2 Aufbau des Zahlensystems – Natürliche Zahlen

(2.1) Die Menge der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$ lässt sich eindeutig durch die Peano-Axiome charakterisieren:
(P1) $1 \in \mathbb{N}$
(P2) $n \in \mathbb{N} \implies n+1 \in \mathbb{N}$
(P3) $n, m \in \mathbb{N},\ n \neq m \implies n+1 \neq m+1$
(P4) $n \in \mathbb{N} \implies n+1 \neq n$
(P5) Wenn für eine Teilmenge $M \subset \mathbb{N}$ gilt

(i) $1 \in M$ (ii) $\forall n \in \mathbb{N}\colon 1, \dots, n \in M \implies n+1 \in M$

dann gilt $M = \mathbb{N}$.

(2.2) Es ist genau dann $n < m$, wenn m durch (mehrfaches) Ausführen der Nachfolgeoperation $+1$ erreicht wird.

(2.3) (P5) ist äquivalent zu:
(P5') Wenn für eine Teilmenge $M \subset \mathbb{N}$ gilt

(i) $1 \in M$ (ii') $\forall n \in \mathbb{N}\colon n \in M \implies n+1 \in M$

dann gilt $M = \mathbb{N}$.
(P5") Jede Teilmenge $S \subset \mathbb{N}$, $S \neq \emptyset$, besitzt ein genau ein kleinstes Element.

(2.4) Eine endliche Menge mit N Elementen besitzt 2^N Teilmengen.
(2.5) Es gibt $N!$ Permutationen eines N-Tupels.

2 Aufbau des Zahlensystems – Natürliche Zahlen

(2.6) Eine endliche Menge mit N Elementen besitzt $\binom{N}{k} = \frac{N!}{(N-k)!\,k!}$ Teilmengen mit k Elementen (dabei setze $0! := 1$). Insbesondere gilt $\sum_{k=0}^{N} \binom{N}{k} = 2^N$.

(2.7) a) Für die *Binomialkoeffizienten* gilt:

$$\binom{N}{0} = \binom{N}{N} = 1 \qquad \text{und} \qquad \binom{N+1}{k} = \binom{N}{k} + \binom{N}{k-1} \quad \text{für} \quad 1 \le k \le N.$$

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

Kombinatorik - Theorie der Anzahlbestimmung

(2.8) Aus einer Menge A mit N Elementen kann man folgende Stichproben vom Umfang k ziehen:

a) N^k geordnete Stichproben mit Wiederholungen $(k \in \mathbb{N})$

b) $\frac{N!}{(N-k)!}$ geordnete Stichproben ohne Wiederholungen $(k \in \{1,\dots,N\})$

c) $\binom{N}{k}$ ungeordnete Stichproben ohne Wiederholungen $(k \in \{1,\dots,N\})$

d) $\binom{N+k-1}{k}$ ungeordnete Stichproben mit Wiederholungen $(k \in \mathbb{N})$.

2 Aufbau des Zahlensystems – Algebraische Grundlagen

Eine Menge G mit einer Verknüpfung

$$\begin{aligned} *: \quad & G \times G \longrightarrow G \\ & (a,b) \longmapsto a * b \end{aligned}$$

heißt *Halbgruppe*, wenn gilt:

I) Assoziativgesetz $(a * b) * c = a * (b * c)$ für alle $a,b,c \in G$.

II) Es existiert ein neutrales Element $e \in G$, d. h. $e * a = a * e = a$ für alle $a \in G$

Eine Halbgruppe G heißt *Gruppe*, wenn gilt:

III) Jedes Element $a \in G$ besitzt ein Inverses $a^{-1} \in G$, d. h. $a * a^{-1} = a^{-1} * a = e$.

IV) Eine Gruppe heißt *kommutativ*, wenn $a * b = b * a$ für alle $a,b \in G$.

Eine kommutative Gruppe R mit Verknüpfung $+$ und neutralem Element 0 heißt *Ring*, wenn auf R eine weitere Verknüpfung $\cdot$ definiert ist, wenn $R \setminus \{0\}$ mit $\cdot$ eine Halbgruppe ist, und wenn gilt:

V) Distributionsgesetz $a \cdot (b+c) = a \cdot b + a \cdot c$ für alle $a,b,c \in R$.

Ein *Körper* K ist ein Ring, für den $K \setminus \{0\}$ mit $\cdot$ eine kommutative Gruppe ist.
Ein angeordneter Körper K ist ein Körper mit einer Ordnungsrelation " $\leq$ " mit

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

2 Aufbau des Zahlensystems – Reelle Zahlen

(2.9) Der Körper der reellen Zahlen $\mathbb{R}$ ist ein angeordneter Körper, der die rationalen Zahlen $\mathbb{Q}$ enthält, und der das *Vollständigkeitsaxiom* erfüllt:

(2.10) $M \subset \mathbb{R}$ heißt *nach unten beschränkt*, wenn eine *untere Schranke* $a \in \mathbb{R}$ existiert mit $a \leq x$ für $x \in M$, und M heißt *nach oben beschränkt*, wenn eine *obere Schranke* $a \in \mathbb{R}$ existiert mit $x \leq a$ für $x \in M$.

Das *Infimum* $\inf M$ ist die größte untere Schranke von M, d.h.
$$\inf M = s \iff \forall \varepsilon > 0 \exists x \in M\colon\ x < s + \varepsilon$$

Das *Supremum* $\sup M$ ist die kleinste obere Schranke von M, d.h.
$$\sup M = s \iff \forall \varepsilon > 0 \exists x \in M\colon\ x > s - \varepsilon.$$

Falls $\inf M \in M$, dann heißt $\inf M = \min M$ das *Minimum*.

Falls $\sup M \in M$, dann heißt $\sup M = \max M$ das *Maximum*.

(2.11) a) Jede nicht leere nach oben beschränkte Menge besitzt ein Supremum.
b) Jede nicht leere nach unten beschränkte Menge besitzt ein Infimum.

(2.12) a) $\forall x \in \mathbb{R}\ \exists\ n \in \mathbb{N}\colon \qquad x < n$
b) $\forall \varepsilon > 0\ \exists\ m \in \mathbb{N}\colon \qquad \frac{1}{m} < \varepsilon$
c) $\forall x \in \mathbb{R}\ \forall\ \varepsilon > 0\ \exists\ q \in \mathbb{Q}\colon \qquad |x - q| < \varepsilon$

(2.13) Für $a \geq 0$ und $N \in \mathbb{N}$ besitzt die Gleichung $x^N = a$ genau eine positive Lösung in $\mathbb{R}$.

2 Aufbau des Zahlensystems – Komplexe Zahlen

(2.14) Sei i die imaginäre Einheit mit $\mathrm{i}^2 = -1$, und sei $\mathbb{C} = \{z = x + \mathrm{i}y \mid x, y \in \mathbb{R}\}$ die Menge der komplexen Zahlen.

(2.15) $\mathbb{C}$ ist ein Körper, der $\mathbb{R}$ und i enthält.

(2.16) a) Für $z = x + \mathrm{i}y$ heißt $x = Re(z)$ der Realteil und $y = Im(z)$ der Imaginärteil von z.
b) $\bar{z} = x - \mathrm{i}y$ ist die konjugiert komplexe Zahl zu z.
c) $|z| = \sqrt{x^2 + y^2}$ ist der Betrag von z.

(2.17) Es gibt genau N verschiedene komplexe Zahlen $z_k = \exp\left(\mathrm{i}\,\frac{2\pi k}{n}\right)$, $k = 0, \ldots, N-1$, mit $z^N = 1$.

(2.18) Für $a_1, \ldots, a_n,\ b_1, \ldots, b_N \in \mathbb{C}$ gilt:

1) allgemeine Dreiecksungleichung $\left|\sum_{k=1}^{N} a_k\right| \leq \sum_{k=1}^{N} |a_k|$

2) Cauchy-Schwarz-Ungleichung $\sum_{k=1}^{N} |a_k b_k| \leq \left(\sum_{k=1}^{N} |a_k|^2\right)^{1/2} \left(\sum_{k=1}^{N} |b_k|^2\right)^{1/2}$

3) Minkowski-Ungleichung $\left(\sum_{k=1}^{N} |a_k + b_k|^2\right)^{1/2} \leq \left(\sum_{k=1}^{N} |a_k|^2\right)^{1/2} + \left(\sum_{k=1}^{N} |b_k|^2\right)^{1/2}$

2 Aufbau des Zahlensystems – Komplexe Zahlen

(2.19) Fundamentalsatz der Algebra:
Jedes Polynom P mit $\operatorname{grad} P \geq 1$ besitzt eine komplexe Nullstelle $\xi \in \mathbb{C}$. d.h. $P(\xi) = 0$.

(2.20) Jedes Polynom P mit $\operatorname{grad} P = N \geq 1$ besitzt eine Zerlegung

$$P(z) = a_N(z - z_1)\dots(z - z_N) .$$

Dabei sind $z_1, \dots, z_N \in \mathbb{C}$ die (nicht notwendig verschiedenen) Nullstellen von P.

(2.21) $\xi \in \mathbb{C}$ heißt k-fache Nullstelle von $P(z)$, falls $P(z) = (z - \xi)^k Q(z)$ und
$Q(\xi) \neq 0$, $\operatorname{grad} q = N - k$.

(2.22) Wenn für $P(z) = \sum_{k=0}^{N} a_k z^k$, $Q(z) = \sum_{k=0}^{N} b_k z^k$ und $P(\xi_j) = Q(\xi_j)$ für $n+1$ verschiedene ξ_j gilt,
dann gilt $P = Q$ (also $a_k = b_k$ für alle $k = 0, \dots, N$).

(2.23) Polynomdivision mit Rest: Zu Polynomen P und Q mit $\operatorname{grad} P \geq \operatorname{grad} Q \geq 1$
existieren Polynome S und R mit $\operatorname{grad} R < \operatorname{grad} Q$ und

$$P(z) = S(z)Q(z) + R(z) .$$

2 Aufbau des Zahlensystems – Endliche Körper

(2.24) Eine Zahl $m \in \mathbb{N}$ heißt Teiler von $n \in \mathbb{N}$, falls $k \in \mathbb{N}$ existiert mit $n = k \cdot m$.
Wenn $n > 1$ und wenn n nur die Teiler 1 und n besitzt, heißt n *Primzahl*.

(2.25) Jede Zahl $n \in \mathbb{N}, n > 1$ besitzt eine Darstellung $n = \prod_{i=1}^{r} p_i^{m_i}$ mit Primzahlen $p_i \neq p_j$ und $m_i \in \mathbb{N}$.
Dabei sind die Exponenten m_i eindeutig bestimmt.

(2.26) Zu $n, m \in \mathbb{N}$ definiere

$$\text{ggT}(n,m) = \max\{k \in \mathbb{N} \mid k \text{ teilt } n \text{ und } m\}$$
$$\text{kgV}(n,m) = \min\{k \in \mathbb{N} \mid n \text{ und } m \text{ teilen } k\}.$$

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

(2.27) *Euklidischer Algorithmus* zu $n, m \in \mathbb{N}$

$$\begin{aligned}
&r_0 = n,\ r_1 = m \\
&r_0 = s_1 r_1 + r_2 && r_2 \in \{1, \ldots, r_1 - 1\} \\
&r_1 = s_2 r_2 + r_3 && r_3 \in \{1, \ldots, r_2 - 1\} \\
&\quad \vdots \\
&r_{k-1} = s_k r_k + r_{k+1} && \text{mit } \ r_{k+1} = 0 \ .
\end{aligned}$$

Es gilt: $r_k = \text{ggT}(n,m)$ und es existieren $a, b \in \mathbb{Z}$ mit $\text{ggT}(n,m) = an + bm$.

2 Aufbau des Zahlensystems – Endliche Körper

(2.28) $x \equiv y \mod m \iff \exists k \in \mathbb{Z}\colon x - y = km$ *(„x kongruent y modulo m“)*

(2.29) $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ für $m \geq 2$ ist ein kommutativer Ring *(Restklassenring)* mit
$a +_m b = c \iff a + b \equiv c \mod m$
$a \cdot_m b = c \iff a \cdot b \equiv c \mod m$

(2.30) $x \in \mathbb{Z}_m \setminus \{0\}$ besitzt genau dann ein multiplikatives Inverses $y \in \mathbb{Z}_m$, wenn x und m teilerfremd sind (d.h. $\mathrm{ggT}(x, m) = 1$).

(2.31) Der Restklassenring $\mathbb{Z}_m$ ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist.

(2.32) Sei $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m \mid \mathrm{ggT}(x, m) = 1\} = \{x_1, \ldots, x_{\varphi(m)}\}$ die Menge der zu m teilerfremden Zahlen. Dann gilt: $\mathbb{Z}_m^*$ ist eine Gruppe bezüglich der Multiplikation in $\mathbb{Z}_m$.

(2.33) Seien $a, m \in \mathbb{N}$ teilerfremd. Dann gilt $a^{\varphi(m)} \equiv 1 \mod m$.

(2.34) Die Gruppe der Permutationen von $\{1, \ldots, n\}$ wird mit
$S_n = S(\{1, \ldots, n\}) = \{f\colon \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid f \text{ bijektiv}\}$ bezeichnet.

(2.35) S_n wird von den Transpositionen $[a, b]$ erzeugt, d.h. $\sigma \in S_n$ lässt sich als Verknüpfung $\sigma = \tau_1 \circ \cdots \circ \tau_r$ von Transpositionen darstellen.