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 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 unendliche 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 $n+1$ eine 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 besitzt $n+1$ eine Primfaktorzerlegung, da k und m je eine besitzen.

Der ggT und das kgV.

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

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

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

$$\mathrm{kgV}(n,m) := \min\{k \mid n \text{ und } m \text{ teilen } k\}$$

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 $p1, \ldots, p_k$ und Exponenten $r_1, \ldots, r_k, s_1, \ldots, s_k \geq 0$ gilt

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

Beispiel zu ggT und kgV.

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

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

und

$$n \cdot m = 525 \cdot 180 = 15 \cdot 6300 = \mathrm{ggT} \cdot \mathrm{kgV}$$

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

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

Der Euklidische Algorithmus.

Für $n, m \in \mathbb{N}$ läßt sich der ggT mit dem Verfahren der iterierten Division bestimmen.

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

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

(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: $r_j = ggT(n, m)$.

Beispiel zum Algorithmus und $\mathbb{Z}$–Kombination.

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

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

$\Longrightarrow$ ggT(3054,1002) $= 6$, kgV(3054,1002) $= 3054 \cdot 1002/6 = 510018$.

$\mathbb{Z}$–Kombination des 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

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

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

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

$$|\sqrt{2} - q| < \varepsilon$$

Axiomensystem für die reellen Zahlen.

(I) Regeln der Addition ($(\mathbb{R}, +)$ ist eine Abelsche Gruppe):

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

(II) Regeln der Multiplikation ($(\mathbb{R} \setminus \{0\}, +)$ Abelsche Gruppe):

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

(III) Distributivgesetz (Regeln (I)–(III): Körperaxiome):

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

Weitere Axiome für die reellen Zahlen.

(IV) Ordnungseigenschaften

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

(b) $x \leq x$

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

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

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

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

(V) Vollständigkeitsaxiom (Dedekind, 1872)

Sei $\mathbb{R} = L \cup R$ zerlegt in nichtleere Mengen mit $\forall\, x \in L, y \in R : x < y$. Dann gibt es genau eine Schnittzahl $s \in \mathbb{R}$ mit

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

Eine Bemerkung und Rechnen mit Ungleichungen.

Bemerkung: Die Menge der rationalen Zahlen $\mathbb{Q}$ erfüllt nicht das Vollständigkeitsaxiom (V). Denn für

$$L := \{x \in \mathbb{Q} \mid x^2 < 2 \vee x < 0\}$$

$$R := \{x \in \mathbb{Q} \mid x^2 > 2 \wedge x > 0\}$$

gibt es keine Schnittzahl. Diese wäre $x = \sqrt{2} \notin \mathbb{Q}$.

Weitere Regeln beim Rechnen mit Ungleichungen (mit den Axiomen (IV))

(1) $x \leq y \Rightarrow -x \geq -y$

(2) $(x \leq y \wedge z \leq 0) \Rightarrow x \cdot z \geq y \cdot z$

(3) $x^2 \geq 0$

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

(5) $(0 \leq x \leq y \wedge 0 \leq u \leq v) \Rightarrow x \cdot u \leq y \cdot v$

Der Betrag einer reellen Zahl.

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

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

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) $|a| = 0 \Rightarrow a = 0$

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

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

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

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

Obere und untere Schranke, Supremum und Infimum.

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

1) Die Zahl $x \in \mathbb{R}$ heißt obere Schranke von M, falls gilt:

$$\forall\, w \in M : \; w \leq x$$

Analog definiert man den Begriff untere Schranke von M.

2) Die Menge M heißt nach oben (bzw. nach unten) beschränkt, falls es eine obere (bzw. untere) Schranke von M gibt.

3) Die Zahl $s \in \mathbb{R}$ heißt Supremum von M, mit Notation

$$s = \sup_{x \in M} M = \sup(M),$$

falls s die kleinste obere Schranke von M ist, d.h.

- s ist eine obere Schranke von M
- für jede beliebige obere Schranke x von M gilt: $s \leq x$

Analog definiert man den Begriff Infimum von M.

Beispiele zu Supremum und Infimum.

Beispiel: Betrachte das Intervall $I = [1, 2) = \{x \in \mathbb{R} \,|\, 1 \leq x < 2\}$
Dann ist

- jede Zahl $x \geq 2$ eine obere Schranke von I,
- jede Zahl $x \leq 1$ eine untere Schranke von I.

Also gilt

$$\sup [1, 2) = 2 \qquad \inf [1, 2) = 1$$

Beispiel: Betrachte die Menge $M \subset \mathbb{R}$ definiert durch

$$M := \left\{ x \in \mathbb{R} \,|\, x = \frac{1}{n} + \frac{1}{n+1},\ n \in \mathbb{N} \right\} = \left\{ \frac{3}{2}, \frac{5}{6}, \frac{7}{12}, \frac{9}{20}, \frac{11}{30}, \dots \right\}$$

Dann gilt

$$\sup M = \frac{3}{2} \qquad \inf M = 0$$

Zur Existenz eines Supremums und Infimums.

Satz: Jede nichtleere, nach oben (bzw. unten) beschränkte Menge $M \subset \mathbb{R}$ besitzt ein Supremum (bzw. Infimum).

Beweis: Mit Hilfe des Vollständigkeitsaxioms.

Folgerungen:

1) Die Menge $\mathbb{N}$ der natürlichen Zahlen ist nicht nach oben beschränkt.
2) Für alle $x \in \mathbb{R}$ gilt:

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

3) Zwischen zwei reellen Zahlen $x < y$ gibt es immer (unendlich viele) rationale Zahlen.