Modul
Grundbildung Lineare Algebra und analytische Geometrie SoSe 2010

Hinweis: Dieses Manuskript setzt das Skript aus dem letzten Semester fort. Es ist nur verständlich und von Nutzen für Personen, die gleichzeitig regelmäßig und aktiv die zugehörige Vorlesung besuchen (also nicht nur körperlich anwesend sind), und es wurde auch nur für diesen Hörerkreis geschrieben. Es erhebt keinen Anspruch auf Vollständigkeit, Fehler sind zwar ärgerlich, aber leider nicht auszuschließen!

3 Gruppen

1 Grundlegendes über Gruppen

Bereits zu Beginn des zweiten Kapitels über Zahlen[1] haben wir im Zusammenhang mit Körpern den Begriff Gruppe erwähnt und einige Beispiele für Gruppen kennengelernt. Damals wurde gesagt (vielleicht erinnern Sie sich), dass zu einer Gruppe eine binäre Verknüpfung gehört, für die das Assoziativgesetz gültig ist. Ferner wurde die Existenz eines sogenannten neutralen Elements verlangt, außerdem sollte jedes Element ein inverses Element besitzen. Jetzt wollen wir unser Wissen vertiefen und systematisieren.

Def 1.1 Jede nichtleere Menge G mit einer binären Verknüpfung $* : G \times G \to G$ heißt *Gruppoid*, geschrieben $(G, *)$.

An Stelle von binäre Verknüpfung sagt man auch *binäre Operation (auf G)*.

Beispiele: Bei welchen der folgenden Mengen mit den zugehörigen Operationen handelt es sich um Gruppoide?

Menge	$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$	$\{1\}$	$\{2\}$	$\mathbb{Q}^+$
Operation	$+$	$-$	$*$	$\cdot$	$+$	$\star$

Hierbei sollen $*$ und $\star$ so definiert sein: $n * m := \max\{4n + 3m, 315\}$, $\quad r \star s := \sqrt{r \cdot s}$.

Bei den Elementen von Gruppoiden muss es sich nicht um Zahlen handeln, auch $(\operatorname{Pot} M, \cup)$, $(\operatorname{Pot} M, \cap)$ oder $(\operatorname{Abb}(\mathbb{R}, \mathbb{R}), \circ)$ sind Gruppoide (mit $\circ$ ist die Verkettung von Abbildungen gemeint).

Besteht ein Gruppoid nur aus endlich vielen Elementen, können wir alle möglichen Verknüpfungsergebnisse in Form einer *Verknüpfungstafel* aufschreiben:

$\circ$	a	b	c	$\cdots$
a				
b		X		
c				
$\vdots$				

An der Stelle X wird das Ergebnis $b \circ c$ eingetragen usw.

[1] Siehe Skript S. 23

Beispiele: Gesucht sind die Verknüpfungstafeln der Gruppoide $(\mathbb{Z}_4, \cdot_4)$ und $(\mathbb{Z}_4, +_4)$

$\cdot_4$	0	1	2	3
0				
1				
2				
3				

$+_4$	0	1	2	3
0				
1				
2				
3				

Wir werden diese Tafeln in Vorlesung und/oder Übung ergänzen.

Für eine endliche Menge G sind zwei Gruppoide $(G, \circ)$ und $(G, *)$ verschieden, falls sich die zugehörigen Verknüpfungstafeln an mindestens einer Stelle unterscheiden. Für $|G| = n$ gibt es also $n^{(n^2)}$ viele verschiedene Gruppoide – zu jeder Verknüpfungstafel gehören n^2 Einträge, für jeden Eintrag gibt es n Möglichkeiten. Da die Gruppoid–Definition recht allgemein ist, sind die meisten Beispiele uninteressant. Wir wollen daher nur noch Gruppoide mit zusätzlichen Eigenschaften untersuchen. Wenn die Verknüpfung eindeutig klar ist oder wenn es nicht auf die spezielle Verknüpfung ankommt (wie manchmal in Definitionen oder in Sätzen) werden wir kürzer von dem Gruppoid G reden und die zugehörige Verknüpfung je nach Laune mit $\circ$ oder $*$ bezeichnen.

Def 1.2 $e \in G$ heißt *neutrales Element* oder *Einselement* : $\Longleftrightarrow \quad e \circ x = x \circ e = x \quad \forall x \in G.$

Beispiele: 1) In $(\mathbb{Z}, +)$ ist 0, in $(\mathbb{R}, \cdot)$ ist 1 neutrales Element.

2) In $(\mathbb{Z}, -)$ ist 0 *nicht* neutral, denn es gilt nicht für alle Zahlen $0 - z = z$, beispielsweise erhalten wir für $1 \in \mathbb{Z}$ die Ungleichung $0 - 1 = -1 \neq 1$.

3) $(\mathbb{N}, \mathrm{kgV})$: Hier ist 1 neutrales Element, denn $\mathrm{kgV}\,(n, 1) = n = \mathrm{kgV}\,(1, n)$ für alle $n \in \mathbb{N}$.

4) Das Gruppoid $(\mathrm{Pot}\,(M), \cup)$ hat $\emptyset$ als neutrales Element.

Satz 1.1 Jedes Gruppoid G hat höchstens ein neutrales Element.

Beweis: Angenommen, e_1 und e_2 sind beide neutrale Elemente von G. Wir untersuchen $e_1 * e_2$:

e_1 ist neutral, also $e_1 * e_2 = e_2$. Da e_2 ebenfalls neutral ist, gilt $e_1 * e_2 = e_1$. Insgesamt folgt $e_1 = e_2$.

Def 1.3 Ein Gruppoid G heißt *kommutativ* oder *abelsch* (nach *N. H. Abel*, 1802–1829) : $\Longleftrightarrow$

$$x * y = y * x \quad \forall x, y \in G.$$

Beispiele: 1) $(\mathbb{N}, +)$ und $(\mathbb{R}, \cdot)$ sind kommutativ, $(\mathbb{Z}, -)$ ist nicht kommutativ, denn es ist beispielsweise $1 - 0 \neq 0 - 1$.

2)

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	b	b

ist nicht abelsch wegen $b * c \neq c * b$. (a ist neutrales Element.)

Bei endlichen Gruppoiden kann man die Kommutativität der Verknüpfung und die Existenz eines neutralen Elements an der Verknüpfungstafel erkennen:

- G ist abelsch $\iff$ Die Verknüpfungstafel ist symmetrisch bzgl. der Hauptdiagonalen (links oben nach rechts unten).
- x ist neutral $\iff$ Die Elemente in der zugehörigen Zeile und Spalte stimmen mit der Reihenfolge der Elemente am Rande der Verknüpfungstafel überein.

Für den Rest dieses Kapitels sei e stets das neutrale Element.

Def 1.4 Sei G ein Gruppoid mit neutralem Element e, sei $x \in G$.
$y \in G$ heißt *invers* zu x oder *inverses Element von* $x \quad :\iff \quad x \circ y = y \circ x = e$.

Auf Grund der Definition gilt: Wenn y invers zu x ist, ist x gleichzeitig invers zu y. Je nach der speziellen Verknüpfung schreibt man das inverse Element von x häufig $y = x^{-1}$ oder $y = -x$. Falls die Verknüpfung eines Elements x mit sich selbst das neutrale Element ergibt, falls also $x \circ x = e$ gilt, nennt man x *selbstinvers*.

Das neutrale Element e ist wegen $e * e = e$ stets *selbstinvers*.

Beispiele: 1) In $(\mathbb{Z}, +)$ ist $-z$ zu z invers: $z + (-z) = -z + z = 0$. Jedes Element hat genau ein Inverses, nur das neutrale Element 0 ist selbstinvers.

2) In $(\mathbb{R}, \cdot)$ mit neutralem Element 1 ist $a^{-1} = \frac{1}{a}$ zu $a \neq 0$ invers, 0 besitzt kein inverses Element. Mit 1 und -1 existieren zwei selbstinverse Elemente.

3) Im Gruppoid $(\mathbb{N}, \mathrm{kgV})$ besitzt nur das Einselement 1 ein inverses Element ($1^{-1} = 1$).

4) Analoges gilt für $(\mathrm{Pot}\,(M), \cup)$: $\emptyset^{-1} = \emptyset$, keine andere Teilmenge von M besitzt ein Inverses.

5) Aus der Verknüpfungstafel von Beispiel 2) (im Anschluss an Def 1.3) mit dem Einselement a erkennen wir: Wegen $b * c = a$ ist b „linksinvers“ zu c und c ist „rechtsinvers“ zu b. Da für alle Elemente x stets $x * b \neq a$ und $c * x \neq a$ ist, besitzen b und c trotzdem keine inversen Elemente.

Wir interessieren uns besonders für Gruppoide, bei denen die Verknüpfung das Assoziativgesetz erfüllt – wie es beispielsweise bei der Addition und Multiplikation von Zahlen oder bei der Verkettung von Abbildungen der Fall ist.

Def 1.5 Ein Gruppoid G heißt *Halbgruppe* $:\iff$ Die Verknüpfung $*$ ist assoziativ, d.h., es gilt
$x * (y * z) = (x * y) * z$ für alle $x, y, z \in G$.

In Halbgruppen kann man auf das Setzen von Klammern verzichten. Die n–fache Verknüpfung eines Elements mit sich selbst schreibt man $x * \cdots * x = x^n$ oder $x * \cdots * x = nx$, beispielsweise in $(\mathbb{N}, +)$
$5 + 5 + 5 = 3 \cdot 5$ oder in $(\mathbb{R}, \cdot) \quad \pi \cdot \pi \cdot \pi \cdot \pi = \pi^4$.

Beispiele: 1) $(\mathbb{N}, +)$, $(\mathbb{R}, \cdot)$, $(\mathrm{Pot}\,(M), \cup)$ sind Halbgruppen.

2) $(\mathbb{Z}, -)$ ist keine Halbgruppe, denn für $a \neq 0$ ist $a - (a - a) = a \neq (a - a) - a = -a$.

3)

$*$	a	b	c
a	c	b	a
b	b	c	a
c	a	a	c

Dieses Gruppoid ist keine Halbgruppe, denn $a * (a * b) \neq (a * a) * b$.
Ferner besitzt es kein neutrales Element, ist aber abelsch.

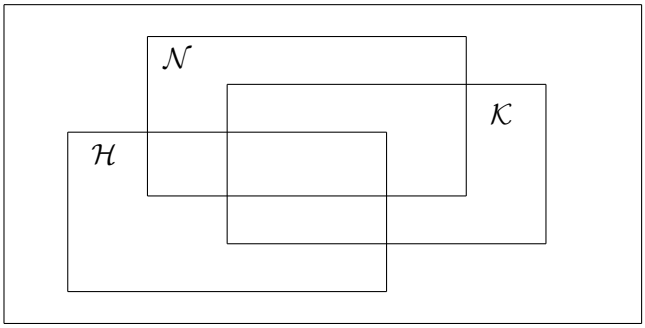
Frage: Ist $(\mathrm{Pot}\,(M), \oplus)$ eine Halbgruppe, $A \oplus B := (A \backslash B) \cup (B \backslash A) = (A \cup B) \backslash (A \cap B)$?

Satz 1.2 In einer Halbgruppe G mit neutralem Element hat jedes Element höchstens ein Inverses.

Beweis: Sei e das neutrale Element. Angenommen, a_1 und a_2 sind beide invers zu a.

$$\Rightarrow \qquad a_1 = a_1 \circ e = a_1 \circ (a \circ a_2) = (a_1 \circ a) \circ a_2 = e \circ a_2 = a_2$$

Zur Überprüfung unseres bisherigen Wissens über Gruppoide sehen wir uns ein Mengendiagramm an. Hierbei steht $\mathcal{N}$ für die Gruppoide mit neutralem Element, $\mathcal{H}$ für Halbgruppe und $\mathcal{K}$ für Kommutativität.



Frage: In welches der acht Teilgebiete der obigen Zeichnung gehören die folgenden Beispiele?

1) $(\mathbb{Z}, -)$ 2) $(\mathbb{N}, +)$ 3) $(\mathbb{Z}, +)$

4)

$*$	e	a	b
e	e	a	b
a	a	b	b
b	b	a	a

5)

$*$	e	a	b
e	e	a	b
a	a	b	a
b	b	a	a

6)

$*$	x	y	z
x	z	y	x
y	y	z	x
z	x	x	z

7) $(\mathrm{Abb}\,(\{a,b\},\{a,b\}), \circ)$ 8) $(\{f \in \mathrm{Abb}\,(\{a,b\},\{a,b\}) \mid f \text{ nicht bijektiv }\}, \circ)$

Die Halbgruppen mit neutralem Element, bei denen jedes Element genau ein Inverses besitzt, sind besonders interessant. Die folgende Definition steht im Einklang mit der Bemerkung zum Gruppenbegriff aus dem ersten Semester (Skript Seite 23).

Def 1.6 Eine Halbgruppe G heißt *Gruppe* : $\Longleftrightarrow$

(1) G besitzt ein neutrales Element e mit $a \circ e = e \circ a = a \quad \forall a \in G$

(2) Zu jedem $a \in G$ existiert ein Inverses a^{-1} mit $a \circ a^{-1} = a^{-1} \circ a = e$

Beispiel: $(\mathbb{Z}, +)$ ist eine Gruppe mit neutralem Element 0, zu z ist $-z$ invers.

Satz 1.3 In jeder Gruppe existiert genau ein neutrales Element. Zu jedem Element gibt es genau ein inverses Element.

Beweis: Die *eindeutige* Existenz des neutralen Elements wurde bereits in Satz 1.1 für beliebige Gruppoide bewiesen. Die *Existenz* des inversen Elements folgt direkt aus der Gruppendefinition, die *Eindeutigkeit* aus Satz 1.2; denn jede Gruppe ist insbesondere eine Halbgruppe mit neutralem Element.

Wir fassen zusammen: Ist eine Menge M mit einer Verknüpfung $\circ$ gegeben und wollen wir wissen, ob $(M, \circ)$ eine Gruppe ist, müssen wir überprüfen:

- Ist $M \neq \emptyset$? Dies ist fast immer trivial und wird häufig durch den Nachweis des neutralen Elements (siehe unten) erledigt, darf aber z.B. in Aufgaben nicht vergessen werden!
- Ist $\circ$ eine Verküpfung, d.h., ist $\circ$ auf M abgeschlossen?
- Ist die Verknüpfung assoziativ?
- Gibt es ein neutrales Element?
- Gibt es zu jedem Element ein Inverses?

Einige Gruppen sollte man kennen, wenn man in Prüfungen nicht unangenehm auffallen will:

1) Wichtige Beispiele für unendliche Gruppen sind $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$.

2) Für jede natürliche Zahl n ist $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$, versehen mit der Moduloaddition $+_n$ eine endliche kommutative Gruppe; für jede Primzahl p ist $(\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}, \cdot_p)$ ebenfalls eine endliche kommutative Gruppe.[2]

3) Alle bijektiven Abbildungen einer Menge $M \neq \emptyset$ auf sich bilden eine Gruppe mit der Verkettung $\circ$ als Verknüpfung. ($\circ$ ist assoziativ, *id* ist neutrales Element, zu f ist die Umkehrabbildung f^{-1} invers.)

Mindestens genau so wichtig ist es zu wissen, dass $(\mathbb{N}, +)$ und $(\mathbb{N}_0, +)$ *keine* Gruppen sind. Es gibt in $\mathbb{N}_0$ zwar ein neutrales Element, nämlich die Zahl 0, aber keine Zahl außer 0 besitzt ein inverses Element; auch $(\mathbb{Z}^*, \cdot)$ und $(\mathbb{Q}, \cdot)$ sind *keine* Gruppen (Begründung?)

Jede einelementige Menge $M = \{x\}$ wird durch $x \circ x := x$ zu einer Gruppe $(M, \circ)$. Gibt es auch für $M = \{a, b\}$ eine Verknüpfung $\circ$, so dass $(M, \circ)$ eine Gruppe ist? OBdA sei a das notwendige neutrale Element. In der zugehörigen Verknüpfungstafel sind damit alle Einträge bis auf $b \circ b$ vorgegeben:

$*$	a	b
a	a	b
b	b	?

Ferner muss b ein inverses Element besitzen: $\exists x \in \{a, b\} : b \circ x = x \circ b = a$. Dies bedeutet $b \circ b = a$. Die Verknüpfungstafel einer Gruppe mit den Elementen a und b kann nur so aussehen:

$\circ$	a	b
a	a	b
b	b	a

Gilt das Assoziativgesetz? Es sind acht Gleichungen zu untersuchen, hierbei kürzen wir ab jetzt $x \circ y$ usw. durch xy ab:

$$\begin{array}{llll} a(aa) = (aa)a & a(ab) = (aa)b & a(ba) = (ab)a & a(bb) = (ab)b \\ b(aa) = (ba)a & b(ab) = (ba)b & b(ba) = (bb)a & b(bb) = (bb)b \end{array}$$

[2] Einzelheiten zu den Verknüpfungen $+_n$ bzw. $\cdot_n$ finden Sie im Skript (erstes Semester, Seite 36).

Nach Erledigung dieser Fleißaufgabe wissen wir: $(M, \circ)$ ist eine Gruppe.

Analog fragen wir uns, ob es eine Gruppe mit drei Elementen gibt. Sei $M = \{a, b, c\}$, gesucht ist eine passende Verknüpfung. Wenn wir oBdA a als Einselement voraussetzen, haben wir folgende Verknüpfungstafel zu ergänzen:

$\circ$	a	b	c
a	a	b	c
b	b	?	?
c	c	?	?

Für die vier Fragezeichen kommen theoretisch $3 \cdot 3 \cdot 3 \cdot 3 = 81$ mögliche Kombinationen aus a, b und c in Frage. Wir werden gleich sehen, dass man diese Zahl durch allgemeingültige Aussagen wesentlich einschränken kann.

Satz 1.4 In jeder Gruppe G sind für alle Elemente $a, b \in G$ die Gleichungen $ax = b$ und $ya = b$ für jeweils genau ein x, y in G lösbar. (Beachte: mit ax ist $a \circ x$ gemeint).

Beweis: Wir zeigen die eindeutige Lösbarkeit von $ax = b$:

Sei a^{-1} das inverse Element zu a und e das Einselement von G. Dann gilt für $x := a^{-1}b \in G$:

$$ax = a(a^{-1}b) = (aa^{-1})b = eb = b$$

Damit ist die *Existenz* einer Lösung von $ax = b$ bewiesen.

Zur *Eindeutigkeit*: Sei v eine weitere Lösung, also $av = b$. Es folgt

$$x = a^{-1}b = a^{-1}(av) = (a^{-1}a)v = ev = v$$

Den Beweis zu $ya = b$ möge man zur Übung selbst durchführen.

Beispiel: Im Gruppoid $(\mathbb{R}, \circ)$ mit $x \circ y := x + y - xy$ ist die Gleichung $1 \circ x = 1$ (setze in Satz 4.1 $a = b = 1$) für jede reelle Zahl x erfüllt, daher kann $(\mathbb{R}, \circ)$ keine Gruppe sein.

Eine oft benutzte Folgerung aus dem letzten Satz ist die bereits von den Körpern bekannte *Kürzungsregel*:

Korollar In jeder Gruppe G gilt für alle $a, x_1, x_2, y_1, y_2 \in G$

$$\begin{aligned} ax_1 &= ax_2 \quad \Rightarrow \quad x_1 = x_2 \\ y_1a &= y_2a \quad \Rightarrow \quad y_1 = y_2 \end{aligned}$$

Für endliche Gruppen bedeutet Satz 1.4, dass in der Verknüpfungstafel einer Gruppe in jeder Zeile und in jeder Spalte jedes Element genau einmal vorkommen muss. Für unser Problem, ob es eine Gruppe mit drei Elementen gibt, bedeutet dies, dass es nicht 81 verschiedene, sondern nur eine mögliche Ergänzung für die vier Fragezeichen geben kann:

Wir untersuchen $bc =?$. Aus Satz 1.4 folgt $bc = a$; denn b kommt in der zugehörigen Zeile und c in der entsprechenden Spalte bereits vor. Aus den gleichen Gründen folgt nacheinander $bb = c$, $cb = a$, $cc = b$:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Fazit: Wenn es eine Gruppe mit den drei Elementen a, b, c gibt (a neutral), dann muss sie die vorliegende Verknüpfungstafel besitzen. Direkt können wir die Inversenbedingung ablesen: b und c sind zueinander invers. Nicht direkt erkennen können wir, ob das Assoziativgesetz gilt. Wir verzichten auf einen langwierigen und langweiligen Beweis und nehmen einfach zur Kenntnis, dass dieses Gesetz ebenfalls erfüllt ist und somit tatsächlich eine Gruppe vorliegt.

In Satz 1.4 haben wir bewiesen, dass in jeder Gruppe die eindeutige Lösbarkeit der Gleichungen $ax = b$ und $ya = b$ gelten muss. Die Umkehrung dieser Aussage ist falsch, dies haben Sie (hoffentlich) in den Übungen erfahren. Setzt man in einem Gruppoid allerdings die Gültigkeit des Assoziativgesetzes voraus, kann man aus der eindeutigen Lösbarkeit die restlichen Gruppeneigenschaften folgern. Wir formulieren dies als Satz, werden aber weder in der Vorlesung, noch in Prüfungen näher darauf eingehen.

Satz 1.5 Eine Halbgruppe ist eine Gruppe $\iff$ Die Gleichungen $ax = b$ und $ya = b$ sind in G lösbar für alle $a, b \in G$.

„$\Rightarrow$“ ist bereits durch Satz 1.4 bewiesen. Neu ist die andere Richtung „$\Leftarrow$“, die nur für Halbgruppen gilt. Für Interessenten folgt ein formaler Beweis dieser Tatsache:

Beweis: von „$\Leftarrow$“: Zu zeigen ist: Wenn in einer Halbgruppe $ax = b$ und $ya = b$ lösbar sind, dann gelten

(1) Es existiert ein Einselement e
(2) Zu jedem $a \in G$ existiert ein Inverses a^{-1}

Zu (1): Sei $g \in G$ beliebig. (Da G nach Voraussetzung Halbgruppe, ist $G \neq \emptyset$). Wegen der Lösbarkeit gibt es $e \in G$ mit $eg = g$. (Setze in $ya = b$ für a und b jeweils g ein und nenne die Lösung e.)

Beh: Dieses Element e ist das gesuchte neutrale Element.

Bew: Sei $a \in G$ beliebig. Wegen der Lösbarkeitsvoraussetzung gibt es zu g von oben ein $x \in G$ mit $gx = a$. Insgesamt folgt

$$ea = e(gx) = (eg)x = gx = a \qquad \forall a \in G,$$

analog zeigt man $ae = a$.

Zu (2): Da die Gleichungen $ya = e$ und $az = e$ für jedes $a \in G$ lösbar sind, ist y linksinvers und z rechtsinvers zu a. Wie im Beweis zu Satz 1.2 folgt $y = z$, damit ist y das gesuchte inverse Element a^{-1}.

Die nächste Aussage ist wieder von allgemeinem Interesse. Was weiß man in Gruppen über das inverse Element eines inversen Elements? Wie hängen die inversen Elemente von a, b und ab zusammen?

Satz 1.6 In jeder Gruppe G gilt

(1) $(a^{-1})^{-1} = a$ für jedes $a \in G$
(2) $(ab)^{-1} = b^{-1}a^{-1}$ für alle $a, b \in G$

Beweis: (1) Folgt direkt aus der Kürzungsregel: $a^{-1}a = e = a^{-1}(a^{-1})^{-1} \Rightarrow a = (a^{-1})^{-1}$

(2): Nach Definition ist $(ab)(ab)^{-1} = e$, ferner gilt $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$. Aus der Kürzungsregel folgt dann die Behauptung $(ab)^{-1} = b^{-1}a^{-1}$.

Korollar Für $a_1, a_2, \ldots, a_n \in G$ gilt $(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}$.

2 Weitere Beispiele für Gruppen

Wir haben im letzten Abschnitt Gruppen mit einem, zwei oder drei Elementen kennengelernt.

Def 2.1 Eine Gruppe G hat die *Ordnung* n, geschrieben $\operatorname{ord} G = n$ oder $|G| = n$, falls G aus n Elementen besteht.

Wenn eine Gruppe unendlich viele Elemente besitzt, schreiben wir $\operatorname{ord} G = \infty$ und sprechen von unendlicher Ordnung, wobei im Einzelfall zwischen abzählbar oder überabzählbar unterschieden werden sollte.

Beispiele: $(\mathbb{Z}, +)$ ist eine Gruppe unendlicher Ordnung, $(\operatorname{Pot}(M), \oplus)$ hat für $|M| = n$ die Ordnung 2^n.

Satz 2.1 Für jedes $n \in \mathbb{N}$ gibt es mit $(\mathbb{Z}_n, +_n)$ eine Gruppe der Ordnung n.

Beweisidee: Bekanntlich ist $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Weil $+_n$ (Addition modulo n) abgeschlossen und assoziativ ist, liegt eine Halbgruppe vor. Mit $0 \in \mathbb{Z}_n$ gibt es ein neutrales Element, zu $k \in \mathbb{Z}_n \backslash \{0\}$ ist $n - k \in \mathbb{Z}_n$ invers.

Untersuchen wir $(\mathbb{Z}_n, +_n)$ genauer, stellen wir fest, dass jedes Element als eventuell mehrfaches Verknüpfungsergebnis der 1 mit sich selbst geschrieben werden kann:

$$1 = 1, \quad 2 = 1 +_n 1, \quad \ldots \quad n-1 = 1 +_n \ldots +_n 1 \ (n-1 \,\text{mal}), \quad 0 = 1 +_n \ldots +_n 1 \ (n \,\text{mal})$$

Kürzen wir die k–fache modulo–n–Addition durch $k \cdot 1$ ab und beachten, dass in diesem Sinn $n \cdot 1 = 0 = 0 \cdot 1$ gilt, ist

$$\mathbb{Z}_n = \{k \cdot 1 \mid k = 0, \ldots, n-1\} \ = \ \{k \cdot 1 \mid k = 1, \ldots, n\}$$

Man sagt, *das Element* 1 *erzeugt die Gruppe* $\mathbb{Z}_n$.

Allgemein kürzt man in Gruppen die k–fache Verknüpfung eines Elements g mit sich selbst je nach Schreibweise der Verknüpfung durch $k \cdot g = kg$ oder g^k ab. Bei multiplikativer Schreibweise ist $g^0 = e$ (für jedes Element g) das neutrale Element.

Frage: Was ist g^{-k} für $k \in \mathbb{N}$? *Antwort*: $g^{-k} = g^{(-1)k} = g^{-1} \ldots g^{-1} = (g \ldots g)^{-1} = (g^k)^{-1}$.

Def 2.2 Eine Teilmenge $S \subseteq G$ heißt *Erzeugendensystem von* G, wenn jedes Element von G als Verknüpfung von endlich vielen Elementen, die entweder selbst oder deren Inverse in S liegen, geschrieben werden kann.

Jede Gruppe mit mehr als einem Element besitzt unterschiedliche Erzeugendensysteme. Als sparsame Menschen interessieren wir uns für Erzeugendensysteme mit möglichst wenig Elementen.

Beispiele: 1) In der Gruppe $(\mathbb{Z}_n, +_n)$ ist $S = \{1\}$ für jedes $n \in \mathbb{N}$ ein Erzeugendensystem, gleiches gilt für $(\mathbb{Z}, +)$.

2) In $(\mathbb{Z}_3, +_3)$ ist neben $\{1\}$ auch $\{2\}$ ein minimales Erzeugendensystem: $2 +_3 2 = 1, \ 2 +_3 2 +_3 2 = 0$.

3) *Fragen*: Warum ist $\{2\}$ kein Erzeugendensystem von $(\mathbb{Z}_4, +_4)$? Ist $\{3\}$ ein Erzeugendensystem von $(\mathbb{Z}_4, +_4)$?

4) In der Gruppe $\mathbb{Z} \times \mathbb{Z}$ mit komponentenweiser Addition gilt $S = \{(0,1), (1,0)\}$. *Fragen*: Warum ist $\{(1,1)\}$ kein Erzeugendensystem? Warum gibt es in dieser Gruppe kein einelementiges Erzeugendensystem?

5) $(\mathbb{R}, +)$ besitzt kein endliches Erzeugendensystem.

Def 2.3 Eine Gruppe G mit einem einelementigen Erzeugendensystem heißt *zyklisch*.

Beispielsweise ist $(\mathbb{Z}_5, +_5)$ eine zyklische Gruppe der Ordnung 5, $(\mathbb{Z}, +)$ ist eine unendliche zyklische Gruppe. $\mathbb{Z} \times \mathbb{Z}$ mit komponentenweiser Addition und $(\mathbb{R}, +)$ sind nicht zyklisch.

Satz 2.2 Jede zyklische Gruppe ist abelsch.[3]

Der einfache Beweis dieses Satzes wird in den Übungen erledigt.

Frage: Gilt auch die Umkehrung von Satz 2.2?

Man kann zeigen, dass jede Gruppe von Primzahlordnung zyklisch sein muss. Für Gruppen anderer Ordnung gilt dies nicht. Hierzu sehen wir uns ein Quadrat mit den Eckpunkten A, B, C, D und Mittelpunkt (=Schwerpunkt) M an. Es gibt vier Drehungen um M, die das Quadrat auf sich abbilden. Die Menge der Drehungen sei

$$\text{Dreh}\,(\square) = \{id = \delta_0, \delta_1, \delta_2, \delta_3\}$$

mit Drehwinkel $i \cdot \frac{\pi}{2}$ für $\delta_i,\ i = 0, 1, 2, 3$. Mit der Verkettung als Verknüpfung erhalten wir für diese Drehungen folgende Verknüpfungstafel:

$\circ$	id	δ_1	δ_2	δ_3
id	id	δ_1	δ_2	δ_3
δ_1	δ_1	δ_2	δ_3	id
δ_2	δ_2	δ_3	id	δ_1
δ_3	δ_3	id	δ_1	δ_2

Wir untersuchen weitere Abbildungen, die das Quadrat auf sich abbilden. $\text{Spg}\,(\square) := \{id, s_1, s_2, \delta_2\}$ enthält außer der Drehung δ_2 (siehe oben) die Geradenspiegelungen (Spiegelachse jeweils durch gegenüberliegende Seitenmitten des Quadrats) $s_1 : \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$ und $s_2 : \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$. Die Drehung δ_2 können wir übrigens auch als Punktspiegelung an M auffassen. Wir geben die Verknüpfungstafel für $(\text{Spg}\,(\square), \circ)$ an:

$\circ$	id	s_1	s_2	δ_2
id	id	s_1	s_2	δ_2
s_1	s_1	id	δ_2	s_2
s_2	s_2	δ_2	id	s_1
δ_2	δ_2	s_2	s_1	id

Man kann den Verknüpfungstafeln leicht entnehmen, dass es sich in beiden Fällen um Gruppen handelt[4]. Die Drehgruppe ist zyklisch, da δ_1 oder δ_3 die Gruppe erzeugen. Die Spiegelungsgruppe ist nicht zyklisch: Weil hier jedes Element selbstinvers ist, kann es kein Erzeugendensystem mit nur einem Element geben.

Es gibt bei einem Quadrat zwei weitere Geradenspiegelungen, die wir bisher nicht berücksichtigt haben, nämlich $s_3 : \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}$ und $s_4 : \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}$ mit Achsen durch diagonal gegenüberliegende Punkte. Insgesamt existieren vier Drehungen (inklusive der Identität) und vier Spiegelungen, die das Quadrat auf sich abbilden.

[3] Anders ausgedrückt: G zyklisch $\Rightarrow$ G abelsch.

[4] Beachte: die Verkettung von Abbildungen ist nach Satz I.4.2 assoziativ.

Dies kann man auf beliebige regelmäßige n–Ecke übertragen: Jedes n–Eck besitzt n solcher Drehungen (inklusive der Identität) und n Geradenspiegelungen. Drehungen hintereinander ausgeführt ergeben wieder eine Drehung (man addiere die Drehwinkel modulo 360°), zwei Spiegelungen ergeben ebenfalls eine Drehung. Verknüpft man Drehung und Spiegelung (egal in welcher Reihenfolge), erhält man (von der Reihenfolge abhängig unterschiedliche) Spiegelungen. Insgesamt gilt

Def 2.4 und **Satz 2.3** Die Menge aller Drehungen und Spiegelungen eines regelmäßigen n–Ecks auf sich bildet mit der Verkettung die sogenannte *Diedergruppe*[5] D_n . Die Diedergruppe hat die Ordnung $2n$ und ist für $n \geq 3$ nicht kommutativ, ein Erzeugendensystem besteht aus einer Drehung (beispielsweise δ_1) und einer Spiegelung.

Wenn wir die Ecken eines regelmäßigen n–Ecks mit den Zahlen $1, 2, \ldots, n$ bezeichen, erkennen wir, dass jede Abbildung der Diedergruppe als Permutation der Eckenmenge $\{1, 2, \ldots, n\}$ aufgefasst werden kann. Ab $n \geq 4$ gibt es aber Permutationen, die weder als Drehungen, noch als Spiegelungen an einer Geraden gedeutet werden können. Für *alle* Permutationen einer n–elementigen Menge gilt

Def 2.5 und **Satz 2.4** Die Menge aller Permutationen einer n–elementigen Menge bildet mit der Verkettung die sogenannte *symmetrische Gruppe vom Index n*, geschrieben S_n. Die symmetrische Gruppe hat die Ordnung $n!$ und ist für $n \geq 3$ nicht kommutativ.

Beispiele: 1) $S_1 = \{f : \{1\} \to \{1\} \text{ bijektiv } \} = \{id\}$

2) $S_2 = \{f : \{1,2\} \to \{1,2\} \text{ bijektiv } \} = \left\{id, \begin{pmatrix} 1\,2 \\ 2\,1 \end{pmatrix}\right\}$.

3) $S_3 = \left\{\begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}\right\}$.

Bei der Angabe der Abbildungen haben wir jeweils Urbild und zugehöriges Bild untereinander geschrieben. Mit der sogenannten *Zykelschreibweise* kennt der Mathematiker für Permutationen eine wesentlich elegantere und gleichzeitig kürzere Schreibweise. Im Fall S_3 lautet sie

$$S_3 = \{id = (1), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)\} .$$

Frage: Wer hat das Prinzip der Zykelschreibweise erkannt?

Später werden wir es intensiv mit folgenden Gruppen zu tun bekommen:

Satz 2.5 Sei $n \in \mathbb{N}$. Dann ist $(\mathbb{R}^n, +)$ mit $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$ eine abelsche, nicht zyklische Gruppe.

Der einfache Beweis erfordert nur wenig geistige Anstrengung, ist aber bei exakter Ausführung etwas länglich und sei als Übung empfohlen.

[5] Getrennt gesprochen Di – eder..., nicht mit langem i. Falsche Aussprache in mündlichen Prüfungen kommt in der Regel nicht gut an!

3 Untergruppen

Betrachten wir noch einmal die Diedergruppe D_n. Beschränken wir uns auf die Teilmenge aller Drehungen, erkennen wir, dass diese bezüglich der Verkettung ebenfalls eine Gruppe bildet – anders als die Teilmenge aller Spiegelungen.

Def 3.1 Sei $(G, *)$ eine Gruppe. $U \subset G$ heißt *Untergruppe von* $G \iff (U, *)$ ist Gruppe.

In Untergruppe und Gruppe müssen die gleichen Verknüpfungsvorschriften gelten, *beispielsweise* ist $(\mathbb{Z}_2, +_2)$ *keine* Untergruppe von $(\mathbb{Z}, +)$ oder von $(\mathbb{Z}_4, +_4)$.

Beispiele: 1) Jede Gruppe G besitzt die *trivialen* Untergruppen G und $\{e\}$, wobei mit e natürlich das neutrale Element von G gemeint ist.

2) Jede Gruppe der Ordnung 2 oder 3 besitzt nur triviale Untergruppen.

3) $G = S_3$ besitzt außer $\{id\}$ und S_3 die nichttrivialen Untergruppen $\{id, (12)\}$, $\{id, (13)\}$, $\{id, (23)\}$ und $\{id, (123), (132)\}$, alle anderen Teilmengen sind keine Untergruppen.

4) $(\{1, -1\}, \cdot)$ und $(\mathbb{Q}^*, \cdot)$ sind zwei der vielen Untergruppen von $(\mathbb{R}^*, \cdot)$.

Frage: Welche Untergruppen besitzt $(\mathbb{Z}, +)$?

Ob eine Teilmenge einer Gruppe selbst eine Gruppe ist, kann man natürlich durch Überprüfung der Gruppenaxiome feststellen. Zum Glück geht es aber auch einfacher:

Satz 3.1 Für $\emptyset \neq U \subset G$ gelte $ab^{-1} \in U \ \ \forall a, b \in U$. Dann ist U eine Untergruppe.

Beweis: Zu zeigen sind nach Def. 1.6:

1. U ist ein Gruppoid, d.h., die Verknüpfung ist abgeschlossen: Wird am Ende des Beweises erledigt.

2. Die Verknüpfung ist assoziativ: Dies ist klar, da U Teilmenge einer Gruppe ist.

3. U besitzt ein neutrales Element: Da $U \neq \emptyset \Rightarrow \exists\, a \in U$. Nach Voraussetzung ist dann (mit $b = a$) $aa^{-1} = e \in U$.

4. Zu jedem $u \in U$ ist auch $u^{-1} \in U$: Sei $u \in U$. Zusammen mit $e \in U$ folgt $eu^{-1} = u^{-1} \in U$.

Jetzt zu 1., wir zeigen die Abgeschlossenheit der Verknüpfung auf U: Seien $a, b \in U$. Mit b ist wie in 4. gezeigt auch $b^{-1} \in U$ und es folgt $a(b^{-1})^{-1} = ab \in U$.

An Stelle von $ab^{-1} \in U$ kann man auch $a^{-1}b \in U$ überprüfen, in endlichen Gruppen reicht sogar der Nachweis von $ab \in U$.

Beispiel: $G = (\mathbb{Z}, +)$, $U := \{5 \cdot z \mid z \in \mathbb{Z}\}$ ist Untergruppe von G:

Wegen $0 = 5 \cdot 0 \in U$ ist $U \neq \emptyset$, mit $a = 5 \cdot z_1 \in U$ und $b = 5 \cdot z_2 \in U$ ist auch $a + (-b) = 5z_1 + (-5z_2) = 5(z_1 - z_2) \in U$.

Für jede natürliche Zahl n ist somit $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$ (bezüglich der Addition), abgekürzt geschrieben $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.[6]

[6] Das Zeichen $\leq$ kann ab jetzt in zwei verschiedenen Bedeutungen vorkommen, einerseits als die bekannte Kleiner–gleich–Beziehung zwischen Zahlen, zum anderen als Abkürzung für ist–Untergruppe–von. In beiden Fällen handelt es sich übrigens um eine Ordnungsrelation!

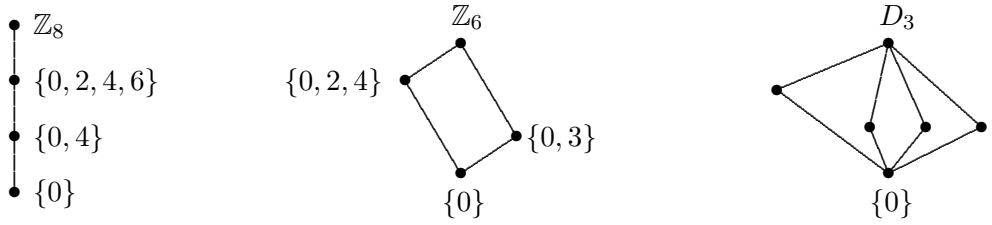
Beispiele: 1) $(8\mathbb{Z},+) \leq (4\mathbb{Z},+) \leq (2\mathbb{Z},+) \leq (\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$.

2) $(\{0\},+_8) \leq (\{0,4\},+_8) \leq (\{0,2,4,6\},+_8) \leq (\mathbb{Z}_8,+_8)$.

3) $(\{0,3\},+_6) \leq (\mathbb{Z}_6,+_6)$, $(\{0,2,4\},+_6) \leq (\mathbb{Z}_6,+_6)$, aber $(\{0,3\},+_6)$ ist keine Untergruppe von $(\{0,2,4\},+_6)$ (oder umgekehrt).

Interessiert man sich für *alle* Untergruppen einer Gruppe und deren Abhängigkeiten untereinander, bietet sich eine zeichnerische Darstellung als *Untergruppenverband* an. Hierbei wird jede der beteiligten Gruppen durch einen dicken Punkt dargestellt. Untergruppe und zugehörige „Obergruppe“ werden durch eine Linie verbunden, wobei die Untergruppe zu dem in der Zeichnung tiefer liegenden Punkt gehört. Existiert nun ein Kantenzug von einem unteren zu einem oberen Punkt, wobei jede der beteiligten Teilstrecken die gleiche Richtung von unten nach oben haben muss, ist die untere Gruppe eine Untergruppe der oberen.

Beispiel: Die Untergruppenverbände von $(\mathbb{Z}_8,+_8)$ (links), $(\mathbb{Z}_6,+_6)$ (Mitte), $(D_3,\circ)$ (rechts, wird in der Vorlesung weiter beschriftet):



in der mittleren Skizze gilt beispielsweise $\{0\} \leq \mathbb{Z}_6$ (es gibt zwei entsprechende Kantenzüge), aber $\{0,3\}$ ist keine Untergruppe von $\{0,2,4\}$.

Frage: Wie sieht der Untergruppenverband von D_4 aus? (Hinweis: Es gibt fünf Untergruppen der Ordnung 2 und drei der Ordnung 4).

Steigt man etwas tiefer in die Gruppentheorie ein, kann man beweisen, dass bei endlichen Gruppen die Ordnung einer Untergruppe immer ein Teiler der Gruppenordnung sein muss. Das heißt aber nicht, dass es immer zu jedem Teiler der Gruppenordnung eine Untergruppe mit dieser Ordnung gibt.

Beispiele: 1) $\mathbb{Z}_{12}$ hat keine echte Untergruppe mit mehr als sechs Elementen.

2) $(\mathbb{Z}_{11},+_{11})$ besitzt nur triviale Untergruppen, da 11 eine Primzahl ist.

4 Isomorphie

Wir wollen die bekannten Gruppentafeln von $(\mathrm{Dreh}\,(\square),\circ)$, $(\mathrm{Spg}\,(\square),\circ)$ und $(\mathbb{Z}_4,+_4)$ vergleichen und uns die Frage stellen, wie „verschieden“ die zugehörigen Gruppen sind:

$\circ$	id	δ_1	δ_2	δ_3
id	id	δ_1	δ_2	δ_3
δ_1	δ_1	δ_2	δ_3	id
δ_2	δ_2	δ_3	id	δ_1
δ_3	δ_3	id	δ_1	δ_2

$\circ$	id	s_1	s_2	δ_2
id	id	s_1	s_2	δ_2
s_1	s_1	id	δ_2	s_2
s_2	s_2	δ_2	id	s_1
δ_2	δ_2	s_2	s_1	id

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Wir stellen fest: Durch Umbenennung ($id \mapsto 0$, $\delta_1 \mapsto 1$, $\delta_2 \mapsto 2$, $\delta_3 \mapsto 3$) geht $\mathrm{Dreh}\,(\square)$ in $\mathbb{Z}_4$ über, eine analoge einfache Übertragung von oder nach $\mathrm{Spg}\,(\square)$ ist nicht möglich.

Def 4.1 Eine Gruppe $(G, \circ)$ heißt *isomorph zu* einer Gruppe $(H, *)$, geschrieben $(G, \circ) \simeq (H, *)$ oder $G \simeq H :\Longleftrightarrow$

$$\exists f : G \to H \text{ bijektiv und strukturerhaltend, d.h., } f(x \circ y) = f(x) * f(y) \text{ für alle } x, y \in G \, .$$

Die zugehörige Abbildung $f : G \to H$ heißt *Isomorphismus* von G nach H.

Beispiel: $(\mathrm{Dreh}\,(\square), \circ) \simeq (\mathbb{Z}_4, +_4) \not\simeq (\mathrm{Spg}\,(\square), \circ)$

Ist $(G, \circ)$ zu $(H, *)$ isomorph, dann auch umgekehrt $(H, *)$ zu $(G, \circ)$ (eventuell Übung), daher kann man sagen: $(G, \circ)$ und $(H, *)$ sind *zueinander isomorph*. Die Relation „isomorph zu“ ist symmetrisch. Es gilt sogar

Satz 4.1 Die Isomorphie–Relation für Gruppoide ist eine Äquivalenzrelation.

Beweis: Wir haben Reflexivität (r), Symmetrie (s) und Transitivität (t) zu zeigen.

zu (r): *Beh*: Für jedes Gruppoid gilt $(G, \circ) \simeq (G, \circ)$.

Bew: Die Identität $id : G \to G$ ist die gesuchte strukturerhaltende Bijektion: $id(x \circ y) = x \circ y = id(x) \circ id(y)$ für alle $x, y \in G$.

zu (s): Eventuell Übung.

zu (t): Sei $(G, \star) \simeq (H, *)$ und $(H, *) \simeq (K, \times)$, zu zeigen ist $(G, \star) \simeq (K, \times)$. Auf Grund der Voraussetzungen gibt es strukturerhaltende Bijektionen $f : G \to H$ und $g : H \to K$ mit

$$f(a \star b) = f(a) * f(b) \quad \forall a, b \in G \qquad \text{und} \qquad g(x * y) = g(x) \times g(y) \quad \forall x, y \in H \, .$$

Dann ist $g \circ f : G \to K$ nach Satz I.4.3 bijektiv mit

$$\begin{aligned} (g \circ f)(a \star b) &= g(f(a \star b)) = g(f(a) * f(b)) \\ &= g(f(a)) \times g(f(b)) = (g \circ f)(a) \times (g \circ f)(b) \quad \forall a, b \in G \, . \end{aligned}$$

Warum interessiert man sich für Isomorphismen? Isomorphe Gruppen unterscheiden sich im Wesentlichen nur durch unterschiedliche Bezeichnungen, in allen interessanten Eigenschaften stimmen sie überein. Kann man beispielsweise feststellen, dass eine unbekannte Gruppe G isomorph zur Gruppe $(\mathbb{Z}_n, +_n)$ ist, so gelten alle Sätze über zyklische Gruppen der Ordnung n auch für G.

Beispiel: Wir vergleichen $(\mathbb{Q}\backslash\{1\}, *)$, $\quad x * y := xy - x - y + 2$, mit der bekannten Gruppe $(\mathbb{Q}^*, \cdot)$. Die Abbildung $f : \mathbb{Q}\backslash\{1\} \to \mathbb{Q}^*$, $f(x) := x - 1$, ist bijektiv (beachte: für jedes $x \in \mathbb{Q}\backslash\{1\}$ ist $f(x) \neq 0$). Bezüglich der üblichen Multiplikation in $\mathbb{Q}^*$ liegt Strukturerhaltung vor; denn für alle $x, y \in \mathbb{Q}\backslash\{1\}$ gilt

$$f(x * y) = x * y - 1 = (xy - x - y + 2) - 1 = x(y - 1) - (y - 1) = (x - 1)(y - 1) = f(x) \cdot f(y)$$

Damit sind $(\mathbb{Q}\backslash\{1\}, *)$ und $(\mathbb{Q}^*, \cdot)$ zueinander isomorphe Gruppen. Übrigens ist auch die Umkehrabbildung $g = f^{-1} : \mathbb{Q}^* \to \mathbb{Q}\backslash\{1\}$, $\quad g(x) := x + 1$, ein Isomorphismus. (Als Übung bitte überprüfen).

Wie wir gleich sehen werden, können wir jetzt ohne große Mühe neutrales Element und selbstinverse Elemente der Gruppe $(\mathbb{Q}\backslash\{1\}, *)$ angeben. Es gilt nämlich

Satz 4.2 Sei f ein Isomorphismus von der Gruppe $(G, \circ)$ mit neutralem Element e_G auf die Gruppe $(H, *)$ mit neutralem Element e_H. Dann ist $f(e_G) = e_H$.

Beweis: $e_H * f(e_G) = f(e_G) = f(e_G \circ e_G) = f(e_G) * f(e_G)$, die Behauptung folgt aus der Kürzungsregel.

Korollar Isomorphe Gruppen haben die gleiche Anzahl an selbstinversen Elementen.

Beweis: x selbstinvers $\Rightarrow f(x)^2 = f(x^2) = f(e_G) = e_H \Rightarrow f(x)$ selbstinvers, der Rest folgt aus der Symmetrie der Isomorphie.

Für zueinander inverse Elemente x, x^{-1} gilt entsprechend

$$e_H = f(e_G) = f(x \circ x^{-1}) = f(x) * f(x^{-1}) \quad \Rightarrow \quad (f(x))^{-1} = f(x^{-1})$$

Beispiele: 1) (Fortsetzung) $(\mathbb{Q}\backslash\{1\}, *)$ hat wegen $g(1) = 2$ das neutrale Element 2. Weil in $(\mathbb{Q}^*, \cdot)$ außer dem neutralen Element 1 auch -1 selbstinvers ist, besitzt $(\mathbb{Q}\backslash\{1\}, *)$ ebenfalls zwei selbstinverse Elemente, nämlich 2 und 0 (wegen $g(-1) = 0$).

Wir suchen in $\mathbb{Q}\backslash\{1\}$ das inverse Element von 12: Wegen $f(12) = 11$ und $11^{-1} = \frac{1}{11}$ (in der Gruppe $(\mathbb{Q}^*, \cdot)$) ist das gesuchte Element $g\left(\frac{1}{11}\right) = \frac{1}{11} + 1 = \frac{12}{11}$.

(Berechnen Sie zur Übung $12 * \frac{12}{11}$. Überlegen Sie vor Beginn der Rechnung, wie das Ergebnis lauten muss!)

2) Die Nichtisomorphie der Gruppen $(\mathbb{Z}_4, +_4)$ und $(\mathrm{Spg}(\square), \circ)$ liegt jetzt auf der Hand: Im Gegensatz zu den Elementen von $\mathbb{Z}_4$ ist jede Spiegelung selbstinvers. Die beiden Gruppen besitzen eine unterschiedliche Anzahl an selbstinversen Elementen, sie können daher zueinander nicht isomorph sein.

Die Spiegelungsgruppe $(\mathrm{Spg}(\square), \circ)$ ist isomorph zur sogenannten *Kleinschen Vierergruppe* V_4 (benannt nach *F. Klein*, 1849–1925) mit der Gruppentafel

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Wir merken uns: Bis auf Isomorphie gibt es

- jeweils genau eine Gruppe der Ordnung 1, 2, 3, 5. (Dies gilt für jede Primzahl).
- genau zwei Gruppen der Ordnung 4: Jede Gruppe der Ordnung 4 ist entweder zu $\mathbb{Z}_4$ oder zu V_4 isomorph.
- genau zwei Gruppen der Ordnung 6: Jede abelsche Gruppe der Ordnung 6 ist zu $\mathbb{Z}_6$, jede nicht abelsche zu S_3 isomorph. Es gilt $D_3 \simeq S_3$.
- genau eine unendliche zyklische Gruppe, nämlich $\mathbb{Z}$. Unendliche Gruppen, die zu $\mathbb{Z}$ nicht isomorph sind, sind nicht zyklisch.

Bei größeren Gruppen kann es bezüglich der (Nicht)isomorphie kompliziert zugehen, beispielsweise gibt es bereits 14 nichtisomorphe Gruppen der Ordnung 16.

Außer Isomorphismen gibt weitere Morphismen, denn leider ist nicht jede Bijektion zwischen Gruppen strukturerhaltend und nicht jede strukturerhaltende Abbildung bijektiv. *Homomorphismus* ist ein anderer Name für Strukturerhaltung (ohne Bijektivitätsvoraussetzung). Einen Homomorphismus einer Gruppe *in sich* nennt man *Endomorphismus* . Interessant sind Isomorphismen einer Gruppe *auf sich*, sie nennt man *Automorphismen*. Alle Automorphismen einer Gruppe G bilden mit der Verkettung selbst eine Gruppe, die sogenannte *Automorphismengruppe* $\operatorname{Aut} G$. So ähnlich wie ein Arzt Krankheiten an Hand ihrer Symptome erkennen kann, verrät die Automorphismengruppe $\operatorname{Aut} G$ einem Mathematiker viele Einzelheiten über die zugehörige Gruppe G.

Beispiel: Gesucht ist $\operatorname{Aut} \mathbb{Z}_4$. Weil das neutrale Element unter jedem Automorphismus f auf sich abgebildet wird und $f(2) = 2$ gelten muss (2 ist außer dem neutralen Element das einzige selbstinverse Element der Gruppe $\mathbb{Z}_4$), kann es nur zwei Kandidaten für einen Automorphismus geben, nämlich die identische Abbildung und (1 3) (Zykelschreibweise).

Nachrechnen ergibt, dass beide Abbildungen strukturerhaltend sind. Da es bis auf Isomorphie nur eine Gruppe mit zwei Elementen gibt, ist $(\operatorname{Aut} \mathbb{Z}_4, \circ) \simeq (\mathbb{Z}_2, +_2)$.

Frage: Zu welcher Ihnen bekannten Gruppe ist $\operatorname{Aut} V_4$ isomorph?

Wir beenden den Abschnitt mit zwei Fragen, die auch schon in Prüfungen gestellt wurden.

Fragen: 1) Ist $(\mathbb{Q}, +) \simeq (\mathbb{Q}^*, \cdot)$? 2) Ist $(\mathbb{Q}, +) \simeq (\mathbb{R}, +)$?

Antworten: Jeweils nein; die Anzahl der Selbstinversen ist unterschiedlich bzw. es gibt keine Bijektion zwischen den jeweiligen Mengen. Aber welche Begründung hilft bei der Beantwortung welcher Frage?