then y would be an upper bound of A. Then (C) furnishes that A has a least upper bound $\alpha = \sup A$. Since $x > 0$, $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of A. Hence $\alpha - x < mx$ for some $m \in \mathbb{N}$. But then $\alpha < (m+1)x$, which is impossible, since α is an upper bound of A.
We give an alternative proof for (a) and show that $\mathbb{N}$ is not bounded above. Suppose to the contrary that $\mathbb{N}$ has an upper bound. By (C), $\mathbb{N}$ has a least upper bound, say $\alpha = \sup \mathbb{N}$. By Lemma 1.12 (2) to $\varepsilon = 1/2$ there exists an $n \in \mathbb{N}$ such that $\alpha - 1/2 < n$. Adding 1 we obtain $\alpha < \alpha + 1/2 < n + 1$. We conclude that α is not an upper bound of $\mathbb{N}$ since $n + 1 \in \mathbb{N}$ and $n + 1 > \alpha$. A contradiction!
(b) Since $x < y$, we have $y - x > 0$ and (a) furnishes a positive integer n such that $n(y - x) > 1$. Apply (a) again to obtain positive integers m_1 and m_2 with $m_1 > nx$ and $m_2 > -nx$. Then

$$-m_2 < nx < m_1.$$

Hence there is an integer m with $-m_2 \le m \le m_1$ such that

$$m - 1 \le nx < m.$$

If we combine these inequalities, we obtain

$$nx < m \le 1 + nx < ny.$$

Since $n > 0$, it follows that $x < m/n < y$. This proves (b) with $p = m/n$. ∎

Remark: If $x, y \in \mathbb{Q}$ with $x < y$, then there exists $z \in \mathbb{R} \setminus \mathbb{Q}$ with $x < z < y$; chose $z = (x - y)/\sqrt{2} + y$.
We shall show that $E := \{1/n \mid n \in \mathbb{N}\}$ has infimum 0. Obviously, 0 is a lower bound. Suppose that $\alpha > 0$. Since $\mathbb{R}$ is Archimedean, we find $m \in \mathbb{N}$ such that $1 < m\alpha$ or, equivalently $1/m < \alpha$. Hence, α is not a lower bound for E which proves the claim.

Remarks 1.5 (a) Axiom (C) is equivalent to the Archimedean property together with the *topological* completeness ("Every Cauchy sequence in $\mathbb{R}$ is convergent," see Proposition 2.16).
(b) Axiom (C) is equivalent to the *axiom of nested intervals*, see Proposition 2.9 below: Let $I_n := [a_n, b_n]$ a sequence of closed nested intervals ($I_{n+1} \subseteq I_n$) such that:

For all $\varepsilon > 0$ there exists n_0 such that $0 \le b_n - a_n < \varepsilon$ for all $n \ge n_0$.

For any such interval sequence $\{I_n\}$ there exists a unique real number $a \in \mathbb{R}$ which is a member of all intervals, i. e. $\{a\} = \bigcap_{n\in\mathbb{N}} I_n$.

Supremum and Infimum revisited

The following equivalent definition for the supremum of sets of real numbers is often used in the sequel.

Lemma 1.12 *Suppose that $E \subset \mathbb{R}$. Then α is the supremum of E if and only if*

(1) *α is an upper bound for E,*
(2) *For all $\varepsilon > 0$ there exists $x \in E$ with $\alpha - \varepsilon < x$.*

Proof. Suppose first that $\alpha = \sup E$. Then α is an upper bound for E. Since α is the least upper bound of E any smaller number is not an upper bound. Hence, $\alpha - \varepsilon < \alpha$ is not an upper bound; that is there exist $x \in E$ with $x > \alpha - \varepsilon$.
Suppose now that the conditions (1) and (2) of the lemma are fulfilled. We will show that the second condition for the least upper bound is satisfied. For, let $\beta < \alpha$ and set $\varepsilon = \alpha - \beta$. Hence $\varepsilon > 0$. By (2), there exists $x \in E$ such that $\alpha - \varepsilon < x$. That is $\alpha - (\alpha - \beta) = \beta < x$. We conclude that β is not an upper bound for E. Hence $\alpha = \sup E$. ∎

Lemma 1.13 (a) *Let $M \subset \mathbb{R}$ and $N \subset \mathbb{R}$ nonempty subsets which are bounded above. Then $M + N := \{m + n \mid m \in M, n \in N\}$ is bounded above and*

$$\sup(M + N) = \sup M + \sup N.$$

(b) *Let $M \subset \mathbb{R}_+$ and $N \subset \mathbb{R}_+$ nonempty subsets which are bounded above. Then $MN := \{mn \mid m \in M, n \in N\}$ is bounded above and*

$$\sup(MN) = \sup M \sup N.$$

Proof. (a) Let $s = \sup M$ and $t = \sup N$; then $s \geq m$ for all $m \in M$ and $t \geq n$ for all N in N. Hence $s + t \geq x$ for all $x \in M + N$, and $s + t$ is an upper bound for $M + N$. Let $\varepsilon > 0$ be given. Since $s = \sup M$ Lemma 1.12 furnishes the existence of some $m \in M$ with $m > s - \varepsilon/2$. Similarly, there is some $n \in N$ with $n > t - \varepsilon/2$. Taking the sum of both inequalities gives $m + n > s + t - \varepsilon$. By Lemma 1.12, $s + t$ is the least upper bound of $M + N$.
(b) Let $s = \sup M$ and $t = \sup N$; then $s \geq m$ for all $m \in M$ and $t \geq n$ for all n in N. Hence $st \geq x$ for all $x \in MN$, and st is an upper bound for MN. If $s = 0$ or $t = 0$, $M = \{0\}$ or $N = \{0\}$ and the statement is clear. Suppose now $s > 0$ and $t > 0$. Let $\varepsilon > 0$ be given. Choose $\varepsilon_1 < \varepsilon$ such that

$$\varepsilon_1 < s(s+t) \quad \text{and} \quad \varepsilon_1 < t(s+t). \tag{1.6}$$

Then, by Lemma 1.12, there exist $m \in M$ and $n \in N$ such that

$$m > s - \frac{\varepsilon_1}{s+t} \quad \text{and} \quad n > t - \frac{\varepsilon_1}{s+t}. \tag{1.7}$$

The inequalities (1.6) ensure that the right hand sides of (1.7) are positive. So we can multiply them:

$$mn > \left(s - \frac{\varepsilon_1}{s+t}\right)\left(t - \frac{\varepsilon_1}{s+t}\right) = st - \varepsilon_1 + \frac{\varepsilon_1^2}{s+t} > st - \varepsilon_1 > st - \varepsilon.$$

Using Lemma 1.12 again, we conclude that st is the least upper bound of MN. ■

1.1.6 The Absolute Value

For $x \in \mathbb{R}$ one defines

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

Lemma 1.14 *For $a, x, y \in \mathbb{R}$ we have*
(a) $|x| \geq 0$ *and* $|x| = 0$ *if and only if* $x = 0$. *Further* $|-x| = |x|$.
(b) $\pm x \leq |x|$, $|x| = \max\{x, -x\}$, *and* $|x| \leq a \iff (x \leq a \quad \text{and} \quad -x \leq a)$.
(c) $|xy| = |x|\,|y|$ *and* $|x/y| = |x| / |y|$ *if* $y \neq 0$.
(d) $|x + y| \leq |x| + |y|$ *(triangle inequality).*
(e) $||x| - |y|| \leq |x + y|$.

Proof. The first part of (a) is clear by Proposition 1.9 (a).
For the second part suppose first $x \geq 0$. Then $-x < 0$ and consequently $|-x| = -(-x) = x = |x|$. If $x < 0$ then $-x > 0$ and $|-x| = -x = |x|$. This proves (a).
(b) Suppose first that $x \geq 0$. Then $x \geq 0 \geq -x$ and we have $\max\{x, -x\} = x = |x|$.If $x < 0$ then $-x > 0 > x$ and $\max\{-x, x\} = -x = |x|$. This proves the first part of (b).

The second part of (b) stems from the fact that the maximum of a set coincides with its supremum and a is an upper bound of $\{x, -x\}$.
One proves the first part of (c) by verifying the four cases i) $x, y \geq 0$, ii) $x \geq 0$, $y < 0$, iii) $x < 0$, $y \geq 0$, and iv) $x, y < 0$. To the second part.
Since $x = (x/y) \cdot y$ we have by (c) $|\,x\,| = |\,x/y\,|\,|\,y\,|$. The claim follows.
(d) Since $\pm x \leq |\,x\,|$ and $\pm y \leq |\,y\,|$ by (b) it follows from Proposition 1.8 (b) that $\pm(x+y) \leq |\,x\,| + |\,y\,|$. By the second part of (b) this means $|\,x+y\,| \leq |\,x\,| + |\,y\,|$.
(e) Inserting $u := x + y$ and $v := -y$ into $|\,u+v\,| \leq |\,u\,| + |\,v\,|$ one obtains $|\,x\,| \leq |\,x+y\,| + |\,-y\,| = |\,x+y\,| + |\,y\,|$. Adding $-|\,y\,|$ on both sides one obtains $|\,x\,| - |\,y\,| \leq |\,x+y\,|$. Changing the role of x and y in the last inequality yields $-(|\,x\,| - |\,y\,|) \leq |\,x+y\,|$. The claim follows using (b). ∎

Q 11. Define a relation $<$ on $\mathbb{R}^2 = \{(x, y) \mid x,\, y \in \mathbb{R}\}$ by

$$(x, y) < (x', y') \quad \text{if} \quad (x < x' \quad \text{or} \quad (x = x' \quad \text{and} \quad y < y')).$$

Prove that with this relation, $(\mathbb{R}^2, <)$ is an ordered set. Is $(\mathbb{R}^2, <)$ order complete?

1.1.7 Powers of real numbers

We shall prove the existence of nth roots of positive reals. We already know x^n, $n \in \mathbb{Z}$. It is recursively defined by $x^n := x^{n-1} \cdot x$, $x^1 := x$, $n \in \mathbb{N}$ and $x^n := 1/x^{-n}$ for $n < 0$.

Proposition 1.15 (Bernoulli's inequality) (a) *Let $x \geq -1$ and $n \in \mathbb{N}$. Then we have*

$$(1 + x)^n \geq 1 + nx.$$

Equality holds if and only if $x = 0$ or $n = 1$.
(b) *If $y > 0$ and $n \in \mathbb{N}$ we have*

$$y^{\frac{1}{n}} \leq 1 + \frac{1}{n}(y - 1).$$

Equality holds if and only if $y = 1$ or $n = 1$.

Proof. (a) We use induction over n. In case $n = 1$ we obtain equality. Suppose the claim is true for some fixed $n \geq 1$. Since $1 + x \geq 0$ by Proposition 1.9 (b) multiplication of the induction assumption by this factor yields

$$(1 + x)^{n+1} \geq (1 + nx)(1 + x) = 1 + (n + 1)x + nx^2 \geq 1 + (n + 1)x.$$

This proves the assertion for $n + 1$. We have equality in the second estimation only if $x = 0$. It turns out that the first estimation is also an equality in this case.
(b) Putting $x := y^{\frac{1}{n}} - 1$ we have $x > -1$ and (a) applies:

$$y = (y^{1/n})^n \geq 1 + n(y^{1/n} - 1) \iff \frac{1}{n}(y - 1) \geq y^{1/n} - 1.$$

The claim follows. ∎

Lemma 1.16 (a) *For $x, y \in \mathbb{R}$ with $x, y > 0$ and $n \in \mathbb{N}$ we have*

$$x < y \Longleftrightarrow x^n < y^n.$$

(b) *For $x, y \in \mathbb{R}_+$ and $n \in \mathbb{N}$ we have*

$$nx^{n-1}(y-x) \le y^n - x^n \le ny^{n-1}(y-x). \tag{1.8}$$

We have equality if and only if $n = 1$ or $x = y$.

Proof. (a) Observe that

$$y^n - x^n = (y-x)\sum_{k=1}^{n} y^{n-k}\, x^{k-1} = c(y-x)$$

with $c := \sum_{k=1}^{n} y^{n-k}\, x^{k-1} > 0$ since $x, y > 0$. The claim follows.
(b) We have

$$\begin{aligned} y^n - x^n - nx^{n-1}(y-x) &= (y-x)\sum_{k=1}^{n}\left(y^{n-k}x^{k-1} - x^{n-1}\right) \\ &= (y-x)\sum_{k=1}^{n} x^{k-1}\left(y^{n-k} - x^{n-k}\right) \ge 0 \end{aligned}$$

since by (a) $y - x$ and $y^{n-k} - x^{n-k}$ have the same sign. The proof of the second inequality is quite analogous. ∎

Proposition 1.17 *For every real $x > 0$ and every positive integer $n \in \mathbb{N}$ there is one and only one $y > 0$ such that $y^n = x$.*

This number y is written $\sqrt[n]{x}$ or $x^{\frac{1}{n}}$, and it is called "the nth root of x".
Proof. The uniqueness is clear since by Lemma 1.16 (a) $0 < y_1 < y_2$ implies $0 < y_1^n < y_2^n$. Set

$$E := \{t \in \mathbb{R}_+ \mid t^n < x\}.$$

Observe that $E \ne \varnothing$ since $0 \in E$. We show that E is bounded above. By Bernoulli's inequality and since $x < nx$ we have

$$\begin{aligned} t \in E &\Leftrightarrow t^n < x < 1 + nx < (1+x)^n \\ &\underset{\text{Lemma 1.16}}{\Leftrightarrow} t < 1 + x \end{aligned}$$

Hence, $1 + x$ is an upper bound for E. By the order completeness of $\mathbb{R}$ there exists $y \in \mathbb{R}$ such that $y = \sup E$. We have to show that $y^n = x$. For, we will show that each of the inequalities $y^n > x$ and $y^n < x$ leads to a contradiction.
Assume $y^n < x$ and consider $(y+h)^n$ with "small" h $(0 < h < 1)$. Lemma 1.16 (b) implies

$$0 \le (y+h)^n - y^n \le n\,(y+h)^{n-1}(y+h-y) < h\,n(y+1)^{n-1}.$$

Choosing h small enough that $h\,n(y+1)^{n-1} < x - y^n$ we may continue

$$(y+h)^n - y^n \le x - y^n.$$

Consequently, $(y+h)^n < x$ and therefore $y+h \in E$. Since $y+h > y$, this contradicts the fact that y is an upper bound of E.
Assume $y^n > x$ and consider $(y-h)^n$ with "small" h $(0 < h < 1)$. Again by Lemma 1.16 (b) we have

$$0 \le y^n - (y-h)^n \le n\,y^{n-1}(y - y + h) < h\,ny^{n-1}.$$

Choosing h small enough that $h\,ny^{n-1} < y^n - x$ we may continue

$$y^n - (y-h)^n \le y^n - x.$$

Consequently, $x < (y-h)^n$ and therefore $t^n < x < (y-h)^n$ for all t in E. Hence $y - h$ is an upper bound for E smaller than y. This contradicts the fact that y is the *least* upper bound. Hence $y^n = x$, and the proof is complete. ■

Corollary 1.18 *If a and b are positive real numbers and $n \in \mathbb{N}$ then $(ab)^{1/n} = a^{1/n}\,b^{1/n}$.*

Proof. Put $\alpha = a^{1/n}$ and $\beta = b^{1/n}$. Then

$$ab = \alpha^n \beta^n = (\alpha\beta)^n,$$

since multiplication is commutative (Axiom (M2)). The uniqueness assertion of Proposition 1.17 shows therefore that

$$(ab)^{1/n} = \alpha\beta = a^{1/n}\,b^{1/n}.$$

■

Lemma 1.19 *Fix $b > 0$.* (a) *If $m, n, p, q \in \mathbb{Z}$ and $n > 0$, $q > 0$, and $r = m/n = p/q$. Then we have*

$$(b^m)^{1/n} = (b^p)^{1/q}. \tag{1.9}$$

Hence it makes sense to define $b^r = (b^m)^{1/n}$.
(b) *If $a, b > 0$ are real and $r, s \in \mathbb{Q}$ then we have*

$$a^{r+s} = a^r a^s, \quad a^{rs} = (a^r)^s, \quad \textit{and} \quad (ab)^r = a^r b^r.$$

Proof. (a) Using the power laws in the case that the exponents are positive integers $a^{kl} = (a^k)^l = (a^l)^k$ and the definition of the nth root $(c^{1/n})^n = c$ we obtain

$$\left((b^m)^{\frac{1}{n}}\right)^{nq} = \left(\left((b^m)^{\frac{1}{n}}\right)^n\right)^q = (b^m)^q = b^{mq} = b^{pn} = (b^p)^n = \left(\left((b^p)^{\frac{1}{q}}\right)^q\right)^n = \left((b^p)^{\frac{1}{q}}\right)^{nq}.$$

Taking the nqth root and using its uniqueness, we obtain our assertion.
The proofs of the statements in (b) are also purely algebraic. We prove only the second statement and leave the rest as an exercise. For, let $r = m/n$ and $s = p/q$ with positive integers n and q and integers m, p. We obtain

$$\left(\left(a^{\frac{m}{n}}\right)^{\frac{p}{q}}\right)^{nq} = \left(\left(\left(a^{\frac{m}{n}}\right)^{\frac{p}{q}}\right)^{q}\right)^{n} = \left(\left(\left(\left(a^{\frac{m}{n}}\right)^{p}\right)^{\frac{1}{q}}\right)^{q}\right)^{n} = \left(\left(\left(a^{m}\right)^{\frac{1}{n}}\right)^{p}\right)^{n} = (a^m)^p = a^{mp}.$$

Taking the nqth root we obtain

$$\left(a^{\frac{m}{n}}\right)^{\frac{p}{q}} = (a^{mp})^{\frac{1}{nq}} = a^{\frac{mp}{nq}},$$

and therefore, $(a^r)^s = a^{rs}$. ■

Definition 1.9 Fix $b > 1$. If $x \in \mathbb{R}$ define

$$b^x = \sup\{b^p \mid p \in \mathbb{Q},\, p < x\}.$$

For $0 < b < 1$ set

$$b^x = \frac{1}{(1/b)^x}.$$

Without proof we give the familiar laws for powers and exponentials. Later we will redefine the power b^x with real exponent. Then we are able to give easier proofs.

Lemma 1.20 *If $a, b > 0$ and $x, y \in \mathbb{R}$, then*
(a) $b^{x+y} = b^x b^y$, $b^{x-y} = b^x/b^y$
(b) $b^{xy} = (b^x)^y$
(c) $(ab)^x = a^x b^x$.

1.1.8 Review of Trigonometric Functions

Degrees and Radians

The circumference C and the area A of a circle with radius r are

$$C = 2\pi r \quad \text{and} \quad A = \pi r^2,$$

where $\pi = 3.14159\ldots$. We will give a precise definition of π later. If two rays are drawn from the center of a circle, both the length and the area of the part of the circle between the rays are proportional to the angle between the rays. So that the length C_θ and the area A_θ are determined by

$$C_\theta = \frac{\theta}{360^\circ} 2\pi r, \quad A_\theta = \frac{\theta}{360^\circ}\pi r^2 \quad (\theta \text{ in degrees}).$$

These formulas become simpler if we adopt the *radian* unit of measure, in which the total angular measure of a circle (360°) is defined to be 2π.

$$C_\theta = \theta\, r, \quad A_\theta = \frac{1}{2}\theta r^2, \quad (\theta \text{ in radians}).$$

Conversion between radians and degrees are made by multiplying or dividing by the factor $\frac{360^\circ}{2\pi}$.
The following table gives some important angles in degrees and radians:

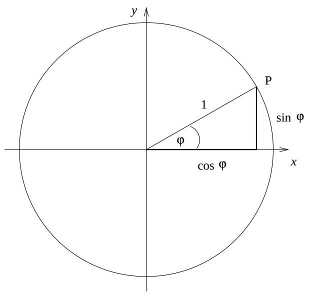
Degrees	0°	30°	45°	60°	90°	120°	135°	150°	180°	270°	360°
Radians	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\frac{2\pi}{3}$	$\frac{3\pi}{4}$	$\frac{5\pi}{6}$	π	$\frac{3\pi}{2}$	2π

Sine and Cosine

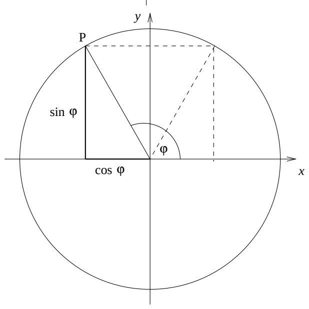
The sine, cosine, and tangent functions are defined in terms of ratios of sides of a right triangle:

$$\begin{aligned}
\cos\theta &= \frac{\text{side adjacent to } \theta}{\text{hypotenuse}}, \\
\sin\theta &= \frac{\text{side opposite to } \theta}{\text{hypotenuse}}, \\
\tan\theta &= \frac{\text{side opposite to } \theta}{\text{side adjacent to } \theta}.
\end{aligned}$$

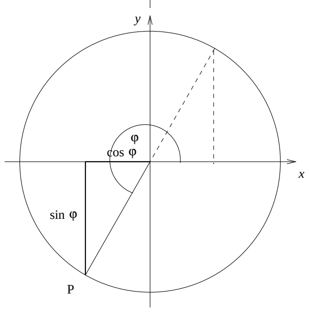
Let φ be any angle between 0° and 360°. Further let P be the point on the unit circle (with center in $(0,0)$ and radius 1) such that the ray from P to the origin $(0,0)$ and the positive x-axis make an angle φ. Then $\cos\varphi$ and $\sin\varphi$ are defined to be the x-coordinate and the y-coordinate of the point P, respectively.



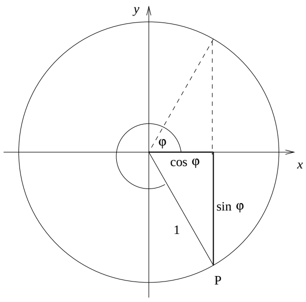
If the angle φ is between 0° and 90° this new definition coincides with the definition using the right triangle since the hypotenuse which is a radius of the unit circle has now length 1.



If $90^\circ < \varphi < 180^\circ$ we find $\cos\varphi = -\cos(180^\circ - \varphi) < 0$ and $\sin\varphi = \sin(180^\circ - \varphi) > 0$.



If $180^\circ < \varphi < 270^\circ$ we find $\cos\varphi = -\cos(\varphi - 180^\circ) < 0$ and $\sin\varphi = -\sin(\varphi - 180^\circ) < 0$.



If $270° < \varphi < 360°$ we find $\cos\varphi = \cos(360° - \varphi) > 0$ and $\sin\varphi = -\sin(360° - \varphi) < 0$.

For angles greater than 360° or less than 0° define

$$\cos\varphi = \cos(\varphi + k\,360°), \quad \sin\varphi = \sin(\varphi + k\,360°),$$

where $k \in \mathbb{Z}$ is chosen such that $0° \le \varphi + k\,360° < 360°$. Thinking of φ to be given in radians, cosine and sine are functions defined for all real φ taking values in the closed interval $[-1, 1]$.
If $\varphi \ne \frac{\pi}{2} + k\pi$, $k \in \mathbb{Z}$ then $\cos\varphi \ne 0$ and we define

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

If $\varphi \ne k\pi$, $k \in \mathbb{Z}$ then $\sin\varphi \ne 0$ and we define

$$\cot\varphi := \frac{\cos\varphi}{\sin\varphi}.$$

In this way we have defined cosine, sine, tangent, and cotangent for arbitrary angles.

Special Values

x in degrees	0°	30°	45°	60°	90°	120°	135°	150°	180°	270°	360°
x in radians	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\frac{2\pi}{3}$	$\frac{3\pi}{4}$	$\frac{5\pi}{6}$	π	$\frac{3\pi}{2}$	2π
$\sin x$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	0	-1	0
$\cos x$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{\sqrt{2}}{2}$	$-\frac{\sqrt{3}}{2}$	-1	0	1
$\tan x$	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	/	$-\sqrt{3}$	-1	$-\frac{\sqrt{3}}{3}$	0	/	0

Addition Formulas

We need the following two addition formulas for cosine and sine.

$$\begin{aligned} \cos(x+y) &= \cos x\cos y - \sin x\sin y, \\ \sin(x+y) &= \sin x\cos y + \cos x\sin y. \end{aligned} \tag{1.10}$$

The Pythagorean theorem in the trigonometric form reads as

$$\sin^2 x + \cos^2 x = 1. \tag{1.11}$$

1.2 Complex numbers

Some algebraic equations do not have solutions in the real number system. For instance the quadratic equation $x^2 - 4x + 8 = 0$ gives 'formally'

$$x_1 = 2 + \sqrt{-4} \quad \text{and} \quad x_2 = 2 - \sqrt{-4}.$$

We will see that one can work with this notation.

Definition 1.10 A *complex number* is an ordered pair (a, b) of real numbers. "Ordered" means that $(a, b) \neq (b, a)$ if $a \neq b$. Two complex numbers $x = (a, b)$ and $y = (c, d)$ are said to be equal if and only if $a = c$ and $b = d$. We define

$$\begin{aligned} x + y &:= (a + c, b + d), \\ xy &:= (ac - bd, ad + bc). \end{aligned}$$

Theorem 1.21 *These definitions turn the set of all complex numbers into a field, with* $(0, 0)$ *and* $(1, 0)$ *in the role of* 0 *and* 1.

Proof. We simply verify the field axioms as listed in Definition 1.5. Of course, we use the field structure of $\mathbb{R}$.
Let $x = (a, b)$, $y = (c, d)$, and $z = (e, f)$. (A1) is clear.
(A2) $x + y = (a + c, b + d) = (c + a, d + b) = y + x$.
(A3) $(x+y)+z = (a+c, b+d)+(e, f) = (a+c+e, b+d+f) = (a, b)+(c+e, d+f) = x+(y+z)$.
(A4) $x + 0 = (a, b) + (0, 0) = (a, b) = x$.
(A5) Put $-x := (-a, -b)$. Then $x + (-x) = (a, b) + (-a, -b) = (0, 0) = 0$.
(M1) is clear.
(M2) $xy = (ac - bd, ad + bc) = (ca - db, da + cb) = yx$.
(M3) $(xy)z = (ac - bd, ad + bc)(e, f) = (ace - bde - adf - bcf, acf - bdf + ade + bce) = (a, b)(ce - df, cf + de) = x(yz)$.
(M4) $x \cdot 1 = (a, b)(1, 0) = (a, b) = x$.
(M5) If $x \neq 0$ then $(a, b) \neq (0, 0)$, which means that at least one of the real numbers a, b is different from 0. Hence $a^2 + b^2 > 0$ and we can define

$$\frac{1}{x} := \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Then

$$x \cdot \frac{1}{x} = (a, b) \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right) = (1, 0) = 1.$$

(D)

$$\begin{aligned} x(y + z) &= (a, b)(c + e, d + f) = (ac + ae - bd - bf, ad + af + bc + be) \\ &= (ac - bd, ad + bc) + (ae - bf, af + be) \\ &= xy + yz. \end{aligned}$$

■

Remark 1.6 For any real numbers we have $(a,0)+(b,0)=(a+b,0)$ and $(a,0)(b,0)=(ab,0)$. This shows that the complex numbers $(a,0)$ have the same arithmetic properties as the corresponding real numbers a. We can therefore identify $(a,0)$ with a. This gives us the real field as a subfield of the complex field.
Note that we have defined the complex numbers without any reference to the mysterious square root of -1. We now show that the notation (a,b) is equivalent to the more customary $a+b\mathrm{i}$.

Definition 1.11 $\mathrm{i} := (0,1)$.

Proposition 1.22 (a) $\mathrm{i}^2=-1$. (b) *If* $a,b\in\mathbb{R}$ *then* $(a,b)=a+b\mathrm{i}$.

Proof. (a) $\mathrm{i}^2=(0,1)(0,1)=(-1,0)=-1$.
(b) $a+b\mathrm{i}=(a,0)+(b,0)(0,1)=(a,0)+(0,b)=(a,b)$. ■

Definition 1.12 If a,b are real and $z=a+b\mathrm{i}$, then the complex number $\overline{z}:=a-b\mathrm{i}$ is called the *conjugate* of z. The numbers a and b are the *real part* and the *imaginary part* of z, respectively. We shall write $a=\operatorname{Re} z$ and $b=\operatorname{Im} z$.

Proposition 1.23 *If z and w are complex, then*
(a) $\overline{z+w}=\overline{z}+\overline{w}$,
(b) $\overline{zw}=\overline{z}\cdot\overline{w}$,
(c) $z+\overline{z}=2\operatorname{Re} z$, $\quad z-\overline{z}=2\mathrm{i}\operatorname{Im} z$,
(d) $z\,\overline{z}$ *is positive real except when* $z=0$.

Proof. (a), (b), and (c) are quite trivial. To prove (d) write $z=a+b\mathrm{i}$ and note that $z\,\overline{z}=a^2+b^2$. ■

Definition 1.13 If z is complex number, its *absolute value* $|\,z\,|$ is the (nonnegative) root of $z\,\overline{z}$; that is $|\,z\,|:=\sqrt{z\,\overline{z}}$.

The existence (and uniqueness) of $|\,x\,|$ follows from Proposition 1.23 (d). Note that when x is real, then $x=\overline{x}$, hence $|\,x\,|=\sqrt{x^2}$. Thus $|\,x\,|=x$ if $x>0$ and $|\,x\,|=-x$ if $x<0$. We have recovered the definition of the absolute value for real numbers, see Subsection 1.1.6.

Proposition 1.24 *Let z and w be complex numbers . Then*
(a) $|\,z\,|>0$ *unless* $z=0$,
(b) $|\,\overline{z}\,|=|\,z\,|$,
(c) $|\,zw\,|=|\,z\,|\,|\,w\,|$,
(d) $|\operatorname{Re} z\,|\le|\,z\,|$,
(e) $|\,z+w\,|\le|\,z\,|+|\,w\,|$.

Proof. (a) and (b) are trivial. Put $z = a + b\mathrm{i}$ and $w = c + d\mathrm{i}$, with a, b, c, d real. Then

$$|\,zw\,|^2 = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = |\,z\,|^2\ |\,w\,|^2$$

or $|\,zw\,|^2 = (|\,z\,|\ |\,w\,|)^2$. Now (c) follows from the uniqueness assertion for roots.
To prove (d), note that $a^2 \le a^2 + b^2$, hence

$$|\,a\,| = \sqrt{a^2} \le \sqrt{a^2 + b^2} = |\,z\,|\,.$$

To prove (e), note that $\overline{z}\,w$ is the conjugate of $z\,\overline{w}$, so that $z\,\overline{w} + \overline{z}w = 2\,\mathrm{Re}\,(z\,\overline{w})$. Hence

$$\begin{aligned} |\,z + w\,|^2 &= (z + w)(\overline{z} + \overline{w}) = z\,\overline{z} + z\,\overline{w} + \overline{z}\,w + w\,\overline{w} \\ &= |\,z\,|^2 + 2\,\mathrm{Re}\,(z\,\overline{w}) + |\,w\,|^2 \\ &\le |\,z\,|^2 + 2\,|\,z\,|\ |\,w\,| + |\,w\,|^2 = (|\,z\,| + |\,w\,|)^2. \end{aligned}$$

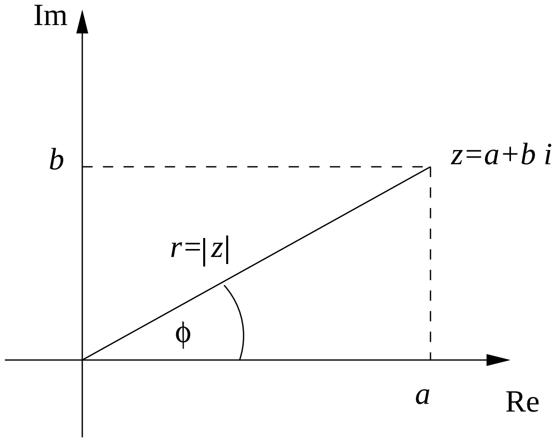
Now (e) follows by taking square roots. ∎

Q 12. If $z\,\overline{z} = 1$ compute $|\,1 + z\,|^2 + |\,1 - z\,|^2$.
Q 13. If $z_1, \dots, z_n$ are complex, prove that

$$|\,z_1 + z_2 + \cdots + z_n\,| \le |\,z_1\,| + \cdots + |\,z_n\,|\,.$$

1.2.1 The Complex Plane and the Polar form

There is a bijective correspondence between complex numbers and the points of a plane.



By the Pythagorean theorem it is clear that $|\,z\,| = \sqrt{a^2 + b^2}$ is exactly the distance of z from the origin 0. The angle φ between the positive real axis and the half-line $0z$ is called the *argument* of z and is denoted by $\varphi = \arg z$. If $z \ne 0$, the argument φ is uniquely determined up to integer multiples of 2π

Elementary trigonometry gives

$$\sin\varphi = \frac{b}{|\,z\,|}, \quad \cos\varphi = \frac{a}{|\,z\,|}.$$

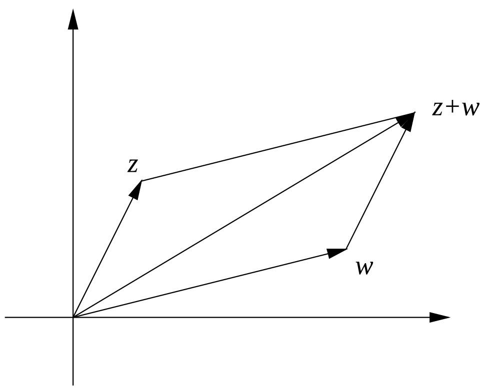
This gives with $r = |\,z\,|$, $a = r\cos\varphi$ and $b = r\sin\varphi$. Inserting these into the rectangular form of z yields

$$z = r(\cos\varphi + \mathrm{i}\sin\varphi), \tag{1.12}$$

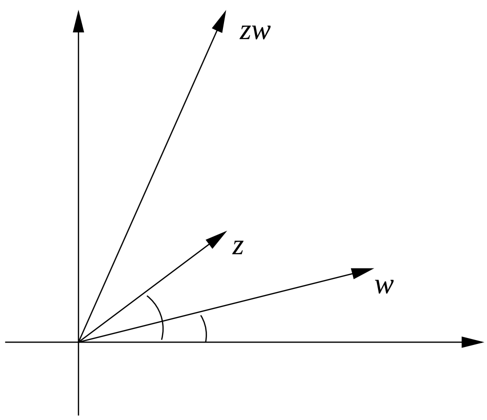
which is called the *polar form* of the complex number z.

Example 1.6 a) $z = 1 + \mathrm{i}$. Then $|z| = \sqrt{2}$ and $\sin\varphi = 1/\sqrt{2} = \cos\varphi$. This implies $\varphi = \pi/4$. Hence, the polar form of z is $1 + i = \sqrt{2}(\cos\pi/4 + \mathrm{i}\sin\pi/4)$.
b) $z = -\mathrm{i}$. We have $|-\mathrm{i}| = 1$ and $\sin\varphi = -1$, $\cos\varphi = 0$. Hence $\varphi = 3\pi/2$ and $-\mathrm{i} = 1(\cos 3\pi/2 + \mathrm{i}\sin 3\pi/2)$.
c) Computing the rectangular form of z from the polar form is easier.

$$z = 32(\cos 7\pi/6 + \mathrm{i}\sin 7\pi/6) = 32(-\sqrt{3}/2 - \mathrm{i}/2) = -16\sqrt{3} - 16\mathrm{i}.$$



The addition of complex numbers corresponds to the addition of vectors in the plane. The geometric meaning of the inequality $|z + w| \le |z| + |w|$ is: the sum of two edges of a triangle is bigger than the third edge.



Multiplying complex numbers $z = r(\cos\varphi + \mathrm{i}\sin\varphi)$ and $w = s(\cos\psi + \mathrm{i}\sin\psi)$ in the polar form gives

$$\begin{aligned} zw &= rs(\cos\varphi + \mathrm{i}\sin\varphi)(\cos\psi + \mathrm{i}\sin\psi) \\ &= rs(\cos\varphi\cos\psi - \sin\varphi\sin\psi) + \\ &\qquad \mathrm{i}(\cos\varphi\sin\psi + \sin\varphi\cos\psi) \\ zw &= rs(\cos(\varphi+\psi) + \mathrm{i}\sin(\varphi+\psi)), \end{aligned} \tag{1.13}$$

where we made use of the addition laws for sin and cos in the last equation.

Hence, the product of complex numbers is formed by taking the product of their absolute values and the sum of their arguments.
The geometric meaning of multiplication by w is a similarity transformation of $\mathbb{C}$. More precisely, we have a rotation around 0 by the angle ψ and then a dilatation with factor s and center 0.
Similarly, if $w \neq 0$ we have

$$\frac{z}{w} = \frac{r}{s}\left(\cos(\varphi - \psi) + \mathrm{i}\sin(\varphi - \psi)\right). \tag{1.14}$$

Proposition 1.25 (De Moivre's formula) *Let $z = r(\cos\varphi + \mathrm{i}\sin\varphi)$ be a complex number with absolute value r and argument φ. Then for all $n \in \mathbb{Z}$ one has*

$$z^n = r^n(\cos(n\varphi) + \mathrm{i}\sin(n\varphi)). \tag{1.15}$$

Proof. (a) First let $n > 0$. We use induction over n to prove De Moivre's formula. For $n = 1$ there is nothing to prove. Suppose (1.15) is true for some fixed n. We will show that the assertion is true for $n + 1$. Using induction hypothesis and (1.13) we find

$$z^{n+1} = z^n \cdot z = r^n(\cos(n\varphi) + \mathrm{i}\sin(n\varphi))r(\cos\varphi + \mathrm{i}\sin\varphi) = r^{n+1}(\cos(n\varphi + \varphi) + \mathrm{i}\sin(n\varphi + \varphi)).$$

This proves the induction assertion.
(b) If $n < 0$, then $z^n = 1/(z^{-n})$. Since $1 = 1(\cos 0 + \mathrm{i}\sin 0)$, (1.14) and the result of (a) gives

$$z^n = \frac{1}{z^{-n}} = \frac{1}{r^{-n}}\left(\cos(0-(-n)\varphi) + \mathrm{i}\sin(0-(-n)\varphi)\right) = r^n(\cos(n\varphi) + \mathrm{i}\sin(n\varphi)).$$

This completes the proof. ∎

Example 1.7 Compute the polar form of $z = \sqrt{3} - 3\mathrm{i}$ and compute z^{15}.
We have $|\,z\,| = \sqrt{3+9} = 2\sqrt{3}$, $\cos\varphi = 1/2$, and $\sin\varphi = -\sqrt{3}/2$. Therefore, $\varphi = -\pi/3$ and $z = 2\sqrt{3}(\cos(-\pi/3) + \sin(-\pi/3))$. By the De Moivre's formula we have

$$\begin{aligned} z^{15} &= (2\sqrt{3})^{15}\left(\cos\left(-15\frac{\pi}{3}\right) + \mathrm{i}\sin\left(-15\frac{\pi}{3}\right)\right) = 2^{15}3^7\sqrt{3}(\cos(-5\pi) + \mathrm{i}\sin(-5\pi)) \\ z^{15} &= -2^{15}3^7\sqrt{3}. \end{aligned}$$

1.2.2 Roots of Complex Numbers

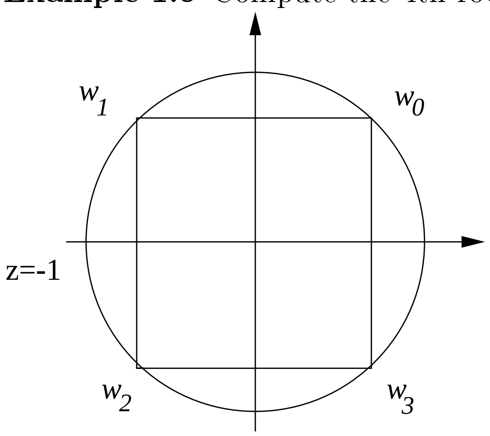
Let $z \in \mathbb{C}$ and $n \in \mathbb{N}$. A complex number w is called an *nth root of* z if $w^n = z$. In contrast to the real case, roots of complex numbers *are not unique*. We will see that there are exactly n different nth roots of z for every $z \neq 0$.
Let $z = r(\cos\varphi + \mathrm{i}\sin\varphi)$ and $w = s(\cos\psi + \mathrm{i}\sin\psi)$ an nth root of z. De Moivre's formula gives $w^n = s^n(\cos n\psi + \mathrm{i}\sin n\psi)$. If we compare w^n and z we get $s^n = r$ or $s = \sqrt[n]{r} \geq 0$. Moreover $n\psi = \varphi + 2k\pi$, $k \in \mathbb{Z}$ or $\psi = \dfrac{\varphi}{n} + \dfrac{2k\pi}{n}$, $k \in \mathbb{Z}$. For $k = 0, 1, \dots, n-1$ we obtain different values $\psi_0, \psi_1, \dots, \psi_{n-1}$ modulo 2π. We summarize.

Lemma 1.26 *Let $n \in \mathbb{N}$ and $z = r(\cos\varphi + \mathrm{i}\sin\varphi) \neq 0$ a complex number. Then the complex numbers*

$$w_k = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + \mathrm{i}\sin\frac{\varphi + 2k\pi}{n}\right), \quad k = 0, 1, \dots, n-1$$

are the n different nth roots of z.

Example 1.8 Compute the 4th roots of $z = -1$.



$|\,z\,| = 1 \Longrightarrow |\,w\,| = \sqrt[4]{1} = 1$, $\arg z = \varphi = 180^\circ$. Hence

$$\begin{aligned} \psi_0 &= \frac{\varphi}{4}, \\ \psi_1 &= \frac{\varphi}{4} + \frac{1 \cdot 360^\circ}{4} = 135^\circ, \\ \psi_2 &= \frac{\varphi}{4} + \frac{2 \cdot 360^\circ}{4} = 225^\circ, \\ \psi_3 &= \frac{\varphi}{4} + \frac{3 \cdot 360^\circ}{4} = 315^\circ. \end{aligned}$$

We obtain

$$\begin{aligned}
w_0 &= \cos 45^\circ + \mathrm{i}\sin 45^\circ &&= \frac{1}{2}\sqrt{2} + \mathrm{i}\frac{1}{2}\sqrt{2}\\
w_1 &= \cos 135^\circ + \mathrm{i}\sin 135^\circ &&= -\frac{1}{2}\sqrt{2} + \mathrm{i}\frac{1}{2}\sqrt{2},\\
w_2 &= \cos 225^\circ + \mathrm{i}\sin 225^\circ &&= -\frac{1}{2}\sqrt{2} - \mathrm{i}\frac{1}{2}\sqrt{2},\\
w_3 &= \cos 315^\circ + \mathrm{i}\sin 315^\circ &&= \frac{1}{2}\sqrt{2} - \mathrm{i}\frac{1}{2}\sqrt{2}.
\end{aligned}$$

Geometric interpretation of the nth roots. The nth roots of $z \neq 0$ form a regular n-gon in the complex plane with center 0. The vertices lie on a circle with center 0 and radius $\sqrt[n]{|\,z\,|}$.

1.3 Inequalities

1.3.1 The Arithmetic-Geometric mean inequality

Proposition 1.27 *Let $n \in \mathbb{N}$ and $x_1, \dots, x_n$ be in $\mathbb{R}_+$. Then*

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}. \tag{1.16}$$

We have equality if and only if $x_1 = x_2 = \cdots = x_n$.

Proof. We use forward-backward induction over n. First we show (1.16) is true for all n which are powers of 2. Then we prove that if (1.16) is true for some $n+1$, then it is true for n. Hence, it is true for all positive integers.
The inequality is true for $n = 1$. Let $a, b \geq 0$ then $(\sqrt{a} - \sqrt{b})^2 \geq 0$ implies $a + b \geq 2\sqrt{ab}$ and the inequality is true in case $n = 2$. Equality holds if and only if $a = b$. Suppose it is true for some fixed $k \in \mathbb{N}$; we will show that it is true for $2k$. Let $x_1, \dots, x_k, y_1, \dots, y_k \in \mathbb{R}_+$. Using induction assumption and the inequality in case $n = 2$, we have

$$\begin{aligned}
\frac{1}{2k}\left(\sum_{i=1}^k x_i + \sum_{i=1}^k y_i\right) &\geq \frac{1}{2}\left(\frac{1}{k}\sum_{i=1}^k x_i + \frac{1}{k}\sum_{i=1}^k y_i\right) \geq \frac{1}{2}\left(\left(\prod_{i=1}^k x_i\right)^{1/k} + \left(\prod_{i=1}^k y_i\right)^{1/k}\right)\\
&\geq \left(\prod_{i=1}^k x_i \prod_{i=1}^k y_i\right)^{\frac{1}{2k}}.
\end{aligned}$$

This completes the 'forward' part. Assume now (1.16) is true for $n+1$. We will show it for n. Let $x_1, \dots, x_n \in \mathbb{R}_+$ and set $A := (\sum_{i=1}^n x_i)/n$. By induction assumption we have

$$\begin{aligned}
\frac{1}{n+1}\left(x_1 + \cdots + x_n + A\right) \geq \left(\prod_{i=1}^n x_i A\right)^{\frac{1}{n+1}} &\iff \frac{1}{n+1}(nA + A) \geq \left(\prod_{i=1}^n x_i\right)^{\frac{1}{n+1}} A^{\frac{1}{n+1}}\\
A \geq \left(\prod_{i=1}^n x_i\right)^{\frac{1}{n+1}} A^{\frac{1}{n+1}} \iff A^{\frac{n}{n+1}} \geq \left(\prod_{i=1}^n x_i\right)^{\frac{1}{n+1}} &\iff A \geq \left(\prod_{i=1}^n x_i\right)^{1/n}.
\end{aligned}$$

It is trivial that in case $x_1 = x_2 = \cdots = x_n$ we have equality. Suppose that equality holds in a case where at least two of the x_i are different, say $x_1 < x_2$. Consider the inequality with the new set of values $x_1' := x_2' := (x_1 + x_2)/2$, and $x_i' = x_i$ for $i \geq 3$. Then

$$\left(\prod_{k=1}^{n} x_k\right)^{1/n} = \frac{1}{n}\sum_{k=1}^{n} x_k = \frac{1}{n}\sum_{k=1}^{n} x_k' \geq \left(\prod_{k=1}^{n} x_k'\right)^{1/n}.$$

$$x_1 x_2 \geq x_1' x_2' = \left(\frac{x_1 + x_2}{2}\right)^2 \iff 4x_1x_2 \geq x_1^2 + 2x_1x_2 + x_2^2 \iff 0 \geq (x_1 - x_2)^2.$$

This contradicts the choice $x_1 < x_2$. Hence, $x_1 = x_2 = \cdots = x_n$ is the only case where equality holds. This completes the proof. ∎

Now we extend Bernoulli's inequality to rational exponents.

Proposition 1.28 (Bernoulli's inequality) *Let $a \geq -1$ real and $r \in \mathbb{Q}$. Then*
(a) $(1 + a)^r \geq 1 + rx$ *if* $r \geq 1$,
(b) $(1 + a)^r \leq 1 + rx$ *if* $r \leq 1$.
Equality holds if and only if $a = 0$ or $r = 1$.

Proof. (b) Let $r = m/n$ with $m \leq n$, $m, n \in \mathbb{N}$. Apply (1.16) to $x_i := 1 + a$, $i = 1, \dots, m$ and $x_i := 1$ for $i = m + 1, \dots, n$. We obtain

$$\frac{1}{n}\left(m(1 + a) + (n - m)1\right) \geq \left((1 + a)^m \cdot 1^{n-m}\right)^{\frac{1}{n}}$$
$$\frac{m}{n}\, a + 1 \geq (1 + a)^{\frac{m}{n}},$$

which proves (b). Equality holds if $n = 1$ or if $x_1 = \cdots = x_n$ i. e. $a = 0$.
(a) Now let $s \geq 1$, $z \geq -1$. Setting $r = 1/s$ and $a := (1 + z)^{1/r} - 1$ we obtain $r \leq 1$ and $a \geq -1$. Inserting this into (b) yields

$$(1 + a)^r \leq \left((1 + z)^{\frac{1}{r}}\right)^r \leq 1 + r\left((1 + z)^s - 1\right)$$
$$z \leq r\left((1 + z)^s - 1\right)$$
$$1 + sz \leq (1 + z)^s.$$

This completes the proof of (a). ∎

Corollary 1.29 (Bernoulli's inequality) *Let $a \geq -1$ real and $x \in \mathbb{R}$. Then*
(a) $(1 + a)^x \geq 1 + xa$ *if* $x \geq 1$,
(b) $(1 + a)^x \leq 1 + xa$ *if* $x \leq 1$. *Equality holds if and only if $a = 0$ or $x = 1$.*

Proof. (a) First let $a > 0$. By Proposition 1.28 (a) $(1 + a)^r \geq 1 + ra$ if $r \in \mathbb{Q}$. Hence,

$$(1 + a)^x = \sup\{(1 + a)^r \mid r \in \mathbb{Q},\, r < x\} \geq \sup\{1 + ra \mid r \in \mathbb{Q},\, r < x\} = 1 + xa.$$

Now let $-1 \leq a < 0$. Then $r < x$ implies $ra > xa$, and Proposition 1.28 (a) implies

$$(1+a)^r \geq 1 + ra > 1 + xa. \tag{1.17}$$

By Definition 1.9

$$(1+a)^x = \frac{1}{\sup\{(1/(a+1))^r \mid r \in \mathbb{Q},\, r < x\}} \underset{\text{HW 2.1}}{=} \inf\{(1+a)^r \mid r \in \mathbb{Q},\, r < x\}.$$

Taking in (1.17) the infimum over all $r \in \mathbb{Q}$ with $r < x$ we obtain

$$(1+a)^x = \inf\{(1+a)^r \mid r \in \mathbb{Q},\, r < x\} \geq 1 + xa.$$

(b) The proof is analogous, so we omit it. ■

Proposition 1.30 (Young's inequality) *If $a, b \in \mathbb{R}_+$ and $p > 1$, then*

$$ab \leq \frac{1}{p}\, a^p + \frac{1}{q}\, b^q, \tag{1.18}$$

where $1/p + 1/q = 1$. Equality holds if and only if $a^p = b^q$.

Proof. First note that $1/q = 1 - 1/p$. We reformulate Bernoulli's inequality for $y \in \mathbb{R}_+$ and $p > 1$

$$y^p - 1 \geq p(y-1) \iff \frac{1}{p}(y^p - 1) + 1 \geq y \iff \frac{1}{p} y^p + \frac{1}{q} \geq y.$$

If $b = 0$ the statement is always true. If $b \neq 0$ insert $y := ab/b^q$ into the above inequality:

$$\begin{aligned} \frac{1}{p}\left(\frac{ab}{b^q}\right)^p + \frac{1}{q} &\geq \frac{ab}{b^q} \\ \frac{1}{p}\frac{a^p b^p}{b^{pq}} + \frac{1}{q} &\geq \frac{ab}{b^q} \qquad \mid \cdot b^q \\ \frac{1}{p} a^p + \frac{1}{q} b^q &\geq ab, \end{aligned}$$

since $b^{p+q} = b^{pq}$. We have equality if $y = 1$ or $p = 1$. The later is impossible by assumption. $y = 1$ is equivalent to $b^q = ab$ or $b^{q-1} = a$ or $b^{(q-1)p} = a^p$ $(b \neq 0)$. If $b = 0$ equality holds if and only if $a = 0$. ■

Proposition 1.31 (Hölder's inequality) *Let $p > 1$, $1/p + 1/q = 1$, and $x_1, \dots, x_n \in \mathbb{R}_+$ and $y_1, \dots, y_n \in \mathbb{R}_+$ non-negative real numbers. Then*

$$\sum_{k=1}^n x_k y_k \leq \left(\sum_{k=1}^n x_k^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^n y_k^q\right)^{\frac{1}{q}}. \tag{1.19}$$

We have equality if and only if there exists $c \in \mathbb{R}$ such that for all $k = 1, \dots, n$, $x_k^p / y_k^q = c$ (they are proportional).

Proof. Set $A := (\sum_{k=1}^n x_k^p)^{\frac{1}{p}}$ and $B := (\sum_{k=1}^n y_k^q)^{\frac{1}{q}}$. The cases $A = 0$ and $B = 0$ are trivial. So we assume $A, B > 0$. By Young's inequality we have

$$\begin{aligned}
\frac{x_k}{A} \cdot \frac{y_k}{B} &\leq \frac{1}{p}\,\frac{x_k^p}{A^p} + \frac{1}{q}\,\frac{y_k^q}{B^q} \\
\Longrightarrow \frac{1}{AB}\sum_{k=1}^n x_k y_k &\leq \frac{1}{pA^p}\sum_{k=1}^n x_k^p + \frac{1}{qB^q}\sum_{k=1}^n y_k^q \\
&= \frac{1}{p\sum x_k^p}\sum x_k^p + \frac{1}{q\sum y_k^q}\sum y_k^q \\
&= \frac{1}{p} + \frac{1}{q} = 1 \\
\Longrightarrow \sum_{k=1}^n x_k y_k &\leq \left(\sum_{k=1}^n x_k^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^n y_k^q\right)^{\frac{1}{q}}.
\end{aligned}$$

Equality holds if and only if $x_k^p/A^p = y_k^q/B^q$ for all $k = 1, \ldots, n$. Therefore, $x_k^p/y_k^q = \text{const}$. ■

Corollary 1.32 (Cauchy–Schwarz inequality) *In case $p = q = 2$ we have*

$$\sum_{k=1}^n x_k y_k \leq \sqrt{\sum_{k=1}^n x_k^2}\sqrt{\sum_{k=1}^n y_k^2}, \quad x_k, y_k \geq 0. \tag{1.20}$$

$$|\,\vec{x} \cdot \vec{y}\,| \leq \|x\|\,\|y\|$$

Corollary 1.33 (Complex Hölder's inequality) *Let $p > 1$, $1/p + 1/q = 1$ and $x_k, y_k \in \mathbb{C}$, $k = 1, \ldots, n$. Then*

$$\sum_{k=1}^n |\,x_k y_k\,| \leq \left(\sum_{k=1}^n |\,x_k\,|^p\right)^{\frac{1}{p}} \left(\sum_{k=1}^n |\,y_k\,|^q\right)^{\frac{1}{q}}.$$

Equality holds if and only if $|\,x_k\,|^p / |\,y_k\,|^q = \text{const.}$ for $k = 1, \ldots, n$.

Proof. Set $x_k := |\,x_k\,|$ and $y_k := |\,y_k\,|$ in (1.19). This will prove the statement. ■

Corollary 1.34 (Complex Cauchy–Schwarz inequality) *If $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ are complex numbers, then*

$$\left|\sum_{k=1}^n x_k \overline{y_k}\right|^2 \leq \sum_{k=1}^n |\,x_k\,|^2 \sum_{k=1}^n |\,y_k\,|^2. \tag{1.21}$$

Proof. Using the general triangle inequality, Proposition 1.24 (e) and the complex Hölder inequality we obtain

$$\left| \sum_{k=1}^{n} x_k \, \overline{y_k} \right| \leq \sum_{k=1}^{n} |\, x_k \,|\, |\, y_k \,| \leq \left(\sum_{k=1}^{n} |\, x_k \,|^2 \right)^{1/2} \left(\sum_{k=1}^{n} |\, y_k \,|^2 \right)^{1/2}.$$

This proves the statement. ∎

Proposition 1.35 (Minkowski's inequality) *If $x_1, \dots, x_n \in \mathbb{R}_+$ and $y_1, \dots, y_n \in \mathbb{R}_+$ and $p \geq 1$ then*

$$\left(\sum_{k=1}^{n} (x_k + y_k)^p \right)^{\frac{1}{p}} \leq \left(\sum_{k=1}^{n} x_k^p \right)^{\frac{1}{p}} + \left(\sum_{k=1}^{n} y_k^p \right)^{\frac{1}{p}}. \tag{1.22}$$

Equality holds if $p = 1$ or if $p > 1$ and $x_k / y_k = \mathrm{const}$.

Proof. The case $p = 1$ is obvious. Let $p > 1$. As before let $q > 0$ be the unique positive number with $1/p + 1/q = 1$. We compute

$$\begin{aligned} &\sum_{k=1}^{n} (x_k + y_k)^p = \sum_{k=1}^{n} (x_k + y_k)(x_k + y_k)^{p-1} = \sum_{k=1}^{n} x_k (x_k + y_k)^{p-1} + \sum_{k=1}^{n} y_k (x_k + y_k)^{p-1} \\ &\underset{(1.19)}{\leq} \left(\sum x_k^p \right)^{\frac{1}{p}} \left(\sum_k (x_k + y_k)^{(p-1)q} \right)^{\frac{1}{q}} + \left(\sum y_k^p \right)^{\frac{1}{p}} \left(\sum_k (x_k + y_k)^{(p-1)q} \right)^{\frac{1}{q}} \\ &\leq \left(\left(\sum x_k^p \right)^{1/p} + \left(\sum y_k^q \right)^{1/q} \right) \left(\sum (x_k + y_k)^p \right)^{1/q}. \end{aligned}$$

We can assume that $\sum (x_k + y_k)^p > 0$. Using $1 - \dfrac{1}{q} = \dfrac{1}{p}$ by taking the quotient of the last inequality by $\left(\sum (x_k + y_k)^p \right)^{1/q}$ we obtain the claim.
Equality holds if $x_k^p / (x_k + y_k)^{(p-1)q} = \mathrm{const.}$ and $y_k^p / (x_k + y_k)^{(p-1)q)} = \mathrm{const.}$; that is $x_k / y_k = \mathrm{const}$. ∎

Corollary 1.36 (Complex Minkowski's inequality) *If $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{C}$ and $p \geq 1$ then*

$$\left(\sum_{k=1}^{n} |\, x_k + y_k \,|^p \right)^{\frac{1}{p}} \leq \left(\sum_{k=1}^{n} |\, x_k \,|^p \right)^{\frac{1}{p}} + \left(\sum_{k=1}^{n} |\, y_k \,|^p \right)^{\frac{1}{p}}. \tag{1.23}$$

Equality holds if $p = 1$ or if $p > 1$ and $x_k / y_k = \lambda > 0$.

Proof. Using the triangle inequality gives $|\, x_k + y_k \,| \leq |\, x_k \,| + |\, y_k \,|$; hence $\sum_{k=1}^{n} |\, x_k + y_k \,|^p \leq \sum_{k=1}^{n} (|\, x_k \,| + |\, y_k \,|)^p$. The real version of Minkowski's inequality now proves the assertion. ∎

If $x = (x_1, \dots, x_n)$ is a vector in $\mathbb{R}^n$ or $\mathbb{C}^n$, the (non-negative) number

$$\|x\|_p := \left(\sum_{k=1}^{n} | x_k |^p \right)^{\frac{1}{p}}$$

is called the *p-norm* of the vector x. Minkowski's inequalitie then reads as

$$\|x + y\|_p \le \|x\|_p + \|y\|_p$$

which is the triangle inequality for the p-norm.

1.4 Appendix A: Powers with Real Exponents and Logarithms

Lemma 1.37 (a) *For $a, b > 0$ and $r \in \mathbb{Q}$ we have*

$$a < b \Longleftrightarrow a^r < b^r \quad \textit{if } r > 0,$$
$$a < b \Longleftrightarrow a^r > b^r \quad \textit{if } r < 0.$$

(b) *For $a > 0$ and $r, s \in \mathbb{Q}$ we have*

$$r < s \Longleftrightarrow a^r < a^s \quad \textit{if } a > 1,$$
$$r < s \Longleftrightarrow a^r > a^s \quad \textit{if } a < 1.$$

Proof. Suppose that $r > 0$, $r = m/n$ with integers $m, n \in \mathbb{Z}$, $n > 0$. Using Lemma 1.16 (a) twice we get

$$a < b \Longleftrightarrow a^m < b^m \Longleftrightarrow (a^m)^{\frac{1}{n}} < (b^m)^{\frac{1}{n}},$$

which proves the first claim. The second part $r < 0$ can be obtained by setting $-r$ in place of r in the first part and using Proposition 1.9 (e).
(b) Suppose that $s > r$. Put $x = s - r$, then $x \in \mathbb{Q}$ and $x > 0$. By (a), $1 < a$ implies $1 = 1^x < a^x$. Hence $1 < a^{s-r} = a^s/a^r$, and therefore $a^r < a^s$. If $s < r$, then $x = s - r < 0$ and, by (a), $1 < a$ implies $1 > a^x = a^s/a^r$. Hence, $a^r > a^s$. The proof for $a < 1$ is similar. ∎

Our aim is to define b^x for arbitrary *real* x.

Lemma 1.38 *Let b, p be real numbers with $b > 1$ and $p > 0$. Set*

$$M = \{b^r \mid r \in \mathbb{Q}, r < p\}, \quad M' = \{b^s \mid s \in \mathbb{Q}, p < s\}.$$

Then

$$\sup M = \inf M'.$$

Proof. (a) M is bounded above by arbitrary b^s, $s \in Q$, with $s > p$, and M' is bounded below by any b^r, $r \in \mathbb{Q}$, with $r < p$. Hence $\sup M$ and $\inf M'$ both exist.
(b) Since $r < p < s$ implies $a^r < b^s$ by Lemma 1.37, $\sup M \le b^s$ for all $b^s \in M'$. Taking the infimum over all such b^s, $\sup M \le \inf M'$.
(c) Let $s = \sup M$ and $\varepsilon > 0$ be given. We want to show that $\inf M' < s + \varepsilon$. Choose $n \in \mathbb{N}$ such that

$$1/n < \varepsilon/(s(b-1)). \tag{1.24}$$

By Proposition 1.11 there exist $r, s \in \mathbb{Q}$ with

$$r < p < s \quad \text{and} \quad s - r < \frac{1}{n}. \tag{1.25}$$

Using $s - r < 1/n$, Bernoulli's inequality (part 2), and (1.24), we compute

$$b^s - b^r = b^r(b^{s-r} - 1) \le s(b^{\frac{1}{n}} - 1) \le s\frac{1}{n}(b-1) < \varepsilon.$$

Hence

$$\inf M' \le b^s < b^r + \varepsilon \le \sup M + \varepsilon.$$

Since ε was arbitrary, $\inf M' \le \sup M$, and finally, with the result of (b), $\inf M' = \sup M$. ∎

Corollary 1.39 *Suppose $p \in \mathbb{Q}$ and $b > 1$ is real. Then*

$$b^p = \sup\{b^r \mid r \in \mathbb{Q}, r < p\}.$$

Proof. For all rational numbers $r, p, s \in \mathbb{Q}$, $r < p < s$ implies $a^r < a^p < a^s$. Hence $\sup M \le a^p \le \inf M'$. By the lemma, these three numbers coincide. ∎

1.4.1 Logarithms

Fix $b > 1$, $y > 0$. We can prove the existence of a unique real x such that $b^x = y$ by completing the following outline. This number x is called the *logarithm of y to the base b*, and we write $x = \log_b y$.
(a) It $t > 1$ and $n > (b-1)/(t-1)$, then $b^{1/n} < t$. (Use Bernoulli's inequality.)
(b) If w is such that $b^w < y$, then $b^{w+1/n} < y$ for sufficiently large n (apply (a) with $t = yb^{-w}$.)
(c) If $b^w > y$, then $b^{w-1/n} > y$ for sufficiently large n.
(d) Let $A := \{w \mid b^w < y\}$ and show that $x = \sup A$ satisfies $b^x = y$.
(e) Prove that this x is unique.

Lemma 1.40 *For any $a > 0$, $a \neq 1$ we have*
(a) $\log_a(bc) = \log_a b \log_a c$ *if* $b, c > 0$*;*
(b) $\log_a(b^c) = c \log_a b$*, if* $b > 0$*;*
(c) $\log_a b = \dfrac{\log_d b}{\log_d a}$ *if* $b, d > 0$ *and* $d \neq 1$*.*

Later we will give an alternative definition of the logarithm function and we will prove the properties (a), (b), and (c).