Kapitel 2

Algebraische Grundstrukturen

§6 Gruppen

In den Beispielen in Kapitel 0 hatten wir Mengen betrachtet, auf denen eine Addition "+" erklärt war. Wir hatten gesehen, daß die Rechengesetze in den betrachteten Fällen weitgehend übereinstimmten. Im folgenden wollen wir uns von den konkreten "Modellen" lösen und diese gemeinsamen Eigenschaften untersuchen.

Wir werden am Beispiel der Gruppen ein Stück weit den axiomatischen Aufbau einer Theorie verfolgen. Wir starten mit einem Axiomensystem, das aus bestimmten ausgewählten Rechenregeln besteht. Wir werden dann weitere Regeln entwickeln, Teilstrukturen studieren und Abbildung zwischen Gruppen, die die grundlegenden Rechenregeln respektieren, betrachten. Schließlich werden wir noch sogenannte Faktorstrukturen studieren.

(6.1) Definition: Sei $\mathcal{G}$ eine nicht leere Menge und $\circ$ eine Abbildung von $\mathcal{G} \times \mathcal{G}$ nach $\mathcal{G}$ ($\circ$ wird auch Verknüpfung auf $\mathcal{G}$ genannt), die die folgenden Bedingungen erfüllt:

(1) Für alle $a, b, c \in \mathcal{G}$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziativgesetz).

(2) Es gibt ein Element $e \in \mathcal{G}$ (neutrales Element oder auch Einselement) mit

(α) $e \circ a = a$ für alle $a \in \mathcal{G}$ und

(β) Zu jedem $a \in \mathcal{G}$ gibt es ein $b \in \mathcal{G}$ (Linksinverses) mit $b \circ a = e$

Dann heißt $\mathcal{G}$ eine **Gruppe** bezüglich $\circ$. Gilt zusätzlich

(3) Für alle $a, b \in \mathcal{G}$ gilt $a \circ b = b \circ a$

so nennen wir $\mathcal{G}$ eine kommutative oder **abelsche**[1] **Gruppe**.

[1] N. Abel *5.8.1802 Finnö (Norwegen), †6.4.1829 Froland, als Stipendiat in Paris, Berlin und Italien, leistete bedeutende Beiträge auf den Gebieten der algebraischen Gleichungen, elliptischen Kurven und Reihenlehre

Es ist üblich, das Bild $a \circ b$ mit ab, manchmal auch mit $a+b$ zu bezeichnen. Wenn es auf die spezielle Verknüpfung nicht ankommt, werden wir dies auch so machen. Sollen gleichzeitig die Verknüpfung "$\cdot$" und "$+$" auf einer Menge $\mathcal{G}$ betrachtet werden, so schreiben wir $\mathcal{G}(\cdot)$ bzw. $\mathcal{G}(+)$, um auszudrücken, welche Verknüpfung gerade betrachtet wird. Schreibt man $\mathcal{G}(+)$, so wird man üblicherweise das Element e mit 0 bezeichnen.

In dem Axiomensystem für eine Gruppe kommen $\mathcal{G}$ und $\circ$ als Variable vor. Wir wissen also weder, was wir verknüpfen, da die Gruppe $\mathcal{G}$ kein konkretes Objekt ist, noch - als Folge davon - wie wir die Verknüpfung bewerkstelligen.

In der Anwendung müssen wir $\mathcal{G}$ und $\circ$ durch konkrete Mengen bzw. Verknüpfungen ersetzen. Jede aus den Axiomen hergeleitete Aussage gilt damit automatisch in jedem Modell.

Neben der Möglichkeit der gleichzeitigen Untersuchung der Eigenschaften vieler mathematischer Objekte gibt es noch einen zweiten Grund für das axiomatische Vorgehen. Bei der Beschreibung von Vorgängen in der Natur werden (undefinierte) Grundbegriffe und Zusammenhänge zwischen diesen aus der Anschauung entnommen und in (unbeweisbaren) Axiomen an den Anfang einer Theorie gestellt. Ist das Axiomensystem gut gewählt, so ergeben sich weitere Übereinstimmungen mit dem untersuchten Sachverhalt der Umwelt. Ziel ist dann oft der Nachweis, daß bis auf Schreib- und Bezeichnungsweise nur ein Modell für das Axiomensystem existiert. Wir werden dies bei der Untersuchung der Vektorräume genauer sehen.

(6.2) Beispiele: (a) Ist $\mathcal{M} \neq \varnothing$ eine Menge. So ist $\Sigma(\mathcal{M})$ mit der Hintereinanderausführung von Abbildungen einer Gruppe. Siehe (3.15),(3.10), (3.11) und (3.13).

Sei $\mathcal{M} = \{1, 2, 3\}$ und $f, g \in \Sigma(\mathcal{M})$ mit $f(1) = 1$, $f(2) = 3$, $f(3) = 2$ und $g(1) = 2$, $g(2) = 1$, $g(3) = 3$. Dann ist

$$(f \circ g)(1) = 3 \neq (g \circ f)(1) = 2.$$

Also ist im allgemeinen $\Sigma(\mathcal{M})$ nicht abelsch.

(b) $\mathbb{Z}(+)$ ist eine Gruppe (abelsch)

(c) $\mathbb{Q}(+)$ ist eine abelsche Gruppe; $(\mathbb{Q} \setminus \{0\})(\cdot)$ ist eine abelsche Gruppe; $(\mathbb{Z} \setminus \{0\})(\cdot)$ ist keine Gruppe, da es zu 2 kein Inverses gibt !

(d) Sei $\mathcal{M}$ eine Menge $\mathcal{P}(\mathcal{M})$ die Potenzmenge von $\mathcal{M}$. Für $\mathcal{H}, \mathcal{Y} \in \mathcal{P}(\mathcal{M})$ setze

$$\mathcal{H} + \mathcal{Y} = (\mathcal{H} \cup \mathcal{Y}) \setminus (\mathcal{H} \cap \mathcal{Y})$$

Man nennt diese Verknüpfung auch **symmetrische Differenz**.

Es ist $\mathcal{P}(\mathcal{M})(+)$ eine Gruppe: Zunächst ist $\mathcal{H}+\mathcal{Y} \in \mathcal{P}(\mathcal{M})$, also ist $+$ eine Verknüpfung.

Assoziativität: Seien $\mathcal{H}, \mathcal{Y}, \mathcal{Z} \in \mathcal{P}(\mathcal{M})$. Dann müssen wir $\mathcal{H}+(\mathcal{Y}+\mathcal{Z}) = (\mathcal{H}+\mathcal{Y})+\mathcal{Z}$ zeigen. Dazu sind zwei Inklusionen zu beweisen:

$$(\alpha) \qquad \mathcal{H}+(\mathcal{Y}+\mathcal{Z}) \subseteq (\mathcal{H}+\mathcal{Y})+\mathcal{Z}, \text{ für alle} \mathcal{H}, \mathcal{Y}, \mathcal{Z} \in \mathcal{P}(\mathcal{M}).$$

Sei $u \in \mathcal{H}+(\mathcal{Y}+\mathcal{Z}) = (\mathcal{H} \cup (\mathcal{Y}+\mathcal{Z})) \setminus (\mathcal{H} \cap (\mathcal{Y}+\mathcal{Z}))$

Fall 1: $u \in \mathcal{H}$: Dann ist $u \notin \mathcal{H} \cap (\mathcal{Y}+\mathcal{Z})$, also ist $u \notin \mathcal{Y}+\mathcal{Z}$, d.h. $u \notin (\mathcal{Y} \cup \mathcal{Z}) \setminus (\mathcal{Y} \cap \mathcal{Z})$. Ist $u \in \mathcal{Y} \cap \mathcal{Z}$, so ist u wegen $u \in \mathcal{H}$ auch in $\mathcal{H} \cap \mathcal{Y}$ enthalten. Also ist $u \notin (\mathcal{H} \cup \mathcal{Y}) \setminus (\mathcal{H} \cap \mathcal{Y}) = \mathcal{H}+\mathcal{Y}$. Weiter ist $u \in \mathcal{Z}$, d.h. $u \in ((\mathcal{H}+\mathcal{Y}) \cup \mathcal{Z}) \setminus ((\mathcal{H}+\mathcal{Y}) \cap \mathcal{Z}) = (\mathcal{H}+\mathcal{Y})+\mathcal{Z}$. Ist $u \notin \mathcal{Y} \cap \mathcal{Z}$. Dann ist $u \notin \mathcal{Y}$ und $u \notin \mathcal{Z}$, da $u \notin \mathcal{Y}+\mathcal{Z}$ war. Also ist $u \notin \mathcal{H} \cap \mathcal{Y}$, d.h. $u \in (\mathcal{H} \cup \mathcal{Y}) \setminus (\mathcal{H} \cap \mathcal{Y}) = \mathcal{H}+\mathcal{Y}$ und $u \in ((\mathcal{H}+\mathcal{Y}) \cup \mathcal{Z}) \setminus ((\mathcal{H}+\mathcal{Y}) \cap \mathcal{Z}) = (\mathcal{H}+\mathcal{Y})+\mathcal{Z}$. Insgesamt ist also in Fall 1: $u \in (\mathcal{H}+\mathcal{Y})+\mathcal{Z}$.

Fall 2: $u \notin \mathcal{H}$: Dann ist $u \in \mathcal{Y}+\mathcal{Z} = (\mathcal{Y} \cup \mathcal{Z}) \setminus (\mathcal{Y} \cap \mathcal{Z})$. Ist $u \in \mathcal{Y}$, so ist $u \notin \mathcal{Z}$. Also ist $u \in (\mathcal{H} \cup \mathcal{Y}) \setminus (\mathcal{H} \cap \mathcal{Y}) = \mathcal{H}+\mathcal{Y}$ und $u \in ((\mathcal{H}+\mathcal{Y}) \cup \mathcal{Z}) \setminus ((\mathcal{H}+\mathcal{Y}) \cap \mathcal{Z}) = (\mathcal{H}+\mathcal{Y})+\mathcal{Z}$. Ist $u \notin \mathcal{Y}$, so ist $u \in \mathcal{Z}$. Also ist $u \notin (\mathcal{H} \cup \mathcal{Y}) \setminus (\mathcal{H} \cap \mathcal{Y}) = \mathcal{H}+\mathcal{Y}$ und somit $u \in ((\mathcal{H}+\mathcal{Y}) \cup \mathcal{Z}) \setminus ((\mathcal{H}+\mathcal{Y}) \cap \mathcal{Z}) = (\mathcal{H}+\mathcal{Y})+\mathcal{Z}$.

Insgesamt ist (α) für alle $\mathcal{H}, \mathcal{Y}, \mathcal{Z} \in \mathcal{P}(\mathcal{M})$ bewiesen.

$$(\beta) \qquad (\mathcal{H}+\mathcal{Y})+\mathcal{Z} \subseteq \mathcal{H}+(\mathcal{Y}+\mathcal{Z}) \text{ für alle } \mathcal{H}, \mathcal{Y}, \mathcal{Z} \in \mathcal{P}(\mathcal{M}).$$

Es ist offenbar $\mathcal{A}+\mathcal{B} = \mathcal{B}+\mathcal{A}$ für alle $\mathcal{A}, \mathcal{B} \in \mathcal{P}(\mathcal{M})$. Somit gilt:

$$(\mathcal{H}+\mathcal{Y})+\mathcal{Z} = \mathcal{Z}+(\mathcal{H}+\mathcal{Y}) = \mathcal{Z}+(\mathcal{Y}+\mathcal{H}) \underset{(\alpha)}{\subseteq} (\mathcal{Z}+\mathcal{Y})+\mathcal{H} = \mathcal{H}+(\mathcal{Z}+\mathcal{Y}) = \mathcal{H}+(\mathcal{Y}+\mathcal{Z}).$$

Damit ist $+$ assoziativ.

Neutrales Element: Das neutrale Element ist die leere Menge :

$$\varnothing + \mathcal{H} = (\varnothing \cup \mathcal{H}) \setminus (\varnothing \cap \mathcal{H}) = \mathcal{H} \setminus \varnothing = \mathcal{H} \text{ für alle } \mathcal{H} \in \mathcal{P}(\mathcal{M}).$$

Inverse: Jedes Element ist zu sich selbst invers :

$$\mathcal{H}+\mathcal{H} = (\mathcal{H} \cup \mathcal{H}) \setminus (\mathcal{H} \cap \mathcal{H}) = \mathcal{H} \setminus \mathcal{H} = \varnothing.$$

Also ist $\mathcal{P}(\mathcal{M})(+)$ eine abelsche Gruppe.

In der Definition der Gruppe gibt es gewisse Unsymmetrien. So wird z.B. von einem Linksinversen gesprochen aber nicht von einem Rechtsinversen. Auch wird das Einselement nur von einer Seite definiert. Wir hätten die Definition auch mit Rechtsinversen statt Linksinversen geben können. Dann wäre zunächst ein anderer Gruppenbegriff definiert worden. Im folgenden Satz wollen wir zeigen, daß diese Unsymmetrien nur scheinbar sind. Man hätte natürlich auch die Definition gleich symmetrisch machen können, dies hätte dann aber den Nachteil gehabt, daß man, wenn man zeigen will, daß eine gewisse Menge mit einer Verknüpfung eine Gruppe ist, mehr nachweisen muß, als mit unserer Definition.

(6.3) Satz: *Ist $\mathcal{G}$ eine Gruppe mit neutralem Element e, so gilt:*

(a) *Es ist auch $a \circ e = a$ für alle $a \in \mathcal{G}$.*

(b) *Ist $f \circ a = a$ für ein f und alle $a \in \mathcal{G}$, so ist $f = e$*
(Eindeutigkeit des neutralen Elements).

(c) *Ist $b \circ a = e$, so ist auch $a \circ b = e$ und b ist eindeutig bestimmt.*

Beweis: (a) Sei $a \in \mathcal{G}$. Dann gibt es ein $b \in \mathcal{G}$ mit $b \circ a = e$ und ein $c \in \mathcal{G}$ mit $c \circ b = e$. Das liefert

$$c \circ e = c \circ (b \circ a) \underset{(6.1)(1)}{=} (c \circ b) \circ a = e \circ a = a.$$

Also ist

$$a = c \circ e = c \circ (e \circ e) \underset{(6.1)(1)}{=} (c \circ e) \circ e = a \circ e.$$

(b) Es ist $f \underset{(a)}{=} f \circ e = e$

(c) Es gibt ein $c \in \mathcal{G}$ mit $c \circ b = e$. Also ist

$$e = c \circ b = c \circ (e \circ b) = c \circ ((b \circ a) \circ b) \underset{(6.1)(1)}{=} (c \circ (b \circ a)) \circ b \underset{(6.1)(1)}{=} ((c \circ b) \circ a) \circ b = (e \circ a) \circ b = a \circ b.$$

Sei nun $x \circ a = b \circ a = e$. Dann ist

$$x = x \circ e = x \circ (a \circ b) \underset{(6.1)(1)}{=} (x \circ a) \circ b = e \circ b = b.$$

Also ist b eindeutig durch a bestimmt.□

Wir werden das zu a eindeutig bestimmte Element b mit $b \circ a = e$ mit a^{-1} bezeichnen.

Nun wollen wir weitere Rechenregeln beweisen.

(6.4) Satz: *Sei $\mathcal{G}$ eine Gruppe. Dann gilt:*

(a) *Ist $a \in \mathcal{G}$, so ist $(a^{-1})^{-1} = a$.*

(b) *Sind $a, b \in \mathcal{G}$, so ist $(ab)^{-1} = b^{-1}a^{-1}$.*

(c) *Sind $a, b \in \mathcal{G}$, so gibt es eindeutig bestimmte $x, y \in \mathcal{G}$ mit $ax = b = ya$.*

(d) *Sind $a, x, y \in \mathcal{G}$ mit $ax = ay$, so ist $x = y$. Ist $xa = ya$, so ist auch $x = y$.*

Beweis: (a) Es ist $aa^{-1} \underset{(6.3)}{=} e$. Also ist $a = (a^{-1})^{-1}$.

(b) $(b^{-1}a^{-1})(ab) \underset{(6.1)(1)}{=} b^{-1}(a^{-1}(ab)) \underset{(6.1)(1)}{=} b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$. Nach (6.3) ist dann $(ab)^{-1} = b^{-1}a^{-1}$.

(c) Setze $x = a^{-1}b$. Dann ist $a(a^{-1}b) = (aa^{-1})b = b$. Also ist $x = a^{-1}b$ eine Lösung. Sei $\tilde{x}$ eine weitere Lösung. Dann ist $a\tilde{x} = b$ und somit $e = b^{-1}b = b^{-1}(a\tilde{x}) = (b^{-1}a)\tilde{x}$. Nun ist $\tilde{x} = (b^{-1}a)^{-1} = a^{-1}b = x$. Genauso folgt die Eindeutigkeit der Lösung $y = ba^{-1}$ der Gleichung $ya = b$.

(d) Ist $ax = ay$, so ist $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = y$.

Ist $xa = ya$, so ist $a^{-1}x^{-1} = (xa)^{-1} = (ya)^{-1} = a^{-1}y^{-1}$. Nun folgt $x^{-1} = y^{-1}$ und dann auch $x = y$.□

Das Assoziativgesetz ist nur für 3 Elemente $a, b, c \in \mathcal{G}$ gefordert. Im Beweis von (6.3)(c) haben wir aber gesehen, daß man auch 4 verschiedene Elemente beliebig klammern kann. Vom Rechnen mit reellen Zahlen sind wir gewohnt, Klammern einfach wegzulassen. Daß dies nicht nur für die reellen Zahlen sondern für beliebige Gruppen richtig ist, werden wir im folgenden Satz sehen.

(6.5) Allgemeines Assoziativgesetz: *Sei $\mathcal{G}$ eine Gruppe, $a_1, \ldots, a_n \in \mathcal{G}$, $(n \geq 1)$. Jedes Produkt $a_1, \ldots, a_n$ mit beliebiger sinnvoller Beklammerung liefert denselben Wert. Genauer (mathematischer!). Definiere rekursiv:*

$$P(a_1) = \{a_1\},\ P(a_1, a_2) = \{a_1a_2\},\ P(a_1, a_2, a_3) = \{a_1(a_2a_3) = (a_1a_2)a_3\}.$$

Allgemein:

$$P(a_1, \ldots, a_k) = \{xy \mid x \in P(a_1, \ldots, a_m), y \in P(a_{m+1}, \ldots, a_k) \text{ für ein } m \text{ mit } 1 \leq m < k\}.$$

Dann enthält $P(a_1, \ldots, a_n)$ genau ein Element, nämlich

$$a_1(a_2(a_3(\ldots a_n))\ldots) =: a_1a_2\ldots a_n.$$

Beweis: Wir beweisen die Behauptung, daß $P(a_1, \ldots, a_k)$ genau ein Element enthält, durch Induktion nach k.

$k = 1$: $P(a_1) = \{a_1\}$ ist klar.

$k > 1$: Die Behauptung sei für alle $m < k$ bereits bewiesen.

Sei $xy \in P(a_1, \ldots, a_k)$. Dann ist $x \in P(a_1, \ldots, a_m), y \in P(a_{m+1}, \ldots, a_k)$. Sei zuerst $m = 1$. Dann ist $x = a_1$. Per Induktion besteht $P(a_2, \ldots, a_k)$ nur aus einem Element, nämlich $a_2(a_3(\ldots a_k))\ldots)$. Also ist $xy = a_1(a_2(\ldots a_k)\ldots)$.

Sei nun $m > 1$: Wie eben besteht per Induktion $P(a_1, \ldots, a_m)$ nur aus dem einzigen Element $a_1(a_2(\ldots a_m)\ldots)$. Setze $z = a_2(a_3(\ldots a_m))\ldots)$. Dann ist $x = a_1 z$ mit $z \in P(a_2, \ldots, a_m)$. Es ist

$$xy = (a_1 z)y \underset{(6.1)(1)}{=} a_1(zy)$$

Nun ist $zy \in P(a_2, \ldots, a_k) = \{a_2(a_3(\ldots a_k)\ldots)\}$. Also ist $xy = a_1(a_2(\ldots a_k))\ldots)$.

Damit ist der Satz bewiesen.□

Wir wollen die Axiome noch in einem anderen Licht betrachten. Sei $a \in \mathcal{G}$ fest gewählt. Wir betrachten

$$r_a : \mathcal{G} \longrightarrow \mathcal{G} : x \longrightarrow x \circ a(\text{ Rechtstranslation})$$
$$l_a : \mathcal{G} \longrightarrow \mathcal{G} : x \longrightarrow a \circ x(\text{ Linkstranslation})$$

Beides sind Abbildungen. Nun besagt (6.4)(c), daß r_a und l_a beide surjektiv sind, und es besagt (6.4)(d), daß beide injektiv sind. Also sind sowohl Rechtsmultiplikation als auch Linksmultiplikation in Gruppen bijektive Abbildungen. Es gilt aber auch die Umkehrung. Ist $\mathcal{G}$ eine Menge mit einer assoziativen Verknüpfung, so folgen die anderen Axiome der Gruppe aus der Forderung, daß r_a und l_a für alle $a \in \mathcal{G}$ bijektive Abbildungen sind.

Sei $a \in \mathcal{G}$. Dann gibt es zu a ein e_a, so daß $e_a \circ a = a$ ist (Surjektivität von r_a). Sei nun $b \in \mathcal{G}$ beliebig gewählt, so gibt es ein $y \in \mathcal{G}$ mit $b = a \circ y$ (Surjektivität von l_a). Das liefert nun

$$e_a \circ b = e_a \circ (a \circ y) = (e_a \circ a) \circ y = a \circ y = b.$$

Somit ist e_a ein neutrales Element, da die Surjektivität von r_b liefert, daß es zu b ein $x \in \mathcal{G}$ gibt, so daß $x \circ b = e_a$ ist.

Wir können somit endliche Gruppen durch sogenannte Gruppentafeln beschreiben. Sei $\mathcal{G} = \{a_1, \ldots, a_n\}$, so stellen wir eine Tabelle auf mit i Zeilen und Spalten, deren Einträge an der Stelle (i, j) genau $a_i \circ a_j$ sind. Die Bijektivität von l_a und r_a bedeutet, daß in jeder Zeile und Spalte jedes Element der Gruppe genau einmal vorkommt. Dies kann man leicht nachprüfen. Will man dann entscheiden, ob die vorgegebene Menge mit dieser Verknüpfung eine Gruppe ist, muss man nur noch die Assozitivatät nachprüfen.

Wir wollen dies an einem Beispiel erläutern. Sei $\mathcal{G} = \{a_1, a_2, a_3\}$. Gibt es eine Verknüpfung auf $\mathcal{G}$, so daß $\mathcal{G}$ eine Gruppe wird ? Wir können annehmen, daß a_1 das neutrale Element ist. Dann lautet die erste Zeile der Gruppentafel a_1, a_2, a_3. Das gleiche gilt für die erste Spalte. Also

$$\begin{array}{ccc} a_1 & a_2 & a_3 \\ a_2 & * & * \\ a_3 & * & * \end{array}$$

Da in der zweiten Zeile jedes Gruppenelement genau einmal vorkommen muß, lautet sie entweder a_2, a_1, a_3 oder a_2, a_3, a_1. Im ersten Fall haben wir für die zweite Spalte bereits a_2, a_1, was dann a_2, a_1, a_3 liefert. Dann wäre aber in der dritten Zeile zweimal der Eintrag a_3, was nicht sei kann. Damit ist die Tafel festgelegt.

$$\begin{array}{ccc} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \\ a_3 & a_1 & a_2 \end{array}$$

Wir müßten nun nachprüfen, ob das Assoziativgesetz erfüllt ist. Dann hätten wir gesehen, daß es nur eine Verknüpfung gibt, so daß $\mathcal{G}$ eine Gruppe wird. Wie wir später noch sehen werden, gibt es eine Gruppe mit drei Elementen. Da wir gerade gesehen haben, daß es maximal eine solche Gruppe gibt, folgt nun, daß wir gerade die Verknüpfung für eine Gruppe mit drei Elementen gefunden haben. Es gibt somit genau eine Gruppe mit drei Elementen.

Wir könnten nun fortfahren, die Definition des Vektorraumes aus Kapitel 0 exakt zu machen. Wir wollen aber einen kleinen Abstecher in die Theorie der Gruppen unternehmen. Dies kann später als Modell für die Untersuchungen von Vektorräumen dienen. Die erste Frage, die man sich in einer Strukturtheorie stellt, ist die nach Unterstrukturen.

(6.6) Definition: Sei $\mathcal{G}$ eine Gruppe mit Verknüpfung $\circ$. Eine **Untergruppe** von $\mathcal{G}$ ist eine nicht leere Teilmenge $\mathcal{U}$, die hinsichtlich $\circ$ selbst eine Gruppe ist. Schreibe dafür $U \leq G$.

Der nachfolgende Satz gibt ein einfaches Kriterium dafür, daß eine Teilmenge einer Gruppe eine Untergruppe ist.

(6.7) Satz: *Sei $\mathcal{G}$ eine Gruppe mit Verknüpfung $\circ$ und $\mathcal{U} \subseteq \mathcal{G}$, $\mathcal{U} \neq \varnothing$. Dann ist $\mathcal{U}$ genau dann eine Untergruppe von $\mathcal{G}$, wenn die folgenden Bedingungen gelten.*

(i) *Für alle $u, v \in \mathcal{U}$ ist stets $u \circ v \in \mathcal{U}$.*

(ii) *Ist $u \in \mathcal{U}$, so ist auch $u^{-1} \in \mathcal{U}$.*

Ist $|\mathcal{U}| < \infty$, so genügt (i).

Beweis: Nach (6.6) erfüllt eine Untergruppe (i) und (ii). Erfülle nun umgekehrt $\mathcal{U}$ (i) und (ii). Dann ist nur zu zeigen, daß $e \in \mathcal{U}$ ist, wobei e das neutrale Element von $\mathcal{G}$ sei. Die anderen formalen Axiome aus (6.1) gelten auch in $\mathcal{U}$, da sie in $\mathcal{G}$ gelten. Da $\mathcal{U}$ nicht leer ist, gibt es ein $u \in \mathcal{U}$. Nach (ii) ist $u^{-1} \in \mathcal{U}$. Nach (i) ist $e = u \circ u^{-1} \in \mathcal{U}$.

Sei nun $\mathcal{U}$ endlich. Halte $u \in \mathcal{U}$ fest. Die Abbildung $f : \mathcal{U} \to \mathcal{U}$ mit $f(v) = u \circ v$ ist nach (6.1)(2)(β) injektiv. Also haben $\mathcal{U}$ und $f(\mathcal{U})$ die gleiche Mächtigkeit. Da $\mathcal{U}$ endlich ist, ist dann $|\mathcal{U}| = |f(\mathcal{U})|$ und

$$\mathcal{U} = \{u \circ v \,\big|\, v \in \mathcal{U}\},$$

nach (5.7). Also ist $u = u \circ v$ für ein geeignetes $v \in \mathcal{U}$. Nun ist $v = u^{-1} \circ u \circ v = u^{-1} \circ u = e$. Damit ist $e \in \mathcal{U}$. Es gilt aber auch, daß $e = u \circ w \in \mathcal{U}$ für ein geeignetes $w \in \mathcal{U}$ ist. Damit ist $u^{-1} = w \in \mathcal{U}$ und somit gilt (ii).□

(6.8) Beispiel: (a) $\mathbb{Z}(+)$ ist Untergruppe von $\mathbb{R}(+)$. Aber $\mathbb{N}(+)$ ist keine Untergruppe von $\mathbb{Z}(+)$, obwohl (6.7)(i) gilt. Somit ist (6.7)(ii) für unendliche Gruppen nicht entbehrlich.

(b) Sei $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$, $n \in \mathbb{N}$. Dann ist $n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Dies ergibt sich aus den folgenden drei Aussagen.

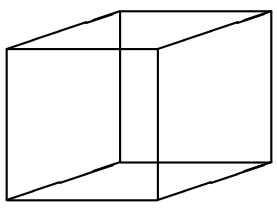
(1) $n\mathbb{Z} \neq \varnothing$, da $0 \in n\mathbb{Z}$.

(2) Sind $nz_1, nz_2 \in \mathbb{Z}$, so ist

$$nz_1 + nz_2 = n(z_1 + z_2) \in n\mathbb{Z}.$$

(3) Ist $nz \in \mathbb{Z}$, so ist auch $-nz = n(-z) \in n\mathbb{Z}$.

(c) Die Symmetrien eines Körpers, d.h. alle (orientierungstreuen) Bewegungen des Körpers, die ihn in sich selbst überführen, bilden eine Gruppe. Wir betrachten den Würfel:



Der Würfel hat die folgenden drei Typen von Dreh-Symmetrieachsen:

1. Achsen durch die Mittelpunkte gegenüberliegender Flächen:
   Drehungen um $90°, 180°, 270°$. Das ergibt $3 \cdot 3 = 9$ Drehungen.
2. Die räumlichen Diagonalen:
   Drehungen um $120°$ und $240°$ zu den 4 Raumdiagonalen. Somit gibt es $4 \cdot 2 = 8$ entsprechende Drehungen.
3. Achsen durch die Mitten gegenüberliegender Kanten:
   Drehung um $180°$. Von diesen gibt es 6 Drehungen.

Zusammen mit der Identität haben wir somit 24 Symmetrien gefunden. Jede Symmetrie des Würfels bildet eine Raumdiagonale wieder in eine solche ab. Also werden die 4 Raumdiagonalen permutiert. Wenn wir diese mit $1, 2, 3, 4$ durchnumerieren, so können wir die Symmetrien als Elemente der Gruppe $\Sigma(\{1, 2, 3, 4\})$ auffassen. Diese hat 24 Elemente. Also haben wir alle Symmetrien gefunden.

Im vorherigen Beispiel hatten wir gesehen, daß wir die Gruppe der Symmetrien eines Würfels auch als die Gruppe der Permutationen der Raumdiagonalen auffassen können. D.h., daß vom mathematischen Standpunkt beide Gruppen nicht unterscheidbar sind. Wir wollen dies nun exakt formulieren.

Zunächst dürfen die Grundmengen der Gruppen $\mathcal{G}$ und $\mathcal{H}$ nicht unterscheidbar sein, d.h. es gibt eine bijektive Abbildung

$$f : \mathcal{G} \to \mathcal{H}.$$

Aber auch die Verknüpfungen sollen gleich sein, d.h.

$$f(g \circ h) = f(g) \circ f(h) \quad \text{für alle } g, h \in \mathcal{G}.$$

Beachte, daß $\circ$ auf der rechten und linken Seite eine verschiedene Bedeutung hat.

Im allgemeinen ist nicht nur der Fall, daß f bijektiv ist, interessant, sondern auch, daß f nur eine Abbildung ist. Diese wollen wir nun studieren.

(6.9) Definition: Seien $(\mathcal{G}, o_1), (\mathcal{H}, o_2)$ zwei Gruppen. Eine Abbildung $f : \mathcal{G} \to \mathcal{H}$ heißt ein **Homomorphismus**, falls

$$f(g \, o_1 \, h) = f(g) o_2 f(h) \text{ für alle } g, h \in \mathcal{G}$$

gilt. Ist f surjektiv, so heißt f ein **Epimorphismus**. Ist f injektiv, so heißt f ein **Monomorphismus**. Ist f bijektiv, so heißt f ein **Isomorphismus**. Gibt es zwischen $\mathcal{G}$ und $\mathcal{H}$ einen Isomorphismus, so schreiben wir $\mathcal{G} \cong \mathcal{H}$. Ist $\mathcal{G} = \mathcal{H}$ und f ein Isomorphismus, so nenne f einen **Automorphismus**.

(6.10) Beispiele: (1) Es ist $f : \mathbb{Z}(+) \to \mathbb{R} \setminus \{0\}(\cdot)$ mit $f(z) = r^z$ (für festes $r \in \mathbb{R}$) ein Homomorphismus:

$$f(z_1 + z_2) = r^{z_1+z_2} = r^{z_1} r^{z_2} = f(z_1) f(z_2)$$

(2) $f : \mathbb{C}(+) \to \mathbb{C}(+)$ mit $f : a + bi \to a - bi$ ist Isomorphismus.

(3) Sei $\mathcal{P} = \{a \,\big|\, a \in \mathbb{R}, a > 0\}$. Mit der Multiplikation der reellen Zahlen ist $\mathcal{P}$ eine Gruppe. Sei

$$\log \; : \mathcal{P} \to \mathbb{R}(+)$$

der Logarithmus zur Basis e. Dann gilt

$$\log(ab) = \log(a) + \log(b)$$

Also ist log ein Homomorphismus von $\mathcal{P}$ auf die additive Gruppe $\mathbb{R}(+)$.

Sei $a \in \mathbb{R}$. Dann ist

$$a = \log(e^a).$$

Also ist log ein Epimorphismus.

Ist $\log(a) = \log(b)$, so folgt

$$a = e^{\log(a)} = e^{\log(b)} = b.$$

Also ist $\log : \mathcal{P} \to \mathbb{R}$ ein Isomorphismus.

(6.11) Lemma: *Sei $\mathcal{G}$ eine Gruppe mit neutralem Element e, $\mathcal{G}'$ eine Gruppe mit neutralem Element e' und $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann gilt*

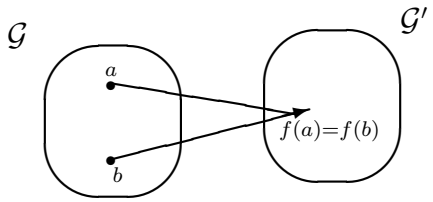
(i) $f(e) = e'$.

(ii) $f(a^{-1}) = f(a)^{-1}$ *für alle* $a \in \mathcal{G}$.

Beweis: (i) $f(e)e' = f(e) = f(e \cdot e) = f(e)f(e)$. Multiplikation mit $f(e)^{-1}$ liefert $e' = f(e)$

(ii) $f(a^{-1})f(a) \underset{(6.9)}{=} f(a^{-1}a) = f(e) \underset{(i)}{=} e'$. Also ist $f(a^{-1}) = f(a)^{-1}$.□

Sei $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus:



Seien $a, b \in \mathcal{G}$ und $f(a) = f(b)$. Dann ist $e' = f(a)^{-1}f(b) \underset{(6.11)(b)}{=} f(a^{-1})f(b) = f(a^{-1}b)$. D.h.

$$f(a) = f(b) \text{ genau für } a^{-1}b \in f^{-}\{e'\}.$$

Es ist also sinnvoll, sich näher mit $f^{-}\{e'\}$ zu befassen.

(6.12) Definition. Seien $\mathcal{G}$ und $\mathcal{G}'$ Gruppen mit neutralen Elementen e bzw. e' und $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann heißt

$$\text{Ker } f := \{x \in \mathcal{G} \mid f(x) = e'\}$$

der **Kern** von f und

$$\text{Im } f := \{f(x) \mid x \in \mathcal{G}\}$$

das **Bild** von f.

(6.13) Lemma: *Seien $\mathcal{G}$ und $\mathcal{G}'$ Gruppen, $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann gilt*

(a) $\text{Ker } f$ *ist eine Untergruppe von* $\mathcal{G}$.

(b) $\text{Im } f$ *ist eine Untergruppe von* $\mathcal{G}'$.

Beweis: (a) Es ist $f(e) = e'$. Also ist $e \in \text{Ker } f$, d.h. $\text{Ker } f \neq \varnothing$.

Seien $u, v \in \text{Ker } f$. Dann ist

$$f(u) = e' = f(v)$$

Also gilt

$$f(uv) = f(u)f(v) = e' \cdot e' = e'$$

Damit ist $uv \in \text{Ker } f$. Weiter ist

$$f(v^{-1}) \underset{(6.11)(b)}{=} f(v)^{-1} = e'^{-1} = e'$$

Also ist $v^{-1} \in \text{Ker } f$. Nun folgt die Behauptung mit (6.7).

(b) Es ist $e' = f(e) \in \text{Im } f$. Somit ist $\text{Im } f \neq \varnothing$.

Seien $u', v' \in \text{Im } f$. Dann gibt es $u, v \in \mathcal{G}$ mit

$$u' = f(u), \quad v' = f(v).$$

Also ist $u'v' = f(u)f(v) = f(uv) \in \operatorname{Im} f$. Weiter ist: $u'^{-1} = f(u)^{-1} = f(u^{-1}) \in \operatorname{Im} f$. Nun folgt die Behauptung mit (6.7).□

Bei Homomorphismen ist es besonders einfach zu entscheiden, ob sie injektiv sind.

(6.14) Lemma: *Seien $\mathcal{G}$ und $\mathcal{G}'$ Gruppen und $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann ist f genau dann ein Monomorphismus, wenn* $\operatorname{Ker} f = \{e\}$ *ist.*

Beweis: (1) Sei f injektiv. Dann hat e' höchstens ein Urbild. Wegen $f(e) = e'$ hat e' genau ein Urbild. Also ist $\operatorname{Ker} f = f^-\{e'\} = \{e\}$.

(2) Sei $\operatorname{Ker} f = \{e\}$. Seien a und $b \in \mathcal{G}$ mit $f(a) = f(b)$. Dann ist $f(a^{-1}b) = f(a)^{-1}f(b) = e'$. Also ist $a^{-1}b \in \operatorname{Ker} f = \{e\}$. Damit ist $a = b$, d.h. f ist injektiv.□

Wie wir in (6.14) gesehen haben, können wir leicht das Urbild des neutralen Elementes kontrollieren. Dies geht aber auch mit jedem anderen Element, wie das nächste Lemma zeigt.

(6.15) Lemma: *Seien $\mathcal{G}$ und $\mathcal{G}'$ Gruppen und $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann ist für jedes $a \in \mathcal{G}$:*

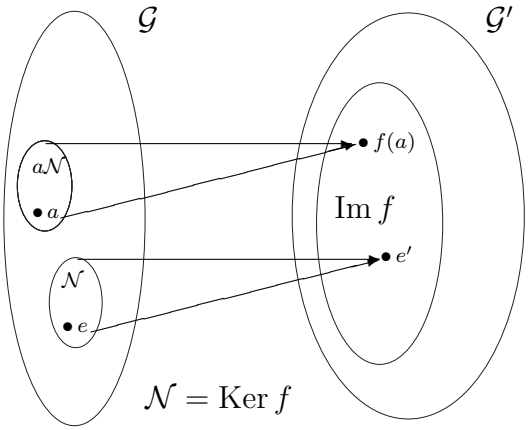
$$f^-\{f(a)\} = a \operatorname{Ker} f := \{at \mid t \in \operatorname{Ker} f\}.$$

Beweis: Ist $f(a) = f(b)$, so hatten wir bereits $a^{-1}b \in \operatorname{Ker} f$ gesehen, d.h. $b \in a \operatorname{Ker} f$.

Sei umgekehrt $b \in a\operatorname{Ker} f$, so ist $a^{-1}b \in \operatorname{Ker} f$, d.h.

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

Also $f(a) = f(b)$.□



(6.16) Definition: Sei $\mathcal{G}$ eine Gruppe und $\mathcal{U}$ eine Untergruppe von $\mathcal{G}$. Für jedes $g \in \mathcal{G}$ heißt

$$g\mathcal{U} := \{gu \mid u \in \mathcal{U}\}$$

eine **Linksnebenklasse** von $\mathcal{U}$ in $\mathcal{G}$ und

$$\mathcal{U}g := \{ug \mid u \in \mathcal{U}\}$$

eine **Rechtsnebenklasse** von $\mathcal{U}$ in $\mathcal{G}$.

(6.17) Lemma: *Sei $\mathcal{G}$ eine Gruppe und $\mathcal{U} \leq \mathcal{G}$. Dann gilt*

$$\mathcal{G} = \bigcup_{g \in \mathcal{G}} g\mathcal{U} \text{ und } g\mathcal{U} \cap h\mathcal{U} = \begin{cases} g\mathcal{U} & \text{oder} \\ \varnothing \end{cases}$$

Entsprechendes gilt für Rechtsnebenklassen.

Beweis: Da $g \in g\mathcal{U}$ ist, ist die erste Aussage offenbar. Sei $x \in g\mathcal{U} \cap h\mathcal{U}$. Dann ist

$$(*) \quad x = gu_1 = hu_2, \text{ mit geeigneten } u_1, u_2 \in \mathcal{U}.$$

Sei $gu \in g\mathcal{U}$. Dann ist

$$gu \underset{(*)}{=} (hu_2u_1^{-1})u \in h\mathcal{U}$$

Also ist $g\mathcal{U} \subseteq h\mathcal{U}$. Ist $hu \in h\mathcal{U}$, so ist

$$hu \underset{(*)}{=} (gu_1u_2^{-1})u \in g\mathcal{U}$$

Also ist $h\mathcal{U} \subseteq g\mathcal{U}$, d.h. $h\mathcal{U} = g\mathcal{U}$.□

Besonders interessant sind Untergruppen $\mathcal{U}$, bei denen die Begriffe Rechtsnebenklasse und Linksnebenklasse zusammenfallen, bei denen also jede Rechtsnebenklasse auch eine Linksnebenklasse ist. Diese wollen wir nun untersuchen.

(6.18) Definition: Eine Untergruppe $\mathcal{N}$ einer Gruppe $\mathcal{G}$ heißt **Normalteiler**[2] oder **normale Untergruppe**, falls für alle $g \in \mathcal{G}$

$$g\mathcal{N} = \mathcal{N}g$$

gilt. Schreibe $\mathcal{N} \trianglelefteq \mathcal{G}$ oder auch $\mathcal{N} \triangleleft \mathcal{G}$, wenn $\mathcal{N} \neq \mathcal{G}$ betont werden soll.

Bei einer kommutativen Gruppe ist jede Untergruppe ein Normalteiler.

[2]E. Galois *25.10.1811 Bourg-la Reine, †31.5.1832 Paris. Beschäftigte sich mit der Frage, für welche Polynomgleichungen es Lösungsformeln für die Nullstellen gibt, die denen der Gleichung vom Grad 2, 3 oder 4 ähneln, d.h. neben den arithmetischen Operationen nur noch Wurzelausdrücke benötigen. Hierzu erstellte er die Anfänge der Gruppentheorie. Wesentlich war seine Entdeckung des Normalteilerbegriffes, der die ganze Frage einer Induktion zugänglich machte. Die ersten Axiome der Gruppentheorie, wie wir sie angegeben haben finden sich in dem Lehrbuch von H. Weber "Algebra" von 1893.

Die wesentliche Bedeutung des Normalteilerbegriffes liegt darin, daß mit einem Normalteiler eine neue Gruppe definiert werden kann, die zwar keine Untergruppe der gegebenen Gruppe ist, deren Struktur aber viel mit der Ausgangsgruppe gemein hat. Diese wollen wir nun durchführen.

(6.19) Definition: Sei $\mathcal{G}$ eine Gruppe und $\mathcal{N} \trianglelefteq \mathcal{G}$. Dann bezeichne mit $\mathcal{G}/\mathcal{N}$ die Menge der Nebenklassen $\{a\mathcal{N} \mid a \in \mathcal{G}\}$. Auf $\mathcal{G}/\mathcal{N}$ definieren wir eine Verknüpfung wie folgt :

Für $a, b \in \mathcal{G}$ sei

$$(aN) \circ (bN) := (ab)N.$$

Wir nennen $\mathcal{G}/\mathcal{N}$ die **Faktorgruppe** von $\mathcal{G}$ nach $\mathcal{N}$.

Daß die Bezeichnung Faktor**gruppe** in (6.19) gerechtfertigt ist, zeigt der nächste Satz.

(6.20) Satz: *Sei $\mathcal{G}$ eine Gruppe und $\mathcal{N} \trianglelefteq \mathcal{G}$. Dann ist $\mathcal{G}/\mathcal{N}$ mit der in (6.19) definierten Verknüpfung $\circ$ eine Gruppe.*

Beweis: Wir müssen zunächst zeigen, daß $\circ$ eine Abbildung ist. Das Problem ist, daß wir $\circ$ mit Hilfe von Vertretern a, b definiert haben. Es ist zu zeigen, daß die Definition von der Wahl der Vertreter unabhängig ist.

Sei $a\mathcal{N} = a'\mathcal{N}$ und $b\mathcal{N} = b'\mathcal{N}$. Also ist $a' = an_1$ und $b' = bn_2$ mit geeigneten $n_1, n_2 \in \mathcal{N}$. Dann ist $(a'b')\mathcal{N} = (an_1bn_2)\mathcal{N}$. Da $\mathcal{N} \trianglelefteq \mathcal{G}$, ist $n_1b \in \mathcal{N}b = b\mathcal{N}$, d.h. es gibt ein $n_3 \in \mathcal{N}$ mit

$$n_1b = bn_3.$$

Dann ist

$$(a'b')\mathcal{N} = (abn_3n_2)\mathcal{N} = (ab)\mathcal{N}\text{, da } n_3n_2\mathcal{N} = \mathcal{N} \text{ ist.}$$

Assoziativität: Seien $a, b, c \in \mathcal{G}$. Dann ist

$$((a\mathcal{N}) \circ (b\mathcal{N})) \circ (c\mathcal{N}) = (ab)\mathcal{N} \circ c\mathcal{N} = ((ab)c)\mathcal{N} \underset{\substack{Ass.\\ in\,\mathcal{G}}}{=} (a(bc))\mathcal{N} = (a\mathcal{N}) \circ (bc)\mathcal{N} =$$

$$a\mathcal{N} \circ ((b\mathcal{N}) \circ (c\mathcal{N})).$$

Neutrales Element: Es ist $\mathcal{N} = e\mathcal{N}$ das neutrale Element:

$$\mathcal{N} \circ (a\mathcal{N}) = (ea)\mathcal{N} = a\mathcal{N} \text{ für alle } a \in \mathcal{G}.$$

Inverses: Sei $a \in \mathcal{G}$. Dann ist

$$(a\mathcal{N}) \circ (a^{-1}\mathcal{N}) = (aa^{-1})\mathcal{N} = e\mathcal{N} = \mathcal{N}.$$

Also ist $a^{-1}\mathcal{N}$ das Inverse zu $a\mathcal{N}$.□

In endlichen Gruppen öffnet (6.20) die Tür zu Induktionsbeweisen. Sei $|\mathcal{G}| < \infty$ und $1 \neq \mathcal{N} \neq \mathcal{G}$ ein Normalteiler. Dann ist sowohl $|\mathcal{N}|$ als auch $|\mathcal{G}/\mathcal{N}|$ kleiner als $|\mathcal{G}|$. Somit ist eine Induktion nach $|\mathcal{G}|$ vielversprechend. Der Induktionsanfang sind dann Gruppen, die keinen solchen Normalteiler besitzen. Diese nennt man **einfach**. Eine der großen Leistungen dieses Jahrhunderts ist die Klassifikation aller endlichen einfachen Gruppen.

(6.21) Beispiel: Sei $\mathcal{G} = \mathbb{Z}(+)$. Für $m \in \mathbb{N}$ setze $\mathcal{U} = m\mathbb{Z}$. Dann ist $\mathcal{U} \trianglelefteq \mathcal{G}$. Für $r \in \mathbb{Z}$ ist

$$r + m\mathbb{Z} = \{x \in \mathbb{Z} \mid x \equiv r \text{ (modulo } m)\}$$

Man nennt das auch die Restklasse von r modulo m. Es gilt

$$\mathbb{Z} = \bigcup_{r=0}^{m-1} (r + m\mathbb{Z})$$

Wir schreiben $\mathbb{Z}_m$ für die Menge dieser Restklassen, also $\mathbb{Z}/m\mathbb{Z}$.

Abkürzend schreibe $\bar{x}$ für $x + m\mathbb{Z}$. Dann gilt nach (6.20)

$$\bar{x} + \bar{y} = \overline{x + y}.$$

Die Abbildung $k : \mathbb{Z} \to \mathbb{Z}$ mit $k(x) = \bar{x}$ ist also ein Homomorphismus von $\mathbb{Z}$ auf $\mathbb{Z}/m\mathbb{Z}$.

(6.22) Satz: *Seien $\mathcal{G}$ und $\mathcal{G}'$ Gruppen und $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann ist* $\operatorname{Ker} f \trianglelefteq \mathcal{G}$.

Beweis: Sei $g \in \mathcal{G}$. Wir müssen $g(\operatorname{Ker} f) = (\operatorname{Ker} f)g$ zeigen. Nach (6.15) ist $g(\operatorname{Ker} f) = f^{-}\{f(g)\}$. Sei $xg \in (\operatorname{Ker} f)g$, mit $x \in \operatorname{Ker} f$. Dann gilt

$$f(xg) = f(x)f(g) = e'f(g) = f(g).$$

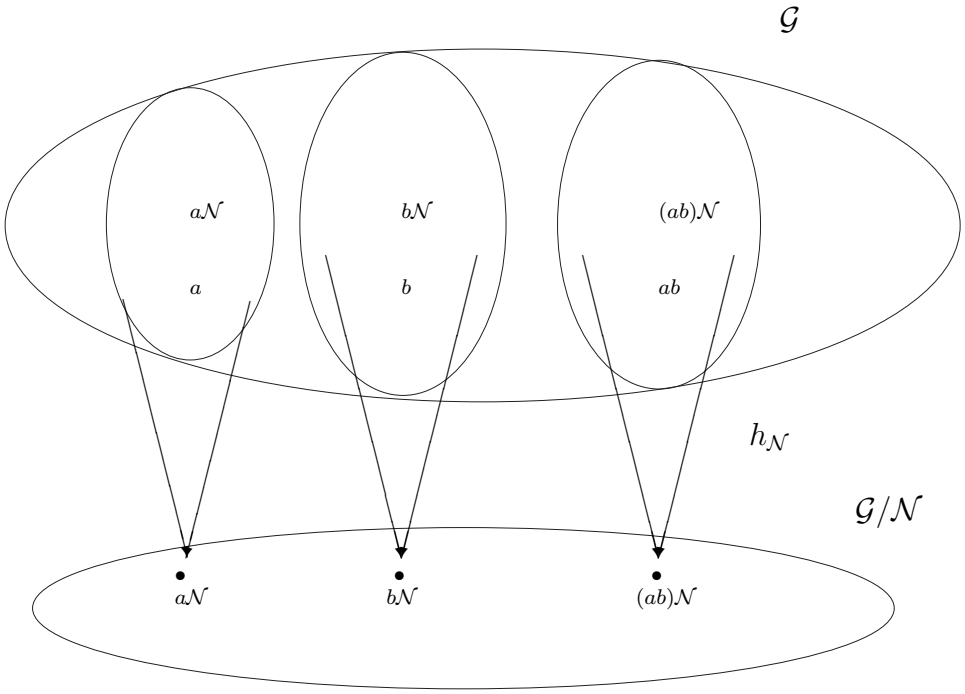
Also ist auch $(\operatorname{Ker} f)g \subseteq f^-\{f(g)\}$.

Sei nun umgekehrt $f(y) = f(g)$. Dann ist $f(yg^{-1}) = f(y)f(g)^{-1} = e'$. Also ist $yg^{-1} \in \operatorname{Ker} f$ und $y \in (\operatorname{Ker} f)g$. Damit ist $f^-\{f(g)\} \subseteq (\operatorname{Ker} f)g$. Somit haben wir

$$(\operatorname{Ker} f)g = g\,(\operatorname{Ker} f).\square$$

Ist f ein Homomorphismus, so haben wir gesehen, daß $\operatorname{Ker} f$ ein Normalteiler ist. Wir wollen nun zeigen, daß auch die Umkehrung hiervon gilt, also ist $\mathcal{N}$ ein Normalteiler, so gibt es einen Homomorphismus f, der genau $\mathcal{N}$ als Kern hat. Hierzu verallgemeinern wir zunächst den Homomorphismus k aus (6.21).

(6.23) Lemma: *Sei $\mathcal{N}$ ein Normalteiler der Gruppe $\mathcal{G}$. Dann ist $h_{\mathcal{N}} : \mathcal{G} \to \mathcal{G}/\mathcal{N}$ mit $h_{\mathcal{N}}(x) = x\mathcal{N}$ ein Homomorphismus von $\mathcal{G}$ auf $\mathcal{G}/\mathcal{N}$ mit* $\operatorname{Ker} h_{\mathcal{N}} = \mathcal{N}$.



Beweis: (a) $h_{\mathcal{N}}$ ist Homomorphismus. Seien $a, b \in \mathcal{G}$. Dann ist

$$h_{\mathcal{N}}(ab) = (ab)\mathcal{N} = (a\mathcal{N}) \circ (b\mathcal{N}) = h_{\mathcal{N}}(a) \circ h_{\mathcal{N}}(b).$$

(b) Klar ist, daß $h_{\mathcal{N}}$ surjektiv ist.

(c) Sei $x \in \operatorname{Ker} h_{\mathcal{N}}$. Dann ist

$$\mathcal{N} = h_{\mathcal{N}}(x) = x\mathcal{N}.$$

Also ist $x \in \mathcal{N}$. Ist umgekehrt $x \in \mathcal{N}$, so ist $h_{\mathcal{N}}(x) = x\mathcal{N} = \mathcal{N}$, d.h. $x \in \operatorname{Ker} h_{\mathcal{N}}$.$\square$

(6.24) Definition: Wir nennen den Homomorphismus $h_{\mathcal{N}}$ aus (6.23) den **kanonischen Homomorphismus**.

(6.25) Homomorphiesatz: *Seien $\mathcal{G}$ und $\mathcal{G}'$ Gruppen und $f : \mathcal{G} \to \mathcal{G}'$ ein Homomorphismus. Dann gilt*

$$\mathcal{G}/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$$

Beweis: Wir definieren eine Abbildung

$$i : \mathcal{G}/\mathrm{Ker}\, f \to \mathrm{Im}\, f$$

durch

$$i(a\,\mathrm{Ker}\, f) = f(a) \quad , \quad a \in \mathcal{G}.$$

Zunächst ist zu zeigen, daß i eine Abbildung ist. Dazu ist zu zeigen, daß der Wert von i in obiger Definition von der Auswahl des Vertreters a der Nebenklasse unabhängig ist. Sei dazu $a\,\mathrm{Ker}\, f = a'\mathrm{Ker}\, f$, also $a' = ax$, mit geeignetem $x \in \mathrm{Ker}\, f$. Dann ist

$$i(a'\mathrm{Ker}\, f) = f(a') = f(ax) = f(a)f(x) \underset{x\in\mathrm{Ker}\, f}{=} f(a) = i(a\,\mathrm{Ker}\, f).$$

Nun zeigen wir, daß i ist ein Homomorphismus ist. Seien $a, b \in \mathcal{G}$. Dann ist

$$i((a\,\mathrm{Ker}\, f)(b\,\mathrm{Ker}\, f)) = i((ab)\mathrm{Ker}\, f) = f(ab) = f(a)f(b) = i(a\,\mathrm{Ker}\, f)i(b\,\mathrm{Ker}\, f).$$

Wir zeigen, daß i surjektiv ist. Sei $a' \in \mathrm{Im}\, f$. Dann gibt es ein $a \in \mathcal{G}$ mit $f(a) = a'$. Also gilt:

$$i(a\,\mathrm{Ker}\, f) = f(a) = a'.$$

Schließlich zeigen wir noch, daß i injektiv ist. Nach (6.14) genügt es,

$$\mathrm{Ker}\, i = \{\mathrm{Ker}\, f\}$$

zu zeigen.

$$\begin{aligned} \mathrm{Ker}\, i &= \{a\,\mathrm{Ker}\, f \mid a \in \mathcal{G}, i(a\,\mathrm{Ker}\, f) = e'\} = \{a\,\mathrm{Ker}\, f \mid a \in \mathcal{G} \text{ und } f(a) = e'\} \\ &= \{a\,\mathrm{Ker}\, f \mid a \in \mathrm{Ker}\, f\} = \{\mathrm{Ker}\, f\}.\square \end{aligned}$$

Aus (6.25) folgt, daß alle homomorphen Bilder einer Gruppe $\mathcal{G}$ isomorph zu den Faktorgruppen von $\mathcal{G}$ sind. Kennt man also alle Normalteiler von $\mathcal{G}$, so kennt man auch die Struktur aller homomorphen Bilder. Nur die Gruppe $\mathcal{G}$ ist entscheidend, die Gruppe $\mathcal{G}'$ spielt somit keine Rolle mehr.

Übungsaufgaben

1) Zeige: $\mathbb{Z}$ mit der Verknüpfung

$$a * b = a + b - 1$$

ist eine kommutative Gruppe ($+$ und $-$ beziehen sich dabei auf die gewöhnliche Zahlenaddition und -subtraktion).

2) Sei $\mathcal{G}$ eine Gruppe, e das Einselement von $\mathcal{G}$ und $a \in \mathcal{G}$. Man definiere Potenzen von a rekursiv durch:
$a^0 = e$, $a^k = a \cdot a^{k-1}$, $k \in \mathbb{N}$,
$a^k = (a^{-k})^{-1}$, $k \in \mathbb{Z}$, $-k \in \mathbb{N}$.

Zeige:

(a) $a^{j+k} = a^j \cdot a^k$, für alle $j, k \in \mathbb{Z}$
(b) $a^{jk} = (a^j)^k$, für alle $j, k \in \mathbb{Z}$.

3) Sei $\mathcal{G}$ eine Gruppe und $a, b \in \mathcal{G}$. Zeige : Sind a und b vertauschbar, d.h. $ab = ba$, so ist $(ab)^k = a^k b^k$ für alle $k \in \mathbb{Z}$.

4) Sei $\mathcal{G}$ eine Gruppe, e das Einselement von $\mathcal{G}$. Zeige :

(a) Ist $a = a^{-1}$ für alle $a \in \mathcal{G}$, so ist $\mathcal{G}$ kommutativ.
(b) Ist $a^2 = e$ für alle $a \in \mathcal{G}$, so ist $\mathcal{G}$ kommutativ.
(c) Ist $(ab)^2 = a^2 \cdot b^2$ für alle $a, b \in \mathcal{G}$, so ist $\mathcal{G}$ kommutativ.

5) Sei $\mathcal{G}$ eine Gruppe und $\mathcal{M}$ eine Teilmenge von $\mathcal{G}$. Setze

$$\mathcal{C}_{\mathcal{G}}(\mathcal{M}) = \{x \mid x \in \mathcal{G},\, xm = mx \text{ für alle } m \in \mathcal{M}\}.$$

Zeige, daß $\mathcal{C}_{\mathcal{G}}(\mathcal{M})$ eine Untergruppe von $\mathcal{G}$ ist.

6) Sei $\mathcal{G}$ eine endliche Gruppe, die eine gerade Anzahl von Elementen enthält. Zeige, daß ein vom neutralen Element e verschiedenes Element a mit $a^2 = e$ existiert.

7) Sei $\mathcal{G}$ eine Gruppe mit der Eigenschaft, daß für drei aufeinanderfolgende ganze Zahlen i gilt

$$(ab)^i = a^i b^i \text{ für alle } a, b \in \mathcal{G}.$$

Zeige, $\mathcal{G}$ ist kommutativ.

8) Seien $\mathcal{G}$ und $\mathcal{H}$ Gruppen und α ein Homomorphismus von $\mathcal{G}$ nach $\mathcal{H}$. Zeige:

(a) Ist $\mathcal{M} \trianglelefteq \mathcal{H}$, so ist $\alpha^-(\mathcal{M}) = \{x \mid x \in \mathcal{G}, \alpha(x) \in \mathcal{M}\}$ ein Normalteiler von $\mathcal{G}$.
(b) Ist α ein Epimorphismus und $\mathcal{N} \trianglelefteq \mathcal{G}$, so ist $\alpha(\mathcal{N}) \trianglelefteq \mathcal{G}$.

9) $\tilde{\mathcal{Q}} = \{\frac{m}{n} \mid m, n \in \mathbb{N}\}$ ist eine Gruppe bezüglich der normalen Multiplikation rationaler Zahlen.

   (a) Zeige $\mathcal{S} = \{2^k \mid k \in \mathbb{Z}\}$ ist eine Untergruppe von $\tilde{\mathcal{Q}}$.

   (b) Gib eine Menge $\mathcal{R} \subseteq \tilde{\mathcal{Q}}$ an, so daß gilt
   (1) $\tilde{\mathcal{Q}} = \bigcup_{r \in \mathcal{R}} r\mathcal{S}$
   (2) $r\mathcal{S} \cap r'\mathcal{S} = \varnothing$ für $r, r' \in \mathcal{R},\ r \neq r'$.

10) Sei $\mathbb{R}^*$ die Gruppe der von 0 verschiedenen reellen Zahlen bezüglich der Multiplikation, $\mathcal{Q}^*$ die Gruppe der von 0 verschiedenen rationalen Zahlen bezüglich der Multiplikation und $\mathbb{Z}$ die Gruppe der ganzen Zahlen bezüglich der Addition.

    Man prüfe nach, ob die folgenden Abbildungen Gruppenhomomorphismen sind. (Wo dies der Fall ist, beweise man es, wo nicht, belege man dies durch ein Gegenbeispiel)
    $\psi : \mathbb{R}^* \to \mathbb{R}^*$ definiert durch $\psi(x) = x^4$, $x \in \mathbb{R}^*$
    $\varphi : \mathcal{Q}^* \to \mathbb{R}^*$ definiert durch $\varphi(x) = 2^x$, $x \in \mathcal{Q}^*$
    $\sigma : \mathbb{Z} \to \mathcal{Q}^*$ definiert durch $\sigma(x) = 2^x$, $x \in \mathbb{Z}$.

11) Sei φ ein Homomorphismus einer Gruppe $\mathcal{G}$ in eine Gruppe $\mathcal{H}$. Es sei $\mathcal{U}$ die Menge der Untergruppen von $\mathcal{G}$, die Ker φ enthalten. Sei ferner $\mathcal{T}$ die Menge aller Untergruppen von $\varphi(\mathcal{G})$. Man zeige, daß

$$\beta : \begin{cases} \mathcal{U} \to \mathcal{T} \\ u \to \varphi(u) \end{cases} \quad , u \in \mathcal{U}$$

    eine bijektive Abbildung von $\mathcal{U}$ auf $\mathcal{T}$ ist.

12) Sei $\mathcal{G}$ eine Gruppe, $\mathcal{H} \leq \mathcal{G}$ und $\mathcal{N} \trianglelefteq \mathcal{G}$. Zeige, daß $\mathcal{N} \cap \mathcal{H} \trianglelefteq \mathcal{H}$ ist.

13) Sei $\mathcal{G}$ eine Gruppe und $\mathcal{N} \leq \mathcal{G}$. Setze

$$g^{-1}\mathcal{N}g = \{g^{-1}ng \mid n \in \mathcal{N}\},\ g \in \mathcal{G}.$$

    Zeige:

    (a) $\mathcal{N}$ ist genau dann normal in $\mathcal{G}$, falls $g^{-1}\mathcal{N}g = \mathcal{N}$ für alle $g \in \mathcal{G}$ ist.

    (b) Für jedes $g \in \mathcal{G}$ ist $g^{-1}\mathcal{N}g$ eine Untergruppe von $\mathcal{G}$.

    (c) Setze $\mathcal{M} = \bigcap_{g \in \mathcal{G}} g^{-1}\mathcal{N}g$. Dann ist $\mathcal{M} \trianglelefteq \mathcal{G}$ und $\mathcal{M}$ ist der größte Normalteiler von $\mathcal{G}$, der in $\mathcal{N}$ liegt.

14) Sei $\mathcal{G}$ eine Gruppe und α ein Homomorphismus von $\mathcal{G}$ nach $\mathcal{G}$. Sei $\mathcal{N} \trianglelefteq \mathcal{G}$ mit $\alpha(\mathcal{N}) \subseteq \mathcal{N}$.

    (a) Zeige, daß durch die Vorschrift
$$\bar{\alpha}(g\mathcal{N}) = (\alpha(g))\mathcal{N}$$
    ein Homomorphismus $\bar{\alpha}$ von $\mathcal{G}/\mathcal{N}$ nach $\mathcal{G}/\mathcal{N}$ definiert wird.

    (b) Ist α ein Automorphismus von $\mathcal{G}$, so ist die in (a) definierte Abbildung ein Automorphismus von $\mathcal{G}/\mathcal{N}$.

15) Seien m und n natürliche Zahlen. Zeige

$$m\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}.$$

(Hinweis: Wende auf $\varphi : m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, definiert durch $\varphi(mr) = r + n\mathbb{Z}$, $r \in \mathbb{Z}$, den Homomorphiesatz an)

16) Sei $\mathcal{U}$ eine Untergruppe von $\mathcal{G}$. Zeige: Hat $\mathcal{U}$ genau zwei Linksnebenklassen $\mathcal{U} = e\mathcal{U}$ und $x\mathcal{U}$, so ist $\mathcal{U} \trianglelefteq \mathcal{G}$.

§7 Ringe und Körper

Außer der Verknüpfung + gab es in § 0 stets noch die Skalarmultiplikation. Dabei waren die Skalare reelle Zahlen. Fragen der Anwendung fordern, daß auch andere Skalarenbereiche zugelassen werden.

Wir werden von den reellen und komplexen Zahlen ausgehend die Begriffe Ring und Körper definieren. Dies scheint zunächst nicht sonderlich interessant zu sein, da wir außer $\mathbb{R}$, $\mathbb{C}, \mathbb{Q}$ und $\mathbb{Z}$ kaum Beispiele kennen. Das wird sich aber in §13 und §25 ändern. Auch werden wir sehen, daß es einen Körper gibt, der nur aus 0 und 1 besteht. Dieser verhält sich in vielerlei Hinsicht anders als die reellen Zahlen. Er spielt in der Kodierungstheorie und der theoretischen Informatik eine wichtige Rolle. Es ist bemerkenswert, daß unsere noch zu entwickelnde Theorie der Vektorräume nicht zwischen dem Körper $\mathbb{R}$ und jenem, der nur zwei Elemente besitzt, unterscheidet.

(7.1) Definition: Sei $\mathcal{R}$ eine nicht leere Menge. Auf $\mathcal{R}$ seien zwei Verknüpfungen definiert:

$$\text{“}+\text{”}: \begin{cases} \mathcal{R} \times \mathcal{R} \to \mathcal{R} \\ (a,b) \to a+b \end{cases} \quad \text{und} \quad \text{“}\cdot\text{”}: \begin{cases} \mathcal{R} \times \mathcal{R} \to \mathcal{R} \\ (a,b) \to a \cdot b =: ab \end{cases}$$

so daß folgendes gilt:

(1) $\mathcal{R}(+)$ ist eine abelsche Gruppe.

(2) Für alle $a, b, c \in \mathcal{R}$ gilt

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

Es gibt ein Element $e \in \mathcal{R}$ mit $e \cdot a = a = a \cdot e$ für alle $a \in \mathcal{R}$.

(3) Für alle $a, b, c \in \mathcal{R}$ gilt

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

Dann nennen wir $\mathcal{R}$ einen **Ring**

(4) Gilt zusätzlich, daß $\mathcal{R} \setminus \{0\}$ bezüglich “$\cdot$” eine kommutative Gruppe ist, so nennen wir $\mathcal{R}$ einen **Körper**[1]

[1] Das erste Lehrbuch, das den Begriff des Körpers, wie er hier vorgestellt wurde, enthält, ist das Buch von H. Weber “Algebra” von 1893. Der Begriff Körper geht wohl auf Dedekind (1871) zurück.

(7.2) Beispiele: (a) $\mathbb{Z}(+,\cdot)$; $\mathbb{Q}(+,\cdot)$; $\mathbb{R}(+,\cdot)$; $\mathbb{C}(+,\cdot)$ sind Ringe. Die letzten drei sind Körper. Aber $\mathbb{Z}(+,\cdot)$ ist kein Körper.

(b) $\mathbb{Z}_m(+,\cdot)$; $m \in \mathbb{N}$, ist ein Ring (siehe (6.21)). Hierbei ist

$$(r + m\mathbb{Z}) \cdot (s + m\mathbb{Z}) := rs + m\mathbb{Z}.$$

Ist m keine Primzahl, also $m = r \cdot s$ mit $r \neq m \neq s$, so gilt

$$(r + m\mathbb{Z}) \cdot (s + m\mathbb{Z}) = r \cdot s + m\mathbb{Z} = m\mathbb{Z}.$$

Also kann in $\mathbb{Z}_m$ das Produkt zweier von Null verschiedener Elemente gleich Null sein. Insbesondere ist $\mathbb{Z}_m$ kein Körper, denn sei

$$t + m\mathbb{Z} \in \mathbb{Z}_m \text{ mit } (t + m\mathbb{Z})(r + m\mathbb{Z}) = 1 + m\mathbb{Z},$$

dann ist

$$\begin{aligned} s + m\mathbb{Z} &= (1 + m\mathbb{Z}) \cdot (s + m\mathbb{Z}) = ((t + m\mathbb{Z}) \cdot (r + m\mathbb{Z})) \cdot (s + m\mathbb{Z}) \\ &= (t + m\mathbb{Z}) \cdot ((r + m\mathbb{Z}) \cdot (s + m\mathbb{Z})) = (t + m\mathbb{Z}) \cdot (o + m\mathbb{Z}) = m\mathbb{Z}. \end{aligned}$$

Das liefert aber, daß s von m geteilt wird, ein Widerspruch.

Es kann also in einem Ring durchaus $ab = 0$ sein, ohne daß $a = 0$ oder $b = 0$ ist. Auf der anderen Seite gibt es Ringe wie $\mathbb{Z}$, in denen das nicht vorkommt. Das führt zu der folgenden Definition.

(7.3) Definition: (a) Ein Ring $\mathcal{R}$ heißt **nullteilerfrei**, falls für alle $a, b \in \mathcal{R}$ stets gilt:

$$\text{Ist } ab = 0, \text{ so ist } a = 0 \text{ oder } b = 0.$$

(b) Ein Ring heißt **Integritätsbereich**, falls er nullteilerfrei ist, $ab = ba$ für alle $a, b \in \mathcal{R}$ gilt, und $|\mathcal{R}| \geq 2$ ist.

Die Ringe in (7.2)(a) sind sämtlich Integritätsbereiche. Nun können wir (7.2) (b) aufgreifen und beweisen:

(7.4) Lemma: *Sei K ein Körper*

(a) *Ist $a \in K$, so ist $a \cdot 0 = 0 \cdot a = 0$.*

(b) *K ist nullteilerfrei.*

Beweis: (a) Es ist $0 \cdot a + 1 \cdot a = (0+1) \cdot a = 1 \cdot a = 0 + 1 \cdot a$. Also ist $0 \cdot a = 0$. Genauso folgt $a \cdot 0 = 0$.

(b) Seien $a, b \in K$ mit $ab = 0$. Sei $a \neq 0$. Dann gibt es ein $c \in K$ mit $ca = 1$. Nun gilt: $b = 1 \cdot b = (ca)b = c(ab) = c \cdot 0 \underset{(a)}{=} 0$.□

(7.5) Beispiele: (a) Sei $\mathcal{X}$ eine Menge und $\mathcal{R}$ ein kommutativer Ring ($ab = ba$ für alle $a, b \in \mathcal{R}$). Sei $\mathcal{A}$ die Menge aller Abbildungen von $\mathcal{X}$ nach $\mathcal{R}$. Für $f, g \in \mathcal{A}$ definiere:

$$\begin{array}{rcl} f + g : x & \to & f(x) + g(x) \\ f \ \cdot \ g : x & \to & f(x) \cdot g(x) \end{array}$$

Dann ist $\mathcal{A}$ ein kommutativer Ring, der i.a. nicht nullteilerfrei ist.

(b) Sei $\mathcal{G}(+)$ eine abelsche Gruppe und

$$End(\mathcal{G}) = \{f \mid f : \mathcal{G} \to \mathcal{G},\ f \text{ ist Homomorphismus}\}.$$

Definiere für $f, g \in End(\mathcal{G})$:

$$\begin{array}{rcl} f + g : x & \to & f(x) + g(x) \\ f \ \cdot \ g : x & \to & f(g(x)) \end{array}$$

Dann ist $End(\mathcal{G})$ bezüglich $+$ und $\cdot$ ein Ring, der sogenannte **Endomorphismenring** von $\mathcal{G}$.

(c) Sei $\mathcal{R} = \{0, 1\}$ mit den Verknüpfungen $\oplus$ und $\odot$, die durch die folgenden Tafeln gegeben sind :

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

Man kann 0 als "gerade" und 1 als "ungerade" interpretieren. Die obigen Tafeln repräsentieren dann das Verhalten der Addition und Multiplikation gerader und ungerader Zahlen. $\mathcal{R}$ ist mit diesen Verknüpfungen ein Körper.

(d) Für jede Primzahl p ist $\mathbb{Z}_p$ ein Körper. Dies wollen wir hier nicht beweisen (Siehe aber Aufgabe 6). Spezialfall $p = 2$:

$$\mathcal{R} = \{\bar{0}, \bar{1}\}, \quad \bar{0} = 0 + 2\mathbb{Z}, \quad \bar{1} = 1 + 2\mathbb{Z}.$$

Die Verknüpfungen $\overline{x + y} = \bar{x} + \bar{y}$ und $\overline{xy} = \bar{x}\bar{y}$ führen zu den folgenden Tabellen:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Ein Vergleich mit Beispiel (c) zeigt, daß die Bijektion

$$i : \begin{cases} \mathbb{Z}_2 & \to & \{0,1\} \\ \bar{0} & \to & 0 \\ \bar{1} & \to & 1 \end{cases}$$

sowohl mit den Additionen als auch mit den Multiplikationen auf $\mathbb{Z}_2$ und $\{0,1\}$ "verträglich" ist. Dies wollen wir gleich in eine Definition aufnehmen.

(7.6) Definition: Seien $(\mathcal{R}, +, \cdot)$ und $(\mathcal{S}, \hat{+}, \hat{\cdot})$ Ringe. Eine Abbildung $f : \mathcal{R} \to \mathcal{S}$ heißt (Ring-) **Homomorphismus**, falls für alle $x, y \in \mathcal{R}$

$$f(x+y) = f(x)\hat{+}f(y) \text{ und } f(x \cdot y) = f(x)\hat{\cdot}f(y)$$

gilt. Ein bijektiver (Ring-) Homomorphismus heißt (Ring-) Isomorphismus.

Die Abbildung i aus (7.5) (d) ist also ein Ring-Isomorphismus zwischen den beiden Ringen $(\mathbb{Z}_2, +, \cdot)$ und $(\{0,1\}, \oplus, \odot)$.

Sei $m \in \mathbb{N}$. Die Abbildung $^- : x \to x + m\mathbb{Z}$ aus (6.21) ist ein Ringhomomorphismus von $\mathbb{Z}$ nach $\mathbb{Z}_m$.

Anwendung: "Neunerprobe": Gegeben sei $n \in \mathbb{N}$. Wir fragen, ob 9 ein Teiler von n ist.

Seien $a_0, \ldots, a_k$ die Ziffern der Dezimaldarstellung von n. Also $n = \sum_{i=0}^{k} a_i 10^i$. Gehen wir nach $\mathbb{Z}_9$ über, so lautet die Frage, ob $\bar{n} = \bar{0}$ ist.

$$\bar{n} = \overline{\sum_{i=0}^{k} a_i 10^i} = \sum_{i=0}^{k} \overline{a_i 10^i} = \sum_{i=0}^{k} \bar{a}_i \overline{10}^i = \sum_{i=0}^{k} \bar{a}_i \bar{1} = \sum_{i=0}^{k} \bar{a}_i = \overline{\sum_{i=0}^{k} a_i}.$$

Hierbei haben wir mehrfach benutzt, daß $x \to \bar{x}$ ein Ring-Homomorphismus ist. Weiter haben wir $\overline{10} = \bar{1}$ benutzt. Nun folgt offenbar die bekannte Regel:

n ist genau dann durch 9 teilbar, wenn die Quersumme durch 9 teilbar ist.

Wir haben die Körper $\mathbb{R}$ und $\mathbb{Z}_2$ kennengelernt. Es gibt einen wichtigen Unterschied zwischen diesen Körpern. In $\mathbb{Z}_2$ gilt $1 + 1 = 0$, was in $\mathbb{R}$ falsch ist. Dies führt zu der folgenden Definition.

(7.7) Definition: Sei $(K, +, \cdot)$ ein Körper.

(a) Für $a \in K,\ n \in \mathbb{N}$ definieren wir

$$n \cdot a := \underbrace{a + a + \ldots + a}_{n \text{ Summanden}} = \underbrace{(1 + 1 + \ldots + 1)}_{n \text{ Summanden}} \cdot a = (n \cdot 1) \cdot a$$

(wobei 1 das neutrale Element in K sei).

(b) Ist $m \cdot 1 \neq 0$ für alle $m \in \mathbb{N}$, so sagen wir: K hat die **Charakteristik** 0; in Zeichen: $\operatorname{char} K = 0$. Andernfalls nennen wir die kleinste natürliche Zahl n mit $n \cdot 1 = 0$ die Charakteristik von K : $\operatorname{char} K = n$.

(7.8) Beispiele: $\mathbb{Z}_2$ hat Charakteristik 2; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben Charakteristik 0.

Es erhebt sich nun die Frage, welche Zahlen als Charakteristik vorkommen können. Der nächste Satz sagt aus, daß es z.B. keinen Körper der Charakteristik 4 gibt.

(7.9) Satz: *Ist K ein Körper und* $\operatorname{char} K \neq 0$*, so ist* $\operatorname{char} K$ *eine Primzahl.*

Beweis: Sei $\operatorname{char} K = p \cdot q$ mit $p, q \neq 1$ und $p, q \in \mathbb{N}$. Es gilt

$$0 = (p \cdot q) \cdot 1 \ = \ \underbrace{(1 + 1 + \ldots + 1)}_{p \cdot q - \text{Summanden}} \ = \ \underbrace{(1 + \ldots + 1)}_{p - \text{Summanden}} \cdot \underbrace{(1 + \ldots 1)}_{q - \text{Summanden}} \ = \ (p \cdot 1)(q \cdot 1).$$

Da ein Körper nullteilerfrei ist, (7.4)(b), folgt: $p \cdot 1 = 0$ oder $q \cdot 1 = 0$, ein Widerspruch.□

Es kommt jede Primzahl als Charakteristik vor. Die Körper $\mathbb{Z}_p$ haben stets die Charakteristik p. Diese spielen in den Anwendungen eine immer wichtigere Rolle. Obwohl sie sehr verschieden zu $\mathbb{R}$ und $\mathbb{C}$ sind, gelten doch alle Sätze, die aus (7.1) abgeleitet werden, gleichzeitig für $\mathbb{R}$ und $\mathbb{Z}_p$.

Übungsaufgaben

1) Zeige: Ist $K \subseteq \mathbb{R}$ ein Körper bezüglich der auf $\mathbb{R}$ definierten Multiplikation und Addition, so ist $\mathbb{Q} \subseteq K$.

2) Jeder endliche Integritätsbereich $\mathcal{R}$ mit $|\mathcal{R}| \geq 2$ ist ein Körper.

3) In einem beliebigen Körper gilt $x^2 = 1$ nur für $x = 1$ und $x = -1$. Wie sieht das in $\mathbb{Z}_8$ aus?

4) Zeige an einem Beispiel, daß eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$, die die folgenden Axiome erfüllen, kein Körper zu sein braucht:

   (1) K mit $+$ ist eine abelsche Gruppe.

   (2) $K \setminus \{0\}$ mit $\cdot$ ist eine abelsche Gruppe.

   (3) Für alle $a, b, c \in K$ ist
   $$a(b+c) = ab + ac$$

   (Hinweis: Es gibt ein Beispiel mit einer Menge K mit $|K| = 2$)

5) Sei $K = \mathbb{Z}_2$. Wir definieren auf $K \times K$ Verknüpfungen $+$ und $\cdot$ durch
$$\begin{aligned}(a,b) + (c,d) &= (a+c, b+d)\\ (a,b) \cdot (c,d) &= (ac+bd, ad+bc+bd)\end{aligned}$$
   für alle $a, b, c, d \in K$.

   Zeige, daß $K \times K$ dadurch zu einem Körper mit 4 Elementen wird.
   Ist $K \times K \cong \mathbb{Z}_4$?

6) Sei p eine Primzahl und $r \in \mathbb{Z}$ mit $p \nmid r$.

   a) (Euklidischer Algorithmus) Setze $r = x_0$ und $p = x_1$. Betrachte den folgenden Algorithmus : Setze
   $$x_{i-1} = \lambda_i x_i + x_{i+1}, \text{ mit } |x_{i+1}| < |x_i|, \text{ falls } x_i \neq 0 \text{ ist }, i \geq 1, \text{ und } \lambda_i \in \mathbb{Z}.$$
   (Division von x_{i-1} durch x_i mit Rest.)
   Der Algorithmus endet, falls $x_j = 0$ ist. Zeige, daß dann $|x_{j-1}| = 1$ gilt.

   b) Es gibt $a, b \in \mathbb{Z}$ mit
   $$ap + br = 1.$$
   (Benutze a).

   c) Sei $\bar{x} \in \mathbb{Z}_p$ mit $\bar{x} \neq \bar{0}$. Zeige, daß es ein $\bar{y} \in \mathbb{Z}_p$ mit $\bar{x}\bar{y} = \bar{1}$ gibt.
   (Benutze b).

   d) Zeige, daß $\mathbb{Z}_p$ ein Körper ist.