# 1. Teil: Gruppen

## 1. Definitionen und einfache Eigenschaften

**Definition:** Es sei $G \neq \varnothing$ eine Menge und $\cdot$ eine (binäre) Verknüpfung auf $G$ (d.h. eine Abbildung $G \times G \to G$, $(a,b) \mapsto a \cdot b$). Gilt

$(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall a,b,c \in G$ (Assoziativität)

so wird $(G, \cdot)$ als Halbgruppe bezeichnet.

**Bemerkungen:** 1) In der Aussage, dass $\cdot$ eine Verknüpfung auf $G$ ist, ist enthalten, dass $G$ bezüglich $\cdot$ abgeschlossen ist, d.h. $a \cdot b \in G\ \forall a,b \in G$.
2) Die Verknüpfung $\cdot$ wird oft nicht geschrieben, d.h. man schreibt $ab$ statt $a \cdot b$.
3) Ist klar, welche Verknüpfung gemeint ist, so schreibt man statt $(G, \cdot)$ oft nur $G$.
4) Ist $G = \{a_1, \dots, a_n\}$ endlich, so kann die Verknüpfung durch eine Verknüpfungstafel angegeben werden:

| $\cdot$ | $a_1$ | $\cdots$ | $a_j$ | $\cdots$ | $a_n$ |
|---|---|---|---|---|---|
| $a_1$ | $a_1a_1$ | $\cdots$ | $a_1a_j$ | $\cdots$ | $a_1a_n$ |
| $\vdots$ | $\vdots$ | | $\vdots$ | | $\vdots$ |
| $a_i$ | $a_ia_1$ | $\cdots$ | $a_ia_j$ | $\cdots$ | $a_ia_n$ |
| $\vdots$ | $\vdots$ | | $\vdots$ | | $\vdots$ |
| $a_n$ | $a_na_1$ | $\cdots$ | $a_na_j$ | $\cdots$ | $a_na_n$ |

**Definition:** Ist $(G, \cdot)$ eine Halbgruppe und $a_1, \dots, a_n \in G$, so definiert man das Produkt $a_1 \cdots a_n \in G$ für $n \geq 3$ induktiv durch $a_1 \cdots a_n := (a_1 \cdots a_{n-1})a_n$ (d.h. $a_1 \cdot a_2 \cdot a_3 = (a_1 \cdot a_2) \cdot a_3$ und $a_1 \cdot a_2 \cdot a_3 \cdot a_4 = (a_1 \cdot a_2 \cdot a_3) \cdot a_4 = \big((a_1 \cdot a_2) \cdot a_3\big) \cdot a_4$). Statt $a_1 \cdots a_n$ schreibt man auch $\prod_{i=1}^{n} a_i$.

**Satz 1:** Es sei $G$ eine Halbgruppe und $a_1, \dots, a_n \in G$. Verknüpft man $a_1, \dots, a_n$ (in dieser Reihenfolge) auf irgendeine sinnvolle Weise durch Klammerung, so erhält man stets das oben definierte Standardprodukt $a_1 \cdots a_n$.

**Bemerkung:** Es gilt also z.B. $a_1\big((a_2a_3)(a_4a_5)\big) = a_1a_2a_3a_4a_5 = \big(((a_1a_2)a_3)a_4\big)a_5$.

**Beweis:** Wir zeigen zunächst $(a_1 \cdots a_{m-1})(a_m \cdots a_n) = a_1 \cdots a_n$ für $1 < m \leq n$ mittels Induktion nach $n$. Für $n \in \{1,2,3\}$ ist nichts zu zeigen. Es sei nun $n \geq 4$. Für $m = n$ folgt die Behauptung aus der Definition des Produkts $a_1 \cdots a_n$. Für $m < n$ gilt

$$(a_1 \cdots a_{m-1})(a_m \cdots a_n) = (a_1 \cdots a_{m-1})\big((a_m \cdots a_{n-1})a_n\big)$$
$$= \big((a_1 \cdots a_{m-1})(a_m \cdots a_{n-1})\big)a_n \overset{\text{IV}}{=} (a_1 \cdots a_{n-1})a_n = a_1 \cdots a_n$$

Wir zeigen nun die eigentliche Behauptung mittels Induktion nach $n$. Für $n \in \{1,2,3\}$ ist wieder nichts zu zeigen. Ist $n \geq 4$ und $p$ irgendein sinnvolles Produkt von $a_1, \dots, a_n$, so muss $p = x \cdot y$ gelten, wobei $x$ ein sinnvolles Produkt von $a_1, \dots, a_{m-1}$ und $y$ ein sinnvolles Produkt von $a_m, \dots, a_n$ ist (für $1 < m \leq n$). Nach Induktionsvoraussetzung ist $x = a_1 \cdots a_{m-1}$ und $y = a_m \cdots a_n$ und die Behauptung folgt aus dem bisher gezeigten.

**Definition:** Es sei $(G, \cdot)$ eine Halbgruppe. Gibt es ein $e \in G$ mit der Eigenschaft, dass $e \cdot a = a \cdot e = a \ \forall a \in G$, so wird $G$ als Monoid bezeichnet und $e$ wird neutrales Element des Monoids genannt.

**Satz 2:** Das neutrale Element eines Monoids ist eindeutig bestimmt.

**Beweis:** Es sei $(G, \cdot)$ ein Monoid und $e, f \in G$ neutrale Elemente. Dann $e = e \cdot f = f \cdot e = f$.

**Definition:** Es sei $(G, \cdot)$ ein Monoid mit neutralem Element $e$. Ein $a \in G$ heißt invertierbar, wenn es ein $x \in G$ gibt, derart dass $a \cdot x = x \cdot a = e$. Das Element $x$ wird als inverses Element von $a$ bezeichnet.

**Bemerkung:** Ist $(G, \cdot)$ ein Monoid mit neutralem Element $e$, so ist $e$ invertierbar, da $e \cdot e = e$.

**Satz 3:** Es sei $(G, \cdot)$ ein Monoid mit neutralem Element $e$. Ist $a \in G$ invertiertbar, so ist sein inverses Element eindeutig bestimmt.

**Beweis:** Sind $x, y \in G$ inverse Elemente von $a$, so ist

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

**Definition:** Ist $(G, \cdot)$ ein Monoid und $a \in G$ invertierbar, so wird das inverse Element von $a$ mit $a^{-1}$ bezeichnet. (Diese Notation ist wegen Satz 3 sinnvoll.)

**Satz 4:** Es sei $(G, \cdot)$ ein Monoid mit neutralem Element $e$.
(i) Ist $a \in G$ invertiertbar, so ist auch $a^{-1}$ invertiertbar und $(a^{-1})^{-1} = a$.
(ii) Sind $a, b \in G$ beide invertiertbar, so ist auch $a \cdot b$ invertierbar und $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

**Beweis:** (i) Das folgt aus $a \cdot a^{-1} = a^{-1} \cdot a = e$ und der Eindeutigkeit des Inversen von $a^{-1}$.
(ii) Es ist $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$ und völlig analog $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. Die Behauptung folgt nun aus der Eindeutigkeit des Inversen von $a \cdot b$.

**Definition:** Es sei $(G, \cdot)$ ein Monoid. Ist jedes $a \in G$ invertiertbar, so wird $(G, \cdot)$ Gruppe genannt.

**Definition:** Es sei $(G, \cdot)$ eine Gruppe. Gilt zusätzlich

$a \cdot b = b \cdot a \ \forall a, b \in G$ (Kommutativität)

so wird $(G, \cdot)$ als abelsche (oder kommutative) Gruppe bezeichnet.

**Satz 5:** Es sei $G$ eine abelsche Gruppe, $a_1, \dots, a_n \in G$ und $i_1, \dots, i_n$ eine Permutation von $1, \dots, n$. Dann gilt $a_{i_1} \cdots a_{i_n} = a_1 \cdots a_n$.

**Beweis:** Übung

**Bemerkung:** Man kann Satz 5 auch folgendermaßen formulieren:
Ist $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ eine bijektive Abbildung, so ist $a_{\sigma(1)} \cdots a_{\sigma(n)} = a_1 \cdots a_n$.

**Bemerkungen:** 1) Die Gruppenaxiome lauten also:
Ist $G \neq \varnothing$ eine Menge und $\cdot : G \times G \to G$ eine Verknüpfung, so müssen gelten:

1) $(ab)c = a(bc) \ \forall a, b, c \in G$ (Assoziativität)
2) $\exists e \in G \ \forall a \in G : ea = ae = a$ (neutrales Element)
3) $\forall a \in G \ \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$ (inverses Element von $a$)

Gilt zusätzlich

4) $ab = ba \ \forall a, b \in G$ (Kommutativität)

so handelt es sich um eine abelsche Gruppe.

2) Die Verknüpfung vieler Gruppen wird als $+$ geschrieben (d.h. man schreibt $a + b$ statt $a \cdot b$), insbesondere wenn die Gruppe abelsch ist. Das neutrale Element wird dann in der Regel mit 0 bezeichnet, das inverse Element von $a$ als $-a$ und die Gruppenaxiome der (abelschen) Gruppe $(G, +)$ lauten:

1) $(a + b) + c = a + (b + c) \ \forall a, b, c \in G$ (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 von $a$)
4) $a + b = b + a \ \forall a, b \in G$ (Kommutativität)

**Beispiele:** 1) Ist $V$ ein Vektorraum, so ist $(V, +)$ nach Definition eine abelsche Gruppe. Insbesondere gilt: Ist $K$ ein Körper, so ist $(K^n, +)$ eine abelsche Gruppe (mit $n \in \mathbb{N} \setminus \{0\}$). Z.B. sind $(\mathbb{Q}^n, +)$, $(\mathbb{R}^n, +)$ und $(\mathbb{C}^n, +)$ abelsche Gruppen.

2) Ist $(K, +, \cdot)$ ein Körper, so ist insbesondere $(K, +)$ eine abelsche Gruppe (also z.B. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$) und $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe (also z.B. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ und $(\mathbb{C} \setminus \{0\}, \cdot)$).

3) Allgemein gilt: Ist $(R, +, \cdot)$ ein Ring, so ist $(R, +)$ eine abelsche Gruppe (also z.B. $(\mathbb{Z}, +)$).

4) Die Menge $\{+1,-1\}$, versehen mit der Multiplikation $1\cdot 1=(-1)\cdot(-1)=1$ und $1\cdot(-1)=(-1)\cdot 1=-1$ ist eine abelsche Gruppe mit der folgenden Verknüpfungstafel:

| $\cdot$ | $+1$ | $-1$ |
|---|---|---|
| $+1$ | $+1$ | $-1$ |
| $-1$ | $-1$ | $+1$ |

5) Ist $m\in\mathbb{N}\setminus\{0,1\}$ und bezeichnet $\mathbb{Z}_m=\{\overline{0},\overline{1},\dots,\overline{m-1}\}$ die Restklassen modulo $m$, ist (nach Bsp. 3) und Zahlentheorie) $(\mathbb{Z}_m,+)$ eine abelsche Gruppe und die primen Restklassen $(\mathbb{Z}_m^*,\cdot)$ (mit $\mathbb{Z}_m^*=\{\overline{a}\in\mathbb{Z}_m\mid \mathrm{ggT}(a,m)=1\}=\{\overline{a}\in\mathbb{Z}_m\mid \overline{a}\text{ ist invertierbar}\}$) bilden eine abelsche Gruppe (nach Zahlentheorie). Insbesondere gilt: Ist $p$ eine Primzahl, so ist $(\mathbb{Z}_p^*,\cdot)$ (mit $\mathbb{Z}_p^*=\{\overline{1},\overline{2},\dots,\overline{p-1}\}$) eine abelsche Gruppe (was auch aus Bsp. 2) folgt, da $(\mathbb{Z}_p,+,\cdot)$ ein Körper ist).

6) Ist $K$ ein Körper, $n\in\mathbb{N}\setminus\{0\}$ und bezeichnet $M_n(K)$ die Menge aller $n\times n$-Matrizen mit Eintragungen aus $K$, so ist die *General Linear Group*

$$\mathrm{GL}_n(K)=\{A\in M_n(K)\mid A\text{ ist invertierbar}\}=\{A\in M_n(K)\mid \det A\neq 0\}$$

mit der Matrizenmultiplikation eine Gruppe (siehe Lineare Algebra), die für $n\geq 2$ nicht abelsch ist.

7) Ist $K$ ein Körper und $n\in\mathbb{N}\setminus\{0\}$, so ist die *Special Linear Group*

$$\mathrm{SL}_n(K)=\{A\in M_n(K)\mid \det A=1\}$$

mit der Matrizenmultiplikation eine Gruppe (siehe Linear Algebra).

8) Für $n\in\mathbb{N}\setminus\{0\}$ ist die *Orthogonale Gruppe*

$$\mathrm{O}(n)=\left\{A\in\mathrm{GL}_n(\mathbb{R})\,\middle|\,A^{-1}=A^T\right\}$$

eine Gruppe (siehe Lineare Algebra). (Dabei bezeichnet $A^T$ die transponierte Matrix der Matrix $A$.)

9) Für $n\in\mathbb{N}\setminus\{0\}$ ist die *Unitäre Gruppe*

$$\mathrm{U}(n)=\left\{A\in\mathrm{GL}_n(\mathbb{C})\,\middle|\,A^{-1}=\overline{A}^T\right\}$$

eine Gruppe (siehe Lineare Algebra). (Dabei bezeichnet $\overline{A}^T$ die transponierte, komplex konjugierte Matrix der Matrix $A$.)

10) Ist $X\neq\varnothing$ eine Menge, so ist die *Symmetrische Gruppe*

$$S_X=\{f:X\to X\mid f\text{ ist bijektiv}\}$$

mit der Verknüpfung von Abbildungen eine Gruppe. Im Spezialfall $X=\{1,\dots,n\}$ schreibt man $S_n$ statt $S_{\{1,\dots,n\}}$, d.h. $S_n=\left\{\sigma:\{1,\dots,n\}\to\{1,\dots,n\}\mid\sigma\text{ ist bijektiv}\right\}$.

11) Wir betrachten ein Rechteck und die folgenden vier Abbildungen, die es invariant lassen:

- $I$ (Identität, d.h. das Rechteck bleibt unverändert)
- $R$ (Rotation um den Mittelpunkt des Rechtecks um 180°)
- $S_1$ (Spiegelung an der senkrechten Symmetrieachse)
- $S_2$ (Spiegelung an der waagrechten Symmetrieachse)

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

| $\circ$ | $I$ | $R$ | $S_1$ | $S_2$ |
|---|---|---|---|---|
| $I$ | $I$ | $R$ | $S_1$ | $S_2$ |
| $R$ | $R$ | $I$ | $S_2$ | $S_1$ |
| $S_1$ | $S_1$ | $S_2$ | $I$ | $R$ |
| $S_2$ | $S_2$ | $S_1$ | $R$ | $I$ |

Das ist tatsächlich eine Gruppe:

- Abgeschlossenheit kann man an der Verknüpfungtafel ablesen.
- Assoziativität gilt immer für die Verknüpfung von Abbildungen.
- $I$ ist neutrales Element.
- Jedes Element ist sein eigenes Inverses
  (d.h. $I^{-1} = I$, $R^{-1} = R$, $S_1^{-1} = S_1$ und $S_2^{-1} = S_2$).

Da die Verknüpfungstafel symmetrisch bezüglich der Diagonale ist, handelt es sich um eine abelsche Gruppe.

**Definition:** Es sei $G$ eine Halbgruppe, $a \in G$ und $n \in \mathbb{N} \setminus \{0\}$. Dann setzt man

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n\text{-mal}}.$$

**Definition:** Es sei $G$ ein Monoid mit neutralem Element $e$ und $a \in G$. Zusätzlich zur vorangegangenen Definition setzt man $a^0 := e$.

**Lemma 6:** Es sei $G$ ein Monoid mit neutralem Element $e$, sowie $a \in G$ invertierbar und $n \in \mathbb{N} \cup \{0\}$. Dann ist $a^n$ invertierbar und $(a^n)^{-1} = (a^{-1})^n$.

**Beweis:** Induktion nach $n$. Für $n = 0$ ist $(a^0)^{-1} = e^{-1} = e = (a^{-1})^0$ und für $n = 1$ ist $(a^1)^{-1} = a^{-1} = (a^{-1})^1$. Schließlich ist

$$(a^{n+1})^{-1} = (a^n \cdot a)^{-1} \overset{\text{Satz 4 (ii)}}{=} a^{-1} \cdot (a^n)^{-1} \overset{\text{IV}}{=} a^{-1} \cdot (a^{-1})^n = (a^{-1})^{n+1}.$$

**Definition:** Es sei $G$ ein Monoid mit neutralem Element $e$, $a \in G$ invertierbar und $n \in \mathbb{Z}$, $n < 0$. Dann setzt man $a^n := \left(a^{|n|}\right)^{-1} = \left(a^{-1}\right)^{|n|}$ (wobei die letzte Gleichung wegen Lemma 6 gilt).

**Bemerkung:** Wird die Verknüpfung + geschrieben, so werden die letzte drei Definitionen zu $n \cdot a = \underbrace{a + \ldots + a}_{n\text{-mal}}$ (für $n \in \mathbb{N} \setminus \{0\}$), $0 \cdot a = 0$ (wobei auf der linken Seite $0 \in \mathbb{Z}$ und auf der rechten Seite $0 \in G$ gilt) und $n \cdot a = -(|n|a) = |n|(-a)$ (für $n \in \mathbb{Z}$, $n < 0$).

**Satz 7:** (i) Ist $G$ eine Halbgruppe und $a \in G$, so gilt $a^m a^n = a^{m+n}$ $\forall m, n \in \mathbb{N} \setminus \{0\}$.
(ii) Ist $G$ ein Monoid und $a \in G$, so gilt $a^m a^n = a^{m+n}$ $\forall m, n \in \mathbb{N} \cup \{0\}$.
(iii) Ist $G$ ein Monoid und $a \in G$ invertierbar, so gilt $a^m a^n = a^{m+n}$ $\forall m, n \in \mathbb{Z}$.

**Beweis:** (i) Das folgt aus Satz 1.
(ii) Ist $m = 0$, so ist $a^m a^n = a^0 a^n = e a^n = a^n = a^{0+n} = a^{m+n}$.
Ist $n = 0$, so ist $a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$.
Der Fall $m > 0$ und $n > 0$ wurde bereits in (i) bewiesen.
(iii) 1. Fall: $m = 0$ oder $n = 0$: Das zeigt man wie in (ii).
2. Fall: $m > 0$ und $n > 0$: Das wurde bereits in (i) bewiesen.
3. Fall: $m < 0$ und $n < 0$: Hier ist

$$\begin{aligned} a^m a^n &= \left(a^{-1}\right)^{|m|}\left(a^{-1}\right)^{|n|} \overset{\text{2. Fall}}{=} \left(a^{-1}\right)^{|m|+|n|} \\ &= \left(a^{-1}\right)^{-m-n} = \left(a^{-1}\right)^{-(m+n)} = \left(a^{-1}\right)^{|m+n|} = a^{m+n}. \end{aligned}$$

4. Fall: $m < 0 < n$: Induktion nach $n$. Es sei zunächst $n = 1$.
Falls $m = -1$, so ist $a^m a^n = a^{-1}a = e = a^0 = a^{-1+1} = a^{m+n}$.
Falls $m \leq -2$, so ist

$$\begin{aligned} a^m a^n &= \left(a^{-1}\right)^{|m|} a = \left(\left(a^{-1}\right)^{|m|-1} a^{-1}\right) a = \left(a^{-1}\right)^{|m|-1}\left(a^{-1}a\right) \\ &= \left(a^{-1}\right)^{|m|-1} e = \left(a^{-1}\right)^{|m|-1} = a^{-|m|+1} = a^{m+1} = a^{m+n} \end{aligned}$$

Nun kann man den Induktionsschritt durchführen:

$$a^m a^{n+1} = a^m (a^n a) = (a^m a^n) a \overset{\text{IV}}{=} a^{m+n} a = a^{(m+n)+1} = a^{m+(n+1)}$$

Dabei gilt das vorletzte Gleichheitszeichen für $m + n \geq 0$ wegen des 1. bzw. 2. Falls und für $m + n < 0$ wegen des Induktionsanfangs.
5. Fall: $n < 0 < m$: Diesen Fall kann man analog zum 4. Fall mit Induktion nach $m$ zeigen.

**Satz 8:** (i) Ist $G$ eine Halbgruppe und $a \in G$, so gilt $(a^m)^n = a^{mn}\ \forall m, n \in \mathbb{N} \setminus \{0\}$.
(ii) Ist $G$ ein Monoid und $a \in G$, so gilt $(a^m)^n = a^{mn}\ \forall m, n \in \mathbb{N} \cup \{0\}$.
(iii) Ist $G$ ein Monoid und $a \in G$ invertierbar, so gilt $(a^m)^n = a^{mn}\ \forall m, n \in \mathbb{Z}$.

**Beweis:** (i) Das gilt wegen

$$(a^m)^n = \underbrace{a^m \dots a^m}_{n\text{-mal}} \overset{\text{Satz } 1}{=} a^{m+\dots+m} = a^{mn}.$$

(ii) Ist $m = 0$, so ist $(a^m)^n = (a^0)^n = e^n = e = a^0 = a^{0 \cdot m} = a^{mn}$.
Ist $n = 0$, so ist $(a^m)^n = (a^m)^0 = e = a^0 = a^{m \cdot 0} = a^{mn}$.
Der Fall $m > 0$ und $n > 0$ wurde bereits in (i) bewiesen.
(iii) Ist $n = 0$, so zeigt man das wie in (ii).
Für $n > 0$ verwende Induktion nach $n$. Für $n = 1$ ist $(a^m)^n = (a^m)^1 = a^m = a^{m \cdot 1} = a^{mn}$.
Der Induktionsschritt lautet $(a^m)^{n+1} = (a^m)^n a^m \overset{\text{IV}}{=} a^{mn} a^m \overset{\text{Satz } 7}{=} a^{mn+m} = a^{m(n+1)}$.
Für $n = -1$ besagt die Behauptung $(a^m)^{-1} = a^{-m}$. Für $m > 0$ ist das die Definition. Für $m = 0$ folgt es aus $(a^m)^{-1} = (a^0)^{-1} = e^{-1} = e = a^0 = a^{-0} = a^{-m}$. Für $m < 0$ kann man es umformulieren zu $\left(a^{-|m|}\right)^{-1} = a^{|m|}$, was zu $a^{-|m|} = \left(a^{|m|}\right)^{-1}$ äquivalent und daher korrekt ist.
Ist $n < 0$ beliebig, so gilt die Behauptung wegen

$$(a^m)^n = \left((a^m)^{|n|}\right)^{-1} = \left(a^{m|n|}\right)^{-1} = a^{-m|n|} = a^{mn}.$$

**Satz 9:** (i) Ist $G$ eine Halbgruppe und $a, b \in G$ erfüllen die Bedingung $ab = ba$, so gilt $(ab)^n = a^n b^n\ \forall n \in \mathbb{N} \setminus \{0\}$.
(ii) Ist $G$ ein Monoid und $a, b \in G$ erfüllen $ab = ba$, so gilt $(ab)^n = a^n b^n\ \forall n \in \mathbb{N} \cup \{0\}$.
(iii) Ist $G$ ein Monoid und $a, b \in G$ sind invertierbar und erfüllen die Bedingung $ab = ba$, so gilt $(ab)^n = a^n b^n\ \forall n \in \mathbb{Z}$.

**Beweis:** (i) Wir zeigen zunächst $ab^n = b^n a\ \forall n \in \mathbb{N} \setminus \{0\}$ mit Induktion nach $n$.
Für $n = 1$ ist das die Voraussetzung. Der Induktionsschritt ist

$$ab^{n+1} = a(b^n b) = (ab^n)b \overset{\text{IV}}{=} (b^n a)b = b^n(ab) = b^n(ba) = (b^n b)a = b^{n+1}a.$$

Wir zeigen nun die eigentliche Behauptung, ebenfalls mit Induktion nach $n$. Für $n = 1$ ist nichts zu zeigen. Der Induktionsschritt ist

$$(ab)^{n+1} = (ab)^n(ab) \overset{\text{IV}}{=} (a^n b^n)(ab) = a^n(b^n a)b = a^n(ab^n)b = (a^n a)(b^n b) = a^{n+1}b^{n+1}.$$

(ii) Für $n = 0$ ist $(ab)^n = (ab)^0 = e = ee = a^0 b^0 = a^n b^n$. Für $n \geq 1$ wurde die Behauptung bereits in (i) gezeigt.

(iii) Für $n \geq 0$ wurde die Behauptung bereits gezeigt. Wir zeigen zunächst, dass auch $a^{-1}b^{-1} = b^{-1}a^{-1}$ gilt:

$$a^{-1}b^{-1} \overset{\text{Satz 4 (ii)}}{=} (ba)^{-1} = (ab)^{-1} \overset{\text{Satz 4 (ii)}}{=} b^{-1}a^{-1}$$

Für $n < 0$ gilt nun

$$(ab)^n = \big((ab)^{-1}\big)^{|n|} = \big(b^{-1}a^{-1}\big)^{|n|} = \big(a^{-1}b^{-1}\big)^{|n|} = \big(a^{-1}\big)^{|n|}\big(b^{-1}\big)^{|n|} = a^n b^n.$$

**Bemerkungen:** 1) Ist $G$ eine Gruppe, so gelten Satz 7 (iii) und Satz 8 (iii) für alle $a \in G$ und alle $m, n \in \mathbb{Z}$, d.h. $a^m a^n = a^{m+n}$ und $(a^m)^n = a^{mn}$ $\forall a \in G\ \forall m, n \in \mathbb{Z}$.
2) Ist $G$ eine abelsche Gruppe, so gilt Satz 9 (iii) für alle $a, b \in G$ und alle $n \in \mathbb{Z}$, d.h. $(ab)^n = a^n b^n$ $\forall a, b \in G\ \forall\ n \in \mathbb{Z}$.
3) Ist $(G, +)$ eine additiv geschriebene abelsche Gruppe, so werden die Sätze 7, 8 und 9 zu

$$\begin{aligned}
n(a+b) &= na + nb && \forall n \in \mathbb{Z}\ \forall a, b \in G \text{ (Satz 9 (iii))} \\
(m+n)a &= ma + na && \forall m, n \in \mathbb{Z}\ \forall a \in G \text{ (Satz 7 (iii))} \\
n(ma) &= (nm)a && \forall m, n \in \mathbb{Z}\ \forall a \in G \text{ (Satz 8 (iii))} \\
1 \cdot a &= a && \forall a \in G \text{ (nach Definition)}
\end{aligned}$$

Wäre $\mathbb{Z}$ ein Körper, so hätten wir gezeigt, dass $G$ ein Vektorraum über $\mathbb{Z}$ ist. Stattdessen sagt man, $G$ sei ein $\mathbb{Z}$-Modul.