Ralf Gerkmann

Mathematisches Institut
Ludwig-Maximilians-Universität München

Vorlesungsskript

Algebra und Zahlentheorie

Zusammenfassung

Algebraische Strukturen wie Gruppen, Ringe und Körper bilden die unverzichtbare Grundlage für jedes Teilgebiet der Mathematik, angefangen beim Lösen elementarer zahlentheoretischer Probleme oder algebraischer Gleichungen, über die Klassifikation diskreter geometrischer Strukturen und topologischer Räume bis hin zu fortgeschrittenen Bereichen wie der Algebraischen Geometrie oder der Harmonischen Analysis. Auch in vielen Anwendungsgebieten, in der Informatik beispielsweise in der Kryptographie und in der Theorie der Programmiersprachen, innerhalb der Physik etwa in der Klassischen Mechanik, der Quantenmechanik und der Elementarteilchenphysik, spielen sie eine wichtige Rolle.

Jeder der drei oben genannten algebraischen Strukturen ist ein eigener Vorlesungsteil gewidmet, wobei wir allerdings den theoretischen Konzepten, die in allen drei Gebieten auftreten (zum Beispiel Faktorstrukturen und Homomorphiesätze), besondere Beachtung schenken. Beim Aufbau der Gruppentheorie orientieren uns unter anderem am sog. *Klassifikationsproblem*, bei dem wir vor allem durch die zuletzt behandelten Sylowsätze noch entscheidende Fortschritte erzielen. Bei der Ringtheorie stehen als Motivation vor allem Probleme der klassischen Zahlentheorie im Vordergrund. Im letzten Teil der Vorlesung befassen wir uns mit der Theorie der algebraischen Körpererweiterungen. Den krönenden Abschluss der Algebra wird die (im Sommersemester behandelte) Galoistheorie bilden, bei der die Gruppen- und die Körpertheorie miteinander verbunden werden. Im Einzelnen werden in der zweisemestrigen Vorlesung folgende Themen behandelt.

- Definition der algebraischen Grundstrukturen: Gruppen, Ringe und Körper
- Homomorphismen, Unter- und Faktorstrukturen, Konstruktion von Erweiterungen
- zyklische und abelsche Gruppen
- semidirekte Produkte und Auflösbarkeit
- Gruppenoperationen und Sylowsätze
- Kongruenzrechnung
- Teilbarkeit und eindeutige Primfaktorzerlegung
- endliche und algebraische Körpererweiterungen
- Fortsetzung von Körperhomomorphismen
- normale Körperweiterungen
- Theorie der endlichen Körper
- Galoistheorie und Anwendungen

Inhaltsverzeichnis

§ 1. *Definition der Gruppen, Beispiele*

Zusammenfassung. Das Ziel dieses Kapitels besteht darin, mit dem Gruppenbegriff, den wir schon aus der Linearen Algebra kennen, besser vertraut zu werden. Zunächst betrachten wir eine große Anzahl konkreter Beispiele von Gruppen: Gruppen als Bestandteile algebraischer Strukturen, Permutationsgruppen, lineare Gruppen und Symmetriegruppen. Anschließend sehen wir uns an, wie der Begriff der Gruppe auf einfacheren Konzepte, denen der Halbgruppe und des Monoids, aufgebaut ist. Mit Hilfe von direkten Produkten können gegebene Gruppen zu komplexeren Gruppen zusammengesetzt werden. Zum Schluss erläutern wir noch ein großes fernes Ziel der Gruppentheorie, die *Klassifikation* der Gruppen.

Wichtige Grundbegriffe

- Halbgruppen, Monoide und Gruppen
- Permutationsgruppe, symmetrische Gruppe
- Bewegung, Symmetriegruppe
- Abgeschlossenheit einer Teilmenge unter einer Verknüpfung
- direktes Produkt zweier Gruppen

Im gesamten ersten Teil der Vorlesung dreht sich alles um die folgende Definition, die bereits aus der Linearen Algebra bekannt ist.

Definition 1.1 Eine ***Gruppe*** ist ein Paar $(G, *)$ bestehend aus einer nichtleeren Menge G und einer Verknüpfung $*$ auf G (also einer Abbildung $G \times G \to G$), so dass die folgenden Bedingungen erfüllt sind.

(i) Die Verknüpfung ist assoziativ, d.h. es gilt $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.

(ii) Es gibt ein ausgezeichnetes Element $e \in G$, genannt das ***Neutralelement*** der Gruppe, mit der Eigenschaft, dass $e * a = a * e = a$ für alle $a \in G$ gilt.

(iii) Für jedes Element $a \in G$ gibt es ein Element $a^{-1} \in G$, genannt das zu a ***inverse Element***, mit $a * a^{-1} = a^{-1} * a = e$.

Gilt darüber hinaus $a * b = b * a$ für alle $a, b \in G$, dann spricht man von einer ***abelschen*** oder auch einer ***kommutativen*** Gruppe.

Bevor wir uns mit dieser Definition genauer auseinandersetzen, sollten wir uns zunächst klarmachen, dass uns viele konkrete Beispiele von Gruppen bereits bekannt sind.

(1) Gruppen kommen als Bestandteile anderer, uns bereits bekannter algebraischer Strukturen, vor. Ist etwa $(R, +, \cdot)$ ein Ring, ist $(R, +)$ eine abelsche Gruppe, mit dem Neutralelement 0_R. Zum Beispiel ist $(\mathbb{Z}, +)$ eine abelsche Gruppe.

(2) Wichtige Beispiele für abelsche Gruppen erhält man durch die bereits bekannten Restklassenringe $\mathbb{Z}/n\mathbb{Z}$. Für jedes $n \in \mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe bestehend aus n Elementen. Hier ist $\bar{0} = 0+n\mathbb{Z}$, die Restklasse der Null, das Neutralelement.

(3) Ist $(K, + \cdot)$ ein Körper, dann ist $(K^\times, \cdot)$ eine Gruppe. Dabei bezeichnet $K^\times$ die Menge $K \setminus \{0_K\}$, also die Gesamtheit aller Körperelemente ungleich dem Nullelement 0_K. Beispielsweise ist $(\mathbb{C}^\times, \cdot)$ eine abelsche Gruppe, und für jede Primzahl p ist $(\mathbb{F}_p^\times, \cdot)$ ist eine abelsche Gruppe mit $p-1$ Elementen. (Wir erinnern daran, dass für jede Primzahl p der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, den wir dann auch mit $\mathbb{F}_p$ bezeichnet hatten.)

(4) Ist K ein Körper und $(V, +, \cdot)$ ein K-Vektorraum, dann ist $(V, +)$ eine abelsche Gruppe. Beispielsweise ist $(\mathbb{R}^2, +)$ eine abelsche Gruppe, wobei $+$ die Vektoraddition durch $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ bezeichnet.

Mit den symmetrischen Gruppen sind uns aus der Linearen Algebra auch schon Beispiele für nicht-abelsche Gruppen bekannt. Im Hinblick auf spätere Anwendungen führen wir hier einen etwas allgemeineren Begriff ein. Für jede Menge X sei $\mathrm{Abb}(X)$ die Menge der Abbildungen $X \to X$.

Definition 1.2 Sei X eine Menge. Dann ist das Paar $(\mathrm{Per}(X), \circ)$ bestehend aus der Teilmenge $\mathrm{Per}(X) \subseteq \mathrm{Abb}(X)$ der *bijektiven* Abbildungen $X \to X$ und der Komposition $\circ$ von Abbildungen eine Gruppe, die man als ***Permutationsgruppe*** der Menge X bezeichnet. Die Elemente von $\mathrm{Per}(X)$ nennt man auch ***Permutationen*** von X.

Ist $n \in \mathbb{N}$ und $M_n = \{1, ..., n\}$, dann ist $S_n = \mathrm{Per}(M_n)$ die bereits aus der Lineare Algebra bekannte ***symmetrische Gruppe***. Wir haben in der Linearen Algebra die Gruppeneigenschaft nur für S_n nachgewiesen, aber der Beweis ist für eine beliebige Permutationsgruppe $\mathrm{Per}(X)$ derselbe: Zunächst erinnern wir daran, dass die Komposition $\sigma \circ \tau$ zweier bijektiver Abbildungen $\sigma, \tau : X \to X$ wiederum eine bijektive Abbildung ergibt, so dass es sich bei $\circ$ tatsächlich um eine Verknüpfung auf $\mathrm{Per}(X)$ handelt. Auch wissen wir bereits, dass sich die Komposition von Abbildungen assoziativ verhält, also $(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)$ für alle $\rho, \sigma, \tau \in \mathrm{Per}(X)$ gilt. Der Grund dafür war, dass die Anwendung der beiden Abbildungen links und rechts auf ein beliebiges Element $x \in X$ jeweils übereinstimmend das Element $\rho(\sigma(\tau(x)))$ ergibt.

Für jedes $\sigma \in \mathrm{Per}(X)$ gilt jeweils $\sigma \circ \mathrm{id}_X = \sigma$ und $\mathrm{id}_X \circ \sigma = \sigma$. Auch dies überprüft man durch, dass man $\sigma \circ \mathrm{id}_X$ und $\mathrm{id}_X \circ \sigma$ auf ein beliebiges $x \in X$ anwendet; das Ergebnis ist in beiden Fällen $\sigma(x)$. Also ist id_X das Neutralelement der Gruppe $(\mathrm{Per}(X), \circ)$. Schließlich gilt noch $\sigma \circ \sigma^{-1} = \mathrm{id}_X$ und $\sigma^{-1} \circ \sigma = \mathrm{id}_X$ für jedes $\sigma \in \mathrm{Per}(X)$, wobei σ^{-1} jeweils die Umkehrabbildung bezeichnet. Dies folgt direkt aus der Definition der Umkehrabbildung. Die Gleichungen zeigen, dass σ^{-1} jeweils das zu σ inverse Element ist.

Wir geben einige Eigenschaften der symmetrischen Gruppe S_n an, die zum Teil in der Lineare Algebra hergeleitet wurden, und die wir von nun an als bekannt voraussetzen.

(i) Die Gruppe S_n besteht aus $n!$ Elementen.

(ii) Die Elemente der Gruppe S_n können in der sog. ***Tabellenschreibweise*** dargestellt werden: Sind $a_1, ..., a_n \in M_n$ vorgegeben, dann verwenden wir den Ausdruck

$$\sigma \quad = \quad \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

zur Darstellung der Abbildung $\sigma : M_n \to M_n$ gegeben durch $\sigma(k) = a_k$ für $1 \leq k \leq n$. Offenbar ist σ genau dann in S_n enthalten, wenn jede Zahl aus M_n unter den Werten $a_1, ..., a_n$ genau einmal vorkommt.

(iii) Sei $n \in \mathbb{N}$ und $k \in \{2, ..., n\}$. Ein ***k-Zykel*** in S_n ist ein Element $\sigma \in S_n$ mit der folgenden Eigenschaft: Es gibt eine k-elementige Teilmenge $\{m_1, ..., m_k\} \subseteq M_n$, so dass

$$\sigma(x) \quad = \quad \begin{cases} m_{i+1} & \text{falls } x = m_i \ , \ 1 \leq i < k \\ m_1 & \text{falls } x = m_k \\ x & \text{sonst} \end{cases}$$

für alle $x \in M_n$ erfüllt ist. Für ein solches Element wird die Notation $\sigma = (m_1 \ ... \ m_k)$ verwendet. Die 2-Zykel in S_n bezeichnet man auch als ***Transpositionen***.

(iv) Die ***Signumsfunktion*** ist eine Abbildung $\text{sgn} : S_n \to \{\pm 1\}$, die die Gleichung $\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$ für alle $\sigma, \tau \in S_n$ erfüllt. Ist σ ein k-Zykel, dann gilt $\text{sgn}(\sigma) = (-1)^{k-1}$.

(v) Die Teilmenge $A_n \subseteq S_n$ gegeben durch $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = +1\}$ wird als ***alternierende Gruppe*** bezeichet.

Sind $\sigma, \tau \in A_n$, dann gilt dasselbe für das Produkt $\sigma \circ \tau$, denn es gilt $\text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = (+1)(+1) = +1$. Die Gleichungskette

$$\text{sgn}(\sigma^{-1}) \quad = \quad (+1)\text{sgn}(\sigma^{-1}) \quad = \quad \text{sgn}(\sigma)\text{sgn}(\sigma^{-1}) \quad = \quad \text{sgn}(\sigma \circ \sigma^{-1}) \quad = \quad \text{sgn}(\text{id}_{\mathbb{R}^n}) \quad = \quad +1$$

zeigt, dass auch σ^{-1} in A_n enthalten ist. Es lässt sich nun leicht zeigen, dass A_n mit der Komposition $\circ$ als Verknüpfung tatsächlich ebenfalls eine Gruppe bildet.

Wir werden später mit Hilfsmitteln der Gruppentheorie beweisen, dass jedes Element aus S_n auf im wesentlichen eindeutige Weise als Produkt disjunkter Zyklen dargestellt werden kann. Eine solche Darstellung bezeichnet man als ***Zykelschreibweise***. Die Zykelschreibweise ermöglicht es, die Elemente von S_n in Klassen einzuteilen und auf diese Weise eine bessere Übersicht herzustellen.

Definition 1.3 Ist $r \in \mathbb{N}$ und sind $k_1, ..., k_r \in \mathbb{N}$ mit $k_1 \geq ... \geq k_r \geq 2$, dann bezeichnet man das Tupel $(k_1, ..., k_r)$ als ***Zerlegungstyp*** eines Elements $\sigma \in S_n$, wenn σ als Produkt disjunkter Zyklen der Längen $(k_1, ..., k_r)$ dargestellt werden kann.

Beispielsweise ist $\sigma = (1\ 2\ 3)(4\ 5)(6\ 7) \in S_7$ ein Element vom Zerlegungstyp $(3, 2, 2)$. Der Identität id wird per Konvention das leere Tupel () als Zerlegungstyp zugeordnet.

Beispielsweise sind die Elemente der Gruppe S_3 durch die folgenden Tabellen gegeben.

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

In Zykelschreibweise ermöglicht eine übersichtlichere Aufzählung der Elemente, wenn man diese nach Zerlegungstyp ordnet; es ist

$$S_3 \quad = \quad \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Auch die Elemente der Gruppe S_4 lassen sich noch leicht in Zykelschreibweise angeben. Schreiben wir nacheinander alle Elemente der Zerlegungstypen (), (2), (3), (4) und (2, 2) hin, so erhalten wir die Aufzählung

$$\begin{gathered} S_4 \quad = \quad \{\ \mathrm{id}\ ,\ (1\ 2)\ ,\ (1\ 3)\ ,\ (1\ 4)\ ,\ (2\ 3)\ ,\ (2\ 4)\ ,\ (3\ 4)\ , \\ (1\ 2\ 3)\ ,\ (1\ 3\ 2)\ ,\ (1\ 2\ 4)\ ,\ (1\ 4\ 2)\ ,\ (1\ 3\ 4)\ ,\ (1\ 4\ 3)\ ,\ (2\ 3\ 4)\ ,\ (2\ 4\ 3)\ , \\ (1\ 2\ 3\ 4)\ ,\ (1\ 3\ 2\ 4)\ ,\ (1\ 4\ 3\ 2)\ ,\ (1\ 2\ 4\ 3)\ ,\ (1\ 3\ 4\ 2)\ ,\ (1\ 4\ 2\ 3)\ ,\ (1\ 2)(3\ 4)\ ,\ (1\ 3)(2\ 4)\ ,\ (1\ 4)(2\ 3)\ \}. \end{gathered}$$

Zu beachten ist noch, dass die Zykelschreibweise nicht ganz eindeutig ist. So gilt in S_4 beispielsweise

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

also bezeichnen die Schreibweisen (1 2 3 4) und (2 3 4 1) dasselbe Element der Gruppe S_4.

Satz 1.4 Die Gruppe S_n ist für $n \leq 2$ abelsch und für $n \geq 3$ nicht abelsch.

Beweis: Im Fall $n = 1$ ist die Aussage klar, denn es gilt $S_1 = \{\mathrm{id}\}$. Für $n = 2$ besteht S_n aus den beiden Elementen id und (1 2). Hier kann man die Gleichung $\sigma \circ \tau = \tau \circ \sigma$ für alle $\sigma, \tau \in S_2$ leicht „von Hand“ überprüfen, indem man die vier Möglichkeiten einzeln durchgeht; beispielsweise ist $(1\ 2) \circ \mathrm{id} = (1\ 2) = \mathrm{id} \circ (1\ 2)$. Für $n \geq 3$ gilt dagegen $(1\ 2) \circ (2\ 3) = (1\ 2\ 3)$ und $(2\ 3) \circ (1\ 2) = (1\ 3\ 2)$, und diese Elemente sind offenbar voneinander verschieden. □

Aus der Linearen Algebra sind uns noch weitere Beispiele für nicht-abelsche Gruppen bekannt.

(1) Ist $n \in \mathbb{N}$ und K ein Körper, dann ist das Paar $(\mathrm{GL}_n(K), \cdot)$ bestehend aus der Menge $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$-Matrizen über K mit der Multiplikation $\cdot$ von Matrizen als Verknüpfung eine Gruppe, die sog. ***allgemeine lineare Gruppe*** über dem Körper K. Sie ist nur für $n = 1$ abelsch, ansonsten nicht-abelsch.

(2) Auch die Teilmenge $\mathrm{SL}_n(K)$ bestehend aus den Matrizen $A \in \mathrm{GL}_n(K)$ mit $\det(A) = 1_K$ bildet mit der Multiplikation von Matrizen eine Gruppe. Man bezeichnet sie als ***spezielle lineare Gruppe***. Auch sie ist für alle $n \geq 2$ nicht-abelsch.

(3) Über dem Körper $K = \mathbb{R}$ haben wir im dritten Semester noch für beliebiges $n \in \mathbb{N}$ die ***orthogonale Gruppe*** $\mathcal{O}(n)$ kennengelernt. Diese besteht aus den orthogonalen Matrizen von $\mathrm{GL}_n(\mathbb{R})$, also den Matrizen A mit der Eigenschaft ${}^tA \cdot A = E_n$. Eine zur Orthogonalität äquivalente Bedingung kann, wie wir wissen, mit dem euklidischen Standard-Skalarprodukt formuliert werden und lautet, dass $\langle Av, Aw \rangle = \langle v, w \rangle$ für alle Vektoren $v, w \in \mathbb{R}^n$ gilt. Die Matrizen der Teilmenge $\mathrm{SO}(n) = \mathcal{O}(n) \cap \mathrm{SL}_n(\mathbb{R})$ bilden ebenfalls mit der Multiplikation von Matrizen eine Gruppe, die ***spezielle orthogonale Gruppe***. In der Vorlesung hatten wir gesehen, dass beispielsweise $\mathrm{SO}(3)$ aus Drehungen besteht (um eine beliebige Achse durch $0_{\mathbb{R}^3}$, den Koordinatenursprung), und dass bei $\mathcal{O}(3)$ die Spiegelungen an einer Ebene durch $0_{\mathbb{R}^3}$ hinzukommen.

(4) Über dem Körper $K = \mathbb{C}$ gibt es entsprechend die ***unitäre Gruppe*** $\mathcal{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t\bar{A} \cdot A = E_n\}$ und die ***spezielle unitäre Gruppe*** $\mathrm{SU}(n) = \mathcal{U}(n) \cap \mathrm{SL}_n(\mathbb{C})$. Die Elemente von $\mathcal{U}(n)$ werden auch als *unitäre Matrizen* bezeichnet. Eine Matrix $A \in \mathrm{GL}_n(\mathbb{C})$ ist genau dann unitär, wenn $\langle Av, Aw\rangle = \langle v, w\rangle$ für alle $v, w \in \mathbb{C}^n$ erfüllt ist, wobei $\langle\cdot,\cdot\rangle$ in diesem Fall das *hermitesche Standard-Skalarprodukt* gegeben durch $\langle v, w\rangle = \sum_{j=1}^n v_j \bar{w}_j$ bezeichnet.

Auch bei den allgemeinen und den speziellen linearen Gruppen kann man sich die Frage stellen, aus wievielen Elemente diese bestehen. Ist K ein unendlicher Körper (z.B. $K = \mathbb{R}$), dann ist die Elementezahl von $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$ ebenfalls unendlich. Wir werden später in der Körpertheorie zeigen, dass es für jede Primzahlpotenz q einen im Wesentlichen eindeutig bestimmten Körper $\mathbb{F}_q$ im q Elementen gibt. (Vorsicht: Ist q keine Primzahl, dann stimmt $\mathbb{F}_q$ nicht mit dem Restklassenring $\mathbb{Z}/q\mathbb{Z}$ überein.) Es gilt nun

$$|\mathrm{GL}_n(\mathbb{F}_q)| \quad = \quad q^{\frac{1}{2}n(n-1)} \prod_{k=1}^{n} (q^k - 1) \quad \text{für alle } n \in \mathbb{N} \text{ und jede Primzahlpotenz } q.$$

Diese Gleichung kann man sich folgendermaßen klarmachen: Aus der Linearen Algebra wissen wir, dass eine Matrix $A \in \mathcal{M}_n(\mathbb{F}_q)$ genau dann invertierbar ist, wenn ihre n Spaltenvektoren, die wir hier mit $v_1, ..., v_n \in \mathbb{F}_q^n$ bezeichnen wollen, linear unabhängig sind, was wegen $\dim \mathbb{F}_q^n = n$ dazu äquivalent ist, dass diese Vektoren eine Basis des $\mathbb{F}_q$-Vektorraums $\mathbb{F}_q^n$ bilden. Der *Basisergänzungssatz* aus der Linearen Algebra besagt, dass wir jedes linear unabhängige System von Vektoren zu einer Basis ergänzen können. Dies bedeutet, dass wir jede Basis von $\mathbb{F}_q^n$ dadurch aufbauen können, dass wir die Vektoren $v_1, v_2, ..., v_n$ nacheinander geeignet wählen.

Wir überlegen uns nun, wieviele Möglichkeiten es für die Wahl einer Basis gibt. Für jeden Vektor $v_1 \in \mathbb{F}_q^n$ ist $\{v_1\}$ genau dann linear unabhängig, wenn $v_1 \neq 0_{\mathbb{F}_q^n}$ gilt. Dies bedeutet, dass wir $q^n - 1$ Möglichkeiten haben, das erste Element v_1 unserer Basis zu wählen. Ist nun v_1 bereits bewählt, so ist für jeden Vektor v_2 die Menge $\{v_1, v_2\}$ genau dann linear unabhängig, wenn v_2 nicht in $\langle v_1\rangle_{\mathbb{F}_q}$, dem von v_1 aufgespannten Untervektorraum, enthalten ist. Da dieser Untervektorraum aus q Elementen besteht, bleiben also $q^n - q$ Möglichkeiten für die Wahl von v_2. Bei der Wahl von v_3 sind entsprechend die q^2 Elemente von $\langle v_1, v_2\rangle_{\mathbb{F}_q}$ ausgeschlossen usw. Auf diese Weise kommen wir auf $\prod_{k=0}^{n-1}(q^n - q^k)$ Möglichkeiten für das gesamte System $v_1, v_2, ..., v_n$. Für den k-ten Faktor gilt $q^n - q^k = q^k(q^{n-k} - 1)$. Schreiben wir die Faktoren q^k vor das Produkt, so erhalten wir die angegebene Formel, mit dem Vorfaktor $q^{\sum_{k=0}^{n-1} k} = q^{\frac{1}{2}(n-1)n}$, wobei die Gleichheit $\prod_{k=0}^{n-1}(q^{n-k} - 1) = \prod_{k=1}^{n}(q^k - 1)$ durch Umparametrisierung zu Stande kommt. Mit Hilfe von etwas Gruppentheorie beweisen wir später noch die Gleichung

$$|\mathrm{SL}_n(\mathbb{F}_q)| \quad = \quad q^{\frac{1}{2}n(n-1)} \prod_{k=2}^{n} (q^k - 1).$$

Gruppen spielen unter anderem in der Geometrie, und hier besonders bei der Klassifikation geometrischer Strukturen, eine wichtige Rolle. Auf diesen Aspekt soll nun etwas genauer eingegangen werden. Im Linearen Algebra-Teil des dritten Semesters war uns der Begriff der ***Bewegung*** begegnet. Dabei handelte es sich um eine Abbildung $\phi : \mathbb{R}^n \to \mathbb{R}^n$, unter der Abstände zwischen beliebigen gleich bleiben, d.h. es gilt $\|\phi(v) - \phi(w)\| = \|v - w\|$ für alle $v, w \in \mathbb{R}^n$, wobei $\|\cdot\|$ die bekannte eudklidische Standard-Norm auf dem $\mathbb{R}^n$ bezeichnet. Dort hatten wir auch erfahren, dass für jede Bewegung ϕ jeweils ein eindeutig bestimmter Vektor $u \in \mathbb{R}^n$ und eine eindeutig bestimmte Matrix $A \in \mathcal{O}(n)$ existieren, so dass $\phi(v) = u + Av$ für alle $v \in \mathbb{R}^n$ erfüllt ist. Wir verwenden für die Bewegung, die durch diesen Vektor u und diese Matrix A gegeben ist, die Bezeichnung $\phi_{u,A}$. In dem Fall, dass A in $\mathrm{SO}(n)$ liegt, hatten wir von einer *orientierungserhaltenden* Bewegung gesprochen, ansonsten von einer *orientierungsumkehrenden* Bewegung.

Definition 1.5 Die Menge der Bewegungen im $\mathbb{R}^n$ bildet zusammen mit der Komposition eine Gruppe, die wir mit $\mathcal{B}_n$ bezeichnen. Die orientierungserhaltenden Bewegungen bilden ebenso eine Gruppe; diese bezeichnen wir mit $\mathcal{B}_n^+$.

Für den Nachweis der Gruppeneigenschaften müssen wir zunächst überprüfen, dass die Komposition zweier Bewegungen wiederum eine Bewegung ist. Seien dazu $A, A' \in \mathcal{O}(n)$ und $u, u', v \in \mathbb{R}^n$ vorgegeben. Es gilt

$$(\phi_{u,A} \circ \phi_{u',A'})(v) \quad = \quad \phi_{u,A}(u' + A'v) \quad = \quad u + A(u' + A'v) \quad = \quad (u + Au') + AA'v.$$

Dies zeigt, dass $\phi_{u,A} \circ \phi_{u',A'}$ mit $\phi_{u+Au',AA'}$ übereinstimmt, und dies ist wiederum eine Bewegung, weil mit A und A' auch AA' ein Element von $\mathcal{O}(n)$ ist. Da sich die Komposition beliebiger Abbildungen assoziativ verhält, gilt auch in $\mathcal{B}_n$ das Assoziativgesetz. Das Neutralelement in $\mathcal{B}_n$ ist durch die identische Abbildung $\mathrm{id}_{\mathbb{R}^n}$ gegeben. Dass es sich dabei um eine orthogonale Abbildung handelt, erkennt man daran, dass $\mathrm{id}_{\mathbb{R}^n} = \phi_{0_{\mathbb{R}^n},E_n}$ gilt und die Einheitsmatrix E_n orthogonal ist. Schließlich müssen wir noch zeigen, dass jedes Element $\phi_{u,A} \in \mathcal{B}_n$ (mit $u \in \mathbb{R}^n$ und $A \in \mathcal{O}(n)$) ein Inverses besitzt. Für alle $v, w \in \mathbb{R}^n$ gilt die Äquivalenz

$$w = \phi_{u,A}(v) \quad \Leftrightarrow \quad w = u + Av \quad \Leftrightarrow \quad A^{-1}w = A^{-1}u + v \quad \Leftrightarrow \quad v = A^{-1}(-u) + A^{-1}w \quad \Leftrightarrow \quad v = \phi_{A^{-1}(-u),A^{-1}}.$$

Dies zeigt, dass $\phi_{A^{-1}(-u),A^{-1}}$ die Umkehrabbildung von $\phi_{u,A}$ ist, und weil mit A auch A^{-1} in $\mathcal{O}(n)$ liegt, handelt es sich dabei um eine Bewegung. In der Gruppe $\mathcal{B}_n$ ist also $\phi_{A^{-1}(-u),A^{-1}}$ das zu $\phi_{u,A}$ inverse Element. Nach demselben Schema zeigt man, dass auch $\mathcal{B}_n^+$ eine Gruppe ist.

Definition 1.6 Ist $T \subseteq \mathbb{R}^n$ eine beliebige Teilmenge, dann bezeichnet man

$$\mathrm{Sym}(T) \quad = \quad \{\phi \in \mathcal{B}_n \mid \phi(T) = T\}$$

als ***Symmetriegruppe*** von T. Die Elemente von $\mathrm{Sym}^+(T) = \mathrm{Sym}(T) \cap \mathcal{B}_n^+$ bezeichnet man als ***orientierungserhaltende Symmetrien*** der Menge T.

Für alle $\phi, \psi \in \mathrm{Sym}(T)$ sind auch $\phi \circ \psi$ und ϕ^{-1} in $\mathrm{Sym}(T)$ enthalten. Denn auf Grund der Gruppeneigenschaft von $\mathcal{B}_n$ sind die beiden Abbildungen ebenfalls in $\mathcal{B}_n$ enthalten; außerdem gilt $(\phi \circ \psi)(T) = \phi(\psi(T)) = \phi(T) = T$ und auf Grund der Bijektivität von ϕ auch $\phi^{-1}(T) = \phi^{-1}(\phi(T)) = (\phi^{-1} \circ \phi)(T) = \mathrm{id}_{\mathbb{R}^n}(T) = T$. Der Nachweis der Gruppeneigenschaften von $\mathrm{Sym}(T)$ ist nun reine Routine. (Er wird sich im nächsten Kapitel noch etwas weiter vereinfachen, wenn wir $\mathrm{Sym}(T)$ als sog. *Untergruppe* von $\mathcal{B}_n$ erkennen.) Auch der Nachweis, dass $\mathrm{Sym}^+(T)$ eine Gruppe ist, bereitet keine Schwierigkeiten.

Zu interessanten geometrischen Anwendungen kommt man nun, indem man Teilmengen $T \subseteq \mathbb{R}^n$ mit einer bestimmten geometrischen Bedeutung betrachtet. In der Analysis mehrerer Variablen haben wir den Begriff der *konvexen Teilmenge* des $\mathbb{R}^n$ eingeführt. Eine Teilmenge $T \subseteq \mathbb{R}^n$ haben wir ***konvex*** genannt, wenn für alle $v, w \in T$ jeweils die Verbindungsstrecke $[v, w]$ ganz in T enthalten ist. Ist $X \subseteq \mathbb{R}^n$ eine beliebige Teilmenge des $\mathbb{R}^n$ und sind $T, T' \subseteq \mathbb{R}^n$ beliebige konvexe Mengen mit $T \supseteq X$ und $T' \supseteq X$, dann ist auch $T \cap T'$ eine konvex Menge mit dieser Eigenschaft.

Die *kleinste* konvexe Teilmenge des $\mathbb{R}^n$, die eine Teilmenge $X \subseteq \mathbb{R}^n$ enthält, wird die ***konvexe Hülle*** von X genannt und mit $\mathrm{conv}(X)$ bezeichnet. Die konvexe Hülle einer endlichen Teilmenge vom $\mathbb{R}^n$ bezeichnet man als ***Polytop***. Ist X nicht in einem echten affinen Unterraum des $\mathbb{R}^n$ enthalten, spricht man von einem *nicht ausgearteten* Polytop.

Definition 1.7 Sei $n \in \mathbb{N}$ mit $n \geq 3$, und für $0 \leq k < n$ sei der Punkt $P_{n,k} \in \mathbb{R}^2$ gegeben durch $P_{n,k} = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$. Dann bezeichnen wir die konvexe Hülle der endlichen Punktmenge $\{P_{n,k} \mid 0 \leq k < n\}$ als das *regelmäßiges Standard-n-Eck* Δ_n. Die Symmetriegruppe $D_n = \mathrm{Sym}(\Delta_n)$ wird die n-te ***Diedergruppe*** genannt.

Es bezeichne $\rho \in \mathcal{B}_n^+$ die Drehung um den Koordinatenursprung $0_{\mathbb{R}^2}$ mit dem Winkel $\frac{2\pi}{n}$ und $\tau \in \mathcal{B}_n$ die Spiegelung an der x-Achse. Wie man leicht überprüft, bleibt die Punktmenge $\{P_{n,k} \mid 0 \leq k < n\}$ unter ρ und τ unverändert, und daraus kann auch leicht $\rho(\Delta_n) = \Delta_n$ und $\tau(\Delta_n) = \Delta_n$ abgeleitet werden. Dies bedeutet, dass ρ und τ in $D_n = \mathrm{Sym}(\Delta_n)$ enthalten sind. Auf Grund der Gruppeneinschaft liegen auch beliebige Kompositionen von ρ und τ in D_n. Mit den Methoden der *Diskreten Geometrie* kann man zeigen, dass D_n aus genau $2n$ Elementen besteht; es gilt

$$D_n \quad = \quad \{\rho^k \mid 0 \leq k < n\} \cup \{\rho^k \circ \tau \mid 0 \leq k < n\}.$$

Wir werden später sehen, wie sich zumindest mit geringem Aufwand überprüfen lässt, dass die Elemente der Menge rechts eine Gruppe bilden. Der erste Teil der Menge aus Drehungen; genauer gesagt ist ρ^k die Drehung um $0_{\mathbb{R}^n}$ mit dem Winkel $\frac{2k\pi}{n}$. Bei den Abbildungen $\rho^k \circ \tau$ handelt es sich um Spiegelungen unterschiedlichen Typs. Ist n ungerade, dann durchläuft die Achse jeder Spiegelung durch eine Ecke und eine gegenüberliegende Kante des Polytops. Ist n dagegen gerade, dann läuft die Spiegelungsachse entweder durch zwei gegenüberliegende Ecken oder durch zwei gegenüberliegende Seiten von Δ_n.

Dass die Abbildungen der Form $\rho^k \circ \tau$ Spiegelungen sind, ist keineswegs offensichtlich, deshalb betrachten wir die Sache etwas genauer. Für jedes $\alpha \in \mathbb{R}$ sei $R_\alpha \in \mathrm{SO}(2)$ die Matrix, welche die Drehung um $0_{\mathbb{R}^2}$ mit dem Winkel α beschreibt, also

$$R_\alpha \quad = \quad \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Wie man sich leicht anschaulich klar macht (oder auch nachrechnen kann), gilt $R_\alpha \circ R_\beta = R_{\alpha+\beta}$ und $\tau \circ R_\alpha \circ \tau = R_{-\alpha}$ für beliebige $\alpha, \beta \in \mathbb{R}$, wobei wir R_α der Einfachheit halber als Bezeichnung für die Abbildung $v \mapsto R_\alpha v$ verwenden. Nach Definition gilt $\rho^k = R_{2k\pi/n}$ für $0 \leq k < n$.

Der Einfachheit halber beschränken wir uns auf den Fall, dass n ungerade ist. Sei $k \in \mathbb{Z}$ mit $0 \leq k < n$. Die Spiegelung an der Achse, die durch $0_{\mathbb{R}^n}$ und den Punkt $P_{n,k}$ verläuft, ist gegeben durch $\rho^k \circ \tau \circ \rho^{-k}$. Denn durch ρ^{-k} wird der Punkt $P_{n,k}$ auf den Punkt $P_{n,0}$ der x-Achse gedreht, anschließend durch τ gespiegelt und anschließend der Punkt $P_{n,0}$ durch ρ^k wieder zurückbewegt. Wendet man die Gleichung $\tau \circ R_\alpha \circ \tau = R_{-\alpha}$ auf den Wert $\alpha = -\frac{2k\pi}{n}$ an, so erhält man die Gleichung $\tau \circ \rho^{-k} \circ \tau = \rho^k$, was auf Grund der Identität $\tau^2 = \mathrm{id}_{\mathbb{R}^2} \Leftrightarrow \tau^{-1} = \tau$ zu $\tau \circ \rho^{-k} = \rho^k \circ \tau$ umgeformt werden kann. Einsetzen ergibt

$$\rho^k \circ \tau \circ \rho^{-k} \quad = \quad \rho^k \circ \rho^k \circ \tau \quad = \quad \rho^{2k} \circ \tau.$$

Es gilt $\rho^n = R_{2\pi/n}^n = R_{2\pi} = \mathrm{id}_{\mathbb{R}^2}$. Wählen wir $m \in \{0, 1\}$ so, dass $\ell = 2k - mn$ die Bedingung $0 \leq \ell < n$ erfüllt, dann gilt $\rho^{2k} = R_{2k\pi/n} = R_{2k\pi/n - 2m\pi} = R_{(2k-mn)\pi/n} = R_{2\ell\pi/n} = \rho^\ell$. Es gilt also $\rho^k \circ \tau \circ \rho^{-k} = \rho^\ell \circ \tau$. Damit ist nachgewiesen, dass es sich bei dem Element $\rho^\ell \circ \tau$ tatsächlich um eine Spiegelung von Δ_n handelt. Wie man leicht überprüft, durchläuft ℓ alle ganzen Zahlen mit $0 \leq \ell < n$, wenn k denselben Bereich durchläuft (sofern n ungerade ist). Dies zeigt, dass der zweite Teil der Menge von oben tatsächlich vollständig aus Spiegelungen besteht.

Es gibt noch eine andere Möglichkeit, dies zu überprüfen. Wie ρ wird auch die Bewegung τ durch eine orthogonale Matrix dargestellt, nämlich durch

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Diese Matrix hat die Determinate -1, während für alle $\alpha \in \mathbb{R}$ jeweils $\det(R_\alpha) = +1$ gilt. Die Abbildung $\rho^\ell \circ \tau$ besitzt nun die Darstellungsmatrix $R_{2\ell\pi/n}S$, und deren Determinante ist gleich $\det(R_{2\ell\pi/n}S) = \det(R_{2\ell\pi/n})\det(S) = (+1)(-1) = -1$. Nun verwendet man die bekannte Tatsache, dass die orthogonalen Matrizen mit Determinante -1 genau die linearen Abbildungen sind, welche die Spiegelung bzgl. einer Achse durch $0_{\mathbb{R}^2}$ beschreiben. Die Matrizen dieser Form besitzen immer die beiden Eigenwerte ± 1, und die Spiegelungsachse ist durch einen beliebigen Eigenvektor zum Eigenwerte $+1$ gegeben.

Wir betrachten nun einige geometrisch interessante Polytope in Dimension 3. Ein Punkt, den man als Durchschnitt eines Polytops P mit einer (affinen) Ebene erhält, wird als ***Ecke*** von von P bezeichnet. Eine Strecke, die als Durchschnitt von P mit einer Ebene zu Stande kommt, wird ***Kante*** von P genannt. Jede nichtleere Teilmenge, die als Durchschnitt von P mit einer Ebene E zu Stande kommt, bei der der Rest P vollständig auf einer Seite von E liegt und die weder eine Ecke noch eine Kante ist, wird als ***Seite*** von P bezeichnet. Wir bezeichnen zwei Teilmengen $S, T \subseteq \mathbb{R}^3$ als ***kongruent***, wenn ein $\phi \in \mathcal{B}_n$ mit $\phi(S) = T$ existiert. Von grundlegender Bedeutung in der Geometrie ist nun die folgende Definition.

Definition 1.8 Ein nicht ausgeartetes Polytop im $\mathbb{R}^3$ bezeichnet man als ***regulär*** oder auch als ***Platonischen Körper***, wenn all seine Seiten zueinander regelmäßige kongruente n-Ecke sind und sich an jeder Ecke dieselbe Anzahl von Seiten treffen.

Zwei Teilmengen $S, T \subseteq \mathbb{R}^3$ bezeichnet man als ***ähnlich***, wenn ein Skalierungsfaktor $r \in \mathbb{R}^+$ und ein $\phi \in \mathcal{B}_n$ existieren, so dass $T = \phi(rS)$ gilt. Dabei ist $rS = \{rp \mid p \in S\}$ die Teilmenge des $\mathbb{R}^3$, die durch Skalierung von S mit dem Faktor r zu Stande kommt. Seit der Antike ist bekannt, dass es bis auf Ähnlichkeit genau fünf Platonische Körper gibt.

(1) Einen ***Tetraeder*** erhält man als konvexe Hülle der vier Punkte $P_1 = (1,1,1)$, $P_2 = (1,-1,-1)$, $P_3 = (-1,1,-1)$, $P_4 = (-1,-1,1)$. Allgemein kommt eine Tetrader dadurch zu Stande, dass man über dem Schwerpunkt eines gleichseitigen Dreiecks eine weitere Ecke hinzufügt und dabei die Höhe so wählt, dass alle Kanten gleich lang werden. Jeder Tetraeder hat vier regelmäßige Dreiecke als Seiten, außerdem sechs Kanten und vier Ecken.

(2) Einen ***Oktader*** erhält man zum Beispiel als konvexe Hülle der sechselementigen Punktmenge bestehend aus $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$, $(0, 0, \pm 1)$. Allgemein konstruiert man einen Oktaeder dadurch, dass man über und unter dem Mittelpunkt eines Quadrats zwei weitere Ecken hinzufügt, wobei die Abstände so gewählt werden, dass alle Kanten dieselbe Länge haben. Jeder Oktaeder hat acht Seiten, zwölf Kanten und sechs Ecken.

(3) Einen ***Würfel*** erhält man unter anderem als konvexe Hülle der achtelementigen Punktmenge bestehend aus $(\pm 1, \pm 1, \pm 1)$ (d.h. man bildet alle acht Vorzeichenkombinationen). Geometrisch wird jeder Würfel dadurch konstruiert, indem man von einem Quadrat im Raum ausgeht, durch Parallelverschiebung ein weiteres Quadrat bildet und dann die korrespondierenden Ecken miteinander verbindet, wobei der Verschiebungsvektor so gewählt wird, dass die neu entstandenen Kanten auf den Quadraten senkrecht stehen und dieselbe Länge wie die Seiten der Quadrate haben. Jeder Würfel besitzt sechs Seiten, zwölf Kanten und acht Ecken.

(4) Einen ***Dodekaeder*** erhält man zum Beispiel als konvexe Hülle der 20 Punkte

$$(\pm\tau,\pm\tau,\pm\tau),\quad (\pm\tau_1,\pm 1,0),\quad ,(\pm 1,0,\pm\tau_1),\quad ,(0,\pm\tau_1,\pm 1)\quad ,$$

wobei jeweils alle Vorzeichenkombinationen zu berücksichtigen sind, $\tau = \frac{1}{2}(\sqrt{5}+1)$ das Verhältnis des *goldenen Schnitts* bezeichnet und $\tau_1 = \tau + 1$ ist. (Wenn eine Strecke s im Verhältnis $\tau : 1$ in zwei Teilstrecken a und b geteilt wird, dann gilt $\tau = \frac{a}{b} = \frac{s}{a}$.) Für eine geometrische Konstruktion geht man von einem regelmäßigen Fünfeck aus, setzt an jede Seite ein gleichartiges Fünfeck und fügt anschließend die sechs Fünfecke zu einer Halbkugelschale zusammen. Zwei identische Halbkugelschalen dieser Form können dann zu einem Dodekaeder zusammengesetzt werden. Jeder Dodekaeder besitzt 12 Seiten, 30 Kanten und 20 Ecken.

(5) Einen ***Ikosaeder*** erhält man unter anderem als konvexe Hülle der zwölf Punkte

$$(0,\pm 1,\pm\tau),\quad (\pm 1,0,\pm\tau),\quad (\pm 1,\pm\tau,0).$$

Für eine geometrische Konstruktion geht man von zwei parallel übereinanderliegenden, regelmäßigen Fünfecken aus und verdreht diese in einem 36°-Winkel gegeneinander. Jede Ecke des oberen Fünfecks wird mit den zwei nächstgelegenen Ecken des unteren Fünfecks verbunden. Man erhält auf diese Weise zwischen den beiden Fünfecken zehn gleichschenklige Dreiecke. Anschließend wird der Abstand zwischen den parallelen Fünfecken so eingestellt, dass die zehn gleichschenkligen Dreicke zu gleichseitigen Dreiecken werden. Nun setzt man noch einen Punkt senkrecht über den Mittelpunkt des oberen Fünfecks und verbindet diesen Punkt mit den Eckpunkten des Fünfecks. Auf diese Weise erhält man fünf weitere Dreiecke. Die Höhe des neuen Punkts wird so gewählt, dass die fünf Dreiecke zu gleichseitigen Dreiecken werden. Zum Schluss setzt man einen Punkt unter das untere Fünfeck und erzeugt auf dieselbe Weise fünf weitere gleichseitige Dreiecke, die an dem neuen Punkt anliegen. Jeder Ikosaeder besteht aus 20 Seiten, 30 Kanten und besitzt 12 Ecken.

Definition 1.9 Bezeichnet $\mathbb{T}$ einen beliebigen Tetraeder, dann nennt man $\mathrm{Sym}(\mathbb{T})$ eine ***Tetraedergruppe*** und $\mathrm{Sym}^+(\mathbb{T})$ eine ***eigentliche*** Tetraedergruppe. Ist $\mathbb{O}$ ein Oktaeder, dann wird $\mathrm{Sym}(\mathbb{O})$ eine ***Oktaedergruppe*** und $\mathrm{Sym}^+(\mathbb{O})$ eine ***eigentliche Oktaedergruppe***. Entsprechend werden (eigentliche) Würfelgruppen, Dodekaedergruppen und Ikosaedergruppen definiert.

Ein typische Element von $\mathrm{Sym}^+(\mathbb{O})$ erhält man dadurch, dass man zwei gegenüberliegen Ecken, die Mittelpunkte zweier gegenüberliegender Kanten oder die Mittelpunkte zweier gegenüberliegender Seiten durch Achsen miteinander verbindet und dann Rotationen um diese Achse betrachtet, die das Polytop $\mathbb{O}$ in sich überführen. Auf diese Weise erhält man sogenannte ***dreizählige*** bzw. zweizählige bzw. vierzählige Symmetrien. Jedes nicht orientierungserhaltende Element aus $\mathrm{Sym}(\mathbb{O})$ kommt durch eine Spiegelung zu Stande, wobei die Spiegelungsebene durch zwei gegenüberliegende Ecken, Kanten oder Seiten laufen kann.

Nachdem wir nun eine Vielzahl konkreter Beispiele von Gruppen zu sehen bekommen haben, wenden wir nun wieder allgemeineren, abstrakten Konzepten zu.

Definition 1.10 Seien G und H Gruppen. Dann bildet das kartesische Produkt $G \times H$ mit der Verknüpfung $*$ gegeben durch

$$(g_1,h_1)*(g_2,h_2) \quad = \quad (g_1g_2,h_1h_2) \qquad \text{für alle} \quad (g_1,h_1),(g_2,h_2) \in G \times H$$

ebenfalls eine Gruppe. Man nennt sie das ***(äußere) direkte Produkt*** von G und H. Sind G und H abelsch, dann gilt dasselbe für $(G \times H, *)$.

Beweis: Zunächst beweisen wir das Assoziativgesetz. Seien $(g_1,h_1),(g_2,h_2),(g_3,h_3) \in G \times H$ vorgegeben. Nach Definition der Verknüpfung $*$ und auf Grund der Assoziativität der Verknüpfungen von G und H erhalten wir

$$\begin{aligned}((g_1,h_1)*(g_2,h_2))*(g_3,h_3) \quad &= \quad (g_1g_2,h_1h_2)*(g_3,h_3) \quad = \quad ((g_1g_2)g_3,(h_1h_2)h_3) \quad = \\ (g_1(g_2g_3),h_1(h_2h_3)) \quad &= \quad (g_1,h_1)*(g_2g_3,h_2h_3) \quad = \quad (g_1,h_1)*((g_2,h_2)*(g_3,h_3)).\end{aligned}$$

Seien nun e_G, e_H die Neutralelemente der Gruppen G und H. Für alle $(g,h) \in G \times H$ gilt dann $(g,h)*(e_G,e_H) = (ge_G,he_H) = (g,h)$ und ebenso $(e_G,e_H)*(g,h) = (e_Gg,e_Hh) = (g,h)$. Dies zeigt, dass $e_{G\times H} = (e_G,e_H)$ das Neutralelement von $(G \times H, *)$ ist. Schließlich gilt auch $(g,h)*(g^{-1},h^{-1}) = (gg^{-1},hh^{-1}) = (e_G,e_H) = e_{G\times H}$ und $(g^{-1},h^{-1})*(g,h) = (g^{-1}g,h^{-1}h) = (e_G,e_H) = e_{G\times H}$. Dies zeigt, dass (g^{-1},h^{-1}) jeweils ein Inverses von (g,h) ist, für alle $(g,h) \in G \times H$. Insgesamt sind damit alle Gruppenaxiome verifiziert.

Beweisen wir nun noch die zusätzliche Aussage. Laut Annahme sind G und H abelsch. Seien $(g_1,h_1),(g_2,h_2) \in G \times H$ vorgegeben. Dann gilt $(g_1,h_1)*(g_2,h_2) = (g_1g_2,h_1h_2) = (g_2g_1,h_2h_1) = (g_2,h_2)*(g_1,h_1)$. □

Beispielsweise ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ eine achtelementige abelsche Gruppe, und $S_4 \times S_5$ ist eine nicht-abelche Gruppe bestehend aus $(4!)\cdot(5!) = 24\cdot 120 = 2880$ Elementen. Als nächstes sehen wir uns, auf welche Weise der Gruppenbegriff auf einfacheren algebraischen Strukturen aufgebaut ist.

Definition 1.11

(i) Eine ***Halbgruppe*** ist ein Paar $(G, *)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $*$ auf G.

(ii) Ein Element $e \in G$ der Halbgruppe wird als ***Neutralelement*** bezeichnet, wenn $e*a = a$ und $a*e = a$ für alle $a \in G$ erfüllt ist.

(iii) Eine Halbgruppe mit mindestens einem Neutralelement bezeichnet man als ***Monoid***.

Jede Halbgruppe besitzt höchstens ein Neutralelement. Sei nämlich $(G, *,)$ eine Halbgruppe, und seien e, e' Neutralelemente von $(G, *)$. Weil e Neutralelement ist, gilt $a*e = a$ für alle $a \in G$, insbesondere also $e'*e = e'$. Weil e' Neutralelement ist, gilt $e'*a = a$ für alle $a \in G$, also insbesondere $e'*e = e$. Insgesamt erhalten wir $e' = e'*e = e$.

Jedes Monoid $(G, *)$ besitzt also ein eindeutig bestimmtes Neutralelement, für das wir, wie beiden Gruppen, die Bezeichung e oder e_G einführen.

Definition 1.12 Sei $(G, *)$ ein Monoid mit dem Neutralelement e_G. Ein Element $g \in G$ wird ***invertierbar*** in $(G, *)$ genannt, wenn ein $h \in G$ mit $g * h = h * g = e_G$ existiert. Man nennt h in diesem Fall ein ***Inverses*** von g.

Wir formulieren einige einfache Regeln für das Rechnen mit inversen Elementen.

Proposition 1.13 Sei $(G, *)$ ein Monoid.

(i) Jedes Element $g \in G$ besitzt höchstens ein Inverses; sofern es existiert, wird es mit g^{-1} bezeichnet.

(ii) Seien $g, h \in G$ invertierbare Elemente. Dann sind auch die Elemente $g * h$ und g^{-1} invertierbar, und es gilt $(g * h)^{-1} = h^{-1} * g^{-1}$ und $(g^{-1})^{-1} = g$.

(iii) Das Neutralelement e_G ist invertierbar, und es gilt $e_G^{-1} = e_G$.

Beweis: zu (i) Nehmen wir an, dass h und h' beides Inverse von g sind. Dann gilt $g * h = e_G$ und $h' * g = e_G$, und es folgt $h = e_G * h = (h' * g) * h = h' * (g * h) = h' * e_G = h'$.

zu (ii) Die Gleichungen $(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e_G * h = h^{-1} * h = e_G$ und $(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e_G * g^{-1} = g * g^{-1} = e_G$ zeigen, dass $h^{-1} * g^{-1}$ das (eindeutig bestimmte) Inverse von G ist. Ebenso sieht man anhand der Gleichungen $g^{-1} * g = e_G$ und $g * g^{-1} = e_G$, dass es sich bei g um das Inverse von g^{-1} handelt.

zu (iii) Wie unter (ii) folgt dies direkt aus der Gleichung $e_G * e_G = e_G$. □

Als Folge dieser Proposition ist nun klar, dass die Gruppen genau diejenigen Monoide sind, bei denen alle Elemente invertierbar sind. Wie wir nun aber sehen werden, lässt sich aus jedem Monoid stets eine Gruppe gewinnen.

Definition 1.14 Sei $(X, \circ)$ eine Menge mit einer Verknüpfung. Eine Teilmenge $U \subseteq X$ wird ***abgeschlossen*** unter $\circ$ genannt, wenn für alle $x, y \in U$ auch das Element $x \circ y$ in U liegt.

Ist $U \subseteq X$ abgeschlossen unter $\circ$, dann ist die Abbildung $\circ_U : U \times U \to X$, die man durch Einschränkung von $\circ$ auf die Teilmenge $U \times U \subseteq X \times X$ erhält, zugleich eine Abbildung $U \times U \to U$, also eine Verknüpfung auf U.

Beispielsweise ist die Teilmenge $\mathbb{N} \subseteq \mathbb{Z}$ abgeschlossen unter der Addition und der Multiplikation auf $\mathbb{Z}$, denn die Summe und das Produkt von zwei positiven ganzen Zahlen ist wiederum positiv. Dagegen ist die Menge $A = \{1, 2, 3\}$ nicht abgeschlossen unter der Addition auf $\mathbb{Z}$, denn es gilt $1, 3 \in A$, aber das Element $4 = 1+3$ ist nicht in A enthalten. Die Menge A ist auch nicht abgeschlossen unter der Multipliktation, denn einerseits gilt $2, 3 \in A$, andererseits aber $6 = 2 \cdot 3 \notin A$.

Satz 1.15 Sei $(G, *)$ ein Monoid und $G^\times \subseteq G$ die Teilmenge der invertierbaren Elemente. Dann ist $G^\times$ abgeschlossen unter der Verknüpfung $*$, und $(G^\times, *_{G^\times})$ ist eine Gruppe. Das Neutralelement e_G von G ist zugleich das Neutralelement von $(G^\times, *_{G^\times})$.

Beweis: Nach Proposition 1.13 (ii) ist das Produkt zweier invertierbarer Elemente wiederum invertierbar. Die Teilmenge $G^\times \subseteq G$ ist also unter $*$ abgeschlossen, und somit existiert, wie oben erläutert, eine Verknüpfung $*_{G^\times}$ auf $G^\times$. Wir überprüfen nun für $(G^\times, *_{G^\times})$ die Gruppenaxiome. Das Assoziativgesetz ist in $G^\times$ erfüllt, denn für alle $g, h, k \in G^\times$ gilt

$$g *_{G^\times} (h *_{G^\times} k) \quad = \quad g * (h * k) \quad = \quad (g * h) * k \quad = \quad (g *_{G^\times} h) *_{G^\times} k.$$

Das Assoziativgesetz „überträgt“ sich also von $(G, *)$ auf $(G, *_{G^\times})$. Nach Proposition 1.13 (iii) ist e_G in $G^\times$ enthalten, und für alle $g \in G^\times$ gilt $g *_{G^\times} e_G = g * e_G = g$ und $e_G *_{G^\times} g = e_G * g = g$. Dies zeigt, dass e_G in der Halbgruppe $(G^\times, *_{G^\times})$ ein Neutralelement ist. Somit ist $(G^\times, *_{G^\times})$ ein Monoid, mit Neutralelement $e_{G^\times} = e_G$.

Wiederum auf Grund von Proposition 1.13 (ii) folgt aus $g \in G^\times$ auch $g^{-1} \in G^\times$. Wegen $g *_{G^\times} g^{-1} = g * g^{-1} = e_G$ und $g^{-1} *_{G^\times} g = g^{-1} * g = e_G$ ist g^{-1} das Inverse von g in $(G^\times, *)$. Jedes Element aus $G^\times$ ist also im Monoid $(G^\times, *)$ invertierbar. Somit ist $(G^\times, *_{G^\times})$ eine Gruppe. □

Der Einfachheit halber wird die Verknüpfung der Gruppe $(G^\times, *_{G^\times})$ von nun an einfach wieder mit $*$ bezeichnet.

Wie wir anhand der bisherigen Beispiele bereits deutlich geworden ist, werden bei Halbgruppen, Monoiden und Gruppen in zwei unterschiedlichen Schreibweisen verwendet, die von der Form des Verknüpfungssymbols abhängen. Bei einem „punktähnlichen“ Symbol wie $\cdot$ oder $\odot$ bezeichnet man das Neutralelement eines Monoids neben e_G auch mit 1_G, und die Schreibweise für das Inverse eines Elements g ist stets g^{-1}. Man spricht in diesem Zusammenhang von ***multiplikativer Schreibweise***. Häufig wird ein punktähnliches Verknüpfungssymbol auch weggelassen, das Element $g \cdot h$ also mit gh bezeichnet.

Bei einem „plusartigen“ Verknüpfungssymbol wie $+$ oder $\oplus$ verwendet man für das Neutralelement die Notation 0_G, und die Schreibweise für das Inverse von g ist $-g$ statt g^{-1}. Die Gleichungen $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$ und $(g^{-1})^{-1} = g$ haben bei additiver Schreibweise also die Form $-(g + h) = (-h) + (-g)$ und $-(-g) = g$. Hier spricht man von ***additiver Schreibweise***; sie ist nur bei abelschen Halbgruppen (bzw. Monoiden oder Gruppen) gebräuchlich.

Ein wichtiges (und zugleich noch weit entferntes) Ziel der Algebra besteht darin, für jede Zahl $n \in \mathbb{N}$ „alle“ Gruppen mit n Elementen zu bestimmen. Ein grundsätzliches Problem besteht aber darin, dass es einerseits unüberschaubar viele n-elementige Mengen M gibt, auf den man jeweils eine Gruppenstruktur definieren könnte (durch Angabe einer Verknüpfung $\cdot$, einem Neutralelement $e \in M$ und einer Inversenabbildung $M \to M$, $a \mapsto a^{-1}$), dass sich aber andererseits viele dieser Gruppen anhand ihrer Strukturmerkmale gar nicht unterscheiden. (Was für Merkmale das sein können, ist das Thema der folgenden Kapitel.) Um diesem Problem zu begegnen, für man den *Isomorphiebegriff* in die Gruppentheorie ein.

Definition 1.16 Man bezeichnet zwei Gruppen $(G, \cdot)$ und $(H, *)$ als ***isomorph*** und schreibt $G \cong H$, wenn eine bijektive Abbildung $\phi : G \to H$ existiert, so dass $\phi(g \cdot g') = \phi(g) * \phi(g')$ für alle $g, g' \in G$ erfüllt ist.

Mit Hilfe des *Chinesischen Restsatzes* werden wir beispielsweise zeigen können, dass die Gruppen $\mathbb{Z}/15\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ zueinander isomorph sind. Durch die Hilfsmittel, die wir im Kapitel über Gruppenoperationen entwickeln werden, werden wir bezüglich der Diedergruppen und der Symmetriegruppen der platonischen Körper zeigen können

(i) Jede Diedergruppe D_n (mit $n \geq 3$) ist isomorph zu einer $2n$-elementigen Untergruppe von S_n.

(ii) Für die Symmetriegruppen des Tetraeders gilt $\mathrm{Sym}^+(\mathbb{T}) \cong A_4$ und $\mathrm{Sym}(\mathbb{T}) \cong S_4$.

(iii) Es gilt $\mathrm{Sym}^+(\mathbb{O}) \cong \mathrm{Sym}^+(\mathbb{W}) \cong S_4$ und $\mathrm{Sym}(\mathbb{O}) \cong \mathrm{Sym}(\mathbb{W}) \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$ für die Symmetriegruppen von Würfel und Oktaeder.

(iv) Für die Symmetriegruppen von Dodekaeder und Ikosaeder gilt $\mathrm{Sym}^+(\mathbb{D}) \cong \mathrm{Sym}^+(\mathbb{I}) \cong A_5$ und $\mathrm{Sym}(\mathbb{D}) \cong \mathrm{Sym}(\mathbb{I}) \cong A_5 \times \mathbb{Z}/2\mathbb{Z}$.

Dass die Symmetriegruppe von Würfel und Oktaeder bzw. Dodekaeder und Ikosaeder isomorph sind, hat folgenden Grund: Jedem nicht-ausgearteten Polytop P mit dem Nullpunkt $0_{\mathbb{R}^3}$ in seinem Inneren kann mit Hilfe des euklidischen Skalarprodukts durch

$$P^\vee \quad = \quad \{x \in \mathbb{R}^3 \mid \langle x, y \rangle \leq 1 \, \forall y \in P\}$$

ein sogenanntes ***duales Polytop*** zugeordnet werden. Dieses ist ebenfalls nicht-ausgeartet und enthält $0_{\mathbb{R}^3}$ als inneren Punkt. Jede Ecke von P entspricht einer Seite von $P^\vee$, jede Seite von P entspricht einer Ecke von $P^\vee$, und es gibt eine bijektive Korrespondenz zwischen den Kanten von P und denen von $P^\vee$. Es ist relativ leicht zu sehen, dass stets P und $P^\vee$ isomorphe Symmetriegruppen besitzen, und dass $(P^\vee)^\vee = P$ gilt. Durch Dualisierung eines Würfels erhält man einen Oktaeder, und ein Dodekaeder wird durch diesen Vorgang in ein Ikosaeder überführt. Ein Tetrader geht durch Dualisierung in einen anderen Tetraeder über.

Wie wir sehen werden, haben stimmen zwei isomorphe Gruppen bezüglich jedes Strukturmerkmals überein. Dazu gehört zum Beispiel die Anzahl der Untegruppen und Normalteiler, die Anzahl der Elemente bestimmter Ordnung und Eigenschaften wie „zyklisch“, „abelsch“ oder „auflösbar“, um nur ein paar der Merkmale zu nennen, mit denen wir uns im weiteren Verlauf befassen. Die Frage, welche „wesentlich voneinander verschiedenen“ Untergruppen einer bestimmten Ordnung n es gibt, lässt sich mit dem Isomorphiebegriff folgendermaßen konkretisieren.

Definition 1.17 Das ***Klassifikationsproblem für endliche Gruppen*** kann folgendermaßen formuliert werden: Gegeben ein $n \in \mathbb{N}$, bestimme alle Gruppen mit n Elementen bis auf Isomorphie. Damit ist gemeint: Bestimme eine Zahl $r(n)$ und Gruppen $G_1, G_2, \ldots, G_{r(n)}$ mit der Eigenschaft, dass *jede* Gruppe G mit $|G| = n$ zu genau einer dieser Gruppen isomorph ist.

Aus der Formulierung ergibt sich unmittelbar, dass in der Liste der $r(n)$ Gruppen für $1 \leq i, j \leq r(n)$ nur dann $G_i \cong G_j$ gilt, wenn $i = j$ ist. Mit Hilfe der Theorie, die wir hier entwickeln, werden wir zeigen können

- Ist p eine Primzahl, dann ist jede Gruppe G mit $|G| = p$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$. Es gilt also $r(p) = 1$.
- Für jede Primzahl p gilt: Jede Gruppe G mit $|G| = p^2$ ist entweder isomorph zu $\mathbb{Z}/p^2\mathbb{Z}$ oder isomorph zu $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Es gilt also $r(p^2) = 2$.
- Für jede ungerade Primzahl p gilt außerdem: Jede Gruppe der Ordnung $2p$ ist entweder isomorph zu $\mathbb{Z}/2p\mathbb{Z}$ oder zur Diedergruppe D_p. Es gilt also auch $r(2p) = 2$.

Des Weiteren werden wir in der Lage sein, alle Gruppen mit ≤ 15 Elementen bis auf Isomorphie zu bestimmen. Das Ergebnis kann in der folgenden Tabelle zusammengefasst werden.

n	$r(n)$	Gruppen bis auf Isomorphie
1	1	$\mathbb{Z}/1\mathbb{Z}$
2	1	$\mathbb{Z}/2\mathbb{Z}$
3	1	$\mathbb{Z}/3\mathbb{Z}$
4	2	$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	1	$\mathbb{Z}/5\mathbb{Z}$
6	2	$\mathbb{Z}/6\mathbb{Z},\ S_3$
7	1	$\mathbb{Z}/7\mathbb{Z}$
8	5	$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ Q_8$
9	2	$\mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	2	$\mathbb{Z}/10\mathbb{Z},\ D_5$
11	1	$\mathbb{Z}/11\mathbb{Z}$
12	5	$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z},\ D_6,\ A_4,\ \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
13	1	$\mathbb{Z}/13\mathbb{Z}$
14	2	$\mathbb{Z}/14\mathbb{Z},\ D_7$
15	1	$\mathbb{Z}/15\mathbb{Z}$

Dabei bezeichnet Q_8 die sog. ***Quaternionengruppe*** bestehend aus der achtelementigen Menge $\{\pm E, \pm I, \pm J, \pm K\} \subseteq \mathrm{GL}_2(\mathbb{C})$ mit den Matrizen

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad I = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \quad , \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Bei $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ handelt es sich um ein ***semidirektes Produkt***, eine Verallgemeinerung des direkten Produkts aus diesem Kapitel, das wir zu einem späteren Zeitpunkt noch definieren werden.

§ 2. *Untergruppen und der Satz von Lagrange*

Zusammenfassung. Eine *Untergruppe* ist eine Teilmenge U einer Gruppe G mit der Eigenschaft, dass e_G in U liegt, und mit $g, h \in U$ auch gh und g^{-1} in U enthalten sind. Durch diese Bedingungen ist sichergestellt, dass auch U die Struktur einer Gruppe besitzt. Jeder Teilmenge S einer Gruppe G kann eine Untergruppe $\langle S \rangle$ zugeordnet werden. Es handelt sich dabei um die kleinste Untergruppe von G, die S enthält. Oft reicht eine recht kleine Teilmenge S aus, um sogar ganz G zu erzeugen; bei den symmetrischen Gruppen S_n genügt beispielsweise eine zweielementige Menge. Untergruppen, die von einem einzigen Element erzeugt werden, nennt man *zyklisch*.

Der *Satz von Lagrange* besagt, dass bei einer endlichen Gruppe G die Ordnung jeder Untergruppe U ein Teiler von $|G|$ ist. Der Beweis beruht auf der Beobachtung, dass jede Untergruppe U eine *Zerlegung* der Gruppe in gleich große Teilmengen ermöglicht, die sog. Links- und Rechtsnebenklassen der Untergruppe. Wir wiederholen den bereits aus der Linearen Algebra bekannten Zusammenhang zwischen Zerlegungen und Äquivalenzrelationen. Für den praktischen Umgang mit Nebenklassenzerlegungen ist das Konzept der *Repräsentantensysteme* hilfreich.

Wichtige Grundbegriffe

- n-te Potenz eines Gruppenelements ($n \in \mathbb{Z}$) ´
- Definition der Untergruppen
- Erzeugendensysteme einer Gruppe
- zyklische Gruppe
- Konjugation von Gruppenelementen
- Links- und Rechtsnebenklassen einer Untergruppe
- Repräsentantensystem
- Index $(G : U)$ einer Untergruppe

Zentrale Sätze

- Gruppen-Eigenschaft der Untergruppen
- Existenz und Eindeutigkeit der von einer Teilmenge $S \subseteq G$ erzeugten Untergruppe $\langle S \rangle$
- Vertauschbarkeit von Permutationen mit disjunktem Träger
- Satz von Lagrange
- Kleiner Satz von Fermat

Bereits in der Analysis-Vorlesung wurde die ***n*-te Potenz** eines Körperelements für alle $n \in \mathbb{Z}$ definiert. Die Definition lässt sich problemlos auf die Elemente einer Halbgruppe bzw. eines Monoids übertragen.

Definition 2.1 Ist $(G, *)$ eine Halbgruppe und $g \in G$ ein beliebiges Element, dann definiert man rekursiv $g^1 = g$ und $g^{n+1} = g^n * g$ für alle $n \in \mathbb{N}$. Ist $(G, *)$ ein Monoid, dann setzt man $g^0 = e_G$. Ist g darüber hinaus invertierbar, dann setzt man $g^{-n} = (g^n)^{-1}$ für alle $n \in \mathbb{N}$ und hat damit insgesamt g^n für alle $n \in \mathbb{Z}$ definiert.

Lemma 2.2 Sei $(G, *)$ eine Halbgruppe.

(i) Für alle $g \in G$ und $m, n \in \mathbb{N}$ gilt $g^m * g^n = g^{m+n}$ und $(g^m)^n = g^{mn}$.

(ii) Sind $g, h \in G$ ***vertauschbare*** Elemente, gilt also $g * h = h * g$, dann folgt $(g * h)^n = g^n * h^n$ für $g, h \in G$ und $n \in \mathbb{N}$.

(iii) Ist allgemeiner $\{g_1, ..., g_r, h_1, ..., h_r\}$ eine Menge in G bestehend aus paarweise vertauschbaren Elementen (mit $r \in \mathbb{N}$), dann gilt die Regel

$$(g_1 * ... * g_r) * (h_1 * ... * h_r) \quad = \quad (g_1 * h_1) * ... * (g_r * h_r)$$

und außerdem $(g_1 * ... * g_r)^m = g_1^m * ... * g_r^m$.

In einem Monoid gelten alle Regeln entsprechend für $m, n \in \mathbb{N}_0$, im Falle invertierbarer Elemente g, h für $m, n \in \mathbb{Z}$.

Den *Beweis* dieses Lemmas behandeln wir in den Übungen.

Liegt die Halbgruppe $(G, +)$ in additiver Schreibweise vor, dann schreibt man ng statt g^n. Die rekursive Definition der n-ten Potenz lautet dann $1 \cdot g = g$ und $(n+1)g = ng + g$, und die übrigen Rechenregeln nehmen die folgende Form an.

$$mg + ng = (m+n)g \quad , \quad n(mg) = (mn)g \quad , \quad n(g+h) = ng + nh \quad ,$$
$$(g_1 + ... + g_r) + (h_1 + ... + h_r) = (g_1 + h_1) + ... + (g_r + h_r) \quad , \quad g_1 + ... + g_r = g_r + ... + g_1 \quad ,$$
$$m(g_1 + ... + g_r) = mg_1 + ... + mg_r.$$

Man beachte, dass die dritte bis sechste Regel wiederum die Vertauschbarkeit der Elemente erfordert. Allerdings hatten wir ja bereits bemerkt, dass die additive Schreibweise nur bei kommutativen Strukturen verwendet wird.

Definition 2.3 Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ wird ***Untergruppe*** von G genannt, wenn e_G in U liegt und für alle $a, b \in U$ auch die Elemente $a \cdot b$ und a^{-1} in U liegen.

Die Schreibweise $U \leq G$ bedeutet, dass U eine Untergruppe von G ist.
Wir ergänzen die Definition um zwei Bemerkungen.

(1) In der Definition enthalten ist die Bedingung, dass U eine unter der Verknüpfung $\cdot$ abgeschlossene Teilmenge ist. Wie in § 1 ausgeführt, erhält man somit durch Einschränkung eine Verknüpfung $\cdot_U$ auf U.

(2) Unmittelbar aus Definition ergibt sich auch, dass für alle $a \in U$ und $m \in \mathbb{Z}$ auch a^m in U enthalten ist, und das für jedes $r \in \mathbb{N}$ mit $a_1, ..., a_r \in U$ auch das Produkt $a_1 \cdot ... \cdot a_r$ in U enthalten ist. Beide Aussagen zeigt man durch einfache Induktionsbeweise.

An die Bemerkung (1) schließt sich folgende Feststellung an, durch den Begriff „Untergruppe“ letztlich rechtfertigt.

Proposition 2.4 Das Paar $(U, \cdot_U)$ ist eine Gruppe.

Beweis: Die Verknüpfung $\cdot_U$ stimmt auf ihrem gesamten Definitionsbereich mit $\cdot$ überein. Wieder überträgt sich das Assoziativgesetz von $(G, \cdot)$ auf $(U, \cdot_U)$, d.h. für alle $a, b, c \in U$ gilt $(a \cdot_U b) \cdot_U c = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot_U (b \cdot_U c)$ für alle $a, b, c \in U$. Auf Grund der Voraussetzung $e_G \in U$ und wegen $e_G \cdot_U a = e_G \cdot a = a$, $a \cdot_U e_G = a \cdot e_G = a$ ist e_G ein Neutralelement der Halbgruppe $(U, \cdot_U)$; die Halbgruppe ist also ein Monoid. Für jedes $a \in U$ ist auch a^{-1} in U enthalten. Die Gleichungen $a \cdot_U a^{-1} = a \cdot a = e_G$ und $a^{-1} \cdot_U a = a^{-1} \cdot a = e_G$ zeigen jeweils, dass a im Monoid $(U, \cdot_U)$ ein invertierbares Element ist, und das Inverse von a in $(G, \cdot)$ zugleich das Inverse von a in $(U, \cdot_U)$. Insgesamt ist $(U, \cdot_U)$ also tatsächlich eine Gruppe. □

Bereits im ersten Kapitel sind uns eine Vielzahl von Untergruppen begegnet.

(i) Ist G eine beliebige Gruppe, dann sind $\{e_G\}$ und G Untergruppen von G. Man bezeichnet $\{e_G\}$ auch als die ***triviale*** Untergruppe von G. Für beide Mengen kontrolliert man unmittelbar, dass die Untergruppen-Bedingungen erfüllt sind.

(ii) Die Gruppe $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$, und diese wiederum ist eine Untergruppe von $(\mathbb{R}, +)$.

(iii) Für jedes $n \in \mathbb{N}$ ist die alternierende Gruppe A_n eine Untergruppe der symmetrischen Gruppe S_n. Des Weiteren ist die vierelementige Menge

$$V_4 \quad = \quad \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

ihrerseits eine Untergruppe von A_4. Man nennt sie die ***Kleinsche Vierergruppe***. Zum Nachweis der Untergruppen-Eigenschaft bemerken wir zunächst, dass das Neutralelement id von A_4 in V_4 liegt. Die Verknüpfungstabelle

$\circ$	id	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
id	id	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2)(3 4)	(1 2)(3 4)	id	(1 4)(2 3)	(1 3)(2 4)
(1 3)(2 4)	(1 3)(2 4)	(1 4)(2 3)	id	(1 2)(3 4)
(1 4)(2 3)	(1 4)(2 3)	(1 3)(2 4)	(1 2)(3 4)	id

hat nur Einträge in V_4; dies zeigt, dass V_4 eine bezüglich $\circ$ abgeschlossene Teilmenge von A_4 ist. Außerdem rechnet man unmittelbar nach, dass

$$((1\ 2)(3\ 4))^2 \quad = \quad ((1\ 3)(2\ 4))^2 \quad = \quad ((1\ 4)(2\ 3))^2 \quad = \quad \mathrm{id}$$

gilt und somit neben id auch jedes andere Element in V_4 sein eignes Inverses ist. Für jedes $\sigma \in V_4$ gilt also insbesondere $\sigma^{-1} \in V_4$, wodurch auch die letzte Untergruppen-Eigenschaft nachgewiesen ist.

(iv) Die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ ist eine Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}_n(K)$ (für jeden Körper K und $n \in \mathbb{N}$). Ebenso ist $\mathcal{O}(n)$ eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$, und $\mathcal{U}(n)$ ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{C})$.

(v) Die Gruppe $\mathcal{B}_n$ der Bewegungen ist eine Untergruppe von $\mathrm{Per}(\mathbb{R}^n)$, und $\mathcal{B}_n^+$ ist eine Untergruppe von $\mathcal{B}_n$, und wiederum auch von $\mathrm{Per}(\mathbb{R}^n)$.

(vi) Für jede Teilmenge $T \subseteq \mathbb{R}^n$ ist die Symmetriegruppe $\mathrm{Sym}(T)$ eine Untergruppe von $\mathcal{B}_n$, und $\mathrm{Sym}^+(T)$ ist eine Untergruppe von $\mathcal{B}_n^+$.

Um die Struktur einer Gruppe G zu verstehen, ist es wichtig, einen Überblick über die Untergruppen von G zu erhalten. Als nächstes befassen wir uns deshalb mit der Frage, wie sich die Untergruppen auf möglichst effiziente Weise spezifieren lassen. Dies führt uns auf den Begriff des *Erzeugendensystems*.

Proposition 2.5 Sei $(G, \cdot)$ eine Gruppe, und sei $(U_i)_{i \in I}$ eine Familie von Untergruppen von G. Dann ist auch $U = \bigcap_{i \in I} U_i$ eine Untergruppe von G.

Beweis: Weil jedes U_i eine Untergruppe von $(G, \cdot)$ ist, gilt $e_G \in U_i$ für alle $i \in I$ und damit auch $e_G \in U$. Seien nun $a, b \in U$ vorgegeben. Dann gilt $a, b \in U_i$ für alle $i \in I$, und aus der Untergruppe-Eigenschaft von U_i folgt jeweils $ab \in U_i$ und $a^{-1} \in U_i$, für jedes $i \in I$. Daraus wiederum folgt $ab \in U$ und $a^{-1} \in U$. □

In vielen Situationen ist es wünschenswert, Untergruppen auf möglichst kurze und einfache Art und Weise zu spezifizieren. Eine einfache Möglichkeit ist die Beschreibung von Untergruppen durch Erzeugendensysteme.

Satz 2.6 Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Dann gibt es eine eindeutig bestimmte Untergruppe U von G mit den folgenden Eigenschaften.

(i) $U \supseteq S$

(ii) Ist V eine weitere Untergruppe von G mit $V \supseteq S$, dann folgt $V \supseteq U$.

Beide Bedingungen lassen sich zusammenfassen in der Aussage, dass U die *kleinste* Untergruppe von G ist, die S als Teilmenge enthält.

Beweis: *Existenz:* Sei (U_i) die Familie aller Untergruppen von G mit $U_i \supseteq S$. Dann ist nach Proposition 2.5 auch $U = \bigcap_{i \in I} U_i$ eine Untergruppe von G, und aus $U_i \supseteq S$ für alle $i \in I$ folgt $U \supseteq S$. Sei nun V eine weitere Untergruppe von G mit $V \supseteq S$. Dann gilt $V = U_j$ für ein $j \in I$, und weil nach Definition $U \subseteq U_i$ für alle $i \in I$ gilt, folgt $V \supseteq U$.

Eindeutigkeit: Seien U, U' zwei Untergruppen von G, die beide (i) und (ii) erfüllen. Dann gilt $U \supseteq S$ und $U' \supseteq S$. Aus der Eigenschaft (ii) für U folgt $U' \supseteq U$, und aus Eigenschaft (ii) für U' folgt $U \supseteq U'$, insgesamt also $U = U'$. □

Definition 2.7 Die Untergruppe U aus Satz 2.6 wird die von S ***erzeugte*** Untergruppe genannt und mit $\langle S \rangle$ bezeichnet. Ist V eine beliebige Untergruppe von G, dann wird jede Teilmenge T von G mit $V = \langle T \rangle$ ein ***Erzeugendensystem*** von V genannt.

Ist S eine einelementige Teilmenge einer Gruppe G, $S = \{g\}$ für ein $g \in G$, dann verwendet man die Notation $\langle g \rangle$ an Stelle der korrekten, aber umständlichen Schreibweise $\langle \{g\} \rangle$. Auch bei endlichen Mengen mit mehr Elementen wird häufig an Stelle von $\langle \{g_1, ..., g_n\} \rangle$ die einfachere Notation $\langle g_1, ..., g_n \rangle$ verwendet. Wir betrachten nun eine Reihe von Beispielen für Erzeugendensysteme von Untergruppen.

(i) In jeder Gruppe G gilt $\langle\varnothing\rangle = \{e_G\}$. Denn wie wir bereits festgestellt haben, ist $\{e_G\}$ eine Untergruppe, und diese enthält trivialerweise $\varnothing$ als Teilmenge. Andererseits ist e_G in jeder Untergruppe U von G enthalten, also ist $\{e_G\}$ eine Teilmenge jeder Untergruppe V von G mit $V \supseteq \varnothing$.

(ii) Es ist leicht zu sehen, dass die Gruppe $(\mathbb{Z}, +)$ von der einelementigen Menge $\{1\}$ erzeugt wird, denn jedes Element $k \in \mathbb{Z}$ kann in der Form $k \cdot 1$ dargestellt werden, wobei $k \cdot 1$ die k-te Potenz des Elements 1 in additiver Schreibweise bedeutet. Ebenso ist $\{-1\}$ ein Erzeugendensystem, denn jedes $k \in \mathbb{Z}$ hat die Darstellung $k = (-k) \cdot (-1)$. Allgemein gilt $\langle m\rangle = m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$ für jedes $m \in \mathbb{N}_0$.

Wir werden später sehen, dass alle Untergruppen von $(\mathbb{Z}, +)$ diese Form haben. Dass sich alle Untergruppen einer Gruppe so leicht angeben lassen, ist leider nur sehr selten der Fall.

Definition 2.8 Eine Gruppe G wird ***zyklisch*** genannt, wenn ein $g \in G$ mit $G = \langle g\rangle$ existiert. Existiert eine endliche Teilmenge $S \subseteq G$ mit $G = \langle S\rangle$, dann nennt man G eine ***endlich erzeugte*** Gruppe.

Die zyklischen Gruppen werden wir in § 3 ausführlich studieren. Ein einfaches Beispiel ist, wie wir oben gesehen haben, die Gruppe $(\mathbb{Z}, +)$. Die endlich erzeugten Gruppen sind leider nicht so übersichtlich, aber in § 5 werden wir zumindest die endlich erzeugten *abelschen* Gruppen bis auf Isomorphie klassifizieren. Es ist relativ leicht zu sehen, dass beispielsweise die Gruppe $(\mathbb{Q}, +)$ nicht endlich erzeugt ist. Den Beweis behandeln wir in den Übungen.

Unser nächstes Ziel besteht darin, die in einer Untergruppe der Form $\langle S\rangle$ liegenden Elemente explizit anzugeben. Dazu verwenden wir sowohl die im Anschluss an Definition 2.3 formulierte Eigenschaft von Untergruppen als auch die in Proposition 1.13 formulierten Rechenregeln für invertierbare Elemente. Um die folgenden Aussagen zu vereinfachen, führen wir die folgende Konvention ein: Das Neutralelement e_G einer Gruppe G ist bei uns stets ein Produkt aus null Faktoren. Der Ausdruck $g_1 \cdot \ldots \cdot g_r$ steht also im Fall $r = 0$ für das Element e_G.

Satz 2.9 Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge.

(i) Die Elemente von $\langle S\rangle$ sind gegeben durch

$$\langle S\rangle \quad = \quad \{g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0\ ,\ g_1, \ldots, g_r \in S, \varepsilon_k \in \{\pm 1\} \text{ für } 1 \leq k \leq r\}.$$

(ii) Sei S endlich, $S = \{g_1, \ldots, g_m\}$ für ein $m \in \mathbb{N}_0$, und setzen wir voraus, dass jedes Element der Menge S mit jedem anderen vertauschbar ist. Dann gilt

$$\langle S\rangle = \{g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \mid e_k \in \mathbb{Z} \text{ für } 1 \leq k \leq m\}.$$

Beweis: zu (i) Sei U die Teilmenge auf der rechten Seiten der Gleichung. Zunächst überprüfen wir, dass U eine Untergruppe von G ist. Da wir in der Definition von U Produkte der Länge $r = 0$ eingeschlossen haben, ist das Neutralelement e_G in U enthalten. Seien nun $g, g' \in U$ vorgegeben. Dann gibt es nach Definition Elemente $r, s \in \mathbb{N}_0$,

$g_1, ..., g_r, g'_1, ..., g'_s \in S$ und $\varepsilon_1, ..., \varepsilon_r, \varepsilon'_1, ..., \varepsilon'_s \in \{\pm 1\}$, so dass $g = g_1^{\varepsilon_1} \cdot ... \cdot g_r^{\varepsilon_r}$ und $g' = (g'_1)^{\varepsilon'_1} \cdot ... \cdot (g'_s)^{\varepsilon_s}$ erfüllt ist. Offenbar sind die Elemente

$$gg' = g_1^{\varepsilon_1} \cdot ... \cdot g_r^{\varepsilon_r} \cdot (g'_1)^{\varepsilon'_1} \cdot ... \cdot (g'_s)^{\varepsilon_s} \qquad \text{und} \qquad g^{-1} = g_r^{-\varepsilon_r} \cdot ... \cdot g_1^{-\varepsilon_1}$$

nach Definition ebenfalls in U enthalten. Also handelt es sich bei U tatsächlich um eine Untergruppe von G. Außerdem enthält sie S als Teilmenge: Ist $g \in S$ beliebig vorgegeben, dann setzt man $g_1 = g$, $\varepsilon_1 = 1$ und erhält $g = g_1^{\varepsilon_1} \in U$.

Nun müssen wir noch zeigen, dass U die kleinste Untergruppe von G mit $U \supseteq S$ ist. Sei V eine beliebige Untergruppe von G mit $V \supseteq S$; nachzuweisen ist $V \supseteq U$. Zunächst bemerken wir, dass das Produkt der Länge $r = 0$ in V enthalten ist, denn als Untergruppe von G enthält V das Neutralelement e_G. Seien nun $r \in \mathbb{N}$, $g_1, ..., g_r \in S$ und $\varepsilon_1, ..., \varepsilon_r \in \{\pm 1\}$. Wegen $S \subseteq V$ gilt dann auch $g_1, ..., g_r \in V$. Weil V eine Untergruppe von G ist, folgt $g_k^{\varepsilon_k} \in V$ für $1 \leq k \leq r$ und schließlich $g_1^{\varepsilon_1} \cdot ... \cdot g_r^{\varepsilon_r} \in V$. Damit ist der Nachweis der Inklusion $U \subseteq V$ erbracht.

zu (ii) Hier gehen wir nach demselben Schema vor und zeigen zunächst, dass die Menge auf der rechten Seite der Gleichung, die wir mit U bezeichnen, eine Untergruppe von G ist. Durch Setzen von $e_k = 0$ für $1 \leq k \leq m$ sieht man, dass U das Neutralelement enthält. Seien nun $g, g' \in U$ vorgegeben. Dann gibt es Elemente $e_1, ..., e_m, e'_1, ..., e'_m \in \mathbb{Z}$ mit $g = g_1^{e_1} \cdot ... \cdot g_m^{e_m}$ und $g' = g_1^{e'_1} \cdot ... \cdot g_m^{e'_m}$. Es folgt

$$gg' \quad = \quad (g_1^{e_1} \cdot ... \cdot g_m^{e_m})(g_1^{e'_1} \cdot ..... \cdot g_m^{e'_m}) \quad = \quad (g_1^{e_1} g_1^{e'_1}) \cdot ... (g_m^{e_m} g_m^{e'_m}) \quad = \quad g_1^{e_1+e'_1} \cdot ... \cdot g_m^{e_m+e'_m}$$

und

$$g^{-1} \quad = \quad (g_1^{e_1} \cdot ... \cdot g_m^{e_m})^{-1} \quad = \quad (g_m^{e_m})^{-1} \cdot ... \cdot (g_1^{e_1})^{-1} \quad = \quad g_m^{-e_m} \cdot ... \cdot g_1^{-e_1} \quad = \quad g_1^{-e_1} \cdot ... \cdot g_m^{-e_m} \in U.$$

Damit ist der Nachweis der Untergruppen-Eigenschaft abgeschlossen. Nun zeigen wir, dass $U \supseteq S$ gilt. Sei dazu $k \in \{1, ..., m\}$ vorgegeben. Setzen wir $e_k = 1$ und $e_i = 0$ für $1 \leq i \leq m$ mit $i \neq k$, dann erhalten wir $g_k = g_1^{e_1} \cdot ... \cdot g_m^{e_m} \in U$. Sei nun V eine beliebige Untergruppe von G mit $V \supseteq S$. Dann gilt $g_k \in V$ für $1 \leq k \leq m$. Sind $e_1, ..., e_m \in \mathbb{Z}$ beliebig vorgegeben, dann folgt auf Grund der Untergruppen-Eigenschaft $g_k^{e_k} \in V$ für $1 \leq k \leq m$ und schließlich $g_1^{e_1} \cdot ... \cdot g_m^{e_m} \in V$. Damit ist der Nachweis von $U \subseteq V$ abgeschlossen. □

Folgerung 2.10

(i) Ist G eine Gruppe und $g \in G$, dann gilt $\langle g \rangle = \{g^e \mid e \in \mathbb{Z}\}$.

(ii) Jede zyklische Gruppe ist abelsch.

Beweis: Die Aussage (i) ist der Spezialfall von Satz 2.9 (ii) mit $m = 1$. Zum Beweis von (ii) sei G eine zyklische Gruppe und $g_1 \in G$ ein Element mit $G = \langle g_1 \rangle$. Sind $g, h \in G$ beliebig vorgegeben, dann gilt nach (i) $g = g_1^m$ und $h = g_1^n$ für geeignete $m, n \in \mathbb{Z}$. Es folgt $gh = g_1^m g_1^n = g_1^{m+n} = g_1^{n+m} = g_1^n g_1^m = hg$. □

Als konkretes Beispiel betrachten wir nun Erzeugendensysteme der symmetrischen Gruppen S_n und der alternierenden Gruppen A_n. Für den Beweis benötigen wir den folgenden Begriff: Der ***Träger*** $\mathrm{supp}(\sigma)$ eines Elements $\sigma \in S_n$ ist die Menge aller $j \in M_n$ mit $\sigma(j) \neq j$. Wird σ als Produkt disjunkter Zykel dargestellt, so besteht der Träger aus genau denjenigen Elementen, die in einem der Zykel vorkommen.

Das Konzept des Trägers ist vor allem aus folgendem Grund wichtig: Seien $\sigma, \tau \in S_n$ mit $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$. Dann sind die Elemente σ und τ ***vertauschbar***, d.h. es gilt

$$\sigma \circ \tau \quad = \quad \tau \circ \sigma.$$

Zum Beweis bemerken wir vorweg: Für jedes $\sigma \in S_n$ und jedes $k \in M_n$ gilt $k \in \text{supp}(\sigma)$ genau dann, wenn auch $\sigma(k)$ in $\text{supp}(\sigma)$ liegt. Denn wäre $k \in \text{supp}(\sigma)$ und $\sigma(k) \notin \text{supp}(\sigma)$, dann würde $\sigma(k) = \sigma(\sigma(k))$ gelten, im Widerspruch zur Bijektivität von σ. Der Fall $k \notin \text{supp}(\sigma)$ und $\sigma(k) \in \text{supp}(\sigma)$ kann ebenfalls nicht eintreten, denn aus $k \notin \text{supp}(\sigma)$ folgt $\sigma(k) = k$.

Nun überprüfen wir, dass unter der Voraussetzung $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ die Abbildungen $\sigma \circ \tau$ und $\tau \circ \sigma$ auf jedem $k \in M_n$ übereinstimmen. Für $k \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$ gilt $(\sigma \circ \tau)(k) = k = (\tau \circ \sigma)(k)$. Betrachten wir nun den Fall $k \in \text{supp}(\sigma)$ und $k \notin \text{supp}(\tau)$. Dann gilt $(\sigma \circ \tau)(k) = \sigma(\tau(k)) = \sigma(k)$ und wegen $\sigma(k) \in \text{supp}(\sigma)$ und $\sigma(k) \notin \text{supp}(\tau)$ auch $(\tau \circ \sigma)(k) = \tau(\sigma(k)) = \sigma(k)$. Der Fall $k \notin \text{supp}(\sigma)$ und $k \in \text{supp}(\tau)$ läuft analog. Der Fall $k \in \text{supp}(\sigma)$ und $k \in \text{supp}(\tau)$ schließlich kann auf Grund der Voraussetzung nicht eintreten.

Satz 2.11 Sei $n \in \mathbb{N}$ beliebig.

(i) Die Menge der Transpositionen bildet ein Erzeugendensystem von S_n.

(ii) Die Menge der 3-Zykel bilden ein Erzeugendensystem von A_n.

Beweis: zu (i) Wir beweisen durch vollständige Induktion über $|\text{supp}(\sigma)|$, dass jedes $\sigma \in S_n$ als Produkt von Transpositionen dargestellt werden kann, wobei wir id wie immer als „leeres“ Produkt mit null Faktoren ansehen. Im Fall $|\text{supp}(\sigma)| = 0$ gilt $\text{supp}(\sigma) = \emptyset$ und $\sigma = \text{id}$, also ist hier nichts zu zeigen. Elemente $\sigma \in S_n$ mit $|\text{supp}(\sigma)| = 1$ existieren nicht, und die Elemente mit $|\text{supp}(\sigma)| = 2$ sind genau die Transpositionen.

Sei nun $k \in \{3, \ldots, n\}$ und $\sigma \in S_n$ mit $|\text{supp}(\sigma)| = k$, und setzen wir die Aussage für Werte $< k$ per Induktionsannahme voraus. Sei $i \in \text{supp}(\sigma)$ beliebig gewählt und $\tau = (i\ \sigma(i)) \circ \sigma$. Mit i auch $\sigma(i)$ in $\text{supp}(\sigma)$ enthalten. Damit ist klar, dass jedes $k \notin \text{supp}(\sigma)$ auch nicht in $\text{supp}(\tau)$ enthalten ist, also $\text{supp}(\tau) \subseteq \text{supp}(\sigma)$ gilt. Andererseits ist offenbar $\tau(i) = i$, also $i \in \text{supp}(\sigma) \setminus \text{supp}(\tau)$ und deshalb sogar $\text{supp}(\tau) \subsetneq \text{supp}(\sigma)$. Wir können damit die Induktionsvoraussetzung auf τ anwenden und erhalten eine Darstellung $\tau = \tau_1 \circ \ldots \circ \tau_r$ von τ als Produkt von Transpositionen τ_k. Folglich ist auch $\sigma = (i\ \sigma(i))^{-1} \circ \tau = (i\ \sigma(i))^{-1} \circ \tau_1 \circ \ldots \circ \tau_r$ als Produkt von Transpositionen darstellbar.

zu (ii) Sei $T \subseteq S_n$ die Menge der 3-Zyklen in S_n. Wir zeigen zunächst, dass jedes $\sigma \in A_n$ das Produkt von 3-Zyklen dargestellt werden kann und beweisen damit die Inklusion $A_n \subseteq \langle T \rangle$. Nach (i) besitzt σ eine Darstellung $\sigma = \tau_1 \circ \ldots \circ \tau_r$ als Produkt von Transpositionen, und wegen $\text{sgn}(\sigma) = 1$ und $\text{sgn}(\tau_k) = -1$ für $1 \leq k \leq r$ ist r gerade. Nun gilt allgemein für je zwei Transpositionen mit einem gemeinsamen Element im Träger die Gleichung $(i\ j) \circ (i\ k) = (i\ k\ j)$, wie man unmittelbar überprüft. Stimmen zwei Elemente im Träger überein, dann gilt offenbar $(i\ j) \circ (i\ j) = \text{id}$. Sind $(i\ j)$ und $(k\ \ell)$ schließlich disjunkte Zykel, dann gilt $(i\ j) \circ (k\ \ell) = (i\ k\ j) \circ (i\ k\ \ell)$. Somit kann jeder der Faktoren $\tau_1 \circ \tau_2$, $\tau_3 \circ \tau_4$, ..., $\tau_{r-1} \circ \tau_r$ als Produkt von 0 bis zwei 3-Zyklen dargestellt werden. Damit ist der Beweis von $A_n \subseteq \langle T \rangle$ abgeschlossen. Umgekehrt hat jeder 3-Zykel ein positives Signum, somit gilt $T \subseteq A_n$. Da $\langle T \rangle$ die kleinste Untergruppe ist, die T als Teilmenge enthält, folgt $\langle T \rangle \subseteq A_n$ und insgesamt $\langle T \rangle = A_n$. □

Wie wir gleich sehen werden, genügen sogar *zwei* Elemente, um die gesamte Gruppe S_n zu erzeugen; dieses Resultat wird auch später in der Galoistheorie benötigt. Hierfür benötigen wir den Begriff der ***Konjugation***. Sind g und h Elemente einer Gruppe G, dann bezeichnet man ghg^{-1} als das Element, dass durch Konjugation h mit g entsteht.

Proposition 2.12 Für jedes $n \in \mathbb{N}$ ist die Menge $\{\sigma, \tau\}$ bestehend aus den beiden Elementen $\sigma = (1\ 2\ \ldots\ n)$ und $\tau = (1\ 2)$ ein Erzeugendensystem von S_n. Ist n eine ungerade Primzahl, dann wird S_n sogar von *jeder* zweielementigen Menge bestehend aus einem n-Zykel und einer Transposition erzeugt.

Beweis: Für das Verständnis dieses Beweises ist es hilfreich, sich vorher die Auswirkung der Konjugation eines Elements von S_n mit einem anderen Element klar zu machen. (Wir gehen im Kapitel über die Klassengleichung detailliert darauf ein.) Beispielsweise entsteht durch Konjugation von τ mit σ das Element

$$\sigma\tau\sigma^{-1} \quad = \quad (\sigma(1)\,\sigma(2)) \quad = \quad (2\ 3).$$

Ebenso erhält man durch Konjugation von τ mit σ^2, σ^3, ... die Transpositionen (3 4), (4 5), ... und durch Konjugation von τ mit σ^{n-2} schließlich die Transposition $(n-1\ n)$. Sei nun $i \in \{1, ..., n-1\}$ vorgegeben. Dann gilt

$$(i+1\ \ i+2)\circ(i\ \ i+1)\circ(i+1\ \ i+2) = (i\ \ i+2)\,, \quad (i+2\ i+3)\circ(i\ \ i+2)\circ(i+2\ i+3) = (i\ \ i+3) \quad \text{usw.}$$

Insgesamt kann auf diese Weise jedes Element $(i\ \ i+k)$ mit $i+k \leq n$ gebildet werden. Dies zeigt, dass $\langle\sigma, \tau\rangle$ die gesamte Menge $T \subseteq S_n$ aller Transpositionen enthält. Es folgt $\langle\sigma, \tau\rangle = \langle T\rangle$, und wegen $\langle T\rangle = S_n$ nach Satz 2.11 ist damit die erste Aussage bewiesen.

Der Beweis der zweiten Aussage ist recht umfangreich; darüber hinaus müssen wir im hinteren Teil auf ein wenig Zahlentheorie und Kongruenzrechnung zurückgreifen, die wir erst später in der Vorlesung entwickeln. Sei $p = n$ eine ungerade Primzahl, $\sigma = (i_1\ i_2\ \ldots\ i_p)$ ein p-Zykel und τ eine beliebige Transposition. Definieren wir $\rho \in S_p$ durch

$$\rho \quad = \quad \begin{pmatrix} 1 & 2 & \cdots & p \\ i_1 & i_2 & \ldots & i_p \end{pmatrix}^{-1} \quad ,$$

dann ist das Element $\tilde{\sigma} = \rho\sigma\rho^{-1}$ gegeben durch $\tilde{\sigma} = (\rho(i_1) \ldots \rho(i_p)) = (1\ 2\ \ldots\ p)$. Sei außerdem $\tilde{\tau} = \rho\tau\rho^{-1}$. Wie man leicht überprüft, ist durch die Konjugationsabbildung $\phi_\rho(\alpha) = \rho\alpha\rho^{-1}$ ein Automorphismus von S_p definiert. Es gilt $\phi_\rho(\langle\sigma, \tau\rangle) = \langle\phi_\rho(\sigma), \phi_\rho(\tau)\rangle = \langle\tilde{\sigma}, \tilde{\tau}\rangle$, denn einerseits ist $\{\tilde{\sigma}, \tilde{\tau}\}$ eine Teilmenge von $\phi_\rho(\langle\sigma, \tau\rangle)$, und andererseits gilt $\{\sigma, \tau\} \subseteq \phi_\rho^{-1}(\langle\tilde{\sigma}, \tilde{\tau}\rangle)$, woraus $\langle\sigma, \tau\rangle \subseteq \phi_\rho^{-1}(\langle\tilde{\sigma}, \tilde{\tau}\rangle)$ und $\phi_\rho(\langle\sigma, \tau\rangle) = \langle\tilde{\sigma}, \tilde{\tau}\rangle$ folgt. Wenn wir nun zeigen können, dass $\langle\tilde{\sigma}, \tilde{\tau}\rangle = S_p$ gilt, dann folgt daraus $\langle\sigma, \tau\rangle = \phi_\rho^{-1}(S_p) = \phi_{\rho^{-1}}(S_p) = S_p$. Aus diesem Grund dürfen wir im nachfolgenden Teil des Beweises σ, τ durch $\tilde{\sigma}, \tilde{\tau}$ ersetzen und annehmen, dass $\sigma = (1\ 2\ \ldots\ p)$ gilt.

Sei $\tau = (i\ j)$ mit $i, j \in M_p$ und $i < j$. Dann ist auch das Element $\sigma^{1-i}\tau\sigma^{i-1} = (1\ j-i+1)$ in $\langle\sigma, \tau\rangle$ enthalten. Nach Ersetzung von τ durch dieses Element können wir annehmen, dass τ die Form $(1\ i)$ mit $1 < i \leq p$ hat. Wir zeigen nun: Sind $k, r \in \mathbb{N}$ mit $1 \leq k \leq p-1$ und $r \in M_p$, und gilt $r \equiv 1 + k(i-1) \bmod p$, dann liegt das Element $(1\ r)$ in $\langle\sigma, \tau\rangle$. Wir beweisen die Aussage durch vollständige Induktion über k; die Zahl r ist durch k jeweils eindeutig festgelegt. Für $k = 1$ ist $r = i$, und dass $(1\ i)$ in $\langle\sigma, \tau\rangle$ liegt, ist bereits bekannt. Setzen wir nun die Aussage für ein $k \in \mathbb{N}$ mit $1 \leq k < p-1$ voraus, und seien $r, s \in M_p$ die eindeutig bestimmten Elemente mit $r \equiv 1 + k(i-1) \bmod p$ und $s \equiv 1 + (k+1)(i-1) \bmod p$. Ist $r + (i-1) < p$, dann gilt $s = r + (i-1)$ und somit $\sigma^{r-1}(1\ i)\sigma^{1-r} = (r\ s)$. Im Fall $r + (i-1) > p$ gilt $s = r + (i-1) - p$ und $\sigma^{r-1-p}(1\ i)\sigma^{1+p-r} = (r\ s)$. In beiden Fällen zeigt die Gleichung $(r\ s)(1\ r)(r\ s) = (1\ s)$, dass auch $(1\ s)$ in $\langle\sigma, \tau\rangle$ enthalten ist.

Wegen $\mathrm{ggT}(i-1, p) = 1$ existieren nun nach dem Lemma von Bézout $k, \ell \in \mathbb{Z}$ mit $k(i-1) + \ell p = 1$. Dabei ist p kein Teiler von k, da aus der Gleichung ansonsten $p \mid 1$ folgen würde. Sei $x \in \mathbb{Z}$ so gewählt, dass $1 \leq k + px \leq p-1$ gilt. Dann folgt $(k+px)(i-1) + (\ell - x(i-1))p = 1$; nach Ersetzung von k durch $k+px$ und ℓ durch $\ell - x(i-1)$ können

wir also $1 \leq k \leq p-1$ voraussetzen. Wenden wir nun die im vorherigen Abschnitt bewiesene Aussage auf dieses k an und setzen wir $r = 2$, dann gilt $r \in M_p$, $r = 1+1 = 1+k(i-1)+\ell p \equiv 1+k(i-1) \bmod p$ und $(1\ r) = (1\ 2) \in \langle \sigma, \tau \rangle$. Wegen $\sigma = (1\ 2\ \ldots\ p) \in \langle \sigma, \tau \rangle$ enthält $\langle \sigma, \tau \rangle$ auf Grund der ersten Aussage der Proposition also ein vollständiges Erzeugendensystem von S_p. □

Wenden wir uns nun dem zweiten Thema dieses Kapitels zu, dem Satz von Lagrange.

Definition 2.13 Sei $(G, \cdot)$ eine Gruppe und U eine Untergruppe. Eine Teilmenge von G, die mit einem geeigneten $g \in G$ in der Form

$$gU \quad = \quad \{gu \mid u \in U\}$$

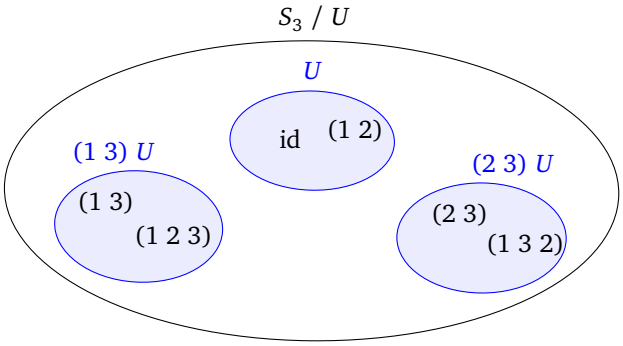
geschrieben werden kann, wird ***Linksnebenklasse*** von U genannt. Ebenso bezeichnet man die Teilmengen der Form $Ug = \{ug \mid u \in U\}$ mit $g \in G$ als ***Rechtsnebenklassen*** von U.

Desweiteren führen wir die Bezeichnung G/U für die Menge der Linksnebenklassen und $U\backslash G$ für die Menge der Rechtsnebenklassen von U ein. Es gilt also $G/U = \{gU \mid g \in G\}$ und $U\backslash G = \{Ug \mid g \in G\}$. Sei beispielsweise $G = S_3$ und $U = \langle (1,2) \rangle = \{\mathrm{id}, (1\ 2)\}$. Dann sind die Linksnebenklassen von U gegeben durch

$$\begin{array}{rcll}
\mathrm{id} \circ U & = & \{\mathrm{id} \circ \mathrm{id}, \mathrm{id} \circ (1\ 2)\} & = & \{\mathrm{id}, (1\ 2)\} \\
(1\ 2) \circ U & = & \{(1\ 2) \circ \mathrm{id}, (1\ 2) \circ (1\ 2)\} & = & \{(1\ 2), \mathrm{id}\} \\
(1\ 3) \circ U & = & \{(1\ 3) \circ \mathrm{id}, (1\ 3) \circ (1\ 2)\} & = & \{(1\ 3), (1\ 2\ 3)\} \\
(2\ 3) \circ U & = & \{(2\ 3) \circ \mathrm{id}, (2\ 3) \circ (1\ 2)\} & = & \{(2\ 3), (1\ 3\ 2)\} \\
(1\ 2\ 3) \circ U & = & \{(1\ 2\ 3) \circ \mathrm{id}, (1\ 2\ 3) \circ (1\ 2)\} & = & \{(1\ 2\ 3), (1\ 3)\} \\
(1\ 3\ 2) \circ U & = & \{(1\ 3\ 2) \circ \mathrm{id}, (1\ 3\ 2) \circ (1\ 2)\} & = & \{(1\ 3\ 2), (2\ 3)\}
\end{array}$$

Es gilt also $S_3/U = \{\ \{\mathrm{id}, (1\ 2)\}\ ,\ \{(1\ 3), (1\ 2\ 3)\}\ ,\ \{(2\ 3), (1\ 3\ 2)\}\ \}$.

Graphisch kann die Menge S_3/U der Linksnebenklassen folgendermaßen dargestellt werden.



Die Elemente von S_3/U sind die Linksnebenklassen U, $(1\ 2)U$ und $(2\ 3)U$, also die blau gezeichneten Objekte. Die Permutation $(1\ 2\ 3)$ ist ein Element von S_3 und auch ein Element der Linksnebenklasse $(1\ 3)U$, die ja ihrerseits eine Teilmenge von S_3 ist. Aber $(1\ 2\ 3)$ ist *kein* Element von S_3/U, denn die Elemente von S_3/U sind nach Definition bestimmte *Teilmengen* von S_3, keine *Elemente* von S_3!

Offenbar ist es möglich, dass zwei Nebenklassen gU und hU übereinstimmen, ohne dass $g = h$ ist. In unserem Beispiel gilt etwa $(1\ 3) \circ U = (1\ 2\ 3) \circ U$. Nach dem gleichen Schema können wir auch die Rechtsnebenklassen von U bestimmen.

$$\begin{array}{lcll} U \circ \mathrm{id} & = & \{\mathrm{id} \circ \mathrm{id}, (1\ 2) \circ \mathrm{id}\} & = & \{\mathrm{id}, (1\ 2)\} \\ U \circ (1\ 2) & = & \{\mathrm{id} \circ (1\ 2), (1\ 2) \circ (1\ 2)\} & = & \{(1\ 2), \mathrm{id}\} \\ U \circ (1\ 3) & = & \{\mathrm{id} \circ (1\ 3), (1\ 2) \circ (1\ 3)\} & = & \{(1\ 3), (1\ 3\ 2)\} \\ U \circ (2\ 3) & = & \{\mathrm{id} \circ (2\ 3), (1\ 2) \circ (2\ 3)\} & = & \{(2\ 3), (1\ 2\ 3)\} \\ U \circ (1\ 2\ 3) & = & \{\mathrm{id} \circ (1\ 2\ 3), (1\ 2) \circ (1\ 2\ 3)\} & = & \{(1\ 2\ 3), (2\ 3)\} \\ U \circ (1\ 3\ 2) & = & \{\mathrm{id} \circ (1\ 3\ 2), (1\ 2) \circ (1\ 3\ 2)\} & = & \{(1\ 3\ 2), (1\ 3)\} \end{array}$$

Die Menge der Rechtsnebenklassen $U\backslash G$ ist also gegeben durch $\{U\ ,\ \{(1\ 3), (1\ 3\ 2)\}\ ,\ \{(2\ 3), (1\ 2\ 3)\}\}$.

Das Beispiel zeigt, dass Links- und Rechtsnebenklassen im Allgemeinen nicht übereinzustimmen brauchen. Beispielsweise ist $\{(1\ 3), (1\ 2\ 3)\}$ zwar eine Links- aber keine Rechtsnebenklasse von U. Ist U aber Untergruppe einer *abelschen* Gruppe, dann gilt $gU = Ug$ für alle $g \in G$. Ist nämlich $h \in gU$ vorgegeben, dann gilt $h = gu = ug$ für ein $u \in U$, und es folgt $h \in Ug$. Damit ist $gU \subseteq Ug$ nachgewiesen, und die umgekehrte Inklusion beweist man genauso.

Wir bemerken noch, dass jedes $g \in G$ sowohl in der Linksnebenklasse gU als auch in der Rechtsnebenklasse Ug enthalten ist. Dies folgt direkt aus den Gleichungen $g = g \cdot e_G = e_G \cdot g$ und der Tatsache, dass e_G in U liegt.

Bei unserem Beispiel fällt auf, dass jede Links- oder Rechtsnebenklasse genauso viele Elemente enthält wie die Untergruppe U selbst. Diese Beobachtung ist auch im allgemeinen Fall zutreffend.

Lemma 2.14 Sei G eine Gruppe, U eine Untergruppe von G und $g \in G$ ein beliebiges Element. Dann sind die Abbildungen

$$\tau_g^\ell : U \to gU\ ,\ h \mapsto gh \qquad \text{und} \qquad \tau_g^r : U \to Ug\ ,\ h \mapsto hg \qquad \text{jeweils bijektiv.}$$

Ist U endlich, dann gilt also $|U| = |gU| = |Ug|$ für alle $g \in G$.

Beweis: Wir beschränken und auf den Beweis der Surjektivität und der Injektivität der Abbildung τ_g^ℓ. Sei $h \in gU$ vorgegeben. Dann existiert nach Definition von gU ein $u \in U$ mit $h = gu$. Es gilt also $\tau_g^\ell(u) = gu = h$. Damit ist die Surjektivität bewiesen. Seien nun $u_1, u_2 \in U$ mit $\tau_g^\ell(u_1) = \tau_g^\ell(u_2)$. Dann folgt $u_1 = g^{-1}gu_1 = g^{-1}\tau_g^\ell(u_1) = g^{-1}\tau_g^\ell(u_2) = g^{-1}gu_2 = u_2$. Dies zeigt, dass τ^ℓ auch injektiv ist. Die letzte Aussage folgt unmittelbar aus der Tatsache, dass zwei Mengen, zwischen denen eine Bijektion existiert, gleichmächtig sind. □

Für das Hauptziel dieses Abschnitts, den Beweis des Satzes von Lagrange, ist die Beobachtung entscheidend, dass die Linksnebenklassen in G/U eine Zerlegung der Menge G bilden, ein Begriff, den wir bereits aus der Linearen Algebra kennen. Zur Erinnerung: Unter einer Zerlegung einer Menge X verstehen wir ein System $\mathcal{Z} \subseteq \mathcal{P}(X)$ von Teilmengen von X mit den Eigenschaften $\emptyset \notin \mathcal{Z}$, $\bigcup_{A \in \mathcal{Z}} A = X$ und $\forall A, B \in \mathcal{Z} : A \neq B \Rightarrow A \cap B = \emptyset$; zwei verschiedene Mengen in einer Zerlegung sind also disjunkt. Man vergewissere sich anhand des Beispiels vom Anfang des Kapitels mit $G = S_3$ und $U = \langle (1\ 2) \rangle$, dass sowohl G/U als auch $U\backslash G$ in der Tat eine Zerlegung von S_3 liefert.

Aus der Linearen Algebra wissen wir auch, dass der Begriff der Zerlegung mit dem Konzept der Äquivalenzrelation eng verbunden ist. Eine Äquivalenzrelation $\equiv$ auf einer Menge X ist eine reflexive, symmetrische und transitive Relation. Für jedes $x \in X$ wird $[x] = \{y \in X \mid x \equiv y\}$ die Äquivalenzklasse von x bezüglich $\equiv$ genannt. Zwischen den Äquivalenzrelationen auf einer Menge X und den Zerlegungen von X besteht nun der folgende Zusammenhang: Ist

$\equiv$ eine Äquivalenzrelation auf X, so bilden die Äquivalenzklassen bezüglich $\equiv$ eine Zerlegung von X. Ist umgekehrt $\mathcal{Z}$ eine Zerlegung von X, so erhält man durch

$$x \equiv_{\mathcal{Z}} y \quad \Leftrightarrow \quad \exists A \in \mathcal{Z} : x, y \in A$$

eine Äquivalenzrelation auf X. Für eine Menge X und eine Zerlegung $\mathcal{Z}$ von X gilt offenbar allgemein: Genau dann ist X endlich, wenn sowohl $|\mathcal{Z}|$ als auch $|A|$ für jedes $A \in \mathcal{Z}$ endlich ist, und in diesem Fall ist dann die Gleichung $|X| = \sum_{A \in \mathcal{Z}} |A|$ erfüllt. Diese einfache Beobachtung wird später beim Beweis des Satzes von Lagrange eine wichtige Rolle spielen.

Lemma 2.15 Sei G eine Gruppe und U eine Untergruppe von G. Dann folgt für alle $g, h \in G$ aus $h \in gU$ jeweils $gU = hU$.

Beweis: Setzen wir $h \in gU$ voraus. Dann gibt es ein $u \in U$ mit $h = gu$. Zum Nachweis der Inklusion „$\subseteq$“ sei $h_1 \in gU$ vorgegeben. Dann gibt es ein $u_1 \in U$ mit $h_1 = gu_1$, und es folgt $h_1 = h(u^{-1}u_1) \in hU$. Ist umgekehrt $h_1 \in hU$, dann gilt $h_1 = hu_2$ für ein $u_2 \in U$. Wir erhalten $h_1 = g(u_1u_2) \in gU$. □

Satz 2.16 Sei G eine Gruppe und $U \leq G$. Dann ist sowohl durch G/U als auch durch $U\backslash G$ eine Zerlegung von G gegeben. Die zugehörigen Äquivalenzrelationen auf G sind definiert durch $g \equiv_\ell h \Leftrightarrow h \in gU$ bzw. $g \equiv_r h \Leftrightarrow h \in Ug$.

Beweis: Wir beweisen die beiden Teilaussagen lediglich für die Menge G/U der Linksnebenklassen. Zunächst zeigen wir, dass es sich dabei um eine Zerlegung von G handelt, und überprüfen dafür die drei definierenden Bedingungen, die wir gerade wiederholt haben. Jede Teilmenge $A \in G/U$ hat die Form $A = gU$ für ein $g \in G$, und es gilt $g = g \cdot e_G \in gU$ wegen $e_G \in U$. Dies zeigt, dass $A \neq \emptyset$ gilt, die leere Menge in G/U also nicht vorkommt. Weil jedes $g \in G$ in gU liegt, also einem Element von G/U, ist auch die Eigenschaft $G = \bigcup_{A \in G/U} A$ erfüllt. Seien nun $A, B \in G/U$ mit $A \cap B \neq \emptyset$ vorgegeben, und sei $h \in A \cap B$. Nach Lemma 2.15 folgt daraus $A = hU = B$. Setzen wir für $A, B \in G/U$ umgekehrt $A \neq B$ voraus, dann muss also $A \cap B = \emptyset$ gelten.

Nach Definition ist die zur Zerlegung G/U gehörende Äquivalenzrelation $\equiv_\ell$ definiert durch die Bedingung, dass für je zwei Elemente $g, h \in G$ jeweils genau dann $g \equiv_\ell h$ erfüllt ist, wenn ein $A \in G/U$ mit $g, h \in A$ existiert. Aber wegen Lemma 2.15 folgt aus $g \in A$ bereits $A = gU$, so dass $g \equiv_\ell h$ also $h \in gU$ impliziert. Setzen wir umgekehrt $h \in gU$ voraus, dann ist durch $A = gU$ ein Element von G/U mit $g, h \in A$ gegeben, und es folgt $g \equiv_\ell h$. □

Im weiteren Verlauf bezeichnen wir mit $X/\equiv$ die Menge der Äquivalenzklassen einer Äquivalenzrelation $\equiv$. Es handelt sich also nach Definition um die Menge $\{[x] \mid x \in X\}$.

Definition 2.17 Sei X eine Menge und $\equiv$ eine Äquivalenzrelation auf X. Eine Teilmenge $R \subseteq X$ wird ***Repräsentantensystem*** der Äquivalenzklassen von $\equiv$ genannt, wenn durch $R \to X/\equiv$, $x \mapsto [x]$ eine bijektive Abbildung gegeben ist. Mit anderen Worten, in jeder Äquivalenzklasse ist genau ein Element aus R enthalten.

Im Beispiel $G = S_3$, $U = \langle(1\ 2)\rangle$ von oben ist $\{\mathrm{id}, (1\ 3), (2\ 3)\}$ ein Repräsentantensystem von G/U. Gleiches gilt für die Mengen $\{\mathrm{id}, (1\ 2\ 3), (2\ 3)\}$ und $\{(1\ 2), (1\ 3), (1\ 3\ 2)\}$. Die Wahl eines Repräsentantensystems ist also keineswegs eindeutig.

Als nächstes zeigen wir, wie sich aus einem Repräsentantensystem der Linksnebenklassen ein Repräsentantensystem der Rechtsnebenklassen gewinnen lässt.

Proposition 2.18 Sei G eine Gruppe und U eine Untergruppe. Ist R ein Repräsentantesystem der Linksnebenklassen, dann ist $R' = \{g^{-1} \mid g \in R\}$ ein Repräsentantensystem der Rechtsnebenklassen, und durch $g \mapsto g^{-1}$ ist eine Bijektion zwischen R und R' definiert.

Beweis: Zu zeigen ist, dass für jedes $h \in G$ die Rechtsnebenklasse Uh genau ein Element aus R' enthält. Sei also $h \in G$ vorgegeben. Zunächst beweisen wir, dass in Uh ein Element aus R' liegt. Nach Voraussetzung enthält die Linksnebenklasse $h^{-1}U$ ein Element $g \in R$. Es gibt also ein $u \in U$ mit $g = h^{-1}u$. Daraus folgt $g^{-1} = u^{-1}h$. Diese Gleichung wiederum zeigt, dass die Rechtsnebenklasse Uh das Element $g^{-1} \in R'$ enthält.

Nehmen wir nun an, die Rechtsnebenklasse Uh enthält die beiden Elemente $h_1, h_2 \in R'$. Dann gibt es $u, v \in U$ mit $h_1 = uh$ und $h_2 = vh$. Nach Definition von R' gibt es außerdem $g_1, g_2 \in R$ mit $g_1^{-1} = h_1$, $g_2^{-1} = h_2$. Es folgt $g_1 = h_1^{-1} = h^{-1}u^{-1}$ und $g_2 = h_2^{-1} = h^{-1}v^{-1}$. Die Gleichungen zeigen, dass die Elemente $g_1, g_2 \in R$ beide in der Linksnebenklasse $h^{-1}U$ liegen. Weil R ein Repräsentantensystem der Linksnebenklassen ist, muss $g_1 = g_2$ gelten. Daraus wiederum folgt $h_1 = h_2$.

Dass die Abbildung $R \to R'$, $g \mapsto g^{-1}$ surjektiv ist, folgt direkt aus der Definition von R'. Andererseits folgt aus $g^{-1} = h^{-1}$ sofort $g = h$, somit ist die Abbildung auch injektiv. □

Aus der Proposition folgt unmittelbar, dass zwischen G/U und $U\backslash G$ eine Bijektion existiert, die aus den Bijektionen $G/U \to R \to R' \to U\backslash G$ zusammengesetzt ist. Dies bedeutet, dass die Mengen G/U und $U\backslash G$ gleichmächtig sind.

Definition 2.19 Sei G eine Gruppe und U eine Untergruppe. Die Mächtigkeit $|G/U|$ der Menge G/U wird der ***Index*** von U in G genannt und mit $(G : U)$ bezeichnet.

Aus unserer Vorüberlegung folgt, dass man zur Definition des Index genauso gut die Mächtigkeit der Menge $U\backslash G$ der Rechtsnebenklassen verwenden könnte. Im Beispiel oben haben wir gesehen, dass es im Fall $G = S_3$ und $U = \langle(1\ 2)\rangle$ jeweils drei Links- und drei Rechtsnebenklassen gibt. Hier gilt also $(G : U) = 3$.

Satz 2.20 *(Satz von Lagrange)*

Sei G eine endliche Gruppe und U eine Untergruppe. Dann gilt $|G| = (G : U)|U|$. Insbesondere ist die Ordnung $|U|$ der Untergruppe immer ein Teiler der Gruppenordnung $|G|$.

Beweis: Sei $R \subseteq G$ ein Repräsentantensystem der Linksnebenklassen. Weil nach Definition der Repräsentantensysteme eine Bijektion $R \to G/U$ existiert, gilt $|R| = |G/U| = (G : U)$. Nach Proposition 2.16 ist G/U eine Zerlegung von G,

und nach Lemma 2.14 gilt $|gU| = |U|$ für alle Linksnebenklassen. Wir erhalten

$$|G| \quad = \quad \sum_{A \in G/U} |A| \quad = \quad \sum_{g \in R} |gU| \quad = \quad \sum_{g \in R} |U| \quad = \quad |R| \cdot |U| \quad = \quad (G : U)|U|. \qquad \square$$

Im Beispiel oben ist die Gleichung aus dem Satz von Lagrange offenbar erfüllt, denn im Fall $G = S_3$, $U = \langle (1\ 2) \rangle$ gilt $|G| = 6$ und $(G : U)|U| = 3 \cdot 2 = 6$. Die Untergruppe $V = \langle (1\ 2\ 3) \rangle$ in S_3 ist von Ordnung 3, da $(1\ 2\ 3)$ ein Element der Ordnung 3 ist. Der Satz von Langrange liefert hier für den Index den Wert

$$(G : V) \quad = \quad \frac{|G|}{|V|} \quad = \quad \frac{6}{3} \quad = \quad 2.$$

Die Zerlegung einer Gruppe in ihre Linksnebenklassen liefert auch eine Aussage für beliebige, nicht notwendigerweise endliche, Gruppen.

Folgerung 2.21 Sei G eine Gruppe und U eine Untergruppe. Genau dann ist G endlich, wenn sowohl U als auch G/U endliche Mengen sind (und in diesem Fall gilt dann natürlich der Satz von Lagrange).

Beweis: „⇒“ Ist G endlich, dann ist U als Teilmenge von G offenbar ebenfalls endlich. Sei $R \subseteq G$ ein Repräsentantensystem der Menge G/U der Linksnebenklassen. Dann gibt es eine Bijektion von R nach G/U. Weil R als Teilmenge von G endlich ist, handelt es sich auch bei G/U um eine endliche Menge.

„⇐“ Setzen wir nun voraus, dass U und G/U endlich sind. Weil für jedes $g \in G$ zwischen U und gU jeweils eine Bijektion existiert, ist damit auch jede Linksnebenklasse endlich. Weil es nach Voraussetzung nur endlich viele Linksnebenklassen gibt, ist G als Vereinigung der endlich vielen Linksnebenklassen selbst eine endliche Menge. $\square$

Wir haben beim Beweis der bisherigen Sätze mehrmals verwendet, dass für die Linksnebenklassen einer Untergruppe U in einer Gruppe G stets ein Repräsentantensystem existiert. Dass dies tatsächlich der Fall ist, wird durch das sogenannte ***Auswahlaxiom*** der Mengenlehre gewährleistet. Dieses stellt sicher, dass aus jeder Linksnebenklasse ein Repräsentant ausgewählt und die ausgewählten Elemente zu einer neuen Menge R zusammengeführt werden können. Da in den Vorlesungen die Axiome der Mengenlehre normalerweise nicht behandelt werden, fällt die Verwendung des Auswahlaxioms nicht auf, zumal seine Gültigkeit selbstverständlich und trivial erscheint.

Wir notieren noch zwei Folgerungen aus dem Satz von Lagrange.

Satz 2.22

(i) Jede Gruppe von Primzahlordnung ist zyklisch.

(ii) Sei G eine Gruppe, und seien $U, V \subseteq G$ endliche Untergruppen teilerfremder Ordnung. Dann gilt $U \cap V = \{e_G\}$.

Beweis: zu (i) Wegen $|G| > 1$ gibt es mindestens ein Element $g \in G \setminus \{e_G\}$. Nach dem Satz von Lagrange ist $\mathrm{ord}(g) = |\langle g \rangle|$ ein Teiler der Gruppenordnung p. Weil p eine Primzahl ist, gibt es nur die beiden Möglichkeiten $\mathrm{ord}(g) = 1$ oder $\mathrm{ord}(g) = p$. Wegen $g \neq e_G$ scheidet die erste Möglichkeit aus. Es gilt damit $|\langle g \rangle| = p = |G|$, also $G = \langle g \rangle$.

zu (ii) Sei $U_1 = U \cap V$. Dann ist U_1 eine Untergruppe von U, und nach dem Satz von Lagrange ist $|U_1|$ ein Teiler von $|U|$. Ebenso ist U_1 eine Untergruppe von V, also teilt $|U_1|$ auch $|V|$. Die Zahl $|U_1|$ ist also ein gemeinsamer Teiler von $|U|$ und $|V|$. Weil $|U|$ un d $|V|$ teilerfremd sind, folgt $|U_1| = 1$ und $U_1 = \{e_G\}$. □

§ 3. *Elementordnungen und die Struktur zyklischer Gruppen*

Zusammenfassung. Die *Ordnung* $\operatorname{ord}(g)$ eines Gruppenelements ist die kleinste natürliche Zahl m mit $g^m = e_G$; existiert eine solche Zahl nicht, dann setzt man $\operatorname{ord}(g) = \infty$. Die Ordnung kann auf zwei weitere Arten charakterisiert werden. Kennt man $\operatorname{ord}(g)$, so kann $\operatorname{ord}(g^a)$ für jedes $a \in \mathbb{Z}$ berechnet werden. Im weiteren Verlauf des Kapitels untersuchen wir die Untergruppenstruktur zyklischer Gruppen. Eine Besonderheit dieser Gruppen besteht darin, dass die Anzahl der Untergruppen mit der Anzahl der Teiler ihrer Ordnung übereinstimmt.

Wichtige Grundbegriffe	***Zentrale Sätze***
– Ordnung einer Gruppe	– äquivalente Charakterisierung der Elementordnung
– Ordnung eines Gruppenelements	– Rechenregeln für die Elementordnung
– Eulersche φ-Funktion	– Beschreibung der Untergruppen zyklischer Gruppen
	– Charakterisierung zyklischer Gruppen
	– Kleiner Satz von Fermat

Wir beginnen mit der Definition der Gruppen- und Elementordnung.

Definition 3.1 Sei G eine Gruppe. Die Anzahl $|G|$ der Elemente von G wird die ***Ordnung*** von G genannt. Ist $g \in G$ ein beliebiges Element, dann bezeichnen wir $\operatorname{ord}(g) = |\langle g \rangle|$ als die Ordnung von g.

Da $\langle g \rangle$ für jedes $g \in G$ jeweils eine Untergruppe von G ist, folgt aus dem Satz von Lagrange unmittelbar: Ist $n = |G|$ endlich, dann folgt

$$\operatorname{ord}(g) \mid n \quad \text{für alle } g \in G.$$

In § 2 wurde gezeigt, dass die Elemente einer zyklischen Gruppe $\langle g \rangle$ genau die ganzahligen Potenzen von a sind, also die Elemente der Form g^a mit $a \in \mathbb{Z}$. Es kann allerdings vorkommen, dass $g^a = g^b$ gilt, obwohl $a \neq b$ ist.

Lemma 3.2 Sei G eine Gruppe, $g \in G$ und $m \in \mathbb{N}$ mit $g^m = e_G$. Dann ist die von g erzeugte Untergruppe gegeben durch $\langle g \rangle = \{g^r \mid 0 \leq r < m\}$.

Beweis: Die Inklusion „$\supseteq$“ ergibt sich direkt aus Folgerung 2.10. Zum Nachweis von „$\subseteq$“ sei $h \in \langle g \rangle$ vorgegeben. Wiederum auf Grund der Proposition gibt es ein $n \in \mathbb{Z}$ mit $h = g^n$. Dividieren wir n durch m mit Rest, so erhalten wir ein $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 \leq r < m$. Es gilt $h = g^n = g^{qm+r} = (g^m)^q \cdot g^r = e_G^q \cdot g^r = g^r$. Also ist h in der Menge auf der rechten Seite enthalten. □

Satz 3.3 Sei G eine Gruppe und $g \in G$ ein beliebiges Element. Dann sind für jedes $n \in \mathbb{N}$ die folgenden Aussagen äquivalent.

(i) $n = \text{ord}(g)$

(ii) Es gibt ein $m \in \mathbb{N}$ mit $g^m = e_G$, und darüber hinaus ist n die ***minimale*** natürliche Zahl mit dieser Eigenschaft.

(iii) Für alle $m \in \mathbb{Z}$ gilt $g^m = e_G$ genau dann, wenn m ein Vielfaches von n ist.

Beweis: „(i) ⇒ (ii)“ Da $\text{ord}(g)$ und damit die Menge $\langle g \rangle$ nach Voraussetzung endlich ist, können die Elemente $g, g^2, g^3, \ldots$ nicht alle voneinander verschieden sein. Es gibt also $i, j \in \mathbb{N}$ mit $i < j$ und $g^i = g^j$. Setzen wir $m = j - i$, dann gilt $g^m = g^{j-i} = g^j \cdot (g^i)^{-1} = e_G$, also existiert ein $m \in \mathbb{N}$ mit $g^m = e_G$.

Weil die zyklische Gruppe $\langle g \rangle$ insgesamt nur n verschiedene Elemente besitzt, können bereits die Elemente g, g^2, ..., g^{n+1} nicht alle verschieden sein. Wir können also für das j von oben $j \leq n+1$ und damit $m \leq n$ voraussetzen. Wäre $m < n$, dann würde $\langle g \rangle$ auf Grund des Lemmas aus der höchstens m-elementigen Menge $\{e_G, g, \ldots, g^{m-1}\}$ bestehen, im Widerspruch zu $|\langle g \rangle| = n$. Es gilt also $m = n$, und n ist die minimale natürliche Zahl mit der Eigenschaft $g^n = e_G$.

„(ii) ⇒ (iii)“ Sei $m \in \mathbb{Z}$ mit $g^m = e_G$ vorgegeben. Dann gibt es $q, r \in \mathbb{Z}$ mit $m = qn + r$ und $0 \leq r < n$. Es gilt $g^r = g^{m-qn} = g^m \cdot (g^n)^{-q} = e_G \circ e_G = e_G$. Da n nach Voraussetzung die *minimale* natürliche Zahl mit $g^n = e_G$ ist, muss $r = 0$ gelten, und m ist somit ein Vielfaches von n. Setzen wir umgekehrt voraus, dass m ein Vielfaches von n ist, $m = kn$ für ein $k \in \mathbb{Z}$, dann gilt $g^m = g^{kn} = (g^n)^k = e_G^k = e_G$.

„(iii) ⇒ (i)“ Nach Voraussetzung gilt $g^n = e_G$, und auf Grund des Lemmas ist $\langle g \rangle = \{e_G, g, \ldots, g^{n-1}\}$. Würden zwei Elemente in dieser Menge übereinstimmen, dann gäbe es $i, j \in \mathbb{Z}$ mit $0 \leq i < j \leq n-1$ und $g^i = g^j$, es wäre also $g^{j-i} = e_G$. Dies aber wäre ein Widerspruch zur Voraussetzung, da n wegen $0 < j - i < n$ kein Teiler von $j - i$ ist. Dies zeigt, dass $\langle n \rangle$ tatsächlich aus genau n verschiedenen Elementen besteht, also $\text{ord}(g) = |\langle g \rangle| = n$ gilt. □

Wir geben einige Beispiele für Elementordnungen an.

(i) Ist $n \in \mathbb{N}$ und $G = (\mathbb{Z}/n\mathbb{Z}, +)$, dann ist $\bar{1} = 1 + n\mathbb{Z}$ ein Element der Ordnung n, denn es gilt $k \cdot \bar{1} = \bar{k} \neq \bar{0}$ für $1 \leq k < n$ und $n \cdot \bar{1} = n + n\mathbb{Z} = 0 + n\mathbb{Z} = \bar{0}$.

(ii) In § 1 (auf Seite 9) haben wir für jedes $\alpha \in \mathbb{R}$ das Element D_α der orthogonalen Gruppe $\mathcal{O}(2)$ definiert. Es handelte sich dabei um die Matrix, die eine Drehung um den Ursprung $0_{\mathbb{R}^2}$ mit dem Winkel α im Bogenmaß beschreibt. Wie man leicht überprüft, ist $D_{2\pi/n}$ für jedes $n \in \mathbb{N}$ ein Element der Ordnung n in $\mathcal{O}(2)$.

(iii) In den Diedergruppen D_n (mit $n \geq 3$) sind die n Spiegelungen alles Elemente der Ordnung 2.

Mit Hilfe von Satz 3.3 können wir die Elemente einer endlichen, zyklischen Gruppe nun genau angeben.

Folgerung 3.4 Sei G eine Gruppe. Besitzt $g \in G$ die endliche Ordnung n, dann sind durch $e_G, g, g^2, \ldots, g^{n-1}$ die n verschiedenen Elemente der zyklischen Gruppe $\langle g \rangle$ gegeben.

Beweis: Nach Satz 3.3 gilt $g^n = e_G$, und auf Grund von Lemma 3.2 gilt $\langle g\rangle = \{e_G, g, g^2, ..., g^{n-1}\}$. Wegen $|\langle g\rangle| = n$ sind alle Elemente in dieser Aufzählung verschieden. □

Für Elemente unendlicher Ordnung lässt sich eine zu Satz 3.3 weitgehend analoge Äquivalenzaussage formulieren.

Satz 3.5 Ist G eine Gruppe und $g \in G$, dann sind die folgenden Aussagen äquivalent.

(i) $\text{ord}(g) = \infty$

(ii) Es gibt kein $n \in \mathbb{N}$ mit $g^n = e_G$.

(iii) Die Abbildung $\phi : \mathbb{Z} \to G$, $k \mapsto g^k$ ist injektiv.

Beweis: „(i) ⇒ (ii)“ Angenommen, es gilt $g^n = e_G$ für ein $n \in \mathbb{N}$. Dann würde aus Lemma 3.2 die Gleichung $\langle g\rangle = \{e_G, g, ..., g^{n-1}\}$ folgen, im Widerspruch dazu, dass $\text{ord}(g) = |\langle g\rangle|$ unendlich ist.

„(ii) ⇒ (iii)“ Angenommen, ϕ ist nicht injektiv. Dann gäbe es Elemente $k, \ell \in \mathbb{Z}$ mit $k < \ell$ und $\phi(k) = \phi(\ell)$. Daraus würde $g^k = g^\ell \Leftrightarrow g^\ell (g^k)^{-1} = e_G \Leftrightarrow g^{\ell-k} = e_G$ folgen, was aber wegen $\ell - k \in \mathbb{N}$ im Widerspruch zur Voraussetzung steht.

„(iii) ⇒ (i)“ Es gilt $\phi(\mathbb{Z}) = \{g^k \mid k \in \mathbb{Z}\} = \langle g\rangle$. Auf Grund der Injektivität von ϕ erhalten wir $\text{ord}(g) = |\langle g\rangle| = |\phi(\mathbb{Z})| = |\mathbb{Z}| = \infty$. □

Beispielsweise ist 1 ein Element unendlicher Ordnung in $(\mathbb{Z}, +)$, denn es gilt $n \cdot 1 \neq 0$ für alle $n \in \mathbb{N}$.

In den symmetrischen Gruppen lassen sich die Ordnungen von Elementen leicht ermitteln. Zur Vorbereitung erinnern wir an die Definition des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen einer endlichen Menge ganzer Zahlen. Seien $a_1, ..., a_r \in \mathbb{Z}$ vorgegeben. Eine Zahl $d \in \mathbb{N}$ heißt ***gemeinsamer Teiler*** dieser Zahlen, wenn $d \mid a_k$ für $1 \leq k \leq r$ gilt. Man nennt d den ***größten*** gemeinsamen Teiler dieser Zahlen und schreibt $d = \text{ggT}(a_1, ..., a_r)$, wenn $d' | d$ für jeden gemeinsamen Teiler d' von $a_1, ..., a_r$ gilt. Zwei Zahlen a und b werden als ***teilerfremd*** bezeichnet, wenn $\text{ggT}(a, b) = 1$ ist.

Eine natürliche Zahl $d \in \mathbb{N}$ heißt ***gemeinsames Vielfaches*** von $a_1, ..., a_r$, wenn $a_k \mid d$ für $1 \leq k \leq r$ gilt, und ***kleinstes gemeinsames Vielfaches***, wenn $d \mid d'$ für jedes gemeinsame Vielfache d' dieser Zahlen erfüllt ist. Wir bezeichnen das kleinste gemeinsame Vielfache mit $\text{kgV}(a_1, ..., a_r)$. Sowohl der größte gemeinsame Teiler als auch das kleinste gemeinsame Vielfache existieren, sobald die Zahlen $a_1, ..., a_r$ nicht alle gleich Null sind, und sie sind in diesem Fall auch eindeutig bestimmt.

Satz 3.6 Sei $n \in \mathbb{N}$ und $\sigma \in S_n$.

(i) Ist σ ein k-Zykel $(2 \leq k \leq n)$, dann gilt $\text{ord}(\sigma) = k$.

(ii) Ist σ ein Element vom Zerlegungtyp $(k_1, ..., k_r)$, dann gilt $\text{ord}(\sigma) = \text{kgV}(k_1, ..., k_r)$.

Beweis: zu (i) Nach Voraussetzung gibt es eine k-elementige Teilmenge $\{a_1, ..., a_k\} \subseteq M_n$ mit $\sigma = (a_1\ a_2\ ...\ a_k)$. Durch vollständige Induktion über $m \in \mathbb{N}_0$ kontrollieren wir zunächst, dass für alle $m \in \mathbb{N}_0$ und $\ell, j \in \{1, ..., k\}$ mit $\sigma^m(a_\ell) = a_j$ jeweils die Kongruenz $\ell + m \equiv j \bmod k$ erfüllt ist.

Für $m = 0$ gilt dies wegen $\sigma^0(a_\ell) = \mathrm{id}(a_\ell) = a_\ell$ und $\ell + 0 \equiv \ell \bmod k$. Sei nun $m \in \mathbb{N}_0$, und sei $j \in \{1, ..., k\}$ die eindeutig bestimmte Zahl mit $\sigma^m(a_\ell) = a_j$; dann gilt $\ell + m \equiv j \bmod k$ auf Grund der Induktionsvoraussetzung. Ist nun $j < k$, dann gilt $\sigma^{m+1}(a_\ell) = \sigma(\sigma^m(a_\ell)) = \sigma(a_j) = a_{j+1}$ und $\ell + (m+1) \equiv j + 1 \bmod k$. Im Fall $j = k$ gilt $\sigma^{m+1}(a_\ell) = \sigma(a_k) = a_1$, und wegen $\ell + (m+1) \equiv k + 1 \equiv 1 \bmod k$ ist die Kongruenz auch in diesem Fall erfüllt.

Es ist nun leicht zu sehen, dass k die kleinste natürliche Zahl mit $\sigma^k = \mathrm{id}$ ist. Ist nämlich $m \in \mathbb{N}$ mit $m < k$ und $\sigma^m(a_1) = a_j$, dann gilt $j \equiv 1 + m \not\equiv 1 \bmod k$, und somit erst recht $j \neq 1$ und $a_j \neq a_1$, also $\sigma^m \neq \mathrm{id}$. Für $\ell, j \in \{1, ..., k\}$ mit $\sigma^k(a_\ell) = a_j$ gilt dagegen $\ell + k \equiv j \bmod k$, also $\ell \equiv j \bmod k$ und damit $\ell = j$. Die Zahlen $a_1, ..., a_k$ werden also durch σ^k auf sich abgebildet, und für die Elemente von $i \in M_n \setminus \{a_1, ..., a_k\}$ gilt dies wegen $\sigma(i) = i$ natürlich ebenso.

zu (ii) Nach Definition des Zerlegungstyps existiert für $1 \leq j \leq r$ jeweils ein k_j-Zykel σ_j, so dass $\sigma = \sigma_1 \circ ... \circ \sigma_r$ gilt und die Zykel σ_j paarweise disjunkt sind. Wie wir in § 2 festgestellt haben, sind σ_i und σ_j für $1 \leq i, j \leq r$ als Elemente mit disjunktem Träger jeweils vertauschbar, und wegen Lemma 2.2 folgt daraus $\sigma^n = \sigma_1^n \circ ... \circ \sigma_r^n$ für alle $n \in \mathbb{Z}$. Auf Grund der Disjunktheit der Träger ist auch leicht zu sehen, dass genau dann $\sigma^n = \mathrm{id}$ gilt, wenn $\sigma_j^n = \mathrm{id}$ für $1 \leq j \leq r$ erfüllt ist.

Sei nun $m = \mathrm{ord}(\sigma)$; wir zeigen, dass m die definierenden Eigenschaften des kgV von $k_1, ..., k_r$ besitzt. Aus der Gleichung $\sigma_1^m \circ ... \circ \sigma_r^m = \sigma^m = \mathrm{id}$ folgt $\sigma_j^m = \mathrm{id}$ für $1 \leq j \leq r$. Nach Satz 3.3 zeigt dies, dass m ein gemeinsames Vielfaches von $k_j = \mathrm{ord}(\sigma_j)$ mit $1 \leq j \leq r$ ist. Sei nun n ein beliebiges gemeinsames Vielfaches von $k_1, ..., k_r$. Dann folgt $\sigma_j^n = \mathrm{id}$ für $1 \leq j \leq r$ mit Satz 3.3. Wir erhalten $\sigma^n = \sigma_1^n \circ ... \circ \sigma_r^n = \mathrm{id}$ und somit $m \mid n$, erneut durch eine Anwendung von Satz 3.3. Es handelt sich bei m also tatsächlich um die Zahl $\mathrm{kgV}(k_1, ..., k_r)$. □

Der Satz zeigt uns zum Beispiel, dass in der Gruppe S_5 nur Elemente der Ordnungen $1, 2, 3, 4, 5$ und 6 existieren. Denn neben der Identität, den 2-, 3-, 4- und 5-Zyklen gibt es in S_5 noch Elemente der Zerlegungtypen $(2, 2)$ und $(3, 2)$, und es gilt $\mathrm{kgV}(2, 2) = 2$ und $\mathrm{kgV}(3, 2) = 6$. Insbesondere ist $\sigma = (1\ 2\ 3)(4\ 5)$ ein Element der Ordnung 6 in S_5. Im weiteren Verlauf beschäftigen wir uns nun mit der Untergruppenstruktur zyklischer Gruppen.

Satz 3.7 Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer gilt: Sei G eine zyklische Gruppe, g ein Element mit $G = \langle g \rangle$ und U eine Untergruppe $\neq \{e_G\}$. Dann gibt es ein $m \in \mathbb{N}$ mit $U = \langle g^m \rangle$. Ist $\mathrm{ord}(g) = n$ endlich, dann kann die Zahl m so gewählt werden, dass sie ein Teiler von n ist.

Beweis: Weil U nichttrivial ist, gibt es ein $r \in \mathbb{Z}$, $r \neq 0$ mit $g^r \in U$. Weil mit g^r auch $(g^r)^{-1} = g^{-r}$ in U enthalten ist, gibt es auch natürliche Zahlen r mit $g^r \in U$. Sei nun $m \in \mathbb{N}$ die *minimale* natürliche Zahl mit der Eigenschaft $g^m \in U$. Wir zeigen, dass dann $U = \langle g^m \rangle$ gilt.

Die Inklusion „$\supseteq$“ gilt nach Definition der erzeugten Untergruppe. Nehmen wir nun an, dass „$\subseteq$“ nicht erfüllt ist. Dann gibt es ein Element $h \in U \setminus \langle g^m \rangle$ und ein $b \in \mathbb{Z}$ mit $h = g^b$. Durch Division mit Rest erhalten wir $q, r \in \mathbb{Z}$ mit $b = qm + r$ und $0 \leq r < m$. Dabei ist der Fall $r = 0$ ausgeschlossen, denn ansonsten wäre b ein Vielfaches von m und h damit doch in $\langle g^m \rangle$ enthalten. So aber gilt $h \cdot (g^m)^{-q} = g^r \in U$, im Widerspruch zur Minimalität von m. Damit ist die Gleichung $U = \langle g^m \rangle$ bewiesen.

Sei nun $n = \text{ord}(g)$ endlich, und nehmen wir an, dass m kein Teiler von n ist. Dann gibt es $q, r \in \mathbb{Z}$ mit $n = qm + r$ und $0 < r < m$. Es gilt dann $g^r = g^{n-mq} = g^n \cdot (g^m)^{-q} = (g^m)^{-q} \in U$, im Widerspruch dazu, dass m mit der Eigenschaft $g^m \in U$ minimal gewählt wurde. □

Aus der Klassifikation der Untergruppen einer zyklischen Gruppe können wir das folgende zahlentheoretische Resultat herleiten.

Satz 3.8 *(Lemma von Bézout)*

Seien $m, n \in \mathbb{Z}$, $(m, n) \neq (0, 0)$. Dann gibt es $a, b \in \mathbb{Z}$ mit $am + bn = \text{ggT}(m, n)$.

Beweis: Sei $G = (\mathbb{Z}, +)$ und $U = \langle m, n \rangle$, die von m und n erzeugte Untergruppe. Nach Satz 2.9 (ii) gilt $U = \mathbb{Z}m + \mathbb{Z}n = \{am + bn \mid a, b \in \mathbb{Z}\}$. Weil $(\mathbb{Z}, +)$ zyklisch ist, gibt es nach Satz 3.7 ein $d \in \mathbb{N}$ mit $U = \langle d \rangle$. Wir zeigen, dass $d = \text{ggT}(m, n)$ erfüllt ist.

Wegen $m, n \in \langle d \rangle$ gibt es $k, \ell \in \mathbb{Z}$ mit $m = kd$ und $n = \ell d$. Dies zeigt, dass d jedenfalls ein gemeinsamer Teiler von m und n ist. Sei nun d' ein weiterer gemeinsamer Teiler. Dann gibt es $k', \ell' \in \mathbb{Z}$ mit $m = k'd'$ und $n = \ell' d'$. Die Elemente m, n liegen also in der Untergruppe $\langle d' \rangle$, und nach Definition der erzeugten Untergruppe folgt $\langle d \rangle = U = \langle m, n \rangle \subseteq \langle d' \rangle$. Insbesondere ist d in $\langle d' \rangle$ enthalten, es gibt also ein $r \in \mathbb{Z}$ mit $d = rd'$. Folglich ist d' ein Teiler von d. Damit ist der Beweis der Gleichung $d = \text{ggT}(m, n)$ abgeschlossen. Wegen $d \in U$ gibt es nun $a, b \in \mathbb{Z}$ mit $am + bn = d = \text{ggT}(m, n)$. □

Mit Hilfe des Lemma von Bézout lassen sich wichtige Rechenregeln für Elementordnungen herleiten.

Satz 3.9 Sei G eine Gruppe und $g \in G$ ein Element der endlichen Ordnung n.

(i) Für beliebiges $m \in \mathbb{Z}$ gilt $\text{ord}(g^m) = n$ genau dann, wenn $\text{ggT}(m, n) = 1$ ist.

(ii) Ist $d \in \mathbb{N}$ ein Teiler von n, dann gilt $\text{ord}(g^d) = \frac{n}{d}$.

(iii) Für beliebiges $m \in \mathbb{Z}$ gilt $\text{ord}(g^m) = \frac{n}{d}$ mit $d = \text{ggT}(m, n)$.

Beweis: zu (i) „⇒“ Wegen $g^m \in \langle g \rangle$ ist $\langle g^m \rangle$ eine Untergruppe von $\langle g \rangle$. Ist $\text{ord}(g^m) = n = \text{ord}(g)$, dann muss $\langle g^m \rangle = \langle g \rangle$ gelten. Es existiert also ein $k \in \mathbb{Z}$ mit $g = (g^m)^k = g^{km}$. Wir erhalten $g^{1-km} = e_G$ und damit $n | (1 - km)$, weil n die Ordnung von g ist. Sei nun $d \in \mathbb{N}$ ein Teiler von n und m. Aus $d | n$ folgt dann insbesondere $d | (1 - km)$. Damit ist d auch ein Teiler von $km + (1 - km) = 1$, also muss $d = 1$ sein. Wir haben damit gezeigt, dass 1 der einzige (natürliche) gemeinsame Teiler von m und n ist, und es folgt $\text{ggT}(m, n) = 1$ wie gewünscht.

„⇐“ Wegen $g^m \in \langle g \rangle$ ist $\langle g^m \rangle$ eine Untergruppe von $\langle g \rangle$. Auf Grund des Lemmas von Bézout gibt es $a, b \in \mathbb{Z}$ mit $am + bn = \text{ggT}(m, n) = 1$. Es folgt

$$g \quad = \quad g^1 \quad = \quad g^{am+bn} \quad = \quad (g^m)^a \cdot (g^n)^b \quad = \quad (g^m)^a \cdot e_G^b \quad = \quad g^{am} \quad \in \quad \langle g^m \rangle.$$

Also ist auch umgekehrt $\langle g \rangle$ eine Untergruppe von $\langle g^m \rangle$. Insgesamt erhalten wir $\langle g \rangle = \langle g^m \rangle$ und $\text{ord}(g^m) = |\langle g^m \rangle| = |\langle g \rangle| = \text{ord}(g) = n$.

zu (ii) Wegen $n = \mathrm{ord}(g)$ gilt für jedes $k \in \mathbb{Z}$ die Äquivalenz $(g^d)^k = e_G \Leftrightarrow g^{dk} = e_G \Leftrightarrow n|(dk) \Leftrightarrow \frac{n}{d} \mid k$. Auf Grund von Satz 3.3 (iii) folgt daraus $\mathrm{ord}(g^d) = \frac{n}{d}$

zu (iii) Seien m' und n' so gewählt, dass $m = m'd$ und $n = n'd$ gilt. Zu zeigen ist, dass $\mathrm{ord}(g^m) = n'$ gilt. Da d ein Teiler von n ist, können wir zunächst den bereits bewiesenen Teil (ii) anwenden und erhalten $\mathrm{ord}(g^d) = n'$. Ferner sind m' und n' teilerfremd. Denn wäre p ein gemeinsamer Primfaktor dieser beiden Zahlen, dann könnten wir $m = m'd = m''pd$ und $n = n'd = n''pd$ mit geeigneten $m'', n'' \in \mathbb{N}$ schreiben. Folglich wäre pd ein größerer gemeinsamer Teiler von m und n als d, im Widerspruch zur Definition von d. So aber können wir (i) auf das Gruppenelement g^d und die Zahl m' anwenden und erhalten $\mathrm{ord}(g^d) = \mathrm{ord}((g^d)^{m'}) = \mathrm{ord}(g^{m'd}) = \mathrm{ord}(g^m)$, insgesamt also das gewünschte Ergebnis. □

Ist beispielsweise G eine Gruppe und $g \in G$ ein Element der Ordnung 24, dann gilt $\mathrm{ord}(g^7) = \mathrm{ord}(g) = 24$, $\mathrm{ord}(g^6) = 4$ und $\mathrm{ord}(g^{10}) = 12$.

Die in der Zahlentheorie eine wichtige Rolle spielende ***Eulersche φ-Funktion*** ist für jedes $n \in \mathbb{N}$ definiert durch

$$\varphi(n) \quad = \quad |\{k \in \mathbb{Z} \mid 0 \le k < n \ , \ \mathrm{ggT}(k,n) = 1\}| \, .$$

In der Ringtheorie (Kapitel § 13) werden wir zeigen, dass für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ stets $\varphi(mn) = \varphi(m)\varphi(n)$ gilt, außerdem $\varphi(p^r) = p^{r-1}(p-1)$ für jede Primzahl p und jedes $r \in \mathbb{N}$. Damit lässt sich $\varphi(n)$ für jede natürliche Zahl n leicht berechnen.

Ist $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung n, dann sind g^k mit $0 \le k < n$ nach Folgerung 3.4 (i) die n verschiedenen Elemente von G. Aus Satz 3.9 (i) kann daher unmittelbar abgeleitet werden, dass G insgesamt $\varphi(n)$ Elemente der vollen Ordnung n enthält. Es gibt also genau $\varphi(n)$ Elemente h in G mit der Eigenschaft $G = \langle h \rangle$. Beispielsweise besitzt jede zyklische Gruppe der Ordnung 24 jeweils genau $\varphi(24) = \varphi(2^3)\varphi(3) = 4 \cdot 2 = 8$ erzeugende Elemente.

Gelegentlich ist auch das folgende Kriterium für die Bestimmung der Ordnung hilfreich.

Satz 3.10 Sei G eine Gruppe und $n \in \mathbb{N}$. Ein Element $g \in G$ hat genau dann die Ordnung n, wenn $g^n = e_G$ und für jeden Primteiler p von n jeweils $g^{n/p} \neq e_G$ gilt.

Beweis: „⇒“ Ist $n = \mathrm{ord}(g)$, dann ist $n \in \mathbb{N}$ nach Satz 3.3 minimal mit $g^n = e_G$. Insbesondere gilt dann $g^{n/p} \neq e_G$ für jeden Primteiler p von n. „⇐“ Sei $m = \mathrm{ord}(g)$ und das angegebene Kriterium für ein $n \in \mathbb{N}$ erfüllt. Aus der Gleichung $g^n = e_G$ folgt zunächst $m|n$. Nehmen wir nun an, dass m ein echter Teiler von n ist. Dann besitzt die Zahl $\frac{n}{m} \in \mathbb{N}$ einen Primteiler p. Ist $k \in \mathbb{N}$ mit $\frac{n}{m} = kp$, dann folgt $n = kpm$ und $\frac{n}{p} = km$. Wegen $g^m = e_G$ würden wir $g^{n/p} = (g^m)^k = e_G^k = e_G$ erhalten, im Widerspruch zur Annahme $g^{n/p} \neq e_G$. □

Satz 3.11 Sei G eine zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$.

(i) Ist $\mathrm{ord}(g) = \infty$, dann sind die verschiedenen Untergruppen von G gegeben durch $U_0 = \{e_G\}$ und $U_m = \langle g^m \rangle$, wobei m die natürlichen Zahlen durchläuft.

(ii) Ist $\mathrm{ord}(g) = n$ endlich, dann sind $U_d = \langle g^d \rangle$ die verschiedenen Untergruppen von G, wobei d die Teiler von n durchläuft. Dabei gilt jeweils $|U_d| = \frac{n}{d}$.

In (i) und (ii) gilt $U_m \subseteq U_{m'}$ für $m, m' \in \mathbb{N}$ genau dann, wenn m' ein Teiler von m ist.

Beweis: zu (i) Sei U eine beliebige Untergruppe $\neq \{e_G\}$ von G. Nach Satz 3.7 gibt es ein $m \in \mathbb{N}$ mit $U = \langle g^m \rangle$, also ist $U = U_m$ für dieses m. Seien nun $m, m' \in \mathbb{N}$ vorgegeben. Setzen wir $U_m \subseteq U_{m'}$ voraus, dann gilt insbesondere $g^m \in U_{m'}$, und folglich gibt es ein $k \in \mathbb{Z}$ mit $g^m = (g^{m'})^k = g^{km'}$, also $g^{km'-m} = e_G$. Weil die Ordnung von g unendlich ist, folgt daraus $km' - m = 0 \Leftrightarrow m = km'$, wie wir im Anschluss an Folgerung 3.4 gesehen haben. Also ist m' ein Teiler von m. Sei nun umgekehrt $m' | m$ vorausgesetzt, also $m = km'$ für ein $k \in \mathbb{Z}$. Dann gilt $g^m = (g^{m'})^k \in U_{m'}$ und somit $U_m \subseteq U_{m'}$.

zu (ii) Sei auch hier eine beliebige Untergrupe $U \neq \{e_G\}$ vorgegeben. In diesem Fall folgt aus Satz 3.7, dass $U = U_d$ für einen Teiler d von n gilt. Im Fall $U = \{e_G\}$ ist offenbar $U = U_n$. Für jeden Teiler d von n gilt außerdem $\mathrm{ord}(g^d) = \frac{n}{d}$ nach Satz 3.9 (ii). Daraus folgt jeweils $|U_d| = \frac{n}{d}$.

Der Beweis der Implikation „$m' | m \Rightarrow U_m \subseteq U_{m'}$“ läuft genau wie im Fall unendlicher Ordnung. Auch der Beweis der Umkehrung braucht nur geringfügig modifiziert werden. Aus $g^m \in U_{m'}$ folgt $g^m = (g^{m'})^k = g^{m'k}$ und somit $g^{m-m'k} = e_G$ für ein $k \in \mathbb{Z}$. Wegen $\mathrm{ord}(g) = n$ erhalten wir $n \mid (m - m'k)$ nach Satz 3.3. Es gibt also ein $\ell \in \mathbb{Z}$ mit $\ell n = m - m'k$ oder $m'k = m - \ell n$. Aus $m' \mid (m - \ell n)$ und $m' \mid (\ell n)$ folgt, dass m' ein Teiler von m ist. □

Bei einer zyklischen Gruppe der Ordnung $n \in \mathbb{N}$ stimmt die Anzahl der Untergruppen also überein mit der Anzahl der Teiler $d \in \mathbb{N}$ von n. Die Zahl $12 = 2^2 \cdot 3^1$ besitzt beipielsweise die sechs Teiler $2^i 3^j$ mit $i \in \{0, 1, 2\}$ und $j \in \{0, 1\}$; dies sind die Zahlen $1, 2, 3, 4, 6$ und 12. Dementsprechend besitzt jede zyklische Gruppe der Ordnung 12 genau sechs Untergruppen. Genauer gilt: Ist G zyklisch von Ordnung 12 und $g \in G$ ein erzeugendes Element, dann sind die Untergruppen von G durch folgende Tabelle gegeben.

Untergruppe	U_1	U_2	U_3	U_4	U_6	U_{12}
Ordnung	12	6	4	3	2	1

Dabei ist $U_d = \langle g^d \rangle$ für jeden Teiler d von 12, insbesondere $U_1 = \langle g^1 \rangle = G$ und $U_{12} = \langle g^{12} \rangle = \langle e_G \rangle = \{e_G\}$.

Zum Abschluss zeigen wir noch, dass die zyklischen Gruppen durch die soeben beschriebene Untergruppeneigenschaft sogar charakterisiert werden können.

Satz 3.12 Sei G eine endliche Gruppe der Ordnung n mit der Eigenschaft, dass G für jedes Teiler $d \in \mathbb{N}$ von n genau eine Untergruppe U_d mit $|U_d| = d$ besitzt. Dann ist G eine zyklische Gruppe.

Beweis: Wir beweisen zunächst die Gleichung $\sum_{d|n} \varphi(d) = n$ für die Eulersche φ-Funktion. Sei dazu H eine zyklische Gruppe der Ordnung n. Nach Satz 3.11 gibt es für jeden Teiler $d \in \mathbb{N}$ in H genau eine Untergruppe V_d der Ordnung d. Diese ist nach Satz 3.7 ebenfalls zyklisch, und wie wir oben festgestellt haben, besitzt diese genau $\varphi(d)$ Elemente der Ordnung d. Umgekehrt muss jedes $h \in H$ mit $\mathrm{ord}(h) = d$ in V_d liegen, weil ansonsten $\langle h \rangle$ eine von V_d verschiedene Untergruppe der Ordnung d wäre. Also ist $\varphi(d)$ die Gesamtzahl der Element der Ordnung d in H. Weil nun die Ordnung jedes Elements nach dem Satz von Lagrange ein Teiler von n ist, und weil n auch die Gesamtzahl der Elemente von H ist, erhalten wir die Gleichung $\sum_{d|n} \varphi(d) = n$, wenn die Anzahlen der Elemente der Ordnung d in H für alle Teiler d von n aufaddieren.

Sei nun G eine Gruppe mit den im Satz angegebenen Eigenschaften, und sei d ein echter Teiler von n. Ist $g \in G$ mit $\text{ord}(g) = d$, dann ist $\langle g \rangle$ die einzige Untergruppe der Ordnung d von G, und diese ist zyklisch. Als solche besitzt sie genau $\varphi(d)$ Elemente der Ordnung d. Gäbe es in G mehr als $\varphi(d)$ Elemente der Ordnung d, dann könnten diese nicht alle in $\langle g \rangle$ liegen, und folglich hätte G mehr als eine Untergruppe der Ordnung d, im Widerspruch zur Voraussetzung. ¸ Für jeden echten Teiler d von n gibt es also höchstens $\varphi(d)$ Elemente der Ordnung d in G. Bezeichnet D die Menge der echten Teiler von n in $\mathbb{N}$, dann liefert der Beweisanfang die Ungleichung $\sum_{d \in D} \varphi(d) < n$. Dies zeigt, dass es in G nicht nur Elemente geben kann, deren Ordnung ein echter Teiler von n ist. Statt dessen muss es in G auch Elemente der Ordnung n geben. Daraus folgt, dass G zyklisch ist. □

Aus dem Satz von Lagrange und dem Konzept der Elementordnung ergibt sich noch eine für die elementare Zahlentheorie wichtige Folgerung.

Folgerung 3.13 *(Kleiner Satz von Fermat)*

Für jede Primzahl p und alle $a \in \mathbb{Z}$ gilt $a^p \equiv a \bmod p$. Ist p kein Teiler von a, dann gilt darüber hinaus $a^{p-1} \equiv 1 \bmod p$.

Beweis: Es gilt $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, somit ist $(\mathbb{Z}/p\mathbb{Z})^\times$ eine Gruppe der Ordnung $p-1$. Für jedes $a \in \mathbb{Z}$ ist $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ äquivalent zu $p \nmid a$. Weil die Ordnung jedes Elements der Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ die Gruppenordnung teilt, gilt $(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$ für diese a, was zu $a^{p-1} \equiv 1 \bmod p$ äquivalent ist. Durch Multiplikation dieser Kongruenz mit a folgt $a^p \equiv a \bmod p$. Diese Kongruenz ist auch im Fall $p \mid a$ erfüllt, denn dann gilt auch $p \mid a^p$ und somit $a^p \equiv 0 \equiv a \bmod p$. □

§ 4. *Homomorphismen und Faktorgruppen*

Zusammenfassung. Ein *Homomorphismus* zwischen zwei Gruppen G, H ist eine Abbildung $G \to H$, die verträglich mit den Gruppenverknüpfungen ist. Diese spielen in der Gruppentheorie eine wichtige Rolle, weil man durch sie die Struktur der Gruppen G und H zueinander in Beziehung setzen und sie miteinander vergleichen kann. Beispielsweise hängen die Untergruppen von G und H sowie die in G und H auftretenden Elementordnungen miteinander zusammen.

Als zweites wichtiges Thema dieses Kapitels behanden wir die *Faktorgruppen*. Diese kommen dadurch zu Stande, dass man auf der Menge G/N der Linksnebenklassen einer Untergruppe N von G eine Gruppenstruktur definiert. Dies funktioniert allerdings nur bei Untergruppen N von G mit einer zusätzlichen Eigenschaft, den sogenannten *Normalteilern*. Der Homomorphiesatz für Gruppen stellt zwischen den Homomorphismen und den Faktorgruppen einen Zusammenhang her. Der Korrespondenzsatz bringt zum Ausdruck, dass sich ein Teil der Struktur der Gruppe G auch in der Faktorgruppe G/N widerspiegelt. Allerdings ist Letzere häufig einfacher zu untersuchen, da sie aus weniger Elementen besteht.

Wichtige Grundbegriffe

- Gruppenhomomorphismus
- Mono-, Epi- und Isomorphismus
- Endo- und Automorphismen einer Gruppe
- Normalteiler einer Gruppe (Notation $N \trianglelefteq G$)
- Komplexprodukt zweier Teilmengen einer Gruppe
- inneres (semi-)direktes Produkt
- Faktorgruppe, kanonischer Epimorphismus
- induzierter Homomorphismus

Zentrale Sätze

- Erhaltung der Untergruppen-Eigenschaft unter Homomorphismen
- Isomorphismus $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ für eine zyklische Gruppe G der Ordnung n
- Isomorphismus zwischen innerem und äußerem direkten Produkt zweier Normalteiler
- Homomorphiesatz für Gruppen
- Isomorphiesätze für Gruppen
- Korrespondenzsatz für Gruppen

Wir beginnen mit der Definition der Gruppenhomorphismen.

Definition 4.1 Sind $(G, *)$ und $(H, \circ)$ Gruppen, so bezeichnet man eine Abbildung $\phi : G \to H$ als ***Gruppenhomomorphismus***, wenn $\phi(g * g') = \phi(g) \circ \phi(g')$ für alle $g, g' \in G$ gilt.

Obwohl in der Definition nur gefordert wird, dass ϕ verträglich mit den Verknüpfungen der Gruppen G und H ist, werden auch das Neutralelement und inverse Elemente aufeinander abgebildet.

Lemma 4.2 Sei ϕ ein Homomorphismus zwischen den Gruppen $(G, *)$ und $(H, \circ)$. Dann gilt

$$\phi(e_G) = e_H \qquad \text{und} \qquad \phi(g^{-1}) = \phi(g)^{-1} \quad \text{für alle} \quad g \in G.$$

Beweis: Es gilt $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \circ \phi(e_G)$, und durch Multiplikation beider Seiten von links mit $\phi(e_G)^{-1}$ erhält man

$$\phi(e_G)^{-1} \circ \phi(e_G) \quad = \quad \phi(e_G)^{-1} \circ \phi(e_G) \circ \phi(e_G) \quad ,$$

also $e_H = e_H \circ \phi(e_G)$ und schließlich $e_H = \phi(e_G)$. Für jedes $g \in G$ gilt außerdem $\phi(g) \circ \phi(g^{-1}) = \phi(g * g^{-1}) = \phi(e_G) = e_H$. Multipliziert man beide Seiten von links mit $\phi(g)^{-1}$, so erhält man $\phi(g)^{-1} \circ \phi(g) \circ \phi(g^{-1}) = \phi(g)^{-1} \circ e_H$, somit $e_H \circ \phi(g)^{-1} = \phi(g)^{-1}$ und schließlich $\phi(g^{-1}) = \phi(g)^{-1}$. □

Definition 4.3 Seien $(G, *)$ und $(H, \circ)$ Gruppen und $\phi : G \to H$ ein Homomorphismus von Gruppen. Man bezeichnet ϕ als

(i) ***Monomorphismus***, wenn ϕ injektiv

(ii) ***Epimorphismus***, wenn ϕ surjektiv

(iii) ***Isomorphismus***, wenn ϕ bijektiv ist.

Einen Gruppen-Homomorphismus $\phi : G \to G$ von $(G, \cdot)$ nach $(G, \cdot)$ bezeichnet man als ***Endomorphismus*** von G. Ist die Abbildung ϕ außerdem bijektiv, dann spricht man von einem ***Automorphismus*** der Gruppe G. Die Menge der Automorphismen bezeichnen wir mit $\mathrm{Aut}(G)$. Wir bemerken, dass nach Definition 1.16 zwei Gruppen G und H genau dann zueinander isomorph sind, wenn ein Isomorphismus $\phi : G \to H$ existiert.

Lemma 4.4 Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(g^n) = \phi(g)^n$ für alle $g \in G$ und $n \in \mathbb{Z}$.

Beweis: Sei $g \in G$ vorgegeben. Zunächst beweist man die Gleichung für alle $n \in \mathbb{N}_0$ durch vollständige Induktion. Für $n = 0$ ist die Gleichung wegen $\phi(g^0) = \phi(e_G) = e_H = \phi(g)^0$ erfüllt, und setzen wir sie für n voraus, dann ist sie wegen

$$\phi(g^{n+1}) \quad = \quad \phi(g^n \cdot g) \quad = \quad \phi(g^n) \cdot \phi(g) \quad = \quad \phi(g)^n \cdot \phi(g) \quad = \quad \phi(g)^{n+1}$$

auch für $n + 1$ gültig. Für alle $n \in \mathbb{N}$ gilt außerdem $\phi(g^{-n}) = \phi((g^n)^{-1}) = \phi(g^n)^{-1} = (\phi(g)^n)^{-1} = \phi(g)^{-n}$. Dies zeigt, dass die Gleichung auch für negative Exponenten, und damit insgesamt für alle $n \in \mathbb{Z}$ gültig ist. □

Der folgende Isomorphismus wird später im Kapitel über Gruppenoperationen eine wichtige Rolle spielen.

Satz 4.5 Seien X, Y Mengen und $\phi : X \to Y$ eine Bijektion. Dann ist durch die Abbildung $\hat{\phi} : \mathrm{Per}(X) \to \mathrm{Per}(Y)$, $\sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$ ein Isomorphismus von Gruppen definiert.

Beweis: Sei $\sigma \in \mathrm{Per}(X)$ vorgegeben. Durch Komposition der Abbildungen $\phi^{-1} : Y \to X$, $\sigma : X \to X$ und $\phi : X \to Y$ erhält man eine Abbildung $Y \to Y$, und als Komposition bijektiver Abbildungen ist $\phi \circ \sigma \circ \phi^{-1}$ ebenfalls bijektiv. Also ist durch die angegebene Zuordnung $\hat{\phi}$ tatsächlich eine Abbildung $\mathrm{Per}(X) \to \mathrm{Per}(Y)$ definiert. Um zu zeigen, dass $\hat{\phi}$ ein Homomorphismus von Gruppen ist, seien $\sigma, \tau \in \mathrm{Per}(X)$ vorgegeben. Dann gilt

$$\hat{\phi}(\sigma\circ\tau) \quad = \quad \phi\circ\sigma\circ\tau\circ\phi^{-1} \quad = \quad \phi\circ\sigma\circ(\phi^{-1}\circ\phi)\circ\tau\circ\phi^{-1} \quad =$$
$$(\phi\circ\tau\circ\phi^{-1})\circ(\phi\circ\sigma\circ\phi^{-1}) \quad = \quad \hat{\phi}(\sigma)\circ\hat{\phi}(\tau).$$

Um zu zeigen, dass $\hat{\phi}$ bijektiv ist, genügt es zu bemerken, dass durch die Zuordnung $\sigma \mapsto \phi^{-1}\circ\sigma\circ\phi$ eine Umkehrabbildung $\hat{\psi} : \mathrm{Per}(Y) \to \mathrm{Per}(X)$ von $\hat{\phi}$ gegeben ist. Für jedes $\sigma \in \mathrm{Per}(Y)$ ist nämlich $\phi^{-1}\circ\sigma\circ\phi$ eine Abbildung $X \to X$, und wiederum bijektiv als Komposition bijektiver Abbildungen. Also ist $\hat{\psi}$ tatsächlich eine Abbildung von $\mathrm{Per}(Y)$ nach $\mathrm{Per}(X)$. Außerdem gilt für alle $\sigma \in \mathrm{Per}(X)$ jeweils

$$(\hat{\psi}\circ\hat{\phi})(\sigma) \quad = \quad \hat{\psi}(\hat{\phi}(\sigma)) \quad = \quad \hat{\psi}(\phi\circ\sigma\circ\phi^{-1}) \quad = \quad \phi^{-1}\circ(\phi\circ\sigma\circ\phi^{-1})\circ\phi \quad =$$
$$(\phi^{-1}\circ\phi)\circ\sigma\circ(\phi^{-1}\circ\phi) \quad = \quad \mathrm{id}_X\circ\sigma\circ\mathrm{id}_X \quad = \quad \sigma \quad = \quad \mathrm{id}_{\mathrm{Per}(X)}(\sigma) \quad ,$$

also $\hat{\psi}\circ\hat{\phi} = \mathrm{id}_{\mathrm{Per}(X)}$. Durch eine analoge Rechnung zeigt man $\hat{\phi}\circ\hat{\psi} = \mathrm{id}_{\mathrm{Per}(Y)}$. Dies zeigt, dass $\hat{\psi}$ tatsächlich die Umkehrabbildung von $\hat{\phi}$ ist. □

Nach Satz 4.5 gilt $\mathrm{Per}(X) \cong S_n$ für jede n-elementige Menge X, denn die Gleichung $|X| = n$ bedeutet ja gerade, dass eine bijektive Abbildung zwischen M_n und X existiert.

Wir befassen uns noch mit den Endo- und Automorphismen einer Gruppe und legen dafür eine beliebige Gruppe $(G,\cdot)$ zu Grunde. Sind $\phi_1, \phi_2 : G \to G$ zwei Endomorphismen von G, dann ist auch $\phi_1\circ\phi_2$ ein Endomorphismus von G, denn für alle $g,h \in G$ gilt

$$(\phi_1\circ\phi_2)(gh) \quad = \quad \phi_1(\phi_2(gh)) \quad = \quad \phi_1(\phi_2(g)\cdot\phi_2(h)) \quad =$$
$$\phi_1(\phi_2(g))\cdot\phi_1(\phi_2(h)) \quad = \quad (\phi_1\circ\phi_2)(g)\cdot(\phi_1\circ\phi_2)(h).$$

Ist ϕ_3 ein weiterer Endomorphismus, dann gilt $(\phi_1\circ\phi_2)\circ\phi_3 = \phi_1\circ(\phi_2\circ\phi_3)$; diese Gleichung wurde früher bereits für beliebge Kompositionen von Abbildungen verifiziert. Außerdem gilt $\phi_1\circ\mathrm{id}_G = \mathrm{id}_G\circ\phi_1 = \phi_1$. Dies zeigt, dass die Menge $\mathrm{End}(G)$ der Endomorphismen von G zusammen mit der Komposition $\circ$ als Verknüpfung ein Monoid bildet, mit id_G als Neutralelement. Es gilt nun

Proposition 4.6 Die invertierbaren Elemente in $\mathrm{End}(G)$ sind genau die Automorphismen der Gruppe G.

Beweis: Ist ϕ in $\mathrm{End}(G)$ ein invertierbares Element, dann gibt es ein $\psi \in \mathrm{End}(G)$ mit $\psi\circ\phi = \mathrm{id}_G$ und $\phi\circ\psi = \mathrm{id}_G$. Aus den Gleichungen folgt, dass ϕ bijektiv ist. Als bijektiver Homomorphismus ist ϕ nach Definition ein Automorphismus.

Sei nun umgekehrt ϕ ein Automorphismus von G. Dann ist ϕ bijektiv. Wir zeigen weiter unten, dass die Umkehrabbildung ϕ^{-1} von ϕ ein Gruppenhomomorphismus ist. Weil mit ϕ auch ϕ^{-1} bijektiv ist, ist durch ϕ^{-1} dann insgesamt ein Automorphismus gegeben. Darüber hinaus zeigen die Gleichungen $\phi^{-1}\circ\phi = \mathrm{id}_G$ und $\phi\circ\phi^{-1} = \mathrm{id}_G$, dass es sich bei ϕ im Monoid $\mathrm{End}(G)$ um ein invertierbares Element handelt.

Zum Nachweis der Homomorphismus-Eigenschaft von ϕ^{-1} seien $g,h \in G$ vorgegeben. Auf Grund der Homomorphismus-Eigenschaft von ϕ gilt $\phi(\phi^{-1}(g)\cdot\phi^{-1}(h)) = \phi(\phi^{-1}(g))\cdot\phi(\phi^{-1}(h)) = gh$. Durch Anwendung von ϕ^{-1} auf beide Seiten dieser Gleichung erhalten wir $\phi^{-1}(g)\phi^{-1}(h) = \phi^{-1}(gh)$. Also ist ϕ^{-1} verträglich mit der Verknüpfung von G und damit ein Homomorphismus. □

Durch Anwendung von Satz 1.15 erhalten wir nun

Satz 4.7 Die Automorphismen einer Gruppe G bilden mit der Verknüpfung $\circ$ selbst eine Gruppe. Man nennt sie die ***Automorphismengruppe*** $\mathrm{Aut}(G)$ der Gruppe G.

Ergänzend bemerken wir noch, dass allgemein gilt: Ist $\phi : G \to H$ ein Isomorphismus von Gruppen, dann gilt dasselbe für die Umkehrabbildung $\phi^{-1} : H \to G$. Der Nachweis dafür funktioniert genauso wie im zweiten Teil des Beweises von Proposition 4.6. Allerdings lassen sich zwei Isomorphismen $G \to H$ in der Regel nicht verknüpfen (jedenfalls nicht durch die Komposition von Abbildungen), also bilden die Isomorphismen zwischen G und H im Allgemeinen keine Gruppe.

Als nächstes befassen wir uns mit der Beziehung zwischen Homomorphismen und Untergruppen.

Proposition 4.8 Sei $\phi : G \to H$ ein Gruppenhomomorphismus, außerdem U eine Untergruppe von G und V eine Untergruppe von H. Dann gilt

(i) Die Bildmenge $\phi(U)$ ist eine Untergruppe von H.

(ii) Die Urbildmenge $\phi^{-1}(V)$ ist eine Untergruppe von G.

Beweis: zu (i) Wegen $e_G \in U$ und $\phi(e_G) = e_H$ ist $e_H \in \phi(U)$ enthalten. Seien nun $g', h' \in \phi(U)$ vorgegeben. Dann gibt es Elemente $g, h \in U$ mit $\phi(g) = g'$ und $\phi(h) = h'$. Mit g, h liegen auch die Elemente gh und g^{-1} in U. Es folgt $g'h' = \phi(g)\phi(h) = \phi(gh) \in \phi(U)$, und ebenso erhalten wir $(g')^{-1} = \phi(g)^{-1} = \phi(g^{-1}) \in \phi(U)$.

zu (ii) Aus $\phi(e_G) = e_H \in V$ folgt $e_G \in \phi^{-1}(V)$. Sind $g, h \in \phi^{-1}(V)$ vorgegeben, dann gilt $\phi(g), \phi(h) \in V$. Es folgt $\phi(gh) = \phi(g)\phi(h) \in V$ und somit $gh \in \phi^{-1}(V)$. Ebenso gilt $\phi(g^{-1}) = \phi(g)^{-1} \in V$, also $g^{-1} \in \phi^{-1}(V)$. □

Eine besonders wichtige Rolle spielen in der Gruppentheorie der ***Kern*** $\ker(\phi) = \phi^{-1}(\{e_H\})$ und das ***Bild*** $\mathrm{im}(\phi) = \phi(G)$ eines Gruppenhomomorphismus. Nach Proposition 4.8 ist $\ker(\phi)$ eine Untergruppe von G und $\mathrm{im}(\phi)$ eine Untergruppe von H. Beispielsweise ist für jedes $n \in \mathbb{N}$ die ***alternierende Gruppe*** A_n als Kern des Signums-Homomorphismus $\mathrm{sgn} : S_n \to \{\pm 1\}$ eine Untergruppe der symmetrischen Gruppe S_n.

Aus der Linearen Algebra ist bekannt, dass die Determinante auf der Menge $\mathcal{M}_{n,K}$ der $(n \times n)$-Matrizen über einem Körper K die Multiplikativitätsregel $\det(AB) = \det(A)\det(B)$ erfüllt. Außerdem gilt $\det(A) \neq 0$ genau dann, wenn A invertierbar ist. Daraus folgt, dass die Determinantenfunktion einen Gruppenhomomorphismus $\det : \mathrm{GL}_n(K) \to K^\times$ definiert. Die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ ist nach Definition genau der Kern dieses Homomorphismus.

Kerne und Bilder sind bereits aus der Linearen Algebra im Zusammenhang mit linearen Abbildungen bekannt. Wie dort gilt auch hier der Zusammenhang

Proposition 4.9 Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Die Abbildung ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{e_G\}$ gilt.

Beweis: „⇒“ Ist ϕ ein Monomorphismus, dann ist e_G das einzige Element, das auf e_H abgebildet wird. Also gilt $\ker(\phi) = \{e_G\}$. „⇐“ Setzen wir $\ker(\phi) = \{e_G\}$ voraus, und seien $g, h \in G$ mit $\phi(g) = \phi(h)$ vorgegeben. Dann gilt $\phi(g)\phi(h)^{-1} = e_H$, und wir erhalten $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = e_H$. Nach Definition des Kerns folgt $gh^{-1} \in \ker(\phi)$. Auf Grund der Voraussetzung bedeutet dies $gh^{-1} = e_G$ und somit $g = h$. □

In vielen Anwendungen erweist es sich als nützlich, dass ein Homomorphismus $G \to H$ bereits durch die Bilder eines Erzeugendensystems eindeutig festgelegt ist. Der Grund dafür besteht darin, dass viele bedeutende Gruppen (wie zum Beispiel die symmetrische Gruppen) sehr kleine Erzeugendensysteme besitzen.

Satz 4.10 *(Eindeutigkeit von Homomorphismen)*

Seien G, H Gruppen und $S \subseteq G$ ein Erzeugendensystem von G. Sind $\phi, \phi' : G \to H$ Gruppenhomomorphismen mit $\phi(s) = \phi'(s)$ für alle $s \in S$, dann folgt $\phi = \phi'$.

Beweis: Wir zeigen, dass die Teilmenge $U = \{g \in G \mid \phi(g) = \phi'(g)\}$ eine Untergruppe von G ist. Wegen $\phi(e_G) = e_H = \phi'(e_G)$ ist $e_G \in U$. Sind $g, h \in U$ beliebig vorgegeben, dann gilt

$$\phi(gh) = \phi(g)\phi(h) = \phi'(g)\phi'(h) = \phi'(gh) \qquad \text{und} \qquad \phi(g^{-1}) = \phi(g)^{-1} = \phi'(g)^{-1} = \phi'(g^{-1}) \quad ,$$

also gilt $gh \in U$ und $g^{-1} \in U$. Weil U nach Voraussetzung die Menge S enthält, gilt $G = \langle S \rangle \subseteq U$ und somit $G = U$. Die Abbildungen ϕ und ϕ' stimmen also auf der gesamten Gruppe G überein. □

Ist also beispielsweise $S = \{a, b\}$ ein zweielementiges Erzeugendensystem einer Gruppe G, dann ist jeder Homomorphismus $\phi : G \to H$ in eine beliebige Gruppe H bereits durch die Bilder $\phi(a), \phi(b) \in H$ eindeutig festgelegt.

Kommen wir nun zur Frage nach der *Existenz* von Homomorphismen. Für zwei beliebige Gruppen G und H ist durch $G \to H$, $g \mapsto e_H$ ein Homomorphismus definiert; man bezeichnet ihn als den ***trivialen*** Homomorphismus. Ob es weitere Homomorphismen zwischen G und H gibt, ist in der Regel nicht leicht zu entscheiden. Der Fall, dass es sich bei G um eine *zyklische* Gruppe handelt, ist eine der seltenen Situationen, in denen weit reichende allgemeine Aussagen möglich sind.

Proposition 4.11 Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Ist $g \in G$ ein Element von endlicher Ordnung n, dann ist auch $\mathrm{ord}(\phi(g))$ endlich, und ein Teiler von n.

Beweis: Auf Grund der Homomorphismus-Eigenschaft gilt $\phi(g)^n = \phi(g^n) = \phi(e_G) = e_H$. Aus den Teilen (ii) und (iii) von Satz 3.3 folgt sowohl die Endlichkeit von $\mathrm{ord}(\phi(g))$ als auch die Teiler-Eigenschaft. □

Proposition 4.12 *(Existenz von Homomorphismen auf zyklischen Gruppen)*

Sei G eine zyklische Gruppe, $g \in G$ ein erzeugendes Element, H eine weitere Gruppe und $h \in H$. Ist $\mathrm{ord}(g) = \infty$ oder $\mathrm{ord}(g)$ endlich und ein Vielfaches von $\mathrm{ord}(h)$, dann existiert ein (eindeutig bestimmter) Gruppenhomomorphismus $\phi : G \to H$ mit $\phi(g) = h$.

Beweis: Die Eindeutigkeit folgt in beiden Fällen aus Satz 4.10. Für die Existenz betrachten wir zunächst den Fall $\mathrm{ord}(g) = \infty$ und definieren die Abbildung ϕ durch $\phi(g^n) = h^n$ für alle $n \in \mathbb{Z}$. Dann ist ϕ eine wohldefinierte Abbildung und ein Homomorphismus, denn alle Elemente aus G lassen sich auf eindeutige Weise in der Form g^m mit $m \in \mathbb{Z}$ darstellen, und für alle $m, n \in \mathbb{Z}$ gilt $\phi(g^m g^n) = \phi(g^{m+n}) = h^{m+n} = h^m h^n = \phi(g^m)\phi(g^n)$.

Sei nun $n = \text{ord}(g)$ endlich und ein Vielfaches von $\text{ord}(h)$. Dann definieren wir ϕ als Abbildung durch $\phi(g^k) = h^k$ für $0 \leq k < n$. Wir zeigen, dass dann $\phi(g^m) = h^m$ für alle $m \in \mathbb{Z}$ erfüllt ist. Division von m durch n mit Rest liefert $q, r \in \mathbb{Z}$ mit $m = qn + r$ und $0 \leq r < n$. Da n ein Vielfaches von $\text{ord}(h)$ ist, gilt $h^n = e_H$, und es folgt

$$\phi(g^m) \quad = \quad \phi(g^{qn+r}) \quad = \quad \phi((g^n)^q g^r) \quad = \quad \phi(g^r) \quad = \quad h^r \quad = \quad (h^n)^q h^r \quad = \quad h^{qn+r} \quad = \quad h^m.$$

Wie im Fall unendlicher Ordnung prüft man nun die Homomorphismus-Eigenschaft von ϕ. □

Folgerung 4.13 Je zwei unendliche zyklische Gruppen sind isomorph. Ebenso sind zwei endliche zyklische Gruppen derselben Ordnung isomorph.

Beweis: Seien G und H unendliche zyklische Gruppen und $g \in G$, $h \in H$ mit $G = \langle g \rangle$ sowie $H = \langle h \rangle$. Dann gibt es nach Proposition 4.12 eindeutig bestimmte Homomorphismen $\phi : G \to H$ und $\psi : H \to G$ mit $\phi(g) = h$ und $\psi(h) = g$. Es gilt $(\psi \circ \phi)(g) = g$. Aber nach Satz 4.10 gibt es nur einen Homomorphismus $G \to G$ mit $g \mapsto g$, nämlich id_G. Somit ist $\psi \circ \phi = \text{id}_G$. Ebenso schließt man aus der Gleichung $(\phi \circ \psi)(h) = h$, dass $\phi \circ \psi = \text{id}_H$ gilt. Die Abbildungen ϕ und ψ sind also zueinander invers und damit bijektiv. Es folgt $G \cong H$. Im Fall endlicher Ordnung verläuft der Beweis analog. □

Mit Hilfe dieser Ergebnisse können wir nun die Automorphismengruppe zyklischer Gruppen bestimmen. Dazu betrachten wir die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$. Nach Satz 1.15 bildet diese Menge mit der Multiplikation als Verknüpfung eine Gruppe, die man als ***prime Restklassengruppe*** bezeichnet. Mit dem folgenden Kriterium lasse sich die Elemente dieser Gruppen leicht bestimmen.

Proposition 4.14 Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das Element $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann in $(\mathbb{Z}/n\mathbb{Z})^\times$ enthalten, wenn $\text{ggT}(a, n) = 1$ ist.

Beweis: „⇒“ Ist $a + n\mathbb{Z}$ im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ invertierbar, dann existiert ein $b \in \mathbb{Z}$ mit $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$. Daraus folgt $ab + n\mathbb{Z} = 1 + n\mathbb{Z}$, was wiederum zu $ab \equiv 1 \bmod n$ äquivalent ist. Die Zahl $1 - ab$ ist also teilbar durch n; es existiert also ein $k \in \mathbb{Z}$ mit $1 - ab = kn$, was zu $ab + kn = 1$ umgeformt werden kann. Ist nun $d \in \mathbb{N}$ ein gemeinsamer Teiler von a und n, dann folgt aus der letzten Gleichung, dass d auch ein Teiler von 1 sein und somit $d = 1$ gelten muss. Damit ist $\text{ggT}(a, n) = 1$ nachgewiesen.

„⇐“ Aus $\text{ggT}(a, n) = 1$ folgt mit Satz 3.8, dem Lemma von Bézout, die Existenz von $b, k \in \mathbb{Z}$ mit $ab + kn = 1$. Dasdurch erhalten wir im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ die Gleichung

$$(a + n\mathbb{Z})(b + n\mathbb{Z}) \quad = \quad ab + n\mathbb{Z} \quad = \quad ab + kn + n\mathbb{Z} = 1 + n\mathbb{Z}.$$

Dies zeigt, dass $a + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ invertierbar ist. □

Sei nun G eine zyklische Gruppe der endlichen Ordnung n und $g \in G$ mit $G = \langle g \rangle$. Wegen Satz 3.9 ist $\text{ord}(g^a)$ für jedes $a \in \mathbb{Z}$ ein Teiler von n. Wir können also Proposition 4.12 anwenden und erhalten für jedes $a \in \mathbb{Z}$ einen eindeutig bestimmten Endomorphismus

$$\tau_a : G \to G \qquad \text{mit} \qquad \tau_a(g) = g^a.$$

Sind $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod n$, dann gilt $\tau_a = \tau_b$. Um dies zu überprüfen, genügt es wegen $G = \langle g \rangle$ nach Proposition 4.10 nachzuweisen, dass die Elemente $\tau_a(g) = g^a$ und $\tau_b(g) = g^b$ übereinstimmen. Aber wegen $a \equiv b \bmod n$ existiert ein $k \in \mathbb{Z}$ mit $b = a + kn$, und daraus folgt tatsächlich $g^b = g^a + nk = g^a \cdot (g^n)^k = g^a \cdot e_G^k = g^a$. Durch die Zuordnung $a + n\mathbb{Z} \mapsto \tau_a$ ist also eine wohldefinierte Abbildung $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}(G)$ gegeben.

Satz 4.15 Durch Einschränkung der Abbildung ϕ auf $(\mathbb{Z}/n\mathbb{Z})^\times$ erhält man einen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(G)$.

Beweis: Zunächst zeigen wir, dass ϕ verträglich mit der Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ und der Komposition auf $\mathrm{End}(G)$ ist. Für alle $a, b \in \mathbb{Z}$ gilt

$$(\tau_a \circ \tau_b)(g) \quad = \quad \tau_a(\tau_b(g)) \quad = \quad \tau_a(g^b) \quad = \quad \tau_a(g)^b \quad = \quad (g^a)^b \quad = \quad g^{ab} \quad = \quad \tau_{ab}(g).$$

Eine Anwendung von Satz 4.10 liefert $\tau_a \circ \tau_b = \tau_{ab}$, und es folgt $\phi(a + n\mathbb{Z}) \circ \phi(b + n\mathbb{Z}) = \phi(ab + n\mathbb{Z})$. Als nächstes überprüfen wir, dass ϕ die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z}$ der invertierbare Elemente von $\mathbb{Z}/n\mathbb{Z}$ surjektiv auf $\mathrm{Aut}(G)$ abbildet. Offenbar ist τ_1 der eindeutig bestimmte Endomorphismus von G, der g auf g abbildet; daraus folgt $\tau_1 = \mathrm{id}_G$. Ist nun $a + n\mathbb{Z}$ ein invertierbares Element, dann existiert ein $b \in \mathbb{Z}$ mit $(a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z}$. Die soeben bewiesene Gleichung liefert

$$\tau_a \circ \tau_b \quad = \quad \phi(a + n\mathbb{Z}) \circ \phi(b + n\mathbb{Z}) \quad = \quad \phi(1 + n\mathbb{Z}) \quad = \quad \tau_1 \quad = \quad \mathrm{id}_G \quad ,$$

und ebenso erhält man $\tau_b \circ \tau_a = \mathrm{id}_G$. Dies zeigt, dass τ_a ein Automorphismus von G und ϕ somit $(\mathbb{Z}/n\mathbb{Z})^\times$ nach $\mathrm{Aut}(G)$ abbildet. Umgekehrt ist jedes Element $\tau \in \mathrm{Aut}(G)$ ist im Bild von $\phi|_{(\mathbb{Z}/n\mathbb{Z})^\times}$ enthalten. Denn wegen $\tau(g) \in \langle g \rangle$ existiert ein $a \in \mathbb{Z}$ mit $\tau(g) = g^a = \tau_a(g)$, woraus $\tau = \tau_a$ folgt, erneut auf Grund von Proposition 4.10. Wegen $\tau(g^m) = \tau(g)^m = (g^a)^m$ für alle $m \in \mathbb{Z}$ besteht das Bild $\tau(G)$ nur aus Potenzen von g^a. Wegen $\tau \in \mathrm{Aut}(G)$ gilt insbesondere $\tau(G) = G$; also muss g^a in G ein Element der Ordnung n sein. Daraus folgt $\mathrm{ggT}(a, n) = 1$ (nach Teil (i) von Satz 3.9) und somit $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ (nach Proposition 4.14).

Also ist durch $\phi|_{(\mathbb{Z}/n\mathbb{Z})^\times}$ ein surjektiver Gruppenhomomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G)$ gegeben. Dieser ist auch injektiv. Ist nämlich $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\phi(a + n\mathbb{Z}) = \mathrm{id}_G$ vorgegeben, dann folgt $g^a = \tau_a(g) = \phi(a + n\mathbb{Z})(g) = \mathrm{id}_G(g) = g^1$. Wir erhalten $g^{a-1} = e_G$, also $n \mid (a-1)$, damit $a \equiv 1 \bmod n$ und $a + n\mathbb{Z} = 1 + n\mathbb{Z}$. Die Injektivität folgt nun aus Proposition 4.9. □

Auch im Fall, dass $G = \langle g \rangle$ unendlich ist, lässt sich die Automorphismengruppe leicht angeben. Nach Proposition 4.12 sind die Endomorphismen einer solchen Gruppe G genau die Abbildungen der Form $\tau_a(g) = g^a$, wobei a die Menge $\mathbb{Z}$ der ganzen Zahlen durchläuft. Im Gegensatz zum endlichen Fall gilt hier $\tau_a = \tau_b$ für $a, b \in \mathbb{Z}$ genau dann, wenn $a = b$ ist, denn nur in diesem Fall ist $g^a = g^b$. Wie in Satz 4.15 überprüft man, dass durch $\mathbb{Z} \to \mathrm{End}(G)$, $a \mapsto \tau_a$ ein Isomorphismus zwischen den Monoiden $(\mathbb{Z}, \cdot)$ und $(\mathrm{End}(G), \circ)$ gegeben ist. Wiederum ist τ_a genau dann ein Automorphismus, wenn a in $(\mathbb{Z}, \cdot)$ invertierbar ist, und die invertierbaren Elemente in dieser Gruppen sind ± 1.

Wie bei den zyklischen Gruppen endlicher Ordnung kommt man so zu dem Ergebnis $(\mathrm{Aut}(G), \circ) \cong (\{\pm 1\}, \cdot)$. Da es sich bei $(\{\pm 1\}, \cdot)$ und $(\mathbb{Z}/2\mathbb{Z}, +)$ um zyklische Gruppen der Ordnung 2 handelt, sind diese nach Folgerung 4.13 isomorph. Somit gilt auch $(\mathrm{Aut}(G), \circ) \cong (\mathbb{Z}/2\mathbb{Z}, +)$ für jede unendliche zyklische Gruppe G.

Ist U eine Untergruppe, dann bilden die Nebenklassen gU lediglich eine Menge, die wir mit G/U bezeichnet haben. Wir betrachten nun im weiteren Verlauf einen speziellen Typ von Untergruppen, die es uns ermöglichen werden, auf der Menge G/U wiederum eine Gruppenstruktur zu definieren.

Definition 4.16 Sei G eine Gruppe. Eine Untergruppe U von G wird ***Normalteiler*** von G genannt (Schreibweise $U \trianglelefteq G$), wenn $gU = Ug$ für alle $g \in G$ gilt.

Für die Normalteiler-Eigenschaft einer Untergruppe gibt es mehrere äquivalente Kriterien.

Proposition 4.17 Sei G eine Gruppe und U eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

(i) U ist Normalteiler von G.

(ii) Es gilt $gUg^{-1} \subseteq U$ für alle $g \in G$, wobei $gUg^{-1} = \{gug^{-1} \mid u \in U\}$ ist.

(iii) Es gilt $gUg^{-1} = U$ für alle $g \in G$.

Beweis: „(i) $\Rightarrow$ (ii)“ Seien $g \in G$ und $h \in gUg^{-1}$ vorgegeben. Dann gibt es ein $u \in U$ mit $h = gug^{-1}$. Auf Grund der Gleichung $gU = Ug$ finden wir ein $u' \in U$ mit $gu = u'g$. Es folgt $h = (u'g)g^{-1} = u' \in U$. Damit ist die Inklusion $gUg^{-1} \subseteq U$ nachgewiesen.

„(ii) $\Rightarrow$ (iii)“ Sei $g \in G$ vorgegeben. Auf Grund der Voraussetzung genügt es, die Inklusion $U \subseteq gUg^{-1}$ zu beweisen. Seien $g \in G$ und $u \in U$ vorgegeben. Nach Voraussetzung gilt auch $g^{-1}Ug \subseteq U$, also liegt das Element $u' = g^{-1}ug$ in U. Es folgt $u = gu'g^{-1} \in gUg^{-1}$.

„(iii) $\Rightarrow$ (i)“ Zunächst beweisen wir die Inklusion $gU \subseteq Ug$. Sei dazu $h \in gU$ vorgegeben. Dann gibt es ein $u \in U$ mit $h = gu$. Nach Voraussetzung liegt das Element $u' = gug^{-1}$ in U. Es gilt also $h = u'g \in Ug$. Zum Beweis von $Ug \subseteq gU$ sei nun umgekehrt $h \in Ug$ enthalten, also $h = ug$ für ein $u \in U$. Wegen $g^{-1}Ug = U$ liegt $u' = g^{-1}ug$ in U. Daraus folgt $h = gu' \in gU$. □

Ist G eine beliebige Gruppe, dann sind $\{e_G\}$ und G stets Normalteiler von G. Man nennt eine Gruppe G ***einfach***, wenn $G \neq \{e_G\}$ gilt und es neben diesen beiden keine weiteren Normalteiler von G gibt. Ist G abelsch, dann ist *jede* Untergruppe von G ein Normalteiler; vgl. die Bemerkung unmittelbar vor Lemma 2.14. Eine abelsche Gruppe ist also nur dann einfach, wenn sie außer $\{e_G\}$ und G keine weiteren Untergruppen besitzt. Wir werden später sehen, dass dies bei abelschen Gruppen nur auf die Gruppen von Primzahlordnung zutrifft. Nicht-kommutative einfache Gruppen haben dagegen (anders als die Bezeichung „einfach“ vermuten lässt) in der Regel eine sehr komplizierte Struktur.

Gilt $N \trianglelefteq G$, dann gilt offenbar auch $N \trianglelefteq U$ für jede Untergruppe U von G mit $U \supseteq N$. Neben dem direkten Nachrechnen lässt sich die Normalteiler-Eigenschaft auch durch folgende Kriterien feststellen.

Satz 4.18

(i) Ist G eine Gruppe und U eine Untergruppe mit $(G:U)=2$, dann gilt $U \trianglelefteq G$.

(ii) Ist G eine Gruppe und $(N_i)_{i\in I}$ eine Familie von Normalteilern, dann ist auch $N=\bigcap_{i\in I} N_i$ ein Normalteiler von G.

(iii) Sei nun $\phi: G \to H$ ein Gruppenhomomorphismus. Ist N ein Normalteiler von H, dann ist $\phi^{-1}(N)$ ein Normalteiler von G.

(iv) Ist ϕ surjektiv und N Normalteiler von G, dann ist $\phi(N)$ Normalteiler von H.

Beweis: zu (i) Sei $g \in G$ beliebig. Ist g in U enthalten, dann gilt $gU = U = Ug$. Setzen wir nun $g \notin U$ voraus. Dann ist gU eine von U verschiedene Linksnebenklasse in G. Wegen $(G:U)=2$ sind U und gU die einzigen Linksnebenklassen, und wir erhalten eine disjunkte Zerlegung $G = U \cup gU$, also $gU = G \setminus U$. Ebenso zeigt man $Ug = G \setminus U$. Insgesamt erhalten wir $gU = Ug$.

zu (ii) Für beliebiges $g \in G$ ist zu zeigen, dass $gNg^{-1} \subseteq N$ gilt. Sei also $h \in gNg^{-1}$. Dann gibt es ein $n \in N$ mit $h = gng^{-1}$. Weil jedes N_i Normalteiler und nach Voraussetzung n in jedem N_i enthalten ist, gilt $h = gng^{-1} \in N_i$ für alle $i \in I$. Also liegt h in N.

zu (iii) Sei $n \in \phi^{-1}(N)$, also $\phi(n) \in N$. Dann gilt $h\phi(n)h^{-1} \in N$ für alle $h \in H$. Insbesondere gilt $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} \in N$ für alle $g \in G$, also $gng^{-1} \in \phi^{-1}(N)$ für alle $g \in G$.

zu (iv) Sei $n \in \phi(N)$, also $n = \phi(n')$ für ein $n' \in G$. Ist nun $h \in H$ beliebig vorgegeben, dann finden wir auf Grund der Surjektivität von ϕ ein $g \in G$ mit $\phi(g) = h$. Weil N Normalteiler von G ist, gilt $gn'g^{-1} \in N$. Es folgt $hnh^{-1} = \phi(g)\phi(n')\phi(g)^{-1} = \phi(gn'g^{-1}) \in \phi(N)$. □

Beispielsweise ist $N = \langle(1\ 2\ 3)\rangle$ ein Normalteiler von S_3, denn aus $|N| = 3$ und $|S_3| = 6$ folgt $(G:N) = 2$ nach dem Satz von Lagrange. Die Untergruppe $U = \langle(1\ 2)\rangle$ ist dagegen *kein* Normalteiler von S_3, denn wie wir bereits in §4 gesehen haben, stimmen Links- und Rechtsnebenklassen von U nicht überein. Für $g = (1\ 2\ 3)$ beispielsweise gilt $gU = \{(1\ 2\ 3), (1\ 3)\}$ und $Ug = \{(1\ 2\ 3), (2\ 3)\}$.

Aus Teil (iii) von Satz 4.18, angewendet auf den Normalteiler $\{e_H\}$ von H, folgt insbesondere, dass ***Kerne von Homomorphismen stets Normalteiler*** sind. Umgekehrt werden wir in Kürze sehen, dass jeder Normalteiler auch Kern eines geeigneten Homomorphismus ist.

Man beachte, dass Teil (iv) ohne die Voraussetzung der Surjektivität falsch wird. Als Beispiel betrachte man die Inklusionsabbildung $\phi: \langle(1\ 2)\rangle \to S_3$, $\sigma \mapsto \sigma$. Offenbar gilt $\phi(\langle(1\ 2)\rangle) = \langle(1\ 2)\rangle$ und $\langle(1\ 2)\rangle \trianglelefteq \langle(1\ 2)\rangle$. Aber andererseits ist $\langle(1\ 2)\rangle$, wie bereits festgestetllt, kein Normalteiler von S_3.

In bestimmten Situationen können Normalteiler verwendet werden, um Gruppen in äußere direkte Produkte kleinerer Gruppen zu zerlegen. Zur Vorbereitung definieren wir

Definition 4.19 Sei G eine Gruppe, und seien $A, B \subseteq G$ beliebige Teilmengen. Dann nennt man die Teilmenge $AB = \{ab \mid a \in A, b \in B\}$ das ***Komplexprodukt*** von A und B.

Bei Gruppen in additiver Schreibweise verwendet man für das Komplexprodukt die Schreibweise $A+B$ statt AB. Die folgenden „Rechenregeln“ für Komplexprodukte werden wir im weiteren Verlauf der Vorlesung an mehreren Stellen verwenden, in diesem Kapitel beispielsweise weiter unten beim Beweis des Korrespondenzsatzes.

Lemma 4.20 Sei G eine Gruppe, und seien U und N Untergruppen von G.

(i) Gilt $U \cap N = \{e\}$, dann hat jedes Element $g \in UN$ eine eindeutige Darstellung der Form $g = un$, mit $u \in U$ und $n \in N$.

(ii) Gilt $U \subseteq N$, dann folgt $UN = N$.

(iii) Gilt $UN = NU$, dann ist UN eine Untergruppe von G. Ersteres ist insbesondere dann gegeben, wenn N ein Normalteiler von G ist.

(iv) Sind N und U beides Normalteiler von G, dann folgt $UN \trianglelefteq G$.

Beweis: zu (i) Sei $g \in UN$. Die Existenz einer Darstellung der angegebenen Form ist auf Grund der Definition des Komplexprodukts offensichtlich. Nehmen wir nun an, es gibt $u, u' \in U$ und $n, n' \in N$ mit $g = un = u'n'$. Dann kann die Gleichung $un = u'n'$ umgeformt werden zu $(u')^{-1}u = n'n^{-1}$. Dieses Produkt liegt in $U \cap N = \{e\}$. Es folgt $(u')^{-1}u = e$ und $n'n^{-1} = e$, also $u = u'$ und $n = n'$.

zu (ii) Ist $g \in N$, dann gilt $g = e_G g \in UN$. Liegt umgekehrt g in UN, dann gibt es $u \in U$ und $n \in N$ mit $g = un$. Da N als Untergruppe von G unter der Verknüpfung abgeschlossen ist und u, n in N liegen, folgt $g = un \in N$.

zu (iii) Wir beweisen die Untergruppen-Eigenschaft von UN unter der gegebenen Voraussetzung. Zunächst ist das Neutralelement $e_G = e_G e_G$ wegen $e_G \in U$ und $e_G \in N$ in UN enthalten. Seien nun $g, g' \in UN$ vorgegeben. Dann gibt es $u, u' \in U$ und $n, n' \in N$ mit $g = un$ und $g' = u'n'$. Auf Grund der Voraussetzung finden wir ein $u'' \in U$ und $n'' \in N$ mit $nu' = u''n''$, so dass das Element

$$gg' \quad = \quad (un)(u'n') \quad = \quad u(nu')n' \quad = \quad u(u''n'')n' \quad = \quad (uu'')(n''n')$$

in UN liegt. Aus $g^{-1} = (un)^{-1} = n^{-1}u^{-1} \in NU$ und $NU = UN$ folgt auch $g^{-1} \in UN$.

Sei nun N ein Normalteiler von G und $g \in UN$. Dann gibt es Elemente $u \in U$ und $n \in N$ mit $g = un$. Auf Grund der Normalteiler-Eigenschaft gilt $uN = Nu$, es existiert also ein $n' \in N$ mit $un = n'u$. Dies zeigt, dass g in NU enthalten ist, und wir haben damit die Inklusion $UN \subseteq NU$ bewiesen. Der Nachweis der Inklusion $NU \subseteq UN$ funktioniert analog.

zu (iv) Sei $g \in G$ beliebig. Um zu zeigen, dass UN Normalteiler von G ist, müssen wir die Inklusion $g(UN)g^{-1} \subseteq UN$ nachrechnen. Ist $h \in g(UN)g^{-1}$, dann gibt es Elemente $u \in U$ und $n \in N$ mit $h = g(un)g^{-1}$. Da U Normalteiler von G ist, gilt $gug^{-1} \in U$, und aus $N \trianglelefteq G$ folgt $gng^{-1} \in G$. Insgesamt erhalten wir $h = g(un)g^{-1} = (gug^{-1})(gng^{-1}) \in UN$. □

Selbst wenn U und N beides Untergruppen von G sind, braucht das Komplexprodukt UN im Allgemeinen keine Untergruppe von G zu sein. Als Beispiel betrachten wir $G = S_3$, $U = \langle(1\ 2)\rangle$ und $N = \langle(1\ 3)\rangle$. Dann ist $UN = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$. Nach dem Satz von Lagrange kann diese vierelementige Teilmenge keine Untergruppe der sechselementigen Gruppe S_3 sein.

In § 1 hatten wir die Diedergruppen D_n für $n \geq 3$ als Symmetriegruppen des regelmäßigen n-Ecks definiert. Mit dem soeben eingeführten Konzept des Komplexprodukts können wir nun auf einfache Art nachweisen, dass die in § 1 angegebene Menge von Elementen eine Untergruppe der orthogonalen Gruppe $\mathcal{O}(2)$ bildet. Als weiteres Hilfsmittel benötigen wir noch den folgenden Begriff.

Definition 4.21 Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann nennt man $N_G(U) = \{g \in G \mid gUg^{-1} = U\}$ den ***Normalisator*** von U in G.

Die Bedeutung des Normalisators wird durch die folgende Proposition deutlich.

Proposition 4.22 Sei G eine Gruppe und U eine Untergruppe. Dann ist $N_G(U)$ die größte Untergruppe H von G mit der Eigenschaft, dass U Normalteiler von H ist.

Beweis: Die Untergruppen-Eigenschaft von $N_G(U)$ haben wir in den Übungen nachgewiesen; wir werden sie später im Kapitel über Gruppenoperationen noch einmal auf einem anderen Weg herleiten. Für jedes $g \in N_G(U)$ gilt $gUg^{-1} = U$ nach Definition von $N_G(U)$. Dies zeigt, dass $U \trianglelefteq N_G(U)$ ist. Sei nun H eine beliebige Untergruppe von G mit der Eigenschaft $U \trianglelefteq H$. Für jedes $h \in H$ gilt dann $hUh^{-1} = U$ und somit $h \in N_G(U)$. Also ist H tatsächlich in $N_G(U)$ enthalten. □

In § 1 hatten wir die Bezeichnung ρ_n für die $\frac{2\pi}{n}$-Drehung um den Punkt $(0,0)$ und τ für die Spiegelung an der x-Achse eingführt. Wie man leicht überprüft, gilt $\mathrm{ord}(\rho_n) = n$ und $\mathrm{ord}(\tau) = 2$. Nach Folgerung 3.4 gilt für die erzeugten zyklischen Untergruppen somit $\langle \rho_n \rangle = \{\rho_n^k \mid 0 \leq k < n\}$ und $\langle \tau \rangle = \{\tau^0, \tau^1\}$. Das Komplexprodukt dieser beiden zyklischen Untergruppen von $\mathcal{O}(2)$ ist somit gegeben durch

$$\langle \rho_n \rangle \langle \tau \rangle \quad = \quad \{\rho_n^k \mid 0 \leq k < n\} \cup \{\rho_n^k \tau \mid 0 \leq k < n\} \quad ;$$

dies sind genau die in § 1 angegebenen Elemente. Um zu zeigen, dass das Komplexprodukt eine Untergruppe von $\mathcal{O}(2)$ ist, genügt es nach Lemma 4.20 zu überprüfen, dass $\langle \rho_n \rangle$ ein Normalteiler von $\langle \rho_n, \tau \rangle$ ist. Dazu wiederum reicht es nach Proposition 4.22 nachzuweisen, dass ρ_n und τ beide im Normalisator $N_{\langle \rho_n, \tau \rangle}(\langle \rho_n \rangle)$ enthalten sind, denn daraus folgt, dass $\langle \rho_n, \tau \rangle$ mit dem Normalisator übereinstimmt. Das Element ρ_n ist wegen $\rho_n \in \langle \rho_n \rangle$ offensichtlich im Normalisator enthalten. Für τ verwenden wir die aus § 1 bekannte Gleichung $\tau \rho_n^{-k} \tau = \rho_n^k$ für $0 \leq k < n$, die wegen $\tau = \tau^{-1}$ zu $\tau \rho_n^k \tau^{-1} = \rho_n^{-k}$ umgeformt werden kann. Diese zeigt, dass $\tau \langle \rho_n \rangle \tau^{-1}$ mit $\langle \rho_n \rangle$ übereinstimmt und τ somit auch im Normalisator enthalten ist.

Als weitere Anwendungen des Komplexprodukts führen wir die folgenden Begriffe ein.

Definition 4.23 Sei G eine Gruppe, und seien U, N Untergruppen von G. Wir bezeichnen G als ***inneres direktes Produkt*** von U und N, wenn U und N beides Normalteiler von G sind und $G = UN$ sowie $U \cap N = \{e\}$ gilt. Ist lediglich N eine Normalteiler von G, aber nicht notwendigerweise die Untergruppe U, dann spricht man von einem inneren ***semidirekten*** Produkt.

Die inneren semidirekten Produkte werden wir erst später genauer untersuchen. Die wesentliche Motivation für die Einführung der inneren direkten Produkte besteht in der Verbindung zu den äußeren direkten Produkten der Form $G \times H$, die wir bereits in § 1 definiert haben.

Proposition 4.24 Sei G eine Gruppe und inneres direktes Produkt ihrer Untergruppen U und N. Dann gilt $G \cong U \times N$.

Beweis: Wir zeigen zunächst, dass für alle $u \in U$ und $n \in N$ die Gleichung $un = nu$ erfüllt ist. Wir beweisen die äquivalente Gleichung $unu^{-1}n^{-1} = e$. Weil N ein Normalteiler von G ist, gilt $unu^{-1} \in N$, und somit liegt auch $unu^{-1}n^{-1}$ in N. Andererseits ist auch U ein Normalteiler von G. Es folgt $nu^{-1}n^{-1} \in U$ und $unu^{-1}n^{-1} \in U$. Insgesamt gilt also $unu^{-1}n^{-1} \in U \cap N = \{e\}$, also $unu^{-1}n^{-1} = e$.

Nun zeigen wir, dass durch die Abbildung $\phi : U \times N \to G$, $(u,n) \mapsto un$ ein Isomorphismus von Gruppen definiert ist. Zum Nachweis der Homomorphismus-Eigenschaft seien $(u_1,n_1),(u_2,n_2) \in U \times N$ vorgegeben. Durch Anwendung der zu Beginn bewiesenen Gleichung $u_1n_2 = n_2u_1$ erhalten wir

$$\begin{aligned}\phi(u_1,n_1)\phi(u_2,n_2) &= (u_1n_1)(u_2n_2) = u_1(n_1u_2)n_2 = u_1(u_2n_1)n_2 = \\ (u_1u_2)(n_1n_2) &= \phi(u_1u_2,n_1n_2) = \phi((u_1,n_1)(u_2,n_2)).\end{aligned}$$

Jedes $g \in G$ kann als Produkt $g = un$ mit $u \in U$ und $n \in N$ dargestellt werden. Dies beweist die Surjektivität von ϕ, und die Eindeutigkeit der Darstellung folgt direkt aus Teil (i) von Lemma 4.20. □

Wir bemerken noch, dass die Bijektivität der Abbildung $U \times N \to UN$, $(u,n) \mapsto un$ auch dann noch gegeben ist, wenn U und N nur Untergruppen, aber keine Normalteiler von G sind. Auch dies ist eine direkte Folgerung aus Teil (i) von Lemma 4.20. Sind U und N insbesondere *endliche* Untergruppen von G mit $U \cap N = \{e\}$, dann gilt also $|UN| = |U| \cdot |N|$.

Sei G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Existiert ein weiterer Normalteiler U von G mit $G = NU$ und $N \cap U = \{e_G\}$, dann kann, wie wir soeben gesehen haben, die Gruppe G in die Bestandteile N und U „zerlegt“ werden. Aber auch, wenn ein solcher Normalteiler U nicht existiert, ist eine Zurückführung der Struktur von G auf „einfachere“ Bestandteile möglich.

Hier kommen die sog. Faktorgruppen ins Spiel. Für die Definition der Verknüpfung auf diesen Gruppen wiederholen wir einen wichtigen, bereits aus der Linearen Algebra bekannten, Satz.

Satz 4.25 Seien X und Y Mengen und sei $\equiv$ eine Äquivalenzrelation auf X.

(i) Ist $f : X \to Y$ eine Abbildung mit der Eigenschaft, dass für alle $x, x' \in X$ aus $x \equiv x'$ jeweils $f(x) = f(x')$ gilt, dann existiert eine eindeutig bestimmte Abbildung $\bar{f} : X/\equiv \to Y$ mit $\bar{f}([x]) = f(x)$ für alle $x \in X$.

(ii) Ist $g : X \times X \to Y$ eine Abbildung mit der Eigenschaft, dass für alle $x, x' \in X$ und $y, y' \in X$ aus $x \equiv x'$ und $y \equiv y'$ jeweils $g(x,y) = g(x',y')$ folgt, dann existiert eine eindeutig bestimmte Abbildung $\bar{g} : (X/\equiv) \times (X/\equiv) \to Y$ mit $\bar{g}([x],[y]) = g(x,y)$ für alle $x, y \in X$

Man nennt $\bar{f}$ bzw. $\bar{g}$ die durch f bzw. g ***induzierte*** Abbildung.

Beweis: Die Eindeutigkeit von $\bar{f}$ und $\bar{g}$ ist jeweils offensichtlich, denn durch die angegebenen Bedingungen sind $\bar{f}$ und $\bar{g}$ auf ihrem Definitionsbereich eindeutig festgelegt. Zum Nachweis der Existenz verwenden wir ein Repräsentantensystem $R \subseteq X$ der Äquivalenzklassen. Für jedes $x \in X$ sei $x_R \in R$ jeweils das eindeutig bestimmte Element

in der Äquivalenzklasse von x. Dann definieren wir $\bar{f}$ und $\bar{g}$ durch $\bar{f}([x]) = f(x_R)$ und $\bar{g}([x],[y]) = g(x_R, y_R)$. (Diese Definitionen sind eindeutig auf Grund der Tatsache, dass x_R und y_R jeweils nur von den Äquivalenzklassen $[x],[y] \in X/\equiv$ abhängen, nicht aber von der Wahl der Elemente x und y innerhalb ihrer jeweiligen Klasse.) Auf Grund unserer Voraussetzungen an die Abbildungen f und g gilt für alle $x, y \in X$ jeweils $f(x_R) = f(x)$ und $g(x_R, y_R) = g(x, y)$, insgesamt also $\bar{f}([x]) = f(x)$ und $\bar{g}([x],[y]) = g(x, y)$ wie gefordert. □

Die Gültigkeit des Satzes ist keineswegs so selbstverständlich, wie es auf den ersten Blick erscheint. Beispielsweise existiert *keine* Abbildung $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ mit $f(a+3\mathbb{Z}) = a+4\mathbb{Z}$ für alle $a \in \mathbb{Z}$. Denn aus der Existenz einer solchen Abbildung würde sich auf Grund der Gleichung $2+3\mathbb{Z} = 5+3\mathbb{Z}$ in $\mathbb{Z}/3\mathbb{Z}$ die Gleichung $2+4\mathbb{Z} = f(2+3\mathbb{Z}) = f(5+3\mathbb{Z}) = 5+4\mathbb{Z}$ ergeben, im Widerspruch zu $5+4\mathbb{Z} = 1+4\mathbb{Z} \neq 2+4\mathbb{Z}$.

Proposition 4.26 Sei G eine Gruppe und N ein Normalteiler von G. Dann gibt es auf der Menge G/N eine eindeutig bestimmte Verknüpfung $\cdot$ mit der Eigenschaft

$$(gN)\cdot(hN) \quad = \quad (gh)N \qquad \text{für alle} \quad g,h \in G.$$

Beweis: Dies erhält man unmittelbar durch Anwendung von Satz 4.25 (ii) auf die Relation $\equiv_\ell$ gegeben durch $g \equiv_\ell g' \Leftrightarrow g' \in gN$ für alle $g, g' \in G$ und auf die Abbildung $G \times G \to G/N$, $(g,h) \mapsto (gh)N$. Die Voraussetzungen des Satzes sind erfüllt, denn sind $g, g', h, h' \in G$ mit $g \equiv_\ell g'$ und $h \equiv_\ell h'$ vorgegeben, dann gibt es Element $n_1, n_2 \in N$ mit $g' = gn_1$ und $h' = hn_2$. Auf Grund der Normalteiler-Eigenschaft ist $n' = h^{-1}n_1h$ in N enthalten. Stellen wir diese Gleichung zu $n_1h = hn'$ um, so erhalten wir $g'h' = (gn_1)(hn_2) = (gh)n'n_2 \in (gh)N$ und somit $g'h' \equiv_\ell gh$. □

Man kann übrigens zeigen, dass für eine beliebige Untergruppe U die Existenz einer Verknüpfung $\cdot$ auf der Menge G/U mit $(gU)\cdot(hU) = (gh)U$ äquivalent zur Normalteiler-Eigenschaft von U ist. Den Beweis dieser Aussage sehen wir uns in den Übungen an.

Um die soeben bewiesene Proposition zu illustrieren, betrachten wir als Beispiel die Gruppe $G = S_3$ und die Untergruppe $N = \langle(1\ 2\ 3)\rangle$. Dann besteht die Menge G/N der Linksnebenklassen aus den beiden Elementen

$$\mathrm{id}\ N = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} \quad , \quad (1\ 2)N = \{(1\ 2), (1\ 2)(1\ 2\ 3), (1\ 2)(1\ 3\ 2)\} = \{(1\ 2), (2\ 3), (1\ 3)\}.$$

Wegen $(G : N) = 2$ ist N ein Normalteiler von G. Für die soeben definierte Verknüpfung $\cdot$ auf G/N gilt beispielsweise $(\mathrm{id}\ N)\cdot((1\ 2)N) = (\mathrm{id} \circ (1\ 2))N = (1\ 2)N$ und $((1\ 2)N)\cdot((1\ 2)N) = ((1\ 2)\circ(1\ 2)) = \mathrm{id}\ N$. Insgesamt ist die Verknüpfungstabelle von $\cdot$ gegeben durch

$\cdot$	id N	$(1\ 2)N$
id N	id N	$(1\ 2)N$
$(1\ 2)\ N$	$(1\ 2)N$	id N

Stellt man die Nebenklasse $(1\ 2)N$ durch andere Repräsentanten dar, so liefert die Verknüpfung $\cdot$ dennoch dasselbe Ergebnis. Beispielsweise gilt $(1\ 2)N = (2\ 3)N = (1\ 3)N$, und man erhält entsprechend $((2\ 3)N)\cdot((1\ 3)N) = ((2\ 3)\circ(1\ 3))N = (1\ 2\ 3)N = N$. Als nächstes zeigen wir nun, dass die Verknüpfung $\cdot$ auf der Menge G/N eine Gruppenstruktur definiert.

Satz 4.27 Sei G eine Gruppe und N ein Normalteiler. Dann ist die Menge G/N der Linksnebenklassen mit der Verknüpfung $gN \cdot hN = (gh)N$ eine Gruppe, die sogenannte ***Faktorgruppe*** von G modulo N. Die Abbildung $\pi_N : G \to G/N$, $g \mapsto gN$ ist ein Epimorphismus von Gruppen, der sog. ***kanonische Epimorphismus***.

Beweis: Wir müssen für die gegebene Verknüpfung die Gruppenaxiome überprüfen. Zum Nachweis der Assoziativität seien $g_1, g_2, g_3 \in G$ vorgegeben. Dann gilt

$$\begin{aligned}(g_1N \cdot g_2N) \cdot g_3N &= (g_1g_2)N \cdot g_3N = ((g_1g_2)g_3)N = (g_1(g_2g_3))N = \\ g_1N \cdot (g_2g_3)N &= g_1N \cdot (g_2N \cdot g_3N).\end{aligned}$$

Die Nebenklasse $\bar{e} = e_GN = N$ übernimmt die Rolle des Neutralelements, denn für alle $g \in G$ gilt $gN \cdot e_GN = (ge_G)N = gN$ und $e_GN \cdot gN = (e_Gg)N = gN$. Außerdem gilt $gN \cdot g^{-1}N = (gg^{-1})N = e_GN = \bar{e}$ und ebenso $g^{-1}N \cdot gN = e_GN = \bar{e}$, also ist $g^{-1}N$ das zu gN inverse Element in G/N.

Überprüfen wir nun die angegebenen Eigenschaften der Abbildung π_N. Für alle $g, g' \in G$ gilt $\pi_N(gg') = (gg')N = (gN)(g'N) = \pi_N(g)\pi_N(g')$. Somit ist π_N ein Homomorphismus. Ist $gN \in G/N$ vorgegeben, dann gilt $\pi_N(g) = gN$. Also ist π_N surjektiv. □

Wie wir bereits wissen, sind Homomorphismen nicht nur mit der Gruppenverknüpfung, sondern auch mit der Potenzierung von Elementen verträglich. Damit können wir eine naheliegende Potenzierungsregel für Elemente in Faktorgruppen herleiten: Für $g \in G$ und $n \in \mathbb{Z}$ gilt $(gN)^n = \pi_N(g)^n = \pi_N(g^n) = (g^n)N$.

Ein wichtiges Beispiel für Faktorgruppen sind die bereits bekannten ***Restklassengruppen***. Sei $G = (\mathbb{Z}, +)$, $n \in \mathbb{N}$ und $U = \langle n \rangle = n\mathbb{Z}$. Dann sind die Elemente von $G/U = \mathbb{Z}/n\mathbb{Z}$ die schon zuvor erwähnten Restklassen der Form $a + n\mathbb{Z}$ mit $a \in \mathbb{Z}$. Wir bemerken noch, dass jede zyklische Grupper der Ordnung n isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$ ist. Dies ergibt sich unmittelbar aus Folgerung 4.13.

Für viele Anwendungen ist es nützlich, Faktorgruppen mit anderen, möglicherweise „natürlicher“ erscheinenden Gruppen zu identifizieren. Das zentrale Hilfsmittel dazu ist der Homomorphiesatz, dem wir uns nun zuwenden.

Proposition 4.28 Sei $\phi : G \to H$ ein Gruppen-Homomorphismus und $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \ker(\phi)$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\bar{\phi} : G/N \to H$ mit

$$\bar{\phi}(gN) = \phi(g) \qquad \text{für alle } g \in G.$$

Man nennt $\bar{\phi}$ den durch ϕ ***induzierten*** Homomorphismus.

Beweis: Die Eindeutigkeit von $\bar{\phi}$ ist klar, weil durch die Gleichung die Bilder aller Elemente von G/N festgelegt sind. Zum Beweis der Existenz wenden wir wiederum Satz 4.25 an, diesmal Teil (i). Demnach genügt es zu zeigen, dass für alle $g, g' \in G$ mit $g \equiv_\ell g'$ jeweils $\phi(g) = \phi(g')$ gilt. Aber dies ist der Fall, denn $g \equiv_\ell g'$ ist nach Definition äquivalent zu $g' \in gN$, was wiederum mit $(g')^{-1}g \in N$ gleichbedeutend ist. Wegen $N \subseteq \ker(\phi)$ folgt daraus $\phi(g')^{-1}\phi(g) = \phi((g')^{-1}g) = e_H$ und somit $\phi(g) = \phi(g')$. Nun überprüfen wir noch, dass $\bar{\phi}$ ein Homomorphismus ist. Seien $\bar{g}$, $\bar{h} \in G/N$ und $g, h \in G$ mit $\bar{g} = gN$ und $\bar{h} = hN$. Dann gilt $\bar{\phi}(\bar{g}\bar{h}) = \bar{\phi}((gN)(hN)) = \bar{\phi}((gh)N) = \phi(gh) = \phi(g)\phi(h) = \bar{\phi}(gN)\bar{\phi}(hN) = \bar{\phi}(\bar{g})\bar{\phi}(\bar{h})$. □

Satz 4.29 *(Homomorphiesatz für Gruppen)*
Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus

$$\bar{\phi} : G/\ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi).$$

Ist der Homomorphismus ϕ surjektiv, dann erhält man also einen Isomorphismus $G/\ker(\phi) \cong H$.

Beweis: Nach Satz 4.18 (iii) ist $N = \ker(\phi)$ ein Normalteiler von G. Anwendung von Proposition 4.28 auf diesen Normalteiler liefert einen von ϕ induzierten Homomorphismus $\bar{\phi} : G/N \to H$. Auf Grund der Gleichung $\bar{\phi}(gN) = \phi(g)$ für alle $g \in G$ stimmen $\mathrm{im}(\phi)$ und $\mathrm{im}(\bar{\phi})$ überein. Wir können $\bar{\phi}$ somit als *surjektiven* Homomorphismus $G/N \to \mathrm{im}(\phi)$ auffassen. Zusätzlich ist $\bar{\phi}$ injektiv. Ist nämlich $\bar{g} \in \ker(\bar{\phi})$, $\bar{g} = gN$ mit $g \in N$, dann gilt $\phi(g) = \bar{\phi}(\bar{g}) = e_H$. Es folgt $g \in \ker(\phi)$, also $g \in N$, und damit ist $\bar{g} = gN = e_G N = \bar{e}$ das Neutralelement in G/N. Es gilt also $\ker(\bar{\phi}) = \{\bar{e}\}$. Nach Proposition 4.9 folgt daraus die Injektivität von $\bar{\phi}$. □

Wir betrachten nun eine Reihe von Anwendungsbeispielen für den Homomorphiesatz.

(i) Sei G eine Gruppe und $\phi : G \to \{e_G\}$ gegeben durch $g \mapsto e_G$ für alle $g \in G$. Dann ist $\mathrm{im} = \{e_G\}$, und ϕ induziert einen Isomorphismus $G/G \cong \{e_G\}$.

(ii) Die identische Abbildung $\mathrm{id}_G : G \to G$ hat den Kern $\{e_G\}$ und die gesamte Gruppe G als Bild. Sie induziert also einen Isomorphismus $G/\{e_G\} \cong G$.

(iii) Sei K ein Körper und $n \in \mathbb{N}$. Der Determinanten-Homomorphismus $\det : \mathrm{GL}_n(K) \to K^\times$ besitzt, wie wir in § 2 gesehen haben, die Gruppe $\mathrm{SL}_n(K)$ als Kern. Außerdem ist sie surjektiv, denn für jedes $a \in K^\times$ gibt es eine invertierbare Matrix mit Determinante a, beispielsweise die Diagonalmatrix mit den Einträgen $a, 1, ..., 1$. Somit liefert der Homomorphiesatz einen Isomorphismus $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^\times$.

(iv) Die Signumsfunktion $\mathrm{sgn} : S_n \to \{\pm 1\}$ hat als Kern die Untergruppe $A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$, die bereits aus der Linearen Algebra bekannte alternierende Gruppe. Außerdem ist sie für $n \geq 2$ surjektiv, wegen $\mathrm{sgn}(\mathrm{id}) = 1$ und $\mathrm{sgn}((1\ 2)) = -1$. Also induziert sgn einen Isomorphismus $S_n/A_n \cong \{\pm 1\}$.

Eine wichtige Anwendung der Faktorgruppen besteht darin, dass sie in vielen Fällen das Studium der Untergruppen einer Gruppe G vereinfachen. Ist nämlich $N \trianglelefteq G$, dann korrespondieren die Untergruppen von G/N, wie wir gleich sehen werden, zu bestimmten Untergruppen der Gruppe G. Dies ist der Inhalt des Korrespondenzsatzes, den wir als nächstes beweisen werden. Da G/N in der Regel eine einfachere Struktur als G besitzt, lassen sich die Untergruppen dort im allgemeinen leichter bestimmen.

Proposition 4.30 Sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $\pi_N : G \to G/N$ der kanonische Epimorphismus.

(i) Ist U eine Untergruppe von G, dann gilt $\pi_N^{-1}(\pi_N(U)) = UN$.

(ii) Ist $\bar{U}$ eine Untergrupe von G/N, dann gilt $\pi_N(\pi_N^{-1}(\bar{U})) = \bar{U}$.

Beweis: zu (i) Sei $g \in \pi_N^{-1}(\pi_N(U))$. Dann liegt $\pi_N(g)$ in $\pi_N(U)$, es gibt also ein $u \in U$ mit $\pi_N(g) = \pi_N(u)$. Für das Element $n = u^{-1}g$ gilt $nN = \pi_N(n) = \pi_N(u)^{-1}\pi_N(g) = \bar{e} = N$, also ist $nN = N$ und insbesondere $n \in N$. Es

folgt $g = un \in UN$. Ist umgekehrt $g \in UN$, dann gibt es Elemente $u \in U$ und $n \in N$ mit $g = un$. Wir erhalten $\pi_N(g) = \pi_N(un) = \pi_N(u)\pi_N(n) = \pi_N(u)\bar{e} = \pi_N(u)$, und es folgt $g \in \pi_N^{-1}(\pi_N(U))$.

zu (ii) Die Inklusion $\pi_N(\pi_N^{-1}(\bar{U})) \subseteq \bar{U}$ folgt unmittelbar aus der Definition von Bild- und Urbildmenge. Für die umgekehrte Inklusion sei $\bar{g} \in \bar{U}$ vorgegeben und $g \in G$ mit $gN = \bar{g}$. Dann gilt $\pi_N(g) = \bar{g}$ und somit $g \in \pi_N^{-1}(\bar{U})$ nach Definition der Urbildmenge $\pi_N^{-1}(\bar{U})$. Es folgt $\bar{g} = \pi_N(g) \in \pi_N(\pi_N^{-1}(\bar{U}))$. □

Satz 4.31 *(Korrespondenzsatz für Gruppen)*

Sei G eine Gruppe, N ein Normalteiler, $\bar{G} = G/N$ und $\pi_N : G \to \bar{G}$ der kanonische Epimorphismus. Ferner sei $\bar{\mathcal{G}}$ die Menge der Untergruppen von $\bar{G}$ und $\mathcal{G}_N$ die Menge der Untergruppen U von G mit $U \supseteq N$. Dann sind die beiden Abbildungen

$$\mathcal{G}_N \longrightarrow \bar{\mathcal{G}}\ ,\ U \mapsto \pi_N(U) \qquad \text{und} \qquad \bar{\mathcal{G}} \longrightarrow \mathcal{G}_N\ ,\ \bar{U} \mapsto \pi_N^{-1}(\bar{U})$$

bijektiv und zueinander invers. Außerdem gilt:

(i) Für $U, V \in \mathcal{G}_N$ gilt $U \subseteq V$ genau dann, wenn $\pi_N(U) \subseteq \pi_N(V)$ erfüllt ist.

(ii) Genau dann ist $U \in \mathcal{G}_N$ ein Normalteiler von G, wenn $\pi_N(U)$ ein Normalteiler von $\bar{G}$ ist.

(iii) Ist $U \in \mathcal{G}_N$ von endlichem Index in G und $\bar{U} = \pi_N(U)$, dann gilt $(G : U) = (\bar{G} : \bar{U})$.

Beweis: Sei $U \in \mathcal{G}_N$, also eine Untergruppe von G mit $U \supseteq N$. Dann gilt $\pi_N^{-1}(\pi_N(U)) = UN = NU = U$, wobei wir im ersten Schritt Proposition 4.30 (i), im zweiten Lemma 4.20 (iii) und im dritten Lemma 4.20 (ii) verwendet haben. Umgekehrt liefert Teil (ii) von Proposition 4.30 die Gleichung $\pi_N(\pi_N^{-1}(\bar{U})) = \bar{U}$ für alle Untergruppen $\bar{U}$ von $\bar{G}$.

zu (i) Seien $U, V \in \mathcal{G}_N$ mit $U \subseteq V$. Dann gilt offenbar $\pi_N(U) \subseteq \pi_N(V)$. Ist umgekehrt $\pi_N(U) \subseteq \pi_N(V)$ vorausgesetzt, dann folgt $U = \pi_N^{-1}(\pi_N(U)) \subseteq \pi_N^{-1}(\pi_N(V)) = V$.

zu (ii) Weil der kanonische Homomorphismus π_N surjektiv ist, folgen „⇒“ bzw. „⇐“ aus Satz 4.18 (iv) bzw. (iii).

zu (iii) Wir zeigen, dass durch $\bar{g}\bar{U} \mapsto \pi_N^{-1}(\bar{g}\bar{U})$ eine Bijektion zwischen den Linksnebenklassen von $\bar{U}$ und den Linksnebenklassen von U gegeben ist. Sei $\bar{g} \in \bar{G}$ und $g \in G$ ein Element mit $\pi_N(g) = \bar{g}$. Dann gilt $gU = \pi_N^{-1}(\bar{g}\bar{U})$. Ist nämlich $gu \in gU$ mit $u \in U$ vorgegeben, dann folgt $\pi_N(gu) = \pi_N(g)\pi_N(u) = \bar{g}\pi_N(u) \in \bar{g}\bar{U}$ und somit $gu \in \pi_N^{-1}(\bar{g}\bar{U})$. Ist umgekehrt $h \in \pi_N^{-1}(\bar{g}\bar{U})$ vorgegeben, dann folgt $\pi_N(h) \in \bar{g}\bar{U}$, also $\pi_N(h) = \bar{g}\bar{u}$ für ein $\bar{u} \in \bar{U}$. Bezeichnet $u \in U$ ein Urbild von $\bar{u}$, dann gilt also $hN = guN$. Es gibt also ein $n \in N$ mit $h = gun$, und wegen $U \supseteq N$ folgt $h \in gU$.

Es ist unmittelbar klar, dass die Zuordnung surjektiv ist, denn jede Nebenklasse von U hat die Form gU mit einem $g \in G$, und folglich ist $gU = \pi_N^{-1}(\bar{g}\bar{U})$ mit $\bar{g} = \pi_N(g)$. Auch die Injektivität ist offensichtlich. Sind nämlich $\bar{g}_1\bar{U}$ und $\bar{g}_2\bar{U}$ zwei verschiedene Nebenklassen in $\bar{G}/\bar{U}$, dann sind sie als Teilmengen von $\bar{G}$ disjunkt. Die Urbildmengen $\pi_N^{-1}(\bar{g}_1\bar{U})$ und $\pi_N^{-1}(\bar{g}_2\bar{U})$ müssen dann erst recht disjunkt sein, und insbesondere voneinander verschieden. □

Wir verwenden nun den Korrespondenzsatz für Gruppen, um alle Untergruppen von $(\mathbb{Z}, +)$ zu bestimmen, die die Untergruppe $\langle 44 \rangle$ enthalten. Sei $\pi_{\langle 44 \rangle} : \mathbb{Z} \to \mathbb{Z}/44\mathbb{Z}$ der kanonische Epimorphismus. Die Gruppe $(\mathbb{Z}/44\mathbb{Z}, +)$ ist eine zyklische Gruppe der Ordnung 44. Durch Satz 3.11 haben wir eine vollständige Beschreibung der Untergruppen von $(\mathbb{Z}/44\mathbb{Z}, +)$ zur Verfügung: Zu jedem Teiler der Gruppenordnung 44 gibt es eine eindeutig bestimmte Untergruppe, und diese werden erzeugt durch gewisse Potenzen des Erzeugers $\bar{1}$ von $\mathbb{Z}/44\mathbb{Z}$. Die vollständige Liste der

Untergruppen ist also gegeben durch

$$\langle\bar{1}\rangle\ ,\ \langle\bar{2}\rangle\ ,\ \langle\bar{4}\rangle\ ,\ \langle\overline{11}\rangle\ ,\ \langle\overline{22}\rangle\ ,\ \langle\overline{44}\rangle = \{\bar{0}\}.$$

Der Korrespondenzsatz besagt nun, dass es korrespondierend zu diesen sechs Untergruppen von $\mathbb{Z}/44\mathbb{Z}$ genau sechs Untergruppen von $(\mathbb{Z},+)$ gibt, die $\langle 44\rangle$ enthalten. Offenbar ist $\langle 44\rangle$ in $\langle a\rangle$ enthalten für die Zahlen $a \in \{1,2,4,11,22,44\}$, denn jedes ganzzahlige Vielfache von 44 ist auch ein Vielfaches von a für jede Zahl a in dieser Menge. Der Korrespondenzsatz liefert uns die Information, dass es keine weiteren Untergruppen U von $(\mathbb{Z},+)$ mit $U \supseteq \langle 44\rangle$ gibt.

Auch die folgenden beiden Sätze, mit denen wir dieses Kapitel abschließen, erweisen sich beim Umgang mit Faktorgruppen immer wieder als nützlich.

Satz 4.32 *(Isomorphiesätze)*

Sei G eine Gruppe, $N \trianglelefteq G$ und U eine Untergruppe von G.

(i) Dann ist $N \cap U$ ein Normalteiler von U, und es gilt $U/(N \cap U) \cong (UN)/N$.

(ii) Ist auch $U \trianglelefteq G$ und gilt $U \supseteq N$, dann gilt $G/U \cong (G/N)/(U/N)$.

Beweis: zu (i) Zunächst bemerken wir, dass UN nach Lemma 4.20 eine Untergruppe von G ist, und aus $N \trianglelefteq G$ folgt $N \trianglelefteq UN$. Wir wenden nun den Homomorphiesatz, Satz 4.29, an auf den Homomorphismus $\phi : U \to (UN)/N$, $u \mapsto uN$ der durch Komposition der Inklusionsabbildung $U \hookrightarrow G$ mit dem kanonischen Epimorphismus π_N zu Stande kommt. Diese Abbildung ist surjektiv, denn jedes Element in $(UN)/N$ hat die Form $(un)N$ mit $u \in U$ und $n \in N$. Wegen $u^{-1}(un) = n \in N$ gilt $(un)N = uN$, und es folgt $\phi(u) = uN = (un)N$. Der Kern von ϕ ist genau die Untergrupe $N \cap U$, denn für alle $u \in U$ gilt die Äquivalenz

$$u \in \ker(\phi) \quad\Leftrightarrow\quad \phi(u) = N \quad\Leftrightarrow\quad uN = N \quad\Leftrightarrow\quad u \in N \quad\Leftrightarrow\quad u \in N \cap U.$$

Also liefert der Homomorphiesatz tatsächlich den angegebenen Isomorphismus.

zu (ii) Nach Definition gilt $U/N = \pi_N(U)$ mit dem kanonischen Epimorphismus $\pi_N : G \to G/N$. Aus $U \trianglelefteq G$ und Satz 4.18 (iv) folgt somit, dass U/N ein Normalteiler von G/N ist. Wir wenden nun den Homomorphiesatz auf die Abbildung $\psi : G \to (G/N)/(U/N)$, $g \mapsto gN(U/N)$ an, die durch Hintereinanderschaltung der beiden Epimorphismen π_N und $\pi_{U/N}$ zu Stande kommt. Als Komposition zweier Epimorphismen ist auch ψ ein Epimorphismus. Damit der Homomorphiesatz das gewünschte Ergebnis liefert, müssen wir noch zeigen, dass $\ker(\psi) = U$ gilt. Tatsächlich gilt für alle $g \in G$ die Äquivalenz

$$g \in \ker(\psi) \quad\Leftrightarrow\quad \psi(g) = U/N \quad\Leftrightarrow\quad gN(U/N) = U/N \quad\Leftrightarrow\quad gN \in U/N \quad\Leftrightarrow\quad \exists\, u \in U : gN = uN \quad\Leftrightarrow$$

$$\exists\, u \in U : g^{-1}u \in N \quad\Leftrightarrow\quad \exists\, u \in U, n \in N : g^{-1}u = n \quad\Leftrightarrow\quad \exists\, u \in U, n \in N : g = un^{-1} \quad\overset{U \supseteq N}{\Leftrightarrow}\quad g \in U. \qquad \square$$

In Teil (ii) von Satz 4.32 werden tatsächlich Faktorgruppen von Faktorgruppen gebildet, ein auf den ersten Blick etwas unanschaulicher Vorgang. Wir illustrieren diese Aussage deshalb anhand eines Beispiels. Sei $G = (\mathbb{Z}, +)$. Weil G abelsch ist, sind die Untergruppen $N = \langle 6 \rangle$ und $U = \langle 2 \rangle$ Normalteiler von G, und wegen $6 = 3 \cdot 2 \in U$ gilt $N \subseteq U$. Das Bild von U unter dem kanonischen Epimorphismus besteht aus allen Vielfachen von $\bar{2} = 2 + 6\mathbb{Z}$, ist also durch $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ gegeben. Der zweite Isomorphiesatz liefert uns somit

$$\mathbb{Z}/2\mathbb{Z} \quad = \quad G/U \quad \cong \quad (G/N)/(U/N) \quad \cong \quad (\mathbb{Z}/6\mathbb{Z})/\langle \bar{2} \rangle.$$

Nach demselben Schema zeigt man leicht: Sind $m, n \in \mathbb{N}$ und ist m ein Teiler von n, dann gilt $\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/\langle \bar{m} \rangle$, mit $\bar{m} = m + n\mathbb{Z}$.

§ 5. *Endlich erzeugte abelsche Gruppen*

Zusammenfassung. In diesem Kapitel werden wir mit Hilfe der bisher entwickelten theoretischen Werkzeuge alle endlich erzeugten abelschen Gruppen bis auf Isomorphie bestimmen. Genauer zeigen wir, dass jede solche Gruppe isomorph zu einem äußeren direkten Produkt von (unendlichen und endlichen) zyklischen Gruppe ist. Insbesondere können wir dann für jedes $n \in \mathbb{N}$ eine endliche Liste $G_1, ..., G_r$ von Gruppen angeben, so dass jede abelsche Gruppe der Ordnung n zu einem der G_i isomorph ist. Dies wird am Ende des Kapitels für die Zahl $n = 100$ exemplarisch vorgeführt.

Wichtige Grundbegriffe	*Zentrale Sätze*
– freie endlich erzeugte abelsche Gruppe	– Zerlegung endlich erzeugter abelscher Gruppen in einen freien Anteil und eine endliche abelsche Gruppe
– Torsionsuntergruppen abelscher Gruppen	– Zerlegung endlicher abelscher Gruppen in ein Produkt endlicher zyklischer Gruppen
– torsionfreie abelsche Gruppe	– Chinesischer Restsatz für Gruppen

In § 2 haben wir eine Gruppe G als *endlich erzeugt* bezeichnet, wenn eine endliche Teilmenge $S \subseteq G$ mit $G = \langle S \rangle$ existiert. Im weiteren Verlauf werden wir wiederholt auf die folgende Hilfsaussage zurückgreifen.

Lemma 5.1 Seien G, H beliebige Gruppen. Ist G endlich erzeugt und existiert ein surjektiver Homomorphismus $\phi : G \to H$, dann ist auch H endlich erzeugt.

Beweis: Sei $S = \{g_1, ..., g_r\}$ ein endliches Erzeugendensystem von G. Wir zeigen, dass $\phi(S) = \{\phi(g_1), ..., \phi(g_r)\}$ ein Erzeugendensystem von H ist. Sei dazu U eine beliebige Untergruppe von H, die $\phi(S)$ enthält. Zu zeigen ist $U = H$. Nun ist $\phi^{-1}(U)$ nach Proposition 4.8 eine Untergruppe von G, und diese enthält S als Teilmenge. Wegen $G = \langle S \rangle$ folgt $\phi^{-1}(U) = G$. Aber daraus ergibt sich direkt $U = H$. Ist nämlich $h \in H$, dann existiert auf Grund der Surjektivität von ϕ ein $g \in G$ mit $\phi(g) = h$. Dieses ist zugleich in $\phi^{-1}(U)$ enthalten, und daraus folgt $h = \phi(g) \in U$. □

Von nun an sind alle in diesem Kapitel vorkommenden Gruppen abelsch und werden in additiver Schreibweise dargestellt. Für das Komplexprodukt zweier Teilmengen A, B einer Gruppe G verwenden wir entsprechend die Schreibweise $A + B$ statt AB. Für das innere direkte Produkt verwenden wir hier die folgende Notation: Wir schreiben $G = U \oplus V$, wenn U und V Untergruppen von $(G, +)$ sind und G ein inneres direktes Produkt von U und V ist. Diese Schreibweise ist nur bei abelschen Gruppen üblich. Sie erinnert an die Notation für die direkte Summen von Untervektorräumen eines K-Vektorraums V. Tatsächlich werden wir in diesem Kapitel stellenweise den Vektorraum-Begriff zu Hilfe nehmen.

Definition 5.2 Sei G eine abelsche Gruppe und $m \in \mathbb{N}$.

(i) Man nennt $G[m] = \{g \in G \mid mg = 0_G\}$ die ***m*-Torsionsuntergruppe** von G.

(ii) Die Teilmenge $\mathrm{Tor}(G) = \bigcup_{n \in \mathbb{N}} G[n]$ wird die ***Torsionsuntergruppe*** von G genannt.

Man überprüft leicht, dass sowohl $G[m]$ für jedes $m \in \mathbb{N}$ als auch $\mathrm{Tor}(G)$ tatsächlich Untergruppen von G sind. Denn offenbar ist 0_G sowohl in $G[m]$ als auch in $\mathrm{Tor}(G)$ enthalten. Seien nun $g,h \in G[m]$ vorgegeben. Dann gilt $mg = mh = 0_G$, und es folgt $m(g+h) = mg + mh = 0_G + 0_G = 0_G$ und $m(-g) = -(mg) = -0_G = 0_G$. Dies zeigt, dass auch $g+h$ und $-g$ in $G[m]$ liegen. Also ist $G[m]$ tatsächlich eine Untergruppe von G. Zum Nachweis der Untergruppen-Eigenschaft von $\mathrm{Tor}(G)$ seien nun $g,h \in \mathrm{Tor}(G)$. Dann gibt es nach Definition $m,n \in \mathbb{N}$ mit $g \in G[m]$ und $h \in G[n]$, also $mg = 0_G$ und $nh = 0_G$. Es folgt $(mn)g = n(mg) = n0_G = 0_G$ und $(mn)h = m(nh) = m0_G = 0_G$, also $g,h \in G[mn]$. Wie soeben gezeigt, sind damit auch $g+h$ und $-g$ in $G[mn]$ enthalten, und damit erst recht in $\mathrm{Tor}(G)$. Also ist auch $\mathrm{Tor}(G)$ eine Untergruppe von G. Man beachte aber, dass für eine nicht-abelsche Gruppe G die Teilmenge $\{g \in G \mid g^m = e_G\}$ im Allgemeinen keine Untergruppe von G ist!

Definition 5.3 Sei G eine endlich erzeugte abelsche Gruppe.

(i) Wir bezeichnen G als ***torsionsfrei***, wenn $\mathrm{Tor}(G) = \{0_G\}$ gilt.

(ii) Die Gruppe G ist ***frei***, wenn für ein $r \in \mathbb{N}_0$ ein Isomorphismus zwischen G und $(\mathbb{Z}^r,+)$ existiert, wobei $\mathbb{Z}^0 = \{0\}$ gesetzt wird.

Wie man unmittelbar überprüft, ist jede freie endlich erzeugte abelsche Gruppe auch torsionsfrei. Unser erstes Ziel in diesem Abschnitt ist der Nachweis, dass jede endlich erzeugte abelsche Gruppe als äußeres direktes Produkt einer freien endlich erzeugten abelschen Gruppe und einer endlichen abelschen Gruppe dargestellt werden kann.

Proposition 5.4

(i) Jede Untergruppe einer freien endlich erzeugten abelschen Gruppe ist eine freie endlich erzeugte abelsche Gruppe.

(ii) Jede torsionsfreie endlich erzeugte abelsche Grupe ist frei.

Beweis: zu (i) Da jede endlich erzeugte freie abelsche Gruppe nach Definition isomorph zu $\mathbb{Z}^n$ für ein $n \in \mathbb{N}_0$ ist, genügt es, die Aussage für Gruppen dieser Form zu beweisen. Wir zeigen durch vollständige Induktion über $n \in \mathbb{N}_0$: Ist U eine Untergruppe von $\mathbb{Z}^n$, dann ist U eine freie endlich erzeugte abelsche Gruppe. Für $n = 0$ ist $\mathbb{Z}^n = U = \{0\}$ und die Aussage somit offensichtlich. Für $n = 1$ können wir Satz 3.7 anwenden, weil $(\mathbb{Z},+)$ zyklisch ist. Die Untergruppe U stimmt demnach mit $m\mathbb{Z}$ für ein $m \in \mathbb{N}_0$ überein. Sie ist also selbst entweder unendlich zyklisch oder trivial, also isomorph zu $\mathbb{Z}^1$ oder $\mathbb{Z}^0$.

Sei nun $n \geq 1$, und setzen wir voraus, dass die Aussage für Untergruppen von $\mathbb{Z}^n$ gültig ist. Sei U eine Untergruppe von $\mathbb{Z}^{n+1}$ und $\pi : \mathbb{Z}^{n+1} \to \mathbb{Z}$ die Projektionsabbildung auf die letzte Komponente, also gegeben durch $(a_1,\ldots,a_{n+1}) \mapsto a_{n+1}$. Nach Definition gilt $\ker(\pi) = \mathbb{Z}^n \times \{0\} \cong \mathbb{Z}^n$, also ist $\ker(\pi|_U) = \ker(\pi) \cap U$ isomorph zu einer Untergruppe von $\mathbb{Z}^n$. Nach Induktionsvoraussetzung ist $\ker(\pi|_U)$ ebenfalls eine freie endlich erzeugte abelsche Gruppe und somit isomorph zu $\mathbb{Z}^r$ für ein $r \in \mathbb{N}_0$.

Das Bild $\pi(U)$ ist eine Untergruppe von $\mathbb{Z}$ und somit, wie zu Beginn gezeigt, entweder gleich $\{0\}$ oder gleich $m\mathbb{Z}$ für ein $m \in \mathbb{N}$. Im Fall $\pi(U) = \{0\}$ gilt $U = \ker(\pi_U) \cong \mathbb{Z}^r$, und wir sind fertig. Betrachten wir nun den Fall $\pi(U) = m\mathbb{Z}$ mit $m \in \mathbb{N}$. Wählen wir ein $v \in U$ mit $\pi(v) = m$, dann wird die Untergruppe $\langle v \rangle$ von U isomorph auf $m\mathbb{Z}$ abgebildet.

Wir überprüfen nun, dass U ein inneres direktes Produkt von $\ker(\pi_U)$ und $\langle v\rangle$ ist. Zunächst einmal sind $\ker(\pi|_U)$ und $\langle v\rangle$ als Untergruppen der abelschen Gruppe U Normalteiler von U. Außerdem gilt $\ker(\pi|_U)\cap\langle v\rangle = \{0_{\mathbb{Z}^{n+1}}\}$. Ist nämlich w ein Element im Durchschnitt, dann gilt $w = kv$ für ein $k\in\mathbb{Z}$. Darüber hinaus gilt $km = k\pi(v) = \pi(kv) = (\pi|_U)(w) = 0$, und somit $k = 0$ und $w = kv = 0_{\mathbb{Z}^{n+1}}$.

Für den Nachweis von $U = \ker(\pi|_U)+\langle v\rangle$ stellen wir zunächst fest, dass „$\supseteq$“ wegen $\ker(\pi|_U)\subseteq U$ und $v\in U$ offenbar erfüllt ist. Zum Beweis von „$\subseteq$“ sei $w\in U$ vorgegeben. Wegen $\pi(U) = m\mathbb{Z}$ gilt $\pi(w) = km$ für ein $k\in\mathbb{Z}$. Setzen wir nun $w' = w-kv$, dann erhalten wir $w = w'+kv$ mit $kv\in\langle v\rangle$ und $(\pi|_U)(w') = \pi(w') = \pi(w)-k\pi(v) = km-km = 0$, also $w'\in\ker(\pi|_U)$. Damit ist $w\in\ker(\pi|_U)+\langle v\rangle$ nachgewiesen. Insgesamt sind damit die Voraussetzungen von Proposition 4.24 erfüllt, und wir erhalten $U\cong\ker(\pi|_U)\times\pi(U)\cong\mathbb{Z}^r\times m\mathbb{Z}\cong\mathbb{Z}^r\times\mathbb{Z} = \mathbb{Z}^{r+1}$.

zu (ii) Sei G eine torsionsfreie endlich erzeugte abelsche Gruppe. Weiter sei S ein endliches Erzeugendensystem und $T = \{g_1,\dots,g_n\}\subseteq S$ eine *maximale* Teilmenge von S mit der Eigenschaft, dass die Abbildung $\phi : \mathbb{Z}^n\to G$, $(a_1,\dots,a_n)\mapsto a_1g_1+\dots+a_ng_n$ injektiv ist. Dann ist die Untergruppe $U = \langle T\rangle$ von G frei, denn als Abbildung $\mathbb{Z}^n\to U$ ist ϕ auch surjektiv, die Gruppe U also isomorph zu $\mathbb{Z}^n$.

Nun sei $g\in S\setminus T$ ein beliebiges Element. Auf Grund der Torsionsfreiheit gilt $ag\neq 0_G$ für alle $a\in\mathbb{Z}$, $a\neq 0$. Wegen der Maximalität von T finden wir aber einen Satz $(a,a_1,\dots,a_n)$ ganzer Zahlen mit $ag+a_1g_1+\dots+a_ng_n = 0_G$ und $a\neq 0$, $a_i\neq 0$ für ein $i\in\{1,\dots,n\}$. Wegen $ag = -a_1g_1-\dots-a_ng_n$ ist dann ag in U enthalten. Auf diese Weise erhalten wir für jedes $g\in S$ ein $a_g\in\mathbb{Z}$ mit $a_gg\in U$, wobei wir im Fall $g\in T$ jeweils $a_g = 1$ setzen können. Weil S endlich ist, können wir das kleinste gemeinsame Vielfache dieser Zahlen bilden und finden so ein $a\in\mathbb{N}$ mit $aS\subseteq U$. Wegen $G = \langle S\rangle$ gilt dann auch $aG\subseteq U$. Nun ist $\psi : G\to G$, $g\mapsto ag$ ein (auf Grund der Torsionsfreiheit) injektiver Homomorphismus, dessen Bild $\psi(G)$ in der freien abelschen Gruppe U enthalten ist. Nach Teil (i) ist $G\cong\psi(G)$ damit selbst eine freie, endlich erzeugte abelsche Gruppe. □

Satz 5.5 Ist G eine endlich erzeugte abelsche Gruppe, dann gilt $G\cong\mathbb{Z}^r\times\mathrm{Tor}(G)$ für ein $r\in\mathbb{N}_0$. Darüber hinaus ist $\mathrm{Tor}(G)$ eine endliche abelsche Gruppe.

Beweis: Zunächst bemerken wir, dass die Faktorgruppe $G/\mathrm{Tor}(G)$ eine torsionsfreie endlich erzeugte abelsche Gruppe ist. Zum Beweis sei $\bar g\in\mathrm{Tor}(G/\mathrm{Tor}(G))$ vorgegeben, mit $\bar g = g+\mathrm{Tor}(G)$ für ein $g\in G$. Dann gilt $m\bar g = 0_{G/\mathrm{Tor}(G)}$ für ein $m\in\mathbb{N}$. Es folgt $mg+\mathrm{Tor}(G) = m(g+\mathrm{Tor}(G)) = m\bar g = 0_{G/\mathrm{Tor}(G)} = 0_G+\mathrm{Tor}(G)$ und somit $mg\in\mathrm{Tor}(G)$. Daraus wiederum folgt, dass ein $n\in\mathbb{N}$ mit $(nm)g = n(mg) = 0_G$ existiert. Aber damit ist auch g in $\mathrm{Tor}(G)$ enthalten und $\bar g = g+\mathrm{Tor}(G) = 0+\mathrm{Tor}(G) = 0_{G/\mathrm{Tor}(G)}$. Insgesamt haben wir $\mathrm{Tor}(G/\mathrm{Tor}(G)) = \{0_{G/\mathrm{Tor}(G)}\}$, also die Torsionsfreiheit der Gruppe $G/\mathrm{Tor}(G)$, nachgewiesen.

Weil $G/\mathrm{Tor}(G)$ torsionsfrei ist, gilt $G/\mathrm{Tor}(G)\cong\mathbb{Z}^r$ für ein $r\in\mathbb{N}_0$, nach Proposition 5.4 (ii). Sei ϕ die Komposition des kanonischen Epimorphismus $G\to G/\mathrm{Tor}(G)$ mit diesem Isomorphismus, seien $v_1,\dots,v_r$ Urbilder der Einheitsvektoren $e_1,\dots,e_r\in\mathbb{Z}^r$ unter ϕ, und sei $U = \langle v_1,\dots,v_r\rangle$. Wir zeigen, dass $G = U\oplus\mathrm{Tor}(G)$ gilt. Weil G abelsch und U und $\mathrm{Tor}(G)$ Untergruppen von G sind, handelt es sich um Normalteiler. Zum Nachweis von $U\cap\mathrm{Tor}(G) = \{0_G\}$ sei g ein Element im Durchschnitt. Wegen $g\in\mathrm{Tor}(G)$ gilt $mg = 0_G$ für ein $m\in\mathbb{N}$. Wegen $g\in U$ gibt es außerdem $k_1,\dots,k_r\in\mathbb{Z}$ mit $g = k_1v_1+\dots+k_rv_r$. Es folgt $mg = mk_1v_1+\dots+mk_rv_r$ und $0_{\mathbb{Z}^r} = \phi(mg) = mk_1e_1+\dots+mk_re_r = (mk_1,\dots,mk_r)$. Es gilt also $mk_i = 0$ und somit auch $k_i = 0$ für $1\le i\le r$, und dies wiederum bedeutet $g = 0_G$. Für den Nachweis von $G = U+\mathrm{Tor}(G)$ sei $g\in G$ vorgegeben. Sei $(k_1,\dots,k_r) = \phi(g)$, $h = k_1v_1+\dots+k_rv_r$ und $g' = g-h$. Dann ist $g = g'+h$, $h\in U$ und $\phi(g') = \phi(g)-\phi(h) = (k_1,\dots,k_r)-(k_1,\dots,k_r) = 0_{\mathbb{Z}^r}$, also $g'\in\ker(\phi)$. Aber der Kern von

ϕ stimmt mit dem Kern des kanonischen Epimorphismus $G \to G/\mathrm{Tor}(G)$ überein, und dies ist $\mathrm{Tor}(G)$. Also ist g' in $\mathrm{Tor}(G)$ enthalten. Also liegt $g = h + g'$ in $U + \mathrm{Tor}(G)$.

Insgesamt ist $G = U + \mathrm{Tor}(G)$ damit nachgewiesen. Mit Proposition 4.24 erhalten wir $G \cong U \times \mathrm{Tor}(G)$. Wie man leicht überprüft, ist die Abbildung $\phi|_U : U \to \mathbb{Z}^r$ surjektiv (denn wegen $\phi(v_i) = e_i$ werden alle Einheitsvektoren getroffen) und injektiv (denn das einzige Urbild von $0_{\mathbb{Z}^r}$ ist 0_G), außerdem ein Homomorphismus. Es gilt also $U \cong \mathbb{Z}^r$. Damit ist $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$ gezeigt. Die Gruppe $\mathrm{Tor}(G)$ ist offenbar abelsch, außerdem ist sie als Bild von G unter dem surjektiven Homomorphismus $G \to \mathrm{Tor}(G)$, der durch Komposition von $G \cong U \times \mathrm{Tor}(G)$ mit der Projektion auf die zweite Komponente zu Stande kommt, nach Lemma 5.1 endlich erzeugt. Sei $\{h_1, ..., h_s\}$ ein endliches Erzeugendensystem von $\mathrm{Tor}(G)$. Wegen $h_i \in \mathrm{Tor}(G)$ gibt es jeweils ein $m_i \in \mathbb{N}$ mit $m_i h_i = 0_G$, für $1 \le i \le s$. Wegen Lemma 3.2 folgt jeweils $\langle h_i \rangle = \{kh_i \mid 0 \le k < m_i\}$. Zusammen mit Satz 2.9 (ii) erhalten wir

$$\mathrm{Tor}(G) \quad = \quad \{k_1h_1 + ... + k_sh_s \mid k_1, ..., k_s \in \mathbb{Z}\} \quad = \quad \{k_1h_1 + ... + k_sh_s \mid 0 \le k_i < m_i\}.$$

Es gibt in $\mathrm{Tor}(G)$ also höchstens $\prod_{i=1}^{s} m_i$ verschiedene Elemente. Insbesondere ist $\mathrm{Tor}(G)$ endlich. □

Wir werden nun zeigen, dass jede endliche abelsche Gruppe in ein äußeres direktes Produkt endlicher *zyklischer* Gruppen zerlegt werden kann. In der Linearen Algebra wurde gezeigt, dass $\mathbb{Z}/p\mathbb{Z}$ für jede Primzahl p ein Körper ist, und die Bezeichnung $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für diesen Körper eingeführt.

Lemma 5.6

(i) Sei G eine abelsche Gruppe, seien $s \in \mathbb{N}_0$, $m_1, ..., m_s \in \mathbb{N}$ und $g_1, ..., g_s \in G$ mit $\mathrm{ord}(g_i) \mid m_i$ für $1 \le i \le s$. Sei $U = \langle g_1, ..., g_s \rangle$. Dann gibt es einen surjektiven Gruppenhomomorphismus $\phi : \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_s\mathbb{Z} \to U$ mit

$$\phi(\bar{a}_1, ..., \bar{a}_s) \quad = \quad a_1g_1 + ... + a_sg_s \qquad \text{für alle} \quad a_1, ..., a_s \in \mathbb{Z}.$$

(ii) Ist G eine abelsche Gruppe mit $G[p] = G$, dann gibt es eine Abbildung $\cdot : \mathbb{F}_p \times G \to G$ mit $\bar{a} \cdot g = ag$ für alle $a \in \mathbb{Z}$ und $g \in G$. Mit dieser Abbildung wird auf G die Struktur eines $\mathbb{F}_p$-Vektorraums definiert.

Beweis: zu (i) Wir definieren die Abbildung ϕ, indem wir $\phi(\bar{a}_1, ..., \bar{a}_s) = a_1g_1 + ... + a_rg_r$ für $0 \le a_i < m_i$ setzen. Die Gleichung ist dann automatisch für beliebige $a_i \in \mathbb{Z}$ erfüllt. Wenden wir nämlich Division mit Rest auf jedes a_i an und schreiben $a_i = q_im_i + r_i$ mit $0 \le r_i < m_i$, dann gilt auf Grund der Elementordnungen jeweils $m_ig_i = 0_G$ und somit $a_ig_i = (q_im_i + r_i)g_i = q_i(m_ig_i) + r_ia_i = q_i \cdot 0_G + r_ia_i = r_ia_i$. Wegen $\bar{a}_i = \bar{r}_i$ in $\mathbb{Z}/m_i\mathbb{Z}$ für $1 \le i \le r$ folgt dann $\phi(\bar{a}_1, ..., \bar{a}_r) = \phi(\bar{r}_1, ..., \bar{r}_s) = r_1g_1 + ... + r_sg_s = a_1g_1 + ... + a_sg_s$. Mit Hilfe dieser Gleichung kann die Homomorphismus-Eigenschaft nun unmittelbar nachgerechnet werden. Nach Satz 2.9 gilt $U = \{a_1g_1 + ... + a_sg_s \mid a_1, ..., a_s \in \mathbb{Z}\}$. Damit ist auch klar, dass ϕ surjektiv ist.

zu (ii) Die Existenz einer solchen Abbildung erhalten wir, indem wir (i) für jedes $g \in G$ auf $s = 1$, $m_1 = p$ und $g = g_1$ anwenden. Wir zeigen nun, dass $(U, +, \cdot)$ die Vektorraum-Axiome erfüllt. Nach Definition ist $(U, +)$ eine abelsche Gruppe. Seien nun $\bar{a}, \bar{b} \in \mathbb{F}_p$ und $g, h \in G$ vorgegeben, und seien $a, b \in \mathbb{Z}$ Urbilder von $\bar{a}, \bar{b}$ unter dem kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{F}_p$. Dann gilt $(\bar{a} + \bar{b}) \cdot g = \overline{a+b} \cdot g = (a+b)g = ag + bg = \bar{a} \cdot g + \bar{b} \cdot g$, $\bar{a} \cdot (g + h) = a(g + h) = ag + ah = \bar{a} \cdot g + \bar{a} \cdot h$, $(\bar{a}\bar{b}) \cdot g = \overline{ab} \cdot g = abg = a(bg) = \bar{a} \cdot (\bar{b} \cdot g)$ und $\bar{1} \cdot g = 1g = g$. □

Satz 5.7 Sei G eine abelsche Gruppe.

(i) Sind $m, n \in \mathbb{N}$ teilerfremd, dann gilt $G[mn] \cong G[m] \times G[n]$.

(ii) Sei $n \in \mathbb{N}$ mit $G[n] = G$, und sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n, mit $r \in \mathbb{N}_0$, Primzahlen $p_1, ..., p_r$ und Exponenten $e_1, ..., e_r \in \mathbb{N}$. Dann ist $G \cong G[p_1^{e_1}] \times ... \times G[p_r^{e_r}]$.

Beweis: zu (i) Wegen Proposition 4.24 genügt es, $G[mn] = G[m] \oplus G[n]$ nachzuweisen. Offenbar gilt $G[m] \subseteq G[mn]$, denn ist $g \in G[m]$, dann folgt $mg = 0_G$, damit auch $(mn)g = n(mg) = n0_G = 0_G$ und somit $g \in G[mn]$. Ebenso erhält man $G[n] \subseteq G[mn]$, und als Untergruppen der abelschen Gruppe G sind $G[m]$ und $G[n]$ auch Normalteiler. Zum Nachweis von $G[m] \cap G[n] = \{0_G\}$ sei $g \in G[m] \cap G[n]$ vorgegeben. Dann gilt $mg = ng = 0_G$, also ist $\mathrm{ord}(g)$ ein gemeinsamer Teiler von m und n. Auf Grund der Teilerfremdheit von m und n folgt $\mathrm{ord}(g) = 1$, also $g = 0_G$. Daraus folgt $G[m] \cap G[n] \subseteq \{0_G\}$; die Inklusion „$\supseteq$“ ist offensichtlich. Es bleibt $G[mn] = G[m] + G[n]$ zu zeigen. Die Inklusion „$\supseteq$“ folgt direkt aus $G[m] \subseteq G[mn]$ und $G[n] \subseteq G[mn]$. Zum Nachweis von „$\subseteq$“ sei $g \in G[mn]$. Nach dem Lemma 3.8 von Bézout gibt es $k, \ell \in \mathbb{Z}$ mit $km + \ell n = 1$. Es folgt $g = 1g = (km)g + (\ell n)g$. Wegen $n(km)g = k(mn)g = k0_G = 0_G$ liegt $(km)g$ in $G[n]$, und wegen $m(\ell n)g = \ell(mn)g = \ell 0_G = 0_G$ ist $(\ell n)g$ in $G[m]$ enthalten. Damit ist $g = (km)g + (\ell n)g \in G[m] + G[n]$ nachgewiesen.

zum (ii) Wir schicken voraus: Ist G eine abelsche Gruppe und sind $m, n \in \mathbb{N}$ mit $m \mid n$, dann gilt $G[m] = G[n][m]$. Nun beweisen wir die Aussage durch vollständige Induktion über die Anzahl r der verschiedenen Primfaktoren p_i von n. Im Fall $r \in \{0, 1\}$ braucht nichts gezeigt werden. Sei nun $r > 1$, und setzen wir die Aussage für kleinere Werte von r voraus. Sei $n = \prod_{i=1}^{r} p_i^{e_i}$ die Primfaktorzerlegung von n. Setzen wir $m = \prod_{i=1}^{r-1} p_i^{e_i}$, dann gilt $n = mp_r^{e_r}$ und $\mathrm{ggT}(m, p_r^{e_r}) = 1$. Die Untergruppe $H = G[m]$ erfüllt $H[m] = H$. Wir können also die Induktionsvoraussetzung auf H anwenden; diese liefert einen Isomorphismus $H \cong H[p_1^{e_1}] \times ... \times H[p_{r-1}^{e_{r-1}}] \cong G[p_1^{e_1}] \times ... \times G[p_{r-1}^{e_{r-1}}]$. Nach Teil (i) gilt außerdem $G = G[n] \cong H \times G[p_r^{e_r}]$. Insgesamt erhalten wir somit den angegebenen Isomorphismus. □

Als weiteres Hilfsmittel benötigen wir

Satz 5.8 *(Chinesischer Restsatz für Gruppen)*
Sind $m, n \in \mathbb{N}$ teilerfremd, dann existiert ein Isomorphismus $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ abelscher Gruppen.

Wir werden im Kapitel über Kongruenzrechnng zeigen, dass $\mathbb{Z}/(mn)\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sogar als Ringe isomorph sind; dies liefert insbesondere einen Isomorphismus zwischen den abelschen Gruppen. Man kann den Isomorphismus mit den hier zur Verfügung stehenden Mitteln aber auch leicht direkt zeigen. Definieren wir in $(\mathbb{Z}/(mn)\mathbb{Z}, +)$ die Untergruppen $U = \langle n + (mn)\mathbb{Z} \rangle$ und $V = \langle m + (mn)\mathbb{Z} \rangle$, dann gilt zunächst $U \cap V = \{0_{\mathbb{Z}/(mn)\mathbb{Z}}\}$. Liegt nämlich $a + (mn)\mathbb{Z}$ im Durchschnitt dieser Untergruppen, dann ist a ein Vielfaches sowohl von n als auch von m. Auf Grund der Teilerfremdheit von m und n ist a damit auch ein Vielfaches von mn, und es folgt $a + (mn)\mathbb{Z} = 0_{\mathbb{Z}/(mn)\mathbb{Z}}$.

Nach dem Lemma 3.8 von Bézout gibt es außerdem $k, \ell \in \mathbb{Z}$ mit $kn + \ell m = \mathrm{ggT}(m, n) = 1$. Weil $u = kn + (mn)\mathbb{Z}$ in U und $v = \ell m + (mn)\mathbb{Z} \in V$ in V liegt, folgt daraus, dass $U + V$ den Erzeuger $u + v = 1 + (mn)\mathbb{Z}$ von $\mathbb{Z}/(mn)\mathbb{Z}$ enthält und somit $U + V = \mathbb{Z}/(mn)\mathbb{Z}$ gilt. Insgesamt ist $\mathbb{Z}/(mn)\mathbb{Z}$ damit ein inneres direktes Produkt von U und

V, und mit Proposition 4.24 folgt $\mathbb{Z}/(mn)\mathbb{Z} \cong U \times V$. Nach Teil (ii) von Satz 3.9 ist $n + (mn)\mathbb{Z} = n \cdot (1 + (mn)\mathbb{Z})$ ein Element der Ordnung $\frac{mn}{n} = m$, also gilt $U \cong \mathbb{Z}/m\mathbb{Z}$. Ebenso erhält man $V \cong \mathbb{Z}/n\mathbb{Z}$. Insgesamt erhalten wir $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Man beachte, dass der Chinesische Restsatz nur für teilerfremde $m, n \in \mathbb{N}$ gültig ist! Beispielsweise ist $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$. Denn $\mathbb{Z}/4\mathbb{Z}$ enthält mit $\bar{1}$ ein Element der Ordnung 4, während die Gleichung $2 \cdot (\bar{a}, \bar{b}) = (\bar{0}, \bar{0})$ für alle $(\bar{a}, \bar{b}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ zeigt, dass es in dieser Gruppe nur Elemente der Ordnung 1 und 2 gibt.

Satz 5.9 Sei $e \in \mathbb{N}_0$, p eine Primzahl und G eine endliche abelsche Gruppe mit $G[p^e] = G$. Dann gibt es ein $r \in N_0$ und $n_1, ..., n_r \in \mathbb{N}$, so dass

$$G \quad \cong \quad \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \qquad \text{gilt.}$$

Beweis: Wir beweisen die Aussage durch vollständige Induktion über e. Ist $e = 0$, dann gilt $G[1] = G$, also $g = 1 \cdot g = 0_G$ für alle $g \in G$. Es folgt $G = \{0_G\}$, und die Behauptung ist offenbar mit $r = 0$ erfüllt. Sei nun $e \geq 1$, und setzen wir die Aussage für Werte kleiner als e voraus. Für die Gruppe $H = pG$ gilt $H[p^{e-1}] = H$. Nach Induktionsvoraussetzung gibt es $r \in \mathbb{N}_0$, $n_1, ..., n_r$ und einen Isomorphismus $\phi : \mathbb{Z}/p^{n_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r}\mathbb{Z} \to H$. Seien $h_1, h_2, ..., h_r \in H$ die Bilder der Elemente

$$(\bar{1}, \bar{0}, \bar{0}, ..., \bar{0}) \quad , \quad (\bar{0}, \bar{1}, \bar{0}, ..., \bar{0}) \quad , \quad ... \quad , \quad (\bar{0}, \bar{0}, \bar{0}, ..., \bar{1}).$$

Wegen $h_i \in pG$ gibt es jeweils ein $g_i \in G$ mit $pg_i = h_i$, für $1 \leq i \leq r$. Wir zeigen nun zunächst, dass die Gruppe $U = \langle g_1, ..., g_r \rangle$ isomorph zu $\mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z}$ ist. Dazu betrachten wir die Abbildung

$$\psi : \mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \to U \quad , \quad (\bar{a}_1, ...\bar{a}_r) \mapsto a_1 g_1 + ... + a_r g_r.$$

Nach Lemma 5.6 (i) ist dies ein surjektiver Gruppenhomomorphismus. Außerdem ist die Abbildung injektiv. Gilt nämlich $\psi(\bar{a}_1, ..., \bar{a}_r) = 0_G$ und ist $a_i \in \mathbb{Z}$ jeweils ein Urbild von $\bar{a}_i$, dann ist $a_1 g_1 + ... + a_r g_r = 0_G$ nach Definition von ψ. Es folgt $\phi(a_1 + p^{n_1}\mathbb{Z}, ..., a_r + p^{n_r}\mathbb{Z}) = a_1 h_1 + ... + a_r h_r = p(a_1 g_1 + ... + a_r g_r) = p0_G = 0_G$. Weil ϕ injektiv ist, erhalten wir $a_i + p^{n_i}\mathbb{Z} = 0 + p^{n_i}\mathbb{Z}$ und $p^{n_i} \mid a_i$, für $1 \leq i \leq r$. Insbesondere gibt es jeweils ein $b_i \in \mathbb{Z}$ mit $pb_i = a_i$. Nun folgt weiter $\phi(b_1 + p^{n_1}\mathbb{Z}, ..., b_r + p^{n_r}\mathbb{Z}) = b_1 h_1 + ... + b_r h_r = pb_1 g_1 + ... + pb_r g_r = a_1 g_1 + ... + a_r g_r = 0_G$. Wiederum auf Grund der Injektivität von ϕ erhalten wir $b_i + p^{n_i}\mathbb{Z} = 0 + p^{n_i}\mathbb{Z}$, also $p^{n_i} \mid b_i$ und $p^{n_i+1} \mid a_i$ für $1 \leq i \leq r$. Dies wiederum bedeutet $(\bar{a}_1, ..., \bar{a}_r) = (\bar{0}, ..., \bar{0})$. Insgesamt ist ψ also tatsächlich ein Isomorphismus.

Nach Lemma 5.6 (ii) besitzen $G[p] \cap U$ und $G[p]$ jeweils die Struktur eines $\mathbb{F}_p$-Vektorraums. Dabei ist $G[p] \cap U$ als Untergruppe offenbar auch ein Untervektorraum von $G[p]$. Wir wählen nun eine Basis $\{v_1, ..., v_s\}$ von $G[p] \cap U$ und ergänzen diese durch $v_{s+1}, ..., v_t$ (mit $s, t \in \mathbb{N}_0$ und $s \leq t$) zu einer Basis von $G[p]$. Anschließend definieren wir $V = \langle v_{s+1}, ..., v_t \rangle$. Als $(t-s)$-dimensionaler $\mathbb{F}_p$-Vektorraum ist V isomorph zu $\mathbb{F}_p^{t-s}$. Als abelsche Gruppe ist V damit isomorph zu $\mathbb{F}_p^{t-s} = (\mathbb{Z}/p\mathbb{Z})^{t-s}$. Wenn wir zeigen können, dass $G = U \oplus V$ gilt, dann folgt $G \cong U \times V \cong \mathbb{Z}/p^{n_1+1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{n_r+1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^{t-s}$ nach Proposition 4.24. Damit hat G dann bis auf Isomorphie die im Satz angegebene Form.

Als Untergruppen der abelschen Gruppe G sind U und V auch Normalteiler. Zum Beweis der Gleichung $U \cap V = \{0_G\}$ sei $g \in U \cap V$ vorgegeben. Wegen $V \subseteq G[p]$ liegt g dann in $(G[p] \cap U) \cap V$. Wäre g ungleich Null, dann könnte man g als nichttriviale $\mathbb{F}_p$-Linearkombination der Basis $\{v_1, ..., v_s\}$ von $G[p] \cap U$ darstellen, und $-g$ als nichttriviale

$\mathbb{F}_p$-Linearkombination der Basis $\{v_{s+1}, ..., v_t\}$ von V. Insgesamt würde man eine nichttriviale Linearkombination von $g + (-g) = 0_G$ durch $\{v_1, ..., v_t\}$ erhalten. Aber dies steht im Widerspruch zur linearen Unabhängigkeit dieser Menge. Also ist nur $g = 0_G$ möglich. Nun zeigen wir noch $G = U + V$. Sei dazu $g \in G$ beliebig vorgegeben. Dann liegt pg in pG, und folglich gibt es $k_1, ..., k_r \in \mathbb{Z}$ mit $pg = k_1h_1 + ... + k_rh_r$. Setzen wir $g' = k_1g_1 + ... + k_rg_r$ und $g'' = g - g'$, dann gilt $g' \in U$ und $pg'' = pg - pg' = pg - pk_1g_1 - ... - pk_rg_r = k_1h_1 + ... + k_rh_r - k_1h_1 - ... - k_rh_r = 0_G$, also $g'' \in G[p]$. Weil $\{v_1, ..., v_t\}$ eine Basis von $G[p]$ als $\mathbb{F}_p$-Vektorraum ist, kann g'' in der Form $\ell_1v_1 + ... + \ell_tv_t$ geschrieben werden, mit $\ell_1, ..., \ell_t \in \mathbb{Z}$. Es ist dann $g'' = g_1 + g_2$ mit $g_1 = \ell_1v_1 + ... + \ell_sv_s \in U$ und $g_2 = \ell_{s+1}v_{s+1} + ... + \ell_tv_t \in V$. Insgesamt hat g also die Form $g = g' + g'' = (g' + g_1) + g_2$ mit $g' + g_1 \in U$ und $g_2 \in V$. □

Wir können nun das Hauptergebnis dieses Kapitels formulieren.

Satz 5.10 *(Hauptsatz über endlich erzeugte abelsche Gruppe)*
Sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es $r, s \in \mathbb{N}_0$ und $d_1, ..., d_s \in \mathbb{N}$ mit

$$G \quad \cong \quad \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}.$$

Dabei können die Zahlen d_i so gewählt werden, dass sie entweder (i) alle Primzahlpotenzen sind oder (ii) $d_i \mid d_{i+1}$ für $1 \leq i < s$ erfüllt ist. Im Fall (ii) gezeichnet man die Zahlen d_i als ***Elementarteiler*** der abelschen Gruppe.

Beweis: Nach Satz 5.5 gilt $G \cong \mathbb{Z}^r \times \mathrm{Tor}(G)$, und die Gruppe $\mathrm{Tor}(G)$ ist endlich. Setzen wir $H = \mathrm{Tor}(G)$ und $n = |H|$, dann gilt $H[n] = n$. Ist $n = \ prod_{i=1}^{t} p_i^{e_i}$, dann gilt $H \cong H[p_1^{e_1}] \times ... \times H[p_r^{e_r}]$ nach Satz 5.7 (ii), und wegen Satz 5.9 ist $H[p_i^{e_i}]$ jeweils isomorph zu einem äußeres direktes Produkt zyklischer Gruppen von p_i-Potenzordnung. Also ist G insgesamt isomorph zu einem äußeren direkten Produkt der Form (i).

Im Ringtheorie-Teil der Vorlesung wird der Begriff des ***Exponenten*** $\exp(G)$ einer Gruppe G eingeführt und gezeigt, dass der Exponent einer Gruppe, die zu $\mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_u\mathbb{Z}$ mit $m_1, ..., m_u \in \mathbb{N}$ isomorph ist, mit dem kgV von $m_1, ..., m_u$ übereinstimmt. Wir beweisen durch vollständige Induktion über $|H|$, dass G auch eine Zerlegung der unter (ii) beschriebenen Form besitzt, und setzen $d = \exp(H)$. Sei $H \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_u\mathbb{Z}$ die Darstellung nach (i) von H als äußeres direktes Produkt zyklischer Gruppe von Primzahlpotenzordnung m_i.

Im Fall $|H| = 1$ ist nichts zu zeigen. Setzen wir nun voraus, dass H nicht trival ist, und sei $\prod_{j=1}^{v} p_j^{f_j}$ die Primfaktorzerlegung von d. Wegen $\mathrm{kgV}(m_1, ..., m_u) = d$ müssen die Faktoren $p_1^{f_1}, ..., p_v^{f_v}$ unter $m_1, ..., m_u$ vorkommen, andererseits darf es aber keine höheren Potenzen von $p_1, ..., p_v$ unter diesen Zahlen geben. Setzen wir $H_1 = \mathbb{Z}/p_1^{f_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_v^{f_v}\mathbb{Z}$, dann gilt $H \cong H_1 \times H_2$ bis auf Reihenfolge der Faktoren, wobei in H_2 die Faktoren der Form $\mathbb{Z}/m_i\mathbb{Z}$ zusammengefasst sind, die in H, aber nicht in H_1 vorkommen. Es gilt dann $|H_2| < |H|$, und nach Induktionsvoraussetzung gibt es Zahlen $d_1, ..., d_s$ mit $H_2 \cong \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}$ und der oben beschriebenen Eigenschaft. Außerdem gilt $H_1 \cong \mathbb{Z}/d\mathbb{Z}$ nach dem Chinesischen Restsatz, Satz 5.8, denn die Zahlen $p_j^{f_j}$ sind paarweise teilerfremd. Weil der Exponent von H_2 ein Teiler von d ist, gilt $d_i \mid d$ für $1 \leq i \leq s$. Setzen wir $d_{s+1} = d$, dann ist $d_1, ..., d_{s+1}$ eine Folge natürlicher Zahlen mit den gewünschten Eigenschaften. □

Sowohl die Bedingung (i) als auch die Bedingung (ii) in Satz 5.10 kann dazu genutzt werden, um zum Beispiel alle abelschen Gruppen der Ordnung $100 = 2^2 5^2$ bis auf Isomorphie anzugeben. Durch (i) erhält man die vier Isomorphietypen

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \quad , \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Andererseits finden wir zur Zahl 100 die Elementarteilerketten 100, 2|50, 5|20 und 10|10, was die Isomorphietypen

$$\mathbb{Z}/100\mathbb{Z} \quad , \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z} \quad , \quad \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \quad , \quad \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$

liefert. Mit dem Chinesischen Restsatz überprüft man leicht, dass diese vier Gruppen mit den vier zuvor gefundenen bis auf Isomorphie übereinstimmen.

Zu bemerken ist noch, dass im Fall (ii) der Wert $r+s$ die ***minimale*** Anzahl der Elemente eines Erzeugendensystems von G angibt. Insbesondere gilt $r+s=1$ genau dann, wenn G eine zyklische Gruppe ist. Ist nämlich p ein beliebiger Primteiler von d_1, dann existiert ein Epimorphismus

$$\phi : \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^{r+s} \quad , \quad (a_1, ..., a_r, b_1 + d_1\mathbb{Z}, ..., b_s + d_s\mathbb{Z}) \mapsto (a_1 + p\mathbb{Z}, ..., b_s + p\mathbb{Z}).$$

Sei $g_1, ..., g_t$ ein t-elementiges Erzeugendensystem von G. Dann liefern die Bilder der Elemente in der Gruppe $H = (\mathbb{Z}/p\mathbb{Z})^{r+s}$ ein Erzeugendensystem von H. Dieses Erzeugendensystem ist dann zugleich eine Basis von H als $\mathbb{F}_p$-Vektorraum. Da in einem $(r+s)$-dimensionalen Vektorraum jedes Erzeugendensystem aus mindestens $r+s$ Elementen besteht, muss $t \geq r+s$ gelten. Andererseits besitzt die Gruppe $\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_s\mathbb{Z}$ offenbar ein $(r+s)$-elementiges Erzeugendensystem (gegeben durch die Einheitsvektoren), somit auch die Gruppe G.

Literaturverzeichnis

[1] Michael Artin. *Algebra - Aus dem Englischen übersetzt von Annette A'Campo*. Basel: Birkhäuser Basel, 1998.

[2] Janko Böhm. *Grundlagen der Algebra und Zahlentheorie* -. Berlin Heidelberg New York: Springer-Verlag, 2016.

[3] Siegfried Bosch. *Algebra* -. Berlin, Heidelberg, New York: Springer Berlin, 2023.

[4] Falko Lorenz und Franz Lemmermeyer. *Algebra 1 - Körper und Galoistheorie*. Heidelberg: Spektrum Akademischer Verlag, 2007.

[5] Stefan Müller-Stach und Jens Piontkowski. *Elementare und algebraische Zahlentheorie - Ein moderner Zugang zu klassischen Themen*. Berlin Heidelberg New York: Springer-Verlag, 2011.