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*

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

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

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

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

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

□

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

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

und

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

□

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

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

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

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

$\mathbb{Z}$-Kombination des $\mathrm{ggT}(n, m)$ 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

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

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):

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

(II) Regeln der Multiplikation:

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

(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

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

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

Rechnen mit Ungleichungen und Beträgen.

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

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

(3) $x^2 \geq 0$

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

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

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

(1):

$$x \leq y \Longrightarrow x + (-x - y) \leq y + (-x - y) \Longrightarrow -y \leq -x.$$

(2):

$$\begin{aligned} x \leq y \wedge z \leq 0 &\implies x \leq y \wedge (-z) \geq 0 \\ &\implies x \cdot (-z) \leq y \cdot (-z) \\ &\implies x \cdot z \geq y \cdot z \end{aligned}$$

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

(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 $M = \{x \in \mathbb{R} \mid x = \frac{2n+1}{n(n+1)}, n \in \mathbb{N}\} = \{\frac{3}{2}, \frac{5}{6}, \frac{7}{12}, \frac{9}{20}, \frac{11}{30}, \ldots\}$ 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.

3 Konvergenz von Folgen und Reihen

3.1 Normierte Vektorräume

Definition: *Sei V ein normierter Vektorraum über $\mathbb{R}$. Eine Abbildung $\|\cdot\| : V \to [0,\infty)$ heißt* Norm *auf V, falls die folgenden Eigenschaften erfüllt sind.*

(N1) $\|v\| = 0 \Longleftrightarrow v = 0$ *(*Definitheit*);*

(N2) $\|\lambda \cdot v\| = |\lambda| \cdot \|v\|$ *für alle* $\lambda \in \mathbb{R}$, $v \in V$ *(*Homogenität*);*

(N3) $\|v + w\| \leq \|v\| + \|w\|$ *für alle* $v, w \in V$ *(*Dreiecksungleichung*).*

V zusammen mit $\|\cdot\|$ heißt dann normierter Vektorraum*.*

Beispiele für Normierte Vektorräume.

- $\mathbb{R}$ mit der Betragsfunktion $|\cdot|$ ist ein normierter Vektorraum.
- Für $n \geq 1$ ist der $\mathbb{R}^n$, zusammen mit der p-Norm, $p \in \mathbb{N}$,

$$\|x\|_p = \left(\sum_{j=1}^{n} |x_j|^p \right)^{1/p}, \qquad \text{für } x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n,$$

ein normierter Vektorraum.

Spezialfall: Für $p = 2$ bekommt man die Euklidische Norm

$$\|x\|_2 = \sqrt{\sum_{j=1}^{n} x_j^2} \qquad \text{für } x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n.$$

Weiterhin $(p = \infty)$**:** Die Maximumnorm

$$\|x\|_\infty = \max_{1 \leq j \leq n} |x_j| \qquad \text{für } x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n.$$

Weitere Beispiele für Normierte Vektorräume.

Sei $V = C[a, b]$ der Vektorraum aller *stetigen* Funktionen auf $[a, b] \subset \mathbb{R}$.

- Dann ist die p-Norm

$$\|f\|_p = \left(\int_a^b |f(x)|^p \, dx \right)^{1/p}, \qquad \text{für } f \in C[a, b],$$

für $p \in \mathbb{N}$ eine Norm auf V.

- **Wichtiger Spezialfall:** Für $p = 2$ ist die Euklidische Norm

$$\|f\|_2 = \sqrt{\int_a^b |f(x)|^2 \, dx}, \qquad \text{für } f \in C[a, b],$$

eine Norm auf V.

- **Weiterhin** $(p = \infty)$**:** Die Maximumnorm ist gegeben durch

$$\|f\|_\infty = \max_{a \le x \le b} |f(x)|, \qquad \text{für } f \in C[a, b].$$

3.2 Folgen

Definition: *Sei V normierter Vektorraum mit Norm $\|\cdot\|$. Eine* Folge *ist eine Abbildung $\mathbb{N} \to V$, $n \mapsto a_n$, kurz $(a_n)_{n\in\mathbb{N}}$ oder $(a_n)_{n\geq 1}$.* □

Beispiele für Folgen.

- Reelle Folgen (Folgen reeller Zahlen), d.h. $V = \mathbb{R}$, z.B. ist

$$a_n = \frac{1}{n}, \qquad \text{für } n \in \mathbb{N},$$

  eine reelle Folge.

- Komplexe Folgen (Folgen komplexer Zahlen), d.h. $V = \mathbb{C}$, z.B. ist

$$a_n = i^n, \qquad \text{für } n \in \mathbb{N},$$

  eine komplexe Folge.

Weitere Beispiele für Folgen.

- Vektorenfolgen (Folgen von Vektoren), $V = \mathbb{R}^n$ oder $V = \mathbb{C}^n$, z.B. ist

$$a_n = \left(\frac{1}{n}, n, \frac{1}{n^2}\right)^T \in \mathbb{R}^3, \qquad \text{für } n \in \mathbb{N},$$

  eine Folge reeller Vektoren.

- Funktionenfolgen (Folge von Funktionen), etwa $V = C[a, b]$, z.B. ist für $[a, b] = [0, 1]$ die Folge

$$f(x) = x^n, \qquad \text{für } x \in [0, 1] \text{ und } n \in \mathbb{N},$$

  eine Funktionenfolge.