Sebastian Thomas

RWTH Aachen, WS 2016/17
16.11.2016

Diskrete Strukturen
Vorlesung 8

6 Algebraische Strukturen

Bisher haben wir Mengen und Abbildungen zwischen Mengen betrachtet. Die aus der Schule bekannten Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ haben jedoch neben der Zusammenfassung ihrer Elemente noch mehr Struktur – wir können etwa Elemente addieren und multiplizieren. Dieser Aspekt soll in diesem Abschnitt formalisiert werden. Wir beleuchten die algebraische Struktur dieser Zahlbereiche und gelangen dadurch zu Begriffen wie Gruppe und Ring, von denen wir im weiteren Verlauf auch neue Beispiele kennenlernen werden.

Verknüpfungen

Unser intuitives Verständnis der Zahlbereiche lässt an der Gültigkeit des folgenden Satzes keinen Zweifel:

(6.1) Satz.

(a) (i) Für $m, n, p \in \mathbb{N}$ gilt $m + (n + p) = (m + n) + p$.
(ii) Für $m, n \in \mathbb{N}$ gilt $m + n = n + m$.
(iii) Für $m, n, p \in \mathbb{N}$ gilt $m(np) = (mn)p$.
(iv) Für $m \in \mathbb{N}$ gilt $1m = m1 = m$.
(v) Für $m, n \in \mathbb{N}$ gilt $mn = nm$.

(b) (i) Für $m, n, p \in \mathbb{N}_0$ gilt $m + (n + p) = (m + n) + p$.
(ii) Für $m \in \mathbb{N}_0$ gilt $0 + m = m + 0 = m$.
(iii) Für $m, n \in \mathbb{N}_0$ gilt $m + n = n + m$.
(iv) Für $m, n, p \in \mathbb{N}_0$ gilt $m(np) = (mn)p$.
(v) Für $m \in \mathbb{N}_0$ gilt $1m = m1 = m$.
(vi) Für $m, n \in \mathbb{N}_0$ gilt $mn = nm$.

(c) (i) Für $x, y, z \in \mathbb{Z}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{Z}$ gilt $0 + x = x + 0 = x$.
(iii) Für $x \in \mathbb{Z}$ gilt $(-x) + x = x + (-x) = 0$.
(iv) Für $x, y \in \mathbb{Z}$ gilt $x + y = y + x$.
(v) Für $x, y, z \in \mathbb{Z}$ gilt $x(yz) = (xy)z$.
(vi) Für $x \in \mathbb{Z}$ gilt $1x = x1 = x$.
(vii) Für $x, y \in \mathbb{Z}$ gilt $xy = yx$.
(viii) Für $x, y, z \in \mathbb{Z}$ gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

(d) (i) Für $x, y, z \in \mathbb{Q}$ gilt $x + (y + z) = (x + y) + z$.
(ii) Für $x \in \mathbb{Q}$ gilt $0 + x = x + 0 = x$.
(iii) Für $x \in \mathbb{Q}$ gilt $(-x) + x = x + (-x) = 0$.
(iv) Für $x, y \in \mathbb{Q}$ gilt $x + y = y + x$.
(v) Für $x, y, z \in \mathbb{Q}$ gilt $x(yz) = (xy)z$.
(vi) Für $x \in \mathbb{Q}$ gilt $1x = x1 = x$.

(vii) Für $x \in \mathbb{Q} \setminus \{0\}$ gilt $x^{-1}x = xx^{-1} = 1$.

(viii) Für $x, y \in \mathbb{Q}$ gilt $xy = yx$.

(ix) Für $x, y, z \in \mathbb{Q}$ gilt $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

Die Rechenregeln aus Satz (6.1) geben die grundsätzlichen Eigenschaften der Addition und der Multiplikation von rationalen Zahlen und gewissen Teilmengen wieder. Im Folgenden wollen wir diese Eigenschaften genauer analysieren, formalisieren und so zu neuen Begrifflichkeiten auf einer abstrakten Ebene gelangen, welche sich dann wiederum bei weiteren Beispielen in ganz anderen Bereichen verwenden lassen.
Zunächst müssen wir uns darüber im Klaren werden, was eine Addition bzw. eine Multiplikation eigentlich ist. Bei der Addition natürlicher Zahlen m und n ordnen wir diesen ihre Summe $m + n$ zu. In Abschnitt 3 haben wir gesehen, dass sich solche Zuordnungen mit Hilfe von Abbildungen formalisieren lassen. Da jeder Ausdruck der Form $m + n$ aus den beiden Summanden m und n entsteht, ordnen wir bei der Addition einem Paar (m, n) in $\mathbb{N}$, also einem Element in $\mathbb{N} \times \mathbb{N}$, das Element $m + n$ in $\mathbb{N}$ zu. Bei der Addition handelt es sich also um eine Abbildung

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (m, n) \mapsto m + n.$$

Wir werden nun Abbildungen von dieser Form systematisch studieren und ihnen deswegen eine eigene Bezeichnung verleihen.

(6.2) Definition (Verknüpfung)**.** Es sei eine Menge X gegeben. Eine *Verknüpfung* (oder *binäre algebraische Operation*) auf X ist eine Abbildung $m\colon X \times X \to X$. Für $(x, y) \in X \times X$ schreiben wir $x\, m\, y := m(x, y)$.

Da zu einer gegebenen Menge X die Start- und die Zielmenge einer Verknüpfung auf X eindeutig festgelegt sind ($X \times X$ bzw. X), lassen wir diese Angaben im Folgenden meist weg.

(6.3) Beispiel.

(a) Auf $\mathbb{N}$ haben wir die Verknüpfungen $(m, n) \mapsto m + n$ und $(m, n) \mapsto m \cdot n$.

(b) Auf $\mathbb{N}_0$ haben wir die Verknüpfungen $(m, n) \mapsto m + n$ und $(m, n) \mapsto m \cdot n$.

(c) Auf $\mathbb{Z}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

(d) Auf $\mathbb{Q}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

Verknüpfungen auf endlichen Mengen lassen sich durch *Verknüpfungstafeln* verbildlichen:

(6.4) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben. Auf $\{a, b, c\}$ haben wir eine Verknüpfung m, welche durch folgende Verknüpfungstafel gegeben ist:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben. Auf $\{a, b, c, d, e\}$ haben wir eine Verknüpfung m, welche durch folgende Verknüpfungstafel gegeben ist:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Natürlich gibt es auf $\mathbb{N}$ und den anderen Zahlbereichen noch viel mehr Verknüpfungen, doch diese beiden zeichnen sich durch besondere Eigenschaften aus, wie wir in Satz (6.1) gesehen haben. Wir wollen diese Eigenschaften nun für allgemeine Verknüpfungen studieren.

(6.5) Definition (Assoziativität, Kommutativität)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben.

(a) Wir sagen, dass m *assoziativ* ist, wenn für $x, y, z \in X$ stets

$$x\, m\, (y\, m\, z) = (x\, m\, y)\, m\, z$$

gilt.

(b) Wir sagen, dass m *kommutativ* ist, wenn für $x, y \in X$ stets

$$x\, m\, y = y\, m\, x$$

gilt.

Die Aussagen aus Satz (6.1)(a)(i), (ii), (iii), (v) lassen sich nun auch kurz wie folgt formulieren:

(6.6) Beispiel. Die Verknüpfungen $(m, n) \mapsto m + n$ und $(m, n) \mapsto m \cdot n$ auf $\mathbb{N}$ sind assoziativ und kommutativ.

(6.7) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist m assoziativ und kommutativ.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist m nicht assoziativ und nicht kommutativ.

Beweis.

(a) Wegen

$$\begin{aligned}
&a\, m\, (a\, m\, a) = a\, m\, a = a = a\, m\, a = (a\, m\, a)\, m\, a,\\
&a\, m\, (a\, m\, b) = a\, m\, b = b = a\, m\, b = (a\, m\, a)\, m\, b,\\
&a\, m\, (a\, m\, c) = a\, m\, c = c = a\, m\, c = (a\, m\, a)\, m\, c,\\
&a\, m\, (b\, m\, a) = a\, m\, b = b = b\, m\, a = (a\, m\, b)\, m\, a,\\
&a\, m\, (b\, m\, b) = a\, m\, c = c = b\, m\, b = (a\, m\, b)\, m\, b,\\
&a\, m\, (b\, m\, c) = a\, m\, a = a = b\, m\, c = (a\, m\, b)\, m\, c,\\
&a\, m\, (c\, m\, a) = a\, m\, c = c = c\, m\, a = (a\, m\, c)\, m\, a,\\
&a\, m\, (c\, m\, b) = a\, m\, a = a = c\, m\, b = (a\, m\, c)\, m\, b,\\
&a\, m\, (c\, m\, c) = a\, m\, b = b = c\, m\, c = (a\, m\, c)\, m\, c,\\
&b\, m\, (a\, m\, a) = b\, m\, a = b = a\, m\, a = (b\, m\, a)\, m\, a,\\
&b\, m\, (a\, m\, b) = b\, m\, b = c = a\, m\, b = (b\, m\, a)\, m\, b,\\
&b\, m\, (a\, m\, c) = b\, m\, c = a = a\, m\, c = (b\, m\, a)\, m\, c,
\end{aligned}$$

$$b\,m\,(b\,m\,a) = b\,m\,b = c = b\,m\,a = (b\,m\,b)\,m\,a,$$
$$b\,m\,(b\,m\,b) = b\,m\,c = a = b\,m\,b = (b\,m\,b)\,m\,b,$$
$$b\,m\,(b\,m\,c) = b\,m\,a = b = b\,m\,c = (b\,m\,b)\,m\,c,$$
$$b\,m\,(c\,m\,a) = b\,m\,c = a = c\,m\,a = (b\,m\,c)\,m\,a,$$
$$b\,m\,(c\,m\,b) = b\,m\,a = b = c\,m\,b = (b\,m\,c)\,m\,b,$$
$$b\,m\,(c\,m\,c) = b\,m\,b = c = c\,m\,c = (b\,m\,c)\,m\,c,$$
$$c\,m\,(a\,m\,a) = c\,m\,a = c = c\,m\,a = (c\,m\,a)\,m\,a,$$
$$c\,m\,(a\,m\,b) = c\,m\,b = a = c\,m\,b = (c\,m\,a)\,m\,b,$$
$$c\,m\,(a\,m\,c) = c\,m\,c = b = c\,m\,c = (c\,m\,a)\,m\,c,$$
$$c\,m\,(b\,m\,a) = c\,m\,b = a = a\,m\,a = (c\,m\,b)\,m\,a,$$
$$c\,m\,(b\,m\,b) = c\,m\,c = b = a\,m\,b = (c\,m\,b)\,m\,b,$$
$$c\,m\,(b\,m\,c) = c\,m\,a = c = a\,m\,c = (c\,m\,b)\,m\,c,$$
$$c\,m\,(c\,m\,a) = c\,m\,c = b = b\,m\,a = (c\,m\,c)\,m\,a,$$
$$c\,m\,(c\,m\,b) = c\,m\,a = c = b\,m\,b = (c\,m\,c)\,m\,b,$$
$$c\,m\,(c\,m\,c) = c\,m\,b = a = b\,m\,c = (c\,m\,c)\,m\,c$$

ist m assoziativ.

Wegen

$$a\,m\,b = b = b\,m\,a,$$
$$a\,m\,c = c = c\,m\,a,$$
$$b\,m\,c = a = c\,m\,a$$

gilt $x\,m\,y = y\,m\,x$ für alle $x, y \in \{a, b, c\}$ mit $x \neq y$. Da für $x, y \in \{a, b, c\}$ mit $x = y$ ebenfalls $x\,m\,y = x\,m\,x = y\,m\,x$ gilt, ist m somit kommutativ.

(b) Wegen

$$b\,m\,(a\,m\,a) = b\,m\,b = e \neq c = d\,m\,a = (b\,m\,a)\,m\,a$$

ist m nicht assoziativ. Wegen

$$a\,m\,b = c \neq d = b\,m\,a$$

ist m nicht kommutativ. □

In Satz (6.1)(a)(iv) haben wir gesehen, dass dem Element $1 \in \mathbb{N}$ eine besondere Stellung bzgl. der Multiplikation von natürlichen Zahlen zukommt: Multipliziert man ein Element $n \in \mathbb{N}$ mit 1, egal von welcher Seite, so erhält man als Produkt das Element n zurück. Eine ganz ähnliche Rolle hat das Element $0 \in \mathbb{N}_0$ bzgl. der Addition von $\mathbb{N}_0$, siehe Satz (6.1)(b)(ii): Addiert man 0 zu einem Element $n \in \mathbb{N}_0$, so bekommt man als Summe wieder n. Wir abstrahieren wieder:

(6.8) Definition (neutrales Element)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Ein *neutrales Element* (in X) bzgl. m ist ein Element e in X, welches

$$e\,m\,x = x\,m\,e = x$$

für alle $x \in X$ erfüllt.

(6.9) Beispiel. Es ist 1 ein neutrales Element bzgl. der Verknüpfung $(m, n) \mapsto m \cdot n$ auf $\mathbb{N}$.

(6.10) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist a ein neutrales Element in $\{a, b, c\}$ bzgl. m.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist e ein neutrales Element in $\{a, b, c, d, e\}$ bzgl. m.

Beweis.

(a) Wegen $a\, m\, x = x\, m\, a = x$ für alle $x \in \{a, b, c\}$ ist a ein neutrales Element bzgl. m.

(b) Wegen $e\, m\, x = x\, m\, e = x$ für alle $x \in \{a, b, c, d, e\}$ ist e ein neutrales Element bzgl. m. □

Wir werden nun sehen, dass es bzgl. einer Verknüpfung niemals mehrere neutrale Elemente geben kann.

(6.11) Bemerkung. Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Dann gibt es höchstens ein neutrales Element bzgl. m.

Beweis. Es seien neutrale Elemente e und e' in X bzgl. m gegeben. Da e neutral ist, gilt $emx = x$ für alle $x \in X$, also insbesondere $e\, m\, e' = e'$. Da e' neutral ist, gilt $x\, m\, e' = x$ für alle $x \in X$, also insbesondere $e\, m\, e' = e$. Insgesamt haben wir

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

□

Die Addition auf $\mathbb{N}$ liefert ein Beispiel für eine Verknüpfung bzgl. derer es kein neutrales Element gibt.
Das wesentliche Merkmal, was die ganzen Zahlen von den natürlichen Zahlen unterscheidet, ist das Hinzukommen von negativen Elementen. Diese haben die Eigenschaft, dass sie zu dem entsprechenden positiven Element addiert die Zahl 0, das neutrale Element bzgl. der Addition, ergeben. Ganz ähnlich liefert die Multiplikation mit einem inversen Element in $\mathbb{Q}$ die Zahl 1, das neutrale Element bzgl. der Multiplikation.
Wir abstrahieren von der konkreten Situation:

(6.12) Definition (inverses Element)**.** Es seien eine Menge X, eine Verknüpfung m auf X, ein neutrales Element e bzgl. m und ein $x \in X$ gegeben.

(a) Ein *linksinverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches $y\, m\, x = e$ erfüllt.

(b) Ein *rechtsinverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches $x\, m\, y = e$ erfüllt.

(c) Ein *inverses Element* (in X) zu x bzgl. m ist ein Element y in X, welches links- und rechtsinvers zu x bzgl. m ist.

(6.13) Beispiel. Es ist $\frac{4}{3}$ ein zu $\frac{3}{4}$ inverses Element bzgl. der Verknüpfung $(m, n) \mapsto m \cdot n$ auf $\mathbb{Q}$.

(6.14) Beispiel.

(a) Es seien verschiedene Objekte a, b, c gegeben und auf $\{a, b, c\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Dann ist b ein zu c inverses Element in $\{a, b, c\}$ bzgl. m.

(b) Es seien verschiedene Objekte a, b, c, d, e gegeben und auf $\{a, b, c, d, e\}$ sei eine Verknüpfung m durch folgende Verknüpfungstafel gegeben:

m	a	b	c	d	e
a	b	c	d	e	a
b	d	e	a	c	b
c	e	d	b	a	c
d	c	a	e	b	d
e	a	b	c	d	e

Dann ist b ein zu b inverses Element in $\{a, b, c, d, e\}$ bzgl. m. Ferner ist c linksinvers zu a und d rechtsinvers zu a bzgl. m.

Beweis.

(a) Nach Beispiel (6.10)(a) ist a ein neutrales Element bzgl. m. Wegen $b\,m\,c = c\,m\,b = a$ ist daher b ein zu c inverses Element bzgl. m.

(b) Nach Beispiel (6.10)(b) ist e ein neutrales Element bzgl. m. Wegen $b\,m\,b = e$ ist daher b ein zu b inverses Element bzgl. m. Wegen $c\,m\,a = e$ ist ferner c linksinvers zu a bzgl. m und wegen $a\,m\,d = e$ ist d rechtsinvers zu a bzgl. m. □

Wir haben hier zwischen linksinversen, rechtsinversen und inversen Elementen unterschieden, da es Situationen gibt, in welchen ein Element ein linksinverses Element, aber kein rechtsinverses Element hat, und umgekehrt. Ist die betrachtete Verknüpfung assoziativ, so kann es jedoch nicht passieren, dass ein Element verschiedene links- und rechtsinverse Elemente hat:

(6.15) Bemerkung. Es seien eine Menge X, eine assoziative Verknüpfung m auf X und ein neutrales Element e bzgl. m gegeben. Ferner seien $x \in X$, ein linksinverses Element y und ein rechtsinverses Element y' zu x bzgl. m gegeben. Dann gilt

$$y = y'.$$

Beweis. Da e neutral bzgl. m ist, gilt $y\,m\,e = y$ und $e\,m\,y' = y'$. Da y linksinvers zu x bzgl. m ist, gilt $y\,m\,x = e$. Da y' rechtsinvers zu x bzgl. m ist, gilt $x\,m\,y' = e$. Unter Ausnutzung der Assoziativität von m erhalten wir

$$y = y\,m\,e = y\,m\,(x\,m\,y') = (y\,m\,x)\,m\,y' = e\,m\,y' = y'.$$ □

Man vergleiche den Beweis der vorangegangenen Bemerkung (6.15) mit dem Beweis von Bemerkung (3.19).

(6.16) Korollar. Es seien eine Menge X, eine assoziative Verknüpfung m auf X, ein neutrales Element e bzgl. m und ein $x \in X$ gegeben. Dann gibt es höchstens ein inverses Element zu x bzgl. m.

Beweis. Es seien inverse Elemente y und y' zu x gegeben. Dann ist y insbesondere linksinvers und y' insbesondere rechtsinvers zu x bzgl. m, so dass aus Bemerkung (6.15) bereits $y = y'$ folgt. □

Halbgruppen und Monoide

Als nächstes wollen wir uns davon lösen, Verknüpfungen als eigenständige Objekte zu betrachten. Wir wollen den Standpunkt einnehmen, dass Verknüpfungen „fest“ zu einer Menge dazugehören, und wollen die Menge zusammen mit den Verknüpfungen als eine gemeinsame „algebraische Struktur“ ansehen.
Obwohl wir auf $\mathbb{N}$ und $\mathbb{N}_0$ mehrere uns vertraute Verknüpfungen haben, begnügen wir uns zunächst mit „einfacheren“ Strukturen und studieren Mengen, die mit genau einer Verknüpfung versehen sind und einige der gerade eingeführten Eigenschaften erfüllen. Mengen, welche mit zwei miteinander verträglichen Verknüpfungen ausgestattet sind, werden dann später eingeführt.

(6.17) Definition (Halbgruppe, kommutative Halbgruppe, Monoid)**.**

(a) Eine *Halbgruppe* besteht aus einer Menge M zusammen mit einer assoziativen Verknüpfung m auf M. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Halbgruppe als auch die unterliegende Menge mit M. Die Verknüpfung m wird *Multiplikation* (oder *Halbgruppenverknüpfung*) von M genannt.

Für eine Halbgruppe M mit Multiplikation m schreiben wir $\cdot = \cdot^M := m$ und $xy = x \cdot y$ für $x, y \in M$.

(b) Eine Halbgruppe M heißt *kommutativ*, falls die Multiplikation von M kommutativ ist.

(c) Ein *Monoid* ist eine Halbgruppe M, welche ein neutrales Element bzgl. $\cdot^M$ besitzt. Die Halbgruppenverknüpfung eines Monoids M wird auch *Monoidverknüpfung* von M genannt. Das neutrale Element bzgl. der Multiplikation wird auch *Eins* (oder *Einselement*) von M genannt und als $1 = 1^M$ notiert.

Bei der Festlegung „$\cdot = \cdot^M := m$“ in Definition (6.17)(a) für die Multiplikation einer Halbgruppe handelt es sich um eine Notation, um in einer abstrakt (d.h. nicht in einem konkreten Beispiel) gegebenen Halbgruppe einfach von der Verknüpfung sprechen zu können und diese nicht immer explizit erwähnen zu müssen. In der Regel werden wir also von einer „Halbgruppe M“ anstatt von einer „Halbgruppe M mit Multiplikation m“ sprechen, die Multiplikation als implizit gegeben ansehen und diese dann mit dem Symbol $\cdot$ bezeichnen. Die Bezeichnung $\cdot^M$ werden wir nur dann verwenden, wenn wir explizit darauf hinweisen möchten, dass diese Multiplikation zu M gehört (etwa, wenn wir mehrere Halbgruppen auf einmal betrachten); in der Regel werden wir jedoch darauf verzichten.
Die Notationen „$\cdot$“ und „1“ sowie auch die Bezeichnungen „Multiplikation“ und „Eins“ sind von Beispielen wie dem der natürlichen Zahlen motiviert. Es gibt auch andere Beispiele, wo die Halbgruppenverknüpfung keine Multiplikation im vertrauten Sinne ist. In diesen konkret gegebenen Beispielen verwenden wir weiterhin die jeweils vorliegende Notation, die durch das Beispiel mitgebracht wird; siehe insbesondere Bemerkung (12.1).
Mit Hilfe der Standardnotation in einer Halbgruppe M liest sich die Assoziativität der Multiplikation wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.

Ist eine Halbgruppe M kommutativ, so gilt neben der Assoziativität zusätzlich noch:

- *Kommutativität.* Für $x, y \in M$ ist $xy = yx$.

Mit Hilfe der Standardnotation in einem Monoid M lesen sich dessen *Axiome*, d.h. dessen definierende Eigenschaften, wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in M$ derart, dass für $x \in M$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für $x \in M$.

Da Monoide insbesondere Halbgruppen sind, erhalten wir auch den Begriff eines *kommutativen Monoids*.
Neben der Multiplikation auf den natürlichen Zahlen ist auch die Addition assoziativ und kommutativ. Für kommutative Halbgruppen, Monoide und Gruppen haben sich daher noch andere Bezeichnungen und Schreibweisen eingebürgert:

(6.18) Definition (abelsche Halbgruppe, abelsches Monoid)**.**

(a) Eine *abelsche Halbgruppe* ist eine kommutative Halbgruppe A mit Halbgruppenverknüpfung $+ = +^A$, genannt *Addition* von A.

(b) Ein *abelsches Monoid* ist eine abelsche Halbgruppe A, welche ein neutrales Element bzgl. $+^A$ besitzt. Das neutrale Element bzgl. der Addition wird auch *Null* (oder *Nullelement*) von A genannt und als $0 = 0^A$ notiert.

Eine abelsche Halbgruppe ist also strukturell gesehen das Gleiche wie eine kommutative Halbgruppe; wir verwenden lediglich in abstrakten abelschen Halbgruppen eine andere Standardnotation: Abstrakte Halbgruppen (die ggf. auch mal kommutativ sein dürfen, aber im Allgemeinen nicht müssen) werden multiplikativ geschrieben, abstrakte abelsche Halbgruppen werden additiv geschrieben.
Insbesondere gilt: Alle Aussagen über beliebige Halbgruppen und über kommutative Halbgruppen (in multiplikativer Notation geschrieben) bleiben auch für abelsche Halbgruppen (in additiver Notation geschrieben) korrekt. Umgekehrt bleiben alle Aussagen über abelsche Halbgruppen (in additiver Notation geschrieben) auch für kommutative Halbgruppen (in multiplikativer Notation geschrieben) korrekt. Bei der Verwendung solcher Aussagen muss gegebenenfalls nur die jeweilige Notation angepasst werden. In der Regel werden wir getroffene Aussagen über Halbgruppen nicht für abelsche Halbgruppen in additiver Notation wiederholen.
Mit Hilfe der Standardnotation in einer abelschen Halbgruppe A lesen sich deren Axiome wie folgt:

- *Assoziativität.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.

- *Kommutativität.* Für $x, y \in A$ ist $x + y = y + x$.

Die Axiome eines abelschen Monoids A sind die eines kommutativen Monoids in additiver Notation:

- *Assoziativität.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in A$ derart, dass für $x \in A$ stets $n + x = x + n = x$ gilt. Dieses n ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für $x \in A$.
- *Kommutativität.* Für $x, y \in A$ ist $x + y = y + x$.

Vom Rechnen in den natürlichen Zahlen sind wir es gewohnt, bei Produkten aus mehreren Faktoren bzw. Summen aus mehreren Summanden keine Klammern zu setzen. Dies ist durch die Assoziativität gerechtfertigt, da verschiedene Klammerungen zum selben Wert führen würden. Wir übertragen diese Konvention auf den allgemeinen Fall:

(6.19) Konvention. Wegen der Assoziativität der Multiplikation einer Halbgruppe bzw. der Addition einer abelschen Halbgruppe kommt es bei iterierter Bildung nicht auf die Klammerung an. Im Regelfall lassen wir daher die Klammern im Folgenden weg.

Nachdem wir alle in Satz (6.1)(a), (b) auftauchenden Phänomene analysiert und von den konkreten Beispielen $\mathbb{N}$ und $\mathbb{N}_0$ abstrahiert haben, lassen sich diese nun kurz wie folgt reformulieren.

(6.20) Beispiel.

(a) (i) Die Menge $\mathbb{N}$ zusammen mit der üblichen Addition ist eine abelsche Halbgruppe, aber kein abelsches Monoid.

(ii) Die Menge $\mathbb{N}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid. Die Eins von $\mathbb{N}$ ist die übliche Eins.

(b) (i) Die Menge $\mathbb{N}_0$ zusammen mit der üblichen Addition ist ein abelsches Monoid. Die Null von $\mathbb{N}_0$ ist die übliche Null.

(ii) Die Menge $\mathbb{N}_0$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid. Die Eins von $\mathbb{N}_0$ ist die übliche Eins.

(6.21) Beispiel. Es gibt ein nicht-kommutatives Monoid mit genau drei Elementen, dessen Multiplikation durch folgende Verknüpfungstafel gegeben ist.

$\cdot$	1	c_1	c_2
1	1	c_1	c_2
c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2

Das Stringmonoid

Nach der bis hierher erfolgten abstrakten Begriffsbildung können wir nun das folgende Beispiel untersuchen, in welchem sich die soeben eingeführte Struktur eines Monoids erkennen lässt.

(6.22) Bemerkung. Es sei eine Menge X gegeben. Die Menge $\dot{\bigcup}_{k \in \mathbb{N}_0} X^k$ wird zu einem Monoid mit Monoidverknüpfung

$$((x_1, \ldots, x_k), (y_1, \ldots, y_l)) \mapsto (x_1, \ldots, x_k, y_1, \ldots, y_l)$$

und Einselement $( )$.

(6.23) Definition (Stringmonoid)**.** Es sei eine Menge X gegeben. Das Monoid mit unterliegender Menge $\dot{\bigcup}_{k \in \mathbb{N}_0} X^k$ und der Verknüpfung $((x_1, \ldots, x_k), (y_1, \ldots, y_l)) \mapsto (x_1, \ldots, x_k, y_1, \ldots, y_l)$ aus Bemerkung (6.22) wird *Stringmonoid* (oder *freies Monoid* oder *Wortmonoid*) über X genannt und als X^* notiert. Die Monoidverknüpfung von X^* wird *Konkatenation* (oder *Aneinanderhängung*) genannt. Ein Element von X^* wird *String* (oder *Zeichenkette*) in X genannt. Das Einselement von X^* wird *leerer String* in X genannt und als $\varepsilon := ( )$ notiert.
Für einen String $(x_1, \ldots, x_k)$ in X schreiben wir $x_1 \ldots x_k := (x_1, \ldots, x_k)$.

(6.24) Beispiel.

(a) Es sei ein Objekt a gegeben. Dann ist das Stringmonoid über $\{a\}$ gegeben durch

$$\{a\}^* = \{\varepsilon, a, aa, aaa, \dots\}.$$

(b) Es seien verschiedene Objekte a und b gegeben. Dann ist das Stringmonoid über $\{a, b\}$ gegeben durch

$$\{a, b\}^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, \dots\}.$$

Die Wichtigkeit des Stringmonoids, insbesondere in der (theoretischen) Informatik, ergibt sich durch die Betrachtung von Teilmengen:

(6.25) Definition (Sprache)**.** Es sei eine Menge X gegeben. Eine (*formale*) *Sprache* über X ist eine Teilmenge von X^*.
Es sei eine Sprache L über X gegeben. Die Menge X wird das *Alphabet* von L. Ein Element von X wird *Zeichen* (oder *Buchstabe*) in L genannt. Ein Element von L wird *Wort* in L genannt.

Da für eine Menge X auch das Stringmonoid X^* eine Sprache über X ist, werden die Strings in X, d.h. die Elemente von X^*, auch Wörter in X^* genannt.
Als Anwendungsbeispiel geben wir eine mögliche Formalisierung für die Sprache der Aussagenlogik, vgl. Definition (1.1), an:

(6.26) Anwendungsbeispiel. Das Alphabet der Aussagenlogik sei modelliert als Menge X gegeben durch

$$X = \{A_1, A_2, A_3, \dots\} \dot\cup \{0, 1, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\} \dot\cup \{(,)\}.$$

Die Sprache der Aussagenlogik lässt sich dann als (formale) Sprache über X auffassen.

Auch eine beliebige Programmiersprache, wie z.B. C, lässt sich als formale Sprache modellieren:

(6.27) Anwendungsbeispiel. Die Befehle und erlaubten Zeichen einer Programmiersprache seien als Elemente einer Menge X modelliert. Quelltexte für diese Programmiersprache lassen sich dann als Wörter einer Sprache über X auffassen.

Als kurzen Ausblick skizzieren wir das *Wortproblem*: Es sei eine Menge X gegeben. Für einen String x in X bezeichnen wir einen String x' in X als einen *Unterstring* (oder *Teilstring*) von x, falls es Strings p und s in X mit $x = px's$ gibt.
Ferner sei eine symmetrische Relation r auf X^* gegeben. Die bzgl. r in Relation stehenden Strings in X fassen wir als „Ersetzungsregeln“ im folgenden Sinn auf: Es seien Strings x und y in X gegeben. Wir sagen, dass x und y durch eine elementare Ersetzung auseinander hervorgehen, wenn es Strings p, s, x', y' in X mit $x = px's$, $y = py's$ und $x'\ r\ y'$ gibt, d.h. falls y durch Ersetzung des Unterstrings x' von x durch den Unterstring y' entsteht und umgekehrt.
Das Wortproblem ist nun folgendes: Es seien Strings x und y in X gegeben. Lässt sich überprüfen, ob x und y durch eine endliche Folge von elementaren Ersetzungen auseinander hervorgehen? In vielen Fällen ist dieses Problem nachweislich unentscheidbar.
Es sei L_x die bzgl. Inklusion kleinste Sprache, welche zum einen x enthält und welche zum anderen mit jedem Wort z in L_x auch alle diejenigen Strings in X enthält, die durch eine elementare Ersetzung aus z hervorgehen. ([1])
Mit Hilfe von L_x lässt sich das Wortproblem wie folgt umformulieren: Lässt sich überprüfen, ob y ein Wort von L_x ist?

[1] D.h. einerseits ist L_x eine Sprache derart, dass x in L_x enthalten ist, und so, dass mit jedem Wort z in L_x auch alle diejenigen Strings in X enthalten sind, welche durch eine elementare Ersetzung aus z hervorgehen, und andererseits gilt für jede Sprache L derart, dass x in L_x enthalten ist, und so, dass mit jedem Wort z in L_x auch alle diejenigen Strings in X enthalten sind, bereits, dass jedes Wort in L_x auch ein Wort von L ist.

Invertierbare Elemente

Wir legen eine Sprechweise für die Existenz eines inversen Elements bzgl. der Monoidverknüpfung in einem gegebenen Monoid fest:

(6.28) Definition (Invertierbarkeit)**.**

(a) Es sei ein Monoid M gegeben. Ein Element x in M heißt *invertierbar* in M (oder eine *Einheit* von M), falls es ein inverses Element zu x bzgl. $\cdot$ gibt. Das zu einem invertierbaren Element x in M bzgl. $\cdot$ inverse Element y wird auch das *Inverse* (oder das *inverse Element*) zu x in M genannt und als $x^{-1} = (x^{-1})^M := y$ notiert.

Die *Menge der invertierbaren Elemente* in M bezeichnen wir mit

$$M^\times = \{x \in M \mid x \text{ ist invertierbar}\}.$$

(b) Es sei ein abelsches Monoid A gegeben. Ein Element x in A heißt *negierbar* in A, falls es ein inverses Element zu x bzgl. $+^A$ gibt. Das zu einem negierbaren Element x in A bzgl. $+^A$ inverse Element y wird auch das *Negative* (oder das *negative Element*) zu x in A genannt und als $-x = (-x)^A := y$ notiert.

Die etwas ungewöhnlich aussehende Notation $(x^{-1})^M$ in Definition (6.28)(a) soll lediglich deutlich machen, in welchem Monoid wir das Inverse zu x bilden – nämlich gerade im Monoid M. Wir werden diese Notation nur dann verwenden, wenn wir explizit darauf hinweisen wollen, in welchem Monoid das Inverse gebildet wird.
Bei additiv geschriebenen abelschen Monoiden wird die Notation $M^\times$ in aller Regel nicht verwendet.

(6.29) Beispiel.

(a) Es ist ${\mathbb{N}_0}^\times = \{1\}$, d.h. das einzige invertierbare Element in $\mathbb{N}_0$ (bzgl. der üblichen Multiplikation) ist 1.

(b) Das einzige negierbare Element in $\mathbb{N}_0$ (bzgl. der üblichen Addition) ist 0.

(c) Für jede Menge X ist $(X^*)^\times = \{\varepsilon\}$.

Wir wollen einige einfache Eigenschaften von invertierbaren Elementen herleiten.

(6.30) Proposition. Es sei ein Monoid M gegeben.

(a) Für $x, y \in M^\times$ ist auch $xy \in M^\times$ mit $(xy)^{-1} = y^{-1}x^{-1}$.

(b) Es ist $1 \in M^\times$ mit $1^{-1} = 1$.

(c) Für $x \in M^\times$ ist auch $x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$.

Beweis. Dies lässt sich analog zu Proposition (3.21) beweisen. Die Details seien dem Leser zur Übung überlassen. □

(6.31) Bemerkung. Es seien ein Monoid M und $a \in M^\times$, $b, x \in M$ gegeben.

(a) Genau dann gilt $ax = b$, wenn $x = a^{-1}b$ ist.

(b) Genau dann gilt $xa = b$, wenn $x = ba^{-1}$ ist.

Beweis.

(a) Wenn $ax = b$ gilt, dann auch

$$x = 1x = a^{-1}ax = a^{-1}b.$$

Umgekehrt, wenn $x = a^{-1}b$ ist, dann haben wir nach Proposition (6.30)(c) auch

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

(b) Dies lässt sich analog zu (a) beweisen. □

(6.32) Korollar. Es sei ein Monoid M gegeben.

(a) Es seien $a \in M^\times$, $x, y \in M$ gegeben. Wenn $ax = ay$ oder $xa = ya$ gilt, dann ist $x = y$.

(b) Es seien $a \in M^\times$, $x \in M$ gegeben. Wenn $ax = a$ oder $xa = a$ gilt, dann ist $x = 1$.

Beweis.

(a) Es gelte $ax = ay$; der andere Fall wird analog bewiesen. Nach Bemerkung (6.31)(a) ist dann

$$x = a^{-1}ay = 1y = y.$$

(b) Es gelte $ax = a$; der andere Fall wird analog bewiesen. Dann haben wir $ax = a1$ und also $x = 1$ nach (a). □

Gruppen

Im abelschen Monoid der ganzen Zahlen $\mathbb{Z}$ zusammen mit der üblichen Addition ist jedes Element negierbar, vgl. Satz (6.1)(c)(iii). Für eine solche Situation benutzen wir einen neuen Begriff, den wir jetzt einführen wollen.

(6.33) Definition ((abelsche) Gruppe)**.**

(a) Eine *Gruppe* ist ein Monoid G, in welchem jedes Element von G invertierbar ist. Die Monoidverknüpfung einer Gruppe G wird auch *Gruppenverknüpfung* von G genannt.

(b) Eine *abelsche Gruppe* ist ein abelsches Monoid A, in welchem jedes Element von A negierbar ist.

Die Axiome einer Gruppe G in Standardnotation lesen sich insgesamt wie folgt:

- *Assoziativität.* Für $x, y, z \in G$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in G$ derart, dass für $x \in G$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für $x \in G$.
- *Existenz der Inversen.* Für jedes $x \in G$ existiert ein $y \in G$ mit $yx = xy = 1$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Ist G kommutativ, so gilt zusätzlich noch:

- *Kommutativität.* Für $x, y \in G$ ist $xy = yx$.

Die Axiome einer abelschen Gruppe A sind die einer kommutativen Gruppe in additiver Notation. Wir betonen noch einmal: Jede kommutative Gruppe lässt sich als abelsche Gruppe auffassen und umgekehrt – strukturell gesehen sind es die gleichen Objekte, wir bringen durch die unterschiedlichen Terminologien lediglich zum Ausdruck, welche Notation wir verwenden. Insbesondere bleiben alle Aussagen über Gruppen auch für abelsche Gruppen gültig, sie müssen nur in der Notation angepasst werden.
Wir fassen einige Eigenschaften aus Satz (6.1)(c), (d) mit Hilfe der neuen Terminologien noch einmal zusammen:

(6.34) Beispiel.

(a) (i) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Addition ist eine abelsche Gruppe. Die Null von $\mathbb{Z}$ ist die übliche Null. Für $x \in \mathbb{Z}$ ist das Negative zu x in $\mathbb{Z}$ das übliche Negative.

(ii) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid, aber keine Gruppe. Die Eins von $\mathbb{Z}$ ist die übliche Eins.

(b) (i) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Addition ist eine abelsche Gruppe. Die Null von $\mathbb{Q}$ ist die übliche Null. Für $x \in \mathbb{Q}$ ist das Negative zu x in $\mathbb{Q}$ das übliche Negative.

(ii) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Multiplikation ist ein kommutatives Monoid, aber keine Gruppe. Die Eins von $\mathbb{Q}$ ist die übliche Eins.

(iii) Die Menge $\mathbb{Q} \setminus \{0\}$ zusammen mit der üblichen Multiplikation ist eine kommutative Gruppe. Die Eins von $\mathbb{Q} \setminus \{0\}$ ist die übliche Eins. Für $x \in \mathbb{Q} \setminus \{0\}$ ist das Inverse zu x in $\mathbb{Q} \setminus \{0\}$ das übliche Inverse.

(6.35) Konvention. Wenn wir in Zukunft von der abelschen Gruppe $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Addition. Wenn wir vom kommutativen Monoid $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Multiplikation. Ähnlich für $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Q}$, $\mathbb{R}$.

(6.36) Beispiel. Es gibt eine nicht-kommutative Gruppe mit genau sechs Elementen, dessen Multiplikation durch folgende Verknüpfungstafel gegeben ist.

$\cdot$	1	τ_1	τ_2	τ_3	σ_1	σ_2
1	1	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	1	σ_2	σ_1	τ_3	τ_2
τ_2	τ_2	σ_1	1	σ_2	τ_1	τ_3
τ_3	τ_3	σ_2	σ_1	1	τ_2	τ_1
σ_1	σ_1	τ_2	τ_3	τ_1	σ_2	1
σ_2	σ_2	τ_3	τ_1	τ_2	1	σ_1

Wie von den ganzen Zahlen bekannt, liefert die Existenz von negativen Elementen in einer abelschen Gruppe eine neue Verknüpfung:

(6.37) Definition (Subtraktion)**.** Es sei eine abelsche Gruppe A gegeben. Die Verknüpfung $(x, y) \mapsto x + (-y)$ auf A wird *Subtraktion* von A genannt und als $-$ notiert.

Wir betonen, dass die Addition einer abelschen Gruppe A ein Teil der Daten von A ist (d.h. A besteht aus der unterliegenden Menge, die unter Missbrauch der Notation ebenfalls mit A bezeichnet wird, und der Addition). Hingegen wird die Subtraktion mit Hilfe der Addition und den negativen Elementen definiert und ist insbesondere somit durch die Daten (unterliegende Menge und Addition) eindeutig festgelegt.
Da Gruppen (multiplikativ geschrieben) nicht kommutativ sein müssen, können wir die analoge Verknüpfung $(x, y) \mapsto x : y$, wie etwa aus dem Beispiel $\mathbb{Q} \setminus \{0\}$ bekannt, nicht bilden: für Gruppenelemente x und y muss im Allgemeinen nicht $xy^{-1} = y^{-1}x$ gelten. Genauer gesagt erhalten wir zwei Verknüpfungen, welche im Allgemeinen nicht übereinstimmen und für welche sich keine neue Notation eingebürgert hat.

Die Gruppe der invertierbaren Elemente

Während in einer Gruppe jedes Element invertierbar ist, haben wir in einem beliebigen Monoid auch nicht-invertierbare Elemente. In Beispiel (6.34)(b)(iii) haben wir gesehen, dass wir eine Gruppe erhalten, wenn wir die Multiplikation des Monoids $\mathbb{Q}$ auf die Menge der invertierbaren Elemente $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ einschränken. Dieses Resultat lässt sich auf beliebige Monoide verallgemeinern:

(6.38) Bemerkung. Für jedes Monoid M wird $M^\times$ eine Gruppe, wobei die Multiplikation auf $M^\times$ durch

$$x \cdot^{M^\times} y = x \cdot^{M} y$$

für $x, y \in M$ gegeben ist.

Beweis. Dies sei dem Leser zur Übung überlassen. □

(6.39) Definition (Gruppe der invertierbaren Elemente)**.** Es sei ein Monoid M gegeben. Die Gruppe $M^\times$ mit der Multiplikation aus Bemerkung (6.38) heißt *Gruppe der invertierbaren Elemente* (oder *Einheitengruppe*) von M.

Ein Monoid G ist also genau dann eine Gruppe, wenn $G^\times = G$ ist.

(6.40) Beispiel.

(a) Es ist

$$\mathbb{Z}^\times = \{1, -1\}.$$

(b) Es ist

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}.$$

Ringe und Körper

Bei den uns vertrauten Strukturen spielen jeweils Addition und Multiplikation eine wichtige Rolle. Aus diesem Grund wollen wir als nächstes algebraische Strukturen betrachten, deren unterliegende Mengen mit zwei Verknüpfungen versehen sind.

(6.41) Definition (Ring, kommutativer Ring, Körper)**.**

(a) Ein *Ring* (genauer *unitärer Ring* oder *Ring mit Eins* oder *Ring mit Einselement*) besteht aus einer abelschen Gruppe R zusammen mit einer Verknüpfung m auf R so, dass die unterliegende Menge von R ein Monoid mit Multiplikation m wird und so, dass folgendes Axiom gilt.

- *Distributivität.* Für alle $x, y, z \in R$ ist

$$x\, m\, (y + z) = (x\, m\, y) + (x\, m\, z),$$
$$(x + y)\, m\, z = (x\, m\, z) + (y\, m\, z).$$

Unter Missbrauch der Notation bezeichnen wir sowohl den besagten Ring als auch die unterliegende abelsche Gruppe mit R. Die Verknüpfung m wird *Multiplikation* von R genannt.

Für einen Ring R mit Multiplikation m schreiben wir wie üblich $\cdot = \cdot^R := m$ und $xy = x \cdot y$ für $x, y \in R$.

(b) Ein Ring R heißt *kommutativ*, falls die Multiplikation von R kommutativ ist.

(c) Ein *Körper* ist ein kommutativer Ring K, in welchem $1 \neq 0$ gilt und in welchem jedes Element von $K \setminus \{0\}$ invertierbar (bzgl. der Multiplikation $\cdot^K$) ist.

(6.42) Konvention. In Ringen lassen wir die Klammern um Produkte meistens weg, d.h. es gelte *Punkt- vor Strichrechnung.*

Wir verwenden die in Definition (6.18)(a) bzw. Definition (6.17)(a) eingeführten Notationen für die Addition einer abelschen Halbgruppe (und also insbesondere einer abelschen Gruppe) bzw. für die Multiplikation einer Halbgruppe (und also insbesondere eines Monoids) auch weiterhin für Ringe. Ebenso verwenden wir die Notationen und Begriffe für die neutralen und inversen Elemente bzgl. dieser Verknüpfungen, vgl. Definition (6.28)(a) und Definition (6.37).
Die Axiome eines Rings R in Standardnotation lesen sich also wie folgt:

- *Assoziativität der Addition.* Für $x, y, z \in R$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in R$ derart, dass für $x \in R$ stets $n + x = x + n = x$ gilt. Dieses n ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in R$.
- *Existenz der Negativen.* Für jedes $x \in R$ existiert ein $y \in R$ mit $y + x = x + y = 0$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- *Kommutativität der Addition.* Für $x, y \in R$ ist $x + y = y + x$.
- *Assoziativität der Multiplikation.* Für $x, y, z \in R$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in R$ derart, dass für $x \in R$ stets $ex = xe = x$ gilt. Dieses e ist nach Bemerkung (6.11) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in R$.
- *Distributivität.* Für $x, y, z \in R$ ist $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$.

Ist R kommutativ, so gilt zusätzlich noch:

- *Kommutativität der Multiplikation.* Für $x, y \in R$ ist $xy = yx$.

Ist R ein Körper, so ist R kommutativ und es gilt ferner noch:

- *Existenz der Inversen.* Es ist $1 \neq 0$. Für jedes $x \in K \setminus \{0\}$ existiert ein $y \in K$ mit $yx = xy = 1$. Dieses y ist nach Korollar (6.16) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Selbstverständlich bleiben alle Aussagen über (abelsche) Gruppen für die einem Ring unterliegende abelsche Gruppe, bestehend aus der unterliegenden Menge zusammen mit der Addition des Rings, sowie alle Aussagen über Monoide für das einem Ring unterliegende Monoid, bestehend aus der unterliegenden Menge zusammen mit der Multiplikation des Rings, gültig.
Mit Hilfe der Begriffe aus Definition (6.41) lassen sich die Aussagen aus Satz (6.1)(c), (d) noch knapper zusammenfassen:

(6.43) Beispiel.

(a) Die Menge $\mathbb{Z}$ zusammen mit der üblichen Addition und der üblichen Multiplikation ist ein kommutativer Ring, aber kein Körper. Die Null von $\mathbb{Z}$ ist die übliche Null und die Eins von $\mathbb{Z}$ ist die übliche Eins. Für $x \in \mathbb{Z}$ ist das Negative zu x in $\mathbb{Z}$ das übliche Negative.

(b) Die Menge $\mathbb{Q}$ zusammen mit der üblichen Addition und der üblichen Multiplikation ist ein Körper. Die Null von $\mathbb{Q}$ ist die übliche Null und die Eins von $\mathbb{Q}$ ist die übliche Eins. Für $x \in \mathbb{Q}$ ist das Negative zu x in $\mathbb{Q}$ das übliche Negative und für $x \in \mathbb{Q} \setminus \{0\}$ ist das Inverse zu x in $\mathbb{Q}$ das übliche Inverse.

(6.44) Konvention. Wenn wir in Zukunft vom (kommutativen) Ring $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der üblichen Addition und der üblichen Multiplikation. Ähnlich für $\mathbb{Q}$ und $\mathbb{R}$.

(6.45) Beispiel. Es gibt einen Körper mit genau zwei Elementen, der Null 0 und der Eins 1, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(6.46) Beispiel. Es gibt einen nicht-kommutativen Ring mit genau acht Elementen, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind.

$+$	0	1	e_1	e_2	n	u	s_1	s_2
0	0	1	e_1	e_2	n	u	s_1	s_2
1	1	0	e_2	e_1	u	n	s_2	s_1
e_1	e_1	e_2	0	1	s_1	s_2	n	u
e_2	e_2	e_1	1	0	s_2	s_1	u	n
n	n	u	s_1	s_2	0	1	e_1	e_2
u	u	n	s_2	s_1	1	0	e_2	e_1
s_1	s_1	s_2	n	u	e_1	e_2	0	1
s_2	s_2	s_1	u	n	e_2	e_1	1	0

$\cdot$	0	1	e_1	e_2	n	u	s_1	s_2
0	0	0	0	0	0	0	0	0
1	0	1	e_1	e_2	n	u	s_1	s_2
e_1	0	e_1	e_1	0	n	s_1	s_1	n
e_2	0	e_2	0	e_2	0	e_2	0	e_2
n	0	n	0	n	0	n	0	n
u	0	u	e_1	s_2	n	1	s_1	e_2
s_1	0	s_1	e_1	n	n	e_1	s_1	0
s_2	0	s_2	0	s_2	0	s_2	0	s_2

Eine Axiomatisierung der Eigenschaften von $\mathbb{N}_0$, welche Addition und Multiplikation involviert, wird manchmal *Halbring* genannt. Da eine solche Struktur für uns im Folgenden nur von untergeordnetem Interesse sein würde, werden wir solche Strukturen nicht einführen und genauer betrachten.
Im Folgenden halten wir einige elementare Eigenschaften von Ringen und Körpern fest.

(6.47) Proposition. Es sei ein Ring R gegeben.

(a) Für $a \in R$ gilt $a \cdot 0 = 0 \cdot a = 0$.

(b) Für $a, b \in R$ gilt $a(-b) = (-a)b = -ab$.

(c) Für $a, b \in R$ gilt $(-a)(-b) = ab$.

Beweis.

(a) Für $a \in R$ gilt

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

und damit $a \cdot 0 = 0$ nach Korollar (6.32)(b).

(b) Für $a, b \in R$ gilt

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

nach (a) und damit $-ab = a(-b)$. Die andere Gleichung zeigt man analog.

(c) Für $a, b \in R$ gilt

$$(-a)(-b) = -a(-b) = -(-ab) = ab$$

nach (b). □

Die Ringe $\mathbb{Z}$ und $\mathbb{Q}$ sind nullteilerfrei, eine Eigenschaft, welche nicht in jedem Ring gilt. Nullteilerfreie kommutative Ringe sind unter folgendem Namen bekannt:

(6.48) Definition (Integritätsbereich)**.** Ein *Integritätsbereich* ist ein kommutativer Ring R mit $1 \neq 0$ und so, dass folgende Eigenschaft gilt:

- *Nullteilerfreiheit.* Für $a, b \in R$ aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt.

(6.49) Beispiel. Es gibt einen kommutativen Ring mit genau vier Elementen, dessen Addition und Multiplikation durch folgende Verknüpfungstafeln gegeben sind, welcher kein Integritätsbereich ist.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Der Ring aus Beispiel (6.46) liefert ein Beispiel für einen nicht-kommutativen Ring, welcher nicht nullteilerfrei ist, d.h. in welchem es zwei (nicht notwendigerweise verschiedene) von Null verschiedene Elemente gibt, deren Produkt Null ist.

(6.50) Proposition. Jeder Körper ist ein Integritätsbereich.

Beweis. Es seien ein Körper K und $a, b \in K$ mit $ab = 0$ gegeben. Ferner gelte $a \neq 0$. Dann ist $a \in K^\times$, nach Bemerkung (6.31)(a) und Proposition (6.47)(a) folgt also $b = a^{-1}0 = 0$. □

(6.51) Beispiel. Der Ring $\mathbb{Z}$ ist ein Integritätsbereich.

Beweis. Nach Proposition (6.50) ist $\mathbb{Q}$ als Körper ein Integritätsbereich, d.h. für $a, b \in \mathbb{Q}$ folgt aus $ab = 0$ stets $a = 0$ oder $b = 0$. Wegen $\mathbb{Z} \subseteq \mathbb{Q}$ folgt dann aber insbesondere für $a, b \in \mathbb{Z}$ aus $ab = 0$ stets $a = 0$ oder $b = 0$. Folglich ist auch $\mathbb{Z}$ ein Integritätsbereich. □

(6.52) Bemerkung. Es sei ein kommutativer Ring R mit $1 \neq 0$ gegeben. Die folgenden Bedingungen sind äquivalent:

(a) Es ist R ein Integritätsbereich.

(b) Für $a, x, y \in R$ folgt aus $ax = ay$ stets $a = 0$ oder $x = y$.

Beweis. Dies sei dem Leser zur Übung überlassen. □