1. Gruppen

Def.: Es sei $G (\neq \emptyset)$ eine Menge und $\circ : G \times G \to G$ eine Verknüpfung (d.h. eine Abbildung $\circ : G \times G \to G, (a,b) \mapsto a \circ b$). Wenn

1) $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a,b,c \in G$ (Assoziativität)

2) $\exists e \in G \; \forall a \in G : e \circ a = a \circ e = a$ (neutrales Element)

3) $\forall a \in G \; \exists x \in G : a \circ x = x \circ a = e$ (inverses Element)

erfüllt sind, so wird $(G, \circ)$ als Gruppe bezeichnet. Gilt zusätzlich

4) $a \circ b = b \circ a \quad \forall a,b \in G$ (Kommutativität),

so wird $(G, \circ)$ eine abelsche (oder kommutative) Gruppe genannt.

Satz 1 Es sei $(G, \circ)$ eine Gruppe

(i) Das neutrale Element von G ist eindeutig bestimmt,

(ii) Das inverse Element jedes Elements $a \in G$ ist eindeutig bestimmt

Beweis: (i) Angenommen, $e, f \in G$ sind beides neutrale Elemente (d.h. $e \circ a = a \circ e = a \quad \forall a \in G$ und $f \circ a = a \circ f = a \quad \forall a \in G$). Dann $e = e \circ f = f$.

(ii) Angenommen, $x, y \in G$ sind beides inverse Elemente für $a \in G$ (d.h. $a \circ x = x \circ a = e$ und $a \circ y = y \circ a = e$). Dann

$$x = x \circ e = x \circ (a \circ y) = (x \circ a) \circ y = e \circ y = y.$$

Bemerkungen: 1) Wegen der Eindeutigkeit des inversen Elements von a, ist es sinnvoll, dafür a^{-1} zu schreiben. Bedingung 3) oben kann daher auch

3) $\forall a \in G \; \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$

geschrieben werden.

2) Zusätzlich zu den Bedingungen 1) – 3) (bzw. 4)) muss man auch überprüfen, dass $a \circ b \in G \quad \forall a,b \in G$ gilt (Abgeschlossenheit). Diese Bedingung ist in der Def. in der Voraussetzung enthalten, dass $\circ : G \times G \to G$ eine Verknüpfung ist.

3) Die Verknüpfung $\circ$ wird oft als Punkt oder gar nicht geschrieben, d.h. man schreibt statt $a \circ b$ nur $a \cdot b$ oder ab.

4) Ist klar, welche Verknüpfung gemeint ist, wird sie oft weggelassen. D.h. man spricht nur von der Gruppe G statt von $(G, \circ)$.

5) Bei vielen abelschen Gruppen wird die Verknüpfung + geschrieben. Das neutrale Element wird dann meistens mit 0 (Null) und das inverse Element zu a mit $-a$ bezeichnet. Die Gruppenaxiome für die abelsche Gruppe $(G,+)$ sind dann

0) $a+b \in G \quad \forall a,b \in G$ (Abgeschlossenheit)

1) $(a+b)+c = a+(b+c) \quad \forall a,b,c \in G$ (Assoziativität)

2) $\exists 0 \in G \ \forall a \in G: 0+a = a+0 = a$ (neutrales Element)

3) $\forall a \in G \ \exists -a \in G: a+(-a) = (-a)+a = 0$ (inverses Element)

4) $a+b = b+a \quad \forall a,b \in G$

6) Ist $(G,\circ)$ eine endliche Gruppe, d.h. $G=\{a_1,\dots,a_n\}$, so kann die Verknüpfung $\circ$ durch eine Verknüpfungstafel gegeben werden, d.h.

$(G,\circ)$	a_1	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1\circ a_1$	$\cdots$	$a_1\circ a_j$	$\cdots$	$a_1\circ a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	$a_i\circ a_1$	$\cdots$	$a_i\circ a_j$	$\cdots$	$a_i\circ a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	$a_n\circ a_1$	$\cdots$	$a_n\circ a_j$	$\cdots$	$a_n\circ a_n$

An der Verknüpfungstafel kann man viele Eigenschaften der Gruppe (wie neutrales Element und inverse Elemente) ablesen. Die Gruppe ist genau dann abelsch wenn sie bezüglich der Diagonale symmetrisch ist.

4.3.2024

Bsp.: 1) $(\mathbb{Z},+)$ ist eine abelsche Gruppe mit neutralem Element 0, inverses Element zu $a\in\mathbb{Z}$ ist $-a$.

2) Versieht man die Menge $G=\{1,-1\}$ mit der üblichen Multiplikation, d.h.

$\cdot$	1	-1
1	1	-1
-1	-1	1

so ist $(G,\cdot)$ eine abelsche Gruppe mit neutralem Element 1 und $(\pm 1)^{-1} = \pm 1$.

3) $(\mathbb{Q},+)$, $(\mathbb{R},+)$ und $(\mathbb{C},+)$ sind abelsche Gruppen, wieder mit neutralem Element 0 und inversem Element $-a$ zu a. (Allgemeiner gilt: Ist $(K,+,\cdot)$ ein Körper, so ist (nach Definition eines Körpers) $(K,+)$ eine abelsche Gruppe mit neutralem Element 0 und inversem Element $-a$ zu $a\in K$.)

4) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ und $(\mathbb{C}^*, \cdot)$ sind abelsche Gruppen. (Dabei bezeichnet $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ und $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.) Neutrales Element ist 1 und inverses Element von a ist $a^{-1} = \frac{1}{a}$. (Allgemein gilt: Ist $(K, +, \cdot)$ ein Körper, so ist (nach Definition eines Körpers) $(K^*, \cdot)$ eine abelsche Gruppe (wobei $K^* = K \setminus \{0\}$) mit neutralem Element 1 und inversem Element $a^{-1} = \frac{1}{a}$ zu $a \in K^*$.)

Satz 2 Versieht man $\mathbb{R}^2 = \left\{ \binom{x}{y} \middle| x, y \in \mathbb{R} \right\}$ mit der komponentenweisen Addition $\binom{x_1}{y_1} + \binom{x_2}{y_2} := \binom{x_1 + x_2}{y_1 + y_2}$, so ist $(\mathbb{R}^2, +)$ eine abelsche Gruppe.

Beweis: $\left(\binom{x_1}{y_1} + \binom{x_2}{y_2}\right) + \binom{x_3}{y_3} = \binom{(x_1+x_2)+x_3}{(y_1+y_2)+y_3} = \binom{x_1+(x_2+x_3)}{y_1+(y_2+y_3)} = \binom{x_1}{y_1} + \left(\binom{x_2}{y_2} + \binom{x_3}{y_3}\right) \quad \forall \binom{x_1}{y_1}, \binom{x_2}{y_2}, \binom{x_3}{y_3} \in \mathbb{R}^2$

Neutrales Element ist $\binom{0}{0}$, inverses Element zu $\binom{x}{y}$ ist $\binom{-x}{-y}$.

$\binom{x_1}{y_1} + \binom{x_2}{y_2} = \binom{x_1+x_2}{y_1+y_2} = \binom{x_2+x_1}{y_2+y_1} = \binom{x_2}{y_2} + \binom{x_1}{y_1} \quad \forall \binom{x_1}{y_1}, \binom{x_2}{y_2} \in \mathbb{R}^2$

Notation: Wir verwenden in dieser Vorlesung die Bezeichnungen $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ und $\mathbb{N}^+ = \{1, 2, 3, 4, \dots\}$ (aber nicht die Bezeichnung $\mathbb{N}^*$).

Bemerkung: Es gilt die folgende Verallgemeinerung von Satz 2: Es sei $n \in \mathbb{N}^+$. Versieht man $\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| x_1, \dots, x_n \right\}$ mit der komponentenweisen Addition

$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$, so ist $(\mathbb{R}^n, +)$ eine abelsche Gruppe.

Satz 3 Es sei $X (\neq \emptyset)$ eine Menge und $S_X := \{ f : X \to X \mid f \text{ ist bijektiv} \}$. Versieht man S_X mit der Verknüpfung von Funktionen, so ist $(S_X, \circ)$ eine Gruppe. Sie ist genau dann abelsch wenn $|X| \in \{1, 2\}$.

Beweis: Sind $f : X \to X$ und $g : X \to X$ beide bijektiv, so ist auch $g \circ f : X \to X$ eine bijektive Abbildung. Die Verknüpfung von Funktionen ist stets assoziativ. Neutrales Element ist die Identität $id_X : X \to X$, $id_X(x) = x \ \forall x \in X$. Inverses Element der bijektiven Abbildung $f : X \to X$ ist $f^{-1} : X \to X$.

Ist $|X| = 1$, o.B.d.A. $X = \{a\}$, so ist $S_X = \{\varepsilon\}$ mit $\varepsilon(a) = a$ und Verknüpfungstafel

$\circ$	ε
ε	ε

, d.h. $(S_X, \circ)$ ist abelsch. Ist $|X| = 2$, o.B.d.A. $X = \{a, b\}$, so ist $S_X = \{\varepsilon, \tau\}$ mit $\varepsilon(a) = a$, $\varepsilon(b) = b$ und $\tau(a) = b$, $\tau(b) = a$ und Verknüpfungstafel

$\circ$	ε	τ
ε	ε	τ
τ	τ	ε

, d.h. $(S_X, \circ)$ ist abelsch. Ist $|X| \geq 3$, so gibt es paarweise verschiedene $a, b, c \in X$. Es seien $\sigma, \tau \in S_X$ definiert als $\sigma(a) = b$, $\sigma(b) = c$, $\sigma(c) = a$ und

$\sigma(x)=x \ \forall x\in X\setminus\{a,b,c\}$ sowie $\tau(a)=b$, $\tau(b)=a$ und $\tau(x)=x \ \forall x\in X\setminus\{a,b\}$.

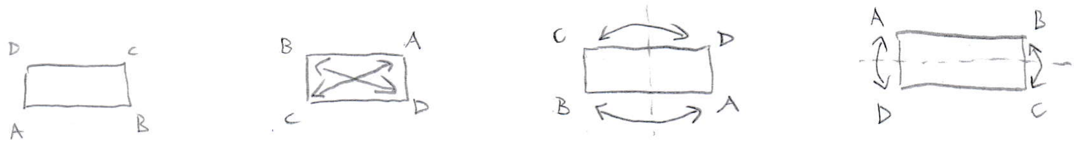
Dann ist $(\tau\circ\sigma)(a)=\tau(\sigma(a))=\tau(b)=a$ aber $(\sigma\circ\tau)(a)=\sigma(\tau(a))=\sigma(b)=c$, dh $\tau\circ\sigma\neq\sigma\circ\tau$.

Def.: Ist $X\ (\neq\emptyset)$ eine Menge, so wird $(S_X,\circ)$ als symmetrische Gruppe von X bezeichnet. Ist $X=\{1,\dots,n\}$ (mit $n\in\mathbb{N}^+$), so schreibt man S_n (statt $S_{\{1,\dots,n\}}$) für die symmetrische Gruppe und nennt ihre Elemente $\sigma\in S_n$ Permutationen.

Bemerkung: Die folgenden Beispiele illustrieren die Bedeutung des Gruppenbegriffs in der Geometrie. Tatsächlich kann man sich viele Gruppen als die Gesamtheit aller Symmetrien (einer bestimmten Art) vorstellen, die ein bestimmtes Objekt besitzt.
Genau genommen sollte man die darin auftretenden Begriffe (wie Punkt, Ebene, Dreieck, Quadrat, Translation, Rotation, etc.) sauber definieren bevor man sie verwendet. Wir verschieben das auf später und verlassen uns einstweilen auf die Anschauung.

Bspe.: 1) Wir betrachten das Rechteck 

und die folgenden vier Abbildungen, die es bijektiv auf sich selbst abbilden und dabei alle Abstände unverändert lassen (dh Isometrien sind):

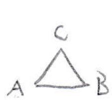


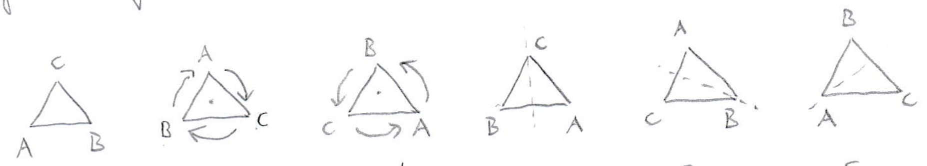
I	R	S_1	S_2
(Identität)	(Rotation um den Mittelpunkt um 180°)	(Spiegelung an senkrechter Symmetrieachse)	(Spiegelung an waagrechter Symmetrieachse)

Die Menge $\{I,R,S_1,S_2\}$ bildet mit der Verknüpfung von Abbildungen eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	I	R	S_1	S_2
I	I	R	S_1	S_2
R	R	I	S_2	S_1
S_1	S_1	S_2	I	R
S_2	S_2	S_1	R	I

Abgeschlossenheit kann man sofort an der Verknüpfungstafel ablesen und Assoziativität gilt für Verknüpfung von Abbildungen immer. I ist neutrales Element und alle Elemente sind ihre eigenen inversen Elemente (dh $I^{-1}=I$, $R^{-1}=R$, $S_1^{-1}=S_1$ und $S_2^{-1}=S_2$). Da die Verknüpfungstafel symmetrisch ist, ist die Gruppe abelsch.

2) Wir betrachten die folgenden sechs Abbildungen, die das gleichseitige Dreieck  bijektiv auf sich selbst abbilden und Isometrien sind:



I $\quad R^-$ $\quad R^+$ $\quad S_C$ $\quad S_B$ $\quad S_A$

Dabei ist I die Identität, R^- und R^+ Rotationen um $120°$ um den Mittelpunkt im bzw gegen den Uhrzeigersinn und S_A, S_B, S_C Spiegelungen an den angegebenen Symmetrieachsen. Es sei $D_3 = \{I, R^-, R^+, S_A, S_B, S_C\}$. Dann ist $(D_3, \circ)$ eine (nichtabelsche) Gruppe (wobei $\circ$ wieder die Verknüpfung von Abbildungen bezeichnet), die Symmetriegruppe des gleichseitigen Dreiecks.

Beachte: Jede Isometrie, die das Dreieck bijektiv auf sich selbst abbildet, muss die Eckpunkte auf die Eckpunkte abbilden, d.h. sie permutiert die Eckpunkte. Da es $3! = 6$ solche Permutationen gibt, kann es nur 6 solche Abbildungen geben.

3) Analog betrachten wir die folgenden acht Abbildungen, die ein Quadrat bijektiv auf sich selbst abbilden und Isometrien sind:

$$I \qquad \underbrace{R \quad R^2 \quad R^3}_{\text{Drehungen um } 90°,\, 180°,\, 270°} \qquad \underbrace{S_0 \quad S_1 \quad S_2 \quad S_3}_{\text{Spiegelungen an Symmetrieachsen}}$$

Identität

Bezeichnet $D_4 = \{I, R, R^2, R^3, S_0, S_1, S_2, S_3\}$, so ist $(D_4, \circ)$ wieder eine (nichtabelsche) Gruppe, die Symmetriegruppe des Quadrats. Auch hier gibt es keine weiteren Isometrien, die das Quadrat bijektiv auf sich selbst abbilden. Wegen $8 < 4! = 24$ kann man aber nicht wie beim Dreieck argumentieren.

4) Ist $n \in \mathbb{N}^+$, $n \geq 3$, so bezeichnet allgemein $(D_n, \circ)$ die Symmetriegruppe des regelmäßigen n-Ecks (d.h. die Gruppe aller Isometrien, die das n-Eck bijektiv auf sich selbst abbilden). Sie enthält $|D_n| = 2n$ Elemente, nämlich

- I, die Identität
- $R, R^2, \dots, R^{n-1}$, Rotationen um den Mittelpunkt des n-Ecks. Dabei bezeichnet R die Rotation um $\frac{360°}{n}$ (bzw $\frac{2\pi}{n}$) und daher R^k die Rotation um $\frac{k}{n} \cdot 360°$ (bzw $\frac{k}{n} \cdot 2\pi$) für $1 \leq k \leq n-1$.

- n Spiegelungen an Geraden, die durch den Mittelpunkt gehen
  Ist n ungerade, so gehen diese Geraden durch einen Eckpunkt und die gegenüberliegende Seite (wie oben im Fall $n=3$).
  Ist n gerade, so gehen $\frac{n}{2}$ dieser Geraden durch zwei gegenüberliegende Eckpunkte und $\frac{n}{2}$ durch die Mittelpunkte zweier gegenüberliegender Seiten (wie oben im Fall $n=4$)

5) Für $v \in \mathbb{R}^2$ bezeichne T_v die Translation (d.h. Verschiebung) des $\mathbb{R}^2$ um den Vektor v, d.h. $T_v: \mathbb{R}^2 \to \mathbb{R}^2$, $T_v(x) = x+v$. Bezeichnet $\mathcal{T} = \{T_v \mid v \in \mathbb{R}^2\}$ die Menge aller Translationen, so ist $(\mathcal{T}, \circ)$ eine abelsche Gruppe.

6) Es sei P ein fester Punkt der Ebene und α ein Winkel (mit $0° \leq \alpha < 360°$), sowie R_α die Rotation (d.h. Drehung) der Ebene um den Punkt P um den Winkel α gegen den Uhrzeigersinn. Bezeichnet $\mathcal{R} := \{R_\alpha \mid 0° \leq \alpha < 360°\}$, so ist $(\mathcal{R}, \circ)$ eine abelsche Gruppe.

5.3.2024

Def.: Es sei $(G,\circ)$ eine Gruppe und $H \subseteq G$, $H \neq \emptyset$. Ist H mit derselben Verknüpfung eine Gruppe, so wird H Untergruppe von G genannt.

Satz 4 (Untergruppenkriterium) Es sei $(G,\circ)$ eine Gruppe und $H \subseteq G$, $H \neq \emptyset$.
Dann sind äquivalent:

(i) H ist Untergruppe von G,

(ii) $a \circ b \in H$ $\forall a,b \in H$ und $a^{-1} \in H$ $\forall a \in H$,

(iii) $a \circ b^{-1} \in H$ $\forall a,b \in H$

Beweis: (i) $\Rightarrow$ (ii) Folgt aus der Abgeschlossenheit (von H) und der Existenz inverser Elemente in H.
(ii) $\Rightarrow$ (iii) Sind $a,b \in H$, so ist auch $b^{-1} \in H$ und daher auch $a \circ b^{-1} \in H$.
(iii) $\Rightarrow$ (i) Da $H \neq \emptyset$ gibt es ein $x \in H$. Daher $e = x \circ x^{-1} \in H$. Ist $a \in H$, so ist auch $a^{-1} = e \circ a^{-1} \in H$. Sind $a,b \in H$, so ist auch $a \circ b = a \circ (b^{-1})^{-1} \in H$. Da Assoziativität auf ganz G gilt, gilt sie auch auf H

Bemerkungen: 1) Der einfachste Weg zu zeigen, dass $(G,\circ)$ eine Gruppe ist, ist oft, zu zeigen, dass G Untergruppe einer bekannten Gruppe ist.

2) Ist $(G,+)$ eine abelsche Gruppe und $H \subseteq G$, $H \neq \emptyset$, so wird Satz 4 zu:

H ist Untergruppe von G
$\Leftrightarrow$ $a+b \in H$ $\forall a,b \in H$ und $-a \in H$ $\forall a \in H$
$\Leftrightarrow$ $a-b \in H$ $\forall a,b \in H$

Bspe.: 1) Die Menge der geraden Zahlen $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$ ist eine Untergruppe von $(\mathbb{Z},+)$: Sind $m,n \in 2\mathbb{Z}$, so $\exists k,l \in \mathbb{Z}: m = 2k,\ n = 2l \Rightarrow m-n = 2k-2l = 2(k-l) \in 2\mathbb{Z}$ und die Beh. folgt aus Satz 4.

2) Allgemeiner gilt: Ist $m \in \mathbb{Z}$, so ist $m\mathbb{Z} := \{km \mid k \in \mathbb{Z}\}$ Untergruppe von $(\mathbb{Z},+)$.

3) $(\mathbb{Z},+)$ ist Untergruppe von $(\mathbb{Q},+)$, $(\mathbb{Q},+)$ ist Untergruppe von $(\mathbb{R},+)$ und $(\mathbb{R},+)$ ist Untergruppe von $(\mathbb{C},+)$. Natürlich kann man in dieser Kette auch einzelne Gruppen überspringen. Z.B. ist $(\mathbb{Z},+)$ auch Untergruppe von $(\mathbb{R},+)$.

4) $(\{1,-1\},\cdot)$ ist Untergruppe von $(\mathbb{Q}^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$ ist Untergruppe von $(\mathbb{R}^*,\cdot)$ und $(\mathbb{R}^*,\cdot)$ ist Untergruppe von $(\mathbb{C}^*,\cdot)$.

5) Es seien $a,b \in \mathbb{R}$ und $U := \left\{\binom{x}{y} \in \mathbb{R}^2 \mid ax+by=0\right\}$. Dann ist U eine Untergruppe von $(\mathbb{R}^2,+)$: Sind $\binom{x_1}{y_1}, \binom{x_2}{y_2} \in U$, so $ax_1+by_1 = ax_2+by_2 = 0$ und daher $a(x_1-x_2)+b(y_1-y_2) = (ax_1+by_1)-(ax_2+by_2) = 0$, d.h. $\binom{x_1}{y_1} - \binom{x_2}{y_2} = \binom{x_1-x_2}{y_1-y_2} \in U$.

6) Allgemeiner gilt: Ist $n \in \mathbb{N}^+$, $a_1,\ldots,a_n \in \mathbb{R}$ und $U = \left\{\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} \in \mathbb{R}^n \mid a_1x_1+\cdots+a_nx_n = 0\right\}$, so ist U Untergruppe von $(\mathbb{R}^n,+)$.

7) Bezeichnet $G = \{I,R,S_1,S_2\}$ die vier Isometrien, die ein Rechteck bijektiv auf sich selbst abbilden (wie in Bsp 1) auf Seite 4), so sind $(\{I\},\circ)$, $(\{I,R\},\circ)$, $(\{I,S_1\},\circ)$, $(\{I,S_2\},\circ)$ und $(G,\circ)$ alles Untergruppen von $(G,\circ)$.

8) Wir werden später zeigen: $\{f: \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ ist Isometrie}\}$ ist Untergruppe der symmetrischen Gruppe von $\mathbb{R}^2$, d.h. der Gruppe $(S_{\mathbb{R}^2},\circ)$ aller bijektiven Abbildungen des $\mathbb{R}^2$ auf sich selbst.

9) Wir werden später zeigen: Die Translationen der Ebene und die Rotationen der Ebene um einen Punkt bilden beides Untergruppen der Isometrien der Ebene.

10) Ist $n \in \mathbb{N}^+$, $n \geq 3$, so permutiert jedes $\sigma \in D_n$ die Ecken eines regelmäßigen n-Ecks. Daher kann D_n als Untergruppe von $(S_n,\circ)$ aufgefasst werden.

11) Jede Gruppe $(G,\circ)$ enthält die Untergruppen $(\{e\},\circ)$ und $(G,\circ)$.

<u>Satz 5</u> Es sei $(G,\circ)$ eine Gruppe. Dann gelten:

(i) $(a^{-1})^{-1} = a \quad \forall a \in G$,

(ii) $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad \forall a,b \in G$.

<u>Beweis</u>: (i) Folgt aus $a \circ a^{-1} = a^{-1} \circ a = e$ und der Eindeutigkeit des inversen Elements zu a^{-1} (Satz 1(ii)).

(ii) $(a\circ b)\circ(b^{-1}\circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e$ und analog $(b^{-1}\circ a^{-1})\circ(a\circ b) = e$. Die Beh. folgt aus der Eindeutigkeit des inversen Elements zu $a \circ b$ (Satz 1(ii)).

Def.: Es sei $(G,\circ)$ eine Gruppe und $a\in G$. Man definiert

$a^n = \underbrace{a\circ\cdots\circ a}_{n\text{-mal}}$ für $n\in\mathbb{N}^+$, $a^0 = e$ und $a^{-n} := (a^{-1})^n = (a^n)^{-1}$ für $n\in\mathbb{N}^+$.

(Die letzte Gleichung folgt aus $(a^{-1})^n\circ a^n = a^n\circ(a^{-1})^n = e\ \forall n\in\mathbb{N}^+$.)

Satz 6 Es sei $(G,\circ)$ eine Gruppe. Dann gelten

(i) $a^m\circ a^n = a^{m+n}\quad \forall a\in G\ \forall m,n\in\mathbb{Z}$,

(ii) $(a^m)^n = a^{mn}\quad \forall a\in G\ \forall m,n\in\mathbb{Z}$,

(iii) $(a\circ b)^n = a^n\circ b^n\quad \forall a,b\in G$ mit der Eigenschaft $a\circ b = b\circ a$ $\forall n\in\mathbb{Z}$

Der Beweis verwendet Satz 5, Fallunterscheidungen und Induktion. Wir lassen ihn aus.

Bemerkung: Ist $(G,+)$ eine abelsche Gruppe, so wird die obige Def. zu:

$na := \underbrace{a+\cdots+a}_{n\text{-mal}}$ für $n\in\mathbb{N}^+$, $\underbrace{0}_{\in\mathbb{Z}}\cdot a := \underbrace{0}_{\in G}$ und $(-n)a := n(-a) = -(na)$ für $n\in\mathbb{N}^+$

und Satz 6 wird zu

$$ma + na = (m+n)a \quad \forall a\in G\ \forall m,n\in\mathbb{Z},$$
$$m(na) = (mn)a \quad \forall a\in G\ \forall m,n\in\mathbb{Z},$$
$$n(a+b) = na+nb \quad \forall a,b\in G\ \forall n\in\mathbb{Z}.$$

Bemerkung: Der Aufbau dieses Kapitels ist nicht ganz sauber:

- In Bsp. 3, auf Seite 6 wird R^2 und R^3 verwendet, definiert werden solche Ausdrücke aber erst auf Seite 9.
- Im Beweis von Satz 4 (Seite 7) wird verwendet, dass $(b^{-1})^{-1} = b$, bewiesen wird das aber erst in Satz 5 (Seite 8)

Man kann diese Probleme beseitigen, indem man den Schluss des Kapitels (ab Satz 5) auf Seite 5 (nach der Definition der symmetrischen Gruppe) verschiebt