KAPITEL 5

Operationen von Gruppen auf Mengen

DEFINITION. *Eine* **Operation** *(oder auch* **Aktion***) einer (multiplikativ geschriebenen) Gruppe G (mit neutralem Element e) auf einer Menge S ist gegeben durch eine Abbildung*

$$G \times S \to S, \quad (g, s) \mapsto g \cdot s,$$

wobei folgende Bedingungen erfüllt sind:

- $(gh) \cdot s = g \cdot (h \cdot s)$ *für alle $g, h \in G$ und $s \in S$.*
- $e \cdot s = s$ *für alle $s \in S$.*

Schreibt man die Abbildung $G \times S \to S$ als $(g, s) \mapsto g * s$, so lauten die Bedingungen

- $(gh) * s = g * (h * s)$ *für alle $g, h \in G$ und $s \in S$.*
- $e * s = s$ *für alle $s \in S$.*

Wir beginnen mit Beispielen.

Beispiel: Die Gruppe S_n operiert auf der Menge $S = \{1, \ldots, n\}$ durch

$$\sigma * i = \sigma(i) \text{ für } \sigma \in S_n \text{ und } i \in \{1, \ldots, n\},$$

denn es gilt

$$(\sigma\tau) * i = (\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(\tau * i) = \sigma * (\tau * i)$$

und

$$\mathrm{id} * i = \mathrm{id}(i) = i.$$

($\sigma * i$ haben wir nur geschrieben, damit man die Gültigkeit der Axiome besser sehen kann. Man kann natürlich auch einfach sagen: S_n operiert auf $\{1, \ldots, n\}$ durch $(\sigma, i) \mapsto \sigma(i)$.)

Beispiel: Ist K ein Körper und $n \in \mathbb{N}$, so operiert die multiplikative Gruppe $\mathrm{GL}_n(K)$ auf $K^n = \{ \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} : c_1, \ldots, c_n \in K \}$ durch

$$(A, c) \mapsto Ac,$$

denn es gilt (nach den Regeln der Matrizenrechnung)

$$(AB)c = A(Bc) \quad \text{und} \quad \mathbf{1}_n c = c.$$

G operiert auf sich selbst durch Konjugation. Sei G eine (multiplikativ geschriebene) Gruppe mit neutralem Element e. Wir definieren

$$g * x = gxg^{-1} \text{ für } g \in G \text{ und } x \in G.$$

Dies ist eine Operation von G auf sich selbst, denn es gilt

$$(gh) * x = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = g(h * x)g^{-1} = g * (h * x)$$

und

$$e * x = exe^{-1} = x.$$

Wir sagen: G operiert auf sich selbst durch Konjugation.

Datei: alg_operationen.tex. Version vom 11.12.2023

Beispiel: Sind $\sigma, \tau \in S_n$ und hat τ die Zykelzerlegung

$$\tau = (a_{1,1}, \ldots, a_{1,\ell_1})(a_{2,1}, \ldots, a_{2,\ell_2}) \ldots (a_{r,1}, \ldots, a_{r,\ell_r}),$$

so gilt

$$\sigma\tau\sigma^{-1} = (\sigma(a_{1,1}), \ldots, \sigma(a_{1,\ell_1}))(\sigma(a_{2,1}), \ldots, \sigma(a_{2,\ell_2})) \ldots (\sigma(a_{r,1}), \ldots, \sigma(a_{r,\ell_2})).$$

Wir haben auch gesehen, dass zwei Permutationen genau dann konjugiert sind, wenn sie den gleichen Typ $(\ell_1, \ell_2, \ldots, \ell_r)$ haben.

Beispiel: In der symmetrischen Gruppe S_6 gilt für $\sigma = (13)(254)$

$$\sigma\Big((14)(2356)\Big)\sigma^{-1} = (32)(5146) = (1465)(23).$$

Beispiel: Die alternierende Gruppe A_4 operiert auf sich selbst durch Konjugation:

$$(a, b) \mapsto aba^{-1}.$$

Wir haben dazu eine Tabelle angelegt, wobei in der Zeile von a und der Spalte von b das Element $a * b = aba^{-1}$ steht:

$a * b = aba^{-1}$	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(12)(34)	(1)	(12)(34)	(13)(24)	(14)(23)	(142)	(124)	(132)	(123)	(243)	(234)	(143)	(134)
(13)(24)	(1)	(12)(34)	(13)(24)	(14)(23)	(134)	(143)	(234)	(243)	(123)	(132)	(124)	(142)
(14)(23)	(1)	(12)(34)	(13)(24)	(14)(23)	(243)	(234)	(143)	(134)	(142)	(124)	(132)	(123)
(123)	(1)	(14)(23)	(12)(34)	(13)(24)	(123)	(132)	(234)	(243)	(142)	(124)	(143)	(134)
(132)	(1)	(13)(24)	(14)(23)	(12)(34)	(123)	(132)	(143)	(134)	(243)	(234)	(124)	(142)
(124)	(1)	(13)(24)	(14)(23)	(12)(34)	(243)	(234)	(124)	(142)	(123)	(132)	(143)	(134)
(142)	(1)	(14)(23)	(12)(34)	(13)(24)	(134)	(143)	(124)	(142)	(243)	(234)	(132)	(123)
(134)	(1)	(14)(23)	(12)(34)	(13)(24)	(243)	(234)	(132)	(123)	(134)	(143)	(124)	(142)
(143)	(1)	(13)(24)	(14)(23)	(12)(34)	(142)	(124)	(234)	(243)	(134)	(143)	(132)	(123)
(234)	(1)	(13)(24)	(14)(23)	(12)(34)	(134)	(143)	(132)	(123)	(142)	(124)	(234)	(243)
(243)	(1)	(14)(23)	(12)(34)	(13)(24)	(142)	(124)	(143)	(134)	(123)	(132)	(234)	(243)

Wir sehen hier: (12)(34), (13)(24), (14)(23) sind konjugiert, $(123), (134), (142), (243)$ sind konjugiert, $(132), (124), (143), (234)$ sind konjugiert. Aber (123) und (132) sind nicht konjugiert, obwohl sie in S_4 konjugiert sind.

DEFINITION. *Operiert die Gruppe G auf der Menge S, so heißt für $s \in S$*

$$G \cdot s = \{g \cdot s : g \in G\}$$

die **Bahn** *(oder der* **Orbit***) von s (unter G) oder die G-***Bahn** *von s. Die Menge*

$$G_s = \{g \in G : g \cdot s = s\}$$

heißt die **Fixgruppe** *(oder die* **Standgruppe** *oder die* **Isotropiegruppe** *oder der* **Stabilisator***) von s.*

Beispiel: Wir betrachten wieder die Operation von $G = A_4$ auf sich selbst durch Konjugation. Wir sehen folgende Bahnen:

$$\begin{aligned}
G \cdot (1) &= \{(1)\}, \\
G \cdot (12)(34) = G \cdot (13)(24) = G \cdot (14)(23) &= \{(12)(34), (13)(24), (14)(23)\}, \\
G \cdot (123) = G \cdot (134) = G \cdot (142) = G \cdot (243) &= \{(123), (134), (142), (243)\}, \\
G \cdot (132) = G \cdot (143) = G \cdot (124) = G \cdot (234) &= \{(132), (143), (124), (234)\}.
\end{aligned}$$

Folgende Fixgruppen ergeben sich:

$$\begin{aligned} G_{(1)} &= A_4, \\ G_{(12)(34)} = G_{(13)(24)} = G_{(14)(23)} &= \{(1), (12)(34), (13)(24), (14)(23)\}, \\ G_{(123)} = G_{(132)} &= \{(1), (123), (132)\}, \\ G_{(124)} = G_{(142)} &= \{(1), (124), (142)\}, \\ G_{(134)} = G_{(143)} &= \{(1), (134), (143)\}, \\ G_{(234)} = G_{(243)} &= \{(1), (234), (243)\}. \end{aligned}$$

Schaut man sich das Beispiel an, entdeckt man einige Gesetzmäßigkeiten, die im folgenden Lemma allgemein aufgeschrieben sind:

LEMMA. *Die Gruppe G operiere auf einer Menge S.*

(1) *Für $s, s' \in S$ gilt:*
$$s' \in G \cdot s \quad \Longrightarrow \quad G \cdot s' = G \cdot s.$$
(2) *Zwei Bahnen $G \cdot s'$ und $G \cdot s$ sind also identisch oder disjunkt:*
$$G \cdot s' = G \cdot s \text{ oder } G \cdot s' \cap G \cdot s = \emptyset.$$
(3) *Ist $s_i, i \in I$ ein Repräsentantensystem der Bahnen, dann ist*
$$S = \bigcup_{i \in I} G \cdot s_i \quad \text{mit} \quad G \cdot s_i \cap G \cdot s_j = \emptyset \text{ für } i \neq j$$
eine disjunkte Zerlegung von S in G-Bahnen.

Beweis: Ist $s' \in G \cdot s$, d.h. $s' = g' \cdot s$ für ein $g' \in G$, so gilt
$$G \cdot s' = \{gs' : g \in G\} = \{gg's : g \in G\} = \{gs : g \in G\} = G \cdot s.$$
Aus
$$G \cdot s_1 \cap G \cdot s_2 \neq \emptyset \text{ folgt dann } G \cdot s_1 = G \cdot s_2.$$
Der Rest ist dann klar. ■

Beispiel: Durch die Operation von A_4 auf sich selbst durch Konjugation wird A_4 in folgende vier Bahnen zerlegt:
$$A_4 = \{(1)\} \cup \{(12)(34), (13)(24), (14)(23)\} \cup \{(123), (134), (142), (243)\} \cup \{(132), (143), (124), (234)\}.$$

LEMMA. *G operiere auf der Menge S.*

(1) *Für $s \in S$ ist die Fixgruppe*
$$G_s = \{g \in G : g \cdot s = s\}$$
eine Untergruppe von G.
(2) *Liegen s_1, s_2 in der gleichen G-Bahn, d.h. gibt es ein $g_{21} \in G$ mit $s_2 = g_{21} \cdot s_1$, so gilt*
$$G_{s_2} = g_{21} G_{s_1} g_{21}^{-1},$$
die Fixgruppen G_{s_1} und G_{s_2} sind also konjugiert.
(3) *Ist G' eine Untergruppe von G, die konjugiert zur Fixgruppe G_s von s ist, d.h. gibt es ein $g' \in G$ mit $G' = g' G_s g'^{-1}$, so ist G' die Fixgruppe von $s' = g' \cdot s$.*

Beweis:

(1) Wir überprüfen die Untergruppeneigenschaften:
- Sind $g_1, g_2 \in G_s$, d.h. $g_1 \cdot s = s$ und $g_2 \cdot s = s$, so gilt $(g_1 g_2) \cdot s = g_1(g_2 \cdot s) = g_1 \cdot s = s$, also $g_1 g_2 \in S$.
- Ist $g \in G_s$, so folgt aus $g \cdot s = s$ die Gleichung $g^{-1} \cdot s = g^{-1} \cdot (g \cdot s) = (g^{-1} g) \cdot s = e \cdot s = s$, also gilt auch $g^{-1} \in G_s$.
- Wegen $e \cdot s = s$ gilt $e \in G_s$.

(2) Liegen s_1, s_2 in der gleichen G-Bahn, d.h. gibt es ein $g_{21} \in G$ mit $s_2 = g_{21} \cdot s_1$, so gilt:

$$\begin{aligned} g \in G_{s_2} &\iff g \cdot s_2 = s_2 \iff gg_{21} \cdot s_1 = g_{21} \cdot s_1 \iff \\ &\iff g_{21}^{-1} g g_{21} \cdot s_1 = s_1 \iff g_{21}^{-1} g g_{21} \in G_{s_1} \iff \\ &\iff g \in g_{21} G_{s_1} g_{21}^{-1}, \end{aligned}$$

also

$$G_{s_2} = g_{21} G_{s_1} g_{21}^{-1},$$

wie behauptet.

(3) Sei $G' = g' G_s g'^{-1}$. Dann gilt für $s' = g' \cdot s$

$$G_{s'} = g' G_s g'^{-1} = G',$$

also ist G' die Fixgruppe von s'. ■

LEMMA. *G operiere auf der Menge S. Sei $s \in S$. Dann ist die Abbildung*

$$G/G_s \to G \cdot s, \quad gG_s \mapsto g \cdot s$$

von den Linksnebenklassen von G_s in G in die Bahn von s wohldefiniert und bijektiv. Ist G endlich, so gilt insbesondere

$$|G \cdot s| = |G/G_s| = [G : G_s]$$

(Die Bahnlänge ist der Index der Fixgruppe), was man auch in der Form

$$|G \cdot s| \cdot |G_s| = |G|$$

schreiben kann. (Bahnlänge · Ordnung der Fixgruppe = Gruppenordnung.)

Beweis: Für $g, h \in G$ gilt:

$$g \cdot s = h \cdot s \iff h^{-1} g \cdot s = s \iff h^{-1} g \in G_s \iff gG_s = hG_s.$$

Also ist

$$G/G_s \to G \cdot s, \quad gG_s \mapsto g \cdot s$$

wohldefiniert und bijektiv. Daraus folgt auch der Rest. ■

Die Formel des folgenden Satzes heißt bei Lang **orbit decomposition formula**, bei Bosch und Fischer **Bahnengleichung**, bei Karpfinger/Meyberg **Anzahlformel**.

SATZ (Bahnengleichung - orbit decomposition formula). *Die endliche Gruppe operiere auf der endlichen Menge S. Sei $s_1, \ldots, s_r \in S$ ein Repräsentantensystem der Bahnen, d.h. wir haben die disjunkte Zerlegung*

$$S = \bigcup_{i=1}^{r} G \cdot s_i \quad \textit{mit} \quad G \cdot s_i \cap G \cdot s_j = \emptyset \textit{ für } i \neq j.$$

Dann gilt

$$|S| = \sum_{i=1}^{r} [G : G_{s_i}].$$

Beispiel: Wir betrachten $G = S_3$, also

$$G = \{(1), (12), (13), (23), (123), (132)\}$$

mit $|G| = 6$. Wir betrachten die 2-elementigen Teilmengen on G:

$$\begin{aligned} S = \Big\{ &\{(1),(12)\}, \{(1),(13)\}, \{(1),(23)\}, \{(1),(123)\}, \{(1),(132)\}, \\ &\{(12),(13)\}, \{(12),(23)\}, \{(12),(123)\}, \{(12),(132)\}, \\ &\{(13),(23)\}, \{(13),(123)\}, \{(13),(132)\}, \\ &\{(23),(123)\}, \{(23),(132)\}, \\ &\{(123),(132)\} \Big\}. \end{aligned}$$

Wir lassen G auf S durch Multiplikation von links operieren, d.h.

$$(\sigma, \{\tau_1, \tau_2\}) \mapsto \sigma \cdot \{\tau_1, \tau_2\} = \{\sigma\tau_1, \sigma\tau_2\}.$$

Wegen

$$(\sigma\rho)\{\tau_1, \tau_2\} = \{\sigma\rho\tau_1, \sigma\rho\tau_2\} = \sigma\left(\rho\{\tau_1, \tau_2\}\right) \quad \text{und} \quad e\{\tau_1, \tau_2\} = \{e\tau_1, e\tau_2\} = \{\tau_1, \tau_2\}$$

ist dies tatsächlich eine Operation. Nun bestimmen wir Bahnen:

$$\begin{aligned}
G \cdot \{(1),(12)\} &= \Big\{\{(1),(12)\}, \{(13),(123)\}, \{(23),(132)\}\Big\}, \\
G \cdot \{(1),(13)\} &= \Big\{\{(1),(13)\}, \{(12),(132)\}, \{(23),(123)\}\Big\}, \\
G \cdot \{(1),(23)\} &= \Big\{\{(1),(23)\}, \{(12),(123\}, \{(13),(132)\}\Big\}, \\
G \cdot \{(1),(123)\} &= \Big\{\{(1),(123)\}, \{(1),(132)\}, \{(12),(13)\}, \{(12),(23)\}, \{(13),(23)\}, \{(123),(132)\}\Big\}
\end{aligned}$$

Die zugehörigen Fixgruppen sind

$$G_{\{(1),(12)\}} = \langle(12)\rangle, \quad G_{\{(1),(13)\}} = \langle(13)\rangle, \quad G_{\{(1),(23)\}} = \langle(23)\rangle, \quad G_{\{(1),(123)\}} = \{(1)\}.$$

Wir verallgemeinern das letzte Beispiel und beweisen damit einen wichtigen Satz. Zuvor folgen zwei Definitionen:

DEFINITION. *Sei p eine Primzahl.*

(1) *Eine* **p-Gruppe** *ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist, also $|G| = p^\ell$.*
(2) *Ist G eine endliche Gruppe und p ein Primteiler der Gruppenordnung, so kann man schreiben $|G| = p^\ell m$ mit $\ell \geq 1$ und $p \nmid m$. Eine Untergruppe $S \subseteq G$ heißt eine* **p-Sylowgruppe** *(oder* **p-Sylowuntergruppe***) von G, falls $|S| = p^\ell$ gilt. (Anders ausgedrückt: Eine p-Sylowgruppe von G ist eine p-Untergruppe von G, deren Index in G teilerfremd zu p ist.)*

Beispiel: Es ist $|S_3| = 6 = 2 \cdot 3$. Die 2-Sylowgruppen von S_3 sind

$$\{(1),(12)\}, \quad \{(1),(13)\}, \quad \{(1),(23)\}.$$

Es gibt genau eine 3-Sylowgruppe, nämlich

$$\{(1),(123),(132)\}.$$

Wir beginnen mit einem Lemma.

LEMMA. *Sei $n \in \mathbb{N}$ und p ein Primteiler von n, sodass wir zerlegen können $n = p^\ell \cdot m$ mit $\ell \geq 1$ und $p \nmid m$. Dann ist der Binomialkoeffizient*

$$\binom{n}{p^\ell} = \binom{p^\ell \cdot m}{p^\ell}$$

nicht durch p teilbar.

Beweis: Wir formen um:

$$\begin{aligned}
\binom{p^\ell m}{p^\ell} &= \frac{p^\ell m \cdot (p^\ell m - 1) \cdot (p^\ell m - 2) \ldots (p^\ell m - (p^\ell - 1))}{p^\ell \cdot (p^\ell - 1) \cdot (p^\ell - 2) \ldots 1} = \prod_{0 \leq i \leq p^\ell - 1} \frac{p^\ell m - i}{p^\ell - i} = \\
&= m \cdot \prod_{1 \leq i \leq p^\ell - 1} \frac{p^\ell m - i}{p^\ell - i}.
\end{aligned}$$

Für $1 \leq i \leq p^\ell - 1$ ist $v_p(i) \leq \ell - 1$, und damit $v_p(i) < v_p(p^\ell m) = v_p(p^\ell)$, also

$$v_p(p^\ell m - i) = \min(v_p(p^\ell m), v_p(i)) = v_p(i) \quad \text{und} \quad v_p(p^\ell - i) = \min(v_p(p^\ell), v_p(i)) = v_p(i),$$

sodass gilt

$$v_p\left(\frac{p^\ell m - i}{p^\ell - i}\right) = 0.$$

Daraus folgt sofort

$$v_p\left(\binom{p^\ell m}{p^\ell}\right) = 0,$$

was gezeigt werden sollte. ■

LEMMA. *Sei G eine endliche Gruppe, p ein Teiler der Gruppenordnung, $|G| = p^\ell m$ mit $p \nmid m$. Sei S die Menge aller p^ℓ-elementigen Teilmengen von G, also*

$$S = \{A \subseteq G : |A| = p^\ell\} \quad \textit{mit} \quad |S| = \binom{p^\ell m}{p^\ell}.$$

G operiert auf S durch Multiplikation von links:

$$(g, A) \mapsto gA = \{ga : a \in A\}.$$

(1) *Für die Fixgruppe G_A einer Menge $A \in S$ gilt:*

$$G_A = \{g \in G : gA = A\} \quad \textit{und} \quad |G_A| \leq p^\ell.$$

(2) *Ist für $A \in S$ die Bahnlänge $|G \cdot A|$ nicht durch p teilbar, so gilt*

$$|G_A| = p^\ell,$$

d.h. G_A ist eine p-Sylowuntergruppe von G.

(3) *$|S|$ ist nicht durch p teilbar, also gibt es eine Menge $A \in S$ mit*

$$|G_A| = p^\ell.$$

Beweis:

(0) Ist $g \in G$ und $A \in S$, d.h. $A \subseteq G$ mit $|A| = p^\ell$, so hat auch $gA = \{ga : a \in A\}$ genau p^ℓ Elemente. Also erhalten wir durch Linksmultiplikation eine Operation von G auf S:

$$(g, A) \mapsto gA,$$

da die Eigenschaften

$$(gh)A = \{gha : a \in A\} = g(hA) \quad \text{und} \quad eA = A$$

klar sind.

(1) Die Fixgruppe von A ist nach Definition

$$G_A = \{g \in G : gA = A\}.$$

Ist $A = \{a_1, \ldots, a_{p^\ell}\}$, so gibt es zu $g \in G_A$ einen Index i mit $ga_1 = a_i$, also $g = a_i a_1^{-1}$. Es folgt

$$G_A \subseteq \{a_i a_1^{-1} : 1 \leq i \leq p^\ell\},$$

und damit insbesondere

$$|G_A| \leq p^\ell.$$

(2) Die Ordnung der Fixgruppe von $A \in S$ können wir zerlegen

$$|G_A| = p^{\ell'} m' \text{ mit } p \nmid m' \text{ und } \ell' \leq \ell \text{ und } m' \mid m.$$

Die Bahnlänge von A ist der Index der Fixgruppe, also

$$|G \cdot A| = [G : G_A] = \frac{|G|}{|G_A|} = p^{\ell - \ell'} \cdot \frac{m}{m'}.$$

Ist die Bahnlänge nicht durch p teilbar, so folgt $\ell' = \ell$, also $|G_A| = p^\ell m'$. Mit $|G_A| \leq p^\ell$ ergibt sich $m' = 1$, und damit

$$|G_A| = p^\ell.$$

(3) Sei $A_i, i \in I$, ein Repräsentantensystem der Bahnen. Dann gilt also

$$|S| = \bigcup_{i\in I} G \cdot A_i \text{ mit } G \cdot A_i \cap G \cdot A_j = \emptyset \text{ für } i \neq j,$$

und damit

$$|S| = \sum_{i\in I} |G \cdot A_i|.$$

Das vorangegangene Lemma besagt, dass $|S|$ nicht durch p teilbar ist, d.h. $p \nmid |S|$. Dann gibt es aber auch mindestens einen Index i mit $p \nmid |G \cdot A_i|$. Teil (2) liefert dann, dass die Fixgruppe von A_i genau p^ℓ Elemente hat, also

$$|G_{A_i}| = p^\ell,$$

wie behauptet. ■

Wir formulieren das wichtige Ergebnis nochmals als Satz:

SATZ. *Ist G eine endliche Gruppe, so gibt es zu jedem Primteiler p der Gruppenordnung mindestens eine p-Sylowgruppe. Ausführlich: Gilt $p \mid |G|$, zerlegt man $|G| = p^\ell m$ mit $p \nmid m$, so gibt es (mindestens) eine Untergruppe $P \subseteq G$ mit p^ℓ Elementen.*

Beispiel: Ist G eine endliche Gruppe mit 48 Elementen, so enthält wegen $48 = 2^4 \cdot 3$ die Gruppe G jeweils mindestens eine Untergruppe der Ordnung 16 und 3.

Wir beweisen mit der letzten Erkenntnis einen Struktursatz für Gruppen der Ordnung $2p$ (mit einer Primzahl $p \geq 3$).

Bemerkung: Folgende Gruppen der Ordnung $2p$ (mit einer Primzahl $p \geq 3$) kennen wir bereits:

(1) Zyklische Gruppen der Ordnung $2p$. Sie sind alle isomorph zur additiv geschriebenen Gruppe $\mathbb{Z}_{2p}$. Wir haben auch bereits gesehen, dass man $\mathbb{Z}_{2p}$ als Produkt schreiben kann: $\mathbb{Z}_{2p} \simeq \mathbb{Z}_2 \times \mathbb{Z}_p$.

(2) Die Diedergruppe D der Ordnung $2p$ wird erzeugt von Elementen δ und σ mit

$$\operatorname{ord}(\delta) = p, \quad \operatorname{ord}(\sigma) = 2 \quad \text{und der Relation} \quad \sigma\delta\sigma^{-1} = \delta^{-1}.$$

Es ist

$$D = \{\delta^i : 0 \leq i \leq p-1\} \cup \{\delta^i\sigma : 0 \leq i \leq p-1\}.$$

Die Ordnung der Elemente:

- $\delta^0 = e$ hat Ordnung 1.
- Die p Elemente $\delta^i\sigma$ mit $0 \leq i \leq p-1$ haben alle Ordnung 2.
- Die $p-1$ Elemente δ^i mit $1 \leq i \leq p-1$ haben alle Ordnung p.

Der folgende Satz sagt, dass es bis auf Isomorphie keine anderen Gruppen der Ordnung $2p$ gibt.

SATZ. *Ist $p \geq 3$ eine Primzahl und G eine Gruppe der Ordnung $2p$, so ist G isomorph zur zyklischen Gruppe mit $2p$ Elementen oder isomorph zur Diedergruppe mit $2p$ Elementen, also*

$$G \simeq \langle g \rangle \quad \textit{mit} \quad \operatorname{ord}(g) = 2p$$

oder

$$G \simeq \langle \delta, \sigma \rangle \quad \textit{mit} \quad \operatorname{ord}(\delta) = p, \quad \operatorname{ord}(\sigma) = 2, \quad \sigma\delta\sigma^{-1} = \delta^{-1}.$$

Beweis: Nach dem vorangegangenen Satz enthält G Untergruppen der Ordnung 2 und p. Da 2 und p Primzahlen sind, sind diese Untergruppen zyklisch, d.h. es gibt $\sigma, \delta \in G$ mit

$$\operatorname{ord}(\sigma) = 2 \quad \text{und} \quad \operatorname{ord}(\delta) = p.$$

Da die Untergruppe $\langle\delta\rangle$ Ordnung p hat, hat sie Index 2 in G, ist also Normalteiler. Insbesondere bedeutet dies

$$\sigma\langle\delta\rangle\sigma^{-1} \subseteq \langle\delta\rangle.$$

Es gibt also ein $k \in \mathbb{Z}$ mit

$$\sigma\delta\sigma^{-1} = \delta^k.$$

Nun gilt wegen $\sigma^2 = e$

$$\delta = \sigma^2\delta\sigma^{-2} = \sigma(\sigma\delta\sigma^{-1})\sigma^{-1} = \sigma\delta^k\sigma^{-1} = \left(\sigma\delta\sigma^{-1}\right)^k = \left(\delta^k\right)^k = \delta^{k^2}.$$

Wegen $\operatorname{ord}(\delta) = p$ unter sich die Exponenten 1 und k^2 um ein Vielfaches von p, d.h. $p \mid k^2 - 1$, und damit $p \mid (k-1)(k+1)$. Da p eine Primzahl ist, gibt es zwei Möglichkeiten:

- **Fall $p \mid k-1$:** Da sich k und 1 um ein Vielfaches von p unterscheiden, gilt $\delta^1 = \delta^k$, und damit
$$\sigma\delta\sigma^{-1} = \delta, \quad \text{also} \quad \sigma\delta = \delta\sigma.$$
Durch Induktion sieht man, dass $(\delta\sigma)^i = \delta^i\sigma^i$ für alle $i \geq 1$ gilt. Damit gilt
$$(\delta\sigma)^{2p} = \delta^{2p}\sigma^{2p} = e, \quad (\delta\sigma)^p = \delta^p\sigma^p = \sigma^p = \sigma \neq e, \quad (\delta\sigma)^2 = \delta^2\sigma^2 = \delta^2 \neq e,$$
woraus
$$\operatorname{ord}(\delta\sigma) = 2p$$
folgt. Es ist also $G = \langle\delta\sigma\rangle$, d.h. G ist zyklisch.
- **Fall $p \mid k+1$:** Da sich k und -1 um ein Vielfaches von p unterschieden, gilt $\delta^k = \delta^{-1}$, und damit
$$\sigma\delta\sigma^{-1} = \delta^{-1}.$$
Mit $\operatorname{ord}(\delta) = p$ und $\operatorname{ord}(\sigma) = 2$ ist damit klar, dass G eine Diedergruppe der Ordnung $2p$ ist.

Damit ist der Satz bewiesen. ■

DEFINITION. *G sei eine Gruppe, die auf einer Menge S operiert.*

(1) *Operiert eine Gruppe G auf einer Menge S, so heißt $s \in S$ ein* **Fixpunkt**, *falls $gs = s$ für alle $g \in G$ gilt. Äquivalent dazu ist*
$$G_s = G \quad \textit{und} \quad Gs = \{s\}.$$

(2) *G operiert* **transitiv** *auf S, wenn es nur eine G-Bahn gibt, d.h. wenn für ein beliebiges $s \in S$ gilt*
$$S = G \cdot s = \{g \cdot s : g \in G\}.$$

Bemerkung: Ist G eine Untergruppe der symmetrischen Gruppe S_n, so operiert natürlich G auch auf $\{1, \ldots, n\}$. Man sagt, G ist eine **transitive Untergruppe** von S_n, wenn $\{1, \ldots, n\}$ eine G-Bahn unter dieser Operation ist.

Beispiel: Wir betrachten Untergruppen der S_4:

- $A_4 = \{(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$ ist eine transitive Untergruppe von S_4.
- $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ ist eine transitive Untergruppe der S_4.
- $\{(1), (12)(34)\}$ ist keine transitive Untergruppe - die Bahnen sind $\{1, 2\}$ und $\{3, 4\}$, hat aber keinen Fixpunkt.
- $\{(1), (123), (132)\}$ ist keine transitive Untergruppe von S_4 - die Bahnen sind $\{1, 2, 3\}$ und $\{4\}$ - und hat den Fixpunkt 4.

Die Formel des folgenden Satz heißt bei Lang **class formula**, bei Bosch, Fischer und Karpfinger/Meyberg **Klassengleichung**.

SATZ. *G sei eine endliche Gruppe. Sie operiere auf sich selbst durch Konjugation, d.h. $(h, g) \mapsto hgh^{-1}$.*

(1) *Die Fixpunkte der Operation sind genau die Elemente des Zentrums $Z(G) = \{g \in G : gh = hg$ für alle $h \in G\}$, d.h.*
$$\{g \in G : hgh^{-1} = g \textit{ für alle } h \in G\} = Z(G).$$

(2) *Sei $g_1, \ldots, g_r$ ein Repräsentantensystem der Bahnen (Konjugationsklassen), die nicht nur aus einem Element bestehen, d.h. für die Fixgruppen $G_{g_i} = \{g \in G : gg_ig^{-1} = g_i\}$ gilt $[G : G_{g_i}] \geq 2$. Dann gilt die* **Klassengleichung** *(**class formula**)*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : G_{g_i}].$$

Beweis:

(1) Für $g \in G$ gilt:

$$\begin{aligned} g \text{ ist Fixpunkt der Operation} &\iff G_g = \{h \in G : hgh^{-1} = g\} = G \iff \\ &\iff gh = hg \text{ für alle } h \in G \iff \\ &\iff g \in Z(G). \end{aligned}$$

(2) G wird durch die Operation in disjunkte Bahnen zerlegt:

$$G = \bigcup_{g \in Z(g)} \{g\} \cup \bigcup_{1 \leq i \leq r} \text{Bahn}(g_i) = Z(G) \cup \bigcup_{1 \leq i \leq r} \text{Bahn}(g_i),$$

woraus

$$|G| = |Z(G)| + \sum_{i=1}^{r} |\text{Bahn}(g_i)| = |Z(G)| + \sum_{i=1}^{r} [G : G_i]$$

folgt, wie behauptet. ■

Als Folgerung erhalten wir:

Satz. *Ist G eine p-Gruppe, d.h. $|G| = p^\ell$ für ein $\ell \in \mathbb{N}$, so gilt $Z(G) \neq \{e\}$, d.h. das Zentrum besteht nicht nur aus dem neutralen Element.*

Beweis: Wir betrachten die Klassengleichung:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : G_{g_i}] \quad \text{mit} \quad [G : G_{g_i}] \geq 2.$$

Wegen $|G| = p^\ell$ (für ein $\ell \geq 1$) und $[G : G_{g_i}] \geq 2$ gilt auch $p \mid [G : G_{g_i}]$. Mit $p \mid |G|$ folgt auch $p \mid |Z(G)|$, und damit die Behauptung. ■

Mit dem vorangegangenen Satz können wir Gruppen der Ordnung p^2 klassifizieren:

Satz. *Ist G eine Gruppe mit p^2 Elementen, wobei p eine Primzahl ist, so gilt*

$$G \simeq \mathbb{Z}_{p^2} \quad \text{oder} \quad G \simeq \mathbb{Z}_p \times \mathbb{Z}_p.$$

G ist also zyklisch oder isomorph zum Produkt zweier zyklischer Gruppen der Ordnung p. Insbesondere ist G abelsch.

Beweis:

(1) Wir zeigen zunächst, dass jede Gruppe G der Ordnung p^2 eine abelsche Gruppe ist.

- Da das Zentrum $Z(G)$ eine Untergruppe von G ist, gilt

$$|Z(G)| \in \{1, p, p^2\}.$$

Gerade haben wir gezeigt, dass die Ordnung des Zentrum nicht 1 sein kann, also folgt

$$|Z(G)| \in \{p, p^2\}.$$

- Wir betrachten den Fall, dass $|Z(G)| = p$ ist. Dann hat $G/Z(G)$ Ordnung p, ist also zyklisch von Ordnung p. Wir haben aber schon gesehen, dass aus „$G/Z(G)$ zyklisch“ die Aussage „G abelsch“ folgt. Dies impliziert $Z(G) = G$ und damit $|Z(G)| = p^2$. Also ist der Fall $|Z(G)| = p$ nicht möglich.

- Damit bleibt nur die Möglichkeit $|Z(G)| = p^2$, d.h. $Z(G) = G$. G ist also eine abelsche Gruppe.

(2) Ist $a \in G$, so gilt $\operatorname{ord}(a) \mid p^2$, also $\operatorname{ord}(a) \in \{1, p, p^2\}$. Wir unterscheiden zwei Möglichkeiten:

- Gibt es ein $a \in G$ mit $\operatorname{ord}(a) = p^2$, so ist $G = \langle a \rangle$. G ist also zyklisch von Ordnung, und damit
$$G \simeq \mathbb{Z}_{p^2}.$$
- Es bleibt nur noch der Fall, dass alle vom neutralen Element verschiedenen Elemente Ordnung p haben. Wir wählen $a \in G \setminus \{e\}$. Dann ist $\langle a \rangle$ eine Untergruppe der Ordnung p. Wir wählen $b \in G \setminus \langle a \rangle$. Es gilt $\operatorname{ord}(b) = p$. Wegen
$$\langle a \rangle \subsetneq \langle a, b \rangle \subseteq G$$
folgt
$$G = \langle a, b \rangle.$$
Wir definieren
$$\phi : \mathbb{Z}_p \times \mathbb{Z}_p \to G, \quad (i, j) \mapsto a^i b^j$$
und zeigen, dass ϕ ein Gruppenhomomorphismus ist:
$$\begin{aligned}
\phi((i_1, j_1) +_{\bmod p} (i_2, j_2)) &= \phi((i_1 +_{\bmod p} i_2, j_1 +_{\bmod p} j_2)) = \\
&= \phi((i_1 + i_2) \bmod p, (j_1 + j_2) \bmod p) = \\
&= \phi((i_1 + i_2 - \left\lfloor \frac{i_1 + i_2}{p} \right\rfloor p, j_1 + j_2 - \left\lfloor \frac{j_1 + j_2}{p} \right\rfloor p) = \\
&= a^{i_1 + i_2 - \lfloor \frac{i_1 + i_2}{p} \rfloor p} b^{j_1 + j_2 - \lfloor \frac{j_1 + j_2}{p} \rfloor p} = a^{i_1 + i_2} b^{j_1 + j_2} = \\
&= a^{i_1} b^{j_1} \cdot a^{i_2} b^{j_2} = \phi((i_1, j_1)) \cdot \phi((i_2, j_2)).
\end{aligned}$$
Da ϕ surjektiv ist und $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2 = |G|$ gilt, ist ϕ bijektiv, also ein Isomorphismus:
$$G \simeq \mathbb{Z}_p \times \mathbb{Z}_p.$$
Damit haben wir alle Behauptungen bewiesen. ■

Eine andere Folgerung aus der Nichttrivialität des Zentrums einer p-Gruppe ist folgender Satz:

SATZ. *Jede p-Gruppe ist auflösbar. Genauer: Ist G eine Gruppe der Ordnung p^n (mit einer Primzahl p und $n \in \mathbb{N}$), so existieren für $i = 0, \ldots, n$ Untergruppen G_i der Ordnung p^i, sodass G_i normal in G_{i+1} und G_{i+1}/G_i zyklisch von Ordnung p ist:*
$$G = G_n \supseteq G_{n-1} \supseteq G_{n-2} \supseteq \cdots \supseteq G_2 \supseteq G_1 \supseteq G_0 = \{e\} \quad \textit{mit} \quad |G_i| = p^i \quad \textit{und} \quad G_i/G_{i+1} \simeq \mathbb{Z}_p.$$

Beweis: Wir beweisen dies durch Induktion nach n (mit $|G| = p^n$). Für $n = 1$ ist die Aussage klar. Sei also $n \geq 2$ und die Aussage bereits für alle p-Gruppen mit einer Ordnung $< p^n$ bewiesen. Da $Z(G)$ nichttrivial ist, enthält $Z(G)$ ein Element a der Ordnung p. Dann ist $G_1 = \langle a \rangle$ eine Gruppe der Ordnung p, die auch ein Normalteiler ist, da a im Zentrum liegt. Die Faktorgruppe G/G_1 hat Ordnung p^{n-1}. Nach Induktionsvoraussetzung gibt es Untergruppen
$$G/G_1 = \overline{G}_n \supseteq \overline{G}_{n-1} \supseteq \cdots \supseteq \overline{G}_2 \supseteq \overline{G}_1 = \{\overline{e}\}$$
mit $|\overline{G}_i| = p^{i-1}$, sodass $\overline{G}_i$ normal in $\overline{G}_{i+1}$ ist mit $\overline{G}_{i+1}/\overline{G}_i \simeq \mathbb{Z}_p$. Ist $\pi : G \to G/G_1$ die kanonische Abbildung, definiert man $G_i = \pi^{-1}(\overline{G}_i)$ für $i = 2, \ldots, n$, so erhält man das gewünschte Ergebnis nach einem Lemma, das bei der Behandlung der Normalreihen bewiesen wurde. ■

Beispiel: Für die Diedergruppe D der Ordnung 8, also
$$D = \langle \delta, \sigma \rangle \quad \text{mit} \quad \operatorname{ord}(\delta) = 4, \quad \operatorname{ord}(\sigma) = 2, \quad \sigma\delta\sigma^{-1} = \delta^{-1}$$
ist
$$D \supseteq \langle \delta \rangle \supseteq \langle \delta^2 \rangle \supseteq \{e\}$$
eine Normalreihe mit Faktoren isomorph zu $\mathbb{Z}_2$.

Eine Gruppe operiert durch Multiplikation auf den Linksnebenklassen einer Untergruppe. Damit konstruieren wir einen Gruppenhomomorphismus:

LEMMA. *Sei G eine Gruppe und H eine Untergruppe vom Index n. Seien $g_1, \dots, g_n \in G$ mit $G/H = \{g_1H, \dots, g_nH\}$ und $H_i = g_iH$, sodass*

$$G/H = \{H_1, \dots, H_n\}$$

gilt. Dann gilt:

(1) *Für jedes $g \in G$ gibt es ein $\phi(g) \in S_n$, sodass gilt*

$$gH_i = H_{\phi(g)(i)} \text{ für } i = 1, \dots, n.$$

(2) *$\phi : G \to S_n$ ist ein Gruppenhomomorphismus.*
(3) *$\phi(G)$ ist eine transitive Untergruppe von S_n.*
(4) *Es ist*

$$\mathrm{Kern}(\phi) = \bigcap_{i=1}^{n} g_iHg_i^{-1} = \bigcap_{g \in G} gHg^{-1},$$

und insbesondere $\mathrm{Kern}(\phi) \subseteq H$.

Beweis:

(1) Für $g \in G$ ist $gH_i = gg_iH$ eine Linksnebenklasse von H in G, also existiert ein Index j mit $gg_iH = g_jH$. Wir definieren $\phi(g) : \{1, \dots, n\} \to \{1, \dots, n\}$ durch $\phi(g)(i) = j$, also

$$gH_i = H_{\phi(g)(i)}.$$

Wir müssen noch zeigen, dass $\phi(g)$ bijektiv ist. Sei $\phi(g)(i) = \phi(g)(j)$, d.h. $gH_i = gH_j$. Dann folgt aber $H_i = H_j$, also $i = j$, was die Injektivität von $\phi(g)$, und damit die Bijektivität zeigt. Also ist $\phi(g) \in S_n$.

(2) Wir zeigen, dass $\phi : G \to S_n$ ein Gruppenhomomorphismus ist: Aus

$$H_{\phi(gh)(i)} = ghH_i = g(hH_i) = gH_{\phi(h)(i)} = H_{\phi(g)(\phi(h)(i))} = H_{(\phi(g) \circ \phi(h))(i)}$$

folgt $\phi(gh)(i) = (\phi(g) \circ \phi(h))(i)$, also

$$\phi(gh) = \phi(g) \circ \phi(h).$$

(3) Es gilt für $i, j \in \{1, \dots, n\}$

$$H_{\phi(g_jg_i^{-1})(i)} = g_jg_i^{-1}H_i = g_jg_i^{-1}g_iH = g_jH = H_j,$$

also

$$\phi(g_jg_i^{-1})(i) = j.$$

Insbesondere ist $\phi(G)$ eine transitive Untergruppe von S_n.

(4) Für $g \in G$ gilt:

$$\begin{aligned}
g \in \mathrm{Kern}(\phi) &\iff \phi(g) = \mathrm{id} \iff gH_i = H_i \text{ für } i = 1, \dots, n \iff \\
&\iff gg_iH = g_iH \text{ für } i = 1, \dots, n \iff \\
&\iff g_i^{-1}gg_iH = H \text{ für } i = 1, \dots, n \iff \\
&\iff g_i^{-1}gg_i \in H \text{ für } i = 1, \dots, n \iff \\
&\iff g \in g_iHg_i^{-1} \text{ für } i = 1, \dots, n \iff \\
&\iff g \in \bigcap_{1 \le i \le n} g_iHg_i^{-1}.
\end{aligned}$$

Daher ist

$$\mathrm{Kern}(\phi) = \bigcap_{1 \le i \le n} g_iHg_i^{-1}.$$

Ist $g \in G$, so gibt es ein g_i mit $g = g_ih$. Dann ist

$$gHg^{-1} = (g_ih)H(g_ih)^{-1} = g_i(hHh^{-1})g_i^{-1} = g_iHg_i^{-1}.$$

Also können wir auch schreiben

$$\mathrm{Kern}(\phi) = \bigcap_{g \in G} gHg^{-1}.$$

Aus dieser Darstellung sieht man auch die Beziehung $\mathrm{Kern}(\phi) \subseteq H$. ■

Im Spezialfall $H = \{e\}$ erhalten wir folgenden Satz:

SATZ. *Sei G eine endliche Gruppe der Ordnung n. Wir schreiben $G = \{g_1, \ldots, g_n\}$. Für jedes $g \in G$ gibt es dann ein $\phi(g) \in S_n$ mit*

$$gg_i = g_{\phi(g)(i)}.$$

Dann ist

$$\phi : G \to S_n$$

ein injektiver Gruppenhomomorphismus und das Bild eine transitive Untergruppe von S_n. (Jede endliche Gruppe der Ordnung n ist also isomorph zu einer transitiven Untergruppe von S_n.)

Beweis: Mit $H = \{e\}$ liefert der vorangegangene Satz $\mathrm{Kern}(\phi) \subseteq H = \{e\}$, also $\mathrm{Kern}(\phi) = \{e\}$. Also ist ϕ eine Einbettung. Der Rest steht schon im Satz. ■

Beispiel: Wir betrachten

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\},$$

wobei wir G additiv schreiben. Wir nummerieren die Elemente:

$$g_1 = (0,0), \quad g_2 = (0,1), \quad g_3 = (1,0), \quad g_4 = (1,1)$$

und erstellen eine Verknüpfungstabelle:

$+$	$g_1 = (0,0)$	$g_2 = (0,1)$	$g_3 = (1,0)$	$g_4 = (1,1)$
$g_1 = (0,0)$	$g_1 = (0,0)$	$g_2 = (0,1)$	$g_3 = (1,0)$	$g_4 = (1,1)$
$g_2 = (0,1)$	$g_2 = (0,1)$	$g_1 = (0,0)$	$g_4 = (1,1)$	$g_3 = (1,0)$
$g_3 = (1,0)$	$g_3 = (1,0)$	$g_4 = (1,1)$	$g_1 = (0,0)$	$g_2 = (0,1)$
$g_4 = (1,1)$	$g_4 = (1,1)$	$g_3 = (1,0)$	$g_2 = (0,1)$	$g_1 = (0,0)$

Daher ist

$$\phi((0,0)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1), \quad \phi((0,1)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34),$$

$$\phi((1,0)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24), \quad \phi((1,1)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23).$$

Daher ist

$$\phi(G) = \{(1), (12)(34), (13)(24), (14)(23)\}$$

die uns bereits bekannte Kleinsche Vierergruppe V.

Weitere Beispiele für Gruppenoperationen:

(1) **Operation durch Konjugation**

(a) **G operiert auf den nichtleeren Teilmengen von G durch Konjugation:** Wir definieren

$$g * S = gSg^{-1} \text{ für } g \in G \text{ und } S \subseteq G.$$

Mit den Rechenregeln für Produkte von Teilmengen zeigen wir, dass dies eine Operation ist:

$$(gh) * S = (gh)S(gh)^{-1} = ghSh^{-1}g^{-1} = g(hSh^{-1})g^{-1} = g(h * S)g^{-1} = g * (h * S)$$

und

$$e * S = eSe^{-1} = S.$$

(b) G **operiert auf Untergruppen von G durch Konjugation:** Da für $g \in G$ die Abbildung $G \to G$, $x \mapsto gxg^{-1}$ ein Automorphismus ist, ist mit U auch gUg^{-1} eine Untergruppe. Wir definieren

$$g * U = gUg^{-1}.$$

Natürlich ist dies auch eine Operation, da Untergruppen auch Teilmengen von G sind. Zwei Untergruppen U, V nennt man **konjugiert**, wenn es ein $g \in G$ gibt mit $V = gUg^{-1}$. Die Fixgruppe einer Untergruppe U nennt man den **Normalisator** $N_G(U)$:

$$N_G(U) = \{g \in G : gUg^{-1} = U\}.$$

Ist G endlich, so ist also die Anzahl der zu U konjugierten Untergruppen der Index $[G : N_G(U)]$ des Normalisators in G.

(2) **Operation durch Linksmultiplikation bzw. Translation**

(a) G **operiert auf sich selbst durch Linksmultiplikation:** Wir definieren

$$g * s = gs.$$

Trivialerweise ist dies eine Operation.

(b) G **operiert auf nichtleeren Teilmengen von G durch Linksmultiplikation:** Wir definieren

$$g * S = gS \text{ für } g \in G \text{ und } S \subseteq G.$$

Dies ist eine Operation:

$$(gh) * S = (gh)S = g(hS) = g * (h * S) \quad \text{und} \quad e * S = eS = S.$$

Schreibt man die Verknüpfung von G als Addition $+$, so spicht man auch von „Translation“ statt „Linksmultiplikation“:

$$g * S = g + S \text{ für } g \in G \text{ und } S \subseteq G.$$

(c) G **operiert auf den Linksnebenklassen einer Untergruppe H durch Linksmultiplikation:** Sei $G/H = \{aH : a \in G\}$. Dann sei

$$g * (aH) = gaH.$$

Wegen

$$(gh) * (aH) = (gh)(aH) = (gha)H = g * (h * aH) \quad \text{und} \quad e * (aH) = eaH = aH$$

ist dies eine Operation.

Das folgende Lemma zeigt, dass eine Operation von G auf S eigentlich nichts anderes als ein Gruppenhomomorphismus $G \to \mathfrak{S}(S)$ ist.

LEMMA. *Sei G eine Gruppe und S eine Menge.*

(1) *G operiere auf der Menge S vermöge $(g, s) \mapsto g * s$. Für $g \in G$ werde definiert*

$$\phi_g : S \to S \text{ mit } \phi_g(s) = g * s.$$

Dann gilt:

(a) *Für $g, h \in G$ gilt:*

$$\phi_g \circ \phi_h = \phi_{gh}, \quad \phi_e = \mathrm{id}_S, \quad \phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \mathrm{id}_S.$$

(b) *Die Abbildung*

$$\Phi : G \to \mathfrak{S}(S), \quad g \mapsto \phi_g$$

ist ein Gruppenhomomorphismus und es gilt für $g \in G$, $s \in S$

$$\Phi(g)(s) = g * s.$$

(2) *Ist $\Phi : G \to \mathfrak{S}(S)$ ein Gruppenhomomorphismus, so wird durch*

$$g * s = \Phi(g)(s)$$

eine Operation von G auf S definiert.

Beweis:

(1) (a) Es gilt

$$(\phi_g * \phi_h)(s) = \phi_g(\phi_h(s)) = \phi_g(h * s) = g * (h * s) = (gh) * s = \phi_{gh}(s),$$

was $\phi_g \circ \phi_h = \phi_{gh}$ beweist.

$$\phi_e(s) = e * s = s = \mathrm{id}_S(s)$$

zeigt $\phi_e = \mathrm{id}$. Mit diesen beiden Regeln folgt nun

$$\phi_g \circ \phi_{g^{-1}} = \phi_{gg^{-1}} = \phi_e = \mathrm{id}_S \quad \text{und} \quad \phi_{g^{-1}} \circ \phi_g = \phi_{g^{-1}g} = \phi_e = \mathrm{id}_S.$$

Dies zeigt die dritte Formel.

(b) Aus der dritten Formel folgt, dass ϕ_g bijektiv ist. Also ist $\Phi : G \to \mathfrak{S}(S)$ wohldefiniert. Wegen

$$\Phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \Phi(g) \circ \Phi(h)$$

ist Φ ein Gruppenhomomorphismus. Die Eigenschaft $\Phi(g)(s) = \phi_g(s) = g * s$ ist klar.

(2) Seien $g, h \in G$ und $s \in S$. Dann gilt

$$g * (h * s) = g * \Phi(h)(s) = \Phi(g)(\Phi(h)(s)) = (\Phi(g) \circ \Phi(h))(s) = \Phi(gh)(s) = (gh) * s$$

und

$$e * s = \Phi(e)(s) = \mathrm{id}_S(s) = s.$$

Also wird durch $g * s$ eine Operation von G auf S definiert. ■