Algebraische Grundstrukturen

Robert Wisbauer

http://math.uni-duesseldorf.de/ wisbauer/

SS 2005

Inhaltsverzeichnis

Vorbetrachtung

Aufgabe und Ziel dieses Kurses ist es, eine Einführung in die mathematische Denk- und Arbeitsweise zu geben.

Dabei soll der Aufbau einer mathematischen Theorie auch exemplarisch geübt werden. Das dabei zu errichtende Begriffsgebäude, nämlich die lineare Algebra, wird sich als äußerst nützlich in vielen Teilen der Mathematik und deren Anwendungen erweisen. Deshalb wird das Fundament in der später nötigen Allgemeinheit gelegt.

Diese Zielsetzung ist nicht ganz problemlos. Eine (zu) große Allgemeinheit und Abstraktheit macht Anfängern erfahrungsgemäß Schwierigkeiten. Andererseits hat die übermäßige Fixierung auf ein Beispiel auch ihre Tücken. Die Besonderheiten des speziellen Falles können den Blick von der Allgemeingültigkeit eines Konzepts ablenken.

Im folgenden wird dem dadurch Rechnung getragen, daß die Grundbegriffe abstrakt formuliert und dann an mehreren Beispielen veranschaulicht werden.

Um eine gewisse Vorstellung von dem zu geben, was später gemacht wird, betrachten wir einige algebraische Strukturen, die allen gut bekannt sind. Dies gibt uns Gelegenheit, gleich einige Notationen festzulegen:

$\mathbb{N}$	die natürlichen Zahlen $\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	die ganzen Zahlen $\{0, \pm 1, \pm 2, \ldots\}$
$\mathbb{Q}$	die rationalen Zahlen $\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
$\mathbb{R}$	die reellen Zahlen
$\mathbb{C}$	die komplexen Zahlen

In $\mathbb{N}$ haben wir zum Beispiel die Verknüpfungen $+$ und $\cdot$, das sind Abbildungen

$$\begin{aligned} + &: \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a + b\,, \\ \cdot &: \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a \cdot b\,, \end{aligned}$$

mit den Gesetzmäßigkeiten (für alle a, b, $c \in \mathbb{N}$):

$$\begin{aligned} (a + b) + c &= a + (b + c) \quad \text{Assoziativgesetze} \\ (a \cdot b) \cdot c &= a \cdot (b \cdot c) \\ a + b &= b + a \quad \text{Kommutativgesetze} \\ a \cdot b &= b \cdot a \end{aligned}$$

Im Zusammenwirken der beiden Verknüpfungen gilt:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \quad \text{Distributivgesetze} \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Bezüglich Multiplikation und Addition gibt es jeweils ein Element, das die anderen Elemente nicht verändert:

$$\begin{aligned} 1 \cdot a = a &\quad \text{neutrales Element (bzgl. } \cdot\text{)} \\ 0 + a = a &\quad \text{neutrales Element (bzgl. } +\text{)} \end{aligned}$$

In $\mathbb{Z}$ können wir zu jedem $a \in \mathbb{Z}$ ein Element b finden mit

$$a + b = 0 \qquad \text{inverses Element bzgl. } + \,.$$

In $\mathbb{Q}$ gibt es zu jedem Element $a \neq 0$ ein b mit

$$a \cdot b = 1 \qquad \text{inverses Element bzgl. } \cdot \,.$$

Diese Eigenschaften haben auch $\mathbb{R}$ und $\mathbb{C}$. Man beachte, daß bei den oben herausgestellten Beziehungen z.B. die Anordnung der Elemente der betrachteten Mengen keine Rolle spielt. Die Unterschiede zwischen $\mathbb{Q}$ und $\mathbb{R}$ bzw. $\mathbb{C}$ beziehen sich nicht auf die bisher erwähnten Gesetzmäßigkeiten, sondern sind anderer Art. So ist etwa in $\mathbb{R}$ die Gleichung $x^2 = a$ für $a \in \mathbb{R}$ mit $a > 0$ lösbar. In $\mathbb{C}$ ist dies sogar für beliebige $a \in \mathbb{C}$ der Fall.

Als weitere Besonderheit sei auf das Zusammenwirken von verschiedenen Bereichen hingewiesen. Wenn man zum Beispiel die Elemente aus $\mathbb{Q}$ mit Elementen aus $\mathbb{Z}$ multipliziert, so ergibt sich wieder ein Element aus $\mathbb{Q}$, d.h. wir haben eine Abbildung

$$(\mathbb{Z}, \mathbb{Q}) \to \mathbb{Q},\ (z, g) \mapsto z \cdot g,$$

mit den Eigenschaften ($z, z_i \in \mathbb{Z},\ q, q_i \in \mathbb{Q},\ i = 1, 2$)

$$\begin{array}{rcll} (z_1 + z_2)q & = & z_1 q + z_2 q & \\ z_1(z_2 q) & = & (z_1 z_2)q & (*) \\ z(q_1 + q_2) & = & zq_1 + zq_2 & \\ 1z & = & z\,. & \end{array}$$

Ähnliches läßt sich auch für die Paare $(\mathbb{Z}, \mathbb{R})$, $(\mathbb{Q}, \mathbb{R})$, $(\mathbb{Q}, \mathbb{C})$ und viele andere beobachten.

Die Algebra beschäftigt sich ganz allgemein mit Verknüpfungen auf irgendwelchen Mengen M, also Abbildungen

$$\tau : M \times M \to M, \quad (m, n) \mapsto m\tau n,$$

die gewissen Gesetzmäßigkeiten genügen. Die oben formulierten spielen dabei eine herausragende Rolle. So werden wir (M, τ) eine *Halbgruppe* nennen, wenn für τ das Assoziativgesetz gilt. Gilt zudem das Kommutativgesetz, so spricht man von einer *kommutativen Halbgruppe*. $\mathbb{N}$ ist also sowohl für $+$, als auch für $\cdot$ eine kommutative Halbgruppe.

Gibt es für $\tau : M \times M \to M$ ein neutrales Element und zu jedem $m \in M$ ein Inverses, so nennt man (M, τ) eine *Gruppe*.

Mengen M mit zwei Verknüpfungen $+$ und $\cdot$ nennt man *Ringe*, wenn $(M, +)$ eine kommutative Gruppe und $(M, \cdot)$ eine Halbgruppe mit neutralem Element ist und zudem die Distributivgesetze gelten. Somit sind $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ Ringe.

Ist in einem Ring jedes von Null veschiedene Element invertierbar, so spricht man von einem *Divisionsring* oder *Schiefkörper*. Ist zudem die Multiplikation kommutativ, so hat man einen *Körper*. $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper.

Schließlich noch ein Blick auf die Situation, in der zwei algebraische Systeme verbunden sind.

Sei $(R, +, \cdot)$ ein Ring und $(M, +)$ eine kommutative Gruppe. Gibt es eine Abbildung

$$(R, M) \to M,\ (r, m) \mapsto rm,$$

welche die Bedingungen $(*)$ erfüllt, so nennt man das Paar (R, M) einen *R-Modul*. Ist R ein Körper, so werden R-Moduln auch als *Vektorräume* (oder *lineare Räume*) bezeichnet.

Damit haben wir die wichtigsten Grundbegriffe der linearen Algebra angesprochen. Wir haben uns dabei der Schreibweisen bedient, die aus der Schule geläufig sind.

Um damit in allgemeinen Situationen arbeiten zu können, müssen wir Begriffe wie „Paar von Mengen“ oder „Abbildungen“ präziser fassen. Dies gehört zur Problemstellung der Mengenlehre und soll im ersten Kapitel geschehen.

Die algebraischen Strukturen wie Gruppen, Ringe und Körper werden im zweiten Kapitel eingeführt und ihre grundlegenden Eigenschaften herausgestellt, soweit sie für die hier vorgesehene Anwendung relevant sind.

Kapitel 1

Mengentheoretische Grundlagen

Ziel dieses Kapitels ist es, die mengentheoretischen Begriffe und Techniken bereitzustellen, die wir beim Aufbau der (Linearen) Algebra benötigen.

Auch wenn wir eine gewisse Vertrautheit im formalen Umgang mit Mengen voraussetzen, so sollen doch die Grundtatsachen der Mengenlehre festgehalten werden, die wir als gegeben ansehen wollen (Axiome). An der Entwicklung dieser Theorie zu Beginn unseres Jahrhunderts waren zum Beispiel die Mathematiker G. Cantor, E. Zermelo und A. Fraenkel maßgeblich beteiligt.

Das Überprüfen von eventuellen logischen Abhängigkeiten oder der Vollständigkeit eines solchen Axiomensystems ist ein nicht-triviales Problem der Mengenlehre, auf das wir hier nicht eingehen können.

Beim ersten Durchlesen wird vielleicht der tiefere Sinn oder die Zweckmäßigkeit der Formulierungen nicht gleich erkennbar sein. Mit zunehmender Erfahrung im Umgang mit diesen Begriffen wird jedoch das Verständnis dafür wachsen.

1 Axiome der Mengenlehre

Eine *Menge* setzt sich aus ihren Elementen zusammen. Der grundlegende Begriff der Mengenlehre ist die Element-Beziehung: Für jedes Objekt a muß sich feststellen lassen, ob es zu einer gegebenen Menge A gehört oder nicht. Es gilt also

a ist Element von A (a ist enthalten in A, $a \in A$), oder
a ist nicht Element von A ($a \notin A$).

Mit dieser Beziehung soll festgestellt werden können, ob zwei Mengen gleich sind. Dies geschieht in Form des folgenden Postulats:

1.1 Extensionalitätsaxiom
Zwei Mengen A, B sind genau dann gleich, wenn sie dieselben Elemente haben, also $A = B$ genau dann, wenn

$$x \in A \Rightarrow x \in B \quad \text{und} \quad x \in B \Rightarrow x \in A.$$

Damit sind Mengen eindeutig durch ihre Elemente bestimmt.

Der Pfeil $P \Rightarrow Q$ zwischen zwei Aussagen P, Q bedeutet dabei die logische Implikation *falls P gilt, dann gilt auch Q*; man sagt dazu auch *aus P folgt Q* oder *P impliziert Q*.

Die logische Äquivalenz von P und Q wird mit $P \Leftrightarrow Q$ bezeichnet. Die obige Aussage könnte also auch so formuliert werden:

$$A = B \text{ genau dann, wenn } [x \in A \Leftrightarrow x \in B].$$

Da wir die Zugehörigkeit zu einer Menge als entscheidbar annehmen, können wir nun festlegen:

1.2 Definition
Eine Menge B heißt *Teilmenge* einer Menge A, wenn jedes Element aus B auch Element von A ist, d.h.

$$B \subset A \text{ genau dann, wenn } x \in B \Rightarrow x \in A.$$

Man beachte, daß in dieser Notation $B \subset A$ auch für $B = A$ gilt.

Als nächste Grundforderung wird verlangt, daß man durch Eigenschaften von Elementen Teilmengen aussondern kann.

1.3 Aussonderungsaxiom
Zu jeder Menge A und jeder Eigenschaft P (die ein Element von A haben kann) gibt es eine Teilmenge B von A, die gerade aus den Elementen von A mit dieser Eigenschaft besteht:

$$B = \{x \in A \mid P(x)\} \subset A.$$

Bislang haben wir zwar von Eigenschaften von Mengen gesprochen, doch wissen wir noch nicht, ob es überhaupt Mengen gibt. Dies wollen wir natürlich haben und fordern daher als Axiom, daß es (mindestens) eine Menge gibt.

1.4 Existenz der leeren Menge
Es gibt eine Menge, die keine Elemente enthält.
Man nennt diese die leere Menge *und bezeichnet sie mit $\emptyset$.*

Falls es überhaupt eine Menge A gibt, so folgt aus dem Aussonderungsaxiom die Existenz der leeren Menge als

$$\emptyset = \{x \in A \mid x \neq x\}.$$

Nach Defintion ist $\emptyset$ Teilmenge jeder Menge A, also $\emptyset \subset A$. So gilt auch $\emptyset \subset \emptyset$, aber $\emptyset \notin \emptyset$.

Eine strengeres Fundament für die Mengenlehre war notwendig geworden, als man um die Jahrhundertwende erkannte, daß man mit den bis dahin als zulässig angesehenen Bildungen zu widersprüchlichen Ergebnissen gelangen konnte. So war damals die Annahme zulässig, daß es eine Menge gibt, die alle anderen Mengen enthält (*Allmenge*). Durch Eigenschaften von Elementen sollten dann auch Teilmengen davon festgelegt sein. Der britische Philosoph und Mathematiker B. Russell machte (im Jahre 1902) darauf aufmerksam, daß die (erlaubte) Bildung der Menge A aller Mengen, die nicht Element von sich selbst sind, also

$$A := \{x \mid x \notin x\},$$

nicht sinnvoll ist (*Russellsche Paradoxie*). Man sieht leicht, daß weder die Aussage $A \in A$ noch $A \notin A$ gelten kann.

Es ist eine Konsequenz des Aussonderungsaxioms, daß die Bildung einer Allmenge in unserem Rahmen nicht zulässig ist:

1.5 Satz
Es gibt keine Menge von Mengen, die jede Menge als Element enthält.

Beweis: Es ist zu zeigen, daß es zu jeder Menge A von Mengen eine Menge B gibt, die nicht Element von A ist. Dazu betrachten wir

$$B = \{x \mid x \in A, x \notin x\}.$$

Angenommen $B \in A$. Es gilt $B \in B$ oder $B \notin B$.
- Aus $B \in B$ folgt $B \notin B$, nach Definition von B.
- Aus $B \notin B$ folgt $B \in B$, ebenfalls nach Definition von B.
Dies sind Widersprüche, und somit muß $B \notin A$ gelten. □

Das nächste Axiom fordert, daß man aus *vorgegebenen* Mengen eine Menge bilden kann, die jede dieser Mengen als Teilmenge enthält. Aus sprachlichen Gründen nennen wir eine *Menge von Mengen* auch ein *Mengensystem*.

1.6 Vereinigungsaxiom
Zu jedem Mengensystem $\mathcal{M}$ gibt es eine Menge, welche genau alle Elemente enthält, die zu mindestens einer Menge des gegebenen Systems gehören:

$$\bigcup_{A \in \mathcal{M}} = \{x \mid \textit{es gibt ein } A \in \mathcal{M} \textit{ mit } x \in A\}.$$

Speziell ergibt dies für zwei Mengen A und B die Vereinigung

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}.$$

Damit kann man zu zwei Elementen x, y die *Paarmenge* bilden:

$$\{x, y\} = \{x\} \cup \{y\}$$

Aus der Kommutativität von $\cup$ (d.h. $A \cup B = B \cup A$) folgt, daß

$$\{x, y\} = \{y, x\} \qquad \text{(ungeordnetes Paar)}.$$

Will man die Reihenfolge von zwei Elementen berücksichtigen, so kann man dies mit der von K. Kuratowski vorgeschlagenen

1.7 Definition
Als *geordnetes Paar* von Elementen $x, y \in A$ bezeichnet man

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Für die Menge aller solcher Paare schreibt man

$$A \times A = \{(a, b) \mid a, b \in A\}.$$

Dabei kommt es wirklich auf die Reihenfolge der Elemente an:

1.8 Satz
Seien A eine Menge und $x, y, u, v \in A$. Dann gilt $(x, y) = (u, v)$ genau dann, wenn $x = u$ und $y = v$.

Beweis: $\Leftarrow$ ist klar.
$\Rightarrow$: Nehmen wir an, daß $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. Dann gilt

$$\{x\} \in \{\{u\}, \{u, v\}\}, \quad \{x, y\} \in \{\{u\}, \{u, v\}\},$$

also $\{x\} = \{u\}$ oder $\{x\} = \{u, v\}$ und $\{x, y\} = \{u\}$ oder $\{x, y\} = \{u, v\}$.

Angenommen $\{x\} = \{u, v\}$. Dann gilt $x = u = v$ und damit auch $x = y$. Damit ist dann auch die Behauptung des Satzes gezeigt.

Angenommen $\{x\} = \{u\}$, also $x = u$.
$\{x, y\} = \{u\}$ ergibt wieder $x = u = y = v$, also obigen Fall.
$\{x, y\} = \{u\}$ hat $y = v$ zur Folge. Also ist die Behauptung des Satzes ebenfalls erfüllt. □

Obige Bildung kann auch auf die Vereinigung von zwei Mengen angewendet werden. Dies ermöglicht die Formulierung eines Begriffs, der sich als sehr nützlich erweisen wird:

1.9 Definition
Als *geordnetes Paar* von Mengen A, B bezeichnet man

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Als weitere Folgerung aus dem Vereinigungsaxiom ergibt sich mit Hilfe des Aussonderungsaxioms die Existenz des *Durchschnitts* von Mengen:

1.10 Satz
Zu jedem Mengensystem $\mathcal{M}$ gibt es genau eine Menge, welche genau diejenigen Elemente enthält, die in jeder Menge aus $\mathcal{M}$ enthalten sind:

$$\bigcap_{M \in \mathcal{M}} M := \{x \in \bigcup_{M \in \mathcal{M}} M \mid x \in M \text{ für alle } M \in \mathcal{M}\}.$$

Man bezeichnet diese Menge als den Durchschnitt *der Mengen aus $\mathcal{M}$.*
Speziell für zwei Mengen A und B bedeutet dies

$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}.$$

Wir wollen einige Eigenschaften von Durchschnitt und Vereinigung zusammenstellen, die sich unmittelbar aus den Definitionen ergeben:

Eigenschaften
A, B und C seien Teilmengen einer Menge I. Dann gilt:

(1) $A \cap A = A$, $A \cup A = A$ (Idempotenz);

(2) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (Kommutativität);

(3) $A \cap (B \cap C) = (A \cap B) \cap C$,
$A \cup (B \cup C) = (A \cup B) \cup C$ (Assoziativität);

(4) $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$ (Absorption);

(5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Distributivität);

(6) $A \cap B = A \Leftrightarrow A \subset B \Leftrightarrow A \cup B = B$ (Konsistenz).

Eine weitere mengentheoretische Bildung, die durch das Aussonderungsaxiom ermöglicht wird, ist die *Differenzmenge*:

1.11 Definition
Sind A und B Mengen, so heißt

$$A \setminus B = \{x \in A \mid x \notin B\}$$

die *Differenzmenge* zwischen A und B.
Gilt $B \subset A$, so nennt man $A \setminus B$ das *Komplement* von B in A.

Als Zusammenhang zwischen $\cap$, $\cup$ und $\setminus$ läßt sich etwa für Mengen A, B, C als leichte Übung zeigen:

$$\begin{aligned} A \setminus (A \setminus B) &= A \cap B \\ A \cap (B \setminus C) &= (A \cap B) \setminus (A \cap C) \\ A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C). \end{aligned}$$

Im nächsten Axiom wird verlangt, daß die Gesamtheit der Untermengen einer Menge wieder eine Menge (ein Mengensystem) bildet:

1.12 Potenzmengenaxiom
Zu jeder Menge A gibt es eine Menge, deren Elemente die Teilmengen von A sind. Man nennt sie die Potenzmenge von A, also

$$\mathcal{P}(A) = \{U \mid U \subset A\}.$$

Formale Folgerungen aus dieser Festlegung sind für Mengen A, B:

(i) $B \subset A \Leftrightarrow B \in \mathcal{P}(A)$

(ii) $B \subset A \Leftrightarrow \mathcal{P}(B) \subset \mathcal{P}(A)$

(iii) $\emptyset \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$.

Wir haben zwar schon die Existenz von Mengen gefordert, wissen aber noch nicht, ob es Mengen mit unendlich vielen Elementen gibt. Dies müssen wir durch weitere Forderungen sicherstellen.

1.13 Definition
Als *Nachfolger* einer Menge A bezeichnen wir die Menge

$$A^+ = A \cup \{A\}.$$

Eine Menge von Mengen A heißt *induktiv*, wenn $\emptyset \in A$ und zu jedem Element aus A auch sein Nachfolger zu A gehört.

1.14 Unendlichkeitsaxiom
Es gibt eine induktive Menge.

Mit den bisher festgelegten Axiomen haben wir die Möglichkeit, ein Modell für die natürlichen Zahlen $\mathbb{N}$ anzugeben. Deren Existenz haben wir zwar ohnehin geglaubt, wenn wir aber unsere weitere Theorie nur auf vorgegebene Sachverhalte stützen wollen, so muß auch $\mathbb{N}$ seinen Platz in diesem System haben.

Man kann die Menge der natürlichen Zahlen nun als minimale induktive Menge definieren und etwa durch eine Menge von Mengen repräsentieren:

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \emptyset \cup \{\emptyset\} = \{\emptyset\} \\ 2 &= \{0,1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \\ n+1 &= n^+ . \end{aligned}$$

Basierend auf den Festlegungen

$$m + 0 = m, \quad m + n^+ = (m + n)^+$$

kann dann auch die Arithmetik von $\mathbb{N}$ gewonnen werden. Eine genauere Ausführung dazu findet man z.B. in dem Buch von Enderton zur Mengenlehre.

Da hierbei die natürlichen Zahlen als minimale induktive Menge festgelegt wurden, ergibt sich die

Induktionseigenschaft: Ist $A \subset \mathbb{N}$ eine Teilmenge mit

(i) $0 \in A$ und

(ii) $n \in A \Rightarrow n + 1 \in A$,

dann ist $A = \mathbb{N}$.

Dies sind natürlich nur Andeutungen zur Einführung der natürlichen Zahlen, um klar zu machen, in welchem Kontext man sie realisieren kann. Wir werden die allgemein vertrauten Eigenschaften von $\mathbb{N}$ ohne weitere Rechtfertigung benutzen.

Ausgehend von $\mathbb{N}$, können mit algebraischen Methoden $\mathbb{Z}$ und $\mathbb{Q}$ konstruiert werden. Um die rationalen Zahlen $\mathbb{Q}$ zu den reellen Zahlen $\mathbb{R}$ zu erweitern, benötigt man topologische Überlegungen.

Nun kommen wir zu einer Forderung, deren Gültigkeit man ohne weiteres akzeptiert, die jedoch nicht aus unseren bisherigen Axiomen gefolgert werden kann.

Ist ein System nicht-leerer Mengen gegeben, so soll es möglich sein, aus jeder Menge genau ein Element herauszugreifen, und diese herausgenommenen Elemente zu einer neuen Menge zusammenzufassen. Setzen wir voraus, daß die Mengen des gegebenen Mengensystems paarweise disjunkt sind, so läßt sich dies folgenderweise formulieren:

1.15 Auswahlaxiom
Sei $\mathcal{M}$ ein Mengensystem nicht-leerer Mengen und $A \cap B = \emptyset$ für alle A, $B \in \mathcal{M}$ mit $A \neq B$. Dann gibt es eine Menge M, so daß für jedes $A \in \mathcal{M}$ die Menge $A \cap M$ genau ein Element enthält.

Für die Bedeutung des Auswahlaxioms werden wir später mehr Verständnis gewinnen. Man kann auch *ohne* das Auswahlaxiom Mengenlehre und Mathematik betreiben, doch werden wir es heranziehen, wenn wir es brauchen (etwa zum Beweis der Existenz einer Basis in einem Vektorraum).

Mit den angeführten Axiomen und den ersten Folgerungen daraus können wir die mengentheoretischen Begriffsbildungen begründen, die wir für die Algebra benötigen. Sie sind jedoch nicht für alle Probleme der Mengenlehre und Mathematik ausreichend. Für spezielle Konstruktionen können und müssen weitere Axiome dazugenommen werden.

2 Relationen

Der Begriff einer allgemeinen *Relation* zwischen zwei Mengen A, B geht vom geordneten Paar $A \times B$ aus. Die dazu angegebenen Bildungen mögen auf den ersten Blick etwas ungewohnt erscheinen. Ihre Bedeutung wird jedoch bei der Behandlung spezieller Relationen in den nachfolgenden Abschnitten klar.

2.1 Definition
Seien A und B Mengen. Eine Teilmenge $R \subset A \times B$ nennen wir eine *Relation zwischen A und B*.

Speziell heißt eine Teilmenge $R \subset A \times A$ eine *Relation auf A*.

Man sagt $x \in A$ und $y \in B$ *stehen in Relation* R, wenn $(x, y) \in R$, und schreibt dafür xRy.

Als *Definitionsbereich* bzw. *Wertebereich* von R bezeichnen wir

$$\begin{aligned} \mathbb{D}(R) &= \{x \in A \mid \text{es gibt ein } y \in B \text{ mit } (x, y) \in R\}, \\ \mathbb{W}(R) &= \{y \in B \mid \text{es gibt ein } x \in A \text{ mit } (x, y) \in R\}. \end{aligned}$$

$\mathbb{D}(R)$ ist die Menge aller ersten Komponenten der Elemente in R, $\mathbb{W}(R)$ die Menge der zweiten Komponenten.

Nach diesen Definitionen gilt $R \subset \mathbb{D}(R) \times \mathbb{W}(R)$, d.h. R ist auch eine Relation zwischen $\mathbb{D}(R)$ und $\mathbb{W}(R)$. Außerdem ist R auch eine Relation auf $\mathbb{D}(R) \cup \mathbb{W}(R)$, denn

$$R \subset \mathbb{D}(R) \times \mathbb{W}(R) \subset (\mathbb{D}(R) \cup \mathbb{W}(R)) \times (\mathbb{D}(R) \cup \mathbb{W}(R)).$$

Man beachte, daß im allgemeinen nicht $R = \mathbb{D}(R) \times \mathbb{W}(R)$ gelten wird.

Zu zwei Relationen R, S zwischen A und B sind offensichtlich auch $R \cap S$ und $R \cup S$ Relationen zwischen A und B.

2.2 Beispiele. A und B seien Mengen.

(i) Die *leere Relation*: $R = \emptyset \subset A \times B$
Es gibt kein Paar (x, y), das diese Relation erfüllt.
$\mathbb{D}(R) = \mathbb{W}(R) = \emptyset$.

(ii) Die *Allrelation*: $R = A \times B \subset A \times B$
Alle $(x, y) \in A \times B$ erfüllen diese Relation.
$\mathbb{D}(R) = A$, $\mathbb{W}(R) = B$, $R = \mathbb{D}(R) \times \mathbb{W}(R) = A \times B$.

(iii) Die *Gleichheitsrelation*: $R = \Delta_A = \{(x, x) \mid x \in A\} \subset A \times A$
$(x, y) \in R$ genau dann, wenn $x = y$.
$\mathbb{D}(R) = \mathbb{W}(R) = A$.

(iv) Eine bekannte Relation auf $\mathbb{N}$ ist die $\leq$-Beziehung, gegeben durch

$$R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y - x \in \mathbb{N}\}.$$

$\mathbb{D}(R) = \mathbb{W}(R) = \mathbb{N}$.

(v) Die Relation auf $\mathbb{N}$ *x ist Nachbar von y*, d.h. x und y unterscheiden sich um 1, ist bestimmt durch

$$R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x - y = 1 \text{ oder } y - x = 1\}.$$

$\mathbb{D}(R) = \mathbb{W}(R) = \mathbb{N}$.

(vi) Die Relation auf $\mathbb{R}$,
$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\},$$
wird durch den Einheitskreis in der Ebene dargestellt.
$\mathbb{R} \neq \mathbb{W}(R) = \mathbb{D}(R) = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$.

(vii) Auf der Potenzmenge $\mathcal{P}(A)$ einer Menge A ist durch die Teilmengenbeziehung (Inklusion) eine Relation gegeben:
$$R = \{(U, V) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid U \subset V\}.$$
$\mathbb{D}(R) = \mathbb{W}(R) = \mathcal{P}(A)$.

Durch bloßes Vertauschen der Argumente läßt sich aus einer gegebenen Relation eine neue gewinnen:

2.3 Definition
Ist R eine Relation zwischen den Mengen A und B, so nennen wir die Relation zwischen B und A
$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}$$
die *Umkehrrelation von* R (*konverse* Relation).

Zu jeder Relation R kann R^{-1} gebildet werden, und es gilt $(R^{-1})^{-1} = R$.

Eine wichtige Bildung ist die *Verknüpfung* oder *Komposition* von zwei Relationen zwischen passenden Mengen:

2.4 Definition
A, B, C seien Mengen, R eine Relation zwischen A und B, S eine Relation zwischen B und C. Dann heißt die Relation
$$S \circ R = \{(x, z) \in A \times C \mid \text{es gibt ein } y \in B \text{ mit } (x, y) \in R \text{ und } (y, z) \in S\}$$
die *Verknüpfung* (*Komposition*) von R und S.

Damit kann man auch mehrere Relationen R, S, T zwischen geeigneten Mengen verknüpfen, und es gilt das *Assoziativgesetz*
$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Zwischen Verknüpfung und Umkehrrelation haben wir folgende Beziehung:

2.5 Hilfssatz
Seien A, B, C Mengen, R eine Relation zwischen A und B und S eine Relation zwischen B und C. Dann gilt
$$(S \circ R)^{-1} = R^{-1} \circ S^{-1} \subset C \times A$$

Beweis:
$$\begin{aligned}
(z, x) \in (S \circ R)^{-1} &\Leftrightarrow (x, z) \in S \circ R \\
&\Leftrightarrow \text{es gibt ein } y \in B \text{ mit } (x, y) \in R,\ (y, z) \in S \\
&\Leftrightarrow \text{es gibt ein } y \in B \text{ mit } (y, x) \in R^{-1},\ (z, y) \in S^{-1} \\
&\Leftrightarrow (z, x) \in R^{-1} \circ S^{-1}.
\end{aligned}$$

□

Speziell kann man jede Relation mit ihrer Umkehrrelation verknüpfen:

2.6 Hilfssatz
Sei R eine Relation zwischen den Mengen A und B. Dann gilt:

(a) *$R^{-1} \circ R$ ist eine Relation auf A mit*
   (1) $R^{-1} \circ R = \{(x,z) \in A \times A \mid$ *es gibt* $y \in B$ *mit* $(x,y), (z,y) \in R\}$
   (2) $\Delta_{\mathbb{D}(R)} \subset R^{-1} \circ R$
   (3) $(R^{-1} \circ R)^{-1} = R^{-1} \circ R$

(b) *$R \circ R^{-1}$ ist eine Relation auf B mit*
   (1) $R \circ R^{-1} = \{(x,z) \in B \times B \mid$ *es gibt* $y \in A$ *mit* $(y,x), (y,z) \in R\}$
   (2) $\Delta_{\mathbb{W}(R)} \subset R \circ R^{-1}$
   (3) $(R \circ R^{-1})^{-1} = R \circ R^{-1}$

Beweis: (a.1) Nach Definition der Komposition von R mit R^{-1} gilt

$$\begin{aligned} (x,z) \in R^{-1} \circ R \quad &\Leftrightarrow \quad \text{es gibt } y \in B \text{ mit } (x,y) \in R,\ (y,z) \in R^{-1} \\ &\Leftrightarrow \quad \text{es gibt } y \in B \text{ mit } (x,y) \in R,\ (z,y) \in R. \end{aligned}$$

(a.2) Für jedes $x \in \mathbb{D}(R)$ gibt es - nach Definition von $\mathbb{D}(R)$ - ein $y \in B$ mit $(x,y) \in R$. Damit ist $(x,x) \in R^{-1} \circ R$.

(a.3) Dies ergibt sich mit 2.5:

$$(R^{-1} \circ R)^{-1} = R^{-1} \circ (R^{-1})^{-1} = R^{-1} \circ R.$$

(b) folgt aus Teil (a). Man beachte, daß der Definitionsbereich von R gleich dem Wertebereich von R^{-1} ist: $\mathbb{D}(R) = \mathbb{W}(R^{-1})$. □

Es ist klar, daß im allgemeinen $R \circ R^{-1}$ und $R^{-1} \circ R$ verschieden sind.

2.7 Definition
Sei R eine Relation zwischen den Mengen A, B und U eine Teilmenge von A. Dann schreiben wir

$$R(U) = \{b \in B \mid \text{es gibt ein } u \in U \text{ mit } (u,b) \in R\} \subset B\,.$$

Speziell für $U = \{x\}$, $x \in A$, setzt man

$$R(x) = \{b \in B \mid (x,b) \in R\}.$$

Damit gilt $R(A) = \mathbb{W}(R)$, $R^{-1}(B) = \mathbb{D}(R)$ und

$$\begin{aligned} (x, R(x)) &= \{(x,y) \mid y \in R(x)\} \subset R \text{ für alle } x \in A, \\ R &= \bigcup \{(x, R(x)) \mid x \in A\}, \\ R^{-1}(y) &= \{x \in A \mid (x,y) \in R\} \text{ für alle } y \in B\,. \end{aligned}$$

Für zwei Relationen R, S zwischen geeigneten Mengen haben wir:

$$\begin{aligned} S(R(U)) &= S \circ R(U), \\ S(R(x)) &= S \circ R(x), \\ R^{-1} \circ R(x) &= \{z \in A \mid \text{ es gibt ein } y \in R(x) \text{ mit } (z,y) \in R\}\,. \end{aligned}$$

3 Abbildungen

In diesem und den nächsten beiden Paragraphen wollen wir spezielle Relationen betrachten. Dazu gehört auch der Begriff der „Abbildung“ zwischen zwei Mengen, den Sie wahrscheinlich nicht als Relation kennengelernt haben, sondern als *Zuordnung* oder *Zuordnungsvorschrift*.

Die Darstellung von Abbildungen als Relationen ist zwar nicht anschaulicher als die Beschreibung als „Zuordnung“, sie ist jedoch – mit der Mengenlehre als Grundlage – logisch exakt und elementar formulierbar. Zudem erlaubt uns dies, die in §2 beobachteten Gesetzmäßigkeiten für Relationen auch für Abbildungen zu benutzen.

3.1 Definition
Eine Relation F zwischen zwei Mengen A, B heißt *Abbildung* oder *Funktion*, wenn

(1) $\mathbb{D}(F) = A$;

(2) gilt für $x \in A$ und $y, z \in B$, daß $(x, y) \in F$ und $(x, z) \in F$, so ist $y = z$.

F nennt man dann *Abbildung (Funktion) von A nach B*.

Eine Abbildung wird bestimmt durch das Tripel $(A, B; F)$. Also sind zwei Abbildungen $(A, B; F)$ und $(C, D; G)$ gleich, wenn $A = C$, $B = D$ und $F = G$. Man nennt A die *Quelle* und B das *Ziel* der Abbildung F. Nach Definition gilt

$$\begin{array}{rcccl} A & = & \text{Quelle } F & = & \mathbb{D}(F), \\ B & = & \text{Ziel } F & \supset & \mathbb{W}(F). \end{array}$$

Relationen mit der Eigenschaft (2) in 3.1 heißen *eindeutige Relationen*. Solche Relationen werden durch Einschränkung auf $\mathbb{D}(F)$ zu Abbildungen.

Äquivalent zu 3.1 können wir sagen:

Eine Relation F zwischen den Mengen A und B ist eine *Abbildung*, wenn für jedes $x \in A$ die Menge $F(x)$ aus *genau einem* Element besteht.

Somit ermöglicht eine Abbildung F eine eindeutige Zuordnung

$$f : A \to B, x \mapsto F(x) \text{ für alle } x \in A.$$

Man schreibt $f(x) := F(x) = \{b \in B \mid (x, b) \in F\}$, und für $U \subset A$ setzt man

$$f(U) := F(U) = \{b \in B \mid \text{es gibt ein } u \in U \text{ mit } (u, b) \in F\}.$$

Man nennt F auch den *Graphen der Abbildung f*. Diese Bezeichnung ist von dem Spezialfall $f : \mathbb{R} \to \mathbb{R}$ abgeleitet, in dem der Graph von f gerade die Kurve in der reellen Ebene ergibt, die zu f gehört.

Ist eine Abbildung als Zuordnung $f : A \to B$ gegeben, dann wird durch

$$F = \{(x, f(x)) \mid x \in A\} \subset A \times B$$

die zugehörige Relation beschrieben.

Von den in 2.2 gegebenen Relationen ist nur die Gleichheit eine Abbildung. $\Delta_A \subset A \times A$ bestimmt die *identische Abbildung*

$$id_A : A \to A, \quad x \mapsto x \text{ für alle } x \in A.$$

Die in 2.2(vi) betrachtete Relation auf $\mathbb{R}$, $R = \{(x, y) \mid x^2 + y^2 = 1\}$, kann durch Einschränkung der Quelle auf $\mathbb{D}(R)$ und geeignete Beschränkung des Zielbereichs zur Abbildung werden:

$$\mathbb{D}(R) = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\} \to \mathbb{R}^+ = \{y \in \mathbb{R} \mid y > 0\}.$$

Sind zwei Abbildungen F und G mit geeigneten Quellen und Zielen gegeben, so kann man diese zu einer neuen Relation $G \circ F$ verknüpfen. Dies ist wieder eine Abbildung:

3.2 Hilfssatz
Seien A, B, C Mengen und $f : A \to B$, $g : B \to C$ Abbildungen, bestimmt durch $F \subset A \times B$ und $G \subset B \times C$. Dann ist auch die durch die Verknüpfung $G \circ F$ gebildete Relation eine Abbildung.
Diese bezeichnen wir mit $g \circ f : A \to C$.

Beweis: Es ist zu zeigen, daß für alle $x \in A$ die Menge $G \circ F(x) = G(F(x))$ aus genau einem Element besteht:
Da F Abbildung ist, besteht $F(x)$ aus genau einem Element von B.
Da G Abbildung ist, besteht $G(F(x))$ aus genau einem Element von C. □

Im allgemeinen braucht die Umkehrrelation F^{-1} einer Abbildung keine Abbildung zu sein. Dies kann man sich etwa an der Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, klar machen. Es gilt jedoch:

3.3 Hilfssatz. *Sei $F \subset A \times B$ eine Abbildung.*

(1) *Dann gilt für $F^{-1} \circ F \subset A \times A$:*
   (i) $\Delta_A \subset F^{-1} \circ F$
   (ii) $(F^{-1} \circ F)^{-1} = F^{-1} \circ F$
   (iii) $(F^{-1} \circ F) \circ (F^{-1} \circ F) \subset F^{-1} \circ F$.
   Es gilt $(x, z) \in F^{-1} \circ F$ genau dann, wenn $F(x) = F(z)$.

(2) $F \circ F^{-1} = \Delta_{\mathbb{W}(F)} \subset B \times B$.

Beweis: (i) und (ii) folgen sofort aus Hilfssatz 2.6.
(iii) Für $(x, z) \in (F^{-1} \circ F) \circ (F^{-1} \circ F)$ gilt: Es gibt $y \in A$ mit

$$(x, y) \in F^{-1} \circ F, \quad (y, z) \in F^{-1} \circ F,$$

d.h. es gibt ein $u \in B$ mit $(x, u) \in F$, $(y, u) \in F$ und ein $v \in B$ mit $(y, v) \in F$, $(z, v) \in F$.
Da F Abbildung ist, folgt aus $(y, u) \in F$ und $(y, v) \in F$, daß $u = v$. Dann ist $(x, u) \in F$ und $(z, u) \in F$, also $(x, z) \in F^{-1} \circ F$ □

Der Fall (2) in 3.3 beschreibt eine Situation, in der die Verknüpfung einer Relation mit einer Abbildung wieder eine Abbildung ergibt.
Daß F^{-1} keine Abbildung ist, kann als Ursache haben:

(1) $\mathbb{D}(F^{-1}) = \mathbb{W}(F) \subset B$, es muß nicht $\mathbb{W}(F) = B$ gelten.

(2) Für ein $y \in \mathbb{W}(F)$ kann $F^{-1}(y)$ mehr als nur ein Element enthalten.

Abbildungen, in denen solche „Defekte“ nicht auftreten, verdienen besonderes Interesse:

3.4 Definition
Sei $f : A \to B$ eine Abbildung.

(1) f heißt *surjektiv*, wenn $f(A) = B$,
   d.h. zu jedem $z \in B$ gibt es ein $x \in A$ mit $f(x) = z$.

(2) f heißt *injektiv* (oder *eineindeutig*), wenn für $x \neq y \in A$ auch $f(x) \neq f(y)$, d.h. aus $f(x) = f(y)$ folgt $x = y$.

(3) f heißt *bijektiv*, wenn es injektiv und surjektiv ist.

Folgerungen

(1) f ist genau dann surjektiv, wenn $\mathbb{W}(F) = B$.

(2) Eine Abbildung $f = (A, B; F)$ ist genau dann *injektiv*, wenn die Relation $F^{-1} \subset \mathbb{W}(F) \times A$ eine Abbildung ist.

(3) $f = (A, B; F)$ ist genau dann *bijektiv*, wenn die Relation $F^{-1} \subset B \times A$ eine Abbildung ist.
Dann heißt $f^{-1} = (B, A; F^{-1})$ die *Umkehrabbildung* zu f, und es gilt:

$$\begin{aligned} f^{-1} \circ f &= id_A \text{ (da } F^{-1} \circ F = \Delta_A) \\ f \circ f^{-1} &= id_B \text{ (da } F \circ F^{-1} = \Delta_B, \text{ vgl. 3.3).} \end{aligned}$$

Beweis: (1) Dies folgt unmittelbar aus den Definitionen.

(2) $\Rightarrow$ Sei f injektiv.

$$\begin{aligned} (z,x) \in F^{-1}, (z,y) \in F^{-1} &\Leftrightarrow (x,z) \in F, (y,z) \in F \\ &\Rightarrow f(x) = f(y) \\ &\Rightarrow x = y \text{ wegen } F \text{ injektiv} \\ &\Rightarrow F^{-1} \text{ ist Abbildung.} \end{aligned}$$

$\Leftarrow$ F^{-1} sei Abbildung, $f(x) = f(y) =: z$.

$$\begin{aligned} (x,z) \in F, (y,z) \in F &\Leftrightarrow (z,x) \in F^{-1}, (z,y) \in F^{-1} \\ &\Rightarrow x = y \\ &\Rightarrow f \text{ ist injektiv.} \end{aligned}$$

(3) Die Behauptung ergibt sich aus (1) und (2). □

Für die Komposition von Abbildungen haben wir die Beziehungen:

3.5 Satz
Seien $f : A \to B$, $g : B \to C$ Abbildungen. Dann gilt:

(1) *Sind f und g injektiv (surjektiv, bijektiv), so ist auch $g \circ f$ injektiv (surjektiv, bijektiv).*

(2) *Ist $g \circ f$ injektiv, so ist auch f injektiv.*
Ist $g \circ f$ surjektiv, so ist auch g surjektiv.
Ist $g \circ f$ bijektiv, so ist f injektiv und g surjektiv.

Der einfache Beweis dazu sei dem Leser zur Übung belassen. Damit können wir folgende Kennzeichnung von bijektiven Abbildungen angeben:

3.6 Korollar
Eine Abbildung $f : A \to B$ ist genau dann bijektiv, wenn es eine Abbildung $g : B \to A$ gibt mit

$$g \circ f = id_A, \quad f \circ g = id_B$$

Es gilt dann $g = f^{-1}$ (die inverse Abbildung ist somit eindeutig bestimmt).

Beweis: Nach 3.5 folgt aus $g \circ f = id_A$, daß f injektiv ist und aus $f \circ g = id_B$, daß f surjektiv ist. Damit existiert f^{-1}, und aus der ersten Gleichung folgt $f^{-1} = g \circ (f \circ f^{-1}) = g$. □

Man beachte, daß die Gültigkeit von nur einer der beiden Gleichungen, z.B. $f \circ g = id_B$, *nicht* die Bijektivität von f zur Folge hat.

Es folgt aus dem Auswahlaxiom, daß es zu *jeder* surjektiven Abbildung $f : A \to B$ eine Abbildung $g : B \to A$ gibt mit $f \circ g = id_B$. Dazu ist folgende Formulierung des Auswahlaxioms 1.15 von Nutzen:

3.7 Auswahlaxiom II
Zu jeder Relation $R \subset A \times B$ gibt es eine Abbildung $F \subset \mathbb{D}(R) \times B$ mit $F \subset R$.

Beweis: Die Relation R ordnet jedem $x \in \mathbb{D}(R)$ eine Menge $R(x) \subset B$ zu. Nach dem Auswahlaxiom 1.15 können wir aus jeder Menge $R(x)$ ein y_x herausnehmen. Die so gebildeten Paare $F = \{(x, y_x) \mid x \in \mathbb{D}(R)\}$ bilden eine Abbildung $\mathbb{D}(R) \to B$.

Nehmen wir nun an, das Auswahlaxiom II gilt. Sei $\mathcal{M}$ eine Menge von elementfremden Mengen, und setze $B := \bigcup_{A \in \mathcal{M}} A$. Betrachte die Relation

$$R := \{(A, a) \mid A \in \mathcal{M} \text{ und } a \in A\} \subset \mathcal{M} \times B\,.$$

Dann gibt es eine Abbildung $F \subset R \subset \mathcal{M} \times B$, und für die Menge $F(\mathcal{M})$ gilt $F(A) = F(\mathcal{M}) \cap A$ für jedes $A \in \mathcal{M}$. Damit sind die Bedingungen des Auswahlaxioms erfüllt. □

Aus Hilfssatz 3.3 kann man dann ableiten:

3.8 Satz
Sei $f = (A, B; F)$ eine surjektive Abbildung. Dann gibt es eine Abbildung $g = (B, A; G)$ mit $f \circ g = id_B$.

Beweis: Nach 3.3 gilt $F \circ F^{-1} = \Delta_B$. Zu der Relation F^{-1} können wir wegen 3.7 eine Abbildung $g = (B, A; G)$ finden mit $G \subset F^{-1}$.
Dafür gilt $F \circ G \subset F \circ F^{-1} = \Delta_B$. Außerdem ist $\Delta_B \subset F \circ G$, denn zu jedem $x \in B$ gibt es

$$y \in A \text{ mit } (x, y) \in G \subset F^{-1} \subset B \times A,$$

also $(y, x) \in F$, und somit ist $(x, x) \in F \circ G$. □

Wir haben bei den Folgerungen zu 3.4 gesehen, daß für eine injektive Abbildung $f = (A, B; F)$ die Umkehrrelation F^{-1} eine Abbildung von $\mathbb{W}(F)$ in A ist mit $F^{-1} \circ F = id_A$ (beachte $\mathbb{W}(F^{-1}) = A$).

Man kann die Abbildung $(\mathbb{W}(F), A; F^{-1})$ so zu einer Funktion $g = (B, A; G)$ fortsetzen (erweitern), daß die Beziehung $G \circ F = id_A$ erhalten bleibt. Damit gilt analog zu 3.8:

3.9 Satz
Sei $f = (A, B; F)$ eine injektive Abbildung. Dann gibt es eine Abbildung $g = (B, A; G)$ mit $g \circ f = id_A$.

Beweis: Wir wählen ein beliebiges (festes) $x_0 \in A$ und definieren

$$g(y) = \begin{cases} F^{-1}(y) & \text{für } y \in \mathbb{W}(F) \\ x_0 & \text{für } y \notin \mathbb{W}(F) \end{cases}$$

Die zugehörige Menge $G \subset B \times A$ ist dabei

$$G = \{(y, F^{-1}(y)) \mid y \in \mathbb{W}(F)\} \cup \{(y, x_0) \mid y \in B \setminus \mathbb{W}(F)\}$$

Man beachte, daß für $g \circ f$ der Wert von g an den Stellen $y \notin \mathbb{W}(F)$ keine Rolle spielt. Es ist leicht nachzuprüfen, daß $g(f(x)) = x$ für alle $x \in A$. □

Abbildungen $f : A \to B$, die jedem Element $x \in A$ den gleichen Wert $y \in B$ zuordnen, heißen *konstante Abbildungen*. Solche Abbildungen lassen sich zwischen zwei beliebigen nichtleeren Mengen A, B angeben. Eine Abbildung $f = (A, B; F)$ ist genau dann konstant, wenn $F = \{(x, y) \mid x \in A\}$ für ein (festes) $y \in B$.

In der nachstehenden Liste wird angegeben, wie sich Abbildungen gegenüber mengentheoretischen Bildungen wie Durchschnitt, Vereinigung und Komplement verhalten.

3.10 Abbildungen und Mengenoperationen

Seien $f : A \to B$ eine Abbildung und $U, U' \subset A$. Dann gilt:

(1) $U \subset U' \Rightarrow f(U) \subset f(U')$; $\quad f(U \cup U') = f(U) \cup f(U')$.

(2) $f(U) \setminus f(U') \subset f(U \setminus U')$; $\quad f(U \cap U') \subset f(U) \cap f(U')$.

Für jede Menge $\mathcal{U}$ von Teilmengen von A gilt:

(3) $f(\bigcup\limits_{U \in \mathcal{U}} U) = \bigcup\limits_{U \in \mathcal{U}} f(U)$; $\quad f(\bigcap\limits_{U \in \mathcal{U}} U) \subset \bigcap\limits_{U \in \mathcal{U}} f(U)$.

Für Teilmengen V, V' von B gilt:

(4) $V \subset V' \Rightarrow f^{-1}(V) \subset f^{-1}(V')$; $\quad f^{-1}(V \cup V') = f^{-1}(V) \cup f^{-1}(V')$.

(5) $f^{-1}(V) \setminus f^{-1}(V') = f^{-1}(V \setminus V')$; $\quad f^{-1}(V \cap V') = f^{-1}(V) \cap f^{-1}(V')$.

Für jede Menge $\mathcal{V}$ von Teilmengen von B gilt:

(6) $f^{-1}(\bigcup\limits_{V \in \mathcal{V}} V) = \bigcup\limits_{V \in \mathcal{V}} f^{-1}(V)$; $\quad f^{-1}(\bigcap\limits_{V \in \mathcal{V}} V) = \bigcap\limits_{V \in \mathcal{V}} f^{-1}(V)$.

Der Beweis dazu ist nicht schwierig und sei dem Leser überlassen.

Hat man mit einer Menge von Elementen oder Mengen zu arbeiten, so kann man häufig die Ausdrucksweise dadurch vereinfachen, daß man diese mit einem Index versieht (indiziert). Wählt man etwa zwei Elemente aus einer Menge B, so schreibt man $b_1, b_2 \in B$. In diesem Fall ist die Indexmenge $I = \{1, 2\}$, und die Elemente $b_1, b_2 \in B$ sind bestimmt als Bilder einer Abbildung

$$f : I \to B, \quad 1 \mapsto b_1,\ 2 \mapsto b_2.$$

Allgemeiner formulieren wir:

3.11 Familie von Elementen

Seien I und M Mengen, $f : I \to M$ eine Abbildung. Man nennt dann f auch eine *(I-indizierte) Familie von Elementen* und schreibt dafür

$$(f(i) \,|\, i \in I) \ \text{ oder } (f(i))_{i \in I}.$$

Setzt man $f(i) := b_i$, so beschreibt auch $(b_i)_{i \in I}$ die Abbildung f.

Zwei Abbildungen $f, g : I \to M$ sind genau dann gleich, wenn die Familien $(f(i))_{i \in I}$ und $(g(i))_{i \in I}$ gleich sind, d.h. wenn $f(i) = g(i)$ für alle $i \in I$.

Man achte darauf, die Familie $(f(i))_{i \in I}$ von der Menge der Bildelemente $\{f(i) \mid i \in I\} \subset B$ zu unterscheiden. Die Schreibweise $(f(i) \,|\, i \in I)$ legt die Abbildung fest, die Bildmenge dagegen nicht.

Spezialfälle

(1) $I = \{1\}$. $\quad \{1\} \to B$ wird durch ein $b \in B$ bestimmt.

(2) $I = \{1, 2\}$. $\quad \{1, 2\} \to B$ ergibt Paare $b_1, b_2 \in B$ ($b_1 = b_2$ möglich).

(3) $I = \{1, \ldots, n\}$. $\quad \{1, \ldots, n\} \to B$ nennt man *n-Tupel* $(b_1, \ldots, b_n)$.

(4) $I = \mathbb{N}$. $\quad \mathbb{N} \to B$ nennt man *Folgen*.

(5) Ist $B = \mathcal{B}$ eine Menge von Mengen, so ergibt eine Abbildung $I \to \mathcal{B}$ eine *Familie von Mengen* oder ein *indiziertes Mengensystem*.

Nach Definition der Abbildungen zwischen Mengen A und B bildet die Gesamtheit dieser Abbildungen eine Menge, die wir mit $\mathrm{Abb}(A,B)$ bezeichnen wollen ($\mathrm{Abb}(A,B) \subset \mathcal{P}(A \times B)$). Die oben betrachteten Fälle ergeben folgende Entsprechungen (mit $\widehat{=}$ bezeichnet):

(1)	$\mathrm{Abb}(\{1\}, B)$	$\widehat{=}$	B.
(2)	$\mathrm{Abb}(\{1,2\}, B)$	$\widehat{=}$	$B \times B$.
(3)	$\mathrm{Abb}(\{1,\ldots,n\}, B)$	$\widehat{=}$	Menge der n-Tupel mit Elementen aus B.
(4)	$\mathrm{Abb}(\mathbb{N}, B)$	$\widehat{=}$	Menge der Folgen mit Elementen aus B.
(5)	$\mathrm{Abb}(I, \mathcal{M})$	$\widehat{=}$	$\{(M_i)_{i\in I} \mid M_i \in \mathcal{M}\}$.

In (2) haben wir das geordnete Paar $B \times B$ als $\mathrm{Abb}(\{1,2\}, B)$ wiederentdeckt. Auch das geordnete Paar $A \times B$ läßt sich ähnlich darstellen:

$$\begin{aligned} A \times B &\;\widehat{=}\; \{f \in \mathrm{Abb}(\{1,2\}, A \cup B) \mid f(1) \in A, f(2) \in B\}, \\ A_1 \times A_2 &\;\widehat{=}\; \{f \in \mathrm{Abb}(\{1,2\}, A_1 \cup A_2) \mid f(1) \in A_1, f(2) \in A_2\}. \end{aligned}$$

Man nennt dies auch das *Produkt* der Mengen A_1, A_2. Ausgehend davon kann man schrittweise das *Produkt* von mehreren Mengen bilden:

$$A_1 \times A_2 \times A_3 \times \cdots = ((A_1 \times A_2) \times A_3) \times \cdots.$$

Man kann dies auch beschreiben durch

$$A_1 \times \cdots \times A_n = \{f \in \mathrm{Abb}(\{1,\ldots,n\}, \bigcup_{i=1}^{n} A_i) \mid f(i) \in A_i,\ i = 1,\ldots,n\}.$$

Allgemein definieren wir daher:

3.12 Definition
Sei I eine Menge, $(A_i)_{i\in I}$ eine Familie von Mengen. Dann nennt man

$$\prod\nolimits_{i\in I} A_i = \{f \in \mathrm{Abb}(I, \bigcup\nolimits_{i\in I} A_i) \mid f(i) \in A_i \text{ für jedes } i \in I\}$$

das (*kartesische*) *Produkt* der Mengen A_i. Kurzschreibweise: $\prod_I A_i$.
Die Elemente von $\prod A_i$ sind die Familien $(a_i)_{i\in I}$ mit $a_i \in A_i$.
Dabei ist $(a_i)_{i\in I} = (b_i)_{i\in I}$ genau dann, wenn $a_i = b_i$ für alle $i \in I$.

Ist $A_i = A$ für alle $i \in I$, so schreibt man $\prod_{i\in I} A_i = A^I$, d.h. es gilt

$$A^I = \prod\nolimits_{i\in I} A_i = \mathrm{Abb}(I, A).$$

Für $I = \{1,\ldots,n\}$ haben wir damit

$$A^n = A \times \ldots \times A = \mathrm{Abb}(\{1,\ldots,n\}, A).$$

In 3.12 ist nichts darüber gesagt, ob das Produkt einer beliebigen Familie von Mengen überhaupt existiert. Diese Existenz wird uns durch eine weitere Version des Auswahlaxioms gesichert.

3.13 Auswahlaxiom III
Zu jeder Familie $(A_i)_{i\in I}$ von nicht-leeren Mengen A_i existiert das kartesische Produkt $\prod_{i\in I} A_i$.

Beweis: Wählen wir gemäß dem Auswahlaxiom für jedes $i \in I$ ein $a_i \in A_i$ und definieren

$$f : I \to \bigcup_{i\in I} A_i, \quad i \mapsto a_i,$$

dann ist $f \in \prod_{i\in I} A_i$.

Gilt andererseits $\prod_{i\in I} A_i \neq \emptyset$ für nicht-leere Mengen A_i, dann gibt es $f \in \prod_{i\in I} A_i$ und $f(i) = a_i \in A_i$ für alle $i \in A$. □

Wir haben $\prod A_i$ als Abbildungen $I \to \bigcup A_i$ definiert. Durch Anwenden dieser Abbildungen auf ein Element $k \in I$ ergibt sich eine Abbildung

$$\{f \in \mathrm{Abb}(I, \bigcup_i I A_i) \mid f(i) \in A_i\} \to A_k, \quad f \mapsto f(k)\,.$$

In etwas handlicherer Notation läßt sich das so ausdrücken:

3.14 Definition
Sei $(A_i)_{i\in I}$ eine Familie von Mengen. Die zu $k \in I$ definierte Abbildung

$$\pi_k : \prod_{i\in I} A_i \to A_k, \quad (a_i)_{i\in I} \mapsto a_k,$$

nennt man die *k-te Projektion* von $\prod_I A_i$ auf A_k.

3.15 Hilfssatz
Ist $(A_i)_{i\in I}$ eine Familie von nicht-leeren Mengen, so ist für jedes $k \in I$ die Projektion $\pi_k : \prod_I A_i \to A_k$ surjektiv.

Beweis: Sei $a_k \in A_k$. Dann wählen wir beliebige $a_i \in A_i$ für $i \in I \setminus \{k\}$ (Auswahlaxiom), und wir erhalten

$$\pi_k((a_i)_{i\in I}) = a_k.$$

Also ist π_k surjektiv. □

Folgende Eigenschaft des Produkts von Mengen ist von Bedeutung:

3.16 Satz *(Universelle Eigenschaft des Produkts von Mengen)*
Zur Indexmenge I und einer Familie von Mengen $(A_i)_{i\in I}$ seien

$\prod_I A_i$ das kartesische Produkt dieser Mengen und

$(\pi_k : \prod_I A_i \to A_k)_{k\in I}$ die Familie der Projektionen.

Dann gibt es zu jeder Menge B und jeder Familie $(f_k : B \to A_k)_{k\in I}$ von Abbildungen genau eine Abbildung $f : B \to \prod_I A_i$ mit $\pi_k \circ f = f_k$,

Man sagt, für jedes $k \in I$ ist folgendes Diagramm kommutativ:

$$\begin{array}{ccc} B & \xrightarrow{f_k} & A_k \\ f \searrow & & \nearrow \pi_k \\ & \prod_I A_i & \end{array}$$

Beweis: Wir definieren $f : B \to \prod_I A_i$, $b \mapsto (f_i(b))_{i\in I}$ und erhalten

$$\pi_k \circ f(b) = \pi_k((f_i(b))_{i\in I}) = f_k(b) \text{ für jedes } b \in B.$$

Es bleibt noch die Eindeutigkeit von f zu zeigen. Angenommen, es gibt ein $g : B \to \prod_I A_i$ mit $\pi_k \circ g = f_k$, also $\pi_k \circ g(b) = f_k(b)$ für alle $b \in B$.

Angenommen $f \neq g$, d.h. es gibt ein $b \in B$ mit $f(b) \neq g(b) \in \prod_I A_i$. Dann gibt es ein $k \in I$ mit

$$\pi_k \circ f(b) \neq \pi_k \circ g(b).$$

Dies bedeutet aber $f_k(b) \neq f_k(b)$, ein Widerspruch. □

Zu einer Menge B und einer Familie $(A_i)_{i\in I}$ von Mengen kann man die Menge $\mathrm{Abb}(B, \prod_I A_i)$ und das Produkt der Mengen $\mathrm{Abb}(B, A_i)$, bezeichnet mit $\prod_I \mathrm{Abb}(B, A_i)$, bilden. Die universelle Eigenschaft des Produktes besagt gerade, daß wir diese beiden Mengen identifizieren können:

3.17 Korollar
Sei B eine Menge und $(A_i)_{i\in I}$ eine Familie von Mengen. Dann ist folgende Abbildung bijektiv:

$$\mathrm{Abb}(B, \prod\nolimits_I A_i) \to \prod\nolimits_I \mathrm{Abb}(B, A_i), \quad f \mapsto (\pi_i \circ f)_{i\in I}\,.$$

Beweis: Zunächst zeigen wir die Injektivität.

$$\begin{aligned} f \neq g \quad &\Rightarrow \quad \text{es gibt ein } b \in B \text{ mit } f(b) \neq g(b) \\ &\Rightarrow \quad \text{es gibt ein } k \in I \text{ mit } \pi_k \circ f(b) \neq \pi_k \circ g(b) \\ &\Rightarrow \quad \pi_k \circ f \neq \pi_k \circ g\,. \end{aligned}$$

Nun zur Surjektivität.

Sei $(h_i)_{i\in I} \in \prod_I \mathrm{Abb}(B, A_i)$. Dann gibt es nach 3.16 ein $f : B \to \prod_I A_i$ mit $\pi_k \circ f = h_k$ für alle $k \in I$, also $(\pi_i \circ f)_{i\in I} = (h_i)_{i\in I}$. □

4 Äquivalenzrelationen

Wir haben in §3 *Abbildungen* als Relationen mit speziellen Eigenschaften kennengelernt. Auch in diesem Paragraphen werden wir Relationen auf einer Menge mit besonderen Eigenschaften untersuchen.

4.1 Definition
Sei R eine Relation auf der Menge A, also $R \subset A \times A$.

(1) R heißt *reflexiv*, wenn $\Delta_A \subset R$, d.h. $(a,a) \in R$ für alle $a \in A$.

(2) R heißt *symmetrisch*, wenn $R = R^{-1}$, d.h. $(a,b) \in R \Rightarrow (b,a) \in R$.

(3) R heißt *transitiv*, wenn $R \circ R \subset R$,
d.h. $(x,y) \in R$ und $(y,z) \in R \Rightarrow (x,z) \in R$.

(4) R heißt *Äquivalenzrelation*, wenn R reflexiv, symmetrisch und transitiv ist.

Beispiele

(1) Die *gröbste* Äquivalenzrelation ist die Allrelation $(R = A \times B)$.

(2) Die *kleinste* oder *feinste* Äquivalenzrelation ist die Gleichheit $(R = \Delta_A)$: Dabei steht jedes Element nur mit sich selbst in Relation.

(3) Eine Äquivalenzrelation R auf $\mathbb{N}$ ist gegeben durch
$R = \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid n \text{ und } m \text{ haben die gleiche Quersumme}\}$
(in Dezimaldarstellung).

Sei R eine Relation auf A. Zu jedem Element $a \in A$ haben wir die Menge $R(a)$ gebildet, also die Menge der Elemente $b \in A$ mit $(a,b) \in R$. Falls R transitiv ist, gilt dafür $R(R(a)) = R(a)$.

Ist R eine Äquivalenzrelation, so nennt man die Elemente in $R(a)$ *äquivalent* zu a (bezüglich R). Wir halten fest:

4.2 Definition
Sei R eine Äquivalenzrelation auf A. Dann schreiben wir für $a \in A$

$$[a] := R(a) = \{b \in A \mid (a,b) \in R\}$$

und nennen dies die *Äquivalenzklasse* von a (bezüglich R).

Die Gesamtheit der Äquivalenzklassen bildet eine Menge, nämlich eine Teilmenge der Potenzmenge $\mathcal{P}(A)$ von A, die wir mit A/R bezeichnen, also

$$A/R = \{[a] \mid a \in A\} = \{R(a) \mid a \in A\}.$$

Man beachte, daß bei dieser Beschreibung für verschiedene $a, b \in A$ durchaus $[a] = [b]$ sein kann. Mit obigen Bezeichnungen gilt:

4.3 Hilfssatz
Sei R eine Äquivalenzrelation auf A. Für Elemente $a, b \in A$ sind folgende Aussagen äquivalent:

(a) $[a] = [b]$;

(b) $[a] \cap [b] \neq \emptyset$;

(c) $(a,b) \in R$.

Beweis: (a)⇒(b): $a \in [a] \cap [b] \neq \emptyset$.

(b)⇒(c): Ist $[a] \cap [b] \neq \emptyset$, dann gibt es ein $c \in A$ mit $(a, c) \in R$ und $(c, b) \in R$, also $(a, b) \in R$ (wegen Transitivität).

(c)⇒(a): Gilt $(a, b) \in R$, so ist $a \in [b]$ und $b \in [a]$, also $[a] \subset [b]$ und $[b] \subset [a]$. □

Die Bildung der Äquivalenzklassen definiert eine Abbildung von A in die Menge A/R der Äquivalenzklassen. Wie bezeichnen sie so:

4.4 Definition
Sei R eine Äquivalenzrelation auf A. Dann heißt die Abbildung

$$p_R : A \to A/R, \quad a \mapsto [a] \text{ für } a \in A,$$

die (zu R gehörende) *kanonische Abbildung (Projektion).*

Es ist klar, daß p_R surjektiv ist.

Erinnern wir uns nun an eine Äquivalenzrelation, die wir früher schon kennengelernt haben:

Ist $f = (A, B; F)$ eine Abbildung, so wird $F^{-1} \circ F$ eine Relation auf A. Wir haben in 3.3 gesehen, daß dies eine reflexive, symmetrische und transitive Relation ist. Dabei bedeutet $(a, b) \in F^{-1} \circ F$, daß es ein $c \in B$ gibt mit $(a, c) \in F$ und $(c, b) \in F^{-1}$, also $(b, c) \in F$.

Somit gilt $(a, b) \in F^{-1} \circ F$ genau dann, wenn $f(a) = f(b)$, also:

4.5 Satz
Sei $f = (A, B; F)$ eine Abbildung. Dann ist

$$R_f = F^{-1} \circ F = \{(a, b) \in A \times A \mid f(a) = f(b)\}$$

eine Äquivalenzrelation auf A.

Die dazu gehörende kanonische Projektion auf die Menge der Äquivalenzklassen bezeichnen wir mit $p_f : A \to A/R_f$.

Damit haben wir das Diagramm

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p_f}\searrow & & \\ & A/R_f & \end{array} .$$

Wir suchen nun eine Abbildung $\overline{f} : A/R_f \to B$, die dieses Diagramm kommutativ ergänzt, also mit $f = \overline{f} \circ p_f$. Falls es ein solches $\overline{f}$ gibt, muß somit $f(a) = \overline{f} \circ p_f(a) = \overline{f}([a])$ gelten. Wir schlagen daher die Zuordnung vor:

$$\overline{f} : A/R_f \to B, \quad \overline{f}([a]) = f(a).$$

Diese Festlegung erscheint zunächst von der Auswahl des Repräsentanten a aus $[a]$ abhängig. Betrachten wir also $a, b \in A$ mit $[a] = [b]$. Dann gilt nach 4.3 $(a, b) \in R_f$, was – nach Definition von R_f – gerade $f(a) = f(b)$ bedeutet. Unsere Zuordnung ist somit nicht von der Auswahl des Repräsentanten abhängig, d.h. $\overline{f}$ ist eine Abbildung.

$\overline{f}$ ist sogar injektiv. Gilt nämlich $[a] \neq [b]$, also $f(a) \neq f(b)$, so ist auch

$$\overline{f}([a]) = f(a) \neq f(b) = \overline{f}([b]).$$

Fassen wir zusammen:

4.6 Satz
Jede Abbildung $f : A \to B$ läßt sich darstellen als Komposition der

surjektiven Abbildung $p_f : A \to A/R_f$ und der

injektiven Abbildung $\overline{f} : A/R_f \to B$,

d.h. folgendes Diagramm ist kommutativ:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p_f}\searrow & & \nearrow{\scriptstyle \overline{f}} \\ & A/R_f & \end{array}$$

Als Folgerung daraus halten wir fest:

4.7 Korollar
Zu jeder Abbildung $f : A \to B$ gibt es eine bijektive Abbildung zwischen A/R_f und $\mathbb{W}(f)$ (= Bild von f).

Beweis: Nach Konstruktion gilt $\mathbb{W}(f) = \mathbb{W}(\overline{f})$.
Damit ist $\overline{f} : A/R_f \to \mathbb{W}(f)$ injektiv und surjektiv, also bijektiv. □

Wir haben sowohl Abbildungen als auch Äquivalenzrelationen als Relationen kennengelernt. Es ist leicht zu sehen, daß eine Relation, die Abbildung und Äquivalenzrelation ist, schon die Identität sein muß. Weitere Eigenschaften von Relationen werden im nächsten Abschnitt untersucht.

5 Ordnungsrelationen

Auch in diesem Paragraphen wollen wir uns mit Relationen mit besonderen Eigenschaften befassen, den *Ordnungsrelationen*. Diese sind für die Analysis von größerer Bedeutung als für die lineare Algebra. Wir wollen hier hauptsächlich jene Punkte herausarbeiten, die für uns von Interesse sein werden. Zunächst die Definition:

5.1 Definition
Sei R eine Relation auf A (d.h. $R \subset A \times A$).

(1) R heißt *antisymmetrisch*, wenn $R \cap R^{-1} \subset \Delta_A$ (vgl. 2.2(iii)), d.h. wenn für alle $a, b \in A$ gilt: $(a,b) \in R$ und $(b,a) \in R \Rightarrow a = b$.

(2) R heißt *Ordnungsrelation*, wenn R reflexiv, antisymmetrisch und transitiv ist. Man nennt dann A auch eine (durch R) *(teilweise) geordnete Menge*.

Schreibweise: $(a,b) \in R \Leftrightarrow a \leq_R b$ oder auch $a \leq b$.

Eine Ordnungsrelation R, die zugleich Äquivalenzrelation ist, kann nur die Identität sein, denn

$$\left.\begin{array}{ll} \text{symmetrisch} & R = R^{-1} \\ \text{antisymmetrisch} & R \cap R^{-1} \subset \Delta_A \\ \text{reflexiv} & \Delta_A \subset R \end{array}\right\} \Rightarrow \Delta_A = R.$$

Bekannte Beispiele von Ordnungsrelationen sind:

(1) $\leq$ auf $\mathbb{N}$, $\quad R = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y - x \in \mathbb{N} \cup \{0\}\}$.

(2) $\subset$ auf der Potenzmenge einer Menge A:

$$R = \{(U,V) \in \mathcal{P}(A) \times \mathcal{P}(B) \mid U \subset V\}.$$

Im ersten Beispiel beobachten wir als zusätzliche Eigenschaft, daß zwei Elemente $x, y \in \mathbb{N}$ immer vergleichbar sind: $x \leq y$ oder $y \leq x$. Relationen mit dieser Eigenschaft spielen eine besondere Rolle:

5.2 Definition
Eine Ordnungsrelation R auf A heißt *lineare* (oder *totale*) *Ordnung*, wenn

$$R \cup R^{-1} = A \times A,$$

d.h. für je zwei Elemente $a, b \in A$ gilt $(a,b) \in R$ oder $(b,a) \in R$.

Eine symmetrische Relation mit dieser Eigenschaft wäre die Allrelation.

Lineare Ordnungen werden auch *vollständige* oder *totale Ordnungen* genannt. Bei gewöhnlichen Ordnungsrelationen spricht man auch von *teilweisen Ordnungen* oder *Halbordnungen*.

$(\mathbb{N}, \leq)$, $(\mathbb{Q}, \leq)$ und $(\mathbb{Z}, \leq)$ sind Beispiele für lineare Ordnungen,
$(\mathcal{P}(A), \subset)$ ist eine teilweise Ordnung.

Elemente in geordneten Mengen können sich durch folgende Eigenschaften auszeichnen:

5.3 Definition
Sei $(A, \leq)$ eine geordnete Menge, $B \subset A$ eine Teilmenge.

$b \in B$ heißt *größtes Element* von B, wenn für alle $b' \in B$ stets $b' \leq b$.

$b \in B$ heißt *maximales Element* von B, wenn für alle $b' \in B$ gilt:
$b \leq b' \Rightarrow b' = b$, d.h. es gibt kein Element in B, das größer als b ist.

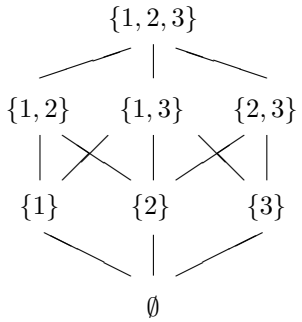
$a \in A$ heißt *obere Schranke* von B, wenn $b \leq a$ für alle $b \in B$.

$a \in A$ heißt *Supremum* oder *obere Grenze* von B in A, wenn a kleinste obere Schranke von B ist, d.h. für alle oberen Schranken a' von B gilt $a \leq a'$.

Entsprechend werden *kleinste* und *minimale Elemente*, *untere Schranke* und *Infimum* definiert.

Elemente mit diesen Eigenschaften braucht es nicht zu geben.
Jedes größte Element in B ist auch maximal. Dagegen kann es mehrere maximale Elemente in B geben, die nicht vergleichbar sind.

Wir wollen diese Begriffe an einem einfachen Beispiel erläutern, bei dem wir die Teilmengenbeziehung angeben:
A = Potenzmenge von $\{1, 2, 3\}$:



$\{1, 2, 3\}$ ist größtes Element in A, $\emptyset$ ist kleinstes Element in A.
In $B = A \setminus \{\{1, 2, 3\}, \emptyset\}$ gibt es weder größtes noch kleinstes Element. $\{1, 2\}, \{1, 3\}$ und $\{2, 3\}$ sind maximale Elemente darin, $\{1, 2, 3\}$ ist Supremum davon.
Die Teilmenge $\{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$ von A ist bezüglich $\subset$ linear geordnet, ebenso die Teilmenge $\{\{2\}, \{2, 3\}\}$. Beide Mengen besitzen ein Supremum (sogar ein größtes Element).

5.4 Definition
Eine nicht-leere, geordnete Menge $(A, \leq)$ heißt *induktiv geordnet*, wenn jede nicht-leere (bezüglich $\leq$) linear geordnete Teilmenge eine obere Schranke besitzt.

Man beachte, daß Teilmengen von induktiv geordneten Mengen nicht wieder induktiv geordnet sein müssen.

Beispiel
Für jede Menge $A \neq \emptyset$ ist die Potenzmenge $(\mathcal{P}(A), \subset)$ induktiv geordnet:
Sei $\mathcal{U} \subset \mathcal{P}(A)$, $\mathcal{U}$ linear geordnet. Dann ist

$$S = \bigcup_{U \in \mathcal{U}} U \in \mathcal{P}(A)$$

Supremum von $\mathcal{U}$: Da $U \subset S$ für alle $U \in \mathcal{U}$, ist S obere Schranke. Für jedes $T \in \mathcal{P}(A)$ mit $U \subset T$ für alle $U \in \mathcal{U}$ gilt $S = \bigcup_{U \in \mathcal{U}} U \subset T$.

Die Bedeutung der induktiv geordneten Mengen liegt darin, daß man in ihnen - mit Hilfe des Auswahlaxioms - die Existenz von maximalen Elementen zeigen kann. Dies führt zu einer vierten Variation des Auswahlaxioms.

5.5 Auswahlaxiom IV: Zornsches Lemma

Jede induktiv geordnete Menge besitzt maximale Elemente.

Der Beweis ist zwar im wesentlichen mit den uns bereits bekannten Begriffen zu führen, erfordert aber doch eine gewisse Vertiefung in die Denkweise der Mengenlehre (vgl. Enderton, Theorem 6M).

Fragen wir uns, was das Zornsche Lemma für die induktiv geordnete Potenzmenge einer Menge A bringt. Nun, für diesen Fall ergibt sich nichts neues, da wir in $\mathcal{P}(A)$ bereits ein maximales Element kennen: A selbst ist sogar größtes Element in $\mathcal{P}(A)$.

Die hauptsächlichen Anwendungen werden sich für uns auf *Teilmengen* von $\mathcal{P}(A)$ beziehen.

Nach diesen Ausführungen zur (abstrakten) Mengenlehre wollen wir uns nun den eigentlichen Objekten unseres Interesses, den algebraischen Strukturen zuwenden.

Kapitel 2

Algebraische Grundstrukturen

Bei der Addition oder Multiplikation von Zahlen wird zwei Zahlen a, b eine neue Zahl $a+b$ oder $a \cdot b$ zugeordnet. Man nennt dies eine *Verknüpfung* auf der Menge der (natürlichen, reellen) Zahlen.

Wir werden im nächsten Paragraphen zunächst Mengen mit *einer* Verknüpfung untersuchen (Gruppen, Halbgruppen). Im darauffolgenden Paragraphen wird dann das Zusammenspiel von zwei Verknüpfungen behandelt, wie wir es ebenfalls von den Zahlen her kennen (Ringe, Körper).

6 Halbgruppen und Gruppen

Zur Festlegung der algebraischen Grundbegriffe bedienen wir uns der Sprache und der Methoden der Mengenlehre.

6.1 Definition
Sei A eine nicht-leere Menge. Eine *Verknüpfung* τ auf A ist eine Abbildung von $A \times A$ in A:

$$\tau : A \times A \to A, \quad (a,b) \mapsto a \,\tau\, b.$$

Als Beispiel dazu haben wir schon $+$ und $\cdot$ auf $\mathbb{N}$ kennengelernt.

Ist τ eine Verknüpfung auf A, so ist für $c \in A$ auch $(a \,\tau\, b, c) \in A \times A$ und $(a \,\tau\, b) \,\tau\, c \in A$. Analog läßt sich auch $a \,\tau\, (b \,\tau\, c) \in A$ bilden. Für beliebiges τ muß sich dabei keineswegs das gleiche Element ergeben. Schauen wir uns ein einfaches Beispiel dazu an.

Verknüpfungen auf endlichen Mengen A können wir durch *Verknüpfungstafeln* angeben. Dabei schreibt man die Elemente von A einmal als erste Zeile und einmal als erste Spalte einer quadratischen Tafel und setzt das Element $a \,\tau\, b$ in den Schnitt der Zeile a mit der Spalte b.

Sei z. B. $A = \{a, b\}$ und $\tau : A \times A \to A$ gegeben durch die

Verknüpfungstafel

τ	a	b
a	b	b
b	a	b

$$(a \,\tau\, b) \,\tau\, a = b \,\tau\, a = a$$
$$a \,\tau\, (b \,\tau\, a) = a \,\tau\, a = b$$

Dabei führen die beiden angesprochenen Bildungen zu verschiedenen Ergebnissen. Wir werden uns hier jedoch für solche Verknüpfungen interessieren, bei denen das Ergebnis unabhängig von der Reihenfolge der Ausführung ist.

6.2 Definition
Sei H eine nicht-leere Menge.

Eine Verknüpfung $\tau : H \times H \to H$ heißt *assoziativ*, wenn

$$(a\,\tau\,b)\,\tau\,c = a\,\tau\,(b\,\tau\,c) \text{ für alle } a,\, b,\, c \in H.$$

(H, τ) nennt man dann eine *Halbgruppe*.
(H, τ) heißt *kommutative Halbgruppe*, wenn zudem $a\,\tau\,b = b\,\tau\,a$ für alle $a,\, b \in H$ gilt.
Ist H endlich, so nennt man die Zahl der Elemente von H die *Ordnung von* H.

Ist aus dem Zusammenhang klar, welche Verknüpfung gemeint ist, so schreibt man für (H, τ) nur H.

Es läßt sich durch Induktion zeigen, daß sich in einer Halbgruppe bei jedem endlichen Produkt die Klammern beliebig setzen lassen, also z.B.

$$(a_1\,\tau\,(a_2\,\tau\,a_3))\,\tau\,a_4 = a_1\,\tau\,((a_2\,\tau\,a_3)\,\tau\,a_4).$$

6.3 Beispiele von Halbgruppen

(1) $\mathbb{N}$ bildet mit $\tau = +$ und $\tau = \cdot$ je eine kommutative Halbgruppe.

(2) Für die Abbildung $\tau : A \times A \to A$, $(a, b) \mapsto a$, gilt die Assoziativität, nicht aber die Kommutativität, falls es $a \neq b$ in der Menge A gibt, denn

$$a\,\tau\,b = a \neq b = b\,\tau\,a.$$

(3) Die Potenzmenge $\mathcal{P}(A)$ einer Menge A ist eine Halbgruppe mit $\cap$ (oder $\cup$).

(4) Sei $A \neq \emptyset$ eine Menge, $\mathrm{Abb}(A) := \mathrm{Abb}(A, A)$ die Menge der Abbildungen von A in A. Dann ist $(\mathrm{Abb}(A), \circ)$ eine Halbgruppe mit

$$\mathrm{Abb}(A) \times \mathrm{Abb}(A) \to \mathrm{Abb}(A),\ (f, g) \mapsto g \circ f.$$

Sie ist nicht kommutativ, wenn A mehr als ein Element enthält:
Seien $c \neq b \in A$, $\quad f : A \to A, \quad a \mapsto b$ für alle $a \in A$,
$\qquad\qquad\qquad\quad\ g : A \to A, \quad a \mapsto c$ für alle $a \in A$.
Dann gilt $g \circ f(a) = c \neq b = f \circ g(a)$, also $g \circ f \neq f \circ g$.

(5) Ist $A \neq \emptyset$ eine Menge und (H, τ) eine Halbgruppe, dann wird $\mathrm{Abb}(A, H)$ zu einer Halbgruppe durch

$$f\,\tau'\,g : A \to H,\ a \mapsto f(a)\,\tau\,g(a) \text{ für alle } a \in A.$$

(6) Ist $(H_i, \tau_i)_{i \in I}$ eine Familie von Halbgruppen, so läßt sich auch auf dem kartesischen Produkt $\prod_I H_i$ eine Verknüpfung τ definieren, die $(\prod_I H_i, \tau)$ zu einer Halbgruppe macht:

$$(a_i)_I\,\tau\,(b_i)_I := (a_i\,\tau_i\,b_i)_I.$$

Sehen wir uns an, welche besonderen Eigenschaften Elemente einer Halbgruppe haben können:

6.4 Definition

Sei (H, τ) eine Halbgruppe.

(1) Ein Element $e \in H$ heißt

rechtsneutrales Element, wenn $a\,\tau\,e = a$ für alle $a \in H$,

linksneutrales Element, wenn $e\,\tau\,a = a$ für alle $a \in H$,

neutrales Element, wenn $a \tau e = e \tau a = a$ für alle $a \in H$.

(2) Hat H ein neutrales Element e, dann heißt ein Element $b \in H$

rechtsinvers zu $a \in H$, wenn $a \tau b = e$,

linksinvers zu $a \in H$, wenn $b \tau a = e$,

invers zu $a \in H$, wenn $a \tau b = b \tau a = e$. Man schreibt dafür $b =: a^{-1}$.

Wir wollen dazu gleich einige Beobachtungen festhalten:

(1) Eine Halbgruppe hat höchstens ein neutrales Element: Sind e und e' neutrale Elemente, dann gilt $e = e \tau e' = e'$.

(2) Zu einem $a \in H$ gibt es höchstens ein inverses Element: Sind b und b' invers zu a, dann gilt: $b = b \tau e = b \tau (a \tau b') = (b \tau a) \tau b' = e \tau b' = b'$.

(3) Ist b invers zu a und b' invers zu a', dann ist $b' \tau b$ invers zu $a \tau a'$.

Prüfen wir, ob es in den Beispielen von 6.3 solche Elemente gibt:

(i) $(\mathbb{N}, +)$: 0 ist neutrales Element; $(\mathbb{N}, \cdot)$: 1 ist neutrales Element.
Nur zu 0 bzw. 1 gibt es inverse Elemente.

(ii) $(a, b) \mapsto a$: Jedes Element ist rechtsneutral; es gibt kein linksneutrales Element, wenn A mehr als ein Element enthält.

(iii) $(\mathcal{P}(A), \cap)$: A ist neutrales Element;
$(\mathcal{P}(A), \cup)$: $\emptyset$ ist neutrales Element.

(iv) $(\mathrm{Abb}(A), \circ)$: id_A ist neutrales Element. Zu $f \in \mathrm{Abb}(A)$ gibt es ein Inverses, wenn f invertierbar ist (Umkehrabbildung).

(v) $(\mathrm{Abb}(A, H), \tau')$: Hat H ein neutrales Element e, so ist das neutrale Element von $\mathrm{Abb}(A, H)$ die konstante Abbildung $\widetilde{e} : A \to H$, $a \mapsto e$.

(vi) $(\prod_I H_i, \tau)$: Hat jedes H_i ein neutrales Element e_i, so ist $(e_i)_{i \in I}$ neutrales Element in $\prod_I H_i$.

Wie an den Beispielen zu sehen ist, braucht es in Halbgruppen weder neutrale noch inverse Elemente zu geben. Halbgruppen, in denen es diese Elemente immer gibt, sind von besonderer Bedeutung:

6.5 Definition
Eine Halbgruppe (H, τ) heißt *Gruppe*, wenn gilt:

(1) Es gibt ein neutrales Element $e \in H$;

(2) Zu jedem $a \in H$ gibt es ein Inverses.

Ist die Verknüpfung τ kommutativ, so nennt man (H, τ) eine *kommutative* oder auch *abelsche Gruppe* (in Erinnerung an den norwegischen Mathematiker N.H. Abel).

Die in 6.5 gestellten Forderungen (1) und (2) lassen sich durch die Lösbarkeit bestimmter Gleichungen ausdrücken. Es gilt:

6.6 Satz
Für eine Halbgruppe H sind folgende Eigenschaften äquivalent:

(a) *(H, τ) ist eine Gruppe;*

(b) *Zu je zwei Elementen $a, b \in H$ gibt es genau ein $x \in H$ mit $a \tau x = b$ und genau ein $y \in H$ mit $y \tau a = b$.*

Beweis: $(a) \Rightarrow (b)$ Sei (H, τ) eine Gruppe, $a, b \in H$. Für $x = a^{-1} \tau b$ gilt

$$a \tau x = a \tau (a^{-1} \tau b) = (a \tau a^{-1}) \tau b = b.$$

Zur Eindeutigkeit von x: Gelte $a \tau x = b = a \tau x'$ für $x, x' \in H$. Dann folgt $x = a^{-1} \tau (a \tau x) = a^{-1} \tau b$ und $x' = a^{-1} \tau (a \tau x') = a^{-1} \tau b$.

Analog erhält man die Lösung von $y \tau a = b$.

$(b) \Rightarrow (a)$ Es gelte (b). Dann hat $a \tau x = a$ eine Lösung $e \in H$, also $a \tau e = a$. Wir zeigen, daß dieses e neutrales Element ist.

Sei $b \in H$ beliebig und $c \in H$ mit $c \tau a = b$. Dann gilt

$$b \tau e = (c \tau a) \tau e = c \tau (a \tau e) = c \tau a = b,$$

also ist e rechts neutral. Betrachte nun ein $b' \in H$ mit $e \tau b' = b$. Dann gilt

$$e \tau b = e \tau (e \tau b') = (e \tau e) \tau b' = e \tau b' = b.$$

Somit ist e auch links neutral.

Es bleibt noch, ein Inverses zu $a \in H$ zu finden. Nach Voraussetzung gibt es zu $a, e \in H$ Elemente $b, b' \in H$ mit $a \tau b = e$, $b' \tau a = e$. Daraus ergibt sich

$$b' = b' \tau e = b' \tau (a \tau b) = (b' \tau a) \tau b = e \tau b = b.$$

Also ist b invers zu a. □

Als Beispiel für Gruppen kennen wir etwa die ganzen Zahlen $(\mathbb{Z}, +)$ und die rationalen Zahlen $(\mathbb{Q}, +)$ bzw. $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Die in 6.3 angegebenen Beispiele für Halbgruppen sind allesamt keine Gruppen. Einige von ihnen lassen sich in Gruppen einbetten, etwa $(\mathbb{N}, +)$ und $(\mathbb{N} \setminus \{0\}, \cdot)$. Die meisten davon enthalten (wenn auch manchmal triviale) Gruppen. Solche Unterstrukturen sind von großem Interesse:

6.7 Definition
Sei (H, τ) eine Halbgruppe.

Eine Teilmenge $U \subset H$ heißt *Unterhalbgruppe*, wenn für $a, b \in U$ auch $a \tau b \in U$ gilt. Man sagt dazu, *U ist abgeschlossen gegenüber τ*. (U, τ) ist Halbgruppe.

Besitzt (H, τ) ein neutrales Element, dann heißt $U \subset H$ *Untergruppe*, wenn es Unterhalbgruppe ist und zu jedem $a \in U$ auch $a^{-1} \in U$ gilt.

(U, τ) ist dann eine Gruppe mit neutralem Element $e \in U$.

In jeder Halbgruppe (H, τ) mit neutralem Element e ist die Menge $H^\times$ der invertierbaren Elemente in H eine Untergruppe, denn

$e \in H^\times$, $a \in H^\times$ (also invertierbar) $\Rightarrow a^{-1} \in H^\times$ und

$a, b \in H^\times \Rightarrow a \tau b \in H^\times$.

Sehen wir uns wieder die in 6.3 gegebenen Beispiele daraufhin an:

(i) In $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ ist $2\mathbb{N}$ (= gerade Zahlen) eine Unterhalbgruppe.
$\{1\}$ ist Untergruppe von $(\mathbb{N}, \cdot)$.

(ii) $(a, b) \mapsto a$: $\{a\} \subset A$ ist wohl Gruppe, aber nicht Untergruppe, da A kein neutrales Element hat.

(iii) $\{A\}$ ist Untergruppe von $(\mathcal{P}(A), \cap)$, $\{\emptyset\}$ Untergruppe von $(\mathcal{P}(A), \cup)$.
$\{\emptyset, A\}$ ist Unterhalbgruppe von $(\mathcal{P}(A), \cap)$ und $(\mathcal{P}(A), \cup)$, aber in keinem Fall Untergruppe ($\emptyset \cap ? = A$, $A \cup ? = \emptyset$).

(iv) $(\mathrm{Abb}(A), \circ)$: Die surjektiven, die injektiven sowie die konstanten Abbildungen bilden jeweils Unterhalbgruppen. Die bijektiven Abbildungen sind eine Untergruppe.

(v) $(\mathrm{Abb}(A, H), \tau')$: Ist U Untergruppe von H, dann ist $\mathrm{Abb}(A, U)$ Untergruppe von $\mathrm{Abb}(A, H)$.

Als Abbildungen zwischen Halbgruppen interessieren uns vor allem solche, die mit den Verknüpfungen verträglich sind:

6.8 Definition
Seien (H_1, τ_1) und (H_2, τ_2) Halbgruppen. Eine Abbildung $f : H_1 \to H_2$ heißt (Halbgruppen-)*Homomorphismus*, wenn für alle $a, b \in H_1$ gilt

$$f(a \,\tau_1\, b) = f(a) \,\tau_2\, f(b)$$

Man nennt dann $f : H_1 \to H_2$ einen

Monomorphismus,	wenn f injektiv ist,
Epimorphismus,	wenn f surjektiv ist,
Isomorphismus,	wenn f bijektiv ist,
Endomorphismus,	wenn $H_1 = H_2$,
Automorphismus,	wenn $H_1 = H_2$ und f Isomorphismus ist.

Sind H_1 und H_2 Gruppen, so nennt man einen Halbgruppen-Homomorphismus $f : H_1 \to H_2$ auch *Gruppen-Homomorphismus*.

Die Mengen der Homo-, Endo- bzw. Automorphismen bezeichnet man mit $\mathrm{Hom}(H_1, H_2)$, $\mathrm{End}(H_1)$ bzw. $\mathrm{Aut}(H_1)$. $\mathrm{End}(H_1)$ und $\mathrm{Aut}(H_1)$ sind offensichtlich Unterhalbgruppen von $\mathrm{Abb}(H_1, H_1)$.

Schauen wir uns einige Beispiele zu diesen Begriffen an.

6.9 Beispiele von Homomorphismen

(1) Sei $(G, \cdot)$ eine Gruppe. Zu $a \in G$ definieren wir

$$I_a : G \to G, \quad x \mapsto a \cdot x \cdot a^{-1}.$$

I_a ist ein Homomorphismus, denn

$$\begin{aligned} I_a(x \cdot y) &= a \cdot (x \cdot y) \cdot a^{-1} \\ &= a \cdot x \cdot (a^{-1} \cdot a) \cdot y \cdot a^{-1} \quad = \quad I_a(x) \cdot I_a(y). \end{aligned}$$

I_a ist injektiv, denn aus $a \cdot x \cdot a^{-1} = a \cdot y \cdot a^{-1}$ folgt $x = y$.
I_a ist surjektiv, denn für $b \in G$ gilt

$$I_a(a^{-1} \cdot b \cdot a) = a \cdot a^{-1} \cdot b \cdot a \cdot a^{-1} = b.$$

Man nennt I_a einen *inneren Automorphismus*.

(2) Seien H_1, H_2 Halbgruppen und e_2 neutrales Element in H_2. Dann ist

$$H_1 \to H_2, \quad x \mapsto e_2 \text{ für alle } x \in H_1,$$

ein (trivialer) Homomorphismus.

(3) Die *Exponentialfunktion*

$$\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot\,), \quad x \mapsto e^x,$$

ist ein Homomorphismus, da $e^{x+y} = e^x e^y$.

Auch der *Logarithmus*

$$\log : (\mathbb{R}_{>0}, \cdot\,) \to (\mathbb{R}, +), \quad x \mapsto \log(x),$$

ist ein Homomorphismus, denn $\log(xy) = \log(x) + \log(y)$.

(4) Sei $(H, \cdot\,)$ eine Halbgruppe. Dann ist die Linksmultiplikation mit einem $a \in H$ eine Abbildung von H in sich,

$$L_a : H \to H, \quad x \mapsto a \cdot x.$$

Damit erhalten wir einen Homomorphismus

$$\lambda : (H, \cdot\,) \to (\mathrm{Abb}(H, H), \circ), \quad a \mapsto L_a.$$

Nach Definition gilt nämlich

$$L_{a \cdot b}(x) = (a \cdot b) \cdot x = a \cdot (b \cdot x) = L_a(L_b(x)) = L_a \circ L_b(x),$$

also $a \cdot b \mapsto L_a \circ L_b$. Ist a invertierbar, dann ist L_a bijektiv.

Ist H eine Gruppe, so ist λ monomorph, und H ist isomorph zu einer Untergruppe der bijektiven Abbildungen von H in sich.

Ähnliche Bildungen kann man natürlich auch mit Rechtsmultiplikationen durchführen. Man beachte, daß sich dann bei λ die Reihenfolge der Multiplikation im Bild umdreht.

Halten wir weitere Eigenschaften von Homomorphismen fest:

6.10 Satz
Sei $f : (H_1, \tau_1) \to (H_2, \tau_2)$ ein Homomorphismus von Halbgruppen.

(1) *Ist U_1 eine Unterhalbgruppe von H_1, dann ist $f(U_1)$ eine Unterhalbgruppe von H_2.*

(2) *Ist U_2 eine Unterhalbgruppe von H_2, dann ist $f^{-1}(U_2) = \emptyset$ oder eine Unterhalbgruppe von H_1.*

Beweis: (1) Sei $a_2, b_2 \in f(U_1) \subset H_2$. Dann gibt es $a_1, b_1 \in H_1$ mit $f(a_1) = a_2$, $f(b_1) = b_2$, und es gilt

$$a_2 \,\tau_2\, b_2 = f(a_1) \,\tau_2\, f(b_1) = f(a_1 \,\tau_1\, b_1) \in f(U_1).$$

(2) Seien $f^{-1}(U_2) \neq \emptyset$ und $a_1, b_1 \in f^{-1}(U_2)$, d.h. $f(a_1), f(b_1) \in U_2$, und

$$f(a_1 \,\tau_1\, b_1) = f(a_1) \,\tau_2\, f(b_1) \in U_2,$$

also $a_1 \,\tau_1\, b_1 \in f^{-1}(U_2)$. □

Wenn auch die Kennzeichnung von Homomorphismen zwischen Halbgruppen die gleiche ist wie zwischen Gruppen, so erzwingt die Gruppenstruktur doch zusätzliche Eigenschaften der Homomorphismen:

6.11 Satz
Seien $f : (G_1, \tau_1) \to (G_2, \tau_2)$ ein Gruppen-Homomorphismus, $e_1 \in G_1$ und $e_2 \in G_2$ die neutralen Elemente. Dann gilt:

(1) $f(e_1) = e_2$ *und* $f(a^{-1}) = (f(a))^{-1}$ *für alle* $a \in G_1$.

(2) *Ist* U_1 *Untergruppe von* G_1*, dann ist* $f(U_1)$ *Untergruppe von* G_2.

(3) *Ist* U_2 *Untergruppe von* G_2*, dann ist* $f^{-1}(U_2)$ *Untergruppe von* G_1.

Beweis: (1) Aus $e_1 \,\tau_1\, e_1 = e_1$ folgt $f(e_1) = f(e_1) \,\tau_2\, f(e_1)$ und

$$e_2 = f(e_1) \,\tau_2\, (f(e_1))^{-1} = f(e_1).$$

(2) und (3) folgen damit aus Satz 6.10. □

Eine wichtige Eigenschaft von Homomorphismen ist die Tatsache, daß ihre Komposition (als Abbildungen) wieder strukturverträglich ist:

6.12 Satz
Seien $f : H_1 \to H_2$, $g : H_2 \to H_3$ *Homomorphismen von Halbgruppen.*

(1) *Dann ist auch* $g \circ f : H_1 \to H_3$ *ein Homomorphismus.*

(2) *Ist* f *ein Isomorphismus, dann ist auch die Umkehrabbildung* $f^{-1} : H_2 \to H_1$ *ein Isomorphismus.*

Beweis: (1) ist leicht nachzuprüfen.

(2) Wir haben $f(f^{-1}(x \,\tau_2\, y)) = x \,\tau_2\, y = f(f^{-1}(x) \,\tau_1\, f^{-1}(y))$. Wegen der Injektivität von f gilt damit auch

$$f^{-1}(x \,\tau_2\, y) = (f^{-1}(x) \,\tau_1\, f^{-1}(y)).$$

□

Dies impliziert insbesondere, daß die Komposition von Endomorphismen wieder Endomorphismen ergibt, also

6.13 Korollar
Sei H *eine Halbgruppe. Dann ist* $\mathrm{End}(H)$ *eine Unterhalbgruppe von* $\mathrm{Abb}(H, H)$*, und die Automorphismen* $\mathrm{Aut}(H)$ *bilden die Gruppe der invertierbaren Elemente in* $\mathrm{End}(H)$.

Ist $f : G_1 \to G_2$ ein Gruppen-Homomorphismus, so ist das Urbild **jeder** Untergruppe von G_2 eine Untergruppe von G_1. Speziell ist also auch das Urbild von $\{e_2\} \subset G_2$ eine Untergruppe in G_1. Diese ist für den Homomorphismus f von großer Bedeutung. Man gibt ihr daher einen besonderen Namen:

6.14 Definition
Sei $f : G_1 \to G_2$ ein Gruppen-Homomorphismus, $e_2 \in G_2$ das neutrale Element. Dann nennt man die Untergruppe $f^{-1}(e_2)$ von G_1 den *Kern von* f, also

$$\mathrm{Kern}\, f = \{a \in G_1 \mid f(a) = e_2\}$$

Die wichtigsten Eigenschaften davon fassen wir zusammen in:

6.15 Satz
Seien $f : G_1 \to G_2$ *ein Homomorphismus von Gruppen und* e_1*,* e_2 *die neutralen Elemente von* G_1 *bzw.* G_2*. Für den Kern von* f *gilt:*

(1) *Für* $a, b \in G_1$ *ist genau dann* $f(a) = f(b)$*, wenn* $ab^{-1} \in \mathrm{Kern}\, f$ *(oder* $a^{-1}b \in \mathrm{Kern}\, f$*).*

(2) *Für* $c \in \operatorname{Kern} f$ *ist* $aca^{-1} \in \operatorname{Kern} f$*, also* $a(\operatorname{Kern} f)a^{-1} \subset \operatorname{Kern} f$ *für alle* $a \in G_1$*.*

(3) *Für alle* $a \in G_1$ *gilt* $a \operatorname{Kern} f = (\operatorname{Kern} f)a$*.*

(4) f *ist genau dann injektiv (= monomorph), wenn* $\operatorname{Kern} f = \{e_1\}$ *ist.*

Beweis: (1) Ist $f(a) = f(b)$, dann ist

$$e_2 = f(a)(f(b)^{-1}) = f(a)f(b^{-1}) = f(ab^{-1}),$$

also $ab^{-1} \in \operatorname{Kern} f$. Umgekehrt folgt aus $f(ab^{-1}) = e_2$ auch

$$f(b) = e_2 f(b) = f(a)f(b^{-1})f(b) = f(a).$$

(2) Für $f(c) = e_2$ gilt $f(aca^{-1}) = f(a)f(c)f(a^{-1}) = f(aa^{-1}) = e_2$.

(3) Betrachte $b = ak$, $k \in \operatorname{Kern} f$. Dann ist $ba^{-1} = aka^{-1} \in \operatorname{Kern} f$ und $b \in (\operatorname{Kern} f)a$ nach (2).

(4) Gilt $\operatorname{Kern} f = \{e_1\}$, dann gilt in (1) $ab^{-1} = e_1$, also $a = b$. □

6.16 Definition
Eine Untergruppe U einer Gruppe (G, τ) heißt *Normalteiler* oder *normale Untergruppe*, wenn

$$a \,\tau\, U \,\tau\, a^{-1} \subset U \text{ für alle } a \in G.$$

Es ist leicht zu sehen, daß eine Untergruppe $U \subset G$ genau dann Normalteiler ist, wenn

$$a \,\tau\, U = U \,\tau\, a \text{ für alle } a \in G.$$

In abelschen Gruppen ist natürlich jede Untergruppe Normalteiler.

Zu jeder Untergruppe U einer Gruppe (G, τ) wird eine Äquivalenzrelation auf G definiert durch

$$R_U = \{(a, b) \in G \times G \mid b^{-1} \,\tau\, a \in U\}.$$

Die Äquivalenzklasse zu einem $a \in G$ ist dann $R_U(a) = [a] = a \,\tau\, U$.
Wir bezeichnen die Menge der Äquivalenzklassen mit G/U.

Die Normalteiler einer Gruppe zeichnen sich nun dadurch unter den gewöhnlichen Untergruppen aus, daß auf G/U wieder eine Gruppenstruktur eingeführt werden kann.

6.17 Faktorgruppen
Sei (G, τ) *eine Gruppe mit neutralem Element* e*. Sei* U *Normalteiler in* G*, so wird die Menge der Äquivalenzklassen* G/U *zu einer Gruppe durch die Verknüpfung*

$$[a] \,\tau'\, [b] := [a \,\tau\, b] \text{ für } a, b \in G.$$

Dabei ist $[e]$ *das neutrale Element in* $(G/U, \tau')$*, und* $[a^{-1}]$ *ist das Inverse zu* $[a]$*.*

Beweis: Es ist zu zeigen, daß diese Festlegung unabhängig ist von der Auswahl der Repräsentanten. Dazu betrachten wir $a' \in [a]$ und $b' \in [b]$, also $a' = a \,\tau\, k$ und $b' = a \,\tau\, h$ für geeignete $k, h \in U$. Hierfür gilt

$$\begin{aligned} [a' \,\tau\, b'] \;=\; [a \,\tau\, k \,\tau\, b \,\tau\, h] \;&=\; a \,\tau\, k \,\tau\, b \,\tau\, h \,\tau\, U \;=\; a \,\tau\, k \,\tau\, (b \,\tau\, U) \\ &=\; a \,\tau\, k \,\tau\, (U \,\tau\, b) \;=\; a \,\tau\, U \,\tau\, b \\ &=\; a \,\tau\, b \,\tau\, U \;=\; [a \,\tau\, b]. \end{aligned}$$

Also definiert τ' tatsächlich eine Verknüpfung auf G/U.
Es ist klar, daß $[e]$ neutrales Element ist.
Aus $[a] \,\tau'\, [a^{-1}] = [a \,\tau\, a^{-1}] = [e]$ folgt $[a]^{-1} = [a^{-1}]$. □

Nach 6.15 ist der Kern eines Gruppen-Homomorphismus ein Normalteiler in seiner Quelle.

In 4.5 haben wir zu einer Abbildung $f : G_1 \to G_2$ eine Äquivalenzrelation auf G_1 definiert. Ist f ein Gruppen-Homomorphismus, so haben wir nach 6.15

$$\begin{aligned} R_f &= \{(a,b) \in G_1 \times G_1 \mid f(a) = f(b)\} \\ &= \{(a,b) \in G_1 \times G_1 \mid a^{-1}b \in \operatorname{Kern} f\}. \end{aligned}$$

Damit ist $b \in [a]$ (also $f(b) = f(a)$) genau dann, wenn $b \in a \operatorname{Kern} f$, d.h.

$$a \operatorname{Kern} f = [a] = (\operatorname{Kern} f)a$$

ist die Äquivalenzklasse von $a \in G_1$ bzgl. R_f. Für die Menge der Äquivalenzklassen bedeutet dies

$$G_1/R_f = \{a \operatorname{Kern} f \mid a \in G_1\} =: G_1/\operatorname{Kern} f.$$

Wie wir oben gezeigt haben, haben wir auf $G_1/\operatorname{Kern} f$ eine Gruppenstruktur. Damit kommen wir zu einem der wichtigen Sätze der Gruppentheorie:

6.18 Homomorphiesatz für Gruppen
Sei $f : G_1 \to G_2$ ein Homomorphismus von Gruppen. Dann ist die kanonische Projektion

$$p_f : G_1 \to G_1/\operatorname{Kern} f, \quad a \mapsto [a],$$

ein Gruppenepimorphismus, und es gibt genau einen Monomorphismus

$$\overline{f} : G_1/\operatorname{Kern} f \to G_2$$

mit $f = \overline{f} \circ p_f$, d.h. wir haben das kommutative Diagramm

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle p_f}\searrow & & \nearrow{\scriptstyle \overline{f}} \\ & G_1/\operatorname{Kern} f\,. & \end{array}$$

Beweis: Das kommutative Diagramm kennen wir bereits aus 4.6, und wir wissen von dort, daß p_f surjektiv und $\overline{f}$ injektiv ist. Es bleibt zu zeigen, daß p_f und $\overline{f}$ Homomorphismen sind. Dies sieht man aus den Gleichungen

$$\begin{aligned} p_f(a\,\tau_1\,b) &= [a\,\tau_1\,b] = [a]\,\tau_1'\,[b] = p_f(a)\,\tau_1'\,p_f(b), \\ \overline{f}([a]\,\tau_1'\,[b]) &= \overline{f}([a\,\tau_1\,b]) = f(a\,\tau_1\,b) = f(a)\,\tau_2\,f(b) = \overline{f}([a])\,\tau_2\,\overline{f}([b]). \end{aligned}$$

□

Neu gegenüber Satz 4.6 ist im Homomorphiesatz, daß man bei einem Gruppen-Homomorphismus $f : G_1 \to G_2$ auf $G_1/\operatorname{Kern} f$ eine Gruppenstruktur hat und die auftretenden Abbildungen Homomorphismen sind.

Wie schon angemerkt, ist in abelschen Gruppen jede Untergruppe Normalteiler. Sehen wir uns dazu einen einfachen Fall an.

6.19 Beispiel
Betrachte die Äquivalenzrelation auf $\mathbb{Z}$, die durch die Untergruppe $7\mathbb{Z}$ bestimmt ist, also

$$\begin{aligned} R_7 &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \text{ ist durch } 7 \text{ teilbar}\} \\ &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid (-b) + a \in 7\mathbb{Z}\}. \end{aligned}$$

Dann ist $\mathbb{Z}/7\mathbb{Z}$ eine additive Gruppe mit $[a]+[b]=[a+b]$.
Die Projektion $p_7 : \mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$, $z \mapsto [z]$ ist ein Epimorphismus.
Wie nach Satz 3.8 zu erwarten ist, gibt es eine Abbildung von Mengen, etwa

$$q : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}, \quad [z] \mapsto z_0 \in [z], \text{ mit } z_0 < 7,$$

für die $p_7 \circ q = \mathrm{id}_{\mathbb{Z}/7\mathbb{Z}}$ gilt. Man beachte aber, daß q *kein* Homomorphismus (bzgl. $+$) ist, denn es gilt z.B. $q([5]) = 5$, $q([6]) = 6$ und

$$q([5]+[6]) = q([5+6]) = 4 \neq 11 = 5+6 = q([5]) + q([6]).$$

In der Tat gibt es keinen Homomorphismus $g : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}$ mit $p_7 \circ g = \mathrm{id}_{\mathbb{Z}/7\mathbb{Z}}$. Dies zeigt uns, daß nicht alle Sätze über Abbildungen von Mengen auch für Homomorphismen von Gruppen gelten.

Analog zur Situation bei Abbildungen haben wir auch hier:

6.20 Satz *(Universelle Eigenschaft des Produkts von (Halb-) Gruppen)*
Sei $(H_i, \tau_i)_I$ eine Familie von Halbgruppen und $(\prod_I H_i, \tau')$ das Produkt der H_i mit der Verknüpfung

$$(a_i)_I \, \tau' \, (b_i)_I := (a_i \, \tau_i \, b_i)_I.$$

(1) *Dann sind die Projektionen*

$$\pi_k : \prod\nolimits_I H_i \to H_k, \quad (a_i)_{i\in I} \mapsto a_k,$$

(Halbgruppen-)Epimorphismen.

(2) *Ist H' eine Halbgruppe und $(f_i : H' \to H_i)_{i\in I}$ eine Familie von Homomorphismen, so gibt es genau einen Homomorphismus $f : H' \to \prod_I H_i$ mit*

$$\pi_k \circ f = f_k \quad \text{für alle } k \in I,$$

d.h. folgende Diagramme sind kommutativ:

$$\begin{array}{ccc} H' & \xrightarrow{f_k} & H_k \\ {\scriptstyle f}\searrow & & \nearrow{\scriptstyle \pi_k} \\ & \prod_I H_i. & \end{array}$$

□

Wir wollen schließlich die neu erlernten Begriffe anhand einer wichtigen Gruppe ansehen, auf die wir später zurückgreifen werden.

6.21 Permutationsgruppen
Die bijektiven Abbildungen einer (endlichen) Menge A in sich nennt man *Permutationen* von A.

Die Gruppe aller Permutationen von A heißt *Permutationsgruppe* oder *symmetrische Gruppe* von A. Sie hat die Identität auf A als neutrales Element.

Bei diesen Betrachtungen können wir ohne Einschränkung der Allgemeinheit eine endliche Menge mit n Elementen durch

$$\{1, 2, \ldots, n\}$$

vorgeben. Die symmetrische Gruppe dazu bezeichnet man mit $\mathcal{S}_n$.

Eine Permutation σ davon kann man beschreiben durch

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Permutationen, die lediglich ein Paar von Elementen vertauschen und den Rest festlassen, nennt man *Transpositionen*.

Für jede Transposition τ gilt $\tau^2 = \mathrm{id}$. Ein Beispiel dafür ist etwa

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad \tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{id}\,.$$

Transpositionen sind sozusagen die Bausteine der Permutationen, denn:

6.22 Satz
Jede Permutation ist als Produkt von Transpositionen darstellbar.

Beweis: Es ist klar, daß eine Permutation genau dann die Identität ist, wenn sie n Elemente unverändert läßt.

Sei nun σ eine Permutation, die $r < n$ Elemente festläßt. Für ein $q < n$ mit $\sigma(q) \neq q$ definieren wir eine Transposition τ_1, die q mit $\sigma(q)$ vertauscht und den Rest festläßt. Die Komposition $\tau_1 \circ \sigma$ hat dann $r + 1$ Fixelemente.

Durch weitere Wahl von Transpositionen $\tau_2, \tau_3, ..., \tau_k$ erhält man schließlich n Fixpunkte, also

$$\tau_k \circ \tau_{k-1} \cdots \tau_1 \circ \sigma = \mathrm{id} \qquad \text{und } \sigma^{-1} = \tau_k \circ \cdots \circ \tau_1.$$

Da jede Permutation invertierbar ist, folgt daraus die Behauptung. □

6.23 Definition
Für eine Permutation $\sigma \in \mathcal{S}_n$ definieren wir das *Signum* durch

$$\operatorname{sgn}\sigma = \prod_{i<j} [\sigma(j) - \sigma(i)] \;\Big/\; \prod_{i<j} [j - i]\,.$$

Wie leicht zu sehen ist, stehen über und unter dem Bruchstrich bis auf das Vorzeichen die gleichen Faktoren. Also ist $\operatorname{sgn}\sigma$ gleich $+1$ oder -1.

Die Permutation σ heißt $\begin{cases} \textit{gerade}, & \text{wenn } \operatorname{sgn}\sigma = 1 \\ \textit{ungerade}, & \text{wenn } \operatorname{sgn}\sigma = -1 \end{cases}$.

Für eine Transposition $\tau \in \mathcal{S}_n$ gilt offensichtlich $\operatorname{sgn}\tau = -1$.

Als wichtige Eigenschaft von Signum stellen wir fest:

6.24 Satz
Für je zwei Permutationen σ, $\tau \in \mathcal{S}_n$ gilt

$$\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau.$$

Beweis: Nehmen wir zunächst an, τ sei eine Transposition, welche die Zahlen $k < l$ vertauscht. Ist $i < j$, so haben wir

$$\tau(j) < \tau(i) \text{ genau dann, wenn } i = k,\ j = l,$$

oder – äquivalent dazu –

$$\tau(i) < \tau(j) \text{ genau dann, wenn } (i, j) \neq (k, l).$$

Für jedes $\sigma \in \mathcal{S}_n$ ergibt sich damit

$$\begin{aligned}
&\prod_{i<j}[\sigma\circ\tau(j)-\sigma\circ\tau(i)]\\
&\quad=[\sigma\circ\tau(l)-\sigma\circ\tau(k)]\prod_{i<j,\tau(i)<\tau(j)}[\sigma\circ\tau(j)-\sigma\circ\tau(i)]\\
&\quad=[\sigma\circ\tau(l)-\sigma\circ\tau(k)]\prod_{\tau(i)<\tau(j),i<j}[\sigma(j)-\sigma(i)]\\
&\quad=-\prod_{i<j}[\sigma(j)-\sigma(i)].
\end{aligned}$$

Daraus ersieht man $\operatorname{sgn}(\sigma\circ\tau)=\operatorname{sgn}\sigma\cdot\operatorname{sgn}\tau$.

Sei nun τ eine beliebige Permutation. Nach 6.22 können wir

$$\tau=\tau_1\circ\tau_2\circ\cdots\circ\tau_k$$

mit lauter Transpositionen τ_i schreiben. Damit ist nun leicht zu sehen, daß auch für beliebige τ die gewünschte Beziehung gilt. □

Es gibt noch andere Möglichkeiten, das Signum einer Permutation zu interpretieren. Für $\sigma\in\mathcal{S}_n$ bezeichne $s(\sigma)$ die Anzahl der Paare (i,j) mit $1\le i<j\le n$ und $\sigma(i)>\sigma(j)$. Diese Paare bezeichnet man als *Fehlstände* von σ. Man kann sich überlegen, daß

$$\operatorname{sgn}\sigma=(-1)^{s(\sigma)}.$$

Eine weitere Beschreibung von Signum erhält man durch die Zerlegung von $\sigma\in\mathcal{S}_n$ in ein Produkt von Transpositionen τ_i, also

$$\sigma=\tau_1\circ\tau_2\circ\cdots\circ\tau_k,$$

mit einer ganzen Zahl k. Solche Zerlegungen sind zwar keineswegs eindeutig, und somit ist auch k nicht eindeutig bestimmt, dennoch folgt aus 6.24

$$\operatorname{sgn}\sigma=(-1)^k.$$

Damit können wir zusammenfassen:

6.25 Alternierende Gruppe
Die geraden Permutationen in $\mathcal{S}_n$ sind solche, die eine gerade Anzahl von Fehlständen haben, oder – gleichbedeutend – die als Produkt einer geraden Anzahl von Transpositionen darstellbar sind. Sie bilden eine Untergruppe und – nach 6.24 – sogar einen Normalteiler in $\mathcal{S}_n$.

Man nennt sie die *alternierende Gruppe* $\mathcal{A}_n$.

6.26 Beispiele
(1) Berechnung von Signum in $\mathcal{S}_5$.

$$\begin{aligned}
\sigma_1 &= \begin{pmatrix}1&2&3&4&5\\3&5&4&1&2\end{pmatrix}, & s(\sigma_1)&=7, & \operatorname{sgn}\sigma_1&=-1;\\
\sigma_2 &= \begin{pmatrix}1&2&3&4&5\\2&5&3&1&4\end{pmatrix}, & s(\sigma_2)&=5, & \operatorname{sgn}\sigma_2&=-1;\\
\sigma_1\circ\sigma_2 &= \begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}, & s(\sigma_1\circ\sigma_2)&=4, & \operatorname{sgn}\sigma_1\circ\sigma_2&=1.
\end{aligned}$$

(2) Eigenschaften der $\mathcal{S}_3$. Setze

$\alpha = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}$ und $\beta = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}$.

Dann gilt $\alpha^2 = \mathrm{id}$, $\beta^2 = \mathrm{id}$ und

$$\beta \circ \alpha = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \neq \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} = \alpha \circ \beta.$$

Dies bestätigt, daß $\mathcal{S}_3$ eine nicht-kommutative Gruppe ist.

$U := \{\mathrm{id}, \alpha\}$ ist Untergruppe, da $\alpha^{-1} = \alpha$, aber kein Normalteiler, denn

$$\beta^{-1} \circ \alpha \circ \beta = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \notin U.$$

Die Komposition $\gamma := \alpha \circ \beta$ ist eine gerade Permutation. Die Menge $\{\mathrm{id}, \gamma, \gamma^2\}$ enthält alle geraden Permutationen und ist Normalteiler ($= \mathcal{A}_3$).

7 Ringe und Körper

In diesem Abschnitt untersuchen wir algebraische Strukturen mit zwei Verknüpfungen. Da diese sehr weitgehend den Eigenschaften von $+$ und $\cdot$ in den ganzen Zahlen entsprechen sollen, belegt man sie meist mit diesen Symbolen:

7.1 Definition
Eine Menge R mit zwei Verknüpfungen $+, \cdot$, also ein Tripel $(R, +, \cdot)$, heißt ein *Ring*, wenn gilt:

(i) $(R, +)$ ist eine abelsche Gruppe,

(ii) $(R, \cdot)$ ist eine Halbgruppe mit neutralem Element,

(iii) für alle $a, b, c \in A$ gelten die *Distributivgesetze*
$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c, \\ (a + b) \cdot c &= a \cdot c + b \cdot c. \end{aligned}$$
Dabei folgen wir der Konvention, daß die *Multiplikation* $\cdot$ stärker bindet als die *Addition* $+$.

Man nennt den Ring $(R, +, \cdot)$ *kommutativ*, wenn zusätzlich gilt

$$a \cdot b = b \cdot a \text{ für alle } a, b \in R,$$

wenn also $(R, \cdot)$ eine kommutative Halbgruppe ist.

Das neutrale Element von $(R, +)$ nennt man die *Null* in R und schreibt dafür 0. Das neutrale Element von $(R, \cdot)$ heißt die *Eins* von R, auch *Einselement*, und man bezeichnet es meist mit 1 (oder e). Statt $a \cdot b$ schreibt man häufig nur ab.

Bemerkung: Es macht auch Sinn, Ringe *ohne Einselemente* zu betrachten. Wir wollen hier aber in Ringen im allgemeinen die Existenz einer Eins voraussetzen.

Als elementare Folgerungen notieren wir:

In einem Ring $(R, +, \cdot)$ gelten für alle $a, b \in R$:

$$\begin{aligned} &0 \cdot a = a \cdot 0 = 0, \\ &(-a)b = a(-b) = -ab \text{ und} \\ &(-a)(-b) = ab. \end{aligned}$$

Beweis: Aus $a = (a + 0)$ folgt $aa = aa + a0$ und somit $0 = 0a$.
Analog sieht man $0 = a0$.
Aus $0 = (a + (-a))b = ab + (-a)b$ folgt $-(ab) = (-a)b$. □

7.2 Definition
Ein Ring $(R, +, \cdot)$ heißt *Divisionsring* (auch *Schiefkörper*), wenn $(R \setminus \{0\}, \cdot)$ eine Gruppe ist, wenn es also zu jedem $0 \neq r \in R$ ein Inverses bzgl. der Multiplikation gibt. Dies bezeichnet man mit r^{-1}.

Ein Divisionsring heißt *Körper*, wenn $(R, \cdot)$ kommutativ ist, also $a \cdot b = b \cdot a$ für alle $a, b \in R$.

In einem Divisionsring R ist das Produkt von zwei Elementen a, b nur dann 0, wenn eines der beiden Elemente schon 0 ist: Aus $ab = 0$ und $b \neq 0$ folgt nämlich $0 = (ab)b^{-1} = a$.

7.3 Definition
Sei R ein Ring. Ein Element $a \in R$ heißt *Nullteiler*, wenn es ein $0 \neq b \in R$ gibt mit $ab = 0$.
Ringe, in denen es keine Nullteiler $\neq 0$ gibt, heißen *nullteilerfrei*.
Kommutative Ringe, die nullteilerfrei sind, nennt man *Integritätsringe*.

Zum Beispiel ist jeder Divisionsring nullteilerfrei, und jeder Körper ist Integritätsring.

Wie bei den Gruppen, so interessieren uns auch hier die Abbildungen, welche die Ringstruktur berücksichtigen:

7.4 Definition
Sei $f : R \to S$ eine Abbildung zwischen zwei Ringen R und S. f heißt *(Ring-)Homomorphismus*, wenn für alle $a, b \in R$ gilt:

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b) \\ f(1) &= 1. \end{aligned}$$

Man nennt f einen *Anti-Homomorphismus*, wenn an Stelle der zweiten Bedingung gilt

$$f(a \cdot b) = f(b) \cdot f(a).$$

Als $\operatorname{Kern} f$ bezeichnet man das Urbild der $0 \in S$:

$$\operatorname{Kern} f = \{a \in R \mid f(a) = 0\}$$

Ein Ringhomomorphismus ist also ein Halbgruppen-Homomorphismus zwischen $(R, +)$ und $(S, +)$ sowie zwischen $(R, \cdot)$ und $(S, \cdot)$.

7.5 Hilfssatz
Ist $f : R \to S$ ein Ringhomomorphismus, so gilt:

(1) $\operatorname{Kern} f$ *ist eine Untergruppe von $(R, +)$, und für alle $b \in R$ gilt*

$$b \operatorname{Kern} f \subset \operatorname{Kern} f \quad \textit{und} \quad (\operatorname{Kern} f)b \subset \operatorname{Kern} f.$$

(2) *f ist genau dann ein Monomorphismus, wenn* $\operatorname{Kern} f = \{0\}$ *ist.*

(3) *Ist R ein Divisionsring, so ist f ein Monomorphismus oder die Nullabbildung.*

Beweis: (1) $\operatorname{Kern} f$ ist Untergruppe nach 6.14.
Sei $k \in \operatorname{Kern} f$ und $b \in R$. Dann ist $f(kb) = f(k)f(b) = 0$, also $kb \in \operatorname{Kern} f$.

(2) wurde in Satz 6.15 gezeigt.

(3) Angenommen $0 \neq c \in \operatorname{Kern} f$. Nach (1) gilt dann $1 = c \cdot c^{-1} \in \operatorname{Kern} f$, und für jedes $a \in R$ ergibt sich $f(a) = f(1a) = f(1)f(a) = 0$. □

Wie in 6.17 ausgeführt, haben wir auf $R/\operatorname{Kern} f$ eine Addition. Wegen der in 7.5 angegebenen Eigenschaften der Kerne läßt sich darauf auch eine Multiplikation definieren durch

$$(a + \operatorname{Kern} f) \cdot (b + \operatorname{Kern} f) = ab + \operatorname{Kern} f.$$

Es ist nicht schwierig zu zeigen, daß diese Festlegung unabhängig ist von der Auswahl der Repräsentanten.

Dafür gilt nun wieder

7.6 Homomorphiesatz für Ringe
Sei $f : R \to S$ ein Ringhomomorphismus. Dann gilt:
Die kanonische Projektion $p_f : R \to R/\operatorname{Kern} f$ ist ein (surjektiver) Ringhomomorphismus, und die Abbildung

$$\overline{f} : R/\operatorname{Kern} f \to S, \quad [a] \mapsto f(a),$$

ist ein injektiver Ringhomomorphismus. Wir haben somit folgendes kommutative Diagramm von Ringhomomorphismen:

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle p_f}\searrow & & \nearrow{\scriptstyle \overline{f}} \\ & R/\operatorname{Kern} f. & \end{array}$$

7.7 Definition
Sei R ein Ring. Eine Untergruppe $U \subset (R,+)$ heißt

Linksideal in R, falls $aU \subset U$ für alle $a \in R$,

Rechtsideal in R, falls $Ua \subset U$ für alle $a \in R$,

Ideal in R, falls U Links- und Rechtsideal ist.

Diese Forderungen implizieren, daß jedes einseitige Ideal U selbst bzgl. $\cdot$ abgeschlossen und damit ein Unterring (ohne Eins) ist. Andererseits braucht jedoch ein Unterring kein Links- oder Rechtsideal in R zu sein.

In jedem Ring R sind $\{0\}$ und R Ideale. Man nennt sie die *trivialen Ideale*. Ideale, die ungleich R sind, nennt man *echte* Ideale.

Da R ein Einselement hat, gilt für ein Linksideal $U \subset R$ genau dann $U = R$, wenn $1 \in U$. Letzteres impliziert nämlich $a = a \cdot 1 \in U$ für alle $a \in R$.

Ist $U \subset R$ ein Ideal, so läßt sich auf der Faktorgruppe R/U durch

$$(a+U)\cdot(b+U) := ab+U$$

eine Multiplikation einführen, die $(R/U,+,\cdot)$ zu einem Ring macht.

Die kanonische Projektion $p : R \to R/U$ ist dann ein Ringhomomorphismus mit $\operatorname{Kern} p = U$.

Die Ideale sind bestimmend für die Struktur eines Ringes. Man sagt:

7.8 Definition
Ein Ring R heißt *einfach*, wenn er keine Ideale $\neq \{0\}, R$ enthält.

7.9 Satz. *Sei R ein Ring.*

(1) *R ist genau dann Divisionsring, wenn er keine nicht-trivialen Linksideale enthält.*

(2) *Sei R kommutativ. Dann ist R genau dann ein Körper, wenn er einfach ist.*

Beweis: (1) Sei R ein Ring ohne nicht-triviale Linksideale und $0 \neq a \in R$. Dann ist $0 \neq Ra$ ein Linksideal, also $Ra = R$. Somit gibt es $b \in R$ mit $ba = 1$, d.h. R ist Divisionsring.

Sei R Divisionsring und $U \subset R$ ein Linksideal $\neq 0$. Für ein $0 \neq u \in U$ gilt dann $1 = u^{-1}u \in U$ und damit $U = R$.

(2) Dies ist ein Spezialfall von (1). □

Sehen wir einige Beispiele zu den gegebenen Definitionen an.

7.10 Beispiele

(1) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer Integritätsring.

Für jedes $n \in \mathbb{N}$ bildet $n\mathbb{Z}$ ein Ideal in $\mathbb{Z}$, und wir können dazu den Faktorring $\mathbb{Z}/n\mathbb{Z}$ bilden. Dieser besteht aus n Äquivalenzklassen, die wir mit $\{0,1,\ldots,n-1\}$ markieren können. Addition und Multiplikation darin ergeben sich durch Rechnen *modulo n*.

(2) Über jedem Ring R kann man *Matrizenringe* definieren.

Wir werden später noch allgemeinere Bildungen kennenlernen. Hier wollen wir den einfachsten nicht-trivialen Fall angeben:

Matrizenring $R^{(2,2)}$: Auf den $(2,2)$-Matrizen mit Elementen in R können Addition und Multiplikation definiert werden durch:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} := \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}.$$

Dieser Ring enthält immer Nullteiler, denn

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Er ist nicht kommutativ, da z.B.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

$\begin{pmatrix} R & 0 \\ R & 0 \end{pmatrix}$ und $\begin{pmatrix} 0 & R \\ 0 & R \end{pmatrix}$ sind Linksideale in $R^{(2,2)}$;

$\begin{pmatrix} R & R \\ 0 & 0 \end{pmatrix}$ und $\begin{pmatrix} 0 & 0 \\ R & R \end{pmatrix}$ sind Rechtsideale in $R^{(2,2)}$;

$\begin{pmatrix} R & 0 \\ 0 & 0 \end{pmatrix}$ ist Unterring, aber kein Ideal.

7.11 Ringstruktur auf Mengen von Abbildungen

Sei $(R, +, \cdot)$ ein Ring und I eine Menge. Dann kann auf $\mathrm{Abb}(I, R) = R^I$, der Menge der Abbildungen von I in R (vgl. 3.12), eine Ringstruktur festgelegt werden durch

$$f \oplus g(x) := f(x) + g(x), \quad f \odot g(x) := f(x) \cdot g(x).$$

Die Bedingungen an die Verknüpfungen $\oplus$ und $\odot$ können durch Rückführung auf die entsprechenden Eigenschaften von $+$ und $\cdot$ nachgewiesen werden.

Auch dieser Ring enthält immer Nullteiler, falls I mindestens zwei Elemente hat: Sei R ein Ring und $I = \{i, j\}$ mit $i \neq j$. Definiere Abbildungen $f, g : I \to R$ durch

$$f(i) := 0,\ f(j) := 1; \quad g(i) := 1,\ g(j) := 0.$$

Diese Abbildungen sind nicht Null, aber $f \odot g$ ist Null.

Obige Konstruktion macht (für jeden Ring R) speziell $R \times R$ zu einem Ring (mit Nullteiler) durch komponentenweise Festlegung der Operationen.

Mit den bereitgestellten Mitteln können wir aus gegebenen Ringen weitere Ringe konstruieren. Mit einem ähnlichen Ansatz wie in Beispiel (3) erhalten wir auch den Ring der *Polynome*. Das Rechnen mit Polynomen ist sicher von der Schule her vertraut. Bei genauerem Hinsehen muß man aber doch nachfragen, was es mit der dabei auftretenden *Unbestimmten* auf sich hat. Die nachfolgende Beschreibung liefert den Nachweis, daß wir im Rahmen der von uns aufgebauten Grundlagen mit Polynomen so umgehen dürfen, wie wir es gewohnt sind.

7.12 Polynomring

Sei R ein kommutativer Ring. Auf $\mathrm{Abb}(\mathbb{N}, R) = R^{\mathbb{N}}$, der Menge der Abbildungen $\mathbb{N} \to R$, führen wir eine Addition wie im vorangehenden Beispiel ein, aber eine andere Multiplikation. Bemerkenswert daran ist, daß die Multiplikation auch die Eigenschaften von $\mathbb{N}$ heranzieht:

$$\begin{aligned}(a_i)_{i\in\mathbb{N}} \oplus (b_i)_{i\in\mathbb{N}} &= (a_i + b_i)_{i\in\mathbb{N}},\\ (a_i)_{i\in\mathbb{N}} \odot (b_i)_{i\in\mathbb{N}} &= (c_i)_{i\in\mathbb{N}}, \text{ mit } c_i = \sum_{k=0}^{i} a_k b_{i-k}.\end{aligned}$$

Damit wird $\mathrm{Abb}(\mathbb{N}, R)$ ein kommutativer Ring. Es ist leicht zu sehen, daß das Einselement dargestellt werden kann durch

$$e = (1, 0, 0, \ldots).$$

Sehen wir uns das folgende Element genauer an:

$$X := (0, 1, 0, \ldots), \quad \text{also } X(n) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{für } n \neq 1 \end{cases}.$$

Multiplizieren wir X mit sich, so erhalten wir

$$X^2 = (0, 0, 1, 0, \ldots); \quad X^2(n) = \begin{cases} 1 & \text{für } n = 2 \\ 0 & \text{für } n \neq 2 \end{cases}.$$

Allgemein ergibt sich für $k \in \mathbb{N}$,

$$X^k(n) = \begin{cases} 1 & \text{für } n = k \\ 0 & \text{für } n \neq k \end{cases}.$$

Bezeichne $\mathrm{Abb}_e(\mathbb{N}, R)$ die Abbildungen $\mathbb{N} \to R$, die nur auf endlich vielen $n \in \mathbb{N}$ ungleich Null sind, also darstellbar sind durch

$$(a_i)_{i\in\mathbb{N}} \text{ mit } a_i = 0 \text{ für fast alle } i \in \mathbb{N}.$$

Dies ist offensichtlich ein Unterring von $\mathrm{Abb}(\mathbb{N}, R)$. Jedes Element daraus hat die Form

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) = a_0 + a_1 X + \ldots + a_n X^n.$$

Man nennt $R[X] := (\mathrm{Abb}_e(\mathbb{N}, R), \oplus, \odot)$ den *Polynomring über R in einer Unbestimmten X*.

Die Elemente daraus sind die uns vertrauten Polynome, und wir kehren wieder zur üblichen Notation zurück. Insbesodere haben wir für Addition und Multiplikation von zwei Polynomen (wie erwartet)

$$\begin{aligned}\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} b_j X^j &= \sum_{i=0}^{max(n,m)} (a_i + b_i) X^i,\\ \sum_{i=0}^{n} a_i X^i \cdot \sum_{j=0}^{m} b_j X^j &= \sum_{i=0}^{n+m} \Big(\sum_{k=0}^{i} a_k b_{i-k}\Big) X^i.\end{aligned}$$

Ohne Einschränkung können wir annehmen, daß in obiger Darstellung von Polynomen $a_n \neq 0$ und $b_m \neq 0$. Ist R Integritätsring, so ist auch $a_n b_m \neq 0$, und damit ist das rechts stehende Polynom nicht Null, das heißt:

Ist R ein Integritätsring, so ist auch $R[X]$ ein Integritätsring.

Für jeden kommutativen Ring R ist die Abbildung

$$\varepsilon : R \to Re = (R, 0, 0, \ldots)$$

ein Homomorphismus, der jedem Polynom sein konstantes Glied zuordnet.

Als nützliche Eigenschaft von $R[X]$, die sich leicht nachprüfen läßt, halten wir fest:

Universelle Abbildungseigenschaft von $R[X]$
Zu jedem Ring S, $s \in S$ und jedem Homomorphismus $\varphi : R \to S$ gibt es genau einen Homomorphismus $\Phi : R[X] \to S$ mit $\Phi(X) = s$ und dem kommutativen Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle\varepsilon}\searrow & & \nearrow{\scriptstyle\Phi} \\ & R[X]. & \end{array}$$

Die Wirkung von Φ auf ein Polynom ist beschrieben durch

$$\Phi : a_0 + a_1 X + \ldots + a_n X^n \mapsto \varphi(a_0) + \varphi(a_1)s + \ldots + \varphi(a_n)s^n.$$

Ein wichtiger Schritt beim Aufbau des Zahlensystems ist die Konstruktion der rationalen Zahlen aus den ganzen Zahlen. Auf gleiche Weise erhält man zu jedem Integritätsring den Quotientenkörper, und wir wollen dies skizzieren:

7.13 Quotientenkörper eines Integritätsrings
Sei R ein Integritätsring. Definiere eine Relation auf $R \times (R \setminus \{0\})$:

$$(a, b) \sim (a', b') \text{ genau dann, wenn } ab' = ba'.$$

Dies ist eine Äquivalenzrelation. Wir schreiben für die Äquivalenzklassen
$[(a, b)] = [a, b]$ und bezeichnen ihre Gesamtheit mit

$$Q(R) := \{[a, b] \,|\, a \in R,\, b \in R \setminus \{0\}\}.$$

Darauf betrachten wir die Verknüpfungen

$$\begin{aligned} [a, b] + [a', b'] &:= [ab' + ba', bb'] \\ [a, b] \cdot [a', b'] &:= [aa', bb']. \end{aligned}$$

Es ist nachzuprüfen, daß diese Festlegungen unabhängig sind von der Auswahl der Repräsentanten, und daß damit $(Q(R), +, \cdot)$ zu einem kommutativen Ring wird. Dabei wird $[1, 1]$ das Einselement und $[0, 1]$ das Nullelement.
Das Inverse zu $[a, b]$ mit $a \neq 0$ ist $[b, a]$.

$Q(R)$ ist also ein Körper, der *Quotientenkörper* von R. Die Abbildung

$$R \to Q(R), \quad a \mapsto [a, 1],$$

ist eine *Einbettung* (injektiver Homomorphismus) von R in $Q(R)$.

Setzen wir $\frac{a}{b} := [a, b]$, so erkennen wir, daß die obigen Definitionen gerade die üblichen Rechenregeln für Brüche ergeben.

Es sei angemerkt, daß bei dieser Konstruktion die Kommutativität von R wesentlich mitbenutzt wird. Für nicht-kommutative Ringe sind vergleichbare Bildungen wesentlich aufwendiger.

Als Spezialfall erhält man für $R = \mathbb{Z}$ wie erwartet $Q(\mathbb{Z}) = \mathbb{Q}$.

Für einen Integritätsring R ist auch der Polynomring $R[X]$ Integritätsring (vgl. 7.12), und wir erhalten mit der angegebenen Konstruktion den Quotientenkörper $Q(R[X])$ dazu. Man

nennt diesen den Körper der *rationalen Funktionen*. Seine Elemente lassen sich als Brüche von zwei Polynomen beschreiben.

Mit den vorangegangenen Betrachtungen haben wir gesehen, daß wir mit den bereitgestellten (mengentheoretischen) Grundlagen auch die rationalen Zahlen in unsere Theorie einfügen können. Prinzipiell gilt dies auch für die reellen Zahlen, doch sind dazu auch nicht-algebraische Überlegungen notwendig, mit denen wir uns hier nicht befassen: Man muß $\mathbb{Q}$ zu einem Körper erweitern, in dem alle *Cauchy-Folgen* von Elementen aus $\mathbb{Q}$ einen Grenzwert haben.

Der Schritt von den reellen zu den komplexen Zahlen ist allerdings wieder rein algebraischer Natur. Daher wollen wir ihn hier angeben.

7.14 Die komplexen Zahlen
Auf dem kartesischen Produkt $\mathbb{R} \times \mathbb{R}$ führen wir Addition und Multiplikation ein durch

$$\begin{aligned}(a,b) + (a',b') &:= (a+a', b+b'),\\ (a,b) \cdot (a',b') &:= (aa' - bb', ab' + ba').\end{aligned}$$

Mit diesen Verknüpfungen wird $\mathbb{R} \times \mathbb{R}$ ein Körper, den man den Körper der *komplexen Zahlen* $\mathbb{C}$ nennt.

$(1,0)$ ist das Einselement, $(0,0)$ das Nullelement darin. Das Inverse zu $(0,0) \neq (a,b) \in \mathbb{C}$ bekommt man durch

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right).$$

Wir haben eine Einbettung

$$\mathbb{R} \to \mathbb{C}, \quad a \mapsto a(1,0) = (a,0),$$

und dürfen daher die Elemente $a \in \mathbb{R}$ mit $(a,0) \in \mathbb{C}$ identifizieren. Das Element $i := (0,1)$ hat die Eigenschaft $i^2 = -(1,0)$, und mit obiger Festlegung gilt dann für die Elemente in $\mathbb{C}$

$$(a,b) = a + bi.$$

Dies gibt uns die vertraute und übliche Schreibweise der komplexen Zahlen.

Auf eine weitere algebraische Darstellung von $\mathbb{C}$ wird bei den Aufgaben zu diesem Abschnitt hingewiesen.

Die wohl wichtigste Eigenschaft von $\mathbb{C}$ ist für uns, daß jedes nicht konstante Polynom aus $\mathbb{C}[X]$ eine Nullstelle in $\mathbb{C}$ hat. Dies wird manchmal der *Fundamentalsatz der Algebra* genannt, obwohl er nicht mit algebraischen Methoden alleine bewiesen werden kann. Der erste Beweis dazu stammt von C.F. Gauß (1799).

Eine weitere Besonderheit von $\mathbb{C}$ sei noch erwähnt: Die Abbildung

$$\gamma : \mathbb{C} \to \mathbb{C}, \quad a + ib \mapsto a - ib,$$

ist ein Automorphismus von $\mathbb{C}$ mit $\gamma^2 = \mathrm{id}_{\mathbb{C}}$. Dies kann man einfach nachrechnen.

Einen solchen Automorphismus gibt es für die reellen Zahlen nicht, und natürlich hat auch nicht jedes nicht-konstante Polynom aus $\mathbb{R}[X]$ eine Nullstelle in $\mathbb{R}$.

7.15 Die Quaternionen
Auf dem kartesischen Produkt $\mathbb{R}^4$ führen wir Addition und Multiplikation ein durch

$$\begin{aligned}(a,b,c,d)+(a',b',c',d') &:= (a+a',b+b',c+c',d+d'),\\ (a,b,c,d)\cdot(a',b',c',d') &:= (aa'-bb'-cc'-dd', ab'+ba'+cd'-dc',\\ &\qquad ac'-bd'+ca'+db', ad'+bc'-cb'+da').\end{aligned}$$

Mit diesen Verknüpfungen wird $\mathbb{R}^4$ ein Divisionsring, den man den Ring der *Quaternionen* $\mathbb{H}$ nennt. Das Symbol $\mathbb{H}$ soll an *W.R. Hamilton* erinnern, der als einer der ersten auf die Bedeutung dieses Divisionsrings (in Geometrie und Zahlentheorie) aufmerksam machte.

$1_{\mathbb{H}} := (1,0,0,0)$ ist das Einselement, $(0,0,0,0)$ das Nullelement darin. Das Inverse bekommt man durch

$$(a,b,c,d)^{-1} = \frac{1}{a^2+b^2+c^2+d^2}(a,-b,-c,-d).$$

Wir haben eine Einbettung

$$\mathbb{R} \to \mathbb{H}, \quad a \mapsto a(1,0,0,0) = (a,0,0,0),$$

und dürfen daher die Elemente $a \in \mathbb{R}$ mit $(a,0,0,0) \in \mathbb{H}$ identifizieren.

Setzt man die letzten beiden Komponenten von Elementen aus $\mathbb{H}$ gleich Null, so erhält man gerade die komplexen Zahlen $\mathbb{C}$. Dies ergibt auch eine Einbettung

$$\mathbb{C} \to \mathbb{H}, \quad (a,b) \mapsto (a,b,0,0).$$

Die angegebene Multiplikation der Quaternionen läßt sich handlicher angeben, wenn man bedenkt, daß sie schon durch die Produkte von gewissen *Basiselementen* bestimmt ist. Folgende Notation hat sich dabei eingebürgert:

$$i := (0,1,0,0), \quad j := (0,0,1,0), \quad k := (0,0,0,1).$$

Damit können wir die Elemente von $\mathbb{H}$ schreiben als

$$(a,b,c,d) = a + bi + cj + dk.$$

Die Multiplikation der Basiselemente ergibt

$$\begin{gathered}i^2 = j^2 = k^2 = -1_{\mathbb{H}}\\ ij = -ji = k, \quad jk = -jk = i, \quad ki = -ik = j.\end{gathered}$$

Diese Beziehungen legen die Multiplikation in $\mathbb{H}$ fest. Sie zeigen, daß $\mathbb{H}$ nicht kommutativ ist.

Man sieht daraus auch, daß über $\mathbb{H}$ das Polynom X^2+1 drei verschiedene Nullstellen hat. Über einem kommutativen Körper kann ein Polynom zweiten Grades dagegen höchstens zwei Nullstellen haben.

Ähnlich wie in $\mathbb{C}$ haben wir auch in $\mathbb{H}$ einen Antiautomorphismus

$$\gamma : \mathbb{H} \to \mathbb{H}, \quad a+bi+cj+dk \mapsto a-bi-cj-dk,$$

mit $\gamma^2 = \mathrm{id}_{\mathbb{H}}$. Dies kann man einfach nachrechnen. Damit läßt sich die *Norm* eines Elements definieren durch

$$N(a+bi+cj+dk) := (a+bi+cj+dk)(a-bi-cj-dk) = (a^2+b^2+c^2+d^2)1_{\mathbb{H}},$$

mit der man das Inverse eines Elements $z \in \mathbb{H}$ ausdrücken kann als

$$z^{-1} = \frac{1}{N(z)}\gamma(z).$$

Eine Darstellung von $\mathbb{H}$ als Matrizenring über $\mathbb{C}$ wird in den Aufgaben angegeben.

Wir haben in 7.7 angegeben, daß zu jedem Ideal U in einem Ring R auf R/U eine Ringstruktur definiert werden kann. Dabei stehen Eigenschaften des Ideals U in Wechselbeziehung zu Eigenschaften des Ringes R/U. Folgende Eigenschaft von Idealen ist in diesem Zusammenhang von Bedeutung:

7.16 Definition
Ein echtes Linksideal $U \subset R$ heißt *maximal*, wenn es maximales Element in der Menge der echten Linksideale bezüglich der Inklusion $\subset$ ist, d.h.
für jedes Linksideal $V \subset R$ mit $U \subset V$ ist $U = V$ oder $V = R$.

Die Bedeutung dieser Ideale für die Struktur der zugehörigen Faktorringe liegt in folgender Beobachtung:

7.17 Satz
Sei R ein kommutativer Ring. Ein Ideal $U \subset R$ ist genau dann maximal, wenn der Faktorring R/U ein Körper ist.

Beweis: $\Rightarrow$ Sei U ein maximales Ideal, $p : R \to R/U$ die kanonische Projektion. Ist I ein Ideal in R/U, dann ist $p^{-1}(I)$ ein Ideal in R, das U enthält. Also gilt entweder $p^{-1}(I) = U$ und damit

$$I = p(p^{-1}(I)) = p(U) = [0],$$

oder es ist $p^{-1}(I) = R$ und damit $I = p(R) = R/U$.
Somit gibt es in R/U nur die trivialen Ideale. Nach Satz 7.9 ist dann R/U ein Körper.

$\Leftarrow$ Sei R/U ein Körper, $V \subset R$ ein Ideal mit $U \subset V$. Dann ist $p(V)$ Ideal in R/U, also $p(V) = [0]$ und damit $U = V$, oder $p(V) = R/U$, woraus $V = V + U = R$ folgt. Damit ist U maximales Ideal. □

Die Frage nach der Existenz von maximalen Idealen läßt sich mit Hilfe des Zornschen Lemmas beantworten. Dazu zeigen wir zunächst:

7.18 Hilfssatz
Sei R ein Ring und $K \subset R$ ein Linksideal. Dann ist die Menge $\mathcal{U}$ aller von R verschiedenen Linksideale, die K enthalten, also

$$\mathcal{U} = \{I \subset R \mid I \text{ Linksideal}, K \subset I \text{ und } 1 \notin I\},$$

bezüglich der Inklusion $\subset$ induktiv geordnet.

Beweis: $\mathcal{U}$ ist nicht leer, da $K \in \mathcal{U}$. Sei $\mathcal{V}$ eine linear geordnete Teilmenge von $\mathcal{U}$. Wir zeigen, daß $\overline{U} = \bigcup_{U \in \mathcal{V}} U$ eine kleinste obere Schranke von $\mathcal{V}$ in $\mathcal{U}$ ist. Offensichtlich gilt $1 \notin \overline{U} \supset K$. Auch die gewünschte Minimaleigenschaft von $\overline{U}$ ist klar.

Es bleibt also nur nachzuweisen, daß $\overline{U}$ ein Linksideal ist. Betrachte dazu $a, b \in \overline{U}$. Dann gibt es ein $U \in \mathcal{U}$ mit $a, b \in U$, und damit gilt auch

$$a + b \in U \subset \overline{U} \text{ und } Ra \subset U \subset \overline{U}.$$

Also ist $\overline{U}$ ein Linksideal. □

Als Folgerung daraus erhalten wir den wichtigen

7.19 Satz von Krull
Jedes echte Linksideal in einem Ring R ist in einem maximalen Linksideal enthalten.

Beweis: Sei $K \neq R$ Linksideal in R. Die Menge der echten Linksideale von R, die K enthalten, sind induktiv geordnet. Das Zornsche Lemma garantiert die Existenz von maximalen Elementen in solchen Mengen.
Es ist leicht zu sehen, daß dies maximale Linksideale sind. □

Da in jedem Ring $\{0\}$ ein Ideal ist, ergibt sich aus 7.19 die Existenz von maximalen Linksidealen in allen Ringen (mit Eins!).

Mit einem analogen Beweis kann man auch zeigen, daß in einem Ring jedes Linksideal (Rechtsideal) in einem *maximalen Linksideal (Rechtsideal)* enthalten ist.

Für kommutative Ringe haben wir das

Korollar
Zu jedem kommutativen Ring gibt es einen Epimorphismus $R \to K$ auf einen Körper K.

Beweis: Sei U ein maximales Ideal in R. Dann ist R/U nach 7.17 ein Körper, und die kanonische Projektion $R \to R/U$ ist der gewünschte Epimorphismus. □

7.20 Aufgaben

(1) Sei $K^{(2,2)}$ der Ring der $(2,2)$-Matrizen über einem Körper K. Zeigen Sie:

(i) *$K^{(2,2)}$ ist ein einfacher Ring.*
Bestimmen Sie das Zentrum (vgl. Aufgabe (2)) von $K^{(2,2)}$.

(ii) *Folgende Menge ist ein Unterring von $K^{(2,2)}$:*

$$C(K) := \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in K\}.$$

(iii) *Für $K = \mathbb{R}$ ist $C(\mathbb{R})$ ein Körper.*

(iv) *$f : \mathbb{C} \to C(\mathbb{R})$ mit $a + ib \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ ist ein Isomorphismus.*

(2) Ähnlich wie $\mathbb{C}$ aus $\mathbb{R}$ lassen sich die Quaternionen $\mathbb{H}$ aus $\mathbb{C}$ gewinnen. $\mathbb{H}$ wurde in 7.15 durch eine Multiplikation auf $\mathbb{R}^4$ eingeführt.
Sei $\mathbb{C}^{(2,2)}$ der Ring der $(2,2)$-Matrizen über $\mathbb{C}$. Für $z = a + ib \in \mathbb{C}$ bezeichne $\bar{z} = a - ib$ (konjugiert komplexe Zahl). Zeigen Sie:

(i) *Folgende Menge ist ein Unterring von $\mathbb{C}^{(2,2)}$:*

$$H(\mathbb{C}) := \{\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C}\}.$$

(ii) *$f : \mathbb{H} \to H(\mathbb{C})$ mit $(a, b, c, d) \mapsto \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix}$*
ist ein (Ring-) Isomorphismus.

(iii) *$f(\mathbb{R}, \mathbb{R}, 0, 0) \simeq \mathbb{C}$ liegt nicht im Zentrum von $H(\mathbb{C})$.*

Index