Einschub: Summen, Produkte und Potenzen.

Allgemeine Summen und Produkte.

$$\sum_{k=m}^{n} b_k := b_m + b_{m+1} + \cdots + b_n \quad \text{(falls } m \leq n\text{)}$$

$$\sum_{k=m}^{n} b_k := 0 \quad \text{(falls } m > n\text{, leere Summe)}$$

$$\prod_{k=m}^{n} b_k := b_m \cdot b_{m+1} \cdot \ldots \cdot b_n \quad \text{(falls } m \leq n\text{)}$$

$$\prod_{k=m}^{n} b_k := 1 \quad \text{(falls } m > n\text{, leeres Produkt)}$$

Einschub: Summen, Produkte und Potenzen.

Potenzen.

$$a^n := \begin{cases} \prod_{k=1}^{n} a & \text{für } n \geq 0 \\ 1/(a^{-n}) & \text{für } n < 0 \end{cases}$$

Potenzgesetze.

$$\begin{aligned} a^n \cdot a^m &= a^{n+m} \\ (a^n)^m &= a^{n \cdot m} \end{aligned}$$

Binomialkoeffizienten und deren Eigenschaften.

Definition: *Die Zahlen* $\binom{n}{m}$ *heißen* Binomialkoeffizienten.

Satz:

(a) Für $n, m \in \mathbb{N}$ mit $0 < m \leq n$ gilt die Rekursionsformel

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1},$$

wobei

$$\binom{n}{0} = \binom{n}{n} = 1.$$

(b) Für $n \in \mathbb{N}_0$ und $a, b \in \mathbb{R}$ gilt der Binomische Lehrsatz

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

Beweis von Teil (a): Es gilt

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

■

Beweis von Teil (b): durch vollständige Induktion über n.

- Induktionsanfang ($n = 0$): Es gilt

$$(a+b)^0 = \binom{0}{0} a^0 b^0 = 1.$$

- Induktionsannahme: Für $n \geq 0$ gelte

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

- Induktionsschluss ($n \to n+1$):

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \binom{n}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]a^k b^{n+1-k} + \binom{n}{n}a^{n+1}b^0 \\
&= \binom{n+1}{0}a^0 b^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k} + \binom{n+1}{n+1}a^{n+1}b^0 \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}$$

$\blacksquare$

Direkte Berechnung der Binomialkoeffizienten.

Für $n, m \in \mathbb{N}_0$ mit $m \leq n$ gilt

$$\binom{n}{m} = \frac{n!}{m!(n-m)!} = \frac{n(n-1)\cdot \ldots \cdot (n-m+1)}{1 \cdot 2 \cdot \ldots \cdot m} = \prod_{k=1}^{m} \frac{n-k+1}{k}.$$

Klassisches Beispiel: Zahlenlotto.

Es gibt

$$\binom{49}{6} = \frac{49!}{6!43!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13983816$$

Möglichkeiten, aus einer 49-elementigen Menge eine 6-elementige Teilmenge auszuwählen.

Mit anderen Worten: Die Wahrscheinlichkeit, beim (klassischen) Zahlenlotto "6 aus 49" die 6 richtigen Zahlen zu tippen, beträgt

$$\frac{1}{\binom{49}{6}} = \frac{1}{13983816} = 0.0000000715112384201 8516\ldots$$

Rekursive Berechnung der Binomialkoeffizienten.

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$

Pascalsches Dreieck.

Beispiel:

$$
\begin{aligned}
(a+b)^5 &= 1 \cdot a^0 b^5 + 5 \cdot a^1 b^4 + 10 \cdot a^2 b^3 + 10 \cdot a^3 b^2 + 5 \cdot a^4 b^1 + 1 \cdot a^5 b^0 \\
&= a^5 + 5a^4 b + 10a^3 b^2 + 10a^2 b^3 + 5ab^4 + b^5
\end{aligned}
$$

2.2 Primzahlen

Definition: *Eine natürliche Zahl $m \in \mathbb{N}$ heißt* `Teiler` *von $n \in \mathbb{N}$, falls ein $k \in \mathbb{N}$ existiert mit*

$$n = k \cdot m.$$

Man schreibt dann auch $m|n$. □

Jede Zahl $n \in \mathbb{N}$ besitzt offensichtlich die beiden Teiler 1 und n, denn es gilt stets

$$n = n \cdot 1 = 1 \cdot n$$

Existiert für $n > 1$ *kein* weiterer Teiler, so nennt man n eine `Primzahl`.

Die ersten Primzahlen lauten

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Bemerkung: Es gibt unendlich viele Primzahlen. ■

Hauptsatz der Zahlentheorie.

Satz: Jede natürliche Zahl $n \in \mathbb{N}$ läßt sich als Produkt von Primzahlpotenzen schreiben,

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k},$$

wobei p_j Primzahl und $r_j \in \mathbb{N}_0$ für $1 \leq j \leq k$.

Beweis: durch Induktion über n.

• Induktionsanfang ($n = 1$): Es gilt $1 = 2^0$.

• Induktionsannahme: Alle $k \leq n$ besitzen Primfaktorzerlegung.

• Induktionsschluss ($n \to n + 1$):

Fall 1: Sei $n + 1$ Primzahl. Dann gilt $n + 1 = (n + 1)^1$.

Fall 2: Sei $n + 1$ *keine* Primzahl. Dann gibt es $k, m \leq n$ mit $n + 1 = k \cdot m$. Somit besizt $n + 1$ eine Primfaktorzerlegung, da k und m je eine besitzen. ■

Bemerkung: Für $n > 1$ sind die (verschiedenen) Basen $p_1, \ldots, p_k$ und die zugehörigen Exponenten $r_1, \ldots, r_k \geq 1$ der Primfaktorzerlegung eindeutig.

ggT und kgV.

Definition: *Seien* $n, m \in \mathbb{N}$ *zwei natürliche Zahlen. Dann heißt*

$$\text{ggT}(n, m) = \max\{k \mid k \textit{ teilt } n \textit{ und } k \textit{ teilt } m\}$$

der `größte gemeinsame Teiler` *(ggT) von* n *und* m*. Weiterhin heißt*

$$\text{kgV}(n, m) = \min\{k \mid n \textit{ teilt } k \textit{ und } m \textit{ teilt } k\}$$

das `kleinste gemeinsame Vielfache` *(kgV) von* n *und* m*.* □

Beobachtung: Für

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k} \quad \text{und} \quad m = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_k^{s_k}$$

mit Primfaktoren $p_1, \ldots, p_k$ und Exponenten $r_1, \ldots, r_k, s_1, \ldots, s_k \geq 0$ gilt

$$\begin{aligned} \text{ggT}(n, m) &= p_1^{\min(r_1, s_1)} \cdot p_2^{\min(r_2, s_2)} \cdot \ldots \cdot p_k^{\min(r_k, s_k)} \\ \text{kgV}(n, m) &= p_1^{\max(r_1, s_1)} \cdot p_2^{\max(r_2, s_2)} \cdot \ldots \cdot p_k^{\max(r_k, s_k)} \end{aligned}$$

□

Beispiel. Für

$$\begin{aligned} n &= 525 = 2^0 \cdot 3^1 \cdot 5^2 \cdot 7^1 \\ m &= 180 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^0 \end{aligned}$$

gilt

$$\begin{aligned} \text{ggT}(525, 180) &= 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 15 \\ \text{kgV}(525, 180) &= 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 6300 \end{aligned}$$

und

$$n \cdot m = 525 \cdot 180 = 15 \cdot 6300 = \text{ggT}(525, 180) \cdot \text{kgV}(525, 180).$$

$\square$

Beobachtung: Für alle $n, m \in \mathbb{N}$ gilt

$$n \cdot m = \text{ggT}(n, m) \cdot \text{kgV}(n, m).$$

$\square$

Der Euklidische Algorithmus.

Für $n, m \in \mathbb{N}$ läßt sich deren ggT mit dem `Verfahren der iterierten Division` (`Euklidischer Algorithmus`) bestimmen.

Vorüberlegung: Zu $n, m \in \mathbb{N}$, $n \geq m$, existieren eindeutige $q, r \in \mathbb{N}_0$ mit

$$n = q \cdot m + r, \qquad \text{wobei } 0 \leq r < m.$$

Algorithmus (Euklidischer Algorithmus) **:**

INPUT: $n, m \in \mathbb{N}$ mit $n \geq m$.

- Setze $r_0 = n, r_1 = m$ und $j = 1$;
- **REPEAT**
  - $r_{j-1} = q_j \cdot r_j + r_{j+1}$, wobei $0 \leq r_{j+1} < r_j$;
  - Setze $j = j + 1$;

  UNTIL $(r_{j+1} = 0)$

OUTPUT: $r_j = \text{ggT}(n, m)$.

Beispiel. Für $n = 3054$ und $m = 1002$ liefert der Euklidische Algorithmus:

$$\begin{array}{rcrcrcr} 3054 & = & 3 & \cdot & 1002 & + & 48 \\ 1002 & = & 20 & \cdot & 48 & + & 42 \\ 48 & = & 1 & \cdot & 42 & + & 6 \\ 42 & = & 7 & \cdot & \boxed{6} & + & 0 \end{array}$$

Somit gilt $\text{ggT}(3054, 1002) = 6$ und $\text{kgV}(3054, 1002) = 3054 \cdot 1002/6 = 510018$.

$\mathbb{Z}$-Kombination des $\text{ggT}(n, m)$ von n und m.

$$\begin{aligned} 6 &= 48 - 1 \cdot 42 \\ &= 48 - 1 \cdot (1002 - 20 \cdot 48) = 21 \cdot 48 - 1002 \\ &= 21 \cdot (3054 - 3 \cdot 1002) - 1002 = 21 \cdot 3054 - 64 \cdot 1002. \end{aligned}$$

Die $\mathbb{Z}$-Kombination von $n = 3054$ und $m = 1002$ ist gegeben durch

$$\text{ggT}(3054, 1002) = 6 = 21 \cdot 3054 - 64 \cdot 1002.$$

2.3 Reelle Zahlen

Erweiterung des Zahlenbereichs der natürlichen Zahlen

- Ganze Zahlen

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}.$$

- Rationale Zahlen

$$\mathbb{Q} := \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

BEACHTE: $\sqrt{2} \notin \mathbb{Q}$.

ABER: Die Zahl $\sqrt{2}$ lässt sich beliebig genau durch rationale Zahlen aus $\mathbb{Q}$ *approximieren*, d.h. zu jedem $\epsilon > 0$ gibt es ein $q \in \mathbb{Q}$ mit

$$|\sqrt{2} - q| < \epsilon.$$

DAHER: Definieren den Zahlenbereich $\mathbb{R}$ der reellen Zahlen.

Axiomensystem für die reellen Zahlen.

(I) Regeln der Addition (Abelsche Gruppe)**:**

$$
\begin{array}{llcll}
\text{(a)} & x+(y+z) & = & (x+y)+z & \\
\text{(b)} & x+y & = & y+x & \\
\text{(c)} & x+0 & = & 0+x & = \; x \\
\text{(d)} & x+(-x) & = & (-x)+x & = \; 0
\end{array}
$$

(II) Regeln der Multiplikation:

$$
\begin{array}{llclll}
\text{(a)} & x\cdot(y\cdot z) & = & (x\cdot y)\cdot z & & \\
\text{(b)} & x\cdot y & = & y\cdot x & & \\
\text{(c)} & x\cdot 1 & = & 1\cdot x & = \; x & \\
\text{(d)} & x\cdot\left(\frac{1}{x}\right) & = & \left(\frac{1}{x}\right)\cdot x & = \; 1 & \text{für } x \neq 0
\end{array}
$$

(III) Distributivgesetz: $x\cdot(y+z) = x\cdot y + x\cdot z$

Weitere Axiome für $\mathbb{R}$.

(IV) Ordnungseigenschaften:

(a) $x \leq y \vee y \leq x$

(b) $x \leq x$

(c) $x \leq y \wedge y \leq x \implies x = y$

(d) $x \leq y \wedge y \leq z \implies x \leq z$

(e) $x \leq y \implies x + z \leq y + z$

(f) $x \leq y \wedge z \geq 0 \implies x \cdot z \leq y \cdot z$

(V) Vollständigkeitsaxiom (DEDEKIND, 1872)**:**

Sei $\mathbb{R} = L \cup R$ zerlegt in nichtleere Mengen $L, R \neq \emptyset$ mit $\forall\, x \in L,\ y \in R : x < y$.

Dann gibt es genau eine `Schnittzahl` $s \in \mathbb{R}$ mit

$$\forall\, x \in L,\ y \in R: \quad x \leq s \leq y.$$

Bemerkungen.

- Eine nichtleere Menge mit (I) heißt Abelsche Gruppe.
- Eine nichtleere Menge mit (I)–(III) heißt Körper.
- Ein Körper mit (IV) heißt angeordneter Körper.
- Die rationalen Zahlen $\mathbb{Q}$ bilden einen angeordneten Körper.
- **ABER:** Die rationalen Zahlen erfüllen nicht das Vollständikeitsaxiom!

DENN: Für

$$\begin{aligned} L &:= \{x \in \mathbb{Q} \,|\, x^2 < 2 \vee x < 0\} \\ R &:= \{x \in \mathbb{Q} \,|\, x^2 > 2 \wedge x > 0\} \end{aligned}$$

gibt es keine Schnittzahl in $\mathbb{Q}$. Die Schnittzahl wäre $s = \sqrt{2} \notin \mathbb{Q}$.

Rechnen mit Ungleichungen und Beträgen.

(1) $x \le y \implies -x \ge -y$

(2) $x \le y \wedge z \le 0 \implies x \cdot z \ge y \cdot z$

(3) $x^2 \ge 0$

(4) $x \le y \wedge u \le v \Rightarrow x + u \le y + v$

(5) $0 \le x \le y \wedge 0 \le u \le v \implies x \cdot u \le y \cdot v$

Beweis: Mit Ordnungsaxiomen (IV), z.B.

(1):

$$x \le y \implies x + (-x - y) \le y + (-x - y) \implies -y \le -x.$$

(2):

$$\begin{aligned} x \le y \wedge z \le 0 \quad &\implies \quad x \le y \wedge (-z) \ge 0 \\ &\implies \quad x \cdot (-z) \le y \cdot (-z) \\ &\implies \quad x \cdot z \ge y \cdot z \end{aligned}$$

Definition: *Zu* $a \in \mathbb{R}$ *heißt*

$$|a| := \begin{cases} a & \textit{falls } a \geq 0; \\ -a & \textit{falls } a < 0; \end{cases}$$

der **Betrag** *von* a.

Zu $a, b \in \mathbb{R}$ *heißt* $|a - b|$ *der (nichtnegative)* **Abstand** *der Zahlen* a *und* b.

Eigenschaften:

(1) $|a| \geq 0$

(2) $|a| = 0 \implies a = 0$

(3) $|ab| = |a|\,|b|$

(4) $|a + b| \leq |a| + |b|$ (**Dreiecksungleichung**)

(5) $U_\varepsilon(a) := \{x \in \mathbb{R} \mid |x - a| < \varepsilon\} \quad (\varepsilon > 0)$

$= (a - \varepsilon, a + \varepsilon)$ (**ε-Umgebung von a**)

Definition: *Sei $M \subset \mathbb{R}$ Teilmenge von $\mathbb{R}$.*

(1a) Dann heißt $x \in \mathbb{R}$ `obere Schranke` *von M, falls $\forall\, w \in M : w \leq x$.*

(1b) $x \in \mathbb{R}$ heißt `untere Schranke` *von M, falls $\forall\, w \in M : w \geq x$.*

(2a) M heißt `nach oben beschränkt`*, falls es eine obere Schranke von M gibt.*

(2b) M heißt `nach unten beschränkt`*, falls es untere Schranke von M gibt.*

(3a) $s \in \mathbb{R}$ heißt `Supremum` *von M, falls s die kleinste obere Schranke von M ist.*

(3b) $s \in \mathbb{R}$ heißt `Infimum` *von M, falls s die größte untere Schranke von M ist.*

Bezeichnungen:

- sup(M) Supremum von M;
- inf(M) Infimum von M.

Beispiele:

(1) $M = [1, 2) \subset \mathbb{R}$. Dann gilt inf$(M) = 1$, sup$(M) = 2$.

(2) Für $M = \{x \in \mathbb{R} \,|\, x = \frac{2n+1}{n(n+1)}, n \in \mathbb{N}\} = \left\{\frac{3}{2}, \frac{5}{6}, \frac{7}{12}, \frac{9}{20}, \frac{11}{30}, \ldots\right\}$ gilt inf$(M) = 0$, sup$(M) = 3/2$.

Satz:

Jede nichtleere nach oben beschränkte Menge $M \subset \mathbb{R}$ *besitzt ein Supremum.*

Jede nichtleere nach unten beschränkte Menge $M \subset \mathbb{R}$ *besitzt ein Infimum.*

Beweis: Mit Hilfe des Vollständigkeitsaxioms (V).

Folgerungen:

(1) Die Menge $\mathbb{N}$ der natürlichen Zahlen ist *nicht* nach oben beschränkt.

(2) Für alle $x \in \mathbb{R}$ gilt

$$x > 0 \quad \Longrightarrow \quad \exists\, n \in \mathbb{N} : 0 < \frac{1}{n} < x$$

(3) Zwischen zwei reellen Zahlen $x < y$ liegen (unendlich viele) rationale Zahlen.