

10. Algebraische Strukturen

Die gewöhnlichen mit Zahlen ausgeführten Rechenoperationen (Verknüpfungen) $+$ und \cdot weisen eine Reihe gemeinsamer Eigenschaften auf. Dazu gehört z.B. das Kommutativgesetz ($a + b = b + a$ und $a \cdot b = b \cdot a$) und die analoge Rolle von 0 und 1 in den Gleichungen $a + 0 = a$ bzw. $a \cdot 1 = a$. Auch in anderen Bereichen, etwa in der Mengenalgebra, stößt man auf verwandte Rechengesetze. Die *Algebra* untersucht diese Verhältnisse allgemein und abstrahiert dabei von der besonderen Beschaffenheit der Objekte, mit denen gerechnet wird. Dadurch lassen sich einfachere Begriffe bilden und deren Beziehungen untereinander rationeller (im Sinne einer Denkökonomie) untersuchen. Algebraische Strukturen (Verknüpfungsgebilde) sind Mengen, auf denen Operationen (Verknüpfungen) gegeben sind.

10.1. Verknüpfungsgebilde

Der Begriff "Verknüpfung" stellt eine Verallgemeinerung der gewöhnlichen Rechenoperationen für Zahlen dar. Naheliegende Beispiele für Verknüpfungen sind die von den "Grundrechenarten" her geläufigen Operationen "Addition", "Subtraktion", "Multiplikation" und "Division".

Zum Beispiel wird die Addition zweier ganzer Zahlen x, y aufgefasst als eine Abbildung $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, die dem geordneten Paar (x, y) als Bild die Summe $x + y$ zuordnet: $+(x, y) := x + y$. (Die streng eingehaltene Abbildungsnotation ist, zumindest für zweistellige Verknüpfungen, ungewohnt und unüblich. Anstatt den Abbildungsnamen *vor* das Urbild zu schreiben, wird die herkömmliche Schreibweise beibehalten und das Verknüpfungszeichen *zwischen* die Komponenten des Urbild-Paars geschrieben.)

■ 10.1.1. Definition

Seien A und B nichtleere Mengen. Abbildungen vom Typ $A^2 \rightarrow B$ heißen (zweistellige oder binäre) Verknüpfungen oder Operationen auf A mit Werten in B . Im Falle $B = A$ heißt $\perp : A^2 \rightarrow A$ Verknüpfung in A . Es bezeichnet $x \perp y$ den Funktionswert von $(x, y) \in A^2$ unter \perp .

Zum Beispiel ist die Subtraktion natürlicher Zahlen eine Verknüpfung auf \mathbb{N} mit Werten in \mathbb{Z} , jedoch keine Verknüpfung *in* \mathbb{N} . Bei der Addition natürlicher Zahlen können wir hingegen die kleinere Zielmenge \mathbb{N} wählen, denn es gilt $x + y \in \mathbb{N}$ für alle $x, y \in \mathbb{N}$, d.h. $+$ ist eine Verknüpfung *in* \mathbb{N} .

■ Bezeichnungen

Ist \perp eine Verknüpfung in A , so wird das geordnete Paar (A, \perp) als Verknüpfungsgebilde bezeichnet. A heißt in diesem Zusammenhang Träger(menge) des Verknüpfungsgebildes. Ein anderer Ausdruck für Verknüpfungsgebilde ist algebraische Struktur.

■ Beispiele algebraischer Strukturen

$(\mathbb{Q}, +)$	Addition rationaler Zahlen
(\mathbb{R}, \cdot)	Multiplikation reeller Zahlen
$(\mathbb{Q} \setminus \{0\}, \div)$	Division rationaler Zahlen $\neq 0$
$(\mathbb{Z}, -)$	Subtraktion ganzer Zahlen
(\mathbb{Z}_m, \oplus)	Restklassenaddition modulo m
(\mathcal{S}_n, \circ)	Verkettung von Permutationen
$(\mathcal{P}(M), +)$	Boolesche Summe von Mengen

Man mache sich bei jedem dieser Beispiele klar, weshalb eine Verknüpfung in der jeweils angegebenen Trägermenge vorliegt.

Keine Verknüpfungsgebilde entstehen durch ...

- \mathbb{N} mit der Subtraktion,
- \mathbb{Q} mit der Division,
- \mathbb{Z} mit dem arithmetischen Mittel $\frac{x+y}{2}$ zweier ganzer Zahlen x, y ,
- die Menge aller Spiegelungen (einer Ebene) mit der Verkettung \circ .

Die Verknüpfungsgebilde (\mathcal{S}_n, \circ) und $(\mathcal{P}(M), +)$ zeigen, dass man auch mit Abbildungen bzw. mit Mengen in ähnlichem Sinne wie mit gewöhnlichen Zahlen rechnen kann.

Von besonderer Bedeutung sind in dieser Hinsicht die Restklassenmengen \mathbb{Z}_m , $m \geq 2$, für die wir in Abschnitt 7.3 eine Addition \oplus und eine Multiplikation \odot eingeführt haben.

In einem Verknüpfungsgebilde (A, \perp) tritt gelegentlich die Frage auf, ob sich die Verknüpfung \perp auf eine bestimmte Teilmenge $M \subset A$ einschränken lässt. Man betrachte etwa $(\mathbb{Z}, +)$ und die Teilmenge $2\mathbb{Z}$ der geraden ganzen Zahlen. Offensichtlich ist $x + y \in 2\mathbb{Z}$ für alle $x, y \in 2\mathbb{Z}$; somit lässt sich $(2\mathbb{Z}, +)$ als ein abgeschlossenes Teilgebilde von $(\mathbb{Z}, +)$ auffassen. Das gibt Anlass zu folgender

■ 10.1.2. Definition

Sei (A, \perp) ein Verknüpfungsgebilde. Eine nichtleere Teilmenge M von A heißt abgeschlossen unter \perp (oder abgeschlossen in (A, \perp)), wenn gilt: $x \perp y \in M$ für alle $x, y \in M$. In diesem Fall heißt (M, \perp) auch Teilgebilde (manchmal auch: Untergebilde) von (A, \perp) .

■ Beispiele

Die Menge der geraden Zahlen ist abgeschlossen unter $+$, nicht jedoch die Menge der ungeraden Zahlen. Weitere Beispiele: \mathbb{Z} , \mathbb{Q} und \mathbb{R}^+ sind sämtlich in (\mathbb{R}, \cdot) abgeschlossen.

10.2. Kommutativität

Beim Rechnen mit gewöhnlichen Zahlen benutzt man stillschweigend, dass sich in einer Summe die Summanden und dass sich in einem Produkt die Faktoren vertauschen lassen; z.B.:

$$147 + 36 + 113 = 147 + 113 + 36 = 260 + 36 = 296$$

■ 10.2.1. Definition

Eine Verknüpfung \perp in einer nichtleeren Menge A heißt kommutativ, wenn für alle $x, y \in A$ gilt: $x \perp y = y \perp x$. In diesem Fall heißt auch das zugehörige Verknüpfungsgebilde (A, \perp) kommutativ.

■ Bemerkung

Die Addition $+$ und die Multiplikation \cdot (in \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R}) sind kommutativ, nicht hingegen Subtraktion und Division. Ferner gilt: Addition und Multiplikation von Restklassen sind kommutative Verknüpfungen (vgl. Proposition 7.3.3). Die Verkettung von Abbildungen ist nicht kommutativ.

10.3. Assoziativität

Das Rechenbeispiel aus 10.2 benutzt außer der Kommutativität von $+$ noch eine weitere Eigenschaft der Addition, die aus folgender Schreibweise ersichtlich wird:

$$147 + (36 + 113) = (147 + 36) + 113 = \dots$$

■ Bemerkung

Die Schreibweise mit Klammern ist die genauere, weil ja durch $+$ zwei (und nicht etwa drei oder mehr) Zahlen verknüpft werden. Im Beispiel bedeutet das praktisch, dass zuerst die Klammer $(36 + 113)$ ausgewertet und dann die Summe $147 + (\dots)$ gebildet wird.

Die Umformung macht Gebrauch von der Tatsache, dass "zuerst $113 + 36$ rechnen und das Ergebnis zu 147 addieren" dasselbe Ergebnis liefert wie "zuerst $147 + 113$ rechnen und zu dem Ergebnis 36 addieren". Das allgemeine Rechengesetz, das diese Umformung zum Ausdruck bringt, heißt Assoziativgesetz der Addition. Auch für die Multiplikation gilt diese Rechenregel (vgl. 1.2.1).

■ 10.3.1. Definition

Eine Verknüpfung \perp in einer nichtleeren Menge A heißt assoziativ, wenn für alle $x, y, z \in A$ gilt:
 $x \perp (y \perp z) = (x \perp y) \perp z$. In diesem Fall nennt man das Verknüpfungsgebilde (A, \perp) eine Halbgruppe.

Die Assoziativität ist eine *fundamentale* Eigenschaft. Praktisch alle wichtigen Verknüpfungen, die in der Algebra untersucht werden, sind assoziativ, und solche, die es nicht sind, sind nur in Ausnahmefällen interessant.

■ Beispiele

Die folgenden Verknüpfungsgebilde sind Halbgruppen:

$$(\mathbb{Q}, +), (\mathbb{R}, \cdot), (\mathcal{S}_n, \circ), (\mathcal{P}(M), +), (\mathbb{Z}_m, \oplus), (\mathbb{Z}_m, \odot)$$

■ Bemerkung

Ist Γ irgendeine Menge von Selbstabbildungen einer Menge A , die unter \circ abgeschlossen ist (d.h. mit $f, g \in \Gamma$ ist stets auch $f \circ g \in \Gamma$), dann ist (Γ, \circ) eine Halbgruppe. (Dazu ist lediglich zu beachten, dass die Verkettung \circ in der Gesamtheit aller Selbstabbildungen von A assoziativ ist und die Gleichheit $(f \circ g) \circ h = f \circ (g \circ h)$ wegen der Abgeschlossenheit schon in Γ besteht.)

10.4. Neutrales Element (Einselement)

Die Zahl 1 hat bei der Multiplikation natürlicher, ganzer, rationaler und reeller Zahlen die Eigenschaft, dass für jede Zahl x gilt:

$$1 \cdot x = x \cdot 1 = x$$

Wegen dieser Eigenschaft heißt 1 neutrales Element der Multiplikation. Auch die Addition besitzt (in der Zahl 0) ein solches neutrales Element:

$$0 + x = x + 0 = x$$

■ 10.4.1. Definition

Sei (A, \perp) ein Verknüpfungsgebilde. Ein Element $e \in A$ heißt neutrales Element (oder: Einselement) von (A, \perp) , wenn für alle $x \in A$ gilt: $e \perp x = x \perp e = x$.

■ Bemerkung

Bei einer kommutativen Verknüpfung \perp genügt es, $x \perp e = x$ (für alle $x \in A$) zu fordern.

Bekanntlich existiert außer der Zahl 1 kein weiteres neutrales Element der gewöhnlichen Multiplikation. In der Tat ist allgemein das neutrale Element eines Verknüpfungsgebildes eindeutig bestimmt.

■ 10.4.2. Proposition

In einem Verknüpfungsgebilde (A, \perp) gibt es höchstens ein neutrales Element.

■ Beweis

Seien e_1 und e_2 neutrale Elemente von (A, \perp) . Dann gelten die Gleichungen:

$$(1) \quad e_1 \perp x = x$$

$$(2) \quad x \perp e_2 = x$$

für beliebiges $x \in A$. Setzt man $x = e_2$ in (1) und $x = e_1$ in (2), so ergibt sich $e_1 \perp e_2 = e_2$ und $e_1 \perp e_2 = e_1$, mithin $e_1 = e_2$. ♦

■ Beispiele

<i>Verknüpfungsgebilde</i>	<i>neutrales Element (Einselement)</i>
(\mathbb{Z}_m, \oplus)	0 (als Restklasse)
(\mathbb{Z}_m, \odot)	1 (als Restklasse)
(S_n, \circ)	e (identische Permutation)
$(\mathcal{P}(M), +)$	\emptyset

Die entsprechenden Gleichungen sollten für jedes dieser Beispiele übungshalber nachvollzogen werden.

■ Bemerkung und Beispiel

Es gibt Verknüpfungsgebilde, die kein neutrales Element besitzen.

In \mathbb{R} werde \perp definiert durch $x \perp y := \text{Max}\{x, y\}$. Diese Verknüpfung hat kein Einselement, denn für ein solches e müsste gelten: $\text{Max}\{x, e\} = x \perp e = x$ für alle $x \in \mathbb{R}$. Für $x = e - 1$ führt dies zu einem Widerspruch!

10.5. Invertierbarkeit, Begriff der Gruppe

Hat eine Verknüpfung \perp in einer Menge A ein Einselement e , so ist die Frage sinnvoll, ob zu $a \in A$ ein Element $a' \in A$ existiert, sodass $a \perp a' = e$ und $a' \perp a = e$. Zum Beispiel gibt es zu jeder rationalen Zahl $r \neq 0$ ein $r' \in \mathbb{Q}$ mit der Eigenschaft: $r \cdot r' = r' \cdot r = 1$ (nämlich $r' = \frac{1}{r}$). Diesem Beispiel folgend spricht man von zueinander inversen Elementen bzw. von der Invertierbarkeit eines Elements.

■ 10.5.1. Definition

Sei (A, \perp) ein Verknüpfungsgebilde mit Einselement e . Ein Element $a \in A$ heißt invertierbar, wenn ein $a' \in A$ existiert mit $a \perp a' = a' \perp a = e$. In diesem Fall heißt a' invers zu a (oder inverses Element von a).

■ Bemerkung

Ist a' invers zu a , dann ist auch a invers zu a' (unmittelbar aus der definierenden Gleichung ersichtlich). Das neutrale Element e ist stets invertierbar, denn es gilt: $e \perp e = e$.

■ Beispiele

1. Alle Elemente von $\mathbb{Q} \setminus \{0\}$ besitzen ein multiplikatives Inverses, d.h. sind invertierbar bzgl. der gewöhnlichen Multiplikation rationaler Zahlen. Das Inverse ist jeweils eindeutig bestimmt.
2. Alle ganzen Zahlen sind invertierbar in $(\mathbb{Z}, +)$; das Inverse zu $a \in \mathbb{Z}$ ist eindeutig bestimmt (nämlich als $-a$).
3. Alle Permutationen in \mathcal{S}_n sind invertierbar (bzgl. der Verkettung \circ), denn zu $p \in \mathcal{S}_n$ gilt: $p \circ p^{-1} = p^{-1} \circ p = e$. Das Inverse p^{-1} ist die Umkehrabbildung von p (und nach dem Satz von der Umkehrabbildung, Prop. 8.4.1, eindeutig bestimmt).
4. Alle Teilmengen X von M sind in $(\mathcal{P}(M), +)$ zu sich selbst invers, denn es gilt: $X + X = \emptyset$.

In den genannten Beispielen sind jeweils die Inversen eindeutig bestimmt. Das ist aber nicht notwendig immer so; z.B. hat das durch $x \perp y := x + y - 2x^2y^2$ (für reelle x, y) definierte Verknüpfungsgebilde (\mathbb{R}, \perp) ein neutrales Element (nämlich 0), es gibt aber nicht-invertierbare Elemente (etwa -1) und Elemente mit mehr als einem Inversen (etwa 2). Der Grund dafür liegt darin, dass die betreffende Verknüpfung *nicht assoziativ* ist. Für assoziative Verknüpfungen lässt sich hingegen zeigen, dass die Inversenbildung eindeutig ist (sofern sie möglich ist).

■ 10.5.2. Proposition

Sei (A, \perp) ein Halbgruppe mit Einselement. Dann besitzt ein Element von A höchstens ein Inverses.

■ Beweis

Sei e das (eindeutig bestimmte) Einselement und a irgendein invertierbares Element von A mit Inversen a' und a'' . Es ist zu zeigen: $a' = a''$. Nach Definition gilt: $a \perp a' = e$ und $a'' \perp a = e$. Daraus folgt mit dem Assoziativgesetz:

$$a' = e \perp a' = (a'' \perp a) \perp a' = a'' \perp (a \perp a') = a'' \perp e = a''$$

◆

■ Bezeichnungen

1. Das zu einem invertierbaren Element a aus A eindeutig bestimmte Inverse wird mit a^{-1} bezeichnet.
2. Die Menge der in (A, \perp) invertierbaren Elemente werde mit $\text{Inv}(A, \perp)$ bezeichnet.

Man mache sich damit die folgenden Sachverhalte klar:

$$\begin{array}{lll} \text{Inv}(\mathbb{Z}, +) = \mathbb{Z} & \text{Inv}(\mathbb{Q}, \cdot) = \mathbb{Q} \setminus \{0\} & \text{Inv}(\mathcal{S}_n, \circ) = \mathcal{S}_n \\ \text{Inv}(\mathbb{Z}_m, \oplus) = \mathbb{Z}_m & \text{Inv}(\mathbb{Z}_4, \odot) = \{1, 3\} & \text{Inv}(\mathbb{N}_0, +) = \{0\} \end{array}$$

■ 10.5.3. Bemerkung zu Restklassen, Definition

Nach Prop. 7.3.5 sind die in (\mathbb{Z}_m, \odot) , $m \geq 2$, invertierbaren Restklassen genau die zu m teilerfremden (positiven) $a \in \mathbb{Z}_m$. Ihre Anzahl wird üblicherweise mit $\phi(m)$ bezeichnet (sog. Eulersche ϕ -Funktion). Da somit z.B. in \mathbb{Z}_{10} genau die Restklassen 1, 3, 7, 9 multiplikativ invertierbar sind, gilt $\phi(10) = 4$.

Für Primzahlen p gilt allgemein: $\phi(p) = |\text{Inv}(\mathbb{Z}_p, \odot)| = |\mathbb{Z}_p \setminus \{0\}| = p - 1$. Von 0 verschiedene Restklassen nach einem Primzahlmodul besitzen stets ein Inverses; es lässt sich mit dem Euklidischen Algorithmus berechnen.

■ 10.5.4. Proposition

Sei (A, \perp) eine Halbgruppe mit neutralem Element e . Dann gilt:

- (1) $e \in \text{Inv}(A, \perp)$
- (2) $\text{Inv}(A, \perp)$ ist abgeschlossen unter \perp .
- (3) $(x \perp y)^{-1} = y^{-1} \perp x^{-1}$ für alle $x, y \in \text{Inv}(A, \perp)$.

■ Beweis

Zu (1): Ergibt sich unmittelbar aus $e \perp e = e$.

Zu (2) und (3): Es genügt zu zeigen, dass $y^{-1} \perp x^{-1}$ zu $x \perp y$ invers ist. Nach dem Assoziativgesetz gilt:

$$(y^{-1} \perp x^{-1}) \perp (x \perp y) = (y^{-1} \perp (x^{-1} \perp x)) \perp y = (y^{-1} \perp e) \perp y = y^{-1} \perp y = e$$

und entsprechend ergibt sich $(x \perp y) \perp (y^{-1} \perp x^{-1}) = e$. ♦

Bemerkungen

1. Unter der Voraussetzung von Prop. 10.5.4 (Halbgruppe mit neutralem Element e) ist $\text{Inv}(A, \perp)$ jedenfalls nicht leer (e ist stets invertierbar).
2. Aussage (2) besagt, dass das Verknüpfungsergebnis invertierbarer Elemente wieder invertierbar ist.
3. Aussage (3) liefert die Regel, nach der sich das Inverse eines "Produkts" berechnen lässt. Es handelt sich offenbar um eine direkte Verallgemeinerung der "Umkehrregel" für die Abbildungsverkettung (vgl. Prop. 8.4.2).
4. Ist \perp kommutativ, so gilt auch $(x \perp y)^{-1} = x^{-1} \perp y^{-1}$. Im Allgemeinen, d.h. für nicht-kommutative Verknüpfungen, gilt diese Gleichung jedoch *nicht*.

Eine spezielle Sorte invertierbarer Elemente sind diejenigen, die zu sich selbst invers sind. Zum Beispiel gilt für $p = (1\ 2)(3\ 4) \in \mathcal{S}_4$ die Gleichung $p^{-1} = p$, was sich auch $p^2 = e$ schreiben lässt. Das neutrale Element eines Verknüpfungsgebildes (A, \perp) ist stets zu sich invers ($e^2 = e$). Allgemein heißt $a \in A$ involutorisch, wenn $a^2 = e$. So sind etwa in (\mathbb{Z}_4, \oplus) die Restklassen 0 und 2 involutorisch ($0 \oplus 0 = 0$ bzw. $2 \oplus 2 = 0$). Spiegelungen sind involutorische Kongruenzabbildungen der Ebene. Das Verknüpfungsgebilde $(\mathcal{P}(M), +)$ besteht sogar aus lauter involutorischen Elementen, denn es gilt $A + A = \emptyset$ für alle $A \in \mathcal{P}(M)$.

■ Zum Begriff der Gruppe

Unter einer *Gruppe* versteht man eine Halbgruppe mit Einselement, in der sämtliche Elemente invertierbar sind (siehe die Def. 10.5.5, welche diesen Begriff durch drei Axiome beschreibt). Der Begriff wurde im 19. Jahrhundert zunächst im Zusammenhang mit der Auflösung algebraischer Gleichungen entwickelt. Bald erkannte man auch seine große Bedeutung für die Geometrie, was dann zu einem systematischen Ausbau einer eigenen Gruppentheorie führte. Ein wesentlicher Antrieb für diese Entwicklungen war die *Idee der Symmetrie*. Die Symmetrie einer Figur lässt sich durch die Gesamtheit G aller Transformationen (Abbildungen) ausdrücken, bei denen bestimmte Eigenschaften der Figur erhalten bleiben (vgl. Abschnitt 10.8). Dann bildet G eine Halbgruppe aus lauter invertierbaren Elementen (also genau das, was man unter einer Gruppe versteht). Im Gruppenbegriff lassen sich geometrische und algebraische Betrachtungsweisen verbinden, was zu einem großen Teil seinen Reiz und seine Bedeutung ausmacht.

■ 10.5.5. Definition

Ein Verknüpfungsgebilde (G, \perp) heißt Gruppe, wenn folgende Eigenschaften erfüllt sind:

- (G1) \perp ist assoziativ.
- (G2) Es gibt ein $e \in G$, sodass $e \perp a = a \perp e = a$ für alle $a \in G$.
- (G3) Jedes $a \in G$ besitzt ein Inverses in (G, \perp) .

Bei der allgemeinen Notation von Gruppen (und Halbgruppen) wird häufig (und auch im Folgenden) die zugrunde liegende Verknüpfung *analog zur Multiplikation* aufgefasst und dementsprechend nicht eigens bezeichnet bzw. geschrieben. Die Gleichung aus (G2) lautet damit kürzer $e a = a e = a$; das neutrale Element e heißt daher in diesem Zusammenhang passender *Einselement* oder kurz: *Eins*.

Ist die in der Gruppe G gegebene Verknüpfung kommutativ, so heißt auch G selbst kommutativ (manchmal auch abelsch, zu Ehren des norwegischen Mathematikers N. H. Abel, 1802–1829).

Viele der bisher bekannten Verknüpfungsgebilde sind Gruppen in dem gerade definierten Sinn. Ebenso gelten eine Reihe von früher bewiesenen Aussagen erst recht für Gruppen. Das alles soll jetzt hier noch einmal kurz zusammengestellt werden:

■ Beispiele

1. Die Zahlenmengen \mathbb{Z} , \mathbb{Q} und \mathbb{R} bilden jeweils zusammen mit der gewöhnlichen Addition eine kommutative Gruppe.
2. Die Mengen $\mathbb{Q} \setminus \{0\}$ und $\mathbb{R} \setminus \{0\}$ bilden jeweils zusammen mit der gewöhnlichen Multiplikation eine kommutative Gruppe.
3. Die Menge \mathcal{S}_n aller Permutationen n -ten Grades bildet zusammen mit der Verkettung \circ eine nicht-kommutative Gruppe (die sog. symmetrische Gruppe oder Permutationsgruppe).
4. \mathbb{Z}_m ($m \geq 2$ ganz) bildet zusammen mit der Restklassenaddition \oplus eine kommutative Gruppe.
5. $\mathbb{Z}_m^* := \text{Inv}(\mathbb{Z}_m, \odot)$ ist eine kommutative Gruppe (bezeichnet als prime Restklassengruppe modulo m). Für primes p gilt $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, d.h. die Gruppe \mathbb{Z}_p^* besteht aus genau den $p - 1$ Restklassen $1, \dots, p - 1$.

Die folgende Proposition fasst eine Reihe bisher abgeleiteter Aussagen, soweit sie auf Gruppen anwendbar sind, zusammen:

■ 10.5.6. Proposition

Sei G eine Gruppe. Dann ist das Einselement in G eindeutig bestimmt. Ferner besitzt jedes Element a von G genau ein Inverses a^{-1} in G . Das Inverse eines Produkts ab ($a, b \in G$) ist gleich dem Produkt aus dem Inversen von b und dem Inversen von a : $(ab)^{-1} = b^{-1}a^{-1}$.

10.6. Ringe und Körper

Häufig betrachtet man in einer Menge zwei Verknüpfungen, z.B. die Addition und die Multiplikation in \mathbb{Z} . Beide Verknüpfungen sind durch eine Rechenregel verbunden, die Verteilungs- oder *Distributivgesetz* genannt wird:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

■ 10.6.1. Definition

Seien \perp und τ zwei Verknüpfungen in A . Dann heißt \perp distributiv bzgl. τ , wenn für alle $x, y, z \in A$:

$$(1) \quad x \perp (y \tau z) = (x \perp y) \tau (x \perp z)$$

$$(2) \quad (x \tau y) \perp z = (x \perp z) \tau (y \perp z)$$

Für ganze, rationale und reelle Zahlen ist die Multiplikation distributiv bezüglich der Addition, jedoch ist die Addition nicht distributiv bezüglich der Multiplikation. Dasselbe gilt auch für die entsprechenden Verknüpfungen in \mathbb{Z}_m . Für Mengen ist sowohl \cap distributiv bezüglich \cup als auch umgekehrt \cup distributiv bezüglich \cap .

■ Bemerkung zu Schreibweisen

Das Setzen von Klammern auf den rechten Seiten der Gleichungen (1) und (2) in der Definition ist erforderlich, um festzulegen, welche der beteiligten Operationen zuerst durchzuführen ist. Man kann Klammern durch eine Konvention vermeiden. Es ist dann zu vereinbaren, welche der beiden Operationen \perp und τ den Vorrang erhält. Eine solche Konvention existiert beispielsweise für die Multiplikation und Addition von Zahlen: *Punktrechnung geht vor Strichrechnung*. Wenn man einmal der Multiplikation den Vorrang gegeben hat, so sind Ausdrücke wie $x \cdot z + y \cdot z$ eindeutig auswertbar.

Häufig ist es zweckmäßig, für die Verknüpfungen in einer Menge die vertrauten Symbole '+' oder '·' zu verwenden. Wird nur *eine* Verknüpfung betrachtet, so schreibt man sie gerne als Multiplikation (also \cdot anstelle von \perp), oder man lässt das Operationssymbol überhaupt ganz weg. Bei der gewöhnlichen Multiplikation von Zahlen ist letzteres gang und gäbe, man schreibt also etwa: $xz + yz$ usw.

■ Ringe

Die grundlegenden Rechengesetze, die in den Zahlbereichen \mathbb{Z} , \mathbb{Q} , \mathbb{R} und \mathbb{C} gelten (vgl. 1.2.1), zeigen (wenn A irgendeine dieser Mengen bedeutet): $(A, +)$ ist eine kommutative Gruppe und (A, \cdot) ist eine Halbgruppe, und es gilt das Distributivgesetz $x(y + z) = x \cdot y + x \cdot z$. Auf Grund dieser Eigenschaften nennt man $(A, +, \cdot)$ einen Ring:

■ 10.6.2. Definition

Ein Verknüpfungsgebilde $(A, +, \cdot)$ mit 2-stelligen Verknüpfungen $+$ und \cdot in A heißt Ring, wenn gilt:

- (R1) $(A, +)$ ist eine kommutative Gruppe
- (R2) (A, \cdot) ist eine Halbgruppe
- (R3) \cdot ist distributiv bzgl. $+$

Die oben genannten Ringe weisen aber noch speziellere Eigenschaften auf: Ihre multiplikative Halbgruppe (A, \cdot) besitzt ein Einselement und ist kommutativ. Entsprechend handelt es sich um kommutative Ringe mit Eins. Die Eins eines Rings wird gewöhnlich mit 1 bezeichnet.

Das neutrale Element der additiven Gruppe $(A, +)$ eines Rings nennt man seine Null (bezeichnet mit 0).

■ Beispiele

1. Ein Ring kann *endlich* sein, wie das Beispiel von $(\mathbb{Z}_m, \oplus, \odot)$ zeigt, eines kommutativen Rings mit Einselement.
2. $(m\mathbb{Z}, +, \cdot)$ ist ein (unendlicher) Ring (*Unterring* des Rings der ganzen Zahlen). Die ganze Zahl 0 ist seine Null. Eine Eins besitzt dieser Ring genau dann, wenn $|m| = 1$ ist; in diesem Fall handelt es sich um die ganze Zahl 1. (Begründung!)
3. Sei $(G, +)$ eine (additiv geschriebene) abelsche Gruppe. Es bezeichne E die Menge aller Selbstabbildungen f von G mit der Eigenschaft: $f(x + y) = f(x) + f(y)$ für alle $x, y \in G$. Für zwei Abbildungen $f, g \in E$ sei ihre Summe definiert durch: $(f + g)(x) := f(x) + g(x)$ ($x \in G$). Dann ist $(E, +, \circ)$ ein Ring mit id_E als Eins. (Beweis als Übung!).
4. Ein triviales Beispiel ist der sog. Nullring $A = \{e\}$, der aus nur einem Element besteht, für das $e + e = e$ sowie $e \cdot e = e$ gilt. Man überzeuge sich davon, dass tatsächlich ein Ring vorliegt (dessen Null und Eins dasselbe Element sind).

■ 10.6.3. Proposition

In einem Ring $(A, +, \cdot)$ gelten die "Vorzeichenregeln":

- (1) $a \cdot 0 = 0 \cdot a = 0$
- (2) $a(-b) = (-a)b = -ab$
- (3) $(-a)(-b) = ab$

■ Beweis

Als Übung! ♦

■ Bemerkung

In diesem Einführungskurs ist kein Raum, Ringe eingehender zu behandeln. Es soll aber wegen seiner fachlichen Bedeutung für den Unterricht zumindest das Thema "Division" kurz erörtert werden.

Die oft zu hörende Regel "Durch Null darf nicht dividiert werden!" klingt etwas merkwürdig und beinahe wie ein moralisches Verbot, weshalb es manchmal auch heißt, dass die Division durch Null nicht definiert sei. In der Sprache der Algebra lässt sich diesen reichlich vagen Formulierungen nun aber ein klarer Sinn unterlegen. Wir denken uns einen Ring $(A, +, \cdot)$ mit Eins gegeben. Der "Division durch Null" entspricht hier die Invertierung der Null in der multiplikativen Gruppe des Rings, d.h. der Auflösung der Gleichung $0 \cdot x = 1$. Da in jedem Ring $0 \cdot x = 0$ ist (vgl. Prop. 10.6.3,(1)), müsste somit gelten: $0 = 1$. Die Null (des Rings) hat also nur dann ein Inverses, wenn sie mit der Eins übereinstimmt. Dass dies in der Tat möglich ist, zeigt das oben angeführte Beispiel des Nullrings. Aber auch *nur im Nullring* kann durch Null dividiert werden, denn aus $0 = 1$ folgt sofort: $0 = 0 \cdot x = 1 \cdot x = x$, was heißt: alle Elemente $x \in A$ stimmen mit der Null überein (und das heißt ja gerade, dass A der Nullring ist).

Fazit: Genau in den vom Nullring verschiedenen Ringen besitzt die Null kein multiplikatives Inverses (d.h. "kann nicht durch 0 dividiert werden").

Es liegt nahe zu fragen, welche von 0 verschiedenen Elemente eines Rings ein multiplikatives Inverses besitzen.

■ Beispiel

$(\mathbb{Z}_4, \oplus, \odot)$ ist ein kommutativer Ring mit Eins. Nach Prop. 7.3.5 ist außer 1 nur 3 multiplikativ invertierbar. Es gilt: $3 \odot 3 = 1$. Der Rest 2 ist nicht invertierbar; es gilt sogar: $2 \odot 2 = 0$. Auf ähnliche Verhältnisse trifft man z.B. bei \mathbb{Z}_{12} , wo etwa gilt: $3 \odot 4 = 3 \odot 8 = 0$. – Das hier auftretende Phänomen von "Nullteilern" ist für Ringe auch allgemein von Bedeutung.

■ 10.6.4. Definition

Sei $(A, +, \cdot)$ ein kommutativer Ring (\neq Nullring). Ein Element $a \in A$ heißt Nullteiler, wenn $a \cdot b = 0$ für ein Ringelement $b \neq 0$. Enthält A keine von 0 verschiedenen Nullteiler, so heißt A nullteilerfrei (oder auch: Integritätsring).

Die Zahlbereiche \mathbb{Z} , \mathbb{Q} , \mathbb{R} und \mathbb{C} sind Integritätsringe.

Am Beispiel von \mathbb{Z} sieht man noch folgendes: Auch wenn ein Ring keine echten (d.h. von Null verschiedenen) Nullteiler besitzt, so bedeutet dies doch nicht, dass seine von Null verschiedenen Elemente multiplikativ invertierbar sind. Bei den Ringen \mathbb{Q} , \mathbb{R} und \mathbb{C} ist dies allerdings der Fall (ein Fall, der immerhin so wichtig ist, dass dafür ein neuer Begriff eingeführt wird):

■ 10.6.5. Definition

Ein kommutativer Ring $(A, +, \cdot)$ mit Eins heißt Körper, wenn $(A \setminus \{0\}, \cdot)$ eine Gruppe ist.

In einem Körper lässt sich so rechnen, wie wir es von den rationalen und reellen Zahlen her gewohnt sind. Diese Zahlbereiche sind denn auch die naheliegendsten Beispiele für Körper. Aus Beispiel Nr. 5 zu Def. 10.5.5 ist zu erkennen, dass auch die Reste modulo einer Primzahl p einen (endlichen!) Körper bilden: $(\mathbb{Z}_p, \oplus, \odot)$. Den kleinsten Körper, der nur die Elemente 0 und 1 enthält, gewinnt man hieraus für $p = 2$: $(\{0, 1\}, \oplus, \odot)$.

■ 10.6.6. Proposition

Ein Körper ist stets auch ein Integritätsring.

■ Beweis

Sei $(A, +, \cdot)$ ein Körper sowie $a \in A \setminus \{0\}$ und $ab = 0$. Durch Multiplikation mit dem Inversen von a ergibt sich:
 $0 = a^{-1} 0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$. ♦

Umgekehrt ist ein Integritätsring nicht auch schon ein Körper (wie das Gegenbeispiel \mathbb{Z} zeigt). Wohl gilt hingegen die folgende Aussage:

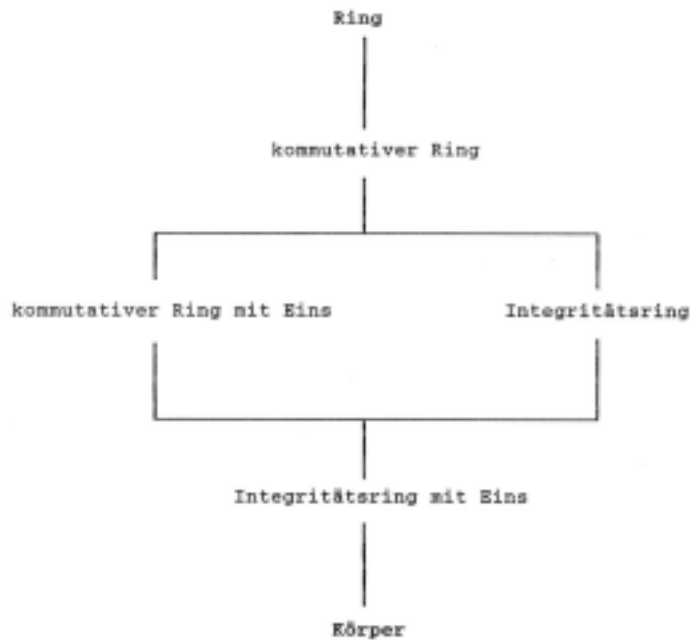
■ 10.6.7. Proposition

Ein endlicher Integritätsring ist ein Körper.

■ Beweis

Sei A ein endlicher Integritätsring. Es ist zu zeigen, dass $(A \setminus \{0\}, \cdot)$ eine Gruppe ist. Da A nullteilerfrei ist, gilt für $a, b \neq 0$ stets $ab \neq 0$, und damit ist die Multiplikation \cdot eine Verknüpfung in $A \setminus \{0\}$; sie ist assoziativ, da (A, \cdot) eine Halbgruppe ist. Sei nun $a \in A \setminus \{0\}$ vorgegeben. Wir definieren eine Abbildung $f : A \rightarrow A$ durch $f(x) := ax$. Dieses f ist injektiv, denn aus $f(x) = f(y)$ folgt $ax = ay$ und nach Prop. 10.6.3 und Distributivgesetz: $0 = ax - ay = a(x - y)$, sodass sich aufgrund der Nullteilerfreiheit $x = y$ ergibt. Als injektive Selbstabbildung einer endlichen Menge ist f sogar bijektiv (vgl. Prop. 8.5.5), es gibt also genau ein $x_0 \in A$ mit $f(x_0) = ax_0 = a$. Dieses (zu a) eindeutig bestimmte x_0 ist Einselement der Halbgruppe (A, \cdot) (und somit unabhängig von a). Begründung: Zu beliebig vorgegebenem $c \in A$ gibt es wegen der Bijektivität von f ein $x \in A$ mit $f(x) = c$, mithin $ax = c$, woraus resultiert:
 $c = ax = (ax_0)x = x_0(ax) = x_0c = cx_0$. Das (eindeutig bestimmte!) Einselement x_0 werde wie üblich 1 genannt. Die Gleichung $ax = 1$ besitzt (wegen der Bijektivität der zu a definierten Abbildung f) eine eindeutige Lösung x , und diese ist offensichtlich invers zu a . ♦

Die folgende Übersicht zeigt die in diesem Abschnitt behandelten Struktur Begriffe in ihrer logischen Abhängigkeit:



10.7. Untergruppen

Für das Studium einer Gruppe sind ihre Untergruppen von zentraler Bedeutung, da diese Aufschluss über ihren Aufbau vermitteln (was allerdings im Folgenden nicht vertieft werden wird).

■ 10.7.1. Definition

Eine (nichtleere) Teilmenge H einer Gruppe G heißt Untergruppe von G , wenn H bezüglich der Gruppenverknüpfung abgeschlossen und eine Gruppe ist.

In einer Gruppe G gibt es stets mindestens eine Untergruppe, nämlich die sog. triviale Untergruppe $\{e\}$, die aus dem Einselement von G besteht. Natürlich ist jede Gruppe Untergruppe von sich selbst.

■ Beispiele

1. \mathbb{Z} ist eine Untergruppe von $(\mathbb{Q}, +)$; \mathbb{Q} ist Untergruppe von $(\mathbb{R}, +)$.
2. Die Menge $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ der ganzzahligen Vielfachen von m (m ganz) ist eine Untergruppe von $(\mathbb{Z}, +)$.
3. Die Restemenge $\{0, 2, 4\}$ ist eine Untergruppe von (\mathbb{Z}_6, \oplus) .
4. Die Permutationenmenge $\{(1)(2)(3)(4), (1\ 3\ 4\ 2), (1\ 4)(2\ 3), (1\ 2\ 4\ 3)\}$ ist eine Untergruppe von (S_4, \circ) .

Die folgende Aussage enthält ein hinreichendes und notwendiges Kriterium dafür, dass eine Teilmenge einer Gruppe G eine Untergruppe von G ist:

■ 10.7.2. Proposition (Untergruppenkriterium)

Sei G eine Gruppe, H eine Teilmenge von G . Dann gilt: H ist Untergruppe von G genau dann, wenn $H \neq \emptyset$ und mit $a, b \in H$ stets auch $a b^{-1} \in H$ gilt.

■ Beweis

1. Eine Untergruppe H von G erfüllt offensichtlich die behauptete Eigenschaft (Begründung!).

2. Sei umgekehrt H eine nichtleere Teilmenge mit $a b^{-1} \in H$ für alle $a, b \in H$. Es ist zu zeigen, dass H eine Gruppe ist. Sei e das Einselement von G . Dann hat man jedenfalls $e = a a^{-1} \in H$. Jedes $a \in H$ ist ferner invertierbar wegen $e a^{-1} \in H$. Unter der Gruppenverknüpfung ist H abgeschlossen, denn zu $a, b \in H$ liegt das Inverse b^{-1} in H , und damit gilt $a b = a (b^{-1})^{-1} \in H$. Daher ist auch das Assoziativgesetz in H erfüllt, und H ist eine Gruppe. ♦

■ Potenzen und Ordnung

Im Folgenden werden für das Rechnen in Gruppen geeignete Begriffe und Regeln entwickelt. Da lediglich *eine* Verknüpfung vorliegt, beschränkt sich das Rechnen auf die wiederholte Anwendung dieser Verknüpfung, d.h. auf das Bilden von Potenzen. Die zugehörigen Begriffe spiegeln dies wider.

Sei G eine Gruppe und $a \in G$. Dann definiert man $a^0 = e$ (Einselement von G), $a^1 = a$, $a^2 = a a$, usw. Um dies allgemein und auch für ganzzahlige Exponenten zu erklären, benötigt man die folgende rekursive Definition:

■ 10.7.3. Definition

Für beliebige Elemente a einer Gruppe G mit dem Einselement e wird definiert:

$$\begin{aligned} a^0 &= e \\ a^{n+1} &= a^n a \quad (\text{für ganze Zahlen } n \geq 0) \end{aligned}$$

Zusätzlich wird für $n < 0$ festgelegt:

$$a^n := (a^{-1})^{-n}$$

■ Bemerkung

Die zuletzt getroffene Festsetzung hat einen Sinn, weil für negatives n die $(-n)$ -te Potenz des Inversen von a bereits definiert wurde. Insgesamt gibt die obige Definition die Gegebenheiten wieder, die vom Rechnen mit rationalen (oder reellen) Zahlen her vertraut sind. Insbesondere gelten die üblichen Rechengesetze für Potenzen:

■ 10.7.4. Proposition

In einer Gruppe G gilt für alle $a \in G$ und für alle $m, n \in \mathbb{Z}$:

- (1) $a^m a^n = a^{m+n}$
- (2) $(a^m)^n = a^{mn}$

- (3) $(a^m)^{-1} = (a^{-1})^m$
- (4) $(a b)^n = a^n b^n$ für jedes $b \in G$ mit $a b = b a$.

■ **Beweis**

Hinweis: Zunächst $m, n \geq 0$ voraussetzen und Beweise durch Induktion führen, anschließend mit Hilfe von Def. 10.7.3 auch negative Exponenten einbeziehen. Die Durchführung der Einzelheiten verläuft dann routinemäßig und bleibt zur Übung. ♦

Es ist von besonderem Interesse, in einer Gruppe G alle Potenzen a^n eines Elements $a \in G$ zu betrachten.

■ **Beispiele**

1. In der additiven Gruppe \mathbb{Z} der ganzen Zahlen bedeutet a^n die ganze Zahl $n a$. Die Potenzen von a sind also gerade die Vielfachen von a und die Potenzen von 1 gerade die ganzen Zahlen.
2. In der additiven Restklassengruppe \mathbb{Z}_6 hat die Restklasse 2 die Potenzen 0, 2, 4. Tatsächlich ist 4 das letzte Element dieser Folge, denn es gilt $4 \oplus 2 = 0$.
3. In \mathcal{S}_4 hat $p = (1\ 3\ 4\ 2)$ die Potenzen $p^0 (= e)$, p , p^2 , p^3 . Es ist $p^4 = e$; daher werden durch höhere Exponenten keine neuen Permutationen erzeugt. Auch durch negative Exponenten entstehen keine neuen Elemente, denn es gilt $p^{-1} = p^3$.

Die Beispiele zeigen: Die Potenzen eines Gruppenelements bilden eine Untergruppe.

■ **10.7.5. Proposition**

Sei G eine beliebige Gruppe und $a \in G$. Die Menge der Potenzen a^n ($n \in \mathbb{Z}$) ist eine Untergruppe von G .

■ **Beweis**

Nach dem Untergruppenkriterium (Prop. 10.7.2) ist zu zeigen, dass zu Potenzen a^n und a^m das Produkt $a^n(a^m)^{-1}$ wieder eine Potenz von a ist. Das ist in der Tat der Fall, denn nach Prop. 10.7.4 gilt:

$$a^n(a^m)^{-1} = a^n(a^{-1})^m = a^n a^{-m} = a^{n-m} \quad \blacklozenge$$

■ **Bezeichnungen**

Die von den Potenzen von $a \in G$ gebildete Untergruppe von G heißt Erzeugnis von a in G , oder: von a erzeugte Gruppe (bzw. Untergruppe in G). Sie werde im Folgenden mit $\langle a \rangle$ bezeichnet. Es ist $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$.

An den zuletzt genannten Beispielen (Nr. 2 und Nr. 3) ist zu beobachten, dass eine Potenz mit einem Exponenten größer als 0 dennoch gleich dem Einselement sein kann.

Bildet man die Potenzen innerhalb einer *endlichen* Gruppe, so ist dies notwendigerweise so. Denn es gibt dann zunächst einmal zwei übereinstimmende Potenzen, etwa $a^r = a^s$, wobei ohne Beschränkung der Allgemeinheit $r < s$ angenommen werden kann. Hieraus folgt sofort: $e = a^{-r} a^s = a^{s-r}$ mit $s - r > 0$.

Ist die Gruppe G unendlich, so lässt sich der eben durchgeführte Schluss nicht aufrechterhalten. Zum Beispiel sind in \mathbb{Z} alle (additiven) Potenzen eines Elementes $a \neq 0$ verschieden!

Die vorangegangenen Betrachtungen führen zu einer Definition, welche die Definition der Ordnung einer Permutation verallgemeinert.

■ 10.7.6. Definition

Sei G eine Gruppe und e das Einselement von G . Gibt es für ein $a \in G$ eine ganze Zahl $n > 0$ mit $a^n = e$, so heißt die kleinste dieser Zahlen Ordnung von a (in G); sie werde mit $\text{ord}(a)$ bezeichnet; andernfalls setzt man $\text{ord}(a) = \infty$ (Ordnung von a in G ist unendlich).

■ Beispiele

1. Die Ordnung der Elemente (ganzen Zahlen) in der additiven Gruppe $(\mathbb{Z}, +)$ ist unendlich.
2. In (\mathbb{Z}_6, \oplus) gilt: $\text{ord}(2) = 3$.
3. Für $p = (1\ 4)(2\ 5\ 3) \in \mathcal{S}_5$ ist $\text{ord}(p) = 6$.

■ Bezeichnung

Die Anzahl der Elemente einer Gruppe G wird als Ordnung von G bezeichnet (symbolisch: $\text{ord}(G)$ oder $|G|$); enthält G unendlich viele Elemente, so schreibt man: $|G| = \infty$.

■ Bemerkung

Trotz der gleichlautenden Bezeichnungen hat die Ordnung eines Elements von der Definition her zunächst mit der Ordnung der Gruppe nichts zu tun. Es stellt sich aber bald heraus, dass doch eine enge sachliche Beziehung zwischen beiden besteht (und dies ist natürlich auch der entstehungsgeschichtliche Grund für die gemeinsame Benennung). Man erkennt diesen Zusammenhang bereits daran, dass in einer Gruppe G für beliebiges $a \in G$ gilt: $\text{ord}(a) = |\langle a \rangle|$, d.h. die Ordnung von a stimmt überein mit der Ordnung der von a in G erzeugten Untergruppe.

Die Gruppe \mathbb{Z} ist von unendlicher Ordnung, und ihre Elemente (außer 0) besitzen ebenfalls unendliche Ordnung. Für die von $a \in \mathbb{Z}$ erzeugte Untergruppe gilt: $\langle a \rangle = a\mathbb{Z}$ (Menge der ganzzahligen Vielfachen von a). Man kann zeigen, dass es außer diesen Vielfachenmengen keine anderen Untergruppen von \mathbb{Z} gibt.

■ 10.7.7. Proposition

$$H \text{ ist Untergruppe von } (\mathbb{Z}, +) \iff H = a\mathbb{Z} \text{ für ein ganzes } a \geq 0$$

■ Beweis

1. " \Leftarrow ": $a\mathbb{Z}$ ist (als Erzeugnis von a) eine Untergruppe von \mathbb{Z} .

2. " \implies ": Es ist umgekehrt zu zeigen, dass eine Untergruppe H von \mathbb{Z} eine Vielfachenmenge ist. Im Fall $H = \{0\} = 0\mathbb{Z}$ ist dies natürlich der Fall. Sei daher H eine nichttriviale Untergruppe und $x \in H$ ein von 0 verschiedenes Element. Da H eine Gruppe ist, gilt auch $-x \in H$; folglich gibt es in H positive Zahlen. Die kleinste von ihnen sei a . Sei nun $h \in H$ beliebig vorgegeben; Division von h durch a mit Rest ergibt dann eine Darstellung $h = aq + r$, wobei $0 \leq r < a$. Nach dem Untergruppenkriterium ist $r = h - qa \in H$. Wegen $r \geq 0$ und der Minimalität von a muss $r = 0$ sein. Somit ist $h = qa$ und $H \subseteq a\mathbb{Z}$ gezeigt. Ist $x \in a\mathbb{Z}$, d.h. $x = na$ für ein ganzes n , so ist auch $x \in H$, weil $a \in H$ und H (als Gruppe) alle 'Potenzen' (d.h. hier: Vielfachen) von a enthält. Mithin ist auch $a\mathbb{Z} \subseteq H$ und insgesamt $a\mathbb{Z} = H$ gezeigt. \blacklozenge

Es liegt nun nahe, auch nach den Untergruppen H von (\mathbb{Z}_m, \oplus) zu fragen.

■ 10.7.8. Proposition

H ist Untergruppe von (\mathbb{Z}_m, \oplus) genau dann, wenn $H = \langle a \rangle$ für einen Rest $a \pmod m$. Dabei ist $\text{ord}(H)$ Teiler der Gruppenordnung m .

■ Beweis

Ist H die triviale Untergruppe, so gilt $H = \{0\} = \langle 0 \rangle$. Sei nun $H \neq \{0\}$ und a kleinster positiver Rest mod m in H . Wie im Beweis zu 10.7.7 zeigt man (bei wörtlicher Wiederholung der Argumente): $\langle a \rangle = H$. Da H endlich ist, ergibt sich: $H = \{0, a, 2a, \dots, (s-1)a\}$; dabei ist s die eindeutig bestimmte ganze Zahl mit $0 \leq (s-1)a < m \leq sa$. Wir zeigen: $m = sa$. – Division von m durch a mit Rest liefert eine Darstellung $m = ka + r$ mit $0 \leq r < a$. Für den Rest gilt: $r = m - ka \equiv ka \pmod m \in H$ und, da a minimal ist, $r = 0$. Daher hat man $m = ka$. Setzt man dies in die Ungleichung für s ein und kürzt anschließend a heraus, so ergibt sich: $s-1 < k \leq s$. Es ist also $k = s$. Insgesamt ist damit gezeigt, dass sowohl a (das erzeugende Element) als auch s (die Untergruppenordnung $\text{ord}(H)$) Teiler der Gruppenordnung m sind. \blacklozenge

■ Beispiel

Für $m = 12$ ergeben sich die folgenden (echten nichttrivialen) Untergruppen von \mathbb{Z}_{12} samt erzeugenden Elemente:

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$	Ordnung: 6
$\langle 3 \rangle = \{0, 3, 6, 9\}$	Ordnung: 4
$\langle 4 \rangle = \{0, 4, 8\}$	Ordnung: 3
$\langle 6 \rangle = \{0, 6\}$	Ordnung: 2

Die Teilerbeziehung zwischen den Ordnungen von Untergruppe und Gruppe gilt nicht nur für die \mathbb{Z}_m , sondern ganz allgemein für alle endlichen Gruppen.

■ 10.7.9. Definition

Eine Gruppe G heißt zyklisch, wenn sie von einem ihrer Elemente erzeugt wird, d.h. wenn ein $a \in G$ existiert mit $G = \langle a \rangle$. Das Element a heißt dann erzeugendes Element von G .

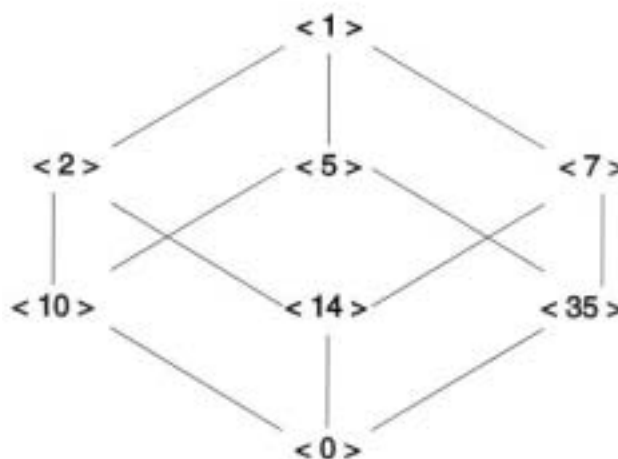
■ Beispiele

Die additiven Gruppen \mathbb{Z} und \mathbb{Z}_m (mit 1 als erzeugendem Element); ferner die Drehungsgruppen, die in Abschnitt 10.8 behandelt werden.

Die Untergruppen der zyklischen Gruppe $G = \mathbb{Z}_{70}$ sind sämtlich Erzeugnisse $\langle q \rangle$ eines Teilers q der Gruppenordnung. Hier eine Übersicht:

m	q	$\langle q \rangle$
1	70	{0}
2	35	{0, 35}
5	14	{0, 14, ..., 56}
7	10	{0, 10, ..., 60}
10	7	{0, 7, ..., 63}
14	5	{0, 5, ..., 65}
35	2	{0, 2, ..., 68}
70	1	{0, 1, ..., 69}

Für eine zyklische Gruppe ist der sog. Gruppengraph (Ordnungsdiagramm der Untergruppen) identisch mit dem Teilerdiagramm für die Gruppenordnung:



■ 10.7.10. Proposition (Satz von Lagrange)

Sei G eine endliche Gruppe, H eine Untergruppe von G . Dann ist $\text{ord}(H)$ ein Teiler von $\text{ord}(G)$.

■ Beweis

Der Beweis folgt einem einfachen Grundgedanken. Man zerlegt die Menge G in gleichgroße Teile, von denen jeder so groß ist wie H . Die fraglichen "Teile" sind sämtlich Mengen der Form $xH := \{xa \mid a \in H\}$, die sog. Linksnebenklassen von H .

(1) Jedes $x \in G$ liegt wegen $x = xe$ ($e = \text{Einselement von } G, e \in H$) in einer Nebenklasse, nämlich $x \in xH$. Da umgekehrt jede Nebenklasse eine Teilmenge von G ist, ist G die Vereinigung sämtlicher Nebenklassen xH , $x \in G$.

(2) Die Mengen H und xH haben (für beliebiges $x \in G$) dieselbe Anzahl von Elementen, denn die Linksmultiplikation, die jedem $a \in H$ das Element xa zuordnet, ist eine bijektive Abbildung von H auf xH . Natürlich haben infolgedessen auch alle Nebenklassen von H dieselbe Elementanzahl.

(3) Schließlich ist noch zu überlegen, dass zwei verschiedene Nebenklassen stets disjunkt sind. Sei dazu a als gemeinsames Element von xH und yH angenommen: $a \in xH \cap yH$. Dann gibt es $u, v \in H$ derart, dass $a = xu$ und $a = yv$. Hieraus folgt $xu = yv$ und damit auch $y^{-1}x = vu^{-1} \in H$ (nach dem Untergruppenkriterium). Ein Element der Nebenklasse xH hat die Form xc , wobei $c \in H$, was sich nun auch schreiben lässt als: $xc = y(y^{-1}x)c = yd$ mit $d := y^{-1}xc \in H$. Es gilt somit $xc \in yH$. Ebenso zeigt man umgekehrt, dass jedes Element der Nebenklasse yH auch zu xH gehört. Insgesamt hat man also $xH = yH$.

Zusammen ergeben die Teile (1), (2) und (3) die Aussage: G ist disjunkte Vereinigung von Mengen, welche dieselbe Anzahl von Elementen haben wie H . ♦

■ 10.7.11. Proposition

Sei G eine endliche Gruppe, e ihr Einselement. Dann gilt für alle $a \in G$:

- (1) $\text{ord}(a)$ ist Teiler von $\text{ord}(G)$
- (2) $a^{\text{ord}(G)} = e$

■ Beweis

Zu (1): Man betrachte die von a erzeugte Untergruppe $H = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$. Für deren Ordnung n gilt $n = \text{ord}(H) = \text{ord}(a)$. Prop. 10.7.10 liefert $\text{ord}(H) \mid \text{ord}(G)$ und damit die Behauptung (1).

Zu (2): Nach (1) haben wir $\text{ord}(G) = k \cdot \text{ord}(a)$ für eine geeignete natürlich Zahl k . Damit ergibt sich unter Beachtung der Potenzrechenregel 10.7.4,(2): $a^{\text{ord}(G)} = a^{k \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^k = e^k = e$. ♦

■ 10.7.12. Korollar (Satz von Euler-Fermat)

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

■ Beweis

Wähle für G die prime Restklassengruppe modulo m : $G = \mathbb{Z}_m^*$. Dann gilt $\text{ord}(G) = \phi(m)$. Einselement von G ist 1 (als Restklasse mod m). Schreibt man damit die Gleichung 10.7.11,(2) als Kongruenz, so steht die Behauptung direkt da. ♦

■ Bemerkung

Die Spezialisierung $m = p$ (Primzahl) liefert unter Beachtung von $\phi(p) = p - 1$ sofort den Lehrsatz ("Kleiner Fermat", vgl. Prop. 7.3.6.): $a^{p-1} \equiv 1 \pmod{p}$ (für teilerfremde a, p).

10.8. Symmetrie(gruppen)

Ein wichtiges Anwendungsgebiet des Gruppenbegriffs ist die Geometrie. Hier beschäftigt man sich mit Symmetriegruppen ebener oder räumlicher Figuren. Eine Symmetriegruppe besteht aus Selbstabbildungen der (euklidischen) Ebene E (oder – im weiteren außer Betracht – des Raums). Dabei werden nicht beliebige Abbildungen, sondern nur *abstandstreue Transformationen*, d.h. Kongruenzabbildungen zugelassen (vgl. die entsprechenden Beispiele aus Kapitel 8 und die Übungen dazu).

■ 10.8.1. Definition

1. Eine Abbildung $f : E \rightarrow E$ heißt abstandstreu, wenn für irgend zwei Punkte P, Q der (euklidischen) Ebene E gilt:
 $|f(P), f(Q)| = |P, Q|$.

(Der Abstand zwischen zwei Punkten X, Y von E ist hier mit $|X, Y|$ bezeichnet.)

2. Eine abstandstreu Surjektion $E \rightarrow E$ heißt Kongruenzabbildung von E . Es bezeichne \mathcal{K}_E die Menge der Kongruenzabbildungen von E . (Die ebenfalls gebräuchliche Bezeichnung Isometrie bringt die Abstandstreue namentlich zum Ausdruck.)

■ Beispiele

Grundtypen von Kongruenzabbildungen (bzw. Isometrien) sind: Verschiebungen (Translationen), Drehungen (Rotationen) und Geradenspiegelungen von E .

■ 10.8.2. Proposition

- (1) $f \in \mathcal{K}_E \implies f$ ist bijektiv
- (2) $f, g \in \mathcal{K}_E \implies f \circ g \in \mathcal{K}_E$
- (3) $f \in \mathcal{K}_E \implies f^{-1} \in \mathcal{K}_E$

■ Beweis

Zum Beweis ist hier zu zeigen: (1) dass eine abstandstreu Abbildung injektiv ist, (2) die Verkettung zweier Kongruenzabbildungen wieder eine Kongruenzabbildung ist, (3) die Umkehrabbildung einer Kongruenzabbildung abstandstreu ist. Beispielsweise sieht man (1) wie folgt ein: Aus $f(P) = f(Q)$ folgt $0 = |f(P), f(Q)| = |P, Q|$, also auch $P = Q$. – (2) und (3) sind ebenso einfach zu verifizieren. ♦

■ 10.8.3. Korollar (und Bezeichnung)

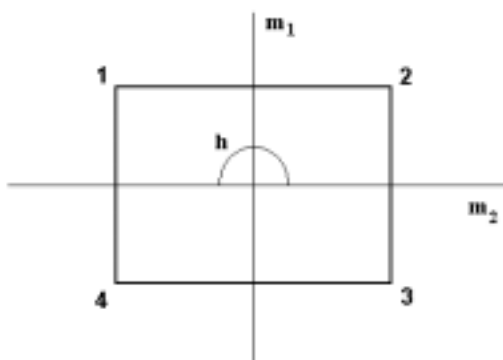
(\mathcal{K}_E, \circ) ist eine (nicht-kommutative) Gruppe, die sog. Kongruenzgruppe (auch: Isometriegruppe oder Bewegungsgruppe) von E .

■ **Beweis**

Für \mathcal{K}_E sind die drei Gruppenaxiome erfüllt: (G1, Assoziativität von \circ) folgt aus 10.8.2,(2) zusammen mit 8.3.4 (vgl. auch die Bemerkung 2 am Ende von Abschnitt 10.3). (G2) wird mit id_E Genüge getan. (G3) gilt aufgrund von 10.8.2,(3). ♦

■ **Symmetriegruppe einer Figur**

Hat man nun eine Figur vorliegen, etwa ein beliebiges Rechteck R (in E) mit den Ecken 1, 2, 3, 4, so stellt sich die Frage, welche Kongruenzabbildungen R fest lassen. Das heißt genauer: Für welche $f \in \mathcal{K}_E$ gilt $f[R] = R$? Eine Kongruenzabbildung f , die diese Forderung erfüllt, heißt Symmetrie oder Deckabbildung von R .



Eine Verschiebung kommt als Deckabbildung offensichtlich nicht in Frage, wohl aber z.B. eine Halbdrehung h der Ebene um den Mittelpunkt von R . Der Einfachheit halber wird sie (hier und allgemein bei Vielecken) *mit der durch sie bewirkten Permutation der Eckenmenge identifiziert*, also hier: $h = (1\ 3)(2\ 4)$ (obwohl keine Identität im strengen Sinne vorliegt!).

Natürlich gehört nicht zu jeder Permutation der Eckenmenge von R auch eine Symmetrie. Zum Beispiel gibt es keine zu $(1)(2\ 3)(4)$ gehörende Deckabbildung von R ; von den 24 möglichen Eckenpermutationen entsprechen sogar nur die folgenden 4 den Symmetrien des Rechtecks: $e, m_1 = (1\ 2)(3\ 4), m_2 = (1\ 4)(2\ 3), h = (1\ 3)(2\ 4)$. Ihre Verkettungsprodukte sind nachstehender Verknüpfungstafel zu entnehmen:

\circ	e	m_1	m_2	h
e	e	m_1	m_2	h
m_1	m_1	e	h	m_2
m_2	m_2	h	e	m_1
h	h	m_2	m_1	e

Aus der Tafel lesen wir ab, dass $R_4 = \{e, m_1, m_2, h\}$ eine Gruppe ist: R_4 ist abgeschlossen bzgl. \circ (somit \circ assoziativ in R_4); ferner ist e Einselement und sind alle Elemente invertierbar (sogar involutorisch). In Erinnerung an den Mathematiker F. Klein (1849-1925) wird R_4 als Kleinsche Vierergruppe bezeichnet.

Nach diesem Beispiel lässt sich der Begriff der Symmetriegruppe nun ohne weiteres auch allgemein erklären:

■ 10.8.4. Definition

Sei F irgendeine nichtleere Teilmenge der Ebene E (im folgenden Figur genannt). Eine Kongruenzabbildung $f \in \mathcal{K}_E$ heißt Symmetrie (oder: Deckabbildung) von F , wenn gilt: $f[F] = F$. Es bezeichne $\text{Sym}(F) := \{f \in \mathcal{K}_E \mid f[F] = F\}$ die Menge aller Symmetrien von F .

Es ist eine fundamentale Tatsache, dass die Symmetrien einer Figur F eine Gruppe (genauer: Untergruppe der Kongruenzgruppe \mathcal{K}_E) bilden. Dies besagt folgende

■ 10.8.5. Proposition

Zu beliebiger Figur F ist $\text{Sym}(F)$ eine Untergruppe von \mathcal{K}_E (die sog. Symmetriegruppe von F).

■ Beweis

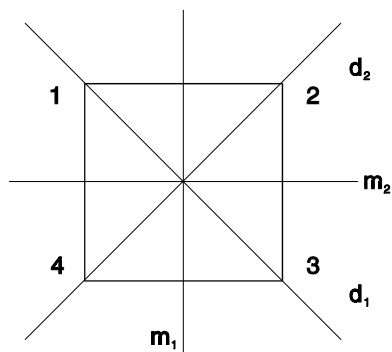
Wir benutzen das Untergruppenkriterium (Prop. 10.7.2). Seien dazu $f, g \in \text{Sym}(F)$ beliebig. Da $\text{Sym}(F)$ bzgl. \circ abgeschlossen ist – denn: $(f \circ g)[F] = f[g[F]] = f[F] = F$ –, genügt es zu zeigen, dass die Umkehrabbildung einer Symmetrie f wieder zu $\text{Sym}(F)$ gehört. Ein Punkt X liegt in $f^{-1}[F]$ genau dann, wenn $f^{-1}(Y) = X$ für ein $Y \in F$, das heißt: $f(X) \in F = f[F]$. Wegen der Injektivität von f ist dies genau für $X \in F$ der Fall, d.h. $f^{-1}[F] = F$. ♦

Die Symmetriegruppen spielen für die geschichtliche und systematische Entwicklung des Gruppenbegriffs in der Mathematik eine zentrale Rolle. So lassen sich mit ihnen geometrische Eigenschaften algebraisch beschreiben. (Auch umgekehrt werden häufig algebraische Sachverhalte geometrisch-anschaulich interpretierbar.) Das Gebiet der Abbildungsgeometrie baut geometrische Aussagenbestände systematisch mit Hilfe von Abbildungsgruppen auf. Zum Studium symmetrischer Figuren vgl. die gut lesbare Einführung von Flachsmeier / Feiste / Manteuffel: *Mathematik und ornamentale Kunstformen*. Mathematische Schülerbücherei. Leipzig: Teubner 1990.

Besonderes Interesse verdienen die Symmetriegruppen regelmäßiger n -Ecke (Polygone) P_n . Die zugehörige Symmetriegruppe wird als Diedergruppe \mathcal{D}_n bezeichnet (sprich: *Di-eder*)

Dieder bedeutet wörtlich "Zweiflächner"; man hat sich dabei das fragliche Vieleck als ein Gebilde im Raum vorzustellen, das eine "Vorderseite" und eine "Rückseite" besitzt. Damit sind nun die Spiegelungen aus \mathcal{D}_n als räumliche Klappbewegungen vorstellbar, die den Dieder mit sich selbst zur Deckung bringen. Vom algebraischen Standpunkt ist dies freilich irrelevant, da ohnehin jede Symmetrie des Dieders als Permutation seiner Eckenmenge beschreibbar ist.

Man betrachte als einfaches Beispiel einer Diedergruppe die \mathcal{D}_4 , die Symmetriegruppe des Quadrats mit den Ecken 1, 2, 3, 4. Sie besteht aus 4 Drehungen und 4 Spiegelungen, hat also die Ordnung 8. Die Drehungen bilden eine zyklische Untergruppe Δ_4 der Ordnung 4. Sie wird erzeugt von der Vierteldrehung (um den Quadratmittelpunkt), zu der die Eckenpermutation $a = (1\ 4\ 3\ 2)$ gehört. Demnach sind e ($:= a^0$), a , a^2 , a^3 die Drehungen um 0° , 90° , 180° , 270° .



Die Spiegelungen bilden zwar keine Untergruppe, doch ist jede der Spiegelungen als Verkettungsprodukt einer einzigen Spiegelung mit einer geeigneten Drehung darstellbar. Sei etwa $b := d_1 = (1)(2\ 4)(3)$ als "Grund"-Spiegelung gewählt. Dann gilt:

$$d_2 = (1\ 3)(2)(4) = b a^2$$

$$m_1 = (1\ 2)(3\ 4) = b a$$

$$m_2 = (1\ 4)(2\ 3) = b a^3$$

Insgesamt lässt sich also jedes Element der \mathcal{D}_4 in der Form a^k (als Drehung) oder $b a^k$ (als Spiegelung) mit $0 \leq k < 4$ darstellen. Die Menge der Spiegelungen erweist sich demnach als Nebenklasse $b \Delta_4$ der Untergruppe der Drehungen:

$$\mathcal{D}_4 = \{e, a, a^2, a^3, b, b a, b a^2, b a^3\}$$

Für das Rechnen mit diesen Elementen sind die folgenden Gleichungen zu Grunde zu legen:

$$a^4 = e \quad (\text{die Vierteldrehung ist ein Element der Ordnung } 4)$$

$$b^2 = e \quad (\text{die Spiegelung ist involutorisch})$$

$$b a = a^{-1} b \quad (\text{dieselbe Spiegelung an der Mittelsenkrechten einer Seite})$$

Tatsächlich lässt sich das beschriebene Vorgehen für beliebige Diedergruppen verallgemeinern. An dieser Stelle wird – unter Verzicht auf einen Beweis – der Inhalt des betreffenden **Hauptsatzes für Diedergruppen** lediglich kurz zusammengestellt und erläutert.

Die \mathcal{D}_n besteht aus n Drehungen und n Spiegelungen, also $\text{ord}(\mathcal{D}_n) = 2n$. Jede Drehung ist darstellbar als Potenz einer "kleinsten" Drehung

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & 1 & 2 & \dots & n-2 & n-1 \end{pmatrix}.$$

Ferner werde als Spiegelungselement

$$b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

gewählt. Es gelten dann die Relationen:

$$(1) \quad a^n = e$$

$$(2) \quad b^2 = e$$

$$(3) \quad b a = a^{-1} b = a^{n-1} b$$

Unter diesen Voraussetzungen ist $d \in \mathcal{D}_n$ genau dann, wenn $d = a^k$ oder $d = b a^k$ für eine ganze Zahl k mit $0 \leq k < n$.

Die Diedergruppe \mathcal{D}_n ist (bis auf Isomorphie – siehe unten) bereits vollständig durch die Relationen (1)–(3) bestimmt. Die Natur der Elemente a, b als Permutationen spielt dabei keine Rolle. Dass a eine "Drehung" und b eine

"Spiegelung" ist, wird nur durch (1) bzw. (2) ausgedrückt; es kommt dann (3) hinzu, um die Abhängigkeit der beiden Elemente untereinander festzulegen. Gleichung (3) ist geometrisch-anschaulich interpretierbar (Übung!).

■ Isomorphie

Das Wort "isomorph" bedeutet "gleichgestaltig" oder "von gleicher Struktur". Der Begriff und die zugrunde liegende Erscheinung spielen in der Mathematik eine große Rolle. Dort hat man z.B. häufig mit Gebilden zu tun, bei denen Elemente unterschiedlicher Herkunft auf entsprechend unterschiedliche Weise verknüpft werden, bei denen aber *dieselbe abstrakte Struktur* zum Vorschein kommt. "Abstrakt" heißt hier, dass von der speziellen Natur der verknüpften Elemente abzusehen ist.

■ Beispiel 1

Die Kleinsche Vierergruppe R_4 ist uns an früherer Stelle als Symmetriegruppe des Rechtecks begegnet. Sie kann aber auch auf ganz andere Weise realisiert werden, etwa als Menge $A = \{f_0, f_1, f_2, f_3\}$ von Funktionen, die durch $f_0(x) = x, f_1(x) = -x, f_2(x) = \frac{1}{x}, f_3(x) = -\frac{1}{x}$ definiert und mittels \circ (Verkettung) verknüpft werden.

Ein Vergleich der zugehörigen Verknüpfungstabellen zeigt, dass sie sich nur durch die Namen, nicht jedoch durch die gegenseitige Beziehung der verknüpften Elemente unterscheiden. Die betreffende Umbenennung beschreibt man dabei am besten als Abbildung $\gamma: A \rightarrow R_4$ mit $\gamma(f_0) = e, \gamma(f_1) = m_1, \gamma(f_2) = m_2, \gamma(f_3) = h$.

γ ist bijektiv und leistet daher die Umbenennung in umkehrbar-eindeutiger Weise. Darüberhinaus – und das ist wesentlich – bildet γ auch die Struktur beider Gebilde aufeinander ab. So besteht in A etwa die Gleichung $f_2 \circ f_1 = f_3$. Wendet man nun γ auf die hier beteiligten Elemente einzeln an, so ergibt sich $h = \gamma(f_3) = \gamma(f_2) \circ \gamma(f_1) = m_1 \circ m_2$, also eine in R_4 gültige Gleichung.

■ 10.8.6. Definition

Eine bijektive Abbildung $\gamma: G \rightarrow H$ zwischen zwei Gruppen G und H heißt Isomorphismus, wenn für alle $a, b \in G$ gilt: $\gamma(ab) = \gamma(a)\gamma(b)$. In diesem Fall heißen die beiden Gruppen zueinander isomorph (symbolisch: $G \cong H$).

Im Sinne dieser Definition ist die Abbildung γ aus Beispiel 1 ein Isomorphismus und sind die betreffenden Verknüpfungsgelände A und R_4 isomorph. Die abstrakte mathematische Betrachtungsweise unterscheidet streng genommen nicht mehr zwischen den beiden Gebilden in ihrer konkreten Beschaffenheit; sie erscheinen als Verkörperungen ein- und derselben (abstrakten) Gruppe.

■ Beispiel 2

Außer der Kleinschen Vierergruppe gibt es noch eine andere (nicht zu R_4 isomorphe) Gruppe der Ordnung 4. Diese wird z.B. verkörpert durch die Restklassengruppe (\mathbb{Z}_4, \oplus) .

Eine Vierergruppe geometrischer Herkunft ist die Gesamtheit Δ_4 der Drehungen (einer Ebene E) um $90^\circ, 180^\circ, 270^\circ$ und $0^\circ (= 360^\circ)$. Vergleicht man die Verknüpfungstabellen, so wird auch die Isomorphie beider Gebilde unmittelbar deutlich: $(\mathbb{Z}_4, \oplus) \cong (\Delta_4, \circ)$. Als Isomorphismus bietet sich in natürlicher Weise die Abbildung an, die $k \in \mathbb{Z}_4$ die Drehung um $k \cdot 90^\circ$ zuordnet.

■ Bemerkung

Die hier aufgezeigte Strukturgleichheit von Drehungsgruppe und additiver Restklassengruppe kommt nicht von ungefähr. Man deute einmal Δ_4 als "Viertelstunden-Uhr"! Dann wird klar, dass das Rechnen mit Viertelstunden nichts anderes ist als Addition modulo 4. Die naturbedingte Periodizität von Zeit- und Kalenderrechnung ist ein kulturgeschichtlich bedeutsamer Hintergrund des Umgangs mit Restklassen.

Die vorangestellten Beispiele sollten nicht den Eindruck entstehen lassen, die Isomorphie zweier Gruppen wäre ihren Verknüpfungstafeln ohne weiteres zu entnehmen. So ist die prime Restklassengruppe \mathbb{Z}_{10}^* ebenfalls zu Δ_4 isomorph, was anhand der Verknüpfungstafeln erst nach geeigneter Umstellung der Restklassen 1, 3, 7, 9 evident wird. Im Falle unendlicher (auch schon bei größeren endlichen) Gruppen verlieren solche Tafeln ohnehin ihren praktischen Wert. Isomorphieaussagen beruhen auf dem Nachweis eines Isomorphismus zwischen beiden Gebilden.

■ Beispiele

1. Sei m beliebig $\in \mathbb{Z}$; es gilt $\mathbb{Z} \cong m\mathbb{Z}$. Das zeigt der Isomorphismus $\gamma: \mathbb{Z} \rightarrow m\mathbb{Z}$, definiert durch $\gamma(k) := mk$ für alle $k \in \mathbb{Z}$ (Bildung des m -fachen einer Zahl).
2. Es gilt $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. Ein geeigneter Isomorphismus ist die Exponentialfunktion $\exp(x) = e^x$ (e Eulersche Zahl), die \mathbb{R} auf \mathbb{R}^+ bijektiv abbildet und für die gilt: $\exp(x+y) = \exp(x) \cdot \exp(y)$. Entsprechend vermittelt der natürliche Logarithmus als Umkehrabbildung von \exp einen Isomorphismus von (\mathbb{R}^+, \cdot) nach $(\mathbb{R}, +)$. Die bekannte Funktionalgleichung $\log(x \cdot y) = \log(x) + \log(y)$ bringt dies zum Ausdruck.