- wohldefiniert,
- ein Gruppen-Homomorphismus,
- injektiv und surjektiv ist. (Dies ist eine Anwendung vom Satz 2.4.1.) Siehe die Aufgaben (Blatt 6). ■

3.2 Operationen von Gruppen auf Mengen und Faktorgruppen

3.2.1 Operationen von Gruppen auf Mengen

Ziel: Die Struktur der Gruppen und Mengen, wie z.B. geometrische Objekte und ihre Symmetrien, besser verstehen!

Sei stets $(G, \circ)$ eine Gruppe.

Definition 3.2.1 (*Operation einer Gruppe auf einer Menge*)

Sei M eine nicht-leere Menge. Eine **Operation von** G **auf** M ist eine Abbildung

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (g, m) & \mapsto & g.m \end{array}$$

mit folgenden Eigenschaften:

(GM1) $e.m = m \quad \forall\, m \in M$;

(GM2) $(g \circ h).m = g.(h.m) \quad \forall\, g, h \in G$ und $\forall\, m \in M$.

Wir sagen auch, dass G **auf** X **operiert**.

(In dieser Definition ist e das neutrale Element von G.)

Beispiel 3.2.2

(a) Die symmetrische Gruppe S_n operiert auf der Menge $M = \{1, 2, \ldots, n\}$ durch

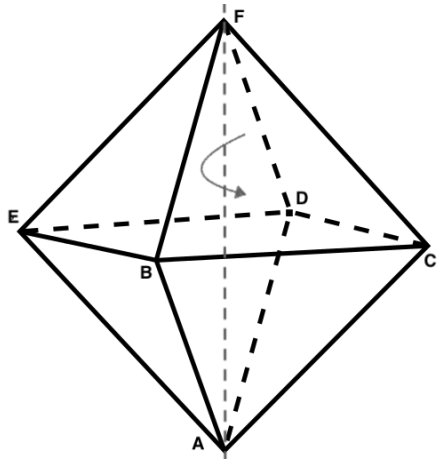
$$\begin{array}{ccc} S_n \times \{1, 2, \ldots, n\} & \longrightarrow & \{1, 2, \ldots, n\} \\ (\sigma, a) & \mapsto & \sigma.a = \sigma(a), \end{array}$$

da $\mathrm{Id}.a = \mathrm{Id}(a) = a$ für alle $a \in \{1, 2, \ldots, n\}$ ist $\Longrightarrow$ **(GM1)** gilt, und es gilt

$$(\sigma \circ \tau).a = (\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma.(\tau.a) \quad \forall\, a \in \{1, 2, \ldots, n\}$$

$\Longrightarrow$ **(GM2)** gilt.

(b) Die Gruppe $G = \mathbb{Z}/4$ Operiert auf dem regulären Oktaeder



durch Drehungen:

- Die Restklasse $\overline{1}$ operiert durch eine Drehung um $+90°$, d.h.

  $\overline{1}.B = C$, $\overline{1}.C = D$, $\overline{1}.D = E$, $\overline{1}.E = B$ und A und F sind fest ($\overline{1}.A = A$, $\overline{1}.F = F$).

- Die Restklasse $\overline{2}$ operiert durch eine Drehung um $+180°$, d.h.

  $\overline{2}.B = D$, $\overline{2}.C = E$, $\overline{2}.D = B$, $\overline{2}.E = C$ und A und F sind fest.

- Die Restklasse $\overline{3}$ operiert durch eine Drehung um $+270°$, d.h.

  $\overline{3}.B = E$, $\overline{3}.C = B$, $\overline{3}.D = C$, $\overline{3}.E = D$ und A und F sind fest.

- Die Restklasse $\overline{0} = \overline{4}$ (das neutrale Element in $G = \mathbb{Z}/4$) operiert durch eine Drehung um $+360° = 0°$. Damit sind die Ecken A, B, C, D, E, F fest.

(Siehe auch `Beamer_Woche_7.pdf`.)

(c) Die Gruppe G operiert auf der Menge $M = G$ selbst durch die Verknüpfung:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, m) & \mapsto & g.m := g \circ m \end{array}$$

Um Operationen von Gruppen auf Mengen zu verstehen, studieren wir einerseits die Elemente der Menge, die fest sind, und anderseits die Elemente, die sich bewegen:

Definition 3.2.3 (*Bahn, Stabilisator*)

Sei G eine Gruppe, die auf einer Menge M operiert, und sei $m \in M$. Dann ist

(i) $G.m := \{g.m \mid g \in G\} \subseteq M$ die **Bahn** von m, und

(ii) $\mathrm{Stab}_G(m) := \{g \in G \mid g.m = m\}$ der **Stabilisator** von m in G.

Bemerkung 3.2.4

Der Stabilisator $\mathrm{Stab}_G(m)$ von $m \in M$ in G ist eine Untergruppe von G.

Beweis: Wir überprüfen, dass $\mathrm{Stab}_G(m)$ die drei Bedingungen der Definition einer Untergruppe erfüllt:

(i) $e.m = m$ nach (GM1) $\Rightarrow e \in \mathrm{Stab}_G(m)$.

(ii) $g, h \in \mathrm{Stab}_G(m) \Rightarrow (g \circ h).m \overset{(GM2)}{=} g.(h.m) = g.m = m$, also $g \circ h \in \mathrm{Stab}_G(m)$.

(iii) $g \in \mathrm{Stab}_G(m) \Rightarrow m \overset{(GM1)}{=} e.m = (g^{-1} \circ g).m \overset{(GM2)}{=} g^{-1}.(g.m) = g^{-1}.m$, also $g^{-1} \in \mathrm{Stab}_G(m)$. ■

Beispiel 3.2.5

(a) Betrachte erneut die Operation der symmetrischen Gruppe S_n auf der Menge $M = \{1, 2, \ldots, n\}$, d.h.

$$\begin{array}{ccc} S_n \times \{1, 2, \ldots, n\} & \longrightarrow & \{1, 2, \ldots, n\} \\ (\sigma, a) & \mapsto & \sigma.a = \sigma(a)\,. \end{array}$$

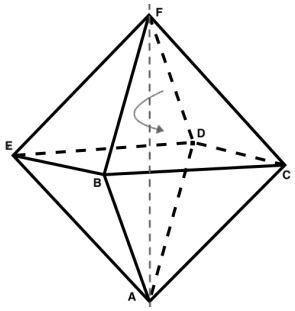
Z.B. ist die Bahn von $a = 1$ die Teilmenge $S_n.1 = \{\sigma.1 \mid \sigma \in S_n\} = \{\sigma(1) \mid \sigma \in S_n\}$. Es gilt

$$\mathrm{Id}(1) = 1,\ (1,2)(1) = 2,\ (1,3)(1) = 3\ \ldots \text{ und } (1,n)(1) = n$$

Somit ist $S_n.1 = \{1, 2, \ldots, n\} = M$, d.h. die ganze Menge M.
Der Stabilisator von $a = n$ in S_n ist

$$\mathrm{Stab}_{S_n}(n) := \{\sigma \in S_n \mid \sigma(n) = n\} = S_{n-1}\,.$$

(b) Sei $G \times \{A, B, C, D, E, F\} \longrightarrow \{A, B, C, D, E, F\}$ die Operation der Gruppe $G = \mathbb{Z}/4$ auf dem regulären Oktaeder durch Drehungen vom Beispiel 3.2.2(b).



· Die Ecken A und F sind fest unter dieser Operation, deswegen sind die Bahnen von A und F einfach

$$\mathbb{Z}/4.A = \{A\} \text{ und } \mathbb{Z}/4.F = \{F\}$$

· Anderseits werden die Ecken B, C, D und F unter dieser Operation vertauscht:

$$\overline{0}.B = B,\ \overline{1}.B = C,\ \overline{2}.B = D, \overline{3}.B = D \quad \Longrightarrow \quad \mathbb{Z}/4.B = \{B, C, D, E\}$$

Ähnlich: die Bahnen von C, D und E sind auch die Teilmenge $\{B, C, D, E\}$.

· Die Stabilisatoren der Ecken sind:

$$\begin{aligned}
\mathrm{Stab}_{\mathbb{Z}/4}(A) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.A = A\} = \mathbb{Z}/4 \\
\mathrm{Stab}_{\mathbb{Z}/4}(F) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.F = F\} = \mathbb{Z}/4 \\
\mathrm{Stab}_{\mathbb{Z}/4}(B) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.B = B\} = \{\overline{0}\} \\
\mathrm{Stab}_{\mathbb{Z}/4}(C) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.C = C\} = \{\overline{0}\} \\
\mathrm{Stab}_{\mathbb{Z}/4}(D) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.D = D\} = \{\overline{0}\} \\
\mathrm{Stab}_{\mathbb{Z}/4}(E) &= \{\overline{a} \in \mathbb{Z}/4 \mid \overline{a}.E = E\} = \{\overline{0}\}
\end{aligned}$$

Siehe auch `Beamer_Woche_7.pdf`.

Anmerkung 3.2.6 (*Eine Äquivalenzrelation*)

Das Bilden der Bahnen definiert eine Äquivalenzrelation $\sim$ auf der Menge M wie folgt: für $m_1, m_2 \in M$ definiere

$$m_1 \sim m_2 \quad \Leftrightarrow \quad \exists\, g \in G \text{ mit } g.m_1 = m_2\,.$$

Somit sind die Äquivalenzklassen genau die Bahnen der Operation von G auf M.

Es folgt, dass je zwei Bahnen $G.m_1$ und $G.m_2$ entweder gleich oder disjunkt sind (siehe Satz 1.5.6 im Skript AGS von J. Böhm).

Weiter nennen wir jedes Element $m \in G.m_1$ einen **Repräsentanten der Bahn** $G.m_1$, denn $G.m = G.m_1$. Ein **vollständiges Repräsentantensystem** der Bahnen ist eine Teilmenge $R \subset M$, sodass jede Bahn $G.m$ genau ein Element von R enthält.

Dann ist M die disjunkte Vereinigung der Bahnen:

$$M = \bigcup_{m \in R} G.m\,,$$

denn eine Äquivalenzrelation partitioniert die Menge in die Äquivalenzklassen.

Beispiel 3.2.7

Die Operation der Gruppe $G = \mathbb{Z}/4$ auf dem regulären Oktaeder partitioniert die Menge der Ecken in 3 Bahnen:

$$\{A, B, C, D, E, F\} = \mathbb{Z}/4.A \cup \mathbb{Z}/4.B \cup \mathbb{Z}/4.F = \{A\} \cup \{B, C, D, E\} \cup \{F\}$$

und $R = \{A, B, F\}$ ist vollständiges Repräsentantensystem der Bahnen.

3.2.2 Die Bahnengleichung

In diesem Abschnitt versuchen wir eine Formel zu entwickeln, um die Elemente der Bahnen einer Operation zu zählen. Diese Formel ist die sogenannte **Bahnengleichung**.

Analog zur Operation einer Gruppe $(G, \circ)$ auf sich selbst (Beispiel 3.2.2(c)) kann man auch die Operation einer Untergruppe $H \leq G$ durch die Verknüpfung betrachten, d.h. die Operation

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \mapsto & h.g := h \circ g \end{array}$$

der Untergruppe H auf der Menge G.
Die Bahnen dieser Operation sind die Teilmengen $H \circ g = \{h \circ g \mid h \in H\}$ der Menge G.

Definition 3.2.8 (*Nebenklassen*)

(a) Die Bahnen $H \circ g = \{h \circ g \mid h \in H\}$ der obigen Operation heißen **Rechtsnebenklassen** von G nach H und wir bezeichnen mit

$$G/H := \{H \circ g \mid g \in G\}$$

die Menge aller Rechtsnebenklassen.

(b) Die **Linksnebenklassen** von G nach H sind die Teilmengen $g \circ H = \{g \circ h \mid h \in H\}$.

(c) Falls die **Rechtsnebenklassen** und die **Linksnebenklassen** gleich sind, d.h. $H \circ g = g \circ H$ für alle $g \in G$, so nennen wir diese einfach die **Nebenklassen** von G nach H.
(Es ist Z.B. der Fall, wenn die Gruppe G ablesch ist.)

Beispiel 3.2.9

Sei $H := n\mathbb{Z}$ mit $n \in \mathbb{N}$ eine Untergruppe von $(\mathbb{Z}, +)$. (Erinnerung: alle Untergruppen von $\mathbb{Z}$ haben die Form $n\mathbb{Z}$.) In diesem Fall ist die Operation von H auf $\mathbb{Z}$

$$\begin{array}{ccc} n\mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (n \cdot k, a) & \mapsto & n \cdot k + a = a + n \cdot k\,. \end{array}$$

Da $\mathbb{Z}$ abelsch ist, sind die Bahnen dieser Operation die Nebenklassen

$$\{a + n \cdot k \mid k \in \mathbb{Z}\} = a + n\mathbb{Z} = \overline{a}\,,$$

d.h. genau die Restklassen modulo n.
In diesem Fall ist die Menge der Nebenklassen $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$, die Gruppe der Restklassen modulo n.

Satz 3.2.10 (*Indexformel, Satz von Lagrange*)

Sei $H \leq G$ eine Untergruppe. Dann gilt

$$|G| = |H| \cdot |G/H|\,.$$

Insbesondere in einer endlichen Gruppe G teilt die Ordnung jeder Untergruppe die Ordnung von G.

Beweis: Wir bemerken zunächst, dass jede Rechtsnebenklasse von G nach H genauso viele Elemente wie H hat, da die Abbildung

$$\begin{array}{ccc} H & \longrightarrow & H \circ g \\ h & \mapsto & h \circ g \end{array}$$

bijektiv ist. (Aufgabe.) Anders gesagt ist $|H| = |H \circ g|$ für alle $g \in G$.

Nach Anmerkung 3.2.6 ist die Menge G die disjunkte Vereinigung aller Bahnen der Operation

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \mapsto & h.g := h \circ g \end{array}$$

d.h.

$$G = \bigcup_{g \in R} H \circ g \,,$$

wobei $R \subseteq G$ ein vollständiges Repräsentantensystem der Bahnen (= Rechtsnebenklassen) ist. Also falls $|G| < \infty$ gilt

$$|G| = \sum_{g \in R} |H \circ g| = \sum_{g \in R} |H| = |R| \cdot |H| = |G/H| \cdot |H| \,.$$

Ist $|G| = \infty$, dann auch $|G/H| = \infty$ oder $|H| = \infty$ und es gilt $\infty = |G| = |H| \cdot |G/H| = \infty$. ■

Damit können wir die gesuchte Formel formulieren und beweisen:

Satz 3.2.11 (*Bahnengleichung*)

Sei $G \times M \longrightarrow M, (g, m) \mapsto g.m$ eine Operation einer Gruppe G auf einer Menge M. Dann gelten:

(a) Ist $m \in M$, so ist die Abbildung

$$\begin{array}{ccc} G/\mathrm{Stab}_G(m) & \longrightarrow & G.m \\ \mathrm{Stab}_G(m) \circ g & \mapsto & g^{-1}.m \end{array}$$

bijektiv. Insbesondere ist $|G/\mathrm{Stab}_G(m)| = |G.m|$.

(b) **Bahnformel:** Ist $m \in M$, so gilt $|G.m| = \frac{|G|}{|\mathrm{Stab}_G(m)|}$.

(c) **Bahnengleichung:** Es gilt

$$|M| = \sum_{m \in R} \frac{|G|}{|\mathrm{Stab}_G(m)|} \,,$$

wobei R ein vollständiges Repräsentantensystem der Bahnen ist.

Beweis:

(a)
- Die Abbildung ist tatsächlich wohldefiniert (Aufgabe).
- Die Abbildung ist offenbar surjektiv nach Definition.
- Die Abbildung ist injektiv, denn für $g_1, g_2 \in G$

$$g_1^{-1}.m = g_2^{-1}.m \;\Rightarrow\; (g_1 \circ g_1^{-1}).m = (g_1 \circ g_2^{-1}).m \;\Rightarrow\; m = (g_1 \circ g_2)^{-1}.m \;\Rightarrow\; g_1 \circ g_2^{-1} \in \mathrm{Stab}_G(m) \,.$$

Somit ist

$$g_2^{-1}.m = (e \circ g_2^{-1}).m = (g_1^{-1} \circ g_1 \circ g_2^{-1}).m = g_1^{-1}.((g_1 \circ g_2^{-1}).m) = g_1^{-1}.m \,.$$

(b) Nach (a) gilt $|G/\mathrm{Stab}_G(m)| = |G.m|$ und nach der Indexformel ist $|G| = |\mathrm{Stab}_G(m)| \cdot |G/\mathrm{Stab}_G(m)|$. Damit gilt:

$$|G| = |\mathrm{Stab}_G(m)| \cdot |G.m| \qquad \Longrightarrow \qquad |G.m| = \frac{|G|}{|\mathrm{Stab}_G(m)|}$$

(c) Nach Anmerkung 3.2.6 ist die Menge M die disjunkte Vereinigung der Bahnen

$$M = \bigcup_{m \in R} G.m$$

und zusammen mit (b) gilt

$$|M| = \sum_{m \in R} |G.m| = \sum_{m \in R} \frac{|G|}{|\mathrm{Stab}_G(m)|}\,.$$

■

Beispiel 3.2.12

Nach Beispiel 3.2.2(b) und Beispiel 3.2.5(b) gilt für die Operation der Gruppe $G = \mathbb{Z}/4$ auf dem regulären Oktaeder

$$M = \{A, B, C, D, E, F\} = \mathbb{Z}/4.A \cup \mathbb{Z}/4.B \cup \mathbb{Z}/4.F$$

(disjunkte Vereinigung der Bahnen) und die Bahnengleichung ist

$$|M| = \frac{|\mathbb{Z}/4|}{|\mathrm{Stab}_{\mathbb{Z}/4}(A)|} + \frac{|\mathbb{Z}/4|}{|\mathrm{Stab}_{\mathbb{Z}/4}(B)|} + \frac{|\mathbb{Z}/4|}{|\mathrm{Stab}_{\mathbb{Z}/4}(F)|} = \frac{|\mathbb{Z}/4|}{|\mathbb{Z}/4|} + \frac{|\mathbb{Z}/4|}{|\{\overline{0}\}|} + \frac{|\mathbb{Z}/4|}{|\mathbb{Z}/4|} = 1 + 4 + 1 = 6\,.$$

3.2.3 Faktorgruppen

Wir studieren nun die Untergruppen $H \leq G$ so, dass die Menge der Rechtsnebenklassen

$$G/H = \{H \circ g \mid g \in G\}$$

(siehe Definition 3.2.8) wieder eine Gruppe ist.

In Beispiel 3.2.9 haben wir gesehen, dass es z.B. der Fall ist, wenn $G = \mathbb{Z}$ und $H = n\mathbb{Z}$ sind, da die Menge der Rechtsnebenklassen $\mathbb{Z}/n\mathbb{Z}$ mit der Gruppe $\mathbb{Z}/n$ der Restklassen modulo n übereinstimmt. Aber es ist nicht wahr im Allgemeinen, dass die Menge der Rechtsnebenklassen G/H zu einer Gruppe wird.

Satz-Definition 3.2.13

Sei $(G, \circ)$ eine Gruppe und sei $H \leq G$ eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

(a) Die Menge $G/H = \{H \circ g \mid g \in G\}$ der Rechtsnebenklassen ist eine Gruppe mit Verknüpfung

$$\begin{array}{rccl} \cdot : & G/H \times G/H & \longrightarrow & G/H \\ & (H \circ g_1, H \circ g_2) & \mapsto & (H \circ g_1) \cdot (H \circ g_2) := H \circ (g_1 \circ g_2)\,, \end{array}$$

neutralem element $H \circ e = H$ und inversem Element $(H \circ g)^{-1} = H \circ g^{-1}$ von $H \circ g \in G/H$.

(b) Die Rechtsnebenklassen und die Linksnebenklassen stimmen übereien, d.h. $H \circ g = g \circ H$ für alle $g \in G$.

Eine Untergruppe $H \leq G$, die die äquivalenten Bedingungen (a) und (b) erfüllt, heißt **Normalteiler** von G und die zugehörige Gruppe G/H heißt die **Faktorgruppe** von G nach H.

Anmerkung 3.2.14

In Bedingung (b) gilt:

$H \circ g = g \circ H$ für alle $g \in G \quad \Longleftrightarrow \quad H = g \circ H \circ g^{-1} = \{g \circ h \circ g^{-1} \mid h \in H\}$ für alle $g \in G$.

Deswegen können wir Bedingung (b) mit folgender Bedingung

$$\text{(b')} \qquad \text{für alle } g \in G \text{ und } h \in H \text{ ist } g \circ h \circ g^{-1} \in H$$

ersetzten, falls notwendig.

Beweis:

(a)⇒(b'): Wir nehmen an, dass $(G/H, \cdot)$ eine Gruppe ist. Sei $g \in G$. Dann ist $H \circ g^{-1} = H \circ (h \circ g^{-1})$ für alle $h \in H$ (dieselbe Rechtsnebenklasse) und somit gilt

$$H \circ e = (H \circ g) \cdot (H \circ g^{-1}) = (H \circ g) \cdot (H \circ (h \circ g^{-1}))$$

wegen der wohldefiniertheit der Verknüpfung. Damit ist

$$H = H \circ e = (H \circ g) \cdot (H \circ (h \circ g^{-1})) = H \circ (g \circ h \circ g^{-1})$$

und wir erhalten $g \circ h \circ g^{-1} \in H$ für alle $h \in H$.

(b)⇒(a): Sobald die Verknüpfung $\cdot : G/H \times G/H \longrightarrow G/H$ wohldefiniert ist, kann man genauso wie im Beweis von Lemma-Definition 3.1.29 zeigen, dass **(G1)**, **(G2)** und **(G3)** gelten.
(Die Argumente sind gleich: ersetze einfach G/H mit $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$, $\cdot$ mit $+$, $H \circ g$ mit $\overline{a} = a + n\mathbb{Z} = n\mathbb{Z} + a$, e mit 0 und $(H \circ g)^{-1}$ mit $-\overline{a}$.)

Deswegen müssen wir zeigen, dass $\cdot : G/H \times G/H \longrightarrow G/H$ wohldefiniert ist, wenn (b) gilt.

Also nehmen wir an, dass $H \circ g = g \circ H$ für alle $g \in G$ gilt. Seien $g_1, g_2, g_1', g_2' \in G$ so, dass $H \circ g_1 = H \circ g_1'$ und $H \circ g_2 = H \circ g_2'$ gilt. Dann ist zu zeigen, dass $(H \circ g_1) \cdot (H \circ g_2) = (H \circ g_1') \cdot (H \circ g_2')$ ist.
Nach (b) gilt $H \circ g_1 = g_1 \circ H$ und $H \circ g_1' = g_1' \circ H$. Damit erhalten wir

$$\begin{aligned}
(H \circ g_1) \cdot (H \circ g_2) &= H \circ (g_1 \circ g_2) \\
&= H \circ H \circ g_1 \circ g_2 \\
&= H \circ g_1 \circ H \circ g_2 \\
&= H \circ g_1' \circ H \circ g_2' \\
&= H \circ H \circ g_1' \circ g_2' \\
&= H \circ (g_1' \circ g_2') = (H \circ g_1') \cdot (H \circ g_2').
\end{aligned}$$

■

Beispiel 3.2.15

(a) Die Untergruppe $H = \{e\}$ von G ist stets ein Normalteiler. Die zugehörige Faktorgruppe ist $G/H = \{\{e\} \circ g \mid g \in G\}$, also die Gruppe G selbst.

(b) Die Untergruppe $H = G$ von G ist stets ein Normalteiler. Die zugehörige Faktorgruppe ist $G/G = \{G \circ e\}$, die nur eine Nebenklasse enthält.

(c) In $\mathbb{Z}$ ist jede Untergruppe $H = n\mathbb{Z}$ ein Normalteiler, da $\mathbb{Z}$ abelsch ist. Die zugehörige Faktorgruppe ist $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$, d.h. die Gruppe der Restklassen modulo n.

(d) (Gegenbeispiel) In $G = S_3$ ist die Untergruppe $H_1 = \{\mathrm{Id}, (1,2)\}$ kein Normalteiler, da $(2,3) \circ H_1 = \{(2,3), (1,3,2)\}$ und $H_1 \circ (2,3) = \{(2,3), (1,2,3)\}$.

Lemma 3.2.16

Ist $\varphi : G \longrightarrow F$ ein Gruppen-Homomorphismus, so ist $\ker(\varphi)$ ein Normalteiler von G. Insbesondere ist die Menge der Nebenklassen $G/\ker(\varphi)$ stets eine Gruppe.

Beweis: Setze $H := \ker(\varphi)$. Seien $g \in G$ und $h \in H$. Dann ist $\varphi(h) = e_F$ nach Definition des Kerns und es gilt

$$\varphi(g \circ h \circ g^{-1}) = \varphi(g) \circ \underbrace{\varphi(h)}_{=e_F} \circ \varphi(g)^{-1} = \varphi(g) \circ e_F \circ \varphi(g)^{-1} = \varphi(g) \circ \varphi(g)^{-1} = e_F \,.$$

Somit ist $g \circ h \circ g^{-1} \in \ker(\varphi) = H$ und Bedingung (b') gilt. Also ist $\ker(\varphi)$ ein Normalteiler von G und $G/\ker(\varphi)$ ist eine Gruppe nach Satz-Definition 3.2.13. ■

Satz 3.2.17 (*Homomorphiesatz*)

Sei $\varphi : G \longrightarrow F$ ein Gruppen-Homomorphismus. Dann gilt

$$G/\ker(\varphi) \cong \mathrm{Bild}(\varphi) \,.$$

Beweis (Sketch): Wir definieren einen Gruppen-Isomorphismus

$$\begin{array}{rccc} \overline{\varphi}: & G/\ker(\varphi) & \longrightarrow & \mathrm{Bild}(\varphi) \\ & \ker(\varphi) \circ g & \mapsto & \varphi(g) \ . \end{array}$$

■

Beispiel 3.2.18

Nach Lemma 3.2.16 ist die alternierende Gruppe A_n stets ein Normalteiler von S_n, da A_n als Kern des Signums

$$\varepsilon : S_n \longrightarrow \{-1, 1\}, \sigma \mapsto \varepsilon(\sigma)$$

definiert wird. Weiter ist das Signum surjektiv nach Definition und somit ist $\mathrm{Bild}(\varphi) = \{-1, 1\}$. Nach dem Homomorphiesatz gilt nun

$$S_n/A_n \cong \{-1, 1\} \,.$$

Somit ist

$$|S_n/A_n| = |\{-1, 1\}| = 2$$

und nach der Indexformel ist $|S_n| = |A_n| \cdot |S_n/A_n|$. Daraus folgt

$$|A_n| = \frac{1}{2}|S_n| \,.$$

3.2.4 Hauptbeispiel 3: Die zyklischen Gruppen

Mit dem Homomorphiesatz können wir eine wichtige Familie von Gruppen klassifizieren: Die sogenannten *zyklischen Gruppen*.

Definition 3.2.19 (*Erzeugnis, Ordnung eines Elements, zyklische Gruppe*)

(a) Für eine nicht-leere Teilmenge E einer Gruppe $(G, \circ)$ definiert man $\langle E \rangle$ als die kleinste Untergruppe von G, die alle Elemente von E enthält. Diese Untergruppe nennt man **das Erzeugnis von** E.

(b) Ist $E = \{g_1, \ldots, g_n\}$ endlich, so schreibt man statt $\langle E \rangle = \langle \{g_1, \ldots, g_n\} \rangle$ kurz $\langle g_1, \ldots, g_n \rangle$.

(c) Ist $E = \{g\}$ (einelementig) für ein Element $g \in G$, so heißt die Untergruppe $\langle g \rangle$ **zyklisch**. Weiter ist $o(g) := |\langle g \rangle|$ die **Ordnung von** g.

(c) Falls G selbst der Form $G = \langle g \rangle$ für ein $g \in G$ ist, so heißt G eine **zyklische Gruppe**.

Anmerkung 3.2.20

(a) Ist $(G, \circ)$ eine Gruppe und $g \in G$, dann setzen wir

$$g^m := \begin{cases} g \circ g \circ \ldots \circ g \quad (m - \text{mal}) & \text{falls } m > 0, \\ e & \text{falls } m = 0, \\ g^{-1} \circ g^{-1} \circ \ldots \circ g^{-1} \quad ((-m) - \text{mal}) & \text{falls } m < 0. \end{cases}$$

Somit ist

$$\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\},$$

da dies die kleinste Untergruppe von G ist, die g enthält.

(b) Die Indexformel liefert: In einer endlichen Gruppe G ist die Ordnung eines Elements $g \in G$ ein Teiler der Gruppenordnung $|G|$, d.h. $o(g) \mid |G|$.

(c) Jede Gruppe G mit $|G|$ prim ist zyklisch.
Beweis: Die Teiler von $|G|$ sind 1 und $|G|$. Damit erhalten wir aus der Indexformel, dass G nur die Untergruppen $\{e\}$ und G besitzt. Somit ist für jedes $g \in G \setminus \{e\}$ schon $\{e\} \neq \langle g \rangle = G$.

Beispiel 3.2.21 (*Klassifikation zyklischer Gruppen*)

Sei $(G, \circ)$ eine zyklische Gruppe und sei $g \in G$ mit $G = \langle g \rangle$. Wir klassifizieren die zyklischen Gruppen wie folgt:

1. Mithilfe der Anmerkung sehen wir, dass die Abbildung

$$\begin{array}{rccc} \varphi: & (\mathbb{Z}, +) & \longrightarrow & \langle g \rangle = G \\ & m & \mapsto & g^m \end{array}$$

ein surjektiver Gruppen-Homomorphismus ist. Insbesondere ist $\text{Bild}(\varphi) = G$.

2. Ist $o(g)$ unendlich, so ist $\ker(\varphi) = \{m \in \mathbb{Z} \mid g^m = e\} = \{0\} \Rightarrow \varphi$ ist injektiv $\Rightarrow \varphi$ ist bijektiv $\Rightarrow \varphi$ ist ein Gruppen-Isomorphismus, d.h.

$$(\mathbb{Z}, +) \cong (G, \circ).$$

3. Ist $o(g)$ endlich, so ist $\ker(\varphi) = n\mathbb{Z}$ für ein $n > 0$ (da $\ker(\varphi)$ eine Untergruppe ist und alle Untergruppen von $\mathbb{Z}$ sind der Form $n\mathbb{Z}$) und der Homomorphiesatz liefert

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n & \xrightarrow{\cong} & \langle g \rangle = G \\ \overline{m} & \mapsto & g^m \ . \end{array}$$

   Insbesondere gilt: $g^{|<g>|} = g^n = g^0 = 1$, da $\overline{n} = \overline{0}$ in $\mathbb{Z}/n$.

Somit haben wir gezeigt: *Jede zyklische Gruppe G endlicher Ordnung ist isomorph zu $(\mathbb{Z}/n, +)$ mit $n = |G|$, jede zyklische Gruppe unendlicher Ordnung ist isomorph zu $(\mathbb{Z}, +)$.*