

Kapitel II: Die algebraischen Strukturen Gruppe, Ring, Körper

Bei den Beispielen des §1 hatten wir Mengen betrachtet, auf denen eine Addition „+“ erklärt war sowie eine Multiplikation mit Elementen aus \mathbb{R} bzw. $\{0, 1\}$. Wir hatten gesehen, dass die Rechengesetze bei den aufgeführten Fällen weitgehend übereinstimmen. Im Folgenden wollen wir uns von den „Modellen“ lösen und diese gemeinsamen Eigenschaften (auf höherer Abstraktionsstufe) untersuchen. Damit behandeln wir indirekt auch die Beispiele aus §1.

M
↓

↑
M

3 Gruppen und Halbgruppen

In allen angeführten Beispielen genügte die „Verknüpfung“ + dem assoziativen Gesetz $(a + b) + c = a + (b + c)$. Wir wollen zunächst Mengen betrachten, auf denen es eine Verknüpfung dieser Eigenschaft gibt – und beginnen so mit einer relativ einfachen algebraischen Struktur.

3.1 Definition: Halbgruppe

Sei H eine Menge, $H \neq \emptyset$. Weiter seien folgende „Axiome“ erfüllt.

(G1) Auf H ist eine **innere (binäre) Verknüpfung** definiert, d.h. eine Abbildung (Zuordnung) $* : H \times H \rightarrow H$. Schreibweise: $a * b := *(a, b)$, also $(a, b) \mapsto a * b$.

Anmerkung. Die in §1 betrachteten Additionen sind Beispiele solcher inneren Verknüpfungen, weiter die Multiplikation auf \mathbb{R} sowie die Multiplikation \odot auf $\{0, 1\}$.

(G2) $\forall a, b, c \in H : (a * b) * c = a * (b * c)$ (d.h. *** ist assoziativ**).

Dann heißt $(H, *)$ eine **Halbgruppe**.

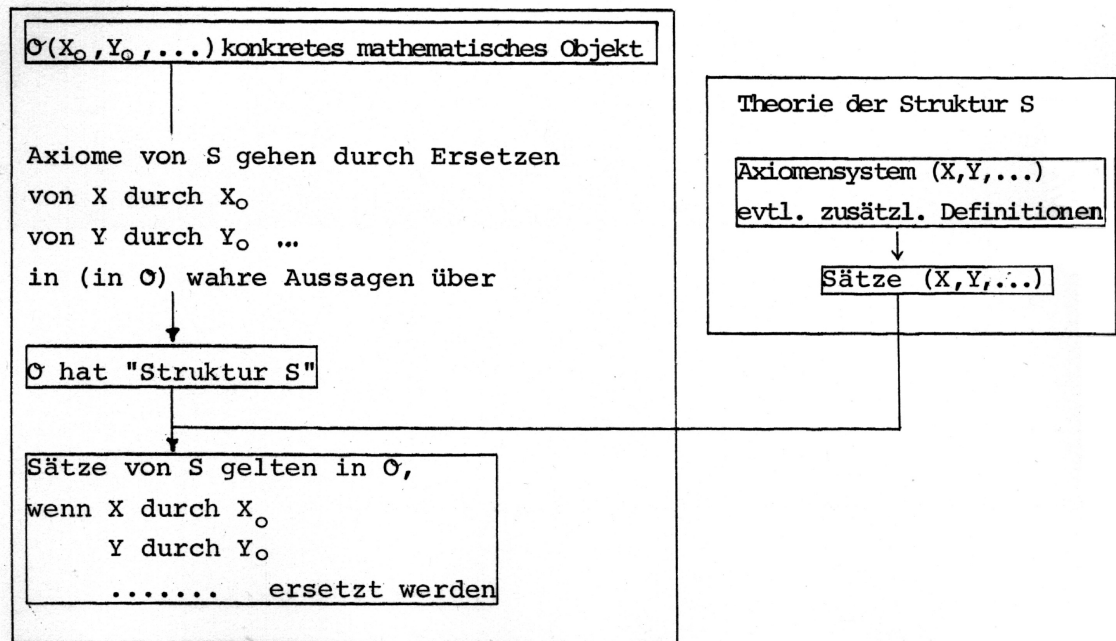
Bemerkung zur Rolle der Axiome: In den „Axiomen“ kommen H und $*$ als „Variable“ vor. Wir dürfen sie in den Anwendungen ersetzen durch jede konkrete Menge H_0 und jede konkrete Verknüpfung $*_0$, für die (G1) und (G2) zu wahren Aussagen werden, also z.B.

- H durch die Menge \mathcal{V} der Vektoren der Ebene und $*$ durch die auf dieser definierte Addition oder
- H durch $\{0, 1\}$ und $*$ durch die auf $\{0, 1\}$ erklärte Addition \oplus (s. 1.5 !) oder
- H durch $\{g, u\}$ und $*$ durch die auf $\{g, u\}$ erklärte Addition \oplus (s. 1.5 !) oder
- H durch $\{0, 1\}$ und $*$ durch \odot usw..

Jede der aus (G1) und (G2) allgemein hergeleiteten Aussagen gilt unter diesen Voraussetzungen auch für H_0 und $*_0$.

Die Anwendungsmöglichkeit einer „axiomatischen Theorie“ auf ein konkretes mathematisches Objekt zeigt das folgende **vereinfachte Schema** (Figur 3.1):

M
↓



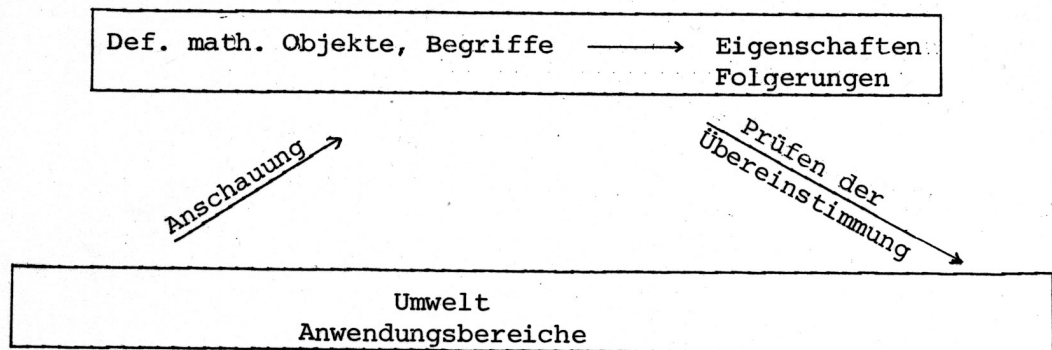
Figur 3.1: Schema für die Anwendung einer axiomatisch definierten Struktur

Beispiel. Hier gehen wir zuerst auf die Halbgruppen-Struktur S ein.

3.2 Exkurs: Mathematik und die reale Welt

Wir vermerken, dass diese Möglichkeit der „gleichzeitigen“ Untersuchung der Eigenschaften einer Vielzahl mathematischer Objekte nur **eine** Seite des axiomatischen Arbeitens ist.

Eine andere, noch tiefer liegende, steht im engen Zusammenhang mit der Beschreibung unserer Umwelt in mathematischen Modellen. Hierbei werden (undefinierte) Grundbegriffe und Zusammenhänge zwischen diesen aus der Anschauung entnommen und in (unbeweisbaren) Axiomen an den Anfang einer Theorie gestellt. Ist das Axiomensystem geeignet gewählt, so ergeben sich auch weitere Übereinstimmungen mit dem untersuchten Sachverhalt der Umwelt, der damit inner-mathematisch „nachmodelliert“ ist. Ziel ist dann oft der Nachweis, dass bis auf Schreib- und Bezeichnungweise **nur ein Modell** für dieses Axiomensystem existiert (Bsp.: Hilbert'sches Axiomensystem des Raumes; → Vorlesung (Elementar-)Geometrie).



Figur 3.2: Mathematik und die reale Welt

Beispiele.

(i) Elemente von $\mathbb{R}^2 \longleftrightarrow$ Punkte der Anschauungsebene.
(Die Pythagoräer versuchten, mit \mathbb{Q}^2 „auszukommen“.)

(ii) Elemente von $\mathcal{V} \longleftrightarrow$ konkrete Parallelverschiebungen der Anschauungsebene.

(Diese Entsprechungen sind nicht beweisbar, da die Objekte der Anschauung entnommen sind).

Ende des Exkurses.

↑
M

Wir kommen zurück zur Halbgruppen-Struktur. Hierfür gibt es viele Beispiele.

Anmerkung. Im folgenden benutzen wir bei Beispielen auch einige Eigenschaften der Verknüpfungen $+$ und \cdot von \mathbb{N} (der Menge der natürlichen Zahlen), von \mathbb{Z} (der Menge der ganzen Zahlen), von \mathbb{Q} (der Menge der rationalen Zahlen) und \mathbb{R} (der Menge der reellen Zahlen). Diese **setzen wir als** aus der Schule oder der Vorlesung Analysis **bekannt voraus**. Da sie hier **lediglich bei Beispielen, Motivation, etc.** vorkommen, wird dadurch der exakte Aufbau nicht gestört.

M
↓

↑
M

Beispiele.

(1) $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}, \cdot) sind Halbgruppen.

(2) $(\mathbb{N}, *_1)$ mit $*_1 : \begin{cases} \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \\ (a, b) \mapsto a^b \end{cases}$ ist keine Halbgruppe, da das Assoziativgesetz

verletzt ist:²³ $2 *_1 (3 *_1 2) = 2^9 \neq 8^2 = (2 *_1 3) *_1 2$.

(3) $(\mathbb{N}, -)$ mit „ $-$ “ : $\begin{cases} \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \\ (a, b) \mapsto a - b \end{cases}$ ist keine Halbgruppe, da „ $-$ “ keine innere

Verknüpfung auf \mathbb{N} ist.

(4) Sei M Menge, $M \neq \emptyset$. Dann sind $(\wp(M), \cap)$, $(\wp(M), \cup)$, $(\wp(M), \Delta)$ Halbgruppen²⁴. (Beweis ?)

(5) $(\mathcal{V}, +)$ ist Halbgruppe (\mathcal{V} Menge der Vektoren der Ebene, soweit in (1.1) behandelt.)

(6) Sei M Menge und $\text{Abb}(M, \mathbb{R}) := \{f | f : M \rightarrow \mathbb{R} \text{ Abbildung}\}$ (andere Schreibweise: \mathbb{R}^M)!
Für $f, g \in \text{Abb}(M, \mathbb{R})$ definieren wir $\mathbf{f} + \mathbf{g}$ durch $(f + g)(x) := f(x) + g(x)$ für alle $x \in M$.
Dann gilt:

$(\text{Abb}(M, \mathbb{R}), +)$ ist Halbgruppe.

Beweis ...

Analog kann man $(\text{Abb}(M, \mathbb{R}), \cdot)$ definieren.

(7) Sei M Menge; dann ist $(\text{Abb}(M, M), \circ)$ Halbgruppe; (Erinnerung: $g \circ h(x) = g(h(x))$.)

Beweis. „ \circ “ ist innere Verknüpfung nach (2.6.1), und das Assoziativgesetz gilt gemäß (2.6.2).

²³wie auch bei „Mädchen(handels)schule“ und „(Mädchen handels)schule“ Hinweis von Prof. Lenz, „(Fachwerk)stadt“ und „Fach(werkstadt)“, „(Vogelflug)linie“ und „Vogel(fluglinie)“, „(Dschungelfeuer)löscher“ und „Dschungel(feuerlöscher)“.

²⁴mit der Potenzmenge $\wp(M)$ von M

3.3 Definition: neutrales Element

Sei $(H, *)$ Halbgruppe, $e \in H$. Dann heißt e **neutrales Element** von $(H, *)$ g.d.w. gilt:

$$\forall a \in H : e * a = a = a * e .$$

Beispiele.

- (a) $(\mathbb{N}, +)$ besitzt kein neutrales Element. (Denn: $e + a = a \Rightarrow e = 0$; $0 \notin \mathbb{N}$).²⁵
 0 ist neutrales Element von $(\mathbb{N}_0, +)$, wobei $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
 1 ist neutrales Element von (\mathbb{N}, \cdot) .
- (b) M ist neutrales Element von $(\wp(M), \cap)$.
 \emptyset ist neutrales Element von $(\wp(M), \cup)$.
 \emptyset ist neutrales Element von $(\wp(M), \Delta)$.
- (c) $\vec{0}$ ist neutrales Element von $(\mathcal{V}, +)$
- (d) Existiert ein neutrales Element von $(\text{Abb}(M, \mathbb{R}), +)$, von $(\text{Abb}(M, \mathbb{R}), \cdot)$?

Anmerkung. Bezeichnet man die Verknüpfung „*“ einer Halbgruppe als Addition „+“, so nennt man ein evtl. existierendes neutrales Element²⁶ auch **Nullelement** „0“, ähnlich im Falle der Multiplikation „·“ auch **Einselement** „1“.

3.4 Satz (Eindeutigkeit des neutralen Elements)

In einer Halbgruppe gibt es höchstens ein neutrales Element.

Beweis. Seien e_1, e_2 neutrale Elemente der Halbgruppe $(H, *)$. Dann gilt:

$$\begin{aligned} e_1 &= e_1 * e_2 && \text{(da } e_2 \text{ neutrales Element ist)} \\ &= e_2 && \text{(da } e_1 \text{ neutrales Element ist).} \end{aligned}$$

□

3.5 Definition: Inverse

Sei $(H, *)$ Halbgruppe mit neutralem Element e ; sei $a \in H$! Dann heißt a **invertierbar**, wenn gilt:

$$\exists \bar{a} \in H : a * \bar{a} = e = \bar{a} * a .$$

\bar{a} heißt dann **Inverse** zu a .

Beispiel. (i) In $(\mathbb{R}, +)$ ist $-r$ Inverse von r (für beliebiges $r \in \mathbb{R}$); in (\mathbb{R}, \cdot) ist nur 0 nicht invertierbar; in $(\mathbb{N}_0, +)$ besitzt allein 0 eine Inverse (nämlich 0 selbst).

²⁵Ein Teil der Mathematiker bezeichnen mit \mathbb{N} abweichend von uns die Menge/Halbgruppe der natürlichen Zahlen *einschließlich* der Null; es gibt sogar eine diesbezügliche DIN-Norm.

²⁶falls keine Verwechslungen zu befürchten sind

(ii) In $(\wp(M), \cap)$ hat kein Element $T \neq M$ eine Inverse: Sei $T \subseteq M$; dann existiert $\bar{T} \subseteq M$ mit $T \cap \bar{T} = M$ nur, wenn $T = M = \bar{T}$ gilt.

(iii) In $(\mathcal{V}, +)$ ist $-\vec{a}$ Inverse von \vec{a} .

Schreibweise der Inversen²⁷: a^{-1} , falls $*$ als Multiplikation,
 $-a$, falls $*$ als Addition geschrieben wird.

3.6 Satz (Zur Eindeutigkeit der Inversen)

Sei $(H, *)$ Halbgruppe mit neutralem Element e . Besitzt dann $a \in H$ ein inverses Element, so ist dieses eindeutig bestimmt.

Beweis. Seien \bar{a}_1, \bar{a}_2 Inverse von a , gelte also insbesondere $\bar{a}_1, \bar{a}_2 \in H$, $a * \bar{a}_2 = e$ und $\bar{a}_1 * a = e$. Dann folgt

$$\begin{aligned} \bar{a}_1 &= \bar{a}_1 * e && (e \text{ ist neutrales Element der Halbgruppe}) \\ &= \bar{a}_1 * (a * \bar{a}_2) && (\text{nach Voraussetzung}) \\ &= (\bar{a}_1 * a) * \bar{a}_2 && (\text{nach dem Assoziativgesetz}) \\ &= e * \bar{a}_2 && (\text{laut Voraussetzung}) \\ &= \bar{a}_2 && (e \text{ ist neutrales Element der Halbgruppe}). \end{aligned}$$

□

(iv) Wir behandeln nun den Spezialfall von Halbgruppen, in denen jedes Element invertierbar ist:

3.7 Definition: Permutation

Sei M n.l. Menge. Eine bijektive Abbildung von M auf sich heißt auch **Permutation**; wir definieren $\mathcal{S}_M := \text{Bij}(M, M) := \{f : f \text{ Permutation von } M\}$ und $\mathcal{S}_n := \mathcal{S}_{\{1, 2, \dots, n\}}$.

Schreibweise: Ist $f \in \mathcal{S}_n$, so schreiben wir auch $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$.

Beispiel. Sei $M = \{1, 2, 3\}$; in Figur 3.3 betrachten wir \mathcal{S}_3 . Man kann zeigen, dass gilt:

$$\mathcal{S}_3 = \{\text{id}_M, \sigma_1, \sigma_2, \sigma_3, \delta_1, \delta_2\}.$$

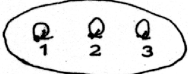


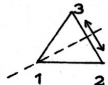

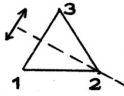

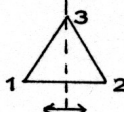



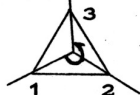
3.8 Hilfssatz (\mathcal{S}_M)

Sei M Menge, $M \neq \emptyset$. Dann gilt:

- (a) (\mathcal{S}_M, \circ) ist Halbgruppe (wie wir später sehen, sogar Gruppe, s. 3.11).
- (b) id_M ist neutrales Element von (\mathcal{S}_M, \circ) .
- (c) Zu $f \in \mathcal{S}_M$ ist f^{-1} Inverse in (\mathcal{S}_M, \circ) .
- (d) Für $|M| \geq 3$ ist (\mathcal{S}_M, \circ) nicht kommutativ²⁸.

²⁷falls keine Verwechslungen zu befürchten sind

²⁸Vgl. Definition (3.9)!

Elemente von \mathcal{S}_3 :	Pfeildiagramm	Anwendung: Symmetrien eines gleichseitigen Dreiecks
$\delta_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}_M$		
$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$		
$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$		
$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$		
$\delta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$		
$\delta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$		

Figur 3.3: Elemente von \mathcal{S}_3 und die entsprechenden Symmetrien eines Dreiecks.

3.9 Definition: kommutative/abelsche Halbgruppe

Eine Halbgruppe $(H, *)$ heißt **kommutativ** oder (synonym) **abelsch**²⁹, wenn für alle $a, b \in H$ gilt:

$$a * b = b * a.$$

Beweis von Hilfssatz (3.8). (a) „ \circ “ ist innere Verknüpfung nach (2.5.4b); das Assoziativgesetz gilt nach (2.5.2).

(b) Beispiel 5 nach (2.5.1)

(c) f^{-1} ist Abbildung nach (2.4.6), Inverse von f nach (2.5.4)(a), Bijektion ebenfalls nach (2.5.4)(a).

(d) Seien o.B.d.A. $\{1, 2, 3\} \subseteq M$; die Fortsetzungen von σ_1 und δ_1 (s. Bsp. oben) auf M kommutieren nicht.

$$\text{Z.B. ist } \sigma_1 \circ \delta_1(1) = \sigma_1(2) = 3 \neq 2 = \delta_1(1) = \delta_1 \circ \sigma_1(1).$$

²⁹nach dem norwegischen Mathematiker Niels Henrik Abel, 1802-1829

□

3.10 Definition: Gruppe

Sei G eine Menge und $*$ eine Verknüpfung auf G ; sei ferner $e \in G$ ein fest gewähltes Element. Weiter seien folgende Axiome erfüllt;

$$(G1) \quad * \text{ ist innere Verknüpfung, also } * : \begin{cases} G \times G \rightarrow G \\ (a, b) \mapsto a * b \end{cases} ;$$

$$(G2) \quad \forall a, b, c \in G : a * (b * c) = (a * b) * c \quad (\text{Assoziativgesetz}) ;$$

$$(G3) \quad \forall a \in G : e * a = a = a * e \quad (\text{Existenz eines neutralen Elements});$$

$$(G4) \quad \forall a \in G \exists \bar{a} : a * \bar{a} = e = \bar{a} * a \quad (\text{Existenz aller Inversen}).$$

Dann heißt $(G, *)$ **Gruppe mit neutralem Element e** .

Anmerkung:

$(G, *)$ Gruppe $\Rightarrow (G, *)$ Halbgruppe mit neutralem Element e (nach (G1), (G2)).

Anmerkung (zur Schreibweise). Die (abstrakt definierte) Verknüpfung $*$ wird (wie oben schon angedeutet) oft als Multiplikation, im Fall einer kommutativen Gruppe auch als Addition geschrieben. Falls keine Verwechslungen (zwischen Menge und Gruppe) zu befürchten sind und klar ist, welche Verknüpfung gemeint ist, schreibt man oft nur G statt $(G, *)$.

3.11 Elementare Eigenschaften von Gruppen

Sei $(G, *)$ Gruppe. Dann gilt:

- (a) In $(G, *)$ existiert genau ein neutrales Element.
- (b) In $(G, *)$ hat jedes Element $a \in G$ genau eine Inverse
Bezeichnung a^{-1} (bzw. $-a$ im Falle additiver Schreibweise).

Beweis. Nach (G3) existiert mindestens ein neutrales Element, nach (3.3) ist dieses eindeutig bestimmt. Nach (G4) existiert zu jedem Element ein inverses Element; nach (3.6) ist die Inverse jeweils eindeutig bestimmt. □

Beispiele:

3.12 Korollar zu (3.8): S_M als Gruppe

Ist M n.l. Menge, so gilt:

(S_M, \circ) ist eine Gruppe.

Sie heißt symmetrische Gruppe auf M ; ist speziell $M = \{1, \dots, n\}$, so heißt sie **symmetrische Gruppe vom Grad n** .

Beispiele weiterer Gruppen. $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)^{30}$, $(\mathbb{Q}, +)$, (\mathbb{Q}^*, \cdot) , $(\mathbb{Z}, +)$, $(\emptyset(M), \Delta)$, $(\mathcal{V}, +)$, $(\{0, 1\}, \oplus)$, $(\{1\}, \odot)$, $(\text{Abb}(M, \mathbb{R}), +)$ und 'die' Menge der Drehungen eines regelmäßigen n -Ecks bzgl. Hintereinanderausführung als Verknüpfung.³¹

Bei den eben aufgeführten Beispielen stehen einige in engem Zusammenhang, z.B. $(\mathbb{R}, +)$ und $(\mathbb{Q}, +)$; es ist ja $\mathbb{Q} \subseteq \mathbb{R}$ und „die Addition auf \mathbb{Q} “ (, die wir kurzfristig mit „ $+_{\mathbb{Q}}$ “ bezeichnen,) stimmt mit der auf \mathbb{R} („ $+_{\mathbb{R}}$ “) überein“. Es gilt also für $q_1, q_2 \in \mathbb{Q}$

$$q_1 +_{\mathbb{Q}} q_2 = q_1 +_{\mathbb{R}} q_2 .$$

3.13 Definition induzierte Verknüpfung, Untergruppe

Seien $(G, *)$ Gruppe (insbesondere $* : G \times G \rightarrow G$) und $U \subseteq G$.

(a) Ist dann $U * U \subseteq U$, so heißt U **abgeschlossen** bzgl. der Verknüpfung $*$; und

$$*_U : \begin{cases} U \times U \rightarrow U \\ (u, v) \mapsto u * v \end{cases}$$

heißt die von G auf U **induzierte (innere) Verknüpfung**. Alternative Bezeichnung $*|_{U \times U \rightarrow U}$.

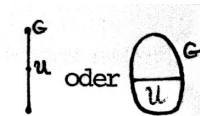
Anmerkung. $*_U$ entsteht dabei aus $*$ durch Einschränkung des Definitions-Bereichs und des Werte-Bereichs auf $U \times U$ bzw. U .

Beispiele: \mathbb{N} und \mathbb{Z} sind abgeschlossen in \mathbb{Q} bzgl. der Addition; \mathbb{N} und \mathbb{Z}^* sind abgeschlossen in (\mathbb{Q}^*, \cdot) .

Ist zusätzlich $(U, *_U)$ Gruppe, so heißt $(U, *_U)$ **Untergruppe** von $(G, *)$ (abgekürzt „ U UG von G “, in Zeichen $U \leq G$.

(b) *Anmerkung.* Ist G **endlich**, so folgt schon aus der Abgeschlossenheit von U bzgl. $*$, dass $(U, *_U)$ Untergruppe ist. (Beweis?)

Ein weiteres Untergruppen-Kriterium ist in (3.16) zitiert (s.u.). Sind keine Verwechslungen zubefürchten, so schreiben, wir statt $*_U$ auch nur $*$.



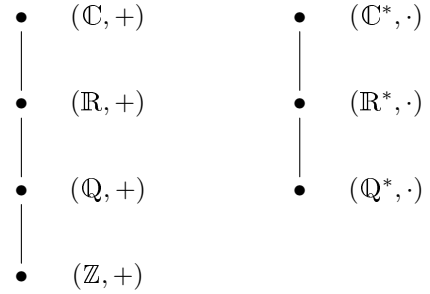
Figur 3.5: Symbolische Darstellung der Untergruppen-Beziehung

Beispiele.

³⁰ $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$

³¹Zu jedem regelmäßigen n -Eck gibt es eine solche Gruppe; nur ist es so, dass sich (für festes n) diese Gruppen „in ihrer Struktur nicht wesentlich unterscheiden“.

- $(\mathbb{Z}, +)$ ist Untergruppe (UG) von $(\mathbb{Q}, +)$;
- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ sind UG'n von $(\mathbb{R}, +)$;
- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sind UG'n von $(\mathbb{C}, +)$;
- (\mathbb{Q}^*, \cdot) ist UG von (\mathbb{R}^*, \cdot) ;
- $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$ sind UG'n von (\mathbb{C}^*, \cdot) .



Figur 3.6: Diagramm für die additiven bzw. multiplikativen Gruppen einiger Zahlbereiche

3.14 Hilfssatz: neutrales Element, Inversen in einer Untergruppe

Seien (G, \cdot) Gruppe, U Untergruppe von G und $a \in U$. Dann gilt:

- (i) e ist neutrales Element von G . $\iff e$ ist neutrales Element von U .
- (ii) a^{-1} ist Inverse von a in G . $\iff a^{-1}$ ist Inverse von a in U .

Beweis. (i) Seien e_U bzw. e_G die neutralen Elemente von U bzw. G , dann gilt:

$$\begin{aligned}
 e_U \cdot e_G &= e_U && \text{(da } e_G \text{ neutrales Element von } G \text{ ist)} \\
 &= e_U \cdot e_U && \text{(da } e_U \text{ neutrales Element von } U \text{ ist)}
 \end{aligned}$$

und damit $e_U \cdot e_U = e_U \cdot e_G$, also $e_U^{-1} \cdot (e_U \cdot e_U) = e_U^{-1} \cdot (e_U \cdot e_G)$, mit der Inversen e_U^{-1} von e_U in G , woraus $e_U = e_G$ folgt.

- (ii) Sei a_G^{-1} Inverse von a in G , a_U^{-1} von a in U . Dann ergibt sich

$$a_U^{-1} \cdot a = a \cdot a_U^{-1} \stackrel{\text{Def.}}{=} e_U \stackrel{(i)}{=} e_G \stackrel{(3.11b)}{\implies} a_G^{-1} = a_U^{-1}.$$

□

3.15 Definition: Komplexschreibweise

Seien (G, \cdot) Gruppe, $A, B \subseteq G$ und $a_0, b_0 \in G$. Dann vereinbaren wir folgende abkürzende Schreibweise („Komplexschreibweise“):

$$\begin{aligned}
 A \cdot B &:= \{a \cdot b : a \in A \wedge b \in B\} \\
 a_0 \cdot B &:= \{a_0 \cdot b : b \in B\} = \{a_0\} \cdot B \\
 A \cdot b_0 &:= A \cdot \{b_0\} \\
 A^{-1} &:= \{a^{-1} : a \in A\}
 \end{aligned}$$

Damit können wir leicht hinreichende (und notwendige) Bedingungen dafür formulieren, dass U eine UG von G bildet:

3.16 Satz (Untergruppenkriterium)

Sei (G, \cdot) eine Gruppe und $U \subseteq G$. Dann gilt

$$U \text{ ist Untergruppe von } G. \iff U \neq \emptyset \wedge U \cdot U^{-1} \subseteq U.$$

(Machen Sie sich bitte klar, wo in der Formulierung von (3.16) G und U die Gruppe (G, \cdot) bzw. Untergruppe (U, \cdot_U) bezeichnen und wo die diesen zugrunde liegenden Mengen!)

Beweis. „ \Rightarrow “ $U \text{ UG} \implies \exists e \in U \implies U \neq \emptyset$
 $U \text{ UG} \xrightarrow{(3.13), (3.10), (3.14)(ii)} U^{-1} \subseteq U \xrightarrow{(3.13), (G1)} U \cdot U^{-1} \subseteq U.$
 „ \Leftarrow “ (G3) $U \neq \emptyset \implies \exists a \in U \implies \exists a^{-1} \in G \xrightarrow{(a \in U)} \exists a^{-1} \in U^{-1},$
 also $e = a \cdot a^{-1} \in U \cdot U^{-1} \subseteq U \xRightarrow{\text{Vor.}} e \in U$
 und e neutrales Element in U .
 (G4) Sei $a \in U$; a^{-1} existiert in G und damit $a^{-1} \in U^{-1}$;
 ferner $e \in U$, also $a^{-1} = e \cdot a^{-1} \in U \cdot U^{-1} \subseteq U$.
 (G1) $[a, b \in U \xrightarrow{\text{s.o.}} a, b^{-1} \in U \implies a(b^{-1})^{-1} \in U \cdot U^{-1} \subseteq U$
 $\xrightarrow{(b^{-1})^{-1}=b} a \cdot b \in U] \implies U$ abgeschlossen (bzgl. \cdot).
 (G2) ist erfüllt, da schon die Obermenge (G, \cdot) assoziativ ist. □

Beispiel. Seien $n \in \mathbb{N}$ und $n\mathbb{Z} := \{n \cdot z : z \in \mathbb{Z}\}$. Dann gilt:

$$(n\mathbb{Z}, +) \text{ ist Untergruppe von } (\mathbb{Z}, +).$$

Beweis. $(\mathbb{Z}, +)$ ist Gruppe, $n\mathbb{Z} \subseteq \mathbb{Z}$; $n\mathbb{Z} \neq \emptyset$; ferner
 $nz_1, nz_2 \in n\mathbb{Z} \implies nz_1 + (-nz_2) = n(z_1 - z_2) \in n\mathbb{Z} \xrightarrow{(3.16)}$ Behauptung. □

Anmerkung. Für $m, n \in \mathbb{N}$ gilt $m\mathbb{Z} \subseteq n\mathbb{Z} \iff n|m \iff \exists t \in \mathbb{N}_0 : m = nt$. Beweis?

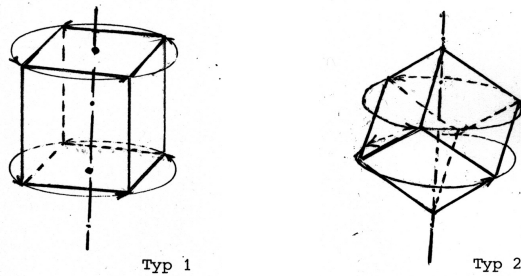
M
↓

3.17 Anhang: Gruppe der Deckbewegungen eines Würfels

Literatur: Grundkurs Mathematik II 2, DIFF-Studienbrief, Tübingen 1972.

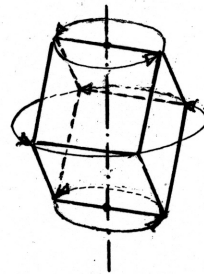
Eigentliche Bewegungen des Raumes sind solche „Kongruenzabbildungen“, die sich aus Translationen (Parallelverschiebungen) und Drehungen zusammensetzen lassen. Unter einer (eigentlichen) **Deckbewegung** eines Körpers im Raum versteht man eine eigentliche Bewegung, die den Körper in sich überführt. Die (eigentlichen) Deckbewegungen eines Körpers beschreiben alle seine Symmetrie-Eigenschaften, wenn man von der Spiegelsymmetrie absieht. Man kann zeigen, dass die Menge der (eigentlichen) Deckbewegungen eines Körpers bzgl. Hintereinanderausführung eine Gruppe bildet. Als Beispiel betrachten wir die **Würfelgruppe** \mathcal{W} , d.h. die Gruppe der eigentlichen Bewegungen des Würfels auf sich. Der Würfel hat die folgenden drei Typen von Dreh-Symmetrieachsen:

1. Achsen durch die Schwerpunkte gegenüberliegender Flächen; Drehung um 90° , 180° , 270° . Es gibt $3 \cdot 3 = 9$ entsprechende Drehungen.



Figur 3.7 a/b: Drehachsen von Deckabbildungen eines Würfels

2. Die räumlichen Diagonalen; Drehung um 120° und 240° . Zu den 4 Raumdiagonalen gibt es $4 \cdot 2 = 8$ entsprechende Drehungen.
3. Achsen durch die Mitte gegenüberliegender Kanten; Drehung um 180° . Von diesem Typ gibt es 6 Drehungen.



Typ 3

Figur 3.7 c: Drehachse einer weiteren Deckabbildung eines Würfels

Zusammen mit der Identität haben wir 24 Deckbewegungen gefunden. Da bei einer Deckbewegung des Würfels jede räumliche Diagonale wieder in eine solche abgebildet wird und umgekehrt jede bijektive Abbildung der Raumdiagonalen zu einer eigentlichen Deckabbildung gehört, ist 24 ($= |S_4|$) auch die genaue Anzahl der eigentlichen Deckabbildungen. Damit haben wir alle Elemente der Würfelgruppe \mathcal{W} angegeben.

Literaturhinweis. Zu Symmetrien (u.a. in Natur und Kunst) allgemein sind die folgenden Abhandlungen besonders lesenswert.

- H.Weyl: Symmetrie, Birkhäuser Verlag, 1981²; (auch als e-book erhältlich)
- E.Quaisser: Die Symmetriestruktur von Figuren. In A.Beutelspacher et al.(Hrsg.): Jahrbuch Überblicke Mathematik 1995, Vieweg Verlag, p.147-161, 1995.(Gebraucht erhältlich)
- R.Wille (Hrsg.): Symmetrie in Geistes- und Naturwissenschaft. Springer Verlag, Berlin etc. 1988; (als e-book erhältlich)

Weitere Literatur:

P.B:Yale: Geometry and Symmetry. Dover Publ., New York 1968.

H.F.Verheyen: Symmetry Orbits. Birkhäuser V., Boston etc. 1996. (auch als e-book erhältlich)

- Beachten sie auch Bücher über Kristallographie!

Übungsaufgaben:

Aufgabe 3.1: Bezeichne \mathcal{W} die Würfelgruppe!

- a) Bestimmen Sie zu jedem Element $x \in \mathcal{W}$ die kleinste Zahl $n \in \mathbb{N}$ mit

$$x^n = \text{id},$$

(die sogenannte Ordnung von x)! Dabei ist $x^n := x \circ x \circ x \circ \dots \circ x$ (mit n 'Faktoren').

- b) Nummerieren Sie die Raumdiagonalen und geben zu jedem Element von \mathcal{W} die entsprechende Permutation der Raumdiagonalen an!
- c) Bestimmen Sie Elemente $x_1, x_2, x_3 \in \mathcal{W}$ derart, dass jedes Element von \mathcal{W} sich als Produkt mit Faktoren aus $\{x_1, x_2, x_3\}$ schreiben lässt! (Man sagt dann, dass x_1, x_2, x_3 die Gruppe \mathcal{W} erzeugen).

Aufgabe 3.2: Bezeichne \mathcal{D}_5 die Gruppe der Symmetrieabbildungen (Dreh- und Spiegelungssymmetrien) „des“ regelmäßigen 5-Ecks! Zeigen Sie, dass gilt:

- a) \mathcal{D}_5 enthält 5 Spiegelungen und 5 Drehungen (einschließlich der Drehung id um 0°).
- b) $|\mathcal{D}_5| = 10$. (Es gibt also keine weiteren Deckabbildungen).
- c) \mathcal{D}_5 enthält genau eine Untergruppe der Elemente-Anzahl (Ordnung) 5 und genau 5 weitere Untergruppen (außer $\{\text{id}\}$ und \mathcal{D}_5 selbst).

Anmerkung: 1.) Diese Gruppe spielte eine Rolle bei der Bestimmung von Prüfwerten für die Nummern der letzten DM-Banknoten.

2.) Diese Aufgabe wird mit Aufgabe 4.2 fortgesetzt.

Aufgabe 3.3 Das Schema $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}$ rationaler Zahlen nennen wir ein **magisches**

Quadrat (über \mathbb{Q} mit 3×3 Feldern), wenn alle Zeilen- und Spaltensummen sowie die Summen beider Diagonalen den gleichen Wert s haben, wenn also gilt:

$$s = a + b + c = d + e + f = g + h + j = a + d + g = b + e + h = c + f + j = a + e + j = c + e + g.$$

Zu zwei magischen Quadraten $M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}$ und $N = \begin{pmatrix} a' & b' & c' \\ d' & e' & f' \\ g' & h' & j' \end{pmatrix}$ definieren

wir eine Summe durch $M + N := \begin{pmatrix} a + a' & b + b' & c + c' \\ d + d' & e + e' & f + f' \\ g + g' & h + h' & j + j' \end{pmatrix}$.

- a) Zeigen Sie: M ist durch (a, b, c) bestimmt, und zu jedem Tripel $(a, b, c) \in \mathbb{Q}^3$ gibt es ein magisches Quadrat mit erster Zeile (a, b, c) !
- b) Beweisen Sie: Die Menge G aller magischen 3×3 -Quadrate über \mathbb{Q} bildet bzgl. der oben definierten Addition eine kommutative Gruppe !