

R 1: Summary: Basic Techniques of Algebra

Last updated: 050819

• SETS AND SET OPERATIONS

1. *Set, Equality, Empty Set:* A set is a well-defined “collection” of distinct “objects”, which are called the *elements* of the set. A set S is well-defined if for each object x it can be decided whether it is an element of S denoted by $x \in S$ or whether it is not an element of S , denoted by $x \notin S$.

The unique set with no elements is called the *empty set* and denoted by the symbol \emptyset .

Two sets A and B are *equal* if they have the same elements, i.e. if for all x holds: $x \in A$ if and only if $x \in B$.

2. *Defining Sets:* A set S can be described in *tabular form* by listing its elements between “curly” parenthesis, for instance

$$S = \{1, 2, 3, 7\}$$

or in *descriptive form* by using its defining property P

$$S = \{x \mid x \text{ has property } P\}.$$

For example, $S = \{x \mid 1 \leq x < 2\}$ is the set of all (real) numbers that are greater than or equal to 1 and smaller than 2.

3. *Important Sets of Numbers:*
 - (a) $\mathbb{N} := \{1, 2, 3, \dots\}$ the set of all *natural numbers*.
 - (b) $\mathbb{N}^0 := \{0, 1, 2, 3, \dots\}$ the set of all *whole numbers*.
 - (c) $\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ the set of all *integers*.
 - (d) $\mathbb{Q} := \{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{N}\}$ the set of all *rational numbers* or *fractions*.
 - (e) \mathbb{R} the set of all *real numbers*.
 - (f) $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$ the set of all *complex numbers*.
4. *Intervals:* Let $a, b \in \mathbb{R}$, then
 - (a) $[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$.
 - (b) $(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$.

$$(c) [a, b) := \{x \in \mathbb{R} \mid a \leq x < b\}.$$

$$(d) (a, b] := \{x \in \mathbb{R} \mid a < x \leq b\}.$$

5. *Subsets:* A set A is called a *subset* of a set B , in symbols $A \subseteq B$, if each element of A is also an element of B , i.e. for all x holds: if $x \in A$ then $x \in B$.

6. *Example:*
 $\{1, 3, 5\} \subseteq \{1, 2, 3, 4, 5\}$.

7. *Operations:* Let A and B be two sets, then the sets

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

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

$$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}$$

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

are called the *intersection* of A and B , the *union* of A and B , the *difference* of A and B and the *Cartesian product* of A and B , respectively. The elements (a, b) of $A \times B$ are called *ordered pairs*. $A \setminus B$ is usually read as “ A without B ”.

8. *Example:*
Let $A := \{1, 2, 3, 4\}$ and $B := \{2, 5\}$ then

$$A \cap B = \{2\},$$

$$A \cup B = \{1, 2, 3, 4, 5\},$$

$$A \setminus B = \{1, 3, 4\},$$

$$A \times B = \{(1, 2), (2, 2), (3, 2), (4, 2), (1, 5), (2, 5), (3, 5), (4, 5)\}$$

and

$$B \times A = \{(2, 1), (2, 2), (2, 3), (2, 4),$$

$$(5, 1), (5, 2), (5, 3), (5, 4)\}$$

9. *Example:*
Let $A := (0, 1]$ and $B := [2, 6]$, then

$$A \times B = (0, 1] \times [2, 6]$$

$$= \{(x, y) \mid 0 < x \leq 1 \text{ and } 2 \leq y \leq 6\}$$

10. *Quantifiers:* Suppose S is a set and P a statement concerning the elements x of S , then it is often convenient to abbreviate the lengthy formulation “for all $x \in S$ the statement P is true” by the more compact symbolic expression

$$\forall x \in S : P.$$

Similarly, we will often replace the phrase “there exists (at least) one $x \in S$ for which the statement P is true” by the shorter expression

$$\exists x \in S : P.$$

11. Example:

Suppose A and B are sets then, by the definition of “ \subseteq ” and “ $\not\subseteq$ ”, we have

$$A \subseteq B \Leftrightarrow (\forall x \in A : x \in B)$$

$$A \not\subseteq B \Leftrightarrow (\exists x \in A : x \notin B)$$

12. Example:

The lengthy formulation of the “Archimidean Axiom”: “For each real number x there exists a natural number n which is greater than or equal to x ” can be shortened to

$$\forall x \in \mathbb{R} \exists n \in \mathbb{N} : n \geq x$$

• FUNCTIONS

1. *Function:* Suppose S and T are sets. A *function* or *map* from S into T is an association which assigns to every element of S precisely one element of T . Instead of saying “ f is a function from S into T ”, we shall often write symbolically $f : S \rightarrow T$.

If $f : S \rightarrow T$ is a function and $x \in S$ then we denote by $f(x)$ the unique element of T assigned to x by f and call it the *value* of f at x or the *image* of x under f .

If $f : S \rightarrow T$ is a function, then the set S is called the *domain* of f , the set T the *co-domain* of f , and the set

$$\text{im}(f) = f(S) = \{f(x) \mid x \in S\}$$

of all images of S under f the *image* of f or the *range* of f .

Moreover, if f is a function from S into T , we often write $x \mapsto f(x)$ to denote the association of $f(x)$ to x . Note that the arrow “ \rightarrow ” describes the global association between the sets S and T , while “ \mapsto ” describes the local association between the elements of S and T .

2. Example:

Let $S = T = \mathbb{R}$, and let $f : \mathbb{R} \rightarrow \mathbb{R}$ be the map defined by $f(x) := x^2$ for all $x \in \mathbb{R}$. We can also express this by saying that f is the map from \mathbb{R} into \mathbb{R} such that $x \mapsto x^2$ for all $x \in \mathbb{R}$. The image of f is the interval $[0, \infty)$.

3. *Injective Functions, One-to-one Functions:* A function $f : S \rightarrow T$ is called *injective* or *one-to-one* if for all $x_1, x_2 \in S$ whenever $x_1 \neq x_2$ then also $f(x_1) \neq f(x_2)$. Note this is equivalent to the statement

$$\forall x_1 x_2 \in S \left(f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \right).$$

4. Example:

The map $f(x) := x^2$ for all $x \in \mathbb{R}$ is *not* injective, since, for example $f(-1) = f(1)$. However, the map $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) := x + 1$ is injective, since $x_1 + 1 = x_2 + 1$ implies $x_1 = x_2$ for all $x_1, x_2 \in \mathbb{R}$.

5. *Surjective Functions, Onto Functions:* A map $f : S \rightarrow T$ is called *surjective* or *onto* if its image $f(S) = T$, i.e. if for any $y \in T$ there exists an $x \in S$ such that $f(x) = y$. Those elements $x \in S$ with $f(x) = y$ are called *inverse images* of y .

6. Example:

The map $f(x) := x^2$ for all $x \in \mathbb{R}$ is *not* surjective, since, for example -1 does not have an inverse image. However, the map $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) := x + 1$ is surjective, since for all $y \in \mathbb{R}$ we have $y = g(y - 1)$.

7. *Bijective Functions:* A map $f : S \rightarrow T$ is called *bijective* if it is both injective and surjective.

8. *Identity Function:* Let S be a nonempty set, then the map $\text{id} = \text{id}_S : S \rightarrow S$ defined by $x \mapsto x$ is called the *identity map* on S .

9. *Composition of Functions:* Suppose S, T and U are sets and $f : S \rightarrow T$ and $g : T \rightarrow U$ are maps. Then we define the *composition* $g \circ f : S \rightarrow U$ of f and g by

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

for all $x \in S$.

10. Example:

Consider again the maps $f, g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) := x^2$ and $g(x) := x + 1$ for all $x \in \mathbb{R}$. Then we can form both $g \circ f$ and $f \circ g$ and we obtain

$$g(f(x))(x) = g(x^2) = x^2 + 1,$$

while

$$f(g(x))(x) = f(x+1) = (x+1)^2$$

for all $x \in \mathbb{R}$. Hence, we see that in general

$$f \circ g \neq g \circ f.$$

11. *Invertible Functions, Inverse Function:* The map $f : S \rightarrow T$ is called *invertible* if there exists a map $g : T \rightarrow S$ such that

$$g \circ f = \text{id}_S \quad \text{and} \quad f \circ g = \text{id}_T, \quad (1)$$

or in other words

$$g(f(x)) = x \quad \forall x \in S \quad (2)$$

$$f(g(y)) = y \quad \forall y \in T \quad (3)$$

If f is invertible then there exists precisely one map g satisfying the equation (1). This map is called the *inverse* map of f and usually denoted by f^{-1} .

12. *Invertibility Criterion:* The function f is invertible if and only if f is injective.
13. *Example: Finding the Inverse:* Consider the function $f : \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R}$ defined by

$$f(x) := \frac{1}{x-1} \quad x \in \mathbb{R} \setminus \{1\}.$$

f is injective since

$$\begin{aligned} f(x_1) = f(x_2) &\Leftrightarrow \frac{1}{x_1-1} = \frac{1}{x_2-1} \\ &\Leftrightarrow x_1-1 = x_2-1 \\ &\Leftrightarrow x_1 = x_2 \end{aligned}$$

for all $x_1, x_2 \in \mathbb{R} \setminus \{1\}$. Therefore, f possesses an inverse function.

The image or range of f is

$$\begin{aligned} \text{im}(f) &= \{f(x) \mid x \in \mathbb{R} \setminus \{1\}\} \\ &= \left\{ \frac{1}{x-1} \mid x \in \mathbb{R} \setminus \{1\} \right\} \\ &= \mathbb{R} \setminus \{0\} \end{aligned}$$

In order to find the defining term for the inverse of f , we follow the procedure:

- Set $y = f(x) = \frac{1}{x-1}$
- Interchange the dependent and independent variable: $x \leftrightarrow y$: $x = \frac{1}{y-1}$.
- Solve for y : $y = 1 + \frac{1}{x}$.

Thus the inverse $f^{-1} : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{1\}$ of f is given by

$$f^{-1}(x) = 1 + \frac{1}{x}$$

for all $x \in \mathbb{R} \setminus \{0\}$.

• AXIOMATIC DESCRIPTION OF THE REAL NUMBER SYSTEM $(\mathbb{R}, +, \cdot, \leq)$

- $(\mathbb{R}, +)$ is a *commutative group*, i.e.
 - $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{R}$, (“+” is associative).
 - $0 + a = a + 0 = a$ for $a \in \mathbb{R}$, (0 is the neutral element with respect to “+”).
 - For each $a \in \mathbb{R}$ there exists a (unique) element $b \in \mathbb{R}$ such that $a + b = b + a = 0$. This unique element b is called the *additive inverse* of a and denoted by $-a$.
 - $a + b = b + a$ for all $a, b \in \mathbb{R}$, (commutative law).
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is a *commutative group*, i.e.
 - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{R} \setminus \{0\}$, (“ \cdot ” is associative).
 - $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{R} \setminus \{0\}$, (1 is the neutral element with respect to “ \cdot ”).
 - For each $a \in \mathbb{R} \setminus \{0\}$ there exists a unique element $b \in \mathbb{R} \setminus \{0\}$ such that $a \cdot b = b \cdot a = 1$. This unique element b is called the *multiplicative inverse* of a and denoted by a^{-1} or $\frac{1}{a}$.
 - $a \cdot b = b \cdot a$ for $a, b \in \mathbb{R} \setminus \{0\}$, (“ \cdot ” is commutative).
- Distributive Law:* $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{R}$, (“ \cdot ” is distributive over “+”).
- (\mathbb{R}, \leq) is a *linearly ordered set*, i.e.
 - $a \leq a$ for all $a \in \mathbb{R}$, (“ \leq ” is reflexive).
 - If $a \leq b$ and $b \leq a$ then $a = b$ for all $a, b \in \mathbb{R}$, (“ \leq ” is anti-symmetric).
 - If $a \leq b$ and $b \leq c$ then $a \leq c$ for all $a, b, c \in \mathbb{R}$, (“ \leq ” is transitive).
 - $a \leq b$ or $b \leq a$ for all $a, b \in \mathbb{R}$, (“ \leq ” is dichotomic).
- Monotony Laws:*
 - If $a \leq b$ and $c \in \mathbb{R}$ then $a + c \leq b + c$ for all $a, b \in \mathbb{R}$.
 - If $a \leq b$ and $c \in \mathbb{R}$ and $c > 0$ then $a \cdot c \leq b \cdot c$ for all $a, b \in \mathbb{R}$.

• SUBTRACTION, DIVISION, STRICT INEQUALITY

- For all $a, b, c \in \mathbb{R}$ with $c \neq 0$ we define $a - b := a + (-b)$ and $\frac{a}{c} := a \cdot c^{-1}$
- For $a, b \in \mathbb{R}$, we define $a < b$ to be equivalent to $a \leq b$ and $a \neq b$.

• CONSEQUENCES OF AXIOMS (1, 2,3)

1. If $a + c = b + c$ then $a = b$ for all $a, b, c \in \mathbb{R}$, (law of cancellation for addition).
2. If $a \cdot c = b \cdot c$ then $a = b$ for all $a, b, c \in \mathbb{R}$ with $c \neq 0$, (law of cancellation for multiplication).
3. $a \cdot 0 = 0$ for all $a \in \mathbb{R}$.
4. $-a = (-1) \cdot a$ for all $a \in \mathbb{R}$.
5. $a \cdot b = 0$ if and only if $a = 0$ or $b = 0$ for all $a, b \in \mathbb{R}$.
6. $-(a + b) = (-a) + (-b) = -a - b$ for all $a, b \in \mathbb{R}$.
7. $\frac{(-a)}{b} = \frac{a}{(-b)} = -\frac{a}{b}$ for all $a, b \in \mathbb{R}$ with $b \neq 0$.
8. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ for all $a, b \in \mathbb{R}$.
9. $(-a) \cdot (-b) = a \cdot b$ for all $a, b \in \mathbb{R}$.
10. $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}$ for all $a, b, c, d \in \mathbb{R}$ with $b, d \neq 0$.
11. $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ for all $a, b, c, d \in \mathbb{R}$ with $b, d \neq 0$.

• CONSEQUENCES OF AXIOM (4) Suppose $a, b, c, d \in \mathbb{R}$, then

1. If $a < b$ then $a + c < b + c$
2. If $a \leq b$ and $c \leq d$ then $a + c \leq b + d$
3. If $a < b$ and $c \leq d$ then $a + c < b + d$
4. If $a < b$ and $0 < c$ then $ac < bc$
5. If $0 \leq a \leq b$ and $0 \leq c \leq d$ then $ac \leq bd$
6. If $0 \leq a < b$ and $0 < c \leq d$ then $ac < bd$
7. If $a \leq b$ and $c < 0$ then $ac \geq bc$
8. If $a < b$ and $c < 0$ then $ac > bc$
9. If $0 < a$ then $0 < \frac{1}{a}$
10. If $0 < a < b$ then $0 < \frac{1}{b} < \frac{1}{a}$
11. $0 < 1$

• ABSOLUTE VALUE

1. For any $x \in \mathbb{R}$ the number

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

is called the *absolute value* of x .

2. If $x, y \in \mathbb{R}$, then
 - (a) $|x| \geq 0$ and $(|x| = 0 \Leftrightarrow x = 0)$
 - (b) $|xy| = |x||y|$
 - (c) $|x + y| \leq |x| + |y|$ (triangle inequality)
3. Suppose $x, a, \varepsilon \in \mathbb{R}$ and $\varepsilon > 0$, then
 - (a) $|x| < \varepsilon \Leftrightarrow -\varepsilon < x < \varepsilon$

(b) $|x - a| < \varepsilon \Leftrightarrow a - \varepsilon < x < a + \varepsilon$

- (c) The two previous statements remain true if “ $<$ ” is replaced by “ \leq ”.

• NATURAL NUMBERS

1. *Natural Numbers:* The set \mathbb{N} of *natural numbers* can be defined as the smallest “inductive” subset of \mathbb{R} , i.e. the smallest subset of \mathbb{R} with the following two properties

- (a) $1 \in \mathbb{N}$
- (b) If $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$.

2. *Mathematical Induction:* Suppose $n_0 \in \mathbb{N}$ and suppose that $\mathcal{A}(n)$ is statement involving the numbers $n \in \mathbb{N}$. Then $\mathcal{A}(n)$ is true for all $n \in \mathbb{N}$ with $n \geq n_0$ provided the following two conditions are satisfied;

- (a) $\mathcal{A}(n_0)$ is true
- (b) For all $n \in \mathbb{N}$ with $n \geq n_0$ holds:
If $\mathcal{A}(n)$ is true then also $\mathcal{A}(n + 1)$ is true.

Note that (ii) is a conditional statement, $\mathcal{A}(n) \Rightarrow \mathcal{A}(n + 1)$, while the claim is unconditional!

3. Example: *Gauss’ Summation Formula:*

For all $n \in \mathbb{N}$:

$$S_n := 1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$$

We establish this formula using mathematical induction. Here $n_0 = 1$. According to (2), we have to verify that the statement is true for $n = 1$ and under the assumption that it is true for a fixed $n \geq 1$ it is also true for $n + 1$.

$(n = 1)$: $S_1 = 1 = \frac{1(1+1)}{2}$.

$(n \rightarrow n + 1)$: Let $n \geq 1$ and suppose that $S_n = \frac{n(n+1)}{2}$. Show that $S_{n+1} = \frac{(n+1)(n+2)}{2}$.

$$\begin{aligned} S_{n+1} &= 1 + \dots + n + (n + 1) \\ &= S_n + (n + 1) = \frac{n(n + 1)}{2} + (n + 1) \\ &= \frac{n(n + 1) + 2(n + 1)}{2} \\ &= \frac{(n + 1)(n + 2)}{2}. \end{aligned}$$

4. *Factorial:* For all $n \in \mathbb{N}^0$, we define the number $n!$ (read: n factorial) recursively by

$$0! := 1 \quad \text{and} \quad (n + 1)! := n!(n + 1),$$

i.e.: $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n - 1) \cdot n$

5. Example:

$$3! = 1 \cdot 2 \cdot 3 = 6, \quad 4! = 3! \cdot 4 = 6 \cdot 4 = 24.$$

6. *Binomial Coefficients:* For all $a \in \mathbb{R}$ and $k \in \mathbb{N}^0$ we define the *Binomial coefficient* $\binom{a}{k}$ recursively by

$$\binom{a}{0} := 1 \quad \text{and} \quad \binom{a}{k+1} := \binom{a}{k} \frac{a-k}{k+1},$$

i.e. for $k > 0$

$$\binom{a}{k} = \frac{a}{1} \frac{(a-1)}{2} \frac{(a-2)}{3} \dots \frac{(a-k+1)}{k}$$

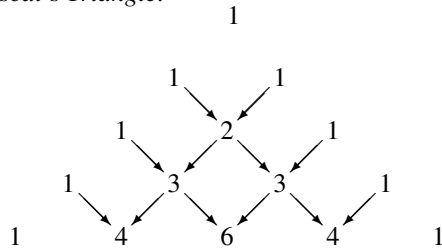
7. Example:

$$\begin{aligned} \binom{2}{0} &= 1 \\ \binom{2}{1} &= \frac{2}{1} = 2 \\ \binom{2}{2} &= \frac{2}{1} \frac{(2-1)}{2} = 1 \\ \binom{3}{0} &= 1 \\ \binom{3}{1} &= \frac{3}{1} = 3 \\ \binom{3}{2} &= \frac{3}{1} \frac{(3-1)}{2} = 3 \\ \binom{3}{3} &= \frac{3}{1} \frac{(3-1)}{2} \frac{(3-2)}{3} = 1 \end{aligned}$$

8. *Properties of the Binomial Coefficients:* Let $k, n \in \mathbb{N}^0$, then

- (a) $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, for $k \leq n$.
- (b) $\binom{n}{k} = \binom{n}{n-k}$, for $k \leq n$.
- (c) $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$, $k \leq n-1$.
- (d) $\binom{n}{k} = 0$, for $k > n$.

9. *Pascal's Triangle:*



The triangular arrangement of the binomial coefficients $\binom{n}{k}$ suggested by the recursion formula

8c allows a systematic computation of the binomial coefficients starting with $\binom{0}{0} = 1$. The coefficients $\binom{n}{0} = \binom{n}{n}$ ($n \in \mathbb{N}^0$) forming the sides of the triangle are all 1, while the coefficients in the interior are the sum of the two binomial coefficients directly above as indicated by the arrows in the diagram above.

• POWERS AND RADICALS

1. *Integer Exponents:* For $a \in \mathbb{R}$ and $n \in \mathbb{N}^0$ we define the *power* a^n recursively by

$$a^0 := 1 \quad \text{and} \quad a^{n+1} := a^n \cdot a,$$

i.e. if $n > 0$, we have

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ times}}$$

If $a \in \mathbb{R} \setminus \{0\}$ and $n \in \mathbb{N}$, then we define

$$a^{-n} := (a^{-1})^n = (a^n)^{-1}.$$

The number a is called the *base*, while the number n is called the *exponent* of the power.

2. Example:

$$\begin{aligned} 5^3 &= 5 \cdot 5 \cdot 5 = 125 \\ 5^{-3} &= \frac{1}{5} \cdot \frac{1}{5} \cdot \frac{1}{5} \\ &= \frac{1}{5 \cdot 5 \cdot 5} = \frac{1}{125} \end{aligned}$$

3. *Roots:* For any $n \in \mathbb{N}$ and any positive $a \in \mathbb{R}$ there exists precisely one positive $r \in \mathbb{R}$ such that

$$r^n = a.$$

This unique number r is called the *principal n -th root* of a and denoted by

$$\sqrt[n]{a} := a^{\frac{1}{n}} := r.$$

If $n \in \mathbb{N}$ is odd, we define $\sqrt[n]{-a} := -\sqrt[n]{a}$. The symbol $\sqrt[n]{a}$ is called a *radical symbol*, the number n the *index* of the radical and the number a the *radicant*.

For any $n \in \mathbb{N}$ and any complex number $z = r(\cos \theta + i \sin \theta) \in \mathbb{C}$, $z \neq 0$, there exist precisely n numbers ω_k ($k = 0, 1, \dots, n-1$) such that

$$\omega_k^n = z \quad k = 0, 1, \dots, n-1,$$

namely,

$$\omega_k = r^{\frac{1}{n}} \left(\cos\left(\frac{\theta}{n} + \frac{2\pi k}{n}\right) + i \sin\left(\frac{\theta}{n} + \frac{2\pi k}{n}\right) \right) \quad (4)$$

$$= r^{\frac{1}{n}} e^{i \frac{\theta + 2\pi k}{n}} \quad (5)$$

for $k = 0, 1, \dots, n - 1$. The numbers ω_k are called n -th roots of z . If $z = 1$, they are called n -th roots of unity.

4. **Example:** The 4-th roots of $-8i$.

We would like to determine the fourth roots of the complex number $-8i$.

First note that the argument of $-8i$ is $3\pi/2$ and $|-8i| = 8$. Thus

$$-8i = 8 \left(\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2} \right).$$

Hence, by (4), the four fourth roots of $-8i$ are given by

$$w_k = 8^{1/4} \left[\cos \frac{1}{4} \left(\frac{3\pi}{2} + 2k\pi \right) + i \sin \frac{1}{4} \left(\frac{3\pi}{2} + 2k\pi \right) \right]$$

for $k = 0, 1, 2, 3$, or explicitly

$$w_0 = 8^{1/4} \left[\cos \frac{3\pi}{8} + i \sin \frac{3\pi}{8} \right]$$

$$w_1 = 8^{1/4} \left[\cos \frac{7\pi}{8} + i \sin \frac{7\pi}{8} \right]$$

$$w_2 = 8^{1/4} \left[\cos \frac{11\pi}{8} + i \sin \frac{11\pi}{8} \right]$$

$$w_3 = 8^{1/4} \left[\cos \frac{15\pi}{8} + i \sin \frac{15\pi}{8} \right]$$

5. **Rational Exponents:** For any positive real number $a \in \mathbb{R}$ and any rational number $\frac{n}{m} \in \mathbb{Q}$, we define

$$a^{\frac{n}{m}} := \sqrt[m]{a^n}.$$

6. **Example:**

$$8^{-\frac{2}{3}} = 8^{\frac{-2}{3}} = \sqrt[3]{8^{-2}} = \sqrt[3]{\frac{1}{8^2}} = \sqrt[3]{\frac{1}{64}} = \frac{1}{4}.$$

7. **Real Exponents:** For any positive real number $a \in \mathbb{R}$ and any real number $r \in \mathbb{R}$, we define

$$a^r := e^{r \ln a}.$$

8. **Example:**

$$\sqrt{3}^{\sqrt{2}} = e^{\sqrt{2} \ln(\sqrt{3})}.$$

9. **Properties of Exponents:** Let $a, b \in \mathbb{R}$ and $r, s \in \mathbb{R}$, then

(a) $a^r \cdot a^s = a^{r+s}$

(b) $\frac{a^r}{a^s} = a^{r-s} = \frac{1}{a^{s-r}}$

(c) $a^r \cdot b^r = (a \cdot b)^r$

(d) $\frac{a^r}{b^r} = \left(\frac{a}{b} \right)^r, \quad b \neq 0$

(e) $(a^r)^s = a^{rs}$

(f) For all $n \in \mathbb{Z}$ we have

$$(-1)^n = \begin{cases} 1, & \text{if } n \text{ is even} \\ -1, & \text{if } n \text{ is odd} \end{cases}$$

10. **Properties of Radicals:** Let $a, b \in \mathbb{R}, a, b > 0$ and $n, m \in \mathbb{N}$, then

(a) $\sqrt[n]{1} = 1, \quad \sqrt[n]{0} = 0$

(b) $\sqrt[n]{a^n} = \left(\sqrt[m]{a} \right)^n = a^{\frac{n}{m}}$

(c) $\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{a \cdot b}$

(d) $\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = \sqrt[n]{\frac{a}{b}}$

(e) $\sqrt[n]{\sqrt[m]{a}} = \sqrt[m]{\sqrt[n]{a}} = \sqrt[nm]{a}$

(f) $\left(\sqrt[n]{a} \right)^n = a$

(g) $\sqrt[n]{a^n} = \begin{cases} |a| & \text{if } n \text{ is even} \\ a & \text{if } n \text{ is odd} \end{cases}$

11. **Binomial Formulas:** For all $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$, we have

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

in particular

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

• **POLYNOMIALS, FACTORIZATION, ETC.**

1. **Polynomial;** An expression of the form

$$\begin{aligned} p(x) &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n \\ &= \sum_{k=0}^n a_kx^k, \end{aligned}$$

is called a *polynomial*. The numbers a_k ($k = 0, 1, \dots, n$) are called the *coefficients* of p , a_0 the absolute term, a_n the *leading coefficient* and n the *degree* of p , denoted by $\deg(p)$, provided $a_n \neq 0$. p is called a *monic polynomial* if the leading coefficient $a_n = 1$. The symbol x is called an *indeterminant*. Polynomials of degree 0, 1, 2, 3 are called *constant, linear, quadratic* and *cubic* polynomials, respectively.

Let p be a polynomial. To emphasize that all the coefficients of p are integers, rational numbers, real numbers or complex numbers, we say that p is a *polynomial over* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or \mathbb{C} , respectively.

2. **Example:**

$p_1(x) = 1 - x$ is a linear polynomial (also called a linear function), $p_2(x) = 4 - 8x - \frac{1}{2}x^2$ is a quadratic polynomial, and $p_3(x) = -\sqrt{2} + x^3 + x^8$ is a polynomial of degree 8. p_1 is a polynomial over \mathbb{Z} , p_2 is a polynomial over \mathbb{Q} , p_3 is a monic polynomial over \mathbb{R} .

3. *Division Algorithm:* If p and d are polynomials with $d \neq 0$ then there exist unique polynomials q and r such that

$$p = dq + r$$

where either $r = 0$ or $\deg(r) < \deg(d)$.

4. In the situation of 3, the polynomial p is called *dividend*, d the *divisor*, q the *quotient* and r the *remainder*.

If $r = 0$, we say that the polynomial d *divides* the polynomial p and we write $d \mid p$.

5. *Example: Long Division*

We divide the polynomial $p(x) = 2x^4 + 4x^3 - 5x^2 + 3x - 2$ by the polynomial $d(x) = x^2 + 2x - 3$ using the procedure called *long division*:

$$\begin{array}{r} \overline{) 2x^4 + 4x^3 - 5x^2 + 3x - 2} \\ \underline{2x^4 + 4x^3 - 6x^2} \\ - x^2 + 3x - 2 \\ \underline{ - x^2 + 2x - 3} \\ x + 1 \end{array}$$

We obtain

$$\begin{aligned} & \overbrace{2x^4 + 4x^3 - 5x^2 + 3x - 2}^{p(x)} = \\ & = \underbrace{(x^2 + 2x - 3)}_{d(x)} \underbrace{(2x^2 + 1)}_{q(x)} + \underbrace{x + 1}_{r(x)} \end{aligned}$$

6. *Example: Long Division*

We divide the polynomial $p(x) = 6x^3 - 19x^2 + 16x - 7$ by the polynomial $d(x) = x - 2$ using long division:

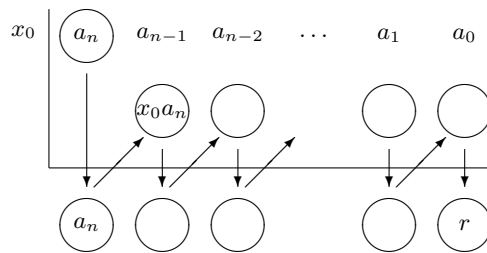
$$\begin{array}{r} \overline{) 6x^3 - 19x^2 + 16x - 7} \\ \underline{6x^3 - 12x^2} \\ - 7x^2 + 16x \\ \underline{- 7x^2 + 14x} \\ 2x - 7 \\ \underline{ 2x - 4} \\ - 3 \end{array}$$

Thus

$$\begin{aligned} & \overbrace{6x^3 - 19x^2 + 16x - 7}^{p(x)} = \\ & = \underbrace{(x - 2)}_{d(x)} \underbrace{(6x^2 - 7x + 2)}_{q(x)} + \underbrace{(-3)}_{r(x)} \end{aligned}$$

Since $\deg(x - 2) = 1$ and $\deg r < 1$, the remainder has to be a constant polynomial. Moreover, since $d(2) = 0$, the value of p at 2 is $p(2) = -3$.

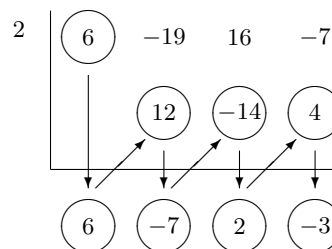
7. *Synthetic Division:* If the divisor is a linear factor of the form $x - x_0$, then long division can be shortened to a procedure called *synthetic division* illustrated below: Let $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ and $d(x) = x - x_0$,



The vertical arrows represent addition of the column elements above the horizontal line, the diagonal arrows multiplication by x_0 . After completion of the algorithm, the entries in the bottom row of the diagram starting with a_n are the coefficients of the quotient polynomial, the right most entry is the remainder r which coincides with the function value of p at x_0 .

8. *Example:*

We divide the polynomial $p(x) = 6x^3 - 19x^2 + 16x - 7$ by the polynomial $d(x) = x - 2$ using synthetic division:



Again, we obtain

$$\begin{aligned} & \overbrace{6x^3 - 19x^2 + 16x - 7}^{p(x)} = \\ & = \underbrace{(x - 2)}_{d(x)} \underbrace{(6x^2 - 7x + 2)}_{q(x)} + \underbrace{(-3)}_{r(x)} \end{aligned}$$

Note that the numbers in the bottom row of the synthetic division diagram are the coefficients of the quotient polynomial in descending order, the right most coefficient is the remainder which equals the value of the polynomial p at $x_0 = -3$.

9. *Zeros:*

10. Suppose $\alpha \in \mathbb{C}$. Then the following three statements are equivalent:

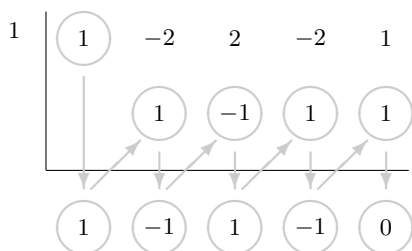
- (a) $p(\alpha) = 0$, i.e. α is a zero of p ;
- (b) $(x - \alpha) \mid p$, i.e. $(x - \alpha)$ divides p ;
- (c) $p(x) = (x - \alpha)q(x)$ for some polynomial q .

11. Example:

Consider the polynomial

$$p(x) = x^4 - 2x^3 + 2x^2 - 2x + 1.$$

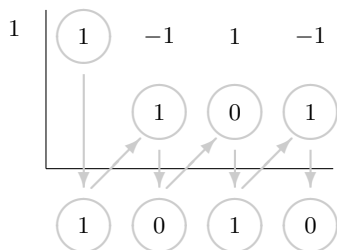
Since $p(1) = 0$, as can be easily verified by inspection, $\alpha_1 = 1$ is a zero of p . We divide p by the linear polynomial $x - \alpha_1 = x - 1$ using synthetic division:



Let $q_0(x) := x^3 - x^2 + x - 1$ denote the quotient polynomial. Note that its coefficients are given by the entries of the last row in the table above. Then

$$p(x) = (x - 1)q_0(x).$$

Clearly, $q_0(1) = 0$. We divide q_0 by $(x - 1)$ using synthetic division:



Let $q_1(x) := x^2 + 1$ denote the quotient polynomial. Again its coefficients can be read of the last row of the synthetic division table. Hence

$$q_0(x) = (x - 1)q_1(x)$$

and thus

$$\begin{aligned} p(x) &= (x - 1)q_0(x) = (x - 1)(x - 1)q_1(x) \\ &= (x - 1)^2(x^2 + 1) = (x - 1)^2(x - i)(x + i). \end{aligned}$$

12. **Multiplicity of a Zero:** If the polynomial p is divisible by $(x - \alpha)^k$ but not by $(x - \alpha)^{k+1}$, where $k \in \mathbb{N}$, then α is called a zero of *multiplicity* k of p .

13. Example:

1 is a zero of multiplicity 2, i and $-i$ are zeroes of multiplicity 1 of the polynomial $p(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$ in the previous example.

14. **Fundamental Theorem of Algebra:** Every non-constant polynomial has at least one zero.

15. **Linear Factorization Theorem:** Every polynomial p of degree $n > 0$ has precisely n zeroes. I.e. there exist numbers $\alpha_1, \alpha_1, \dots, \alpha_n \in \mathbb{C}$ such that

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $a_n \in \mathbb{C}$ is the leading coefficient of p .

16. **Quadratic Formula:** Suppose that $p(x) = ax^2 + bx + c$ is a quadratic polynomial. Then its zeroes are given by the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

17. **Rational Zero Test:** Suppose $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is an integral polynomial, i.e. all coefficients $a_k \in \mathbb{Z}$ are integers and suppose that $\alpha = r/s \in \mathbb{Q}$ is a rational zero of p . Then

$$r \mid a_0 \quad \text{and} \quad s \mid a_n.$$

18. **Variation in Sign:** Suppose $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a real polynomial, i.e. $a_k \in \mathbb{R}$. We say that p has a *variation in sign* if there exists an index $k \in \{0, 1, \dots, n - 1\}$ such that $a_k \cdot a_{k+1} < 0$.

19. Example:

The polynomial $p(x) = 3x^3 - 5x^2 + 6x - 4$ has 3 variations in sign:

$$3 \cdot (-5) < 0, \quad (-5) \cdot 6 < 0, \quad 6 \cdot (-4) < 0.$$

20. **Descartes' Rule of Signs:** Suppose $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a real polynomial, i.e. $a_k \in \mathbb{R}$ with $a_0 \neq 0$. Then the number of positive zeroes of p equals the number of variations in sign of $p(x)$ possible reduced by an even number. Moreover, the number of negative zeroes of p coincides with the number of variations in sign of $p(-x)$ possible reduced by an even number.

21. **Upper and Lower Bound Rule:** Suppose $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a real polynomial, i.e. $a_k \in \mathbb{R}$ and suppose the leading coefficient a_n is positive. Moreover, suppose that p is divided by $(x - c)$ using synthetic division. with last row $c_n = a_n, c_{n-1}, \dots, c_0 = r$. If $c > 0$ and $c_k \geq 0$ for $k = 0, \dots, n$, then c is

an upper bound for the real zeroes of p . If $c < 0$ and the c_k have alternating signs (zero entries count as positive or negative!), then c is a lower bound for the real zeroes of p .

22. Example:
Find the real zeroes of the polynomial

$$p(x) = 6x^3 - 4x^2 + 3x - 2.$$

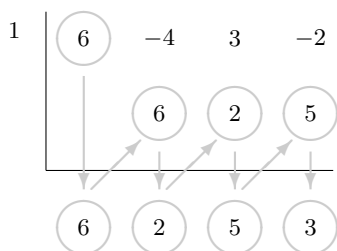
SOLUTION: By the Fundamental Theorem of Algebra, p has precisely 3 zeroes. We first consider the rational zeroes of p if it has any. By the Rational Zero Test, the set Z of rational zeroes of p is contained in the set

$$\begin{aligned} Z &\subseteq \left\{ \frac{s}{t} \mid s \mid (-2) \text{ and } t \mid 6 \right\} \\ &= \left\{ \pm 1, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{1}{6}, \pm \frac{2}{3}, \pm 2 \right\}. \end{aligned}$$

Because p has three variations in sign and $p(-x) = -6x^3 - 4x^2 - 3x - 2$ has none, we can conclude with Descartes' Rule of Signs that p has no negative zeroes and either 3 positive zeroes, or 1 positive zero (and a pair of conjugate complex zeroes). Hence

$$Z \subseteq \left\{ 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{6}, \frac{2}{3}, 2 \right\}.$$

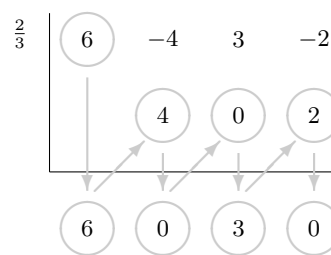
Trying $x = 1$ yields employing synthetic division



Since the remainder $r = 3$ in the last row of the table, we see that $x = 1$ is not a zero of p . However, since the last row consists only of non-negative entries, we know from the Upper and Lower Bound Rule that 1 is an upper bound for the zeroes of p . Hence

$$Z \subseteq \left\{ \frac{1}{2}, \frac{1}{3}, \frac{1}{6}, \frac{2}{3} \right\}.$$

By inspection, we find that $x = \frac{2}{3}$ is a zero of p :



Hence $p(x) = (x - \frac{2}{3})(6x^2 + 3)$. Since $6x^2 + 3$ has no real zeroes, $x = \frac{2}{3}$ is the only real zero of p . \triangleleft

23. *Complex Zeroes Occur in Conjugate Pairs:* Suppose $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ is a real polynomial, i.e. $a_k \in \mathbb{R}$, and suppose that $z = a + bi \in \mathbb{C}$ is a zero of p . Then the conjugate $\bar{z} = a - bi$ is also a zero of p .
24. Example:
Consider the real polynomial $p(x) = x^2 + 1$. Clearly, both i and its conjugate $\bar{i} = -i$ are zeroes of p . Moreover, $(x - i)(x + i) = x^2 + 1 = p(x)$.
25. *The Product of Conjugated Linear Factors is a Real Polynomial:* Let $a + bi \in \mathbb{C}$. Then

$$\begin{aligned} p(x) &= (x - (a + bi))(x - (a - bi)) \\ &= ((x - a) - bi)((x - a) + bi) \\ &= (x - a)^2 - (bi)^2 \\ &= x^2 - 2ax + a^2 + b^2 \end{aligned}$$

is clearly a real quadratic polynomial.

26. *Factorization Theorem:* Every real polynomial has a unique decomposition into a product of real linear factors and real quadratic polynomials that are "irreducible" over \mathbb{R} (i.e. that cannot be written as a product of real linear factors).
27. *Basic Factorization Formulae:*
- (a) $x^2 + 2ax + a^2 = (x + a)^2$
 - (b) $x^2 + (a + b)x + ab = (x + a)(x + b)$
 - (c) $a_1 a_2 x^2 + (a_1 b_2 + a_2 b_1)x + b_1 b_2 = (a_1 x + b_1)(a_2 x + b_2)$
 - (d) $x^2 - a^2 = (x - a)(x + a)$
 - (e) $x^3 - a^3 = (x - a)(x^2 + ax + a^2)$
 - (f) $x^4 - a^4 = (x - a)(x^3 + ax^2 + a^2x + a^3)$
 - (g) $x^3 + a^3 = (x + a)(x^2 - ax + a^2)$
 - (h) $x^5 + a^5 = (x + a)(x^4 - ax^3 + a^2x^2 - a^3x + a^4)$
 - (i) $x^7 + a^7 = (x + a)(x^6 - ax^5 + a^2x^4 - a^3x^3 + a^4x^2 - a^5x + a^6)$