Arithmetik und Algebra

Prof. Dr. Alfred Schreiber

Institut für Mathematik und ihre Didaktik
Universität Flensburg

1. Grundlegendes über Zahlen

1.1. Begriff der Menge

Der mathematische Begriff "Menge" ist grundlegend; er wird daher selbst nicht definiert (d.h. auf noch grundlegendere Begriffe zurückgeführt). Nach G. Cantor (1845-1918), dem Begründer der Mengenlehre, hat man sich unter einer Menge eine *Zusammenfassung* (*Gesamtheit*) *gedanklicher Objekte* vorzustellen. Danach ist ein Sack Kartoffeln kein geeignetes Beispiel einer Menge, wohl aber die Menge aller Kreise in der Ebene, die Menge aller Primzahlen oder die Menge der ungeraden natürlichen Zahlen, die kleiner sind als 10.

Mengen werden häufig mit lateinischen Großbuchstaben A, B, C, …, M, …, X, Y, Z bezeichnet; es gibt aber zahlreiche (sinnvolle) Ausnahmen von dieser Regel.

Wir bezeichnen vorübergehend mit M die Menge der ungeraden natürlichen Zahlen kleiner als 10. Die Zahl 7 gehört offenbar zu M, was man notiert: $7 \in M$. Das Symbol ' $\in$ ' steht für die Elementschaft (Beziehung der Zugehörigkeit) und wird gelesen: "(ist) Element (von)". Alternative Lesarten lauten: "gehört zu", "liegt in", "aus" und dgl. mehr.

Für die Verneinung der Elementschaft schreibt man: $2 \notin M$, d.h. 2 gehört nicht zu (bzw. ist kein Element von) M.

M besteht aus folgenden Elementen: 1, 3, 5, 7, 9. Die Menge M kann in diesem Fall auch in *Listenform* notiert werden: {1, 3, 5, 7, 9}. Allgemein bezeichnet $\{a_1, a_2, \ldots, a_n\}$ diejenige Menge, die aus genau den Objekten $a_1, a_2, \ldots, a_n$ besteht.

Mathematisch interessante Mengen besitzen häufig *unendlich* viele Elemente, z.B. die Menge $\mathbb{N}$ aller natürlichen Zahlen oder: die Menge $\mathbb{P}$ aller Primzahlen. Die Listenform kann das Gemeinte hier nur andeuten (durch die Auslassungspunkte '…'):

$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$

Wo immer möglich, geschieht die Bildung einer Menge nach dem sog. *Prinzip der Komprehension*, d.h. durch Angabe einer Eigenschaft, welche die Elemente der betreffenden Menge (und nur diese) besitzen. Z.B. besteht $\mathbb{P}$ aus genau den (natürlichen) Zahlen n, für die gilt: n ist eine Primzahl. Dabei steht der sprachliche Ausdruck "n ist eine Primzahl" für die hier benötigte mengenbildende (bzw. *aussondernde*) Eigenschaft.

Man notiert dies wie folgt: $\mathbb{P} = \{n \mid n \text{ ist eine Primzahl}\}$

oder noch etwas genauer: $\mathbb{P} = \{n \in \mathbb{N} \mid n \text{ ist eine Primzahl}\}$

Natürlich muss man die Eigenschaft, eine Primzahl zu sein, mathematisch präzise definieren (womit wir uns in einem späteren Kapitel beschäftigen werden).

Eine Menge kann echte oder unechte Teilmenge einer anderen Menge sein. Z.B. ist $\mathbb{P}$ eine echte Teilmenge von $\mathbb{N}$. Wir fassen diesen Sachverhalt allgemein:

■ 1.1.1. Definition

Für irgend zwei Mengen A, B wird definiert:

(1) $A \subseteq B$ genau dann, wenn für alle $x \in A$ gilt: $x \in B$ (jedes Element von A gehört auch zu B).

(2) $A \subset B$ genau dann, wenn $A \subseteq B$ und ein $x \in B$ existiert, für das gilt: $x \notin A$.

(3) $A = B$ genau dann, wenn $A \subseteq B$ und $B \subseteq A$.

■ Bezeichnungen (zu 1.1.1)

$\subseteq$ heißt Inklusion (auch: Teilmengenrelation); die Beziehung (1) drückt aus, dass A eine (unechte) Teilmenge von B ist. Im Fall (2) spricht man von einer echten Teilmenge(nrelation). (3) definiert die Gleichheit von Mengen.

■ Beispiele

(1) $\{1, 3, 5, 7, 9\}$ ist eine (echte) Teilmenge von $\mathbb{N}$: $\{1, 3, 5, 7, 9\} \subset \mathbb{N}$.

(2) $\{1, 3, 5, 7, 9\}$ ist keine (echte oder unechte) Teilmenge von $\mathbb{P}$, geschrieben: $\{1, 3, 5, 7, 9\} \not\subset \mathbb{P}$.

Denn es ist etwa $1 \notin \mathbb{P}$.

(3) $\mathbb{P} \subset \mathbb{N}$.

(4) $\{3, 5, 3, 9, 1, 7\} = \{1, 3, 5, 7, 9\}$.

Eine (in Listenform notierte) Menge hängt nicht davon ab, in welcher Reihenfolge und in welcher Anzahl ihre Elemente auftreten.

(5) $\{2, 2, 2\} = \{2\}$.

■ Bemerkungen

1. Die aus einem einzigen Element a bestehende Menge $\{a\}$ ist sorgfältig zu unterscheiden von dem Element selbst, mithin: $\{a\} \neq a$.

2. Die Mengenbildung ist beliebig schachtelbar, z.B. besteht die Menge {{1, 2}, 7, {2, {3}}} aus den drei Elementen: {1, 2} (selbst eine Menge), 7 und {2, {3}} (letzteres die Menge, die aus den Elementen 2 und {3} besteht).

3. Nach Definition 1.1.1 sind zwei Mengen *A, B* genau dann gleich, wenn sie dieselben Elemente enthalten (sog. *Prinzip der Extensionalität*), d.h. eine Menge ist bereits durch die zu ihr gehörenden Elemente vollständig bestimmt (unabhängig von Reihenfolge oder Vielfachheit).

Definiert man eine Menge durch eine Eigenschaft, die sich nicht erfüllen lässt, so kann sie kein Element enthalten. Eine unerfüllbare Eigenschaft ist sicherlich $x \neq x$; sie führt zur Definition der leeren Menge:

$$\emptyset = \{x \mid x \neq x\}$$

Da $\emptyset$ kein Element enthält, kann von den Elementen $x \in \emptyset$ Beliebiges (auch Falsches) behauptet werden.

■ Bemerkung

Es gibt nur *eine* leere Menge. Dies folgt aus der Definition der Gleichheit (Prinzip der Extensionalität): Ist etwa $\emptyset_1$ebenfalls leer, so gehört jedes $x \in \emptyset$ auch zu $\emptyset_1$, d.h. es gilt $\emptyset \subseteq \emptyset_1$. Da auch umgekehrt $\emptyset_1 \subseteq \emptyset$ der Fall ist, gilt nach Def. 1.1.1,(3): $\emptyset_1 = \emptyset$.

Es ist daher angebracht, von *der* (anstatt von *einer*) leeren Menge zu reden.

■ 1.1.2. Proposition

A, B, C seien irgendwelche Mengen. Dann gilt:

(1) $A \subseteq A$

(2) $\emptyset \subseteq A$

(3) Wenn $A \subseteq B$ und $B \subseteq C$, dann $A \subseteq C$

■ Bezeichnung

Ist eine Menge von $\emptyset$ verschieden, so heißt sie nichtleer. (Eine nichtleere Menge besitzt mindestens ein Element.)

1.2. Zahlbereiche

In Abschnitt 1.1 wurde die Menge $\mathbb{P}$ der Primzahlen aus der Menge $\mathbb{N}$ der natürlichen Zahlen ausgesondert. Die gebräuchlichen Zahlenmengen entstehen aber eigentlich nicht durch Aussonderung aus einer gemeinsamen Obermenge. Vielmehr lassen sie sich durch einen "von unten nach oben" gerichteten konstruktiven Prozess gewinnen.

Der Reihe nach gelangt man dann zu folgenden speziellen Zahlenmengen (auch Zahlbereiche genannt):

$\mathbb{N}$ = Menge der natürlichen Zahlen: {1, 2, 3, 4, 5, …}

$\mathbb{Z}$ = Menge der ganzen Zahlen: {…, −3, −2, −1, 0, 1, 2, 3, …}

$\mathbb{Q}$ = Menge der rationalen Zahlen: $\left\{\frac{p}{q} \;\middle|\; p \in \mathbb{N},\ 0 \neq q \in \mathbb{Z}\right\}$

$\mathbb{R}$ = Menge der reellen Zahlen (Zahlengerade)

$\mathbb{C}$ = Menge der komplexen Zahlen (Zahlenebene): $\{a + b\,i \mid a, b \in \mathbb{R}\}$ mit $i^2 = -1$

Gelegentlich wird auch 0 zu den natürlichen Zahlen gezählt. Die entsprechende Menge wird im Folgenden mit $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ bezeichnet.

Eine vollständige Darlegung aller Schritte, die zum Aufbau des Zahlensystems erforderlich sind, ist recht umfangreich (und ebenso langatmig). Nach Abschluss der Konstruktion hat man dann die aufsteigende Inklusionskette:

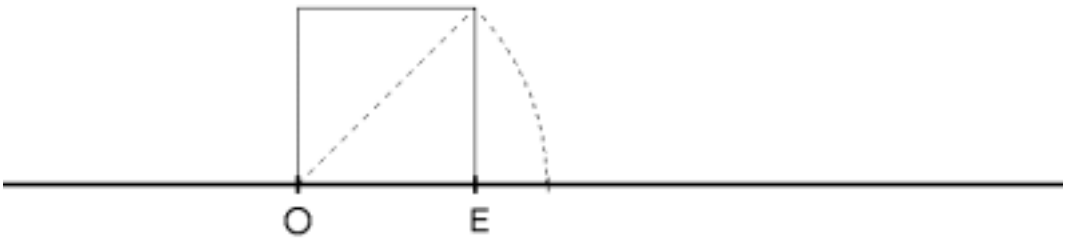
$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

■ Summarische Skizze der wichtigsten Grundgedanken

Durch den Übergang von $\mathbb{N}$ nach $\mathbb{Z}$ werden alle Gleichungen der Form $a + x = b$ (mit natürlichen – und dann auch ganzen – Zahlen a, b) lösbar.

Durch den Übergang von $\mathbb{Z}$ nach $\mathbb{Q}$ werden alle Gleichungen der Form $a\,x = b$ (mit ganzen – und dann auch rationalen – Zahlen a, b, $a \neq 0$) lösbar.

Der Übergang von $\mathbb{Q}$ nach $\mathbb{R}$ ist von ganz anderer Natur. Als geometrisches Modell von $\mathbb{R}$ dient die "Zahlengerade", d.h. eine Gerade mit zwei ausgezeichneten Punkten O (Ursprung, Nullpunkt) und E (Punkt rechts von O im Abstand 1) sowie einer festgelegten Durchlaufungsrichtung. Die Menge $\mathbb{R}$ enthält zu jedem Punkt X rechts von O eine zugehörige Zahl x, welche die Länge der Strecke OX angibt. Wird X an O gespiegelt (nach links abgetragen), so lautet die entsprechende Zahl $-x$. Durch wiederholtes Abtragen von OE links und rechts von O gewinnt man die ganzen Zahlen, durch fortgesetztes Teilen dann auch die rationalen Zahlen. Alle Punkte, die keinen rationalen Abstand von O besitzen, gehören definitionsgemäß zu einer irrationalen Zahl.



Arithmetisch lassen sich reelle Zahlen als (nicht notwendig abbrechende) Dezimalbrüche darstellen, z.B.:

Länge der Diagonalen des Quadrats mit der Seite OE $= \sqrt{2} = 1.414213562\ldots$

Umfang des Kreises mit dem Durchmesser OE $= \pi = 3.141592654\ldots$

Die Auslassungspunkte deuten an, dass die betreffende Zahl nicht "auf einen Schlag" gegeben ist, sondern durch schrittweise Streckenteilung (Intervallschachtelung) angenähert wird, und zwar mit wachsender Anzahl von Nachkommastellen *beliebig genau*.

Die Quadratwurzel aus 2 ist irrational; sie erfüllt die algebraische Gleichung $x^2 - 2 = 0$ und heißt deshalb algebraische Zahl. Die (ebenfalls irrationale) Kreiszahl π erfüllt keine algebraische Gleichung (ein berühmtes von F. Lindemann 1882 bewiesenes Resultat); sie heißt deshalb transzendent. Eine irrationale Zahl ist entweder algebraisch oder transzendent.

Ein weiterer, in gewissem Sinn abschließender Schritt beim Aufbau der Zahlbereiche ist der Übergang von $\mathbb{R}$ nach $\mathbb{C}$. Ausgangspunkt ist dabei die Tatsache, dass schon eine einfache quadratische Gleichung wie $x^2 + 1 = 0$ keine reelle

Lösung besitzt. Rein symbolisch wird eine Lösung $i = \sqrt{-1}$ der Menge $\mathbb{R}$ hinzugefügt, indem man mit Ausdrücken der Form $a + b\,i$ ($a, b \in \mathbb{R}$) so rechnet "wie gewohnt", etwa: $(1 + i)\cdot(2 - 4\,i) = 2 - 4\,i + 2\,i - 4\,i^2 = 6 - 2\,i$. Dadurch werden zunächst alle quadratischen Gleichungen (mit reellen – und dann auch komplexen – Koeffizienten) lösbar. Zum Beispiel hat die Gleichung $x^2 + x + 5 = 0$ die beiden komplexen Lösungen $-\frac{1}{2} \pm \frac{\sqrt{19}}{2}\,i$. Darüberhinaus lässt sich beweisen (*Fundamentalsatz der klassischen Algebra*), dass jede algebraische Gleichung vom Grade n (mit beliebigen komplexen Koeffizienten) in $\mathbb{C}$ lösbar ist, genauer: n komplexe Lösungen besitzt.

■ 1.2.1. Grundlegende Rechengesetze

In den Zahlbereichen von $\mathbb{N}_0$ bis $\mathbb{C}$ gelten bzgl. + (Addition) und · (Multiplikation) eine Reihe von grundlegenden Rechengesetzen (hier lediglich zusammengestellt, ohne auf Begründungszusammenhänge einzugehen):

(Ass1) $a + (b + c) = (a + b) + c$

(Ass2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(Kom1) $a + b = b + a$

(Kom2) $a \cdot b = b \cdot a$

(Dist) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Dabei bedeuten: (Ass) Assoziativgesetz(e), (Kom) Kommutativgesetz(e), (Dist) Distributivgesetz. In letzterem können rechts vom Gleichheitszeichen die Klammern entfallen, wenn man die Multiplikation vorrangig ausführt ("Punktrechnung vor Strichrechnung").

Hinzu kommt die Neutralität der Zahlen 0 und 1:

(Neutr1) $a + 0 = a$

(Neutr2) $a \cdot 1 = a$

■ Bemerkung

Eine wichtige praktische Konsequenz der Assoziativgesetze: Die Klammern in mehrfachen Summen bzw. Produkten können fortgelassen werden. Z.B. hat die Summe $5 + 3 + 7$ einen eindeutigen Sinn, weil die beiden Klammerungen $5 + (3 + 7)$ und $(5 + 3) + 7$ denselben Wert liefern.

■ Ringe

Ist in einem Zahlbereich (der alle o.g. Rechengesetze erfüllt) jede Gleichung der Form $a + x = 0$ lösbar, so spricht man von einem (kommutativen) Ring. Die Zahlbereiche $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ (und auch $\mathbb{C}$) sind kommutative Ringe.

Die (eindeutig bestimmte) Lösung von $a + x = 0$ wird mit $-a$ bezeichnet; ferner notiert man $a - b := a + (-b)$.

Als einfaches Beispiel für eine in einem Ring (hier: $\mathbb{R}$) gültige Folgerung diene

■ 1.2.2. Proposition

Für alle $a \in \mathbb{R}$ gilt: $0 \cdot a = 0$

■ Beweis

Sei (zur Abkürzung) $b = 0 \cdot a$. Dann gilt nach (Neutr1), (Kom2) und (Dist) zunächst:

$$b = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a = b + b$$

Beachtet man nun, dass $-b$ durch die Gleichung $b + (-b) = 0$ definiert ist, so folgt mittels (Ass1) und (Neutr1):

$$0 = b + (-b) = (b + b) + (-b) = b + (b + (-b)) = b + 0 = b$$

was zu beweisen war. ◆

■ Körper

Ist zusätzlich jede Gleichung der Form $a \cdot x = b$ (mit $a \neq 0$) lösbar, so heißt der Bereich ein (kommutativer) Körper. In Körpern ist somit die Division (durch von Null verschiedene Elemente) uneingeschränkt möglich. $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper. (Die hierzu erforderlichen Überlegungen werden ab Kapitel 12 in mehr Einzelheiten behandelt.)

Die (eindeutig bestimmte) Lösung von $a \cdot x = 1$ ($a \neq 0$) wird mit a^{-1} oder $\frac{1}{a}$ bezeichnet; ferner notiert man $\frac{b}{a} := b \cdot a^{-1}$.

1.3. Ordnung

■ Bezeichnungen

1) Ein Punkt A der reellen Zahlengeraden, der rechts von O liegt, entspricht einer positiven Zahl $a \in \mathbb{R}$. Die Menge der positiven reellen Zahlen wird mit $\mathbb{R}^+$ bezeichnet.

2) Für reelle Zahlen a, b schreiben wir $a < b$, wenn $b - a \in \mathbb{R}^+$. (Damit ist $x \in \mathbb{R}^+$ genau dann, wenn $0 < x$.)

(Geometrisch bedeutet die so eingeführte Ordnung: Der zu a gehörige Punkt A liegt auf der Zahlengeraden links von dem zu b gehörigen Punkt B.)

Anstelle von $a < b$ schreibt man auch: $b > a$.

3) Für $a, b \in \mathbb{R}$ bedeutet $a \leq b$ dasselbe wie: $a < b$ oder $a = b$. Ferner schreibt man $a < b < c$ für: $a < b$ und $b < c$ (weitere Varianten möglich, z.B. $a < b \leq c < d$, etc.).

■ 1.3.1. Grundlegende Eigenschaften von <

(1) Nicht $a < a$ (auch notiert als: $a \not< a$)

(2) Wenn $a < b$, dann $b \not< a$.

(3) Wenn $a < b$ und $b < c$, dann $a < c$

(4) $a < b$ oder $a = b$ oder $b < a$

(5) Wenn $a < b$, dann für alle $c \in \mathbb{R}$: $a + c < b + c$

(6) Wenn $a < b$, dann für alle $c \in \mathbb{R}^+$: $a \cdot c < b \cdot c$

(7) Für alle $a, b \in \mathbb{R}$, $b > 0$, gibt es ein $n \in \mathbb{N}$ mit $a < n\,b$

■ Bemerkungen und Bezeichnungen

1) Die aufgeführten Eigenschaften lassen sich an der Zahlengeraden veranschaulichen (Übung!). Auf theoretische Begründungszusammenhänge soll hier nicht eingegangen werden.

2) (1), (2), (3) heißen beziehentlich: Irreflexivität, Asymmetrie, Transitivität. Man beachte: (2) folgt bereits aus (1) und (3). (Setze dazu in (3) $c = a$.) Jede Relation mit diesen Eigenschaften heißt teilweise Ordnung. Die Eigenschaft (4) drückt die *Vergleichbarkeit* irgend zweier Zahlen aus. Gilt neben (1) und (3) auch (4), so spricht man von einer vollständigen Ordnung.

3) (5) und (6) (sog. Monotonie-Eigenschaften) sorgen für die *Verträglichkeit* der Ordnung mit der Addition und der Multiplikation.

4) Eigenschaft (7) ist das sog. Axiom der Messbarkeit. Eine Ordnung mit dieser Eigenschaft heißt archimedisch.

5) Da die Mengen der natürlichen, der ganzen und der rationalen Zahlen Teilmengen von $\mathbb{R}$ sind, hat die hier beschriebene Ordnung auch Gültigkeit in diesen Zahlbereichen. Auf $\mathbb{C}$ lässt sich die geschilderte Ordnung nicht (jedenfalls nicht ohne Einbuße wesentlicher Eigenschaften) ausweiten.

■ 1.3.2. Proposition

Seien a, b reelle Zahlen, $a \neq 0$. Dann gelten folgende Aussagen:

(1) $0 \notin \mathbb{R}^+$

(2) $a \in \mathbb{R}^+$ genau dann, wenn $-a \notin \mathbb{R}^+$

(3) Wenn $a, b \in \mathbb{R}^+$, dann $a + b \in \mathbb{R}^+$

(4) Wenn $a, b \in \mathbb{R}^+$, dann $a \cdot b \in \mathbb{R}^+$

■ Beweis

Zu (1): Wäre $0 \in \mathbb{R}^+$, so hätte man $0 < 0$ entgegen 1.3.1,(1). Zu (3): Nach Voraussetzung $0 < b$. Damit liefert 1.3.1,(5) und (Kom2): $a = a + 0 = 0 + a < b + a = a + b$. Mit 1.3.1,(3) und der Voraussetzung $0 < a$ ergibt sich schließlich: $0 < a + b$. Zu (4): Nach Voraussetzung gilt $0 < a$, also nach Prop. 1.2.2 und 1.3.1,(6): $0 = 0 \cdot b < a \cdot b$. – (2) bleibt als Übung. ◆

■ 1.3.3. Definition (Minimum und Maximum)

Seien a, b irgend zwei reelle Zahlen. Nach 1.3.1,(4) kann nur $a \leq b$ oder $a > b$ der Fall sein. Im ersten Fall wird $\mathrm{Min}(a, b)$ (das Minimum von a, b) definiert als a, im zweiten Fall als b. Entsprechend gilt für das Maximum von a, b: $\mathrm{Max}(a, b) = b$, falls $a \leq b$, sonst $\mathrm{Max}(a, b) = a$.

■ 1.3.4. Proposition

$$\text{Min}(a, b) + \text{Max}(a, b) = a + b$$

■ Bemerkung

Die Definition von Min und Max lässt sich in einfacher Weise auf mehr als zwei Zahlen erweitern, indem man z.B. setzt: $\text{Min}(a, b, c) = \text{Min}(a, \text{Min}(b, c))$, und allgemein:

$$\text{Min}(a_1, a_2, \ldots, a_n) = \text{Min}(a_1, \text{Min}(a_2, \ldots, a_n))$$

Entsprechend für Max. – Offenbar hat jede endliche Menge reeller Zahlen $\{a_1, a_2, \ldots, a_n\}$ jeweils ein eindeutiges Minimum bzw. Maximum.

Die hier angegebene Definition beschreibt nicht, wie man Min/Max möglichst geschickt bzw. mit möglichst geringem Aufwand berechnet! (Diese Aufgabe gehört in das Gebiet der Algorithmik bzw. Informatik.)

■ Reelle Intervalle

Intervalle sind gewisse Teilmengen von $\mathbb{R}$, die sich mit Hilfe der gewöhnlichen Ordnung $<$ festlegen lassen; sie entsprechen im geometrischen Modell (Zahlengerade) den *Teilstrecken* oder den *Halbgeraden*. Die linken und/oder rechten Endpunkte können hinzugerechnet werden oder nicht. Demnach gibt es zu vorgegebenen $a, b \in \mathbb{R}$, $a < b$, die folgenden Fälle ("Teilstrecken"):

$$[a; b] := \{x \in \mathbb{R} \mid a \le x \le b\}$$
$$(a; b] := \{x \in \mathbb{R} \mid a < x \le b\}$$
$$[a; b) := \{x \in \mathbb{R} \mid a \le x < b\}$$
$$(a; b) := \{x \in \mathbb{R} \mid a < x < b\}$$

Ferner setzt man ("Teil-Halbgeraden"):

$$[a; \infty) := \{x \in \mathbb{R} \mid a \le x\}$$
$$(a; \infty) := \{x \in \mathbb{R} \mid a < x\}$$
$$(-\infty; a] := \{x \in \mathbb{R} \mid x \le a\}$$
$$(-\infty; a) := \{x \in \mathbb{R} \mid x < a\}$$

Zur Bezeichnungsweise: $[a; b]$ heißt abgeschlossenes, $(a; b)$ offenes Intervall; das Intervall $(a; b]$ heißt links halboffen (bzw. rechts halbabgeschlossen), usw. Es ist $(0; \infty) = \mathbb{R}^+$; auch die volle Zahlengerade lässt sich als Intervall auffassen: $(-\infty; \infty) = \mathbb{R}$.

1.4. Absolutbetrag

■ 1.4.1. Definition

Sei $a \in \mathbb{R}$ beliebig. Die durch $|a| := \text{Max}(-a, a)$ definierte Zahl heißt Absolutbetrag (oft auch kurz: Betrag) von a.

■ 1.4.2. Proposition

Für alle $a \in \mathbb{R}$ gilt:

(1) $a \leq |a| = |-a|$

(2) Wenn $a \geq 0$, dann $|a| = a$

Wenn $a < 0$, dann $|a| = -a$

(3) $|a \cdot b| = |a| \cdot |b|$

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

■ Beweis

Zu (1)-(3): Übung. – Zu (4): Nach (1) gilt $a \leq |a|$, $b \leq |b|$, also: $a + b \leq |a| + |b|$. Analog ergibt sich aus $-a \leq |a|$, $-b \leq |b|$ (ebenfalls nach (1) gültig): $-(a + b) = (-a) + (-b) \leq |a| + |b|$. Mithin erhält man nach Def. 1.4.1: $|a + b| = \text{Max}(a + b, -(a + b)) \leq |a| + |b|$. ◆

■ Bemerkung

Häufig werden reelle Intervalle mit Hilfe des Absolutbetrags angegeben. Beispiel: Sei I die Menge aller $x \in \mathbb{R}$, welche die Ungleichung $\left|2 - x\right| < \frac{1}{10}$ erfüllen. Um herauszubekommen, inwiefern es sich um ein Intervall (und dann: welches) handelt, sind zunächst *die Betragsstriche mittels einer Fallunterscheidung aufzulösen* (!):

1. Fall: $x \leq 2$. Dann ist $2 - x \geq 0$, also nach Prop. 1.4.2,(2): $|2 - x| = 2 - x < \frac{1}{10}$, und schließlich: $\frac{19}{10} < x$.

2. Fall: $2 < x$. Dann ist $2 - x < 0$, also nach Prop. 1.4.2,(2): $|2 - x| = -(2 - x) < \frac{1}{10}$, und schließlich: $x < \frac{21}{10}$.

Insgesamt hat man: $\frac{19}{10} < x < \frac{21}{10}$, d.h. es ist $I = (1.9; 2.1)$ (beidseitig offenes Intervall).

1.5. Zahlenfolgen

Im Unterschied zu einer Menge von Zahlen kommt es bei einer Folge von Zahlen auf die Reihenfolge an. Die Folge 3, −4, 3, 7 ist *wohl zu unterscheiden* von der Folge 3, 3, −4, 7, obwohl die Menge der Folgenglieder in beiden Fällen dieselbe ist. Auch sind mehrfach vorkommende Elemente keinesfalls zu streichen (wie es bei Mengen der Fall ist). Folgen können endlich oder unendlich sein:

(1) 6, 11, 16, 21, 26, …

(2) $1, \frac{1}{3}, \frac{1}{9}, \frac{1}{27}, \frac{1}{81}, \ldots$

(3) 1, 3, 6, 10, 15, …

Die Auslassungspunkte lassen zunächst offen, wie es weitergeht. Man kann sich die Folge fortgesetzt denken und/oder nach einer bestimmten Anzahl von Gliedern abbrechen (endliche Folge); die Pünktchen '…' implizieren dabei keine Vorgabe, z.B. ist es möglich, dass (1) aus folgenden 6 Gliedern besteht: 6, 11, 16, 21, 26, 13.

Auch eine unendliche Folge kann theoretisch aus "beliebigen" Gliedern bestehen. Z.B. macht die Folge der Dezimalziffern von π einen ziemlich willkürlichen Eindruck. Allerdings liegt hier wie auch in anderen konkreten Fällen unendlicher Zahlenfolgen eine Regelgebundenheit (Gesetzmäßigkeit) vor. Diese drückt man durch einen allgemeinen Beschreibungsterm aus ("Bildungsgesetz"); in den o.g. Beispielen:

(1) $a_n = 5\,n + 6$

(2) $b_n = \left(\frac{1}{3}\right)^n$

(3) $c_n = \frac{1}{2}\,(n+1)\,(n+2)$

Der Index n bezeichnet die Platznummer eines Folgenglieds; er durchläuft alle natürlichen Zahlen, hier beginnend bei 0 ($n \in \mathbb{N}_0$). Man kann aber auch bei $n = 1$ (oder einem anderen Anfangswert) beginnen, z.B. ist $c_n = \frac{1}{2}\,n(n+1)$ für $n \in \mathbb{N}$.

Eine Folge $x_0, x_1, x_2, \ldots$ wird notiert: $(x_n)_{n\geq 0}$ oder kürzer (x_n), wenn der Startwert für n aus dem Zusammenhang hervorgeht. Wir wollen $n \geq 0$ vereinbaren und den Startwert nur dann notieren, wenn er von 0 abweicht.

Die folgende Definition behandelt zwei häufig vorkommende Typen von Folgen:

■ 1.5.1. Definition

a) Eine Zahlenfolge (x_n) heißt arithmetisch (1. Ordnung), wenn ein $d \in \mathbb{R}$ existiert, so dass für alle $n \in \mathbb{N}_0$ gilt: $x_{n+1} = x_n + d$. Die Zahl d ist die *Differenz* benachbarter Folgenglieder.

b) Eine Zahlenfolge (x_n) heißt geometrisch, wenn ein $q \in \mathbb{R}$ existiert, so dass für alle $n \in \mathbb{N}_0$ gilt: $x_{n+1} = x_n \cdot q$. Die Zahl q ist der *Quotient* benachbarter Folgenglieder, sofern diese nicht Null sind.

■ Beispiele

Die obige Folge (a_n) ist arithmetisch, wobei $d = a_{n+1} - a_n = 5\,(n+1) + 6 - (5\,n + 6) = 5$.

Die Folge (b_n) ist geometrisch, wobei $q = \frac{b_{n+1}}{b_n} = \frac{3^n}{3^{n+1}} = \frac{1}{3}$.

Die Folge (c_n) ist weder arithmetisch noch geometrisch. (Sie wird sich in Kapitel 4 als arithmetische Folge 2. Ordnung erweisen.)

■ 1.5.2. Proposition

(1) Ist (x_n) arithmetisch, so gilt: $x_n = d\,n + x_0$ für ein reelles d.

(2) Ist (x_n) geometrisch, so gilt: $x_n = x_0 \cdot q^n$ für ein reelles q.

1.6. Summen und Produkte

■ Summen, Summationszeichen

Zu gegebener Folge $x_0, x_1, \ldots, x_n, \ldots$ betrachtet man häufig die Summe der ersten n Folgenglieder: $x_0 + x_1 + \ldots + x_n$ (die wegen (Ass1) ohne Klammerung geschrieben werden kann).

Solche Summen lassen sich ohne Auslassungspunkte mit Hilfe des Summationszeichens $\sum$ (griechischer Großbuchstabe Sigma) notieren:

$$\sum_{i=0}^{n} x_i$$

Hierbei ist i der Lauf- oder Summationsindex (für den auch andere Variablenzeichen gewählt werden können); 0 ist die untere und n die obere Summationsgrenze (auch diese Grenzen lassen sich beliebig wählen).

■ Beispiele

(1) $$\sum_{k=5}^{11} 2\,k = 2\cdot 5 + 2\cdot 6 + \ldots + 2\cdot 11$$

(2) $$\sum_{j=-2}^{1} \frac{1}{1+3\,j} = \frac{1}{1+3\cdot(-2)} + \frac{1}{1+3\cdot(-1)} + \frac{1}{1+3\cdot 0} + \frac{1}{1+3\cdot 1}$$

(3) $$\sum_{n=5}^{5} 2^n = 2^5$$

(4) $$\sum_{n=1}^{0} n^2 = 0$$

Zu (3): Stimmen untere und obere Grenze der Summation überein, so ist dies der einzige Wert, den der Laufindex annehmen kann; die Summe besteht dann aus nur einem Summanden.

Zu (4): Ist die untere Summationsgrenze größer als die obere, kann der Index keinen Wert annehmen und die Summation nichts zum Summenwert beitragen. Ein solche sog. leere Summe wird gleich Null gesetzt.

■ 1.6.1. Proposition

(1) $$a\cdot\sum_{i=1}^{n} b_i = \sum_{i=1}^{n} a\cdot b_i$$

(2) $$\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$$

■ Bemerkung

(1) verallgemeinert das Distributivgesetz (Dist, 1.2.1) für Summen aus beliebig (endlich) vielen Summanden. (2) ergibt sich durch wiederholtes Anwenden von (Ass1) und (Kom1).

■ Arithmetische und geometrische Reihe

Wir wenden das allgemeine Distributivgesetz auf die Summen arithmetischer und geometrischer Folgen an (auch arithmetische Reihen bzw. geometrische Reihen genannt).

Nach Prop. 1.5.2,(1) hat man $x_k = d\,k + x_0$. Damit ergibt sich nach Prop. 1.6.1,(2):

$$A_n := \sum_{k=0}^{n} x_k = \sum_{k=0}^{n} (d\,k + x_0) = \sum_{k=0}^{n} d\,k + \sum_{k=0}^{n} x_0 = d \sum_{k=1}^{n} k + (n+1)\,x_0$$

Es bleibt noch die Summe $S := \sum_{k=1}^{n} k = 1 + 2 + \ldots + n$ zu berechnen. Natürlich ist ihr Wert unabhängig von der Reihenfolge ihrer Summanden: $S = \sum_{k=1}^{n} (n + 1 - k) = n + (n-1) + \ldots + 1$. Daraus ergibt sich:
$2\,S = \sum_{k=1}^{n} (n+1) = n(n+1)$, mithin: $S = \frac{n(n+1)}{2}$.

Für die geometrische Reihe erhält man unter Benutzung von Prop. 1.5.2,(2) und 1.6.1,(1):

$$G_n := \sum_{k=0}^{n} x_k = \sum_{k=0}^{n} x_0 \cdot q^k = x_0 \cdot \sum_{k=0}^{n} q^k$$

Es bleibt noch die Summe $T := \sum_{k=0}^{n} q^k = 1 + q + q^2 + \ldots + q^n$ zu berechnen. Nach Prop. 1.6.1,(1) ist $q\,T = q + q^2 + \ldots + q^{n+1}$. Wir subtrahieren: $T - q\,T = 1 - q^{n+1}$ und erhalten $T = \frac{1-q^{n+1}}{1-q}$, falls $q \neq 1$ist (sonst $T = n + 1$).

In folgendem Lehrsatz sind beide Resultate zusammengefasst:

■ 1.6.2. Proposition

(1) $A_n = (n+1)\left(\frac{d\,n}{2} + x_0\right)$

(2) $G_n = x_0\,\frac{1-q^{n+1}}{1-q}$ für $q \neq 1$

■ Bemerkung

Für $q = 1$ ist $G_n = (n+1)\,x_0$. Denselben Wert nimmt A_n für $d = 0$ an. Die konstanten Zahlenfolgen sind demnach arithmetisch *und* geometrisch. – Gibt es noch andere Zahlenfolgen mit dieser Eigenschaft? (Übung!).

■ Produkte, Produktzeichen

Zu gegebener Folge $x_0, x_1, \ldots, x_n, \ldots$ betrachtet man das Produkt der (ersten n oder auch aller) Folgenglieder: $x_0 \cdot x_1 \cdot \ldots \cdot x_n$ (das wegen (Ass2) ohne Klammerung geschrieben werden kann).

In Analogie zur Summenschreibweise notiert man solche Produkte ohne Auslassungspunkte mit Hilfe des Produktzeichens $\prod$ (griechischer Großbuchstabe Pi) wie folgt:

$$\prod_{i=0}^{n} x_i$$

■ Beispiele

(1) $\prod_{k=1}^{4} (1-k) = (1-1)\cdot(1-2)\cdot(1-3)\cdot(1-4)$

(2) $\prod_{j=1}^{n} j = 1\cdot 2\cdot \ldots \cdot n$

Zu (2): Das Produkt der ersten n positiven ganzen Zahlen wird auch mit $n!$ bezeichnet (gelesen: n Fakultät). Für $n = 0$ kann der Laufindex keinen Wert annehmen. Das so entstehende leere Produkt trägt nichts zum Produktwert bei und wird daher gleich 1 gesetzt. Es ist also $0! = 1$.

■ Bemerkung

Bezieht sich die Bildung von Summe und Produkt auf alle (unendlich vielen) Glieder einer Zahlenfolge $x_0, x_1, x_2, \ldots$, so wird dies zunächst rein formal durch das *Symbol für Unendlich* (∞) als obere Grenze angedeutet, z.B. für die Summe wie folgt:

$$\sum_{i=0}^{\infty} x_i$$

Summen dieser Form heißen *unendliche Reihen*; sie spielen in der Analysis eine zentrale Rolle. Unter bestimmten Bedingungen (Konvergenz) kann man einer unendlichen Reihe eine reelle Zahl als Wert zuweisen. So gilt z.B. nach Prop. 1.6.2,(2) für die geometrische Reihe (mit $x_0 = 1$ und Quotient q):

$$\sum_{k=0}^{n} q^k = 1 + q + q^2 + \ldots + q^n = \frac{1 - q^{n+1}}{1 - q}$$

Man kann nun zeigen, dass bei $|q| < 1$ der Ausdruck q^{n+1} gegen 0 strebt für $n \to \infty$ und folglich die Summe gegen $\frac{1}{1-q}$ konvergiert. Daher schreibt man:

$$\sum_{k=0}^{\infty} q^k = 1 + q + q^2 + \ldots = \frac{1}{1 - q}$$

Für $q = \frac{1}{2}$ macht man sich diese Gleichung leicht geometrisch an einer Strecke der Länge 2 klar: Wir teilen die Strecke in zwei Hälften der Länge 1, dann die rechte der so entstandenen Hälften in zwei Hälften der Länge $\frac{1}{2}$, dann wiederum die rechte dieser Hälften in zwei Hälften der Länge $\frac{1}{4}$, und so weiter *ad infinitum*: $1 + \frac{1}{2} + \frac{1}{4} + \ldots = 2$.

Eine formal unendliche Reihe hat nur dann einen Sinn, wenn es möglich ist, ihr in einem klar definierten Verfahren (wie hier am Beispiel der geometrischen Reihe vorgeführt) einen Grenzwert zuzuweisen.

2. Elementare Mengenlehre

2.1. Junktoren

Häufig muss man zur Definition einer Menge zwei oder mehr Ausdrücke logisch verbinden. Zum Beispiel sondert man aus $\mathbb{R}$ das Intervall [0; 1] folgendermaßen aus:

$$[0; 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$$

Die Elemente x dieser Teilmenge von $\mathbb{R}$ erfüllen somit die charakteristische Eigenschaft $0 \leq x \leq 1$. Bei genauerem Hinsehen (hier: auf die Definition bzw. Abkürzungsvereinbarung unter 1.3) handelt es sich um die Und-Verbindung (Konjunktion) zweier Teilformeln:

$$0 \leq x \text{ und } x \leq 1$$

Die Partikel "und" nennt man deshalb einen zweistelligen (aussagenlogischen) Junktor (von lat. iungere: verbinden). Ein weiterer solcher Junktor ist die Partikel "oder" (Adjunktion), die man z.B. benötigt, um $x \leq 1$ zu zerlegen: $x < 1$ oder $x = 1$. Ausführlich geschrieben ist $0 \leq x \leq 1$ somit gleichbedeutend mit

$$(0 < x \text{ oder } 0 = x) \text{ und } (x < 1 \text{ oder } x = 1)$$

Beim Aufbau mathematischer Formeln und Aussagen spielt auch die Verneinung (Negation) eine wichtige Rolle, etwa in Ausdrücken wie $1 \notin \mathbb{P}$, $3 \neq 4$, u.ä.m. Da sich die Verneinungspartikel ("nicht") auf nur einen Ausdruck bezieht, ist die Negation ein einstelliger Junktor (der i.a. *vor* den zu verneinenden Ausdruck geschrieben wird):

$$\text{nicht } (1 \in \mathbb{P})$$

Für die Junktoren können (müssen aber nicht!) Abkürzungen verwendet werden.

■ Abkürzungen

Konjunktion:	$\wedge$	(und)
Adjunktion:	$\vee$	(oder)
Negation:	$\neg$	(nicht)

Man verabredet, dass die Negation stärker bindet als Konjunktion, Adjunktion und andere zweistellige Junktoren.

■ Bemerkung

Diese (und andere) logische Junktoren lauten zwar ebenso wie die aus der natürlichen Sprache vertrauten Partikeln; sie haben aber nicht selten eine z.T. andere Bedeutung. Beispiel: *Er nahm die Arznei und er wurde gesund*. Die Konjunktion "und" drückt in diesem Satz (außer der rein logischen Und-Verbindung) eine zeitliche und ursächliche Folgebeziehung aus. Das merkt man unter anderem daran, dass sich die beiden Teilaussagen nicht vertauschen lassen, ohne dass der Satz seinen Sinn ändert: *Er wurde gesund und er nahm die Arznei*. – Dieser Gebrauch der Sprachelemente heißt intensional. Demgegenüber werden logische Junktoren extensional aufgefasst, d.h. ihre Bedeutung hängt nicht vom Sinn der Ausdrücke ab, sondern lediglich von ihrem Wahrheitswert.

■ Bezeichnungen

Den Ausdrücken a, b, c, …, vor die bzw. zwischen die man einen Junktor setzt, muss genau einer der beiden Wahrheitswerte "wahr" (notiert als 1) oder "falsch" (notiert als 0) zugeordnet werden können (Prinzip der Zweiwertigkeit). $W(a)$ bezeichne den Wahrheitswert des Ausdrucks a.

■ 2.1.1. Definition

$$W(\neg\, a) = 1 - W(a)$$
$$W(a \wedge b) = \text{Min}(W(a),\, W(b))$$
$$W(a \vee b) = \text{Max}(W(a),\, W(b))$$

■ Bemerkung zu 2.1.1

Man entnimmt der Definition unmittelbar: $\neg\, a$ ist genau dann wahr, wenn a falsch ist (und umgekehrt); $a \wedge b$ ist genau dann wahr, wenn sowohl a als auch b wahr ist; $a \vee b$ ist genau dann falsch, wenn sowohl a als auch b falsch ist. – Beim umgangssprachlichen "oder" wird vielfach stillschweigend unterstellt, dass die beiden Teilausdrücke a, b nicht beide wahr sind, z.B.: *Dieses Jahr machen wir Ferien in den Bergen oder an der See*. Das hier verwendete ausschließende "oder" meint genauer: "entweder ... oder ..." (Disjunktion). Wenn nicht ausdrücklich hervorgehoben, ist das mathematisch gebrauchte "oder" die Adjunktion (einschließendes "oder"). In diesem Fall gilt offenbar $W(a \vee b) = 1$ auch dann, wenn $W(a) = W(b) = 1$ ist.

■ Ein Junktor für "wenn-dann"

Viele Sätze der Umgangssprache haben die Form: *Wenn a, dann b*. Es ist üblich, einen weiteren zweistelligen Junktor (die sog. Subjunktion, abgekürzt: $\Longrightarrow$) einzuführen, um den 'Wahrheitswertgehalt' dieser Beziehung wiederzugeben. Seine Definition versteht man am besten in Analogie zu einem Versprechen: *Wenn gleich die Sonne scheint, dann gehen wir spazieren*. Der einzige Fall, in dem diese Zusage nicht eingehalten wird, ist der, dass die Sonne scheint und wir nicht spazieren gehen. Daher ist die Aussage schon dann wahr, wenn der Wenn-Teil (die Prämisse) nicht zutrifft.

■ 2.1.2. Definition

Der Ausdruck $a \Longrightarrow b$ (wenn a, dann b) ist eine Abkürzung für den Ausdruck $\neg\, a \vee b$. Ferner ist der Ausdruck $a \Longleftrightarrow b$ (Bisubjunktion: a genau dann, wenn b) eine Abkürzung für $(a \Longrightarrow b) \wedge (b \Longrightarrow a)$.

■ 2.1.3. Proposition

(1) $a \Longrightarrow b$ ist genau dann falsch, wenn a wahr und b falsch ist.

(2) $a \Longleftrightarrow b$ ist genau dann wahr, wenn $W(a) = W(b)$ gilt.

■ Beweis

Zu (1): Nach Definition gilt: $W(a \Rightarrow b) = W(\neg\, a \vee b) = \text{Max}(W(\neg\, a), W(b)) = \text{Max}(1 - W(a), W(b))$. Ist a wahr und b falsch, also $W(a) = 1$ und $W(b) = 0$, so erhalten wir: $W(a \Rightarrow b) = \text{Max}(1 - 1, 0) = 0$. Ist umgekehrt $\text{Max}(1 - W(a), W(b)) = 0$, so ist notwendigerweise $W(a) = 1$ und $W(b) = 0$.

(2) bleibt als Übung. ◆

■ Bemerkungen und Terminologie

(1) Wie beweist man eine Behauptung der Form $a \Longrightarrow b$? Antwort: Man nimmt an (setzt voraus), dass a der Fall ist. Daraufhin schließt man (i.a. schrittweise und unter Benutzung der Voraussetzung a sowie evtl. anderer bereits bekannter Tatsachen), dass auch b gilt. – Sprechweisen: a ist hinreichend für b, oder dazu gleichbedeutend: b ist notwendig für a.

(2) Wie beweist man eine Behauptung der Form $a \Longleftrightarrow b$? Man beweist erstens $a \Longrightarrow b$ und zweitens $b \Longrightarrow a$. Mithin ist in diesem Fall a hinreichend und notwendig für b (ebenso umgekehrt). Sprechweise: a und b heißen logisch äquivalent.

(3) Gelegentlich wird die logische Äquivalenz mehrerer Ausdrücke (etwa von a, b, c) behauptet. Hier führt ein sog. Ringschluss zum Ziel: Man beweist $a \Longrightarrow b$, $b \Longrightarrow c$, $c \Longrightarrow a$. Überlegen Sie warum?

■ Bemerkung

Die Subjunktion ist nicht zu verwechseln mit der logischen Folgerungsbeziehung (obwohl ein Zusammenhang zwischen beiden besteht). In einem Beweis schließt man aus gewissen Voraussetzungen auf weitere Aussagen. Dabei werden Wendungen benutzt wie "daraus ergibt sich", "also gilt", "somit erhalten wir", und dgl. mehr. Es ist nicht ratsam, die damit angedeutete Beziehung mit dem Symbol für die Subjunktion abzukürzen. Beides stimmt inhaltlich nicht überein, aber auch formal nicht: "$\Longrightarrow$" ist keine Relation zwischen Ausdrücken, sondern ein Operator, der zwei Ausdrücke zu einem neuen verbindet. Mögliche Alternativen: 1) umgangssprachliche Wendungen, 2) Ausdrücke untereinander schreiben, 3) Benutzung eines anders aussehenden Schluss-Pfeils (wie z.B. in der Vorlesung gelegentlich: ein nach oben gekrümmter Pfeil in Schreibrichtung). – Generelle Richtschnur: Beweise klar gliedern und sorgfältig auch in Einzelheiten aufschreiben. Logische Symbole führen dabei von sich aus noch nicht zu höherer Genauigkeit. Ihr gelegentlicher Gebrauch kann Schreibarbeit abkürzen. Anfänger sollten vorsichtshalber sparsam mit formallogischer Bezeichnungstechnik umgehen.

■ Wahrheitswertverläufe

In einem zusammengesetzten Ausdruck können die Teilausdrücke unabhängig voneinander verschiedene Wahrheitswerte annehmen. Zum Beispiel gibt es für a, b in $a \wedge b$ oder in $a \Longrightarrow b$ jeweils 4 mögliche Wertepaare $(W(a), W(b))$. Die so entstehenden (d.h. gemäß Def. 2.1.1 und 2.1.2 berechneten) Wahrheitswertverläufe lassen sich in einer Tabelle zusammenstellen:

a	b	$a \wedge b$	$a \Longrightarrow b$
1	1	1	1
1	0	0	0
0	1	0	1
0	0	0	1

Solche Tabellen werden rasch unübersichtlich, wenn die Anzahl der Teilausdrücke zunimmt. Bei 3 Teilausdrücken hat die Tabelle schon 8 Zeilen, und allgemein sind bei n Teilausdrücken 2^n Zeilen zu berechnen!

■ 2.1.4. Definition

Zwei Ausdrücke heißen (logisch) gleichwertig, wenn ihre Wahrheitswertverläufe übereinstimmen. Ein Ausdruck heißt tautologisch (oder: Tautologie), wenn in seinem Wahrheitswertverlauf nur 1 vorkommt.

■ 2.1.5. Proposition

(1) a gleichwertig $\neg \neg a$

(2) $a \Longrightarrow b$ gleichwertig $\neg (a \wedge \neg b)$

(3) $a \Longrightarrow b$ gleichwertig $\neg b \Longrightarrow \neg a$

(4) $\neg (a \wedge b)$ gleichwertig $\neg a \vee \neg b$

(5) $\neg (a \vee b)$ gleichwertig $\neg a \wedge \neg b$

■ Beweis

Durch Vergleich der Wahrheitswertverläufe in einer Tabelle (als Übung).

■ Bemerkungen

1. Die Gleichwertigkeitsbehauptungen in Prop. 2.1.5 führen z.T. traditionelle Namen: Gesetz (1) der doppelten Negation, (3) der Kontraposition, (4) & (5) von de Morgan.

2. Einfache Beispiele tautologischer Ausdrücke sind: $a \vee \neg a$, $0 \Longrightarrow a$, $(\neg a \Longrightarrow 0) \Longrightarrow a$ sowie $(a \wedge (a \Longrightarrow b)) \Longrightarrow b$. (Beweis als Übung).

■ 2.1.6. Proposition

Sind a und b gleichwertige Ausdrücke, so ist $a \Longleftrightarrow b$ eine Tautologie.

■ Beweis

Die Behauptung ergibt sich direkt aus Prop. 2.1.3,(2). ◆

2.2. Mengenoperationen

■ Boolesche Operationen

Hierbei handelt es sich um ein- oder zweistellige Operationen mit Mengen, die mit Hilfe logischer Junktoren definiert werden. Ihre Bezeichnung geht auf G. Boole (1815-1869) zurück.

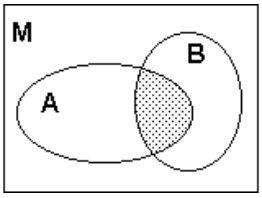
Für die Definition der booleschen Operationen ist es zweckmäßig, von einer Grundmenge M auszugehen und deren Teilmengen zu betrachten.

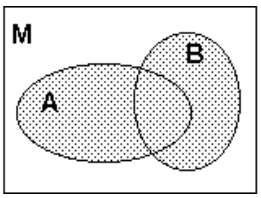
■ 2.2.1. Definition

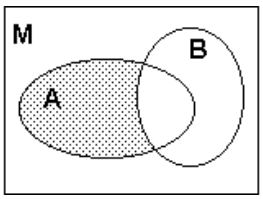
Seien A, B Teilmengen von M. Dann werden Durchschnitt, Vereinigung und Differenz beziehentlich wie folgt festgelegt:

$$A \bigcap B = \{x \in M \mid x \in A \wedge x \in B\}$$
$$A \bigcup B = \{x \in M \mid x \in A \vee x \in B\}$$
$$A \setminus B = \{x \in M \mid x \in A \wedge x \notin B\}$$

■ Veranschaulichung durch Mengendiagramme (Venn-Diagramme)



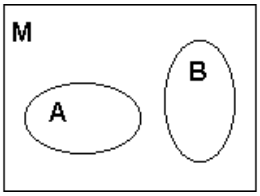




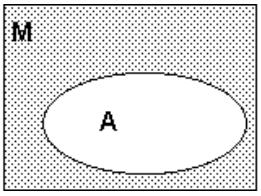
■ Beispiel

Sei $M = \{1, 2, 3, 4, 5\}$, $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$. Dann ergibt sich: $A \cap B = \{2, 3\}$ ("A geschnitten (mit) B"), $A \cup B = \{1, 2, 3, 4\}$ ("A vereinigt (mit) B") und $A \setminus B = \{1\}$ ("A ohne bzw. minus B").

Zwei Mengen A, B heißen disjunkt (oder: elementfremd), wenn $A \cap B = \emptyset$. Die Mengen {1, 2, 3} und {4, 5} sind disjunkt:



Die Differenz $M \setminus A$ heißt Komplement von A (in M), abgekürzt als: A^c (sofern die Bezugsmenge M aus dem Zusammenhang hervorgeht):



Die Vereinigungsmenge zweier Mengen A und B enthält genau die Elemente, die in A oder in B liegen. Das hier benutzte "oder" (Adjunktion) ist einschließend, d.h. ein Element, das sowohl in A als auch in B liegt, gehört auch zur Vereinigung. Schließt man diesen Fall (und damit den Durchschnitt der beiden Mengen) aus, so gelangt man zur sog. booleschen Summe (die der Disjunktion, d.h. der "entweder-oder"-Partikel entspricht):

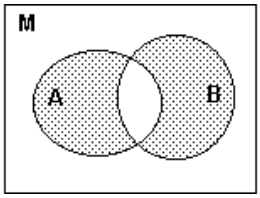
■ 2.2.2. Definition

$$A + B = (A \cup B) \setminus (A \cap B)$$

■ Bemerkung

Man überzeugt sich unschwer von folgender Identität (Übung!):

$$A + B = (A \setminus B) \cup (B \setminus A)$$



Gelegentlich heißt die boolesche Summe (daher) auch "symmetrische Differenz".

■ Kartesisches Produkt (Mengenprodukt)

Ausgehend von Mengen A, B lässt sich in sinnfälliger Weise eine Produktmenge als Gesamtheit aller geordneten Paare (x, y) konstruieren; dabei werden $x \in A$ und $y \in B$ gewählt. Die so entstehende Menge wird mit $A \times B$ bezeichnet und kartesisches Produkt (auch: Mengenprodukt) von A und B genannt.

■ 2.2.3. Definition

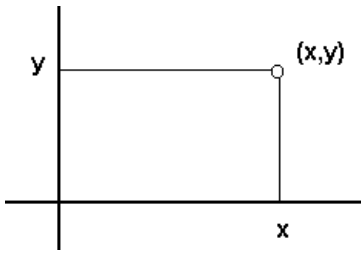
$$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$$

Ein geordnetes Paar (x, y) ist als eine Folge der Länge 2 aufzufassen, deren erstes Glied x und deren zweites Glied y ist. Die definierende Eigenschaft des kartesischen Produkts macht zwar von einem Junktor ($\wedge$) Gebrauch, benützt darüber hinaus aber in Gestalt des geordneten Paars auch den Begriff der Folge (Zuordnung zu Platznummern). Insofern zählt das Mengenprodukt nicht zu den booleschen Operationen.

■ Beispiele

1. Ein Schachbrettfeld wird durch einen Spaltennamen aus $S = \{a, b, c, d, e, f, g, h\}$ und einen Zeilennamen aus $Z = \{1, 2, 3, 4, 5, 6, 7, 8\}$ gekennzeichnet. Bei Spielbeginn steht etwa der weiße Bauer auf dem Feld e2, die schwarze Dame auf d8, usw. Das gesamte Schachbrett besteht aus 64 Feldern $(s, z) \in S \times Z$.

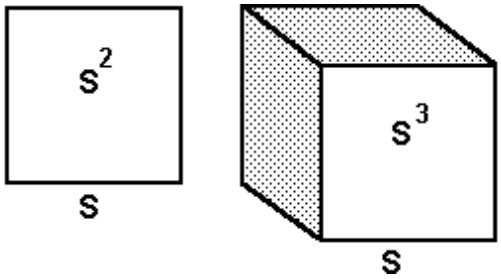
2. Die beim kartesischen Produkt beteiligten Mengen können auch identisch sein. So liefert das Produkt $\mathbb{N} \times \mathbb{N}$ die geeignete mengensprachliche Darstellung des sich im ersten Quadranten ausdehnenden Zahlengitters (der Paare aus positiven ganzen Zahlen). Dasselbe gilt für die reelle Zahlenebene, die man sich als Produkt $\mathbb{R} \times \mathbb{R}$ vorstellen kann; seine Elemente (x, y) werden bekanntlich als kartesische Koordinaten des zugehörigen Punkts bezeichnet:



Kartesische Produkte lassen sich zwanglos auf mehr als zwei Mengen verallgemeinern. Dazu sind lediglich mehrgliedrige (anstelle von zweigliedrigen) Elementfolgen zu betrachten. Allgemein wird das kartesische Produkt von n Mengen $A_1, \ldots, A_n$ definiert als Menge aller n-gliedrigen Folgen (sog. n-Tupel) $(x_1, \ldots, x_n)$, deren k-te Komponente x_k Element von A_k ist:

$$A_1 \times \ldots \times A_n = \{(x_1, \ldots, x_n) \mid x_1 \in A_1 \wedge \ldots \wedge x_n \in A_n\}$$

Ist etwa S eine Strecke (aufgefasst als Menge der auf ihr liegenden Punkte), dann entspricht $S^2 = S \times S$ der aus der Strecke gebildeten Quadratfläche, $S^3 = S \times S \times S$ dem Würfel, usw.:



S^2 und S^3 sind dabei die Menge der Flächenpunkte (x, y) bzw. Raumpunkte (x, y, z) mit $x, y, z \in S$.

2.3. Potenzmenge

Welches sind die Teilmengen von $M = \{1, 2, 3\}$? Die Antwort erhält man am leichtesten durch eine Aufzählung der Teilmengen nach ihrer Anzahl:

Anzahl = 0 : $\emptyset$

Anzahl = 1 : {1}, {2}, {3}

Anzahl = 2 : {1, 2}, {1, 3}, {2, 3}

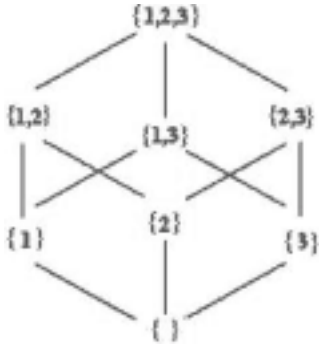
Anzahl = 3 : {1, 2, 3}

Diese 8 Teilmengen von M lassen sich wiederum zu einer Menge zusammenfassen, die man Potenzmenge von M nennt und mit $\mathcal{P}(M)$ bezeichnet. Die Potenzmenge ist also stets eine Menge von Mengen:

$\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

■ Ordnungsdiagramm

Die Elemente der Potenzmenge von {1, 2, 3} lassen sich übersichtlich in einem Diagramm anordnen:



Eine Kante steht dabei für eine Inklusionsbeziehung. Berücksicht man, dass $\subseteq$ transitiv ist, so enthält dass Diagramm sämtliche Inklusionen zwischen den Teilmengen von {1, 2, 3}.

■ 2.3.1. Definition

$\mathcal{P}(A) = \{X \mid X \subseteq A\}$

■ Bemerkung

Für endliche Mengen ist im Prinzip klar, wie ihre Potenzmengen zu bilden sind (bei unendlichen Mengen, etwa $\mathbb{Z}$ oder gar $\mathbb{R}$, liegen die Dinge komplizierter). Die Bildung der Potenzmenge erfolgt offensichtlich nicht nach dem Prinzip der Aussonderung (dazu müsste ja eine geeignete Obermenge bekannt sein!). Man sieht sie daher als ein eigenes Prinzip der Mengenbildung an, durch das eine im Vergleich mit der Ausgangsmenge echt "größere" Menge erzeugt wird. Für endliche Mengen lässt sich dies direkt nachvollziehen (für unendliche Mengen bedarf es dazu subtilerer Überlegungen).

Wir betrachten der Reihe nach die Potenzmengen der leeren Menge, einer 1-elementigen und einer 2-elementigen Menge:

$\mathcal{P}(\emptyset) = \{\emptyset\}$ (und nicht etwa $= \emptyset$!)

$\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$

$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

Es liegt die Vermutung nahe: Die Potenzmenge einer Menge A von n Elementen besitzt 2^n Elemente (Beweis dazu in Kapitel 3). Daher der Name!

2.4. Algebra der Mengen

Legt man die in 2.2 eingeführten Operationen zu Grunde, so lässt sich mit Mengen ähnlich rechnen wie mit Zahlen. Wir wollen uns im Folgenden auf boolesche Operationen beschränken.

Sei M eine für alles Weitere fest gewählte Grundmenge (d.h. gemeinsame Obermenge aller zu betrachtenden Mengen $A, B, C, \ldots$). Die booleschen Operationen werden somit in der Potenzmenge $\mathcal{P}(M)$ ausgeführt.

■ 2.4.1. Proposition

Für beliebige A, B, C gilt:

(1) $A \cap B = B \cap A$

(1') $A \cup B = B \cup A$

(2) $A \cap (B \cap C) = (A \cap B) \cap C$

(2') $A \cup (B \cup C) = (A \cup B) \cup C$

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

(3') $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

■ Bemerkung

(1) und (1') sind Kommutativgesetze, (2) und (2') Assoziativgesetze, (3) und (3') sind Distributivgesetze, die an ihre arithmetischen Analoga erinnern (vgl. 1.2.1). Allerdings gilt für Mengen ein zweites Distributivgesetz (3'), dessen Gegenstück in der Arithmetik $a + (b \cdot c) = (a + b) \cdot (a + c)$ *nicht* gilt!

■ Beweis zu 2.4.1

Die behaupteten Gleichungen geben einfache logische Beziehungen wieder, die sich rein schematisch durch Zugehörigkeitstafeln verifizieren lassen. Darunter ist (in Analogie zu den Wahrheitswerttabellen aus 2.1) ein Fallunterscheidungsschema zu verstehen, das sämtliche Fälle behandelt, die hinsichtlich der Zugehörigkeit eines beliebigen Elementes x von M zu einer der beteiligten Mengen $A, B, C, \ldots$ auftreten können.

Zum Beispiel gibt es für ein Element aus M bei den drei in (3') genannten Mengen 2^3 (= 8) mögliche Fälle von Zugehörigkeit (+) bzw. Nicht-Zugehörigkeit (−):

A	B	C	$A \cup B$	$A \cup C$	$B \cap C$	$A \cup (B \cap C)$	$(A \cup B) \cap (A \cup C)$
+	+	+	+	+	+	+	+
+	+	−	+	+	−	+	+
+	−	+	+	+	−	+	+
−	+	+	+	+	+	+	+
+	−	−	+	+	−	+	+
−	+	−	+	−	−	−	−
−	−	+	−	+	−	−	−
−	−	−	−	−	−	−	−

Die in den letzten beiden Spalten angegebenen Wertverläufe für die linke und rechte Seite von (3') stimmen überein, d.h. ein beliebiges Element von M gehört genau dann zu $A \cup (B \cap C)$, wenn es zu $(A \cup B) \cap (A \cup C)$ gehört. Die Identität (3') ergibt sich somit direkt nach Definition 1.1.1,(3).

Die Überlegungen zu (1,1',2,2',3) sind völlig analog durchzuführen (als Übung).◆

Über das Komplement und sein Zusammenspiel mit Inklusion, Durchschnitt und Vereinigung gibt der folgende Lehrsatz Auskunft.

■ 2.4.2. Proposition

Für beliebige A, B gilt:

(1) $(A^c)^c = A$

(2) $M^c = \emptyset, \emptyset^c = M$

(3) $A \cup A^c = M, A \cap A^c = \emptyset$

(4) $A \subseteq B \Longleftrightarrow B^c \subseteq A^c$

(5) $(A \cup B)^c = A^c \cap B^c$

(5') $(A \cap B)^c = A^c \cup B^c$

■ Bemerkung

Die Gleichungen (5) und (5') heißen erstes bzw. zweites de Morgansches Gesetz. Die Beweise zu (1)-(4) sind unmittelbar, zu (5,5') anhand von Zugehörigkeitstafeln zu führen (als Übung!).◆

■ 2.4.3. Proposition

Für beliebige A, B, C gilt:

(1) $A + (B + C) = (A + B) + C$

(2) $A + B = B + A$

(3) $A + \emptyset = A$

(4) $A + A = \emptyset$

■ Beweis

Mit Hilfe von Zugehörigkeitstafeln (als Übung!).◆

■ Bemerkung

Prop. 2.4.2 gestattet es z.B., die Gleichung $A + X = B$ in algebraischer Manier zu lösen. Übungshalber vollziehe man die bei jedem Schritt angewendeten Regeln nach:

$$A + X = B$$
$$A + (A + X) = A + B$$
$$(A + A) + X = A + B$$
$$\emptyset + X = A + B$$
$$X = A + B$$

Die Lösung $X = A + B$ ist unmittelbar durch Einsetzen in die Ausgangsgleichung ("Probe") zu bestätigen.

3. Vollständige Induktion

Im gewöhnlichen Sprachgebrauch unterscheidet man zwischen Deduktion und Induktion. Man spricht von Deduktion, wenn eine strenge Ableitung einer Aussage aus bestimmten Voraussetzungen (kurzum: ein Beweis) gemeint ist. Der Begriff "Induktion" ist hingegen weniger klar festgelegt. Häufig denkt man dabei an eine Art Begründung (Stützung) allgemeiner Aussagen auf der Grundlage (meist zahlreicher) Einzelfälle. Eine solche Form der Induktion kann nur heuristischen Wert haben; schließlich genügt ein einziges Gegenbeispiel, um eine allgemeine Behauptung zu widerlegen.

Beispiel für eine vorschnelle Verallgemeinerung: $\mathcal{E}(n)$ stehe für "$n^2 - 79\,n + 1601$ ist eine Primzahl". – Prüft man $\mathcal{E}(1)$, $\mathcal{E}(2)$, $\mathcal{E}(3)$ usw., so ist man vielleicht versucht zu glauben, $\mathcal{E}(n)$ sei für alle natürlichen Zahlen $n \geq 1$wahr. Für $n \leq 79$ bestätigt sich dies; allerdings ist die Aussage $\mathcal{E}(80)$ falsch!

Eine Induktionsregel der Art, wonach aus der Gültigkeit von Einzelaussagen $\mathcal{E}(1)$, $\mathcal{E}(2)$, …, $\mathcal{E}(k)$ irgendwie die Gültigkeit von $\mathcal{E}(n)$ für alle $n \geq 1$zu gewinnen wäre, kann es also nicht geben. Die in der Mathematik geübte Induktion verfährt denn auch anders.

3.1. Das allgemeine Induktionsschema

Die natürlichen Zahlen leiten sich her vom Vorgang des Zählens:

$$|\ ,\ ||\ ,\ |||\ ,\ ||||\ ,\ |||||\ ,\ \ldots$$

Die Figuren dieser Folge entstehen aus der leeren Figur (die der 0 entspricht) durch sukzessives Anhängen eines weiteren Strichs an eine einmal erzeugte Figur (Zählfigur). Die drei Punkte hinter der zuletzt angegebenen Figur deuten an, dass das Zählen prinzipiell beliebig fortgesetzt werden kann.

Ist n eine Zählfigur, so heißt $n|$ Nachfolger von n. Mit 0 wird die leere Zählfigur bezeichnet, mit 1 ihr Nachfolger, usw.: $1 = 0|$, $2 = 1|$, $3 = 2|$, … . Die gewöhnliche Addition wird so erklärt, dass $n| = n + 1$ gilt. Auf der Grundlage dieser Konstruktion denken wir uns die Menge $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ der natürlichen Zahlen (einschließlich Null) gegeben. Es handelt sich um eine unendliche Menge: Alle erzeugten Zählfiguren sind verschieden, und mit $n \in \mathbb{N}_0$ ist auch $n + 1 \in \mathbb{N}_0$. (Dasselbe gilt auch für die Menge $\mathbb{N}$.)

Vor diesem Hintergrund lässt sich die Induktion (gelegentlich auch vollständige Induktion genannt) als ein Prinzip gewinnen, das es gestattet, All-Aussagen über natürliche Zahlen zu begründen, und zwar wie folgt:

Vorgelegt sei eine von n abhängige Formel $\mathcal{E}(n)$. Es soll gezeigt werden, dass $\mathcal{E}(n)$ für alle $n \in \mathbb{N}_0$ gilt. Dazu geht man in zwei Schritten vor:

1. Induktionsanfang ($n = 0$): Zeige $\mathcal{E}(0)$

2. Induktionsschluss ($n \to n+1$): Zeige $\mathcal{E}(n) \Longrightarrow \mathcal{E}(n+1)$ für beliebiges $n \geq 0$

Nach Durchführung *beider* Schritte liefert das Induktionsprinzip: Für alle $n \geq 0$ gilt $\mathcal{E}(n)$.

■ Erläuterung

Der Induktionsanfang sichert, dass die fragliche Eigenschaft (Formel) $\mathcal{E}$ auf 0 zutrifft. Dabei kann auch eine andere Startzahl als 0 verwendet werden; in einem solchen Fall liefert die Induktion dementsprechend die Gültigkeit für alle $n \geq$ Startzahl.

Der Induktionsschluss besagt, dass sich die Eigenschaft $\mathcal{E}$ von einer (beliebigen) natürlichen Zahl n auf deren Nachfolger $n+1$ vererbt. Ist dies erst einmal gezeigt, so ergibt sich aus $\mathcal{E}(0)$ sofort $\mathcal{E}(1)$, daraus wiederum $\mathcal{E}(2)$, $\mathcal{E}(3)$, usw. Die Gültigkeit von $\mathcal{E}(n)$ für ein vorgegebenes n ergibt sich somit in n derartigen Vererbungsschritten.

Der Induktionsschluss besteht im Beweis der Subjunktion $\mathcal{E}(n) \Longrightarrow \mathcal{E}(n+1)$. Nach dem, was dazu in Bemerkung (1) im Anschluss an Prop. 2.1.3 gesagt wurde, verläuft die erforderliche Argumentation im Prinzip wie folgt: Man nimmt an, $\mathcal{E}(n)$ gelte für ein n (sog. Induktionsvoraussetzung). Anschließend hat man (unter Verwendung der Induktionsvoraussetzung!) zu zeigen, dass auch $\mathcal{E}(n+1)$ gilt (sog. Induktionsbehauptung). Wichtig: Mit der Induktionsvoraussetzung wird keinesfalls unterstellt, $\mathcal{E}(n)$ sei für alle n wahr!

■ Prinzip der (vollständigen) Induktion

> Sei $\mathcal{E}(n)$ eine von n abhängige Formel ($n \in \mathbb{N}_0$). Gilt $\mathcal{E}(0)$ und ist $\mathcal{E}$ nachfolgererblich, d.h. gilt $\mathcal{E}(n) \Longrightarrow \mathcal{E}(n+1)$ für alle n, so trifft $\mathcal{E}$ auf alle natürlichen Zahlen zu, d.h. für alle $n \geq 0$ gilt $\mathcal{E}(n)$.

Das Induktionsprinzip wird hier nicht bewiesen wie ein gewöhnlicher arithmetischer Satz. Dennoch ist es keine unbegründete Annahme. Eine intuitive Begründung (wie sie aus der obigen Erläuterung hervorgeht) greift auf die Konstruktion der natürlichen Zahlen durch den Zählprozess zurück. Die Induktion wird in der gesamten Mathematik als ein grundlegendes und allgemeines Beweisschema akzeptiert und praktiziert.

3.2. Beispiele

Anhand einer Reihe von Muster-Beispielen soll nun gezeigt werden, wie man das Induktionsprinzip zum Beweis mathematischer Aussagen benutzt. Die Frage, wie man auf die betreffenden Aussagen kommt, bleibt dabei zunächst ausgeklammert. Die Induktion ist zumeist ein nachträglich anzuwendendes Beweisverfahren.

■ 3.2.1. Proposition

$$\text{Für } x \neq 1 \text{ und } n \geq 1 \text{ gilt}: 1 + x + \ldots + x^{n-1} = \frac{x^n - 1}{x - 1}$$

Vgl. hierzu Prop. 1.6.2,(2).

■ Beweis

1. Induktionsanfang $n = 1$: Die Behauptung lautet dann $1 = \frac{x-1}{x-1}$, was offensichtlich richtig ist.

2. Induktionsschluss $n \to n+1$: Die Formel werde für ein (festes, aber beliebiges) $n \geq 1$ als gültig angenommen (Ind.vor.). Nachzuweisen ist die Gültigkeit der Formel für den Nachfolger $n+1$. Dazu wird der Term $x^{(n+1)-1}$ auf beiden Seiten (der Ind.vor.) addiert:

$$1 + x + \ldots + x^{n-1} + x^n = \frac{x^n - 1}{x - 1} + x^n$$

Schreibt man den Ausdruck rechts vom Gleichheitszeichen mit gemeinsamem Nenner, so ergibt sich:

$$1 + x + \ldots + x^n = \frac{x^{n+1} - 1}{x - 1}$$

Aus 1. und 2. ergibt sich nach dem Induktionsprinzip die Gültigkeit der behaupteten Gleichung für alle natürlichen Zahlen $n \geq 1$.◆

■ 3.2.2. Proposition

Für alle $n \geq 3$ gilt: $2^n > 2n + 1$

■ Beweis

1. Induktionsanfang $n = 3$: linke Seite (l.S.) $= 2^3 = 8$; rechte Seite (r.S.) $= 2 \cdot 3 + 1 = 7$. Also l.S. > r.S.

2. Induktionsschluss $n \to n+1$: Es gelte $2^n > 2n + 1$ für ein $n \geq 3$ (Ind.vor.). Es ist zu zeigen (Ind.beh.): $2^{n+1} > 2(n+1) + 1$. Um auf der l.S. der Ungleichung 2^{n+1} zu erhalten, multiplizieren wir die Ind.vor. mit 2. Nach dem Monotoniegesetz (1.3.1,(6)) ergibt sich: $2^n \cdot 2 > 2(2n + 1) = 4n + 2$. Für $n \geq 3$ ist aber gewiss $4n + 2 > 2n + 3 = 2(n+1) + 1$, also insgesamt: $2^{n+1} > 2(n+1) + 1$.◆

■ 3.2.3. Proposition

Sei M eine (endliche) Menge von n Elementen, $n \geq 0$. Die Potenzmenge von M hat dann 2^n Elemente.

■ Beweis

1. Induktionsanfang $n = 0$: In diesem Fall ist $M = \emptyset$ und $\mathcal{P}(M) = \{\emptyset\}$, die Potenzmenge hat also $2^0 = 1$Elemente.

2. Induktionsschluss $n \to n+1$: Sei M eine Menge von n Elementen; ihre Potenzmenge besitzt 2^n Elemente (Ind.vor.). Durch Hinzunahme eines neuen (d.h. in M nicht enthaltenen) Elements a erweitern wir M zu einer Menge $M' = M \cup \{a\}$ von $n+1$ Elementen. Es ist zu zeigen (Ind.beh.): $\mathcal{P}(M')$ hat 2^{n+1} Elemente.

Sei $X \subseteq M'$ beliebig. X ist genau dann eine Teilmenge von M, wenn $a \notin X$. Von diesen gibt es nach Ind.vor. 2^n. Sei nun $a \in X \subseteq M'$. Wir entfernen a und erhalten: $X \setminus \{a\} \subseteq M' \setminus \{a\} = M$. Also gibt es (wiederum nach Ind.vor.) auch 2^n Teilmengen $X \setminus \{a\}$. Fügen wir a wieder hinzu, so resultiert daraus dieselbe Anzahl (2^n) von $X \subseteq M'$ mit $a \in X$. Da

keine Teilmenge, die a nicht enthält, mit einer Teilmenge, die a enthält, übereinstimmt, erhalten wir die Anzahl von $\mathcal{P}(M')$ als die Summe $2^n + 2^n = 2^{n+1}$.◆

Den Gebrauch des Induktionsprinzips erlernt man nach und nach durch das Studium von Muster-Beispielen und – vor allen Dingen – durch eigene Beweistätigkeit. Zu diesem Zweck werden im Folgenden zusätzliche Beispiel-Aussagen aufgeführt, die (wie schon Prop. 3.2.1-3.2.3) auch für sich genommen von Interesse sind.

■ 3.2.4. Proposition

$$\text{Für alle natürlichen Zahlen } n \geq 1 \text{ gilt}: 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

Vgl. hierzu Prop. 1.6.2,(1).

■ 3.2.5. Proposition

$$\text{Für alle natürlichen Zahlen } n \geq 1 \text{ gilt}: 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

■ 3.2.6. Proposition

Für alle $n \geq 1$ gilt: Eine Kreisfläche lässt sich durch n gerade, von Rand zu Rand laufende Schnitte in höchstens $\frac{1}{2}(n^2 + n + 2)$ Teile zerlegen.

Das Bild illustriert den Fall $n = 2$:

■ Beweise zu 3.2.4-6

In der Vorlesung bzw. in den Übungen!

■ Hinweise auf weitere Quellen zur vollständigen Induktion

1. **`http://www.uni-flensburg.de/mathe/zero/aufgaben/_induktion/_induktion.html`**

2. Schüler-Hefte III und XXVI der "Kleinen Ergänzungsreihe zu den Hochschulbüchern für Mathematik" (VEB Deutscher Verlag der Wissenschaften): Sominski, *Die Methode der vollständigen Induktion*, 11. Aufl. 1974; sowie: Golowina/Jaglom, *Vollständige Induktion in der Geometrie*, 1973.

3.3. Das Prinzip der kleinsten Zahl

In Beweisen und Definitionen wird häufig von einer Tatsache Gebrauch gemacht, die anschaulich völlig einleuchtend erscheint: Es sei $\mathcal{E}$ eine Eigenschaft, die wenigstens einer natürlichen Zahl zukommt, d.h. es gilt $\mathcal{E}(n)$ für ein $n \in \mathbb{N}_{(0)}$; dann gibt es eine kleinste natürliche Zahl m mit $\mathcal{E}(m)$. Dieses sog. Prinzip der kleinsten Zahl (PdkZ) lässt sich auch in der Mengensprache ausdrücken:

■ 3.3.1. Proposition

> Sei M eine nichtleere Menge natürlicher Zahlen: $\emptyset \neq M \subseteq \mathbb{N}_0$. Dann gibt es in M ein kleinstes Element, d.h. ein $m \in M$ derart, dass $m \leq k$ für alle $k \in M$.

■ Beispiel

Seien a, b irgendwelche positiven ganzen Zahlen, etwa $a = 6$, $b = 8$. Die Vielfachen von a lauten: 6, 12, 18, 24, 30, usw.; die Vielfachen von b: 8, 16, 24, 32, usw. Die beiden Vielfachen-Mengen sind nicht disjunkt, es findet sich sogar ein kleinstes gemeinsames Vielfaches: 24. – Ist das immer so? Ja! Denn jedenfalls ist $a \cdot b$ ein gemeinsames Vielfaches von a und b, weshalb es nach dem PdkZ auch ein kgV beider Zahlen geben muss.

■ Beweis von 3.3.1

Wir nehmen indirekt an, M besitze kein kleinstes Element, und zeigen mittels vollständiger Induktion die Behauptung: $\{0, 1, \ldots, n\} \cap M = \emptyset$ für alle $n \geq 0$.

1. Ind.anf. $n = 0$: Wäre $0 \in M$, so wäre 0 jedenfalls kleinstes Element von M (entgegen der indirekten Annahme); also $\{0\} \cap M = \emptyset$.

2. Ind.schluss $n \to n + 1$: Sei $\{0, 1, \ldots, n\} \cap M = \emptyset$, d.h. die Zahlen 0, 1, …, n sämtlich nicht in M. Dann gehört auch $n + 1$ nicht zu M, da sonst $n + 1$ kleinstes Element von M wäre. Somit $\{0, 1, \ldots, n + 1\} \cap M = \emptyset$.

Aus 1. und 2. ergibt sich die Behauptung. Dann muss aber M leer sein, im Widerspruch zur Voraussetzung.◆

■ Ergänzende Bemerkungen (bei der Erstlektüre zu überspringen)

(1) Das kleinste Element von M (in Prop. 3.3.1) ist eindeutig bestimmt (Übung!). Es wird mit $\operatorname{Min} M$ bezeichnet.

(2) Ist $M \subseteq \mathbb{N}$ endlich, so gibt es ein größtes Element in M (bezeichnet als $\operatorname{Max} M$). Man identifiziert mit Hilfe des PdkZ zunächst die kleinste Zahl $m > k$ für alle $k \in M$. Es ist dann $m - 1$ das Maximum von M.

(3) Prop. 3.3.1 besagt: Induktionsprinzip $\Longrightarrow$ PdkZ. Umgekehrt lässt sich aber auch das Induktionsprinzip aus dem PdkZ herleiten. Beweisskizze (für theoretisch Interessierte): Sei $\mathcal{E}$ eine Eigenschaft, für die Induktionsanfang und Induktionsschluss verifiziert sind. Beh.: $\mathcal{E}(n)$ gilt für alle $n \geq 0$. – Bew.: Wir nehmen indirekt an, es gäbe ein a, für das $\mathcal{E}(a)$ *nicht* gilt. Sei A die Menge dieser Ausnahmezahlen a; sie ist nichtleer und hat nach dem PdkZ ein Minimum a_0. Es ist $a_0 > 0$, da gemäß Ind.anf. $0 \notin A$; mithin gilt $a_0 - 1 \geq 0$. Aus $a_0 - 1 < a_0$ und der Minimalität von a_0 erhalten wir $a_0 - 1 \notin A$, und d.h.: $\mathcal{E}(a_0 - 1)$. Der Ind.schluss liefert dann die Aussage $\mathcal{E}(a_0)$, im Widerspruch zu $a_0 \in A$.

(4) Zu weiteren Varianten der Induktion und ihrer logischen Beziehung untereinander vgl. A. Schreiber: Über die vollständige Induktion und das sog. induktive Schließen. In: Beiträge zum math.-naturwiss. Unterricht, Heft 35 (1979), 20-31 [als PDF-Datei verfügbar unter **www.alfred-schreiber.de**].

Das PdkZ hat zahlreiche Anwendungen, von denen wir einige noch in späteren Kapiteln kennenlernen werden. Das folgende Anwendungsbeispiel mag die Ausführungen zu Abschnitt 1.2 ergänzen:

■ 3.3.2. Proposition

$\sqrt{2}$ ist irrational.

■ Beweis

Wir nehmen indirekt an, $\sqrt{2}$ wäre rational. Dann ließe sich $\sqrt{2} = \frac{n}{m}$ mit geeigneten natürlichen Zahlen m, n darstellen. Es wäre somit $m\sqrt{2}$ $(= n)$ eine natürliche Zahl. Wir definieren nun die Menge $M = \{m \in \mathbb{N} \mid m\sqrt{2} \in \mathbb{N}\}$. M ist nichtleer; nach dem PdkZ (Prop. 3.3.1) hat sie also ein kleinstes Element $m_0 \in M$. Es ist aber leicht zu sehen, dass die positive (!) Zahl $m_0(\sqrt{2} - 1)$ ein noch kleineres Element von M ist. Dies ist ein Widerspruch! ◆

[Sicherheitshalber wollen wir hier die Floskel ("leicht zu sehen") einmal auf die Probe stellen. Wir überprüfen, ob die angegebene kleinere Zahl zu M gehört, und werten dazu die Klammer aus: $m_0(\sqrt{2} - 1)\sqrt{2} = 2m_0 - m_0\sqrt{2}$. Definitionsgemäß ist $m_0\sqrt{2} \in \mathbb{N}$, also gilt auch $2m_0 - m_0\sqrt{2} \in \mathbb{N}$. Schließlich gilt $1 < \sqrt{2}$ und daher $0 < m_0(\sqrt{2} - 1)$. Diese Kleinigkeiten waren noch zu überlegen.]

4. Arithmetische Folgen

4.1. Differenzenrechnung

Arithmetische Folgen (A.F.) $x_0, x_1, x_2, \ldots$sind (nach der Def. 1.5.1) durch die Eigenschaft gekennzeichnet, dass benachbarte Folgenglieder stets dieselbe Differenz d haben, d.h. $x_{n+1} - x_n = d$ für alle $n \in \mathbb{N}_0$.

Im Weiteren beschäftigen wir uns systematisch mit dem Übergang von einer Zahlenfolge zu der Folge der Differenzen ihrer (benachbarten) Glieder.

■ 4.1.1. Definition

Ist (x_n) eine beliebige Zahlenfolge, so wird definiert $\Delta x_n := x_{n+1} - x_n$ $(n \in \mathbb{N}_0)$. Die Differenzen $\Delta x_0, \Delta x_1, \Delta x_2, \ldots$bilden eine neue Folge, die sog. Differenzenfolge, notiert: (Δx_n). Das Symbol Δ (gelesen: Delta) nennen wir Differenzen-Operator.

■ Beispiele

Sei (x_n) die Folge: $4, -7, 1, 0, 5, 2, 1, 1$. Dann lautet die Differenzenfolge (Δx_n): $-11, 8, -1, 5, -3, -1, 0$.

Ist die Folge durch ein allgemeines Bildungsgesetz gegeben, so ist der Differenzen-Operator direkt auf den entsprechenden Ausdruck anzuwenden. Zum Beispiel ergibt sich für die Folge (c_n) aus 1.5,(3):
$\Delta c_n = \Delta\left(\frac{1}{2}(n+1)(n+2)\right) = \frac{1}{2}(n+2)(n+3) - \frac{1}{2}(n+1)(n+2) = \frac{1}{2}(n+2)(n+3-n-1) = n+2$

Man kann die Anwendung von Δ nach Belieben wiederholen:

$$\Delta^2 x_n := \Delta(\Delta x_n) = \Delta x_{n+1} - \Delta x_n = (x_{n+2} - x_{n+1}) - (x_{n+1} - x_n) = x_{n+2} - 2x_{n+1} + x_n$$

$$\Delta^3 x_n := \Delta(\Delta^2 x_n) = \Delta^2 x_{n+1} - \Delta^2 x_n = x_{n+3} - 3x_{n+2} + 3x_{n+1} - x_n$$

usf.

Es ist naheliegend, noch zu setzen: $\Delta^1 x_n := \Delta x_n$ und $\Delta^0 x_n := x_n$.

Die folgende Proposition zeigt, dass (bzw. wie) sich durch *Summation der Differenzen* die ursprüngliche Folge wieder zurückgewinnen lässt:

■ 4.1.2. Proposition

Für ganze Zahlen $n \geq m \geq 0$ gilt : $\sum_{k=m}^{n} \Delta x_k = x_{n+1} - x_m$

■ Beweis

Die Summe lautet ausgeschrieben: $(x_{m+1} - x_m) + (x_{m+2} - x_{m+1}) + \ldots + (x_{n+1} - x_n)$. Man erkennt ohne weiteres, dass sich alle bis auf zwei Folgenglieder wegheben. Es bleiben: $-x_m$ aus der ersten Klammer, x_{n+1} aus der letzten Klammer.◆

Für $m = 0$ ergibt sich aus Prop. 4.1 .2 speziell die Darstellung : $x_n = x_0 + \sum_{k=0}^{n-1} \Delta x_k \quad (n = 1, 2, \ldots)$.

4.2. Arithmetische Folgen höherer Ordnung

Prop. 1.5.2,(1) besagt, dass eine A.F. (x_n) sich stets in der Form $x_n = a\,n + b$ schreiben lässt; dabei sind a, b reelle Zahlen. Umgekehrt ist eine Folge dieser Form stets arithmetisch:

$$\Delta x_n = \Delta (a\,n + b) = a(n + 1) + b - (a\,n + b) = a$$

Es ist also a die konstante Differenz zwischen benachbarten Folgengliedern und b das Anfangsglied der Folge (wegen $x_0 = a \cdot 0 + b = b$).

Das Ergebnis lässt sich in folgender Bisubjunktion zusammenfassen:

(*) (x_n) ist A.F. $\Longleftrightarrow$ ex. $a, b \in \mathbb{R}$ mit $x_n = a\,n + b$ für alle $n \in \mathbb{N}_0$

Der Begriff der A.F. soll nun (durch die Einführung einer *Ordnung*) erweitert und verfeinert werden. Dazu betrachten wir noch einmal die Beispiel-Folge (c_n) aus 1.5,(3), für die wir oben bereits die Differenz(enfolge) berechnet haben:

$$\Delta c_n = n + 2$$

Zwar ist die Folge (c_n) selbst keine A.F.; ersichtlich ist aber ihre Differenzenfolge arithmetisch, d.h. die zweite Differenzenfolge konstant: $\Delta^2 c_n = \Delta (n + 2) = 1$. Die Folge (c_n) heißt aus diesem Grund A.F. 2-ter Ordnung. In entsprechender Weise definiert man A.F. 3-ter Ordnung, usw.

Allgemein:

■ 4.2.1. Definition

Sei $r \geq 0$ eine ganze Zahl. Eine Zahlenfolge (x_n) heißt arithmetische Folge der Ordnung r (oder: r-ter Ordnung), wenn die Folge der r-ten Differenzen $(\Delta^r x_n)$ konstant ($\neq 0$) ist.

■ Bemerkungen

1. Nach der früheren Def. 1.5.1 ist die aus lauter Nullen bestehende Folge 0, 0, 0, … eine A.F. Aber: Im Sinne der eben gefassten Def. 4.2.1 kann ihr *keine Ordnung* zugeschrieben werden.

2. Eine konstante Folge $a, a, a, \ldots$ mit $a \neq 0$ ist eine A.F. nach Def. 1.5.1. Da die ersten Differenzen sämtlich = 0 sind, ist sie *nicht* von 1-ter Ordnung; vielmehr erhält sie nach Def. 4.2.1 wegen $\Delta^0 (a) = a$ die Ordnung 0.

3. Ist (x_n) eine A.F. der Ordnung r, so gilt: $\Delta^{r+1} x_n = 0$ für alle $n \in \mathbb{N}_0$.

■ 4.2.2. Proposition

Sei $r \geq 1$ eine ganze Zahl. Dann gilt:

(x_n) ist A.F. der Ordnung $r \iff (\Delta^{r-1} x_n)$ ist A.F. der Ordnung 1

■ Beweis

1. "$\Longrightarrow$": Nach Def. 4.2.1 ist die Folge der r-ten Differenzen konstant gleich einem von Null verschiedenen Wert a, d.h. $\Delta^r x_n = a \neq 0$. Auf diese Folge wenden wir die Summation der Differenzen gemäß Prop. 4.1.2 an und beachten dabei $\Delta^r x_n = \Delta (\Delta^{r-1} x_n)$:

$$\Delta^{r-1} x_n = \Delta^{r-1} x_0 + \sum_{k=0}^{n-1} \Delta (\Delta^{r-1} x_k) = \Delta^{r-1} x_0 + \sum_{k=0}^{n-1} a = \Delta^{r-1} x_0 + n\, a$$

Es ist somit $(\Delta^{r-1} x_n)$ eine A.F. (vgl. dazu die Bisubjunktion (*) weiter oben). Wegen $\Delta^r x_n = a \neq 0$ hat die Folge die Ordnung 1.

2. "$\Longleftarrow$": Nach Def. 4.2.1 ist $(\Delta (\Delta^{r-1} x_n))$ konstant ($\neq 0$). Wir beachten wieder $\Delta^r x_n = \Delta (\Delta^{r-1} x_n)$ und erhalten: (x_n) ist eine A.F. der Ordnung r.◆

Die Frage liegt nahe: Wie sieht das allgemeine "Bildungsgesetz" einer arithmetischen Folge der Ordnung $r \geq 0$ aus?

Die nachstehende Aussage gibt eine Antwort für $r = 2$.

■ 4.2.3. Proposition

(x_n) ist A.F. der Ordnung 2 $\iff$ ex. $a, b, c \in \mathbb{R}$, $a \neq 0$, mit $x_n = a\, n^2 + b\, n + c$ für alle $n \in \mathbb{N}_0$

■ Beweis

1. "$\Longrightarrow$": Sei (x_n) irgendeine A.F. 2-ter Ordnung. Nach Prop. 4.2.2 ist dann (Δx_n) eine A.F. der Ordnung 1. Diese ist darstellbar in der Form: $\Delta x_n = a\, n + b$ mit reellen a, b, wobei $a \neq 0$ (nach Def. 4.2.1, da die Ordnung 1 ist). Summation der Differenzen gemäß Prop. 4.1.2 liefert dann (unter Beachtung von Prop. 1.6.1,(2)):

$$x_n = x_0 + \sum_{k=0}^{n-1} \Delta x_k = x_0 + \sum_{k=0}^{n-1} (b + a\, k) = x_0 + b\, n + a \sum_{k=0}^{n-1} k$$

Die zuletzt auftretende Summe haben wir schon früher (z.B. Prop. 3.2.4) ausgewertet zu $\frac{1}{2}(n-1)\,n$. Insgesamt ergibt sich damit: $x_n = x_0 + \left(b - \frac{a}{2}\right) n + \left(\frac{a}{2}\right) n^2$. Wegen $\frac{a}{2} \neq 0$ ist x_n daher von der behaupteten Form.

2. "⟸": Sei nun umgekehrt $x_n = a\,n^2 + b\,n + c$. Man bestätigt nach kurzer Rechnung (Übung!):
$\Delta^2 x_n = x_{n+2} - 2\,x_{n+1} + x_n = \ldots = 2\,a$. Da $a \neq 0$ vorausgesetzt ist, erweist sich (x_n) als A.F. 2-ter Ordnung nach Def. 4.2.1.◆

In Analogie zu Prop. 4.2.3 zeigt man, dass eine A.F. 3-ter Ordnung die Gestalt $x_n = a\,n^3 + b\,n^2 + c\,n + d$ (mit $a \neq 0$) hat, usw. für höhere Ordnungen. Der entsprechende allgemeine Lehrsatz werde hier ohne Beweis mitgeteilt:

■ 4.2.4. Proposition

$$(x_n) \text{ ist A.F. der Ordnung } r \iff \text{ex. } a_r, \ldots, a_1, a_0 \in \mathbb{R},\ a_r \neq 0, \text{ mit } x_n = \sum_{k=0}^{r} a_k\, n^k \text{ für alle } n \in \mathbb{N}_0$$

Für $r = 2$ ergibt sich aus dieser Aussage speziell Prop. 4.2.3.

■ Bemerkung

Die in 4.2.3 (bzw. 4.2.4) gegebene Kennzeichnung besagt: Das Bildungsgesetz x_n einer A.F. r-ter Ordnung ist eine Polynomfunktion vom Grade r mit $r + 1$ reellen Koeffizienten und ganzzahliger Veränderlicher $n \geq 0$; umgekehrt sind diese Polynomfunktionen stets A.F. der Ordnung r. Daher ist z.B. eine A.F. zweiter Ordnung bereits durch die 3 Koeffizienten a, b, c ihrer Polynomdarstellung festgelegt. Hieraus ergibt sich, dass eine A.F. der Ordnung 2 durch irgend drei ihrer Folgenglieder bestimmt ist (und über ein lineares Gleichungssystem berechnet werden kann).

■ Beispiel

Gesucht: eine A.F. (x_n) zweiter Ordnung mit $x_2 = 1$, $x_5 = 0$, $x_9 = 9$.

Lösung: Nach Prop. 4.2.3 ist $x_n = a\,n^2 + b\,n + c$ mit noch zu bestimmenden Koeffizienten a, b, c. Diese genügen aufgrund der oben vorgegebenen Folgenwerte den Bedingungen:

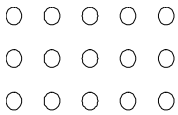
$$\begin{aligned} 4\,a + 2\,b + c &= 1 \\ 25\,a + 5\,b + c &= 0 \\ 81\,a + 9\,b + c &= 9 \end{aligned}$$

Nach Auflösung dieses Gleichungssystems (mittels Schulmethoden) ergibt sich für das allgemeine Glied der gesuchten Folge: $x_n = \frac{31}{84}\,n^2 - \frac{35}{12}\,n + \frac{75}{14}$.

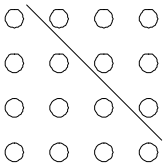
4.3. Figurenzahlen

Ein altes Mittel zur Darstellung natürlicher Zahlen sind Figuren, die man mit Steinchen oder Plättchen legen kann. Hieran erinnert noch das lateinische *calculus* (kleiner Kalkstein) und das davon abstammende Wort "Kalkulieren" (für Rechnen).

Steht ein Steinchen für die Zahl 1, so stellt eine Figur die Anzahl ihrer Steinchen dar. Zum Beispiel repräsentiert das folgende 3×5-Rechteck die Zahl 15 und weist gleichzeitig 3 und 5 als deren Teiler aus:



Durch geschickte Einteilungen der Steinchenmenge einer Figur lassen sich arithmetische Zusammenhänge aufdecken. Teilt man z.B. ein Quadrat entlang seiner Diagonalen, so erscheint es als Summe zweier aufeinanderfolgender Dreiecke:



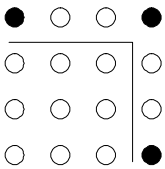
Dem entspricht die Gleichung: $16 = 4^2 = (1 + 2 + 3 + 4) + (1 + 2 + 3)$. Zählt man die Diagonale getrennt, so ergibt sich: $4^2 = 4 + 2\,(1 + 2 + 3)$ und damit für die 3-te sog. Dreieckszahl:

$$1 + 2 + 3 = \frac{4^2 - 4}{2} = \frac{3 \cdot 4}{2}$$

Allgemein erhält man auf diese Weise die n-te Dreieckszahl (die uns bereits früher als Summe der ersten n natürlichen Zahlen begegnet ist):

$$1 + 2 + \ldots + n = \frac{(n+1)^2 - (n+1)}{2} = \frac{n(n+1)}{2}$$

Es liegt nahe, mit Steinchen regelmäßige Vielecke beliebiger Eckenzahl $r \geq 2$ zu legen. Die 2-Ecke entstehen schrittweise durch Anlegen eines zusätzlichen Steinchens an das erste 2-Eck (bestehend aus einem Anfangssteinchen; auch das erste Dreieck besteht ja aus 1 Stein!). Den Übergang vom n-ten zum $(n + 1)$-ten r-Eck veranschaulicht für $r = 4$ die folgende Figur:



Das 4-te Quadrat hat man sich dabei aus dem 3-ten Quadrat entstanden zu denken, indem ein "Winkel" mit 3 (= 4 − 1) neuen Ecken hinzugefügt wird; zwischen je zwei dieser Ecken befinden sich 2 (= 4 − 2) der neuen Steinchen.

Dieser Aufbauschritt lässt sich leicht auf das r-Eck verallgemeinern. Wir bezeichnen mit $F_n^{(r)}$ die Anzahl der Steinchen im n-ten r-Eck. Dann entsteht $F_{n+1}^{(r)}$ aus $F_n^{(r)}$ durch Hinzunahme der entsprechenden Winkelfigur. Diese besitzt $r - 1$ neue Ecken sowie je $n - 1$ neue Zwischensteine auf $r - 2$ Seiten. Damit erhalten wir:

$$(*) \qquad \Delta F_n^{(r)} = F_{n+1}^{(r)} - F_n^{(r)} = r - 1 + (r - 2)\,(n - 1) = (r - 2)\,n + 1$$

Da für $n = 1$ alle r-Ecke aus einem einzigen Steinchen bestehen, ist es sinnvoll, $F_0^{(r)} = 0$ zu vereinbaren. Dann gilt Glg. (*) für alle $r \geq 2$ und $n \geq 0$. Man mache sich den Sachverhalt z.B. auch für $r = 3,\ 5$ und 6 klar!

■ Bemerkung

Die eben hergeleitete Gleichung ermöglicht es, eine *r*-Eckszahl aus der unmittelbar vorangehenden *r*-Eckszahl zu berechnen. Wegen dieses Rücklaufs auf Vorgängerwerte spricht man von einer Rekursion oder rekursiven Darstellung. Im Unterschied dazu erlaubt eine explizite Darstellung die direkte Berechnung des betreffenden Wertes durch Auswertung einer Formel.

Eine explizite Formel für die *n*-te *r*-Eckszahl liefert der folgende Lehrsatz:

■ 4.3.1. Proposition

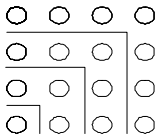
$$F_n^{(r)} = n + (r-2)\,\frac{n(n-1)}{2}$$

■ Beweis I

Durch vollständige Induktion (nach *n*). Beim Induktionsschluss benutzt man zweckmäßigerweise die rekursive Gleichung (*). Zur Übung!

■ Beweis II

Die explizite Darstellung von $F_n^{(r)}$ kann auf direktem Wege durch die Methode der *Summation der Differenzen* gewonnen werden. Die Grundidee lässt sich nun auch geometrisch veranschaulichen: Eine Figur (hier: ein regelmäßiges *r*-Eck) nichts danach anderes ist als die Summe aller zu ihrem schrittweisen Aufbau hinzugenommenen "Winkel-Figuren":



Wir verwenden Prop. 4.2.1 sowie obige Glg. (*) und erhalten allgemein:

$$F_n^{(r)} = F_n^{(r)} - F_0^{(r)} = \sum_{k=0}^{n-1} \Delta\, F_k^{(r)} = \sum_{k=0}^{n-1} ((r-2)\,k + 1) = n + (r-2) \sum_{k=0}^{n-1} k$$

Wertet man noch die Summe in der letzten Zeile aus (vgl. Prop. 3.2.4), so ergibt sich die behauptete Formel.◆

■ Bemerkung

Aus Glg. (*) folgt: $\Delta^2\, F_n^{(r)} = \Delta\,((r-2)\,n + 1) = r - 2$. Demnach bilden die *r*-Eckszahlen (für $r \geq 3$) arithmetische Folgen der Ordnung 2.

4.4. Potenzsummen

Die bisher immer wieder aufgetauchte (und ausgewertete) Summe $1 + 2 + \ldots + n$ gibt Anlass zu dem allgemeineren Problem, beliebige Potenzsummen, d.h. Summen der Form

$$S_k(n) := 1^k + 2^k + \ldots + n^k$$

(mit $k \in \mathbb{N}_0$), ebenfalls in geschlossener Form darzustellen.

Trivialerweise ist $S_0(n) = n$, und wir kennen schon $S_1(n) = \frac{n(n+1)}{2}$ (ferner: $S_2(n)$ aus Prop. 3.2.5 und $S_3(n)$ aus den Übungen). In der allgemeinen Form handelt es sich um kein leichtes Problem. In den Fällen $k = 2, 3, 4, 5$ kommt man aber auf einfache Weise mit der Methode der Summation von Differenzen zum Erfolg (und sieht dabei im Übrigen, wie das Verfahren grundsätzlich auch im allgemeinen Fall fortzuführen ist).

Um $S_2(n)$ auszuwerten, betrachtet man die Differenzenfolge der Kubikzahlen:

$$\Delta k^3 = (k+1)^3 - k^3 = 3k^2 + 3k + 1$$

Anschließend summiert man die Differenzen nach Prop. 4.2.1:

$$(n+1)^3 - 1 = \sum_{k=1}^{n} \Delta k^3 = \sum_{k=1}^{n} (3k^2 + 3k + 1) = 3\,S_2(n) + 3\,S_1(n) + n$$

Da wir $S_1(n)$ bereits kennen, lässt sich diese Gleichung nach $S_2(n)$ auflösen:

$$S_2(n) = \frac{n(n+1)(2n+1)}{6}$$

Um $S_3(n)$ auszuwerten, summiert man in derselben Weise $\Delta k^4 = 4k^3 + 6k^2 + 4k + 1$ und erhält:

$$(n+1)^4 - 1 = 4\,S_3(n) + 6\,S_2(n) + 4\,S_1(n) + n$$

Da nun schon $S_1(n)$ und $S_2(n)$ bekannt sind, kann die Gleichung nach $S_3(n)$ aufgelöst werden. Man gewinnt nach kurzer Rechnung (Übung!) die überraschende Formel:

$$S_3(n) = \frac{n^2(n+1)^2}{4} = S_1(n)^2$$

Das Verfahren lässt sich in derselben Weise fortsetzen, um $S_4(n)$, $S_5(n)$, … zu berechnen. Auf jeder Stufe braucht man dabei alle Ergebnisse der früheren Stufen.

5. Teilbarkeit

5.1. Division mit Rest, Teilbarkeitsrelation

■ Eine Aufteilungsaufgabe

Sollen 17 Pralinen an 5 Personen gleichmäßig verteilt werden, so kann dies auf mehrere Weisen geschehen: Jede Person erhält 1 Praline (Rest 12) oder 2 Pralinen (Rest 7) oder 3 Pralinen (Rest 2). Verlangt man, dass der Rest so klein wie möglich sein soll, so muss er kleiner als der Divisor (hier also: < 5) sein. Es gibt dann genau eine Aufteilung, nämlich diejenige gemäß der Gleichung $17 = 3 \cdot 5 + 2$. Die Bedingung "Rest < Divisor" ist jedoch im allgemeinen für eine eindeutige Aufteilung noch nicht hinreichend. So lassen sich Schulden von 17 Euro auf 5 Personen z.B. wie folgt mit einem Rest < 5 aufteilen:

$$-17 = (-2) \cdot 5 + (-7)$$
$$-17 = (-3) \cdot 5 + (-2)$$
$$-17 = (-4) \cdot 5 + 3$$

In der letzten Gleichung ist der Rest nichtnegativ; dies erzwingt eine eindeutige Darstellung.

■ Veranschaulichung an der Zahlengeraden

Wir stellen die beteiligten ganzen Zahlen $a \geq b > 0$ durch Strecken dar. Für die Division mit Rest $a : b$ kann man b solange von a wegnehmen, bis der Rest r (zum erstenmal!) kleiner als b wird; es ist dann $r \geq 0$. Der Sachverhalt lässt sich auch additiv deuten: Dazu trage man a auf der Zahlengeraden als Strecke von 0 bis a ab und anschließend (ebenfalls bei 0 beginnend) die Strecke b. Solange der Endpunkt von b nicht rechts von a liegt, wird die Strecke b an den rechten Endpunkt der zuletzt abgetragenen Strecke angehängt:

Aus dieser Veranschaulichung wird einsichtig, dass es einen Vervielfacher q (eine nicht-negative ganze Zahl) gibt, so dass $0 \leq q\,b \leq a$ gilt, jedoch $(q + 1)\,b > a$. Die (ganzzahlige) Division $a : b$ hat demnach den Rest $r = a - q\,b$.

Der folgende (grundlegende und wichtige) *Satz von der Division mit Rest* formuliert den Sachverhalt allgemein:

■ 5.1.1. Proposition

Seien $a, b \in \mathbb{Z}$, $b > 0$, beliebig. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$, für die gilt: $a = q\,b + r$ und $0 \le r < b$.

■ Beweis

Der Beweis wird in drei Schritten geführt. In 1. und 2. wird die *Existenz* der behaupteten Darstellung bewiesen, in 3. ihre *Eindeutigkeit.*

1. Wir nehmen zunächst $a \ge 0$ an. Ist $b > a$, so ist die Behauptung mit $q = 0$ und $r = a$ erfüllt. Für das Folgende wird daher $b \le a$ vorausgesetzt. Wir definieren q als kleinste positive Zahl k, für die $(k + 1)\,b > a$ gilt, was (nach dem PdkZ) möglich ist, da es mindestens ein k mit der geforderten Eigenschaft gibt (etwa $k = a$). Es bleibt $q\,b \le a$ zu zeigen. Wäre $q\,b > a$, so hätten wir mit $q_1 = q - 1$eine positive Zahl $< q$ mit $(q_1 + 1)\,b > a$. Dies steht im Widerspruch zur Minimalität von q. Setzen wir für den gesuchten Rest $r = a - q\,b$, so ist $r \ge 0$, es sind also alle Bedingungen erfüllt.

2. Nun werde $a < 0$ vorausgesetzt. Wir setzen $a_1 := |a| > 0$ und erhalten nach Nr. 1 eine Darstellung: $a_1 = q_1\,b + r_1$ mit $0 \le r_1 < b$. Nach Definition des Absolutbetrags ergibt sich: $-a = q_1\,b + r_1$, also:

(*) $\quad a = (-q_1)\,b + (-r_1)$

Ist $r_1 = 0$, so sind wir fertig. Andernfalls ist $r_1 > 0$ und damit $-b < -r_1 < 0$. Addition von b liefert $0 < b - r_1 < b$, es ist also $\hat{r} := b - r_1$ ein geeigneter Rest. Passend zu $\hat{r}$ setzen wir $\hat{q} := -q_1 - 1$ und bestätigen unter Verwendung von (*):

$$\hat{q}\,b + \hat{r} = (-q_1 - 1)\,b + (b - r_1) = (-q_1)\,b + (-r_1) = a$$

3. In den Nrn. 1-2 wurde lediglich die Existenz der behaupteten Darstellung bewiesen. Es fehlt noch der Nachweis, dass es höchstens eine (und damit: genau eine) solche Darstellung gibt. Um dies zu zeigen, nehmen wir an: $a = q_1\,b + r_1$ und $a = q_2\,b + r_2$, wobei $0 \le r_i < b$ für $i = 1, 2$, und folgern hieraus $q_1 = q_2$ und $r_1 = r_2$.

Ohne Einschränkung kann $r_1 \ge r_2$ vorausgesetzt werden. Ausgehend von $q_1\,b + r_1 = q_2\,b + r_2$ und den Ungleichungen für die Reste ergibt sich: $0 \le (q_2 - q_1)\,b = r_1 - r_2 < b - r_2 \le b$. Nach Division durch b wird daraus: $0 \le q_2 - q_1 < 1$, also $q_1 = q_2$; damit ergibt sich direkt auch $r_1 = r_2$.◆

■ 5.1.2. Definition

Die zu ganzen Zahlen a, b $(b > 0)$ eindeutig bestimmten $q, r \in \mathbb{Z}$ heißen Quotient (auch: Ganzteil) bzw. Rest der Division $a : b$. Für den Quotienten q schreibt man $\left[\frac{a}{b}\right]$, der Rest r wird notiert: $a \bmod b$ (gelesen: "a modulo b").

■ Beispiel

$\left[\frac{-17}{5}\right] = -4$ und $(-17) \bmod 5 = 3$. Aber: $-17 \bmod 5 = -2$ (mod bindet stärker als $-, +, \cdot, /$).

■ 5.1.3. Definition

Sind a, b ganze Zahlen; b heißt Teiler von a (oder: a durch b teilbar), wenn es ein $q \in \mathbb{Z}$ gibt mit $a = b \cdot q$. In diesem Fall schreiben wir: $b \mid a$, anderenfalls: $b \nmid a$.

■ Ergänzende Hinweise

1. In Definition 5.1.3 wird die Teilbarkeitsrelation im Wesentlichen dadurch gekennzeichnet, dass eine Division-mit-Rest-Gleichung besteht, deren Rest = 0 ist. Anders als in Prop. 5.1.1 kann allerdings $b \leq 0$ sein. Der Fall $b = 0$ ist nur möglich für $a = 0$ (weil $0 = 0 \cdot q$ für alle q). Es gilt somit $0 \mid 0$, jedoch $0 \nmid a$, falls $a \neq 0$.

2. Für $b \neq 0$ ist die ganze Zahl q mit $a = b \cdot q$ eindeutig bestimmt und heißt dann Komplementärteiler zu b.

3. *Warnung*: Die Schreibweise $b \mid a$ ist keinesfalls mit dem Bruchterm b/a oder $\frac{b}{a}$ zu verwechseln! Ein Bruchterm wie $\frac{3}{2}$ ist der Name für eine rationale Zahl. Hingegen wäre $3 \mid 2$ eine Aussage (!) (und zwar die falsche Aussage, dass 3 ein Teiler von 2 ist).

In folgendem Lehrsatz sind einfache und grundlegende Eigenschaften der Teilbarkeitsrelation zusammengestellt.

■ 5.1.4. Proposition

Für alle ganzen Zahlen a, a', b, b', c, x, y gilt:

(1) $a \mid 0$

(2) $b \mid a \wedge a \mid b \Longleftrightarrow |a| = |b|$

(3) $c \mid b \wedge b \mid a \Longrightarrow c \mid a$

(4) $b \mid a \wedge b' \mid a' \Longrightarrow b\,b' \mid a\,a'$

(5) $c\,b \mid c\,a \wedge c \neq 0 \Longrightarrow b \mid a$

(6) $c \mid a \wedge c \mid b \Longrightarrow c \mid x\,a + y\,b$

(7) $c \mid a \wedge c \mid b \Longrightarrow c \mid a \bmod b$

■ Beweis

(1)-(5) bleiben zur Übung.

Zu (6): Nach Vor. und Def. 5.1.3 gilt: $a = c\,t_1$, $b = c\,t_2$ für geeignete ganze Zahlen t_1, t_2. Damit ergibt sich $x\,a + y\,b = x\,c\,t_1 + y\,c\,t_2 = c(x\,t_1 + y\,t_2)$, d.h. c kommt als Faktor in $x\,a + y\,b$ vor.

Zu (7): Wie unter (6) lässt sich schreiben: $a = c\,t_1$, $b = c\,t_2$ Nach Prop. 5.1.1 haben wir eine Darstellung: $a = q\,b + r$. Damit ergibt sich: $a \bmod b = r = a - q\,b = c\,t_1 - q\,c\,t_2 = c(t_1 - q\,t_2)$, also $c \mid a \bmod b$. ◆

■ Vielfachensummen

Zu gegebenen Zahlen a, b heißen Ausdrücke der Form $x\,a + y\,b$ mit $x, y \in \mathbb{Z}$ (ganzzahlige) Vielfachensummen (oder: Linearkombinationen) von a, b. Entsprechend lassen sich zu ganzen $a_1, \ldots, a_n$ Vielfachensummen $x_1\,a_1 + \ldots + x_n\,a_n$ bilden, wobei $x_1, \ldots, x_n \in \mathbb{Z}$. Ihre Gesamtheit (Menge) werde mit $\mathcal{L}(a_1, \ldots, a_n)$ bezeichnet.

■ Bemerkungen zu 5.1.4

5.1.4,(6) besagt: *Ein Teiler gegebener Zahlen teilt jede Vielfachensumme dieser Zahlen.* (Dies gilt natürlich auch für Vielfachensummen von mehr als zwei Zahlen.)

5.1.4,(7) kann mit Bezug auf eine Division-mit-Rest-Darstellung so formuliert werden: *Ein Teiler von Dividend und Divisor ist auch Teiler des Restes.*

■ Teilermengen

Es ist zweckmäßig, die *positiven* Teiler einer ganzen Zahl a in einer Teilermenge $T(a)$ zusammenzufassen:

$$T(a) := \{t \in \mathbb{N} \mid t \text{ ist Teiler von } a\}$$

Es ist stets $1 \in T(a)$ (trivialer Teiler). Ferner gilt $T(0) = \mathbb{N}$, jedoch sind die Teilermengen $T(a)$ für $a \neq 0$ endlich, z.B. ist $T(4) = \{1, 2, 4\}$ und $T(6) = \{1, 2, 3, 6\}$. Ihr Durchschnitt enthält die gemeinsamen (positiven) Teiler: $T(4) \bigcap T(6) = \{1, 2\}$. Wir notieren: $T(a, b) := T(a) \bigcap T(b)$, und allgemein:

$$T(a_1, \ldots, a_n) := T(a_1) \bigcap \ldots \bigcap T(a_n)$$

Die Menge $T(a_1, \ldots, a_n)$ ist endlich, wenn mindestens ein $a_i \neq 0$ ist. In diesem Fall hat $T(a_1, \ldots, a_n)$ ein Maximum: den größten gemeinsamen Teiler von $a_1, \ldots, a_n$, bezeichnet als $\text{ggT}(a_1, \ldots, a_n)$. Zum Beispiel gilt: $\text{ggT}(4, 6) = \text{Max}\, T(4, 6) = 2$. – Für jedes ganze $a \neq 0$ gilt: $\text{ggT}(a, 0) = |a|$.

Eigenschaften der Teilbarkeitsrelation lassen sich mit Hilfe von Teilermengen ausdrücken. Einige nützliche Varianten enthält der folgende Lehrsatz:

■ 5.1.5. Proposition

(1) $b \mid a \iff T(b) \subseteq T(a)$

(2) $T(a, b) \subseteq T(x\,a + y\,b)$

(3) $T(a, b) = T(b, a \bmod b)$

■ Beweis

Zu (1). "$\Longrightarrow$": Sei $c \in T(b)$; dann ist aufgrund von Prop. 5.1.4,(3) (Transitivität): $c \mid a$, d.h. $c \in T(a)$. – "$\Longleftarrow$": Es ist $b \in T(b) \subseteq T(a)$, mithin: $b \mid a$.

Zu (2). Direkt aus Prop. 5.1.4,(6).

Zu (3). $T(a, b) \subseteq T(b, a \bmod b)$ ergibt sich direkt aus Prop. 5.1.4,(7). Bleibt $T(b, a \bmod b) \subseteq T(a, b)$ zu zeigen. Für den Rest $r := a \bmod b$ gilt eine Darstellung: $a = b\,q + r$ mit $q \in \mathbb{Z}$. Man sieht unmittelbar, dass ein gemeinsamer Teiler von b und r auch ein Teiler von a ist, also $\in T(a, b)$. ◆

■ 5.1.6. Definition

(1) Eine natürliche Zahl p heißt Primzahl (oder kurz: prim), wenn $T(p)$ genau zwei Elemente hat.

(2) Irgend zwei ganze Zahlen a, b heißen relativ prim (oder: teilerfremd), wenn ggT(a, b) = 1.

■ Bemerkung

Aus Def. 5.1.6 ergibt sich unmittelbar: 2 ist eine Primzahl, 1 jedoch nicht. Ferner: Je zwei verschiedene Primzahlen sind teilerfremd. Ist p eine Primzahl und $p \nmid a$, dann sind a, p teilerfremd. – (Alle Begründungen zur Übung!).

5.2. Der euklidische Algorithmus

Euklid (von Alexandria) hat in seinem berühmten mathematischen Lehrbuch *Elemente* (ca. 300 v. Chr.) ein Verfahren der (subtraktiven) *Wechselwegnahme* beschrieben, mit dem sich das gemeinsame Maß zweier Größen bestimmen lässt. Dieser Algorithmus gehört zu den ältesten und wichtigsten in der Mathematik.

Handelt es sich um geometrische Größen, z.B. Längen von Strecken, so bricht das Verfahren nicht immer ab. Zu den bekanntesten Fällen, in denen solche "inkommensurablen" Größen auftreten, gehören: Seite und Diagonale des Quadrats sowie Seite und Diagonale des regelmäßigen Fünfecks.

Im Bereich der ganzen Zahlen endet jede Wechselwegnahme nach endlich vielen Schritten (warum?). Der Vorgang lässt sich im Übrigen dadurch verkürzen, dass man *Subtraktionen mit demselben Subtrahenden* in einer *Division mit Rest* zusammenfasst. Statt also 5 von 17 dreimal nacheinander "wegzunehmen", führen wir ein einziges Mal die Division 17 : 5 (mit Rest 2) durch. Bei der anschließenden Division übernimmt der alte Rest 2 dann die Rolle des neuen Divisors.

Der vollständige Ablauf des euklidischen Algorithmus soll hier zunächst an einem Beispiel dargestellt werden.

■ Beispiel

Für $a = 48$ und $b = 34$ entsteht die folgende Divisionskette:

	Aktueller Rest
34	$r_1 = b$
$48 = 1 \cdot \mathbf{34} + 14$	r_2
$34 = 2 \cdot \mathbf{14} + 6$	r_3
$14 = 2 \cdot \mathbf{6} + 2$	r_4
$6 = 3 \cdot \mathbf{2} + 0$	[Bei Rest $r_5 = 0$ hält das Verfahren an.]

Der letzte nicht verschwindende Rest r_4 (= 2) geht in seinem Vorgänger r_3 (= 6) auf; somit geht er in sämtlichen Resten auf und ist ein gemeinsamer Teiler von a und b. Darüberhinaus ist er sogar größter gemeinsamer Teiler von a und b.

Allgemein zeigt dies der folgende *Satz vom euklidischen Algorithmus*:

■ 5.2.1. Proposition

Seien a, b ganze Zahlen mit $a > b > 0$. Dann wird durch $r_0 = a,\ r_1 = b$ und fortgesetzte Division mit Rest: $r_k = q_{k+1}\, r_{k+1} + r_{k+2}$ $(k = 0, 1, 2, \ldots)$ eine streng-monoton abnehmende Folge $r_0, r_1, r_2, \ldots$nicht-negativer ganzer Zahlen definiert, deren letztes nicht-verschwindendes Glied der größte gemeinsame Teiler von a und b ist.

■ Beweis

1. Die Folge der Reste nimmt ab, da jeder neue Rest durch die Division mit dem unmittelbaren Vorgängerrest entsteht. Nach endlich vielen Schritten wird auf diese Weise der Rest 0 erzwungen.

2. Nach Prop. 5.1.5,(3) besitzt das Restepaar r_k, r_{k+1} dieselben gemeinsamen Teiler wie das Restepaar r_{k+1}, r_{k+2}. Mithin sind (wenn wir die Division-mit-Rest-Folge von oben nach unten durchlaufen) die gemeinsamen Teiler von a, b dieselben wie die von $r_n, 0$ (wenn $r_n > 0$ und $r_{n+1} = 0$). Infolgedessen ist $r_n = \text{ggT}(r_n, 0) = \text{ggT}(a, b)$. ◆

■ Bemerkung

Der euklidische Algorithmus (E.A.) kann im Prinzip als wiederholte Anwendung der Gleichheit 5.1.5,(3) aufgefasst werden. Man beachte: Es ist gleichgültig, welche der beiden Zahlen a, b zu Beginn des Verfahrens als Divisor genommen wird:

$$\begin{aligned} T(34, 48) &= T(48, 34 \bmod 48) = T(48, 34) \\ &= T(34, 48 \bmod 34) = T(34, 14) \\ &= T(14, 34 \bmod 14) = T(14, 6) \\ &= T(6, 14 \bmod 6) = T(6, 2) \\ &= T(2, 6 \bmod 2) = T(2, 0) \\ &= \{1, 2\} \end{aligned}$$

Wir formulieren und beweisen nun eine bedeutsame Folgerung aus dem Satz über den E.A. (sog. *Lemma von Bachet*):

■ 5.2.2. Proposition

Für alle $a, b \in \mathbb{Z}$ gilt: $\text{ggT}(a, b) \in \mathcal{L}(a, b)$

In ausführlicher Formulierung: Der größte gemeinsame Teiler d von a, b ist als Vielfachensumme (Linearkombination) von a und b darstellbar, d.h. es gibt ganze Zahlen x, y, für die gilt: $d = x\, a + y\, b$.

■ Beweis

Nach Prop. 5.2.1 ist $d = \text{ggT}(a, b)$ der letzte im E.A. auftretende positive Rest. Zum Beweis der Behauptung wird gezeigt, dass sich sämtliche Reste r_k als Linearkombinationen von a und b darstellen lassen. Für $r_0 = a$ und $r_1 = b$ ist dies sofort ersichtlich. Auch für r_2 gilt: $r_2 = a - q_1\, b$. Damit berechnet man den nächsten Rest:
$r_3 = r_1 - q_2\, r_2 = b - q_2(a - q_1\, b) = a(-q_2) + b(1 + q_1\, q_2)$, usw. für die folgenden $k = 4, \ldots, n$. Im letzten Schritt erhält man: $d = r_n$ = Linearkombination von a und b. ◆

■ Bemerkungen und Beispiel

Der obige Beweis beschreibt ein Verfahren, mit dem sich die gesuchten Koeffizienten x, y effektiv berechnen lassen. Durch ein "usw." wird darin die Fortsetzung einer Schrittfolge angedeutet, die streng genommen eine vollständige Induktion erfordert (was allerdings das Verständnis etwas erschwert). Eine genauere Darstellung findet man unter **`http://www.uni-flensburg.de/mathe/zero/zero.html`** (anschließend wählen: Veranstaltungen > Algorithmen mit *Mathematica* > Der ggT als Vielfachensumme).

Für den ggT von 48 und 34 ermittelt man mit diesem Verfahren die Linearkombination wie folgt:

$$\begin{aligned}\text{ggT}(48, 34) = 2 &= 14 - 2 \cdot 6 \\ &= 14 - 2 \cdot (34 - 2 \cdot 14) = (-2) \cdot 34 + 5 \cdot 14 \\ &= (-2) \cdot 34 + 5 \cdot (48 - 1 \cdot 34) \\ &= 48 \cdot \mathbf{5} + 34 \cdot \mathbf{(-7)}\end{aligned}$$

Seinen Namen verdankt das in Prop. 5.2.2 ausgesprochene Lemma dem französischen Edelmann Bachet de Méziriac (1581-1638). Mit ihm lassen sich weitere wichtige Aussagen der Teilbarkeitslehre gewinnen:

■ 5.2.3. Proposition

Für natürliche Zahlen a, b, c gilt:

(1) $\text{ggT}(a, b) = 1 \wedge b \mid a\, c \implies b \mid c$

(2) p prim $\wedge\ p \mid a\, b \implies p \mid a \vee p \mid b$

■ Beweis

Zu (1): Nach Prop. 5.2.2 schreiben wir $a\, x + b\, y = 1$ für geeignete ganze Zahlen x, y, also $a\, c\, x + b\, c\, y = c$. Da b das Produkt $a\, c$ teilt, gibt es ein $q \in \mathbb{Z}$ mit $b\, q = a\, c$. Daraus folgt: $c = b\, q\, x + b\, c\, y = b(q\, x + c\, y)$. Mithin ist b Teiler von c.

Zu (2): Ist p Teiler von a, so ist nichts zu zeigen. Im Falle $p \nmid a$ hat man $\text{ggT}(p, a) = 1$(vgl. die Bemerkung zu Def. 5.1.6). Nach der gerade bewiesenen Aussage (1) ist daher $p \mid b$. ◆

■ Bemerkung

Die Aussage von Prop. 5.2.3 findet sich bereits in den *Elementen* des Euklid. Sie wird oft als Hilfsmittel herangezogen und heißt daher gelegentlich auch *Lemma von Euklid.* In mathematischer Umgangssprache: Ist der Teiler eines Produkts relativ prim zu einem der Faktoren, so teilt er den anderen Faktor.

5.3. Lineare diophantische Gleichungen

Für das Folgende setzen wir generell voraus: $a, b, c \in \mathbb{Z}$; mindestens eine der beiden Zahlen a, b ist von Null verschieden.

■ Aufgabe

Suche sämtliche Paare ganzer Zahlen (x, y), welche die Gleichung $a\,x + b\,y = c$ erfüllen.

Bei diesem Aufgabentyp handelt sich um eine lineare Gleichung in zwei *ganzzahligen* Unbekannten mit *ganzzahligen* Koeffizienten. Der kennzeichnende Zusatz "diophantisch" geht zurück auf den griechischen Mathematiker Diophantos von Alexandria (um 250 n. Chr.).

■ Beispiel

Man betrachte: $x + y = 3$

Es lassen sich unmittelbar Lösungspaare finden, etwa $(x, y) = (1, 2)$ oder $(x, y) = (-5, 8)$, usf. Ebenso einfach überlegt man sich die Form der *allgemeinen* Lösung (Lösungsgesamtheit). Offenbar können wir eine der beiden Unbekannten willkürlich mit einer Zahl belegen, z.B. $x = m$ (mit beliebigem $m \in \mathbb{Z}$). Dadurch ist die andere Unbekannte festgelegt: $y = 3 - m$. Die Glg hat also die Lösungsgesamtheit $(x, y) = (m, 3 - m)$ mit $m \in \mathbb{Z}$.

Nicht in allen Fällen liegt die Lösung so auf der Hand. Dennoch ist auch die Behandlung des allgemeinen Falls im Prinzip einfach. Der E.A. (samt Darstellung des ggT als Vielfachensumme) erweist sich dabei als nützliches Werkzeug.

Wir gliedern die Diskussion in drei Schritte:

I. Wann ist die Glg $a\,x + b\,y = c$ überhaupt lösbar?

II. Wie findet man eine (einzelne) Lösung?

III. Wie findet man alle Lösungen (die Lösungsgesamtheit)?

Zu I. Hat die Glg $48\,x + 34\,y = 11$ eine Lösung? Die Antwort lautet: Nein. Denn da der ggT von 48 und 34 (hier: 2) die linke Seite der Gleichung teilt, müsste er auch in der rechten Seite (hier: 11) aufgehen. Anders verhält es sich bei der Glg $48\,x + 34\,y = 12$. Sie besitzt eine Lösung. Denn Prop. 5.2.2 liefert ganze Zahlen x_1, y_1 (hier: $x_1 = 5, y_1 = -7$) mit $48\,x_1 + 34\,y_1 = 2$. Nach Multiplikation mit 6 erkennt man sofort die Lösung: $(x_0, y_0) = (6\,x_1, 6\,y_1) = (30, -42)$. Allgemein: $a\,x + b\,y = c$ ist genau dann lösbar, wenn $\mathrm{ggT}(a, b)$ ein Teiler von c ist.

Zu II. Wir sahen bereits am Beispiel unter Punkt I.: Ist die Glg lösbar, so ergibt sich eine spezielle Lösung (auch partikuläre Lösung genannt) wie folgt: Man berechnet zunächst $d = \mathrm{ggT}(a, b)$ mit dem E.A. sowie Koeffizienten

x_1, y_1 für seine Darstellung als Vielfachensumme: $d = x_1\, a + y_1\, b$. Anschließend multipliziert man mit dem Komplementärteiler c_1 aus $c = c_1 \cdot d$ und erhält die partikuläre Lösung: $(x_0, y_0) = (c_1\, x_1, c_1\, y_1)$. Wir setzen sie in die Glg ein und bestätigen: $a\, x_0 + b\, y_0 = c_1 \cdot (a\, x_1 + b\, y_1) = c_1 \cdot d = c$.

Zu III. Man erhält eine Lösung (x, y) von (*) $a\, x + b\, y = c$ stets in der Form:

$$x = x_0 + x_h$$

$$y = y_0 + y_h$$

wobei (x_h, y_h) eine Lösung der zu (*) gehörigen homogenen Glg $a\, x + b\, y = 0$ ist. Denn $(x_0 + x_h, y_0 + y_h)$ ist eine Lösung von (*):

$$a(x_0 + x_h) + b(y_0 + y_h) = (a\, x_0 + b\, y_0) + (a\, x_h + b\, y_h) = c + 0 = c$$

Sind umgekehrt (x, y) und (x_0, y_0) Lösungen von (*), so ergibt sich durch Subtraktion der Glgen $a\, x + b\, y = c$ und $a\, x_0 + b\, y_0 = c$ sofort $a(x - x_0) + b(y - y_0) = 0$; es ist also $(x_h, y_h) := (x - x_0, y - y_0)$ eine Lösung der homogenen Glg.

Die noch verbleibende Aufgabe besteht also in der Bestimmung sämtlicher $x, y \in \mathbb{Z}$ mit $a\, x + b\, y = 0$. Dividiert man diese Glg durch d, so ergibt sich: $a_1\, x + b_1\, y = 0$, wobei $a = a_1\, d$ und $b = b_1\, d$. Die a_1, b_1 sind dann teilerfremd (Übung!). Formen wir die homogene Glg um zu $a_1\, x = -b_1\, y$, so ergibt sich aus dem Lemma von Euklid: $b_1 \mid x$ und $a_1 \mid y$. Es gibt also ganze Zahlen m, n mit $x = m\, b_1$ und $y = n\, a_1$. Aus $a(b_1\, m) + b(a_1\, n) = 0$ folgt nach Division durch $a\, b_1$ $(= b\, a_1)$ schließlich: $m = -n$. Daher ist

$$(x_h, y_h) = \left(\frac{b}{d}\, m, -\frac{a}{d}\, m\right) \text{mit } m \in \mathbb{Z}$$

die Lösungsgesamtheit der homogenen Gleichung $a\, x + b\, y = 0$.

Wir wenden diese Erkenntnisse auf das Beispiel $48\, x + 34\, y = 12$ an: Die zugehörige homogene Glg $48\, x + 34\, y = 0$ besitzt die Lösungen $(x_h, y_h) = (17\, m, -24\, m)$ $(m \in \mathbb{Z})$. Somit hat die Ausgangsglg die allgemeine Lösung $(x, y) = (30 + 17\, m, -42 - 24\, m)$ $(m \in \mathbb{Z})$.

Wir fassen die Ergebnisse der Diskussion zusammen:

■ 5.3.1. Lösungsverfahren

Gegeben: eine lineare diophantische Glg (*): $a\, x + b\, y = c$

1. Man berechne $d = \text{ggT}(a, b)$ mit dem euklidischen Algorithmus.

2. (*) lösbar $\Longleftrightarrow d \mid c$.

   In diesem Fall bestimme man $x_1, y_1 \in \mathbb{Z}$ mit $d = a\, x_1 + b\, y_1$ und fahre fort.

3. $x_0 = x_1\, \frac{c}{d}$, $y_0 = y_1\, \frac{c}{d}$ ist eine partikuläre Lösung von (*).

4. $x = x_0 + \frac{b}{d}\, m$, $y = y_0 - \frac{a}{d}\, m$ $(m \in \mathbb{Z})$ ist die allgemeine Lösung von (*).

5.4. ggT und kgV

Das Lemma von Bachet besagt, dass sich der größte gemeinsame Teiler d zweier Zahlen a, b stets als Vielfachensumme von a und b darstellen lässt:

$$d \in \mathcal{L}(a, b)$$

Er ist aber nicht einfach "irgendeine" unter den möglichen Linearkombinationen $x\,a + y\,b$. Zunächst einmal müssen die x, y so gewählt werden, dass $d = x\,a + y\,b > 0$ ist. Dies legt es nahe, nur die *positiven* Vielfachensummen zu betrachten. Wir verwenden die Abkürzung

$$\mathcal{L}^+(a, b) := \mathcal{L}(a, b) \bigcap \mathbb{N}$$

bzw. allgemein: $\mathcal{L}^+(a_1, \ldots, a_n) := \mathcal{L}(a_1, \ldots, a_n) \bigcap \mathbb{N}$. Offensichtlich ist $\mathcal{L}^+(a, b)$ eine nichtleere (!) Menge natürlicher Zahlen. Sie besitzt (nach dem PdkZ) ein Minimum, und zwar ist dieses kleinste Element gerade der ggT von a, b. Diese entscheidende Erkenntnis spricht in allgemeiner Form (d.h. für beliebige ganze Zahlen $a_1, \ldots, a_n$) der folgende *Hauptsatz über den ggT* aus:

■ 5.4.1. Proposition

Seien $a_1, \ldots, a_n \in \mathbb{Z}$ beliebig und nicht alle $= 0$. Dann gilt:

$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{Min}\,\mathcal{L}^+(a_1, \ldots, a_n)$.

■ Beweis

Wir setzen $z_0 := \mathrm{Min}\,\mathcal{L}^+(a_1, \ldots, a_n)$ und haben dann zu zeigen: $z_0 = \mathrm{ggT}(a_1, \ldots, a_n)$.

Zunächst schreiben wir z_0 als Vielfachensumme: $z_0 = x_1\,a_1 + \ldots + x_n\,a_n$. Ist $t \in T(a_1, \ldots, a_n)$ (ein gemeinsamer Teiler der a_i und damit $t \mid a_i$), so gilt auch $t \mid z_0$ (nach Prop. 5.1.4,(6)) und damit $t \le z_0$, insbesondere also: $\mathrm{ggT}(a_1 \ldots, a_n) \le z_0$.

Es bleibt noch zu zeigen: $z_0 \le \mathrm{ggT}(a_1, \ldots, a_n)$. Wir weisen dazu nach, dass alle a_i durch z_0 teilbar sind. Denn dann ist $z_0 \in T(a_1) \bigcap \ldots \bigcap T(a_n) = T(a_1, \ldots, a_n)$, d.h. z_0 ein gemeinsamer Teiler (der natürlich höchstens so groß wie der *größte* gemeinsame Teiler sein kann).

Da die Vielfachensumme bzgl. der $a_1, \ldots, a_n$ völlig gleichartig aufgebaut ist, können wir uns stellvertretend darauf beschränken, $z_0 \mid a_1$ zu beweisen. Dazu machen wir Division mit Rest: $a_1 = q\,z_0 + r$, $0 \le r < z_0$. Für den Rest ergibt sich: $r = a_1 - q\,z_0 = a_1 - q(x_1\,a_1 + \ldots + x_n\,a_n) = (1 - q\,x_1)\,a_1 + \sum_{j=2}^{n} (-q\,x_j)\,a_j$. Diese Darstellung von r als Vielfachensumme der $a_1, \ldots, a_n$ kann nicht positiv sein, weil dann in $\mathcal{L}^+(a_1, \ldots, a_n)$ ein Element gefunden worden wäre, das kleiner ist als das Minimum z_0. Somit kann nur $r = 0$ sein, und d.h. $a_1 = q\,z_0$. ◆

■ 5.4.2. Proposition

$$d = \mathrm{ggT}(a_1, \ldots, a_n) \iff T(d) = T(a_1, \ldots, a_n)$$

■ Beweis

Die Behauptung ergibt sich aus Prop. 5.4.1. Letztere wird in der Beweisrichtung "$\Longrightarrow$" für die Inklusion $T(a_1, \ldots, a_n) \subseteq T(d)$ benötigt. Die Einzelheiten bleiben als Übung. ◆

■ Das kleinste gemeinsame Vielfache

Der ggT zweier Zahlen a, b ist als Maximum von $T(a, b)$ erklärt (und erst nachträglich als Minimum einer geeigneten Menge erkannt). Im Unterschied dazu ist das kgV bereits kraft Definition Minimum einer noch festzulegenden Menge $V(a, b)$ gemeinsamer Vielfache von a und b.

Zu einer beliebigen ganzen Zahl betrachten wir zunächst die Menge *aller* ganzzahligen Vielfachen:

$$m\,\mathbb{Z} := \{k \cdot m \mid k \in \mathbb{Z}\}$$

In dieser Schreibweise ist z.B. $2\,\mathbb{Z} = \{0, -2, 2, -4, 4, \ldots\}$ die Menge der geraden ganzen Zahlen. Ferner gilt: $0\,\mathbb{Z} = \{0\}$, $1\,\mathbb{Z} = \mathbb{Z}$, $(-m)\,\mathbb{Z} = m\,\mathbb{Z}$ sowie $m\,\mathbb{Z} \subseteq n\,\mathbb{Z} \Longleftrightarrow n \mid m$ (Begründungen als Übung). Die Menge der gemeinsamen Vielfache von a, b ist $a\,\mathbb{Z} \bigcap b\,\mathbb{Z}$. Zum Beispiel:

$$6\,\mathbb{Z} \bigcap 8\,\mathbb{Z} = \{0, -24, 24, -48, 48, \ldots\}$$

Da für das kgV nur *positive* Vielfache in Betracht gezogen werden, definieren wir die entsprechenden Mengen wie folgt:

$$V(a_1, \ldots, a_n) := (a_1\,\mathbb{Z}) \bigcap \ldots \bigcap (a_n\,\mathbb{Z}) \bigcap \mathbb{N}$$

Damit hat man nun z.B. $V(6, 8) = \{24, 48, \ldots\}$, $V(2) = \{2, 4, 6, \ldots\}$, $V(-2) = V(2)$ sowie $V(0) = \emptyset$. Sind die $a_1, \ldots, a_n$ sämtlich $\neq 0$, so ist $V(a_1, \ldots, a_n)$ nichtleer und besitzt (gemäß PdkZ) ein Minimum:
$\mathrm{kgV}(a_1, \ldots, a_n) := \mathrm{Min}\, V(a_1, \ldots, a_n)$.

In Analogie zu Prop. 5.4.2 erhält man die folgende Aussage über das kgV:

■ 5.4.3. Proposition

$$m = \mathrm{kgV}(a_1, \ldots, a_n) \iff V(m) = V(a_1, \ldots, a_n)$$

■ Beweis

1."$\Longrightarrow$": Sei $c \in V(m)$ beliebig. Dann ist $c = k \cdot m$ für ein $k \in \mathbb{N}$. Andererseits ist $m \in V(a_1, \ldots, a_n)$ und damit $m = s_i\, a_i$ für geeignete $s_i \in \mathbb{N}$ $(1 \leq i \leq n)$. Es ergibt sich $c = (k\, s_i)\, a_i$, also auch $c \in V(a_1, \ldots, a_n)$. Damit ist $V(m) \subseteq V(a_1, \ldots, a_n)$ gezeigt.

Umgekehrt ist nun $V(a_1, \ldots, a_n) \subseteq V(m)$ zu zeigen. Sei dazu $c \in V(a_1, \ldots, a_n)$ irgendein gemeinsames Vielfaches. Da auch m Vielfaches der $a_1, \ldots, a_n$ ist, haben wir Gleichungen: $m = s_i\, a_i$ und $c = t_i\, a_i$ $(i = 1, \ldots, n)$. Es gilt $m \leq c$. Um darüberhinaus $c \in V(m)$ zu zeigen, machen wir Division mit Rest: $c = m\, q + r$, $0 \leq r < m$. Hieraus erhalten wir: $r = c - m\, q = (t_i - s_i\, q)\, a_i$. Es kann aber das r nicht positiv sein, denn es wäre dann ein kleineres gemeinsames Vielfaches als m (im Widerspruch dazu, dass m nach Voraussetzung bereits das kgV ist). Daher gilt $r = 0$ und $m \mid c$.

2. "$\Longleftarrow$": Wegen $m \in V(m) = V(a_1, \ldots, a_n)$, ist m gemeinsames Vielfaches der a_i. Bleibt also nur zu zeigen: $m \leq k$ für jedes $k \in V(a_1, \ldots, a_n)$. Dies ist aber klar, da ein solches k auch $\in V(m)$ ist, d.h. $m \mid k$ und infolgedessen $m \leq k$. ◆

■ Bemerkung

Es ist mit geringem Aufwand möglich, ausgehend von 5.4.3 eine analoge Aussage über die *vollen* Vielfachenmengen zu beweisen: $m = \mathrm{kgV}(a_1, \ldots, a_n) \Longleftrightarrow m\,\mathbb{Z} = (a_1\,\mathbb{Z}) \bigcap \ldots \bigcap (a_n\,\mathbb{Z})$. – (Übung!).

Zwischen dem ggT und dem kgV zweier Zahlen besteht ein einfacher Zusammenhang:

■ 5.4.4. Proposition

Für alle ganzen Zahlen $a, b > 0$ gilt:

$\text{ggT}(a, b) \cdot \text{kgV}(a, b) = a \cdot b$

■ Beweis

1. Wir beweisen zunächst die Hilfsaussage: Zu jedem $d \in T(a, b)$ gibt es ein $m \in V(a, b)$ derart, dass $d \cdot m = a \cdot b$. – Sei dazu d irgendein gemeinsamer Teiler von a und b. Dann hat man $a = k_1\, d$, $b = k_2\, d$ für passende $k_1, k_2 \in \mathbb{N}$ und damit für das Produkt: $a \cdot b = (k_1\, k_2\, d) \cdot d$. Die Zahl $m = k_1\, k_2\, d$ erfüllt die behauptete Gleichung und ist wegen $m = k_1\, b = k_2\, a$ ein gemeinsames Vielfaches von a und b.

2. Die Hilfsbehauptung aus Nr. 1 wird nun auf $d := \text{ggT}(a, b)$ angewendet. Sie liefert dann ein $m \in V(a, b)$ mit $d\, m = a\, b$. Wir vergleichen m mit einem beliebigen $m' \in V(a, b)$, genauer zeigen wir: $m \mid m'$ (also $m \le m'$, womit alles bewiesen ist).

Als gemeinsames Vielfaches von a, b lässt sich m' schreiben: $m' = s_1\, a = s_2\, b$. Ferner stellen wir den ggT als Linearkombination dar: $d = x\, a + y\, b$. Damit ergeben sich folgende Umformungen:

$$m' = m' \cdot \frac{m\, d}{a\, b} = m \cdot m' \cdot \frac{x\, a + y\, b}{a\, b} = m \cdot \left(\frac{x\, m'}{b} + \frac{y\, m'}{a} \right) = m(x\, s_2 + y\, s_1)$$

Da $x\, s_2 + y\, s_1$ eine ganze Zahl ist, gilt $m \mid m'$. ◆

5.5. Primfaktorzerlegung

Zu den wichtigsten Grundtatsachen der elementaren Arithmetik gehört die Erkenntnis, dass die natürlichen Zahlen Produkte aus lauter Primzahlen sind. Die Primfaktoren (PF) sind stets eindeutig bestimmt, d.h. eine Zahl lässt sich nur auf eine einzige Weise als Primzahlprodukt hinschreiben.

In diesem Abschnitt sollen die Überlegungen entwickelt werden, die zu dem nämlichen *Satz über die Primfaktorzerlegung* (PFZ) führen; auch einige Anwendungen in der Arithmetik werden skizziert.

Wenn in jeder natürlichen Zahl eine oder mehrere Primzahlen stecken, so sollte es möglich sein, sie über ein Kriterium zu identifizieren. Dies leistet der folgende *Satz vom kleinsten Primteiler*.

■ 5.5.1. Proposition

(1) Sei $n \ge 2$ ganz und t der kleinste Teiler ≥ 2 von n. Dann ist t prim.

(2) Ist n keine Primzahl, so gilt für den Primteiler aus (1): $t \le \sqrt{n}$.

■ Beweis

Zu (1). Ist – indirekt angenommen – t zusammengesetzt, etwa: $t = r \cdot s$ mit $r, s \geq 2$, so hat man für ein geeignetes ganzes q die Gleichung $n = t \cdot q = r \cdot s \cdot q$. Wegen $r < t$ ist dann aber t nicht der kleinste Teiler (≥ 2) von n (Widerspruch!).

Zu (2). Aus der Minimalität von t ergibt sich unmittelbar: $n = t \cdot k \geq t^2$ (hierbei ist k der Komplementärteiler von t mit $t \leq k$). ◆

■ Die Folge der Primzahlen

Euklid hat in Buch IX seiner *Elemente* gezeigt, wie man auf dieser Grundlage beliebig viele Primzahlen erzeugen kann. Die Folge aller Primzahlen

2, 3, 5, 7, 11, 13, 17, 19, 23, …

ist in diesem Sinne unendlich. Euklid argumentiert folgendermaßen: Sei M irgendeine Menge von Primzahlen, etwa $M = \{a, b, c\}$. Dann bestimmen wir nach Prop. 5.5.1 den kleinsten Primteiler p der Zahl $a\,b\,c + 1$. Damit haben wir eine *neue* Primzahl gewonnen, denn es ist $p \notin M$. Um das einzusehen, schreiben wir $a\,b\,c + 1 = p\,m$ mit passendem $m \in \mathbb{N}$. Wäre nun etwa $p = a$, so hieße das: $1 = a\,m - a\,b\,c = a(m - b\,c)$, was aber wegen $a > 1$ unmöglich sein kann.

■ Beispiele

1. Sei $M = \{3, 7, 17\}$ vorgegeben. Euklids "Primzahlmaschine" liefert zu dieser Menge den kleinsten Primteiler von $3 \cdot 7 \cdot 17 + 1 = 358$, nämlich: die "neue" Primzahl 2.

2. Das Verfahren funktioniert sogar für $M = \emptyset$. Denn das Produkt ist hier = 1; daher ist $p = 2$ (der kleinste Primteiler von 1 + 1).

3. Zu einem Anfangsstück M der Primzahlfolge wird eine neue Primzahl erzeugt, die stets *größer* ist als die Zahlen aus M. Zum Beispiel entsteht aus $M = \{2, 3, 5, 7\}$ die Zahl $p = 211$.

■ 5.5.2. Proposition

> Sei M irgendeine Menge von Primzahlen, m ihr Produkt und p der kleinste Primteiler von $m + 1$. Dann gilt: $p \notin M$. (Zu jeder endlichen Menge von Primzahlen lässt sich eine Primzahl angeben, die nicht in ihr enthalten ist.)

Wir kommen nun zum Satz über die PFZ:

■ 5.5.3. Proposition

> Jede ganze Zahl > 1 lässt sich (bis auf die Reihenfolge) eindeutig als Produkt von Primzahlen darstellen.

■ Beweis

Sei die ganze Zahl $a \geq 2$ beliebig vorgegeben. Wir zeigen 1. die Existenz und 2. die Eindeutigkeit der PFZ von a.

1. Sei p_1 der kleinste Primteiler von a (nach Prop. 5.5.1). Dann gilt $a = p_1\, a_1$ für ein ganzes $a_1 \geq 1$. Ist a prim, so sind wir fertig. Anderenfalls ist $a > a_1 \geq 2$ und wir bestimmen den kleinsten Primteiler p_2 von a_1. Es gilt $a_1 = p_2\, a_2$, $a_2 \geq 1$, also $a = p_1\, p_2\, a_2$. Ist a_1 prim, so sind wir fertig. Anderenfalls haben wir $a_1 > a_2 \geq 2$. Die bei jedem Schritt auftretenden Komplementärteiler bilden eine strikt absteigende Folge: $a > a_1 > a_2$. Daher muss die wiederholte Abspaltung von Primteilern nach endlich vielen Schritten abbrechen. Tritt etwa im m-ten Schritt der Komplementärteiler $a_m = 1$ auf, so gilt $p_m = a_{m-1}$ und $a = p_1\, p_2 \cdot \ldots \cdot p_m$. (Die in diesem Produkt auftretenden PFn sind i.a. nicht sämtlich verschieden.)

2. Wir nehmen eine (weitere) Zerlegung $q_1\, q_2 \cdot \ldots \cdot q_s = a$ an. Dann wäre sicher $p_1 \mid q_1\, q_2 \cdot \ldots \cdot q_s$ und nach dem Lemma von Euklid p_1Teiler eines der q-Faktoren, etwa $p_1 \mid q_k$. Weil $p_1 > 1$ und q_k prim ist, muss sogar $p_1 = q_k$ gelten. Nun verkürzt man beide Zerlegungen jeweils um den Faktor p_1 und q_k und fährt in analoger Weise fort, die restlichen PFn p_i wegzukürzen. Schließlich ergibt sich so $m = s$ sowie die Übereinstimmung der beiden Zerlegungen (bis auf die Reihenfolge ihrer Faktoren). ◆

Üblicherweise fasst man gleiche PFn zu Potenzen zusammen und notiert die PFZ in der Form:

$$a = {p_1}^{\alpha_1}\, {p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$$

Hierbei gilt für die ganzzahligen Exponenten: $\alpha_i \geq 1$.

Es folgen einige Anwendungen der PFZ in der Teilbarkeitslehre.

■ Beschreibung und Abzählung von Teilern

Sei $d \mid a$. In der PFZ von d kommen höchstens die PFn von a vor. Daher können wir schreiben:

$$d = {p_1}^{\delta_1}\, {p_2}^{\delta_2} \cdot \ldots \cdot {p_n}^{\delta_n}, \text{ wobei } 0 \leq \delta_i \leq \alpha_i \text{ für } i = 1, 2, \ldots, n$$

Die Primzahlpotenzen ${p_i}^{\delta_i}$ heißen Primärteiler von a. Zu einem PF p_i gibt es somit $\alpha_i + 1$ Primärteiler. Jeder Teiler von a ist in eindeutiger Weise durch ein Exponenten-Tupel $(\delta_1, \delta_2, \ldots, \delta_n)$ charakterisiert (und umgekehrt). Daher gilt:

■ 5.5.4. Proposition

Für die Anzahl $\tau(a)$ aller Teiler von a gilt:

$$\tau(a) = (\alpha_1 + 1)\,(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_n + 1)$$

■ Beispiel

$a = 46200 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 11^1$. Also $\tau(a) = (3 + 1)\,(1 + 1)\,(2 + 1)\,(1 + 1)\,(1 + 1) = 96$

■ Gemeinsame Teiler

Sind zwei natürliche Zahlen a, b gegeben, so denken wir uns die in den PFZn auftretenden PFn in einer Folge zusammengeführt (vereinigt): $p_1, p_2, \ldots, p_n$. Wir haben dann Produktdarstellungen

$$a = {p_1}^{\alpha_1}\ {p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n} \text{ und } b = {p_1}^{\beta_1}\ {p_2}^{\beta_2} \cdot \ldots \cdot {p_n}^{\beta_n},$$

die keine PFZn im strengen Sinne sind, da ein PF von a nicht notwendigerweise auch PF von b ist (und umgekehrt). Für die zugehörigen Exponenten bedeutet dies:

$$0 \le \delta_i \le \alpha_i \text{ und } 0 \le \delta_i \le \beta_i$$

Hieraus ergibt sich: $0 \le \delta_i \le \text{Min}(\alpha_i, \beta_i)$. Ein gemeinsamer Teiler d von a, b ist daher am größten (d.h. $d = \text{ggT}(a, b)$), wenn die Exponenten δ_i der PFn von d ihr Maximum annehmen: $\delta_i = \text{Min}(\alpha_i, \beta_i)$. Daraus ergibt sich:

■ 5.5.5. Proposition

$$\text{ggT}(a, b) = \prod_{i=1}^{n} {p_i}^{\text{Min}(\alpha_i, \beta_i)}$$

Es gibt auch ein Pendant dieser Aussage für das kleinste gemeinsame Vielfache:

■ 5.5.6. Proposition

$$\text{kgV}(a, b) = \prod_{i=1}^{n} {p_i}^{\text{Max}(\alpha_i, \beta_i)}$$

■ Beweis

Die Behauptung ergibt sich durch direkte Rechnung aus Prop. 5.5.5 unter Verwendung von Prop. 5.4.4 sowie der einfachen Identität: $\text{Min}(\alpha_i, \beta_i) + \text{Max}(\alpha_i, \beta_i) = \alpha_i + \beta_i$ (vgl. Prop. 1.3.4).◆

■ Bemerkung

Die Formeln aus 5.5.5 und 5.5.6 liegen dem Verfahren zu Grunde, mit dem üblicherweise in der Schule der ggT und das kgV ermittelt wird. Da jedesmal erst die PFZ der beteiligten Zahlen hergestellt werden muss, kann dieses Vorgehen bei Auftreten von größeren PFn sehr aufwändig werden. Der euklidische Algorithmus ist verglichen damit die weitaus effizientere (und einfachere) Methode.

■ Die Summe der Teiler einer Zahl

Sei $a \in \mathbb{N}$. Es bezeichnet $\sigma(a) :=$ Summe der Teiler von a (Sigma-Funktion).

Beispiel: $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$

Um zu einer Formel für $\sigma(a)$ zu gelangen, werden zuerst Primzahlpotenzen betrachtet:

$$\sigma(p^\alpha) = 1 + p + p^2 + ... + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1} \quad \text{(geometrische Reihe)}$$

Wenn man σ für Produkte von Primzahlpotenzen berechnen kann, ist man (aufgrund der PFZ) bereits am Ziel. Als Vorbereitung beweisen wir eine Hilfsbehauptung:

(*) Seien a, b teilerfremd. Dann gilt:

$$w \mid a\,b \iff \text{Es gibt } u, v: \; u \mid a\,,\; v \mid b,\; w = u\,v$$

D.h.: die Teiler eines Produkts zweier teilerfremder Zahlen sind genau die Produkte von geeigneten Teilern dieser Zahlen.

Beweis:

"$\Longleftarrow$": Offensichtlich ist $u\,v \mid a\,b$, wenn $u \mid a$ und $v \mid b$.

"$\Longrightarrow$": Sei $w \mid a\,b$. Wir betrachten u := ggT(a, w) und v := ggT(b, w). Natürlich ist $u \mid a$ und $v \mid b$. Es ist also zu zeigen: $w = u\,v$. Zunächst bemerken wir, dass u, v teilerfremd sind (denn ein gemeinsamer Teiler von u, v wäre auch ein gemeinsamer Teiler von a, b). Nun ist $u \mid w$ und $v \mid w$, also auch $u\,v \mid w$ (Übung!). Als nächstes zeigen wir, dass auch umgekehrt w ein Teiler von $u\,v$ ist (womit alles bewiesen ist). Da u und v ggT's sind, schreiben wir sie als Vielfachensumme

$$u = x_1\,a + y_1\,w$$
$$v = x_2\,b + y_2\,w.$$

Hieraus ergibt sich: $u\,v = x_1\,x_2\,a\,b + x_1\,y_2\,a\,w + x_2\,y_1\,b\,w + y_1\,y_2\,w^2$. Nach Voraussetzung ist w ein Teiler von $a\,b$, es enthält somit auch der erste Summand dieser Summe den Faktor w. Daraus folgt: $w \mid u\,v$.◆

Aus der Hilfsbehauptung (*) ergibt sich direkt:

■ 5.5.7. Proposition

Für teilerfremde a, b gilt: $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$

■ Beweis

Jeder Teiler, der in $\sigma(a\,b)$ auftritt, ist nach (*) das Produkt eines Teilers von a und eines Teilers von b, und umgekehrt. Diese Produkte entstehen, wenn man $\sigma(a) \cdot \sigma(b)$ ausmultipliziert.◆

■ 5.5.8. Proposition

$$\sigma(a) = \prod_{i=1}^{n} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

■ Beweis

Die Behauptung folgt aus Prop. 5.5.7. Dabei ist der Spezialfall von Primzahlpotenzen zu verwenden und zu berücksichtigen, dass zwei Primfaktorpotenzen in der PFZ von a teilerfremd sind.◆

■ Beispiele

1. $a = 1800 = 2^3 \cdot 3^2 \cdot 5^2$, also: $\sigma(a) = (1 + 2 + 4 + 8) \cdot (1 + 3 + 9) \cdot (1 + 5 + 25) = 6045$

2. $a = 1486016741376 = 2^{23} \cdot 3^{11}$, also : $\sigma(a) = \frac{2^{24} - 1}{2 - 1} \cdot \frac{3^{12} - 1}{3 - 1} = 4458041569800$

6. Stellenwertsysteme

6.1. B-adische Darstellung ganzer Zahlen

■ Bezeichnungssysteme für Zahlen

Im Umgang mit Zahlen greifen wir auf Zahlennamen (Zahlwörter) wie *eins*, *zwei*, *elf*, *hundert* oder spezielle Zahlsymbole wie 1, 2, 3, usw. zurück. Diese Bezeichnungen sind historisch und in ihrer Ausprägung mehr oder weniger willkürlich. Für die Arithmetik benötigen wir darüberhinaus ein Bezeichnungssystem, das …

(1) auf einer einfachen (leicht durchschaubaren) Systematik aufbaut,

(2) im Prinzip alle (unendlich vielen) natürlichen Zahlen abbildet und dabei …

(3) nicht zu schnell zu langen Bezeichnungen führt,

(4) die Grundrechenarten möglichst bequem durchzuführen gestattet.

Das einfache Hintereinanderschreiben von Einheiten

|, ||, |||, ||||, |||||, ||||||, |||||||, ...

erfüllt zwar die Forderungen (1) und (2), jedoch bei weitem nicht (3) und (4).

Die römische Zahlenschrift notiert ebenfalls zunächst Einheiten: I, II, III, mischt in diese Methode dann aber Subtraktions- und Additionsvorschriften hinein (IV für 4, VI für 6 usw.), wodurch die Darstellung größerer Zahlen und vor allem die grundlegenden Rechenarten rasch unübersichtlich werden.

Demgegenüber liefert das sog. *Stellenwertsystem* bzw. die ihm zu Grunde liegende Idee des wiederholten Bündelns ein Verfahren, mit dem sich die Forderungen (1) bis (4) weitgehend erfüllen lassen. In Ansätzen war das Bündeln bereits bei alten Kulturvölkern ausgeprägt (z.B. bei den Maya zu Grössen von 20; bei den Babyloniern zu 12 und 60, die noch in unserer heutigen Zeit- und Winkelmessung vorkommen). Die Stellenwert*systematik* wurde allerdings erst ca. 500 Jahre n. Chr. in Indien erfunden. Dabei wurde die Null als Zahl "anerkannt" und mit einem eigenen Symbol 0 für "Leere" (sunya) in das System eingeführt, um ausdrücken zu können, dass zu einer bestimmten Bündelgröße *keine* Bündel vorliegen. Das Wort "Ziffer" ist arabischen Ursprungs und bedeutet Null. Die Araber haben das Stellenwertsystem (zur Basis bzw. Bündelgrösse zehn) nach Westen gebracht und dort propagiert.

■ B-adische Darstellung ganzer Zahlen

Wir bezeichnen die Bündelgrösse (auch *Basis* genannt) mit B, wobei $B \geq 2$ ganz. Der Wert $B = 1$ ist uninteressant, weil er nicht zu echtem Bündeln führt. Im Dezimalsystem ist $B = 10$. Man benötigt B Zahlwörter – die sogenannten B-adischen Ziffern – zur Bezeichnung der möglichen Bündelanzahlen, angefangen von Null (0) bis zur größten Zahl unterhalb der Bündelgrösse ($B - 1$).

Das B-adische Stellenwertsystem beruht auf der Tatsache, dass sich eine natürliche Zahl stets als Wert einer Polynomfunktion mit B-adischen Ziffern als Koeffizienten zum Argument B darstellen lässt. Dies besagt der folgende Darstellungssatz:

■ 6.1.1. Proposition

Jede ganze Zahl $a > 0$ ist eindeutig in der Form $a = \sum_{i=0}^{n} c_i B^i$ darstellbar,

wobei $0 \leq c_i < B$ $(i = 0, 1, \ ..., n)$ und $c_n > 0$.

■ Beweis

Vgl. Abschnitt 6.3. ◆

■ Bezeichnung

$\sum_{i=0}^{n} c_i B^i$ wird (in diesem Zusammenhang) abgekürzt notiert: $(c_n\, c_{n-1} \ldots c_1\, c_0)_B$. Die c_i heißen *B-adische Ziffern*. Der Bezug (im Index) auf die Basis kann auch fortfallen, wenn keine Missverständnisse zu befürchten sind.

In der Darstellung von a in Prop. 6.1.1. klammern wir B aus und erhalten die Division-mit-Rest-Form:

$$a = (c_n B^{n-1} + \ldots + c_1)\, B + c_0$$

Die Einerziffer c_0 ist somit Rest der Division $a : B$. Der Ganzteil a_1 dieser Division lässt sich in analoger Weise auf die Division-mit-Rest-Form bringen:

$$a_1 = (c_n B^{n-2} + \ldots + c_2)\, B + c_1$$

Demnach ist die Ziffer c_1 der Rest der Division $a_1 : B$, usw. – Wiederholte Division mit Rest (bei stets gleichem Divisor B) liefert somit die Ziffernfolge der B-adischen Darstellung von a:

■ 6.1.2. Algorithmus (B-adische Bündelung)

Sei $B \geq 2$ (ganz) vorgegeben, $a \in \mathbb{N}$.

Solange $a > 0$, führe aus:

(1) Dividiere a durch B und notiere den Rest z.

(2) Ersetze a durch $\left[\frac{a}{B}\right]$.

Das Verfahren endet nach endlich vielen Schritten (da bei jedem Durchgang ein a entsteht, das kleiner ist als sein Vorgänger). Die dabei entstandene Folge der Reste (in umgekehrter Reihenfolge) c_n, c_{n-1}, ..., c_1, c_0 bildet die B-adische Ziffernfolge, welche die Zahl a darstellt:

$$0 \le c_i < B \qquad (i = 0, 1, \ldots, n)$$

$$a = c_0 + c_1 B + c_2 B^2 + \ldots + c_n B^n$$

Für Rechenbeispiele vgl. die Vorlesung.

■ Spezielle Basen

Die Basis 10 des Dezimalsystems geht vermutlich auf die Anzahl der Finger zurück. Daneben spielen heute, vor allem in der Computertechnik, die Basen 2 und 16 eine wichtige Rolle.

1. *Dyadische* (oder *binäre*) Darstellungen, d.h. solche zur Basis 2, kommen mit den Ziffern 0 und 1 aus und lassen sich daher durch zweiwertige physikalische Zustände ("Strom fließt" – "Strom fließt nicht") modellieren. Natürliche Zahlen schreiben sich als *Bitvektoren* (0-1-Folgen):

$$243 = (243)_{10} = (11110011)_2$$

Bitvektoren sind vor allem für technische Zwecke von Interesse; mit ihnen werden die grundlegenden Rechenoperationen überaus einfach, allerdings werden die Zahlwörter im Mittel mehr als dreimal so lang wie im Dezimalsystem.

2. Fasst man jeweils vier dyadische Ziffern zusammen und ersetzt sie durch ein einziges Symbol, so gelangt man zur *Hexadezimal*-Darstellung mit der Basis $B = 2^4 = 16$:

0000 = 0	0001 = 1	0010 = 2	0011 = 3
0100 = 4	0101 = 5	0110 = 6	0111 = 7
1000 = 8	1001 = 9	1010 = A	1011 = B
1100 = C	1101 = D	1110 = E	1111 = F

Beispiel: $(1111\ 0011)_2 = (F3)_{16} = \$F3 = 243$

Die Schreibweise mit vorangestelltem $-Zeichen ist in der Computertechnik gebräuchlich.

6.2. Das Horner-Schema

Ist umgekehrt eine B-adische Darstellung $c = (c_n\, c_{n-1} \ldots c_1\, c_0)_B$ gegeben, so ist die von ihr repräsentierte Zahl nichts anderes als der Wert der Polynomfunktion $\gamma(x) = \sum_{i=0}^{n} c_i\, x^i$ an der Stelle $x = B$, also: $c = \gamma(B)$.

■ Beispiel

$$(1433)_5 = 1 \cdot 5^3 + 4 \cdot 5^2 + 3 \cdot 5^1 + 3 \cdot 5^0 = 243 = (243)_{10}$$

Diese Berechnung erfordert 3 Additionen und 6 Multiplikationen. Durch Ausklammern lassen sich 3 Multiplikationen einsparen:

$$1\cdot 5^3 + 4\cdot 5^2 + 3\cdot 5^1 + 3\cdot 5^0 = (5^2 + 4\cdot 5 + 3)\cdot 5 + 3 = ((1\cdot 5 + 4)\cdot 5 + 3)\cdot 5 + 3$$

Wertet man die Klammern schrittweise von innen beginnend aus, so erkennt man die Umkehrung des Bündelungsverfahrens (fortgesetzte Division durch die Basis B). In seiner allgemeinen Form heißt dieser Algorithmus *Horner-Schema*.

■ 6.2.1. Algorithmus (Horner-Schema)

Die Polynomfunktion $\gamma(x) = c_0 + c_1\, x + c_2\, x^2 + ... + c_n\, x^n$ sei gegeben. Dann wird der Wert $h = \gamma(B)$ wie folgt berechnet:

(1) Setze $h = c_n$

(2) Für $i = n - 1$ bis 0: Ersetze h durch $h \cdot B + c_i$

Für Rechenbeispiele vgl. die Vorlesung.

6.3. Beweis des Darstellungssatzes

Wir haben 1. die Existenz und 2. die Eindeutigkeit der Darstellung zu zeigen. Den Beweis zu 1. führen wir mit vollständiger Induktion; beim Beweis zu 2. benutzen wir das Prinzip der kleinsten Zahl (PdkZ).

Zu 1.: Die Zahl $a = 1$ ist (als eingliedrige Ziffernfolge) ihre eigene B-adische Darstellung. Für den Induktionsschritt "$a \longrightarrow a + 1$" setzen wir eine Darstellung $a = c_n\, B^n + ... + c_1\, B + c_0$ voraus. Es ist zu zeigen, dass auch $a + 1$ sich so darstellen lässt. Zunächst betrachten wir den Sonderfall: $c_k = B - 1$ für $0 \le k \le n$. Es ergibt sich: $c_0 + 1 = B$, also $c_1\, B + c_0 + 1 = c_1\, B + B = (c_1 + 1)\, B = B^2$, und damit wiederum $c_2\, B^2 + B^2 = (c_2 + 1)\, B^2 = B^3$, usw. bis $a + 1 = (c_n + 1)\, B^n = B^{n+1} = (1\ 0\ \ ...\ 0)_B$, d.h. $a + 1$ hat eine B-adische Darstellung bestehend aus einer 1, gefolgt von $n + 1$ Nullen. Sind nicht sämtliche Ziffern $= B - 1$, so betrachten wir das erste (kleinste) $k \ge 0$ mit $c_k + 1 < B$. Wir können dann in der Darstellung $a + 1 = c_n\, B^n + ... + c_k\, B^k + (c_{k-1}\, B^{k-1} + ... + c_0 + 1)$ die Summe in Klammern (…) so behandeln wie eben den Sonderfall und erhalten: (…) $= B^k$. Damit ergibt sich:

$$a + 1 = c_n\, B^n + ... + c_k\, B^k + B^k = c_n\, B^n + ... + (c_k + 1)\, B^k$$

Dies ist aber wegen $c_k + 1 < B$ eine B-adische Darstellung von $a + 1$. Für $k < n$ ist $c_n > 0$ nach Induktionsvoraussetzung; für $k = n$ geht die Darstellung über in $a + 1 = (c_n + 1)\, B^n$, also ist auch hier die Ziffer mit dem höchsten Stellenwert größer als 0.

Zu 2.: Wir nehmen indirekt an, es gebe Zahlen mit mehr als einer B-adischen Darstellung. Wir wählen a (nach dem PdkZ) als kleinste derartige Zahl; es gibt dann verschiedene B-adische Darstellungen $a = c'_m\, B^m + ... + c'_1\, B + c'_0$ und $a = c_n\, B^n + ... + c_1\, B + c_0$, d.h. es ist $c_i \ne c'_i$ für mindestens ein i. Beide Darstellungen lassen sich deuten als Standardform der Division $a : B$ mit Rest:

$$a = (c'_m\, B^{m-1} + ... + c'_1)\, B + c'_0 \text{ und } a = (c_n\, B^{n-1} + ... + c_1)\, B + c_0$$

Nach Prop. 5.1.1 (Division mit Rest) stimmen die Reste überein, d.h. $c'_0 = c_0$, und ebenso die Ganzteile: $c'_m\, B^{m-1} + ... + c'_1 = c_n\, B^{n-1} + ... + c_1$. Die Ganzteile sind (wegen $B > 1$) kleiner als a, besitzen also aufgrund der Minimalität von a nur *eine* B-adische Darstellung, d.h. es ist $m = n$ und $c'_i = c_i$ $(1 \le i \le n)$. Dies ist ein Widerspruch! ◆

7. Kongruenzen und Restklassen

7.1. Kongruenz modulo *m*

■ 7.1.1. Definition

Sei $m \geq 2$ ganz. Zwei ganze Zahlen a, b heißen kongruent modulo m, wenn sie bei Division durch m denselben Rest lassen, d.h. wenn $a \bmod m = b \bmod m$. Man schreibt dafür kurz: $a \equiv b \bmod m$ oder auch nur $a \equiv b$, wenn der Modul m aus dem Zusammenhang hervorgeht.

■ Beispiele

$$17 \equiv 3 \bmod 7$$
$$7 \equiv -1 \bmod 2$$
$$25 \equiv 0 \bmod 5$$

■ 7.1.2. Proposition

$\equiv$ ist eine Äquivalenzrelation, d.h. für alle ganzen Zahlen a, b gilt:

(1) $a \equiv a \bmod m$

(2) $a \equiv b \bmod m \Longrightarrow b \equiv a \bmod m$

(3) $a \equiv b \bmod m \ \wedge \ b \equiv c \bmod m \Longrightarrow a \equiv c \bmod m$

■ Beweis

Die Gültigkeit dieser Aussagen ergibt sich direkt aus Def. 7.1.1. ◆

■ Bezeichnungen

Die Eigenschaften (1), (2) und (3) aus Prop. 7.1.2 heißen beziehungsweise Reflexivität, Symmetrie und Transitivität.

Die folgende Proposition liefert ein einfaches hinreichendes und notwendiges Kriterium für die Kongruenz zweier ganzer Zahlen.

■ 7.1.3. Proposition

Für alle $a, b \in \mathbb{Z}$ gilt: $a \equiv b \bmod m \iff m \mid a - b$

■ Beweis

1. "$\Longrightarrow$": Nach Voraussetzung hat man Division-mit-Rest Darstellungen $a = q_1\, m + r$ und $b = q_2\, m + r$. Daraus folgt: $a - b = (q_1 - q_2)\, m$.

2. "$\Longleftarrow$": Nach Voraussetzung gibt es ein $q \in \mathbb{Z}$ mit $a - b = q\, m$. Nun machen wir Division durch m mit Rest: $a = q_1\, m + r_1$, $b = q_2\, m + r_2$, wobei $0 \le r_1, r_2 < m$. Daraus ergibt sich: m ist Teiler der Differenz $r_1 - r_2$, und wegen $0 \le |\, r_1 - r_2\, | \; < m$ auch $r_1 = r_2$. ◆

Es erweist sich, dass man mit Kongruenzen zum selben Modul so rechnen kann wie mit gewöhnlichen Gleichungen. Genauer: Aus gültigen Kongruenzen, z.B. $10 \equiv 1 \bmod 3$ und $-7 \equiv 5 \bmod 3$, gewinnt man durch Addieren und Multiplizieren jeweils der linken und rechten Seiten neue (gültige) Kongruenzen, hier: $3 \equiv 6 \bmod 3$ bzw. $-70 \equiv 5 \bmod 3$. Diese Art der Verknüpfungstreue wird mit dem Begriff Kongruenzrelation bezeichnet.

■ 7.1.4. Proposition

$\equiv$ ist eine Kongruenzrelation, d.h. für alle $a, a', b, b' \in \mathbb{Z}$ folgt aus $a \equiv b \bmod m$ und $a' \equiv b' \bmod m$:

(1) $a + a' \equiv b + b' \bmod m$

(2) $a \cdot a' \equiv b \cdot b' \bmod m$

■ Beweis

Behauptung (1) ergibt sich direkt aus der Gleichung: $(a + a') - (b + b') = (a - b) + (a' - b')$, Behauptung (2) aus der Gleichung: $a\, a' - b\, b' = a(a' - b') + (a - b)\, b'$. ◆

Als Spezialfall von 7.1.4,(2) hat man: $a \equiv b \bmod m \implies a\, c \equiv b\, c \bmod m$. Die Umkehrung dieser Aussage (mithin eine Kürzungsregel, welche gestattet, einen Faktor auf beiden Seiten einer Kongruenz zu "streichen") ist im allgemeinen falsch; sie gilt aber, wenn Faktor und Modul relativ prim sind:

■ 7.1.5. Proposition

$a\, c \equiv b\, c \bmod m \wedge c, m$ teilerfremd $\implies a \equiv b \bmod m$

■ Beweis

Nach Prop. 7.1.3 ist m Teiler von $a\, c - b\, c$, also auch von $c(a - b)$. Da m zu c teilerfremd ist, erhalten wir mit dem Lemma von Euklid (Prop. 5.2.3,(1)): $m \mid a - b$. ◆

7.2. Teilbarkeitskriterien

Mittels Kongruenzenrechnung lassen sich Kriterien für die Teilbarkeit ganzer Zahler im Rahmen von Stellenwertsystemen gewinnen.

Jede Kongruenz $a \equiv b \bmod d$ mit einem variablen Testteiler d kann als "Teilbarkeitsregel" aufgefasst werden: a ist genau dann durch d teilbar, wenn b durch d teilbar ist. Um überhaupt nützlich zu sein, muss der Teilbarkeitstest bei einer der beiden Zahlen einfacher sein als bei der anderen, und zudem ein Zusammenhang zwischen den Ziffernfolgen von a und b bestehen.

Wir werden daher in einem Stellenwertsystem zur Basis $B \geq 2$ zu vorgelegter natürlicher Zahl $c = (c_n \ldots c_1\, c_0)_B$ eine "einfacher zu testende" (und i.a. kleinere) Zahl c' suchen, die in bestimmter Weise aus den B-adischen Ziffern von c gebildet ist sowie die Kongruenz erfüllt:

$$c \equiv c' \bmod d$$

■ Beispiel

$B = 10$, $c' = c_n + \ldots + c_1 + c_0$ (Quersumme von c im Dezimalsystem) und $d = 9$. Es gilt: $c \equiv c' \bmod 9$. Zum Beweis zeigt man (nach Prop. 7.1.3), dass 9 die Differenz $c - c' = \sum_{j=0}^{n} (10^j - 1)\, c_j$ teilt. Dies ist in der Tat der Fall, da $10^j - 1 = (10 - 1) \cdot (1 + 10 + \ldots + 10^{j-1})$. – Aus $c \equiv c' \bmod 9$ folgt unmittelbar auch: $c \equiv c' \bmod 3$.

Die aus der Schule bekannten Quersummen- und Endstellenregeln lassen sich in einheitlicher und allgemeiner Form nach folgender Idee gewinnen: Man sucht einen Stellenwert (d.h. eine Potenz der Basis) B^s und eine ganze Zahl ρ derart, dass die Kongruenz

$$B^s \equiv \rho \bmod d$$

erfüllt ist; anschließend reduziert man damit in der B-adischen Darstellung von c alle durch B^s teilbaren Summanden (gemäß den Kongruenzrechenregeln 7.1.4). Wirksame Reduktionen ergeben sich auf diese Weise für Werte $\rho \in \{0, 1, -1\}$ bei möglichst klein gewähltem Exponenten $s \geq 1$.

Ist $c = (c_n \ldots c_1\, c_0)_B$, so wollen wir vereinbaren: $c_k = 0$ für $k > n$. (Führende Nullen in der B-adischen Darstellung einer Zahl verändern den Wert nicht.) Es gilt das folgende allgemeine *Reduktionslemma*:

■ 7.2.1. Proposition

Sei $B \geq 2$ (Basis), $s \geq 1$ und $d \geq 2$ ganze Zahlen. Hat man die Kongruenz $B^s \equiv \rho \bmod d$ für eine ganze Zahl ρ, so gilt für alle natürlichen Zahlen $c = (c_n \ldots c_1\, c_0)_B$:

$$c \equiv \sum_{j=0}^{\left[\frac{n}{s}\right]} (c_{(j+1)\,s-1} \ldots c_{j\,s})_B \cdot \rho^j \bmod d$$

■ Beweis

Wir gruppieren in der B-adischen Darstellung $c = (c_0 + c_1 B + \ldots + c_{s-1} B^{s-1}) + \ldots + c_n B^n$ bei c_0 beginnend je s Summanden in einer "Klammer". Die j-te Klammer lautet: $c_{(j+1)s-1} B^{(j+1)s-1} + \ldots + c_{js} B^{js}$. Im Falle $j > 0$ ist hierin der Faktor B^{js} enthalten. Wir klammern ihn aus und erhalten:

$$c = (c_{s-1} \ldots c_0)_B + \sum_{j=1}^{\left[\frac{n}{s}\right]} (c_{(j+1)s-1} \ldots c_{js})_B \cdot B^{js}$$

Unter Beachtung von $B^{js} = (B^s)^j \equiv \rho^j \bmod d$ liefert dies die behauptete Kongruenz. ◆

Für $\rho = 0$ liefert das Reduktionslemma Endstellenregeln, für $\rho = 1$ Quersummenregeln und für $\rho = -1$ alternierende Quersummenregeln. Im Folgenden sind einige dieser Spezialisierungen aufgeführt.

■ Endstellenregeln

Sei $B^s \equiv 0 \bmod d$. Dann gilt nach Prop. 7.2.1: $c \equiv (c_{s-1} \ldots c_0)_B \bmod d$. Im Dezimalsystem ($B = 10$) ergibt sich für $s = 1$:

$$d \mid c \iff d \mid c_0 \text{ für } d \in \{2, 5\}$$

Für $s = 2$ erhält man

$$d \mid c \iff d \mid (c_1 c_0)_{10} \text{ für } d \in \{2, 4, 5, 10, 20, 25, 50\}$$

■ Quersummenregeln

Sei $B^s \equiv 1 \bmod d$. Dann gilt nach Prop. 7.2.1: $c \equiv \sum_{j=0}^{[n/s]} (c_{(j+1)s-1} \ldots c_{js})_B \bmod d$. Für $s = 1$ erhält man daraus folgende allgemeine Quersummenregel für beliebige Teiler d von $B - 1$: $d \mid c \iff d \mid c_n + \ldots + c_0$. Für $B = 10$ liefert dies die bekannten Regeln für die Teilbarkeit durch 3 und durch 9.

Bei $s = 2$ muss der Testteiler d in $B^2 - 1$ aufgehen. Für $d = B + 1$ ist dies der Fall. Somit gilt:
$B + 1 \mid c \iff B + 1 \mid (c_1 c_0)_B + (c_3 c_2)_B + \ldots$ Im Dezimalsystem: Eine Zahl ist durch 11 teilbar genau dann, wenn ihre Quersumme 2. Ordnung es ist. Beispiel: 1071675 ist durch 11 teilbar, denn: 75 + 16 + 7 + 1 = 99.

■ Alternierende Quersummenregeln

Sei $B^s \equiv -1 \bmod d$. Dann gilt nach Prop. 7.2.1: $c \equiv \sum_{j=0}^{[n/s]} (c_{(j+1)s-1} \ldots c_{js})_B \cdot (-1)^j \bmod d$. Für $s = 1$ erhält man daraus folgende allgemeine Regel für beliebige Teiler d von $B + 1$: $d \mid c \iff d \mid (-1)^n c_n + \ldots - c_1 + c_0$. Für $B = 10$ besagt dies, dass eine Zahl durch 11 teilbar ist, wenn ihre alternierende Quersumme (Wechselquersumme) es ist. Beispiel: 1071675 ist durch 11 teilbar, denn: 5 − 7 + 6 − 1 + 7 − 0 + 1 = 11.

Im Dezimalsystem ergibt sich für $s = 2$: Eine Zahl ist durch 101 genau dann teilbar, wenn ihre alternierende Quersumme 2. Ordnung durch 101 teilbar ist. Für $s = 3$ resultiert aus $10^3 \equiv -1 \bmod 7$ ein Kriterium für den Teiler 7 mit Bezug auf Wechselquersummen 3. Ordnung: $7 \mid c \iff 7 \mid (c_2 c_1 c_0)_{10} - (c_6 c_5 c_4)_{10} + \ldots$ Beispiel: 164471104 ist durch 7 teilbar, denn: $104 - 471 + 164 = -203 = 7 \cdot (-29)$.

7.3. Rechnen mit Rest(klass)en

■ 7.3.1. Definitionen

Sei $a \in \mathbb{Z}$, $m \geq 2$ ganz. Die Menge aller zu a modulo m kongruenten ganzen Zahlen heißt Restklasse (modulo m) von a. Wir notieren sie wie folgt: $[a]_m := \{x \in \mathbb{Z} \mid a \equiv x \bmod m\}$. Jedes $x \in [a]_m$ heißt Repräsentant (Vertreter) der Restklasse $[a]_m$. Ein nichtnegativer Repräsentant $< m$ heißt ausgezeichnet. Es gibt (modulo m) genau m ausgezeichnete Repräsentanten: 0, 1, ..., $m - 1$; ihre Menge wird mit $\mathbb{Z}_m$ bezeichnet.

■ Bemerkung

Ist eine beliebige ganze Zahl a gegeben, so ist $r = a \bmod m$ der ausgezeichnete Repräsentant der Restklasse $[a]_m$, mithin $[a]_m = [r]_m$. – Die Vereinigung aller Restklassen von ausgezeichneten Repräsentanten ganzer Zahler ist gleich $\mathbb{Z}$. Die Restklasse $[0]_m$ enthält genau die durch m teilbaren Zahlen.

■ Beispiel

Sei $m = 5$. Die Restklasse $[17]_5$ besteht aus allen ganzen Zahlen x mit $x \equiv 17 \bmod 5$, d.h. $x - 17 = 5 \cdot k$ mit ganzem k; wir schreiben dies um zu $x = 17 + 5\,k$ ($k \in \mathbb{Z}$). Somit ist $[17]_5 = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$. Ausgezeichneter Repräsentant dieser Restklasse ist der Rest 2. Es gilt $2 \equiv 17 \bmod 5$ und (gleichbedeutend damit) $[17]_5 = [2]_5$. Die Restklasse $[0]_5 = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ enthält genau die durch 5 teilbaren Zahlen.

■ 7.3.2. Definition

Für $a, b \in \mathbb{Z}_m$ wird festgelegt:

(1) $a \oplus b := (a + b) \bmod m$

(2) $a \odot b := (a \cdot b) \bmod m$

$\oplus$ heißt Rest(klassen)addition, $\odot$ Rest(klassen)multiplikation.

■ 7.3.3. Proposition

Restaddition und -multiplikation sind beide assoziativ und kommutativ, sie besitzen 0 bzw. 1 als neutrales Element, und es gilt das Distributivgesetz der Multiplikation bzgl. der Addition. Genauer gilt für alle $a, b, c \in \mathbb{Z}_m$:

$(\text{Ass}_1): a \oplus (b \oplus c) = (a \oplus b) \oplus c$

$(\text{Ass}_2): a \odot (b \odot c) = (a \odot b) \odot c$

$(\text{Kom}_1): \quad a \oplus b = b \oplus a$

$(\text{Kom}_2): \quad a \odot b = b \odot a$

$(\text{Dist}_1): \quad a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

$(\text{Neutr}_1): \quad a \oplus 0 = a$

$(\text{Neutr}_2): \quad a \odot 1 = a$

■ Beweis

(Neutr_1), (Neutr_2) sowie (Kom_1), (Kom_2) sind ganz offensichtlich. Das Distributivgesetz und die beiden Assoziativgesetze müssen im Einzelnen begründet werden.

Zu (Ass_1): Wir haben nach Definition $b \oplus c = (b + c) \bmod m = r_1$ und $a \oplus b = (a + b) \bmod m = r_2$ mit $b + c = q_1\, m + r_1$ und $a + b = q_2\, m + r_2$ $(0 \le r_1,\, r_2 < m)$. Es ergibt sich: $a + r_1 = a + b + c - q_1\, m$, $r_2 + c = a + b + c - q_2\, m$, also:

$$a \oplus (b \oplus c) = (a + r_1) \bmod m = (a + b + c) \bmod m = (r_2 + c) \bmod m = (a \oplus b) \oplus c$$

In völlig analoger Weise zeigt man (Ass_2) (Übung!).

Zu (Dist_1): Wir notieren wieder $b \oplus c = (b + c) \bmod m = r_1$, ferner: $a \odot b = a\, b \bmod m = r_2$ und $a \odot c = a\, c \bmod m = r_3$. Es bestehen Glgen: $b + c = q_1\, m + r_1$, $a\, b = q_2\, m + r_2$ und $a\, c = q_3\, m + r_3$, wobei $0 \le r_i < m$, $i = 1, 2, 3$. Die linke Seite von (Dist_1) ist gleich $a \odot r_1 = a\, r_1 \bmod m$, die rechte Seite $(r_2 + r_3) \bmod m$. Beide stimmen überein:

$a\, r_1 = a(b + c - q_1\, m) = a\, b + a\, c - q_1\, a\, m$, also: $a\, r_1 \bmod m = a\, b + a\, c$

$r_2 + r_3 = (a\, b - q_2\, m) + (a\, c - q_3\, m) = a\, b + a\, c - (q_2 + q_3)\, m$, also: $(r_2 + r_3) \bmod m = a\, b + a\, c$.

◆

In Analogie zum Rechnen mit gewöhnlichen Zahlen liegt die Frage nahe, ob die Gleichung $a \oplus x = 0$ zu vorgegebenem $a \in \mathbb{Z}_m$ eine Lösung (in $\mathbb{Z}_m$) besitzt. Die folgende Proposition bejaht dies:

■ 7.3.4. Proposition

Zu beliebigem $a \in \mathbb{Z}_m$ gibt es genau ein $x \in \mathbb{Z}_m$ mit $a \oplus x = 0$.

■ Beweis

$a \oplus x = 0$ ist nach Definition gleichbedeutend mit $(a + x) \bmod m = 0$, d.h. $a + x = k \cdot m$ für ein geeignetes ganzes k. Da a und x als Elemente von $\mathbb{Z}_m$ gegeben (bzw. gesucht) sind, haben wir $0 \leq a + x \leq 2m - 2$ und damit $k = 1$ als einzig mögliche Wahl. Tatsächlich folgt aus $a + x = m$ auch $a \oplus x = 0$. ◆

■ Bezeichnungen

Die in Prop. 7.4.4 eindeutig bestimmte Lösung x der Glg $a \oplus x = 0$ heißt additives Inverses von a. Dementsprechend heißt eine (eindeutige) Lösung der Glg $a \odot x = 1$ multiplikatives Inverses von a.

Die Existenz multiplikativer Inverser ist *nur unter besonderen Voraussetzungen* gegeben. So hat in $\mathbb{Z}_{10}$ z.B. 3 ein multiplikatives Inverses (hier: 7, weil $3 \odot 7 = 1 \bmod 10$); allerdings gilt dies nicht für 4. Denn aus $4 \odot x = 1$ erhalten wir einerseits $5 \odot (4 \odot x) = 5 \odot 1 = 5$, andererseits nach (Ass_2) (Prop. 7.3.3) auch $(5 \odot 4) \odot x = 0 \odot x = 0$.

Der folgende Lehrsatz gibt ein hinreichendes und notwendiges Kriterium dafür, dass ein vorgegebener Rest $a \in \mathbb{Z}_m$ ein multiplikatives Inverses besitzt.

■ 7.3.5. Proposition

Sei $m \geq 2$ und $a \in \mathbb{Z}_m$ beliebig. Dann gilt:

Es existiert (genau) ein $x \in \mathbb{Z}_m$ mit $a \odot x = 1 \Longleftrightarrow a, m$ sind teilerfremd.

■ Beweis

1. Existenz: Wir notieren äquivalente Umformungen des links von "⟺" stehenden Ausdrucks:

Ex. $x \in \mathbb{Z}_m$ mit $a \odot x = 1$	gdw. $a\,x \bmod m = 1$
	gdw. $a\,x \equiv 1 \bmod m$
	gdw. $m \mid a\,x - 1$
	gdw. $a\,x - 1 = m\,k$ für ein $k \in \mathbb{Z}$
	gdw. ex. $x, y \in \mathbb{Z}$ mit $x\,a + y\,m = 1$ (*).

In (*) liegt eine positive Linearkombination von a, m vor, und zwar die kleinste: $\text{Min}\,\mathcal{L}^+(a, m) = 1$. Nach dem Hauptsatz über den ggT (Prop. 5.4.1) stimmt sie mit dem $\text{ggT}(a, m)$ überein, d.h. $\text{ggT}(a, m) = 1$, was bedeutet: a, m sind teilerfremd.

Sind umgekehrt a, m teilerfremd, so ist der $\text{ggT}(a, m) = 1$ und nach dem Lemma von Bachet (Prop. 5.2.2) als Linearkombination von a und m darstellbar: $1 \in \mathcal{L}(a, m)$. Dies ist nichts anderes als die Aussage (*).

2. Eindeutigkeit: Sei $a \odot x = 1 = a \odot y$ mit teilerfremden a, m. Es folgt $a\,x \equiv a\,y \bmod m$ und mit Hilfe der Kürzungsregel (Prop. 7.1.5): $x \equiv y \bmod m$. Die Bedingung $x, y \in \mathbb{Z}_m$ erzwingt dann $x = y$. ◆

■ Bemerkung

Ist p prim, so haben nach Prop. 7.3.5 *alle* Elemente aus $\mathbb{Z}_p \setminus \{0\}$ ein multiplikatives Inverses. Das heißt: $\mathbb{Z}_p$ ist ein (endlicher!) Körper, in welchem bzgl. der Restaddition und -multiplikation so gerechnet werden kann wie in $\mathbb{Q}$ bzgl. der gewöhnlichen Addition und Multiplikation rationaler Zahlen.

■ Potenzieren in $\mathbb{Z}_m$

Zu $a \in \mathbb{Z}_m$ und ganzem $k \geq 0$ werden die Potenzen a^k ebenso gebildet wie bei gewöhnlichen Zahlen: $a^2 = a \odot a$, $a^3 = a^2 \odot a$, usw.; ferner: $a^1 = a$ und $a^0 = 1$. Aufgrund von Prop. 7.3.3 gelten die vertrauten Rechenregeln für Potenzen: $a^r\, a^s = a^{r+s}$ sowie $(a^r)^s = a^{r\,s}$ und $(a\, b)^r = a^r\, b^r$ (Beweise durch vollständige Induktion als Übung!).

a^k als Element von $\mathbb{Z}_m$ ist nach Definition der Rest $a^k \bmod m$. Um ihn rechnerisch zu bestimmen (z.B. bei größeren Werten von k), zerlegt man den Exponenten in eine Summe: $k = n_1 + n_2 + \ldots$ Man erhält mit der ersten der o.g. Potenzrechenregeln: $a^k = a^{n_1+n_2+\cdots} = a^{n_1}\, a^{n_2} \ldots \bmod m$ und hat so die Aufgabe darauf reduziert, zunächst Reste $a^{n_1} \bmod m$, $a^{n_2} \bmod m$, usw. mit kleineren Exponenten auszuwerten.

■ Beispiele

Welche Endziffer hat 7^{22} im Dezimalsystem? Die Frage ist gleichbedeutend damit, 7^{22} in $\mathbb{Z}_{10}$ bzw. $7^{22} \bmod 10$ zu bestimmen.

Wir können damit beginnen, nach einer Potenz $7^n \equiv 1 \pmod{10}$ zu suchen: $7^2 \equiv 9$, $7^4 \equiv 9^2 \equiv 1$. Division von 22 durch 4 mit Rest liefert dann die Zerlegung: $22 = 4 \cdot 5 + 2$ und die anschließende Reduktion:
$7^{22} \equiv 7^{4\cdot 5+2} \equiv (7^4)^5 \cdot 7^2 \equiv 1^5 \cdot 7^2 \equiv 9$.

Alternativ dazu erzeugt die *Methode des fortgesetzten Quadrierens* eine brauchbare Zerlegung des Exponenten k in Zweierpotenzen. Dazu stellt man $k = 22$ dyadisch dar:

$$22 = (10110)_2 = 2^1 + 2^2 + 2^4 = 2 + 4 + 16$$

Anschließend erzeugt man durch wiederholtes Quadrieren von $a = 7$ den Restevorrat, der bei der Reduktion modulo m (hier: $m = 10$) benötigt wird: $7^2 \equiv 9$, $7^4 \equiv 1$, $7^8 \equiv 1$, $7^{16} \equiv 1$. Es ergibt sich modulo 10:
$7^{22} \equiv 7^2 \cdot 7^4 \cdot 7^{16} \equiv 9 \cdot 1 \cdot 1 \equiv 9$.

Die Quadriermethode bietet sich an, wenn man keine naheliegende Zerlegung mit einem Rest 1 findet. Beispiel: $3^{1000} \bmod 19$. Die dyadische Zerlegung lautet: $1000 = 8 + 32 + 64 + 128 + 256 + 512$. Quadrieren (und Reduzieren) liefert für die Summanden: $3^8 \equiv 6$, $3^{32} \equiv 4$, $3^{64} \equiv 16$, $3^{128} \equiv 9$, $3^{256} \equiv 5$, $3^{512} \equiv 6$. Damit ergibt sich:
$3^{1000} \equiv 6 \cdot 4 \cdot 16 \cdot 9 \cdot 5 \cdot 6 \equiv 16$.

In dem zuletzt behandelten Beispiel hätte man allerdings auch mit der Kongruenz $3^{18} \equiv 1 \bmod 19$ reduzieren können. Diese ergibt sich unmittelbar aus dem sog. *kleinen Satz von Fermat*, der in folgender Proposition formuliert wird:

■ 7.3.6. Proposition

Sei $a \in \mathbb{Z}$ beliebig und p eine Primzahl, die kein Teiler von a ist. Dann gilt: $a^{p-1} \equiv 1 \bmod p$.

■ **Beweis**

In Arithmetik und Algebra II.

8. Abbildungen

Abbildungen (Funktionen) dienen in der Mathematik dazu, Zusammenhänge und Abhängigkeiten zwischen verschiedenen Objekten oder Gegenstandsbereichen darzustellen bzw. herzustellen.

Der Begriff "Abbildung" ist eine *universelle Idee*, deren enorme Tragweite sich vor allem in der Entwicklung der Mathematik seit dem 17. Jahrhundert gezeigt hat. So steht im Mittelpunkt der Analysis der Begriff der (reellen und komplexen) Funktion, und auch Geometrie und Algebra haben durch den Abbildungsgedanken ihr heutiges Gepräge erhalten.

8.1. Darstellungsformen

Abbildungen treten in ganz unterschiedlichen Kontexten auf, und entsprechend vielfältig sind ihre Erscheinungs- bzw. Darstellungsformen.

■ Listen (endliche Zuordnungslisten)

Eine Liste verkörpert eine primitive (endliche) Form der Zuordnung, z.B. werden in einer Preisliste bestimmten Waren ihre Preise zugeordnet:

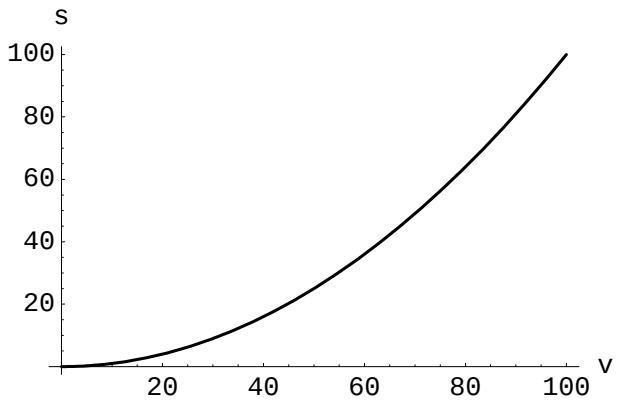
Ware	**Preis (in Euro)**
Kaffeemaschine A	140
Kaffeemaschine B	190
Kaffeemaschine C	300

■ Funktionale Abhängigkeit (zwischen variablen Größen)

Eine veränderliche Größe wird aus einer anderen Größe (abhängig von dieser) aufgrund eines "Gesetzes" berechnet. Z.B. hängt der Bremsweg s eines Autos von dessen Geschwindigkeit v ab und errechnet sich (in sehr grober Näherung) nach der Gleichung ("Fahrschul-Faustformel"):

$$s = \left(\frac{v}{10}\right)^2$$

(s wird in m, v in km/h gemessen und die Bremsbeschleunigung mit $-4\,\mathrm{m/s^2}$ zugrundegelegt). Der Bremsweg hängt somit von der Geschwindigkeit quadratisch ab. Man kann dies durch ein Schaubild im v-s-Koordinatensystem veranschaulichen:



In diesem Beispiel sind Funktionsgleichung und Schaubild (sog. Funktionsgraph) einer Darstellung in Gestalt einer Liste bzw. Tabelle überlegen.

■ Folgen (endliche und unendliche Wertelisten)

Eine Folge a_0, a_1, a_2, … lässt sich als (endliche oder unendliche) Liste auffassen. Dabei werden die Objekte a_i den Platznummern $i \in \{0, 1, 2, \ldots\}$ zugeordnet. Viele in der Praxis betrachtete Folgen entspringen irgendwelchen "Bildungsgesetzen" (vgl. dazu Kapitel 4).

Ein weiteres Beispiel: Die Folge (x_n), definiert durch $x_0 = 1$ und $x_{n+1} = \frac{1}{2}\left(x_n + \frac{2}{x_n}\right)$ für $n \geq 1$, liefert rationale Näherungen für $\sqrt{2}$; genauer gilt: $x_n \longrightarrow \sqrt{2}$ für $n \longrightarrow \infty$:

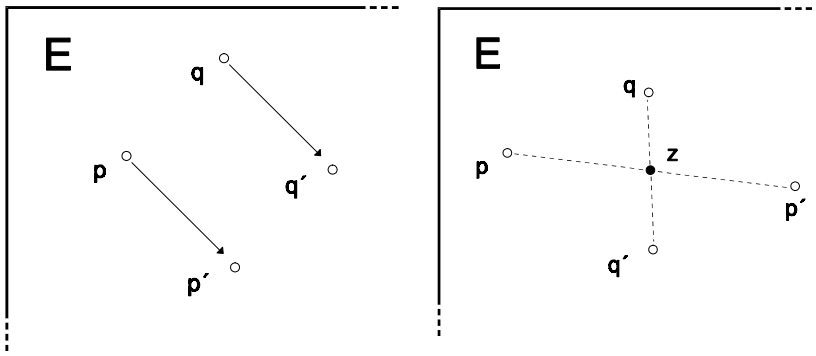
n	x_n
0	1
1	$\frac{3}{2}$
2	$\frac{17}{12}$
3	$\frac{577}{408}$
4	$\frac{665857}{470832}$

usf.

■ Geometrische Transformationen (von Ebene und Raum)

Eine geometrische Transformation (Abbildung) der Ebene E ordnet jedem Punkt p von E einen Punkt p' von E in der Weise zu, dass je zwei Punkte p, q denselben Abstand haben wie die ihnen zugeordneten p', q'. Unter einer solchen Transformation behalten demnach alle Strecken ihre ursprüngliche Länge; man spricht von *Kongruenzabbildungen*. Aus dem Geometrieunterricht der Schule sind ihre Grundtypen bekannt: *Verschiebung*, *Drehung* und *Spiegelung.*

Die folgenden Schaubilder zeigen Zuordnungspaare einer Verschiebung und einer Punktspiegelung (Halbdrehung der Ebene um z):



In völlig entsprechender Weise betrachtet man geometrische Transformationen des Raums.

■ Vorbereitungen zum allgemeinen Abbildungsbegriff

Der allgemeine Begriff der Abbildung (Funktion) fasst die genannten Beispiele (und natürlich viele weitere) unter sich. Man hat sich darunter eine eindeutige Zuordnung zwischen irgend zwei Mengen A und B vorzustellen, notiert: $f : A \longrightarrow B$. Gehört ein Zuordnungspaar (a, b) zu f (wörtlich: $(a, b) \in f$), so schreibt man dies üblicherweise auch als: $b = f(a)$. Durch die Gleichungsnotation kommt zum Ausdruck, dass dem Argument $a \in A$ vermöge f der eindeutig bestimmte Wert $b \in B$ zugeordnet ist.

Wenden wir diese Notation auf das obige Beispiel einer Preisliste f für Kaffemaschinen an: Es gilt dann $(\text{Kaffeemaschine } B, 190) \in f$ bzw. in der Gleichungsnotation: $f(\text{Kaffeemaschine } B) = 190$. Vielleicht hat der Anbieter noch ein (in der Preisliste nicht aufgeführtes) Modell D, das genausoviel kostet wie Modell B. Es ist dann $f(\text{Kaffemaschine } D) = 190$. Man beachte: Die Eindeutigkeit der Preisfunktion f besagt, dass eine Ware nicht verschiedene Preise hat, d.h. für eine Maschine m kann nicht einmal $f(m) = 190$ und zugleich auch $f(m) = 140$ sein. Durch die Schreibweise als Gleichung ist dies von vornherein erzwungen (sonst hätte man sofort Widersprüche wie hier: 190 = 140).

Das Beispiel geometrischer Transformationen berührt noch weitere Aspekte der Notation von Abbildungen. Wird die Ebene E als Produktmenge $\mathbb{R}^2$ (Menge aller Koordinatenpaare (x, y) der Punkte von E) aufgefasst, so lassen sich Kongruenzabbildungen durch geeignete Funktionen $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ beschreiben. Jede solche Funktion f ordnet dem Koordinatenpaar (x, y) eines Punktes $p \in E$ das Koordinatenpaar (x', y') seines Bildpunktes $p' \in E$ zu. Neben der Gleichungsnotation $(x', y') = f(x, y)$ kann auch ein spezieller Pfeil für die Einzelzuordnung verwendet werden: $(x, y) \mapsto (x', y')$. Z.B. bewirkt die Vorschrift $(x, y) \mapsto (x + 2, y - 1)$ eine Verschiebung aller Punkte der Ebene parallel zu dem Ortsvektor, der vom Koordinatenursprung $(0, 0)$ zum Punkt $(2, -1)$ führt. Die Transformation kann auch koordinatenweise angegeben werden:

$$x' = x + 2$$
$$y' = y - 1$$

Dies lässt sich auch in einer Gleichung zusammenfassen: $f(x, y) = (x + 2, y - 1)$. (Die für ein Argument in Paarform strenggenommen erforderliche Schreibweise $f((x, y))$ wird der Einfachheit halber vermieden.)

8.2. Allgemeine Definitionen zum Abbildungsbegriff

Mit der Einführung des Abbildungsbegriffs entsteht ein gewisser Bedarf an terminologischen Vereinbarungen. Diese sind ziemlich allgemein gehalten und für sich genommen nicht besonders gehaltvoll; sie bilden aber unerlässliche Elemente der in allen Zweigen der Mathematik benutzten "Abbildungssprache".

■ 8.2.1. Definition und Notation

Eine Zuordnung (Relation) f zwischen Mengen A und B ist durch eine Menge von Paaren (a, b) mit $a \in A$, $b \in B$ gegeben (d.h. es ist $f \subseteq A \times B$). Sie heißt Abbildung (Funktion) von A nach B (bezeichnet als $f : A \longrightarrow B$), wenn es zu *jedem* $a \in A$ *genau* ein $b \in B$ gibt, das zu a in der Relation f steht: $(a, b) \in f$. Diesen Fall beschreibt man durch die Gleichung: $b = f(a)$.

■ Bezeichnungen

Besteht zu gegebener Abbildung $f : A \longrightarrow B$ eine Gleichung $b = f(a)$, so heißt b Bild(wert) (oder Funktionswert) von a unter f; umgekehrt heißt a Urbild(wert) von b unter f (in älterer Terminologie: Argument). Die Menge A heißt Definitionsmenge (in älterer Terminologie: Definitionsbereich) von f, die Menge B heißt Zielmenge von f. Stimmen Definitions- und Zielmenge überein ($A = B$), so heißt $f : A \longrightarrow A$ Selbstabbildung von A. Eine spezielle Selbstabbildung ist die Identität oder identische Abbildung (von A), $\mathrm{id}_A : A \longrightarrow A$, definiert durch $\mathrm{id}_A(x) := x$ für alle $x \in A$.

■ Bemerkung

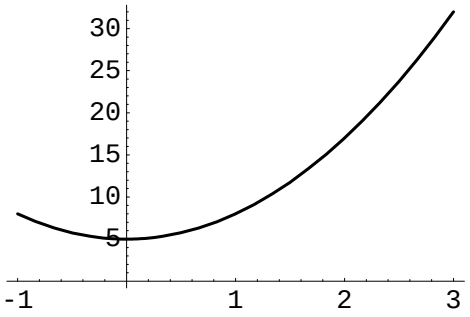
Zwei Abbildungen $f : A \longrightarrow B$ und $g : A \longrightarrow B$ sind gleich ($f = g$) genau dann, wenn für alle $x \in A$ gilt: $f(x) = g(x)$. (Dies ergibt sich direkt aus der Definition der Gleichheit von Mengen, hier: Paarmengen.)

■ 8.2.2. Definition

Sei $f : A \longrightarrow B$ eine Abbildung und $X \subseteq A$. Die Menge aller Bilder unter f von Elementen aus X heißt f-Bild von X (oder: Bild von X unter f), bezeichnet mit $f[X]$. Es ist also $f[X] := \{f(x) \mid x \in X\}$. Die Definition lässt sich auf Mengen $X \not\subseteq A$ wie folgt ausdehnen: $f[X] := \{f(x) \mid x \in X \cap A\}$. Das f-Bild der Definitionsmenge A, d.h. $f[A]$, heißt Wertemenge von f.

■ Beispiel

Sei $f : \mathbb{R} \longrightarrow \mathbb{R}$ definiert durch $f(x) := 3x^2 + 5$ ($x \in \mathbb{R}$), $X = [-1; 1]$. Dann ist $f[X] = [5; 8]$ und $f[\mathbb{R}] = [5; \infty)$.



■ 8.2.3. Proposition

Ist $f : A \longrightarrow B$ eine beliebige Abbildung von A nach B und sind X, Y irgendwelche Teilmengen von A, so gelten die Aussagen:

(1) $f[\emptyset] = \emptyset$

(2) $X \subseteq Y \Longrightarrow f[X] \subseteq f[Y]$

(3) $f[X] \subseteq f[A] \subseteq B$

(4) $f[X \cap Y] \subseteq f[X] \cap f[Y]$

(5) $f[X \cup Y] = f[X] \cup f[Y]$

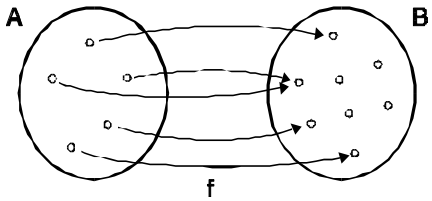
■ Beweis

(1), (2), (3) ergeben sich unmittelbar aus Def. 8.2.2 (Übung!).

Zu (4): Ist $b \in f[X \cap Y]$, so existiert ein $a \in X \cap Y$ mit $b = f(a)$. Da somit $a \in X$ und $a \in Y$, ist auch $b \in f[X]$ und $b \in f[Y]$, mithin $b \in f[X] \cap f[Y]$.

Zu (5): Analog zu (4), wobei hier zusätzlich $f[X] \cup f[Y] \subseteq f[X \cup Y]$ zu zeigen ist. Ist etwa $b \in f[X]$, so hat man $b = f(a)$ für ein $a \in X \subseteq X \cup Y$ und somit $b \in f[X \cup Y]$. Im Fall von $b \in f[Y]$ ist die Überlegung dieselbe. ◆

Eigenschaften von Abbildungen $f : A \longrightarrow B$ lassen sich gut mit Hilfe von Pfeildiagrammen anhand kleiner endlicher Mengen illustrieren. Den allgemeinen Fall stellt ein Diagramm dar, bei dem Elemente von B mehrfach oder auch gar nicht zugeordnet werden:

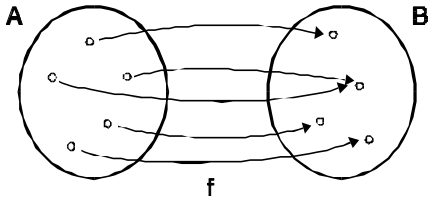


Indem man die eine oder andere dieser Möglichkeiten ausschließt, ergeben sich die im Folgenden definierten Abbildungseigenschaften.

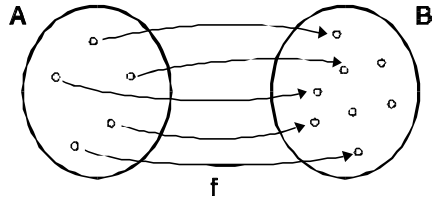
■ 8.2.4. Definition

Sei $f : A \longrightarrow B$ irgendeine Abbildung. f heißt ...

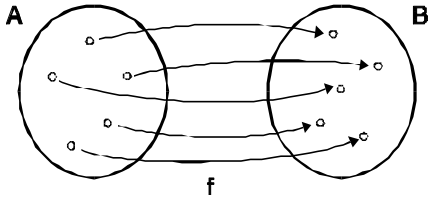
(1) surjektiv (Surjektion oder Abbildung auf B), wenn $f[A] = B$ gilt, d.h. wenn zu jedem $b \in B$ ein $a \in A$ mit $b = f(a)$ existiert:



(2) injektiv (Injektion oder eineindeutig), wenn zu jedem $b \in B$ höchstens ein $a \in A$ mit $b = f(a)$ existiert:



(3) bijektiv (oder Bijektion), wenn f surjektiv und injektiv ist:



■ Bemerkungen

1. Der Gebrauch derartiger Diagramme ist in erster Linie eine anschauliche Hilfe zum generellen Verständnis von Abbildungseigenschaften. Es ist dringend zu empfehlen, zu solchen Schaubildern von vornherein immer auch die logische Beschreibung mitzudenken. In der Praxis führt in den meisten Fällen nur eine formale bzw. rechnerische Betrachtung zum Ziel.

2. Bei einer surjektiven Abbildung stimmen Zielmenge und Wertemenge überein (jedes Element der Zielmenge besitzt mindestens ein Urbild). Bei einer injektiven Abbildung haben verschiedene Argumente (Urbilder) stets verschiedene Funktionswerte (Bilder). In älterer deutschsprachiger Terminologie heißen Bijektionen auch *umkehrbar eineindeutige Abbildungen*.

3. In der Praxis lässt sich die Injektivität einer Abbildung f häufig am zweckmäßigsten wie folgt nachweisen: Man nimmt $f(x) = f(x')$ für beliebige Argumente x, x' an und zeigt dann, dass daraus $x = x'$ folgt.

■ Beispiel (zu Bemerkung 3)

Die (in 8.1 erwähnte) Bremswegfunktion $s : [0; \infty) \longrightarrow [0; \infty)$, definiert durch $s(v) := \frac{v^2}{100}$, ist injektiv. Ist nämlich $s(v) = s(u)$, so ergibt sich $v^2 = u^2$, also $(v + u)(v - u) = 0$. Wäre nun $v \neq u$, so hieße das: $v + u = 0$. Da v, u nicht beide Null sein können, hat man $v + u > 0$ (Widerspruch!); somit muss $v = u$ sein.

■ Weitere Beispiele

1. Sei $Q(n)$ die dezimale Quersumme der natürlichen Zahl n. Dann ist $Q : \mathbb{N} \longrightarrow \mathbb{N}$ eine surjektive, jedoch nicht injektive Abbildung. Zu vorgegebenem $n \in \mathbb{N}$ ist etwa $r_n := \underbrace{11\ldots1}_{n-\text{mal}} \in \mathbb{N}$ ein geeignetes Urbild: $Q(r_n) = n$. Allerdings können verschiedene Argumente gleiche Quersummen besitzen, z.B. $Q(123) = Q(42)$.

2. Sei $M = \{1, 2, 3, 4, 5\}$. Dann ist $f : M \longrightarrow M$, definiert durch $f(1) = 1,\ f(2) = 3,\ f(3) = 5,\ f(4) = 2,\ f(5) = 4$, eine bijektive Selbstabbildung von M.

3. Die Identität $\mathrm{id}_A : A \longrightarrow A$ ist bijektiv.

4. Verschiebungen, Drehungen und Spiegelungen der Ebene E sind surjektiv (anschaulich begründen!). Als abstandstreue Abbildungen f der Ebene auf sich sind sie aber auch bijektiv. Für irgend zwei Punkte $p, q \in E,\ p \neq q$, gilt nämlich: $0 <$ Abstand$(p, q) =$ Abstand$(f(p),\ f(q))$, also $f(p) \neq f(q)$ (da nur voneinander verschiedene Punkte einen positiven Abstand realisieren).

8.3. Verkettung (Komposition)

Zwei Abbildungen $f : A \longrightarrow B$ und $g : B' \longrightarrow C$ lassen sich verketten (hintereinander ausführen), wenn die Wertemenge der einen (hier: f) in der Definitionsmenge der anderen (hier: g) enthalten ist: $f[A] \subseteq B'$. Auf diese Weise gewinnt man eine neue (zusammengesetzte) Abbildung $h : A \longrightarrow C$, die den Elementen von A Werte aus C zuordnet. Dies geschieht einfach dadurch, dass $x \in A$ zunächst unter f den Wert $y = f(x)$ erhält und diesem $y\ (\in B)$ durch g schließlich der Wert $z = g(y)$ zugeordnet wird. Es wird also $h(x) := g(f(x))$ $(x \in A)$ gesetzt.

Die folgende Definition gibt den hier beschriebenen Sachverhalt etwas pedantischer wieder.

■ 8.3.1. Definition

Seien $f : A \longrightarrow B$ und $g : B' \longrightarrow C$ irgendwelche Abbildungen und es gelte $f[A] \subseteq B'$. Es werde $h : A \longrightarrow C$ durch die Vorschrift $h(x) := g(f(x))$ $(x \in A)$ erklärt, d.h. es gelte $z = h(x)$ genau dann, wenn für ein geeignetes $y \in B'$ die Relationen $y = f(x)$ und $z = g(y)$ bestehen.

■ Bemerkung und Bezeichnung

Die in 8.3.1 erklärte Abbildung h ist in eindeutiger Weise durch f und g bestimmt. Man nennt sie Verkettung (auch Komposition oder Hintereinanderausführung) von f und g, bezeichnet als $g \circ f$ (lies: "g nach f"). Mit dieser Bezeichnung gilt: $(g \circ f)(x) = g(f(x))$ für alle in Betracht kommenden Argumente x. *Warnung*: Auch wenn die Verkettung $g \circ f$ existiert, lässt sich nicht immer auch $f \circ g$ bilden. Ferner gilt im Allgemeinen: $g \circ f \neq f \circ g$.

■ Beispiele

1. Zu den Funktionen $f : \mathbb{R} \longrightarrow \mathbb{R},\ f(x) := 3x^2 + 5$, und $g : \mathbb{R} \longrightarrow \mathbb{R},\ g(x) := |1 - x|$, sollen die beiden Verkettungsprodukte $f \circ g$ und $g \circ f$ ermittelt werden. Für alle $x \in \mathbb{R}$ gilt:

$$(f \circ g)(x) = f(g(x)) = 3\,g(x)^2 + 5 = 3\,|1 - x|^2 + 5 = 3\,x^2 - 6\,x + 8$$
$$(g \circ f)(x) = g(f(x)) = |1 - f(x)| = |1 - (3\,x^2 + 5)| = 3\,x^2 + 4$$

2. Die Verkettung geometrischer Transformationen ist das Thema der *Abbildungsgeometrie*. Überlegen Sie sich übungshalber das Ergebnis folgender Verkettungen: zwei Verschiebungen (= Verschiebung); zwei Spiegelungen an zwei sich in einem Punkt schneidenden Geraden (= Drehung um diesen Punkt); zwei Drehungen um denselben Punkt (= Drehung) etc.

Die Abbildungseigenschaften (surjektiv, injektiv, bijektiv) bleiben bei der Verkettung erhalten. Die diesbezüglichen Behauptungen sind im nachstehenden Satz formuliert:

■ 8.3.2. Proposition

Für Abbildungen $f : A \longrightarrow B$ und $g : B \longrightarrow C$ gilt:

(1) g und f surjektiv $\Longrightarrow g \circ f$ surjektiv

(2) g und f injektiv $\Longrightarrow g \circ f$ injektiv

(3) g und f bijektiv $\Longrightarrow g \circ f$ bijektiv

■ Beweis

Vgl. den Abschnitt "Abbildungseigenschaften und Verkettung" unter
www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/em_1998/kapitel_3.htm

■ 8.3.3. Proposition

Für Abbildungen $f : A \longrightarrow B$ und $g : B \longrightarrow C$ gilt:

(1) $g \circ f$ injektiv $\Longrightarrow f$ injektiv

(2) $g \circ f$ surjektiv $\Longrightarrow g$ surjektiv

■ Beweis

Vgl. den Abschnitt "Abbildungseigenschaften und Verkettung" unter
www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/em_1998/kapitel_3.htm

■ 8.3.4. Proposition

Seien $f, g, h : A \longrightarrow A$ beliebige Selbstabbildungen von A. Dann gilt:

(1) $(f \circ g) \circ h = f \circ (g \circ h)$

(2) $f \circ \mathrm{id}_A = \mathrm{id}_A \circ f = f$

■ Beweis

Vgl. den Abschnitt "Rechnen mit Abbildungen" unter
www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/em_1998/kapitel_3.htm

■ Bemerkung

Die Gültigkeit des Assoziativgesetzes für die Verkettung rechtfertigt die klammerfreie Notation: $f \circ g \circ h \circ \ldots$. Die identische Abbildung spielt bei der Verkettung die Rolle eines neutralen Elements.

■ Stückweise definierte Abbildungen

Viele in der Praxis verwendete Funktionen sind nicht durch einen einzigen Ausdruck festgelegt, sondern mit Hilfe einer Fallunterscheidung (bzgl. des Arguments) aus mehreren Rechenausdrücken aufgebaut, so z.B. die Funktion, mit der die Einkommensteuer abhängig vom Einkommen x berechnet wird. Ein besonders einfaches Beispiel dieser Art ist der Absolutbetrag $|x|$, der $= x$ für $x \geq 0$ und $= -x$ für $x < 0$ ist.

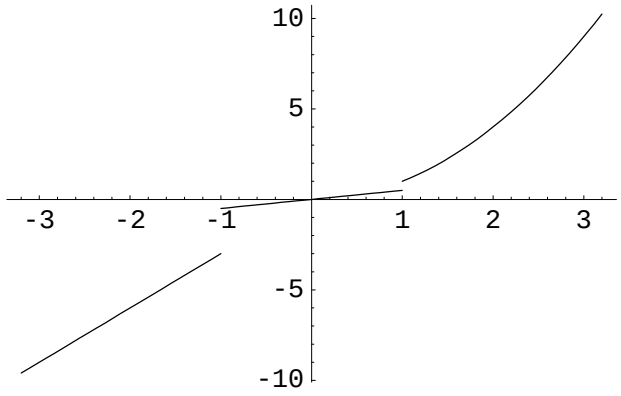
Abbildungen (Funktionen) f, die in dieser Weise gegeben sind, heißen stückweise definiert. Dabei ist bzgl. des Funktionsarguments eine *vollständige Fallunterscheidung* zu treffen: Die Definitionsmenge A von f wird in paarweise disjunkte Teilmengen $C_1, C_2, \ldots, C_m$ zerlegt, deren Vereinigung ganz A ist (sog. Klasseneinteilung). Damit kann dann $f(x)$ für jedes $x \in A$ festgelegt werden, indem man den Wert von $f(x)$ in jedem der möglichen (einander ausschließenden) Fälle $x \in C_j$ $(1 \leq j \leq m)$ angibt.

■ Beispiel

einer stückweise definierten reellen Funktion $f : \mathbb{R} \longrightarrow \mathbb{R}$. Die Definitionsmenge (ganz $\mathbb{R}$) werde in drei Intervalle zerlegt: $I_1 = (-\infty; -1]$, $I_2 = (-1; 1)$, $I_3 = [1; \infty)$, auf denen f jeweils durch unterschiedliche Berechnungsvorschriften festgelegt ist:

$$f(x) := \begin{cases} 3x, & x \in I_1 \\ \frac{x}{2}, & x \in I_2 \\ x^2, & x \in I_3 \end{cases}$$

Der Funktionsgraph von f zeigt an den Grenzen des inneren Intervalls I_2 Sprungstellen:



Eine stückweise definierte Selbstabbildung f einer Menge lässt sich als Verkettungsprodukt ihrer "Fallfunktionen" auffassen, wenn sie nicht aus den "Fallmengen" C_j herausführt: $f[C_j] \subseteq C_j$ für $j = 1, 2, \ldots, m$. (Ein Beispiel hierfür ist die eben definierte Funktion, für die man übungshalber $f[I_1] \subseteq I_1$, $f[I_2] \subseteq I_2$ und $f[I_3] \subseteq I_3$ bestätige).

Wir wollen den Sachverhalt anhand einer stückweise (auf zwei disjunkten Fallmengen C_1, C_2 mit $A = C_1 \cup C_2$) definierten Funktion $f : A \longrightarrow A$ darlegen (was sich problemlos auf den allgemeinen Fall einer beliebigen Anzahl von Fallmengen $C_1, C_2, \ldots, C_m$ erweitern lässt):

$$(*) \qquad f(x) = \begin{cases} g_1(x), & x \in C_1 \\ g_2(x), & x \in C_2 \end{cases}$$

Die folgende stückweise Definition erweitert den Definitionsbereich der g_j auf ganz A:

$$(**) \qquad f_j(x) := \begin{cases} g_j(x), & x \in C_j \\ x, & x \in A \setminus C_j \end{cases}$$

■ 8.3.5. Proposition

Sei $f : A \longrightarrow A$ stückweise gemäß (*) definiert und die $g_j : C_j \longrightarrow C_j$ Selbstabbildungen der C_j ($j = 1, 2$). Dann gilt mit den gemäß (**) definierten Funktionen f_1, f_2:

(1) $f_1 \circ f_2 = f$

(2) $f_2 \circ f_1 = f_1 \circ f_2$

■ Beweis

Zu (1): Für $x \in C_1$ gilt: $(f_1 \circ f_2)(x) = f_1(f_2(x)) = f_1(x) = g_1(x) = f(x)$. Für $x \in C_2$ gilt:
$(f_1 \circ f_2)(x) = f_1(f_2(x)) = f_1(g_2(x)) = g_2(x) = f(x)$.

Zu (2): Wie unter (1) zeigt man für alle $x \in A = C_1 \cup C_2$: $(f_2 \circ f_1)(x) = f(x)$. ◆

In Abschnitt 8.6 werden wir u.a. der Frage nachgehen, wie sich zu gegebener Selbstabbildung einer Menge eine Art "natürlicher" Klasseneinteilung dieser Menge gewinnen lässt (und in deren Gefolge eine Darstellung der Abbildung als kommutierbares Verkettungsprodukt gemäß Prop. 8.3.5).

8.4. Umkehrung

■ 8.4.1. Proposition (Satz von der Umkehrabbildung)

> Zu jeder bijektiven Abbildung $f : A \longrightarrow B$ gibt es genau eine bijektive Abbildung $g : B \longrightarrow A$ derart, dass $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$.

■ Beweis

Vgl. den Abschnitt "Satz von der Umkehrabbildung" unter
www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/em_1998/kapitel_3.htm

■ Bezeichnung

Die nach 8.4.1 zu bijektivem f eindeutig bestimmte Abbildung g heißt inverse Abbildung (auch Umkehrabbildung) von f. Sie wird mit f^{-1} bezeichnet. Mit dieser Bezeichnung gilt: $f^{-1}(f(x)) = x$ für alle $x \in A$ sowie $f(f^{-1}(x)) = x$ für alle $x \in B$.

■ 8.4.2. Proposition ("Umkehrregel")

Seien $f : A \longrightarrow B$, $g : B \longrightarrow C$ bijektive Abbildungen. Dann ist $g \circ f : A \longrightarrow C$ bijektiv, und es gilt: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

■ Beweis

Dass $g \circ f : A \longrightarrow C$ bijektiv ist, ergibt sich aus Prop. 8.3.2. Gemäß Prop. 8.4.1 bleibt daher nur zu zeigen, dass $f^{-1} \circ g^{-1}$ die Umkehrabbildung von $g \circ f$ ist. In der Tat gilt für alle $x \in A$:

$$((f^{-1} \circ g^{-1}) \circ (g \circ f))(x) = f^{-1}(g^{-1}(g(f(x)))) = f^{-1}(\mathrm{id}_B(f(x))) = f^{-1}(f(x)) = \mathrm{id}_A(x)$$

◆

8.5. Iteration

■ 8.5.1. Definition

Sei M eine Menge und $f : M \longrightarrow M$ eine Selbstabbildung von M. Zu ganzem $n \geq 0$ wird eine Abbildung $f^n : M \longrightarrow M$, die n-te Iterierte von f, wie folgt rekursiv definiert:

$$f^0 = \mathrm{id}_M$$

$$f^n = f \circ f^{n-1} \text{ für } n \geq 1$$

■ Bemerkung

Die n-te Iterierte von f ist das n-fache Verkettungsprodukt von f mit sich selbst: $f^n = \underbrace{f \circ \ldots \circ f}_{n\text{-mal}}$

■ Beispiele

1. Sei $M = \{1, 2, 3, 4, 5\}$ und $f : M \longrightarrow M$ definiert durch $f(1) = 1$, $f(2) = 3$, $f(3) = 5$, $f(4) = 2$, $f(5) = 4$. Dann gilt: $f^4 = \mathrm{id}_M$.

2. Sei $f : \mathbb{R} \longrightarrow \mathbb{R}$ definiert durch $f(x) = a\,x + b$ (mit reellen Zahlen a, b). Für $a = 1$ gilt: $f^n(x) = x + n\,b$; für $a \neq 1$ gilt: $f^n(x) = a^n\,x + b \cdot \frac{a^n - 1}{a - 1}$. – Zur Bedeutung und genaueren Diskussion dieses Beispiels vgl. man Kapitel 2 unter **www.uni-flensburg.de/mathe/zero/veranst/modellbildung/modellbildung.html**

■ 8.5.2. Definition

Zu beliebigem $x \in M$ sei $B_x := \{f^k(x) \mid k = 0, 1, 2, \ldots\}$ (bezeichnet als: bei x beginnende Bahn von f).

■ 8.5.3. Proposition

Für Bahnen von Abbildungen $f : M \longrightarrow M$ gilt:

(1) $x \in B_x$

(2) $u \in B_x \implies B_u \subseteq B_x$

(3) $f[B_x] \subseteq B_x$

(4) $f(u) = x \implies B_x \subseteq B_u$

■ Beweis

Zu (1): Klar wegen $x = f^0(x) \in B_x$.

Zu (2): Sei $y \in B_u$, dann ist $y = f^n(u)$ für ein $n \geq 0$. Da nach Voraussetzung $u \in B_x$, hat man $u = f^m(x)$ für ein $m \geq 0$. Damit ergibt sich: $y = f^n(f^m(x)) = f^{n+m}(x)$, also $y \in B_x$.

Zu (3): Sei $y \in f[B_x]$, dann ist $f(u) = y$ für ein $u \in B_x$. Zum einen ist daher $y \in B_u$, zum anderen aufgrund von (2): $B_u \subseteq B_x$, insgesamt also $y \in B_x$.

Zu (4): Ist $y \in B_x$, so ist $y = f^n(x)$ mit einem $n \geq 0$. Nach Einsetzen der Voraussetzung erhalten wir:
$y = f^n(f(u)) = f^{n+1}(u)$, mithin $y \in B_u$. ◆

■ Beispiel

Man betrachte die dezimale Quersummenfunktion $Q : \mathbb{N} \longrightarrow \mathbb{N}$. Die bei $a = 23478791$ beginnende Bahn von Q ist endlich: $B_a = \{23478791, 41, 5\}$. Hat man eine Vorgängerzahl b mit der Quersumme a, so gilt: $B_a \subset B_b$ (vgl. Beh. (4) von Prop. 8.5.3). Die Erweiterung der letzten Bahn lässt sich (in diesem Beispiel) offenbar beliebig fortsetzen.

Der folgende Lehrsatz fördert eine bemerkenswerte Eigenschaft injektiver Abbildungen zutage:

■ 8.5.4. Proposition

> Sei $f : M \longrightarrow M$ eine injektive Abbildung und $a \in M \setminus f[M]$ beliebig (d.h. a ist ein Element, das kein Urbild unter f besitzt, und f ist daher nicht surjektiv). Dann ist die bei a beginnende Bahn B_a eine unendliche Menge.

■ Beweis

Durch Induktion zeigt man: Die $f^k(a)$, $k = 0, 1, 2, \ldots$, sind lauter verschiedene Elemente von M. Vgl. den Abschnitt "Iteration" unter
www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/em_1998/kapitel_3.htm

■ Bemerkung und Beispiel

Eine injektive, aber nicht surjektive Selbstabbildung einer Menge ist nur möglich, wenn die Menge *unendlich viele Elemente* besitzt. Als "Galilei's Paradoxon" bekannt ist die Tatsache, dass durch die Funktion $f(n) = n^2$, $n \in \mathbb{N}$, eine injektive Zuordnung $\mathbb{N} \longrightarrow \mathbb{N}$ realisiert wird, derzufolge es ebensoviele Zahlen wie Quadratzahlen gibt. Andererseits bilden die Quadratzahlen eine echte Teilmenge von $\mathbb{N}$.

■ 8.5.5. Proposition

Sei M eine endliche Menge und f eine Selbstabbildung von M. Dann sind die folgenden Aussagen gleichwertig:

(1) f ist bijektiv

(2) f ist injektiv

(3) f ist surjektiv

■ Beweis

Die Behauptung ergibt sich aus Prop. 8.5.4. Vgl. dazu den Abschnitt "Iteration" unter
www.uni-flensburg.de/mathe/zero/veranst/arithalgebra/schreiber/em_1998/kapitel_3.htm

8.6. Zerlegung endlicher Selbstabbildungen

In diesem Abschnitts wollen wir A als beliebige *endliche* Menge und $f : A \longrightarrow A$ als irgendeine Selbstabbildung von A voraussetzen. Gesucht ist eine Klasseneinteilung $\{C_1, \ldots, C_m\}$ von A, die es erlaubt, f "in natürlicher Weise" als Verkettungsprodukt von Funktionen $f_1, \ldots, f_m$ darzustellen.

Als Fallmengen C_j bieten sich auf den ersten Blick die Bahnen der Abbildung f an. Ihre Vereinigung ist sicherlich $= A$, und für beliebiges $x \in A$ gilt: $f[B_x] \subseteq B_x$ (Eigenschaft (3) in Prop. 8.5.3). Allerdings können wir nicht erwarten, dass irgend zwei Bahnen disjunkt sind.

■ Beispiel

$A = \{1, 2, \ldots, 10\}$, $f(x) = 1 + (2\,x^3) \bmod 10$. Wir berechnen zunächst die Bahnen von f, die bei 1, 2, …, 10 beginnen:

$B_1 = \{1, 3, 5\} = B_3 = B_5$

$B_2 = \{2, 7\}$

$B_4 = \{4, 9\}$

$B_6 = \{6, 3, 5, 1\}$

$B_7 = \{7\}$

$B_8 = \{8, 5, 1, 3\}$

$B_9 = \{9\}$

$B_{10} = \{10, 1, 3, 5\}$

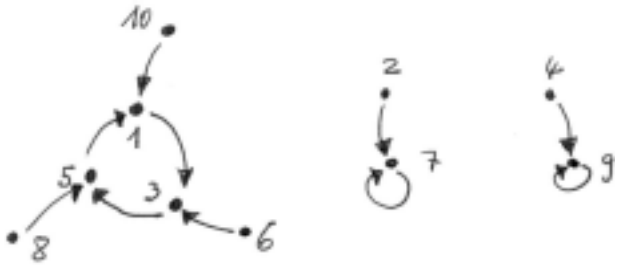
Fassen wir zueinander nicht disjunkte Bahnen zusammen, so entstehen drei Gruppen:

Gruppe 1: $B_1, B_3, B_5, B_6, B_8, B_{10}$

Gruppe 2: B_2, B_7

Gruppe 3: B_4, B_9

Die in jeder Gruppe vorkommenden Elemente aus A bilden einen zusammenhängenden Graphen, in welchem ein Element (eine Ecke) x durch eine gerichtete Kante mit der Ecke y genau dann verbunden ist, wenn $y = f(x)$ gilt:



Beobachtungen:

1. Wir definieren C_1, C_2, C_3 als Vereinigung der Bahnen in den Gruppen 1 bzw. 2 bzw. 3, also:
$C_1 = \{1, 3, 5, 6, 8, 10\}$, $C_2 = \{2, 7\}$, $C_3 = \{4, 9\}$. Diese C_j heißen Orbits von f. Sie bilden eine Klasseneinteilung von A; außerdem gilt $f[C_j] \subseteq C_j$. Damit sind (gemäß Prop. 8.3.5) Abbildungen f_j definiert, deren (kommutierbares) Verkettungsprodukt mit f übereinstimmt:

$$f_1 \circ f_2 \circ f_3 = f$$

2. Der Durchschnitt aller Bahnen, die gemeinsame Elemente besitzen, besteht aus zyklisch (kreisförmig) angeordneten Elementen. Für den ersten Orbit ergibt sich: $B_1 \cap B_3 \cap B_5 \cap B_6 \cap B_8 \cap B_{10} = \{1, 3, 5\}$. Der zweite und dritte Orbit liefern 1-elementige Durchschnitte $\{7\}$ bzw. $\{9\}$ (und entsprechende Kreise der Länge 1).

Es soll nun gezeigt werden, dass sich diese am speziellen Beispiel gemachten Beobachtungen sinngemäß verallgemeinern lassen. Dazu nehmen wir o.E. an: $A = \{1, 2, \ldots, n\}$. Die bei x beginnenden Bahnen B_x ($1 \le x \le n$) werden (wie im Beispiel) in Gruppen eingeteilt, deren jede genau die Bahnen enthält, die nicht disjunkt zueinander sind. Es mögen auf diese Weise m Gruppen entstehen. Es bezeichne C_j die Vereinigung und K_j den Durchschnitt aller Bahnen der j-ten Gruppe ($1 \le j \le m$).

■ 8.6.1. Proposition

(1) $C_1 \cup \ldots \cup C_m = A$ und $C_i \cap C_j = \emptyset$ für $i \neq j$

(2) $f[C_j] \subseteq C_j$ für alle $j = 1, 2, \ldots, m$

■ Beweis

Zu (1): Es ist offensichtlich $C_1 \cup \ldots \cup C_m = B_1 \cup \ldots \cup B_n = A$. Ferner gilt: Der Durchschnitt von $C_i = B_u \cup B_v \cup \ldots$ und $C_j = B_x \cup B_y \cup \ldots$ ergibt sich nach mengenalgebraischen Rechenregeln (vgl. Prop. 2.4.1) als Vereinigung leerer (!) Durchschnitte: $C_i \cap C_j = (B_u \cap B_x) \cup (B_v \cap B_x) \cup (B_u \cap B_y) \cup (B_v \cap B_y) \cup \ldots = \emptyset$.

Zu (2): Nach Prop. 8.2.3,(5) hat man zunächst $f[C_j] = f[B_x \cup B_y \cup \ldots] = f[B_x] \cup f[B_y] \cup \ldots$. Berücksichtigen wir nun auf der rechten Seite dieser Gleichung, dass nach Prop. 8.5.3,(3) $f[B_x] \subseteq B_x$ usw. gilt, so liefert dies die behauptete Inklusion. ◆

■ 8.6.2. Proposition

Sei A eine nichtleere endliche Menge und $f : A \longrightarrow A$ eine beliebige Selbstabbildung von A. Dann gibt es genau eine feinste Klasseneinteilung $C_1, \ldots, C_m$ von A mit $f[C_j] \subseteq C_j$ sowie eindeutig bestimmte Selbstabbildungen $f_1, \ldots, f_m$ von A mit $f = f_1 \circ \ldots \circ f_m$ und

$$f_j(x) = \begin{cases} f(x), & x \in C_j \\ x, & x \in A \setminus C_j \end{cases} \quad (1 \le j \le m).$$

■ Beweis

Die oben durchgeführte Konstruktion liefert eine (feinste) Klasseneinteilung $C_1, \ldots, C_m$ von A, welche (nach Prop. 8.6.1) die Eigenschaft $f[C_j] \subseteq C_j$ besitzt ($j = 1, 2, \ldots, m$). Daher ist g_j, definiert durch $g_j(x) = f(x)$ für $x \in C_j$, eine Selbstabbildung von C_j. Wie in Prop. 8.3.5 erhalten wir hieraus Funktionen f_j, für die die behauptete Zerlegungsgleichung gilt; die Reihenfolge der "Faktoren" f_j spielt dabei keine Rolle.

In Bezug auf die Klasseneinteilung sind die Faktoren des Verkettungsprodukts eindeutig. Um dies nachzuweisen, nehmen wir Abbildungen $h_1, \ldots, h_m$ an, welche die in der Behauptung erwähnten Eigenschaften der $f_1, \ldots, f_m$ besitzen. Wir zeigen $f_j = h_j$ für jedes $j \in \{1, \ldots, m\}$. Wählt man $x \in C_j$ beliebig, so ergibt sich einerseits $f_j(x) = (f_1 \circ \ldots \circ f_m)(x) = f(x)$ und andererseits $h_j(x) = (h_1 \circ \ldots \circ h_m)(x) = f(x)$, mithin $f_j = h_j$.

Schließlich nehmen wir an, es gäbe eine von $\{C_1, \ldots, C_m\}$ verschiedene Klasseneinteilung $\{D_1, \ldots, D_p\}$ mit $f[D_k] \subseteq D_k$ ($1 \le k \le p$). Dann muss es ein C_j und ein D_k mit nichtleerem Durchschnitt S geben. Mit Hilfe von Prop. 8.2.3,(4) ergibt sich: $f[S] \subseteq f[C_j] \cap f[D_k] \subseteq C_j \cap D_k = S$. Man erkennt: Durch geeignetes Abspalten von S aus C_j lässt sich die ursprüngliche Klasseneinteilung weiter verfeinern (Widerspruch). ◆

Im Anschluss an unser obiges Beispiel hatten wir beobachtet: Der Durchschnitt aller Bahnen, die gemeinsame Elemente besitzen, besteht aus zyklisch angeordneten Elementen. Wir verifizieren dies in folgender Form:

■ 8.6.3. Proposition

$f[K_j] = K_j$ für alle $j = 1, 2, \ldots, m$

■ Beweis

Wir setzen $K_j = B_x \bigcap B_y \bigcap \ldots$und wählen $a \in K_j$ beliebig. Da B_a eine der Bahnen ist, deren Durchschnitt K_j ist, hat man $B_a \supseteq K_j$. Andererseits gehört a zu allen Bahnen B_x, B_y, …, so dass nach Prop. 8.5.3,(2) $B_a \subseteq B_x$, $B_a \subseteq B_y$, usw., also auch $B_a \subseteq B_x \bigcap B_y \bigcap \ldots = K_j$. Insgesamt ergibt sich: Zu $a \in K_j$ ist stets $B_a = K_j$. Da $f[B_a] \subseteq B_a$ (nach Prop. 8.5.3,(3)), bleibt noch zu zeigen: $B_a \subseteq f[B_a]$.

1. Fall: $a = f(a)$. Es folgt $B_a = \{a\}$ und $f[B_a] = B_a$.

2. Fall: $a \neq f(a) = a_1$. Da a in sämtlichen B_x, B_y, … vorkommt, muss auch die Sequenz a, a_1 in allen Bahn-Folgen

$$B_x : x,\ f(x),\ f^2(x),\ \ldots$$
$$B_y : y,\ f(y),\ f^2(y),\ \ldots$$
$$\ldots\text{usw.}$$

auftreten. Insbesondere gilt dies für die bei $a_1$beginnende Bahn $B_{a_1} = \{a_1,\ f(a_1),\ f^2(a_1),\ \ldots\}$, die (wegen ihres nichtleeren Durchschnitts mit $B_a = \{a,\ a_1,\ \ldots\}$) zu den K_j "erzeugenden" Bahnen gehört. Das bedeutet aber, dass a unter den $f(a_1),\ f^2(a_1),\ \ldots$ vorkommt und daher zu $f[B_a]$ gehört. Die übrigen Elemente von B_a sind Bilder von a und gehören daher selbstverständlich zu $f[B_a]$. ◆

8.7. Permutationen

Im weitesten Sinn versteht man unter den Permutationen einer Menge M die bijektiven Selbstabbildungen von M. Danach wären z.B. die Kongruenzabbildungen der Ebene E (bzw. $\mathbb{R}^2$) als Permutationen der Ebene anzusehen. Im Folgenden wird der Begriff "Permutation" nur in Bezug auf *endliche* Mengen benutzt.

Als Prototypen endlicher Mengen werden in diesem Abschnitt die Anfangsstücke von $\mathbb{N}$ betrachtet, d.h. die Mengen $A_n := \{1, 2, \ldots, n\}$. Es ist $A_n \neq \emptyset$ für $n \geq 1$; die Elemente von A_n heißen "Ziffern". Dies stellt keine Beschränkung der Allgemeinheit dar.

■ 8.7.1. Definition und Bezeichnungen

Eine bijektive Abbildung $p : A_n \longrightarrow A_n$ heißt Permutation vom Grad n. Für $p(k)$, $k \in A_n$, schreiben wir auch p_k und notieren die Permutation in der Zweizeilenform:

$$p = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$$

Die Identität (hier mit e bezeichnet) ist die Permutation

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Verkettungsprodukte $p \circ q$ werden ohne das Verknüpfungszeichen $\circ$ notiert: $p\,q$. Es bezeichnet $\mathcal{S}_n$ die Menge aller Permutationen vom Grad n.

■ Bemerkung

Aus diversen Lehrsätzen (dieses Kapitels 8) ergeben sich sofort (ohne nochmaligen Beweis) die folgenden Grundtatsachen über Permutationen:

Für alle $p, q, r \in \mathcal{S}_n$ gilt

(1) $p\,q \in \mathcal{S}_n$

(2) $(p\,q)\,r = p(q\,r)$

(3) $p\,e = e\,p = p$

(4) $(p\,q)^{-1} = q^{-1}\,p^{-1}$

Die im vorangehenden Abschnitt behandelte Zerlegung endlicher Selbstabbildungen stellt sich für bijektive Funktionen f stark vereinfacht dar: Ein Orbit C_j und der in ihm enthaltene Kreis K_j fallen jetzt nämlich zusammen. (Sonst müsste es ein Element u von C_j geben, dessen Nachfolger $f(u)$ in K_j liegt. Dort hat aber $f(u)$ einen von u verschiedenen Vorgänger $v \in K_j$, d.h. $f(u) = f(v)$ bei $u \neq v$, im Widerspruch zur Injektivität von f.)

Wir zeigen dies genauer in

■ 8.7.2. Proposition

f injektiv $\Longrightarrow$ $C_j = K_j$ (für alle $j = 1, 2, \ldots, m$).

■ Beweis

Sei wieder – wie im Beweis zu 8.6.3 – $K_j = B_x \bigcap B_y \bigcap \ldots$. Wir nehmen indirekt an, es gebe ein $a \in C_j \setminus K_j$. Die bei a beginnende Bahn B_a hat mit einer der B_x, B_y, … nichtleeren Durchschnitt, weshalb $K_j \subseteq B_a$ gilt. Ein beliebiges $k \in K_j$ lässt sich somit darstellen als $k = f^r(a)$ mit $r \geq 1$ ($r = 0$ ist durch die indirekte Annahme $a \notin K_j$ ausgeschlossen). Wir betrachten das (nach dem PdkZ gesicherte) kleinste $r \geq 1$, für das $f^r(a) \in K_j$. Dann gehört der "Vorgänger" $u := f^{r-1}(a)$ jedenfalls nicht zu K_j . Andererseits besitzt $f^r(a)$ wegen $f[K_j] = K_j$ (Prop. 8.6.3) einen Vorgänger $v \in K_j$, d.h. $f(u) = f(v)$ bei $u \neq v$ (im Widerspruch zur Injektivität von f). ◆

■ Bemerkung und Bezeichnungen

Aus Prop. 8.7.2. geht hervor, dass für Permutationen die Begriffe "Orbit", "Kreis" und "Bahn" zusammenfallen. Wir erhalten daher nach Prop. 8.6.2 zu gegebenem $p \in \mathcal{S}_n$ eine eindeutig bestimmte Zerlegung von $A_n = \{1, 2, \ldots, n\}$ in zyklische Bahnen $K_1, K_2, \ldots, K_m$, für die gilt: $p[K_j] = K_j$ $(1 \leq j \leq m)$. Die Abbildungen

$$z_j(k) := \begin{cases} p(k), & k \in K_j \\ k, & k \in A_n \setminus K_j \end{cases}$$

heißen dementsprechend Zyklen; offensichtlich sind sie bijektiv. Häufig notiert man sie durch Auflistung der zugehörigen Bahnelemente (Ziffern) in Klammern: $z_j = (k\ \ p(k)\ \ p^2(k) \ldots)$. Besteht K_j aus mehr als einem Element, so nennen wir z_j einen echten Zyklus (oder: zyklische Permutation), andernfalls einen trivialen Zyklus.

Wir fassen das für Permutationen grundlegende Ergebnis in einem Lehrsatz zusammen:

■ 8.7.3. Proposition (Zyklenzerlegung von Permutationen)

Jede Permutation p ist (bis auf die Reihenfolge) eindeutig als Zyklenprodukt $p = z_1 \ldots z_m$ darstellbar.

■ Bemerkung

Die Zyklenzerlegung bzw. -schreibweise von Permutationen bringt u.a. Rechenvorteile. So wird ein Zyklus einfach dadurch invertiert, dass man seine Ziffern in umgekehrter Reihenfolge aufschreibt. Bei der Berechnung der *n*-ten Iterierten (Potenz) rücken alle Ziffern um *n* Plätze weiter.

■ Beispiele

1. $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix} \in \mathcal{S}_7$ lautet in Zyklendarstellung: $p = (1\,5)\,(2\,7\,3\,6)$. Der Einerzyklus (4) muss nicht eigens notiert werden (denn: (4) = *e* (Identität)).

Aus der Zyklendarstellung gewinnt man sofort: $p^{-1} = (5\,1)\,(6\,3\,7\,2)$ sowie z.B. $p^2 = (2\,3)\,(7\,6)$ und $p^3 = (1\,5)\,(2\,6\,3\,7)$.

2. Eine Permutation p ist zyklisch, wenn genau einer der Faktoren $z_1, \ldots, z_m$ zu einer Bahn mit Länge > 1 gehört. Z. B. ist die Permutation 4. Grades $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1\,4\,2)$ in diesem Sinne zyklisch.

■ 8.7.4. Proposition

p Zyklus $\Longrightarrow$ Es gibt ein $\alpha \in \mathbb{N}$ mit $p^\alpha = e$.

■ Beweis

Wir betrachten eine beliebige Bahn B_i von p. Nach Prop. 8.6.3 gilt $i \in B_i = p[B_i]$, also $i = p(k)$ für ein $k \in B_i$. Wir stellen k dar als $k = p^r(i)$ mit ganzem $r \geq 0$. Eingesetzt liefert dies: $i = p(p^r(i)) = p^{r+1}(i)$. Wir zeigen, dass für jede Ziffer x gilt: $p^{r+1}(x) = x$. Ist nämlich $x \notin B_i$, so hat man sogar $p(x) = x$. Im anderen Fall, $x \in B_i$, gibt es ein $s \geq 0$ mit $x = p^s(i)$, und wir erhalten: $p^{r+1}(x) = p^{r+1}(p^s(i)) = p^s(p^{r+1}(i)) = p^s(i) = x$. ◆

■ 8.7.5. Proposition

p beliebige Permutation $\Longrightarrow$ Es gibt ein $\alpha \in \mathbb{N}$ mit $p^\alpha = e$.

■ Beweis

Wir stellen p (nach Prop. 8.7.3) als Zyklenprodukt $p = z_1 \ldots z_m$ dar. Prop. 8.7.4 liefert uns zu jedem dieser Zyklen z_j eine natürliche Zahl α_j mit $z_j^{\alpha_j} = e$ $(1 \leq j \leq m)$. Nun sei $\alpha \in V(\alpha_1, \ldots, \alpha_m)$ (ein beliebiges gemeinsames Vielfache der $\alpha_1, \ldots, \alpha_m$), d.h. es gibt positive ganze Zahlen $k_1, \ldots, k_m$ derart, dass $\alpha = k_j\,\alpha_j$ für $j = 1, \ldots, m$. Beachtet man die Vertauschbarkeit der Zyklen, so ergibt sich:

$$p^\alpha = (z_1 \dots z_m)^\alpha = {z_1}^\alpha \dots {z_m}^\alpha = ({z_1}^{\alpha_1})^{k_1} \dots ({z_m}^{\alpha_m})^{k_m} = e^{k_1} \dots e^{k_m} = e$$

◆

■ 8.7.6. Definition

Die kleinste natürliche Zahl α, für die $p^\alpha = e$ ist, heißt Ordnung der Permutation p, notiert: ord(p).

■ Beispiel

Die Permutation $p = (1\,5)\,(2\,7\,3\,6)$ ($\in \mathcal{S}_7$) besitzt die Ordnung 4, denn es gilt $p^4 = e$ sowie $p^\alpha \neq e$ für $1 \leq \alpha < 4$ (Begründung!)

■ 8.7.7. Proposition

Ist $p = z_1\, z_2 \dots z_m$ die Zyklenzerlegung der Permutation p und sind $l_1, l_2, \dots, l_m$ die zugehörigen Zyklenlängen (= Anzahlen von Elementen in den zugehörigen Bahnen), so gilt:
ord(p) = kgV($l_1, l_2, \dots, l_m$).

■ Beweis

1. Wir zeigen zunächst, dass für einen einzelnen Zyklus z mit zugehöriger Bahnlänge l gilt: ord(z) = l. Ist a irgendein Element der Bahn von z, so betrachten wir ihre l Elemente: $a, z(a), \dots, z^{l-1}(a)$. Es gilt: $z^l(a) = a$. Denn wäre, indirekt angenommen, $z^l(a) = z^r(a)$ für $1 \leq r < l$, mithin $z(z^{l-1}(a)) = z(z^{r-1}(a))$, so widerspräche dies der Injektivität von z (wegen $z^{l-1}(a) \neq z^{r-1}(a)$). Zwar gilt für alle $x \notin B_a$ bereits $z^1(x) = x$, doch erhalten wir auf der vollen Definitionsmenge von z allenfalls $z^l = e$ und $z^k \neq e$ für $k < l$. Es ist also l = ord(z).

2. Es gelte nun (wie in Nr. 1 für einen einzelnen Zyklus z aus l Ziffern): $z^\alpha = e$. Dann ist α durch l teilbar. Beweis: Nach Nr. 1 haben wir $z^l = e = z^\alpha$ mit ord(z) = $l \leq \alpha$. Division mit Rest liefert: $\alpha = k \cdot l + r$, wobei $0 \leq r < l$. Ist a irgendeine Ziffer aus der Bahn von z, so gilt: $a = z^\alpha(a) = z^{k\,l+r}(a) = (z^l)^k\,(z^r(a)) = e^k(z^r(a)) = z^r(a)$. Es muss also $r = 0$ sein (da sonst ein Widerspruch zu $1 \leq$ ord(z) = l vorläge).

3. Schließlich gehen wir von $p^\alpha = e$ aus. Es ergibt sich ${z_1}^\alpha\, {z_2}^\alpha \dots {z_m}^\alpha = e$ und (aufgrund der Eindeutigkeitsaussage in Prop. 8.7.3): ${z_j}^\alpha = e$ für $j = 1, 2, \dots, m$. Nach Nr. 2 ist somit $l_j \mid \alpha$ bzw. α ein gemeinsames Vielfaches der Zyklenlängen $l_1, l_2, \dots, l_m$. Daher erweist sich das kleinste $\alpha \geq 1$ mit $p^\alpha = e$ als das kgV der $l_1, l_2, \dots, l_m$. ◆

9. Kombinatorische Grundbegriffe

Die *Kombinatorik* (genauer: die sog. *abzählende* Kombinatorik) beschäftigt sich damit, Objekte bestimmter Beschaffenheit zu zählen. Das läuft darauf hinaus, die Anzahl $|A|$ von endlichen Mengen A zu ermitteln, wobei es sich bei diesen $A's$ um Teilmengen (einer Grundmenge M) handelt, die durch bestimmte strukturelle Eigenschaften gekennzeichnet sind.

Alle im Folgenden auftretenden Mengen $A, B, C, \ldots, M, \ldots$ werden als *endlich* vorausgesetzt.

9.1. Elementare Abzählregeln

■ 9.1.1. Summenregel

Für disjunkte Mengen A, B gilt:

$|A \cup B| = |A| + |B|$

■ 9.1.2. Produktregel

Für beliebige Mengen A, B gilt:

$|A \times B| = |A| \cdot |B|$

■ 9.1.3. Gleichheitsregel (= Zuordnungsregel)

Für beliebige Mengen A, B gilt:

$|A| = |B| \iff$ Es gibt eine bijektive Abbildung $f : A \longrightarrow B$.

■ Bemerkung

An dieser Stelle (wie auch in Lehrbüchern der Kombinatorik üblich) werden die elementaren Abzählregeln als unmittelbar einleuchtende Tatsachen über Anzahlen endlicher Mengen zu Grunde gelegt. Damit soll keineswegs die Notwendigkeit heruntergespielt werden, sie als mathematische Behauptungen, die sie nun einmal sind, auch streng zu beweisen. Wir wollen dennoch darauf verzichten. Die Beweise erfordern nämlich einen Rahmen, der hier nicht zur Verfügung steht; insbesondere müsste es dieser Rahmen gestatten, den Begriff der endlichen Menge genauer zu fassen (wozu es mehrere Alternativen gibt) sowie den Begriff der Anzahl präzise einzuführen, um dann die obigen Regeln, z.B. durch Induktion, zu begründen. Wer sich für diesen Fragenkreis interessiert, mag das Buch von W. Felscher zu Rate ziehen: *Naive Mengen und abstrakte Zahlen I*, B.I.-Wiss.Verlag: Mannheim 1978.

■ 9.1.4. Definition und Bezeichnungen

Sei X eine Menge von n Elementen, $n \geq 0$, $k \geq 0$. Eine k-gliedrige Folge $x_1, x_2, \ldots, x_k$ von lauter verschiedenen Elementen aus X heißt k-Permutation ohne Wiederholung (o. Wdh.) von X. Wenn sich die Elemente wiederholen können, spricht man von einer k-Permutation mit Wiederholung (m. Wdh.) von X. Mit $P(n, k)$ bzw. $P^*(n, k)$ werden die zugehörigen Anzahlen bezeichnet.

■ 9.1.5. Proposition

(1) $P(n, k) = n(n-1)\cdot\ldots\cdot(n-k+1)$ $\quad (0 \leq k \leq n)$

(2) $P^*(n, k) = n^k$ $\quad (n \geq 1, k \geq 0)$

■ Beweis

Zu (1): Das Element x_1 kann auf n Weisen gewählt werden, danach x_2 noch auf $n-1$Weisen, usw. Die Behauptung ergibt sich mit Hilfe der Produktregel. Zu (2): Für jedes der k Elemente gibt es n Wahlmöglichkeiten. ◆

■ Bemerkungen

1. Man beachte: (2) gilt auch dann, wenn $k > n$ ist.

2. In (1) ist der Sonderfall $k = n$ von Interesse: Eine n-Permutation (von n Elementen) kann als *Umordnung* von n Dingen gedeutet werden, d.h. als gewöhnliche Permutation $\in \mathcal{S}_n$. Ihre Anzahl $P(n, n)$ notiert man auch als $n!$ (lies: "n Fakultät"; vgl. auch Abschnitt 1.6).

Die Folge der Fakultäten wächst rasch:

1
1
2
6
24
120
720
5040
40320
362880
3628800
39916800
479001600
6227020800
87178291200
1307674368000
20922789888000
355687428096000
6402373705728000
121645100408832000
2432902008176640000

3. Nach 9.1 .5, (1) gilt : $P(n, k) = \frac{n!}{(n-k)!}$.

4. Es ist 0! = 1, ferner $P^*(0, 0) = 1$.

■ 9.1.6. Proposition

Sei X eine Menge von n Elementen, $n \geq 1$, $\mathcal{P}_0(X)$ die Menge der geradzahligen, $\mathcal{P}_1(X)$ die Menge der ungeradzahligen Teilmengen von X. Dann gilt: $|\mathcal{P}_0(X)| = |\mathcal{P}_1(X)|$.

■ Beweis

Für beliebiges $a \in X$ wird $f : \mathcal{P}_0(X) \to \mathcal{P}_1(X)$ definiert durch $f(M) = M + \{a\}$ für alle $M \in \mathcal{P}_0(X)$. Man zeigt: f ist bijektiv. Dann gilt nach der Gleichheitsregel: $|\mathcal{P}_0(X)| = |\mathcal{P}_1(X)|$. ◆

■ Bemerkung

Aus Prop. 3.2.3 ist bereits bekannt: $|\mathcal{P}(X)| = 2^n = 2^{|X|}$

9.2. Permutationen mit vorgeschriebenen Wiederholungen

■ 9.2.1. Definition

Sei $X = \{x_1, x_2, ..., x_n\}$. Eine k-Permutation von X mit vorgeschriebenen Wiederholungen ist eine Folge von Elementen aus X, in der x_i genau r_i-mal auftritt, wobei $r_1, r_2, \ldots, r_n \geq 0$ und $r_1 + r_2 + \ldots + r_n = k$. Die zugehörige Anzahl werde mit $P(r_1, \ldots, r_n \mid k)$ bezeichnet.

■ 9.2.2. Proposition

$$P(r_1, \ldots, r_n \mid k) = \frac{k!}{r_1! \cdot \ldots \cdot r_n!}$$

■ Beweis

Beweisskizze (anhand eines Beispiels):

Aus den $n = 5$ Buchstaben **A B E L N** sollen 9-Permutationen mit vorgeschriebenen Wiederholungshäufigkeiten 3, 1, 1, 2, 2 gebildet werden. Beispiel einer solchen Permutation ist das Wort **ANNABELLA**.

Insgesamt gibt es $9! = 362880$ Anordnungen verschiedener (hier: farblich unterscheidbar gemachter) Elemente **ANNABELLA**. Werden nun die $3 (= r_1)$ Varianten **A A A** identifiziert (d.h. hinsichtlich ihrer Farbe nicht unterschieden), so fallen alle diejenigen Permutationen (zu einer einzigen) zusammen, die sich nur in der Anordnung der **A A A** unterscheiden. Dies verkleinert die Menge aller Permutationen auf ein 6-tel ihres Umfangs (6 = 3!). Verfährt man in analoger Weise mit den Buchstaben **L** und **N**, so bleiben am Ende $\frac{9!}{3!\,2!\,2!} = 15120$ Permutationen übrig. ◆

■ Bemerkung

Die Permutationen von n Elementen o. Wdh. sind in dem Spezialfall $r_1 = \ldots = r_n = 1$, $k = n$ enthalten. Es gilt: $P(1, \ldots, 1 \mid n) = n!$.

9.3. Kombinationen

Kombinationen sind Folgen von Elementen, bei denen es auf die Reihenfolge nicht ankommt. Sie lassen sich am *Urnenmodell* veranschaulichen: Beim Zahlenlotto "6 aus 49" zieht man 6 Kugeln aus einer Urne mit 49 nummerierten Kugeln. Eine gezogene Kugel wird nicht wieder zurückgelegt, die Ziehung enthält demnach keine Wiederholungen. Da es auf die Reihenfolge nicht ankommt, werden am Ende die 6 Kugeln in der aufsteigenden Folge ihrer Nummern angegeben. Dies ist ein Muster für eine *Kombination ohne Wiederholung*. Würde man die Kugeln wieder zurücklegen, so wäre das Ergebnis einer Ziehung (im allgemeinen) eine *Kombination mit Wiederholung*.

Sei $X = \{x_1, \ldots, x_n\}$ eine beliebige endliche Menge: $|X| = n \geq 0$.

■ 9.3.1. Definition

Eine Folge $x_{j_1}, \ldots, x_{j_k}$ von Elementen aus X heißt k-Kombination (von n Elementen) o. Wdh. bzw. m. Wdh., wenn $j_1 < \ldots < j_k$ bzw. $j_1 \leq \ldots \leq j_k$ gilt. Die zugehörigen Anzahlen werden mit $C(n, k)$ bzw. $C^*(n, k)$ bezeichnet. Traditionell schreibt man für $C(n, k)$ auch $\binom{n}{k}$ (lies: "n über k").

■ Beispiel

$X = \{1, 2, 3\}$. Es gibt sechs 2-Kombinationen m. Wdh.: 11, 12, 22, 13, 33, 23.

■ 9.3.2. Proposition

(1) $$C(n, k) = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}, \text{ wobei } 0 \leq k \leq n$$

(2) $$C^*(n, k) = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k!\,(n-1)!}, \text{ wobei } n \geq 1,\ k \geq 0.$$

■ Beweis

Man zählt Kombinationen zweckmäßig dadurch ab, dass man sie als Permutationen mit vorgeschriebenen Wiederholungen darstellt und die Gleichheitsregel anwendet.

Zu (1). Ist $n = 0$, so auch $k = 0$. In diesem Fall gibt es genau eine 0-Kombination (leere Folge), d.h. $C(0, 0) = 1 = \binom{0}{0}$. Sei nun $n \geq 1$ angenommen. Eine k-Kombination $x_{j_1}, \ldots, x_{j_k}$ o. Wdh. lässt sich eindeutig als 0-1-Folge $f_1 \ldots f_n$ codieren: Man setzt dazu $f_i = 1$, falls i eines der $j_1, \ldots, j_k$ ist, andernfalls $f_i = 0$. Jede so definierte Folge enthält genau k Einsen und $n - k$ Nullen. Nach der Gleichheitregel und der Bemerkung zu 9.2.2 ergibt sich $C(n, k) = P(k, n-k \mid n)$ und somit die Behauptung.

Zu (2). Für $k = 0$ gibt es genau eine 0-Kombination mit Wiederholung (leere Folge), und es gilt $C^*(n, 0) = 1 = \binom{n-1}{0}$. Sei nun $k \geq 1$ angenommen. Eine k-Kombination mit Wiederholung wird in eindeutiger Weise als 0-1-Folge der Länge $n + k - 1$ codiert: Für jedes Vorkommen eines Elements wird eine 1 hingeschrieben; zwischen die 1-Blöcke (die auch leer sein können) wird eine 0 geschrieben. Zum Beispiel bezeichnet (im Fall $n = 7,\ k = 6$) das Wort 001110100110 die folgende 6-Kombination von 7 Elementen mit Wiederholung: $a_3\, a_3\, a_3\, a_4\, a_6\, a_6$. Umgekehrt wird z.B. (im Fall $n = 7,\ k = 4$) $a_2\, a_4\, a_4\, a_7$ als 0100110001 codiert. Allgemein entsteht auf diese Weise eine Folge aus $n + k - 1$ Elementen, darunter k Einsen und $n - 1$ Nullen. Die Gleichheitsregel und Prop. 9.2.2 liefern dann $C^*(n, k) = P(k, n-1 \mid n+k-1)$ und damit die Behauptung. ◆

9.4. Auswertung binomischer Terme

Im Folgenden behandeln wir die Auswertung des allgemeinen binomischen Terms $(a + b)^n$ (n eine natürliche Zahl) und die grundlegenden Eigenschaften der Binomialzahlen $\binom{n}{k}$, $k = 0, 1, 2, \ldots, n$, die in diesem Zusammenhang auftreten.

Für $n = 2$ und $n = 3$ erhält man nach kurzer Rechnung (Ausmultiplizieren!) die aus dem Schulunterricht bekannten Formeln:

$$(a + b)^2 = a^2 + 2\,a\,b + b^2$$
$$(a + b)^3 = a^3 + 3\,a^2\,b + 3\,a\,b^2 + b^3$$

Allgemein: Aus $(a + b)^n$ entstehen durch Ausmultiplizieren lauter Summanden in der Form eines Produkts aus k Faktoren a und $n - k$ Faktoren b, wobei $0 \le k \le n$. Es bezeichne $B(n, k)$ die Anzahl, in der das Produkt $a^k\,b^{n-k}$ auftritt. Die $B(n, k)$ heißen Binomialkoeffizienten (auch: Binomialzahlen).

■ 9.4.1. Proposition (Binomialsatz)

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

■ Beweis

Nach obiger Definition der Binomialkoeffizienten ist $(a + b)^n = \sum_{k=0}^{n} B(n, k)\,a^k\,b^{n-k}$. Wir zeigen $B(n, k) = C(n, k)$. Dazu betrachten wir $(a + b)^n = (a + b)\,(a + b)\,...\,(a + b)$ und bemerken: Das Produkt $a^k\,b^{n-k}$ kommt dadurch zustande, dass aus k der Klammersummen $(a + b)$ der Faktor a (und dann zwangsläufig aus den übrigen $n - k$ der Faktor b) ausgewählt wird. Auf die Reihenfolge kommt es dabei nicht an; es handelt sich also um k-Kombinationen aus n Elementen o. Wdh. Somit ist $B(n, k) = C(n, k)$, und nach Prop. 9.3.2, (1) folgt die Behauptung. ◆

■ 9.4.2. Bemerkung

Eine speziellere Fassung der Binomialformel (mit $a = x$, $b = 1$) lautet:

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

Diese Formel ist nicht wirklich schwächer. Aus ihr lässt sich die allgemeinere Fassung 9.4.1 wieder zurückgewinnen, indem man $x = \frac{a}{b}$ setzt und beide Seiten der Gleichung mit b^n multipliziert.

■ Pascalsches Dreieck

Die Binomialzahlen kommen in vielen Gebieten der Mathematik vor und spielen dort eine wichtige Rolle (z.B. in Kombinatorik, Analysis, Wahrscheinlichkeitsrechnung). Man hat sie schon früh entdeckt, berechnet und in Gestalt des (heute so genannten) *Pascalschen Dreiecks* tabelliert (das aber schon in der altchinesischen Mathematik als "Arithmetisches Dreieck" bekannt war).

In der n-ten Zeile und k-ten Spalte des Pascalschen Dreiecks steht die Zahl $B(n, k) = \binom{n}{k}$, $0 \le k \le n$:

1								
1	**1**							
1	**2**	**1**						
1	**3**	**3**	**1**					
1	**4**	**6**	**4**	**1**				
1	**5**	**10**	**10**	**5**	**1**			
1	**6**	**15**	**20**	**15**	**6**	**1**		
1	**7**	**21**	**35**	**35**	**21**	**7**	**1**	
1	**8**	**28**	**56**	**70**	**56**	**28**	**8**	**1**

Man beobachtet: Der Eintrag in einer Zeile und Spalte – etwa die Zahl 35 in Zeile 7, Spalte 3 – ergibt sich als Summe zweier darüber stehender Werte wie folgt:

$$35 = \binom{7}{3} = \binom{6}{2} + \binom{6}{3} = 20 + 15$$

Diese (wichtigste) und weitere Eigenschaften der Binomialzahlen werden im folgenden Abschnitt behandelt.

9.5. Eigenschaften der Binomialkoeffizienten

■ 9.5.1. Proposition

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

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad \text{für } 1 \le k < n$$

■ 9.5.2. Proposition

$$\binom{n}{k} = \binom{n}{n-k} \quad \text{für } 0 \le k \le n$$

■ Bemerkungen zu den Beweisen

Die Grundeigenschaften der Binomialzahlen 9.5.1 (rekursive Summenformel) und 9.5.2 (Symmetrie) lassen sich direkt nachrechnen sowie auf einfache Weise kombinatorisch deuten (und damit begründen), z.B. 9.5.2: Indem man k Elemente aus n auswählt, legt man auch die übrigen $n - k$ nicht ausgewählten Elemente fest.

■ 9.5.3. Proposition

(1) $$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$$

(2) $$\sum_{k=0}^{n} \binom{n}{k} (-1)^k = \binom{n}{0} - \binom{n}{1} + \ldots + \binom{n}{n} (-1)^n = 0$$

■ Beweis

(1) erhält man aus 9.4.2 für $x = 1$, (2) ebenso für $x = -1$. ◆

Kombinatorische Beweisvarianten. Zu (1): Die Anzahlen aller k-elementigen Teilmengen einer Menge von n Elementen ergeben aufsummiert die Anzahl aller Teilmengen (nämlich: 2^n). Zu (2): Die Anzahlen der Teilmengen ungerader Anzahl werden von den Anzahlen der Teilmengen gerader Anzahl subtrahiert. Dass dabei 0 herauskommt, deckt sich mit der Behauptung von Prop. 9.1.6. ◆

■ 9.5.4. Proposition (Faltungsformel)

$$\sum_{k=0}^{n} \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n}$$

■ Beweis

Einfacher als ein rechnerischer ist ein kombinatorischer Beweis: Wir wählen aus insgesamt r roten und s schwarzen Kugeln n aus, indem wir k rote (und zwangsläufig $n - k$ schwarze) Kugeln in allen möglichen Fällen $k = 0, 1, \ldots, n$ festlegen. Nach der Produktregel gibt es dann $C(r, k) \cdot C(s, n - k)$ Paarungen von roten mit schwarzen Auswahlen. Die Summenregel (über alle Fälle für k) liefert dann die behauptete Gleichung. ◆

Es gibt viele weitere interessante Beziehungen für Binomialzahlen, z.B. die folgenden (hier ohne Beweis mitgeteilten) Gleichungen:

■ 9.5.5. Proposition

(1) $$1\binom{n}{1} + 2\binom{n}{2} + \ldots + n\binom{n}{n} = n\,2^{n-1}$$

(2) $$1^2\binom{n}{1} + 2^2\binom{n}{2} + \ldots + n^2\binom{n}{n} = n(n+1)\,2^{n-2}$$

9.6. Der Multinomialsatz

Der Multinomialsatz ist eine Verallgemeinerung des Binomialsatzes auf Ausdrücke der Form $(a + b + c + ...)^n$. Zum Beispiel ist:

$$(a+b+c)^5 = a^5 + 5\,a^4\,b + 10\,a^3\,b^2 + 10\,a^2\,b^3 + 5\,a\,b^4 + b^5 + 5\,a^4\,c + 20\,a^3\,b\,c + 30\,a^2\,b^2\,c + 20\,a\,b^3\,c + 5\,b^4\,c + 10\,a^3\,c^2 + 30\,a^2\,b\,c^2 + 30\,a\,b^2\,c^2 + 10\,b^3\,c^2 + 10\,a^2\,c^3 + 20\,a\,b\,c^3 + 10\,b^2\,c^3 + 5\,a\,c^4 + 5\,b\,c^4 + c^5$$

Man macht zwei Beobachtungen:

1. Die Koeffizienten der aus *a, b, c* gebildeten Produkte $a^{r_1}\,b^{r_2}\,c^{r_3}$ sind offenbar die Anzahlen der 5-Permutationen mit vorgeschriebenen Wiederholungen: $P(r_1, r_2, r_3 \mid 5)$, wobei $r_1 + r_2 + r_3 = 5$.

2. Die Anzahl der (in der zusammengefassten Form) auftretenden Summanden ist $C^*(3, 5) = 21$ (5-Kombinationen von 3 Elementen m. Wdh.). Auf die Reihenfolge der Faktoren in den Produkten kommt es nicht an.

Diese Beobachtungen lassen sich leicht verallgemeinern (und völlig analog den bei binomischen Ausdrücken gefundenen Tatsachen begründen).

■ 9.6.1. Proposition (Multinomialsatz)

$$(a_1 + a_2 + \ldots + a_s)^n = \sum_{j_1+j_2+\ldots+j_s=n} \frac{n!}{j_1!\,j_2!\ldots j_s!}\,{a_1}^{j_1}\,{a_2}^{j_2}\ldots{a_s}^{j_s}$$

■ Bemerkungen

1. Die Summierung ist über alle Wertefolgen $j_1, j_2, \ldots, j_s$ vorzunehmen, für die $j_1 + j_2 + \ldots + j_s = n$ gilt. Im obigen Beispiel sind das die Exponenten-Tripel: (5, 0, 0), (4, 1, 0), (3, 2, 0) usf.

2. Für $s = 2$ erhält man aus der Multinomialformel als Spezialfall die Binomialformel (im Detail nachvollziehen!).

10. Algebraische Strukturen

Die gewöhnlichen mit Zahlen ausgeführten Rechenoperationen (Verknüpfungen) + und · weisen eine Reihe gemeinsamer Eigenschaften auf. Dazu gehört z.B. das Kommutativgesetz ($a + b = b + a$ und $a \cdot b = b \cdot a$) und die analoge Rolle von 0 und 1 in den Gleichungen $a + 0 = a$ bzw. $a \cdot 1 = a$. Auch in anderen Bereichen, etwa in der Mengenalgebra, stößt man auf verwandte Rechengesetze. Die *Algebra* untersucht diese Verhältnisse allgemein und abstrahiert dabei von der besonderen Beschaffenheit der Objekte, mit denen gerechnet wird. Dadurch lassen sich einfachere Begriffe bilden und deren Beziehungen untereinander rationeller (im Sinne einer Denkökonomie) untersuchen. Algebraische Strukturen (Verknüpfungsgebilde) sind Mengen, auf denen Operationen (Verknüpfungen) gegeben sind.

10.1. Verknüpfungsgebilde

Der Begriff "Verknüpfung" stellt eine Verallgemeinerung der gewöhnlichen Rechenoperationen für Zahlen dar. Naheliegende Beispiele für Verknüpfungen sind die von den "Grundrechenarten" her geläufigen Operationen "Addition", "Subtraktion", "Multiplikation" und "Division".

Zum Beispiel wird die Addition zweier ganzer Zahlen x, y aufgefasst als eine Abbildung $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, die dem geordneten Paar (x, y) als Bild die Summe $x + y$ zuordnet : $+(x, y) := x + y$. (Die streng eingehaltene Abbildungsnotation ist, zumindest für zweistellige Verknüpfungen, ungewohnt und unüblich. Anstatt den Abbildungsnamen *vor* das Urbild zu schreiben, wird die herkömmliche Schreibweise beibehalten und das Verknüpfungszeichen *zwischen* die Komponenten des Urbild-Paars geschrieben.)

■ 10.1.1. Definition

Seien A und B nichtleere Mengen. Abbildungen vom Typ $A^2 \longrightarrow B$ heißen (zweistellige oder binäre) Verknüpfungen oder Operationen auf A mit Werten in B. Im Falle $B = A$ heißt $\perp : A^2 \longrightarrow A$ Verknüpfung in A. Es bezeichnet $x \perp y$ den Funktionswert von $(x, y) \in A^2$ unter $\perp$.

Zum Beispiel ist die Subtraktion natürlicher Zahlen eine Verknüpfung auf $\mathbb{N}$ mit Werten in $\mathbb{Z}$, jedoch keine Verknüpfung *in* $\mathbb{N}$. Bei der Addition natürlicher Zahlen können wir hingegen die kleinere Zielmenge $\mathbb{N}$ wählen, denn es gilt $x + y \in \mathbb{N}$ für alle $x, y \in \mathbb{N}$, d.h. + ist eine Verknüpfung *in* $\mathbb{N}$.

■ Bezeichnungen

Ist $\perp$ eine Verknüpfung in A, so wird das geordnete Paar $(A, \perp)$ als Verknüpfungsgebilde bezeichnet. A heißt in diesem Zusammenhang Träger(menge) des Verknüpfungsgebildes. Ein anderer Ausdruck für Verknüpfungsgebilde ist algebraische Struktur.

■ Beispiele algebraischer Strukturen

$(\mathbb{Q}, +)$	Addition rationaler Zahlen
$(\mathbb{R}, \cdot)$	Multiplikation reeller Zahlen
$(\mathbb{Q} \setminus \{0\}, \div)$	Division rationaler Zahlen $\neq 0$
$(\mathbb{Z}, -)$	Subtraktion ganzer Zahlen
$(\mathbb{Z}_m, \oplus)$	Restklassenaddition modulo m
$(\mathcal{S}_n, \circ)$	Verkettung von Permutationen
$(\mathcal{P}(M), +)$	Boolesche Summe von Mengen

Man mache sich bei jedem dieser Beispiele klar, weshalb eine Verknüpfung in der jeweils angegebenen Trägermenge vorliegt.

Keine Verknüpfungsgebilde entstehen durch …

$\mathbb{N}$ mit der Subtraktion,

$\mathbb{Q}$ mit der Division,

$\mathbb{Z}$ mit dem arithmetischen Mittel $\frac{x+y}{2}$ zweier ganzer Zahlen x, y,

die Menge aller Spiegelungen (einer Ebene) mit der Verkettung $\circ$.

Die Verknüpfungsgebilde $(\mathcal{S}_n, \circ)$ und $(\mathcal{P}(M), +)$ zeigen, dass man auch mit Abbildungen bzw. mit Mengen in ähnlichem Sinne wie mit gewöhnlichen Zahlen rechnen kann.

Von besonderer Bedeutung sind in dieser Hinsicht die Restklassenmengen $\mathbb{Z}_m$, $m \geq 2$, für die wir in Abschnitt 7.3 eine Addition $\oplus$ und eine Multiplikation $\odot$ eingeführt haben.

In einem Verknüpfungsgebilde $(A, \perp)$ tritt gelegentlich die Frage auf, ob sich die Verknüpfung $\perp$ auf eine bestimmte Teilmenge $M \subset A$ einschränken lässt. Man betrachte etwa $(\mathbb{Z}, +)$ und die Teilmenge $2\mathbb{Z}$ der geraden ganzen Zahlen. Offensichtlich ist $x + y \in 2\mathbb{Z}$ für alle $x, y \in 2\mathbb{Z}$; somit lässt sich $(2\mathbb{Z}, +)$ als ein abgeschlossenes Teilgebilde von $(\mathbb{Z}, +)$ auffassen. Das gibt Anlass zu folgender

■ 10.1.2. Definition

Sei $(A, \perp)$ ein Verknüpfungsgebilde. Eine nichtleere Teilmenge M von A heißt abgeschlossen unter $\perp$ (oder abgeschlossen in $(A, \perp)$), wenn gilt: $x \perp y \in M$ für alle $x, y \in M$. In diesem Fall heißt $(M, \perp)$ auch Teilgebilde (manchmal auch: Untergebilde) von $(A, \perp)$.

■ Beispiele

Die Menge der geraden Zahlen ist abgeschlossen unter +, nicht jedoch die Menge der ungeraden Zahlen. Weitere Beispiele: $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}^+$ sind sämtlich in $(\mathbb{R}, \cdot)$ abgeschlossen.

10.2. Kommutativität

Beim Rechnen mit gewöhnlichen Zahlen benutzt man stillschweigend, dass sich in einer Summe die Summanden und dass sich in einem Produkt die Faktoren vertauschen lassen; z.B.:

$$147 + 36 + 113 = 147 + 113 + 36 = 260 + 36 = 296$$

■ 10.2.1. Definition

Eine Verknüpfung $\perp$ in einer nichtleeren Menge A heißt kommutativ, wenn für alle $x, y \in A$ gilt: $x \perp y = y \perp x$. In diesem Fall heißt auch das zugehörige Verknüpfungsgebilde $(A, \perp)$ kommutativ.

■ Bemerkung

Die Addition + und die Multiplikation · (in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) sind kommutativ, nicht hingegen Subtraktion und Division. Ferner gilt: Addition und Multiplikation von Restklassen sind kommutative Verknüpfungen (vgl. Proposition 7.3.3). Die Verkettung von Abbildungen ist nicht kommutativ.

10.3. Assoziativität

Das Rechenbeispiel aus 10.2 benutzt außer der Kommutativität von + noch eine weitere Eigenschaft der Addition, die aus folgender Schreibweise ersichtlich wird:

$$147 + (36 + 113) = (147 + 36) + 113 = \ ...$$

■ Bemerkung

Die Schreibweise mit Klammern ist die genauere, weil ja durch + zwei (und nicht etwa drei oder mehr) Zahlen verknüpft werden. Im Beispiel bedeutet das praktisch, dass zuerst die Klammer (36 + 113) ausgewertet und dann die Summe 147 + (...) gebildet wird.

Die Umformung macht Gebrauch von der Tatsache, dass "zuerst 113 + 36 rechnen und das Ergebnis zu 147 addieren" dasselbe Ergebnis liefert wie "zuerst 147 + 113 rechnen und zu dem Ergebnis 36 addieren". Das allgemeine Rechengesetz, das diese Umformung zum Ausdruck bringt, heißt Assoziativgesetz der Addition. Auch für die Multiplikation gilt diese Rechenregel (vgl. 1.2.1).

■ 10.3.1. Definition

Eine Verknüpfung $\perp$ in einer nichtleeren Menge A heißt assoziativ, wenn für alle $x, y, z \in A$ gilt:
$x \perp (y \perp z) = (x \perp y) \perp z$. In diesem Fall nennt man das Verknüpfungsgebilde $(A, \perp)$ eine Halbgruppe.

Die Assoziativität ist eine *fundamentale* Eigenschaft. Praktisch alle wichtigen Verknüpfungen, die in der Algebra untersucht werden, sind assoziativ, und solche, die es nicht sind, sind nur in Ausnahmefällen interessant.

■ Beispiele

Die folgenden Verknüpfungsgebilde sind Halbgruppen:

$(\mathbb{Q}, +), (\mathbb{R}, \cdot), (\mathcal{S}_n, \circ), (\mathcal{P}(M), +), (\mathbb{Z}_m, \oplus), (\mathbb{Z}_m, \odot)$

■ Bemerkung

Ist Γ irgendeine Menge von Selbstabbildungen einer Menge A, die unter $\circ$ abgeschlossen ist (d.h. mit $f, g \in \Gamma$ ist stets auch $f \circ g \in \Gamma$), dann ist $(\Gamma, \circ)$ eine Halbgruppe. (Dazu ist lediglich zu beachten, dass die Verkettung $\circ$ in der Gesamtheit aller Selbstabbildungen von A assoziativ ist und die Gleichheit $(f \circ g) \circ h = f \circ (g \circ h)$ wegen der Abgeschlossenheit schon in Γ besteht.)

10.4. Neutrales Element (Einselement)

Die Zahl 1 hat bei der Multiplikation natürlicher, ganzer, rationaler und reeller Zahlen die Eigenschaft, dass für jede Zahl x gilt:

$$1 \cdot x = x \cdot 1 = x$$

Wegen dieser Eigenschaft heißt 1 neutrales Element der Multiplikation. Auch die Addition besitzt (in der Zahl 0) ein solches neutrales Element:

$$0 + x = x + 0 = x$$

■ 10.4.1. Definition

Sei $(A, \perp)$ ein Verknüpfungsgebilde. Ein Element $e \in A$ heißt neutrales Element (oder: Einselement) von $(A, \perp)$, wenn für alle $x \in A$ gilt: $e \perp x = x \perp e = x$.

■ Bemerkung

Bei einer kommutativen Verknüpfung $\perp$ genügt es, $x \perp e = x$ (für alle $x \in A$) zu fordern.

Bekanntlich existiert außer der Zahl 1 kein weiteres neutrales Element der gewöhnlichen Multiplikation. In der Tat ist allgemein das neutrale Element eines Verknüpfungsgebildes eindeutig bestimmt.

■ 10.4.2. Proposition

In einem Verknüpfungsgebilde $(A, \perp)$ gibt es höchstens ein neutrales Element.

■ Beweis

Seien e_1 und e_2 neutrale Elemente von $(A, \perp)$. Dann gelten die Gleichungen:

(1) $e_1 \perp x = x$

(2) $x \perp e_2 = x$

für beliebiges $x \in A$. Setzt man $x = e_2$ in (1) und $x = e_1$ in (2), so ergibt sich $e_1 \perp e_2 = e_2$ und $e_1 \perp e_2 = e_1$, mithin $e_1 = e_2$. ◆

■ Beispiele

Verknüpfungsgebilde	*neutrales Element (Einselement)*
$(\mathbb{Z}_m, \oplus)$	0 (als Restklasse)
$(\mathbb{Z}_m, \odot)$	1 (als Restklasse)
$(\mathcal{S}_n, \circ)$	e (identische Permutation)
$(\mathcal{P}(M), +)$	$\emptyset$

Die entsprechenden Gleichungen sollten für jedes dieser Beispiele übungshalber nachvollzogen werden.

■ Bemerkung und Beispiel

Es gibt Verknüpfungsgebilde, die kein neutrales Element besitzen.

In $\mathbb{R}$ werde $\perp$ definiert durch $x \perp y := \text{Max}\{x, y\}$. Diese Verknüpfung hat kein Einselement, denn für ein solches e müsste gelten: $\text{Max}\{x, e\} = x \perp e = x$ für alle $x \in \mathbb{R}$. Für $x = e - 1$ führt dies zu einem Widerspruch!

10.5. Invertierbarkeit, Begriff der Gruppe

Hat eine Verknüpfung $\perp$ in einer Menge A ein Einselement e, so ist die Frage sinnvoll, ob zu $a \in A$ ein Element $a' \in A$ existiert, sodass $a \perp a' = e$ und $a' \perp a = e$. Zum Beispiel gibt es zu jeder rationalen Zahl $r \neq 0$ ein $r' \in \mathbb{Q}$ mit der Eigenschaft: $r \cdot r' = r' \cdot r = 1$ (nämlich $r' = \frac{1}{r}$). Diesem Beispiel folgend spricht man von zueinander inversen Elementen bzw. von der Invertierbarkeit eines Elements.

■ 10.5.1. Definition

Sei $(A, \perp)$ ein Verknüpfungsgebilde mit Einselement e. Ein Element $a \in A$ heißt invertierbar, wenn ein $a' \in A$ existiert mit $a \perp a' = a' \perp a = e$. In diesem Fall heißt a' invers zu a (oder inverses Element von a).

■ Bemerkung

Ist a' invers zu a, dann ist auch a invers zu a' (unmittelbar aus der definierenden Gleichung ersichtlich). Das neutrale Element e ist stets invertierbar, denn es gilt: $e \perp e = e$.

■ Beispiele

1. Alle Elemente von $\mathbb{Q} \setminus \{0\}$ besitzen ein multiplikatives Inverses, d.h. sind invertierbar bzgl. der gewöhnlichen Multiplikation rationaler Zahlen. Das Inverse ist jeweils eindeutig bestimmt.

2. Alle ganzen Zahlen sind invertierbar in $(\mathbb{Z}, +)$; das Inverse zu $a \in \mathbb{Z}$ ist eindeutig bestimmt (nämlich als $-a$).

3. Alle Permutationen in $\mathcal{S}_n$ sind invertierbar (bzgl. der Verkettung $\circ$), denn zu $p \in \mathcal{S}_n$ gilt: $p \circ p^{-1} = p^{-1} \circ p = e$. Das Inverse p^{-1} ist die Umkehrabbildung von p (und nach dem Satz von der Umkehrabbildung, Prop. 8.4.1, eindeutig bestimmt).

4. Alle Teilmengen X von M sind in $(\mathcal{P}(M), +)$ zu sich selbst invers, denn es gilt: $X + X = \emptyset$.

In den genannten Beispielen sind jeweils die Inversen eindeutig bestimmt. Das ist aber nicht notwendig immer so; z.B. hat das durch $x \perp y := x + y - 2\, x^2\, y^2$ (für reelle x, y) definierte Verknüpfungsgebilde $(\mathbb{R}, \perp)$ ein neutrales Element (nämlich 0), es gibt aber nicht-invertierbare Elemente (etwa -1) und Elemente mit mehr als einem Inversen (etwa 2). Der Grund dafür liegt darin, dass die betreffende Verknüpfung *nicht assoziativ* ist. Für assoziative Verknüpfungen lässt sich hingegen zeigen, dass die Inversenbildung eindeutig ist (sofern sie möglich ist).

■ 10.5.2. Proposition

Sei $(A, \perp)$ ein Halbgruppe mit Einselement. Dann besitzt ein Element von A höchstens ein Inverses.

■ Beweis

Sei e das (eindeutig bestimmte) Einselement und a irgendein invertierbares Element von A mit Inversen a' und a''. Es ist zu zeigen: $a' = a''$. Nach Definition gilt: $a \perp a' = e$ und $a'' \perp a = e$. Daraus folgt mit dem Assoziativgesetz:

$$a' = e \perp a' = (a'' \perp a) \perp a' = a'' \perp (a \perp a') = a'' \perp e = a''$$

◆

■ Bezeichnungen

1. Das zu einem invertierbaren Element a aus A eindeutig bestimmte Inverse wird mit a^{-1} bezeichnet.

2. Die Menge der in $(A, \perp)$ invertierbaren Elemente werde mit $\mathrm{Inv}(A, \perp)$ bezeichnet.

Man mache sich damit die folgenden Sachverhalte klar:

$$\mathrm{Inv}(\mathbb{Z}, +) = \mathbb{Z} \qquad \mathrm{Inv}(\mathbb{Q}, \cdot) = \mathbb{Q} \setminus \{0\} \qquad \mathrm{Inv}(\mathcal{S}_n, \circ) = \mathcal{S}_n$$

$$\mathrm{Inv}(\mathbb{Z}_m, \oplus) = \mathbb{Z}_m \qquad \mathrm{Inv}(\mathbb{Z}_4, \odot) = \{1, 3\} \qquad \mathrm{Inv}(\mathbb{N}_0, +) = \{0\}$$

■ 10.5.3. Bemerkung zu Restklassen, Definition

Nach Prop. 7.3.5 sind die in $(\mathbb{Z}_m, \odot)$, $m \geq 2$, invertierbaren Restklassen genau die zu m teilerfremden (positiven) $a \in \mathbb{Z}_m$. Ihre Anzahl wird üblicherweise mit $\phi(m)$ bezeichnet (sog. Eulersche ϕ-Funktion). Da somit z.B. in $\mathbb{Z}_{10}$ genau die Restklassen 1, 3, 7, 9 multiplikativ invertierbar sind, gilt $\phi(10) = 4$.

Für Primzahlen p gilt allgemein: $\phi(p) = |\,\mathrm{Inv}(\mathbb{Z}_p, \odot)\,| = |\,\mathbb{Z}_p \setminus \{0\}\,| = p - 1$. Von 0 verschiedene Restklassen nach einem Primzahlmodul besitzen stets ein Inverses; es lässt sich mit dem Euklidischen Algorithmus berechnen.

■ 10.5.4. Proposition

Sei $(A, \perp)$ eine Halbgruppe mit neutralen Element e. Dann gilt:

(1) $e \in \mathrm{Inv}(A, \perp)$

(2) $\mathrm{Inv}(A, \perp)$ ist abgeschlossen unter $\perp$.

(3) $(x \perp y)^{-1} = y^{-1} \perp x^{-1}$ für alle $x, y \in \mathrm{Inv}(A, \perp)$.

■ Beweis

Zu (1): Ergibt sich unmittelbar aus $e \perp e = e$.

Zu (2) und (3): Es genügt zu zeigen, dass $y^{-1} \perp x^{-1}$ zu $x \perp y$ invers ist. Nach dem Assoziativgesetz gilt:

$$(y^{-1} \perp x^{-1}) \perp (x \perp y) = (y^{-1} \perp (x^{-1} \perp x)) \perp y = (y^{-1} \perp e) \perp y = y^{-1} \perp y = e$$

und entsprechend ergibt sich $(x \perp y) \perp (y^{-1} \perp x^{-1}) = e$. ◆

Bemerkungen

1. Unter der Voraussetzung von Prop. 10.5.4 (Halbgruppe mit neutralem Element e) ist $\mathrm{Inv}(A, \perp)$ jedenfalls nicht leer (e ist stets invertierbar).

2. Aussage (2) besagt, dass das Verknüpfungsergebnis invertierbarer Elemente wieder invertierbar ist.

3. Aussage (3) liefert die Regel, nach der sich das Inverse eines "Produkts" berechnen lässt. Es handelt sich offenbar um eine direkte Verallgemeinerung der "Umkehrregel" für die Abbildungsverkettung (vgl. Prop. 8.4.2).

4. Ist $\perp$ kommutativ, so gilt auch $(x \perp y)^{-1} = x^{-1} \perp y^{-1}$. Im Allgemeinen, d.h. für nicht-kommutative Verknüpfungen, gilt diese Gleichung jedoch *nicht*.

Eine spezielle Sorte invertierbarer Elemente sind diejenigen, die zu sich selbst invers sind. Zum Beispiel gilt für $p = (1\,2)\,(3\,4) \in \mathcal{S}_4$ die Gleichung $p^{-1} = p$, was sich auch $p^2 = e$ schreiben lässt. Das neutrale Element eines Verknüpfungsgebildes $(A, \perp)$ ist stets zu sich invers ($e^2 = e$). Allgemein heißt $a \in A$ involutorisch, wenn $a^2 = e$. So sind etwa in $(\mathbb{Z}_4, \oplus)$ die Restklassen 0 und 2 involutorisch ($0 \oplus 0 = 0$ bzw. $2 \oplus 2 = 0$). Spiegelungen sind involutorische Kongruenzabbildungen der Ebene. Das Verknüpfungsgebilde $(\mathcal{P}(M), +)$ besteht sogar aus lauter involutorischen Elementen, denn es gilt $A + A = \emptyset$ für alle $A \in \mathcal{P}(M)$.

■ Zum Begriff der Gruppe

Unter einer *Gruppe* versteht man eine Halbgruppe mit Einselement, in der sämtliche Elemente invertierbar sind (siehe die Def. 10.5.5, welche diesen Begriff durch drei Axiome beschreibt). Der Begriff wurde im 19. Jahrhundert zunächst im Zusammenhang mit der Auflösung algebraischer Gleichungen entwickelt. Bald erkannte man auch seine große Bedeutung für die Geometrie, was dann zu einem systematischen Ausbau einer eigenen Gruppentheorie führte. Ein wesentlicher Antrieb für diese Entwicklungen war die *Idee der Symmetrie*. Die Symmetrie einer Figur lässt sich durch die Gesamtheit G aller Transformationen (Abbildungen) ausdrücken, bei denen bestimmte Eigenschaften der Figur erhalten bleiben (vgl. Abschnitt 10.8). Dann bildet G eine Halbgruppe aus lauter invertierbaren Elementen (also genau das, was man unter einer Gruppe versteht). Im Gruppenbegriff lassen sich geometrische und algebraische Betrachtungsweisen verbinden, was zu einem großen Teil seinen Reiz und seine Bedeutung ausmacht.

■ 10.5.5. Definition

Ein Verknüpfungsgebilde $(G, \perp)$ heißt Gruppe, wenn folgende Eigenschaften erfüllt sind:

(G1) $\perp$ ist assoziativ.

(G2) Es gibt ein $e \in G$, sodass $e \perp a = a \perp e = a$ für alle $a \in G$.

(G3) Jedes $a \in G$ besitzt ein Inverses in $(G, \perp)$.

Bei der allgemeinen Notation von Gruppen (und Halbgruppen) wird häufig (und auch im Folgenden) die zugrunde liegende Verknüpfung *analog zur Multiplikation* aufgefasst und dementsprechend nicht eigens bezeichnet bzw. geschrieben. Die Gleichung aus (G2) lautet damit kürzer $e\,a = a\,e = a$; das neutrale Element e heißt daher in diesem Zusammenhang passender *Einselement* oder kurz: *Eins*.

Ist die in der Gruppe G gegebene Verknüpfung kommutativ, so heißt auch G selbst kommutativ (manchmal auch abelsch, zu Ehren des norwegischen Mathematikers N. H. Abel, 1802–1829).

Viele der bisher bekannten Verknüpfungsgebilde sind Gruppen in dem gerade definierten Sinn. Ebenso gelten eine Reihe von früher bewiesenen Aussagen erst recht für Gruppen. Das alles soll jetzt hier noch einmal kurz zusammengestellt werden:

■ Beispiele

1. Die Zahlenmengen $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ bilden jeweils zusammen mit der gewöhnlichen Addition eine kommutative Gruppe.

2. Die Mengen $\mathbb{Q} \setminus \{0\}$ und $\mathbb{R} \setminus \{0\}$ bilden jeweils zusammen mit der gewöhnlichen Multiplikation eine kommutative Gruppe.

3. Die Menge $\mathcal{S}_n$ aller Permutationen n-ten Grades bildet zusammen mit der Verkettung $\circ$ eine nicht-kommutative Gruppe (die sog. symmetrische Gruppe oder Permutationsgruppe).

4. $\mathbb{Z}_m$ ($m \geq 2$ ganz) bildet zusammen mit der Restklassenaddition $\oplus$ eine kommutative Gruppe.

5. $\mathbb{Z}_m^* := \mathrm{Inv}(\mathbb{Z}_m, \odot)$ ist eine kommutative Gruppe (bezeichnet als prime Restklassengruppe modulo m). Für primes p gilt $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, d.h. die Gruppe $\mathbb{Z}_p^*$ besteht aus genau den $p - 1$ Restklassen $1, \ldots, p - 1$.

Die folgende Proposition fasst eine Reihe bisher abgeleiteter Aussagen, soweit sie auf Gruppen anwendbar sind, zusammen:

■ 10.5.6. Proposition

Sei G eine Gruppe. Dann ist das Einselement in G eindeutig bestimmt. Ferner besitzt jedes Element a von G genau ein Inverses a^{-1} in G. Das Inverse eines Produkts $a\,b$ ($a,\ b \in G$) ist gleich dem Produkt aus dem Inversen von b und dem Inversen von a: $(a\,b)^{-1} = b^{-1}\,a^{-1}$.

10.6. Ringe und Körper

Häufig betrachtet man in einer Menge zwei Verknüpfungen, z.B. die Addition und die Multiplikation in $\mathbb{Z}$. Beide Verknüpfungen sind durch eine Rechenregel verbunden, die Verteilungs- oder *Distributivgesetz* genannt wird:

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

■ 10.6.1. Definition

Seien $\perp$ und $\top$ zwei Verknüpfungen in A. Dann heißt $\perp$ distributiv bzgl. $\top$, wenn für alle $x,\ y,\ z \in A$:

(1) $x \perp (y \top z) = (x \perp y) \top (x \perp z)$

(2) $(x \top y) \perp z = (x \perp z) \top (y \perp z)$

Für ganze, rationale und reelle Zahlen ist die Multiplikation distributiv bezüglich der Addition, jedoch ist die Addition nicht distributiv bezüglich der Multiplikation. Dasselbe gilt auch für die entsprechenden Verknüpfungen in $\mathbb{Z}_m$. Für Mengen ist sowohl $\bigcap$ distributiv bezüglich $\bigcup$ als auch umgekehrt $\bigcup$ distributiv bezüglich $\bigcap$.

■ Bemerkung zu Schreibweisen

Das Setzen von Klammern auf den rechten Seiten der Gleichungen (1) und (2) in der Definition ist erforderlich, um festzulegen, welche der beteiligten Operationen zuerst durchzuführen ist. Man kann Klammern durch eine Konvention vermeiden. Es ist dann zu vereinbaren, welche der beiden Operationen $\perp$ und $\top$ den Vorrang erhält. Eine solche Konvention existiert beispielsweise für die Multiplikation und Addition von Zahlen: *Punktrechnung geht vor Strichrechnung.* Wenn man einmal der Multiplikation den Vorrang gegeben hat, so sind Ausdrücke wie $x \cdot z + y \cdot z$ eindeutig auswertbar.

Häufig ist es zweckmäßig, für die Verknüpfungen in einer Menge die vertrauten Symbole '+' oder '$\cdot$' zu verwenden. Wird nur *eine* Verknüpfung betrachtet, so schreibt man sie gerne als Multiplikation (also $\cdot$ anstelle von $\perp$), oder man lässt das Operationssymbol überhaupt ganz weg. Bei der gewöhnlichen Multiplikation von Zahlen ist letzteres gang und gäbe, man schreibt also etwa: $x\,z + y\,z$ usw.

■ Ringe

Die grundlegenden Rechengesetze, die in den Zahlbereichen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ gelten (vgl. 1.2.1), zeigen (wenn A irgendeine dieser Mengen bedeutet): $(A, +)$ ist eine kommutative Gruppe und $(A, \cdot)$ ist eine Halbgruppe, und es gilt das Distributivgesetz $x(y + z) = x\,y + x\,z$. Auf Grund dieser Eigenschaften nennt man $(A, +, \cdot)$ einen Ring:

■ 10.6.2. Definition

Ein Verknüpfungsgebilde $(A, +, \cdot)$ mit 2-stelligen Verknüpfungen + und · in A heißt Ring, wenn gilt:

(R1) $(A, +)$ ist eine kommutative Gruppe

(R2) $(A, \cdot)$ ist eine Halbgruppe

(R3) · ist distributiv bzgl. +

Die oben genannten Ringe weisen aber noch speziellere Eigenschaften auf: Ihre multiplikative Halbgruppe $(A, \cdot)$ besitzt ein Einselement und ist kommutativ. Entsprechend handelt es sich um kommutative Ringe mit Eins. Die Eins eines Rings wird gewöhnlich mit 1 bezeichnet.

Das neutrale Element der additiven Gruppe $(A, +)$ eines Rings nennt man seine Null (bezeichnet mit 0).

■ Beispiele

1. Ein Ring kann *endlich* sein, wie das Beispiel von $(\mathbb{Z}_m, \oplus, \odot)$ zeigt, eines kommutativen Rings mit Einselement.

2. $(m\,\mathbb{Z}, +, \cdot)$ ist ein (unendlicher) Ring (*Unterring* des Rings der ganzen Zahlen). Die ganze Zahl 0 ist seine Null. Eine Eins besitzt dieser Ring genau dann, wenn $|m| = 1$ ist; in diesem Fall handelt es sich um die ganze Zahl 1. (Begründung!)

3. Sei $(G, +)$ eine (additiv geschriebene) abelsche Gruppe. Es bezeichne E die Menge aller Selbstabbildungen f von G mit der Eigenschaft: $f(x + y) = f(x) + f(y)$ für alle $x, y \in G$. Für zwei Abbildungen $f, g \in E$ sei ihre Summe definiert durch: $(f + g)(x) := f(x) + g(x)$ $(x \in G)$. Dann ist $(E, +, \circ)$ ein Ring mit id_E als Eins. (Beweis als Übung!).

4. Ein triviales Beispiel ist der sog. Nullring $A = \{e\}$, der aus nur einem Element besteht, für das $e + e = e$ sowie $e \cdot e = e$ gilt. Man überzeuge sich davon, dass tatsächlich ein Ring vorliegt (dessen Null und Eins dasselbe Element sind).

■ 10.6.3. Proposition

In einem Ring $(A +, \cdot)$ gelten die "Vorzeichenregeln":

(1) $a\,0 = 0\,a = 0$

(2) $a(-b) = (-a)\,b = -a\,b$

(3) $(-a)\,(-b) = a\,b$

■ Beweis

Als Übung! ◆

■ Bemerkung

In diesem Einführungskurs ist kein Raum, Ringe eingehender zu behandeln. Es soll aber wegen seiner fachlichen Bedeutung für den Unterricht zumindest das Thema "Division" kurz erörtert werden.

Die oft zu hörende Regel "Durch Null darf nicht dividiert werden!" klingt etwas merkwürdig und beinahe wie ein moralisches Verbot, weshalb es manchmal auch heißt, dass die Division durch Null nicht definiert sei. In der Sprache der Algebra lässt sich diesen reichlich vagen Formulierungen nun aber ein klarer Sinn unterlegen. Wir denken uns einen Ring $(A, +, \cdot)$ mit Eins gegeben. Der "Division durch Null" entspricht hier die Invertierung der Null in der multiplikativen Gruppe des Rings, d.h. der Auflösung der Gleichung $0 \cdot x = 1$. Da in jedem Ring $0 \cdot x = 0$ ist (vgl. Prop. 10.6.3,(1)), müsste somit gelten: $0 = 1$. Die Null (des Rings) hat also nur dann ein Inverses, wenn sie mit der Eins übereinstimmt. Dass dies in der Tat möglich ist, zeigt das oben angeführte Beispiel des Nullrings. Aber auch *nur im Nullring* kann durch Null dividiert werden, denn aus $0 = 1$ folgt sofort: $0 = 0 \cdot x = 1 \cdot x = x$, was heißt: alle Elemente $x \in A$ stimmen mit der Null überein (und das heißt ja gerade, dass A der Nullring ist).

Fazit: Genau in den vom Nullring verschiedenen Ringen besitzt die Null kein multiplikatives Inverses (d.h. "kann nicht durch 0 dividiert werden").

Es liegt nahe zu fragen, welche von 0 verschiedenen Elemente eines Rings ein multiplikatives Inverses besitzen.

■ Beispiel

$(\mathbb{Z}_4, \oplus, \odot)$ ist ein kommutativer Ring mit Eins. Nach Prop. 7.3.5 ist außer 1 nur 3 multiplikativ invertierbar. Es gilt: $3 \odot 3 = 1$. Der Rest 2 ist nicht invertierbar; es gilt sogar: $2 \odot 2 = 0$. Auf ähnliche Verhältnisse trifft man z.B. bei $\mathbb{Z}_{12}$, wo etwa gilt: $3 \odot 4 = 3 \odot 8 = 0$. – Das hier auftretende Phänomen von "Nullteilern" ist für Ringe auch allgemein von Bedeutung.

■ 10.6.4. Definition

Sei $(A, +, \cdot)$ ein kommutativer Ring ($\neq$ Nullring). Ein Element $a \in A$ heißt Nullteiler, wenn $a\,b = 0$ für ein Ringelement $b \neq 0$. Enthält A keine von 0 verschiedenen Nullteiler, so heißt A nullteilerfrei (oder auch: Integritätsring).

Die Zahlbereiche $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Integritätsringe.

Am Beispiel von $\mathbb{Z}$ sieht man noch folgendes: Auch wenn ein Ring keine echten (d.h. von Null verschiedenen) Nullteiler besitzt, so bedeutet dies doch nicht, dass seine von Null verschiedenen Elemente multiplikativ invertierbar sind. Bei den Ringen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ ist dies allerdings der Fall (ein Fall, der immerhin so wichtig ist, dass dafür ein neuer Begriff eingeführt wird):

■ 10.6.5. Definition

Ein kommutativer Ring $(A, +, \cdot)$ mit Eins heißt Körper, wenn $(A\setminus\{0\}, \cdot)$ eine Gruppe ist.

In einem Körper lässt sich so rechnen, wie wir es von den rationalen und reellen Zahlen her gewohnt sind. Diese Zahlbereiche sind denn auch die naheliegendsten Beispiele für Körper. Aus Beispiel Nr. 5 zu Def. 10.5.5 ist zu erkennen, dass auch die Reste modulo einer Primzahl p einen (endlichen!) Körper bilden: $(\mathbb{Z}_p, \oplus, \odot)$. Den kleinsten Körper, der nur die Elemente 0 und 1 enthält, gewinnt man hieraus für $p = 2$: $(\{0, 1\}, \oplus, \odot)$.

■ 10.6.6. Proposition

Ein Körper ist stets auch ein Integritätsring.

■ Beweis

Sei $(A, +, \cdot)$ ein Körper sowie $a \in A\setminus\{0\}$ und $a\,b = 0$. Durch Multiplikation mit dem Inversen von a ergibt sich: $0 = a^{-1}\,0 = a^{-1}(a\,b) = (a^{-1}\,a)\,b = 1 \cdot b = b$. ◆

Umgekehrt ist ein Integritätsring nicht auch schon ein Körper (wie das Gegenbeispiel $\mathbb{Z}$ zeigt). Wohl gilt hingegen die folgende Aussage:

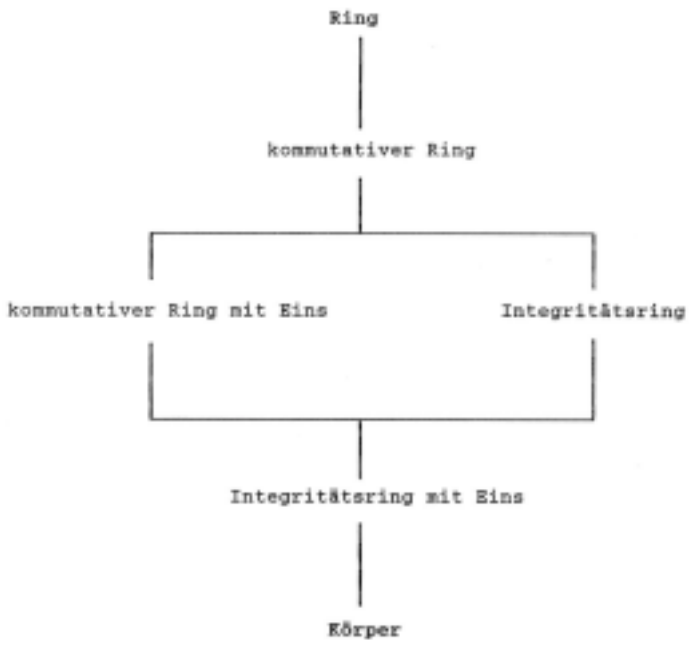
■ 10.6.7. Proposition

Ein endlicher Integritätsring ist ein Körper.

■ Beweis

Sei A ein endlicher Integritätsring. Es ist zu zeigen, dass $(A\setminus\{0\}, \cdot)$ eine Gruppe ist. Da A nullteilerfrei ist, gilt für $a, b \neq 0$ stets $a\,b \neq 0$, und damit ist die Multiplikation $\cdot$ eine Verknüpfung in $A\setminus\{0\}$; sie ist assoziativ, da $(A, \cdot)$ eine Halbgruppe ist. Sei nun $a \in A\setminus\{0\}$ vorgegeben. Wir definieren eine Abbildung $f : A \longrightarrow A$ durch $f(x) := a\,x$. Dieses f ist injektiv, denn aus $f(x) = f(y)$ folgt $a\,x = a\,y$ und nach Prop. 10.6.3 und Distributivgesetz: $0 = a\,x - a\,y = a(x - y)$, sodass sich aufgrund der Nullteilerfreiheit $x = y$ ergibt. Als injektive Selbstabbildung einer endlichen Menge ist f sogar bijektiv (vgl. Prop. 8.5.5), es gibt also genau ein $x_0 \in A$ mit $f(x_0) = a\,x_0 = a$. Dieses (zu a) eindeutig bestimmte x_0 ist Einselement der Halbgruppe $(A, \cdot)$ (und somit unabhängig von a). Begründung: Zu beliebig vorgegebenem $c \in A$ gibt es wegen der Bijektivität von f ein $x \in A$ mit $f(x) = c$, mithin $a\,x = c$, woraus resultiert: $c = a\,x = (a\,x_0)\,x = x_0(a\,x) = x_0\,c = c\,x_0$. Das (eindeutig bestimmte!) Einselement x_0 werde wie üblich 1 genannt. Die Gleichung $a\,x = 1$ besitzt (wegen der Bijektivität der zu a definierten Abbildung f) eine eindeutige Lösung x, und diese ist offensichtlich invers zu a. ◆

Die folgende Übersicht zeigt die in diesem Abschnitt behandelten Strukturbegriffe in ihrer logischen Abhängigkeit:



10.7. Untergruppen

Für das Studium einer Gruppe sind ihre Untergruppen von zentraler Bedeutung, da diese Aufschluss über ihren Aufbau vermitteln (was allerdings im Folgenden nicht vertieft werden wird).

■ 10.7.1. Definition

Eine (nichtleere) Teilmenge H einer Gruppe G heißt Untergruppe von G, wenn H bezüglich der Gruppenverknüpfung abgeschlossen und eine Gruppe ist.

In einer Gruppe G gibt es stets mindestens eine Untergruppe, nämlich die sog. triviale Untergruppe $\{e\}$, die aus dem Einselement von G besteht. Natürlich ist jede Gruppe Untergruppe von sich selbst.

■ Beispiele

1. $\mathbb{Z}$ ist eine Untergruppe von $(\mathbb{Q}, +)$; $\mathbb{Q}$ ist Untergruppe von $(\mathbb{R}, +)$.

2. Die Menge $m\,\mathbb{Z} = \{ m\,k \mid k \in \mathbb{Z} \}$ der ganzzahligen Vielfachen von m (m ganz) ist eine Untergruppe von $(\mathbb{Z}, +)$.

3. Die Restemenge $\{0, 2, 4\}$ ist eine Untergruppe von $(\mathbb{Z}_6, \oplus)$.

4. Die Permutationenmenge $\{(1)\,(2)\,(3)\,(4), (1\,3\,4\,2), (1\,4)\,(2\,3), (1\,2\,4\,3)\}$ ist eine Untergruppe von $(\mathcal{S}_4, \circ)$.

Die folgende Aussage enthält ein hinreichendes und notwendiges Kriterium dafür, dass eine Teilmenge einer Gruppe G eine Untergruppe von G ist:

■ 10.7.2. Proposition (Untergruppenkriterium)

Sei G eine Gruppe, H eine Teilmenge von G. Dann gilt: H ist Untergruppe von G genau dann, wenn $H \neq \emptyset$ und mit $a, b \in H$ stets auch $a\, b^{-1} \in H$ gilt.

■ Beweis

1. Eine Untergruppe H von G erfüllt offensichtlich die behauptete Eigenschaft (Begründung!).

2. Sei umgekehrt H eine nichtleere Teilmenge mit $a\, b^{-1} \in H$ für alle $a, b \in H$. Es ist zu zeigen, dass H eine Gruppe ist. Sei e das Einselement von G. Dann hat man jedenfalls $e = a\, a^{-1} \in H$. Jedes $a \in H$ ist ferner invertierbar wegen $e\, a^{-1} \in H$. Unter der Gruppenverknüpfung ist H abgeschlossen, denn zu $a, b \in H$ liegt das Inverse b^{-1} in H, und damit gilt $a\, b = a\, (b^{-1})^{-1} \in H$. Daher ist auch das Assoziativgesetz in H erfüllt, und H ist eine Gruppe. ◆

■ Potenzen und Ordnung

Im Folgenden werden für das Rechnen in Gruppen geeignete Begriffe und Regeln entwickelt. Da lediglich *eine* Verknüpfung vorliegt, beschränkt sich das Rechnen auf die wiederholte Anwendung dieser Verknüpfung, d.h. auf das Bilden von Potenzen. Die zugehörigen Begriffe spiegeln dies wider.

Sei G eine Gruppe und $a \in G$. Dann definiert man $a^0 = e$ (Einselement von G), $a^1 = a$, $a^2 = a\, a$, usw. Um dies allgemein und auch für ganzzahlige Exponenten zu erklären, benötigt man die folgende rekursive Definition:

■ 10.7.3. Definition

Für beliebige Elemente a einer Gruppe G mit dem Einselement e wird definiert:

$$a^0 = e$$

$$a^{n+1} = a^n\, a \text{ (für ganze Zahlen } n \geq 0)$$

Zusätzlich wird für $n < 0$ festgelegt:

$$a^n := (a^{-1})^{-n}$$

■ Bemerkung

Die zuletzt getroffene Festsetzung hat einen Sinn, weil für negatives n die $(-n)$-te Potenz des Inversen von a bereits definiert wurde. Insgesamt gibt die obige Definition die Gegebenheiten wieder, die vom Rechnen mit rationalen (oder reellen) Zahlen her vertraut sind. Insbesondere gelten die üblichen Rechengesetze für Potenzen:

■ 10.7.4. Proposition

In einer Gruppe G gilt für alle $a \in G$ und für alle $m, n \in \mathbb{Z}$:

(1) $a^m\, a^n = a^{m+n}$

(2) $(a^m)^n = a^{m\,n}$

(3) $(a^m)^{-1} = (a^{-1})^m$

(4) $(a\,b)^n = a^n\,b^n$ für jedes $b \in G$ mit $a\,b = b\,a$.

■ Beweis

Hinweis: Zunächst $m,\ n \geq 0$ voraussetzen und Beweise durch Induktion führen, anschließend mit Hilfe von Def. 10.7.3 auch negative Exponenten einbeziehen. Die Durchführung der Einzelheiten verläuft dann routinemäßig und bleibt zur Übung. ◆

Es ist von besonderem Interesse, in einer Gruppe G alle Potenzen a^n eines Elements $a \in G$ zu betrachten.

■ Beispiele

1. In der additiven Gruppe $\mathbb{Z}$ der ganzen Zahlen bedeutet a^n die ganze Zahl $n\,a$. Die Potenzen von a sind also gerade die Vielfachen von a und die Potenzen von 1 gerade die ganzen Zahlen.

2. In der additiven Restklassengruppe $\mathbb{Z}_6$ hat die Restklasse 2 die Potenzen 0, 2, 4. Tatsächlich ist 4 das letzte Element dieser Folge, denn es gilt $4 \oplus 2 = 0$.

3. In $\mathcal{S}_4$ hat $p = (1\,3\,4\,2)$ die Potenzen $p^0 (= e),\ p,\ p^2,\ p^3$. Es ist $p^4 = e$; daher werden durch höhere Exponenten keine neuen Permutationen erzeugt. Auch durch negative Exponenten entstehen keine neuen Elemente, denn es gilt $p^{-1} = p^3$.

Die Beispiele zeigen: Die Potenzen eines Gruppenelements bilden eine Untergruppe.

■ 10.7.5. Proposition

Sei G eine beliebige Gruppe und $a \in G$. Die Menge der Potenzen a^n $(n \in \mathbb{Z})$ ist eine Untergruppe von G.

■ Beweis

Nach dem Untergruppenkriterium (Prop. 10.7.2) ist zu zeigen, dass zu Potenzen a^n und a^m das Produkt $a^n(a^m)^{-1}$ wieder eine Potenz von a ist. Das ist in der Tat der Fall, denn nach Prop. 10.7.4 gilt:

$$a^n(a^m)^{-1} = a^n(a^{-1})^m = a^n\,a^{-m} = a^{n-m}$$ ◆

■ Bezeichnungen

Die von den Potenzen von $a \in G$ gebildete Untergruppe von G heißt Erzeugnis von a in G, oder: von a erzeugte Gruppe (bzw. Untergruppe in G). Sie werde im Folgenden mit $\langle a \rangle$ bezeichnet. Es ist $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$.

An den zuletzt genannten Beispielen (Nr. 2 und Nr. 3) ist zu beobachten, dass eine Potenz mit einem Exponenten größer als 0 dennoch gleich dem Einselement sein kann.

Bildet man die Potenzen innerhalb einer *endlichen* Gruppe, so ist dies notwendigerweise so. Denn es gibt dann zunächst einmal zwei übereinstimmende Potenzen, etwa $a^r = a^s$, wobei ohne Beschränkung der Allgemeinheit $r < s$ angenommen werden kann. Hieraus folgt sofort: $e = a^{-r}\,a^s = a^{s-r}$ mit $s - r > 0$.

Ist die Gruppe G unendlich, so lässt sich der eben durchgeführte Schluss nicht aufrechterhalten. Zum Beispiel sind in $\mathbb{Z}$ alle (additiven) Potenzen eines Elementes $a \neq 0$ verschieden!

Die vorangegangenen Betrachtungen führen zu einer Definition, welche die Definition der Ordnung einer Permutation verallgemeinert.

■ 10.7.6. Definition

Sei G eine Gruppe und e das Einselement von G. Gibt es für ein $a \in G$ eine ganze Zahl $n > 0$ mit $a^n = e$, so heißt die kleinste dieser Zahlen Ordnung von a (in G); sie werde mit ord(a) bezeichnet; andernfalls setzt man ord(a) = ∞ (Ordnung von a in G ist unendlich).

■ Beispiele

1. Die Ordnung der Elemente (ganzen Zahlen) in der additiven Gruppe $(\mathbb{Z}, +)$ ist unendlich.

2. In $(\mathbb{Z}_6, \oplus)$ gilt: ord(2) = 3.

3. Für $p = (1\,4)\,(2\,5\,3) \in \mathcal{S}_5$ ist ord(p) = 6.

■ Bezeichnung

Die Anzahl der Elemente einer Gruppe G wird als Ordnung von G bezeichnet (symbolisch: ord(G) oder $|G|$); enthält G unendlich viele Elemente, so schreibt man: $|G| = \infty$.

■ Bemerkung

Trotz der gleichlautenden Bezeichnungen hat die Ordnung eines Elements von der Definition her zunächst mit der Ordnung der Gruppe nichts zu tun. Es stellt sich aber bald heraus, dass doch eine enge sachliche Beziehung zwischen beiden besteht (und dies ist natürlich auch der entstehungsgeschichtliche Grund für die gemeinsame Benennung). Man erkennt diesen Zusammenhang bereits daran, dass in einer Gruppe G für beliebiges $a \in G$ gilt: ord(a) = $|\langle a \rangle|$, d.h. die Ordnung von a stimmt überein mit der Ordnung der von a in G erzeugten Untergruppe.

Die Gruppe $\mathbb{Z}$ ist von unendlicher Ordnung, und ihre Elemente (außer 0) besitzen ebenfalls unendliche Ordnung. Für die von $a \in \mathbb{Z}$ erzeugte Untergruppe gilt: $\langle a \rangle = a\,\mathbb{Z}$ (Menge der ganzzahligen Vielfachen von a). Man kann zeigen, dass es außer diesen Vielfachenmengen keine anderen Untergruppen von $\mathbb{Z}$ gibt.

■ 10.7.7. Proposition

H ist Untergruppe von $(\mathbb{Z}, +) \iff H = a\,\mathbb{Z}$ für ein ganzes $a \geq 0$

■ Beweis

1. "⟸": $a\,\mathbb{Z}$ ist (als Erzeugnis von a) eine Untergruppe von $\mathbb{Z}$.

2. "$\Longrightarrow$": Es ist umgekehrt zu zeigen, dass eine Untergruppe H von $\mathbb{Z}$ eine Vielfachenmenge ist. Im Fall $H = \{0\} = 0\,\mathbb{Z}$ ist dies natürlich der Fall. Sei daher H eine nichttriviale Untergruppe und $x \in H$ ein von 0 verschiedenes Element. Da H eine Gruppe ist, gilt auch $-x \in H$; folglich gibt es in H positive Zahlen. Die kleinste von ihnen sei a. Sei nun $h \in H$ beliebig vorgegeben; Division von h durch a mit Rest ergibt dann eine Darstellung $h = a\,q + r$, wobei $0 \leq r < a$. Nach dem Untergruppenkriterium ist $r = h - q\,a \in H$. Wegen $r \geq 0$ und der Minimalität von a muss $r = 0$ sein. Somit ist $h = q\,a$ und $H \subseteq a\,\mathbb{Z}$ gezeigt. Ist $x \in a\,\mathbb{Z}$, d.h. $x = n\,a$ für ein ganzes n, so ist auch $x \in H$, weil $a \in H$ und H (als Gruppe) alle 'Potenzen' (d.h. hier: Vielfachen) von a enthält. Mithin ist auch $a\,\mathbb{Z} \subseteq H$ und insgesamt $a\,\mathbb{Z} = H$ gezeigt. ◆

Es liegt nun nahe, auch nach den Untergruppen H von $(\mathbb{Z}_m, \oplus)$ zu fragen.

■ 10.7.8. Proposition

> H ist Untergruppe von $(\mathbb{Z}_m, \oplus)$ genau dann, wenn $H = \langle a \rangle$ für einen Rest a mod m. Dabei ist ord(H) Teiler der Gruppenordnung m.

■ Beweis

Ist H die triviale Untergruppe, so gilt $H = \{0\} = \langle 0 \rangle$. Sei nun $H \neq \{0\}$ und a kleinster positiver Rest mod m in H. Wie im Beweis zu 10.7.7 zeigt man (bei wörtlicher Wiederholung der Argumente):$\langle a \rangle = H$. Da H endlich ist, ergibt sich: $H = \{0, a, 2\,a, \ldots, (s-1)\,a\}$; dabei ist s die eindeutig bestimmte ganze Zahl mit $0 \leq (s-1)\,a < m \leq s\,a$. Wir zeigen: $m = s\,a$. – Division von m durch a mit Rest liefert eine Darstellung $m = k\,a + r$ mit $0 \leq r < a$. Für den Rest gilt: $r = m - k\,a \equiv k\,a \bmod m \in H$ und, da a minimal ist, $r = 0$. Daher hat man $m = k\,a$. Setzt man dies in die Ungleichung für s ein und kürzt anschließend a heraus, so ergibt sich: $s - 1 < k \leq s$. Es ist also $k = s$. Insgesamt ist damit gezeigt, dass sowohl a (das erzeugende Element) als auch s (die Untergruppenordnung ord(H)) Teiler der Gruppenordnung m sind. ◆

■ Beispiel

Für $m = 12$ ergeben sich die folgenden (echten nichttrivialen) Untergruppen von $\mathbb{Z}_{12}$ samt erzeugenden Elemente:

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$	Ordnung: 6
$\langle 3 \rangle = \{0, 3, 6, 9\}$	Ordnung: 4
$\langle 4 \rangle = \{0, 4, 8\}$	Ordnung: 3
$\langle 6 \rangle = \{0, 6\}$	Ordnung: 2

Die Teilerbeziehung zwischen den Ordnungen von Untergruppe und Gruppe gilt nicht nur für die $\mathbb{Z}_m$, sondern ganz allgemein für alle endlichen Gruppen.

■ 10.7.9. Definition

Eine Gruppe G heißt zyklisch, wenn sie von einem ihrer Elemente erzeugt wird, d.h. wenn ein $a \in G$ existiert mit $G = \langle a \rangle$. Das Element a heißt dann erzeugendes Element von G.

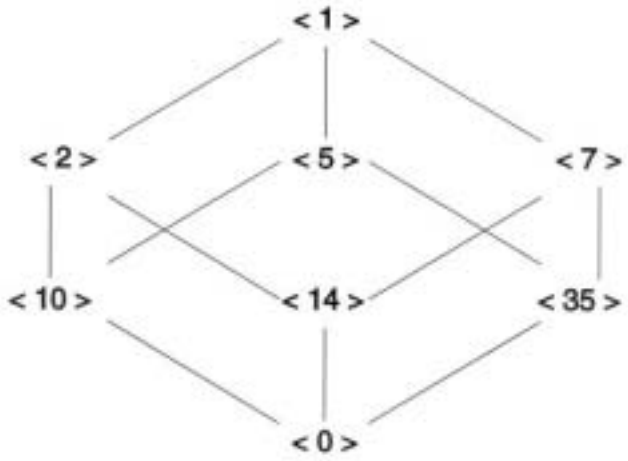
■ Beispiele

Die additiven Gruppen $\mathbb{Z}$ und $\mathbb{Z}_m$ (mit 1 als erzeugendem Element); ferner die Drehungsgruppen, die in Abschnitt 10.8 behandelt werden.

Die Untergruppen der zyklischen Gruppe $G = \mathbb{Z}_{70}$ sind sämtlich Erzeugnisse $\langle q \rangle$ eines Teilers q der Gruppenordnung. Hier eine Übersicht:

m	q	$\langle q \rangle$
1	70	{0}
2	35	{0, 35}
5	14	{0, 14, …, 56}
7	10	{0, 10, …, 60}
10	7	{0, 7, …, 63}
14	5	{0, 5, …, 65}
35	2	{0, 2, …, 68}
70	1	{0, 1, …, 69}

Für eine zyklische Gruppe ist der sog. Gruppengraph (Ordnungsdiagramm der Untergruppen) identisch mit dem Teilerdiagramm für die Gruppenordnung:



■ 10.7.10. Proposition (Satz von Lagrange)

Sei G eine endliche Gruppe, H eine Untergruppe von G. Dann ist ord(H) ein Teiler von ord(G).

■ Beweis

Der Beweis folgt einem einfachen Grundgedanken. Man zerlegt die Menge G in gleichgroße Teile, von denen jeder so groß ist wie H. Die fraglichen "Teile" sind sämtlich Mengen der Form $x\,H := \{\, x\,a \mid a \in H \,\}$, die sog. Linksnebenklassen von H.

(1) Jedes $x \in G$ liegt wegen $x = x\,e$ (e = Einselement von G, $e \in H$) in einer Nebenklasse, nämlich $x \in x\,H$. Da umgekehrt jede Nebenklasse eine Teilmenge von G ist, ist G die Vereinigung sämtlicher Nebenklassen $x\,H$, $x \in G$.

(2) Die Mengen H und $x\,H$ haben (für beliebiges $x \in G$) dieselbe Anzahl von Elementen, denn die Linksmultiplikation, die jedem $a \in H$ das Element $x\,a$ zuordnet, ist eine bijektive Abbildung von H auf $x\,H$. Natürlich haben infolgedessen auch alle Nebenklassen von H dieselbe Elementeanzahl.

(3) Schließlich ist noch zu überlegen, dass zwei verschiedene Nebenklassen stets disjunkt sind. Sei dazu a als gemeinsames Element von $x\,H$ und $y\,H$ angenommen: $a \in x\,H \cap y\,H$. Dann gibt es $u, v \in H$ derart, dass $a = x\,u$ und $a = y\,v$. Hieraus folgt $x\,u = y\,v$ und damit auch $y^{-1}\,x = v\,u^{-1} \in H$ (nach dem Untergruppenkriterium). Ein Element der Nebenklasse $x\,H$ hat die Form $x\,c$, wobei $c \in H$, was sich nun auch schreiben lässt als: $x\,c = y(y^{-1}\,x)\,c = y\,d$ mit $d := y^{-1}\,x\,c \in H$. Es gilt somit $x\,c \in y\,H$. Ebenso zeigt man umgekehrt, dass jedes Element der Nebenklasse $y\,H$ auch zu $x\,H$ gehört. Insgesamt hat man also $x\,H = y\,H$.

Zusammen ergeben die Teile (1), (2) und (3) die Aussage: G ist disjunkte Vereinigung von Mengen, welche dieselbe Anzahl von Elementen haben wie H. ◆

■ 10.7.11. Proposition

Sei G eine endliche Gruppe, e ihr Einselement. Dann gilt für alle $a \in G$:

(1) $\mathrm{ord}(a)$ ist Teiler von $\mathrm{ord}(G)$

(2) $a^{\mathrm{ord}(G)} = e$

■ Beweis

Zu (1): Man betrachte die von a erzeugte Untergruppe $H = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. Für deren Ordnung n gilt $n = \mathrm{ord}(H) = \mathrm{ord}(a)$. Prop. 10.7.10 liefert $\mathrm{ord}(H) \mid \mathrm{ord}(G)$ und damit die Behauptung (1).

Zu (2): Nach (1) haben wir $\mathrm{ord}(G) = k \cdot \mathrm{ord}(a)$ für eine geeignete natürlich Zahl k. Damit ergibt sich unter Beachtung der Potenzrechenregel 10.7.4,(2): $a^{\mathrm{ord}(G)} = a^{k \cdot \mathrm{ord}(a)} = (a^{\mathrm{ord}(a)})^k = e^k = e$. ◆

■ 10.7.12. Korollar (Satz von Euler-Fermat)

$$a^{\phi(m)} \equiv 1 \bmod m$$

■ Beweis

Wähle für G die prime Restklassengruppe modulo m: $G = \mathbb{Z}_m{}^*$. Dann gilt $\mathrm{ord}(G) = \phi(m)$. Einselement von G ist 1 (als Restklasse mod m). Schreibt man damit die Gleichung 10.7.11,(2) als Kongruenz, so steht die Behauptung direkt da. ◆

■ Bemerkung

Die Spezialisierung $m = p$ (Primzahl) liefert unter Beachtung von $\phi(p) = p - 1$ sofort den Lehrsatz ("Kleiner Fermat", vgl. Prop. 7.3.6.): $a^{p-1} \equiv 1 \bmod p$ (für teilerfremde $a,\ p$).

10.8. Symmetrie(gruppen)

Ein wichtiges Anwendungsgebiet des Gruppenbegriffs ist die Geometrie. Hier beschäftigt man sich mit Symmetriegruppen ebener oder räumlicher Figuren. Eine Symmetriegruppe besteht aus Selbstabbildungen der (euklidischen) Ebene E (oder – im weiteren außer Betracht – des Raums). Dabei werden nicht beliebige Abbildungen, sondern nur *abstandstreue Transformationen*, d.h. Kongruenzabbildungen zugelassen (vgl. die entsprechenden Beispiele aus Kapitel 8 und die Übungen dazu).

■ 10.8.1. Definition

1. Eine Abbildung $f : E \longrightarrow E$ heißt abstandstreu, wenn für irgend zwei Punkte P, Q der (euklidischen) Ebene E gilt: $|f(P), f(Q)| = |P, Q|$.

(Der Abstand zwischen zwei Punkten X, Y von E ist hier mit $|X, Y|$ bezeichnet.)

2. Eine abstandstreue Surjektion $E \longrightarrow E$ heißt Kongruenzabbildung von E. Es bezeichne $\mathcal{K}_E$ die Menge der Kongruenzabbildungen von E. (Die ebenfalls gebräuchliche Bezeichnung Isometrie bringt die Abstandstreue namentlich zum Ausdruck.)

■ Beispiele

Grundtypen von Kongruenzabbildungen (bzw. Isometrien) sind: Verschiebungen (Translationen), Drehungen (Rotationen) und Geradenspiegelungen von E.

■ 10.8.2. Proposition

(1) $f \in \mathcal{K}_E \Longrightarrow f$ ist bijektiv

(2) $f, g \in \mathcal{K}_E \Longrightarrow f \circ g \in \mathcal{K}_E$

(3) $f \in \mathcal{K}_E \Longrightarrow f^{-1} \in \mathcal{K}_E$

■ Beweis

Zum Beweis ist hier zu zeigen: (1) dass eine abstandstreue Abbildung injektiv ist, (2) die Verkettung zweier Kongruenzabbildungen wieder eine Kongruenzabbildung ist, (3) die Umkehrabbildung einer Kongruenzabbildung abstandstreu ist. Beispielsweise sieht man (1) wie folgt ein: Aus $f(P) = f(Q)$ folgt $0 = |f(P), f(Q)| = |P, Q|$, also auch $P = Q$. – (2) und (3) sind ebenso einfach zu verifizieren. ◆

■ 10.8.3. Korollar (und Bezeichnung)

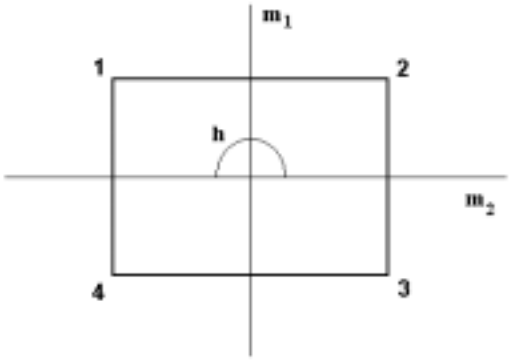
> $(\mathcal{K}_E, \circ)$ ist eine (nicht-kommutative) Gruppe, die sog. Kongruenzgruppe (auch: Isometriegruppe oder Bewegungsgruppe) von E.

■ Beweis

Für $\mathcal{K}_E$ sind die drei Gruppenaxiome erfüllt: (G1, Assoziativität von ○) folgt aus 10.8.2,(2) zusammen mit 8.3.4 (vgl. auch die Bemerkung 2 am Ende von Abschnitt 10.3). (G2) wird mit id_E Genüge getan. (G3) gilt aufgrund von 10.8.2,(3). ◆

■ Symmetriegruppe einer Figur

Hat man nun eine Figur vorliegen, etwa ein beliebiges Rechteck R (in E) mit den Ecken 1, 2, 3, 4, so stellt sich die Frage, welche Kongruenzabbildungen R fest lassen. Das heißt genauer: Für welche $f \in \mathcal{K}_E$ gilt $f[R] = R$? Eine Kongruenzabbildung f, die diese Forderung erfüllt, heißt Symmetrie oder Deckabbildung von R.



Eine Verschiebung kommt als Deckabbildung offensichtlich nicht in Frage, wohl aber z.B. eine Halbdrehung h der Ebene um den Mittelpunkt von R. Der Einfachheit halber wird sie (hier und allgemein bei Vielecken) *mit der durch sie bewirkten Permutation der Eckenmenge identifiziert*, also hier: $h = (1\,3)\,(2\,4)$ (obwohl keine Identität im strengen Sinne vorliegt!).

Natürlich gehört nicht zu jeder Permutation der Eckenmenge von R auch eine Symmetrie. Zum Beispiel gibt es keine zu $(1)\,(2\,3)\,(4)$ gehörende Deckabbildung von R; von den 24 möglichen Eckenpermutationen entsprechen sogar nur die folgenden 4 den Symmetrien des Rechtecks: e, $m_1 = (1\,2)\,(3\,4)$, $m_2 = (1\,4)\,(2\,3)$, $h = (1\,3)\,(2\,4)$. Ihre Verkettungsprodukte sind nachstehender Verknüpfungstafel zu entnehmen:

○	e	m_1	m_2	h
e	e	m_1	m_2	h
m_1	m_1	e	h	m_2
m_2	m_2	h	e	m_1
h	h	m_2	m_1	e

Aus der Tafel lesen wir ab, dass $R_4 = \{e, m_1, m_2, h\}$ eine Gruppe ist: R_4 ist abgeschlossen bzgl. ○ (somit ○ assoziativ in R_4); ferner ist e Einselement und sind alle Elemente invertierbar (sogar involutorisch). In Erinnerung an den Mathematiker F. Klein (1849-1925) wird R_4 als Kleinsche Vierergruppe bezeichnet.

Nach diesem Beispiel lässt sich der Begriff der Symmetriegruppe nun ohne weiteres auch allgemein erklären:

■ 10.8.4. Definition

Sei F irgendeine nichtleere Teilmenge der Ebene E (im folgenden Figur genannt). Eine Kongruenzabbildung $f \in \mathcal{K}_E$ heißt Symmetrie (oder: Deckabbildung) von F, wenn gilt: $f[F] = F$. Es bezeichne $\mathrm{Sym}(F) := \{f \in \mathcal{K}_E \mid f[F] = F\}$ die Menge aller Symmetrien von F.

Es ist eine fundamentale Tatsache, dass die Symmetrien einer Figur F eine Gruppe (genauer: Untergruppe der Kongruenzgruppe $\mathcal{K}_E$) bilden. Dies besagt folgende

■ 10.8.5. Proposition

Zu beliebiger Figur F ist $\mathrm{Sym}(F)$ eine Untergruppe von $\mathcal{K}_E$ (die sog. Symmetriegruppe von F).

■ Beweis

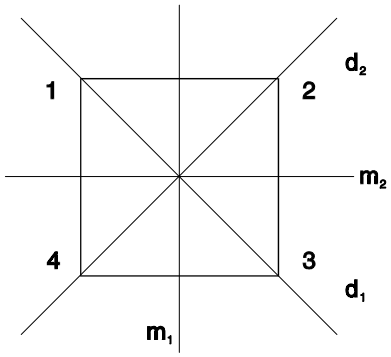
Wir benutzen das Untergruppenkriterium (Prop. 10.7.2). Seien dazu $f, g \in \mathrm{Sym}(F)$ beliebig. Da $\mathrm{Sym}(F)$ bzgl. $\circ$ abgeschlossen ist – denn: $(f \circ g)[F] = f[g[F]] = f[F] = F$ –, genügt es zu zeigen, dass die Umkehrabbildung einer Symmetrie f wieder zu $\mathrm{Sym}(F)$ gehört. Ein Punkt X liegt in $f^{-1}[F]$ genau dann, wenn $f^{-1}(Y) = X$ für ein $Y \in F$, das heißt: $f(X) \in F = f[F]$. Wegen der Injektivität von f ist dies genau für $X \in F$ der Fall, d.h. $f^{-1}[F] = F$. ◆

Die Symmetriegruppen spielen für die geschichtliche und systematische Entwicklung des Gruppenbegriffs in der Mathematik eine zentrale Rolle. So lassen sich mit ihnen geometrische Eigenschaften algebraisch beschreiben. (Auch umgekehrt werden häufig algebraische Sachverhalte geometrisch-anschaulich interpretierbar.) Das Gebiet der Abbildungsgeometrie baut geometrische Aussagenbestände systematisch mit Hilfe von Abbildungsgruppen auf. Zum Studium symmetrischer Figuren vgl. die gut lesbare Einführung von Flachsmeyer / Feiste / Manteuffel: *Mathematik und ornamentale Kunstformen*. Mathematische Schülerbücherei. Leipzig: Teubner 1990.

Besonderes Interesse verdienen die Symmetriegruppen regelmäßiger n-Ecke (Polygone) P_n. Die zugehörige Symmetriegruppe wird als Diedergruppe $\mathcal{D}_n$ bezeichnet (sprich: *Di-eder*)

Dieder bedeutet wörtlich "Zweiflächner"; man hat sich dabei das fragliche Vieleck als ein Gebilde im Raum vorzustellen, das eine "Vorderseite" und eine "Rückseite" besitzt. Damit sind nun die Spiegelungen aus $\mathcal{D}_n$ als räumliche Klappbewegungen vorstellbar, die den Dieder mit sich selbst zur Deckung bringen. Vom algebraischen Standpunkt ist dies freilich irrelevant, da ohnehin jede Symmetrie des Dieders als Permutation seiner Eckenmenge beschreibbar ist.

Man betrachte als einfaches Beispiel einer Diedergruppe die $\mathcal{D}_4$, die Symmetriegruppe des Quadrats mit den Ecken 1, 2, 3, 4. Sie besteht aus 4 Drehungen und 4 Spiegelungen, hat also die Ordnung 8. Die Drehungen bilden eine zyklische Untergruppe Δ_4 der Ordnung 4. Sie wird erzeugt von der Vierteldrehung (um den Quadratmittelpunkt), zu der die Eckenpermutation $a = (1\,4\,3\,2)$ gehört. Demnach sind $e(:= a^0)$, a, a^2, a^3 die Drehungen um $0°, 90°, 180°, 270°$.



Die Spiegelungen bilden zwar keine Untergruppe, doch ist jede der Spiegelungen als Verkettungsprodukt einer einzigen Spiegelung mit einer geeigneten Drehung darstellbar. Sei etwa $b := d_1 = (1)\,(2\,4)\,(3)$ als "Grund"-Spiegelung gewählt. Dann gilt:

$$d_2 = (1\,3)\,(2)\,(4) = b\,a^2$$
$$m_1 = (1\,2)\,(3\,4) = b\,a$$
$$m_2 = (1\,4)\,(2\,3) = b\,a^3$$

Insgesamt lässt sich also jedes Element der $\mathcal{D}_4$ in der Form a^k (als Drehung) oder $b\,a^k$ (als Spiegelung) mit $0 \le k < 4$ darstellen. Die Menge der Spiegelungen erweist sich demnach als Nebenklasse $b\,\Delta_4$ der Untergruppe der Drehungen:

$$\mathcal{D}_4 = \{e,\ a,\ a^2,\ a^3,\ b,\ b\,a,\ b\,a^2,\ b\,a^3\}$$

Für das Rechnen mit diesen Elementen sind die folgenden Gleichungen zu Grunde zu legen:

$a^4 = e$ (die Vierteldrehung ist ein Element der Ordnung 4)

$b^2 = e$ (die Spiegelung ist involutorisch)

$b\,a = a^{-1}\,b$ (dieselbe Spiegelung an der Mittelsenkrechten einer Seite)

Tatsächlich lässt sich das beschriebene Vorgehen für beliebige Diedergruppen verallgemeinern. An dieser Stelle wird – unter Verzicht auf einen Beweis – der Inhalt des betreffenden **Hauptsatzes für Diedergruppen** lediglich kurz zusammengestellt und erläutert.

Die $\mathcal{D}_n$ besteht aus n Drehungen und n Spiegelungen, also $\mathrm{ord}(\mathcal{D}_n) = 2\,n$. Jede Drehung ist darstellbar als Potenz einer "kleinsten" Drehung

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & 1 & 2 & \dots & n-2 & n-1 \end{pmatrix}.$$

Ferner werde als Spiegelungselement

$$b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

gewählt. Es gelten dann die Relationen:

(1) $a^n = e$

(2) $b^2 = e$

(3) $b\,a = a^{-1}\,b = a^{n-1}\,b$

Unter diesen Voraussetzungen ist $d \in \mathcal{D}_n$ genau dann, wenn $d = a^k$ oder $d = b\,a^k$ für eine ganze Zahl k mit $0 \le k < n$.

Die Diedergruppe $\mathcal{D}_n$ ist (bis auf Isomorphie – siehe unten) bereits vollständig durch die Relationen (1) –(3) bestimmt. Die Natur der Elemente a, b als Permutationen spielt dabei keine Rolle. Dass a eine "Drehung" und b eine

"Spiegelung" ist, wird nur durch (1) bzw. (2) ausgedrückt; es kommt dann (3) hinzu, um die Abhängigkeit der beiden Elemente untereinander festzulegen. Gleichung (3) ist geometrisch-anschaulich interpretierbar (Übung!).

■ Isomorphie

Das Wort "isomorph" bedeutet "gleichgestaltig" oder "von gleicher Struktur". Der Begriff und die zugrunde liegende Erscheinung spielen in der Mathematik eine große Rolle. Dort hat man z.B. häufig mit Gebilden zu tun, bei denen Elemente unterschiedlicher Herkunft auf entsprechend unterschiedliche Weise verknüpft werden, bei denen aber *dieselbe abstrakte Struktur* zum Vorschein kommt. "Abstrakt" heißt hier, dass von der speziellen Natur der verknüpften Elemente abzusehen ist.

■ Beispiel 1

Die Kleinsche Vierergruppe R_4 ist uns an früherer Stelle als Symmetriegruppe des Rechtecks begegnet. Sie kann aber auch auf ganz andere Weise realisiert werden, etwa als Menge $A = \{f_0,\ f_1,\ f_2,\ f_3\}$ von Funktionen, die durch $f_0(x) = x,\ f_1(x) = -x,\ f_2(x) = \frac{1}{x},\ f_3(x) = -\frac{1}{x}$ definiert und mittels $\circ$ (Verkettung) verknüpft werden.

Ein Vergleich der zugehörigen Verknüpfungstafeln zeigt, dass sie sich nur durch die Namen, nicht jedoch durch die gegenseitige Beziehung der verknüpften Elemente unterscheiden. Die betreffende Umbenennung beschreibt man dabei am besten als Abbildung $\gamma : A \longrightarrow R_4$ mit $\gamma(f_0) = e,\ \gamma(f_1) = m_1,\ \gamma(f_2) = m_2,\ \gamma(f_3) = h$.

γ ist bijektiv und leistet daher die Umbenennung in umkehrbar-eindeutiger Weise. Darüberhinaus – und das ist wesentlich – bildet γ auch die Struktur beider Gebilde aufeinander ab. So besteht in A etwa die Gleichung $f_2 \circ f_1 = f_3$. Wendet man nun γ auf die hier beteiligten Elemente einzeln an, so ergibt sich $h = \gamma(f_3) = \gamma(f_2) \circ \gamma(f_1) = m_1 \circ m_2$, also eine in R_4 gültige Gleichung.

■ 10.8.6. Definition

Eine bijektive Abbildung $\gamma : G \longrightarrow H$ zwischen zwei Gruppen G und H heißt Isomorphismus, wenn für alle $a, b \in G$ gilt: $\gamma(a\,b) = \gamma(a)\,\gamma(b)$. In diesem Fall heißen die beiden Gruppen zueinander isomorph (symbolisch: $G \cong H$).

Im Sinne dieser Definition ist die Abbildung γ aus Beispiel 1 ein Isomorphismus und sind die betreffenden Verknüpfungsgebilde A und R_4 isomorph. Die abstrakte mathematische Betrachtungsweise unterscheidet streng genommen nicht mehr zwischen den beiden Gebilden in ihrer konkreten Beschaffenheit; sie erscheinen als Verkörperungen ein- und derselben (abstrakten) Gruppe.

■ Beispiel 2

Außer der Kleinschen Vierergruppe gibt es noch eine andere (nicht zu R_4 isomorphe) Gruppe der Ordnung 4. Diese wird z.B. verkörpert durch die Restklassengruppe $(\mathbb{Z}_4, \oplus)$.

Eine Vierergruppe geometrischer Herkunft ist die Gesamtheit Δ_4 der Drehungen (einer Ebene E) um 90 °, 180 °, 270 ° und 0 ° (= 360 °). Vergleicht man die Verknüpfungstafeln, so wird auch die Isomorphie beider Gebilde unmittelbar deutlich: $(\mathbb{Z}_4, \oplus) \cong (\Delta_4, \circ)$. Als Isomorphismus bietet sich in natürlicher Weise die Abbildung an, die $k \in \mathbb{Z}_4$ die Drehung um $k \cdot 90$ ° zuordnet.

■ Bemerkung

Die hier aufgezeigte Strukturgleichheit von Drehungsgruppe und additiver Restklassengruppe kommt nicht von ungefähr. Man deute einmal Δ_4 als "Viertelstunden-Uhr"! Dann wird klar, dass das Rechnen mit Viertelstunden nichts anderes ist als Addition modulo 4. Die naturbedingte Periodizität von Zeit- und Kalenderrechnung ist ein kulturgeschichtlich bedeutsamer Hintergrund des Umgangs mit Restklassen.

Die vorangestellten Beispiele sollten nicht den Eindruck entstehen lassen, die Isomorphie zweier Gruppen wäre ihren Verknüpfungstafeln ohne weiteres zu entnehmen. So ist die prime Restklassengruppe $\mathbb{Z}_{10^*}$ ebenfalls zu Δ_4 isomorph, was anhand der Verknüpfungstafeln erst nach geeigneter Umstellung der Restklassen 1, 3, 7, 9 evident wird. Im Falle unendlicher (auch schon bei größeren endlichen) Gruppen verlieren solche Tafeln ohnehin ihren praktischen Wert. Isomorphieaussagen beruhen auf dem Nachweis eines Isomorphismus zwischen beiden Gebilden.

■ Beispiele

1. Sei m beliebig $\in \mathbb{Z}$; es gilt $\mathbb{Z} \cong m\,\mathbb{Z}$. Das zeigt der Isomorphismus $\gamma : \mathbb{Z} \longrightarrow m\,\mathbb{Z}$, definiert durch $\gamma(k) := m\,k$ für alle $k \in \mathbb{Z}$ (Bildung des m-fachen einer Zahl).

2. Es gilt $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. Ein geeigneter Isomorphismus ist die Exponentialfunktion $\exp(x) = e^x$ (e Eulersche Zahl), die $\mathbb{R}$ auf $\mathbb{R}^+$ bijektiv abbildet und für die gilt: $\exp(x + y) = \exp(x) \cdot \exp(y)$. Entsprechend vermittelt der natürliche Logarithmus als Umkehrabbildung von exp einen Isomorphismus von $(\mathbb{R}^+, \cdot)$ nach $(\mathbb{R}, +)$. Die bekannte Funktionalgleichung $\log(x \cdot y) = \log(x) + \log(y)$ bringt dies zum Ausdruck.