Algebra für Studierende der Informatik

Institut für Analysis
Andreas E. Schroth

Stand: 16.10.2000
Die jeweils aktuelle Version ist als Postscript-Datei erhältlich unter

`http://fb1.math.nat.tu-bs.de/~top/alginf/`

Inhaltsverzeichnis

Zen und die Kunst eine Gleichung zu lösen

Eines der Kultbücher meiner Jugend ist *Zen und die Kunst ein Motorrad zu warten* von Robert M. Pirsig. Dies ist ein Buch mit verschiedenen Handlungs- bzw. Erzählebenen. Die äußerste Handlungsebene beschreibt die Durchquerung der USA mit dem Motorrad von der Ost- zur Westküste. Die innerste Ebene ist ein philosophische Abhandlung. Die Abstraktheit dieser Abhandlung spiegelt den Verlauf der Reise wider. Die Reise startet auf Meereshöhe, erklimmt langsam die Höhen der Rocky Mountains um dann eher schnell wieder auf Meereshöhe herabzusteigen. Parallel dazu beginnen die philosophischen Betrachtungen mit Themen aus dem Alltag, schrauben sich dann in immer höhere Sphären hoch, erreichen einen Höhepunkt an Abstraktion und kommen schließlich auf die Bedeutung dieser Erörterungen im täglichen Leben zurück.

Diese Vorlesung ist so ähnlich aufgebaut. Allerdings starten wir nicht an der Ostküste, sondern, sagen wir mal, irgendwo in Iowa. Vielleicht am 5. Juni 1988, nach der Tagung *Algebraic Logic and Universal Algebra in Computer Science* in Ames, Iowa? Die Rockies sind zwar nicht mehr ganz so weit weg, aber wir fangen ganz unten, bei logischen Grundlagen und naiver Mengenlehre an. Dann kommt, mit den ersten Vorbergen, das Konzept der Relationen. Aber das ist nur eine kleine Übung zum Warmwerden. Es geht wieder herunter ins Tal, zu den natürlichen Zahlen. Von diesen ausgehend ersteigen wir über die ganzen Zahlen und die Polynome das erste Plateau, die Ringe. Ein abstraktes Konzept, das eine Vielzahl mathematischer Objekte umfaßt, drunter solch zentrale wie den Ring der ganzen Zahlen, den Polynomring und den Ring der linearen Abbildungen auf einem Vektorraum.

Für Hobbits sind Ringe vielleicht genug, für uns nicht. Wir ignorieren die speziellen Axiome, die für Ringe gelten und betrachten nur noch Mengen mit Operationen. Dieses abstakte Konzept eines algebraischen Systems ist der höchste Punkt der Reise. Aber selbst in diesem abstrakten Umfeld lassen sich zum Beispiel Morphismen und Quotienten definieren. In einem ständigen hoch und runter werden diese Konzepte eingeführt und dann an konkreten Beispielen demonstriert. Danach geht es langsam bergab, indem wir spezielle Strukturen, wie zum Beispiel Gruppen, genauer untersuchen.

Wenn wir Glück haben und uns beim Abstieg nicht verfahren, kommen wir vielleicht noch rechtzeitig in San Francisco an, um Eric Burdon den *Ring of Fire* besingen zu hören.

In *Zen und die Kunst ein Motorrad zu warten* geht es nicht um Zen und auch nur am Rande um das Warten von Motorrädern. Auch diese Vorlesung beschäftigt sich nicht mit Zen und das Lösen von Gleichungen wird nur indirekt behandelt.

Das Skript zur Vorlesung Algebra für Studierende der Informatik wird kapitelweise parallel zur Vorlesung entstehen.

Das Skript enthält neben den Sätzen und Beweisen der Vorlesung auch eine Vielzahl an erläuternden Bemerkungen sowie Testaufgaben. Manche der Bemerkungen weisen über das in der Vorlesung besprochenen hinaus und sollen interessierten Leserinnen und Lesern Ansatzpunkte für eine weitere Beschäftigung mit dem Stoff geben. Die Testaufgaben sind unterschiedlich schwierig. Sie sollen helfen, das vorgestellte Material zu verstehen und zu vertiefen. Einige dieser Aufgaben werden als Übungsaufgaben gestellt.

Da dies die erste Version des Skriptes ist, sind Fehler kaum zu vermeiden. Bitte teilen Sie mir mit, wenn Sie Fehler finden oder Anregungen haben. Am Ende des Semesters sollte eine korrigierte Version des Skripts erstellt sein.

KAPITEL 1

Mengen, Relationen und Abbildungen

In diesem Kapitel werden zunächst die Grundlagen der Logik und Mengenlehre vorgestellt. Speziell die Grundlagen der Logik werden nur kurz vorgestellt. Für eine eingehendere Untersuchung wird auf die Vorlesung Logik für Studierende der Informatik verwiesen. Nach der Mengenlehre werden Relationen eingeführt und untersucht. Dies ist ein erstaunlich vielseitiges Konzept. Verschiedene Methoden Relationen darzustellen werden behandelt und spezielle Typen von Relationen wie Äquivalenzrelationen, und Ordnungen werden untersucht. Abbildungen werden als ein spezieller Typ von Relationen eingeführt. Das Kapitel wird mit den Kardinalzahlen als eine Äquivalenzrelation auf Mengen von Mengen beendet.

1.1. Mengen

Dieser Abschnitt führt in die Grundlagen der Logik und der Mengenlehre ein. Wir werden in Kapitel 3 die hier vorgestellten Konzepte auch unter einem anderen Blickwinkel betrachten.

1.1 Logische Grundlagen. Aussagen sind entweder *wahr* (w) oder *falsch* (f). Aussagen, denen kein Wahrheitwert zugeordnet werden kann, sind nicht erlaubt. Für Aussagen gibt es die Operatoren

$\wedge$	*logisches und,*	$\Rightarrow$	*Implikation,*
$\vee$	*logisches oder,*	$\Longleftrightarrow$	*Äquivalenz,*
$\dot{\vee}$	*ausschließendes oder,*	$\neg$	*Negation.*

Sie werden wie folgt über Wahrheitstafeln definiert, dabei sind A und B Aussagenvariablen.

A	B	$A \wedge B$	$A \vee B$	$A \dot{\vee} B$	$A \Rightarrow B$	$A \Longleftrightarrow B$	$\neg A$
w	w	w	w	f	w	w	f
w	f	f	w	w	f	f	f
f	w	f	w	w	w	f	w
f	f	f	f	f	w	w	w

1.2 Mengen. Mengen sind eine Ansammlung von Objekten oder Elementen. Mengen können direkt durch explizite Angabe ihrer Elemente oder durch Bedingungen, die die Elemente erfüllen müssen, angegeben werden.

1.3 Beispiele:

1. $\{a, b, c\}$, $\{1, 2, 3, \ldots, 7482\}$, $\{0, 1, 2, 3, \ldots\}$ sind direkte Angaben.
2. Sei $A(x)$ eine Aussage, die von der Variablen x abhängt. Dann ist $\{x \mid A(x)\}$ die Menge der x, für die die Aussage $A(x)$ wahr ist.

1.4 Bemerkung:

1. Elemente einer Menge müssen nicht vom selben Typ sein. So ist zum Beispiel $\{1, \{1\}, \diamond, ?, A\}$ eine Menge.
2. Wie oft und in welcher Reihenfolge Elemente bei der Beschreibung einer Menge angegeben werden ist unerheblich. Zum Beispiel gilt $\{1, 2\} = \{2, 1\} = \{1, 2, 1, 1, 2, 1, 1, 1, 2, 2\}$.
3. Bei der Angabe einer Menge durch Aussagen ist Vorsicht geboten. Zum Beispiel führt die Konstruktion $R := \{x \mid x \notin x\}$ zu Widersprüchen (Das Russelsche Paradoxon).

1.5 Einige spezielle Mengen:

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$	*ganze Zahlen*
$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$	*natürliche Zahlen*
$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ und } n \neq 0\}$	*rationale Zahlen*
$\mathbb{R}$	*reelle Zahlen*
$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$	*komplexe Zahlen*

1.6 Bezeichnung: Für eine Menge A und ein Objekt x schreiben wir:

$$x \in A \ :\Leftrightarrow \ x \text{ ist Element von A,}$$
$$x \notin A \ :\Leftrightarrow \ x \text{ ist nicht Element von A.}$$

1.7 Definition: Seien A und B zwei Mengen.

1. Die Menge A ist eine *Teilmenge* von B, geschrieben $A \subset B$, wenn $x \in A$ stets $x \in B$ impliziert.
2. Es gilt $A = B$ genau dann, wenn $A \subset B$ und $B \subset A$ gilt.

1.8 Bemerkung: Für Mengen beinhaltet $A \subset B$ den Fall $A = B$. Für Zahlen hingegen erzwingt $a < b$ stets $a \neq b$ (vgl. 1.44).

1.9 Definition: Die *leere Menge* ist die Menge, die keine Elemente enthält. Sie wird mit $\emptyset$ oder $\{\}$ bezeichnet.

1.10 Lemma: *Die leere Menge ist Teilmenge jeder Menge.*

Beweis: Angenommen, es gibt eine Menge A mit $\emptyset \not\subset A$. Dann gibt es ein x mit $x \in \emptyset$ und $x \notin A$. Doch $x \in \emptyset$ widerspricht der Definition der leeren Menge. Damit gilt für jede Menge A stets $\emptyset \subset A$. □

1.11 Lemma: *Die leere Menge ist eindeutig.*

Beweis: Seien $\emptyset$ und $\emptyset'$ zwei leere Mengen. Mit Lemma 1.10 gilt $\emptyset \subset \emptyset'$ aber auch $\emptyset' \subset \emptyset$. Nach Definition bedeutet dies $\emptyset = \emptyset'$. □

Für Mengen können die Operationen ‚Vereinigung', ‚Schnitt' und ‚Komplement' definiert werden. Sie hängen eng mit den logischen Operationen zusammen.

1.12 Definition: Für zwei Mengen A und B sei:

$$A \cup B := \{x \mid x \in A \vee x \in B\} \qquad \textit{Vereinigung}$$
$$A \cap B := \{x \mid x \in A \wedge x \in B\} \qquad \textit{Schnitt}$$
$$A \setminus B := \{x \mid x \in A \wedge x \notin B\} \qquad \textit{Komplement von } B \textit{ in } A$$

Neben diesen Operationen gibt es noch weitere Konstruktionen, um aus Mengen neue Mengen zu gewinnen.

1.13 Definition: Für eine Menge A ist

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

die *Potenzmenge* von A. Die Potenzmenge von A ist also die Menge aller Teilmengen von A.

1.14 Definition: Für zwei Mengen A und B ist

$$A \times B := \{(a, b) \mid a \in A \text{ und } b \in B\}$$

das *Produkt* der Mengen A und B. Dabei ist (a, b) ein *Paar* oder eine *geordnete Menge*.

Paare können durch

$$(a, b) \sim \{\{a\}, \{a, b\}\}$$

rein mengentheoretisch beschrieben werden.

Durch

$$A_1 \times A_2 \times \cdots \times A_n \times A_{n+1} := (A_1 \times A_2 \times \cdots \times A_n) \times A_{n+1}$$

wird induktiv das Produkt endlich vieler Mengen definiert.

Für eine Menge A gilt:

$$A^2 := A \times A,$$
$$A^{n+1} := A^n \times A, \qquad n \in \mathbb{N},\ n \geq 2.$$

Diese Definition des Produkts von Mengen funktioniert für höchstens abzählbar viele Mengen. Über Abbildungen kann aber auch das Produkt beliebig vieler Mengen definiert werden (vgl. Definition 1.62).

Mitunter ist es sinnvoll, zwei Mengen als disjunkt zu betrachten, selbst wenn sie gemeinsame Elemente haben. Bereits die Definition des Graphen einer Relation in 1.22 bietet hierfür ein Beispiel. Die Idee ist, Kopien der beteiligten Mengen zu betrachten.

1.15 Definition: Für zwei Mengen A und B ist

$$A \dot\cup B := (A \times \{0\}) \cup (B \times \{1\})$$

die *disjunkte Vereinigung* von A und B.

Anstelle von 0 und 1 können beliebige verschiedene Objekte verwendet werden.

1.16 Testfragen:

1. Ist der Ausdruck „Diese Aussage ist falsch“ eine erlaubte Aussage?
2. Beschreiben Sie das Element $(1, 1, 0, 1) \in \{0, 1\}^4$ rein mengentheoretisch.

1.2. Relationen

Relationen sind ein sehr vielseitiges Konzept. Von besonderem Interesse sind Relationen mit bestimmten Eigenschaften. Wir werden Äquivalenzrelationen, Ordnungen und Abbildungen als spezielle Relationen kennenlernen.

1.17 Definition: Seien A und B zwei Mengen.

1. Eine *Relation* ρ von A nach B ist eine Teilmenge $\rho \subset A \times B$.
2. Eine Relation ρ auf A ist eine Teilmenge $\rho \subset A \times A$, d.h. eine Relation von A nach A.

1.18 Bezeichnung: Für eine Relation $\rho \subset A \times B$ und $(a, b) \in A \times B$ gilt:

$$a \ \rho \ b \ :\Leftrightarrow \ (a, b) \in \rho,$$
$$a \not\rho \ b \ :\Leftrightarrow \ (a, b) \notin \rho.$$

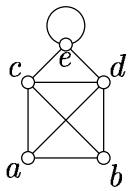
1.19 Beispiele:

1. Die gewöhnliche kleiner-gleich Beziehung $\leq$ ist eine Relation auf $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ und $\mathbb{N}$.
2. Für jede Menge M ist $\subset$ eine Relation auf der Potenzmenge $\mathcal{P}(M)$.
3. Für jede Menge M ist $\in$ eine Relation von M nach $\mathcal{P}(M)$.
4. Sei A die Menge der Java-Befehle und B die Menge der Java-Programme. Dann definiert „wird verwendet in“ eine Relation von A nach B.
5. Sei S die Menge aller Filmschauspielerinnen und Filmschauspieler. Dann wird durch „sind im selben Film aufgetreten“ eine Relation auf S definiert.

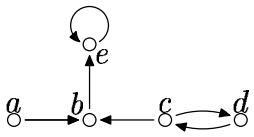
1.20 Definition: Ein *Graph* ist ein Paar $(\mathcal{E}, \mathcal{K})$ mit Eckenmenge $\mathcal{E}$ und Kantenmenge $\mathcal{K} \subset \{\{a, b\} \mid a, b \in \mathcal{E}\}$. Üblicherweise wird ein Graph dargestellt, indem die Ecken als beschriftete Punkte und die Kanten als Verbindungsstrecken gezeichnet werden.

Ein *gerichteter Graph* ist ein Paar $(\mathcal{E}, \mathcal{K})$ mit Eckenmenge $\mathcal{E}$ und Kantenmenge $\mathcal{K} \subset \mathcal{E}^2$. Üblicherweise wird ein gerichteter Graph dargestellt, indem die Ecken als beschriftete Punkte und die Kanten als Pfeile (gerichtete Strecken) gezeichnet werden.

1.21 Beispiele:



Graph



gerichteter Graph

Für den Graph gilt:

$$\mathcal{E} = \{a, b, c, d, e\}$$
$$\mathcal{K} = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{c, e\}, \{d, e\}, \{e\}\}.$$

Für den gerichteten Graph gilt:

$$\mathcal{E} = \{a, b, c, d, e\}$$
$$\mathcal{K} = \{(a, b), (b, e), (c, b), (c, d), (d, c), (e, e)\}.$$

1.22 Definition: Der *Graph* Γ_ρ *einer Relation* ρ von A nach B ist der gerichtete Graph mit Eckenmenge $A \dot\cup B$ und Kantenmenge ρ. Das heißt, es gibt genau dann eine Kante von $a \in A$ nach $b \in B$, wenn $(a, b) \in \rho$ gilt.

Der Graph Γ_ρ einer Relation ρ auf A ist der gerichtete Graph mit Eckenmenge A und Kantenmenge ρ.

1.23 Definition: Die *Matrix* $R_\rho = (r^\rho_{a,b})$ *einer Relation* ρ von A nach B ist die Matrix mit den Einträgen

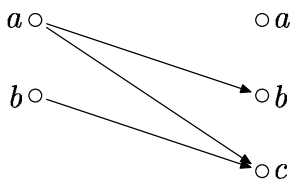
$$r^\rho_{a,b} := \begin{cases} 1, & \text{falls } a \;\rho\; b, \\ 0, & \text{sonst.} \end{cases}$$

Das heißt, die Zeilen werden durch A und die Spalten durch B indiziert. In Zeile $a \in A$ und Spalte $b \in B$ steht genau dann der Eintrag 1, wenn $a \;\rho\; b$ gilt. Alle anderen Einträge sind 0.

Oft wird die Matrix einer Relation in Tabellenform geschrieben in der zusätzlich die Spalten- und Zeilenindizes angegeben sind.

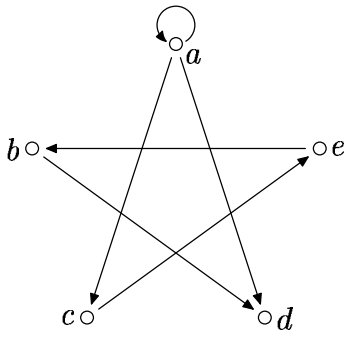
1.24 Beispiele:

1. Für $A = \{a, b\}$, $B = \{a, b, c\}$ mit der Relation $\rho = \{(a, c), (a, b), (b, c)\}$ haben Graph und Matrix folgende Gestalt:



	a	b	c
a	0	1	1
b	0	0	1

2. Die Relation $\rho = \{(a,a),(a,c),(a,d),(b,d),(c,e),(e,b)\}$ auf der Menge $A = \{a,b,c,d,e\}$ hat folgenden Graph und Matrix:



	a	b	c	d	e
a	1	0	1	1	0
b	0	0	0	1	0
c	0	0	0	0	1
d	0	0	0	0	0
e	0	1	0	0	0

1.25 Testfrage: Fassen sie den gerichteten Graphen aus Beispiel 1.21 als den Graph einer Relation auf der Menge $\{a,b,c,d,e\}$ auf. Wie lautet die zugehörige Matrix?

Da Relationen Mengen sind, können die Mengenoperationen auf Relationen angewendet werden. Daneben gibt es noch andere Operationen, die sich aus der speziellen Gestalt von Relationen ergeben.

1.26 Definition: Sei $\rho \subset A \times B$ eine Relation. Die zu ρ *inverse Relation* $\tilde{\rho} \subset B \times A$ ist definiert durch

$$b \,\tilde{\rho}\, a \;:\Leftrightarrow\; a \,\rho\, b.$$

1.27 Beispiel: Die zu $\leq$ bzw. $\subset$ inversen Relationen sind $\geq$ bzw. $\supset$.

1.28 Bemerkungen:

1. Offensichtlich gilt $\tilde{\tilde{\rho}} = \rho$.
2. Der Graph $\Gamma_{\tilde{\rho}}$ ergibt sich aus dem Graphen Γ_ρ, indem alle Pfeile umgedreht werden.
3. Transponieren der Matrix von ρ liefert die Matrix von $\tilde{\rho}$.

1.29 Definition: Für Relationen $\rho \subset A \times B$ und $\sigma \subset B \times C$ ist die *Komposition* $\rho\sigma \subset A \times C$ definiert durch

$$a \,\rho\sigma\, c \;:\Leftrightarrow\; \exists b \in B\colon a \,\rho\, b \,\sigma\, c.$$

Dabei ist $a \,\rho\, b \,\sigma\, c$ eine Abkürzung für $a \,\rho\, b \wedge b \,\sigma\, c$.

Offensichtlich ist die Komposition zweier Relationen wieder eine Relation

Das Inverse der Komposition zweier Relationen ist die Komposition der inversen in umgedrehter Reihenfolge. Dieses Verhalten erinnert (nicht zufällig) an das Verhalten von Transponieren und Multiplizieren bei Matrizen.

1.30 Satz: *Für Relationen $\rho \subset A \times B$ und $\sigma \subset B \times C$ gilt*

$$\widetilde{\rho\sigma} = \tilde{\sigma}\tilde{\rho}.$$

Beweis: Für $(a, c) \in A \times C$ ist $(c, a) \in \widetilde{\rho\sigma} \iff (c, a) \in \tilde{\sigma}\tilde{\rho}$ zu zeigen. Es gilt:

$$\begin{aligned}
c\ \widetilde{\rho\sigma}\ a &\iff a\ \rho\sigma\ c && \text{(Definition der Inversen)}\\
&\iff \exists b \in B\colon a\ \rho\ b\ \sigma\ c && \text{(Definition der Komposition)}\\
&\iff \exists b \in B\colon c\ \tilde{\sigma}\ b\ \tilde{\rho}\ a && \text{(Definition der Inversen)}\\
&\iff c\ \tilde{\sigma}\tilde{\rho}\ a && \text{(Definition der Komposition)}
\end{aligned}$$

□

1.31 Testfrage: Sei ρ die Relation aus Beispiel 1.24.2. Bestimmen Sie den Graphen von $\rho\rho$ direkt aus dem Graphen von ρ.

1.32 Definition: Sei ρ eine Relation auf einer Menge A.

1. ρ ist *reflexiv*, falls $a\ \rho\ a$ für jedes $a \in A$ gilt.
2. ρ ist *symmetrisch*, falls aus $a\ \rho\ b$ stets $b\ \rho\ a$ folgt.
3. ρ ist *antisymmetrisch*, falls aus $a\ \rho\ b$ und $b\ \rho\ a$ stets $a = b$ folgt.
4. ρ ist *transitiv*, falls aus $a\ \rho\ b$ und $b\ \rho\ c$ stets $a\ \rho\ c$ folgt.

1.33 Bemerkung: Für eine Relation ρ auf A gilt:

$$\begin{aligned}
\rho \text{ ist reflexiv} &\iff \{(a, a) \mid a \in A\} \subset \rho,\\
\rho \text{ ist symmetrisch} &\iff \rho = \tilde{\rho},\\
\rho \text{ ist antisymmetrisch} &\iff \rho \cap \tilde{\rho} \subset \{(a, a) \mid a \in A\},\\
\rho \text{ ist transitiv} &\iff \rho\rho \subset \rho.
\end{aligned}$$

1.34 Testfrage: Untersuchen Sie die Relationen aus Beispiel 1.19 auf Reflexivität, Symmetrie, Antisymmetrie und Transitivität.

1.35 Definition: Eine Relation auf einer Menge A ist genau dann eine *Äquivalenzrelation* wenn sie reflexiv, symmetrisch und transitiv ist.

Für eine Äquivalenzrelation $\equiv$ auf A und ein Element $a \in A$ heißt

$$[a]_{\equiv} := \{b \in A \mid b \equiv a\}$$

die *Äquivalenzklasse* von a (bezüglich $\equiv$). Ist klar, um welche Äquivalenzrelation es sich handelt, so wird $[a]$ statt $[a]_\equiv$ geschrieben.

Die Menge der Äquivalenzklassen einer Äquivalenzrelation $\equiv$ auf A wird mit $A/_\equiv$ bezeichnet, d.h.

$$A/_\equiv = \{[a] \mid a \in A\}.$$

Die Menge $A/_\equiv$ heißt der *Quotient von A nach $\equiv$* oder auch A *modulo* $\equiv$.

1.36 Lemma: *Für eine Äquivalenzrelation $\equiv$ auf A und $a, b \in A$ gilt*

$$[a] = [b] \iff a \equiv b.$$

Beweis: Da $\equiv$ reflexiv ist, gilt $b \equiv b$, also $b \in [b]$. Daher folgt aus $[a] = [b]$ auch $b \in [a]$, d.h. $b \equiv a$. Wegen der Symmetrie gilt also $a \equiv b$.

Gilt $a \equiv b$ und $c \in [a]$ so folgt aus der Transitivität $c \equiv b$, also $c \in [b]$. Aus $a \equiv b$ folgt daher $[a] \subset [b]$. Vertauschen von a und b zeigt, daß $a \equiv b$ auch $[b] \subset [a]$ impliziert. Somit folgt $[a] = [b]$ aus $a \equiv b$. □

1.37 Beispiele:

1. Für jede Menge A ist die Gleichheit $=$ eine Äquivalenzrelation auf A. Für jedes Element $a \in A$ gilt $[a] = \{a\}$.
2. Für jede Menge A ist $u := A^2$ eine Äquivalenzrelation auf A. Für jedes Element $a \in A$ gilt $[a] = A$.
3. Sei G die Mengen der Graden in $\mathbb{R}^2$ und $\parallel$ die Parallelrelation, d.h. für $g, h \in G$ gilt $g \parallel h$ falls g und h sich nicht schneiden oder $g = h$ gilt. Dann ist $\parallel$ eine Äquivalenzrelation auf G.
4. Für $m \in \mathbb{N} \setminus \{0\}$ wird auf $\mathbb{Z}$ die *Äquivalenzrelation mod m*, bezeichnet $\equiv_m$, durch

   $$a \equiv_m b \ :\Leftrightarrow\ \exists k \in \mathbb{Z} \colon a - b = km$$

   definiert. Dies ist in der Tat eine Äquivalenzrelation. Die Reflexivität folgt aus $a - a = 0 \cdot m$. Aus $a - b = km$ folgt $b - a = (-k)m$. Das zeigt die Symmetrie. Gilt $a - b = km$ und $b - c = lm$, so folgt $a - c = (k + l)m$. Dies zeigt die Transitivität.

   Der Quotient $\mathbb{Z}/_{\equiv_m}$ wird üblicherweise mit $\mathbb{Z}_m$ bezeichnet.
5. Sei $X := \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ mit der Relation $\sim$ definiert durch

   $$(a, b) \sim (c, d) \ :\Leftrightarrow\ ad = bc.$$

   Dann ist $\sim$ eine Äquivalenzrelation und $X/_\sim$ liefert $\mathbb{Q}$.

1.38 Definition: Eine *Partition* Π einer Menge A ist eine Aufteilung von A in paarweise disjunkte, nichtleere Teilmengen. Genauer, $\Pi = \{\pi_\alpha \mid \alpha \in I\}$, wobei I eine Indexmenge ist, mit

1. $\emptyset \notin \Pi$,
2. $\bigcup_{\alpha \in I} \pi_\alpha = A$,
3. $\pi_\alpha \cap \pi_\beta \neq \emptyset \Rightarrow \pi_\alpha = \pi_\beta$.

Beachten Sie, daß anders als bei der Aufteilung einer Festplatte, die Aufteilung an sich und nicht die einzelnen Teile der Aufteilung Partition heißt.

1.39 Beispiel: $\{\{1,2\},\{3,6\},\{4,5\}\}$ ist eine Partition von $\{1,2,3,4,5,6\}$.

1.40 Satz: *Für jede Äquivalenzrelation* $\equiv$ *auf einer Menge* A *ist*

$$\Pi_\equiv := {}^{A}\!/_{\equiv} = \{[a] \mid a \in A\}$$

eine Partition von A.

Beweis: Die Reflexivität von $\equiv$ impliziert $a \in [a]$ für jedes $a \in A$. Daraus folgt $[a] \neq \emptyset$ für jedes $a \in A$ und $\bigcup_{a \in A}[a] = A$.

Sei nun $a, b \in A$ mit $[a] \cap [b] \neq \emptyset$. Dann gibt es ein c mit $c \in [a] \cap [b]$. Das bedeutet $c \equiv a$ und $c \equiv b$. Anwendung der Symmetrie liefert daraus $a \equiv c \equiv b$, woraus mit der Transitivität $a \equiv b$ folgt. Wegen Lemma 1.36 ist dies gleichbedeutend mit $[a] = [b]$. □

Beachten Sie, daß ein und die selbe Menge einer Partition mit verschiedenen Indizes versehen werden kann, da es bei Mengen unerheblich ist, wie oft ein Element genannt wird.

In der eben ausgeführten Konstruktion ist A die Indexmenge.

Die Konstruktion einer Partition durch eine Äquivalenzrelation kann rückgängig gemacht werden.

1.41 Satz: *Ist* $\Pi = \{\pi_\alpha \mid \alpha \in I\}$ *eine Partition einer Menge* A, *so wird durch*

$$a \equiv_\pi b \;:\Leftrightarrow\; \exists \alpha \in I\colon \{a, b\} \subset \pi_\alpha$$

eine Äquivalenzrelation $\equiv_\pi$ *auf* A *definiert, und es gilt* $\Pi = {}^{A}\!/_{\equiv_\pi}$.

Beweis: Es ist sofort einzusehen, daß $\equiv_\pi$ eine Äquivalenzrelation ist. Zu zeigen ist daher nur $\Pi = {}^{A}\!/_{\equiv_\pi}$. Sei $a \in A$. Dann gibt es ein $\alpha \in I$ mit $a \in \pi_\alpha$. Die Behauptung ist beweisen, wenn gezeigt ist, daß $[a] = \pi_\alpha$ gilt.

Sei $b \in [a]$, also $b \equiv_\pi a$. Dann gibt es ein $\beta \in I$ mit $\{a, b\} \subset \pi_\beta$. Wegen $a \in \pi_\alpha \cap \pi_\beta$ gilt $\pi_\alpha = \pi_\beta$, also auch $b \in \pi_\alpha$. Dies zeigt $[a] \subset \pi_\alpha$.

Sei $b \in \pi_\alpha$. Dann gilt $a \equiv_\pi b$, also auch $b \in [a]$. Dies zeigt $\pi_\alpha \subset [a]$, also mit dem oben gezeigten $[a] = \pi_\alpha$. □

Die Sätze 1.40 und 1.41 zeigen, daß Partitionen und Äquivalenzrelationen gleichwertige Konzepte sind.

1.42 Definition: Eine Menge A mit einer reflexiven, antisymmetrischen und transitiven Relation $\leq$ heißt *teilweise geordnet*. Das heißt, für alle $x, y, z \in A$ gilt:

1. $x \leq x$,
2. $x \leq y \wedge y \leq x \Rightarrow x = y$,
3. $x \leq y \wedge y \leq z \Rightarrow x \leq z$.

Eine teilweise geordnete Menge $(A, \leq)$ heißt *total geordnet*, falls für $x, y \in A$ immer $x \leq y$ oder $y \leq x$ gilt, d.h., falls sich je zwei Elemente von A vergleichen lassen. Total geordnete Mengen heißen auch *Ketten*.

1.43 Beispiele:

1. Die ganzen Zahlen $\mathbb{Z}$ mit der gewöhnlichen ‚kleiner-gleich-Beziehung' sind total geordnet.
2. Für jede Menge M ist $(\mathcal{P}(M), \subset)$ eine teilweise geordnete Menge. Hat M mindestens zwei verschiedene Elemente, etwa a und b, so ist $(\mathcal{P}(M), \subset)$ nicht total geordnet, da weder $\{a\} \subset \{b\}$ noch $\{b\} \subset \{a\}$ gilt.
3. Die *Teilbarkeitsrelation* $\mid$ auf den positiven ganzen Zahlen $P := \mathbb{N} \setminus \{0\}$ wird definiert durch

$$a \mid b \;:\Leftrightarrow\; \exists k \in P\colon b = ka,$$

d.h. $a \mid b$ steht für „a teilt b". Dann ist $(P, \mid)$ eine teilweise geordnete Menge.

Die Reflexivität folgt aus $a = 1 \cdot a$. Gilt $a \mid b$ und $b \mid a$, so gibt es $k, l \in P$ mit $b = ka$ und $a = lb$. Daraus folgt $b = klb$, was nur für $k = l = 1$ möglich ist. Dies zeigt die Antisymmetrie.

Gilt $a \mid b$ und $b \mid c$, so gibt es $k, l \in P$ mit $b = ka$ und $c = lb$. Daraus folgt $c = kla$, also $a \mid c$. Dies zeigt die Transitivität.

Wegen $2 \nmid 3$ und $3 \nmid 2$ ist $(P, \mid)$ keine total geordnete Menge.

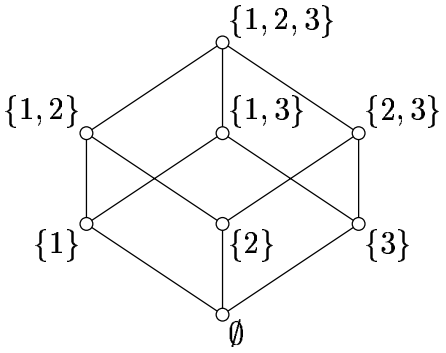
1.44 Bezeichnung: In einer teilweise geordneten Menge $(A, \leq)$ ist die Relation $<$ wie üblich definiert durch

$$a < b \;:\Leftrightarrow\; a \leq b \wedge a \neq b.$$

1.45 Definition: Sei $(A, \leq)$ eine teilweise geordnete Menge und $a, b \in A$. Dann *überlagert* b das Element a, wenn $a < b$ gilt und es kein $c \in A$ mit $a < c < b$ gibt.

Das *Diagramm* der teilweise geordnete Menge $(A, \leq)$ ist der gerichtete Graph mit Eckenmenge A und Kantenmenge $\{(a, b) \mid b \text{ überlagert } a\}$. Üblicherweise wird die Richtung einer Kante nicht mit Pfeilen angegeben, sondern die Ecken werden so angeordnet, daß die Richtung einer Kante immer von unten nach oben zeigt.

1.46 Beispiel: Das Diagramm von $(\mathcal{P}(\{1,2,3\}), \subset)$ hat folgende Gestalt:



1.47 Testfragen:

1. Warum kann das Diagramm einer teilweise geordneten Menge immer gezeichnet werden (solange die Menge endlich ist), d.h. warum können die Punkte wie in Definition 1.45 angedeutet plaziert werden?
2. Wie sehen die Diagramme der teilweise geordneten Mengen aus Beispiel 1.43.1 und 3 aus?

1.48 Definition: Sei $(A, \leq)$ eine teilweise geordnete Menge und $X \subset A$.

1. $x \in X$ ist ein *maximales Element* von X, falls es kein $y \in X$ mit $x < y$ gibt.
2. $x \in X$ ist ein *minimales Element* von X, falls es kein $y \in X$ mit $y < x$ gibt.
3. $x \in X$ ist ein *größtes Element* von X, falls $y \leq x$ für jedes $y \in X$ gilt.
4. $x \in X$ ist ein *kleinstes Element* von X, falls $x \leq y$ für jedes $y \in X$ gilt.
5. $a \in A$ ist eine *obere Schranke* von X, falls $x \leq a$ für jedes $x \in X$ gilt.
6. $a \in A$ ist eine *untere Schranke* von X, falls $a \leq x$ für jedes $x \in X$ gilt.
7. $a \in A$ ist eine *größte untere Schranke*, falls a ein größtes Element in der Menge der unteren Schranken von X ist.
8. $a \in A$ ist eine *kleinste obere Schranke*, falls a ein kleinstes Element in der Menge der oberen Schranken von X ist.

1.49 Beispiel: Sei $X = \{\{2\}, \{1,2\}, \{2,3\}\} \subset A := \mathcal{P}(\{1,2,3\})$. Dann sind $\{1,2\}$ und $\{2,3\}$ maximale Elemente von X, aber X hat kein größtes Element. Das

kleinste Element von X ist $\{2\}$. Untere Schranken von X sind $\{2\}$ und $\emptyset$, davon ist $\{2\}$ die größte. Die einzige obere Schranke ist $\{1,2,3\}$.

1.50 Testfrage: Wie erkennen Sie maximale, minimale, größte und kleinste Elemente im Diagramm einer teilweise geordneten Menge?

1.51 Definition: Für eine teilweise geordnete Menge $(A, \leq)$ ist $(A, \geq)$ die zugehörige *duale teilweise geordnete Menge*. Dabei ist $\geq$ die zu $\leq$ inverse Relation.

1.52 Bemerkung: Das Diagramm von $(A, \leq)$ horizontal gespiegelt, d.h. auf den Kopf gestellt, ergibt ein Diagramm von $(A, \geq)$.

1.53 Definition: Aus einer Aussage S über eine teilweise geordnete Menge $(A, \leq)$ wird die *duale Aussage* $\tilde{S}$ gewonnen, in dem alle $\leq$ durch $\geq$ und alle $\geq$ durch $\leq$ ersetzt werden.

Offensichtlich gilt $\tilde{\tilde{S}} = S$.

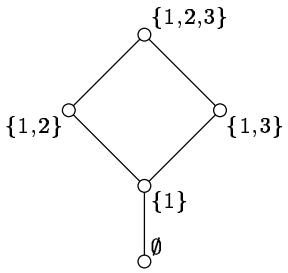
Da $\tilde{S}$ und $(A, \geq)$ auf die gleiche Art und Weise aus S bzw. $(A, \leq)$ gewonnen werden, folgt unmittelbar folgendes Resultat.

1.54 Lemma: *Ist S eine wahre Aussage über eine teilweise geordnete Menge $(A, \leq)$, so ist $\tilde{S}$ eine wahre Aussage über $(A, \geq)$.*

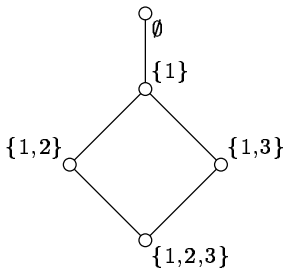
1.55 Beispiel: Sei

$$A := \{\emptyset, \{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}\},$$
$$X := \{\{1,2\}, \{1,3\}\} \subset A.$$

Wir betrachten zunächst die teilweise geordnete Menge $(A, \subset)$. Das heißt, die



$(A, \subset)$



$(A, \supset)$

Ordnungsrelation $\leq$ entspricht der Teilmengenrelation $\subset$. Für jedes $x \in X$ gilt $\{1\} \subset x$, also auch $\{1\} \leq x$.

Die duale geordnete Menge ist $(A, \supset)$. Die Ordnungsrelation $\leq$ entspricht also der Obermengenrelation $\supset$. Für jedes $x \in X$ gilt $x \supset \{1\}$, also auch $\{1\} \geq x$.

Die Aussage $S = \forall x \in X\colon \{1\} \leq x$ ist damit wahr in $(A, \subset)$. Die duale Aussage $\tilde{S} = \forall x \in X\colon \{1\} \geq x$ ist wahr in der dualen geordneten Menge $(A, \supset)$.

1.56 Satz (Dualitätsprinzip): *Ist T eine Aussage, die für alle teilweise geordnete Mengen wahr ist, so ist die duale Aussage $\tilde{T}$ ebenfalls für alle teilweise geordnete Mengen wahr.*

Beweis: Angenommen $\tilde{T}$ gilt nicht für alle teilweise geordnete Mengen. Dann gibt es eine teilweise geordnete Menge $(A, \leq)$, für die $\tilde{T}$ falsch ist. Wegen $\tilde{\tilde{T}} = T$ und Lemma 1.54 ist T keine wahre Aussage über die teilweise geordnete Menge $(A, \geq)$. Dies widerspricht den Annahmen. □

Die folgenden Aussagen sollen das Dualitätsprinzip illustrieren.

1.57 Satz: *Ist $(A, \leq)$ eine teilweise geordnete Menge, so hat jede Teilmenge $X \subset A$ höchstens ein kleinstes Element.*

Beweis: Angenommen l, l' sind kleinste Elemente von X. Dann gilt $l \leq l'$ und $l' \leq l$, da beides auch Elemente von X sind. Doch dann gilt $l = l'$. □

Mit Satz 1.56 folgt aus diesem Resultat unmittelbar der duale Satz.

1.58 Satz: *Ist $(A, \leq)$ eine teilweise geordnete Menge, so hat jede Teilmenge $X \subset A$ höchstens ein größtes Element.*

1.59 Definition: Für Elemente x, y einer teilweise geordneten Menge ist

$$x \vee y \text{ die kleinste obere Schranke von } \{x, y\},$$
$$x \wedge y \text{ die größte untere Schranke von } \{x, y\},$$

falls die größte untere oder kleinste obere Schranke existieren.

Das Element $x \wedge y$ heißt *Schnitt*, das Element $x \vee y$ *Verbindung* von x und y.

1.60 Definition: Eine *Verband* ist eine teilweise geordnete Menge, in der für je zwei Elemente Schnitt und Verbindung existieren.

1.61 Beispiel:

1. Jede total geordnete Menge ist ein Verband. Es gilt $x \vee y = \max\{x, y\}$ und $x \wedge y = \min\{x, y\}$.

2. Für jede Menge M ist $(\mathcal{P}(M), \subset)$ ein Verband. Es gilt $x \vee y = x \cup y$ und $x \wedge y = x \cap y$.
3. Die Teilbarkeitsrelation auf $P = \mathbb{N} \setminus \{0\}$ liefert einen Verband. Für $x, y \in P$ ist $x \vee y$ das kleinste gemeinsame Vielfache und $x \wedge y$ der größte gemeinsame Teiler von x und y.

1.3. Abbildungen

Bis jetzt wurden eingehend Relationen untersucht. Es bietet sich daher an, Abbildungen als spezielle Relationen einzuführen. Diese Definition ist sehr elegant, wenngleich etwas gewöhnungsbedürftig.

1.62 Definition: Eine *Abbildung* oder *Funktion f von A nach B* ist eine Relation $f \subset A \times B$ mit:

1. $\forall a \in A \, \exists b \in B \colon (a, b) \in f$,
   das heißt, jedes Element von A hat ein Bild.
2. $(a, b) \in f \wedge (a, b') \in f \Rightarrow b = b'$,
   das heißt, jedes Element von A hat höchstens ein Bild.

Für eine Abbildung f von A nach B schreiben wir $f \colon A \to B$. Für $a \in A$ bezeichnet $f(a)$ das *Bild von a unter f*, das heißt das Element b von B mit $(a, b) \in f$. Für $S \subset A$ ist $f(S) := \{f(s) \mid s \in S\}$ das Bild der Teilmenge S unter f.

Die Menge aller Abbildungen von A nach B wird mit B^A bezeichnet.

1.63 Bemerkung: Eine Abbildung $f \colon A \to B$ aufgefaßt als Relation entspricht dem Graphen der Funktion in der z.B. aus der Analysis bekannten Sichtweise.

Die Matrix einer Abbildung (aufgefaßt als Relation), liefert die graphische Darstellung einer Funktion, wenn die Einsen durch einen Punkt und die Nullen durch nichts ersetzt werden. Diese Sichtweise verwenden die meisten Programme zum Plotten von Funktionen.

1.64 Testfrage: Überzeugen Sie sich davon, daß für $n \in \mathbb{N} \setminus \{0\}$ und eine Menge A das Produkt A^n gemäß Definition 1.14 mit der Menge $A^{\{1,\dots,n\}}$ identifiziert werden kann.

1.65 Definition: Eine Abbildung $f \colon A \to B$ heißt:

1. *injektiv*, falls $f(a) = f(a')$ stets $a = a'$ impliziert,
2. *surjektiv*, falls für jedes $b \in B$ ein $a \in A$ mit $f(a) = b$ existiert,
3. *bijektiv*, falls f injektiv und surjektiv ist.

1.66 Testfrage: Wie kann Injektivität, Surjektivität und Bijektivität einer Abbildung am Graphen und an der Matrix der Abbildung, aufgefaßt als Relation, abgelesen werden?

1.67 Definition: Für Abbildungen $f\colon A \to B$ und $g\colon B \to C$ ist die *Komposition* oder *Hintereinanderausführung* $g \circ f\colon A \to C$ von f und g definiert durch $g \circ f(x) := g(f(x))$.

1.68 Bemerkung: Vorsicht, hier gibt es (historisch bedingt) eine gemeine Falle. Für zwei Abbildungen $f\colon A \to B$ und $g\colon B \to C$ schreiben wir $g \circ f$ für die Komposition als Abbildungen aber fg für die Komposition als Relationen, obwohl beides das gleiche liefert. (Wenn Sie dem ausweichen wollen, müssen Sie Abbildungen von rechts statt von links wirken lassen. Das heißt, Sie schreiben x^f statt $f(x)$. Denn dann gilt $x^{fg} = (x^f)^g$.)

1.69 Definition: Für eine Teilmenge S von A ist die *charakteristische Funktion* $\chi_S\colon A \to \{0,1\}$ von S (bezüglich A) definiert durch

$$\chi_S(x) := \begin{cases} 1 & \text{falls } x \in S, \\ 0 & \text{sonst.} \end{cases}$$

1.70 Lemma: *Für jede Menge A ist $\chi\colon \mathcal{P}(A) \to \{0,1\}^A\colon S \mapsto \chi_S$ eine Bijektion.*

Beweis: Offensichtlich ist χ eine Funktion, es muß also lediglich Surjektivität und Injektivität nachgewiesen werden.

Für eine Funktion $f\colon A \to \{0,1\}$ sei $S_f := \{a \in A \mid f(a) = 1\}$. Dann gilt $\chi_{S_f} = f$, also ist χ surjektiv.

Sind S und T verschiedene Teilmengen von A, so gibt es ein Element a, das zwar in der einen, nicht aber in der anderen Menge enthalten ist. Doch dann gilt $\chi_S(a) \neq \chi_T(a)$, woraus die Injektivität von χ folgt. □

1.71 Definition: Sei Ω eine Menge von Mengen. Zwei Mengen $A, B \in \Omega$ heißen *äquivalent* oder *gleich mächtig*, falls es eine Bijektion $f\colon A \to B$ gibt.

Dies definiert eine Äquivalenzrelation auf Ω. Die Äquivalenzklasse von A wird mit $|A|$ bezeichnet und heißt *Kardinalität* oder *Mächtigkeit* von A. Die Menge der Äquivalenzklassen heißt *Kardinalzahlen*.

1.72 Bemerkung: Die naive Vorstellung ist, daß Ω die Menge aller Mengen ist. Das führt leider zu logischen Widersprüchen. Daher stellen wir uns Ω als eine möglichst große Menge von Mengen vor, die alle Mengen, die wir kennen, enthält.

1.73 Bezeichnungen: Für $n \in \mathbb{N}\backslash\{0\}$ setzen wir $n = |\{1, \ldots, n\}|$. Ergänzend gilt $0 = |\emptyset|$. Damit sind natürliche Zahlen in natürlicher Weise auch Kardinalzahlen. Mengen A mit $|A| \in \mathbb{N}$ heißen *endlich*. Mengen A mit $|A| \in \mathbb{N} \cup \{|\mathbb{N}|\}$ heißen *abzählbar*. Mengen, die nicht abzählbar sind, heißen *überabzählbar*.

1.74 Definition: Sei Ω eine Menge von Mengen und $K := \{|A| \mid A \in \Omega\}$ die Menge der Kardinalzahlen. Es sei $|A| \leq |B|$, falls es eine injektive Abbildung von A nach B gibt. Dadurch wird eine Relation auf K definiert. Mit dieser Relation wird K eine total geordnete Menge.

Aus Lemma 1.70 folgt unmittelbar das nächste Resultat.

1.75 Lemma: *Für jede Menge A gilt $|\mathcal{P}(A)| = |\{0,1\}^A|$.*

Das nächste, auf Georg Cantor zurückgehende Resultat impliziert, daß es keine größte Kardinalzahl gibt.

1.76 Satz: *Für jede Menge A gilt $|A| < |\mathcal{P}(A)|$.*

Beweis: Es genügt zu zeigen, daß es keine surjektive Abbildung $f\colon A \to \mathcal{P}(A)$ gibt. Für $f\colon A \to \mathcal{P}(A)$ sei $X_f := \{x \in A \mid x \notin f(x)\}$. Die Menge $X_f \in \mathcal{P}(A)$ ist kein Bild unter f, denn angenommen es gibt ein $a \in A$ mit $f(a) = X_f$. Für dieses a gilt $a \in X_f \iff a \notin f(a) = X_f$, eine offensichtlicher Widerspruch. □

Aus diesem Satz folgt unmittelbar:

1.77 Korollar: *Die Potenzmenge von $\mathbb{N}$ ist überabzählbar.*

Es gibt Bijektionen zwischen $\mathbb{R}$ und $\{x \in \mathbb{R} \mid 0 < x < 1\}$. Über Binärentwicklung kann gezeigt werden, daß $\{x \in \mathbb{R} \mid 0 < x < 1\}$ und $\{0,1\}^{\mathbb{N}}$ gleich mächtig sind. Aus Lemma 1.70 und Korollar 1.77 folgt daher unmittelbar:

1.78 Korollar: *Es gilt $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$, d.h. $\mathbb{R}$ ist überabzählbar.*

In jeder Programmiersprache können nur abzählbar viele (endliche) Programme geschrieben werden. Durch ein Programm können höchstens abzählbar viele Abbildungen auf $\mathbb{N}$ beschrieben werden. Wegen $\{0,1\}^{\mathbb{N}} \subset \mathbb{N}^{\mathbb{N}}$ und $\{0,1\}^{\mathbb{N}} = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$ gibt es aber überabzählbar viele Abbildungen auf $\mathbb{N}$. Das heißt:

1.79 Korollar: *Nicht alle Abbildungen $f\colon \mathbb{N} \to \mathbb{N}$ lassen sich in einer Programmiersprache programmieren.*

1.80 Bemerkung: Die (ungelöste) Frage, ob es eine Kardinalzahl κ mit $|\mathbb{N}| < \kappa < |\mathbb{R}|$ gibt, ist die sogenannte *Continuumshypothese*.

1.81 Definition: Für Kardinalzahlen können Rechenoperationen eingeführt werden:

$$|A| + |B| := |A \dot\cup B|$$
$$|A| \cdot |B| := |A \times B|$$
$$|A|^{|B|} := |A^B|$$

1.82 Testfragen:

1. Weisen Sie nach, daß für natürliche Zahlen die Rechenoperationen gemäß Definition 1.81 mit den üblichen Rechenoperationen übereinstimmen.
2. Zeigen Sie, daß für jede Kardinalzahl κ stets $\kappa < 2^\kappa$ gilt.
3. Sei $\aleph_0 := |\mathbb{N}|$. Bestimmen Sie $\aleph_0 + 1$, $\aleph_0 + \aleph_0$ und $\aleph_0 \cdot \aleph_0$.
4. Aus welcher Schrift stammt der Buchstabe $\aleph$ und wie heißt er?
5. Die Tageszeitung (TAZ) hat in ihrem samstäglichen Magazin eine Seite mit „letzten Fragen“. Am 4. März 2000 stellte dort der 7-jährige Philipp White aus Berlin die Frage „Was ist die letzte Zahl vor unendlich“. Wie würden Sie diese Frage beantworten, wenn mit ‚unendlich‘ $\aleph_0$ gemeint ist?

KAPITEL 2

Natürliche Zahlen, ganze Zahlen und Polynome

Ringe bilden, wenn auch nicht explizit genannt, den eigentlichen Schwerpunkt dieses Kapitels. Zunächst werden die natürlichen Zahlen axiomatisch eingeführt. Unmittelbar aus den Eigenschaften der natürlichen Zahlen folgt das Induktionsprinzip. Das Induktionsprinzip wird präsentiert und an Beispielen demonstriert.

Aus den natürlichen Zahlen gehen durch Hinzunehmen der negativen Zahlen die ganzen Zahlen hervor. Interessant ist die Teilbarkeitsrelation auf den ganzen Zahlen. Speziell werden Division mit Rest, größte gemeinsame Teiler, Zerlegung in Primfaktoren und der Euklidsche Algorithmus untersucht.

Die ganzen Zahlen tragen die Struktur eines Ringes. Ringe werden formal definiert. Als weiteres Beilspiel für einen Ring wird der Polynomring eingeführt und untersucht. Am Beispiel der Division mit Rest wird gezeigt, daß, obwohl ganze Zahlen und Polynome verschiedene Objekte sind, die gleichartige Struktur zu ähnlichen Sätzen mit ähnlichen Beweisen führt.

2.1. Natürliche Zahlen

Natürliche Zahlen scheinen uns vertraut. Dennoch, um sauber mit Ihnen arbeiten zu können, müssen sie exakt definiert werden. Dabei treten auch die charakterisierenden Eigenschaften der natürlichen Zahlen hervor. Unser Zugang zu den natürlichen Zahlen erfolgt über die Nachfolgerfunktion. Das ist, zumindest aus der Sicht der Informatik, der naheliegenste Zugang.

2.1 Definition: Sei $\mathbb{N}$ eine Menge mit einem Element 0 und einer Abbildung $\sigma\colon \mathbb{N} \to \mathbb{N}$ die den folgenden Axiomen genügen:

1. Aus $\sigma(m) = \sigma(n)$ folgt $m = n$.
2. Es gibt kein $n \in \mathbb{N}$ mit $\sigma(n) = 0$.
3. Ist $S \subset \mathbb{N}$ mit $0 \in S$ und $\sigma(S) \subset S$, so folgt $S = \mathbb{N}$.

Dann ist $\mathbb{N}$ die Menge der natürlichen Zahlen und σ ist die *Nachfolgerfunktion*. Wir schreiben 1 für $\sigma(0)$.

Allein mit Hilfe der Nachfolgerfunktion können Addition, Multiplikation und Potenzieren definiert werden. Die Definition dieser Rechenoperationen erfolgt rekursiv.

2.2 Definition:

1. *Addition auf* $\mathbb{N}$*:* Für $m, n \in \mathbb{N}$ sei

$$m + 0 := m,$$
$$m + \sigma(n) := \sigma(m + n).$$

2. *Multiplikation auf* $\mathbb{N}$*:* Für $m, n \in \mathbb{N}$ sei

$$m \cdot 0 := 0,$$
$$m \cdot \sigma(n) := m + (m \cdot n).$$

3. *Potenzieren:* Für $m, n \in \mathbb{N}$ sei

$$m^0 := 1,$$
$$m^{\sigma(n)} := m \cdot (m^n).$$

Die Nachfolgerfunktion ist eine sehr nützliche Funktion. Rekursionsverfahren und die beim Programmieren verwendeten Schleifen beruhen meist auf dieser Funktion. Aber auch das Induktionsprinzip beruht auf der Nachfolgerfunktion und dem 3. Axiom aus Definition 2.1.

2.3 Induktionsprinzip: Ist $A(n)$ eine Aussage, die von einem Parameter $n \in \mathbb{N}$ abhängt, so daß

1. die Aussage $A(0)$ wahr ist,
2. Aussage $A(n)$ die Aussage $A(\sigma(n))$ impliziert,

so ist die Aussage $A(n)$ für jedes $n \in \mathbb{N}$ wahr.

Beweise, die das Induktionsprinzip benutzen heißen *Beweise durch Induktion.* Der Beweis für die Assoziativität und Kommutativität der Addition ist ein Beispiel für einen Beweis durch Induktion.

2.4 Satz: *Für alle* $m, n, r \in \mathbb{N}$ *gilt:*

1. $m + (n + r) = (m + n) + r$, *(Assoziativität)*
2. $m + n = n + m$. *(Kommutativität)*

Beweis: Wir zeigen zunächst die Assoziativität. Für $m, n \in \mathbb{N}$ sei $P(r)$ die Aussage $m + (n + r) = (m + n) + r$. Nach Definition der Addition gilt

$$m + (n + 0) = m + n = (m + n) + 0.$$

Daher gilt $P(0)$. Nun der Induktionsschritt:

$$\begin{aligned} m + (n + \sigma(r)) &= m + \sigma(n + r) && \text{Definition der Addition} \\ &= \sigma(m + (n + r)) && \text{Definition der Addition} \\ &= \sigma((m + n) + r) && P(r) \\ &= (m + n) + \sigma(r) && \text{Definition der Addition} \end{aligned}$$

Dies zeigt, daß $P(\sigma(r))$ aus $P(r)$ folgt. Aus dem Induktionsprinzip ergibt sich nun die Assoziativität der Addition.

Für den Nachweis der Kommutativität wird das Induktionsprinzip dreimal angewendet.

Wir zeigen zunächst, daß $m + 0 = 0 + m$ jedes $m \in \mathbb{N}$ gilt. Für $m = 0$ ist die Aussage trivialerweise wahr. Der Induktionsschritt besteht aus der Überlegung

$$\sigma(m) + 0 = \sigma(m + 0) = \sigma(0 + m) = 0 + \sigma(m).$$

Für das erste und dritte Gleichheitszeichen ist die Definition der Addition, für das zweite Gleichheitszeichen die Induktionsvoraussetzung zuständig. Es folgt die Aussage für $\sigma(m)$.

Als nächstes zeigen wir, daß $m + 1 = 1 + m$ für $m \in \mathbb{N}$ gilt. Für $m = 0$ folgt die Aussage aus dem eben gezeigten. Der Induktionsschritt folgt aus

$$\begin{aligned} \sigma(m) + 1 = (m + \sigma(0)) + 1 = (m + 1) + 1 = (1 + m) + 1 \\ = 1 + (m + 1) = 1 + \sigma(m). \end{aligned}$$

Hier geht neben der Definition der Addition und der Aussage für m auch die bereits bewiesene Assoziativität ein.

Wir zeigen nun die Kommutativität. Für $m \in \mathbb{N}$ sei $K(n)$ die Aussage $m + n = n + m$. Mit dem bereits gezeigten gilt $K(0)$. Weiterhin gilt unter Verwendung von $K(n)$ und dem bereits gezeigten:

$$\begin{aligned} m + \sigma(n) = \sigma(m + n) = \sigma(n + m) = n + \sigma(m) = n + (m + 1) \\ = n + (1 + m) = (n + 1) + m = \sigma(n) + m. \end{aligned}$$

Dies ist $K(\sigma(n))$. □

Ab jetzt wird vorausgesetzt, daß die Leserin und der Leser Induktionsbeweise, die ohne besondere Tricks funktionieren, selbstständig ausführen kann. Der Hinweis „folgt durch Induktion“ steht somit für „der Autor kann dies formal durch Induktion beweisen und erwartet das selbe von den Leserinnen und Lesern“.

Auf $\mathbb{N}$ kann eine Ordnung definiert werden.

2.5 Definition: Für $m, n \in \mathbb{N}$ sei $m \leq n$, falls für jede Teilmenge $S \subset \mathbb{N}$ mit $m \in S$ und $\sigma(S) \subset S$ auch $n \in S$ gilt.

Es läßt sich zeigen, daß diese Relation reflexiv, transitiv und antisymmetrisch ist. Außerdem lassen sich je zwei Elemente vergleichen. Reflexivität und Transitivität sind trivial, die beiden anderen Eigenschaften erfordern Induktionsbeweise. Es gilt also

2.6 Satz: *Mit der in Definition 2.5 definierten Relation $\leq$ ist $(\mathbb{N}, \leq)$ eine total geordnete Menge.*

Für diese Ordnung gilt folgender Existenzsatz von kleinsten Elementen.

2.7 Satz: *Jede nichtleere Teilmenge von $\mathbb{N}$ hat ein kleinstes Element.*

Beweis: Sei $\emptyset \neq S \subset \mathbb{N}$. Gilt $0 \in S$, so ist 0 das kleinste Element. Gilt $0 \neq S$, so sei $T := \{m \in \mathbb{N} \mid \forall r \leq m\colon r \notin S\}$. Es gilt $0 \in T$ und $T \cap S = \emptyset$. Aus letzterem folgt $T \neq \mathbb{N}$ wegen $S \neq \emptyset$. Wegen Definition 2.1.3 enthält T daher ein Element n mit $\sigma(n) \notin T$. Das heißt, $\sigma(n) \in S$ aber $\forall m < \sigma(n)\colon m \notin S$. Damit ist $\sigma(n)$ das kleinste Element von S. □

2.8 Bemerkung: Diese Eigenschaft charakterisiert die natürlichen Zahlen. Genauer, sei $(A, \leq)$ eine total geordnete Menge mit:

1. $\forall a \in A\, \exists b \in A\colon a < b$.
2. Jede nichtleere Teilmenge von A hat ein kleinstes Element.
3. Ist B eine Teilmenge, die das kleinste Element von A enthält, und ist für jedes $b \in B$ auch das kleinste Element der Menge $\{x \in A \mid b < x\}$ ebenfalls aus B, so gilt $A = B$.

Dann entspricht $(A, \leq)$ den natürlichen Zahlen mit der in Definition 2.5 definierten Ordnung.

Das kleinste Element von A entspricht 0. Für $a \in A$ ist das kleinste Element von $\{b \in A \mid a < b\}$ der Nachfolger $\sigma(a)$ von a. Es läßt sich zeigen, daß nun die Axiome aus Definition 2.1 gelten.

2.9 Bemerkung: Es ist ein Geschmacksfrage, ob $\mathbb{N}$ die Null enthalten soll oder nicht. (Bedenkt man den Widerstand, den die alten Europäer der Einführung der Null entgegensetzten, kommen einem Zweifel an der Natürlichkeit der Null.) Wer die Null nicht will, muß in Definition 2.1 ‚0' durch ‚1' ersetzen und die Definition der Rechenoperationen anpassen.

2.10 Bemerkung: Für $m, n \in \mathbb{N}$ mit $m \leq n$ gibt es genau ein $d \in \mathbb{N}$ mit $n = m+d$. Durch $n - m := d$ wird die *Subtraktion* definiert.

Für alle bis jetzt definierten Rechenoperationen auf $\mathbb{N}$ gelten die (hoffentlich) bekannten Rechenregeln. Dies kann im Zweifelsfall durch Induktion bewiesen werden.

Das Induktionsprinzip hat diverse Varianten. Mitunter ist die zu beweisende Aussage erst ab einer bestimmten Zahl wahr. Doch dann gilt offensichtlich folgende

2.11 Variante des Induktionsprinzips: Ist $A(n)$ eine Aussage, die von einem Parameter $n \in \mathbb{N}$ abhängt und $n_0 \in \mathbb{N}$, mit:

1. die Aussage $A(n_0)$ ist wahr,
2. für $n \geq n_0$ impliziert Aussage $A(n)$ die Aussage $A(\sigma(n))$,

so ist die Aussage $A(n)$ für jedes $n \in \mathbb{N}$ mit $n_0 \leq n$ wahr.

Manchmal kann die Aussage für $\sigma(n)$ nur unter Verwendung der Aussagen für $k \leq n$ nachgewiesen werden.

2.12 Induktionsprinzip, 2. Form: Ist $A(n)$ eine Aussage, die von einem Parameter $n \in \mathbb{N}$ abhängt, so daß

1. die Aussage $A(0)$ wahr ist,
2. Aussagen $A(0), \ldots, A(n)$ die Aussage $A(\sigma(n))$ implizieren,

so ist die Aussage $A(n)$ für jedes $n \in \mathbb{N}$ wahr.

2.13 Testfrage: Zeigen Sie, daß beiden Formen des Induktionsprinzip äquivalent sind, d.h. leiten Sie 2.12 aus 2.3 und 2.3 aus 2.12 ab.

Der Beweis zum nächsten Satz demonstriert die 2. Form des Induktionsprinzip.

2.14 Satz (Division mit Rest): *Für Zahlen $m, n \in \mathbb{N}$ mit $m \neq 0$ gibt es $q, r \in \mathbb{N}$ mit $r < m$ und $n = qm + r$. Die Zahlen q und r sind eindeutig bestimmt.*

Beweis: Die Existenz der Zahlen q und r wird durch Induktion über n bewiesen. Für $n = 0$ ist die Aussage wahr, es kann $q = r = 0$ gesetzt werden.

Gilt $n+1 < m$, so ist die Aussage wahr, da $q = 0$ und $r = n+1$ gesetzt werden kann.

Sei nun $m \leq n+1$. Wir nehmen an, daß die Aussage für alle $k \in \mathbb{N}$ mit $k \leq n$ wahr ist und zeigen, daß dann auch die Aussage für $\sigma(n) = n+1$ wahr ist. Für $0 < m \leq n+1$ gilt $0 \leq n+1-m \leq n$. Also gibt es nach Induktionsvoraussetzung $q_1, r \in \mathbb{N}$, $r < m$, mit $n+1-m = q_1 m + r$. Doch dann folgt $n+1 = m+q_1 m+r = (1+q_1)m + r$. Also sind $q := q_1 + 1$ und r die gesuchten Zahlen.

Um die Eindeutigkeit zu zeigen, nehmen wir an, es gibt Zahlen $q_1, q_2, r_1, r_2 \in \mathbb{N}$ mit $r_1, r_2 < m$ so daß $n = q_1 m + r_1 = q_2 m + r_2$. Indem notfalls umnumeriert wird, kann $r_1 \leq r_2$ angenommen werden. Dann gilt $(q_1 - q_2)m = r_2 - r_1 < m$. Für $q \in \mathbb{N} \setminus \{0\}$ gilt $m \leq qm$, daher folgt $q_1 - q_2 = 0$. Doch dann gilt $q_1 = q_2$ und $r_1 = r_2$, was zu zeigen war. □

2.2. Ganze Zahlen

Als Menge gilt $\mathbb{Z} := \mathbb{N} \cup \{-n \mid n \in \mathbb{N} \setminus \{0\}\}$. Die Ordnung, die Nachfolgerfunktion, Addition und Multiplikation können von $\mathbb{N}$ auf $\mathbb{Z}$ fortgesetzt werden. Die Betragsfunktion auf $\mathbb{Z}$ wird wie üblich definiert. Dies führt zu den gewohnten Rechenregeln und soll an dieser Stelle nicht ausgeführt werden.

Die Ordnung auf den ganzen Zahlen spielt im folgenden keine Rolle. Wichtig ist hingegen, daß die Betragsfunktion eine Abbildung in eine total geordnete Menge ist.

Die ganzen Zahlen werden später prominentes Beispiel für eine ganz bestimmte Sorte von algebraischen Systemen, den Ringen. Manche der Sätze, die in diesem Abschnitt vorgestellt werden, gelten auch für manche andere Ringe. Testen Sie dies am Ring der Polynome. Die Addition und Multiplikation von Polynomen erfolgt wie gewohnt. Anstatt der Betragsfunktion wird die Funktion, die jedem Polynom seinen Grad zuordnet, betrachtet. Wir werden den Polynomring in Abschnitt 2.3 genauer untersuchen.

Der Beweis zu Satz 2.14 funktioniert auch in $\mathbb{Z}$ und liefert:

2.15 Satz: *Für Zahlen $m, n \in \mathbb{Z}$ mit $m \neq 0$ gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $0 \leq r < |m|$ und $n = qm + r$.*

2.16 Testfrage:

1. Überprüfen Sie, ob der Beweis zu Satz 2.14 tatsächlich auch in $\mathbb{Z}$ funktioniert.

2. In jeder Programmiersprache, die Rechnen mit ganzen Zahlen erlaubt, sind Funktionen implementiert, die für $a, b \in \mathbb{Z}$ die Zahlen q und r mit $a = qb + r$ berechnen. Wie heißen diese Funktionen in der Sprache Ihrer Wahl?

2.17 Definition: Für $a, b \in \mathbb{Z}$ gilt a *teilt* b, geschrieben $a \mid b$, falls es ein $m \in \mathbb{Z}$ mit $b = am$ gibt.

Die Einschränkung von $\mid$ auf die Menge der echt positiven Zahlen liefert eine Ordnung, wie in Beispiel 1.43.3 gezeigt wird. Hingegen ist $(\mathbb{Z}, \mid)$ keine geordnete Menge. Auf $\mathbb{Z}$ geht die Antisymmetrie verloren. Zum Beispiel gilt $2 \mid -2$ und $-2 \mid 2$ aber $2 \neq -2$.

2.18 Definition: Eine Teilmenge $I \subset \mathbb{Z}$ heißt *Ideal* (in $\mathbb{Z}$), falls gilt:

1. $\emptyset \neq I$,
2. $\forall x, y \in I \colon x - y \in I$,
3. $\forall m \in \mathbb{Z}\, \forall x \in I \colon mx \in I$.

Das heißt, eine nichtleere Teilmenge von $\mathbb{Z}$ ist genau dann ein Ideal, wenn sie abgeschlossen bezüglich Addition, Subtraktion und Multiplikation mit Elementen aus $\mathbb{Z}$ ist.

2.19 Beispiel: Für jede nichtleere Teilmenge $A \subset \mathbb{Z}$ ist der Aufspann

$$(A) := \{x \in \mathbb{Z} \mid \exists a_1, \ldots, a_n \in A, \exists k_1, \ldots, k_n \in \mathbb{Z} \colon x = k_1 a_1 + \cdots + k_n a_n\}$$

ein Ideal in $\mathbb{Z}$. Dies wird wie folgt gezeigt:

1. Für $a \in A$ ist $a = 1a \in (A)$, also $\emptyset \neq A \subset (A)$.
2. Seien $x, y \in (A)$. Es gibt
$$\{a_1, \ldots, a_n, b_1, \ldots, b_m\} \subset A,$$
$$\{k_1, \ldots, k_n, l_1, \ldots, l_m\} \subset \mathbb{Z}$$
mit $x = \sum_{i=1}^{n} k_i a_i$ und $y = \sum_{i=1}^{m} l_i b_i$. Für $i \in \{1, \ldots m\}$ sei $k_{n+i} := -l_i \in \mathbb{Z}$ und $a_{n+i} := b_i \in A$. Dann gilt $x - y = \sum_{i=1}^{n+m} k_i a_i \in (A)$.
3. Für $x = \sum_{i=1}^{n} k_i a_i \in (A)$ und $m \in \mathbb{Z}$ ist $mx = \sum_{i=1}^{n} (mk_i) a_i \in (A)$.

2.20 Bezeichnung: Anstatt $(\{a_1, a_2, \ldots, a_n\})$ schreiben wir auch $(a_1, a_2, \ldots, a_n)$.

2.21 Bemerkungen:

1. In Beispiel 2.19 wird gezeigt, daß $A \subset (A)$ gilt.
2. Wir setzen $(\emptyset) := \{0\}$.

2.22 Definition: Ein Ideal I von $\mathbb{Z}$ heißt *Hauptideal*, falls es ein $a \in \mathbb{Z}$ mit $I = (a)$ gibt.

2.23 Beispiele:

1. $(0) = \{0\}$ ist ein Hauptideal.
2. $(1) = \mathbb{Z}$ ist ein Hauptideal.
3. Die Menge der geraden Zahlen ist ein Hauptideal, nämlich (2).
4. Die Menge der ungeraden Zahlen ist kein Ideal, also auch kein Hauptideal.

2.24 Satz: *Jedes Ideal in $\mathbb{Z}$ ist ein Hauptideal.*

Beweis: Das Ideal $\{0\} = (0)$ ist offensichtlich ein Hauptideal. Sei I ein von (0) verschiedenes Ideal in $\mathbb{Z}$. Dann gibt es ein $a \in I$ verschieden von 0. Mit a ist auch $-a$ ein Element von I, also gilt $\emptyset \neq M := I \cap \mathbb{N} \setminus \{0\}$. Wegen Satz 2.7 hat M ein kleinstes Element m. Die Behauptung ist bewiesen, wenn $(m) = I$ gezeigt ist. Nach Konstruktion gilt $m \in I$, also wegen Definition 2.18.3 auch $(m) \subset I$. Es muß daher nur noch die umgekehrte Inklusion $I \subset (m)$ gezeigt werden. Sei $a \in I$. Nach Satz 2.15 gibt es $q, r \in \mathbb{Z}$ mit $0 \leq r < m$ und $a = qm + r$. Umformen liefert $r = a - qm$, damit ist r als Differenz zweier Elemente aus I ebenfalls in I. Zum einen gilt $0 \leq r < m$, zum anderen ist m das kleinste positive Element in I. Dies erzwingt $r = 0$, also $a = qm \in (m)$. Daraus folgt die gewünschte Inklusion $I \subset (m)$. □

Allein mit dieser Eigenschaft und den Rechengesetzen der ganzen Zahlen können viele weitere Eigenschaften gezeigt werden. Der Nachweis, daß der größte gemeinsame Teiler ganzer Zahlen existiert, soll dies demonstrieren.

2.25 Definition: Für $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ ist $g \in \mathbb{N}$ genau dann *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$, falls:

1. $\forall i \in \{1, \ldots, n\}\colon g \mid a_i$.
2. Ist $g' \in \mathbb{N}$ mit $\forall i \in \{1, \ldots, n\}\colon g' \mid a_i$, so folgt $g' \mid g$.

2.26 Lemma: *Für $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ gibt es höchstens einen größten gemeinsamen Teiler.*

Beweis: Angenommen g und g' sind größte gemeinsame Teiler von $a_1, \ldots, a_n$. Das heißt, beide erfüllen die erste Bedingung aus Definition 2.25, weswegen nach der zweiten Bedingung sowohl $g \mid g'$ als auch $g' \mid g$ folgt. Daraus folgt $g = g'$. □

2.27 Testfrage: Dieser Beweis sollte Ihnen bekannt vorkommen. Woher?

2.28 Bezeichnung: Der größte gemeinsame Teiler ganzer Zahlen $a_1, \ldots, a_n$ wird mit $\operatorname{ggt}(a_1, \ldots, a_n)$ bezeichnet.

2.29 Satz: *Für $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ und $g \in \mathbb{Z}$ gilt:*

$$(g) = (a_1, \ldots, a_n) \iff |g| = \operatorname{ggt}(a_1, \ldots, a_n).$$

Beweis: Wir nehmen zunächst $(g) = (a_1, \ldots, a_n)$ an. Wegen $A \subset (A)$ gilt $a_i \in (a_1, \ldots, a_n) = (g)$ für jedes $i \in \{1, \ldots, n\}$. Das heißt, für jedes $i \in \{1, \ldots, n\}$ gibt es $k_i \in \mathbb{Z}$ mit $a_i = k_i g$. Mit anderen Worten, g teilt jedes a_i. Teilt $g' \in \mathbb{Z}$ auch alle a_i, so existiert für jedes $i \in \{1, \ldots, n\}$ ein $l_i \in \mathbb{Z}$ mit $a_i = l_i g'$. Wegen $g \in (g) = (a_1, \ldots, a_n)$ gibt es $t_i \in \mathbb{Z}$ mit $g = t_1 a_1 + \cdots + t_n a_n$. Damit folgt

$$g = \sum_{i=1}^{n} t_i a_i = \sum_{i=1}^{n} t_i l_i g' = g' \sum_{i=1}^{n} t_i l_i,$$

also $g' \mid g$. Somit erfüllt g beide Bedingungen aus Definition 2.25, d.h. $|g| = \operatorname{ggt}(a_1, \ldots, a_n)$.

Wir gehen nun von $|g| = \operatorname{ggt}(a_1, \ldots, a_n)$ aus. Gemäß Satz 2.24 ist $(a_1, \ldots, a_n)$ ein Hauptideal, das heißt es gibt ein $m \in \mathbb{Z}$ mit $(m) = (a_1, \ldots, a_n)$. Mit der bereits gezeigten Implikation folgt $|m| = \operatorname{ggt}(a_1, \ldots, a_n)$, also $m = \pm g$. Doch dann gilt wie gewünscht $(g) = (m) = (a_1, \ldots, a_n)$. □

Dieser Zusammenhang zwischen Idealen und größten gemeinsamen Teilern ermöglicht einen eleganten Beweis für die Existenz größter gemeinsamer Teiler.

2.30 Korollar: *Für $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ gibt es genau einen größten gemeinsamen Teiler.*

Beweis: Es muß nur noch die Existenz gezeigt werden. Nach Satz 2.24 ist das Ideal $(a_1, \ldots, a_n)$ ein Hauptideal. Es gibt also ein $g \in \mathbb{Z}$ mit $(g) = (a_1, \ldots, a_n)$. Wegen Satz 2.29 gilt $|g| = \operatorname{ggt}(a_1, \ldots, a_n)$. □

Aus Satz 2.29 folgt unmittelbar:

2.31 Korollar: *Für $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ gibt es $k_1, \ldots, k_n \in \mathbb{Z}$ mit*

$$\operatorname{ggt}(a_1, \ldots, a_n) = \sum_{i=1}^{n} k_i a_i.$$

2.32 Bezeichnung: Zahlen $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ mit $\operatorname{ggt}(a_1, \ldots, a_n) = 1$ heißen *teilerfremd.*

Beachten Sie, daß in die Beweise von Satz 2.29 und Korollar 2.30 neben den definierenden Eigenschaften größter gemeinsamer Teiler nur Satz 2.24 eingeht.

2.33 Euklidscher Algorithmus: Zur Bestimmung des größten gemeinsamen Teilers g zweier von 0 verschiedener ganzer Zahlen a, b gibt es einen Algorithmus, der auf Euklid zurückgeht. Eine Verfeinerung des Algorithmus bestimmt zudem noch Zahlen s und t mit $g = sa + tb$. Wegen $\operatorname{ggt}(b,a) = \operatorname{ggt}(a,b) = \operatorname{ggt}(-a,b) = \operatorname{ggt}(-a,-b)$ kann $0 < b \leq a$ angenommen werden. Nach Satz 2.15 gibt es für Zahlen $m, n \in \mathbb{Z}$ mit $m \neq 0$ Zahlen $q, r \in \mathbb{Z}$ mit $n = qm + r$. Durch $q = n \operatorname{div} m$ und $r = n \bmod m$ werden zwei Funktionen div und mod definiert. Es gilt genau dann $n \bmod m = 0$, wenn $m \mid n$ gilt.

Wir setzen als Startwerte

$$\begin{aligned} a_0 &:= a, & s_0 &:= 1, & t_0 &:= 0, \\ a_1 &:= b, & s_1 &:= 0, & t_1 &:= 1, \end{aligned}$$

und fahren iterativ fort durch

$$\begin{aligned} a_{n+2} &:= a_n \bmod a_{n+1}, \\ q_{n+2} &:= a_n \operatorname{div} a_{n+1}, \\ s_{n+2} &:= s_n - q_{n+2} s_{n+1}, \\ t_{n+2} &:= t_n - q_{n+2} t_{n+1}. \end{aligned}$$

Dies funktioniert, solange $a_{n+1} \neq 0$ gilt. Für jedes n gilt $a_n = q_{n+2} a_{n+1} + a_{n+2}$. Wegen $0 \leq a_n < a_{n-1} < \cdots < a_1 = b$ gibt es ein $N \in \mathbb{N}$ mit $a_N \neq 0$ und $a_{N+1} = 0$.

Es gilt $g := a_N = \operatorname{ggt}(a,b)$. Wegen $a_{N-1} = q_{N+1} a_N$ teilt $g = a_N$ auch a_{N-1}. Teilt g sowohl a_n als auch a_{n-1}, so teilt g auch $a_{n-2} = q_n a_{n-1} + a_n$. Durch Induktion folgt so, daß g sowohl $a = a_0$ als auch $b = a_1$ teilt. Ist g' eine Zahl, die a_n und a_{n+1} teilt, so wird wegen $a_n = q_{n+2} a_{n+1} + a_{n+2}$ auch a_{n+2} von g' geteilt. Teilt also g' sowohl $a = a_0$ als auch $b = a_1$, so folgt durch Induktion, daß g' auch $g = a_N$ teilt. Daher ist g der größte gemeinsame Teiler von a und b.

Unsere nächste Behauptung ist, daß für jedes $n \in \{0, 1, \ldots, N\}$ stets $a_n = s_n a + t_n b$ gilt. Für $n \in \{0, 1\}$ ist das nach Konstruktion erfüllt. Gilt die Behauptung für n und $n+1$ so ergibt Einsetzen in $a_n = q_{n+2} a_{n+1} + a_{n+2}$ die Beziehung

$$s_n a + t_n b = q_{n+2}(s_{n+1} a + t_{n+1} b) + a_{n+2}$$

also

$$a_{n+2} = (s_n - q_{n+2} s_{n+1}) a + (t_n - q_{n+2} t_{n+1}) b = s_{n+2} a + t_{n+2} b.$$

Dies ist die Behauptung für $n+2$. Durch Induktion gilt daher die Behauptung auch für N, d.h. $g = a_N = s_N a + t_N b$. Damit sind $s := s_N$ und $t := t_N$ die gesuchten Zahlen.

2.34 Testfrage: Implementieren Sie den Euklidschen Algorithmus in einer Sprache Ihrer Wahl. (Die Sprache sollte die Funktionen ‚div' und ‚mod' bereitstellen.)

2.35 Definition: Eine Zahl $p \in \mathbb{N}$ mit $p \geq 2$ heißt *prim* oder *Primzahl*, falls 1 und p die einzigen positiven Zahlen sind, die p teilen.

2.36 Satz: *Jede Zahl $n \in \mathbb{N}$ mit $n \geq 2$ läßt sich als Produkt von Primzahlen darstellen.*

Beweis: Der Beweis wird mit der 2. Form der Induktion geführt. Für die Primzahl 2 ist die Aussage offensichtlich wahr. Wir nehmen nun an, daß die Behauptung für $2 \leq m \leq n$ wahr ist und betrachten $n+1$. Ist $n+1$ eine Primzahl, so ist die Behauptung trivialerweise richtig. Ist $n+1$ keine Primzahl, so gibt es $r, s \in \mathbb{N}$ mit $2 \leq r, s \leq n$ und $n+1 = rs$. Nach Annahme haben r und s eine Zerlegung in Primfaktoren. Zusammen ergibt sich eine Zerlegung von $n+1$ in Primfaktoren. □

2.37 Lemma: *Ist p eine Primzahl, so folgt für Zahlen $a, b \in \mathbb{Z}$ aus $p \mid ab$ stets $p \mid a$ oder $p \mid b$.*

Beweis: Angenommen p teilt ab aber nicht a. Da p eine Primzahl ist, folgt $\operatorname{ggt}(p, a) = 1$ aus $p \nmid a$. Wegen Korollar 2.31 gibt es $s, t \in \mathbb{Z}$ mit $1 = sp + ta$. Multiplikation mit b ergibt $b = spb + tab$. Nach Voraussetzung gilt $p \mid ab$, das heißt es gibt $k \in \mathbb{Z}$ mit $ab = pk$. Dies impliziert

$$b = spb + tab = spb + tkp = p(sb + tk)$$

also $p \mid b$. □

Induktion liefert aus diesem Resultat unmittelbar:

2.38 Korollar: *Ist p eine Primzahl und sind $a_1, \ldots, a_n \in \mathbb{Z}$ so gilt:*

$$p \mid a_1 a_2 \cdots a_n \Rightarrow \exists k \in \{1, \ldots, n\} \colon p \mid a_k.$$

2.39 Satz: *Die Primzahlzerlegung einer Zahl $z \in \mathbb{N}$ mit $z \geq 2$ ist bis auf die Reihenfolge der Faktoren eindeutig.*

Beweis: Der Beweis wird mit der 2. Form der Induktion geführt. Für die Primzahl 2 ist die Aussage offensichtlich wahr. Wir nehmen nun an, daß die Behauptung für $2 \leq m \leq n$ wahr ist und betrachten $n+1$. Ist $n+1$ eine Primzahl, so ist die Behauptung trivialerweise richtig. Ist $n+1$ keine Primzahl, so läßt sich $n+1$ in Primfaktoren zerlegen. Angenommen

$$n+1 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

sind zwei Zerlegungen in Primfaktoren. Es gilt $p_1 \mid q_1 q_2 \cdots q_s$, also gibt es nach Korollar 2.38 einen Faktor q_k mit $p_1 \mid q_k$. Da q_k prim ist, folgt $p_1 = q_k$. Nach umnumerieren kann $k = 1$, also $p_1 = q_1$, angenommen werden. Dann sind $p_2 \cdots p_r$ und $q_2 \cdots q_s$ Zerlegungen in Primfaktoren der ganzen Zahl $^{n+1}/_{p_1} \leq n$. Nach Induktionsvoraussetzung unterscheiden sich die Zerlegungen $p_2 \cdots p_r$ und $q_2 \cdots q_s$ höchstens in der Reihenfolge der Faktoren. Doch dann sind auch die ursprünglichen Zerlegungen bis auf die Reihenfolge ihrer Faktoren gleich. □

2.40 Testfrage: Zeigen Sie, daß es unendlich viele Primzahlen gibt.

2.3. Polynome

Obwohl Polynome ganz andere mathematische Objekte als ganze Zahlen sind, haben sie doch überraschend große strukturelle Gemeinsamkeiten. Bevor wir definieren können, was Polynome über einem beliebigen Körper sind, müssen wir definiert haben, was ein Körper ist. Auf dem Weg dorthin werden außerdem noch Ringe definiert. Ringe und Körper sind Beispiele für algebraische Strukturen, die im nächsten Kapitel untersucht werden.

2.41 Definition: Ein *Ring* $(R, +, \cdot, 0, 1)$ ist eine Menge R mit zwei Operationen $+$ und $\cdot$ sowie zwei ausgezeichneten Elementen 0 und 1 aus R, so daß gilt:

1. $\forall a, b \in R$: $a + b \in R$, Abgeschlossenheit bzgl. Addition
2. $\forall a, b, c \in R$: $(a + b) + c = a + (b + c)$, Assoziativität der Addition
3. $\forall a, b \in R$: $a + b = b + a$, Kommutativität der Addition
4. $\forall a \in R$: $0 + a = a$, Nullelement
5. $\forall a \in R\, \exists b \in R$: $a + b = 0$, Additives Inverses
6. $\forall a, b \in R$: $a \cdot b \in R$, Abgeschlossenheit bzgl. Multiplikation
7. $\forall a, b, c \in R$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, Assoziativität der Multiplikation
8. $\forall a \in R$: $1 \cdot a = a = a \cdot 1$, Einselement
9. $\forall a, b, c \in R$: $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(b + c) \cdot a = b \cdot a + c \cdot a$, Distributivgesetze

2.42 Bezeichnung: Das additive Inverse einer Zahl a ist eindeutig bestimmt und wird mit $-a$ bezeichnet. Wie üblich schreiben wir ab für $a \cdot b$.

2.43 Bemerkung: Die ersten fünf Axiome für einen Ring $(R, +, \cdot, 0, 1)$ besagen, daß R mit der Addition eine kommutative Gruppe ist. Wir werden in Kapitel 5 näher auf Gruppen eingehen.

2.44 Beispiele:

1. Die ganzen Zahlen mit der üblichen Addition und Multiplikation bilden einen Ring.
2. Für $n \in \mathbb{N} \setminus \{0\}$ bildet die Menge der reellen $n \times n$-Matrizen mit der üblichen Addition und Multiplikation einen Ring.

2.45 Definition: Sei $(R, +, \cdot, 0, 1)$ ein Ring. Eine Teilmenge $I \subset R$ heißt *Ideal* (in R), falls gilt:

1. $\emptyset \neq I$,
2. $\forall x, y \in I\colon x - y \in I$,
3. $\forall m \in R \forall x \in I\colon mx \in I$ und $xm \in I$.

2.46 Definition: Sei $(R, +, \cdot, 0, 1)$ ein Ring. Für $A \subset R$ ist (A) das kleinste Ideal in R, das A umfaßt. Ein Ideal $I \subset R$ ist ein *Hauptideal*, falls es ein $m \in I$ mit $I = (m)$ gibt.

2.47 Definition: Ein *Körper* $(\mathbb{K}, +, \cdot, 0, 1)$ ist ein Ring, bei dem zusätzlich gilt:

1. $\forall a, b \in \mathbb{K}\colon ab = ba$.
2. $\forall a \in \mathbb{K} \setminus \{0\}\, \exists b \in \mathbb{K} \setminus \{0\}\colon ab = 1$.

Das heißt, $(\mathbb{K}, +, \cdot, 0, 1)$ ist ein Ring, bei dem $\mathbb{K} \setminus \{0\}$ mit der Multiplikation auch eine kommutative Gruppe ist.

Für $a \in \mathbb{K}$ heißt $b \in \mathbb{K}$ mit $ab = 1$ das multiplikative Inverse zu a und wird mit a^{-1} oder $\frac{1}{a}$ bezeichnet.

2.48 Beispiel: Die Mengen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit den üblichen Rechenoperationen sind Körper.

2.49 Testfrage: Sei $\mathbb{Z}_m$ wie in Beispiel 1.37.4. Wir definieren $[a] + [b] := [a + b]$ und $[a] \cdot [b] := [ab]$. Für welche $m \in \mathbb{N} \setminus \{0\}$ ist $\mathbb{Z}_m$ ein Ring, und für welche $m \in \mathbb{N} \setminus \{0\}$ ist $\mathbb{Z}_m$ ein Körper?

2.50 Bezeichnung: Wir kürzen in Zukunft $(\mathbb{K}, +, \cdot, 0, 1)$ durch $\mathbb{K}$ ab, sofern die Operationen nicht explizit angegeben werden müssen.

2.51 Definition: Sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Ein *Polynom f über K vom Grad n* ist ein formaler Ausdruck der Form

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

mit *Koeffizienten* $a_i \in \mathbb{K}$, wobei $a_n \neq 0$. Die Funktion ‚grad' weist jedem Polynom seinen Grad zu.

Die Menge aller Polynome über $\mathbb{K}$ wird mit $\mathbb{K}[x]$ bezeichnet. Das Polynom 0 heißt *Nullpolynom* und hat Grad $-\infty$. Das Polynom $1 \in \mathbb{K}[x]$ heißt *Einspolynom*.

2.52 Definition: Auf $\mathbb{K}[x]$ sind Skalarmultiplikation, Addition und Multiplikation wie folgt erklärt:

1. *Skalarmultiplikation* Für $b \in \mathbb{K}$ und $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ sei
$$bf := \sum_{i=0}^{n} b a_i x^i.$$
2. *Addition* Sei $f, g \in \mathbb{K}[x]$. Also $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{i=0}^{m} b_i x^i$. Falls $\mathrm{grad} f = n < m = \mathrm{grad} g$, so sei $a_i := 0$ für $i \in \{n+1, \ldots, m\}$. Entsprechend falls $m < n$. Dann gilt:
$$f + g := \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i.$$
3. *Multiplikation* Sei $f, g \in \mathbb{K}[x]$. Also $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{i=0}^{m} b_i x^i$. Für $k \in \{0, \ldots, m+n\}$ sei
$$c_k := a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_0 b_k = \sum_{i=0}^{k} a_i b_{k-i}.$$
Dabei werden fehlende Koeffizienten durch 0 ersetzt. Dann ist
$$f \cdot g := \sum_{k=0}^{n+m} c_k x^k.$$

2.53 Bemerkung: Ist $f = a$ ein Polynom vom Grad 0 oder das Nullpolynom, so gilt $f \cdot g = a \cdot g$ für jedes Polynom $g \in \mathbb{K}[x]$. Die Skalarmultiplikation ist also ein Spezialfall der Multiplikation zweier Polynome.

2.54 Bemerkung: Die Struktur $(\mathbb{K}[x], +, \cdot, 0, 1)$ mit der oben definierten Addition und Multiplikation ist ein Ring, der *Polynomring* über dem Koeffizientenkörper $\mathbb{K}$. Wir schreiben ab jetzt meist abkürzend $\mathbb{K}[x]$ statt $(\mathbb{K}[x], +, \cdot, 0, 1)$.

Mit der oben definierten Skalarmultiplikation und Addition kann $\mathbb{K}[x]$ auch als Vektorraum über $\mathbb{K}$ aufgefaßt werden.

2.55 Testfrage: Zeigen Sie, daß $\mathbb{K}[x]$ in der Tat ein Ring ist.

2.56 Lemma: *Für $f, g \in \mathbb{K}[x]$ gilt:*

1. $\text{grad}(f \cdot g) = \text{grad}f + \text{grad}g$,
2. $\text{grad}(f + g) \leq \max\{\text{grad}f, \text{grad}g\}$.

Beweis: Sei $n := \text{grad}f$ und $m := \text{grad}g$. Dann gilt $c_{n+m} = a_n b_m \neq 0$, also $\text{grad}(f \cdot g) = n + m = \text{grad}f + \text{grad}g$.

Nach Konstruktion gilt $\text{grad}(f + g) \leq \max\{\text{grad}f, \text{grad}g\}$. Falls $\text{grad}f = \text{grad}g = n$ und $a_n = -b_n$ so gilt $\text{grad}(f+g) < n = \max\{\text{grad}f, \text{grad}g\}$. Gleichheit kann also nicht immer erwartet werden. □

2.57 Testfrage: Zeigen Sie, daß diese Gradformeln auch gelten, falls g oder f das Nullpolynom ist.

Das nächste Resultat ist das Analogon zu Satz 2.15. Auf diesem Satz beruhen die großen Ähnlichkeiten zwischen dem Ring der ganzen Zahlen und dem Polynomring über einem Körper.

2.58 Satz: Division mit Rest für Polynome: *Für $f, g \in \mathbb{K}[x]$ mit $g \neq 0$ gibt es eindeutig bestimmte $q, r \in \mathbb{K}[x]$ mit* $\text{grad}r < \text{grad}g$ *und $f = qg + r$.*

Beweis: Zuerst wird die Existenz von q und r bewiesen. Wir untersuchen zunächst den Fall $\text{grad}g = 0$. Dann gibt es $b \in \mathbb{K}\setminus\{0\}$ mit $g = b$. Für $q := \frac{1}{b}f$ gilt $qg = \frac{1}{b} \cdot f \cdot b$ also $f = qg + 0$. Wegen $\text{grad}0 = -\infty < 0 = \text{grad}g$ ist auch die Gradbedingung erfüllt.

Für $\text{grad}g > 0$ führen wir einen Induktionsbeweis 2. Form über $n := \text{grad}f$. Falls $\text{grad}f < \text{grad}g$ so gilt $f = 0 \cdot g + f$ und $\text{grad}f < \text{grad}g$. Dies beweist die Induktionsannahme für $n < \text{grad}g$.

Sei nun $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{i=0}^{m} b_i x^i$ mit $m \leq n$. Wir setzen:

$$\begin{aligned} f_1 &:= f - \frac{a_n}{b_m} x^{n-m} g \\ &= a_n x^n + \cdots + a_0 - \underbrace{\frac{a_n}{b_m} x^{n-m} b_m x^m}_{a_n x^n} - \sum_{i=0}^{n-1} b_i' x^i \\ &= \sum_{i=0}^{n-1} a_i' x^i. \end{aligned}$$

Es gilt $\mathrm{grad} f_1 < n$. Nach Induktionsvoraussetzung gibt es also $q_1, r \in \mathbb{K}[x]$ mit $f_1 = q_1 g + r$ und $\mathrm{grad} r < \mathrm{grad} g$. Dies wird in die Beziehung, die zwischen f und f_1 besteht, eingesetzt:

$$\begin{aligned} f &= \frac{a_n}{b_m} x^{n-m} g + f_1 \\ &= \frac{a_n}{b_m} x^{n-m} g + q_1 g + r \\ &= (\frac{a_n}{b_m} x^{n-m} + q_1) g + r \\ &= qg + r, \end{aligned}$$

mit $q = \frac{a_n}{b_m} x^{n-m} + q_1$ und $\mathrm{grad} r < \mathrm{grad} g$. Dies zeigt die Behauptung für f.

Abschließend wird die Eindeutigkeit der Darstellung gezeigt. Angenommen $f = q_1 g + r_1 = q_2 g + r_2$, wobei $\mathrm{grad} r_1 < \mathrm{grad} g$ und $\mathrm{grad} r_2 < \mathrm{grad} g$. Umstellen der Gleichung ergibt $(q_1 - q_2) g = r_2 - r_1$. Wegen $\mathrm{grad}(r_2 - r_1) \leq \max\{\mathrm{grad} r_1, \mathrm{grad} r_2\} < \mathrm{grad} g$ und $\mathrm{grad}((q_1 - q_2) g) = \mathrm{grad}(q_1 - q_2) + \mathrm{grad} g$ muß $\mathrm{grad}(q_1 - q_2) < 0$, also $\mathrm{grad}(q_1 - q_2) = -\infty$ gelten. Das heißt $q_1 - q_2 = 0$. Doch dann gilt $r_2 - r_1 = (q_1 - q_2) g = 0$, also insgesamt wie gewünscht $q_1 = q_2$ und $r_1 = r_2$. □

Der Beweis des nächsten Resultat ist eine einfache Übungsaufgabe.

2.59 Lemma: *Für Polynome $f_1, \ldots f_r \in \mathbb{K}[x]$ gilt*

$$(f_1, \ldots f_r) = \{h \in \mathbb{K}[x] \mid \exists g_1, \ldots, g_r \in \mathbb{K}[x] \colon g_1 f_1 + \cdots + g_r f_r = h\}.$$

Der Beweis des nächsten Resultat verläuft analog zum Beweis von Satz 2.24 und ist eine Übungsaufgabe.

2.60 Satz: *Jedes Ideal in $\mathbb{K}[x]$ ist ein Hauptideal.*

2.61 Testfragen:

1. Führen sie die Beweise der beiden voranstehenden Aussagen aus.

2. Sei R die Menge der (3×3)-Diagonalmatrizen und I die Menge der Matrizen aus R, für die der dritte Diagonaleintrag gleich 0 ist. Zeigen Sie, daß R mit der üblichen Matrizenmultiplikation und Matrizenaddition ein Ring ist. Zeigen Sie, daß I ein Ideal aber kein Hauptideal in R ist.

2.62 Bemerkung: Ringe, in denen jedes Ideal ein Hauptideal ist, heißen *Hauptidealringe*.

KAPITEL 3

Algebraische Systeme

In dieser Vorlesung und Ihrem seitherigen Studium haben Sie verschiedene mathematische Strukturen kennengelernt. Zum Beispiel sollten Ihnen Vektorräume, Gruppen und Ringe begegnet sein. Bei den aufgeführten Beispielen ist stets eine Menge zusammen mit einigen Operationen und einigen ausgezeichneten Elementen gegeben. Die Eigenschaften der Operationen, genauer, die Regeln, denen sie gehorchen, bestimmen dann, welche Struktur vorliegt.

Wir stellen uns jetzt auf den Standpunkt, daß uns diese Regeln nicht interessieren. Das heißt, wir untersuchen irgendwelche Mengen, auf denen irgendwelche Operationen gegeben sind. Zugegeben, das Konzept ist sehr abstrakt. Da relativ wenig Information vorhanden ist, sind auch kaum spezielle Sätze zu erwarten. Allerdings, die Eigenschaften, die in diesem abstrakten Rahmen gelten, gelten dann automatisch für eine Vielzahl verschiedener Strukturen. Alle Konstruktionen, die in diesem Rahmen sinnvoll formuliert werden können, sind so fundamental, daß sie in vielen Bereichen der Mathematik auftauchen.

Außerdem trennt dieser Ansatz deutlich zwischen den Eigenschaften, die eine solche abstrakte Struktur ohnehin erfüllt, und den speziellen Eigenschaften, die zum Beispiel eine Gruppe oder ein Vektorraum erfüllt.

3.1. Homogene algebraische Systeme

Wie wollen zunächst den Begriff eines (homogenen) algebraischen Systems einführen. Dazu betrachten wir folgende bekannte mathematischen Objekte als Beispiele.

3.1 Beispiele:

1. Der Ring $(\mathbb{Z}, +, \cdot, 0, 1)$ der ganzen Zahlen.
2. Die Potenzmenge $(\mathcal{P}(X), \cup, \cap, \setminus, \emptyset, X)$ einer Menge X zusammen mit den mengentheoretischen Operationen sowie der leeren und der ganzen Menge als ausgezeichneten Mengen.

3. Die Boolsche Algebra $(B, \vee, \wedge, \neg, 0, 1)$. Dabei ist B eine Menge von Aussagen, die abgeschlossen unter den logischen Operationen ist und die konstanten Aussagen 0 und 1 enthält. Die Aussage 0 ist immer falsch, die Aussage 1 ist immer wahr.

Ein Blick auf diese Beispiele zeigt, daß stets eine Menge und diverse Operationen sowie spezielle Elemente gegeben sind. Dies wird nun systematisiert.

3.2 Definition: Ein *(homogenes) algebraisches System* $\mathfrak{A}$ ist ein Paar (A, Ω), wobei $A \neq \emptyset$ die *Trägermenge* und Ω eine Menge von Operationen auf A ist.

Eine *Operation* $\omega \in \Omega$ der *Stelligkeit* $n \in \mathbb{N}$ ist eine Abbildung $\omega\colon A^n \to A$. Dabei wird $A^0 := \{\emptyset\}$ gesetzt. Die Stelligkeit $\alpha(\omega)$ einer Operation Ω heißt auch *Dimension*.

Operationen der Stelligkeit 1 bzw. 2 heißen *unitär* bzw. *binär*. Eine Operation der Stelligkeit 0 zeichnet ein Element der Trägermenge aus.

Ist Ω endlich, so schreiben wir oft $(A, \omega_1, \ldots, \omega_n)$ statt $(A, \{\omega_1, \ldots, \omega_n\})$.

3.3 Beispiele: Wir wollen diese Definition an den oben aufgeführten Beispielen verdeutlichen.

1. Für den Ring der ganzen Zahlen ist $A = \mathbb{Z}$ und $\Omega = \{+, \cdot, 0, 1\}$. Für die einzelnen Operationen gilt:

$$+\colon A^2 \to A, \alpha(+) = 2, \qquad \cdot\colon A^2 \to A, \alpha(\cdot) = 2,$$
$$0\colon A^0 \to A, \alpha(0) = 0, \qquad 1\colon A^0 \to A, \alpha(0) = 0.$$

   Das heißt, die beiden ausgezeichneten Elemente werden als nullstellige Operationen aufgefaßt. Das macht Sinn, denn diese Elemente sind global ausgezeichnet und hängen nicht von einem oder mehreren Elementen aus A, sondern von nichts, also der leeren Menge, ab.

   Für beliebige Ringe gilt analoges.
2. Für die Potenzmenge einer Menge X mit den üblichen Mengenoperationen ist $A = \mathcal{P}(X)$ und $\Omega = \{\cup, \cap, \setminus, \emptyset, X\}$. Die Operationen $\cup$, $\cap$ und $\setminus$ sind zweistellig, die leere und die ganze Menge können als nullstellige Operationen aufgefaßt werden.
3. Für die Boolsche Algebra ist $A = B$ und $\Omega = \{\vee, \wedge, \neg, 0, 1\}$ mit $\alpha(\vee) = \alpha(\wedge) = 2$, $\alpha(\neg) = 1$ und $\alpha(0) = \alpha(1) = 0$.

3.2. Heterogene algebraische Systeme

Homogene algebraische Systeme sind noch nicht allgemein genug. Das Problem ist, daß nur eine Trägermenge gegeben ist. Die Operationen müssen auf dieser Menge definiert sein und ihre Werte in dieser Menge annehmen. Damit sind zum Beispiel Vektorräume keine homogenen algebraischen Systeme. Um auch Vektorräume und andere Systeme, an denen mehrere Mengen beteiligt sind, mit zu erfassen, werden heterogene algebraische Systeme eingeführt.

3.4 Definition: Ein *heterogenes algebraisches System* ist ein Paar $(\{A_i\}_{i\in I}, \Omega)$. Dabei ist $\{A_i\}_{i\in I}$ eine durch die nichtleere Indexmenge I indizierte Menge nichtleerer Trägermengen und Ω eine Menge von Operationen, die wie folgt definiert sind: Jedem $\omega \in \Omega$ ist eine Dimension $n \in \mathbb{N}$ und ein $(n+1)$-Tupel $(i_1, i_2, \ldots, i_{n+1}) \in I^{n+1}$ zugewiesen, so daß ω eine Abbildung der Form

$$\omega\colon A_{i_1} \times A_{i_2} \times \cdots \times A_{i_n} \to A_{i_{n+1}}$$

ist.

Ein homogenes algebraisches System ist also ein heterogenes algebraisches System, bei dem die Indexmenge I genau ein Element enthält.

3.5 Beispiel: Ein Vektorraum V über einem Körper $\mathbb{K}$ ist eine heterogenes System mit $I = \{0, 1\}$. Es gilt $A_0 = \mathbb{K}$ und $A_1 = V$. Zu den Operationen gehören unter anderem Skalarmultiplikation, Addition und das Skalarprodukt. Die Skalarmultiplikation hat Dimension 2. Das zugehörige Tripel lautet $(0, 1, 1)$, denn bei der Skalarmultiplikation wird ein Element aus $A_0 = \mathbb{K}$ und ein Element aus $A_1 = V$ auf ein Element aus A_1 abgebildet. Bei der Vektoraddition wird zwei Vektoren ein neuer Vektor zugeordnet. Die Addition hat also Dimension 2 und das zugehörige Tripel lautet $(1, 1, 1)$. Das Skalarprodukt bildet zwei Vektoren auf einen Skalar ab. Sie hat also auch Dimension 2. Das zugehörige Tripel ist $(1, 1, 0)$.

3.6 Beispiel Automat: Ein *Automat* im Sinne der theoretischen Informatik ist ein heterogenes algebraisches System $((S, X, Z), \{\delta, \lambda\})$ mit den drei Trägermengen

$$S := \text{Menge der Zustände},$$
$$X := \text{Eingabealphabet},$$
$$Z := \text{Ausgabealphabet},$$

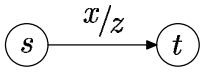
und den beiden Operationen

$$\begin{aligned} &\text{Folgezustandsfunktion:} && \delta\colon S \times X \to S, \\ &\text{Ausgabefunktion:} && \lambda\colon S \times X \to Z. \end{aligned}$$

Die Funktionen werden wie folgt definiert: Erhält der Automat im Zustand $s \in S$ die Eingabe $x \in X$, so wechselt er in den Zustand $\delta(s,x)$ und gibt $\lambda(s,x)$ aus.

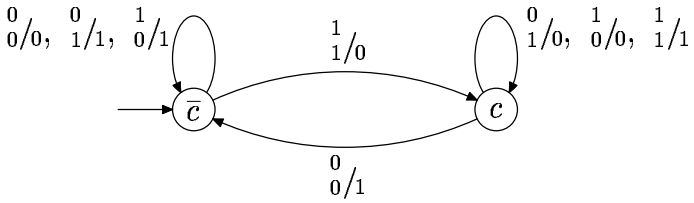
Die Idee ist nun wie folgt. Zu Beginn ist der Automat in einem Grundzustand s_0. Dann wird eine Folge von Symbolen $x_1, x_2, \ldots, x_n$ aus X der Reihe nach eingegeben. Dies führt zu einer Folge von Zuständen $s_0, s_1, \ldots, s_n$, wobei $s_i = \delta(s_{i-1}, x_i)$ für $i \in \{1, \ldots, n\}$. Außerdem wird eine Folge $z_1, \ldots, z_n$ von Symbolen aus Z erzeugt. Es gilt $z_i = \lambda(s_{i-1}, x_i)$ für $i \in \{1, \ldots, n\}$.

Sind $s, t \in S$ zwei Zustände, so bedeutet



daß der Automat, wenn er im Zustand s ist und die Eingabe x erhält, in den Zustand t wechselt und z ausgibt. Mit anderen Worten, $t = \delta(s,x)$ und $z = \lambda(s,x)$.

Wir betrachten nun konkret folgendes Beispiel, ein Automat zur binären Addition:



Es gilt

$$\begin{aligned} S &:= \{c, \overline{c}\}, \\ X &:= \left\{ \begin{matrix} 0 & 0 & 1 & 1 \\ 0\,' & 1\,' & 0\,' & 1 \end{matrix} \right\} \\ Z &:= \{0, 1\}. \end{aligned}$$

Der Zustand c steht für Übertrag, der Zustand $\overline{c}$ für keinen Übertrag. Der Grundzustand ist $\overline{c}$, was durch den Pfeil ohne Beschriftung angegeben wird.

Um die Arbeitsweise des Automaten sehen zu können, addieren wir die beiden Binärzahlen 1001 und 0011. Sie stehen für $1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 9$ und $0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 3$. Wir geben also der Reihe nach, von rechts nach links gelesen, die Paare

$$\begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{matrix}$$

ein. Aus dem obigen Diagramm lesen wir dann ab, ebenfalls von rechts nach links gelesen:

$$\overline{c} \xleftarrow{{}^{1}_{0}/1} \overline{c} \xleftarrow{{}^{0}_{0}/1} c \xleftarrow{{}^{0}_{1}/0} c \xleftarrow{{}^{1}_{1}/0} \overline{c}$$

Die Ausgabe ist also 1100. Dies entspricht $1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 12 = 9 + 3$.

Wir verlassen nun die heterogenen algebraischen Systeme. Das meiste, was wir nun für homogene algebraische Systeme zeigen, gilt so ähnlich auch für heterogene algebraische Systeme, nur daß der Aufwand an Notation viel größer ist.

3.3. Morphismen

In der Linearen Algebra werden lineare Abbildungen untersucht. Das sind Abbildungen zwischen Vektorräumen, die mit der Vektorraumstruktur verträglich sind. Auch in anderen Bereichen der Mathematik spielen strukturverträgliche Abbildungen eine wichtige Rolle. Selbst in dem abstrakten Kontext algebraischer Systeme, lassen sich strukturerhaltende Abbildungen definieren und untersuchen.

3.7 Definition: Ein *Typ von Algebren* ist eine nichtleere Menge $\mathcal{F}$ von Operationssymbolen zusammen mit einer Funktion $t\colon \mathcal{F} \to \mathbb{N}$. Für $n \in \mathbb{N}$ ist

$$\mathcal{F}_n := \{f \in \mathcal{F} \mid t(f) = n\}$$

die Menge der n-stelligen Operationssymbole.

Obwohl streng genommen ein Typ einer Algebra ein Paar $(\mathcal{F}, t)$ ist, wird meist nur $\mathcal{F}$ genannt.

3.8 Definition: Sei $\mathcal{F}$ eine Typ von Algebren und $\mathfrak{A} = (A, \Omega)$ ein algebraisches System. Dann ist $\mathfrak{A}$ ein *algebraisches System vom Typ* $\mathcal{F}$, falls es eine surjektive Abbildung $\tau_{\mathfrak{A}}\colon \mathcal{F} \to \Omega$ gibt mit $\alpha(\tau_{\mathfrak{A}}(f)) = t(f)$ für alle $f \in \mathcal{F}$.

Anstatt $\tau_{\mathfrak{A}}(f)$ schreiben wir auch $f^{\mathfrak{A}}$. Algebraische Systeme vom gleichen Typ heißen *ähnlich*.

Algebraische Systeme vom Typ $\mathcal{F} = \mathcal{F}_1 = \{f\}$ heißen *unitär*. Algebraische Systeme vom Typ $\mathcal{F} = \mathcal{F}_2 = \{f\}$ heißen *binär*.

Ist $\mathfrak{A}$ ein algebraisches System vom Typ $\mathcal{F}$ und $f \in \mathcal{F}$ ein Operationsymbol, so ist $f^{\mathfrak{A}}$ die zugehörige Operation. Die Operation hat natürlich die gleiche Stelligkeit wie das Symbol. Es wird nicht verlangt, daß die Zuordnung bijektiv ist. Eine Operation könnte also verschiedene Symbole haben, aber jede Operation hat mindestens ein Symbol. Für $f \in \mathcal{F}_2$ schreiben wir oft $x\ f\ y$ statt $f(x, y)$. Zum Beispiel ist $x + y$ gebräuchlicher als $+(x, y)$.

3.9 Definition: Seien $\mathfrak{A} = (A, \Omega)$ und $\mathfrak{A}' = (A', \Omega')$ ähnliche Systeme vom Typ $\mathcal{F}$. Ein *Morphismus* oder *Homomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{A}'$ ist eine Abbildung $h\colon A \to A'$ mit

$$h(f^{\mathfrak{A}}(a_1, \ldots, a_{t(f)})) = f^{\mathfrak{A}'}(h(a_1), \ldots, h(a_{t(f)}))$$

für jedes $f \in \mathcal{F}$ und $a_1, \ldots, a_{t(f)} \in A$.

Das heißt, daß im folgenden Abbildungsdiagramm beide Wege von A^n nach A' das gleiche liefern. Dabei gilt $f \in \mathcal{F}_n$ und $h^n(a_1, \ldots, a_n) = (h(a_1), \ldots, h(a_n))$. Ein solches Diagramm heißt *kommutierendes Diagramm.*

$$\begin{array}{ccc} A^n & \xrightarrow{f^{\mathfrak{A}}} & A \\ {\scriptstyle h^n}\downarrow & & \downarrow{\scriptstyle h} \\ (A')^n & \xrightarrow{f^{\mathfrak{A}'}} & A' \end{array}$$

Ein Morphismus h heißt

1. *Monomorphismus*, falls h injektiv ist,
2. *Epimorphismus*, falls h surjektiv ist,
3. *Isomorphismus*, falls h bijektiv ist.

3.10 Testfrage: Seien (A, Ω) und (A', Ω') ähnliche algebraische Systeme und $h\colon A \to A'$ ein Isomorphismus. Zeigen Sie, daß dann auch $h^{-1}\colon A' \to A$ ein Isomorphismus ist.

3.11 Beispiel: Sei $\mathcal{F} = \mathcal{F}_2 = \{f\}$ und $A := \{r \in \mathbb{R} \mid r > 0\}$. Dann sind $\mathfrak{R} := (\mathbb{R}, +)$ und $\mathfrak{A} := (A, \cdot)$ algebraische Systeme von Typ $\mathcal{F}$, da $+$ und $\cdot$ binäre Operationen sind. Es gilt also $f^{\mathfrak{R}} = +$ und $f^{\mathfrak{A}} = \cdot$.

Die Exponentialfunktion $\exp\colon \mathbb{R} \to A$ liefert einen Isomorphismus zwischen $(\mathbb{R}, +)$ und $(A, \cdot)$. Daß dies ein Isomorphismus ist, liegt am Exponentialgesetz. Für $a_1, a_2 \in \mathbb{R}$ gilt:

$$\begin{aligned} \exp(f^{\mathfrak{R}}(a_1, a_2)) &= \exp(a_1 + a_2) = e^{a_1 + a_2} \\ &= e^{a_1} \cdot e^{a_2} = \exp(a_1) \cdot \exp(a_2) = f^{\mathfrak{A}}(\exp(a_1), \exp(a_2)). \end{aligned}$$

Somit ist die Exponentialfunktion ein Morphismus. Da sie auf den angegebenen Mengen mit dem Logarithmus eine Umkehrfunktion besitzt, ist sie ein Isomorphismus.

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \xrightarrow{+} & \mathbb{R} \\ {\scriptstyle \exp \times \exp}\downarrow & & \downarrow{\scriptstyle \exp} \\ A \times A & \xrightarrow{\cdot} & A \end{array} \qquad \uparrow \log$$

Die Exponentialfunktion liefert also einen Isomorphismus zwischen der multiplikativen Struktur der reellen Zahlen und der additiven Struktur der positiven reellen Zahlen. Dieser Isomorphismus ist von großer theoretischer und praktischer Bedeutung. Der Rechenschieber basiert auf diesem Isomorphismus.

3.12 Testfrage: Sei $S := \{z \in \mathbb{C} \mid |z| = 1\}$. Ist $\mu\colon (\mathbb{R}, +) \to (S, \cdot)\colon r \mapsto e^{ir}$ ein Morphismus, ein Monomorphismus, eine Epimorphismus oder gar ein Isomorphismus?

3.13 Definition: Sei (A, Ω) ein algebraisches System. Eine Teilmenge $B \subset A$ definiert eine *Teilalgebra*, falls B abgeschlossen unter Ω ist, wenn also für jedes $\omega \in \Omega$ und jedes Tupel $(a_1, \ldots, a_{\alpha(\omega)}) \in B^{\alpha(\omega)}$ auch $\omega(a_1, \ldots, a_{\alpha(\omega)}) \in B$ gilt.

3.14 Bezeichnung: Definiert $B \subset A$ eine Teilalgebra von (A, Ω), so schreiben wir $(B, \Omega) \leq (A, \Omega)$ oder auch $B \leq A$.

3.15 Satz: *Sei $\mathcal{B}$ eine nichtleere Familie von Teilalgebren eines algebraischen Systems (A, Ω). Dann ist auch $\bigcap_{B \in \mathcal{B}} B$ eine Teilalgebra von (A, Ω).*

Beweis: Sei $\omega \in \Omega$ und $x_1, \ldots, x_{\alpha(\omega)} \in \bigcap_{B \in \mathcal{B}} B$. Dann gilt $x_1, \ldots, x_{\alpha(\omega)} \in B$ für jedes $B \in \mathcal{B}$. Da jedes $B \in \mathcal{B}$ eine Teilalgebra von (A, Ω) definiert, gilt $\omega(x_1, \ldots, x_{\alpha(\omega)}) \in B$ für jedes $B \in \mathcal{B}$. Daraus folgt $\omega(x_1, \ldots, x_{\alpha(\omega)}) \in \bigcap_{B \in \mathcal{B}} B$. Dies zeigt, daß $\bigcap_{B \in \mathcal{B}} B$ abgeschlossen unter Ω ist. □

3.16 Definition: Sei $\mathfrak{A} = (A, \Omega)$ ein algebraisches System und $\emptyset \neq H \subset A$. Sei

$$\mathcal{B} := \{B \mid H \subset B \leq A\}.$$

Dann definiert nach Satz 3.15 auch $[H] := \bigcap_{B \in \mathcal{B}} B$ eine Teilalgebra von $\mathfrak{A}$, die *von H erzeugte Teilalgebra.* Gilt $(A, \Omega) = ([H], \Omega)$, so heißt H eine *Erzeugendensystem* von $\mathfrak{A}$.

3.17 Bemerkung: Diese Definition beschreibt eine sogenannte ‚Konstruktion von oben'. Sie sichert problemlos ab, daß $[H]$ wohldefiniert ist. Um zu wissen, wie die Elemente von $[H]$ aussehen, ist die ‚Konstruktion von unten' geeigneter. Sie wird im nächsten Satz eingeführt.

Auch wenn Vektorräume keine (homogenen) algebraischen Systeme sind, so können Sie sich bei dem folgenden Satz und Beweis an Erzeugendensystemen von Untervektorräumen orientieren. (Ein entsprechender Satz gilt auch für heterogene algebraische Systeme, ist aber aufwendiger zu formulieren.) Beispiele für (homogene) algebraische Systeme folgen.

3.18 Satz: *Sei $\mathfrak{A} = (A, \Omega)$ ein algebraisches System und $\emptyset \neq H \subset A$. Eine Teilmenge $S \subset A$ ist genau dann gleich $[H]$ falls gilt:*

1. $H \subset S$,
2. $\forall \omega \in \Omega \, \forall (a_1, \ldots, a_{\alpha(\omega)}) \in S^{\alpha(\omega)} : \omega(a_1, \ldots, a_{\alpha(\omega)}) \in S$,
3. *Jedes Element aus S läßt sich aus Elementen von H durch eine endliche Kette von Operationen aus Ω gewinnen.*

Beweis: Die ersten beiden Anforderungen an S besagen, daß S eine Teilalgebra von $\mathfrak{A}$ ist, die H enthält. Nach Definition von $[H]$ gilt daher $[H] \subset S$.

Um die umgekehrte Inklusion zu zeigen, definieren wir rekursiv

$$S_0 := H,$$

$$S_{m+1} := S_m \cup \{x \in A \mid \exists \omega \in \Omega \, \exists (a_1, \ldots, a_{\alpha(\omega)}) \in S_m^{\alpha(\omega)} : x = \omega(a_1, \ldots, a_{\alpha(\omega)})\}.$$

Das heißt, S_{m+1} enthält neben den Elementen aus S_m alle Elemente aus A, die mit einer Operation aus Ω aus den Elementen in S_m gewonnen werden können.

Durch Induktion zeigen wir $S_m \subset [H]$ für jedes $m \in \mathbb{N}$. Für $m = 0$ ist die Aussage trivialerweise erfüllt. Sei nun $x \in S_{m+1}$. Falls x bereits in S_m liegt, so gilt nach Induktionsvoraussetzung $x \in [H]$. Liegt x nicht in S_m, so gibt es ein $\omega \in \Omega$ und ein Tupel $(a_1, \ldots, a_{\alpha(\omega)}) \in S_m^{\alpha(\omega)}$ mit $x = \omega(a_1, \ldots, a_{\alpha(\omega)})$. Nach Induktionsvoraussetzung gilt $S_m \subset [H]$, also $(a_1, \ldots, a_{\alpha(\omega)}) \in [H]^{\alpha(\omega)}$. Da $[H]$ als Teilalgebra abgeschlossen unter Ω ist, folgt $x = \omega(a_1, \ldots, a_{\alpha(\omega)}) \in [H]$. Dies zeigt $S_{m+1} \subset [H]$. Damit gilt

$$\bigcup_{m \in \mathbb{N}} S_m \subset [H] \subset S.$$

Die dritte Bedingung an S sagt aus, daß auch

$$S \subset \bigcup_{m \in \mathbb{N}} S_m$$

gilt. Damit folgt wie gewünscht $S = [H]$.

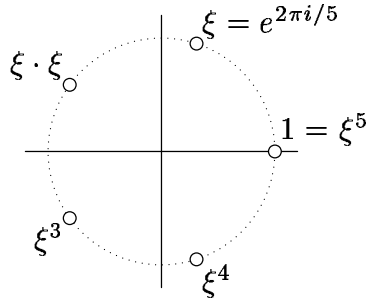
Zum Abschluß muß noch gezeigt werden, daß $[H]$ die drei Bedingungen erfüllt. Die ersten beiden Bedingungen sind nach Konstruktion von $[H]$ erfüllt. Gilt die dritte Bedingung nicht, so gibt es ein $x \in [H]$ mit $x \notin \bigcup_{m \in \mathbb{N}} S_m$, wobei die S_m wie oben definiert sind. Die Vereinigung $S := \bigcup_{m \in \mathbb{N}} S_m$ definiert eine Teilalgebra, die H enthält. Die rekursive Definition stellt nämlich sicher, daß S abgeschlossen bezüglich Ω ist. Doch dann ist S eine echte Teilmenge von $[H]$. Dies widerspricht der Definition von $[H]$. □

3.19 Bemerkung: Die im obigen Satz gezeigte Gleichheit der Konstruktion von oben und der Konstruktion von unten taucht in der Mathematik an verschiedenen

Stellen auf. In der Linearen Algebra wurde Ihnen dieses Prinzip am konkreten Beispiel der Vektorräume vorgeführt. In der Logik werden Sie es im Zusammenhang mit dem Hüllenoperator wiedersehen.

3.20 Beispiele:

1. Es gilt $(\mathbb{Z}, +, \cdot, 0, 1) = [\{-1\}]$. Wegen $1 = (-1) \cdot (-1)$ und $0 = (-1) + 1$ liegen 1 und 0 in $[\{-1\}]$. Jede andere Zahl $z \in \mathbb{Z}$ kann durch höchstens $|z|$ Additionen aus 1 oder -1 gewonnen werden. Tatsächlich sind wesentlich weniger Anwendungen der Addition und Multiplikation erforderlich.
2. Für $n \in \mathbb{N} \setminus \{0\}$ sei $W_n := \{z \in \mathbb{C} \mid z^n = 1\}$ die Menge der n-ten Einheitswurzeln in $\mathbb{C}$. Wir betrachten das algebraische System $\mathfrak{A} := (W_n, \cdot, 1)$. Dieses System ist eine Gruppe. Es gilt $\mathfrak{A} = [\{e^{\frac{2\pi i}{n}}\}]$.



$(W_5, \cdot, 1)$

3.21 Testfrage: Betrachten Sie das algebraische System $\mathfrak{A} := (W_n, \cdot, 1)$ aus dem obigen Beispiel. Wieviele und welche Elemente enthält W_n? Wo liegen diese Elemente in der komplexen Zahlenebene? Zeigen Sie oder widerlegen Sie durch ein Gegenbeispiel: Für jedes $\xi \in W_n \setminus \{1\}$ gilt $\mathfrak{A} = [\{\xi\}]$.

3.4. Unitäre Algebren

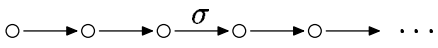
Wir untersuchen nun algebraische Systeme mit nur einer Operation, die zudem noch einstellig ist. Wir erhalten einen vollständigen Überblick über alle solche Systeme.

3.22 Definition: Ein algebraisches System $\mathfrak{A} = (S, \Omega)$ ist eine *unitäre Algebra*, falls Ω nur aus einer einstelligen Operation besteht, das heißt, falls es eine Abbildung $\omega\colon S \to S$ gibt, so daß $\Omega = \{\omega\}$.

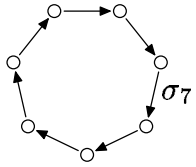
Eine unitäre Algebra ist also ein algebraisches System vom Typ $\mathcal{F} = \mathcal{F}_1 = \{f\}$.

3.23 Beispiele:

1. Die natürlichen Zahlen $\mathbb{N}$ mit der Nachfolgerabbildung σ sind eine unitäre Algebra. Diese unitäre Algebra $(\mathbb{N}, \sigma)$ heißt *Peano-Algebra*. Wir haben in Abschnitt 2.1 gezeigt, daß $(\mathbb{N}, \sigma)$ die natürlichen Zahlen mitsamt der Rechenoperationen bestimmt.
2. Für $n \in \mathbb{N}$ sei $S_n := \{1, 2, \ldots, n\}$ und
$$\sigma_n \colon S_n \to S_n \colon k \mapsto \begin{cases} k+1 & \text{falls } k < n, \\ 1 & \text{falls } k = n. \end{cases}$$
Dann ist (S_n, σ_n) eine unitäre Algebra, die *Uhr-Algebra*.



$(\mathbb{N}, \sigma)$



(S_7, σ_7)

3.24 Testfrage: Führen Sie auf der Uhr-Algebra (S_n, σ_n) wie für die natürlichen Zahlen aus der Funktion σ_n rekursiv Addition und Multiplikation ein. Die Struktur, die Sie erhalten, sollte Ihnen bekannt vorkommen. Welche ist es?

3.25 Definition: Sei $\mathfrak{A} = (S, \omega)$ eine unitäre Algebra. Eine Teilmenge $T \subset S$ heißt ω-abgeschlossen, falls für jedes $t \in T$ auch $\omega(t) \in T$ gilt.

3.26 Bemerkung: Aus dieser Definition folgt unmittelbar, daß ω-abgeschlossene Teilmengen genau die Teilmengen sind, die Teilalgebren definieren.

3.27 Beispiele:

1. In der Peano-Algebra $(\mathbb{N}, \sigma)$ ist für jedes $n \in \mathbb{N}$ die Menge $\{m \in \mathbb{N} \mid n \leq m\}$ eine σ-abgeschlossene Menge. Die einzige andere σ-abgeschlossene Menge ist die leere Menge.
2. In der Uhr-Algebra (S_n, σ_n) sind $\emptyset$ und S_n die einzigen σ_n-abgeschlossenen Mengen.

Für die Peano-Algebra gilt $(\mathbb{N}, \sigma) = [\{0\}]$. Das ist der Grund, warum Induktionsbeweise funktionieren. Für Uhr-Algebren gilt $(S_n, \sigma_n) = [\{1\}]$. Gibt es sonst noch unitäre Algebren, die von einem Element erzeugt werden?

3.28 Definition: Sei (S, ω) eine unitäre Algebra. Durch

$$\omega^0(s) := s,$$
$$\omega^{n+1} := \omega(\omega^n(s))$$

wird für jedes $n \in \mathbb{N}$ eine Abbildung ω^n auf S definiert.

3.29 Lemma: *Sei (S, ω) eine unitäre Algebra und $a \in S$. Dann ist die Abbildung $\Theta\colon \mathbb{N} \to S\colon n \mapsto \omega^n(a)$ ein Morphismus von $(\mathbb{N}, \sigma)$ nach (S, ω).*

Beweis: Für $n \in \mathbb{N}$ gilt

$$\Theta(\sigma(n)) = \Theta(n+1) = \omega^{n+1}(a) = \omega(\omega^n(a)) = \omega(\Theta(n)).$$

Damit ist Θ ein Morphismus. □

3.30 Satz: *Ist $\mathfrak{A} = (S, \omega)$ eine unitäre Algebra und $a \in S$ mit $\mathfrak{A} = [\{a\}]$, so ist der oben definierte Morphismus $\Theta\colon (\mathbb{N}, \sigma) \to (S, \omega)$ ein Epimorphismus.*

Beweis: Sei $s \in S$. Wegen $\mathfrak{A} = [\{a\}]$ gibt es ein $n \in \mathbb{N}$ mit $s = \omega^n(a)$, also $s = \Theta(n)$. Daher ist Θ surjektiv und wegen Lemma 3.29 ein Epimorphismus. □

Wir wollen nun alle unitäre Algebren, die von einem einzelnen Element erzeugt werden können, bestimmen.

3.31 Klassifikation: Sei $\mathfrak{A} = (S, \omega)$ eine unitäre Algebra und $a \in S$ mit $\mathfrak{A} = [\{a\}]$ sowie $\Theta\colon (\mathbb{N}, \sigma) \to (S, \omega)$ der oben untersuchte Epimorphismus.

Sind alle $\omega^n(a)$ paarweise verschieden, d.h. gilt $\omega^n(a) \neq \omega^m(a)$ für $n \neq m$, so ist Θ ein Isomorphismus.

Sind nicht alle $\omega^n(a)$ paarweise verschieden, so gibt es $n \in \mathbb{N}$ und $p \in \mathbb{N} \setminus \{0\}$ mit

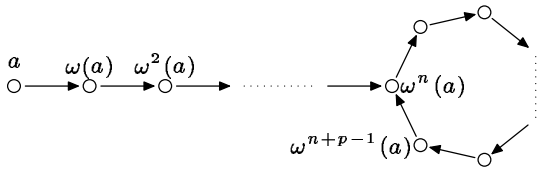
1. $\omega^{n+p}(a) = \omega^n(a)$.
2. $\forall k < n\ \forall l \neq k\colon \omega^k(a) \neq \omega^l(a)$,
3. $\forall 0 < k < p\colon \omega^{n+k}(a) \neq \omega^n(a)$.

Mit anderen Worten, n ist die kleinste Zahl, so daß es ein $m \neq n$ gibt mit $\omega^n(a) = \omega^m(a)$ und p ist die kleinste Zahl mit $\omega^{n+p}(a) = \omega^n(a)$.

Induktion liefert, daß für jedes $m \in \mathbb{N}$ mit $n \leq m$ gilt:

1. $\forall 0 < k < p\colon \omega^{m+k}(a) \neq \omega^m(a)$,
2. $\omega^{m+p}(a) = \omega^m(a)$.

Das heißt, die Menge $\{\omega^n(a), \ldots, \omega^{n+p-1}(a)\}$ definiert eine Teilalgebra, die zur Uhr-Algebra (S_p, σ_p) isomorph ist. Gilt $n = 0$, so ist (S, ω) isomorph zu (S_p, σ_p). Im allgemeinen Fall hat (S, ω) folgendes Diagramm:



3.5. Binäre Algebren

Wir untersuchen nun algebraische Systeme mit nur einer Operation, die zudem noch zweistellig ist. Im Gegensatz zum unitären Fall gibt es nun eine unüberschaubare Vielfalt nichtisomorpher Systeme. Prominenteste Beispiele algebraischer Systeme mit genau einer binären Operation sind Gruppen. Aber auch für Gruppen ist eine vollständige Übersicht aussichtslos. Eine der größten mathematischer Leistungen der letzten Jahrzehnte war die Klassifikation aller endlichen einfachen Gruppen. Und bereits diese Klassifikation war, obwohl sie sich auf ein sehr kleines Feld von Gruppen beschränkt, enorm kompliziert und arbeitsintensiv.

3.32 Definition: Ein algebraisches System $\mathfrak{A} = (S, \Omega)$ ist eine *binäre Algebra*, falls Ω nur aus einer zweistelligen Operation besteht, das heißt, falls es eine Abbildung $\beta\colon S^2 \to S$ gibt, so daß $\Omega = \{\beta\}$.

Eine binäre Operation β heißt *assoziativ*, falls $\beta(\beta(x, y), z) = \beta(x, \beta(y, z))$ für alle $x, y, z \in S$ gilt.

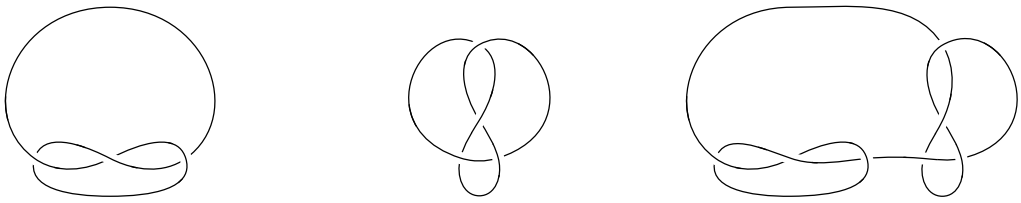
Eine binäre Operation β heißt *kommutativ*, falls $\beta(x, y) = \beta(y, x)$ für alle $x, y \in S$ gilt.

Eine binäre Algebra ist also ein algebraisches System vom Typ $\mathcal{F} = \mathcal{F}_2 = \{f\}$.

3.33 Bezeichnung: Statt $\beta(x, y)$ schreiben wir auch $x\beta y$. Besonders gebräuchlich sind die Schreibweisen $x + y$, $x \cdot y$ und xy.

3.34 Definition: Eine binäre Algebra (S, β) heißt *Halbgruppe*, falls β assoziativ ist.

Ein *Monoid* ist eine Halbgruppe mit *Einselement*, das heißt, es gibt ein Element $1 \in S$ mit $\beta(1, x) = \beta(x, 1) = x$ für alle $x \in S$.



K_1 K_2 $K_1\#K_2$

3.35 Beispiele: Monoide sind eine weitverbreitete Struktur. Die Menge der (mathematischen) Knoten bildet bezüglich einer natürlichen binären Operation # ein Monoid.

In der Theorie der formalen Sprachen tauchen ebenfalls Monoide auf. Sei $A = \{a, b, c, \dots\}$ das Alphabet der Sprache und S die Menge der Worte, die man mit Elementen aus A bilden kann, dabei ist ein Wort eine endliche Folge von Elementen aus A. (Wer Programmiererfahrung hat, sollte an ‚Strings' denken.) Die binäre Operation β ist einfach das Aneinanderfügen von zwei Wörtern. Ist A zum Beispiel das gewöhnliche Alphabet, so gilt $\beta(\text{spiel}, \text{ball}) = \text{spielball}$. Das leere Wort, also das Wort, das keinen Buchstaben enthält, ist ein Einselement. Daher ist (S, β) ein Monoid. Sie sehen an diesem Beispiel auch, daß β nicht kommutativ ist.

3.36 Testfrage: Fast alle Programmiersprachen kennen Strings und das Verknüpfen von Strings. Wie lautet in der Programmiersprache Ihrer Wahl der binäre Operator für das Verknüpfen von Strings und wie wird das leere Wort dargestellt?

3.37 Definition: Eine *Gruppe* ist ein Monoid (S, β) mit Einselement 1, so daß es für jedes $x \in S$ ein $y \in S$ mit $\beta(x, y) = \beta(y, x) = 1$ gibt. Dieses y heißt das *Inverse* von x und wird oft mit x^{-1} bezeichnet.

3.38 Bezeichnung: Ist die Gruppenoperation kommutativ, so wird üblicherweise $(G, +)$ geschrieben. Das Neutralelement heißt dann *Nullelement* oder *Null* und wird mit 0 statt 1 bezeichnet. Das Inverse eines Elements $g \in G$ wird mit $-g$ bezeichnet.

3.39 Beispiele für Monoide und Gruppen:

1. Für eine nichtleere Menge X sei $S := X^X$ die Menge aller Abbildungen auf X und $\beta = \circ$ das Hintereinanderausführen von Abbildungen. Dann ist $(X^X, \circ)$ ein Monoid. Die identische Abbildung ist das Einselement. Sofern X mindestens zwei Elemente hat, ist $(X^X, \circ)$ keine Gruppe.

2. Für eine nichtleere Menge X sie S die Menge aller Relationen auf X und $\beta = \circ$ das Verknüpfen von Relationen. Dann ist $(S, \circ)$ ein Monoid. Die Gleichheitsrelation ‚=' ist das Einselement. Dieses Monoid ist nie eine Gruppe, da die leere Relation kein Inverses besitzt.
3. Für eine nichtleere Menge X sei $S(X)$ die Menge aller bijektiven Abbildungen auf X und $\beta = \circ$ das Hintereinanderausführen von Abbildungen. Dann ist $(S(X), \circ)$ eine Gruppe, die *Permutationsgruppe* von X. Da die Abbildungen bijektiv sind, gibt es stets ein Inverses.
4. Ist $X \neq \emptyset$ eine endliche Menge mit n Elementen, so heißt $(S(X), \circ)$ die *symmetrische Gruppe auf n Elementen.* Sie wird oft mit S_n bezeichnet. Eine einfacher Induktionsbeweis zeigt, daß S_n genau $n!$ Elemente enthält.
5. Ein algebraisches System $(R, +, \cdot, 0, 1)$ ist genau dann ein Ring, wenn $(R, +, 0)$ eine kommutative Gruppe und $(R \setminus \{0\}, \cdot, 1)$ ein Monoid ist, so daß die Distributivgesetze gelten.

3.40 Testfragen:

1. Weisen Sie nach, daß für eine Menge X mit mindestens zwei Elementen das Monoid $(X^X, \circ)$ keine Gruppe ist
2. Bestimmen Sie alle $n \in \mathbb{N} \setminus \{0\}$, für die S_n kommutativ ist.

3.6. Direktes Produkt

Wir wollen nun Methoden vorstellen, wie aus gegebenen algebraischen Systemen neue algebraische Systeme konstruiert werden können. Zunächst stellen wir das direkte Produkt algebraischer Systeme vor. Dafür müssen wir zuerst erklären, was das Produkt beliebiger Mengen ist.

3.41 Definition: Seien X_i, $i \in I$, Mengen, die durch eine Indexmenge I indiziert werden. Dann ist

$$\prod_{i \in I} X_i := \{x \colon I \to \bigcup_{i \in I} X_i \mid \forall i \in I \colon x(i) \in X_i\} \subset \Big(\bigcup_{i \in I} X_i\Big)^I$$

das *Produkt der Mengen X_i, $i \in I$.*

Für $j \in I$ ist $\pi_j \colon \prod_{i \in I} X_i \to X_j \colon x \mapsto x(j)$ die *j-te Projektion.*

Wie für Produkte X^Y ist das Produkt $\prod_{i \in I} X_i$ also eine Menge von Abbildungen. Falls I endlich ist, lassen sich die Elemente des Produkts auch als Tupel darstellen.

3.42 Beispiele:

1. Gibt es eine Menge X mit $\forall i \in I \colon X = X_i$, so gilt $\prod_{i \in I} X_i = X^I$.

2. Für $I = \{1, 2, \ldots, n\}$ gilt

$$\prod_{i \in I} X_i = \prod_{i=1}^{n} X_i = X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid \forall i \in I\colon x_i \in X_i\}.$$

Sofern die Mengen X_i Trägermengen ähnlicher algebraischer Systeme sind, kann auch das Produkt zu einem algebraischen System gemacht werden. Ein Operator wirkt auf dem Produkt, indem er auf den einzelnen Faktoren wirkt.

3.43 Definition: Sei $\mathcal{F}$ ein Typ von Algebren und seien $\mathfrak{A}_i = (A_i, \Omega_i)$, $i \in I$, Algebren vom Typ $\mathcal{F}$. Sei $A := \prod_{i \in I} A_i$. Für $f \in \mathcal{F}$ und $a_1, \ldots, a_{t(f)} \in A$ wird die Operation $f^{\mathfrak{A}}$ auf A definiert durch:

$$\forall i \in I\colon f^{\mathfrak{A}}(a_1, \ldots, a_{t(f)})(i) := f^{\mathfrak{A}_i}(a_1(i), \ldots, a_{t(f)}(i)).$$

Dann ist $\prod_{i \in I} \mathfrak{A}_i := (A, \{f^{\mathfrak{A}} \mid f \in \mathcal{F}\})$ eine Algebra vom Typ $\mathcal{F}$, das *direkte Produkt der Algebren* $\mathfrak{A}_i$, $i \in I$.

3.44 Beispiel: Sei $\mathfrak{A}_1 = \mathfrak{A}_2 = (\mathbb{Z}, +, \cdot, 0, 1)$. Dann ist $\mathfrak{A}_1 \times \mathfrak{A}_2$ die Struktur $(\mathbb{Z} \times \mathbb{Z}, +, \cdot, (0,0), (1,1))$. Dabei gilt:

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &= \{(a, b) \mid a, b \in \mathbb{Z}\}, \\ (a, b) + (c, d) &= (a + b, c + d), \\ (a, b) \cdot (c, d) &= (a \cdot b, c \cdot d). \end{aligned}$$

3.45 Testfragen:

1. Seien $\mathfrak{A}_1$ und $\mathfrak{A}_2$ ähnliche algebraische Systeme. Zeigen Sie, daß $\mathfrak{A}_1 \times \mathfrak{A}_2$ und $\mathfrak{A}_2 \times \mathfrak{A}_1$ isomorph sind.
2. Seien $\mathfrak{A}_i = (A_i, \Omega_i)$, $i \in I$, ähnliche algebraische Systeme. Zeigen Sie, daß für jedes $j \in I$ die j-te Projektion $\pi_j\colon \prod_{i \in I} A_i \to A_j$ ein Epimorphismus ist.
3. Zeigen Sie oder widerlegen Sie durch ein Gegenbeispiel:
   (a) Sind $\mathfrak{A}_1$ und $\mathfrak{A}_2$ Ringe, so ist auch $\mathfrak{A}_1 \times \mathfrak{A}_2$ ein Ring.
   (b) Sind $\mathfrak{A}_1$ und $\mathfrak{A}_2$ Körper, so ist auch $\mathfrak{A}_1 \times \mathfrak{A}_2$ ein Körper.

3.7. Quotientenalgebra

Eine Äquivalenzrelation auf einer Menge A ist eine reflexive, symmetrische und transitive Relation auf A. Gibt es eine Menge Ω von Operationen auf A, so interessieren uns speziell solche Äquivalenzrelationen, die mit den Operationen aus Ω verträglich sind. Für Äquivalenzrelationen bildet die Menge der Äquivalenzklassen auf naheliegende Weise eine Algebra. Diese Algebra kann auch als epimorphes Bild

der ursprünglichen Algebra gewonnen werden. Aber auch die umgekehrte Aussage ist wahr. Jedes epimorphe Bild eines algebraischen Systems läßt sich durch eine Äquivalenzrelation gewinnen. Der erste Isomorphiesatz und der Begriff des Kerns eines Morphismuses verbinden diese beiden Konstruktionen.

3.46 Definition: Eine *Kongruenzrelation* auf einem algebraischen System $\mathfrak{A} = (A, \Omega)$ ist eine Äquivalenzrelation $\equiv$ auf A, die mit allen $\omega \in \Omega$ verträglich ist. Das heißt, für alle $\omega \in \Omega$ und für alle $(a_1, \ldots, a_{\alpha(\omega)}), (b_1, \ldots, b_{\alpha(\omega)}) \in A^{\alpha(\omega)}$ mit $a_i \equiv b_i$ für alle $i \in \{1, \ldots, \alpha(\omega)\}$, gilt $\omega(a_1, \ldots, a_{\alpha(\omega)}) \equiv \omega(b_1, \ldots, b_{\alpha(\omega)})$.

3.47 Beispiel: Sei $(\mathbb{Z}, +, \cdot, -, 0, 1)$ der Ring der ganzen Zahlen. Dabei steht $-$ für die unitäre Operation, die jeder ganzen Zahl ihr negatives zuordnet. Auf diesem algebraischen System definiert jedes $m \in \mathbb{N} \setminus \{0, 1\}$ eine Äquivalenzrelation $\equiv_m$ durch

$$a \equiv_m b \;:\Leftrightarrow\; m \mid (b - a).$$

Daß dies eine Äquivalenzrelation ist, wurde in Beispiel 1.37.4 gezeigt. Diese Äquivalenzrelation ist sogar eine Kongruenzrelation. Dies wird für die einzelnen Operationen und festes m nachgewiesen. Wir schreiben abkürzend $\equiv$ statt $\equiv_m$. Im folgenden gilt stets $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $a_1 \equiv b_1$ und $a_2 \equiv b_2$. Es gibt also $t_1, t_2 \in \mathbb{Z}$ mit $b_i - a_i = t_i m$, $i \in \{1, 2\}$.

1. Sei ω die Addition. Wegen

   $$(b_1 + b_2) - (a_1 + a_2) = (b_1 - a_1) + (b_2 - a_2) = t_1 m + t_2 m = (t_1 + t_2)m$$

   gilt $\omega(a_1, a_2) = a_1 + a_2 \equiv b_1 + b_2 = \omega(b_1, b_2)$. Die Relation ist also mit der Addition verträglich.
2. Sei ω die Multiplikation. Wegen

   $$\begin{aligned} b_1 \cdot b_2 - a_1 \cdot a_2 &= b_1 \cdot b_2 - a_1 \cdot b_2 + a_1 \cdot b_2 - a_1 \cdot a_2 \\ &= (b_1 - a_1) \cdot b_2 + a_1 \cdot (b_2 - a_2) \\ &= t_1 b_2 m + t_2 a_1 m = (t_1 b_2 + t_2 a_1)m \end{aligned}$$

   gilt $\omega(a_1, a_2) = a_1 \cdot a_2 \equiv b_1 \cdot b_2 = \omega(b_1, b_2)$. Die Relation ist also auch mit der Multiplikation verträglich.
3. Wegen $(-b_1 - (-b_1)) = -(b_1 - a_1) = (-t_1)m$ ist die unitäre Operation $-$ mit der Relation verträglich..

Für die nullstelligen Operationen muß nichts gezeigt werden. Damit liegt in der Tat für jedes $m \in \mathbb{N}$ eine Kongruenzrelation vor.

3.48 Testfrage: Sei $(R, +, \cdot, 0, 1)$ ein Ring und I ein Ideal in R. Zeigen Sie, daß durch $a \equiv b \iff b - a \in I$ eine Kongruenzrelation auf R definiert wird.

Für eine Äquivalenzrelation $\equiv$ auf einer Menge A ist der Quotient $A/\equiv$ von A nach $\equiv$ definiert. Ist Ω eine Menge von Operationen, die auf A wirken und ist die Relation $\equiv$ mit allen Operationen aus Ω verträglich, so induzieren die Operationen aus Ω Operationen auf dem Quotienten $A/\equiv$. Der Quotient wird also wieder ein algebraisches System, das ähnlich zu (A, Ω) ist.

3.49 Satz: *Sei $\mathfrak{A} = (A, \Omega)$ ein algebraisches System und $\equiv$ eine Kongruenzrelation auf $\mathfrak{A}$. Sei $A/\equiv$ die Menge der Äquivalenzklassen. Für $\omega \in \Omega$ sei $\overline{\omega}$ definiert durch:*

$$\overline{\omega}([a_1], \ldots, [a_{\alpha(\omega)}]) = [\omega(a_1, \ldots, a_{\alpha(\omega)})].$$

Da $\equiv$ eine Kongruenzrelation ist, ist $\overline{\omega}$ wohldefiniert.
Nach Konstruktion gilt $\alpha(\overline{\omega}) = \alpha(\omega)$. Sei $\overline{\Omega} := \{\overline{\omega} \mid \omega \in \Omega\}$. Es gilt:

1. *$(A/\equiv, \overline{\Omega})$ ist ein algebraisches System, das ähnlich zu (A, Ω) ist.*
2. *Die Abbildung $\pi\colon A \to A/\equiv\colon x \mapsto [x]$ ist ein Epimorphismus.*

Beweis: Für die erste Aussage ist nachzuweisen, daß die Elemente $\overline{\omega} \in \overline{\Omega}$ tatsächlich Operationen auf $A/\equiv$ sind. Sei $\omega \in \Omega$ und $(a_1, \ldots, a_{\alpha(\omega)}), (b_1, \ldots, b_{\alpha(\omega)}) \in A^{\alpha(\omega)}$ mit $[a_i] = [b_i]$, also $a_i \equiv b_i$, für $i \in \{1, \ldots, \alpha(\omega)\}$. Da $\equiv$ eine Kongruenzrelation ist, gilt $\omega(a_1, \ldots, a_{\alpha(\omega)}) \equiv \omega(b_1, \ldots, b_{\alpha(\omega)})$, also $[\omega(a_1, \ldots, a_{\alpha(\omega)})] = [\omega(b_1, \ldots, b_{\alpha(\omega)})]$.

Nach Definition von $\overline{\omega}$ folgt $\overline{\omega}([a_1], \ldots, [a_{\alpha(\omega)}]) = \overline{\omega}([b_1], \ldots, [b_{\alpha(\omega)}])$, das heißt, $\overline{\omega}$ ist wohldefiniert und eine Operation auf $A/\equiv$ mit der selben Stelligkeit wie ω. Damit ist $(A/\equiv, \overline{\Omega})$ ein zu $\mathfrak{A}$ ähnliches algebraische System.

Wir zeigen nun, daß die Abbildung $\pi\colon A \to A/\equiv\colon x \mapsto [x]$ ein Epimorphismus ist. Nach Konstruktion von $A/\equiv$ ist π surjektiv. Daher muß lediglich gezeigt werden, daß π ein Morphismus ist. Für $\omega \in \Omega$ und $(a_1, \ldots, a_{\alpha(\omega)}) \in A^{\alpha(\omega)}$ gilt:

$$\begin{aligned}
\pi(\omega(a_1, \ldots, a_{\alpha(\omega)})) &= [\omega(a_1, \ldots, a_{\alpha(\omega)})] && \text{Definition von } \pi \\
&= \overline{\omega}([a_1], \ldots, [a_{\alpha(\omega)}]) && \text{Definition von } \overline{\omega} \\
&= \overline{\omega}(\pi(a_1), \ldots, \pi(a_{\alpha(\omega)})) && \text{Definition von } \pi
\end{aligned}$$

Damit ist π ein Morphismus. □

Satz 3.49 besagt, daß jede Kongruenzrelation auf einem algebraischen System $\mathfrak{A}$ einen Epimorphismus von $\mathfrak{A}$ auf ein ähnliches System $\mathfrak{A}'$ induziert. Uns interessiert nun, ob diese Konstruktion auch umgedreht werden kann. Das heißt, wir wollen

untersuchen, ob jeder Epimorphismus von $\mathfrak{A}$ auf ein ähnliches System $\mathfrak{A}'$ eine Kongruenzrelation auf $\mathfrak{A}$ induziert, bzw. von einer Kongruenzrelation auf $\mathfrak{A}$ induziert wird.

3.50 Beispiel: Wir betrachten zunächst wieder den Ring $(\mathbb{Z}, +, \cdot, -, 0, 1)$ der ganzen Zahlen mit der Kongruenzrelation $\equiv_m$, die wir mit $\equiv$ abkürzen. Gemäß Satz 3.49 ist die Abbildung $\pi\colon \mathbb{Z} \to \mathbb{Z}_m\colon a \mapsto [a]$ ein Epimorphismus. Nach Lemma 1.36 gilt $a \equiv b$ genau dann, wenn $[a] = [b]$ gilt. Das heißt, $a \equiv b \iff \pi(a) = \pi(b)$. Als Teilmenge von A^2 entspricht die Relation $\equiv$ daher der Menge $\{(a, b) \in A^2 \mid \pi(a) = \pi(b)\}$.

Wir verallgemeinern die Konstruktion dieser Menge für beliebige Morphismen.

3.51 Definition: Sei $f\colon (A, \Omega) \to (A', \Omega')$ ein Morphismus zwischen ähnlichen algebraischen Systemen. Dann heißt

$$\ker(f) := \{(a, b) \in A^2 \mid f(a) = f(b)\} \subset A \times A$$

der *Kern von* f.

3.52 Bemerkung: In der Linearen Algebra ist der Kern $\mathrm{Kern}(\varphi)$ einer linearen Abbildung $\varphi\colon V_1 \to V_2$ definiert durch $\mathrm{Kern}(\varphi) = \{v \in V_1 \mid \varphi(v) = 0\}$. Ähnlich ist der Kern eines Gruppenhomomorphismuses definiert. Diese Kerne sind zwar verschiedene Objekte als die in Definition 3.51 definierten Kerne, tragen aber die gleiche Information. Zum Beispiel gilt für eine lineare Abbildung φ:

$$(v, w) \in \ker(\varphi) \iff w - v \in \mathrm{Kern}(\varphi).$$

3.53 Satz: *Ist* $f\colon (A, \Omega) \to (A', \Omega')$ *ein Morphismus zwischen ähnlichen algebraischen Systemen, so ist* $\ker(f)$ *eine Kongruenzrelation auf* $\mathfrak{A} = (A, \Omega)$.

Beweis: Das Mengensystem $\{f^{-1}(a) \mid a \in f(A) \subset A'\}$ ist eine Partition von A. Wegen Satz 1.41 ist $\ker(f)$ eine Äquivalenzrelation auf A. Es muß also nur noch gezeigt werden, daß $\ker(f)$ mit den Operationen aus Ω verträglich ist.

Sei $\omega \in \Omega$ und $(a_i, b_i) \in \ker(f)$, $i \in \{1, \ldots, \alpha(\omega)\}$. Dann gilt:

$$\begin{aligned} f(\omega(a_1, \ldots, a_{\alpha(\omega)})) &= \omega(f(a_1), \ldots, f(a_{\alpha(\omega)})) && f \text{ ist Morphismus,} \\ &= \omega(f(b_1), \ldots, f(b_{\alpha(\omega)})) && (a_i, b_i) \in \ker(f), \\ &= f(\omega(b_1, \ldots, b_{\alpha(\omega)})) && f \text{ ist Morphismus,} \end{aligned}$$

also $(\omega(a_1, \ldots, a_{\alpha(\omega)}), \omega(b_1, \ldots, b_{\alpha(\omega)})) \in \ker(f)$. Damit ist $\ker(f)$ eine Kongruenzrelation. □

3.54 Bezeichnung: Sind $\mathfrak{A} = (A, \Omega)$ und $\mathfrak{A}' = (A', \Omega')$ ähnliche algebraische Systeme und ist $f\colon \mathfrak{A} \to \mathfrak{A}'$ ein Morphismus, so wird die gemäß Satz 3.49 aus der Kongruenzrelation $\ker(f)$ gebildete Quotientenalgebra $\overline{\mathfrak{A}} = (\overline{A}, \overline{\Omega})$ mit $\mathfrak{A}/\ker(f)$ oder $A/\ker(f)$ bezeichnet.

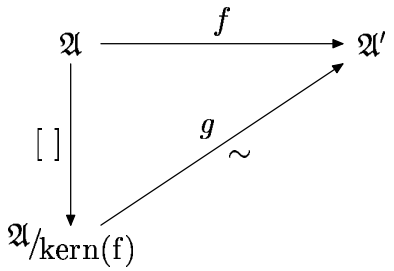
Wir zeigen nun, daß die Konstruktion aus Satz 3.49 auch umgekehrt werden kann.

3.55 Satz (1. Isomorphiesatz): *Sind $\mathfrak{A} = (A, \Omega)$ und $\mathfrak{A}' = (A', \Omega')$ ähnliche algebraische Systeme und ist $f\colon \mathfrak{A} \to \mathfrak{A}'$ ein Epimorphismus, so ist*

$$g\colon \mathfrak{A}/\ker(f) \to \mathfrak{A}'\colon [a] \mapsto f(a)$$

ein Isomorphismus.

Beweis: Da f ein Epimorphismus ist, ist f surjektiv. Also ist auch g surjektiv.



Für $a, b \in A$ gilt:

$$\begin{aligned} g([a]) = g([b]) &\iff f(a) = f(b) \\ &\iff (a, b) \in \ker(f) \\ &\iff [a] = [b] \end{aligned}$$

Damit ist g injektiv. Sei $\omega \in \Omega$ und $a_1, \ldots, a_{\alpha(\omega)} \in A$. Sei $\overline{\omega}$ bzw. ω' die zu ω gehörende Operation in $\overline{\Omega}$ bzw. Ω'. Dann gilt

$$\begin{aligned} g(\overline{\omega}([a_1], \ldots, [a_{\alpha(\omega)}])) &= g([\omega(a_1, \ldots, a_{\alpha(\omega)})]) && \ker(f) \text{ ist Kongruenzrelation,} \\ &= f(\omega(a_1, \ldots, a_{\alpha(\omega)})) && \text{Definition von } g, \\ &= \omega'(f(a_1), \ldots, f(a_{\alpha(\omega)})) && f \text{ ist Morphismus,} \\ &= \omega'(g([a_1]), \ldots, g([a_{\alpha(\omega)}])) && \text{Definition von } g. \end{aligned}$$

Damit ist g ein Morphismus. □

Die Sätze 3.55 und 3.49 besagen, daß Kongruenzrelationen, Quotientenalgebren und Epimorphismen zwischen Algebren äquivalente Konzepte sind.

3.56 Testfrage: Sei $\mathbb{R}[x]$ der Polynomring über $\mathbb{R}$ und $I := (x^2+1)$ das von x^2+1 aufgespannte Ideal. Nach Testfrage 3.48 wird durch $p \equiv q \iff q - p \in I$ eine Kongruenzrelation auf $\mathbb{R}[x]$ definiert. Zeigen Sie, daß die Quotientenalgebra $\mathbb{R}[x]/_{\equiv}$ isomorph zu $(\mathbb{C}, +, \cdot, 0, 1)$ ist.

3.57 Definition: Sei $\mathcal{F}$ ein Typ von Algebren. eine Menge $\mathcal{K}$ von algebraischen Systemen vom Typ $\mathcal{F}$ heißt *Varietät*, falls gilt:

1. Ist $\mathfrak{A} \in \mathcal{K}$ und ist $\mathfrak{A}'$ eine Unteralgebra von $\mathfrak{A}$, so folgt $\mathfrak{A}' \in \mathcal{K}$.
2. Ist $\mathfrak{A}_i \in \mathcal{K}$, $i \in I$, so ist das Produkt $\prod_{i \in I} \mathfrak{A}_i$ ebenfalls in $\mathcal{K}$.
3. Ist $\mathfrak{A} \in \mathcal{K}$, und f ein Epimorphismus von $\mathfrak{A}$ nach $\mathfrak{A}'$, so folgt $\mathfrak{A}' \in \mathcal{K}$.

3.58 Testfrage: Zeigen Sie, daß die Menge aller Gruppen eine Varietät bildet.

3.8. Terme und Termalgebren

Ein algebraisches System $\mathfrak{A} = (A, \Omega)$ besteht aus einer Trägermenge A und einer Menge Ω von Operatoren. Wir wollen nun die rein formalen Aspekte dieser Konstruktion untersuchen. Dies führt zu den Begriffen ‚Term' und ‚Termalgebra'.

Gegeben ist ein Menge X von Symbolen und ein Typ $\mathcal{F}$ von Algebren. Für $f \in \mathcal{F}_n$ betrachten wir den rein formalen Ausdruck $f(x_1, x_2, \ldots, x_n)$ mit $x_i \in X$ falls $n \neq 0$ und den Ausdruck f falls $n = 0$. Alle diese Ausdrücke nehmen wir nun zu X hinzu. Mit dieser neuen Menge wiederholen wir die Konstruktion. Das ganze wird nun iterativ fortgeführt. Dadurch erhalten wir alle formalen Ausdrücke, die sich aus den Variablen aus X und den Operationssymbolen aus $\mathcal{F}$, unter Berücksichtigung der Stelligkeit, zusammensetzen lassen. Dies sind dann die Terme vom Typ $\mathcal{F}$ über X.

Indem den Variablen Werte und den Operationssymbolen Operationen der entsprechenden Stelligkeiten zugeordnet werden, erhalten wir aus einer Termalgebra ein algebraisches System. Verschiedene Belegung der Variablen und Operationssymbole können aus einer Termalgebra unterschiedliche algebraische Systeme liefern. Die Vorstellung ist, daß Termalgebren über den algebraischen Systemen liegen.

3.59 Beispiel: Wir betrachten $X = \{x, y\}$ und $\mathcal{F} = \{\circ\}$ mit $t(\circ) = 2$. Anstatt $\circ(u, v)$ schreiben wir $u \circ v$ oder $(u \circ v)$.

Terme vom Typ $\mathcal{F}$ über X sind dann formale Ausdrücke in $\circ, x, y$ wie zum Beispiel $((x \circ y) \circ (y \circ x)) \circ x$.

Nun interpretieren wir $x = 0 \in \mathbb{N}$ und $y = 1 \in \mathbb{N}$ sowie $\circ = +$. Dadurch gewinnen wir aus der Termalgebra das System $(\mathbb{N}, +)$. Der obige Ausdruck

$((x \circ y) \circ (y \circ x)) \circ x$ wird zu $((0+1)+(1+0))+0 = 2$. Es wird einfach gezählt, wie oft y im Term auftaucht.

Als zweite Interpretation wählen wir

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

und $\circ$ entspricht der Matrizenmultiplikation. Damit gewinnen wir die Gruppe $(G, \circ)$ mit

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Wegen

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

und weil die Matrizenmultiplikation assoziativ ist, gilt

$$((x \circ y) \circ (y \circ x)) \circ x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Obwohl $(\mathbb{N}, +)$ und $(G, \circ)$ von der gleichen Termalgebra herrühren und daher beides binäre Algebren sind, sind sie doch sehr verschieden.

3.60 Definition: Ein *V-Typ* ist ein Tripel $(X, \mathcal{F}, t)$, wobei X und $\mathcal{F}$ nichtleere, disjunkte Mengen sind und $t\colon \mathcal{F} \to \mathbb{N}$ ein Abbildung ist.

Die Elemente von X heißen *Variablen*, die Menge $\mathcal{F}$ heißt *Typ* und die Elemente von $\mathcal{F}$ heißen *Operationssymbole*. Für $f \in \mathcal{F}$ ist $t(f)$ die *Dimension* oder *Stelligkeit* von f. Für $n \in \mathbb{N}$ sei $\mathcal{F}_n := \{f \in \mathcal{F} \mid t(f) = n\}$. Eine V-Typ ist also eine Variablenmenge zusammen mit einem Typ von Algebren.

Die Menge $\mathrm{T}(X)$ aller *Terme vom Typ $\mathcal{F}$ über X* ist der Durchschnitt aller Mengen Y, die folgende Eigenschaften haben:

1. $X \cup \mathcal{F}_0 \subset Y$,
2. Für $f \in \mathcal{F}_n$ und $p_1, \ldots, p_n \in Y$ ist auch der formale Ausdruck $f(p_1, \ldots, p_n)$ ein Element von Y.

3.61 Bemerkung: Bei dieser Definition der Terme vom Typ $\mathcal{F}$ über X liegt wieder eine „Konstruktion von oben“ vor. In der Einleitung zu diesem Abschnitt wurde die „Konstruktion von unten“ angedeutet. Diese Konstruktion von unten sichert, daß die Konstruktion von oben auch funktioniert, genauer, daß es mindestens eine

Menge Y mit den geforderten Eigenschaften gibt. Die folgende Testfrage liefert eine formal korrekte Konstruktion von unten.

3.62 Testfrage: Für einen V-Typ $(X, \mathcal{F}, t)$ wird induktiv definiert:

$$X_0 := X \cup \mathcal{F}_0,$$
$$X_{n+1} := X_n \cup \{f(p_1, \ldots, p_{t(f)}) \mid f \in \mathcal{F} \text{ und } p_1, \ldots, p_{t(f)} \in X_n\}, \qquad n \in \mathbb{N}.$$

Zeigen Sie $\mathrm{T}(X) = \bigcup_{n\in\mathbb{N}} X_n$.

3.63 Bezeichnung: Für $p \in \mathrm{T}(X)$ schreiben wir auch $p(x_1, \ldots, x_n)$ um anzudeuten, daß, nachdem alle Operationen expandiert sind, die Argumente von p aus der Menge $\{x_1, \ldots, x_n\} \subset X$ sind. Allerdings müssen nicht alle diese Elemente auch wirklich als Argumente von p auftreten.

Jedem Term $p(x_1, \ldots, x_n)$ vom Typ $\mathcal{F}$ kann in jedem algebraischen System $\mathfrak{A} = (A, \Omega)$ vom selben Typ eine Operation $p^{\mathfrak{A}}$, die nicht zwingend in Ω liegen muß, zugeordnet werden.

3.64 Definition: Sei $n \in \mathbb{N}$, sei $p(x_1, \ldots, x_n)$ ein Term vom Typ $\mathcal{F}$ über X und sei $\mathfrak{A} = (A, \Omega)$ eine Algebra vom Typ $\mathcal{F}$. Wir definieren eine Abbildung $p^{\mathfrak{A}}\colon A^n \to A$ durch:

1. Ist p eine Variable $x_i \in X$, so gilt $p^{\mathfrak{A}}(a_1, \ldots, a_n) = a_i$. Das heißt, $p^{\mathfrak{A}}$ ist die Projektion auf die i-te Koordinate.
2. Ist p von der Gestalt $f(p_1(x_1, \ldots, x_n), \ldots, p_k(x_1, \ldots, x_n))$ mit $f \in \mathcal{F}_k$, so ist

   $$p^{\mathfrak{A}}(a_1, \ldots, a_n) = f^{\mathfrak{A}}(p_1^{\mathfrak{A}}(a_1, \ldots, a_n), \ldots, p_k^{\mathfrak{A}}(a_1, \ldots, a_n)).$$

   Dabei ist $f^{\mathfrak{A}} = \tau_{\mathfrak{A}}(f)$ die gemäß Definition 3.8 zum Symbol f gehörende Operation in Ω.

3.65 Beispiel: Sei $X = \{x, y\}$ und $\mathcal{F} = \mathcal{F}_2 = \{\circ, \oplus\}$ sowie $\mathfrak{A} = (\{w, f\}, \{\wedge, \vee\})$. Dabei gelte $\tau_{\mathfrak{A}}(\circ) = \wedge$ und $\tau_{\mathfrak{A}}(\oplus) = \vee$. Wir betrachten nun den Term $p(x, y) = (x \circ y) \oplus x \in \mathrm{T}(X)$. Dann gilt $p^{\mathfrak{A}}(w, f) = (w \wedge f) \vee w$.

Ist $(X, \mathcal{F}, t)$ ein V-Typ, so definiert jedes Symbol $f \in \mathcal{F}$ auf natürliche Weise eine Operation der Stelligkeit $t(f)$ auf $\mathrm{T}(X)$. Damit wird $(\mathrm{T}(X), \mathcal{F})$ zu einem algebraischen System vom Typ $\mathcal{F}$.

3.66 Definition: Sei $(X, \mathcal{F}, t)$ ein V-Typ. Die *Termalgebra* $\mathfrak{T}(X)$ *vom Typ* $\mathcal{F}$ *über* X ist das algebraische System $(\mathrm{T}(X), \mathcal{F})$ vom Typ $\mathcal{F}$. Ist $f \in \mathcal{F}$ ein Operationssymbol der Stelligkeit n und sind $p_1, \ldots, p_n \in \mathrm{T}(X)$ Terme, so bildet f, aufgefaßt als Operation, das Tupel $(p_1, \ldots, p_n)$ auf den Term $f(p_1, \ldots, p_n) \in \mathrm{T}(X)$ ab.

Die Termalgebra $(\mathrm{T}(X), \mathcal{F})$ ist das „freie Erzeugnis“ von X und $\mathcal{F}$. *Erzeugnis* bedeutet, daß sich alle Elemente aus $\mathrm{T}(X)$ von durch Elemente von X und $\mathcal{F}$ darstellen lassen. *Frei* bedeutet, daß verschiedene Darstellungen auch verschiedene Elemente lieferen.

3.67 Definition: Sei $\mathcal{K}$ eine Menge von algebraischen Systemen vom Typ $\mathcal{F}$. Sei $\mathfrak{U}(X)$ ein algebraisches System vom Typ $\mathcal{F}$, das durch $X \neq \emptyset$ erzeugt wird. Dann besitzt $\mathfrak{U}(X)$ die *universelle Abbildungseigenschaft* für $\mathcal{K}$ über X, falls für jedes System $\mathfrak{A} = (A, \Omega) \in \mathcal{K}$ und für jede Abbildung $\alpha\colon X \to A$ genau ein Morphismus $\beta\colon \mathfrak{U}(X) \to \mathfrak{A}$ existiert, der α fortsetzt. (Fortsetzen bedeutet, daß $\beta(x) = \alpha(x)$ für $x \in X$ gilt.)

3.68 Beispiel: Sei $\mathcal{K}$ die Menge der unitären Algebren (A, γ). Für jede unitäre Algebra (A, γ) ist γ also eine Abbildung von A nach A. Die Peano-Algebra $(\mathbb{N}, \sigma)$, wo σ die Nachfolgerfunktion ist, hat die universelle Abbildungseigenschaft für $\mathcal{K}$ über $X = \{0\}$. Ist $\alpha\colon X \to A$ eine Abbildung, so gibt es ein $a_0 \in A$ mit $\alpha(0) = a_0$. Wir setzten nun iterativ:

1. $\beta(0) := a_0 = \alpha(0)$,
2. $\beta(\sigma(n)) := \gamma(\beta(n))$.

Die erste Bedingung liefert, daß α von β fortgesetzt wird. Die zweite Bedingung garantiert, daß β ein Morphismus ist. Da jeder andere Morphismus β', der α fortsetzt, auch $\beta'(0) := a_0$ und $\beta'(\sigma(n)) := \gamma(\beta'(n))$ erfüllen muß, ist β eindeutig bestimmt.

Die Peano-Algebra $(\mathbb{N}, \sigma)$ kann mit der Termalgebra über einer einelementigen Menge, deren Operationenmenge aus nur einem einstelligen Operationsymbol besteht, identifiziert werden. Der folgende Satz ist also eine Verallgemeinerung des Beispiels.

3.69 Hauptsatz über Termalgebren: *Sei $(X, \mathcal{F}, t)$ ein V-Typ und $\mathfrak{T}(X)$ die Termalgebra vom Typ $\mathcal{F}$ über X. Dann besitzt $\mathfrak{T}(X)$ die universelle Abbildungseigenschaft für die Menge aller algebraischen Systeme vom Typ $\mathcal{F}$.*

Beweis: Sei $\mathfrak{A} = (A, \Omega)$ ein algebraisches System vom Typ $\mathcal{F}$. Sei $\alpha\colon X \to A$ eine Abbildung. Wir definieren nun $\beta\colon \mathrm{T}(X) \to A$ induktiv durch:

1. $\forall x \in X\colon \beta(x) := \alpha(x)$,
2. $\forall f \in \mathcal{F}, \forall p_1, \ldots, p_{t(f)} \in \mathrm{T}(X)\colon \beta(f(p_1, \ldots, p_{t(f)}) := f^{\mathfrak{A}}(\beta(p_1), \ldots, \beta(p_{t(f)}))$.

Sei X_n wie in Testfrage 3.62. Durch die erste Bedingung wird β auf X_0 definiert. Durch die zweite Bedingung wird β auf X_{n+1} definiert, unter der Voraussetzung, daß β bereits auf X_n definiert ist. Das Induktionsprinzip liefert damit eine Abbildung auf ganz $\mathrm{T}(X) = \bigcup_{n\in\mathbb{N}} X_n$. Eine einfache Induktion zeigt, daß

$$\beta(p(x_1, \ldots, x_n)) = p^{\mathfrak{A}}(\alpha(x_1), \ldots, \alpha(x_n))$$

gilt. Daraus folgt, daß β ein Morphismus ist, der α fortsetzt. Da diese Gleichung für alle Morphismen gelten muß, die α fortsetzten, ist β eindeutig bestimmt. □

3.70 Beispiel: Sei (A, γ) eine unitäre Algebra, sei $X = \{x\}$ und $\mathcal{F} = \mathcal{F}_1 = \{f\}$. Der Satz sagt aus, daß jede Abbildung $\alpha\colon X \to A$ eindeutig zu einem Morphismus $\beta\colon (\mathrm{T}(X), f) \to (A, \gamma)$ fortgesetzt werden kann.

3.71 Definition: Sei $(X, \mathcal{F}, t)$ ein V-Typ. Eine *Identität* vom Typ $\mathcal{F}$ über X ist ein Ausdruck der Form $p \approx q$ mit $p = p(x_1, \ldots, x_n), q = q(x_1, \ldots, x_n) \in \mathrm{T}(X)$.

Ein algebraisches System $\mathfrak{A}$ vom Typ $\mathcal{F}$ *erfüllt die Identität* $p \approx q$, geschrieben $\mathfrak{A}\colon p \approx q$, falls:

$$\forall a_1, \ldots, a_n \in A\colon p^{\mathfrak{A}}(a_1, \ldots, a_n) = q^{\mathfrak{A}}(a_1, \ldots a_n).$$

3.72 Beispiel: Sei $X = \{x\}$ und $\mathcal{F} = \mathcal{F}_2 = \{\circ\}$. Sei $\mathfrak{A} = (A, \cdot)$, wo $A = \{0, 1\} \subset \mathbb{N}$ und $\cdot$ die übliche Multiplikation ist. Es gilt $0 \cdot 0 = 0$ und $1 \cdot 1 = 1$. Also, für jedes $a \in A$ gilt $a \cdot a = a$. Das heißt, die Algebra $\mathfrak{A}$ erfüllt die Identität $p \approx q$ mit $p = x \circ x \in \mathrm{T}(X)$ und $q = x \in \mathrm{T}(X)$.

3.73 Definition: Sei $(X, \mathcal{F}, t)$ ein V-Typ und $p, q \in \mathrm{T}(X)$. Eine Menge $\mathcal{K}$ algebraischer Systeme $\mathfrak{A}$ vom Typ $\mathcal{F}$ *erfüllt die Identität* $p \approx q$, geschrieben $\mathcal{K}\colon p \approx q$, falls $\mathfrak{A}\colon p \approx q$ für alle $\mathfrak{A} \in \mathcal{K}$.

Ist Σ eine Menge von Identitäten vom Typ $\mathcal{F}$ in X, so erfüllt $\mathcal{K}$ die Menge Σ, falls $\mathcal{K}\colon p \approx q$ für alle Identitäten $p \approx q \in \Sigma$. Mit $\mathcal{M}(\Sigma)$ wird die Menge aller algebraischer Systeme vom Typ $\mathcal{F}$, die Σ erfüllen, bezeichnet.

3.74 Definition: Eine Menge $\mathcal{K}$ algebraischer Systeme vom Typ $\mathcal{F}$ heißt *gleichungsdefinierbar*, wenn es eine Variablenmenge X und eine Menge Σ von Identitäten vom Typ $\mathcal{F}$ über X gibt mit $\mathcal{K} = \mathcal{M}(\Sigma)$.

Die gleichungsdefinierbare Menge $\mathcal{M}(\Sigma)$ erhält man also aus der freien Konstruktion $(\mathrm{T}(X), \mathcal{F})$, indem die ‚Freiheit' durch die ‚Gesetze' oder ‚Identitäten' in Σ eingeschränkt wird.

3.75 Beispiel: Die Menge aller Gruppen ist gleichungsdefinierbar. Um dies einzusehen betrachten wir $X = \{x, y, z\}$ und $\mathcal{F} = \{\cdot, \iota, 1\}$ mit $t(\cdot) = 2$, $t(\iota) = 1$ und $t(1) = 0$. Sei Σ die Menge der folgenden Identitäten:

$$\begin{aligned}(x \cdot y) \cdot z &\approx x \cdot (y \cdot z),\\ x \cdot 1 &\approx x,\\ 1 \cdot x &\approx x,\\ x \cdot \iota(x) &\approx 1,\\ \iota(x) \cdot x &\approx 1.\end{aligned}$$

Dann liefert $\mathcal{M}(\Sigma)$ gerade die Menge aller Gruppen. Dabei entspricht $\cdot$ der binären Gruppenoperation, ι dem Invertieren und 1 dem Neutralelement. Denn dann entsprechen diese Identitäten genau den Axiomen für Gruppen. (Die Abgeschlossenheit gilt ohnehin, da wir nur algebraische Systeme betrachten.)

Das Problem ist meist weniger, die richtigen Identitäten zu finden, sondern den Typ richtig zu definieren. Die Identitäten stehen nämlich für Axiome, in denen nur der Allquantor $\forall$ nicht aber der Existenzquantor $\exists$ auftaucht. Existenzquantoren in den Axiomen müssen daher durch geeignete Operationen ersetzt werden. So ist es in diesem Beispiel notwendig, das Invertieren als einstellige Operation und das Neutralelement als nullstellige Operation zu betrachten.

3.76 Testfrage: Zeigen Sie, daß die Menge aller Ringe gleichungsdefinierbar ist.

Der folgende Satz, den wir nicht beweisen werden, schafft eine Verbindung zwischen Varietäten und gleichungsdefinierbaren algebraischen Systemen. Zur Erinnerung, eine Varietät ist eine Menge ähnlicher algebraischer Systeme, die abgeschlossen unter Bildung von Teilalgebren, isomorphen Bildern und Produkten ist.

3.77 Satz (Birkhoff): *Eine Menge $\mathcal{K}$ ähnlicher algebraischer Systemen ist genau dann eine Varietät, wenn $\mathcal{K}$ gleichungsdefinierbar ist.*

Meist läßt sich einfacher nachweisen, daß eine Menge algebraischer Systeme gleichungsdefinierbar ist, anstatt direkt zu zeigen, daß die Menge eine Varietät bildet.

3.78 Beispiel: Wir haben oben (mit wenig Aufwand) gezeigt, daß die Menge der Gruppen gleichungsdefinierbar ist. Also ist diese Menge eine Varietät. Vergleichen Sie diesen Beweis mit Ihrer Lösung von Testfrage 3.58.

3.79 Testfrage: Entscheiden Sie, ob die Menge aller Körper gleichungsdefinierbar ist.

KAPITEL 4

Kategorien und Funktoren

Häufig werden in der Mathematik Objekte, die eine gemeinsame Struktur tragen, zusammen mit den strukturerhaltenden Abbildungen betrachtet. Zum Beispiel ist die Menge der reellen Vektorräume eine typische Objektmenge der Linearen Algebra. Die strukturerhaltenden Abbildungen sind die (reellen) linearen Abbildungen. Wir schränken dieses Beispiel noch etwas ein.

4.1 Beispiel: Objekte sind die Vektorräume $\mathbb{R}^n$, jeweils mit der kanonischen Basis. Jeder linearen Abbildung $\varphi\colon \mathbb{R}^n \to \mathbb{R}^m$ kann dann eindeutig eine reelle $n \times m$-Matrix zugeordnet werden. Das Hintereinanderausführen von linearen Abbildungen entspricht der Multiplikation der entsprechenden Matrizen. Wir betrachten also:

$$
\begin{aligned}
X &:= \{\mathbb{R}^n \mid n \in \mathbb{N} \setminus \{0\}\},\\
\mathfrak{M}_1(n,m) &:= \{M_{n,m} \mid M_{n,m} \text{ ist reelle } n \times m\text{-Matrix}\},\\
\mathfrak{M}_1 &:= \{\mathfrak{M}_1(n,m) \mid m,n \in \mathbb{R} \setminus \{0\}\},\\
\mathfrak{M}_2(n,m) &:= \text{Menge der linearen Abbildungen von } \mathbb{R}^n \text{ nach } \mathbb{R}^m,\\
\mathfrak{M}_2 &:= \{\mathfrak{M}_2(n,m) \mid m,n \in \mathbb{R} \setminus \{0\}\}.
\end{aligned}
$$

Das Paar $(X, \mathfrak{M}_2)$ ist im Wesentlichen die Kategorie der endlichdimensionalen reellen Vektorräume. Das Paar $(X, \mathfrak{M}_1)$ ist ein dazu isomorphe Kategorie. Die Lineare Algebra ist die intensive Beschäftigung mit diesen (und damit verwandten) Kategorien.

Wir betrachten nun ein Kategorie, die eher der Analysis zugeordnet wird. Objekte sind Paare (U,u) mit $u \in U$ und es gibt ein $n \in \mathbb{N}$, so daß U eine offene Teilmenge in $\mathbb{R}^n$ ist. Dieses n ist eindeutig bestimmt. Wir schreiben dafür $d(U)$. Ein Morphismus von (U,u) nach (V,v) ist eine stetig differenzierbare Abbildung

$f\colon U \to V$ mit $f(u) = v$. Also:

$$\begin{aligned} Y &:= \big\{(U,u) \mid u \in U \text{ und } \exists n \in \mathbb{N}\setminus\{0\}\colon U \text{ ist offen in } \mathbb{R}^n\big\},\\ \mathfrak{M}_3((U,u),(V,v)) &:= \text{Menge der stetig differenzierbaren}\\ &\qquad\quad \text{Funktionen } f\colon U \to V \text{ mit } f(u) = v,\\ \mathfrak{M}_3 &:= \big\{\mathfrak{M}_3((U,u),(V,v)) \mid (U,u),(V,v) \in Y\big\}. \end{aligned}$$

In Analysis II werden üblicherweise Ableitungen von Abbildungen aus $\mathfrak{M}_3$ untersucht. Diese Untersuchung liefert eine Verbindung zwischen der Kategorie $(Y,\mathfrak{M}_3)$ und der Kategorie $(X,\mathfrak{M}_1)$.

Wir setzen $\mathfrak{f}((U,u)) := \mathbb{R}^{d(U)}$. Jeder Abbildung $f\colon U \to V$ aus $\mathfrak{M}_3$ mit $f(u) = v$ ordnen wir die Jacobimatrix von f bei u zu. Das heißt, für $f = (f_1,\dots,f_m) \in \mathfrak{M}_3((U,u),(V,v))$ mit $\mathfrak{f}((U,u)) = \mathbb{R}^n$ und $\mathfrak{f}((V,v)) = \mathbb{R}^m$, sei

$$\mathfrak{f}(f) := \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(u_1) & \cdots & \frac{\partial f_1}{\partial x_n}(u_n)\\ \vdots & & \vdots\\ \frac{\partial f_m}{\partial x_1}(u_1) & \cdots & \frac{\partial f_m}{\partial x_n}(u_n) \end{pmatrix}$$

die Matrix der partiellen Ableitungen der verschiedenen Komponenten von f bei u. Damit ist

$$\mathfrak{f}\colon (Y,\mathfrak{M}_3) \to (X,\mathfrak{M}_1)\colon ((U,u),f) \mapsto (\mathfrak{f}((U,u)),\mathfrak{f}(f))$$

eine Abbildung von der dritten Kategorie in die erste Kategorie.

Das besondere an dieser Abbildung ist, daß sie mit der Kategorienstruktur verträglich ist. Für $f \in \mathfrak{M}_3((U,u),(V,v))$ gilt $\mathfrak{f}(f) \in \mathfrak{M}_1(\mathfrak{f}((U,u)),\mathfrak{f}((V,v)))$. Das heißt, ein Morphismus zwischen zwei Objekten aus Y wird auf einen Morphismus zwischen den Bildobjekten abgebildet.

$$\begin{array}{ccc} (U,u) & \xrightarrow{\ f\ } & (V,v)\\ \mathfrak{f}\big\downarrow & & \mathfrak{f}\big\downarrow\\ \mathbb{R}^{d(U)} & \xrightarrow{\ \mathfrak{f}(f)\ } & \mathbb{R}^{d(V)} \end{array}$$

Diese Zuordnung ist sogar mit der Hintereinanderausführung von Morphismen verträglich. Das ist die Aussage der Kettenregel. Für $(U,u),(V,v),(W,w) \in Y$ und $f\colon U \to V$ sowie $g\colon V \to W$ mit $f(u) = v$ ist die Jacobimatrix von $g \circ f$ bei u das Produkt der Jacobimatrix von g bei $f(u) = v$ mit der Jacobimatrix von f bei u. Das heißt, es gilt

$$\mathfrak{f}(g \circ f) = \mathfrak{f}(g) \circ \mathfrak{f}(f).$$

Das folgende Diagramm veranschaulicht die Situation:

$$\begin{array}{ccccc} (U,u) & \xrightarrow{f} & (V,v) & \xrightarrow{g} & (W,w) \\ \mathfrak{f}\downarrow & & \mathfrak{f}\downarrow & & \mathfrak{f}\downarrow \\ \mathbb{R}^{d(U)} & \xrightarrow{\mathfrak{f}(f)} & \mathbb{R}^{d(V)} & \xrightarrow{\mathfrak{f}(g)} & \mathbb{R}^{d(W)} \end{array}$$

Die Ableitung der identische Abbildung auf $(U,u) \in Y$ ist die Einheitsmatrix mit $d(U)$ Spalten, also das Neutralelement in $\mathfrak{M}_1(\mathfrak{f}((U,u)), \mathfrak{f}((U,u)))$.

Eine Abbildung zwischen Kategorien, die die drei eben ausgeführten Eigenschaften hat, heißt Funktor. Funktoren sind also die Morphismen zwischen Kategorien, oder, anders ausgedrückt, Funktoren sind Morphismen in der Kategorie der Kategorien.

Funktoren beachten zwar die Struktur, gehen aber meist mit Informationsverlust einher. So läßt sich im obigen Beispiel weder (U,u) aus $\mathfrak{f}((U,u))$ noch f aus $\mathfrak{f}(f)$ rekonstruieren. Dieser Informationsverlust muß nicht zwingend ein Nachteil sein. Will man einen Funktor zur Lösung eines Problems heranziehen, so muß ein Funktor gewählt werden, der die für das Problem wichtige Information erhält, aber alle überflüssige Information vergißt. Der Funktor beschreibt dann die *Einschränkung auf das Wesentliche.*

Wir wollen nun die Begriffe ‚Kategorie' und ‚Funktor' formal einführen.

4.2 Definition: Eine *Kategorie* $\mathfrak{k}$ besteht aus eine Menge $\mathfrak{O}(\mathfrak{k})$ von *Objekten*, einer Menge $\{\mathfrak{M}(A,B) \mid A,B \in \mathfrak{O}(\mathfrak{k})\}$ von Mengen von *Morphismen* und einer Menge $\{\circ\colon \mathfrak{M}(B,C) \times \mathfrak{M}(A,B) \to \mathfrak{M}(A,C) \mid A,B,C \in \mathfrak{O}(\mathfrak{k})\}$ von *Verknüpfungen*, so daß gilt:

1. Aus $\mathfrak{M}(A,B) \cap \mathfrak{M}(A',B') \neq \emptyset$ folgt $A = A'$ und $B = B'$.
2. Zu jedem Objekt $A \in \mathfrak{O}(\mathfrak{k})$ gibt es ein Morphismus $\mathrm{id} = \mathrm{id}_A \in \mathfrak{M}(A,A)$, so daß für jedes Objekt $B \in \mathfrak{O}(\mathfrak{k})$ und alle Morphismen $f \in \mathfrak{M}(A,B)$, $g \in \mathfrak{M}(B,A)$ gilt:

$$f \circ \mathrm{id} = f,$$
$$\mathrm{id} \circ g = g.$$

$$\begin{array}{ccccc} B & \xrightarrow{g} & A & \xrightarrow{f} & B \\ & \searrow^{\mathrm{id}\circ g} & \downarrow \mathrm{id} & \nearrow_{f\circ \mathrm{id}} & \\ & & A & & \end{array}$$

3. Für alle Objekte $A, B, C, D \in \mathfrak{O}(\mathfrak{k})$ und alle Morphismen $f \in \mathfrak{M}(A, B)$, $g \in \mathfrak{M}(B, C)$, $h \in \mathfrak{M}(C, D)$ zwischen diesen Objekten gilt

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

Die Vorstellung ist, daß die Objekte Mengen mit Struktur sind und die Morphismen aus $\mathfrak{M}(A, B)$ strukturerhaltende Abbildungen von A nach B sind. Die Verknüpfung ist dann meist das Hintereinanderausführen von Abbildungen. Das muß aber nicht zwingend so sein. In dem ersten einführenden Beispiel waren die Morphismen Matrizen. Matrizen sind keine Abbildungen, sondern Zahlenschemata. Die Verknüpfung war in diesem Beispiel die Matrizenmultiplikation.

4.3 Beispiele:

1. Sei $\mathbb{K}$ ein Körper. Die Kategorie der Vektorräume über diesem Körper besteht aus den Vektorräumen über dem Körper als Objekte und den (über diesem Körper) linearen Abbildungen als Morphismen. Die Verknüpfung ist die Hintereinanderschaltung von Abbildungen.
2. Wir betrachten als Objekte irgendwelche nichtleere Mengen und als Morphismen Abbildungen zwischen diesen Mengen. Dies bildet eine Kategorie. Die Verknüpfung ist die Hintereinanderschaltung von Abbildungen.
3. Das vorherige Beispiel kann variiert werden. Die Objekte sind wieder nichtleere Mengen. Die Morphismen sind nun Relationen zwischen diesen Mengen. Die Verknüpfung ist die Komposition von Relationen. Dies bildet eine Kategorie. Die identische Relation auf einer Menge A ist das Neutralelement in $\mathfrak{M}(A, A)$.

   Dieses Kategorie enthält die Kategorie des vorangehenden Beispiels als Unterkategorie, da Abbildungen als Relationen aufgefaßt werden können. Die beiden Beispiele machen deutlich, daß in der Regel die Morphismen nicht durch die Objekte festgelegt sind.
4. Auch in dieser Vorlesung steht ein bestimmter Typ von Kategorien im Mittelpunkt. Objekte sind ähnliche algebraische Systeme und Morphismen sind die Morphismen zwischen diesen ähnlichen algebraischen Systemen. Jeder Typ $\mathcal{F}$ von Algebren definiert also eine Kategorie.

4.4 Testfrage: Definieren Sie die Kategorie der algebraischen Typen. Das heißt, erklären Sie sinnvoll, welche Abbildungen zwischen algebraischen Typen zu Morphismen der Kategorie, deren Objektmenge algebraische Typen sind, werden.

Wir untersuchen nun Morphismen zwischen Kategorien.

4.5 Definition: Seien $\mathfrak{a}$ und $\mathfrak{b}$ Kategorien. Ein *kovarianter Funktor* $\mathfrak{f}\colon \mathfrak{a} \to \mathfrak{b}$ ordnet jedem Objekt A von $\mathfrak{a}$ ein Objekt $\mathfrak{f}(A)$ von $\mathfrak{b}$ und jedem Morphismus f von $\mathfrak{a}$ einen Morphismus $\mathfrak{f}(f)$ von $\mathfrak{b}$ zu, so daß gilt:

1. Für alle Objekte $A, B \in \mathfrak{O}(\mathfrak{a})$ und jeden Morphismus $f \in \mathfrak{M}(A,B)$ gilt $\mathfrak{f}(f) \in \mathfrak{M}(\mathfrak{f}(A), \mathfrak{f}(B))$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \mathfrak{f}}\downarrow & & {\scriptstyle \mathfrak{f}}\downarrow \\ \mathfrak{f}(A) & \xrightarrow{\mathfrak{f}(f)} & \mathfrak{f}(B) \end{array}$$

2. Für jedes Objekt $A \in \mathfrak{O}(\mathfrak{a})$ gilt $\mathfrak{f}(\mathrm{id}_A) = \mathrm{id}_{\mathfrak{f}(A)}$.
3. Für alle Objekte $A, B, C \in \mathfrak{O}(\mathfrak{a})$ und alle Morphismen $f \in \mathfrak{M}(A,B)$, $g \in \mathfrak{M}(B,C)$ gilt $\mathfrak{f}(g \circ f) = \mathfrak{f}(g) \circ \mathfrak{f}(f)$.

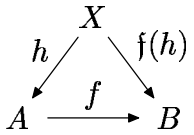
$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ {\scriptstyle \mathfrak{f}}\downarrow & & {\scriptstyle \mathfrak{f}}\downarrow & & {\scriptstyle \mathfrak{f}}\downarrow \\ \mathfrak{f}(A) & \xrightarrow{\mathfrak{f}(f)} & \mathfrak{f}(B) & \xrightarrow{\mathfrak{f}(g)} & \mathfrak{f}(C) \end{array}$$

4.6 Beispiele:

1. Sei $\mathcal{F}$ ein Typ von Algebren und $\mathfrak{a}$ die Kategorie der algebraischen Systeme vom Typ $\mathcal{F}$ und ihre Morphismen gemäß Beispiel 4.3.4. Sei $\mathfrak{O}(\mathfrak{b})$ die Menge aller Trägermengen von algebraischen Systemen aus $\mathfrak{O}(\mathfrak{a})$. Zusammen mit den Abbildungen zwischen solchen Mengen bildet dies die Kategorie $\mathfrak{b}$, vgl. Beispiel 4.3.2. Für $(A,\Omega) \in \mathfrak{O}(\mathfrak{a})$ sei $\mathfrak{f}((A,\Omega)) := A \in \mathfrak{O}(\mathfrak{b})$. Das heißt, jedem algebraischen System wird seine Trägermenge zugeordnet. Für einen Morphismus $f\colon (A,\Omega) \to (B,\Omega')$ sei $\mathfrak{f}(f)$ die entsprechende Abbildung von A nach B. Dann ist $\mathfrak{f}\colon \mathfrak{a} \to \mathfrak{b}$ ein kovarianter Funktor. Da er einfach die algebraische Struktur ‚vergißt', heißt er *Vergißfunktor*.
2. Eine analoge Konstruktion funktioniert für jede Kategorie, bei der Objekte Mengen mit Struktur und Morphismen strukturerhaltende Abbildungen sind. Eine andere Variante ist, nur Teile der Struktur zu vergessen. Sei $\mathfrak{a}$ die Kategorie der Ringe und Ringhomomorphismen und $\mathfrak{b}$ die Kategorie der Gruppen und Gruppenhomomorphismen. Für einen Ring $(R,+,\cdot,0,1) \in \mathfrak{O}(\mathfrak{a})$ sei $\mathfrak{f}((R,+,\cdot,0,1)) := (A,+,0) \in \mathfrak{O}(\mathfrak{b})$. Dies induziert einen kovarianten Funktor von $\mathfrak{a}$ nach $\mathfrak{b}$, der die multiplikative Struktur vergißt, aber die additive Struktur erhält.
3. Sei $\mathfrak{a}$ die Kategorie einer Menge von Mengen und Abbildungen zwischen diesen Mengen gemäß Beispiel 4.3.2. Sei $X \in \mathfrak{O}(\mathfrak{a})$. Sei $\mathfrak{O}(\mathfrak{b}) := \{A^X \mid A \in$

$\mathfrak{O}(\mathfrak{a})\}$, wo A^X für die Menge der Abbildungen von X nach A steht. Dies bildet eine Kategorie $\mathfrak{b}$, wobei die Morphismen die Abbildungen zwischen Elementen aus $\mathfrak{O}(\mathfrak{b})$ sind.

Für $A \in \mathfrak{O}(\mathfrak{a})$ sei $\mathfrak{f}(A) := A^X$ die Menge der Abbildungen von X nach A. Für $A, B \in \mathfrak{O}(\mathfrak{a})$ und $f\colon A \to B$ sei $\mathfrak{f}(f)$ die Abbildung von A^X nach B^X, die jeder Abbildung $h\colon X \to A$ die Abbildung $f \circ h$ zuordnet. Damit ist $\mathfrak{f}$ ein kovarianter Funktor von $\mathfrak{a}$ nach $\mathfrak{b}$.



4.7 Testfrage: Sei $\mathcal{F}$ ein Typ von Algebren. Sei $\mathfrak{a}$ die Kategorie, deren Objekte Mengen und deren Morphismen Abbildungen zwischen diesen Mengen sind. Sei $\mathfrak{b}$ die Kategorie, deren Objekte alle algebraischen Systeme vom Typ $\mathcal{F}$ und deren Morphismen Morphismen zwischen ähnlichen algebraischen Systemen sind.

Für eine Menge $X \in \mathfrak{O}(\mathfrak{a})$ sei $\mathfrak{f}(X) := \mathfrak{T}(X) = (\mathrm{T}(X), \mathcal{F})$ die Termalgebra vom Typ $\mathcal{F}$ über X. Zeigen Sie, daß dies einen kovarianten Funktor von $\mathfrak{a}$ nach $\mathfrak{b}$ induziert.

Es gibt in der Mathematik oft auch die Situation, daß eine Abbildung zwischen Kategorien die Richtung der Morphismen umkehrt. Das ist meist dann der Fall, wenn in der Kategorie die Objekte Mengen von Abbildungen sind. Dies führt zu den kontravarianten Funktoren.

4.8 Definition: Seien $\mathfrak{a}$ und $\mathfrak{b}$ Kategorien. Ein *kontravarianter Funktor* $\mathfrak{f}\colon \mathfrak{a} \to \mathfrak{b}$ ordnet jedem Objekt A von $\mathfrak{a}$ ein Objekt $\mathfrak{f}(A)$ von $\mathfrak{b}$ und jedem Morphismus f von $\mathfrak{a}$ einen Morphismus $\mathfrak{f}(f)$ von $\mathfrak{b}$ zu, so daß gilt:

1. Für alle Objekte $A, B \in \mathfrak{O}(\mathfrak{a})$ und jeden Morphismus $f \in \mathfrak{M}(A, B)$ gilt $\mathfrak{f}(f) \in \mathfrak{M}(\mathfrak{f}(B), \mathfrak{f}(A))$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \mathfrak{f}}\downarrow & & \downarrow{\scriptstyle \mathfrak{f}} \\ \mathfrak{f}(A) & \xleftarrow{\mathfrak{f}(f)} & \mathfrak{f}(B) \end{array}$$

2. Für jedes Objekt $A \in \mathfrak{O}(\mathfrak{a})$ gilt $\mathfrak{f}(\mathrm{id}_A) = \mathrm{id}_{\mathfrak{f}(A)}$.
3. Für alle Objekte $A, B, C \in \mathfrak{O}(\mathfrak{a})$ und alle Morphismen $f \in \mathfrak{M}(A, B)$, $g \in \mathfrak{M}(B, C)$ gilt $\mathfrak{f}(g \circ f) = \mathfrak{f}(f) \circ \mathfrak{f}(g)$.

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \mathfrak{f}\downarrow & & \mathfrak{f}\downarrow & & \mathfrak{f}\downarrow \\ \mathfrak{f}(A) & \xleftarrow{\mathfrak{f}(f)} & \mathfrak{f}(B) & \xleftarrow{\mathfrak{f}(g)} & \mathfrak{f}(C) \end{array}$$

4.9 Beispiel: Sei $\mathfrak{a}$ die Kategorie einer Menge von Mengen und Abbildungen zwischen diesen Mengen gemäß Beispiel 4.3.2. Sei $X \in \mathfrak{O}(\mathfrak{a})$. Sei $\mathfrak{O}(\mathfrak{b}) := \{X^A \mid A \in \mathfrak{O}(\mathfrak{a})\}$, wo X^A für die Menge der Abbildungen von A nach X steht. Dies bildet eine Kategorie $\mathfrak{b}$, wobei die Morphismen die Abbildungen zwischen Elementen aus $\mathfrak{O}(\mathfrak{b})$ sind.

Für $A \in \mathfrak{O}(\mathfrak{a})$ sei $\mathfrak{f}(A) := X^A$ die Menge der Abbildungen von A nach X. Für $A, B \in \mathfrak{O}(\mathfrak{a})$ und $f\colon A \to B$ sei $\mathfrak{f}(f)$ die Abbildung von X^B nach X^A, die jeder Abbildung $h\colon B \to X$ die Abbildung $h \circ f\colon A \to X$ zuordnet. Dann ist $\mathfrak{f}\colon \mathfrak{a} \to \mathfrak{b}$ ein kontravarianter Funktor

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle \mathfrak{f}(h)}\searrow \quad \swarrow{\scriptstyle h} & \\ & X & \end{array}$$

4.10 Testfrage: Sei $\mathbb{K}$ ein Körper und $\mathfrak{a}$ die Kategorie der endlichdimensionalen Vektorräume über $\mathbb{K}$ mit den linearen Abbildungen als Morphismen. Für $V \in \mathfrak{O}(\mathfrak{a})$ sei $\mathfrak{f}(V)$ die Menge der linearen Funktionale auf V, das heißt, die Menge der linearen Abbildungen von V in den Körper $\mathbb{K}$. Diese Menge der linearen Funktionale auf V bildet wieder einen Vektorraum, den Dualraum zu V.

Ergänzen Sie $\mathfrak{f}$ zu einem kontravarianten Funktor von $\mathfrak{a}$ nach $\mathfrak{a}$, indem Sie angeben, wie $\mathfrak{f}$ Morphismen abbildet. Bestimmen Sie $\mathfrak{f} \circ \mathfrak{f}$.

KAPITEL 5

Gruppen

In diesem Abschnitt untersuchen wir Gruppen etwas genauer.

Gruppen sind Mathematik weit verbreitet und wurden intensiv untersucht. Zum Beispiel bildet die Menge aller Permutationen einer festen (nichtleeren) Menge eine Gruppe bezüglich der Komposition von Abbildungen (vgl. Beispiel 3.39.3). Aber auch bei einer Menge mit Struktur bilden die strukturerhaltenden Bijektionen auf dieser Menge eine Gruppe. Betrachten wir hingegen auf einer Menge mit Struktur die strukturerhaltenden Abbildungen auf dieser Menge, so erhalten wir in der Regel lediglich eine Halbgruppe. Halbgruppen treten also weit häufiger als Gruppen auf. Allerdings sind die definierenden Eigenschaften der Halbgruppen nicht stark genug, um darauf eine aussagekräftige Theorie aufzubauen. Ganz im Gegensatz zur Gruppentheorie, die sehr aussagekräftig ist. Der Erfolg der Gruppentheorie liegt darin, daß auf der einen Seite Gruppen sehr gebräuchliche Objekte sind, aber auf der anderen Seite gerade genügend Struktur besitzen, um interessante Eigenschaften ableiten zu können.

Gruppen werden an vielen Stellen der Mathematik erfolgreich als Werkzeug eingesetzt. Bei den Beweisen der folgenden Sätze, die zunächst nichts mit Gruppen zu tun haben, spielt die Gruppentheorie ein zentrale Rolle:

1. Nicht jeder Winkel kann mit Zirkel und Lineal in drei gleiche Winkel unterteilt werden.
2. Es gibt keine Formel zur Bestimmung der Nullstellen eines allgemeinen Polynoms vom Grad 5. (Es gibt wohlbekannte Formeln, mit denen die Nullstellen eines quadratischen Polynoms bestimmt werden können. Diese Formel verwendet nur Wurzelziehen, Addition, Multiplikation und Division. Für Polynome vom Grad 3 und 4 wurden ebenfalls Formeln entwickelt, die nur mit diesen Operationen auskommen. Die Konstruktion einer Formel für Polynome vom Grad 5 wurde lange erfolglos versucht, bis gezeigt wurde, daß es überhaupt nicht geht. Für Polynome höheren Grades gibt es damit erst recht keine Lösungsformel.)

5.1. Gruppen, Untergruppen und Normalteiler

Wir wiederholen zunächst die Definition einer Gruppe als spezielles algebraisches System.

5.1 Definition: Eine *Gruppe* ist ein algebraisches System $(G, \circ, \iota, e)$ mit $\alpha(\circ) = 2$, $\alpha(\iota) = 1$ und $\alpha(e) = 0$, so daß gilt:

1. $\forall a, b, c \in G$: $(a \circ b) \circ c = a \circ (b \circ c)$.
2. $\forall a \in G$: $a \circ e = e \circ a = a$.
3. $\forall a \in G$: $a \circ \iota(a) = \iota(a) \circ a = e$.

Das spezielle Element e heißt *Neutralelement*. Für $a \in G$ heißt $\iota(a)$ das *zu a inverse Element*. Die binäre Operation $\circ$ heißt *Verknüpfung*.

Das Schöne an dieser Definition ist, daß die definierenden Gleichungen nur den Quantor $\forall$ haben. Dadurch ist zum Beispiel rasch nachzuweisen (unter Verwendung des Satzes von Birkhoff), daß die Menge der Gruppen eine Varietät bildet (vgl. Beispiel 3.78).

Die traditionelle Definition hingegen gibt nur Trägermenge und Verknüpfung vor.

5.2 Definition: Eine Gruppe $(G, \circ)$ ist eine Menge G zusammen mit einer Verknüpfung $\circ\colon G \times G \to G$ mit:

1. $\forall a, b, c \in G$: $(a \circ b) \circ c = a \circ (b \circ c)$.
2. $\exists e \in G \, \forall a \in G$: $a \circ e = a$.
3. $\forall a \in G \, \exists b \in G$: $a \circ b = b \circ a = e$.

Auf den ersten Blick scheint die zweite Definition schwächer zu sein. Das folgende Lemma zeigt, daß der Schein trügt.

5.3 Lemma: *Sei $(G, \circ)$ eine Gruppe gemäß Definition 5.2. Dann gilt:*

1. *Für jedes $a \in G$ gibt es genau ein $b = \iota(a) \in G$ mit $a \circ b = b \circ a = e$.*
2. $\forall a \in G$: $e \circ a = a$.
3. *Das Neutralelement ist eindeutig bestimmt, das heißt es gibt genau ein $e \in G$ mit $\forall a \in G$: $a \circ e = a$.*

Beweis:

1. Sei $a, b, b' \in G$ mit $a \circ b = b \circ a = a \circ b' = b' \circ a = e$. Dann gilt:

$$\begin{aligned} b &= b \circ e && \text{Definition 5.2.2} \\ &= b \circ (a \circ b') && \text{Voraussetzung,} \\ &= (b \circ a) \circ b' && \text{Definition 5.2.1,} \\ &= (b' \circ a) \circ b' && \text{Voraussetzung} \\ &= b' \circ (a \circ b') && \text{Definition 5.2.1,} \\ &= b' \circ e && \text{Voraussetzung,} \\ &= b' && \text{Definition 5.2.2.} \end{aligned}$$

2. Sei $a \in G$. Dann gilt:

$$\begin{aligned} e \circ a &= (a \circ \iota(a)) \circ a && \text{Lemma 5.3.1,} \\ &= a \circ (\iota(a) \circ a) && \text{Definition 5.2.1,} \\ &= a \circ e && \text{Lemma 5.3.1,} \\ &= a && \text{Definition 5.2.2.} \end{aligned}$$

3. Angenommen e und e' sind Neutralelemente. Dann gilt:

$$\begin{aligned} e &= e \circ e' && e' \text{ Neutralelement,} \\ &= e' && e \text{ Neutralelement.} \end{aligned}$$

□

5.4 Definition: Eine Gruppe heißt *kommutativ* oder *Abelsch*, falls die Gruppenoperation kommutativ ist.

5.5 Bezeichnung: Wir werden im weiteren zwanglos zwischen den beiden Definitionen von Gruppen wechseln. Oft werden wir sogar nur die Trägermenge angeben, das heißt, wir schreiben „Gruppe G“ statt „Gruppe $(G, \circ)$“. Anstellen $\circ$ verwenden wir auch $\cdot$ für die Gruppenverknüpfung und sprechen dann von der *Gruppenmultiplikation*. In diesem Fall schreiben wir a^{-1} für das Inverse von a und 1 für das Neutralelement. Für $a \cdot b$ schreiben wir auch kurz ab.

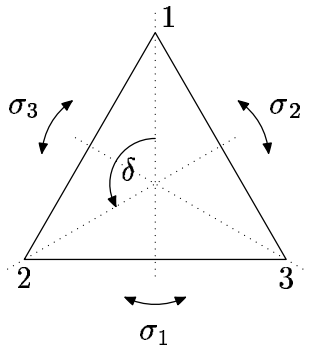
Ist die Gruppenverknüpfung kommutativ, so schreiben wir oft $+$ für die Gruppenverknüpfung und sprechen dann von der *Gruppenaddition*. In diesem Fall schreiben wir $-a$ für das Inverse von a und 0 für das Neutralelement.

5.6 Beispiel: Bereits in Beispiel 3.39.4 wurde die symmetrische Gruppe S_n der Permutationen auf der Menge $\{1, \ldots, n\}$ vorgestellt. Wir untersuchen nun speziell den Fall $n = 3$.

Das Neutralelement der Gruppe bezeichnen wir mit e. Für $i \in \{1, 2, 3\}$ sei σ_i die Permutation, die i festläßt und die beiden Elemente in $\{1, 2, 3\} \setminus \{i\}$ vertauscht. Sei $\delta := \sigma_3\sigma_1$. Es gilt:

$$\begin{aligned}\delta(1) &= \sigma_3(\sigma_1(1)) = \sigma_3(1) = 2,\\ \delta(2) &= \sigma_3(\sigma_1(2)) = \sigma_3(3) = 3,\\ \delta(3) &= \sigma_3(\sigma_1(3)) = \sigma_3(2) = 1.\end{aligned}$$

Offensichtlich gilt $\sigma_i^2 = e = \delta^3$ aber $\delta^2 \neq e$. Daraus folgt $\sigma_i^{-1} = \sigma_i$ für $i \in \{1, 2, 3\}$ und $\delta^{-1} = \delta^2$. Die sechs Elemente der Gruppe sind also $e, \sigma_1, \sigma_2, \sigma_3, \delta, \delta^2$.
Die Gruppe S_3 kann als die Symmetriegruppe eines gleichseitigen Dreiecks betrachtet werden. Jede Permutation der drei Eckpunkte entspricht genau einer Symmetrie des Dreiecks. Die Permutationen σ_i entsprechen Spiegelungen an Winkelhalbierenden, die Permutation δ ist eine Drehung um 120 Grad.



Die folgende Testfrage sagt aus, daß das Invertieren eine Involution ist, die die Reihenfolge umdreht, kurz ein *involutorischer Anitiisomorphismus.*

5.7 Testfrage: Sei $(G, \cdot)$ eine Gruppe. Zeigen Sie:

1. $\forall a \in G\colon (a^{-1})^{-1} = a$.
2. $\forall a, b \in G\colon (ab)^{-1} = b^{-1} \cdot a^{-1}$.

Die Teilalgebren von Gruppen heißen Untergruppen.

5.8 Definition: Sei $(G, \cdot)$ eine Gruppe. Dann ist $(H, \cdot)$ ein *Untergruppe von* $(G, \cdot)$, geschrieben $(H, \cdot) \leq (G, \cdot)$ oder $H \leq G$, falls $(H, \cdot)$ eine Gruppe ist und $H \subset G$ gilt.

Das folgende Resultat charakterisiert die Teilmengen einer Gruppe, die Trägermenge einer Untergruppe sind.

5.9 Lemma: *Sei G eine Gruppe und $\emptyset \neq H \subset G$. Dann ist H genau dann eine Untergruppe von G, wenn für alle $a, b \in H$ das Element ab^{-1} in H liegt.*

Beweis: Ist H eine Untergruppe, so ist H eine Gruppe. Für $a, b \in H$ gilt daher $ab^{-1} \in H$.

Wir wollen nun die umgekehrte Richtung zeigen. Die Assoziativität der Gruppenverknüpfung bleibt bei Einschränkung erhalten. Da H nicht leer ist, gibt es ein $a \in H$. Doch dann ist auch $aa^{-1} = e$ in H.

Für $a \in H$ ist $ea^{-1} = a^{-1}$ in H, das heißt, H enthält mit jedem Element auch dessen Inverses.

Sind $a, b \in H$, so sind auch a, b^{-1} in H, also auch $a \cdot (b^{-1})^{-1} = ab$. □

5.10 Beispiele:

1. Für jede Gruppe mit Neutralelement e ist $\{e\}$ eine Untergruppe.
2. Ist X eine nichtleere Menge und $A \subset X$ sowie $G := S(X)$ die Gruppe aller Permutationen von X. Dann ist
$$F_A := \{g \in G \mid \forall a \in A\colon g(a) = a\}$$
eine Untergruppe von G. Die Elemente dieser Untergruppe sind also genau die Permutationen von X, die alle Elemente von A fixieren.
Für $A = \emptyset$ ist $F_A = G$, für $A = X$ ist $F_A = \{e\}$.
3. Die Untergruppen von S_3 sind, mit den Bezeichnungen aus Beispiel 5.6, die ganze Gruppe S_3, $\{e\}$, $\Sigma_i := \{e, \sigma_i\} = F_{\{i\}}$ und $\Delta := \{e, \delta, \delta^2\}$.

5.11 Bemerkung: Für jede Gruppe G bildet die Menge aller Untergruppen von G bezüglich der Untergruppenrelation $\leq$ einen Verband.

5.12 Testfrage: Stellen Sie den Untergruppenverband von S_3 als Diagramm dar.

5.13 Definition: Ein *Gruppenhomomorphismus* von einer Gruppe $(G, \circ, \iota, e)$ in ein Gruppe $(H, \cdot, j, 1)$ ist ein Morphismus zwischen den algebraischen Systemen $(G, \circ, \iota, e)$ und $(H, \cdot, j, 1)$.

Für Gruppenhomomorphismen gibt es eine Charakterisierung, die der Charakterisierung von Untergruppen aus Lemma 5.9 entspricht.

5.14 Lemma: *Eine Abbildung $h\colon G \to H$ zwischen zwei Gruppen G und H ist genau dann ein Gruppenhomomorphismus, wenn gilt:*
$$\forall a, b \in G\colon h(ab^{-1}) = h(a)(h(b))^{-1}.$$

Beweis: Gezeigt werden muß nur, daß jede Abbildung mit diesen Eigenschaften ein Gruppenhomomorphismus ist, die andere Richtung ist offensichtlich wahr.

Sei e das Neutralelement in G und e' das Neutralelement von H. Es gilt

$$h(e) = h(ee^{-1}) = h(e)(h(e))^{-1} = e'.$$

Das Neutralelement von G wird also auf das Neutralelement von H abgebildet.

Für $a \in G$ gilt mit dem bereits Gezeigten:

$$h(a^{-1}) = h(ea^{-1}) = h(e)(h(a))^{-1} = e'(h(a))^{-1} = (h(a))^{-1}.$$

Also ist h verträglich mit dem Invertieren.

Für $a, b \in G$ gilt mit dem bereits Gezeigten:

$$h(ab) = h(a(b^{-1})^{-1}) = h(a)(h(b^{-1}))^{-1} = h(a)((h(b))^{-1})^{-1} = h(a)h(b).$$

Also ist h verträglich mit den Gruppenmultiplikation. Damit ist h ein Morphismus. □

5.15 Definition: Ein *Gruppenmonomorphismus* ist ein injektiver Gruppenhomomorphismus, ein *Gruppenepimorphismus* ist ein surjektiver Gruppenhomomorphismus und ein *Gruppenisomorphismus* ist ein bijektiver Gruppenhomomorphismus.

Das nächste Resultat besagt, daß jede Gruppe isomorph zu einer Untergruppe einer geeigneten Permutationsgruppe ist.

5.16 Satz: *Für jede Gruppe G gibt es ein X und einen Gruppenmonomorphismus von G in die Permutationsgruppe $S(X)$ von X.*

Beweis: Wir setzen $X := G$ und lassen die Gruppe durch Linksmultiplikation wirken. Das heißt, wir betrachten die Abbildung $f\colon G \to S(G)$ die jedem Gruppenelement $g \in G$ die Permutation $f(g)\colon G \to G\colon h \mapsto gh$ zuordnet.

Für jedes $g, h \in G$ gilt

$$(f(g) \circ f(g^{-1}))(h) = g(g^{-1}h) = (gg^{-1})h = h.$$

Das heißt, $f(g) \circ f(g^{-1})$ ist die identische Abbildung. Damit ist $f(g^{-1})$ das Inverse zu $f(g)$. Insbesondere ist jede Bild $f(g)$ auch tatsächlich eine Bijektion, also invertierbar.

Wir wollen nun nachweisen, daß f injektiv ist. Angenommen g_1, g_2 sind Elemente aus G mit $f(g_1) = f(g_2)$. Die Aussage $f(g_1) = f(g_2)$ bedeutet, daß für alle $h \in G$ gilt:

$$g_1 h = f(g_1)(h) = f(g_2)(h) = g_2 h.$$

Wir setzten $h = e$ und erhalten $g_1 = g_2$.

Es ist noch zu zeigen, daß f ein Morphismus ist. Für $g_1, g_2, h \in G$ gilt:

$$\begin{aligned} f(g_1 g_2^{-1})(h) &= (g_1 g_2^{-1})h = g_1(g_2^{-1}h) = g_1(f(g_2)^{-1}(h)) \\ &= f(g_1)(f(g_2)^{-1}(h)) = (f(g_1) \circ f(g_2)^{-1})(h). \end{aligned}$$

Da $h \in G$ beliebig war, folgt $f(g_1 g_2^{-1}) = f(g_1) \circ f(g_2)^{-1}$. Gemäß Lemma 5.14 ist f ein Morphismus. □

Natürlich wirkt G auch durch Rechtsmultiplikation auf G. Das liefert aber im Allgemeinen eine andere Untergruppe von $S(G)$

5.17 Testfrage: Die Gruppen S_3, $(\mathbb{Z}_6, +)$ und $(\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$ haben alle genau sechs Elemente. Sind sie auch isomorph? Genauer, zeigen oder widerlegen Sie:

1. S_3 ist isomorph zu $(\mathbb{Z}_6, +)$.
2. S_3 ist isomorph zu $(\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$.
3. $(\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$ ist isomorph zu $(\mathbb{Z}_6, +)$.

Die Aussage des folgenden Lemmas sollte Sie an Testfrage 3.48 erinnern. Allerdings verwenden wir nun eine multiplikative statt additive Notation.

5.18 Lemma: *Sie H eine Untergruppe einer Gruppe G. Dann wird durch*

$$a \equiv_H b \;:\Leftrightarrow\; ab^{-1} \in H$$

ein Äquivalenzrelation auf G definiert.

Beweis: Für jedes $a \in G$ gilt $aa^{-1} = e \in H$. Damit ist die Relation reflexiv.

Für $a, b \in G$ gilt

$$a \equiv_H b \iff ab^{-1} \in H \iff (ab^{-1})^{-1} = ba^{-1} \in H \iff b \equiv_H a.$$

Damit ist die Relation symmetrisch.

Für $a, b, c \in G$ gilt

$$\begin{aligned} a \equiv_H b \equiv_H c &\iff ab^{-1} \in H \text{ und } bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} = ac^{-1} \in H \\ &\iff a \equiv_H c. \end{aligned}$$

Dies zeigt, daß die Relation transitiv ist. Zusammengenommen folgt, daß eine Äquivalenzrelation vorliegt. □

5.19 Bemerkung: Im allgemeinen ist die oben definierte Äquivalenzrelation keine Kongruenzrelation. Das folgende Beispiel soll dies demonstrieren.

Sei $G := S_3$ die Permutationsgruppe von $\{1,2,3\}$ mit der Notation aus Beispiel 5.6 und $H := \{e, \sigma_3\} = F_{\{3\}}$. Es gilt $e \equiv_H \sigma_3$ und $\sigma_1 \equiv_H \sigma_3\sigma_1 = \delta$. Weiterhin gilt

$$(\delta\sigma_3)(\sigma_1 e)^{-1} = \delta\sigma_3\sigma_1^{-1} = \delta\sigma_3\sigma_1 = \delta^2 \notin H.$$

Damit ist $\delta\sigma_3$ nicht äquivalent zu $\sigma_1 e$. Dies bedeutet, daß die Äquivalenzrelation keine Kongruenzrelation ist.

Wir werden in Satz 5.33 die Untergruppen charakterisieren, die Kongruenzrelationen induzieren.

5.20 Definition: Für eine Untergruppe H einer Gruppe G und $g \in G$ ist

$gH := \{gh \mid h \in H\}$ die *Linksnebenklasse* nach H, die g enthält,

$Hg := \{hg \mid h \in H\}$ die *Rechtsnebenklasse* nach H, die g enthält.

5.21 Bemerkung: Eine Nebenklasse gH oder Hg ist genau dann eine Untergruppe, wenn $g \in H$ gilt.

5.22 Lemma: *Ist H eine Untergruppe einer Gruppe G, so sind die Rechtsnebenklassen genau die Äquivalenzklassen der Äquivalenzrelation $\equiv_H$.*

Beweis: Für $a, b \in G$ gilt:

$$\begin{aligned} a \equiv_H b &\iff ab^{-1} \in H \iff \exists h \in H\colon ab^{-1} = h \\ &\iff \exists h \in H\colon a = hb \Rightarrow a, b \in Hb. \end{aligned}$$

Umgekehrt, für $a, b, g \in G$ gilt:

$$a, b \in Hg \iff \exists h, l \in H\colon a = hg,\ b = lg.$$

Daraus folgt

$$ab^{-1} = hg(lg)^{-1} = hgg^{-1}l^{-1} = hl^{-1} \in H,$$

also $a \equiv_H b$. □

Da die Rechtsnebenklassen die Äquivalenzklassen der Äquivalenzrelation $\equiv_H$ sind, folgt aus Satz 1.40 unmittelbar folgendes Resultat.

5.23 Korollar: *Ist H eine Untergruppe einer Gruppe G, so bilden die Rechtsnebenklassen eine Partition. Die Gruppe G ist also die disjunkte Vereinigung der Rechtsnebenklassen nach H.*

5.24 Definition: Der *Index* einer Untergruppe H in einer Gruppe G, geschrieben $(G : H)$, ist die Mächtigkeit der Menge der Rechtsnebenklassen nach H.

Ist G eine Gruppe, so daß $|G|$ endlich ist, so heißt $|G|$ die *Ordnung von* G. Dabei steht $|X|$ für die Mächtigkeit der Menge X.

5.25 Satz (Indexformel): *Für jede Untergruppe H einer Gruppe G gilt*

$$|G| = (G : H) \cdot |H| .$$

Beweis: Sei H eine Untergruppe von G. Für jede Rechtsnebenklasse Hg ist $\gamma\colon H \to Hg\colon h \mapsto hg$ eine Bijektion. Daher sind alle Rechtsnebenklassen nach H gleich mächtig. Da G die disjunkte Vereinigung der Rechtsnebenklassen nach H ist, und es $(G : H)$ Rechtsnebenklassen nach H gibt, folgt $|G| = (G : H) \cdot |H|$. □

Aus diesem Resultat folgen unmittelbar folgende nützliche Ergebnisse.

5.26 Korollar: *Ist H eine Untergruppe einer endlichen Gruppe G, so teilt die Ordnung von H die Ordnung von G.*

5.27 Korollar: *Ist G eine endliche Gruppe von Primzahlordnung, das heißt $|G|$ ist prim, so sind $\{e\}$ und G die einzigen Untergruppen von G.*

Alles, was hier für Rechtnebenklassen gemacht wurde, kann auch für Linksnebenklassen gemacht werden. Ist H eine Untergruppe einer Gruppe H, so liefern die Linksnebenklassen in der Regel eine andere Partition als die Rechtsnebenklassen. Aber beide Partitionen sind gleich mächtig. Für den Index von H in G können daher auch die Linksnebenklassen herangezogen werden.

5.28 Testfrage: Sei H eine Untergruppe einer endlichen Gruppe G. Konstruieren Sie eine Äquivalenzrelation auf G, deren Äquivalenzklassen genau die Linksnebenklassen von G nach H sind.

Die Untergruppen, für die jede Linksnebenklasse auch eine Rechtsnebenklasse ist, sind natürlich von besonderem Interesse. Wir untersuchen sie nun.

5.29 Definition: Eine Untergruppe N einer Gruppe G heißt *Normalteiler von* G, geschrieben $N \lhd G$, wenn gilt:

$$\forall g \in G\colon gNg^{-1} = N.$$

Dabei ist $gNg^{-1} := \{gng^{-1} \mid n \in N\}$.

5.30 Lemma: *Für eine Untergruppe N einer Gruppe G sind folgende Aussagen äquivalent:*

1. *N ist Normalteiler von G.*
2. $\forall g \in G, \forall n \in N\colon gng^{-1} \in N$.
3. $\forall g \in G\colon gN = Ng$.

Beweis: Die Äquivalenz der ersten und dritten Aussage folgt aus

$$N = gNg^{-1} \iff Ng = gNg^{-1}g = gN.$$

Die zweite Aussage ist eine Abschwächung der ersten Aussage. Daher muß nur gezeigt werden, daß die erste aus der zweiten Aussage folgt. Dies trifft zu, wenn es für jedes $m \in N$ und jedes $g \in G$ ein $n \in N$ gibt mit $m = gng^{-1}$. Da mit g auch g^{-1} in G liegt, liegt mit der zweiten Aussage auch $n := g^{-1}m(g^{-1})^{-1} = g^{-1}mg$ in N. Für dieses n gilt $gng^{-1} = gg^{-1}mgg^{-1} = m$. □

5.31 Beispiel: Sei $G := S_3$ die Permutationsgruppe von $\{1,2,3\}$ mit den Bezeichnungen aus Beispiel 5.6.

Die Untergruppen $\Sigma_i = \{e, \sigma_i\}$ sind kein Normalteiler, denn für $\{i,j,k\} = \{1,2,3\}$ gilt:

$$\sigma_j\sigma_i\sigma_j^{-1}(i) = \sigma_j\sigma_i\sigma_j(i) = \sigma_j\sigma_i(k) = \sigma_j(j) = j.$$

Damit ist i kein Fixelement von $\sigma_j\sigma_i\sigma_j^{-1}$ also nicht in Σ_i.

Die Untergruppe $\Delta = \{e, \delta, \delta^2\}$ ist ein Normalteiler. Es gilt $|G| = 3! = 6$ und $|\Delta| = 3$, also mit der Indexformel $(G:\Delta) = 2$. Wegen $\sigma_3 \notin \Delta$ ist G damit die disjunkte Vereinigung von Δ und $\Delta\sigma_3$. Für $n \in \Delta$ gilt $n\Delta n^{-1} = \Delta$, da Δ eine Gruppe ist. Für σ_3 gilt:

$$\begin{aligned}
\sigma_3\delta\sigma_3^{-1} &= \sigma_3\delta\sigma_3 = \sigma_3\sigma_3\sigma_1\sigma_3 = \sigma_1\sigma_3 = (\sigma_3\sigma_1)^{-1} = \delta^{-1} = \delta^2 \in \Delta,\\
\sigma_3\delta\delta\sigma_3^{-1} &= \sigma_3\delta\sigma_3\sigma_3\delta\sigma_3 = \delta^2\delta^2 = \delta \in \Delta,\\
\sigma_3 e\sigma_3^{-1} &= e \in \Delta,
\end{aligned}$$

also $\sigma_3 n\sigma_3^{-1} \in \Delta$ für alle $n \in \Delta$. Für $g \in \Delta\sigma_3$ gibt es ein $n \in \Delta$ mit $g = n\sigma_3$. Daher folgt mit dem bereits Gezeigten:

$$g\Delta g^{-1} = n\sigma_3\Delta(n\sigma_3)^{-1} = n\sigma_3\Delta\sigma_3^{-1}n^{-1} = n\Delta n^{-1} = \Delta.$$

Damit ist Δ in der Tat ein Normalteiler.

5.32 Bemerkung: In einer kommutativen Gruppe sind alle Untergruppen Normalteiler. Denn für $g \in G$ und $u \in U \leq G$ gilt $gug^{-1} = ugg^{-1} = u \in U$.

5.33 Satz: *Ist N ein Normalteiler einer Gruppe G, so ist die gemäß Lemma 5.18 konstruierte Relation $\equiv_N$ eine Kongruenzrelation.*

Beweis: In Lemma 5.18 wurde bereits gezeigt, daß die Relation $\equiv_N$ eine Äquivalenzrelation ist. Es muß also nur noch gezeigt werden, daß die Relation mit der Gruppenmultiplikation verträglich ist.

Seien $a, b, c, d \in G$ mit $a \equiv_N b$ und $c \equiv_N d$. Es gibt also $m, n \in N$ mit $ab^{-1} = m$ und $cd^{-1} = n$. Es folgt

$$(ac)(bd)^{-1} = acd^{-1}b^{-1} = anb^{-1} = ana^{-1}ab^{-1} = ana^{-1}m.$$

Da N ein Normalteiler ist, gilt $ana^{-1} \in N$, also auch $ana^{-1}m \in N$. Die bedeutet $ac \equiv_N bd$. □

5.34 Definition: Sei N eine Normalteiler einer Gruppe G. Die Faktorgruppe G/N ist die Gruppe der Nebenklassen von G nach N mit der induzierten Multiplikation. Das heißt, $G/N = (\{gN \mid g \in G\}, \circ)$, wo

$$gN \circ hN = (gh)N.$$

Wegen Satz 5.33 sind die Nebenklassen von G nach N die Äquivalenzklassen einer Kongruenzrelation. Nach Satz 3.49 ist G/N mit der induzierten Multiplikation eine binäre Algebra. Die Nebenklasse $N = eN$ ist das Neutralelement und das multiplikative Inverse zu gN ist $g^{-1}N$. Assoziativität von $\circ$ folgt aus der Assoziativität der Multiplikation auf G. Damit ist G/N eine Gruppe.

Der Kern eines Gruppenhomomorphismus ist, analog zur Linearen Algebra, das Urbild des Neutralelements.

5.35 Definition: Sei $h\colon G \to H$ ein Gruppenhomomorphismus und e das Neutralelement in H. Dann ist

$$\mathrm{Kern}(h) := \{g \in G \mid h(g) = e\}$$

der *Kern von h.*

Aus Satz 3.49 folgt unmittelbar folgendes Resultat.

5.36 Lemma: *Ist N ein Normalteiler einer Gruppe G, so ist $\pi\colon G \to G/N$ ein Epimorphismus und $N = \mathrm{Kern}(\pi)$.*

Das nächste Resultat besagt, daß nicht nur jeder Normalteiler als Kern eines Homomorphismus auftritt, sondern jeder Kern eines Homomorphismus ein Normalteiler ist.

5.37 Lemma: *Ist $h\colon G \to H$ ein Gruppenhomomorphismus, so ist* $\mathrm{Kern}(h)$ *ein Normalteiler in G.*

Beweis: Sei e das Neutralelement in H. Für $a, b \in \mathrm{Kern}(h)$ gilt

$$h(ab^{-1}) = h(a)h(b)^{-1} = ee = e,$$

also $ab^{-1} \in \mathrm{Kern}(h)$. Damit ist $\mathrm{Kern}(h)$ eine Untergruppe von G, Für $g \in G$ und $a \in \mathrm{Kern}(h)$ gilt

$$\begin{aligned} h(gag^{-1}) &= h(g)h(a)h(g)^{-1} && h \text{ ist Gruppenhomomorphismus,} \\ &= h(g)h(g)^{-1} && a \in \mathrm{Kern}(h), \\ &= e, \end{aligned}$$

also $gag^{-1} \in \mathrm{Kern}(h)$. Damit ist $\mathrm{Kern}(h)$ ein Normalteiler. □

Eine lineare Abbildung ist genau dann injektiv, wenn ihr Kern nur aus dem Nullvektor besteht. Eine analoge Aussage gilt auch für Homomorphismen.

5.38 Testfrage: Sei $h\colon G \to H$ ein Gruppenhomomorphismus. Zeigen Sie, daß h genau dann injektiv ist, wenn $\mathrm{Kern}(h)$ nur das Neutralelement aus G enthält.

Das folgende Resultat ist ein Spezialfall von Satz 3.55 und wird daher nicht nochmals bewiesen.

5.39 Satz (Homomorphiesatz): *Ist $h\colon G \to H$ ein Gruppenepimorphismus, so ist* $G/\mathrm{Kern}(h)$ *isomorph zu H.*

5.40 Testfrage: Beweisen Sie diesen Satz ohne auf Satz 3.55 zurückzugreifen.

5.41 Definition: Sei G eine Gruppe mit Neutralelement e und $g \in G$. Die *Ordnung* $\mathrm{ord}(g)$ von g ist die kleinste natürliche Zahl $n > 0$ mit $g^n = e$, falls es solch ein n gibt, und ∞ sonst.

Der *Exponent* $\exp(G)$ von G ist die kleinste natürliche Zahl $n > 0$ mit $g^n = e$ für alle $g \in G$, falls es solch ein n gibt, und ∞ sonst.

5.42 Beispiel: Sei $G := S_3$ mit der Notation aus Beispiel 5.6. Es gilt $\mathrm{ord}(e) = 1$, $\mathrm{ord}(\sigma_i) = 2$ für $i \in \{1, 2, 3\}$ und $\mathrm{ord}(\delta) = \mathrm{ord}(\delta^2) = 3$. Daraus folgt $\exp(G) = 6$.

5.43 Definition: Eine Gruppe G heißt *zyklisch*, wenn es eine $a \in G$ gibt, so daß es für jedes $g \in G$ ein $z \in \mathbb{Z}$ gibt mit $g = a^z$. Dabei gilt $a^0 := e$. Das Element a heißt *erzeugendes Element*.

5.44 Beispiel: Die Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, +)$, $n \in \mathbb{N} \setminus \{0\}$, sind zyklisch. Erzeugende Elemente sind 1 bzw. $[1]$.

Das nächste Resultat besagt, daß die eben aufgeführten zyklischen Gruppen bis auf Isomorphie bereits alle zyklischen Gruppen sind.

5.45 Satz: *Eine zyklische Gruppe G ist entweder isomorph zu $(\mathbb{Z}, +)$ oder es gibt ein $n \in \mathbb{N} \setminus \{0\}$, so daß G isomorph zu $(\mathbb{Z}_n, +)$ ist.*

Beweis: Sei $(G, \cdot)$ eine zyklische Gruppe mit erzeugendem Element a. Die Abbildung

$$f\colon (\mathbb{Z}, +) \to (G, \cdot)\colon z \mapsto a^z,$$

ist ein surjektiver Homomorphismus, also ein Gruppenepimorphismus. Nach dem Homomorphiesatz (Satz 5.39) ist G isomorph zu $\mathbb{Z}/\mathrm{Kern}(f)$.

Gilt $\mathrm{Kern}(f) = \{0\}$, so ist G isomorph zu $(\mathbb{Z}, +)$. Gilt $\mathrm{Kern}(f) \neq \{0\}$ so sei d die kleinste positive Zahl in $\mathrm{Kern}(f)$. Dann sind die Elemente $e, a, a^2, \ldots, a^{d-1}$ paarweise verschieden. Für $z \in \mathbb{Z}$ gibt es $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, d-1\}$ mit $z = qd + r$. Es gilt $a^z = a^{qd+r} = (a^d)^q a^r = e^q a^r = a^r$. Somit sind $e, a, a^2, \ldots, a^{d-1}$ die einzigen Elemente von G. Die Abbildung $G \to \mathbb{Z}_d\colon a^r \mapsto [r]$ ist ein Isomorphismus. □

5.46 Satz: *Jede Gruppe G von Primzahlordnung ist zyklisch.*

Beweis: Sei $a \in G \setminus \{e\}$. Es gilt $d := \mathrm{ord}(a) \neq 1$. Die Elemente $e, a, a^2, \ldots, a^{d-1}$ bilden eine zyklische Untergruppe A der Ordnung d. Die Indexformel Satz 5.25 liefert $|G| = (G : A) \cdot |A| = (G : A) \cdot d$. Da $|G|$ eine Primzahl ist und $d > 1$ gilt, folgt $d = |G|$, also $A = G$. □

5.47 Bemerkung: Im eben geführten Beweis ist a eine beliebiges Element von $G \setminus \{e\}$. Der Beweis liefert daher, daß in einer Gruppe von Primzahlordnung jedes vom Neutralelement verschiedene Element ein erzeugendes Element ist.

5.48 Satz: *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Beweis: Wegen Satz 5.45 muß lediglich gezeigt werden, daß alle Untergruppen von $(\mathbb{Z}, +)$ und für jedes $n \in \mathbb{N} \setminus \{0\}$ alle Untergruppen von $(\mathbb{Z}_n, +)$ zyklisch sind.

Sei H eine Untergruppe von $(\mathbb{Z}, +)$. Im Fall $H = \{0\}$ ist H trivialerweise zyklisch. Gilt $H \neq \{0\}$, so sei a die kleinste positive Zahl in H. Sei $h \in H$. Es gibt $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, a-1\}$ mit $h = qa + r$. Doch dann gilt $r = h - qa \in H$,

also $r \in \{0, 1, \ldots, a-1\} \cap H = \{0\}$. Das heißt, $h = qa$ ist im Aufspann von a. (Wegen der additiven Schreibweise besteht der Aufspann von a aus den Elementen $\{za \mid z \in \mathbb{Z}\}$). Damit liegt H im Aufspann von a. Da H abgeschlossen bezüglich Addition und Invertieren ist, enthält H mit a auch den ganzen Aufspann von a. Damit ist H eine zyklische Untergruppe mit a als erzeugendes Element.

Sei nun H eine Untergruppe von $(\mathbb{Z}_n, +)$. Besteht H nur aus dem Neutralelement, so ist H trivialerweise zyklisch. Besteht H nicht nur aus dem Neutralelement, so sei m das kleinste Element in $\{1, \ldots, n\}$ mit $[m] \in H$. Analog zum eben geführten Beweis folgt, daß H eine zyklische Untergruppe mit $[m]$ als erzeugendes Element ist. □

5.2. Wirkungen von Gruppen auf Mengen

Wir haben bereits in Satz 5.16 eine Gruppe als eine Menge von Operationen auf einer Menge betrachtet. Wir wollen diese Sichtweise nun genauer untersuchen.

5.49 Definition: Eine Gruppe G *wirkt von links* auf einer Menge X, falls es eine Abbildung $\omega\colon G \times X \to X$ gibt mit:

1. $\forall g, h \in G, \forall x \in X\colon \omega(gh, x) = \omega(g, \omega(h, x))$,
2. $\forall x \in X\colon \omega(e, x) = x$.

Üblicherweise schreiben wir $g(x)$ oder gx für $\omega(g, x)$. In dieser Schreibweise lauten die Bedingungen:

1. $\forall g, h \in G, \forall x \in X\colon (gh)(x) = g(h(x))$,
2. $\forall x \in X\colon e(x) = x$.

5.50 Bemerkung: Anstatt *Wirkung* spricht man auch von *Operation einer Gruppe auf einer Menge.*

5.51 Beispiele:

1. Sei G eine Gruppe und X eine Menge. Durch $g(x) := x$ für alle $g \in G$ und $x \in X$ wird eine Wirkung von G auf X definiert. Die Gruppe wirkt, indem sie nichts bewegt.
2. Sei H eine Untergruppe einer Gruppe G. Durch $h(g) := hg$ für alle $h \in H$ und $g \in G$ wird eine Wirkung von H auf G definiert, die *Wirkung durch Linksmultiplikation.* Im Beweis zu Satz 5.16 haben wir diese Wirkung im Spezialfall $H = G$ bereits kennengelernt.
3. Sei N ein Normalteiler einer Gruppe G. Durch $g(n) := gng^{-1}$ für alle $g \in G$ und $n \in N$ wird eine Wirkung von G auf N definiert.

Da N ein Normalteiler ist, gilt $\forall (g,n) \in G \times N\colon g(n) = gng^{-1} \in N$. Für $g, h \in G$ und $n \in N$ gilt

$$(gh)(n) = ghn(gh)^{-1} = ghnh^{-1}g^{-1} = g(h(n)).$$

Für das Neutralelement e und $n \in N$ gilt $e(n) = ene = n$. Damit liegt in der Tat eine Wirkung von G auf N vor.

5.52 Testfrage: Sie G eine Gruppe und X die Menge aller Untergruppen von G. Für $g \in G$ und $U \in X$ sei $g(U) := gUg^{-1}$. Zeigen Sie, daß dies eine Wirkung von G auf X definiert.

Wie sieht diese Wirkung für $G = S_3$ aus?

5.53 Definition: Sei G eine Gruppe, die auf der Menge X wirkt. Durch

$$x \equiv y \ :\Leftrightarrow\ \exists g \in G\colon y = gx$$

wird eine Relation auf X definiert.

5.54 Lemma: *Die eben definierte Relation ist eine Äquivalenzrelation.*

Beweis: Für $x \in X$ gilt $x = ex$, also $x \equiv x$. Die Relation ist also reflexiv.

Angenommen $x, y \in X$ mit $x \equiv y$. Dann gibt es ein $g \in G$ mit $y = gx$. Doch dann gilt $x = g^{-1}gx = g^{-1}y$. Wegen $g^{-1} \in G$ folgt $y \equiv x$, die Relation ist also symmetrisch.

Seien $x, y, z \in X$ mit $x \equiv y \equiv z$. Es gibt also $g, h \in G$ mit $y = gx$ und $z = hy$. Doch dann folgt $z = hgx$. Wegen $hg \in G$ gilt $z \equiv x$, die Relation ist also transitiv. Damit ist die Relation eine Äquivalenzrelation. □

5.55 Bemerkung: Die Äquivalenzklassen dieser Relation können sehr verschieden aussehen. Zum Beispiel wirkt die multiplikative Gruppe $(\mathbb{C} \setminus \{0\}, \cdot)$ durch Linksmultiplikation auf $\mathbb{C}$. Die einzigen Äquivalenzklassen sind $\{0\}$ und $\mathbb{C} \setminus \{0\}$.

5.56 Definition: Sei G eine Gruppe, die auf einer Menge X wirkt. Für $x \in X$ sei

$G_x := \{g \in G \mid gx = x\}$ die *Fixgruppe* oder der *Stabilisator von* x,

$x^G := \{gx \mid g \in G\}$ die *Bahn* oder der *Orbit von* x unter G.

5.57 Lemma: *Sei G eine Gruppe, die auf einer Menge X wirkt. Für $x \in X$ ist G_x eine Untergruppe von G und x^G die Äquivalenzklasse der Wirkung von G auf X, die x enthält.*

Beweis: Für $g, h \in G_x$ gilt

$$gh^{-1}(x) = gh^{-1}(h(x)) = g(x) = x$$

also $gh^{-1} \in G_x$. Damit ist G_x eine Untergruppe von G.

Die zweite Aussage ist offensichtlich wahr. □

5.58 Testfrage: Sei G eine Gruppe, die auf einer Menge X wirkt. Zeigen Sie, daß für alle $g \in G$ und alle $x \in X$ gilt:

$$G_{g(x)} = gG_xg^{-1}.$$

5.59 Definition: Sei G eine Gruppe, die auf einer Menge X wirkt.

1. G wirkt *transitiv auf* X, falls $X = x^G$ für ein $x \in X$.
2. $x \in X$ ist ein *Fixpunkt von* G, wenn $x^G = \{x\}$ gilt.

5.60 Testfragen:

1. Sei G eine Gruppe, die auf einer Menge X wirkt und $x \in X$. Zeigen Sie, daß die Einschränkung der Wirkung von G auf x^G transitiv ist.
2. Sei G eine Gruppe und X die Menge der Untergruppen von G. Durch $g(U) := gUg^{-1}$ wird eine Wirkung von G auf X definiert. Zeigen Sie, daß genau die Normalteiler von G Fixpunkte dieser Wirkung sind.
3. Sei G eine Gruppe, die auf einer Menge X operiert. Zeigen Sie, daß G genau dann transitiv operiert, wenn für alle $x, y \in X$ ein $g \in G$ mit $g(x) = y$ existiert.

Die Ordnungen von Bahn, Stabilisator und Gruppe sind über die Bahnengleichung miteinander verknüpft.

5.61 Satz (Bahnengleichung): *Sei G eine endliche Gruppe, die auf einer Menge X wirkt. Für jedes $x \in X$ gilt*

$$\left|x^G\right| |G_x| = |G| .$$

Beweis: Mit Lemma 5.57 ist $H := G_x$ eine Untergruppe von G. Die Linksnebenklassen von H in G sind paarweise disjunkt. Für $g \in G$ gilt $|gH| = |H|$, denn

$$\varphi\colon H \to gH\colon h \mapsto gh$$

ist eine Bijektion. Die Umkehrabbildung bildet $a \in gH$ auf $g^{-1}a \in H$ ab. Damit sind alle Nebenklassen gleich mächtig.

Es muß noch gezeigt werden, daß es eine bijektive Abbildung β von x^G auf die Menge aller Linksnebenklassen von H gibt.

Sei $y \in x^G$. Dann gibt es eine $g \in G$ mit $gx = y$. Wir setzen $\beta(y) = gH$. Sind $f, g \in G$. Dann gilt

$$f(x) = g(x) \iff g^{-1}f(x) = x \iff g^{-1}f \in H \iff f \in gH \iff fH = gH.$$

Daraus folgt, daß die Abbildung β wohldefiniert und injektiv ist. Ist gH eine Nebenklasse, so gilt $y := g(x) \in x^G$ und $\beta(y) = gH$. Damit ist β surjektiv, also bijektiv. Die Gruppe G ist somit die disjunkte Vereinigung der Nebenklassen $\{\beta(y) \mid y \in x^G\}$ und für jedes $y \in x^G$ gilt $|\beta(y)| = |H| = |G_x|$. Daraus folgt die Bahnengleichung. □

5.62 Testfrage: Zeigen Sie mit der Bahnengleichung, daß $|S_n| = n!$ für $n \in \mathbb{N} \setminus \{0\}$ gilt.

Wir wollen nun Strukturaussagen über Gruppen, insbesondere über endliche Gruppen machen. Zunächst einige spezielle Teilmengen von Gruppen.

5.63 Definition: Sei S eine Teilmenge einer Gruppe G.

1. Die Menge $N_S(G) := \{g \in G \mid gSg^{-1} = S\}$ heißt *Normalisator von S in G.*
2. Die Menge $Z_S(G) := \{g \in G \mid \forall s \in S\colon gsg^{-1} = s\}$ heißt *Zentralisator von S in G.*
3. Die Menge $Z_G(G)$ heißt *Zentrum von G.*

5.64 Bemerkung: Für eine Teilmenge S einer Gruppe G sind $N_S(G)$ und $Z_S(G)$ Untergruppen von G. Offensichtlich gilt $Z_S(G) \leq N_S(G)$. Ist S eine Untergruppe von G, so ist $N_S(G)$ ein Normaltteiler in G.

Eine Gruppe ist genau dann kommutativ, wenn $Z_G(G) = G$ gilt.

5.65 Testfrage: Beweisen Sie die in der vorangehenden Bemerkung aufgestellten Behauptungen.

Als nächstes wollen wir Untergruppen mit Primzahlpotenz untersuchen. Zunächst zeigen wir, daß es zu jedem Primteiler der Gruppenordnung einer kommutativen Gruppe eine Untergruppe dieser Ordnung gibt. Dazu benötigen wir folgende Vorüberlegung.

5.66 Lemma: *Ist G eine endliche kommutative Gruppe so gibt es ein $k \in \mathbb{N}$ mit $|G|$ teilt $\exp(G)^k$.*

Beweis: Wir zeigen die Aussage durch eine Induktionsbeweis über die Gruppenordnung. Für $|G| = 1$, also $G = \{e\}$, ist die Aussage trivialerweise wahr.

Sei nun $|G| = k > 1$. Dann gibt es ein $b \in G \setminus \{e\}$. Sei H die von b erzeugte Untergruppe von G. Es gilt $|H| = \text{ord}(b) \geq 2$, also wird $\exp(G)$ von $|H|$ geteilt. Da G kommutativ ist, ist H ein Normalteiler. Sei $F := {}^{G}/_{H}$ die Faktorgruppe von G nach H. Mit der Indexformel Satz 5.25 gilt

$$|F| = (G : H) = \frac{|G|}{|H|} < |G| = n.$$

Nach Induktionsvoraussetzung gibt es ein $l \in \mathbb{N}$, so daß $\exp(F)^l$ von $|F| = (G : H)$ geteilt wird. Der Exponent $\exp(F)$ der Faktorgruppe ist ein Teiler von $\exp(G)$. Also wird auch $\exp(G)^l$ von $(G : H)$ geteilt. Doch dann wird $\exp(G)^{l+1}$ von $(G : H) \cdot |H| = |G|$ geteilt. □

Das angestrebte Resultat kann nun ohne Aufwand gezeigt werden.

5.67 Lemma: *Ist G eine endliche kommutative Gruppe und p ein Primteiler von $|G|$, so enthält G eine Untergruppe der Ordnung p.*

Beweis: Sei p ein Primteiler von $|G|$. Wegen Lemma 5.66 gibt es ein $g \in G$ und ein $k \in \mathbb{N}$ mit $|G|$ teilt $\text{ord}(g)^k$. Doch dann wird $\text{ord}(g)$ von p geteilt. Sei $s := \frac{\text{ord}(g)}{p} \in \mathbb{N}$. Das Element $h := g^s$ hat Ordnung p, denn $h^n = e \iff g^{sn} = e$. Die von h erzeugte Untergruppe hat also die Ordnung p. □

Wir wollen nun das Resultat verallgemeinern, indem wir beliebige Primzahlpotenzen betrachten. Dazu müssen wir zunächst ein zahlentheoretisches Resultat herleiten.

5.68 Definition: Für $p, n \in \mathbb{N} \setminus \{0\}$ sei $\text{maxex}(p, n)$ die Zahl $r \in \mathbb{N}$ so, daß n von p^r aber nicht von p^{r+1} geteilt wird.

5.69 Testfrage: Sie $p, m, n \in \mathbb{N} \setminus \{0\}$. Zeigen Sie $\text{maxex}(p, nm) = \text{maxex}(p, n) + \text{maxex}(p, m)$.

5.70 Lemma: *Sei $n \in \mathbb{N}$ und p eine Primzahl mit $n = p^r m$ und $\text{ggt}(p, m) = 1$. Sei $r := \text{maxex}(p, n)$. Für $1 \leq s \leq r$ gilt*

$$\text{maxex}(p, \tbinom{n}{p^s}) = r - s.$$

Beweis: Sei $m := \frac{n}{r^r}$. Nach Konstruktion von r gilt $m \in \mathbb{N}$ und $\operatorname{ggt}(p, m) = 1$. Es gilt:

$$\begin{aligned}\binom{n}{p^s} &= \frac{n!}{p^s!(n-p^s)!} \\ &= \frac{n \cdot (n-1) \cdot \cdots \cdot (n-p^s+1)}{1 \cdot 2 \cdot \cdots \cdot p^s} = \prod_{i=1}^{p^s} \frac{n+1-i}{i} \\ &= \frac{n}{p^s} \cdot \frac{(n-1) \cdot \cdots \cdot (n-p^s+1)}{1 \cdot 2 \cdot \cdots \cdot p^{s-1}} \\ &= \frac{mp^r}{p^s} \prod_{i=1}^{p^{s-1}} \frac{n-i}{i} \\ &= mp^{r-s} \prod_{i=1}^{p^{s-1}} \frac{n-i}{i}.\end{aligned}$$

Wegen $\prod_{i=1}^{p^{s-1}} \frac{n-i}{i} = \binom{n-1}{s-1} \in \mathbb{N}$ wird $\binom{n}{p} = mp^{r-s} \prod_{i=1}^{p^{s-1}} \frac{n-i}{i}$ von p^{r-s} geteilt. Wegen $\operatorname{ggt}(p, m) = 1$ wird $\binom{n}{p}$ genau dann von p^{r-s+1} geteilt, wenn $\prod_{i=1}^{p^{s-1}} \frac{n-i}{i}$ von p geteilt wird. Die ganze Zahl $\prod_{i=1}^{p^{s-1}} \frac{n-i}{i}$ wird genau dann von p geteilt, wenn $\operatorname{maxex}(p, \prod_{i=1}^{p^{s-1}} n-i) > \operatorname{maxex}(p, \prod_{i=1}^{p^{s-1}} i)$ gilt. Für $i \leq p^s \leq p^r$ gilt

$$\operatorname{maxex}(p, n-i) = \operatorname{maxex}(p, mp^r - i) = \operatorname{maxex}(p, i).$$

Daraus folgt unmittelbar $\operatorname{maxex}(p, \prod_{i=1}^{p^{s-1}} n-i) = \operatorname{maxex}(p, \prod_{i=1}^{p^{s-1}} i)$, also wird $\binom{n}{p}$ nicht von p^{r-s+1} geteilt. □

5.71 Satz (erster Sylowsatz): *Ist G eine endliche Gruppe und p ein Primteiler von $n := |G|$, so gibt es für jedes $1 \leq s \leq \operatorname{maxex}(p, n)$ eine Untergruppe der Ordnung p^s.*

Beweis: Sei Ξ die Menge der Teilmengen von G, die genau p^s Elemente haben. Elementare Kombinatorik zeigt $|\Xi| = \binom{n}{p^s}$. Durch $g(A) := gA$ für $g \in G$ und $A \in \Xi$ wird eine Wirkung von G auf Ξ definiert. Damit zerfällt Ξ in paarweise disjunkte Bahnen. Sei $\mathcal{A} \subset \Xi$, so daß jede Bahn genau ein Element aus $\mathcal{A}$ enthält. Dann gilt:

$$\begin{aligned}\binom{n}{p^s} = |\Xi| &= \sum_{A \in \mathcal{A}} |a^G| \\ &= \sum_{A \in \mathcal{A}} \frac{|G|}{|G_A|} && \text{Satz 5.61} \\ &= \sum_{A \in \mathcal{A}} (G : G_A) && \text{Satz 5.25}\end{aligned}$$

Wegen Lemma 5.70 wird $\binom{n}{p^s}$ nicht von p^{r-s+1} geteilt. Also gibt es mindestens ein $A \in \mathcal{A} \subset \Xi$, so daß auch $(G : G_A)$ nicht von p^{r-s+1} geteilt wird. Also

$$\operatorname{maxex}(p, (G : G_A)) \leq r - s.$$

Aus

$$\begin{aligned} r &= \operatorname{maxex}(p, |G|) = \operatorname{maxex}(p, |G_A| \cdot (G : G_A)) \\ &= \operatorname{maxex}(p, |G_A|) + \operatorname{maxex}(p, (G : G_A)), \end{aligned}$$

folgt damit $\operatorname{maxex}(p, |G_A|) \geq r - (r - s) = s$. Also $|G_A| \geq p^s$.

Nach Konstruktion ist A eine Teilmenge von G mit p^s Elementen. So, wie die Gruppenwirkung definiert ist, gilt $G_A a \subset A$ für alle $a \in A$. Das heißt, für $a \in A$ gilt

$$|G_A| = |G_A a| \leq |A| = p^s.$$

Zusammen mit dem oben gezeigten gilt also $|G_A| = p^s$. Damit ist $|G_A|$ eine Untergruppe der gewünschten Ordnung. □

Von besonderem Interesse sind Untergruppen mit maximaler Primzahlpotenz.

5.72 Definition: Sei G eine endliche Gruppe. Sei p eine Primzahl, die $|G|$ teilt und sei p^r die maximale p-Potenz, die $|G|$ teilt.

Eine Untergruppe H von G mit $|H| = p^r$ heißt *p-Sylowuntergruppe.*

5.73 Beispiel: Die Gruppe $G = S_3$ hat Ordnung 6. Die Primteiler von 6 sind 2 und 3. Die Untergruppen Σ_i, $i \in \{1, 2, 3\}$, sind die 2-Sylowuntergruppen, die Untergruppe Δ ist die 3-Sylowuntergruppe. Dabei wird die Notation von Beispiel 5.6 verwendet.

Aus Satz 5.71 folgt unmittelbar folgendes Resultat über die Existenz von Sylowuntergruppen.

5.74 Korollar: *Ist G eine endliche Gruppe und p ein Primteiler von $|G|$, so gibt es eine p-Sylowuntergruppe in G.*

Die nächsten beiden Resultate werden der Vollständigkeit halber aufgeführt aber nicht bewiesen.

5.75 Satz (zweiter Sylowsatz): *Je zwei p-Sylowuntergruppen P_1, P_2 einer Gruppe G sind konjugiert, das heißt, es gibt eine $g \in G$ mit $P_2 = gP_1g^{-1}$.*

5.76 Satz (dritter Sylowsatz): *Die Anzahl der verschiedenen p-Sylowuntergruppen einer Gruppe G ist kongruent 1 modulo p.*

Index