KAPITEL 2

Gruppen

Als erstes Beispiel werden wir uns mit einer Struktur beschäftigen, die durch eine einzige assoziative Operation definiert wird. Insbesondere werden wir uns mit Gruppen und mit kommutativen Gruppen beschäftigen, die sich noch wesentlich einfacher benehmen als allgemeine Gruppen.

Grundlegende Definitionen

2.1. Eine Struktur mit einer assoziativen Operation nennt man eine Halbgruppe. Besitzt die Operation ein neutrales Element und inverse Elemente, dann spricht man von einer Gruppe. Einen wichtigen Sonderfall bilden die kommutativen Gruppen. Die strukturerhaltenden Abbildungen zu Halbgruppen und Gruppen nennt man Homomorphismen. Wir werden uns hauptsächlich auf Gruppen konzentrieren und Halbgruppen nur nebenbei behandeln.

Definition 2.1. (1) Eine *Halbgruppe* ist eine Menge G zusammen mit einer Operation $\cdot : G \times G \to G$, die assoziativ ist, also $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ für alle $g_1, g_2, g_2 \in G$ erfüllt.

(2) Eine Halbgruppe heißt *kommutativ*, wen $g \cdot h = h \cdot g$ für alle Elemente $g, h \in G$ gilt.

(3) Eine *Gruppe* ist eine Halbgruppe $(G, \cdot)$ die zusätzlich folgenden Bedingungen erfüllt:

(i) Es gibt ein Element $e \in G$, sodass $e \cdot g = g \cdot e = g$ für alle $g \in G$ gilt ("neutrales Element").

(ii) Zu jedem Element $g \in G$ gibt es ein Element $\tilde{g} \in G$, sodass $g \cdot \tilde{g} = \tilde{g} \cdot g = e$ gilt ("inverse Elemente").

(4) Seien $(G, \cdot)$ und $(H, *)$ Halbgruppen. Ein *Homomorphismus* von G nach H ist eine Funktion $\varphi : G \to H$, sodass $\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2)$ für alle $g_1, g_2 \in G$ gilt. Sind G und H Gruppen, dann spricht man von einem *Gruppenhomomorphismus*.

(5) Seien $(G, \cdot)$ und $(H, *)$ Halbgruppen. Ein *Isomorphismus* von G nach H ist ein Homomorphismus $\varphi : G \to H$, sodass es einen Homomorphismus $\psi : H \to G$ gibt, für den $\varphi \circ \psi = \mathrm{id}_H$ und $\psi \circ \varphi = \mathrm{id}_G$ gilt. Zwei Halbgruppen heißen *isomorph* wenn es einen Isomorphismus zwischen ihnen gibt.

Aus der Definition folgt sofort, dass die Komposition von zwei Homomorphismen wiederum ein Homomorphismus ist. Sind nämlich $(G, \cdot)$, $(H, *)$ und $(K, \odot)$ Halbgruppen und $\varphi : G \to H$ und $\psi : H \to K$ Homomorphismen, dann gilt für $g_1, g_2 \in G$

$$(\psi \circ \varphi)(g_1 \cdot g_2) = \psi(\varphi(g_1 \cdot g_2)) = \psi(\varphi(g_1) * \varphi(g_2)) = \psi(\varphi(g_1)) \odot \psi(\varphi(g_2)),$$

also ist auch $\psi \circ \varphi : G \to K$ ein Homomorphismus.

Ist $\varphi : G \to H$ ein Isomorphismus von Halbgruppen, dann muss der Homomorphismus $\psi : H \to G$ aus der Definition die inverse Funktion φ^{-1} sein. Damit folgt insbesondere, dass $\varphi : G \to H$ eine bijektive Funktion sein muss. Ist umgekehrt $\varphi : G \to H$ ein

bijektiver Homomorphismus, dann sei $\varphi^{-1} : H \to G$ die inverse Funktion zu φ. Dann ist aber

$$\varphi(\varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2)) = \varphi(\varphi^{-1}(h_1)) * \varphi(\varphi^{-1}(h_2)) = h_1 * h_2,$$

und damit $\varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2) = \varphi^{-1}(h_1 * h_2)$. Also ist φ^{-1} automatisch ein Homomorphismus. Somit ist ein Homomorphismus zwischen Halbgruppen genau dann ein Isomorphismus, wenn er (als Funktion) bijektiv ist. Man sieht auch leicht (siehe Übungen), dass Isomorphie eine Äquivalenzrelation ist.

Üblicherweise schreibt man die Operation in Gruppen und Halbgruppen einfach durch hintereinander schreiben der Elemente, d.h. man schreibt alle auftretenden Operationen einfach als $(g, h) \mapsto gh$. Die Definition eines Homomorphismus schreibt sich dann einfach als $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. Man muss bei dieser Schreibweise aber aufpassen, welche Operation jeweils gemeint ist. Einige fundamentale Eigenschaften lassen sich nun leicht abklären:

Proposition 2.1. *Sei G eine Gruppe.*

(1) Ist $g \in G$ so, dass $gh = h$ für ein Element $h \in G$ gilt, dann ist $g = e$. Insbesondere ist das neutrale Element durch die definierende Eigenschaft eindeutig bestimmt.

(2) Zu $g \in G$ gibt es nur ein Element $h \in G$ sodass $gh = e$ gilt und für diese Element gilt dann auch $hg = e$.

Beweis. (1) Da G eine Gruppe ist, gibt es zu $h \in G$ ein Element $\tilde{h} \in G$, sodass $h\tilde{h} = e$ gilt. Dann ist aber $e = h\tilde{h} = (gh)\tilde{h} = g(h\tilde{h}) = ge = g$.

(2) Nach Voraussetzung gibt es ein Element $\tilde{g} \in G$, sodass $\tilde{g}g = g\tilde{g} = e$. Aus $gh = e$ folgt dann $\tilde{g} = \tilde{g}e = \tilde{g}(gh) = (\tilde{g}g)h = eh = h$. □

Wir werden im weiteren die neutralen Elemente aller Gruppen mit e bezeichnen. Wegen Teil (2) ist das inverse Element zu $g \in G$ eindeutig bestimmt und es macht daher Sinn, dieses Element mit g^{-1} zu bezeichnen, was wir ab sofort tun werden. Offensichtlich gilt für $g, h \in G$ die Gleichung $(gh)(h^{-1}g^{-1}) = e$, also folgt aus Teil (2) der Proposition, dass $(gh)^{-1} = h^{-1}g^{-1}$ für alle $g, h \in G$ gilt.

Korollar 2.1. *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist $\varphi(e) = e$ und $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$.*

Beweis. Es gilt $\varphi(e)\varphi(e) = \varphi(ee) = \varphi(e)$ und damit folgt $\varphi(e) = e$ aus Teil (1) der Proposition. Weiters gilt $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e$ und damit folgt $\varphi(g^{-1}) = \varphi(g)^{-1}$ aus Teil (2) der Proposition. □

2.2. Untergruppen und Erzeugendensysteme. Für eine gegeben Halbgruppe oder Gruppe G suchen wir als nächstes, wie in 1.4 besprochen, Teilmengen auf die sich die Operationen einschränken lassen.

Definition 2.2. Sei G eine Halbgruppe.

(1) Eine *Unterhalbgruppe* ist eine Teilmenge $H \subset G$ sodass für beliebige Elemente $h_1, h_2 \in H$ auch $h_1 h_2 \in H$ gilt.

(2) Ist G eine Gruppe, dann heißt eine Unterhalbgruppe $H \subset G$ eine Untergruppe, wenn zusätzlich $e \in H$ und für alle $h \in H$ auch $h^{-1} \in H$ gilt. In diesem Fall schreibt man auch $H \leq G$.

Es ist ganz leicht zu sehen, dass eine Unterhalbgruppe einer Gruppe nicht automatisch eine Untergruppe sein muss. So ist etwa $(\mathbb{N}, +)$ eine Unterhalbgruppe von $(\mathbb{Z}, +)$ aber natürlich keine Untergruppe. Das kann also sogar bei kommutativen Gruppen vorkommen. Andererseits ist offensichtlich, dass für eine Unterhalbgruppe H von G die

definierende Operation von G zu einer Funktion $H \times H \to H$ eingeschränkt werden kann, die H selbst zu einer Halbgruppe und im Fall einer Untergruppe zu einer Gruppe macht.

Sei nun G eine Halbgruppe und $\{H_i : i \in I\}$ eine beliebige Familie von Unterhalbgruppen von G. Dann folgt aus der Definition sofort, dass der Durchschnitt $H := \cap_{i\in I} H_i$ eine Unterhalbgruppe von G ist. Für $h_1, h_2 \in H$ gilt ja $h_1, h_2 \in H_i$ für alle $i \in I$. Da jedes H_i eine Unterhalbgruppe ist, folgt $h_1h_2 \in H_i$ für alle $i \in I$ und damit $h_1h_2 \in H$. Genauso folgt sofort, dass der Durchschnitt über eine beliebige Familie von Untergruppen einer Gruppe selbst eine Untergruppe ist.

Lemma 2.2. *Sei G eine Gruppe und $A \subset G$ eine beliebige Teilmenge. Dann gibt es eine eindeutige Untergruppe $H \leq G$, die folgende Eigenschaft hat: Es ist $A \subset H$ und für jede Untergruppe $\tilde{H} \leq G$ mit $A \subset \tilde{H}$ ist $H \subset \tilde{H}$.*

Beweis. Offensichtlich hat der Durchschnitt über die Familie aller Untergruppen von G, die A enthalten diese Eigenschaft. □

Man nennt die Untergruppe aus der Proposition die *von A erzeugte Untergruppe von G* und bezeichnet sie mit $\langle A\rangle \leq G$. Umgekehrt kann man nun natürlich Teilmengen $E \subset G$ betrachten, die $\langle E\rangle = G$ erfüllen. So eine Teilmenge heißt dann ein *Erzeugendensystem* für G.

Untergruppen sind gut mit Homomorphismen verträglich. Wendet man das auf die offensichtlichen Untergruppen $e \subset G$ und $G \subset G$ an, dann erhält man sofort zwei Untergruppen, die einem Homomorphismus in natürlicher Weise zugeordnet werden können.

Proposition 2.2. *Seien G und H Gruppen und sei $\varphi : G \to H$ ein Homomorphismus.*

(1) Für jede Untergruppe $H' \subset H$ ist das Urbild $\varphi^{-1}(H') = \{g \in G : \varphi(g) \in H'\}$ eine Untergruppe von G. Insbesondere ist $\mathrm{Ker}(\varphi) := \{g \in G : \varphi(g) = e\}$ *eine Untergruppe von G.*

(2) Für jede Untergruppe $G' \subset G$ ist das Bild $\varphi(G') = \{\varphi(g') : g' \in G'\}$ eine Untergruppe von H. Insbesondere ist $\mathrm{Im}(\varphi) := \{\varphi(g) : g \in G\}$ *eine Untergruppe von H.*

(3) φ ist genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = \{e\}$ *gilt.*

(4) Ist E ein Erzeugendensystem für G, dann ist φ eindeutig bestimmt durch die Einschränkung $\varphi|_E : E \to H$ und $\varphi(E) = \{\varphi(g) : g \in E\} \subset H$ ist ein Erzeugendensystem für die Gruppe $\mathrm{Im}(\varphi)$.

Beweis. (1) Für $g_1, g_2 \in \varphi^{-1}(H')$ gilt $\varphi(g_1) \in H'$ und $\varphi(g_2) \in H'$. Da $H' \subset H$ eine Untergruppe ist, folgt $\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \in H'$, also $g_1g_2 \in \varphi^{-1}(H')$. Aus Korollar 2.1 folgt sofort, dass $e \in \varphi^{-1}(H')$ gilt, und dass für $g \in \varphi^{-1}(H')$ auch $g^{-1} \in \varphi^{-1}(H')$ gilt. Die letzte Behauptung ist klar, weil $\{e\} \subset H$ eine Untergruppe ist.

(2) beweist man ganz analog, siehe Übungen.

(3) Ist φ injektiv, dann kann $\varphi(g) = e = \varphi(e)$ nur für $g = e$ gelten, also folgt $\mathrm{Ker}(\varphi) = \{e\}$. Umgekehrt ist $\varphi(g) = \varphi(h)$ äquivalent zu

$$e = \varphi(g)\varphi(h)^{-1} = \varphi(g)\varphi(h^{-1}) = \varphi(gh^{-1}).$$

Ist also $\mathrm{Ker}(\varphi) = \{e\}$, dann kann $\varphi(g) = \varphi(h)$ nur für $gh^{-1} = e$ und damit $g = h$ gelten.

(4) Sei $\psi : G \to H$ ein weiterer Homomorphismus, sodass $\psi|_E = \varphi|_E$ gilt. Betrachte die Teilmenge $G' := \{g \in G : \varphi(g) = \psi(g)\}$. Nach Korollar 2.1 folgt sofort, dass $e \in G'$ und für $g \in G'$ auch $g^{-1} \in G'$ gilt. Da φ und ψ Homomorphismen sind, folgt aus $g_1, g_2 \in G'$ auch $g_1g_2 \in G'$. Damit ist aber $G' \subset G$ eine Untergruppe und nach Voraussetzung ist $E \subset G'$, also $G = G'$.

Für die zweite Behauptung nehmen wir an, dass $H' \subset \mathrm{Im}(\varphi)$ eine Untergruppe ist, die $\varphi(E)$ enthält. Dann ist $\varphi^{-1}(H')$ nach Teil (1) eine Untergruppe von G, die E enthält, also $\varphi^{-1}(H') = G$, weil E ein Erzeugendensystem ist. Das bedeutet aber, dass $\varphi(g) \in H'$ für alle $g \in G$ gilt, also $H' = \mathrm{Im}(\varphi)$. □

Analog wie in der linearen Algebra nennt man $\mathrm{Ker}(\varphi)$ den *Kern* und $\mathrm{Im}(\varphi)$ das *Bild* des Homomorphismus φ.

2.3. Beispiele. Wie wir schon in 1.2 festgestellt haben, ist für jede Menge X die Menge $G := \mathrm{Bij}(X)$ aller bijektiven Funktionen $f : X \to X$ eine Gruppe unter der Komposition. Man kann leicht Untergruppen einer derartigen Gruppe finden: Sei etwa $Y \subset X$ eine Teilmenge. Dann können wir etwa die Teilmenge

$$Z_Y := \{f \in G : f(y) = y \quad \forall y \in Y\}$$

betrachten die offensichtlich eine Untergruppe ist. Analog kann man die Menge N_Y jener $f \in G$ betrachten, für die $f(Y) \subset Y$ gilt und $f|_Y : Y \to Y$ bijektiv ist. (Ist $Y \subset X$ eine endliche Teilmenge, dann folgt die zweite Bedingung aus der ersten, siehe Übungen.)

Um zu sehen, dass N_Y eine Untergruppe ist, bemerken wir zunächst, dass offensichtlich $id_X \in N_Y$ gilt. Sind $f, g \in N_Y$, dann ist $(g \circ f)(Y) \subset g(Y) \subset Y$, und aus der Definition folgt sofort, dass $(g \circ f)|_Y = (g|_Y \circ f|_Y)$ gilt. Damit ist aber $(g \circ f)|_Y$ bijektiv als Komposition zweier bijektiver Funktionen. Für $f \in N_Y$ folgt aus der Bijektivität von $f|_Y$ sofort, dass $f^{-1}(Y) \subset Y$ gilt, und aus der Definition folgt wieder $f^{-1}|_Y = (f|_Y)^{-1}$. Damit ist $N_Y \subset G$ eine Untergruppe.

Diese Überlegungen zeigen aber auch sofort, dass $\varphi(f) := f|_Y$ einen Homomorphismus $\varphi : N_Y \to \mathrm{Bij}(Y)$ definiert. Man sieht leicht, dass dieser Homomorphismus surjektiv ist, also $\mathrm{Im}(\varphi) = \mathrm{Bij}(Y)$ gilt. Ist nämlich $h : Y \to Y$ bijektiv, dann definiert man $f : X \to X$ durch $f(y) := h(y)$ für $y \in Y$ und $f(x) = x$ für $x \notin Y$. Man zeigt leicht, dass f bijektiv ist, und offensichtlich gilt $f \in N_Y \subset \mathrm{Bij}(X)$ und $\varphi(f) = h$. Andererseits können wir auch leicht den Kern $\mathrm{Ker}(\varphi)$ bestimmen. Das neutrale Element von $\mathrm{Bij}(Y)$ ist ja die Identitätsabbildung id_Y. Damit gilt $f \in \mathrm{Ker}(\varphi)$ genau dann, wenn $f|_Y = \mathrm{id}_Y$, also $f(y) = y$ für alle $y \in Y$ gilt. Das zeigt aber, dass $\mathrm{Ker}(\varphi) = Z_Y$ gilt.

Tatsächlich kann man jede Gruppe als Untergruppe eine Bijektionsgruppe realisieren. Das klingt vielleicht überraschend, ist aber eigentlich ganz einfach. Für eine Gruppe G und ein Element $g \in G$ kann man die Funktion $\lambda_g : G \to G$ betrachten, die einfach jedes Element von links mit g multipliziert, also durch $\lambda_g(h) := gh$ definiert ist. Nun ist $g^{-1}(gh) = (g^{-1}g)h = eh = h$ und analog ist $g(g^{-1}h) = h$, also gilt $\lambda_{g^{-1}} \circ \lambda_g = \lambda_g \circ \lambda_{g^{-1}} = \mathrm{id}_G$. Damit ist aber λ_g bijektiv, also $\lambda_g \in \mathrm{Bij}(G)$. Andererseits ist für $g, h, k \in G$ auch $g(hk) = (gh)k$, also ist $(\lambda_g \circ \lambda_h)(k) = \lambda_{gh}(k)$ also $\lambda_g \circ \lambda_h = \lambda_{gh}$. Das sagt aber gerade, dass $\varphi(g) := \lambda_g$ einen Homomorphismus $\varphi : G \to \mathrm{Bij}(G)$ definiert. Ist $g \in \mathrm{Ker}(\varphi)$, dann ist $\lambda_g = \mathrm{id}_G$, also insbesondere $e = \lambda_g(e) = ge = g$, also ist $\mathrm{Ker}(\varphi) = \{e\}$. Aus Proposition 2.2 wissen wir, dass damit φ injektiv ist, also einen Isomorphismus zwischen G und der Untergruppe $\mathrm{Im}(\varphi) \subset \mathrm{Bij}(G)$ definiert. Ist insbesondere G eine endliche Gruppe (d.h. G ist endlich als Menge), dann hat man so G als Untergruppe einer Permutationsgruppe realisiert.

Als weiteres Beispiel beschreiben wir die Untergruppen der kommutativen Gruppe $(\mathbb{Z}, +)$, was sofort Anwendungen auf das Studium allgemeiner Gruppen haben wird. Es mag überraschend sein, dass bei der Beschreibung der additiven Untergruppen von $\mathbb{Z}$ die Multiplikation eine wichtige Rolle spielt. Wir werden das später noch besser verstehen.

Proposition 2.3. *Jede Untergruppe von* $(\mathbb{Z},+)$ *ist von der Form* $n\mathbb{Z} := \{nm : m \in \mathbb{Z}\}$ *für ein* $n \in \mathbb{N}$.

Beweis. Eine Teilmenge $G \subset \mathbb{Z}$ ist nach Definition genau dann eine Untergruppe von $(\mathbb{Z},+)$, wenn $0 \in G$ und für $x, y \in G$ auch $-x \in G$ und $x+y \in G$ gilt. Ist $G = \{0\}$, dann ist $G = 0\mathbb{Z}$. Fall G Elemente $\neq 0$ enthält, dann auch positive Elemente, und in diesem Fall definieren wir $n := \min\{x \in G : x > 0\}$. (Man erinnere sich daran, dass jede nichtleere Teilmenge von $\mathbb{N}$ ein Minimum besitzt.) Dann gilt $n \in G$, also auch $n + n = 2n \in G$ und induktiv folgt $kn \in G$ für alle $k \in \mathbb{N}$. Damit ist aber auch $-kn = (-k)n \in G$ für alle $k \in \mathbb{N}$, also $n\mathbb{Z} \subset G$.

Wäre nun $G \neq n\mathbb{Z}$, dann gäbe es ein Element $x \in G \setminus n\mathbb{Z}$ und indem wir nötigenfalls x durch $-x$ ersetzen können wir $x > 0$ annehmen. Da $x \notin n\mathbb{Z}$ gilt, gibt es ein $k \in \mathbb{N}$, sodass $kn < x < (k+1)n$ gilt. Damit folgt aber $0 < x - kn < n$ und natürlich gilt $x - kn \in G$. Das ist aber ein Widerspruch zur Definition von n. □

Betrachten wir nun ein beliebige Gruppe G (multiplikativ geschrieben) und ein Element $g \in G$. Dann definieren wir g^k für $k \in \mathbb{Z}$ wie folgt: $g^0 := e$, $g^1 := g$, für $k > 0$ definiere induktiv $g^k := g \cdot g^{k-1}$ und schließlich $g^{-k} := (g^k)^{-1}$. Aus dieser Definition folgert man leicht, dass $g^k \cdot g^\ell = g^{k+\ell}$ für alle $k, \ell \in \mathbb{Z}$ gilt, was aber zusammen mit dem obigen bedeutet, dass die Abbildung $\varphi : \mathbb{Z} \to G$, die gegeben ist durch $\varphi(k) := g^k$ ein Homomorphismus von $(\mathbb{Z},+)$ nach G ist.

Nach Proposition 2.2 ist $\mathrm{Im}(\varphi) = \{g^k : k \in \mathbb{Z}\} \subset G$ eine Untergruppe von G und weil $\{1\} \subset \mathbb{Z}$ offensichtlich eine Erzeugendensystem für $(\mathbb{Z},+)$ ist, wird diese Untergruppe von dem Element $\varphi(1) = g$ erzeugt. Nach Proposition 2.3 ist $\mathrm{Ker}(\varphi) = \{k \in \mathbb{Z} : g^k = e\}$ von der Form $n\mathbb{Z}$ für ein Element $n \in \mathbb{N}$. Ist $n > 0$, dann nennt man diese Zahl die *Ordnung des Elements* g. Nach Definition ist das die minimale positive Zahl n, für die $g^n = e$ gilt. Ist $\mathrm{Ker}(\varphi) = \{0\}$, dann sagt man, das Element g hat *unendliche Ordnung*. Offensichtlich ist das neutrale Element e das einzige Element, das Ordnung 1 hat. Insbesondere sehen wir, dass für ein Element $g \in G$ mit unendlicher Ordnung die Untergruppe $\langle\{g\}\rangle$ isomorph zu $(\mathbb{Z},+)$ während man für ein Element mit endlicher Ordnung n eine Gruppe erhält, die isomorph zu $(\mathbb{Z}_n,+)$, der additiven Gruppe der Restklassen modulo n, ist.

Nebenklassen und Quotienten

2.4. Nebenklassen. Als ersten Schritt in Richtung der Quotientenbildung betrachten wir eine Gruppe G und eine Äquivalenzrelation $\sim$ auf G. Dann zerfällt G in die disjunkte Vereinigung der Äquivalenzklassen $[g] = \{h \in G : g \sim h\}$. Die Frage ist nun, wann die Gruppenoperation auf G eine wohldefinierte Operation auf der Menge $G/\sim$ aller Äquivalenzklassen induziert. Man möchte also eine Multiplikation von Äquivalenzklassen definieren, indem man $[g] \cdot [h] := [gh]$ definiert. Diese Definition ist offensichtlich genau dann sinnvoll (d.h. die Multiplikation auf $G/\sim$ ist "wohldefiniert"), wenn aus $g \sim \tilde{g}$ und $h \sim \tilde{h}$ immer $gh \sim \tilde{g}\tilde{h}$ folgt.

Nehmen wir nun an, dass $\sim$ eine derartige Äquivalenzrelation ist und betrachten wir nun die Teilmenge $[e] \subset G$, also die Äquivalenzklasse des neutralen Elements. Gilt $g, h \in [e]$, also $g \sim e$ und $h \sim e$ dann muss $gh \sim ee = e$, also $gh \in [e]$ gelten. Außerdem ist für das inverse Element g^{-1} wegen $g \sim e$ und $g^{-1} \sim g^{-1}$ natürlich $e = gg^{-1} \sim eg^{-1} = g^{-1}$, also gilt auch $g^{-1} \in [e]$. Zusammen mit der offensichtlichen Tatsache, dass $e \in [e]$ gilt, zeigt das, dass $[e] \subset G$ eine Untergruppe von G sein muss.

Eine Untergruppe $H \subset G$ liefert aber sofort zwei Äquivalenzrelationen auf G, für die H die Äquivalenzklasse von e ist: Für $g \in G$ definiert man $gH := \{gh : h \in H\}$

und $Hg := \{hg : h \in H\}$, und nennt gH die *linke Nebenklasse von g bezüglich H* und Hg die *rechte Nebenklasse von g bezüglich H*. Die Eigenschaften von Nebenklassen sind leicht zu verstehen. Wir formulieren und beweisen das entsprechende Resultat nur für die linken Nebenklassen, für rechte Nebenklassen geht alles analog (siehe Übungen).

Lemma 2.4. *Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann sind für zwei Elemente $g, k \in G$ folgende Bedingungen äquivalent:*

(1) $g^{-1}k \in H$
(2) $k \in gH$
(3) $gH \cap kH \neq \emptyset$
(4) $gH = kH$

Beweis. Ist $g^{-1}k \in H$, dann ist $gg^{-1}k = k \in gH$, also gilt (1)⇒(2). Ist $k \in gH$, dann gibt es ein Element $h \in H$ mit $k = gh$. Für $\tilde{h} \in H$ ist dann $k\tilde{h} = g(h\tilde{h})$ und das liegt in gH, weil H eine Untergruppe ist. Damit gilt aber $kH \subset gH$. Nun ist aber $g = kh^{-1} \in kH$, also erhalten wir analog $gH \subset kH$, also gilt (2)⇒(4). Nachdem (4)⇒(3) offensichtlich ist, brauchen wir nur noch (3)⇒(1) zu beweisen: Aus (3) folgt, dass es Elemente $h_1, h_2 \in H$ gibt, sodass $gh_1 = kh_2$ gilt. Multipliziert man diese Gleichung von links mit g^{-1} und von rechts mit $(h_2)^{-1}$, dann erhält man $g^{-1}k = h_1(h_2)^{-1}$, und das liegt in H. □

Aus Bedingung (4) sieht man sofort, dass die Bedingungen des Lemmas eine Äquivalenzrelation auf G definieren. Man schreibt G/H für die Menge der Äquivalenzklassen, also $G/H = \{gH : g \in G\}$. Wie bei jeder Äquivalenzrelation erhält man eine kanonische Funktion $\pi : G \to G/H$, indem man jedem Element seine Äquivalenzklasse zuordnet, also $\pi(g) := gH$ setzt.

Aus diesen Überlegungen erhalten wir sofort ein fundamentales Resultat für die Theorie der endlichen Gruppen. Ist G eine endliche Gruppe, dann nennt man die Anzahl $|G|$ der Elemente von G die *Ordnung* der Gruppe G. Ist $H \leq G$ eine Untergruppe, dann ist natürlich auch H endlich, und es gibt auch nur endlich viele Nebenklassen.

Satz 2.4. *Sei G eine endliche Gruppe, $H \leq G$ eine Untergruppe, und G/H die Menge der linken Nebenklassen. Dann gilt*

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

also ist die Ordnung jeder Untergruppe von G ein Teiler der Ordnung von G.

Insbesondere hat jedes Element $g \in G$ endliche Ordnung (wie in 2.3 definiert), die ebenfalls ein Teiler der Gruppenordnung ist.

Beweis. Wie wir schon in 2.3 festgestellt haben, ist für $g \in G$ die Abbildung $\lambda_g : G \to G$, $\lambda_g(\tilde{g}) := g\tilde{g}$ bijektiv. Insbesondere schränkt sich diese Abbildung zu einer Bijektion zwischen H und gH ein. Damit hat aber jede Nebenklasse genau $|H|$ viele Elemente und G ist die disjunkte (siehe Lemma 2.4) Vereinigung von $|G/H|$ vielen solchen Nebenklassen, also folgt $|G| = |H| \cdot |G/H|$.

Aus 2.3 wissen wir weiters, dass für ein Element $g \in G$ die Anzahl der Elemente der von g erzeugte Untergruppe genau die Ordnung von g ist, also folgt auch die letzte Behauptung. □

Mit Hilfe dieses Satzes können wir endliche Gruppen, deren Ordnung eine Primzahl ist, vollständig beschreiben:

Korollar 2.4. *Sei G eine endliche Gruppe, sodass $|G| =: p$ eine Primzahl ist. Dann ist G isomorph zu $(\mathbb{Z}_p, +)$ und damit insbesondere kommutativ.*

BEWEIS. Sei $g \in G$ ein Element mit $g \neq e$. Dann wissen wir aus 2.3, dass die Ordnung von g größer als 1 sein muss. Nach Satz 2.4 muss diese Ordnung aber p teilen, also gleich p sein. Das bedeutet aber, das G mit der von g erzeugten Untergruppe übereinstimmen muss, und diese ist isomorph zu $(\mathbb{Z}_p, +)$. □

2.5. Normalteiler. Kehren wir zurück zu der Frage einer Äquivalenzrelation $\sim$ auf G, die eine wohldefinierte Multiplikation auf dem Raum der Äquivalenzklassen liefert. Wie wir schon in 2.4 überlegt haben, muss dafür aus $g_1 \sim h_1$ und $g_2 \sim h_2$ immer $g_1g_2 \sim h_1h_2$ folgen. In 2.4 haben wir ebenfalls schon überlegt, dass für so eine Relation die Äquivalenzklasse $[e]$ des neutralen Elements eine Untergruppe K von G sein muss. Für $g, h \in G$ folgt wegen $g^{-1} \sim g^{-1}$ aus $g \sim h$ natürlich $e = g^{-1}g \sim g^{-1}h$. Umgekehrt folgt wegen $g \sim g$ aber aus $g^{-1}h \sim e$ auch $gg^{-1}h \sim ge$, also $h \sim g$. Aus Lemma 2.4 sehen wir somit, dass $g \sim h$ genau dann gilt, wenn $gK = hK$ gilt, also ist die ganze Relation durch $K = [e]$ vollständig bestimmt. Es bleibt also nur noch zu überlegen, welche Untergruppen tatsächlich eine Relation mit den gewünschten Eigenschaften liefern. Das können wir nun leicht charakterisieren:

Satz 2.5. *Sie G eine Gruppe, $K \subset G$ eine Untergruppe und $\pi : G \to G/K$ die natürliche Abbildung auf die Menge der linken Nebenklassen. Dann sind äquivalent:*

1. *Für jedes $g \in G$ ist $gK = Kg$.*
2. *Für jedes $g \in G$ und jedes $k \in K$ ist $gkg^{-1} \in K$.*
3. *Für die Äquivalenzrelation $g \sim h :\Leftrightarrow gK = hK$ folgt aus $g_1 \sim h_1$ und $g_2 \sim h_2$ immer $g_1g_2 \sim h_1h_2$.*
4. *Es gibt eine Gruppenstruktur auf G/K, sodass $\pi : G \to G/K$ ein Gruppenhomomorphismus ist.*
5. *Es gibt eine Gruppe H und einen Homomorphismus $\varphi : G \to H$ mit $K = \mathrm{Ker}(\varphi)$.*

BEWEIS. (1)⇔(2): Für $g \in G$ und $k, \tilde{k} \in K$ ist $gk = \tilde{k}g$ äquivalent zu $\tilde{k} = gkg^{-1}$. Ist (1) erfüllt, dann muss es zu g und k so ein $\tilde{k}$ geben, also folgt (2). Ist umgekehrt (2) erfüllt, dann ist $gk = (gkg^{-1})g$ und $kg = g(g^{-1}kg)$, also folgt (1).

(2)⇒(3): Nach Voraussetzung und Lemma 2.4 gilt $(g_1)^{-1}h_1 \in K$ und $(g_2)^{-1}h_2 \in K$, und wir müssen zeigen, dass auch $(g_1g_2)^{-1}(h_1h_2) \in K$ gilt. Wendet man Eigenschaft (2) auf $(g_2)^{-1}$ und $(g_1)^{-1}h_1$ an, dann erhält man $(g_2)^{-1}(g_1)^{-1}h_1g_2 \in K$ und multipliziert man von rechts mit $(g_2)^{-1}h_2$, dann erhält man

$$(g_2)^{-1}(g_1)^{-1}h_1g_2(g_2)^{-1}h_2 = (g_1g_2)^{-1}(h_1h_2) \in K.$$

(3)⇒(4): Die Bedingung in (3) sagt ja gerade, dass man durch $[g] \cdot [h] = [gh]$ eine wohldefinierte Multiplikation auf der Menge G/K der Äquivalenzklassen erhält. Aus der Assoziativität der Multiplikation auf G folgt sofort, dass auch die Multiplikation auf G/K assoziativ ist, und offensichtlich ist $[e]$ ein neutrales Element. Schließlich folgt wieder nach Definition, dass $[g] \cdot [g^{-1}] = [e]$ gilt. Damit gibt es auch inverse Elemente, also erhalten wir eine Gruppenstruktur auf G/K. Nach Definition ist $\pi(g) = [g]$ also haben wir die Multiplikation dadurch definiert, dass wir verlangt haben, dass π ein Homomorphismus ist.

(4)⇒(5): Haben wir eine Gruppenstruktur auf G/K sodass π ein Homomorphismus ist, dann muss nach Korollar 2.1 $\pi(e) = eK$ das neutrale Element von G/K sein. Dann ist aber $\mathrm{Ker}(\pi) = \{g \in G : gK = eK\}$ und mit Lemma 2.4 folgt $\mathrm{Ker}(\pi) = K$. Also erfüllt $\pi : G \to G/K$ die Bedingungen von (5).

(5)⇒(2): Für $k \in \mathrm{Ker}(\varphi)$ und $g \in G$ gilt

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e\varphi(g)^{-1} = e,$$

also $gkg^{-1} \in \mathrm{Ker}(\varphi)$. □

Definition 2.5. Sei G eine Gruppe.

(1) Ein *Normalteiler* in G oder eine *normale Untergruppe* von G ist eine Untergruppe $N \subset G$, sodass für jedes $k \in N$ und jedes $g \in G$ auch $gkg^{-1} \in N$ gilt. In diesem Fall schreibt man $N \triangleleft G$.

(2) Ist $N \triangleleft G$ ein Normalteiler, dann nennt man G/N mit der Gruppenstruktur aus Bedingung (4) von Satz 2.5 den *Quotienten von G nach N* und $\pi : G \to G/N$ den *kanonischen Quotientenhomomorphismus*.

Bemerke, dass in einer kommutativen Gruppe G für beliebige Elemente $g, k \in G$ natürlich $gkg^{-1} = gg^{-1}k = k$ gilt. Insbesondere ist jede Untergruppe einer kommutativen Gruppe ein Normalteiler.

Bevor wir uns mit Quotientengruppen beschäftigen, wollen wir noch kurz die wichtigsten strukturellen Eigenschaften von Normalteilern zusammenfassen.

Proposition 2.5. *Sei G eine Gruppe.*

(1) Ist $\{N_i : i \in I\}$ eine beliebige Familie von Normalteilern von G. Dann ist $\cap_{i\in I} N_i \subset G$ ein Normalteiler. Insbesondere gibt es für jede Teilmenge $A \subset G$ einen kleinsten Normalteiler $N \triangleleft G$, der $A \subset N$ erfüllt.

(2) Ist H eine weitere Gruppe, $\varphi : G \to H$ ein Homomorphismus und $N \triangleleft H$ ein Normalteiler, dann ist $\varphi^{-1}(N) \subset G$ ein Normalteiler.

Beweis. (1) Aus 2.2 wissen wir bereits, dass $\cap_{i\in I} N_i$ eine Untergruppe von G ist. Für $g \in G$ und $k \in N$ ist aber $k \in N_i$ für alle i, also auch $gkg^{-1} \in N_i$ für alle i nach Satz 2.5. Damit ist $gkg^{-1} \in \cap_{i\in I} N_i$, also ist $\cap_{i\in I} N_i$ ein Normalteiler. Die zweite Aussage folgt sofort, indem man N als den Durchschnitt über alle Normalteiler definiert, die A enthalten.

(2) Für $g \in \varphi^{-1}(N)$ gilt $\varphi(g) \in N$. Ist nun $\tilde{g} \in G$ beliebig, dann ist $\varphi(\tilde{g}g\tilde{g}^{-1}) = \varphi(\tilde{g})\varphi(g)\varphi(\tilde{g})^{-1}$ und das liegt in N, weil N ein Normalteiler in H ist. Damit ist aber $\tilde{g}g\tilde{g}^{-1} \in \varphi^{-1}(N)$. □

Man nennt den kleinsten Normalteiler $N \triangleleft G$, der A enthält, aus Teil (1) der Proposition den *von A erzeugten Normalteiler* von G.

2.6. Quotientengruppen. Ist G eine Gruppe und $N \triangleleft G$ ein Normalteiler, dann ist die Quotientengruppe G/N nach Definition 2.5 die Menge der linken Nebenklassen von Elementen von G bezüglich N, wobei die Multiplikation durch $(g_1N)(g_2N) = (g_1g_2)N$ definiert ist. Viel wichtiger als "wie der Quotient aussieht" ist aber "was der Quotient kann". Das ist die sogenannte *universelle Eigenschaft* einer Quotientengruppe. Man kann leicht zeigen, dass diese Eigenschaft die Quotientengruppe eindeutig bestimmt (siehe Übungen).

Satz 2.6. *Sei G eine Gruppe und $N \triangleleft G$ ein Normalteiler. Dann hat der kanonische Quotientenhomomorphismus $\pi : G \to G/N$ folgende Eigenschaft:*

Ist H eine Gruppe und $\varphi : G \to H$ ein Homomorphismus, sodass $N \subset \mathrm{Ker}(\varphi)$ gilt, dann gibt es einen eindeutig bestimmten Homomorphismus $\underline{\varphi} : G/N \to H$, sodass $\varphi = \underline{\varphi} \circ \pi$ gilt.

BEWEIS. Seien H und $\varphi : G \to H$ gegeben. Da $N \subset \operatorname{Ker}(\varphi)$ gilt, erhalten wir $\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)e = \varphi(g)$ für alle $g \in G$ und $k \in N$. Das sagt aber gerade, dass $\varphi(\tilde{g}) = \varphi(g)$ für alle $\tilde{g} \in gN$ gilt. Damit liefert $\underline{\varphi}(gN) := \varphi(g)$ eine wohldefinierte Abbildung $\underline{\varphi} : G/N \to H$. Nach Definition der Multiplikation auf G/N ist $(g_1N)(g_2N) = (g_1g_2)N$ für $g_1, g_2 \in G$. Damit ist aber

$$\underline{\varphi}((g_1g_2)N) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \underline{\varphi}(g_1N)\underline{\varphi}(g_2N),$$

also ist $\underline{\varphi}$ ein Homomorphismus. Nach Definition gilt auch $\pi(g) = gN$, also sagt unsere Definition gerade $\underline{\varphi}(\pi(g)) = \varphi(g)$ für alle $g \in G$, also $\underline{\varphi} \circ \pi = \varphi$. Da π surjektiv ist, ist $\underline{\varphi}$ durch $\underline{\varphi} \circ \pi$ eindeutig bestimmt. □

Wie man diese Eigenschaft anwenden kann zeigt folgendes Resultat:

Korollar 2.6 (Erster Isomorphiesatz für Gruppen)**.** *Seien G und H Gruppen und sein $\varphi : G \to H$ ein Homomorphismus. Dann induziert φ einen Isomorphismus $\underline{\varphi} : G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$.*

BEWEIS. Sei $\pi : G \to G/\operatorname{Ker}(\varphi)$ der kanonische Quotientenhomomorphismus. Dann gibt es nach Satz 2.6 einen eindeutig bestimmten Homomorphismus $\underline{\varphi} : G/\operatorname{Ker}(\varphi) \to H$, sodass $\varphi = \underline{\varphi} \circ \pi$ gilt. Damit ist aber $\operatorname{Im}(\underline{\varphi}) = \operatorname{Im}(\varphi)$, also kann man $\underline{\varphi}$ auch als surjektiven Homomorphismus $G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ betrachten.

Für $g \in G$ gilt nun aber $\underline{\varphi}(\pi(g)) = \varphi(g)$, also ist $\pi(g) \in \operatorname{Ker}(\underline{\varphi})$ genau dann, wenn $g \in \operatorname{Ker}(\varphi)$, also genau dann, wenn $\pi(g) = \pi(e)$ gilt. Somit besteht der Kern von $\underline{\varphi}$ nur aus dem neutralen Element von $G/\operatorname{Ker}(\varphi)$, also ist $\underline{\varphi} : G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ ein bijektiver Gruppenhomomorphismus und damit ein Isomorphismus. □

2.7. Beispiele. Die nächste Frage die wir uns stellen müssen ist, was wir über eine Gruppe G sagen können, wenn wir einen Normalteiler $N \triangleleft G$ kennen und wissen, wie G/N aussieht. Anders gesagt, müssen wir uns fragen, wie man aus zwei Gruppen eine Gruppe "aufbauen" kann. Eine einfache Möglichkeit ist das Produkt. Für zwei gegebene Gruppen G_1 und G_2 kann man das Produkt $G_1 \times G_2$ der Mengen G_1 und G_2 bilden und hat dann die kanonischen Projektionen $p_1 : G_1 \times G_2 \to G_1$ und $p_2 : G_1 \times G_2 \to G_2$. Das Produkt ist ja einfach die Menge der geordneten Paare (g_1, g_2) mit $g_i \in G_i$ und $p_i(g_1, g_2) = g_i$ für $i = 1, 2$. Nun kann man das Produkt zu einer Gruppe machen, indem man die Operationen komponentenweise definiert. Eleganter ausgedrückt:

Proposition 2.7. *Seien G_1 und G_2 Gruppen. Dann gibt es eine eindeutige Gruppenstruktur auf der Produktmenge $G_1 \times G_2$, sodass die Projektionen $p_i : G_1 \times G_2 \to G_i$ für $i = 1, 2$ Gruppenhomomorphismen sind.*

Ist H eine beliebige Gruppe und ist $\varphi_i : H \to G_i$ ein Gruppenhomomorphismus für $i = 1, 2$, dann gibt es einen eindeutigen Gruppenhomomorphismus $(\varphi_1, \varphi_2) : H \to G_1 \times G_2$ sodass $p_i \circ (\varphi_1, \varphi_2) = \varphi_i$ für $i = 1, 2$ gilt.

BEWEIS. Damit p_1 und p_2 Homomorphismen sind, muss man die Multiplikation durch $(g_1, g_2) \cdot (\tilde{g}_1, \tilde{g}_2) := (g_1\tilde{g}_1, g_2\tilde{g}_2)$ definieren, wobei in den Faktoren das Produkt auf G_1 bzw. auf G_2 verwendet wird. Aus dieser Definition folgt sofort, dass das so definierte Produkt assoziativ ist und ein neutrales Element besitzt, nämlich (e_1, e_2), wobei $e_i \in G_i$ das neutrale Element für $i = 1, 2$ ist (siehe Übungen). Damit gibt es aber auch inverse Elemente, nämlich $(g_1, g_2)^{-1} = ((g_1)^{-1}, (g_2)^{-1})$. Damit haben wir den ersten Teil der Aussage bewiesen.

Für den zweiten Teil definieren wir einfach $(\varphi_1, \varphi_2)(h) := (\varphi_1(h), \varphi_2(h))$. Das erfüllt offensichtlich $p_i \circ (\varphi_1, \varphi_2) = \varphi_i$ für $i = 1, 2$ und ist durch diese Eigenschaft eindeutig

festgelegt. Man verifiziert sofort (siehe Übungen) dass (φ_1, φ_2) ein Homomorphismus ist, wenn φ_1 und φ_2 Homomorphismen sind. □

Man kann nun G_1 in natürlicher Weise als Teilmenge von $G_1 \times G_2$ betrachten, indem man $g_1 \in G_1$ mit (g_1, e) (hier ist $e \in G_2$ das neutrale Element) identifiziert. Anders gesagt, definiert $i_1(g_1) := (g_1, e)$ eine Funktion $i_1 : G_1 \to G_1 \times G_2$ und aus der Definition der Multiplikation auf $G_1 \times G_2$ folgt sofort, dass i_1 ein Homomorphismus ist. Damit ist $\mathrm{Im}(i_1)$ eine Untergruppe von $G_1 \times G_2$ und weil i_1 offensichtlich injektiv ist, ist diese Untergruppen isomorph zu G_1. Andererseits ist ein Element von $G_1 \times G_2$ genau dann von der Form (g_1, e), wenn es durch p_2 auf e abgebildet wird, also in $\mathrm{Ker}(p_2)$ liegt. Damit ist aber $\mathrm{Im}(i_1) = \mathrm{Ker}(p_2)$, also nach Satz 2.5 ein Normalteiler in $G_1 \times G_2$. Nach Korollar 2.6 induziert p_2 einen Isomorphismus $(G_1 \times G_2)/\mathrm{Im}(i_1) \to \mathrm{Im}(p_2) = G_2$. Etwas salopp gesprochen enthält also $G_1 \times G_2$ die Gruppe G_1 als Normalteiler und $(G_1 \times G_2)/G_1 \cong G_2$.

Leider ist die Situation im Allgemeinen nicht so einfach. Betrachten wir etwa die Permutationsgruppe $\mathfrak{S}_3$. Aus der linearen Algebra ist bekannt, dass man jeder Permutation $\sigma \in \mathfrak{S}_n$ ein Signum $\mathrm{sgn}(\sigma) \in \{1, -1\}$ zuordnen kann und dass für eine weitere Permutation τ die Gleichung $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ gilt. Nun bildet aber $\{1, -1\}$ offensichtlich eine kommutative Gruppe unter der Multiplikation, die isomorph zu $\mathbb{Z}_2$ ist und die obige Gleichung sagt gerade, dass man die Signumsabbildung als Homomorphismus $\mathrm{sgn} : \mathfrak{S}_n \to \mathbb{Z}_2$ betrachten kann. Der Kern dieses Homomorphismus ist also ein Normalteiler in $\mathfrak{S}_n$, der üblicherweise mit $\mathfrak{A}_n$ bezeichnet wird. Mann nennt $\mathfrak{A}_n$ die *alternierende Gruppe* auf n Elementen. Nach Konstruktion gilt also $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}_2$ für jedes n.

Für $n = 3$ können wir aber leicht überlegen, wie $\mathfrak{A}_3$ tatsächlich aussieht. Wenn man mit Permutationen vertraut ist, sieht man gleich, dass neben dem neutralen Element nur die beiden Dreierzykel in $\mathfrak{A}_3$ liegen. Daraus kann man leicht sehen, dass $\mathfrak{A}_3 \cong \mathbb{Z}_3$ gilt. Alternativ kann man bemerken, dass $\mathfrak{S}_3$ gerade $3! = 6$ Elemente hat. Aus Satz 2.4 folgt, dass die Gruppe $\mathfrak{A}_3$ Ordnung 3 haben muss und nach Korollar 2.4 folgt $\mathfrak{A}_3 \cong \mathbb{Z}_3$. Insbesondere sehen wir, dass $\mathfrak{S}_3$ den kommutativen Normalteiler $\mathfrak{A}_3$ enthält und dass der Quotient $\mathfrak{S}_3/\mathfrak{A}_3$ isomorph zu $\mathbb{Z}_2$, also ebenfalls kommutativ ist. Wir wissen aber bereits aus 1.2, dass $\mathfrak{S}_3$ nicht kommutativ ist. Da das Produkt von zwei kommutativen Gruppen offensichtlich ebenfalls kommutativ ist, folgt insbesondere, dass $\mathfrak{S}_3$ nicht isomorph zu $\mathbb{Z}_3 \times \mathbb{Z}_2$ sein kann.

Dieses Problem ist keine Folge der Nichtkommutativität, sondern tritt auch bei kommutativen Gruppen auf. Betrachten wir etwa $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, dann ist offensichtlich $\bar{2} \in \mathbb{Z}_4$ ein Element der Ordnung 2, erzeugt also eine (wegen der Kommutativität automatische normale) Untergruppe $H \subset \mathbb{Z}_4$, die isomorph zu $\mathbb{Z}_2$ ist. Der Quotient $\mathbb{Z}_4/H$ hat zwei Elemente, muss also nach Korollar 2.4 ebenfalls isomorph zu $\mathbb{Z}_2$ sein. Nun ist aber $\mathbb{Z}_4$ sicher nicht isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$. Man überprüft nämlich sofort, dass in $\mathbb{Z}_2 \times \mathbb{Z}_2$ alle Elemente außer dem neutralen Element Ordnung 2 haben, während die Elemente $\bar{1}, \bar{3} \in \mathbb{Z}_4$ Ordnung 4 haben.

Kennt man also einen Normalteiler $N \triangleleft G$ und den Quotienten G/N, dann bestimmt das die Gruppen G nicht vollständig. Es liefert aber wichtige Information und es gibt weiter gehende Methoden um zu analysieren, wie viele Möglichkeiten es für eine "passende Gruppe" G bei gegebenem N und G/N gibt ("Erweiterungsproblem"). Wir werden dieses Problem aber nicht weiter studieren.

2.8. Exkurs: Präsentationen. Eine Präsentation einer Gruppe beschreibt die Gruppe durch *Erzeuger* und *Relationen*. Wir werden das hier nur oberflächlich besprechen und nicht auf Details eingehen.

Beginnen wir nun mit einer beliebigen Gruppe G, und einem Erzeugendensystem $E \subset G$, wobei wir der Einfachheit halber annehmen, dass $E = \{g_1, \dots, g_n\}$ endlich ist. Nach Definition bedeutet das nur, dass es keine echte Untergruppe von G gibt, die E enthält. Als nächstes betrachtet man n Symbole $x_1, \dots, x_n$ und bildet die sogenannte *freie Gruppe* $\mathcal{F}(x_1, \dots, x_n)$ über diesen Symbolen. Nach Definition besteht diese Gruppe aus allen "Worten" der Form $x_{i_1}^{j_1} \dots x_{i_k}^{j_k}$ für $k \in \mathbb{N}$, $i_1, \dots, i_k \in \{1, \dots, n\}$ mit $i_\ell \neq i_{\ell+1}$ und $j_1, \dots, j_k \in \mathbb{Z} \setminus \{0\}$. Dabei lässt man das leere Wort e zu, das dann das neutrale Element bildet. Man kann solche Worte multiplizieren, indem man sie einfach hintereinander schreibt, dann so lange $x_i^a x_i^b$ durch x_i^{a+b} ersetzt und x_i^0 weglässt, bis das nicht mehr möglich ist. (Diese Dinge formal sauber zu definieren ist etwas mühsam, die Idee sollte aber verständlich sein.) Das definiert dann eine Multiplikation für die man leicht sieht, dass sie assoziativ ist und dass e ein neutrales Element ist. Außerdem ist $x_{i_k}^{-j_k} \dots x_{i_1}^{-j_1}$ offensichtlich invers zu $x_{i_1}^{j_1} \dots x_{i_k}^{j_k}$, also erhält man eine Gruppenstruktur.

Nun kann man einen Homomorphismus $\varphi : \mathcal{F}(x_1, \dots, x_n) \to G$ definieren, indem man das leere Wort auf da neutrale Element von G und $x_{i_1}^{j_1} \dots x_{i_k}^{j_k}$ auf $g_{i_1}^{j_1} \dots g_{i_k}^{j_k}$ abbildet. Dabei bildet man für die g_i die Potenzen (wie in 2.3 besprochen) und Produkte in G. Da in G ja $g_i^a g_i^b = g_i^{a+b}$ und $g_i^0 = e$ gilt, ist das tatsächlich ein Homomorphismus. Nun ist $\operatorname{Im}(\varphi) \subset G$ eine Untergruppe und natürlich gilt $g_i = \varphi(x_i) \in \operatorname{Im}(\varphi)$ für $i = 1, \dots, n$. Damit ist aber $\operatorname{Im}(\varphi) = G$ und nach dem ersten Isomorphiesatz ist $G \cong \mathcal{F}(x_1, \dots, x_n)/\operatorname{Ker}(\varphi)$.

Dann sucht man eine Familie $\mathcal{R} := \{r_\alpha : \alpha \in A\} \subset \mathcal{F}(x_1, \dots, x_n)$, sodass $\operatorname{Ker}(\varphi)$ der von $\mathcal{R}$ erzeugte Normalteiler ist (siehe Proposition 2.5). Jedes r_α ist nach Definition ein Wort in den Elementen x_i. Wegen $r_\alpha \in \operatorname{Ker}(\varphi)$ erhält man das neutrale Element in G, wenn man dieses Wort aus den g_i statt den x_i bildet, sodass man r_α als *Relation* zwischen den Elementen g_i interpretieren kann. Man sagt dann, dass man ein *Präsentation* der Gruppe G mit Erzeugern $g_1, \dots, g_n$ und Relationen r_α für $\alpha \in A$ gefunden hat.

Solche Präsentationen sind auf der einen Seite relativ handlich. Man kann zum Beispiel Homomorphismen von G in eine beliebige Gruppen H beschreiben: Die Präsentation liefert einen surjektiven Homomorphismus $\varphi : \mathcal{F}(x_1, \dots, x_n) \to G$, also liefert ein Homomorphismus $\psi : G \to H$ die Komposition $\psi \circ \varphi : \mathcal{F}(x_1, \dots, x_n) \to H$ und offensichtlich ist $\operatorname{Ker}(\varphi) \subset \operatorname{Ker}(\psi \circ \varphi)$. Ist Umgekehrt $f : \mathcal{F}(x_1, \dots, x_n) \to H$ ein Homomorphismus mit $\operatorname{Ker}(\varphi) \subset \operatorname{Ker}(f)$, dann erhalten wir nach Satz 2.6 einen Homomorphismus $\underline{f} : \mathcal{F}(x_1, \dots, x_n)/\operatorname{Ker}(\varphi) \to H$ und zusammen mit dem Inversen des Isomorphismus $\overline{\mathcal{F}}(x_1, \dots, x_n)/\operatorname{Ker}(\varphi) \to G$ einen Homomorphismus $G \to H$. Somit sehen wir aber, dass die Menge aller Homomorphismen $G \to H$ in bijektiver Korrespondenz mit der Menge aller jener Homomorphismen $f : \mathcal{F}(x_1, \dots, x_n) \to H$ steht, die $\operatorname{Ker}(\varphi) \subset \operatorname{Ker}(f)$ erfüllen. Nachdem $\operatorname{Ker}(f)$ ein Normalteiler ist, ist die letzte Bedingung äquivalent dazu, das $f(r_\alpha) = e \in H$ für alle $\alpha \in A$ gilt.

Ein Homomorphismus $f : \mathcal{F}(x_1, \dots, x_n) \to H$ ist aber das gleiche wie n Elemente $h_1, \dots, h_n \in H$. Ist f gegeben, dann setzt man einfach $h_i := f(x_i)$ für $i = 1, \dots, n$. Sind umgekehrt die h_i gegeben, dann definiert man f, indem man das Element $x_{i_1}^{j_1} \dots x_{i_k}^{j_k}$ auf $h_{i_1}^{j_1} \dots h_{i_k}^{j_k}$ abbildet, wobei Potenzen und Produkte nun in H zu bilden sind. Die Bedingung, dass $f(r_\alpha) = e$ gilt, bedeutet nun genau, dass die Elemente $h_1, \dots, h_n$ die Relation r_α erfüllen. Da der Homomorphismus $\varphi : \mathcal{F}(x_1, \dots, x_n) \to G$ durch $\varphi(x_i) = g_i$ charakterisiert ist, erfüllt der von f induzierte Homomorphismus $\psi : G \to H$ natürlich

$\psi(g_i) = h_i$ für $i = 1, \dots, n$. Man muss also die Bilder der g_i nur so wählen, dass jede der Relationen r_α erfüllt ist.

In anderer Hinsicht sind aber Präsentation oft nur sehr schwer zu handhaben. Haben wir eine Gruppe G, ein Erzeugendensystem $\{g_1, \dots, g_n\}$ und Relationen r_α gewählt, dann stellt sich natürlich die Frage, ob zwei Produkte der Form $g_{i_1}^{j_1} \dots g_{i_k}^{j_k}$ und $g_{i'_1}^{j'_1} \dots g_{i'_\ell}^{j'_\ell}$ das gleiche Element von g darstellen ("Wortproblem"). Andererseits ist die offensichtliche Frage ob für Familien $\{r_\alpha : \alpha \in A\} \subset \mathcal{F}(x_1, \dots, x_n)$ und $\{\tilde{r}_\beta : \beta \in B\} \subset \mathcal{F}(x_1, \dots, x_m)$ die entsprechenden Gruppen $\mathcal{F}(x_1, \dots, x_n)/K$ und $\mathcal{F}(x_1, \dots, x_m)/\tilde{K}$ (wobei K der von den r_α und $\tilde{K}$ der von den $\tilde{r}_\beta$ erzeugte Normalteiler ist) isomorph sind oder nicht ("Isomorphieproblem"). Man kann beweisen, dass es in allgemeinen endlich erzeugten Gruppen keinen Algorithmus geben kann, um das Wortproblem zu lösen! Ebenso ist das Isomorphieproblem nicht algorithmisch lösbar.

Beispiel 2.8. Betrachten wir die Permutationsgruppe $\mathfrak{S}_3$. Seien $g_1 = (1, 2), g_2 = (2, 3) \in \mathfrak{S}_3$, also die Transpositionen die jeweils zwei benachbarte Elemente vertauschen. Dann gilt natürlich $g_i^2 = \mathrm{id}$ für $i = 1, 2$. Außerdem verifiziert man leicht direkt, dass $g_1 g_2 g_1 = g_2 g_1 g_2$ gilt, weil beide Ausdrücke die Transposition $(1, 3)$ darstellen. Damit erhalten wir $g_1 g_2 g_1 g_2^{-1} g_1^{-1} g_2^{-1} = \mathrm{id}$ und weil $g_i = g_i^{-1}$ für $i = 1, 2$ gilt, kann man das als $(g_1 g_2)^3 = \mathrm{id}$ schreiben. Man überlegt leicht, dass die beiden Transpositionen die Gruppe $\mathfrak{S}_3$ erzeugen. (Allgemein wird $\mathfrak{S}_n$ durch Transpositionen benachbarter Elemente erzeugt, siehe Übungen.)

Daher erhalten wir einen surjektiven Homomorphismus $\varphi : \mathcal{F}(x_1, x_2) \to \mathfrak{S}_3$, der $\varphi(x_i) = g_i$ für $i = 1, 2$ erfüllt. Aus den Überlegungen über Relationen in $\mathfrak{S}_3$ sehen wir, dass x_1^2, x_2^2 und $(x_1 x_2)^3$ in $\mathrm{Ker}(\varphi)$ liegen. Ist $\mathcal{N}$ der von diesen drei Elementen erzeugte Normalteiler, dann gilt natürlich $\mathcal{N} \subset \mathrm{Ker}(\varphi)$ und wir wollen zeigen, dass Gleichheit gilt. Dazu zeigen wir, dass $\mathcal{F}(x_1, x_2)/\mathcal{N}$ wie $\mathcal{F}(x_1, x_2)/\operatorname{Ker}(\varphi) \cong \mathfrak{S}_3$ nur 6 Elemente hat.

Sind $y, z \in \mathcal{F}(x_1, x_2)$, dann rechnen wir für $i \in \mathbb{Z}$

$$y(x_1)^i z (y(x_1)^{i-2} z)^{-1} = y(x_1)^i z z^{-1} (x_1)^{-i+2} y^{-1} = y(x_1)^2 y^{-1},$$

und das liegt offensichtlich in $\mathcal{N}$. Das bedeutet aber, dass $y(x_1)^i z$ und $y(x_1)^{i-2} z$ die gleiche Nebenklasse in $\mathcal{F}(x_1, x_2)/\mathcal{N}$ haben. Wendet man das iterativ an, dann sieht man, dass für gerades i das Element $y(x_1)^i z$ die gleiche Nebenklasse in $\mathcal{F}(x_1, x_2)/\mathcal{N}$ repräsentiert wir yz, während man für ungerades i die gleiche Nebenklasse wie yx_1z erhält. Das gleiche Argument kann man natürlich auf x_2 anwenden. Beginnt man nun mit einem beliebigen Element $x_{i_1}^{j_1} \dots x_{i_k}^{j_k}$, dann ändert sich die Nebenklasse nicht, wenn man die Faktoren mit geradem j_ℓ einfach weglässt und in denen mit ungeradem j_ℓ den Faktor durch x_{j_ℓ} ersetzt. Treten im verbleibenden Term zwei x_1 oder zwei x_2 nebeneinander auf, dann kann man diese ebenfalls weglassen. Also hat jede Nebenklasse einen Repräsentanten der Form $x_{i_1} \dots x_{i_k}$, wobei die i_j abwechselnd gleich 1 und gleich 2 sind.

Nun ist aber $x_1 x_2 x_1 (x_2 x_1 x_2)^{-1} = x_1 x_2 x_1 (x_2)^{-1} (x_1)^{-1} (x_2)^{-1}$ und das repräsentiert die gleiche Nebenklasse wie $(x_1 x_2)^3$, was in $\mathcal{N}$ liegt. Damit repräsentieren aber die Elemente $x_1 x_2 x_1$ und $x_2 x_1 x_2$ die gleiche Nebenklasse. Daraus folgt aber auch, dass jede Nebenklasse durch ein Produkt mit höchstens 3 Faktoren repräsentiert wird, und die beiden verbleibenden Produkte von 3 Faktoren repräsentieren die gleich Klasse. Als Repräsentanten für weitere nichttriviale Klassen kommen aber nur noch x_1, x_2, $x_1 x_2$ und $x_2 x_1$ in Frage, was die Behauptung über die Anzahl der Nebenklassen beweist. Somit erhalten wir eine Präsentation von $\mathfrak{S}_3$ mit zwei Erzeugern x_1 und x_2 und drei Relationen, $(x_1)^2$, $(x_2)^2$ und $(x_1 x_2)^3$.

Wirkungen und Abzählargumente

Als nächstes werden wir uns kurz mit Homomorphismen von allgemeinen Gruppen in Bijektionsgruppen befassen. So einen Homomorphismus kann man äquivalent durch eine sogenannte Wirkung der Gruppe beschreiben. Im Falle von endlichen Gruppen kann man Wirkungen verwenden, um Abzählargumente in der Art von Satz 2.4 zu finden, die, ähnlich wie Korollar 2.4, Konsequenzen für die Strukturtheorie von Gruppen haben.

2.9. Gruppenwirkungen. Wir haben schon 1.2 gesehen, dass das Konzept der Symmetrie eine wesentliche Quelle von Beispielen von Gruppen ist. Versucht man allgemein einer Gruppe G so etwas wie "Symmetrien" einer Menge zuzuordnen, bzw. die Gruppe als Symmetriegruppe zu realisieren, dann gelangt man zum Konzept einer Wirkung.

Definition 2.9. (1) Eine *Wirkung* einer Gruppe G auf einer Menge X ist eine Abbildung $\ell : G \times X \to X$ sodass $\ell(e, x) = x$ für alle $x \in X$ und $\ell(g_1 g_2, x) = \ell(g_1, \ell(g_2, x))$ für alle $g_1, g_2 \in G$ und alle $x \in X$ gilt.

Als ersten Schritt können wir leicht zeigen, dass Wirkungen äquivalent zu Homomorphismen in Bijektionsgruppen sind.

Lemma 2.9. *Sei G eine Gruppe und X eine Menge.*

(1) Ist $\ell : G \times X \to X$ eine Wirkung, dann ist für jedes $g \in G$ die Funktion $\ell_g : X \to X$, die definiert ist durch $\ell_g(x) := \ell(g, x)$, bijektiv und $g \mapsto \ell_g$ definiert einen Homomorphismus $G \to \mathrm{Bij}(X)$.

(2) Ist umgekehrt $\varphi : G \to \mathrm{Bij}(X)$ ein Gruppenhomomorphismus, dann definiert $\ell(g, x) := \varphi(g)(x)$ eine Wirkung von G auf X.

Beweis. (1) Man kann die definierenden Eigenschaften einer Wirkung als $\ell_e(x) = \ell(e, x) = x$ für alle x, also $\ell_e = \mathrm{id}_X$, und als

$$\ell_g \circ \ell_h(x) = \ell_g(\ell(h, x)) = \ell(g, \ell(h, x)) = \ell(gh, x) = \ell_{gh}(x)$$

für alle x, also $\ell_g \circ \ell_h = \ell_{gh}$ lesen. Insbesondere ist $\ell_g \circ \ell_{g^{-1}} = \ell_{gg^{-1}} = \ell_e = \mathrm{id}_X$ und analog erhält man $\ell_{g^{-1}} \circ \ell_g = \mathrm{id}_x$. Damit ist aber die Funktion $\ell_{g^{-1}}$ invers zu ℓ_g, also insbesondere ℓ_g bijektiv für jedes $g \in G$. Hat man das beobachtet, dann kann man $g \mapsto \ell_g$ als Funktion $G \to \mathrm{Bij}(X)$ betrachten, und die Gleichung $\ell_g \circ \ell_h = \ell_{gh}$ sagt dann genau, dass dies ein Gruppenhomomorphismus ist.

(2) Offensichtlich definiert $\ell(g, x) := \varphi(g)(x)$ eine Funktion $\ell : G \times X \to X$. Da $\varphi : G \to \mathrm{Bij}(X)$ ein Homomorphismus ist gilt $\varphi(gh) = \varphi(g) \circ \varphi(h)$ für alle $g, h \in G$. Für jedes Element $x \in X$ gilt daher

$$\ell(gh, x) = \varphi(gh)(x) = \varphi(g)(\varphi(h)(x)) = \varphi(g)(\ell(h, x)) = \ell(g, \ell(h, x)).$$

Außerdem muss nach Korollar 2.1 $\varphi(e)$ das neutrale Element von $\mathrm{Bij}(X)$ sein, also gilt $\varphi(e) = \mathrm{id}_X$. Damit ist aber $\ell(e, x) = x$ für alle $x \in X$, also haben wir verifiziert, dass ℓ eine Wirkung definiert. □

Beispiel 2.9. (1) Sei G eine beliebige Gruppe. Dann kann man die Gruppenoperation als Abbildung $\ell : G \times G \to G$ betrachten, also $\ell(g, h) := gh$ definieren. Die Tatsache, dass $e \in G$ ein neutrales Element ist und die Assoziativität der Gruppenoperation sagen dann gerade, dass ℓ eine Wirkung der Gruppe G auf der Menge G definiert. Nach Lemma 2.9 liefert diese Wirkung einen Homomorphismus $G \to \mathrm{Bij}(G)$. Das ist genau der Homomorphismus, den wir in 2.3 benutzt haben, um G als Untergruppe einer Bijektionsgruppe zu realisieren.

(2) Sei wieder G eine beliebige Gruppe $H \subset G$ eine Untergruppe und betrachte die Menge G/H der linken Nebenklassen. Für $g, g_1, g_2 \in G$ ist nach Lemma 2.4 $g_1H = g_2H$ äquivalent zu $(g_1)^{-1}g_2 \in H$. Nun ist aber $(gg_1)^{-1}(gg_2) = (g_1)^{-1}g^{-1}gg_2 = (g_1)^{-1}g_2$, also gilt in diesem Fall auch $(gg_1)H = (gg_2)H$. Damit kann man aber $\ell : G \times (G/H) \to G/H$ durch $\ell(g, \tilde{g}H) := (g\tilde{g})H$ definieren. Dann gilt offensichtlich $\ell(e, \tilde{g}H) = \tilde{g}H$ für alle $\tilde{g}H \in G/H$. Andererseits ist

$$\ell(g_1g_2, \tilde{g}H) = ((g_1g_2)\tilde{g})H = (g_1(g_2\tilde{g}))H = \ell(g_1, \ell(g_2, \tilde{g}H)).$$

Damit ist ℓ eine Wirkung der Gruppe G auf der Menge G/H der linken Nebenklassen.

(3) Sei Y eine Menge mit mindestens zwei Elementen, $n \in \mathbb{N}$ mit $n \geq 2$ und betrachte $X := Y^n$. Definiere ein Funktion $\alpha : X \to X$ durch $\alpha(y_1, \dots, y_n) := (y_2, \dots, y_n, y_1)$. Dann ist α offensichtlich bijektiv und $\alpha^n = \alpha \circ \dots \circ \alpha = \mathrm{id}_Y$, wobei man n Kopien von α komponiert. Betrachtet man $a \neq b \in Y$ und $(a, b, \dots, b) \in X$, dann sieht man sofort, dass $\alpha^k \neq \mathrm{id}_Y$ für $1 \leq k < n$ gilt. Das bedeutet gerade, dass α als Element der Bijektionsgruppe $\mathrm{Bij}(X)$ Ordnung n hat. Aus 2.3 wissen wir, dass daher die von α erzeugt Untergruppe von $\mathrm{Bij}(X)$ isomorph zu $\mathbb{Z}_n$ ist. Anders gesagt findet man einen injektiven Homomorphismus $\varphi : \mathbb{Z}_n \to \mathrm{Bij}(X)$ der $\varphi(\bar{1}) = \alpha$ erfüllt. Nach Lemma 2.9 bedeutet das gerade, dass wir eine natürliche Wirkung $\ell : \mathbb{Z}_n \times X \to X$ erhalten, die $\ell(\bar{k}, (y_1, \dots, y_n)) = (y_{k+1}, \dots, y_n, y_1, \dots, y_k)$ erfüllt. Man sagt, $\mathbb{Z}_n$ wirkt durch *zyklische Permutationen* auf Y^n.

Bemerkung 2.9. Motiviert durch Beispiel (1), also die Wirkung einer Gruppe auf auf sich selbst durch Multiplikation von links, werden Wirkungen oft einfach mit dem Symbol $\cdot$ bezeichnet. Man schreibt also $g \cdot x$ für $\ell(g, x)$. Die definierenden Eigenschaften einer Wirkung haben dann die Form $e \cdot x = x$ und $g_1 \cdot (g_2 \cdot x) = (g_1g_2) \cdot x$, was an die Definition des neutralen Elements bzw. an das Assoziativgesetz erinnert. Man muss aber bedenken, dass die Wirkung keine Operation auf einer Menge ist, sonder Elemente von zwei verschiedenen Mengen verknüpft. Um die Gefahr von Verwechslungen zu vermeiden werden wir diese Notation nicht verwenden.

Aus Beispiel (2) kann man für eine endliche Gruppe G ein schönes Abzählargument ableiten, dass oft überraschende Schlussfolgerungen erlaubt. Ist G endlich und $H \leq G$ eine Untergruppe, dann wissen wir ja aus Satz 2.4, dass $|H|$ ein Teiler von $|G|$ sein muss, und $|G/H| = |G|/|H|$ gilt. Beispiel (2) zeigt, dass wir einen natürlichen Homomorphismus $\varphi : G \to \mathrm{Bij}(G/H)$ erhalten. Insbesondere ist $\varphi(G)$ eine Untergruppe der Bijektionsgruppe $\mathrm{Bij}(G/H)$, die $|G/H|!$ viele Elemente hat. Daher muss $|\varphi(G)|$ ein Teiler von $|G/H|!$ sein. Nehmen wir nun an, dass $|G|$ selbst kein Teiler von $|G/H|!$ ist, dann folgt, dass φ nicht injektiv sein kann. Nach Satz 2.5 ist daher $K := \mathrm{Ker}(\varphi) \neq \{e\}$ ein Normalteiler von G. Nach Definition liegt ein Element $g \in G$ genau dann in K, wenn $g\tilde{g}H = \tilde{g}H$ für alle $\tilde{g} \in G$ gilt. Insbesondere folgt $geH = eH$, also $g \in H$, und wir erhalten:

Korollar 2.9. *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe, sodass $|G|$ kein Teiler von $|G/H|!$ ist. Dann gibt es einen Normalteiler $K \lhd G$ mit $K \neq \{e\}$ und $K \subset H$, sodass $|G/K|$ ein Teiler von $|G/H|!$ ist.*

Wir werden im nächsten Abschnitt Beispiele für die Anwendung dieses Resultats geben.

2.10. Standgruppen und Bahnen. Man stellt sich eine Wirkung einer Gruppe G auf einer Menge X am besten als Vorschrift vor, wie man die Elemente von G benutzt um Punkte der Menge X zu "bewegen". Damit stellt sich einerseits die Frage, welche

Elemente von G einen gegebenen Punkt in x nicht bewegen. Andererseits ist es natürlich zu fragen, wo man von einem gegeben Punkt $x \in X$ aus "hinkommt". Das motiviert die folgenden Definitionen.

Definition 2.10. Sei $\ell : G \times X \to X$ eine Wirkung einer Gruppe G auf einer Menge X und $x \in X$ ein Punkt.

(1) Die *Standgruppe* oder *Isotropiegruppe* von x ist $G_x := \{g \in G : \ell(g, x) = x\} \subset G$.

(2) Die *Bahn* oder der *Orbit* von x ist die Teilmenge $\mathcal{O}_x := \{\ell(g, x) : g \in G\} \subset X$.

Mit Hilfe dieser Begriffe können wir nun grundlegenden Eigenschaften von Wirkungen relativ leicht ableiten:

Satz 2.10. *Sei $\ell : G \times X \to X$ eine Wirkung einer Gruppe G auf einer Menge X. Dann gilt:*

(1) Für zwei Punkte $x, y \in X$ sind die Bahnen $\mathcal{O}_x$ und $\mathcal{O}_y$ entweder gleich oder disjunkt.

(2) Für jeden Punkt $x \in X$ ist die Standgruppe $G_x \subset G$ eine Untergruppe und es gibt eine natürliche bijektive Abbildung von der Menge G/G_x der linken Nebenklassen auf die Bahn $\mathcal{O}_x$ von x.

Beweis. (1) Falls $\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset$ gilt, sei z ein Punkt in diesem Durchschnitt. Dann gibt es nach Voraussetzung Elemente $g, h \in G$ sodass $z = \ell(g, x)$ und $z = \ell(h, y)$. Nun ist aber

$$y = \ell(h^{-1}h, y) = \ell(h^{-1}, z) = \ell(h^{-1}, \ell(g, x)) = \ell(h^{-1}g, x),$$

also $y \in \mathcal{O}_x$. Damit gilt aber für jedes $\tilde{g} \in G$ auch $\ell(\tilde{g}, y) = \ell(\tilde{g}, \ell(h^{-1}g, x)) = \ell(\tilde{g}h^{-1}g, x) \in O_x$, also $\mathcal{O}_y \subset \mathcal{O}_x$. Ganz analog zeigt man $\mathcal{O}_x \subset \mathcal{O}_y$, also sind die Bahnen gleich.

(2) Nach Definition ist $\ell(e, x) = x$, also $e \in G_x$. Für $g \in G_x$ ist $\ell(g, x) = x$, also

$$\ell(g^{-1}, x) = \ell(g^{-1}, \ell(g, x)) = \ell(g^{-1}g, x) = \ell(e, x) = x,$$

und damit $g^{-1} \in G_x$. Ist h ein weiteres Element in G_x, dann ist

$$\ell(gh, x) = \ell(g, \ell(h, x)) = \ell(g, x) = x.$$

Damit ist auch $gh \in G_x$ und die erste Aussage ist bewiesen.

Für den zweiten Teil betrachten wir die Funktion ℓ^x, die für $g \in G$ gegeben ist durch $\ell^x(g) := \ell(g, x) \in X$. Nach Definition, ist $\ell(g, x) \in \mathcal{O}_x$, also können wir ℓ^x als Funktion $G \to \mathcal{O}_x$ betrachten, die nach Definition surjektiv ist. Sind $g, h \in G$ sodass $\ell(g, x) = \ell(h, x)$ gilt, dann ist

$$x = \ell(g^{-1}, \ell(g, x)) = \ell(g^{-1}, \ell(h, x)) = \ell(g^{-1}h, x),$$

also $g^{-1}h \in G_x$. Umgekehrt folgt aus $x = \ell(g^{-1}h, x)$ natürlich

$$\ell(g, x) = \ell(g, \ell(g^{-1}h, x)) = \ell(gg^{-1}h, x) = \ell(h, x).$$

Damit ist aber $\ell^x(g) = \ell^x(h)$ genau dann erfüllt, wenn $gG_x = hG_x$ gilt, und wir erhalten eine wohldefinierte Funktion $\psi : G/G_x \to \mathcal{O}_x$, indem wir $\psi(gG_x) := \ell^x(g)$ setzen. Diese Funktion ist surjektiv, weil ℓ^x surjektiv ist und injektiv nach Konstruktion, also bijektiv. □

Ist G eine endliche Gruppe, X eine endliche Menge und $\ell : G \times X \to X$ eine Wirkung, dann erhalten wir eine interessante Aussage über die Kardinalität der Menge X: Aus Teil (1) des Satzes sehen wir, dass X die disjunkte Vereinigung der verschiedenen Bahnen der Wirkung ist. Wählen wir in jeder dieser Bahnen einen Punkt, dann erhalten wir

$x_1, \dots, x_k \in X$, sodass X die disjunkte Vereinigung der Teilmengen $\mathcal{O}_{x_1}, \dots, \mathcal{O}_{x_k} \subset X$ ist. Wir werden solche Punkte ein *Repräsentantensystem* für die G–Bahnen nennen. Aus Teil (2) des Satzes wissen wir, dass $\mathcal{O}_{x_i}$ gleich viele Elemente hat, wie die Menge G/G_{x_i} der linken Nebenklassen hat, also gilt $|\mathcal{O}_{x_i}| = |G|/|G_{x_i}|$. Damit erhalten wir:

Korollar 2.10. *Sei $\ell : G \times X \to X$ eine Wirkung einer endlichen Gruppe G auf einer endlichen Menge X und sei $\{x_1, \dots, x_k\} \subset X$ ein Repräsentantensystem für die G–Bahnen in X. Dann gilt*

$$|X| = \sum_{i=1}^{k} |\mathcal{O}_{x_i}| = \sum_{i=1}^{k} |G|/|G_{x_i}|$$

2.11. Eine Anwendung. Um die Resultate der letzten beiden Abschnitte anzuwenden, beweisen wir zunächst ein fundamentales Resultat über die Existenz von Untergruppen. Die Basis dafür ist eine kleine Variation von Beispiel 2.9 (3): Sei G eine Gruppe und $n \in \mathbb{N}$, $n \geq 2$. Dann betrachte $X := \{(g_1, \dots, g_n) \in G^n : g_1 \cdots g_n = e\} \subset G^n$. Nun liegt ein Element $(g_1, \dots, g_n)$ genau dann in X, wenn $g_1 = (g_2 \dots g_n)^{-1}$ gilt. Ist das der Fall, dann ist aber auch $(g_2 \dots g_n)g_1 = e$, also $(g_2, \dots, g_n, g_1) \in X$. Ein analoges Argument zeigt, dass für $(g_1, \dots, g_n) \in X$ auch $(g_n, g_1, \dots, g_{n-1})$ in X liegt. Das bedeutet aber gerade, dass man $\alpha(g_1, \dots, g_n) := (g_2, \dots, g_n, g_1)$ eine Bijektion der Menge X definiert. Damit erhalten wir wie in Beispiel 2.9 (3) eine Wirkung von $\mathbb{Z}_n$ auf X.

Ist G eine endliche Gruppe, dann erlaubt die obige Überlegung auch, die Kardinalität $|X|$ zu bestimmen. Da $(g_1, \dots, g_n) \in X$ genau dann gilt, wenn $g_1 = (g_2 \dots g_n)^{-1}$, kann man $g_2, \dots, g_n \in G$ beliebig wählen und erhält ein eindeutiges Element

$$((g_2 \dots g_n)^{-1}, g_2, \dots, g_n) \in X.$$

Somit ist $|X| = |G|^{n-1}$. Mit Hilfe dieser Überlegungen beweisen wir nun:

Proposition 2.11. *Sei G eine endliche Gruppe und $p \in \mathbb{N}$ eine Primzahl, die $|G|$ teilt. Dann enthält G mindestens ein Element der Ordnung p und damit eine p–elementige Untergruppe, die isomorph zu $\mathbb{Z}_p$ ist.*

Beweis. Betrachte die oben beschriebene Wirkung von $\mathbb{Z}_p$ auf

$$X := \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = e\}.$$

Für jeden Punkt $x \in X$ ist die Standgruppe $(\mathbb{Z}_p)_x$ nach Satz 2.10 eine Untergruppe von $\mathbb{Z}_p$. Da p prim ist, muss diese Gruppe also entweder gleich $\{e\}$ oder gleich $\mathbb{Z}_p$ sein. Im ersten Fall steht $\mathcal{O}_x$ in bijektiver Korrespondenz mit $\mathbb{Z}_p$, also ist $|\mathcal{O}_x| = p$. Im zweiten Fall ist $\mathcal{O}_x = \{x\}$ also $|\mathcal{O}_x| = 1$. Dieser zweite Fall kann aber offensichtlich nur dann eintreten, wenn $x = (g, \dots, g)$ für ein Element $g \in G$ gilt, dass dann nach Definition $g^p = g \dots g = e$ erfüllt. Das gilt sicher für $g = e$. Für $g \neq e$ ist die Ordnung von g größer als 1, aber wegen $g^p = e$ muss diese Ordnung ein Teiler von p und somit gleich p sein.

Wählen wir nun eine Repräsentantensystem $\{x_1, \dots, x_N\}$ für die $\mathbb{Z}_p$–Orbits in X dann können wir das so tun, dass $x_1 = (e, \dots, e)$ gilt, $x_2, \dots, x_k$ von der Form $(g, \dots, g)$ für Elemente der Ordnung p sind (falls diese existieren) und $|\mathcal{O}_{x_i}| = p$ für $i > k$ gilt. Schreiben wir $|G| = ap$ für $a \in \mathbb{N}$, dann erhalten wir aus Korollar 2.10:

$$a^{p-1}p^{p-1} = |G|^{p-1} = |X| = \sum_{i=1}^{N} |\mathcal{O}_{x_i}| = k + (N-k)p$$

Damit erhalten wir aber $k = (a^{p-1}p^{p-2} + k - N)p$ und da $k \geq 1$ ist, muss k ein nichttriviales Vielfaches von p sein. Insbesondere ist $k > 1$. □

In Verbindung mit Korollar 2.9 kann man dieses Resultat benutzen um nicht nur die Existenz von Untergruppen, sondern auch die Existenz von Normalteilern zu beweisen.

Beispiel 2.11. Seien $p > q$ Primzahlen und sei G eine Gruppe der Ordnung $|G| = pq$. (Solche Gruppen werden manchmal pq–Gruppen genannt.) Dann ist p ein Teiler von $|G|$, also erhalten wir aus Proposition 2.11 eine Untergruppe $H \leq G$ mit $H \cong \mathbb{Z}_p$. Dann ist $|G/H| = (pq)/p = q$ und nach Voraussetzung ist $p > q$ und damit kein Teiler von $q!$. Damit kann aber auch $|G| = pq$ kein Teiler von $q!$ sein. Nach Korollar 2.9 muss es einen Normalteiler $K \triangleleft G$ mit $K \neq \{e\}$ und $K \subset H$ geben. Damit ist $|K| > 1$ und weil $K \leq H$ gilt, folgt $|K| = p$ und damit $K = H$.

Damit sehen wir, dass G einen Normalteiler K enthält, der isomorph zu $\mathbb{Z}_p$ ist. Die Gruppe G/K hat dann Ordnung q, also ist $G/K \cong \mathbb{Z}_q$ nach Korollar 2.4.

Für $p = 3$ und $q = 2$ reproduziert das unserer Resultate über die 6–elementige Gruppe $\mathfrak{S}_3$ aus 2.7.

Bemerkung 2.11. Mit ähnlichen Methoden kann man auch stärkere Sätze über die Existenz von Untergruppen in einer endlichen Gruppe G beweisen. Zum Beispiel gibt es für jede Primzahl p und jedes $m \in \mathbb{N}$, sodass p^m die Ordnung $|G|$ teilt, eine Untergruppe $H \leq G$ mit $|H| = p^m$. Ist m maximal mit dieser Eigenschaft, dann kann man auch genauere Aussagen darüber machen, wie viele solche Untergruppen (sogenannte "p–Sylow–Untergruppen") es gibt.

2.12. Konjugationsklassen. Weitere Anwendungen unserer Abzählargumente erhalten wir aus einer natürlichen Wirkung einer beliebigen Gruppe G auf sich selbst. Dazu führen wir zunächst einige Begriffe ein.

Definition 2.12. Sei G eine Gruppe.

(1) Zwei Elemente $x, y \in G$ heißen *konjugiert*, wenn es ein Element $g \in G$ gibt, sodass $y = gxg^{-1}$ gilt. Die Menge $\mathcal{C}(x)$ aller zu x konjugierten Elemente heißt die *Konjugationsklasse* von x.

(2) Für ein Element $x \in G$ ist der *Zentralisator* von x in G die Teilmenge $Z_x := \{g \in G : gx = xg\} \subset G$.

(3) Das *Zentrum* von G ist die Teilmenge $Z(G) := \{g \in G : gh = hg \quad \forall h \in G\}$.

Betrachten wir die Abbildung $\ell : G \times G \to G$, die gegeben ist durch $\ell(g, x) := gxg^{-1}$. Dann ist natürlich $\ell(e, x) = x$ für alle $x \in G$. Außerdem ist

$$\ell(g, \ell(h, x)) = \ell(g, hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \ell(gh, x),$$

also definiert ℓ eine Wirkung von G auf sich selbst. Nach Definition ist die Standgruppe von x bezüglich dieser Wirkung genau der Zentralisator $Z_x \subset G$, also ist Z_x immer eine Untergruppe von G. Ebenfalls nach Definition ist die Bahn von x unter dieser Wirkung genau die Konjugationsklasse $\mathcal{C}(x)$ von x. Nach Satz 2.10 steht somit $\mathcal{C}(x)$ in bijektiver Korrespondenz mit G/C_x, also gilt insbesondere $|\mathcal{C}(x)| = |G|/|Z_x|$. Schließlich ist $Z(G)$ nach Definition der Durchschnitt $\cap_{x \in G} Z_x$ und damit eine (nach Definition kommutative) Untergruppe von G. Für $g \in Z(G)$ und $h \in G$ ist $hgh^{-1} = ghh^{-1} = g \in Z(G)$, also ist das Zentrum sogar ein Normalteiler in G. Umgekehrt ist $gx = xg$ äquivalent zu $gxg^{-1} = x$ und damit $x \in Z(G)$ äquivalent zu $Z_x = G$ und zu $\mathcal{C}(x) = \{x\}$.

Wenden wir auf diese Wirkung nun die Resultate aus 2.10 an, dann sehen wir, dass G die disjunkte Vereinigung der Konjugationsklassen ist. Für $x \in Z(G)$ haben wir jeweils $\mathcal{C}(x) = \{x\}$, alle anderen Elemente haben Konjugationsklassen mit mehr als einem Element, die disjunkt zu $Z(G)$ sind.

Ist G endlich, dann sei $\{x_1, \ldots, x_n\}$ ein Repräsentantensystem für jene Konjugationsklassen, die nicht in $Z(G)$ liegen. Dann können wir Korollar 2.10 zur sogenannten

Klassengleichung spezialisieren:

$$|G| = \sum_{x \in Z(G)} |\{x\}| + \sum_{i=1}^{n} |\mathcal{C}(x_i)| = |Z(G)| + \sum_{i=1}^{n} (|G|/|Z_{x_i}|).$$

Beispiel 2.12. (1) Sei p eine Primzahl und G eine sogenannte p–Gruppe, also eine Gruppe der Ordnung p^m für ein $m \in \mathbb{N}$. Dann behaupten wir, dass G nichttriviales Zentrum hat, also $Z(G) \neq \{e\}$ gilt. Da $|G| = p^m$ gilt, muss jede Untergruppe $H \leq G$ Ordnung p^k für ein $k \leq m$ haben. Ist insbesondere $\{x_1, \ldots, x_n\}$ ein Repräsentantensystem für die Konjugationsklassen, die nicht in $Z(G)$ liegen, dann ist $|Z_{x_i}| = k_i$ für ein $k_i < m$ (weil $Z_x = G$ nur für $x \in Z(G)$ gilt), also $|G|/|Z_{x_i}| = p^{m-k_i}$, und das ist eine positive Potenz von p. Also hat die Klassengleichung die Form

$$p^m = |Z(G)| + \sum_{i=1}^{n} p^{m-k_i}.$$

Klarerweise ist die linke Seite kongruent zu 0 modulo p und weil $m - k_i > 0$ für alle i gilt, ist die rechte Seite kongruent zu $|Z(G)|$ modulo p. Da $|Z(G)| \geq 1$ gilt, muss also $|Z(G)| > 1$ gelten.

(2) Sei wieder p eine Primzahl und G eine Gruppe der Ordnung p^2. Dann behaupten wir, dass G kommutativ ist. Wäre G nicht kommutativ, dann wäre $Z(G) \neq G$ und aus Beispiel (1) wissen wir, dass $Z(G) \neq \{e\}$ ist, also muss $|Z(G)| = p$ gelten. Sei nun $x \in G \setminus Z(G)$, dann ist $Z_x \neq \{e\}$ (sonst wäre $\mathcal{C}(x) = G$) und $Z_x \neq G$, sonst wäre $x \in Z(G)$. Damit gilt aber $|Z_x| = p$. Offensichtlich ist aber $Z(G) \subset Z_x$, also muss $Z_x = Z(G)$ gelten. Da aber offensichtlich auch $x \in Z_x$ gelten muss, ist $x \in Z(G)$, ein Widerspruch.

Einschub: Kommutative Gruppen

Das Wort "Einschub" im Titel kommt daher, dass aus Sicht der Algebra die Theorie der kommutativen Gruppen eigentlich *nicht* Teil der Gruppentheorie ist. Eine kommutative Gruppe trägt nämlich automatisch eine weitere Struktur, die der eines Vektorraumes sehr ähnlich ist, und diese Struktur ist der Schlüssel zum Verständnis solcher Gruppen. Wir werden in diesem Abschnitt die Operation auf einer kommutativen Gruppe immer additiv schreiben.

2.13. Im Prinzip kennen wir die zusätzliche Struktur auf einer kommutativen Gruppen schon aus Abschnitt 2.3. Sei also $(G, +)$ eine kommutative Gruppe. Dann können wir für $g \in G$ die Potenzen g^k für $k \in \mathbb{Z}$ wie in 2.3 betrachten. Nach Definition ist $g^1 = g$ und g^{-1} das inverse Element zu g, das man bei der additiven Schreibweise natürlich mit $-g$ bezeichnet. Für $k > 0$ ist nun $g^k = g + \cdots + g$ (mit k Faktoren), das man in natürlicher Weise mit $k \cdot g$ bezeichnen kann. Für $k < 0$ ist g^k das inverse Element zu g^{-k}, also ist auch dafür die Bezeichnung $k \cdot g$ passend. Wegen der Kommutativität von G gilt natürlich für $g, h \in G$ die Gleichung

$$2 \cdot (g + h) = g + h + g + h = g + g + h + h = (2 \cdot g) + (2 \cdot h),$$

und induktiv zeigt man leicht, dass $k \cdot (g + h) = (k \cdot g) + (k \cdot h)$ für alle $k \in \mathbb{Z}$ gilt. Natürlich gilt auch $(k_1 + k_2) \cdot g = k_1 \cdot g + k_2 \cdot g$ (erste Summe in $\mathbb{Z}$, zweite in G), $(k_1 k_2) \cdot g = k_1 \cdot (k_2 \cdot g)$ und $1 \cdot g = g$ für alle $k_1, k_2 \in \mathbb{Z}$ und alle $g \in G$. Betrachtet man $\cdot$ als Operation $\mathbb{Z} \times G \to G$, dann sind das (zusammen mit der Tatsache, dass $(G, +)$ eine kommutative Gruppe ist) genau die definierenden Eigenschaften eines Vektorraumes,

nur dass $\mathbb{Z}$ kein Körper sondern "nur" ein kommutativer Ring mit Einselement ist. In diesem Fall spricht man dann nicht von Vektorräumen sondern von *Moduln*.

Damit sehen wir, dass jede kommutative Gruppe $(G,+)$ automatisch ein $\mathbb{Z}$–Modul ist. Da umgekehrt jeder $\mathbb{Z}$–Modul nach Definition zunächst einmal eine kommutative Gruppe ist, sind die beiden Begriffe "das gleiche". Ist H eine Untergruppe von $(G,+)$ dann folgt aus der Definition natürlich sofort, dass $k\cdot h \in H$ für alle $h \in H$ und $k \in \mathbb{Z}$ gilt, also ist H automatisch ein $\mathbb{Z}$–Teilmodul von G (der analoge Begriff zu einem Teilraum). Betrachtet man insbesondere die additive Gruppe $(\mathbb{Z},+)$ als kommutative Gruppe, dann liefert die obige Definition von $\cdot$ genau die übliche Multiplikation $\cdot : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ auf $\mathbb{Z}$. Die gerade gemachte Beobachtung über Untergruppen zeigt nun, dass jede Untergruppe von $(\mathbb{Z},+)$ automatisch abgeschlossen unter der Multiplikation mit beliebigen Elementen von $\mathbb{Z}$ ist. (Wir werden so eine Teilmenge später ein *Ideal* in $\mathbb{Z}$ nennen.) Das liefert auch die Erklärung, warum die Multiplikation auf $\mathbb{Z}$ so eine wichtige Rolle in der Beschreibung der Untergruppen von $(\mathbb{Z},+)$ spielt, siehe 2.3.

Eine weitere "Spezialität" von kommutativen Gruppen ist, dass das Produkt neben der in Proposition 2.7 beschriebenen Eigenschaft eine weitere schöne Eigenschaft hat, die für allgemeine Gruppen nicht gilt. Sind G_1 und G_2 Gruppen, dann gibt es neben den beiden Projektionen $G_1 \times G_2 \to G_i$ auch natürliche Inklusionen $j_i : G_i \to G_1 \times G_2$ für $i = 1, 2$. Diese sind gegeben durch $j_1(g_1) := (g_1, e)$ und $j_2(g_2) = (e, g_2)$, wobei wir die neutralen Elemente beider Gruppen mit e bezeichnen. Aus der Definition der Multiplikation folgt sofort, dass j_1 und j_2 Homomorphismen sind.

Nehmen nun an, dass G_1 und G_2 kommutativ sind und dass H eine weitere kommutative Gruppe ist und dass $\varphi_i : G_i \to H$ für $i = 1, 2$ ein Homomorphismus ist. Dann schreiben wir alle Gruppen additiv und definieren wir $\psi : G_1 \times G_2 \to H$ durch $\psi(g_1, g_2) := \varphi_1(g_1) + \varphi_2(g_2)$. Dann gilt nach Konstruktion $(\psi \circ j_1)(g_1) = \varphi_1(g_1) + \varphi_2(e)$, also $\psi \circ j_1 = \varphi_1$ und analog folgt $\psi \circ j_2 = \varphi_2$. Außerdem gilt für $g_i, h_i \in G_i$

$$\begin{aligned}\psi((g_1, g_2) + (h_1, h_2)) &= \psi(g_1 + h_1, g_2 + h_2) = \varphi_1(g_1 + h_1) + \varphi_2(g_2 + h_2)\\ &= \varphi_1(g_1) + \varphi_1(h_1) + \varphi_2(g_2) + \varphi_2(h_2).\end{aligned}$$

Da H kommutativ ist, kann man die mittleren beiden Terme vertauschen, und erhält dann sofort $\psi(g_1, g_2) + \psi(h_1, h_2)$, also ist ψ ein Homomorphismus. Da man für $g_i \in G_i$ das Element (g_1, g_2) offensichtlich als $j_1(g_1) + j_2(g_2)$ schreiben kann folgt, dass jeder Homomorphismus $\psi : G_1 \times G_2 \to H$ durch $\psi \circ j_1$ und $\psi \circ j_2$ eindeutig bestimmt ist. Man erhält also eine ganz analoge (genauer gesagt eine *duale*) Eigenschaft zu der in Proposition 2.7 beschriebenen. Wegen dieser Eigenschaft nennt man das Produkt kommutativer Gruppen oft auch die *direkte Summe* und bezeichnet es mit $G_1 \oplus G_2$. Das ist auch ganz analog zur direkten Summe von Vektorräumen in der linearen Algebra.

Man bemerke, dass die gerade angeführte Eigenschaft nicht für allgemeine Gruppen H funktionieren kann. Das können wir ganz einfach an einem Beispiel sehen. Betrachten wir $G_1 = G_2 = \mathbb{Z}_2$, dann hat $\mathbb{Z}_2 \times \mathbb{Z}_2$ Ordnung 4. Nehmen wir nun $H = \mathfrak{S}_3$, dann wissen wir schon, dass die Transpositionen $\tau_1 := (1, 2)$ und $\tau_2 := (2, 3)$ in H Elemente der Ordnung 2 sind, also die von einer dieser Transpositionen erzeugte Untergruppe isomorph zu $\mathbb{Z}_2$ ist. Entsprechend erhalten wir Homomorphismen $\varphi_i : \mathbb{Z}_2 \to \mathfrak{S}_3$, die $\varphi_i(\bar{1}) = \tau_i$ für $i = 1, 2$ erfüllen. Gäbe es einen Homomorphismus $\psi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathfrak{S}_3$, sodass $\psi \circ j_i = \varphi_i$ für $i = 1, 2$ gilt, dann wäre das Bild $\mathrm{Im}(\varphi)$ eine Untergruppe von $\mathfrak{S}_3$, die höchstens 4 Elemente haben kann. Andererseits wissen wir aber aus Beispiel 2.8, dass $\{\tau_1, \tau_2\}$ ein Erzeugendensystem für $\mathfrak{S}_3$ ist, also müsste $\mathrm{Im}(\varphi) = \mathfrak{S}_3$ gelten. Das ist sowohl aus Gründen der Kardinalität als auch wegen der Kommutativität von $\mathrm{Im}(\varphi)$ ein Widerspruch.

2.14. Die Klassifikation der endlich erzeugten kommutativen Gruppen. Der Beweis des fundamentalen Klassifikationsresultats für kommutative Gruppen beruht ganz auf der Struktur als $\mathbb{Z}$–Moduln, die wir in 2.13 besprochen haben. Wir werden daher hier kaum auf den Beweis eingehen, sondern nur das Resultat formulieren. Wir werden im Kapitel über Ringe etwas zum Beweis sagen.

Wir betrachten also eine kommutative Gruppe $(G, +)$, die ein endliches Erzeugendensystem besitzt. Eine weitere Eigenschaft, die spezifisch für kommutative Gruppen gilt, ist dass die Summe von zwei Elementen endlicher Ordnung selbst wieder endliche Ordnung hat. Es ist nämlich $k \cdot (g + h) = k \cdot g + k \cdot h$ und daraus folgt sofort, dass für $g, h \in G$ mit endlicher Ordnung die Ordnung von $g + h$ gleich dem kleinsten gemeinsamen Vielfachen der Ordnungen von g und h ist. (In einer allgemeinen Gruppe ist etwa $(gh)^2 = ghgh$ und das hat a priori nichts mit g^2 und h^2 zu tun.) Damit folgt aber sofort, dass für eine kommutative Gruppe G die Elemente endlicher Ordnung eine Untergruppe bilden, die sogenannte *Torsionsuntergruppe* $\mathrm{Tors}(G)$ von G.

Man zeigt dann einerseits, dass es eine Untergruppe $H \subset G$ gibt, sodass $G \cong \mathrm{Tors}(G) \oplus H$ und sodass H endlich erzeugt und *frei* ist, das heißt als $\mathbb{Z}$–Modul eine endliche Basis besitzt (die ganz analog definiert ist, wie in der linearen Algebra). Insbesondere ist $H \cong \mathbb{Z}^r$ für eine Zahl $r \in \mathbb{N}$. Es stellt sich heraus, dass diese Zahl nicht von irgendwelchen Wahlen abhängt, sondern nur von der ursprünglichen Gruppe G. Mann nennt r den *Rang* von G.

Andererseits kann man die Struktur von $\mathrm{Tors}(G)$ analysieren. Es stellt sich heraus, dass man die Torsionsuntergruppe als direkte Summe von endlich vielen Gruppen der Form $\mathbb{Z}_n$ ist. Man kann die auftretenden Gruppen noch etwas genauer beschreiben, es stellt sich nämlich heraus, dass man nur Primzahlpotenzen betrachten muss. Damit erhält man:

Satz 2.14. *Sei G eine endliche erzeugte kommutative Gruppe. Dann existieren eindeutige Zahlen $r, s \in \mathbb{N}$ sowie Primzahlen $p_1, \dots, p_s$ (eindeutig bis auf die Reihenfolge) und $k_1, \dots, k_s \in \mathbb{N} \setminus \{0\}$ sodass G isomorph ist zu $\mathbb{Z}^r \oplus \oplus_{i=1}^s \mathbb{Z}_{(p_i)^{k_i}}$.*

Exkurs: Zur Klassifikation von Gruppen

Wir werden an dieser Stelle nur einige wenige Hinweise darauf geben, wie man etwas Ordnung in den (ziemlich großen und komplizierten) "Zoo" der Gruppen bringen kann.

2.15. Die obere Zentralreihe. Der Ausgangspunkt unserer Überlegungen ist, dass man mit Hilfe von Satz 2.14 endlich erzeugte(und insbesondere endliche) kommutative Gruppen vollständig versteht. Aus 2.7 wissen wir schon, dass man gewisse nicht–kommutative Gruppen aus kommutativen Gruppen "aufbauen" kann. Insbesondere haben wir dort gesehen, dass die Permutationsgruppe $\mathfrak{S}_n$ einen Normalteiler $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ besitzt, sodass $\mathfrak{S}_n/\mathfrak{A}_n \cong Z_2$ gilt. Im Fall $n = 3$ ist $\mathfrak{A}_3 \cong \mathbb{Z}_3$, also ebenfalls kommutativ.

Zum Studium der (Nicht–)Kommutativität ist es handlich, folgendes Konzept zu verwenden: Für Elemente g und h einer Gruppe g definiert man den *Kommutator* $[g, h]$ von g und h durch

$$[g, h] := gh(hg)^{-1} = ghg^{-1}h^{-1}.$$

Offensichtlich gilt $[g, h] = e$ genau dann, wenn $gh = hg$ gilt, siehe Proposition 2.1. Aus Korollar 2.1 folgt sofort, dass für einen Homomorphismus $\varphi : G \to H$ zwischen zwei Gruppen und Elemente $g_1, g_2 \in g$ die Gleichung $\varphi([g_1, g_2]) = [\varphi(g_1), \varphi(g_2)]$ gilt.

In 2.12 haben wir gesehen, dass jede Gruppe einen natürlichen kommutativen Normalteiler hat, nämlich das Zentrum $Z(G)$. (Es kann passieren, dass $Z(G) = \{e\}$ gilt,

was zum Beispiel auf $\mathfrak{S}_3$ zutrifft.) In Termen von Kommutatoren gilt

$$Z(G) = \{g \in G : [g,h] = e \quad \forall h \in G\}.$$

Ist $Z_0 := Z(G) \neq \{e\}$, dann kann man den Quotienten G/Z_0 bilden. Dieser Quotient kann selbst wieder ein Zentrum haben, und man kann leicht sehen, wie das Urbild dieses Zentrums in G aussieht. Dazu sei $\pi : G \to \tilde{G} := G/Z_0$ der kanonische Quotientenhomomorphismus, der ja surjektiv ist. Damit ist aber $\pi(g) \in Z(\tilde{G})$ genau dann, wenn $e = [\pi(g), \pi(h)] = \pi([g,h])$ für alle $h \in G$ gilt. Damit ist aber

$$Z_1 := \pi^{-1}(Z(\tilde{G})) = \{g \in G : [g,h] \in Z(G) \quad \forall h \in G\}.$$

Offensichtlich ist $Z_0 \subset Z_1$ und nach Proposition 2.5 ist Z_1 ein Normalteiler in G. Außerdem ist $\pi(Z_1) \cong Z_1/Z_0$ die kommutative Gruppe $Z(\tilde{G})$. Das kann man nun induktiv fortsetzen indem man für $i \geq 1$ induktive $Z_{i+1} \subset G$ als

$$Z_{i+1} := \{g \in G : [g,h] \in Z_i \quad \forall h \in G\}.$$

Offensichtlich ist Z_2 das Urbild des Zentrums von G/Z_1 unter dem kanonischen Quotientenhomomorphismus, also insbesondere ein Normalteiler in G. Damit ist $\pi(Z_2) \cong Z_2/Z_1$ die kommutative Gruppe $Z(G/Z_1)$. Induktiv folgt, dass jedes Z_{i+1} das Urbild des Zentrums in G/Z_i und damit ein Normalteiler in G ist und dass die Gruppe Z_{i+1}/Z_i kommutativ ist. Man erhält damit eine Folge

$$Z_0 \subset Z_1 \subset Z_2 \subset \dots$$

in G, die man die *obere Zentralreihe* von G nennt.

Es kann in jedem Schritt passieren, dass das Zentrum von G/Z_i nur aus dem neutralen Element e besteht. Ist das der Fall, dann ist $Z_{i+1} = Z_i$ und in Folge natürlich $Z_k = Z_i$ für alle $k \geq i$. In diesem Fall sagt man, *die obere Zentralreihe stabilisiert sich* bei einer echten Untergruppe von G.

Andererseits kann an irgendeiner Stelle $Z_{i+1} = G$ gelten, man sagt dann, *die obere Zentralreihe* ist endlich. Ist das der Fall, dann ist natürlich G/Z_i kommutativ. Nun enthält Z_1 den kommutativen Normalteiler Z_0 und Z_1/Z_0 ist ebenfalls kommutativ. Also kann man Z_1 aus kommutativen Gruppen aufbauen. Z_2 enthält Z_1 als Normalteiler und Z_2/Z_1 ist kommutativ, also kann man auch Z_2 aus kommutativen Gruppen aufbauen. Macht man so weiter, dann gelangt man (im Fall dass die obere Zentralreihe endlich ist) in endlich vielen Schritten bis zur Gruppe G, kann also G aus kommutativen Gruppen aufbauen.

2.16. Auflösbare Gruppen. Wie wir oben schon bemerkt haben, bricht die obere Zentralreihe für die Permutationsgruppe $\mathfrak{S}_3$ sofort ab, weil $Z_0 = \{e\}$ und damit $Z_i = \{e\}$ für alle $i \in \mathbb{N}$ gilt. Tatsächlich wissen wir aber aus 2.7, dass $\mathfrak{S}_3$ den Normalteiler $\mathfrak{A}_3 \cong \mathbb{Z}_3$ enthält und $\mathfrak{S}_3/\mathfrak{A}_3 \cong \mathbb{Z}_2$ ebenfalls kommutativ ist. Es stellt sich heraus, dass der "richtige" Begriff dadurch erhalten wird, dass man kommutative Quotienten studiert.

Sei also G eine Gruppe und $N \lhd G$ ein Normalteiler und $\pi : G \to G/N$ der kanonische Quotientenhomomorphismus. Dann ist G/N genau dann kommutativ, wenn $0 = [\pi(g), \pi(h)] = \pi([g,h])$ und damit $[g,h] \in N$ für alle $g, h \in G$ gilt. Damit G/N möglichst groß wir, muss N möglichst klein sein. Es gibt eine offensichtliche minimale Wahl für N, nämlich den von $\{[g,h] : g,h \in G\} \subset G$ erzeugten Normalteiler. Es stellt sich heraus, dass die von dieser Menge erzeugte Untergruppe, die üblicherweise mit $[G,G]$ bezeichnet und die *Kommutatoruntergruppe* von G genannt wird, automatisch ein Normalteiler in G ist. Somit ist G/N genau dann kommutativ, wenn $N \supset [G,G]$

gilt. Der maximale kommutative Quotient $G_{ab} := G/[G,G]$ von G heißt die *Abelisierung* von G. Er besitzt eine universelle Eigenschaft:

Proposition 2.16. *Sei G eine Gruppe und $\pi : G \to G/[G,G] = G_{ab}$ der kanonische Quotientenhomomorphismus in die Abelisierung.*

Ist H eine beliebige kommutative Gruppe und $\varphi : G \to H$ ein Homomorphismus, dann existiert ein eindeutiger Homomorphismus $\underline{\varphi} : G_{ab} \to H$, sodass $\varphi = \underline{\varphi} \circ \pi$.

Beweis. Da H kommutativ ist, gilt für beliebige Elemente $g_1, g_2 \in G$ die Gleichung

$$e = [\varphi(g_1), \varphi(g_2)] = \varphi([g_1, g_2]),$$

also $[g_1, g_2] \in \mathrm{Ker}(\varphi)$. Da $\mathrm{Ker}(\varphi) \subset G$ nach Satz 2.5 ein Normalteiler ist, folgt $[G,G] \subset \mathrm{Ker}(\varphi)$. Damit folgt die Behauptung aus Satz 2.6. □

Beginne nun mit G und betrachte die Kommutatoruntergruppe $G^{(2)} := [G,G]$. Das ist selbst wieder eine Gruppe, also kann man $G^{(3)} := [G^{(2)}, G^{(2)}]$ und induktiv $G^{(k)}$ für alle $k \in \mathbb{N}$ durch $G^{(i+1)} := [G^{(i)}, G^{(i)}]$ definieren. So erhält man eine Folge

$$G \supset G^{(2)} \supset G^{(3)} \supset \dots$$

von Untergruppen in G, die *derivierte Reihe* von G. Nach Konstruktion ist jede $G^{(i)}$ ein Normalteiler in $G^{(i-1)}$ und $G^{(i-1)}/G^{(i)}$ ist eine kommutative Gruppe.

Man nennt die Gruppe G *auflösbar*, wenn $G^{(k)} = \{e\}$ für ein $k \in \mathbb{N}$ gilt. (Der Grund für diesen Namen wird später noch klarer werden.) Ist das der Fall, dann gilt $[g,h] = e$ für alle $g, h \in G^{(k-1)}$, also ist $G^{(k-1)}$ kommutativ. Die Gruppe $G^{(k-2)}$ enthält dann den kommutativen Normalteiler $G^{(k-1)}$ und $G^{(k-2)}/G^{(k-1)}$ ist kommutativ. Damit kann man $G^{(k-2)}$ aus kommutativen Gruppen "aufbauen". Die nächstgrößere Gruppe $G^{(k-3)}$ enthält $G^{(k-2)}$ als Normalteiler, sodass $G^{(k-3)}/G^{(k-2)}$ kommutativ ist, also kann man auch sie aus kommutativen Gruppen aufbauen. Schritt für Schritt sieht man so, dass man eine auflösbare Gruppe G aus kommutativen Gruppen "aufbauen" kann.

Einer der großen Vorteile des Auflösbarkeitsbegriffes ist dass er sich gut vererbt, und zwar sowohl auf Untergruppen als auch auf Quotienten und dass auch noch eine Umkehrung des Vererbungsresultats gilt:

Satz 2.16. *Sei G eine Gruppe, $H \leq G$ eine Untergruppe und $N \triangleleft G$ ein Normalteiler.*
(1) Ist G auflösbar, dann sind auch H und G/N auflösbar.
(2) Sind N und G/N auflösbar, dann ist G auflösbar.

Beweisskizze. (1) Da $H \leq G$ gilt, ist jeder Kommutator in H ein Kommutator in G und daraus folgt leicht, dass $[H,H] \subset [G,G]$, also $H^{(2)} \subset G^{(2)}$. Induktiv folgt $H^{(i)} \subset G^{(i)}$ für alle $i \in \mathbb{N}$.

Sei $\pi : G \to G/N$ der kanonische Quotientenhomomorphismus. Für $x_1, x_2 \in G/N$ finden wir $g_1, g_2 \in G$, sodass $x_i = \pi(g_i)$ für $i = 1, 2$ gilt. Dann ist aber auch

$$[x_1, x_2] = [\pi(g_1), \pi(g_2)] = \pi([g_1, g_2]).$$

Damit ist $\pi([G,G]) \subset G/N$ eine Untergruppe, die alle Kommutatoren enthält, und es folgt $[G/N, G/N] \subset \pi([G,G])$, also $(G/N)^{(2)} \subset \pi(G^{(2)})$. Induktiv erhält man wieder $(G/N)^{(i)} \subset \pi(G^{(i)})$ für alle $i \in \mathbb{N}$.

Ist nun G auflösbar, dann gibt es ein $k \in \mathbb{N}$, sodass $G^{(k)} = \{e\}$ gilt. Für diesen Index ist dann aber auch $H^{(k)} = \{e\}$ und $\pi(G^{(k)}) = \{e\}$ und damit $(G/N)^{(k)} = \{e\}$.

(2) Da G/N auflösbar ist, gibt es einen Index k, sodass $(G/N)^{(k)} = \{e\}$ ist. Wir behaupten, dass dann $G^{(k)} \subset N$ gilt und beweisen das durch Induktion nach k. Ist $k = 2$, dann ist G/N kommutativ, also wissen wir schon, dass $[G,G] = G^{(2)} \subset N$ gilt.

Ist $k > 2$ und die Behauptung für $k-1$ bewiesen, dann betrachten wir den Normalteiler $(G/N)^{(2)} \subset G/N$. Sein Urbild $\tilde{G} := \pi^{-1}((G/N)^{(2)}) \subset G$ ist nach Proposition 2.5 ein Normalteiler in G, der N enthält. Natürlich ist $\tilde{G}/N \cong (G/N)^{(2)}$ via $\pi|_{\tilde{G}}$ und nach Konstruktion ist $(\tilde{G}/N)^{(i)} = (G/N)^{(i+1)}$. Damit folgt laut Induktionsannahme $\tilde{G}^{(k-1)} \subset N$.

Andererseits überlegt man leicht, dass $\pi : G \to G/N$ einen Isomorphismus von $G/\tilde{G}$ auf die kommutative Gruppe $(G/N)/(G/N)^{(2)}$ induziert. Damit ist aber $[G, G] \subset \tilde{G}$, induktiv folgt $G^{(i)} \subset \tilde{G}^{(i-1)}$ und damit $G^{(k)} \subset \tilde{G}^{(k-1)} \subset N$.

Nachdem wir nun wissen, dass $G^{(k)} \subset N$ gilt, folgt $G^{(k+1)} \subset N^{(2)}$ und induktiv $G^{(k+i)} \subset N^{(i+1)}$. Da N auflösbar ist, gibt es einen Index, sodass $N^{(\ell)} = \{e\}$ gilt und damit ist $G^{(k+\ell-1)} = \{e\}$. □

Kann man nun eine Gruppe Schritt für Schritt aus kommutativen Gruppen aufbauen, dann zeigt Teil (2) der Proposition, dass man dabei die Klasse der auflösbaren Gruppen niemals verlässt. In diesem Sinn sind die auflösbaren Gruppen also genau jene Gruppen, die man aus kommutativen Gruppen aufbauen kann.

Beispiel 2.16. Betrachten wir wieder die Permutationsgruppen $\mathfrak{S}_n$ für $n \geq 2$. Aus 2.7 kennen wir den Homomorphismus sgn : $\mathfrak{S}_n \to \mathbb{Z}_2$ und seinen Kern $\mathfrak{A}_n$, die alternierende Gruppe. Da $\mathbb{Z}_2$ kommutativ ist, gilt $\mathfrak{A}_n \supset [\mathfrak{S}_n, \mathfrak{S}_n]$ und man kann elementar zeigen, dass immer Gleichheit gilt. In Fall $n = 3$ ist das offensichtlich, weil wir wissen, dass $\mathfrak{A}_3$ Ordnung 3 hat. Nun ist $[\mathfrak{S}_3, \mathfrak{S}_3] \subset \mathfrak{A}_3$ eine Untergruppe, kann also nur Ordnung 1 oder 3 haben (und damit gleich $\mathfrak{A}_3$ sein). Ordnung 1 ist aber nicht möglich, sonst wäre $[\mathfrak{S}_3, \mathfrak{S}_3] = \{e\}$, also $\mathfrak{S}_3$ kommutativ. Für $n = 3$ ist $(\mathfrak{S}_3)^{(2)} = \mathfrak{A}_3 \cong \mathbb{Z}_3$ kommutativ, also ist $(\mathfrak{S}_3)^{(3)} = \{e\}$ und damit $\mathfrak{S}_3$ auflösbar.

Betrachten wir als nächstes $\mathfrak{A}_4 \subset \mathfrak{S}_4$. Die Ordnung von $\mathfrak{S}_4$ ist $4! = 24$, also hat $\mathfrak{A}_4$ Ordnung 12. Man kann nur direkt zeigen, dass $\mathfrak{A}_4$ einen Normalteiler N enthält, der isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$ (und damit insbesondere kommutativ) ist. Damit hat aber $\mathfrak{A}_4/N$ Ordnung 3 und muss damit isomorph zu $\mathbb{Z}_3$ (und somit ebenfalls kommutativ) sein (siehe Korollar 2.4). Damit ist aber $N \subset [\mathfrak{A}_4, \mathfrak{A}_4]$ und man kann wieder zeigen, dass Gleichheit gilt. Somit ist $(\mathfrak{S}_4)^{(3)} = N$ und $(\mathfrak{S}_4)^{(4)} = \{e\}$, also $\mathfrak{S}_4$ auflösbar.

Man könnte nun erwarten, dass die Geschichte so ähnlich weitergeht. Das ist aber absolut nicht der Fall. Es stellt sich nämlich heraus, dass für $n \geq 5$ die Gruppe $\mathfrak{A}_n$ keine nichttrivialen Normalteiler enthält, also $\{e\}$ und $\mathfrak{A}_n$ die einzigen normalen Untergruppen von $\mathfrak{A}_n$ sind. Nachdem $\mathfrak{A}_n$ nicht kommutativ sein kann, muss also $[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$ gelten. Damit folgt natürlich, dass $(\mathfrak{S}_n)^{(k)} = \mathfrak{A}_n$ für alle $n \geq 5$ und $k \geq 2$ gilt. Insbesondere ist $\mathfrak{S}_n$ nicht auflösbar, falls $n \geq 5$ gilt!

2.17. Einfache Gruppen. Nachdem es keine Hoffnung gibt, allgemeine Gruppen aus kommutativen Gruppen aufzubauen, müssen wir uns allgemeinere "Bausteine" suchen. Dazu definieren wir:

Definition 2.17. Eine Gruppe G heißt einfach, wenn die einzigen normalen Untergruppen von G die triviale Gruppe $\{e\} \subset G$ und G selbst sind.

Wir kennen schon zwei Klassen von einfachen Gruppen. Ist p eine Primzahl, dann hat die Gruppe $\mathbb{Z}_p$ Ordnung p, besitzt also nach Satz 2.4 keine Untergruppen außer $\{e\}$ und $\mathbb{Z}_p$ selbst. Das sind die einzigen kommutativen einfachen Gruppen, weil nach Proposition 2.11 jeder Teiler der Gruppenordnung eine nicht–triviale Untergruppe liefert, die im kommutativen Fall automatisch ein Normalteiler ist. Andererseits wissen wir aus 2.16, dass die alternierende Gruppe $\mathfrak{A}_n$ für $n \geq 5$ einfach ist. Die kleinste dieser Gruppen

ist $\mathfrak{A}_5$ mit Ordnung $5!/2 = 60$ und dies ist tatsächlich die kleinste nicht–kommutative einfache Gruppe.

Nun kann man jede endliche Gruppe aus einfachen Gruppen aufbauen. Sei nämlich G eine endliche Gruppe. Hat G keinen nicht–trivialen Normalteiler, dann ist G selbst einfach, also sind wir fertig. Falls G nicht–triviale Normalteiler besitzt, dann sei $N \triangleleft G$ ein echter Normalteiler (d.h. $N \neq G$) mit maximaler Ordnung. Betrachten wir den kanonischen Quotientenhomomorphismus $\pi : G \to G/N$. Ist $H \triangleleft G/N$ ein Normalteiler mit $H \neq \{e\}$, dann betrachten wir $\pi^{-1}(H) \subset G$. Nach Proposition 2.5 ist das ein Normalteiler und nach Konstruktion ist $N \subset \pi^{-1}(H)$ eine echte Teilmenge. Nach Konstruktion von N muss dann aber $\pi^{-1}(H) = G$, also $H = G/N$ gelten. Somit ist G/N eine einfache Gruppe. Nun können wir die Gruppe N betrachten. Ist N einfach, dann haben wir G aus einfachen Gruppen aufgebaut. Ansonsten können wir wie oben vorgehen, also einen echten Normalteiler $N_2 \subset N$ mit maximaler Ordnung wählen. Nachdem in diesem Prozess in jedem Schritt die Ordnung echt kleiner wird, erreicht man in endlich vielen Schritten eine einfache Gruppe.

Damit ist klar, dass die endlichen einfachen Gruppen die fundamentalen Bausteine für alle endlichen Gruppen sind und es stellt sich die Frage, ob man diese Gruppen beschreiben kann. Das ist tatsächlich möglich, aber die Antwort wird durch einen der komplexesten Beweise in der Geschichte der Mathematik gegeben, der mehrere tausend Seiten beansprucht und bisher noch nicht in durchgehender Form aufgeschrieben wurde. Man muss dazu einerseits Beispiele von endlichen einfachen Gruppen finden, was für sich schon sehr interessante Bezüge zu verschiedenen Teilgebieten der Mathematik liefert. Neben den schon angeführten Beispielen $\mathbb{Z}_p$ für Primzahlen p und $\mathfrak{A}_n$ für $5 \leq n \in \mathbb{N}$ finden sich weitere "Serien" von systematisch konstruierbaren Beispielen, etwa Gruppen von Matrizen über endlichen Körpern. Daneben gibt es aber auch insgesamt 26 weitere Beispiele von endlichen einfachen Gruppen, die sogenannten *sporadischen einfachen Gruppen*, die in kein Schema passen. Von diesen 26 Beispielen können 20 aus einer einzigen Gruppe, der sogenannten *Monstergruppe* (die größte aller sporadischen Gruppen) konstruiert werden. Die kleinste der sporadischen Gruppe hat Ordnung 7920 die Ordnung der Monstergruppe ist ungefähr 8×10^{53}.

Der wirklich schwierige Teil des Beweises ist zu zeigen, dass tatsächlich jede endliche einfache Gruppe isomorph zu einer der Gruppen aus der List ist. Dazu muss man auf eine Vielzahl von Resultaten und in der Literatur studierten Beispielen zurückgreifen, was den Beweis so komplex macht. Die Experten auf dem Gebiet sind aber der Ansicht, dass der Beweis vollständig vorhanden ist. Es läuft derzeit ein großes internationales Projekt mit dem Ziel, den Beweis vollständig aufzuschreiben. Obwohl der bisher aufgeschriebene Teil schon mehrere Bücher füllt, wird es wohl noch etwas dauern, bis ein vollständiger, durchgehend aufgeschriebener Beweis verfügbar sein wird.