## Einführung

Es geht in der Einführung darum die mathematische Sprache zu erklären, die wir benutzen. Wir illustrieren dies an Beispielen, die häufig mehr physikalischer Natur sind, als mathmatischer.

# 1 Mengen

Eine Menge $M$ ist eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens von M genannt werden) zu einem Ganzen.

Diese Objekte werden die Elemente von $M$ genannt. Man schreibt z.B.

$$3 \in M.$$

Das heißt, dass die Zahl 3 ein Element von $M$ ist. Wenn das nicht der Fall ist, schreibt man $3 \notin M$.

Man nennt $N$ eine Teilmenge von $M$, wenn die Aussage $x \in N$ stets $x \in M$ zur Folge hat. Man schreibt in diesem Fall

$$N \subset M.$$

Insbesondere gilt: $M \subset M$.

Definition von Mengen: Man zählt die Elemente der Menge $M$ in geschweiften Klammern auf:

$$M = \{1, 2, 3, A, a, \omega\}$$

Die Existenz der folgenden Mengen setzen wir ohne weitere Erklärung voraus:

1. $\mathbb{N}$ die Menge der natürlichen Zahlen.

2. $\mathbb{Z}$ die Menge der ganzen Zahlen

3. $\mathbb{Q}$ die Menge der rationalen Zahlen

4. $\mathbb{R}$ die Menge der reellen Zahlen.

Teilmengen werden oft durch eine Eigenschaft beschrieben:

$M = \{n \in \mathbb{N} \mid \text{Die Dezimalentwicklung von } n \text{ enthält nur die Ziffern 1 oder 2.}\}$

$$\emptyset = \{n \in \mathbb{N} \mid n \neq n\}$$

Die letzte Menge nennt man die leere Menge. Für jede Menge $M$ gilt $\emptyset \subset M$.

**Operationen mit Mengen**
Man kann aus Mengen neue Mengen bilden:
Es seien $M$ und $N$ zwei Mengen.

1. $M \cup N$ ist die Menge der Objekte $x$, so dass $x \in M$ *oder* $x \in N$.
2. $M \cap N$ ist die Menge der Objekte $x$, so dass $x \in M$ *und* $x \in N$.
3. $M \setminus N$ ist die Menge der Objekte $x$, so dass $x \in M$ und $x \notin N$.

Beispiel: Es seien $A, B, C$ Mengen. Dann gilt:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Eine Abbildung einer Menge $M$ in eine Menge $N$ ist eine Vorschrift $f$, die jedem Element von $M$ ein Element von $N$ zuordnet. Die Menge aller Abbildungen von $M$ nach $N$ bezeichnen wir mit $\mathrm{Abb}(M, N)$. Das Symbol $f : M \to N$ besagt, dass $f$ eine Abbildung von $M$ nach $N$ ist.

Beispiel: Es sei $\mathbb{A}$ der Raum. Man fasst in als eine Menge von Punkten auf. Es sei $E$ eine Ebene im Raum und $\ell$ eine Gerade, die $E$ in genau einem Punkt schneidet. Wir definieren eine Abbildung $\pi : \mathbb{A} \to E$ wie folgt: Es sei $P \in \mathbb{A}$. Wir legen die Gerade $\ell_P$ durch $P$, welche parallel zu $\ell$ ist. Wir definieren:

$$\pi(P) = \ell_P \cap E.$$

Wir nennen $\pi$ die Parallelprojektion längs $\ell$.

Beispiel: Eine Funktion $f : \mathbb{R} \to \mathbb{R}$ ist eine Abbildung. Z.B. $f(x) = x^2$.

Es seien $M$ und $N$ zwei Mengen. Wir bezeichen mit $M \times N$ die Menge aller geordneten Paare $(m, n)$, so dass $m \in M$ und $n \in N$. Man schreibt $M^2 = M \times M$.

Eine *Klasseneinteilung* einer Menge $M$ ist eine Menge von Teilmengen $\mathcal{A}$ von $M$ mit folgenden Eigenschaften:

(1) Die Teilmengen $A \in \mathcal{A}$ sind nicht leer.

(2) Für alle $m \in M$ gibt es ein $A \in \mathcal{A}$, so dass $m \in A$

(3) Es seien $A_1 \in \mathcal{A}$ und $A_2 \in \mathcal{A}$ zwei verschiedene Teilmengen von $M$. Dann gilt
$$A_1 \cap A_2 = \emptyset.$$

Die Teilmengen $A$ nennen wir auch die Klassen. Man nennt ein Element $m \in A$ einen Repräsentanten von $A$.

Beispiel: Es sei $\mathbb{A}$ der dreidimensionale Raum. Darunter verstehen wir den euklidischen Raum, den wir aus der Anschauung oder Schule kennen. Es sei $O \in \mathbb{A}$ ein festgewählter Punkt. Es sei $M = \mathbb{A} \setminus \{O\}$. Es sei $\mathcal{A}$ die Menge der Teilmengen von $M$ die von der Form
$$g \cup \setminus \{O\}$$
sind, wobei $g$ eine Gerade des Raumes $\mathbb{A}$, die durch $O$ geht. Die Menge $\mathcal{A}$ ist eine Klasseneinteilung von $M$. Man nennt $\mathcal{A}$ die projektive Ebene.

Beispiel: Es sei $n$ eine natürliche Zahl. Für jede ganze Zahl $i$, so dass $0 \leq i \leq n-1$ betrachten wir die Menge
$$A_i = \{q \cdot n + i \mid q \in \mathbb{Z}\}.$$
$A_i$ besteht aus den ganzen Zahlen, welche bei der Division durch $n$ den Rest $i$ lassen. Die Menge
$$\mathcal{A} = \{A_0, A_1, \ldots, A_{n-1}\}$$
ist eine Klasseneinteilung der Menge $\mathbb{Z}$. Die Elemente $A_i$ nennt man die Restklassen modulo $n$.

Beispiel: Es sei $f : M \to N$ eine Abbildung. Es sei $n \in N$. Die *Faser* über $n$ dieser Abbildung ist definiert durch
$$f^{-1}(n) = \{m \in M \mid f(m) = n\}$$
Es sei $\mathcal{A}$ die Menge aller Fasern von $f$, die nicht leer sind. Dann ist $\mathcal{A}$ eine Klasseneinteilung von $M$.

Es sei umgekehrt eine Klasseneinteilung $\mathcal{A}$ einer Menge $M$ gegeben. Dann existiert zu jedem Element $m \in M$ genau eine Teilmengen $A(m) \in \mathcal{A}$, so dass

$m \in A(m)$. Die Abbildung $m \mapsto A(m)$ (lies: $m$ wird auf $A(m)$) nennt man die klassifizierende Abbildung der Klasseneinteilung:

$$\nu_{\mathcal{A}} : M \to \mathcal{A}, \quad \nu_{\mathcal{A}}(m) = A(m). \tag{1}$$

Wir fügen eine wichtige Definition ein:

**Definition 1** *Eine Abbildung $f : M \to N$ heißt* surjektiv*, wenn alle Fasern nicht leer sind. Man nennt $f$ injektiv, wenn die Fasern höchstens ein einziges Element enthalten. Man nennt $f$ bijektiv, wenn $f$ injektiv und surjektiv ist.*

Eine Relation $\mathbf{R}$ auf einer Menge $M$ ist eine Teilmenge $\mathbf{R} \subset M \times M$. Es seien $m_1, m_2 \in M$. Man schreibt

$$m_1 \sim_{\mathbf{R}} m_2,$$

wenn $(m_1, m_2) \in \mathbf{R}$ und man schreibt $m_1 \not\sim_{\mathbf{R}} m_2$, wenn das nicht der Fall ist. Oft erwähnt man die Menge $\mathbf{R}$ gar nicht, sondern sagt, dass $\sim$ eine Relation auf $M$ ist. Z.B. sind $<$, $\leq$, $>$, $geq$, $=$ Relationen auf der Menge der reellen Zahlen. Wenn $M$ eine Menge ist, so ist $\subset$ eine Relation auf der Menge der Teilmengen von $M$.

**Definition 2** *Eine Relation $\equiv$ auf einer Menge $M$ heißt eine Äquivalenzrelation, wenn folgende Eigenschaften erfüllt sind:*

*(1) Für alle $m \in M$ gilt:*

$$m \equiv m$$

*(2) Es seien $m_1, m_2 \in M$. Dann gilt:*

$$m_1 \equiv m_2 \;\Rightarrow\; m_2 \equiv m_1.$$

*(3) Es seien $m_1, m_2, m_3 \in M$. Dann gilt:*

$$m_1 \equiv m_2 \text{ und } m_2 \equiv m_3 \;\Rightarrow\; m_1 \equiv m_3.$$

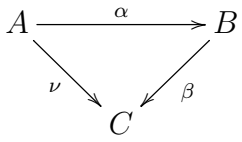
Es sei $\mathcal{A}$ eine Klasseneinteilung von $M$. Wir betrachten die Menge aller Paare $(m_1, m_2) \in M^2$, so dass ein $A \in \mathcal{A}$ existiert, so dass $m_1, m_2 \in A$. Das ist offensichtlich eine Äquivalenzrelation. Wenn man das umkehrt, sieht man, dass man jede Äquivalenzrelation aus einer Klasseneinteilung erhält.

**Kompositum von Abbildungen**

Es seien $A, B, C$ Mengen. Es seien $\alpha : A \to B$ und $\beta : B \to C$ Abbildungen. Dann definiert man das Kompositum $\nu$:

$$\nu : A \to C, \quad \nu(a) := \beta(\alpha(a)),\ a \in A.$$

Wir schreiben $\nu = \beta \circ \alpha$. Diese Beziehung drücken wir so aus: Das folgende Diagramm ist kommutativ:




Es sei $A$ eine Menge. Wir definieren die Abbildung $\mathrm{id}_A : A \to A$ durch $\mathrm{id}_A(a) := a$ für alle $a \in A$. Dann gilt für jede Abbildung $\alpha : A \to B$:

$$\alpha \circ \mathrm{id}_A = \alpha, \quad \mathrm{id}_B \circ \alpha = \alpha.$$

Schließlich betrachten wir eine weitere Abbildung $\gamma : C \to D$. Dann gilt

$$\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha.$$

Man sagt, dass das Kompositum von Abbildungen assoziativ ist.

Es sei $u : A \to B$ eine Abbildung. Wir sagen $v : B \to A$ ist eine *Umkehrabbildung* (= inverse Abbildung), wenn

$$u \circ v = \mathrm{id}_B, \quad v \circ u = \mathrm{id}_A\,. \tag{2}$$

Eine Umkehrabbildung existiert genau dann, wenn $u$ bijektiv ist. Eine Umkehrabbildung $v$ ist durch $u$ eindeutig bestimmt. Man schreibt $v = u^{-1}$.

Beispiel: Wir betrachten Bewegungen des Raumes $\mathbb{A}$. Synonym kann man Verschiebungen sagen. Das sind Abbildungen

$$U : \mathbb{A} \to \mathbb{A},$$

die Längen und Drehrichtungen erhalten. Beispiele sind Drehungen um eine Achse und Parallelverschiebungen. Vektor ist ein anderes Wort für Parallelverschiebung. Es seien $S$ und $T$ Vektoren. Dann definiert man deren Summe:

$$S + T := S \circ T, \tag{3}$$

wobei rechts das Kompositum von Abbildungen steht. Es sei $P, Q \in \mathbb{A}$. Dann gibt es einen eindeutig bestimmten Vektor $T$, so dass $T(P) = Q$. Man schreibt $T = \overrightarrow{PQ}$. Für die Gleichung $T(P) = Q$ schreibt man in der Vektorrechnung

$$P + \overrightarrow{PQ} = Q.$$

Wir kehren zur Definition (3) zurück. Wenn $P \in \mathbb{A}$ ein Punkt ist, so bilden die 4 Punkte

$$P, T(P), S(T(P)), S(P)$$

ein Parallelogramm, weil $S$ eine Parallelverschiebung ist. Daraus folgt, dass $S \circ T = T \circ S$. Nach der Definition der Summe von Vektoren gilt:

$$\overrightarrow{QR} + \overrightarrow{PQ} = \overrightarrow{PR}.$$

Die Abbildung $\mathrm{id}_{\mathbb{A}}$ nennt man den Nullvektor $\vec{0}$ (Stillstand). Weil das Kompositum von Abbildungen assoziativ ist, finden wir die folgenden Rechenregeln für Vektoren $S, T, R$:

$$\begin{gathered} T + \vec{0} = T, \quad \vec{0} + T = T \\ S + T = T + S \\ (S + T) + R = S + (T + R) \end{gathered} \tag{4}$$

Angenommen wir wählen ein Koordinatensystem von $\mathbb{A}$, dessen Ursprung in dem Punkt $O \in \mathbb{A}$ liegt. Einem Punkt $P \in \mathbb{A}$ entsprechen dann Koordinaten $x(P) = (x_1, x_2, x_3)$, wo $x_i \in \mathbb{R}$. Das ist eine bijektive Abbildung

$$\mathbb{A} \to \mathbb{R}^3.$$

Man identifiziert $\mathbb{A}$ mit $\mathbb{R}^3$, d.h. man vergisst den Unterschied zwischen einem Punkt und seinen Koordinaten. Es sei $T(O) = (v_1, v_2, v_3)$ dann gilt:

$$T((x_1, x_2, x_3)) = (x_1 + v_1, x_2 + v_2, x_3 + v_3).$$

Wir nennen $(v_1, v_2, v_3)$ die Koordinaten des Vektors $T$.

**Satz 3** *(Faktorisierungsprinzip) Es sei $\nu : M \to E$ eine surjektive Abbildung von Mengen. Es sei $f : M \to N$ eine Abbildung von Mengen, die auf den Fasern von $\nu$ konstant ist.*

*Dann existiert genau eine Abbildung $g : E \to N$, so dass folgendes Diagramm kommutativ ist:*

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ & {\scriptstyle \nu} \searrow \quad \nearrow {\scriptstyle g} & \\ & E & \end{array} \tag{5}$$

Die Voraussetzung der Satz kann man auch so formulieren: Für alle $m_1, m_2 \in M$ gilt

$$\nu(m_1) = \nu(m_2) \Rightarrow f(m_1) = f(m_2).$$

Es sei $M$ eine Menge mit einer Klasseneinteilung $\mathcal{A}$ und es sei "$\equiv$" die Äquivalenzrelation. Dann kann man das Faktorisierungsprinzip für die klassifizierende Abbildung $\nu_{\mathcal{A}} : M \to \mathcal{A}$ so formulieren:

Es sei $f : M \to N$ eine Abbildung von Mengen, so dass gilt

$$m_1 \equiv m_2 \quad \Rightarrow \quad f(m_1) = f(m_2). \tag{6}$$

Dann existiert genau eine Abbildung $g : \mathcal{A} \to N$ so dass folgendes Diagramm kommutativ ist:

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ & {\scriptstyle \nu_{\mathcal{A}}} \searrow \quad \nearrow {\scriptstyle g} & \\ & \mathcal{A} & \end{array}$$

Wenn man sagt, dass $f$ repräsentantenunabhängig definiert ist, meint man dass (6) gilt.

Es sei $\mathbb{A}$ der Raum. Es sei $V$ die Menge der Vektoren zu $\mathbb{A}$. Dann hat man eine die Abbildung

$$\begin{array}{ccc} \mathbb{A} \times \mathbb{A} & \to & V \\ (P, Q) & \longrightarrow & \overrightarrow{PQ} \end{array} \tag{7}$$

Wenn $(P, Q)$ und $(P_1, Q_1)$ zwei Punktepaare sind, so gilt

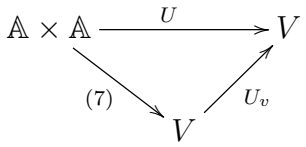
$$\overrightarrow{PQ} = \overrightarrow{P_1Q_1} \tag{8}$$

gdw. $PQQ_1P_1$ ein Parallelogeramm ist. Das ist eine Beschreibung der Äquivalenzrelation "$\equiv$", die durch die Abbildung (7) definiert wird.

Es sei $U : \mathbb{A} \to \mathbb{A}$ eine Bewegung. Dann definieren wir die Abbildung:

$$\tilde{U} : \mathbb{A} \times \mathbb{A} \to V, \quad \tilde{U}((P,Q)) := \overrightarrow{U(P)U(Q)}.$$

Angenommen $(P_1, Q_1)$ ist ein weiteres Punktepaar, so dass (8) gilt. Dann ist $U(P)\,U(Q)\,U(Q_1)\,U(P_1)$ ein Parallelogramm, weil $U$ Parallelogramme auf Parallelogramme abbildet. Folglich gilt $\overrightarrow{U(P)U(Q)} = \overrightarrow{U(P_1)U(Q_1)}$. Also ist $\tilde{U}$ auf den Fasern von (7) konstant. Folglich finden wir nach dem Faktorisierungsprinzip eine Abbildung $U_v$, so dass folgendes Diagramm kommutativ ist:




Man nennt $U_v : V \to V$ die zu $U$ assozierte Abbildung von Vektorräumen. Sie ist durch die folgende Gleichung charakterisiert:

$$U_v(\overrightarrow{PQ}) = \overrightarrow{U(P)U(Q)}. \tag{9}$$

Wenn $S$ und $T$ Vektoren sind, so gilt:

$$U_v(S+T) = U_v(S) + U_v(T), \quad U_v(\vec{0}) = \vec{0}. \tag{10}$$

Das sieht man so ein: Es sei $P \in \mathbb{A}$ ein beliebiger Punkt $P, T(P), (S+T)(P), S(P)$ ist ein Parallelogramm. Das bleibt ein Parallelogramm, wenn man die Bewegung $U$ anwendet:

$$U(P), U(T(P)), U((S+T)(P)), U(S(P)). \tag{11}$$

Aber es gilt nach Definition $U_v(S) = \overrightarrow{U(P)U(S(P))}$, $U_v(T) = \overrightarrow{U(P)U(T(P))}$. Aber die Summe der letzten beiden Vektoren erhält man, wenn man die Punkte $U(P), U(T(P)), U(S(P))$ zu einem Parallelogramm ergänzt. Das ist das Parallelogramm (11). Folglich ist die Summe $U_v(S) + U_v(T)$ gleich dem Vektor $\overrightarrow{U(P)U((S+T)(P))} = U_v(S+T)$. Damit ist (10) bewiesen.

Genauer zeigt unsere Überlegung, dass die erste Gleichung von (10) gilt, wenn $U$ ein Paar paralleler Geraden wieder auf ein Paar paralleler Geraden abbildet. Eine solche Abbildung heißt *affin*.

**Übung:** Mit Hilfe der Umkehrabbildung $U^{-1} : \mathbb{A} \to A$ zu $U$ kann man schreiben

$$U_v(T) = U \circ T \circ U^{-1}.$$

# 2 algebraische Operationen und Gruppen

Es sei $M$ eine Menge. Eine Abbildung $* : M \times M \to M$ nennen wir auch eine (algebraische) Operation. Das Bild eines Paares $(m_1, m_2) \in M^2$ bezeichen wir mit

$$m_1 * m_2.$$

Die Operationen "+", "$\cdot$", "$-$" und ":" sind uns durch den Taschenrechner geläufig.

**Definition 4** *Es sei $(M, *)$ eine Menge mit einer Operation.*
*Man nennt die Operation assoziativ, wenn für alle $m_1, m_2, m_3 \in M$*

$$m_1 * (m_2 * m_3) = (m_1 * m_2) * m_3.$$

*Man nennt die Operation kommutativ, wenn für alle $m_1, m_2 \in M$*

$$m_1 * m_2 = m_2 * m_1. \tag{12}$$

*Ein Element $e \in M$ heißt ein neutrales Element, wenn für alle $m \in M$*

$$e * m = m, \quad m * e = m$$

In der Menge $M$ gibt es höchstens ein neutrales Element bzgl. der Operation $*$.

**Definition 5** *Es sei $(M, *)$ eine Menge mit einer Operation. Wir nennen $M$ eine Gruppe, wenn gilt:*

*(1) Die Operation ist assoziativ.*

*(2) Es gibt ein neutrales Element $e$.*

*(3) Zu jedem Element $m \in M$ gibt es ein Element $m'$, so dass*

$$m * m' = e, \quad m' * m = e.$$

Wenn ein Element $m'$ existiert, so heißt $m'$ ein inverses Element zu $m$. Wenn $m''$ ein weiteres inverses Element zu $m$ ist, so ergibt sich aus der Berechnung von $m' * m * m''$, dass $m = m''$.

Es sei $(\mathbb{Z}, +)$ die Menge der ganzen Zahlen mit der gewöhnlichen Addition als Operation. Das ist eine Gruppe. Das neutrale Element ist die Zahl 0. Wenn $g \in \mathbb{Z}$, so ist $(-g)$ das inverse Element. Genauso hat man die Gruppen $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$.

Die Menge der Vektoren $V$ des Raumes $\mathbb{A}$ ist eine Gruppe bezüglich der Addition "+" von Vektoren. Der Nullvektor $\vec{0}$ ist das neutrale Element (vgl. (4)). Wenn $T = \overrightarrow{PQ}$, so ist $(-T) := \overrightarrow{QP}$ das inverse Element.

Diese Gruppen sind kommutativ, d.h. die Operation erfüllt (12). Man nennt kommutative Gruppen auch abelsch.

Es sei $M$ eine Menge. Eine Permutation von $M$ ist eine bijektive Abbildung $\sigma : M \to M$. Wir bezeichnen die Menge der Permutationen von $M$ mit $\mathrm{Aut}(M)$. Das Kompositum von Abbildungen

$$\sigma \circ \tau, \quad \sigma, \tau \in \mathrm{Aut}(M),$$

definiert eine Gruppe $(\mathrm{Aut}(M), \circ)$. Das neutrale Element ist die Abbildung $\mathrm{id}_M$ und das inverse Element ist die Umkehrabbildung (2).

Es sei $n$ eine natürliche Zahl. Es sei $M = \{1, 2, \ldots, n\}$. Dann bezeichnet man die Gruppe $(\mathrm{Aut}(M), \circ)$ auch mit $\mathcal{S}_n$. Man nennt $\mathcal{S}_n$ die symmetrische Gruppe. Man schreibt eine Permutation oft in Form einer Tabelle:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 5 & 2 & 1 \end{pmatrix}. \tag{13}$$

Unter der Zahl $i$ steht in dieser Tabelle die Zahl $\sigma(i)$, z.B. $\sigma(5) = 2$.

# 3 Die Gruppe der ganzen Zahlen

Die Gruppe $(\mathbb{Z}, +)$ bezeichen wir im folgenden einfach mit $\mathbb{Z}$.

**Definition 6** *Es sei $(M, *)$ eine Gruppe. Eine Untergruppe $N \subset M$ ist eine Teilmenge, so dass für alle $n_1, n_2 \in N$ gilt, dass $n_1 * n_2 \in N$ und so dass $(N, *)$ eine Gruppe ist.*

Es sei $e_N$ das neutrale Element von $(N, *)$. Es sei $e$ das neutrale Element von $M$. Es sei $e'_N \in M$, das inverse Element von $e_N$ in der Gruppe $M$. Dann gilt:

$$(e_N * e_N) * e'_N = e_N * e'_N = e \quad e_N * (e_N * e'_N) = e_N * e = e_N$$

Also gilt notwendigerweise $e_N = e$, d.h. eine Untergruppe muss das neutrale Element von $M$ enthalten. Es sei $n \in N$ und $n'$ das inverse Element in der Gruppe $N$. Es folgt, dass dies auch das inverse Element in der Gruppe $M$ ist.

Es sei $n\mathbb{Z}$, $n \geq 0$. Wir setzen

$$\mathbb{Z}n := \{g \cdot n \mid g \in \mathbb{Z}\} \subset \mathbb{Z}. \tag{14}$$

Diese Teilmengen sind Untergruppen von $\mathbb{Z}$.

**Satz 7** *Jede Untergruppe von $\mathbb{Z}$ in von der Form (14)*

Wir beweisen diesen Satz mit dem Prinzip der vollständigen Induktion:

**Prinzip:** In jeder nichtleeren Teilmenge von $\mathbb{N}$ gibt es ein kleinstes Element.

**Beweis von Satz 7:** Es sei $N \subset \mathbb{Z}$ eine Untergruppe. Wenn $N = \{0\}$, so ist die Behauptung klar. Es sei $u \in N$, $u \neq 0$. Dann gilt $u \in N \cap \mathbb{N}$ oder $-u \in N \cap \mathbb{N}$. Also gilt $\mathbb{N} \cap N \neq \emptyset$. Es sei $n$ das kleinste Element in $N \cap \mathbb{N}$. Dann gilt $\mathbb{Z}n \subset N$. In der Tat, jedes Element $gn \in \mathbb{Z}n$ ist von der Form

$$n + n + \ldots + n, \quad \text{oder} \quad (-n) + (-n) + \ldots + (-n).$$

Diese Elemente gehören zu $N$, weil $N$ eine Untergruppe ist.

Wir beweisen, dass $\mathbb{Z}n = N$. Es genügt zu zeigen, dass $N \cap \mathbb{N} \subset \mathbb{Z}n$. Angenommen, das ist nicht der Fall. Dann gibt es nach vollständiger Induktion ein kleinstes Element $m$ in der Menge aller Elemente von $N \cap \mathbb{N}$, die nicht in $\mathbb{Z}n$ liegen. Nach der Wahl von $n$ folgt $n < m$. Man findet $m + (-n) \in N \cap \mathbb{N}$ und $m + (-n) \notin \mathbb{Z}n$. Das ist eine Widerspruch zur Minimalität von $m$. *Q.E.D.*

Es seien $t, g \in \mathbb{Z}$. Wir sagen $t$ ist ein Teiler von $g$, wenn eine ganze Zahl $q$ existiert, so dass $g = qt$. Wir schreiben $t|g$ oder äquivalent dazu $g \in \mathbb{Z}t$.

**Satz 8** *Es seien $a, b$ ganze Zahlen, die beide von 0 verschieden sind. Dann gibt es genau eine natürliche Zahl $d$ mit folgenden Eigenschaften:*

*(1) $d|a$ und $d|b$.*

*(2) Wenn $t$ eine ganze Zahl ist, so dass $t|a$ und $t|b$, so gilt $t|d$.*

*Es gibt Zahlen $x, y \in \mathbb{Z}$, so dass*

$$d = xa + yb.$$

**Beweis:** Wir betrachten die Menge $N = \{xa + yb \mid x, y \in \mathbb{Z}\}$. Das ist eine Untergruppe $N \subset \mathbb{Z}$. Aus Satz folgt, dass eine natürliche Zahl $d$ existiert, so dass $N = \mathbb{Z}d$. Da insbesondere $a, b \in \mathbb{Z}d$ ist die Eigenschaft (1) erfüllt. Andererseits gilt wegen $d \in N$ eine Gleichung

$$d = xa + yb.$$

Daraus folgt die Eigenschaft (2). Die Eindeutigkeit von $d$ ist klar. *Q.E.D.* Man nennt $d$ den größten gemeisamen Teiler von $a$ und $b$ und schreibt

$$d = \text{g. g. T.}(a, b).$$

**Korollar 9** *Es seien $a, b \in \mathbb{Z}$ beide von 0 verschieden. Es sei $1 = \text{g. g. T.}(a, b)$. Es sei $u \in \mathbb{Z}$. Dann gilt*

$$a|ub \quad \Rightarrow \quad a|u.$$

**Beweis:** Man multipliziert die Gleichung $1 = xa + yb$ mit $u$. *Q.E.D.*

Wenn $\text{g. g. T.}(a, b) = 1$, so nennt man $a$ und $b$ *teilerfremd*.

Wenn $p$ eine Primzahl ist, so gilt für beliebige $a, b \in \mathbb{Z}$:

$$p|ab \quad \Rightarrow \quad p|a \text{ oder } p|b.$$

Daraus folgt, dass man jede natürliche Zahl eindeutig als Produkt von Primzahlen schreiben kann.

**Definition 10** *Es seien $(M, *)$ und $(N, \bullet)$ zwei Mengen mit Operationen. Ein Homomorphismus $f : M \to N$ ist eine Abbildung, so dass*

$$f(m_1 * m_2) = f(m_1) \bullet f(m_2), \quad m_1, m_2 \in M.$$

Folgendes ist extrem nützlich:

**Lemma 11** *Es sei $(M, *)$ eine Gruppe mit dem neutralen Element $e$. Es sei $f : M \to N$ ein Homomorphismus wie in Definition 10.*

*Dann ist die Abbildung $f$ genau dann injektiv, wenn die Faser über $f(e) \in N$ gilt*

$$f^{-1}(f(e)) = \{e\}. \tag{15}$$

**Beweis**: Wenn $f$ injektiv ist, so enthält die Faser $f^{-1}(f(e))$ nach Definition nur ein Element und muss folglich mit $\{e\}$ übereinstimmen.

Wir zeigen die Umkehrung: Es seien $m_1, m_2 \in M$, so dass $f(m_1) = f(m_2)$. Wir müssen $m_1 = m_2$ beweisen. Wir finden $m' \in M$, so dass $m' * m_1 = e = m_1 * m'$. Dann gilt:

$$f(e) = f(m' * m_1) = f(m') \bullet f(m_1) = f(m') \bullet f(m_2) = f(m' * m_2).$$

Dann folgt aus (15), dass $e = m' * m_2$. Wenn man von links mit $m_1$ multipliziert erhält man $m_1 = m_2$. *Q.E.D.*

Bemerkung: Wenn in der Definition 10 $(M, *)$ und $(N, \bullet)$ Gruppen sind, so folgt, dass $f(e)$ das neutrale Element von $N$ ist. ($e$ ist das neutrale Element von $M$.)

Es sei $n \in \mathbb{N}$. Es seien

$$A_0, A_1, \ldots, A_{n-1} \tag{16}$$

die Restklassen modulo $n$. Man definiert die Summe von zwei Restklassen $A_i$ und $A_j$ wie folgt. Man wählt beliebig ganze Zahlen $a_i \in A_i$ und $a_j \in A_j$. Dann existiert $A_k$, so dass $a_i + a_j \in A_k$. Damit diese Definition sinnvoll ist muss man zeigen, dass $A_k$ unabhängig von der Wahl von $a_i$ und $a_j$ ist. Mit Hilfe der Äquivalenzrelation "$\equiv \pmod n$" zur Klasseneinteilung (16) können wir die Unabhängigkeit so formulieren:

$$a_i \equiv a_i' \pmod n \text{ und } a_j \equiv a_j' \pmod n \quad \Rightarrow \quad a_i + a_j \equiv a_i' + a_j' \pmod n. \tag{17}$$

Jetzt können wir definieren $A_i + A_j := A_k$. Dadurch erhält man eine Operation "+" auf der Klasseneinteilung

$$\mathbb{Z}/n\mathbb{Z} := \{A_0, A_1, \ldots, A_{n-1}\}.$$

Diese Operation "+" ist dadurch charakterisiert, dass die klassifizierende Abbildung

$$\nu : (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$$

ein Homomorphismus ist.

Man kann die Gleichung (17) nach dem Faktorisierungsprinzip auch so interpretieren: Es gibt eine Abbildung $\mathbf{s} : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, so dass folgendes Diagramm kommutativ ist:

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \\ {\scriptstyle \nu\times\nu}\downarrow & & \downarrow{\scriptstyle \nu} \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\mathbf{s}} & \mathbb{Z}/n\mathbb{Z} \end{array} \tag{18}$$

Variante: Man kann auf $\mathbb{Z}$ die Multiplikation "$\cdot$" als Operation nehmen. Man kann zeigen, dass genau eine Operation "$\cdot$" auf $\mathbb{Z}/n\mathbb{Z}$ existiert, so dass

$$\nu : (\mathbb{Z}, \cdot) \to (\mathbb{Z}/n\mathbb{Z}, \cdot)$$

ein Homomorphismus ist.

Insbesondere haben wir für alle $m \in \mathbb{Z}$ eine Abbildung

$$\begin{array}{rccc} m: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & a(\mathrm{mod}\, n) & \mapsto & ma(\mathrm{mod}\, n). \end{array}$$

Wenn g. g. T.$(m, n) = 1$, so ist die letzte Abbildung bijektiv.

# 4 Vektoren und lineare Abbildungen

Es sei $\mathbb{A}$ der Raum. Es sei $V$ der Raum der Vektoren von $\mathbb{A}$.

Es sei $T = \overrightarrow{PQ} \neq \vec{0}$. Es sei $\lambda \in \mathbb{R}$, $\lambda \geq 0$. Es sei $R$ der Punkt auf dem Strahl $s$, der in $P$ beginnt und durch $Q$ verläuft, so dass $|PR| = \lambda |PQ|$. Dann definiert man $\lambda T := \overrightarrow{PR}$ und nennt das die Streckung von $T$ um den Faktor $\lambda$. Wenn $\lambda$ negativ ist, so setzt man $\mu = -\lambda$ und definiert $\lambda T = -(\mu v)$. Wenn $T$ der Nullvektor ist, so definiert man

$$\lambda \vec{0} := \vec{0}.$$

Man nennt $\lambda T$ die *Streckung* von $T$ um den Faktor $\lambda$.

Man hat für $n \in \mathbb{N}$:

$$nT = T + T + \ldots + T, \quad n \text{ Summanden.}$$

Genauso kann man $(1/n)T$ als den eindeutig bestimmten Vektor erhalten, so dass

$$T = (1/n)T + (1/n)T + \ldots + (1/n)T, \quad n \text{ Summanden.}$$

Auf diese Weise kann man die Streckung mit einem Faktor $\lambda \in \mathbb{Q}$ definieren, ohne den Abstand von Punkten zu erwähnen.

Wenn man ein Koordinatensystem wählt und $T$ die Koordinaten $(v_1, v_2, v_3)$ hat, so hat $\lambda T$ die Koordinaten $(\lambda v_1, \lambda v_2, \lambda v_3)$.

Es seien $T_1$, $T_2$, $T_3$ drei Vektoren. Wir wählen einen festen Punkt $O$. Die Vektoren heißen *linear unabhängig*, wenn die Punkte

$$O, O + T_1, O + T_2, O + T_3.$$

nicht in einer Ebene liegen. Die Definition von linear unabhängig hängt nicht von der Wahl $O$ ab. Wenn $T$ ein beliebieger Vektor ist, so gibt es eindeutig bestimmte Zahlen $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$, so dass

$$T = \lambda_1 T_1 + \lambda_2 T_2 + \lambda_3 T_3 \tag{19}$$

Genauer bedeutet das: Wenn $S$ ein weiterer Vektor ist:

$$S = \mu_1 T_1 + \mu_2 T_2 + \mu_3 T_3$$

Dann gilt

$$S = T \qquad \Leftrightarrow \quad \mu_1 = \lambda_1 \text{ und } \mu_2 = \lambda_2 \text{ und } \mu_3 = \lambda_3. \tag{20}$$

Wir nennen $\lambda_1, \lambda_2, \lambda_3$ die *Koordinaten* des Vektors $T$ bezüglich $T_1, T_2, T_3$.

Es seien $A, B, B', C, C'$ verschiedene Punkte, so dass $A, B, B'$ auf einer Geraden liegen und $A, C, C'$ auf einer anderen Geraden, und so dass die Geraden $BC$ und $B'C'$ parallel sind. Das ist die Situation des Strahlensatzes. Es sei $\lambda\overrightarrow{AB} = \overrightarrow{AB'}$. Dann gilt nach den Strahlensätzen

$$\overrightarrow{AC'} = \lambda\overrightarrow{AC}, \quad \overrightarrow{B'C'} = \lambda\overrightarrow{BC}.$$

Wir erhalten die Gleichung:

$$\lambda(\overrightarrow{AC} - \overrightarrow{AB}) = \lambda\overrightarrow{BC} = \overrightarrow{B'C'} = \overrightarrow{AC'} - \overrightarrow{AB'} = \lambda\overrightarrow{AC} - \lambda\overrightarrow{AB}.$$

Wir setzen $T = \overrightarrow{AC} - \overrightarrow{AB}$ und $S = \overrightarrow{AB}$. Dann erhalten wir das Distributivgesetz der Vektorrechnung:

$$\lambda T + \lambda S = \lambda(S + T).$$

Umgekehrt folgen aus dieser Gleichung die Strahlensätze.

Aus der Definition der Streckung eines Vektors folgt:

$$(\lambda + \mu)T = \lambda T + \mu T$$

Für die Summe der Vektoren $T$ und $S$ aus (19) und (20) ergibt sich daher

$$T + S = (\lambda_1 + \mu_1)T_1 + (\lambda_2 + \mu_2)T_2 + (\lambda_3 + \mu_3)T_3.$$

Es sei $U : \mathbb{A} \to \mathbb{A}$ eine Bewegung und $U_v : V \to V$ die assozierte Abbildung auf dem Vektorraum $V$ (siehe: (9). Dann gilt

$$U_v(\lambda T) = \lambda U_v(T). \tag{21}$$

**Definition 12** *Man nennt eine Abbildung $\alpha : V \to V$ linear, wenn*

*(1)* $\alpha(\vec{0}) = \vec{0}$

*(2) Für alle Vektoren $S, T \in V$ gilt*

$$\alpha(S + T) = \alpha(S) + \alpha(T).$$

*(3) Für alle Vektoren $T \in V$ und alle $\lambda \in \mathbb{R}$ gilt:*

$$\alpha(\lambda T) = \lambda\alpha(T).$$

Es sei $U : \mathbb{A} \to \mathbb{A}$ eine Drehung. Dann ist nach (21) und (10) die Abbildung $U_v : V \to V$ linear.

Eine lineare Abbildung $\alpha : V \to V$, kann man durch eine Matrix beschreiben. Man wählt linear unabhängige Vektoren $T_1, T_2, T_3$ wie oben. Dann findet man $a_{ij} \in \mathbb{R}$, so dass

$$\alpha(T_j) = a_{1j}T_1 + a_{2j}T_2 + a_{3j}T_3, \quad j = 1, 2, 3. \tag{22}$$

Man nennt die folgende Liste von reellen Zahlen

$$\text{Matrix } (\alpha) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \tag{23}$$

die Matrix der linearen Abbildung $\alpha$ bezüglich $T_1, T_2, T_3$.

In dem Spezialfall $\alpha = \mathrm{id}_V$ erhalten wir die Matrix:

$$\text{Matrix } (\mathrm{id}_V) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Es sei $\alpha$ wieder eine beliebige lineare Abbildung. Es sei $T$ ein beliebiger Vektor, den wir in der Form (19). Die Koordinaten $\lambda'_i$ von $\alpha(T)$ sind definiert durch die Gleichung:

$$\alpha(T) = \lambda'_1 T_1 + \lambda'_2 T_2 + \lambda'_3 T_3. \tag{24}$$

Wir können die Koordinaten $\lambda_i'$ berechnen: Da $\alpha$ linear ist, finden wir aus (19)

$$\alpha(T) = \lambda_1\alpha(T_1) + \lambda_2\alpha(T_2) + \lambda_3\alpha(T_3).$$

Wenn wir für $\alpha(T_j)$ die Gleichungen (22) einsetzen und (20) verwenden, sehen wir das wir die Koordinaten $\lambda_i'$ wie folgt erhalten:

$$\begin{aligned} \lambda_1' &= a_{11}\lambda_1 + a_{12}\lambda_2 + a_{13}\lambda_3 \\ \lambda_2' &= a_{21}\lambda_1 + a_{22}\lambda_2 + a_{23}\lambda_3 \\ \lambda_3' &= a_{31}\lambda_1 + a_{32}\lambda_2 + a_{33}\lambda_3 \end{aligned} \tag{25}$$

Man schreibt diese Gleichungen symbolisch

$$\begin{pmatrix} \lambda_1' \\ \lambda_2' \\ \lambda_3' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \tag{26}$$

Die Listen, die aus einer Spalte bestehen nennt man Spaltenvektoren:

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \tag{27}$$

Man sagt, dass sich die linke Seite von (26) aus der Multiplikation der Matrix (23) mit dem Spaltenvektor (27) ergibt.

Wir betrachten eine weitere lineare Abbildung $\beta : V \to V$. Wir schreiben die Matrix von $\beta$:

$$\text{Matrix } (\beta) = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \tag{28}$$

Wir können die Matrix $\beta \circ \alpha$ berechnen:

$$\text{Matrix } (\beta \circ \alpha) = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} \tag{29}$$

Dazu wenden wir auf die Gleichung (26) die Abbildung $\beta$ an. Daraus sieht man, dass man die erste Spalte der Matrix (29) erhält, in dem man die Matrix (28) mit der ersten Spalte der Matrix (23) multipliziert. Die nächste

Spalte von (29) bekommt man, wenn man mit der zweiten Spalte von (23) multipliziert. Wir schreiben für diese Matrixmultiplikation:

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} \tag{30}$$

Als Beispiel bestimmen wir die Matrix einer Drehung bezüglich eines rechtwinkligen Koordinatensystems. Anstelle des Raumes $\mathbb{A}$ betrachten wie eine Ebene $\mathbb{E}$. Wir wählen einen Ursprung $O \in \mathbb{E}$ und ein rechtwinkliges Koordinatensystem von $\mathbb{E}$ mit diesem Ursprung.

Die Menge aller Vektoren $\overrightarrow{OP}$, so dass $P \in \mathbb{E}$ ist der Vektorraum $W$ der Parallelverschiebungen von $\mathbb{E}$.

Es sei $U(\phi) : E \to E$ die Drehung um den Punkt $O$ und den Drehwinkel $\phi$. Es sei $U_v(\phi) : W \to W$ die Drehung der Vektoren.

Es sei $T_1$ der Vektor mit den Koordinaten $(1, 0)$ und $T_2$ der Vektor mit den Koordinaten $(0, 1)$. Es sei $P$ der Punkt mit den Koordinaten $(x, y)$ und es sei $T = \overrightarrow{OP}$. Dann gilt:

$$T = xT_1 + yT_2.$$

Dann gilt

$$U_v(\phi)(T_1) = \cos\phi T_1 + \sin\phi T_2$$

Diese Gleichung ist gerade die Definition der Winkelfunktionen sin und cos. Daraus folgt

$$U_v(\phi)(T_2) = -\sin\phi T_1 + \cos\phi T_2.$$

Also sieht die Matrix der Drehung $U_v(\phi)$ wie folgt aus:

$$\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}. \tag{31}$$

Es sei $U(\psi)$ die Drehung um der Winkel $\psi$. Dann gilt:

$$U(\psi) \circ U(\phi) = U(\psi + \phi)$$

Daraus ergibt sich für die Abbildungen des Vektorraums $W$:

$$U_v(\psi) \circ U_v(\phi) = U_v(\psi + \phi).$$

Nach der Regel (30) für die Matrix eines Kompositums von linearen Abbildungen finden wir:

$$\begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} = \begin{pmatrix} \cos(\psi+\phi) & -\sin(\psi+\phi) \\ \sin(\psi+\phi) & \cos(\psi+\phi) \end{pmatrix}.$$

Wenn man die Matrixmultiplikation ausführt erhält man die Additionstheoreme für die Funktionen sin and cos.

# 5 Polynome

Es sei $K = \mathbb{Q}$ oder $K = \mathbb{R}$.

**Definition 13** *Es sei $F : K \to K$ eine Abbildung. Man nennt $F$ ein Polynomfunktion, wenn eine ganze Zahl $n \geq 0$ und Elemente $a_0, a_1, \ldots, a_n$ existieren, so dass für alle $x \in K$*

$$F(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0. \tag{32}$$

Es ist klar, dass das Produkt und die Summe von zwei Polynomfunktionen wieder eine Polynomfunktion ist. Den Ausdruck auf der rechten Seite von (32) nennt man ein Polynom, also eine Regel nach der man eine Polynomfunktion berechnen kann.

Als Beispiel betrachten wir Polynomfunktion $G$, und $I$, die gegeben sind durch

$$G(x) = b_{n-1} x^{n-1} + \ldots + b_1 x + b_0, \quad I(x) = x - u, \tag{33}$$

wobei $b_0, \ldots, b_{n-1} \in K$ und $u \in K$. Dann erhalten wir die Funktion $G(x) \cdot I(x)$ in der Form:

$$G(x)I(x) = b_{n-1} x^n + (b_{n-2} - u b_{n-1}) x^{n-1} + \ldots + (b_0 - u b_1) x - u b_0. \tag{34}$$

Eine Nullstelle einer Polynomfunktion $F$ ist ein $u \in K$, so dass $F(u) = 0$.

**Satz 14** *Es sei die Polynomfunktion $F(x)$ durch den Ausdruck auf der rechten Seite von (32) gegeben. Es sei $a_n \neq 0$, wobei $n \geq 0$. Dann hat $F$ höchstens $n$ verschiedene Nullstellen.*

**Beweis:** Es sei $u \in K$ eine Nulstelle von $F$. Wir behaupten, dass es Elemente $b_0, \ldots, b_{n-1}$ gibt, die Lösungen der folgenden Gleichungen sind

$$\begin{array}{l} a_n = b_{n-1},\ a_{n-1} = b_{n-2} - ub_{n-1},\ \ldots\ a_1 = b_0 - ub_1 \\ a_0 = -ub_0. \end{array} \tag{35}$$

In der Tat, aus der ersten Zeile von Gleichungen, lassen sich die Elemente $b_{n-1}, \ldots, b_0$ eindeutig berechnen, so dass diese Gleichungen erfüllt sind. Wir müssen beweisen, dass dann auch die letzte Gleichung erfüllt ist. Wenn man die Gleichungen der ersten Zeile ineinander einsetzt ergibt sich:

$$\begin{aligned} b_0 &= a_1 + ub_1 = a_1 + ua_2 + u^2 b_2 = \ldots \\ &= a_1 + ua_2 + u^2 a_3 + \ldots u^{n-1} a_n. \end{aligned}$$

Also ist die letzte Gleichung $a_0 + ub_0 = 0$ von (35) äquivalent mit $F(u) = 0$.

Wenn wir diese Koeffizienten $b_i$ in (33) nehmen, so erhalten wir $F(x) = G(x) \cdot I(x)$. Wenn $u'$ eine Nullstelle von $F$ ist, so dass $u' \neq u$, so gilt $I(u') = (u' - u) \neq 0$. Da $F(u') = G(u')I(u')$ muss $u'$ eine Nullstelle von $G$ sein. Wir haben $b_{n-1} = a_n \neq 0$. Nach Induktion dürfen wir daher annehmen, dass $G$ weniger als $n - 1$ verschiedene Nullstellen hat. Daraus folgt die Behauptung. *Q.E.D.*

**Korollar 15** *(Identitätssatz für Polynome). Es sei $F : K \to K$ eine Polynomfunktion. Es seien $a_n, \ldots, a_0, b_n, \ldots, b_0 \in K$, so dass wir $F(x)$ nach den folgenden beiden Regeln berechnen können:*

$$\begin{aligned} F(x) &= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \\ F(x) &= b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0. \end{aligned}$$

*Dann gilt $a_i = b_i$ für $0 \leq i \leq n$.*

**Beweis:** Die Differenz der beiden Audrücke für $F(x)$ hätte unendlich viele Nullstellen. Deshlb folgt die Behauptung aus dem letzten Satz. *Q.E.D.*

Das bedeutet, dass die Koeffizienten $a_i \in K$ auf der rechten Seite von (32) durch die Abbildung $F$ eindeutig bestimmt sind, wenn man einmal davon absieht, dass man auf der rechten Seite Terme der Form $0x^m$ mit $m > n$ hinzufügen kann, ohne an $F$ etwas zu ändern.

Eine Polynomfunktion $F$ bestimmt also den Ausdruck auf der rechten Seite auf (32) eindeutig. Deshalb bezeichnen wir eine Polynomfunktion im folgenden auch einfach als Polynom.

Es sei $F \neq 0$ ein Polynom. Dann hat $F$ eine eindeutige Darstellung:

$$F(x) = c_d x^d + c_{d-1} x^{d-1} + \ldots + c_1 x + c_0, \tag{36}$$

wobei $c_d, \ldots, c_0 \in K$ und $c_d \neq 0$. Man nennt $d$ den Grad des Polynoms und schreibt $d = \deg F$. Wenn $F$ das Nullpolynom ist, setzen wie $\deg F = -\infty$. Wenn $G$ ein weiteres Polynom ist, so ergibt sich unmittelbar:

$$\deg(F \cdot G) = \deg F + \deg G, \quad \deg(F + G) \leq \max\{\deg F, \deg G\}. \tag{37}$$

**Korollar 16** *Es seien $F$ und $G$ Polynome, so dass $F \cdot G = 0$. Dann gilt $F = 0$ oder $G = 0$.*

Das folgt aus (37).

**Satz 17** *(Division mit Rest) Es sei $F \neq 0$ ein Polynom von Grad $d$. Es sei $G$ ein Polynom.*

*Dann existieren Polynome $Q$ und $P$, so dass $\deg P < d$ und $\deg Q \leq \deg G - d$ und*

$$G = Q \cdot F + P.$$

**Beweis:** Wenn $\deg G < d$, so kann man $Q = 0$ nehmen. Wir schreiben $F$ in der Form (36) und $G$ wie folgt:

$$G(x) = b_e x^e + b_{e-1} x^{e-1} + \ldots + b_1 x + b_0,$$

wobei $e = \deg G \geq d$. Wir betrachten, das Polynom

$$G_1 = G - (b_e/c_d) x^{e-d} F.$$

In dieser Formel und im weiteren ist $x^0 := 1$. Dann gilt $\deg G_1 < e$ und wir können Induktion anwenden. *Q.E.D.*

Die folgende Korollare haben wir schon bewiesen bevor wir den Begriff Grad (= deg) hatten.

**Korollar 18** *Es sei $F \neq 0$ ein Polynom vom Grad $d > 0$. Es sei $u \in K$, so dass $F(u) = 0$. Dann gibt es ein Polynom $Q$, so dass $\deg Q = d - 1$ und so dass*

$$F(x) = (x - u) \cdot Q(x), \quad \textit{für alle } x \in K.$$

Ein $u \in K$, so dass $G(u) = 0$, nennt man eine Nullstelle von $G$.

**Korollar 19** *Es sei $G \neq 0$ ein Polynom vom Grad $e \geq 0$. Dann besitzt $G$ höchstens $e$ verschiedene Nullstellen.*

Es sei $K[x]$ die Menge aller Polynome. Das ist eine Gruppe bezüglich der Addidion "+" von Polynomen.

**Definition 20** *Eine Teilmenge $\mathfrak{a} \subset K[x]$ nennen wir ein Ideal, wenn $\mathfrak{a}$ eine Untergrupe bezüglich "+" von $K[x]$ ist, und wenn gilt:*

$$G \in K[x],\ P \in \mathfrak{a} \quad \Rightarrow \quad G \cdot P \in \mathfrak{a}.$$

Wenn $F \in K[x]$ ein Polynom ist, so definiert man

$$K[x]F = \{G \cdot F \mid G \in K[x]\}$$

Diese Menge ist offensichtlich ein Ideal. Man nennt Ideale dieser Form Hauptideale. Für $H \in K[x]F$ schreibt man auch $F|H$ ($F$ teilt $H$).

**Satz 21** *(Hauptidealsatz) Jedes Ideal $\mathfrak{a} \subset K[x]$ ist ein Hauptideal.*

**Beweis:** Man kann $\mathfrak{a} \neq 0$. Dann gibt es eine Polynom $F \neq 0$, $F \in \mathfrak{a}$ welches minimalen Grad hat. Nach der Division mit Rest folgt $\mathfrak{a} = K[x]F$. *Q.E.D.*

Wir nennen ein Polynom $F$ (32) unitär, wenn $F \neq 0$ und wenn $a_n = 1$.

**Korollar 22** *Es seien $F$ und $G$ von $0$ verschiedene Polynome. Dann gibt es genau ein unitäres Polynom $D$ mit den folgenden Eigenschaften:*

*(1) $D|F$ und $D|G$.*

*(2) Wenn $H$ ein Polynom ist, so dass $H|F$ und $H|G$, so gilt $H|D$.*

*Es gibt Polynome $P, Q \in K[x]$, so dass*

$$D = P \cdot F + Q \cdot G.$$

Man nennt ein unitäres Polynom $P$ vom Grad $d \geq 1$ ein Primpolynom, wenn es kein Polynom $H$ gibt, so dass $d > \deg H \geq 1$ gibt, so dass $H|F$. Insbesondere ist jedes unitäre Polynom vom Grad 1 ein Primpolynom. In Analogie zur Primzerlegung ganzer Zahlen findet man:

**Satz 23** *Es sei $F \neq 0$ ein Polynom. Dann kann man $F$ bis auf die Reihenfolge der Faktoren in eindeutiger Weise schreiben:*

$$F = a \cdot P_1 \cdot \ldots \cdot P_r,$$

*wobei $a \in K$ und $P_1, \ldots, P_r$ Primpolynome sind.*

Bemerkung: Gauß hat in seiner Dissertation bewiesen: Es sei $P \in \mathbb{R}[x]$ ein Primpolynom. Dann gilt: $\deg P \leq 2$. Man hat das den Fundamentalsatz der Algebra genannt.

Die Polynome $K[x]$ sind mit zwei Operationen $+$ und $\cdot$ versehen.

**Definition 24** *Ein Ring $(R, +, \cdot)$ ist eine Menge, die mit zwei Operationen versehen ist, so dass gilt:*

*1) $(R, +)$ ist eine kommutative Gruppe.*

*2) $(R, \cdot)$ ist eine assoziative Operation mit einem neutralen Element.*

*3) Für alle $a, b, c \in R$ gilt*

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c), \quad c \cdot (a + b) = (c \cdot a) + (c \cdot b).$$

In einem Ring schreibt man $0_R$ für das neutrale Element von $(R, +)$ und $1_R$ für das neutrale Element von $(R, \cdot)$. Wenn $r \in R$, so bezeichnet man mit $(-r)$ das inverse Element von $r$ bezüglich der Operation $+$. Es gilt:

$$(-1) \cdot a = (-a) = a \cdot (-1).$$

Wenn zusätzlich die Operation $\cdot$ kommutativ ist, so redet man von einem kommutativen Ring.

Beispiele: $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}[x], \mathbb{R}[x]$ sind kommutative Ringe. Die Menge $\mathbb{Z}[x]$ aller Polynome, deren Koeffizienten ganzzahlig sind, ist mit den Operationen $+$ und $\cdot$ ebenfalls ein Ring.

Wir betrachten jetzt Polynome in mehreren Variablen. Es sei $n > 0$ eine natürliche Zahl. Wir bezeichen mit $\mathbb{Z}^n_{\geq 0}$ die Menge allen Folgen ganzer Zahlen $(t_1, \ldots, t_n)$, wobei $t_i \geq 0$.

Eine Funktion $F : K^n \to K$ heißt Polynomfunktion, wenn es in der folgenden Form berechnen kann: Es gibt Elemente $a_{t_1,\ldots,t_n} \in K$, für alle $(t_1, \ldots, t_n) \in \mathbb{Z}^n_{\geq 0}$, so dass $a_{(t_1,\ldots,t_n)} = 0$ bis auf endlich viele der $(t_1, \ldots, t_n)$. Aus diesen Elementen erhält man die Funktion $F$ wie folgt:

$$F(x_1, x_2, \ldots, x_n) = \sum_{(t_1,\ldots,t_n) \in \mathbb{Z}^n_{\geq 0}} a_{t_1,\ldots,t_n} x_1^{t_1} x_2^{t_2} \cdot \ldots \cdot x_n^{t_n}. \tag{38}$$

**Satz 25** *(Identitätssatz für Polynome). Zwei Polynomfunktionen seien durch die folgenden Rechenregeln gegben:*

$$\begin{aligned} F(x_1, x_2, \ldots, x_n) &= \sum_{(t_1,\ldots,t_n)\in\mathbb{Z}^n_{\geq 0}} a_{t_1,\ldots,t_n} x_1^{t_1} x_2^{t_2} \cdot \ldots \cdot x_n^{t_n}, \\ G(x_1, x_2, \ldots, x_n) &= \sum_{(t_1,\ldots,t_n)\in\mathbb{Z}^n_{\geq 0}} b_{t_1,\ldots,t_n} x_1^{t_1} x_2^{t_2} \cdot \ldots \cdot x_n^{t_n} \end{aligned} \tag{39}$$

*Angenommen es gibt eine unendliche Menge $A \subset K$, so dass für alle $(x_1, \ldots, x_n) \in A^n$*

$$F(x_1, \ldots, x_n) = G(x_1, \ldots, x_n).$$

*Dann gilt $a_{t_1,\ldots,t_n} = b_{t_1,\ldots,t_n}$ für alle $(t_1, \ldots, t_n) \in \mathbb{Z}^n_{\geq 0}$.*

**Beweis:** Wenn man die beiden Gleichnungen (39) voneinander subtrahiert, so sieht man, dass es genügt, die folgende Aussage zu beweisen:

Es sei $F(x_1, x_2, \ldots, x_n) = 0$ für alle $(x_1, x_2, \ldots, x_n) \in A^n$. Dann gilt $a_{t_1,\ldots,t_n} = 0$ für alle $(t_1, \ldots, t_n) \in \mathbb{Z}^n_{\geq 0}$.

Um das zu beweisen betrachten wir folgende Polynome in $n-1$ Variablen. Wir fixieren eine ganze Zahl $j > 0$ und setzen:

$$F_j(x_2, \ldots, x_n) = \sum_{(t_2,\ldots,t_n)\in\mathbb{Z}^{n-1}_{\geq 0}} a_{j,t_2,\ldots,t_n} x_2^{t_2} \cdot \ldots \cdot x_n^{t_n},$$

Es gibt eine Zahl $m$, so dass $a_{j,t_2,\ldots,t_n} = 0$ für $j > m$. Dann gilt:

$$\begin{aligned} &F(x_1, x_2, \ldots, x_n) = \\ &x_1^m F_m(x_2, \ldots, x_n) + x_1^{m-1} F_{m-1}(x_2, \ldots, x_n) + \ldots + F_0(x_2, \ldots, x_n). \end{aligned} \tag{40}$$

Wir fixieren eine beliebigen Vektor $(x_2, \ldots, x_n) \in D^{n-1}$ und fassen die rechte Seite von (40) als Polynom in der Variablen $x_1$ auf. Aus dem Korollar 15 erhalten wir, dass $F_j(x_2, \ldots, x_n) = 0$ für alle $(x_2, \ldots x_n) \in D^{n-1}$. Durch Induktion über $n$ erhalten wir $a_{j,t_2,\ldots,t_n} = 0$. *Q.E.D.*

Wir sehen das die "Koeffizienten" $a_{(t_1,\ldots,t_n)} \in K$ in (38) durch die Funktion $F$ eindeutig bestimmt sind. Es sei $F \neq 0$ Man kann also $F$ in der Form (40) schreiben, wobei die $F_j$ Polynomfunktionen in den Variablen $x_2, \ldots, x_n$ sind und $F_m \neq 0$. Man sieht aus Korollar 16, dass diese Darstellung eindeutig ist. Man nennt $m$ den Grad der Polynomfunktion $F$ bezüglich der Variablen $x_1$.

**Korollar 26** *Es seien $F$ und $G$ Polynomfunktionen in $n$ Variablen, so dass $F \cdot G = 0$. Dann gilt $F = 0$ oder $G = 0$.*

Das folgert man aus Korollar 16.

**Grundaufgaben der Kombinatorik**

Es sei $[1,n] = \{1,\ldots,n\}$. Es sei $M$ eine Menge, die aus $n$ Elementen besteht. Wir schreiben $\sharp M = n$.

Dann gilt

$$\begin{aligned} \sharp(\mathrm{Abb}([1,r],M)) &= n^r, \\ \sharp(\text{Injektionen } ([1,r],M)) &= n\cdot(n-1)\cdot\ldots\cdot(n+1-r), \end{aligned}$$

Wenn $n = r$ ist, so sind die Injektionen in der zweiten Zeile Bijektionen. Wir nennen eine solchen Bijektion eine Anordnung von $M$.

$$\sharp(\text{Anordungen } M) = n\cdot(n-1)\cdot\ldots\cdot 2\cdot 1 = n!.$$

**Aufgabe 1:** Es seien $n_1,\ldots,n_r \in \mathbb{N}$. Wir suchen die Anzahl aller Abbildungen $f : M \to [1,r]$, so dass

$$\sharp f^{-1}(\{i\}) = n_i. \tag{41}$$

Damit es überhaupt solche Abbildungen $f$ gibt muss $n_1 + n_2 + \ldots + n_r = n = \sharp M$ gelten. In diesem Fall ist die Anzahl dieser Abbildungen

$$\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_r!}. \tag{42}$$

Es sei $A_i = f^{-1}(\{i\}) \subset M$. Dann erhält man eine Klasseneinteilung von $M$

$$A_1 \cup A_2 \cup \ldots \cup A_r = M.$$

Aber die Menge $\mathcal{A} = \{A_1,\ldots,A_r\}$ ist angeordnet! Eine Funktion $f$, die (41) erfüllt, ist offenbar dasgleiche wie eine angeordnete Klasseneinteilung mit $\sharp A_i = n_i$.

Zum Beweis von (42) legen wir die Elemente von $M$ in einer beliebigen Anordnung vor uns hin. Wir haben $n!$ Möglichkeiten. Dann tuen wir die ersten $n_1$ Elemente in die Klasse $A_1$ und die nächsten $n_2$ Elemente in die Klasse $A_2$ u.s.w.. Auf diese Weise erhalten wir alle eine angeordnete Klasseneinteilung mit $\sharp A_i = n_i$. Wir können aber noch die Elemente innerhalb jeder Klasse $A_i$ auf beliebige Weise umordnen, ohne dass sich an dem Ergebnis etwas ändert. Für diese Umordnungen gibt es $n_1!\cdot n_2!\cdot\ldots\cdot n_r!$ Möglichkeiten.

**Variante:** Man kann auch fordern, dass einige Fasern leer sind, d.h. $\sharp f^{-1}(\{i\}) = n_i = 0$ für gewisse $i$. Dann bleibt die Formel (42) richtig, wenn man $0! = 1$ verabredet.

**Aufgabe 2:** (Kombinationen) Wieviele verschiedene Teilemenge aus $k$ Elementen kann man aus der Menge $M$ auswählen? Antwort:

$$\frac{n!}{k! \cdot (n-k)!}.$$

Beweis: Es sei $A_1 \subset M$ eine Teilmenge, so dass $\sharp A_1 = k$. Daraus erhält man die Klasseneinteilung $A_1 \cup (M \setminus A_1) = M$. Folglich ist das ein Spezialfall der letzten Aufgabe. Man benutzt die folgende Abkürzung

$$\binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}. \tag{43}$$

**Satz 27** *(polynomische Lehrsatz)*

*Es sei $R$ ein kommutativer Ring. Dann gilt für beliebige Elemente $x_1, \ldots, x_r \in R$*

$$(x_1 + x_2 + \ldots + x_r)^n = \sum_{n_1+n_2+\ldots+n_r=n} \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_r!} x_1^{n_1} \cdot x_2^{n_2} \cdot \ldots \cdot x_r^{n_r}. \tag{44}$$

*Hier erstreckt sich die Summe über alle Folgen ganzer Zahlen $n_1, n_2, \ldots, n_r$, so dass $n_i \geq 0$ und so dass $n_1 + n_2 + \ldots + n_r = n$.*

**Beweis:** Wenn man mit Hilfe des Distributivgesetzes ausmultipliziert, so erhält man:

$$(x_1 + x_2 + \ldots + x_r)^n = \sum w_1 \cdot \ldots \cdot w_n.$$

Hier erstreckt sich die Summe über alle Worte $\mathbf{w} = w_1 w_2 \ldots w_n$ in den Symbolen $x_1, \ldots, x_r$. Das sind $r^n$ Summanden. Wir ordnen einem Wort $\mathbf{w}$ die folgenden Teilmengen von $[1, n]$ zu:

$$A_i = \{j \in [1, n] \mid w_j = x_i\}, \quad i = 1, \ldots r.$$

Dann gilt $[1, n] = A_1 \cup A_2 \cup \ldots \cup A_r$. Diese Vereinigung ist disjunkt. Das ist wie eine geordnete Klasseneinteilung, nur dass die Mengen $A_i$ auch leer sein können. Es sei $\sharp A_i = n_i$. Dann gilt

$$w_1 \cdot \ldots \cdot w_n = x_1^{n_1} \cdot \ldots \cdot x_r^{n_r}.$$

Wir erhalten die Formel (44) aus der Variante zu Aufgabe 1. *Q.E.D.*

Wir erinnern, dass $\equiv \pmod n$ die Äquivalenzrelation zur Klasseneinteilung (16) bezeichnet. Sie heißt Kongruenz modulo $n$.

**Korollar 28** *Es sei $p$ eine Primzahl. Es sei $a \in \mathbb{Z}$. Dann gilt*

$$a^p \equiv a \pmod p$$

**Beweis:** O.B.d.A $a \in \mathbb{N}$, da man $a$ durch eine kongruente Zahl ersetzen kann. Wir schreiben $a = 1 + 1 + \ldots + 1$. Aus dem polynomischen Lehrsatz erhält man

$$(1 + 1 + \ldots 1)^p \equiv 1^p + 1^p + \ldots + 1^p \equiv a \pmod p,$$

da die übrigen Koeffizienten $p!/(n_1! \cdot \ldots \cdot n_a!)$ in (44) durch $p$ teilbar sind. *Q.E.D.*

**Aufgabe 3:** Es seien $n, r \in \mathbb{N}$. Es sei $n \geq r$. Wieviele Folgen $(n_1, \ldots, n_r)$ natürlicher Zahlen existieren, so dass

$$n_1 + \ldots + n_r = n \tag{45}$$

gilt? Antwort:

$$\binom{n-1}{r-1}. \tag{46}$$

In der Tat, man betrachtet die Folge von natürlichen Zahlen $n_1, n_1 + n_2, n_1 + n_2 + n_3, \ldots, n_1 + n_2 + \ldots + n_{r-1}$. Das ist eine Teilmenge aus $r-1$ Elementen von $[1, n-1]$. Umgekehrt erhält man aus jeder Teilmenge von $r-1$ Elementen auf diese Weise eine Lösung. Also ist die Anwort eine Folgerung aus Aufgabe 2.

**Variante:** Wir suchen die Anzahl der Folgen ganzer Zahlen $(n_1, \ldots, n_r)$, so dass $n_i \geq 0$ und (45) erfüllt ist. Antwort:

$$\binom{n+r-1}{r-1}.$$

In der Tat, wir betrachten die Gleichung

$$(n_1 + 1) + (n_2 + 1) + \ldots (n_r + 1) = n + r.$$

Wir setzen $m_i = n_i + 1$. Das sind natürliche Zahlen. Wir erhalten eine Aufgabe vom Typ 3.

**Aufgabe 4:** (Kombinationen mit Wiederholungen) Es sei $M$ eine Menge aus $n$ Elementen wie bisher. Wir betrachten Teilmengen $T \subset M$, die mit einer Funktion $f : T \to \mathbb{N}$ versehen sind. Wir nennen $D := (T, f)$ eine Teilmenge mit Wiederholungen. Das Element $t \in T$ wird $f(t)$-mal wiederholt. Wir setzen

$$\sharp D = \sum_{t \in T} f(t).$$

Wieviele Teilmengen mit Wiederholungen $D$ der Menge $M$ gibt es, so dass

$$\sharp D = k.$$

gilt? Antwort:

$$\binom{k+n-1}{n-1}. \tag{47}$$

In der Tat: Man kann $D$ auch einfach durch eine Funktion $f : M \to \mathbb{Z}_{\geq 0}$ beschreiben. Die Teilmenge $T$ sind diejenigen Elemente $t \in T$, so dass $f(t) \neq 0$. Dann muss man Lösungen $f(m)$ der folgenden Gleichung finden

$$\sum_{m \in M} f(m) = k.$$

Das ist die Variante von Aufgabe 3.

Übung:

$$\binom{k+n-1}{n-1} = \binom{k+n-1}{k}.$$

Dieser Ausdruck passt besser zu (43).