**Skript zur Vorlesung**

# Einführung in Geometrie und Algebra Aufbaukurs

**Wintersemester 2006/07**
**(vierstündig)**

**Prof. Dr. Annette Werner**

# Inhaltsverzeichnis

# 1 Euklidische Bewegungen

Wir wollen das Studium interessanter Untergruppen der Euklidischen Bewegungsgruppe fortsetzen, das wir in LAAG II begonnen haben. Dazu wiederholen wir zunächst einige Begriffe und Resultate aus dem Aufbaukurs LAAG II.

**Definition 1.1** Eine Abbildung $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ heißt **euklidische Bewegung** oder **Isometrie** des $\mathbb{R}^2$, falls $\beta$ abstandstreu ist, d.h. falls für alle $x, y \in \mathbb{R}^2$ gilt

$$||\beta(x) - \beta(y)|| = ||x - y|| \tag{1}$$

Hier ist $||z|| = \sqrt{\langle z, z\rangle}$ die Länge eines Vektors bezüglich des kanonischen Skalarprodukts $\langle , \rangle$.
Ist $\beta$ eine abstandstreue lineare Abbildung, so nennen wir $\beta$ eine **lineare Isometrie.**
Im Aufbaukurs LAAG II, Lemma 9.2, haben wir gesehen, dass jede Isometrie $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ mit $\beta(0) = 0$ eine lineare Isometrie ist.
Für eine lineare Isometrie $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ folgt aus $\beta(0) = 0$ die Gleichung $||\beta(x)|| = ||x||$ für alle $x \in \mathbb{R}^2$.
Da für beliebige $x, y \in \mathbb{R}^2$

$$||x + y||^2 = ||x||^2 + 2\langle x, y\rangle + ||y||^2$$

gilt, folgt daraus $\langle \beta(x), \beta(y)\rangle = \langle x, y\rangle$, d.h. $\beta$ lässt das kanonische Skalarprodukt invariant.
Daher ist die Koordinatenmatrix $A_{\beta,B,B}$ von $\beta$ bezüglich der kanonischen Basis $B$ eine orthogonale Matrix, d.h. ein Element von $O(2, \mathbb{R})$. Insbesondere gilt also $\det A_{\beta,B,B} \in \{\pm 1\}$.
Paradebeispiel einer nicht-linearen Isometrie ist die **Translation** (Verschiebung)

$$\begin{array}{rccc} t_b : \mathbb{R}^2 & \to & \mathbb{R}^2 \\ x & \mapsto & x + b \end{array}$$

um ein $b \in \mathbb{R}^2$.
Ist $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ eine beliebige Isometrie und $b = \beta(0)$, so lässt $\gamma = t_{-b} \circ \beta$ den Nullpunkt fest, ist also eine lineare Isometrie. Also ist $\beta = t_b \circ \gamma$ die Komposition einer linearen Isometrie mit einer Translation.
Daraus folgt insbesondere, dass $\beta$ bijektiv ist, mit Umkehrabbildung $\beta^{-1} = \gamma^{-1} \circ t_{-b}$. Also ist $\beta^{-1}$ auch eine Isometrie. Daher ist

$$\mathcal{B}_2 = \{\beta : \mathbb{R}^2 \to \mathbb{R}^2 \text{ Isometrie } \}$$

eine Gruppe, wir nennen sie die euklidische Bewegungsgruppe des $\mathbb{R}^2$. Schreiben wir ein Element $\beta \in \mathcal{B}_2$ als Komposition $\beta = t_b \circ \gamma$ einer linearen Isometrie $\gamma$ mit der Translation $t_b$, so sind $b$ und $\gamma$ eindeutig bestimmt. Aus $t_b \circ \gamma = t_c \circ \sigma$ mit $b, c \in \mathbb{R}^2$ und linearen Isometrien $\gamma$ und $\sigma$ folgt nämlich

$$t_{-c} \circ t_b = \sigma \circ \gamma^{-1},$$

also ist $t_{-c} \circ t_b = t_{b-c}$ eine lineare Abbildung, woraus $b - c = 0$ folgt. Daher ist $b = c$ und $\gamma = \sigma$.
Wir können also definieren:

**Definition 1.2** Sei $\beta \in \mathcal{B}_2$ mit $\beta = t_b \circ \gamma$ für eine lineare Isometrie $\gamma$ und ein $b \in \mathbb{R}^2$. Dann heißt $\beta$ **orientierungserhaltend**, falls $\det(\gamma) = 1$ und orientierungsumkehrend, falls $\det(\gamma) = -1$ ist.
Hier ist natürlich $\det(\gamma)$ die Determinante einer (und damit jeder) Koordinatenmatrix von $\gamma$.
Sind $\beta_1 = t_{b_1} \circ \gamma_1$ und $\beta_2 = t_{b_2} \circ \gamma_2$ zwei Euklidische Bewegungen, so ist

$$\begin{aligned} \beta_1 \circ \beta_2 &= t_{b_1} \circ \gamma_1 \circ t_{b_2} \circ \gamma_2 \\ &= t_{b_1} \circ t_{\gamma_1(b_2)} \circ \gamma_1 \circ \gamma_2, \end{aligned}$$

da $\gamma_1(x + b_2) = \gamma_1(x) + \gamma_1(b_2)$ gilt. Also ist die Komposition von orientierungserhaltenden Abbildungen wieder orientierungserhaltend. Allgemeiner folgt aus dieser Gleichung, dass die Orientierungsabbildung

$$\begin{aligned} \mathcal{B}_2 &\to \{\pm 1\} \\ \beta = t_b \circ \gamma &\mapsto \det(\gamma) \end{aligned}$$

ein Gruppenhomomorphismus ist.
In vielen Anwendungen tauchen Untergruppen der eukldidischen Bewegungsgruppe (und andere Gruppen) als Symmetriegruppen auf.

**Definition 1.3** Ist $F \subset \mathbb{R}^2$ eine Teilmenge der Ebene, so heißt $\beta \in B_2$ eine **Symmetrie von** F, falls $\beta(F) = F$ gilt.

**Proposition 1.4** Die Menge aller Symmetrien einer Teilmenge $F \subset \mathbb{R}^2$ ist eine Gruppe (bezüglich Verknüpfung). Wir nennen sie die Symmetriegruppe von $F$.

**Beweis :** Offenbar ist $\mathrm{id}(F) = F$. Gilt $\beta(F) = F$ und $\beta'(F) = F$, so folgt auch $\beta' \circ \beta(F) = F$ sowie $\beta^{-1}(F) = F$.

Die Symmetriegruppen von Tapetenmustern, die zwei unabhängige Translationssymmetrien haben, werden wir später ausführlich studieren.
Jetzt wollen wir zunächst die Elemente in $\mathcal{B}_2$ noch etwas genauer beschreiben. Wir geben die Elemente von $\mathcal{B}_2$ in Koordinaten bezüglich der kanonischen Basis von $\mathbb{R}^2$ an. Also gilt:

1) Die Translation $t_b$ um $b = \binom{b_1}{b_2} \in \mathbb{R}^2$ ist die Abbildung $t_b\binom{x_1}{x_2} = \binom{x_1+b_1}{x_2+b_2}$.

2) Die Drehung $d_\theta$ (gegen den Uhrzeigersinn) um den Winkel $\theta \in [0, 2\pi[$ um 0 ist die lineare Abbildung

$$d_\theta \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

   Wir verwenden die Notation $d_\theta$ auch für beliebige $\theta \in \mathbb{R}$. Natürlich gilt $d_{\theta+2\pi} = d_\theta$.

3) Die Spiegelung $s$ an der $x_1$-Achse ist gegeben durch

$$s \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}.$$

Ist $\gamma$ eine lineare Isometrie, so ist die Koordinatenmatrix $A$ von $\gamma$ bezüglich der kanonischen Basis des $\mathbb{R}^2$ ein Element aus $O(2, R)$. Gilt $\det \gamma = \det A = 1$, so folgt mit der Gleichung $AA^t = E_2$ die Existenz eines $\theta \in [0, 2\pi[$ mit

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \text{ d.h. } \gamma = d_\theta.$$

Ist $\det \gamma = \det A = -1$, so folgt mit der Gleichung $AA^t = E_2$ die Existenz eines $\theta \in [0, 2\pi[$ mit

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix},$$

vgl. Aufgabe 36 in LAAG II. In diesem Fall ist $\gamma$ die Spiegelung an der Geraden $l$, die im Winkel $\frac{\theta}{2}$ zur $x_1$-Achse $\langle\binom{1}{0}\rangle$ steht, d.h. es ist $\gamma(y_1 + y_2) = y_1 - y_2$, falls $y_1 \in l$ und $y_2 \in l^\perp$ ist. Wir schreiben für diese Abbildung auch $\gamma = s_l$. Nun gilt

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Also folgt $s_l = d_\theta \circ s$, d.h. eine beliebige Spiegelung lässt sich immer als Verknüpfung der Spiegelung an der $x_1$-Achse mit einer Drehung schreiben. Somit ist jedes $\beta \in \mathcal{B}_2$ entweder von der Form $\beta = t_a \circ d_\theta$ oder von der Form $\beta = t_a \circ d_\theta \circ s$.

Ab jetzt lassen wir die Verknüpfungszeichen $\circ$ weg und notieren die Verknüpfung in $B_2$ einfach als Multiplikation. $\square$

**Lemma 1.5** In $\mathcal{B}_2$ gelten folgende Rechenregeln für $a, b \in \mathbb{R}^2$ und $\theta, \eta \in [0, 2\pi[$:

i) $t_a t_b = t_{a+b}$

ii) $d_\theta d_\eta = d_{\theta+\eta}$

iii) $s^2 = 1$

iv) $d_\theta t_a = t_{d_\theta(a)} d_\theta$

v) $s t_a = t_{s(a)} s$

vi) $s d_\theta = d_{-\theta} s$

**Beweis :** Übungsaufgabe. $\square$

Die Gruppe $\mathcal{B}_2$ enthält für jeden Punkt $a \in \mathbb{R}^2$ die Drehung (gegen den Uhrzeigersinn) $d_{\theta,a}$ um $a$ mit Winkel $\theta \in [0, 2\pi[$. Diese ist nämlich gerade die Abbildung

$$d_{\theta,a} = t_a d_\theta t_{-a}.$$

(Machen Sie sich das geometrisch klar!).
Mit Hilfe der Rechenregeln aus Lemma 1.5 gilt also

$$d_{\theta,a} = t_{a+d_\theta(-a)} d_\theta.$$

Ferner ist $d_\theta = d_{\theta,0}$.
Für jede Gerade $l \in \mathbb{R}^2$ und jedes $a \in \mathbb{R}^2$ ist $a + l$ eine affine Gerade in $\mathbb{R}^2$.
Die Gruppe $\mathcal{B}_2$ enthält das Element

$$s_{l,a} = t_a s_l t_{-a}.$$

Diese Abbildung ist gerade die Spiegelung an der affinen Geraden $a + l$. (Machen Sie sich das geometrisch klar!).
Mit Hilfe der Rechenregeln aus Lemma 1.5 gilt also

$$s_{l,a} = t_{a+s_l(-a)} s_l.$$

Ferner ist $s_l = s_{l,0}$.
Ist $b \in l$, so nennt man die Komposition $t_b s_{l,a}$ eine Gleitspiegelung. Erst wird an einer affinen Gerade gespiegelt, dann parallel zu dieser Geraden verschoben.

**Satz 1.6** i) Jede orientierungserhaltende Isometrie $\beta \in \mathcal{B}_2$ ist entweder eine Translation (d.h. $\beta = t_a$ für ein $a \in \mathbb{R}^2$) oder eine echte Drehung um einen Punkt $a \in \mathbb{R}^2$ (d.h. $\beta = d_{\theta,a}$ für ein $\theta \in ]0, 2\pi[$).

ii) Jede orientierungsumkehrende Isometrie $\beta \in \mathcal{B}_2$ ist entweder eine Spiegelung an einer affinen Geraden (d.h. $\beta = s_{l,a}$ für eine Gerade $l$ und ein $a \in \mathbb{R}^2$) oder eine echte Gleitspiegelung (d.h. $\beta = t_b s_{l,a}$ für eine Gerade $l$, ein $a \in \mathbb{R}^2$ und ein $b \in l, b \neq 0$).

**Beweis :**

i) Es sei $\beta$ eine orientierungserhaltende Isometrie, die keine Translation ist. Wir müssen zeigen, dass $\beta$ dann eine Drehung um ein $a \in \mathbb{R}^2$ ist.

Jedes Element aus $\mathcal{B}_2$ ist von der Form $t_b d_\theta$ oder $t_b d_\theta s$. Da $t_b d_\theta s$ orientierungsumkehrend ist, muss

$$\beta = t_b d_\theta$$

für ein $b \in \mathbb{R}^2$ und ein $\theta \in [0, 2\pi[$ sein. Nach unserer Annahme gilt $\theta \neq 0$.

Wir zeigen nun, dass $\beta$ einen Fixpunkt hat, d.h. dass es ein $a \in \mathbb{R}^2$ gibt mit $\beta(a) = a$. Dazu zeigen wir, dass die Gleichung $t_b d_\theta(x) = x$ in $\mathbb{R}^2$ lösbar ist. Definitionsgemäß gilt $t_b d_\theta(x) = d_\theta(x) + b$. Die Gleichung $t_b d_\theta(x) = x$ ist also äquivalent zu dem homogenen linearen Gleichungssystem

$$x - d_\theta(x) = b.$$

Dieses hat die Koeffizientenmatrix

$$\begin{pmatrix} 1 - \cos\theta & \sin\theta \\ -\sin\theta & 1 - \cos\theta \end{pmatrix},$$

deren Determinante

$$(1 - \cos\theta)^2 + \sin^2\theta = 2 - 2\cos\theta$$

wegen $\theta \in ]0, 2\pi[$ ungleich Null ist. Somit ist die Koeffizientenmatrix invertierbar, d.h. die Gleichung $x - d_\theta(x) = b$ hat eine eindeutig bestimmte Lösung $a \in \mathbb{R}^2$.

Aus $\beta(a) = a$ folgt nun, dass

$$t_{-a}\beta t_a(0) = 0$$

ist. Somit ist $t_{-a}\beta t_a$ eine lineare Isometrie, also eine Drehung oder Spiegelung. Da das Produkt von orientierungserhaltenden Abbildungen wieder orientierungserhaltend ist, muss $t_{-a}\beta t_a$ eine Drehung, also $t_{-a}\beta t_a = d_\eta$ für ein $\eta \in [0, 2\pi[$ sein. Da $\beta$ keine Translation ist, gilt sogar $\eta \in ]0, 2\pi[$. Somit folgt

$$\beta = t_a d_\eta t_{-a} = d_{\eta,a},$$

also ist $\beta$ eine Drehung um $a$.

ii) Es sei $\beta$ eine orientierungsumkehrende Isometrie. Da jedes Element aus $\mathcal{B}_2$ sich entweder als $t_b d_\theta$ oder als $t_b d_\theta s$ schreiben lässt, folgt $\beta = t_b d_\theta s$ für ein $b \in \mathbb{R}^2$ und ein $\theta \in [0, 2\pi]$. Nun gilt $d_\theta s = s_l$, für die Gerade $l \subset \mathbb{R}^2$, die im Winkel $\frac{\theta}{2}$ zur $x_1$-Achse $\langle \binom{1}{0} \rangle$ steht. Also ist $d_{-\theta/2}(d_\theta s)d_{\theta/2} = s$, die Spiegelung an der $x_1$-Achse. Das ist geometrisch sofort klar. Man kann es auch mit den Rechenregeln aus Lemma 1.5 nachprüfen:

$$(d_{-\theta/2}d_\theta)(sd_{\theta/2}) = d_{\theta/2}sd_{\theta/2} = d_{\theta/2}d_{-\theta/2}s = s.$$

Somit folgt

$$\begin{aligned} d_{-\theta/2}\beta d_{\theta/2} &= d_{-\theta/2}t_b(d_\theta s)d_{\theta/2} \\ &\overset{1.5}{=} t_{d_{-\theta/2}(b)}d_{-\theta/2}(d_\theta s)d_{\theta/2} \\ &= t_c s \end{aligned}$$

für den Punkt $c = d_{-\theta/2}(b) \in \mathbb{R}^2$. Schreiben wir $c = \binom{c_1}{c_2}$, so ist

$$t_c s \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + c_1 \\ -x_2 + c_2 \end{pmatrix}.$$

Dies ist eine Gleitspiegelung an der affinen Geraden $a + l_0$, wobei

$$l_0 = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$$

die $x_1$-Achse bezeichnet und

$$a = \begin{pmatrix} 0 \\ \frac{1}{2}c_2 \end{pmatrix}$$

ist. Das kann man sich geometrisch leicht klarmachen und algebraisch folgendermaßen nachrechnen. Mit $b = \begin{pmatrix} c_1 \\ 0 \end{pmatrix} \in l_0$ gilt

$$t_b s_{l_{0,a}} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = t_b \begin{pmatrix} x_1 \\ -x_2 + c_2 \end{pmatrix} = \begin{pmatrix} x_1 + c_1 \\ -x_2 + c_2 \end{pmatrix}.$$

Also folgt $d_{-\theta/2}\beta d_{\theta/2} = t_b s_{l_{0,a}}$.

Somit gilt

$$\begin{aligned} \beta &= d_{\theta/2} t_b s_{l_{0,a}} d_{-\theta/2} = (d_{\theta/2} t_b t_a) s (t_{-a} d_{-\theta/2}) \\ &\overset{1.5}{=} t_{d_{\theta/2}}(b) t_{d_{\theta/2}}(a) d_{\theta/2} s d_{-\theta/2} t_{d_{\theta/2}(-a)} \\ &= t_{b'} t_{a'} (d_\theta s) t_{-a'} \end{aligned}$$

für $b' = d_{\theta/2}(b)$ und $a' = d_{\theta/2}(a)$.

Ist $l$ die Gerade mit $d_\theta s = s_l$, so gilt $b' \in l$, also ist $\beta$ eine Gleitspiegelung an der affinen Geraden $a' + l$.
Im Fall $b' = 0$ ist $\beta$ eine Spiegelung an der affinen Geraden $a' + l$, im Fall $b' \neq 0$ ist $\beta$ eine echte Gleitspiegelung. □

Diese Klassifikation der Isometrien hat bemerkenswerte Konsequenzen. Es folgt zum Beispiel, dass die Komposition von zwei Drehungen um verschiedene Punkte eine Translation oder eine Drehung um einen dritten Punkt ist, da sie die Orientierung erhält. Diese Tatsache ist nicht offensichtlich.
Translationen und echte Gleitspiegelungen haben offenbar keine Fixpunkte. Eine echte Drehung um einen Punkt $a$ (d.h. $d_{\theta,a}$ mit $\theta \neq 0$) hat genau einen Fixpunkt, nämlich $a$. Eine Spiegelung $s_{l,a}$ hat als Fixpunktmenge genau die Spiegelachse $a + l$.
Es seien $s_{l,a}$ und $s_{l',a'}$ zwei Spiegelungen an nicht-parallelen affinen Geraden $a + l$ und $a' + l'$ (d.h. es gelte $l \neq l'$). Dann ist $s_{l,a}, s_{l',a'}$ als Komposition zweier orientierungsumkehrender Abbildungen orientierungserhaltend. Da $l \neq l'$ ist, haben die affinen Geraden $a + l$ und $a' + l'$ genau einen Schnittpunkt $b$. Dieser ist ein Fixpunkt von $s_{l,a} s_{l',a'}$. Nach Satz 1.6 ist also die orientierungserhaltende Abbildung $s_{l,a} s_{l',a'}$ eine Drehung um ihren Fixpunkt $b$.

**Definition 1.7** Eine Untergruppe $G$ der Euklidischen Bewegungsgruppe $\mathcal{B}_2$ heißt **diskret**, falls es ein $\varepsilon > 0$ gibt, so dass die folgenden Bedingungen gelten:

i) Ist $t_a \in G$ und $a \neq 0$, so ist $|a| \geq \varepsilon$.

ii) Ist $d_\theta \in G$ und $\theta \neq 0$, so ist $|\theta| \geq \varepsilon$.

$G$ ist also diskret, falls $G$ keine beliebig „kleinen“ Translationen oder Drehungen enthält.
Mit $\mathcal{T}$ bezeichnen wir die Untergruppe aller Translationen in $\mathcal{B}_2$. Die Abbildung

$$\begin{aligned} \varphi : \mathbb{R}^2 &\to \mathcal{T} \\ a &\mapsto t_a \end{aligned}$$

vermittelt nach Lemma 1.5 einen Gruppenisomorphismus. Ist $G$ eine diskrete Untergruppe von $\mathcal{B}_2$, so vermittelt $\varphi$ einen Isomorphismus von $L_G = \{a \in \mathbb{R}^2 : t_a \in G\}$ auf die Untergruppe $\mathcal{T} \cap G$ von $G$. Da $G$ diskret ist, existiert ein $\varepsilon > 0$, so dass gilt: Ist $a \in L_G$ mit $|a| < \varepsilon$, so folgt $a = 0$. Eine Untergruppe von $\mathbb{R}$ mit dieser Eigenschaft nennt man auch **diskrete Untergruppe** von $\mathbb{R}^2$.

**Lemma 1.8** Eine Untergruppe $L \subset \mathbb{R}^2$ ist genau dann diskret, wenn es ein $\varepsilon > 0$ gibt, so dass der Abstand zwischen verschiedenen Elementen $a, b \in L$ mindestens $\varepsilon$ beträgt.

**Beweis :** Haben verschiedene Elemente in $L$ mindestens den Abstand $\varepsilon$, so folgt wegen $0 \in L$ für alle $a \neq 0$, dass $||a|| = ||a - 0|| \geq \varepsilon$ ist. Gilt umgekehrt $||a|| \geq \varepsilon$ für alle $a \neq 0$ aus $L$, so folgt für $a \neq b$ in $L$ wegen $a - b \in L$ auch $||a - b|| \geq \varepsilon$. Also ist der Abstand von $a$ und $b \geq \varepsilon$. □

**Satz 1.9** Sei $L$ eine diskrete Untergruppe von $\mathbb{R}^2$.

i) Eine beschränkte Teilmenge $M \subset \mathbb{R}^2$ enthält nur endlich viele Elemente aus $L$.

ii) Ist $L \neq \{0\}$, so enthält $L$ einen Vektor $a \neq 0$ minimaler Länge, d.h. für jedes $b \neq 0$ in $L$ gilt $||b|| \geq ||a||$.

**Beweis :**

i) Ist $M \subset \mathbb{R}^2$ beschränkt, so ist $M$ in einer genügend großen Kreisscheibe $S_r = \{x \in \mathbb{R}^2 : ||x|| \leq r\}$ enthalten. Es genügt zu zeigen, dass $L \cap S_r$ endlich ist. Sind $a$ und $b$ zwei verschiedene Punkte in $L$, so sind für geeignetes $\varepsilon > 0$ die offenen Kreisscheiben

$$\begin{aligned} D_{\varepsilon/2}(a) &= \{x \in \mathbb{R}^2 : ||x - a|| < \frac{\varepsilon}{2}\} \text{ und} \\ D_{\varepsilon/2}(b) &= \{x \in \mathbb{R}^2 : ||x - b|| < \frac{\varepsilon}{2}\} \end{aligned}$$

disjunkt, da $L$ diskret ist.

Wir können nach Vergrößern von $r$ annehmen, dass für alle $a \in L \cap S_r$ auch $D_{\varepsilon/2}(a)$ in $S_r$ enthalten ist.

Angenommen, $L \cap S_r$ wäre unendlich. Dann enthielte $S_r$ also unendlich viele disjunkte Kreisscheiben vom Radius $\varepsilon/2$. Das kann nicht sein, da der Flächeninhalt der Kreisscheibe $S_r$ endlich ist.

ii) Ist $L \neq 0$, so existiert ein $b \neq 0$ in $L$. Die Kreisscheibe $\{x \in \mathbb{R}^2 : ||x|| \leq ||b||\}$ vom Radius $||b||$ um 0 enthält nach i) nur endlich viele Elemente in $L$. In dieser endlichen Menge gibt es ein $a \in L$ mit $a \neq 0$, so dass $||a||$ minimal ist. Man beachte, dass $a$ nicht eindeutig bestimmt ist.

□

Den Beweis von i) des vorangehenden Satzes kann man mit ein paar topologischen Grundkenntnissen auch so führen: Ist $M$ beschränkt, so ist $M$ in einer kompakten Teilmenge $K \subset \mathbb{R}^2$ enthalten. Für verschiedene $a, b \in L$ ist höchstens eines der Elemente $a, b$ in einer beliebigen offenen Kreisscheibe vom Radius $\varepsilon/2$. Wir betrachten nun die offene Überdeckung von $K$, die aus den offenen Kreisscheiben vom Radius $\varepsilon/2$ um alle Punkte bedeutet. Da $K$ kompakt ist, enthält sie eine endliche Teilüberdeckung. Also ist $K \cap L$ endlich.
Nun können wir die diskreten Untergruppen von $\mathbb{R}^2$ folgendermaßen beschreiben:

**Satz 1.10** Für eine diskrete Untergruppe $L$ von $\mathbb{R}^2$ gibt es die folgenden drei Möglichkeiten:

i) $L = \{0\}$

ii) Es gibt ein $a \neq 0$ mit
$$L = \{ma : m \in \mathbb{Z}\} = \mathbb{Z}a,$$
d.h. $L$ ist die von $a$ erzeugte zyklische Untergruppe von $\mathbb{R}^2$.

iii) Es gibt zwei linear unabhängige Vektoren $a, b$ in $\mathbb{R}^2$ mit
$$L = \{ma + nb : m, n \in \mathbb{Z}\} = \mathbb{Z}a + \mathbb{Z}b.$$
In diesem Fall nennt man $L$ ein Gitter in $\mathbb{R}^2$ und das Erzeugendensystem $(a, b)$ heißt auch Gitterbasis von $L$.

**Beweis :** Wir nehmen an, dass $L \neq 0$ eine diskrete Untergruppe von $\mathbb{R}^2$ ist. Dann müssen wir zeigen, dass einer der Fälle ii) oder iii) eintritt.
**1. Fall:** Es gibt eine Gerade $l \subset \mathbb{R}^2$ mit $L \subset l$.
In diesem Fall wählen wir mit Hilfe von Satz 1.9 ii) einen Vektor $a \neq 0$ in $L$ mit minimaler Länge. Wir behaupten, dass
$$L = \{ma : m \in \mathbb{Z}\} = \mathbb{Z}a$$
gilt.

Da $L$ eine Untergruppe des $\mathbb{R}^2$ ist, gilt $\mathbb{Z}a \subset L$. Sei umgekehrt $v \in L$. Da $a$ ein Erzeuger der Geraden $l$ ist und $L \subset l$ gilt, gibt es ein $r \in \mathbb{R}$ mit $v = ra$. Wir können $r$ schreiben als $r = n + r_0$ mit $n \in \mathbb{Z}$ und $0 \leq r_0 < 1$. Dann ist $v - na = ra - na = r_0 a$ ein Vektor in $L$, für den

$$||v - na|| = r_0||a|| < ||a||$$

gilt. Aufgrund der Minimalität von $a$ folgt $v - na = 0$, d.h. $v = na$ liegt in der Tat in $\mathbb{Z}a$. Also ist $L$ vom Typ ii).
**2. Fall:** Es gibt zwei linear unabhängige Vektoren $(a', b')$ in $L$. Es sei $l = \langle a' \rangle$ die von $a'$ aufgespannte Gerade, und $a$ ein Vektor $\neq 0$ in $l \cap L$ mit minimaler Länge. Dann wissen wir nach dem ersten Fall

$$l \cap L = \mathbb{Z}a$$

Wir betrachten nun das Parallelogramm $P'$ mit den Eckpunkten $0, a, b'$ und $a + b'$.
$P'$ enthält als beschränkte Menge nach Satz 1.9 nur endlich viele Elemente aus $L$. Unter diesen endlich vielen Gitterpunkten wählen wir ein $b \notin l$ in $P' \cap L$ aus, dessen Abstand zur Gerade $l$ minimal ist. Hier ist der Abstand von $b$ zu $l$ natürlich definiert als

$$d(b, l) = \inf\{||b - c|| : c \in l\}.$$

Nun betrachten wir das Parallelogramm $P$ mit den Eckpunkten $0, a, b, a + b$.
Wir wollen nun zeigen, dass $P \cap L = \{0, a, b, a + b\}$ gilt. Es sei $c \neq 0$ in $P \cap L$. Dann zeigen wir zunächst, dass $c$ oder $c - a$ in $P'$ liegt. Es gilt nämlich $c = xa + yb$ mit $0 \leq x, y \leq 1$. Ferner ist $b \in P'$, also $b = ra + sb'$ für $0 \leq r, s \leq 1$. Daraus folgt

$$c = (x + ry)a + syb'$$

mit $0 \leq x + ry \leq 2$ und $0 \leq sy \leq 1$. Also ist entweder $c$ oder $c - a$ von der Form $ua + vb'$ für $0 \leq u, v \leq 1$, d.h. $c$ oder $c - a$ liegt in $P'$.
Ist $c \in P'$, so gilt entweder $c \in l$, d.h. $c = a$, oder es folgt aufgrund der Minimalität von $b$, dass $d(c, l) \geq d(b, l)$ gilt. Wir behaupten, dass daraus schon $y = 0$ oder $y = 1$ folgt. Ist nämlich $y \neq 0$, so ist der Abstand von $c = xa + yb$ zu dem Punkt $\lambda a \in l$ mit $\lambda \in \mathbb{R}$ gleich

$$||c - \lambda a|| = ||(x - \lambda)a + yb|| = y||b - \frac{\lambda - x}{y}a||.$$

Gehen wir auf beiden Seiten zum Infimum über alle $\lambda$ über, so folgt $d(c, l) \leq yd(b, l)$, wegen $d(c, l) \geq d(b, l)$ folgt somit $y = 1$.
Ist $c - a \in P'$ und $c \neq a$, so folgt aufgrund der Minimalität von $b$, dass $d(c - a, l) \geq d(b, l)$ gilt. Auch hier folgt daraus schon $y = 0$ oder $y = 1$. Ist nämlich $y \neq 0$, so gilt

für alle $\lambda a \in l (\lambda \in \mathbb{R})$

$$||c - a - \lambda a|| = ||(x - 1 - \lambda)a + yb|| = y||b - \frac{\lambda + 1 - x}{y} a||.$$

Daraus folgt wie oben

$$d(c, l) \leq y d(b, l),$$

woraus sich $y = 1$ ergibt.
Also ist $c = xa$ oder $c = xa + b$ für ein $x \in [0, 1]$. Ist $c = xa$, so liegt $c$ in $L \cap l = \mathbb{Z}a$, woraus wegen $c \neq 0$ bereits $c = a$ folgt. Ist $c = xa + b$, so ist $c - b \in L \cap l = \mathbb{Z}a$, woraus $x \in \{0, 1\}$, also $c = b$ oder $c = a + b$ folgt.
Somit gilt in der Tat $P \cap L = \{0, a, b, a + b\}$. Das folgende Lemma zeigt nun, dass $L = \{ma + nb : m, n \in \mathbb{Z}\}$, also vom Typ ii) ist. □

**Lemma 1.11** Es seien $a$ und $b$ linear unabhängige Vektoren in einer Untergruppe $L$ von $\mathbb{R}^2$. Ferner sei $P$ das Parallelogramm, das von $a$ und $b$ aufgespannt wird. Falls $L \cap P$ nur aus den Eckpunkten $0, a, b$ und $a + b$ besteht, so ist

$$L = \{ma + nb : m, n \in \mathbb{Z}\} = \mathbb{Z}a + \mathbb{Z}b.$$

**Beweis :** Es sei $v \in L$. Da $(a, b)$ eine Basis von $\mathbb{R}^2$ ist, können wir $v$ darstellen als $v = ra + sb$ mit $r, s \in \mathbb{R}$. Wir schreiben $r = m + r_0$ und $s = n + s_0$ mit $m, n \in \mathbb{Z}$ und $r_0, s_0 \in [0, 1[$. Dann ist $r_0 a + s_0 b = v - ma - nb$ in $P \cap L$, also einer der Eckpunkte $0, a, b$ und $a + b$. Wegen $r_0, s_0 < 1$ folgt $r_0 a + s_b b = 0$, also $v = ma + nb$. Daher ist $L \subset \{ma + nb : m, n \in \mathbb{Z}\}$. Da $L$ eine Untergruppe von $\mathbb{R}^2$ ist, die $a$ und $b$ enthält, gilt auch die andere Inklusion. □

Ein Element $v$ eines Gitters $L$ heißt **primitiv**, falls aus $v = mw$ mit $m \in \mathbb{Z}$ und $x \in L$ schon $v = \pm w$ folgt.

**Korollar 1.12** Jedes primitive Element eines Gitters lässt sich zu einer Gitterbasis ergänzen.

**Beweis :** Das zeigt man genauso wie den 2. Fall im Beweis von Satz 1.10. □

**Satz 1.13** Es sei $L \subset \mathbb{R}^2$ ein Gitter. Dann besitzt $L$ eine Gitterbasis $(a, b)$, die genau eine der folgenden Bedingungen erfüllt:

i) $||a|| < ||b|| < ||a - b|| < ||a + b||$.

In diesem Fall heißt $L$ **schiefes Gitter.**

ii) $||a|| < ||b|| < ||a - b|| = ||a + b||$

In diesem Fall heißt $L$ **rechtwinkliges Gitter.**

iii) $||a|| = ||b|| < ||a - b|| = ||a + b||$.

In diesem Fall heißt $L$ **quadratisches Gitter.**

iv) $||a|| < ||b|| = ||a - b|| < ||a + b||$.

In diesem Fall heißt $L$ **rechtwinklig flächenzentriertes oder Rautengitter.**

v) $||a|| = ||b|| = ||a - b|| < ||a + b||$.

In diesem Fall heißt $L$ **hexagonales Gitter.**

**Beweis :** Es sei $(a, b)$ eine Gitterbasis von $L$. Wir können nach Korollar 1.12 annehmen, dass $a$ ein Vektor minimaler Länge in $L$ ist. Indem wir evtl. $b$ durch $a - b$ ersetzen, können wir außerdem $||a - b|| \geq ||b||$ annehmen. Ersetzen wir dann ggf. noch $b$ durch $-b$, so können wir $||a + b|| \geq ||a - b||$ annehmen.
Also gilt

$$||a|| \leq ||b|| \leq ||a - b|| \leq ||a + b||.$$

Es gilt $||a - b|| = ||a + b||$ genau dann, wenn $\langle a, b\rangle = 0$ ist, d.h. wenn $a$ und $b$ senkrecht aufeinander stehen. In diesem Fall ist $||a - b||^2 = ||a||^2 + ||b||^2 > ||b||^2$, also tritt einer der Fälle ii) und iii) ein. Ist $||a - b|| < ||a + b||$, so muss einer der Fälle i), iv),v) oder

$$||a|| = ||b|| < ||a - b|| < ||a + b||$$

eintreten.
In diesem Fall bilden $a - b$ und $a + b$ ein Rechteck, und wir sind nach geeignetem Basiswechsel im Fall iv). □

# 2 Tapetengruppen

Jetzt wollen wir diskrete Untergruppen $G \subset B_2$ klassifizieren, für die die Untergruppe

$$L_G = \{a \in \mathbb{R}^2 : t_a \in G\}$$

des $\mathbb{R}^2$ ein Gitter ist. Solche Gruppen nennt man auch **Tapetengruppen**.
Wir haben zu Beginn von § 1 nachgerechnet, dass für Elemente $\beta_1 = t_{b_1}\gamma_1$ und $\beta_2 = t_{b_2}\gamma_2$ in $\mathcal{B}_2$ mit $b_1, b_2 \in \mathbb{R}^2$ und linearen Isometrien $\gamma_1, \gamma_2$ gilt

$$\beta_1\beta_2 = t_{b_1+\gamma_1(b_2)}\gamma_1\gamma_2.$$

Bezeichnen wir die Gruppe der linearen Isometrien des $\mathbb{R}^2$ mit $O(\mathbb{R}^2)$, so ist die Abbildung

$$\begin{aligned} \Phi : \mathcal{B}_2 &\rightarrow O(\mathbb{R}^2) \\ \beta = t_b\gamma &\mapsto \gamma \end{aligned}$$

ein Gruppenhomomorphismus. Also ist $\overline{G} := \Phi(G) \subset O(\mathbb{R}^2)$ eine Untergruppe. Sie wird auch Punktgruppe von $G$ genannt. Der Kern des surjektiven Gruppenhomomorphismus

$$\Phi : G \rightarrow \overline{G}$$

ist gerade die zu $L_G$ isomorphe Untergruppe $G \cap \mathcal{T}$ von $G$. Wir haben also eine exakte Sequenz $0 \rightarrow L_G \rightarrow G \rightarrow \overline{G} \rightarrow 0$. $\Phi$ bildet definitionsgemäß die Drehung $d_{\theta,a}$ um $a$ auf die Drehung $d_\theta$ um 0 ab, die Spiegelung $s_{l,a}$ auf die Spiegelung $s_l$ sowie die Gleitspiegelung $t_b s_{a,l} (b \in l)$ ebenfalls auf $s_l$. Mit $G$ ist auch $\overline{G}$ diskret.

**Lemma 2.1** Diskrete Untergruppen von $O(\mathbb{R}^2)$ sind endlich.

**Beweis :** Ist $H$ eine diskrete Untergruppe von $O(\mathbb{R}^2)$, so ist

$$H_0 = \{h \in H : h \text{ orientierungserhaltend }\}$$

eine Untergruppe von $H$.
Die orientierungserhaltenden Abbildungen in $H_o$ sind gerade die in $H_o$ enthaltenen Drehungen. Da $H$ diskret ist, ist auch $H_o$ diskret, also nach Übungsaufgabe 3, Blatt 3 endlich. Ist $H = H_o$, so sind wir fertig. Existiert ein $h \in H \setminus H_o$, so gilt für jedes $h' \in H \setminus H_o$, dass $hh'$ orientierungserhaltend, also in $H_o$ ist. Für $h'$ gibt es also auch nur endlich viele Möglichkeiten. □

**Erinnerung**(LAAG II):
In der linearen Algebra haben wir endliche Untergruppen von $\mathcal{B}_2$ studiert. Es gilt

→ Jede endliche Untergruppe $H$ von $\mathcal{B}_2$ hat einen Fixpunkt, d.h. es gibt ein $x \in \mathbb{R}^2$ mit $h(x) = x$ für alle $h \in H$.

→ Ersetzt man $H$ durch $t_{-x}Ht_x$ für den Fixpunkt $x$, so erhält man eine endliche Untergruppe von $\mathcal{B}_2$ mit Fixpunkt 0, d.h. eine endliche Untergruppe von $O(\mathbb{R}^2)$.

→ Jede endliche Untergruppe $H$ von $O(\mathbb{R}^2)$ ist entweder von der Form

$$C_n = \{d_\theta^k : k = 0, \ldots, n-1\}$$

mit $\theta = \frac{2\pi}{n}$

oder konjugiert zu einer Untergruppe der Form

$$D_n = \{d_\theta^i s^j : i = 0, \ldots, n-1, j = 0, 1\}$$

mit $\theta = \frac{2\pi}{n}$ (d.h. es gilt $H = g^{-1}D_n g$ für ein $g \in \mathcal{B}_2$).

Die Gruppe $C_n$ ist die von der Drehung um den Winkel $\frac{2\pi}{n}$ erzeugte endliche zyklische Untergruppe von $O(\mathbb{R}^2)$. Die Gruppe $D_n$ heißt Diedergruppe, sie besteht aus allen Produkten von Potenzen von $d_\theta$ und $s$ (der Spiegelung an der $x_1$-Achse). Man sagt auch, $D_n$ ist von $d_\theta$ und $s$ erzeugt. Mit unseren Rechenregeln Lemma 1.5 gilt

$$(d_\theta^i s)(d_\theta^k s^l) = d_\theta^{i-k} s^{l+1},$$

wobei wir $d_\theta^{n+2\pi} = d_\theta$ und $s^{n+2} = s^n$ benutzen können, um dieses Element in die oben angegebene Form zu bringen.
Also erhalten wir folgendes Korollar zu Lemma 2.1:

**Korollar 2.2** Für jede diskrete Untergruppe $H$ von $O(\mathbb{R}^2)$ gibt es ein $n \geq 1$, so dass $H = C_n$ oder $H$ konjugiert zu $D_n$ gilt.

Insbesondere ist für jede diskrete Gruppe $G$ in $\mathcal{B}_2$ die Punktgruppe $\overline{G}$ von der Form $\overline{G} = C_n$ oder $\overline{G}$ konjugiert zu $D_n$. Jetzt wollen wir das Gitter $L_G$ mit der Punktgruppe $\overline{G}$ in Verbindung bringen.

**Satz 2.3** Sei $G$ eine diskrete Untergruppe von $B_2$ mit Translationsgitter $L_G$ und Punktgruppe $\overline{G}$. Dann gilt für jedes $h \in \overline{G}$ die Inklusion $h(L_G) \subset L_G$.

Aus Satz 2.3 folgt für jedes $h \in G$, dass $h(L_G) \subset L_G$ und $h^{-1}(L_G) \subset L_G$ gilt. Also ist sogar $h(L_G) = L_G$. Daher besagt Satz 2.3, dass $\overline{G}$ eine Untergruppe der Symmetriegruppe von $L_G$ ist.

**Beweis von Satz 2.3 :** Wir müssen für jedes $a \in L_G$ und jedes $h \in \overline{G}$ zeigen, dass $h(a) \in L_G$ ist. Mit anderen Worten, ist $t_a \in G$ und $h = \Phi(g) \in \overline{G}$, so ist $t_{h(a)} \in G$ zu zeigen. Nun ist $G$ eine Gruppe, aus $g \in G$ und $t_a \in G$ folgt also $gt_ag^{-1} \in G$. Nach Definition von $\Phi$ gilt $g = t_bh$ für ein $b \in \mathbb{R}^2$. Also können wir berechnen

$$\begin{aligned} gt_ag^{-1} = t_bht_ah^{-1}t_{-b} &\overset{1.5}{=} t_bt_{h(a)}hh^{-1}t_{-b} \\ &= t_bt_{h(a)}t_{-b} = t_{h(a)}. \end{aligned}$$

Somit ist in der Tat $h(a) \in L_G$. □

Laut Satz 2.3 operiert für jede diskrete Gruppe $G$ die Punktegruppe $\overline{G}$ auf $L_G$. Allerdings operiert im allgemeinen nicht die gesamte Gruppe $G$ auf $L_G$!
Jetzt können wir folgenden wichtigen Satz beweisen, der uns helfen wird, die Tapetengruppen zu klassifizieren:

**Satz 2.4 (Kristallographisches Grundgesetz)** Es sei $H \subset O(\mathbb{R}^2)$ eine endliche Untergruppe der Symmetriegruppe eines Gitters $L$. Dann gilt

i) Jede Drehung $d_\theta$ in $H$ hat die Ordnung 1,2,3,4 oder 6 (d.h. $\theta = \frac{2\pi k}{n}$ für ein $n = 1, 2, 3, 4$ oder 6 und ein $0 \leq k < n$.)

ii) Es gibt ein $n \in \{1, 2, 3, 4, 6\}$, so dass $H = C_n$ oder $H$ konjugiert zu $D_n$ ist.

**Beweis :**

i) Da $H$ endlich ist, gibt es auch nur endlich viele Drehungen in $H$. Es sei $d_\theta \in H$ die Drehung mit dem kleinsten Drehwinkel $\theta \in [0, 2\pi[$. Ferner sei $a \neq 0$ ein Vektor minimaler Länge in $L$. Nach Voraussetzung ist $d_\theta(a) \in L$, also folgt

$$b = d_\theta(a) - a \in L.$$

Da $a$ minimale Länge hat, gilt $||b|| \geq ||a||$.

Nun gilt offenbar

$$\begin{aligned} ||b||^2 = ||a - d_\theta(a)||^2 &= ||a||^2 - 2\langle a, d_\theta(a)\rangle + ||d_\theta(a)||^2 \\ &= 2||a||^2 - 2\langle a, d_\theta(a)\rangle, \end{aligned}$$

woraus mit LAAG II, Definition 10.10 (Basiskurs)

$$\begin{aligned}\cos\theta &= \frac{\langle a, d_\theta(a)\rangle}{||a||\ ||d_\theta(a)||} \\ &= \frac{1}{2}\ \frac{2\langle a, d_\theta(a)\rangle}{||a||^2} \leq \frac{1}{2}\ \frac{||a||^2}{||a||^2} = \frac{1}{2}\end{aligned}$$

folgt.

Also ist der Winkel $\theta \in [0, 2\pi[$ größer oder gleich $\frac{\pi}{3} = \frac{2\pi}{6}$.

Da $H$ endlich ist, muss $\theta$ von der Form $\theta = \frac{2\pi}{n}$ für ein $n \in \mathbb{N}$ sein. Also muss $1 \leq n \leq 6$ sein.

Angenommen, $n = 5$, d.h. $\theta = \frac{2\pi}{5}$. Dann ist $b' = d_\theta^2(a) + a \in L$. Aus

$$2\theta = \frac{4\pi}{5} > \frac{4\pi}{6} = \frac{2\pi}{3}$$

folgt

$$-\frac{1}{2} > \cos 2\theta = \frac{\langle a, d_\theta^2(a)\rangle}{||a||\ ||d_\theta^2(a)||} = \frac{\langle a, d_\theta^2(a)\rangle}{||a||^2},$$

also $-||a||^2 > 2\langle a, d_\theta^2(a)\rangle$, woraus

$$\begin{aligned}||d_\theta^2(a) + a||^2 &= ||d_\theta^2(a)||^2 + 2\langle a, d_\theta(a)\rangle + ||a||^2 \\ &= 2||a||^2 + 2\langle a, d_\theta(a)\rangle \\ &< ||a||^2\end{aligned}$$

folgt.

Dies ist ein Widerspruch zu der Tatsache, dass $a$ minimale Länge hat. Somit kann der Fall $n = 5$ nicht eintreten.

Ist $d_\eta$ eine beliebige Drehung in $H$, so schreiben wir $\eta = k\theta + r$ mit $k \in \mathbb{N}_0$ und $r \in [0, \theta[$. Dann ist $d_{\eta - k\theta} = d_r$ in $H$, woraus wegen Minimalität von $\theta$ bereits $\eta = k\theta$ folgt. Somit ist $\eta = \frac{2\pi k}{n}$ für ein $n \in \{1, 2, 3, 4, 6\}$.

ii) Nach Korollar 2.2 ist $H = C_n$ oder konjugiert zu $D_n$ für ein $n \geq 1$. Da $C_n$ und $D_n$ jeweils eine Drehung um den Winkel $\theta = \frac{2\pi}{n}$ enthalten, muss nach i)

$$n \in \{1, 2, 3, 4, 6\}$$

gelten.

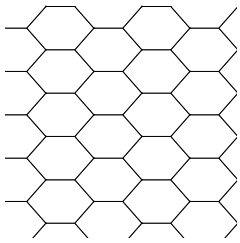
□

Wir wollen jetzt bis auf Isomorphie alle Tapetengruppen bestimmen.

**Satz 2.5** Es sei $\varphi : G \to G'$ ein Isomorphismus von Tapetengruppen. Dann bildet $\varphi$ Translationen auf Translationen, Drehungen auf Drehungen, Spiegelungen auf Spiegelungen und echte Gleitspiegelungen auf echte Gleitspiegelungen ab. Jede Isomorphie erhält also den Typ eines Elementes.

**Beweis :** Ist $g \in G$ eine Drehung oder Spiegelung, so hat $g$ endliche Ordnung, d.h. es gibt ein $d \in \mathbb{N}$ mit $g^d = 1$. Ist $g$ eine echte Translation oder eine echte Gleitspiegelung, so hat $g$ keine endliche Ordnung. Mit $g$ hat auch $\varphi(g)$ endliche bzw. keine endliche Ordnung.
Sei nun $t_a \in G$ eine echte Translation. Dann hat $\varphi(t_a)$ keine endliche Ordnung, d.h. $\varphi(t_a)$ ist eine echte Translation oder eine echte Gleitspiegelung. Ist $\varphi(t_a)$ eine echte Gleitspiegelung, so existiert eine Translation $t_b \in G'$, so dass der Vektor $b$ nicht auf der Spiegelgeraden liegt.
Es gibt ein $g \in G$ mit $\varphi(g) = t_b$. Da $t_b$ keine endliche Ordnung hat, ist $g$ eine echte Translation oder echte Gleitspiegelung. In jedem Fall ist $g^2$ eine Translation, kommutiert also mit $t_a$. Also kommutiert $\varphi(t_a)$ mit $\varphi(g^2) = t_{2b}$, was der Tatsache widerspricht, dass $b$ nicht auf der Spiegelgeraden liegt Also ist $\varphi(t_a)$ eine Translation.
Ist $g \in G$ eine echte Gleitspiegelung, so ist $\varphi(g)$ eine echte Translation oder eine echte Gleitspiegelung. Wenden wir das soeben Gezeigte auf $\varphi^{-1}$ an, so folgt, dass $\varphi(g)$ keine Translation sein kann.
Ist $g$ eine Spiegelung, so ist $g^2 = 1$, also erfüllt auch $\varphi(g)$ die Bedingung $\varphi(g)^2 = 1$. Somit ist $\varphi(g)$ eine Spiegelung oder eine Drehung.
Ist $\varphi(g)$ eine Drehung, so sei $t_b \in G$ eine Translation, für die der Vektor $b$ nicht senkrecht zur Spiegelachse steht. Dann ist mit Lemma 2.7 das Element $t_b g$ von $G$ eine echte Gleitspiegelung. Daher ist auch $\varphi(t_b g) = \varphi(t_b)\varphi(g)$ eine echte Gleitspiegelung. Das widerspricht der Tatsache, dass $\varphi(g)$ eine Drehung und damit orientierungserhaltend ist. Somit ist $\varphi(g)$ eine Spiegelung. Ist $g$ eine Drehung, so folgt wieder durch Betrachten von $\varphi^{-1}$, dass $\varphi(g)$ keine Spiegelung sein kann. Als Element endlicher Ordnung muss $\varphi(g)$ also eine Drehung sein. □

Jetzt können wir die Tapetengruppen bis auf Isomorphie klassifzieren.
Oft werden wir eine Tapetengruppe als Symmetriegruppe einer Figur angeben. Zeichnen wir dabei eine Figur $F$ wie die folgende:



so sei immer das entsprechende Muster in die gesamte Ebene $\mathbb{R}^2$ fortgesetzt gemeint. Oft geben wir eine Untergruppe von $\mathcal{B}_2$ über ihre Erzeuger an. Das bedeutet Folgendes:

**Definition 2.6** Es sei $H$ eine Gruppe und $h_1, \ldots, h_n \in H$. Die von $h_1, \ldots, h_n$ erzeugte Untergruppe $H' = \langle h_1, \ldots, h_n \rangle$ ist definiert als

$$H' = \left\{ \prod_{j=1}^{N} h_{ij}^{\sigma_j} : N \in \mathbb{N}, \sigma_j \in \{1, -1\} \text{ und } i_j \in \{1, \ldots, n\} \text{ für alle } j \right\}$$

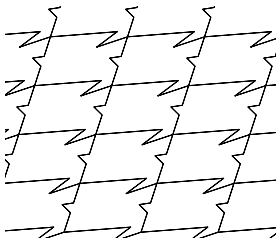
$H'$ besteht also aus beliebigen Produkten der Elemente $h_1, \ldots, h_n$ und $h_1^{-1}, \ldots, h_n^{-1}$. Man überzeugt sich sofort davon, dass diese Teilmenge von $H$ wirklich eine Untergruppe von $H$ ist.
Wir brauchen zur Vorbereitung noch folgendes Lemma.

**Lemma 2.7** Es sei $s_{l,a}$ eine Spiegelung und $t_b$ eine Translation in $B_2$. Dann ist $t_b s_{l,a}$ genau dann eine Spiegelung, wenn $b$ orthogonal zur Geraden $l$ ist. Ansonsten ist $t_b s_{l,a}$ eine echte Gleitspiegelung.

**Beweis :** Das Element $t_b s_{l,a}$ ist orientierungsumkehrend, also nach Satz 1.6 eine Spiegelung oder echte Gleitspiegelung. Eine Spiegelung ist es genau dann, wenn es einen Fixpunkt hat. Angenommen, es gilt $t_b s_{l,a}(y) = y$ für ein $y \in \mathbb{R}^2$. Wir schreiben $y = a + y_1 + y_2$ mit $y_1 \in l$ und $y_2 \in l^\perp$. Dann ist $t_b s_{l,a}(y) = a + y_1 - y_2 + b$. Aus $t_b s_{l,a}(y) = y$ folgt somit $y_2 = -y_2 + b$, also $b = 2y_2 \in l^\perp$.
Ist umgekehrt $b \in l^\perp$, so ist $s_{l,a}(a + \frac{1}{2}b) = a - \frac{1}{2}b$, also hat $t_b s_{l,a}$ den Fixpunkt $a + \frac{1}{2}b$, ist also eine Drehung. □

Nun sei $G$ eine Tapetengruppe mit Gitter $L_G$ und Punktegruppe $\overline{G}$. Nach Satz 2.4 ist $\overline{G} = C_n$ für $n = \{1, 2, 3, 4, 6\}$ oder $\overline{G}$ konjugiert zu $D_n$ für $n = \{1, 2, 3, 4, 6\}$.
Wir gehen jetzt nacheinander die Möglichkeiten für $\overline{G}$ durch. Aus Zeitmangel werden wir allerdings nicht alle Beweise vorführen.

**Satz 2.8** Ist $\overline{G} = 1$, so ist $G = L_G = \mathbb{Z}a + \mathbb{Z}b$ ein Gitter. Dann ist $G = \text{Sym}F$ für die folgende Figur $F$:

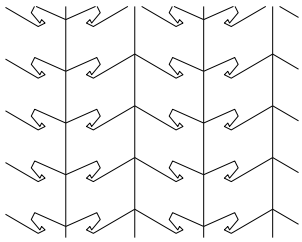


$G$ heißt vom Typ $p1$.

**Beweis :** Ist $\overline{G} = 1$, so folgt aus der exakten Sequenz $1 \to L_G \to G \to \overline{G} \to 1$, dass $G = L_G$ ist. $F$ besteht aus einem nicht-drehsymmetrischen Muster, das sich entlang eines schiefen Gitters wiederholt. Da ein schiefes Gitter offenbar von keiner Spiegelung und nur von der Drehung um $\pi$ invariant gelassen wird, ist Sym$F$ ein Gitter, also isomorph zu $G$. □

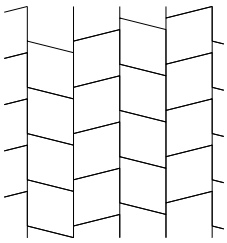
**Satz 2.9** Ist $\overline{G} = D_1$, also $\overline{G} = \{1, s_m\}$ für eine Spiegelung $s_m$, so gibt es bis auf Isomorphie drei Möglichkeiten für $G$.

i) $L_G$ besitzt eine Gitterbasis $(a, b)$ mit $a \perp b$, und für $l = \langle a \rangle$ ist $G \simeq \langle t_a, t_b, s_l \rangle$. Diese Gruppe besteht aus den Translationen in $L_G$ und allen Gleitspiegelungen der Form $t_{ma} s_{l, \frac{n}{2}b}$ für $n, m \in \mathbb{Z}$. Also ist $G \simeq \text{Sym}F$ für folgende Figur $F$:



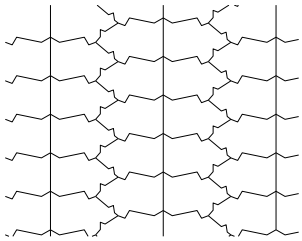
$G$ heißt vom Typ $pm$.

ii) $L_G$ besitzt eine Gitterbasis $(a, b)$ mit $a \perp b$ und für $l = \langle a \rangle$ ist $G$ isomorph zu der Gruppe, die von $t_a, t_b$ und der echten Gleitspiegelung $t_{\frac{1}{2}a} s_l$ erzeugt wird. Diese besteht aus den Translationen in $L_G$ und allen Gleitspiegelungen der Form $t_{(m+\frac{1}{2})a} s_{l, \frac{n}{2}b}$ für $n, m \in \mathbb{Z}$. Also ist $G \simeq \text{Sym}F$ für folgende Figur $F$:



$G$ heißt vom Typ $pg$.

iii) $L_G$ besitzt eine Gitterbasis $(a, c)$ mit $c = \frac{1}{2}(a + b)$ für ein $b \perp a$. Für $l = \langle a \rangle$ ist $G \simeq \langle t_a, t_c, s_l \rangle$. Diese Gruppe besteht aus den Translationen in $L_G$, den Gleitspiegelungen $t_{ma} s_{l, \frac{n}{2} b}$ für $m, n \in \mathbb{Z}$ sowie den echten Gleitspiegelungen $t_{\frac{m}{2} a} s_{l, \frac{n}{4} b}$ für $m, n \in \mathbb{Z}$. Also ist $G \simeq \mathrm{Sym} F$ für $F$:



$G$ heißt vom Typ $cm$.

**Beweis :** Da $\overline{G} = \{1, s_l\}$ ist, enthält $G$ keine echte Drehung und alle Spiegelungen und Gleitspiegelungen in $G$ haben als Spiegelachse eine affine Gerade der Form $x + l$. Nach Satz 2.3 lässt $s_l$ das Gitter $L_G$ invariant. Also kann $L_G$ kein schiefes Gitter sein. Gehen wir die Liste in Satz 1.13 durch, so stellen wir fest, dass $L_G$ zwei orthogonale Vektoren $a$ und $b$ enthält, wobei wir $a$ so wählen können, dass $l = \langle a \rangle$ gilt. Wir können außerdem annehmen, dass $a$ und $b$ primitiv sind.
Ist $(a, b)$ keine Gitterbasis von $L_G$, so gibt es nach Lemma 1.11 einen Punkt $c \in L_G$ im Parallelogramm $P$, das von $a$ und $b$ aufgespannt wird, der kein Eckpunkt ist. Schreiben wir $c = ra + sb$ mit $0 \leq r, s \leq 1$, so ist

$$c + s_l(c) = 2ra \in L_G \cap \langle a \rangle.$$

Ferner ist

$$2c - (c + s_l c) = 2sb \text{ in } L_G \cap \langle b \rangle,$$

woraus $s \in \{0, \frac{1}{2}, 1\}$ folgt. Da $c$ keiner der Eckpunkte ist und $a$ und $b$ primitiv sind, folgt

$$c = \frac{1}{2}(a + b).$$

In diesem Fall ist $L_G$ also ein Rautengitter.
Enthält $G$ eine Spiegelung $s_{l,y}$, so ersetzen wir $G$ durch die isomorphe Gruppe $t_y G t_{-y}$ und können annehmen, dass $s_l$ in $G$ liegt. Enthält $G$ keine Spiegelung, so sei $t_x s_{l,y}$ eine echte Gleitspiegelung in $G$. Wir ersetzen wieder $G$ durch $t_{-y} G t_y$ und können dann $y = 0$ annehmen. Also ist $t_x s_l \in G$ mit $0 \neq x \in l$. Indem wir mit geeignetem $t_{ma}, m \in \mathbb{Z}$ multiplizieren, können wir wegen $s_l \notin G \quad x = \lambda a$ für $0 < \lambda < 1$ annehmen. Dann ist $t_{2x} = (t_x s_l)^2 \in G$, also $2x \in L_G \cap l = \mathbb{Z}a$, woraus $x = \frac{1}{2}a$ folgt.
Somit enthält $G$ entweder $s_l$ oder $t_{\frac{1}{2}a} s_l$. Wir haben also insgesamt vier Fälle zu untersuchen.

**1. Fall:** $s_l \in G, (a, b)$ Gitterbasis
Ist dann $g \in G \setminus L_G$, so ist $g = t_x s_{l,y}$ eine Spiegelung oder echte Gleitspiegelung. Schreiben wir $y = \alpha a + \beta b$ mit $\alpha, \beta \in \mathbb{R}$, so ist $y + l = \beta b + l$, also können wir $y \in \langle b \rangle$ annehmen. Dann ist

$$g s_l = t_x t_y s_l t_{-y} s_l \in G,$$

also $x + y - s_l(y) = x + 2y \in L_G$, woraus

$$x \in \mathbb{Z}a \text{ und } y \in \frac{1}{2}\mathbb{Z}b$$

folgt. Somit liegt $g$ in $\langle t_a, t_b, s_l \rangle$. Wir sind also im Fall i) der Behauptung.

**2. Fall:** $t_{\frac{1}{2}a} s_l \in G$, $(a, b)$ Gitterbasis
Ist dann $g \in G \setminus L_G$, so ist wie oben $g = t_x s_{l,y}$ mit $x \in \langle a \rangle$ und $y \in \langle b \rangle$. Also ist

$$t_{\frac{1}{2}a} s_l g = t_{\frac{1}{2}a} s_l t_x t_y s_l t_{-y} \in G,$$

woraus

$$(x + \frac{1}{2}a) - 2y \in L_G$$

folgt. Somit ist $(x + \frac{1}{2}a) \in \mathbb{Z}a$ und $y \in \frac{1}{2}\mathbb{Z}b$. Wir sind also im Fall ii) der Behauptung.

**3. Fall:** $s_l \in G, (a, c)$ Gitterbasis für $c = \frac{1}{2}(a + b)$
Ist dann $g \in G \setminus L_G$, so ist wieder $g = t_x s_{l,y}$ mit $x \in \langle a \rangle$ und $y \in \langle b \rangle$. Also folgt $g s_l = t_x t_y s_l t_{-y} s_l \in G$, und somit

$$x + y - s_l(y) = x + 2y \in L_G = \mathbb{Z}a + \mathbb{Z}c.$$

Also liegt

$$g = t_{x+2y}s_l$$

in der von $s_l, t_a$ und $t_c$ erzeugten Gruppe, wir sind also im Fall iii) der Behauptung.

**4. Fall:** $t_{\frac{1}{2}a}s_l \in G, (a, c)$ Gitterbasis für $c = \frac{1}{2}(a + b)$
Dann ist

$$t_{-\frac{1}{2}(a+b)}t_{\frac{1}{2}a}s_l = t_{-\frac{1}{2}b}s_l \in G$$

Nach Lemma 2.7 ist das eine Spiegelung. Ersetzen wir $G$ durch die isomorphe Gruppe $t_{-\frac{1}{4}b}Gt_{\frac{1}{4}b}$, so können wir annehmen, dass $s_l \in G$ ist, also sind wir im Fall iii) der Behauptung. □

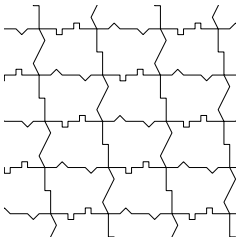
**Satz 2.10** Wir nehmen an, dass $\overline{G}$ die Drehung $d_\pi$ enthält, aber keine weiteren echten Drehungen. Dann gibt es folgende Möglichkeiten für $G$:

i) Für eine Gitterbasis $(a, b)$ von $L_G$ ist

$$G \simeq \langle t_a, t_b, d_\pi \rangle$$

Diese Gruppe besteht aus den Translationen in $L_G$ und allen Drehungen der Form $d_{\pi,\frac{ma+nb}{2}}$ für , $m, n \in \mathbb{Z}$.

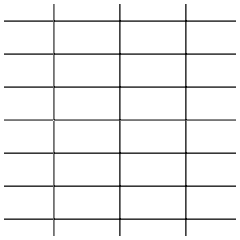
Also ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



$G$ heißt vom Typ $p2$.

ii) $L_G$ besitzt eine Gitterbasis $(a, b)$ mit $a \perp b$, und für $l = \langle a \rangle$ ist $G \simeq \langle t_a, t_b, d_\pi, s_l \rangle$.

Dann ist $G \simeq$ Sym$F$ für folgende Figur $F$:



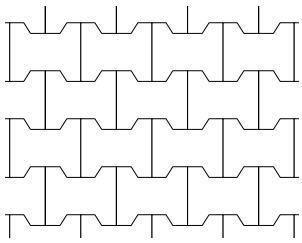
$G$ besteht aus den Translationen in $L_G$, den Drehungen $d_{\pi,\frac{ma+nb}{2}}$ für $m,n \in \mathbb{Z}$ sowie den (Gleit-)-Spiegelungen $t_{ma}s_{l,\frac{n}{2}b}$ und $t_{mb}s_{l^\perp,\frac{n}{2}b}$ für $m,n \in \mathbb{Z}$.

$G$ heiß vom Typ $pmm$.

iii) $L_G$ besitzt eine Gitterbasis der Form $(a,c)$ mit $c = \frac{1}{2}(a+b)$ und $a \perp b$, und für $l = \langle a \rangle$ ist $G \simeq \langle t_a, t_c, d_\pi, s_l \rangle$.

Also besteht $G$ aus den Translationen in $L_G$, den Drehungen $d_{\pi,\frac{ma+nc}{2}}$ für $m,n \in \mathbb{Z}$, den (Gleit-)spiegelungen $t_{ma}s_{l,\frac{n}{2}b}$ und $t_{mb}s_{l^\perp,\frac{n}{2}a}$, sowie den echten Gleitspiegelungen $t_{\frac{m}{2}a}s_{l,\frac{n}{4}b}$ und $t_{\frac{m}{2}b}s_{l,\frac{n}{4}a}$, jeweils für $m,n \in \mathbb{Z}$.

Also ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:

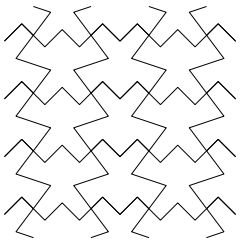


$G$ heißt vom Typ $cmm$.

iv) $L_G$ besitzt eine Gitterbasis $(a,b)$ mit $a \perp b$ und für $l = \langle a \rangle$ ist

$$G \simeq \langle t_a, t_b, d_\pi, s_{l,\frac{1}{4}b} \rangle$$

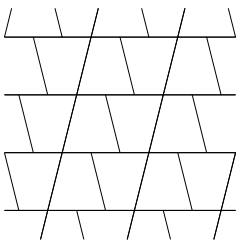
Dann ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



$G$ heißt vom Typ $pmg$.

v) $L_G$ besitzt eine Gitterbasis der Form $(a, b)$ mit $a \perp b$ und für $l = \langle a \rangle$ ist $G \simeq \langle t_a, t_b, d_\pi, t_{\frac{1}{2}a} s_{l\,\frac{1}{4}b} \rangle$.

Dann ist $G \simeq \mathrm{Sym} F$ für folgende Figur $F$:



$G$ heißt vom Typ $pgg$.

**Beweis :** Da $\overline{G}$ die Drehung $d_\pi$ enthält, enthält $G$ eine Drehung der Form $t_x d_\pi$ für ein $x \in \mathbb{R}^2$. Es ist $t_x d_\pi = t_{x/2} d_\pi d_{-x/2} = d_{\pi, \frac{x}{2}}$. Wir ersetzen $G$ durch die zu $G$ isomorphe Gruppe $t_{-\frac{x}{2}} G t_{\frac{x}{2}}$ und können annehmen, dass $d_\pi \in G$ gilt.
Ist $d_{\theta,y}$ eine beliebige echte Drehung in $G$, so ist $\overline{d_{\theta,y}} = d_\theta \in \overline{G}$, also ist $\theta = \pi$.
Aus $d_{\pi,y} \in G$ folgt $t_{2y} = d_{\pi,y} d_\pi \in G$, also $2y \in L_G$. Daher ist $d_{\pi,y} = t_{2y} d_\pi$ in der von $d_\pi$und $t_a, t_b$ erzeugten Untergruppe von $\mathcal{B}_2$, wenn $\alpha, \beta$ eine Gitterbasis von $L_G$ ist. Enthält $G$ keine Spiegelungen oder Gleitspiegelungen, so folgt daraus bereits $G \simeq \langle t_a, t_b, d_\pi \rangle$ für eine Gitterbasis $(a, b)$ von $L_G$, d.h. wir sind im Fall i).
Wir können also annehmen, $G$ enthält eine Gleitspiegelung $t_x s_{l,y}$. Dann ist $s_l \in \overline{G}$ und auch $s_{l^\perp} = s_l d_\pi \in \overline{G}$. Da $L_G$ von $\overline{G}$ invariant gelassen wird, kann $L_G$ kein schiefes Gitter sein. Wie im Beweis von Satz 2.9 finden wir also primitive Vektoren $a$ und $b$ in $L_G$ mit $l = \langle a \rangle$ und $a \perp b$. Somit ist $l^\perp = \langle b \rangle$.

Enthält $G$ eine Spiegelung $s_{l,y}$, so können wir wie in Satz 2.9 $y \in l^\perp$ annehmen. Dann enthält $G$ auch $s_{l,y}d_\pi = t_y s_l t_{-y} d_\pi = t_{2y} s_l d_\pi = t_{2y} s_{l^\perp}$, woraus nach Quadrieren $4y \in L_G$ folgt. Also gilt $4y \in L_G \cap l^\perp = \mathbb{Z}b$, d.h. $y \in \frac{1}{4}\mathbb{Z}b$.
Ist $y \in \frac{1}{2}\mathbb{Z}b$, so ist $s_l = t_{-2y} s_{l,y} \in G$. Also liegt entweder $s_l$ oder $s_{l,\frac{1}{4}b}$ in $G$. Ein analoges Argument zeigt, dass entweder $s_{l^\perp}$ oder $s_{l^\perp,\frac{1}{4}a}$ in $G$ liegen, wenn $G$ eine Spiegelung mit zu $l^\perp$ paralleler Achse enthält.
Enthält $G$ keine Spiegelung der Form $s_{l,y}$, aber eine echte Gleitspiegelung $t_x s_{l,y}$ mit $x \in l$ und $y \in l^\perp$, so folgt $2x \in L_G \cap l = \mathbb{Z}a$ und $x \notin L_G \cap l = \mathbb{Z}a$, also $x \in \frac{1}{2}\mathbb{Z}a \setminus \mathbb{Z}a$. Indem wir mit geeignetem $t_{ma}(m \in \mathbb{Z})$ multiplizieren, erhalten wir $t_{\frac{1}{2}a} s_{l,y} \in G$. Also enthält $G$ auch

$$t_{\frac{1}{2}a} s_{l,y} d_\pi = t_{\frac{1}{2}a} t_y s_l t_{-y} d_\pi = t_{\frac{1}{2}a+2y} s_{l^\perp},$$

woraus nach Quadrieren

$$\frac{1}{2}a + 2y + s_{l^\perp}(\frac{1}{2}a + 2y) = 4y \in L_G$$

folgt.
Wie oben schließen wir, dass entweder $t_{\frac{1}{2}a} s_l$ oder $t_{\frac{1}{2}a} s_{l,\frac{1}{4}b}$ in $G$ liegen.
Ein analoges Argument zeigt im Fall, dass $G$ keine Spiegelung, aber eine echte Gleitspiegelung mit zu $l^\perp$ paralleler Achse enthält, dass $t_{\frac{1}{2}b} s_{l^\perp}$ oder $t_{\frac{1}{2}b}, s_{l^\perp \frac{1}{4}a}$ in $G$ liegen.
Da $\overline{G}$ nur die Drehung $d_\pi$ enthält, kann $\overline{G}$ höchstens die Spiegelungen $s_l$ und $s_{l^\perp}$ enthalten.
Nun betrachten wir folgende Fälle:

1) $s_l \in G$. Dann ist auch $s_{l^\perp} = s_l d_\pi \in G$.

   Ist $(a, b)$ eine Gitterbasis von $L_G$, so gilt für eine beliebige Gleitspiegelung $t_x s_{l,y}(x \in l, y \in l^\perp)$ in $G$:

   $$t_x, s_{l,y} s_l = t_{x+2y} \in G, \text{ also } x + 2y \in L_G,$$

   woraus $x \in \mathbb{Z}a, y \in \frac{1}{2}\mathbb{Z}b$ folgt. Somit ist $t_x s_{l,y} \in \langle t_a, t_b, s_l d_\pi \rangle$.

   Analog ist eine beliebige Gleitspiegelung an einer zu $l^\perp$ parallelen Achse in $\langle t_a, t_b, s_{l^\perp} \rangle \subset \langle t_a, t_b, s_l, d_\pi \rangle$. enthalten, wir sind also im Fall ii).

2) Es sei wieder $s_l \in G$, aber $(a, b)$ keine Gitterbasis von $L_G$. Dann zeigt man wie in Satz 2.9, dass $(a, c)$ für $c = \frac{1}{2}(a + b)$ eine Gitterbasis von $L_G$ ist.

   Ist nun $t_x s_{l,y}(x \in l, y \in l^\perp)$ eine beliebige Gleitspiegelung in $G$, so folgt nach Multiplikation mit $s_l$ wieder $x + 2y \in L_G$, d.h. $t_{x+2y} \in \langle t_a, t_c \rangle$ woraus $t_x, s_{l,y} \in \langle t_a, t_c, s_l, d_\theta \rangle$ folgt.

Analog verfährt man für Gleitspiegelungen entlang zu $l^\perp$ parallelen Achsen. Also sind wir im Fall iii).

3) Es sei $s_l \notin G$, also $s_{l,\frac{1}{4}b} \in G$. Dann folgt $s_{l^\perp} \notin G$. Ferner ist die Gleitspiegelung

$$s_{l,\frac{1}{4}b} d_\pi = t_{\frac{1}{2}b} s_l d_\pi = t_{\frac{1}{2}b} s_{l^\perp} \in G.$$

Falls nun die Spiegelung $s_{l^\perp,\frac{1}{4}a} \in G$ ist, so ist auch

$$s_{l^\perp,\frac{1}{4}a} s_{l,\frac{1}{4}b} = t_{\frac{1}{2}a} s_{l^\perp} t_{\frac{1}{2}b} s_l = t_{\frac{1}{2}(a+b)}$$

in $G$, also ist $L_G$ ein Rautengitter, erzeugt von $(a, c)$ mit $c = \frac{1}{2}(a + b)$. Insbesondere enthält $G$ die Drehung $t_c d_\pi = d_{\pi,\frac{1}{4}(a+b)}$. Die zu $G$ isomorphe Gruppe $t_{-\frac{1}{4}(a+b)} G t_{\frac{1}{4}(a+b)}$, enthält somit $d_\pi$ und die Spiegelungen

$$\begin{aligned} s_l &= d_{-\frac{1}{4}(a+b)} s_{l,\frac{1}{4}b} d_{\frac{1}{4}(a+b)} \text{ sowie} \\ s_{l^\perp} &= d_{-\frac{1}{4}(a+b)} s_{l^\perp,\frac{1}{4}a} d_{\frac{1}{4}(a+b)}, \end{aligned}$$

somit sind wir wieder bei 2).

4) Es sei $s_l \notin G$, aber $s_{l,\frac{1}{4}b} \in G$ und $G$ enthalte keine Spiegelung an zu $l^\perp$ paralleler Achse. Dann enthält $G$ die Gleitspiegelung

$$s_{l,\frac{1}{4}b} d_\pi = t_{\frac{1}{2}b} s_{l^\perp}.$$

Wäre $(a, b)$ keine Gitterbasis, so könnten wir wie in Satz 2.9 zeigen, dass $c = \frac{1}{2}(a + b)$ in $L_G$ liegt. Dann wäre $t_{-\frac{1}{2}(a+b)} s_{l^\perp,\frac{1}{4}b} = t_{-\frac{1}{2}a} s_{l^\perp}$ in $G$, was unserer Annahme widerspricht, da dieses Element nach Lemma 2.7 eine Spiegelung ist.

Wir behaupten nun, dass $G \simeq \langle t_a, t_b, d_\pi, s_{l,\frac{1}{4}b} \rangle$ ist, d.h. dass wir im Fall iv) sind. Ist nämlich für $x \in l$ und $y \in l^\perp$ das Element $t_x s_{l,y} \in G$ eine beliebige Gleitspiegelung an zu $l$ paralleler Achse, so folgt

$$t_x s_{l,y} s_{l,\frac{1}{4}b} = t_x t_y s_l t_{-y} t_{\frac{1}{4}b} s_l t_{-\frac{1}{4}b} = t_{x+2y+\frac{1}{2}b} \in G,$$

d.h.

$$t_{x+2y+\frac{1}{2}b} \in \langle t_a, t_b \rangle.$$

Also ist $t_x s_{l,y} \in \langle t_a, t_b, s_{l,\frac{1}{4}b} \rangle$.

Ist $t_y s_{l^\perp,x} \in G$ eine Gleitspiegelung an zu $l^\perp$ paralleler Achse mit $y \in l^\perp, x \in l$, so folgt

$$t_y s_{l^\perp,x}, s_{l,\frac{1}{4}b} d_\pi = t_y s_{l^\perp,x} t_{\frac{1}{2}b} s_{l^\perp} = t_{y+2x+\frac{1}{2}b} \in G,$$

also

$$t_y s_{l^\perp,x} \in \langle t_a, t_b, d_\pi, s_{l\frac{1}{4}b} \rangle.$$

5) Angenommen, $G$ enthält keine Spiegelung an einer zu $l$ parallelen Achse. Falls $G$ eine Spiegelung an einer zu $l^\perp$ parallelen Achse enthält, so vertauschen wir $a$ und $b$ (und damit $l$ und $l^\perp$) und sind im Fall 4).

6) Es bleibt der Fall, dass $G$ nur echte Gleitspiegelungen entlang zu $l$ und $l^\perp$ parallelen Achsen enthält. Dann kann weder $t_{\frac{1}{2}a}s_l$ noch $t_{\frac{1}{2}b}s_{l^\perp}$ in $G$ sein, denn

$$t_{\frac{1}{2}a}s_l d_\pi = t_{\frac{1}{2}a}s_{l^\perp}$$

und

$$t_{\frac{1}{2}b}s_{l^\perp} d_\pi = t_{\frac{1}{2}b}s_l$$

sind Spiegelungen nach Lemma 2.7. Wie in 4) zeigt man, dass $(a, b)$ eine Gitterbasis ist. Also ist $t_{\frac{1}{2}a}s_{l,\frac{1}{4}b} \in G$ und $t_{\frac{1}{2}b}s_{l^\perp,\frac{1}{4}a} \in G$.

Man beachte, dass

$$t_{\frac{1}{2}b}s_{l^\perp,\frac{1}{4}a} = t_{\frac{1}{2}a}s_{l\frac{1}{4}b}d_\pi$$

gilt. Mit den üblichen Argumenten zeigt man

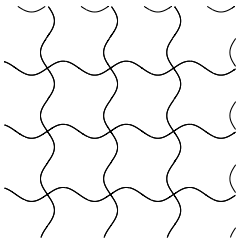
$$G \simeq \langle t_a, t_b, d_\pi, t_{\frac{1}{2}a}, s_{l,\frac{1}{4}b}\rangle.$$

□

**Satz 2.11** Wir nehmen an, dass $\overline{G}$ die Drehung $d_{\pi/2}$ enthält. Dann gibt es folgende Möglichkeiten für $G$.

i) Es gibt eine Gitterbasis $(a, b)$ von $L_G$ mit $b = d_{\pi/2}(a)$ und $G \simeq \langle t_a, d_{\pi/2}\rangle$

Also ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:

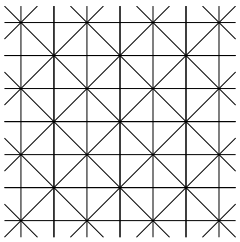


$G$ heißt vom Typ $p4$.

ii) $L_G$ hat eine Gitterbasis $(a, b)$ mit $b = d_{\pi/2}(a)$ und für $l = \langle a \rangle$ ist

$$G \simeq \langle t_a, d_{\pi/2}, s_l \rangle.$$

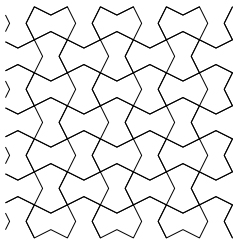
Also ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



$G$ heißt vom Typ $p4m$.

iii) $L_G$ besitzt eine Gitterbasis $(a, b)$ mit einem kürzesten Vektor $a$ und $b = d_{\pi/2}(a)$, und für $l = \langle a \rangle$ ist $G \simeq \langle t_a, d_{\pi/2}, t_{\frac{1}{2}a} s_{l,\frac{1}{4}b} \rangle$.

Dann ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



$G$ heißt vom Typ $p4g$.

**Beweis :** Da $\overline{G}$ eine Drehung um $\frac{\pi}{2}$ enthält und $L_G$ invariant lässt, muss $L_G$ ein quadratisches Gitter sein. Es sei $(a, b)$ eine Gitterbasis von $L_G$ mit $a \perp b$ und $||a|| = ||b||$, wobei $a$ und $b$ Vektoren minimaler Länge sind. Dann ist $d_{\pi/2}a = \pm b$, wir können also $d_{\pi/2}a = b$ annehmen. $G$ enthält eine Drehung der Form $d_{\frac{\pi}{2},y}$ für ein $y \in \mathbb{R}^2$. Nach Übergang zu der isomorphen Gruppe $t_{-y/2}Gt_{y/2}$ können wir annehmen, dass $d_\pi \in G$ gilt.

**1. Fall:** $G$ enthält keine Spiegelung oder Gleitspiegelung.

Dann ist jedes Element in $G$ eine Translation oder Drehung. Ist $g \in G$ eine Translation, also $g = t_c$ für ein $c \in L_G$, dann ist $g \in \langle t_a, t_b \rangle$. Wegen $d_{\pi/2} t_a d_{\pi/2}^{-1} = t_{d_{\pi/2}(a)} d_{\pi/2} d_{\pi/2}^{-1} = t_b$ folgt also $g \in \langle t_a, d_{\pi/2} \rangle$.
Ist $g = d_{\theta,y} \in G$ eine Drehung, so ist $d_\theta \in \overline{G}$. Da $d_{\pi/2} \in \overline{G}$ ist, folgt nach Satz 2.4, dass $\theta = k\frac{\pi}{2}$ für ein $k \in \{0,1,2,3\}$ ist.
Somit ist

$$d_{\theta,y} d_{-k\pi/2} = t_y d_\theta t_{-y} d_{-k\pi/2} = t_{y+d_\theta(-y)} \in G,$$

also $y + d_\theta(-y) \in L_G$. Somit ist $d_{\theta,y} \in \langle t_a, t_b, d_{\pi/2} \rangle = \langle t_a, d_{\pi/2} \rangle$.
Also gilt hier $G = \langle t_a, d_{\pi/2} \rangle$, d.h. wir sind im Fall i).
Wir können also annehmen, dass $\overline{G}$ eine Spiegelung enthält. Diese lässt $L_G$ invariant. Also muss sie als Spiegelachse die Gerade $\langle a \rangle, \langle b \rangle, \langle a+b \rangle$ oder $\langle a-b \rangle$ haben. Nach Multiplikation mit Potenzen von $d_{\pi/2}$ sehen wir, dass $\overline{G}$ in jedem Fall die Spiegelung $s_l$ an $l = \langle a \rangle$ enthält. Somit ist $t_x s_{l,y} \in G$ für ein $x \in l$ und ein $y \in l^\perp$. Wie im Beweis von Satz 2.9 folgt $x \in -\frac{1}{2}\mathbb{Z}a$ und $y \in \frac{1}{4}\mathbb{Z}b$, d.h. eines der Elemente $s_l, s_{l,\frac{1}{4}b}, t_{\frac{1}{2}a} s_l$ oder $t_{\frac{1}{2}a} s_{l\frac{1}{4}b}$ liegt in $G$.
**2. Fall:** $s_l \in G$.
Dann sind auch die Spiegelungen an $l^\perp = \langle b \rangle$, an $\langle a+b \rangle$ und an $\langle a-b \rangle$ in $G$. Mit den üblichen Argumenten zeigt man $G \simeq \langle t_a, d_{\pi/2}, s_l \rangle$, wir sind also im Fall ii).
**3. Fall:** $s_l \notin G$.
Wäre $s_{l\frac{1}{4}b} \in G$, so wäre auch

$$d_{\pi/2} s_{l,\frac{1}{4}b} d_{\pi/2} = t_{d_{\pi/2}(\frac{1}{2}b)} d_{\pi/2} s_l d_{\pi/2} = t_{-\frac{1}{2}a} s_l$$

in $G$, also

$$s_{l,\frac{1}{4}b} t_{-\frac{1}{2}a} s_l = t_{\frac{1}{2}(b-a)} \in G,$$

somit $\frac{1}{2}(b-a) \in L_G$. Da dies ein Vektor kleinerer Länge als $a$ ist, kann dieser Fall nicht eintreten. Wäre $t_{\frac{1}{2}a} s_l \in G$, so folgte $d_{\pi/2} t_{\frac{1}{2}a} s_l d_{\pi/2} = t_{d_{\pi/2}(\frac{1}{2}a)} d_{\pi/2} s_l d_{\pi/2} = t_{-\frac{1}{2}b} s_l \in G$, also wieder $t_{\frac{1}{2}(a-b)} \in G$, was zu einem Widerspruch führt.
Also muss $t_{\frac{1}{2}a} s_{l,\frac{1}{4}b} \in G$ gelten. Wie zuvor zeigt man $G = \langle t_a, d_{\pi/2}, t_{\frac{1}{2}a} s_{l,\frac{1}{4}b} \rangle$. □

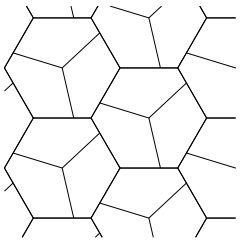
Mit den Sätzen 2.8, 2.9, 2.10, 2.11 haben wir alle Tapetengruppen $G$ klassifiziert, für die $\overline{G}$ nur Drehungen der Ordnung 1,2 oder 4 enthält. Nach dem kristallographischen Grundgesetz Satz 2.4 bleiben die Fälle zu untersuchen, in denen $\overline{G}$ eine Drehung der Ordnung 3 oder 6 enthält.

**Satz 2.12** Es sei $d_{2\pi/3} \in \overline{G}$, aber $d_{2\pi/6} \notin \overline{G}$. Dann ist $L_G$ ein hexagonales Gitter, und es gibt folgende Möglichkeiten für $G$.

i) Es gibt eine Gitterbasis von $L_G$ der Form $(a, b)$ mit $b = d_{\pi/3(a)}$ und

$$G \simeq \langle t_a, t_b, d_{2\pi/3} \rangle.$$

Dann enthält $G$ keine (Gleit-)spiegelungen. Es ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:

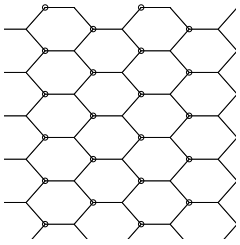


$G$ heißt vom Typ $p3$.

ii) Es gibt eine Gitterbasis von $L_G$ der Form $(a, b)$ mit einem kürzesten Vektor $a$ und $b = d_{\pi/3}(a)$ und für $l = \langle a \rangle$ gilt

$$G \simeq \langle t_a, t_b, d_{2\pi/3}, d_{\pi/3} s_l \rangle.$$

Dann liegen alle Drehmittelpunkte auf Spiegelachsen. Es ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



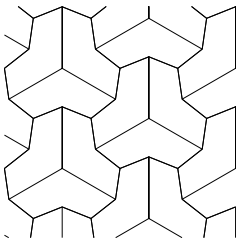
$G$ heißt vom Typ $p3m1$.

iii) Es gibt eine Gitterbasis von $L_G$ der Form $(a, b)$ mit einem kürzesten Vektor $a$ und $b = d_{\pi/3}(a)$, und für $l = \langle a \rangle$ gilt

$$G \simeq \langle t_a, t_b, d_{2\pi/3}, s_l \rangle.$$

In diesem Fall gibt es Drehmittelpunkte, die nicht auf Spiegelgeraden liegen.

Es ist $G \simeq \mathrm{Sym}F$ für $F$:



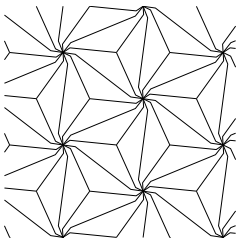
$G$ heißt vom Typ $p31m$.

(Vorsicht: Die letzten beiden Bezeichnungen gehen in der Literatur etwas durcheinander.).

**Satz 2.13** Es sei $d_{\pi/3} = d_{2\pi/b}$ in $\overline{G}$. Dann ist $L_G$ ein hexagonales Gitter, und es gibt folgende Möglichkeiten für $G$:

i) Es gibt eine Gitterbasis $(a, b)$ von $L_G$ mit einem kürzesten Vektor $a$ und $b = d_{\pi/3}(a)$ und $G \simeq \langle t_a, d_{\pi/3} \rangle$.

Dann enthält $G$ keine (Gleit-)spiegelungen. Es ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



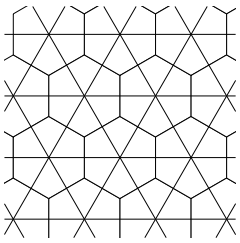
$G$ heißt vom Typ $p6$.

ii) Es gibt eine Gitterbasis $(a, b)$ von $L_G$ mit einem kürzesten Vektor $a$ und $b = d_{\pi/3}(a)$, so dass für $l = \langle a \rangle$

$$G \simeq \langle t_a, d_{\pi/3}, s_l \rangle$$

gilt.

Dann enthält $G$ auch die Spiegelungen an den Geraden im Winkel $\pi/6, \pi/3, \pi/2, 2\pi/3, 5\pi/6$ an $l$. Es ist $G \simeq \mathrm{Sym}F$ für folgende Figur $F$:



$G$ heißt vom Typ $p6m$.

Damit haben wir alle Tapetengruppen bis auf Isomorphie bestimmt.

Um den Isomorphietyp einer Tapetengruppe $G$ zu bestimmen, kann man wie folgt vorgehen:

<table>
<tr><td rowspan="2">Kleinste Drehung in $G$</td><td colspan="2">Enthält $G$ eine Spiegelung?</td></tr>
<tr><td>ja</td><td>nein</td></tr>
<tr><td>$d_{2\pi/6} = d_{\pi/3}$</td><td>$p6m$</td><td>$p6$</td></tr>
<tr><td>$d_{2\pi/4} = d_{\pi/2}$</td><td>Gibt es Spiegelachsen im Winkel $\pi/4$?<br>Ja: $p4m$<br>Nein: $p4g$</td><td>$p4$</td></tr>
<tr><td>$d_{2\pi/3}$</td><td>Gibt es Drehmittelpunkte außerhalb der Spiegelachsen?<br>Ja: $p31m$<br>Nein: $p3m1$</td><td>$p3$</td></tr>
<tr><td>$d_{\pi}$</td><td>Gibt es Spiegelachsen im Winkel $\pi/2$?<br><table><tr><td>Ja</td><td>Nein</td></tr><tr><td>Gibt es Drehmittelpunkte außerhalb der Spiegelachsen?<br>Ja: $cmm$<br>Nein: $pmm$</td><td>$pmg$</td></tr></table></td><td>Enthält $G$ eine Gleitspiegelung?<br>Ja: $pgg$<br>Nein: $p2$</td></tr>
<tr><td>Keine</td><td>Gibt es eine Gleitspiegelachse, die keine Spiegelachse ist?<br>Ja: $cm$<br>Nein: $pm$</td><td>Enthält $G$ eine Gleitspiegelung?<br>Ja: $pg$<br>Nein: $p1$</td></tr>
</table>

Tapetengruppen werden auch **kristallographische Gruppen in Dimension 2** genannt. In höheren Dimensionen sind kristallographische Gruppen definiert als diskrete Untergruppen $G$ der euklidischen Bewegungsgruppe des $\mathbb{R}^n$, deren Translationsuntergrupppe $L_G$ ein Gitter im $\mathbb{R}^n$ ist.

# 3 Gruppen

Wir haben in der linearen Algebra schon die Definition einer Gruppe kennengelernt: Eine **Gruppe** $G$ ist eine Menge mit einer Verknüpfung $G \times G \to G$, die wir oft als $(a, b) \mapsto ab$ schreiben, so dass gilt:

i) Die Verknüpfung ist assoziativ

ii) Es gibt ein neutrales Element 1, d.h. für alle $a \in G$ ist $1a = a = a1$.

iii) Zu jedem $a \in G$ gibt es ein inverses Element $b \in G$, d.h. es gilt $ab = ba = 1$.

Das neutrale Element und das inverse Element zu $a$ sind eindeutig bestimmt. Wir bezeichnen das Inverse zu $a$ auch mit $a^{-1}$. Gilt zusätzlich

iv) $ab = ba$ für alle $a, b \in G$,

so heißt $G$ **kommutativ** oder **abelsch**.
Eine Teilmenge $H \subset G$ heißt **Untergruppe** von $G$, falls i) $1 \in H$, ii) $a, b \in H \Rightarrow ab \in H$ und iii) $a \in H \Rightarrow a^{-1} \in H$ gilt.
Eine Abbildung $\varphi : G \to G'$ zwischen zwei Gruppen heißt Gruppenhomomorphismus oder einfach Homomorphismus, falls für alle $a, b \in G$ gilt

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Dann folgt $\varphi(1) = 1$ und $\varphi(a^{-1}) = \varphi(a)^{-1}$.
Der Gruppenhomomorphismus $\varphi : G \to G'$ heißt **Isomorphismus**, falls $\varphi$ ein Inverses besitzt, d.h. falls es einen Gruppenhomomorphismus $\psi : G' \to G$ gibt mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_{G'}$.
Ein injektiver Gruppenhomomorphismus heißt **Monomorphismus**, ein surjektiver Gruppenhomomorphismus heißt **Epimorphismus**.

**Definition 3.1** Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus.

i) Der **Kern** von $\varphi$ ist definiert als $\mathrm{Kern}\varphi = \{a \in G : \varphi(a) = 1\} \subset G$.

ii) Das **Bild** von $\varphi$ ist definiert als Bild$\varphi = \{b \in G' :$ es gibt ein $a \in G$ mit $\varphi(a) = b\} \subset G'$.

**Lemma 3.2** Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus.

i) Kern$\varphi$ ist eine Untergruppe von $G$, Bild$\varphi$ ist eine Untergruppe von $G'$.

ii) $\varphi$ ist ein Monomorphismus $\Leftrightarrow$ Kern$\varphi = \{1\}$.

iii) $\varphi$ ist ein Epiomorphismus $\Leftrightarrow$ Bild$\varphi = G'$.

iv) $\varphi$ ist ein Isomorphismus $\Leftrightarrow$.

$\varphi$ ist ein Monomorphismus und ein Epimorphismus (d.h. injektiv und surjektiv).

**Beweis :**

i) Das haben wir in Übungsaufgabe 1, Blatt 3 gezeigt.

ii) Sei $\varphi$ ein Monomorphismus (d.h. injektiv). Ist $a \in$ Kern$\varphi$, so gilt $\varphi(a) = 1 = \varphi(1)$, also $a = 1$. Daher ist Kern$\varphi = 1$. Ist umgekehrt Kern$\varphi = 1$, so sei $\varphi(a) = \varphi(b)$. Dann folgt

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1,$$

also wegen Kern $\varphi = 1$ schon $ab^{-1} = 1$, d.h. $a = b$. Daher ist $\varphi$ injektiv.

iii) ist klar.

iv) „$\Rightarrow$“: klar

„$\Leftarrow$“: Ist $\varphi : G \to G'$ injektiv und surjektiv, so definieren wir

$$\begin{aligned} \psi \quad : \quad & G' \to G \\ & b \mapsto \text{ das eindeutig bestimmte } a \in G \text{ mit } \varphi(a) = b. \end{aligned}$$

Man rechnet leicht nach, dass $\psi$ ein Gruppenhomomorphismus mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_{G'}$ ist.

□

**Definition 3.3** Sei $G$ eine Gruppe. Eine Untergruppe $H \subset G$ heißt **Normalteiler** (Notation $H \lhd G$), falls für alle $h \in H$ und alle $g \in G$ gilt

$$ghg^{-1} \in H.$$

Mit der Bezeichnung $gHg^{-1} = \{ghg^{-1} : h \in H\}$ können wir das auch so ausdrücken: $H$ ist Normalteiler in $G$ genau dann, wenn für alle $g \in G$ die Gleichung $gHg^{-1} = H$ gilt.
**Beispiel:**

i) Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus, so ist Kern$\varphi$ ein Normalteiler in $G$.

ii) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

**Definition 3.4** Ist $G$ eine Gruppe, so heißt die Teilmenge

$$Z(G) = \{z \in G : gz = zg \text{ für alle } g \in G\}$$

das **Zentrum** von $G$.

$Z(G)$ ist eine Untergruppe von $G$, da aus $gz_1 = z_1g$ und $gz_2 = z_2g$ für alle $g \in G$ bereits

$$\begin{aligned} g(z_1z_2) &= (gz_1)z_2 = (z_1g)z_2 = z_1(gz_2) \\ &= z_1(z_2g) = (z_1z_2)g \end{aligned}$$

und somit $z_1z_2 \in Z(G)$ folgt.
Das Zentrum von $G$ ist sogar ein Normalteiler von $G$. Ist nämlich $g \in G$ und $z \in Z(G)$, so ist $gzg^{-1} = zgg^{-1} = z$, also insbesondere $gZ(G)g^{-1} = Z(G)$.
**Beispiel:**

i) Ist $G$ eine abelsche Gruppe, so gilt $Z(G) = G$.

ii) $Z(GL(n, K)) = K^\times$ für jeden Körper $K$ (Aufbaukurs LAAG II).

**Definition 3.5** Es sei $G$ eine Gruppe und $H \subset G$ eine Untergruppe. Eine Linksnebenklasse von $H$ in $G$ ist eine Teilmenge von $G$ der Gestalt

$$aH = \{ab : b \in H\}.$$

**Beispiel:** Es sei

$$V = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

mit der Matrixmultiplikation die sogenannte **Kleinsche Vierergruppe** und $H$ die Untergruppe

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Dann ist

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} H = H, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} H = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} H = H, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

**Lemma 3.6** Sei $G$ eine Gruppe und $H \subset G$ eine Untergruppe. Für zwei Linksnebenklassen $aH$ und $bH$ in $G$ sind äquivalent:

i) $aH = bH$

ii) $aH \cap bH \neq \emptyset$

iii) $a \in bH$

iv) $b^{-1}a \in H$.

**Beweis :** i) $\Rightarrow$ ii) Es sei $aH = bH$. Dann ist $a = a1 \in aH$, also $aH \neq \emptyset$, daher ist $aH \cap bH = aH \neq \emptyset$.
ii) $\Rightarrow$ iii) Ist $c \in aH \cap bH$, so gilt $c = ah_1 = bh_2$ für $h_1, h_2 \in H$. Daraus folgt $a = bh_2h_1^{-1} \in bH$.
iii) $\Rightarrow$ iv) Ist $a \in bH$, so ist $b^{-1}a \in b^{-1}bH = H$.
iv) $\Rightarrow$ i) Ist $b^{-1}a \in H$, so folgt $a \in bH$, also auch $aH \subset bH$. Da $H$ eine Untergruppe von $G$ ist, ist mit $b^{-1}a$ auch $(b^{-1}a)^{-1} = a^{-1}b$ in $H$. Also ist $b \in aH$ und daher $bH \subset aH$. Insgesamt folgt $aH = bH$. □

**Satz 3.7** Zwischen je zwei Linksnebenklassen von $H$ in $G$ gibt es eine bijektive Abbildung. (Man sagt auch, sie sind gleichmächtig).
Zwei Linksnebenklassen sind entweder disjunkt oder gleich. $G$ ist disjunkte Vereinigung von Linksnebenklassen.

**Beweis :** Für $a, b \in G$ betrachten wir die Abbildung

$$\begin{aligned} f \quad : \quad & G \to G \\ & g \mapsto ba^{-1}g. \end{aligned}$$

Die Einschränkung von $f$ auf $aH$ vermittelt eine Abbildung

$$f_{|_{aH}} : aH \to bH.$$

Diese ist bijektiv mit Umkehrabbildung

$$bH \to aH, g \mapsto ab^{-1}g.$$

Die zweite Behauptung folgt aus Lemma 3.6. Da jedes $a \in G$ in der Linksnebenklasse $aH$ liegt, ist $G$ die Vereinigung aller Linksnebenklassen, mit Lemma 3.6 also disjunkte Vereinigung gewisser Linksnebenklassen. □

Die Elemente einer Linksnebenklasse $aH$ werden auch Vertreter (oder Repräsentanten) dieser Linksnebenklasse genannt. Für jeden Vertreter $b$ von $aH$, also jedes Element $b \in aH$ gilt $bH = aH$ nach Lemma 3.6.

**Definition 3.8** Mit $G/H$ bezeichnen wir die Menge der Linksnebenklassen von $H$ in $G$.

Ganz analog kann man auch Rechtsnebenklassen $Ha$ definieren, nämlich als Teilmengen von $G$ der Form

$$Ha = \{ha : h \in H\}.$$

Die bijektive Abbildung

$$\begin{aligned} G &\to G \\ g &\mapsto g^{-1} \end{aligned}$$

induziert eine Bijektion zwischen der Menge der Linksnebenklassen $G/H$ und der Menge der Rechtsnebenklassen, die wir mit $H/G$ bezeichnen.

**Definition 3.9**

i) Die Anzahl der Elemente in $G/H$ bezeichnen wir als $(G : H)$, wir nennen $(G : H)$ den **Index** von $H$ in $G$.

ii) Ist $G$ endlich, so bezeichnen wir mit $\mathrm{ord}(G)$ (**Ordnung** von $G$) die Anzahl der Elemente in $G$.

**Satz 3.10 (Satz von Lagrange)** Ist $G$ eine endliche Gruppe und $H$ eine Untergruppe, so gilt

$$\mathrm{ord}(G) = \mathrm{ord}(H)(G : H).$$

**Beweis :** Nach Satz 3.7 ist $G$ die disjunkte Vereinigung von $(G : H)$-vielen Linksnebenklassen. Jede Linksnebenklasse hat genauso viele Elemente wie $1H = H$, also folgt die Behauptung. □

Aus Satz 3.10 folgt, dass für eine endliche Gruppe $G$ die Ordnung jeder Untergruppe ein Teiler von ord$(G)$ ist.

**Lemma 3.11** Die Untergruppe $H \subset G$ ist genau dann ein Normalteiler von $G$, wenn für alle $g \in G$

$$gH = Hg$$

gilt, d.h. wenn für jedes $g \in G$ die zugehörige Linksnebenklasse mit der Rechtsnebenklasse übereinstimmt.
In diesem Fall nennen wir die Nebenklasse $gH = Hg$ auch Restklasse von $g$ modulo $H$.

**Beweis :** Das folgt sofort aus Definition 3.3 □

Nun wollen wir zeigen, dass man für einen Normalteiler $H$ in $G$ eine Quotientengruppe $G/H$ definieren kann. Das funktioniert ähnlich wie für Quotientenvektorräume.
Wir definieren ganz allgemein für Teilmengen $X$ und $Y$ von $G$ das Produkt

$$XY = \{xy : x \in X, y \in Y\}$$

**Lemma 3.12** Ist $H \subset G$ ein Normalteiler, so gilt für alle $a, b \in G$ die Gleichung $(aH)(bH) = abH$. In diesem Fall definiert

$$\begin{aligned} G/H \times G/H &\to G/H \\ (aH, bH) &\mapsto (aH)(bH) = abH \end{aligned}$$

eine Verknüpfung, die $G/H$ zu einer Gruppe macht. Das neutrale Element ist $1H$, das Inverse zu $aH$ ist $a^{-1}H$.
Ist $H$ ein Normalteiler, so heißt $G/H$ Faktor- oder Restklassengruppe von $G$ modulo $H$.

**Beweis :** Es gilt $(aH)(bH) = a(Hb)H = abHH = abH$. Die Gruppenaxiome lassen sich leicht nachrechnen. □

**Beispiel:** $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ aus LAAG I (Aufbaukurs).
Ist $H$ kein Normalteiler in $G$, so funktioniert diese Argumentation nicht. Dann muss nämlich das Produkt von zwei Linksnebenklassen keine Linksnebenklasse sein.

**Korollar 3.13** Ist H$\subset G$ ein Normalteiler, so ist die Abbildung

$$\begin{aligned} \pi \quad : \quad & G \to G/H \\ & a \mapsto aH \end{aligned}$$

ein Epimorphismus mit Kern$\pi = H$.

**Beweis :** Da

$$\pi(a)\pi(b) = (aH)(bH) = abH = \pi(ab)$$

gilt, ist $\pi$ ein Homomorphismus. Offensichtlich ist $\pi$ surjektiv. Ferner gilt

$$a \in \text{Kern}\pi \Leftrightarrow aH = 1H = H \overset{3.6}{\Leftrightarrow} a \in H.$$

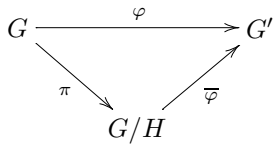
□

Wie viele algebraische Konstruktionen hat auch die Quotientenabbildung $\pi : G \to G/H$ eine universelle Eigenschaft.

**Satz 3.14 (Homomorphiesatz)** Es sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und $H \subset G$ ein Normalteiler mit $H \subset$ Kern$\varphi$.
Dann existiert genau ein Gruppenhomomorphismus

$$\overline{\varphi} : G/H \to G',$$

so dass das Diagramm




kommutiert. (Mit anderen Worten, es gilt $\varphi = \overline{\varphi} \circ \pi$).
Es gilt Bild $\overline{\varphi}$ = Bild$\varphi$, Kern$\overline{\varphi} = \pi$(Kern$\varphi$) und Kern$\varphi = \pi^{-1}$(Kern$\overline{\varphi}$). Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $H =$ Kern$\varphi$ gilt.

**Beweis :** Wir suchen einen Homomorphismus $\overline{\varphi} : G/H \to G'$ mit $\varphi(a) = \overline{\varphi}(\pi a) = \overline{\varphi}(aH)$. Da $\pi : G \to G/H$ surjektiv ist, ist $\overline{\varphi}$ durch diese Gleichung schon eindeutig bestimmt. Wir müssen also nur prüfen, dass die Abbildung

$$\begin{aligned} \overline{\varphi} \quad : \quad & G/H \to G' \\ & aH \mapsto \varphi(a) \end{aligned}$$

wohldefiniert und ein Homomorphismus ist. Gilt $aH = bH$, so ist nach Lemma 3.6 $b^{-1}a \in H$. Wegen $H \subset$ Kern$\varphi$ folgt $\varphi(b^{-1}a) = 1$, also $\varphi(a) = \varphi(b)$. Daher ist $\overline{\varphi}$ in

der Tat wohldefiniert. Es gilt $\overline{\varphi}(ab) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a)\overline{\varphi}(b)$, somit ist $\overline{\varphi}$ ein Gruppenhomomorphismus. Offenbar ist Bild$\overline{\varphi}$ = Bild$\varphi$ und Kern$\overline{\varphi} = \pi$(Kern$\varphi$).
Es bleibt noch Kern$\varphi = \pi^{-1}$(Kern$\overline{\varphi}$) zu zeigen. Ist $a \in$ Kern$\varphi$, d.h. $\varphi(a) = 1$, so folgt $\overline{\varphi}(\pi(a)) = \varphi(a) = 1$, also $a \in \pi^{-1}$(Kern$\overline{\varphi}$). Ist umgekehrt $a \in \pi^{-1}$(Kern$\overline{\varphi}$), also $\overline{\varphi}(\pi(a)) = 1$, so ist $\varphi(a) = 1$, also $a \in$ Kern$\varphi$. □

**Korollar 3.15** Ist $\varphi : G \to G'$ ein Epimorphismus, so ist $G' \simeq G/$Kern$\varphi$ mit einem kanonischen („ausgezeichneten") Isomorphismus.

**Beweis :** Nach Satz 3.14 existiert ein eindeutig bestimmter Homomorphismus

$$\overline{\varphi} : G/\text{Kern}\varphi \to G' \text{ mit } \varphi = \overline{\varphi} \circ \pi.$$

Da Kern$\overline{\varphi} = \pi$(Kern$\varphi$) $= 1$ und Bild$\overline{\varphi}$ = Bild$\varphi = G'$ ist, ist $\overline{\varphi}$ bijektiv und somit ein Isomorphismus. □

**Korollar 3.16** Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus und $G$ endlich, so gilt ord$(G) =$ ord(Kern$\varphi$)ord(Bild$\varphi$).

**Beweis :** Ist $G$ endlich, so sind auch die Gruppen Kern$\varphi$ und Bild$\varphi$ endlich. Nach Korollar 3.15 gilt $G/$Kern$\varphi \simeq$ Bild$\varphi$, mit Satz 3.10 folgt

$$\begin{aligned} \text{ord}(G) &= \text{ord}(\text{Kern}\varphi)(G : \text{Kern}\varphi) \\ &= \text{ord}(\text{Kern}\varphi)\text{ord}(\text{Bild}\varphi). \end{aligned}$$

□

**Definition 3.17** Ist $M$ eine beliebige Teilmenge einer Gruppe $G$, so ist die Menge

$$\langle M \rangle = \{x_1^{\sigma_1} : \cdots : x_n^{\sigma_1} : n \in \mathbb{N}, x_1, \ldots, x_n \in M, \sigma_1, \ldots, \sigma_n \in \{\pm\}\}$$

eine Gruppe (ÜA). Sie heißt die von $H$ erzeugte Untergruppe von $G$.

Diese Definition verallgemeinert Satz 2.5, in dem wir nur endliche Teilmengen $M$ betrachtet haben.
Wir nennen eine Gruppe **endlich erzeugt**, falls es eine endliche Teilmenge $M \subset G$ mit $\langle M \rangle = G$ gibt. Die Elemente aus $M$ heißen auch die Erzeuger von $G$.

**Definition 3.18** Eine Gruppe $G$ heißt zyklisch, falls es ein $g \in G$ mit

$$G = \langle \{g\} \rangle$$

gibt. Dafür schreiben wir auch $G = \langle g \rangle$. Also gilt $G = \{g^n : n \in \mathbb{Z}\}$. Offenbar ist jede zyklische Gruppe abelsch.

**Satz 3.19**

i) Eine Gruppe $G$ ist genau dann zyklisch, wenn es einen surjektiven Gruppenhomomorphismus $\mathbb{Z} \to G$ gibt.

ii) Für eine zyklische Gruppe gilt:

$$\begin{array}{lcll} G & \simeq & \mathbb{Z}, & \text{falls ord}(G) = \infty \\ G & \simeq & \mathbb{Z}/m\mathbb{Z}, & \text{falls ord}(G) = m < \infty. \end{array}$$

Hier ist $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ die von $m$ erzeugte zyklische Untergruppe von $\mathbb{Z}$. Diese ist ein Normalteiler in $\mathbb{Z}$, da $\mathbb{Z}$ abelsch ist. Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ können wir identifizieren mit der Menge $\{0, 1, \ldots, m-1\}$, auf der die Addition als Rest modulo $m$ der gewöhnlichen Addition in $\mathbb{Z}$ definiert ist.

**Beweis :**

i) Ist $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$, so definiert $n \mapsto g^n$ einen Epimorphismus $\mathbb{Z} \to G$. Ist umgekehrt $\psi : \mathbb{Z} \to G$ ein Epimorphismus, so sei $g = \psi(1)$. Da $\psi$ surjektiv ist, ist jedes $h \in G$ von der Form $\psi(n) = \psi(n \cdot 1) = \psi(1)^n = g^n$. Also ist $G = \langle g \rangle$.

ii) Ist $G = \langle g \rangle$, so betrachten wir wieder

$$\begin{array}{rcl} \psi & : & \mathbb{Z} \to G \\ & & n \mapsto g^n. \end{array}$$

Dann gilt nach Korollar 3.15 $\mathbb{Z}/\text{Kern}\psi \simeq G$. Kern$\psi$ ist als Untergruppe von $\mathbb{Z}$ der Form $d\mathbb{Z}$ für ein $d \in \mathbb{Z}$ (LAAG I, ). Ist ord$(G) = \infty$, so muss $d\mathbb{Z} = 0$ sein, woraus $\mathbb{Z} \simeq G$ folgt. Ist ord$(G) = m < \infty$, so muss $m = d$, also $\mathbb{Z}/m\mathbb{Z} \simeq G$ sein. □

**Satz 3.20**

i) Ist $G$ eine zyklische Gruppe, so ist auch jede Untergruppe $H \subset G$ zyklisch.

ii) Ist $G$ zyklisch und $\varphi : G \to G'$ ein Gruppenhomomorphismus, so sind auch Kern$\varphi$ und Bild$\varphi$ zyklisch.

**Beweis :**

i) Sei $\psi : \mathbb{Z} \to G$ ein Epimorphismus. Dann ist $\psi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$, also von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Somit ist $\psi^{-1}(H) = \langle m \rangle$ zyklisch. Daher ist $\psi(\psi^{-1}(H)) = \langle \psi(m) \rangle$ eine zyklische Gruppe. Da $\psi$ surjektiv ist, gilt ferner $H = \psi^{-1}(H))$.

ii) Ist $G = \langle g \rangle$, so ist Bild$\varphi = \langle \varphi(g) \rangle$ ebenfalls zyklisch. Kern$\varphi \subset G$ ist als Untergruppe von $G$ nach i) zyklisch.

□

**Definition 3.21** Es sei $G$ eine Gruppe und $a \in G$. Die **Ordnung von** $a$ (Notation ord$(a)$) ist definiert als die Ordnung der Gruppe $\langle a \rangle = \{1, a, a^{-1}, a^2, a^{-2}, \dots\}$.

Da $\langle a \rangle$ zyklisch ist, gilt nach Satz 3.19 $\langle a \rangle \simeq \mathbb{Z}$, falls ord$(a) = \infty$, und $\langle a \rangle \simeq \mathbb{Z}/m\mathbb{Z}$, falls ord$(a) = m < \infty$. Ist ord$(a) = m < \infty$, so folgt aus diesem Isomorphismus

$$a^k = 1 \Leftrightarrow \text{ord}(a) \mid k.$$

Also ist ord$(a)$ die kleinste positive Zahl $k$ mit $a^k = 1$.

**Satz 3.22 (Kleiner Fermat'scher Satz)** Sei $G$ eine endliche Gruppe und $a \in G$. Dann ist ord$(a)$ ein Teiler vor ord$(G)$. Insbesondere gilt $a^{\text{ord}(G)} = 1$.

**Beweis :** Aus dem Satz von Lagrange 3.10 folgt ord$(G) =$ ord$(a)(G : \langle a \rangle)$. Also gilt ord$(a) \mid$ ord$(G)$, woraus $a^{\text{ord}(G)} = 1$ folgt. □

Manchmal wird auch nur die entsprechende Aussage für $G = (\mathbb{Z}n/\mathbb{Z})^\times$ als kleiner Fermat'scher Satz bezeichnet. Hier ist $(\mathbb{Z}/n\mathbb{Z})^\times$ die Gruppe der Einheiten in dem Ring $\mathbb{Z}/n\mathbb{Z}$ (siehe LAAG I). Es gilt $(\mathbb{Z}/n\mathbb{Z})^\times = \{d \in \{0, 1, \dots, n-1\} : \text{ggT}(d, n) = 1\}$. Ist nämlich $d + n\mathbb{Z}$ invertierbar in $\mathbb{Z}/n\mathbb{Z}$, so gibt es ein $e \in \mathbb{Z}$ mit $de \equiv 1 \text{mod} n$, d.h. $n \mid (de - 1)$. Jeder gemeinsame Teiler $k$ von $d$ und $n$ teilt also die Eins. Ist umgekehrt ggT$(d, n) = 1$, so gibt es (nach LAAG I Basiskurs, Proposition 4.9) ganze Zahlen $k, l$ mit $1 = kd + ln$, woraus

$$kd \equiv 1 \text{ mod } n,$$

also $d \in (\mathbb{Z}/n\mathbb{Z})^\times$ folgt.

Mit $\varphi(n)$ bezeichnet man die Ordnung der Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$, also die Anzahl der zu $n$ teilerfremden Zahlen zwischen 0 und $(n-1)$. Die Funktion $n \mapsto \varphi(n)$ heißt **Euler'sche Phifunktion**. Für eine Primzahl $p$ gilt offenbar $\varphi(p) = p - 1$. Der kleine Fermat'sche Satz sagt nun in $(\mathbb{Z}/n\mathbb{Z})^\times$: Ist $a$ teilerfremd zu $n$, so ist $a^{\varphi(n)} \equiv 1 \bmod n$. Ist $n = p$ eine Primzahl, so gilt also für jedes $a \in \mathbb{Z}$ mit $p \nmid a$:

$$a^{p-1} \equiv 1 \bmod p.$$

Diese Tatsache ist Grundlage einfacher Primzahltests.

**Korollar 3.23** Es sei $G$ eine Gruppe, so dass $\mathrm{ord}(G) = p$ eine Primzahl ist. Dann ist $G$ zyklisch, $G \simeq \mathbb{Z}/p\mathbb{Z}$, und für jedes $a \in G$ mit $a \neq 1$ gilt $\mathrm{ord}(a) = p$. Jedes $a \neq 1$ aus $G$ ist ein Erzeuger von $G$.

**Beweis :** Sei $a \neq 1$ in $G$. Dann ist $\mathrm{ord}(a) > 1$ und nach Definition 3.21 ein Teiler von $\mathrm{ord}(G) = p$, woraus $\mathrm{ord}(a) = p = \mathrm{ord}(G)$ folgt. Also ist $\langle a \rangle \subset G$ eine Untergruppe mit voller Elementezahl, woraus $\langle a \rangle = G$ folgt. □

Sind $G$ und $G'$ Gruppen, so kann man auf der Produktmenge $G \times G'$ durch $(g_1, g_1') \cdot (g_2, g_2') = (g_1 g_2, g_1' g_2')$ eine Verknüpfung definieren, die $G \times G'$ zu einer Gruppe macht. Dann sind die Projektionen

$$\begin{aligned} p : G' \times G' &\to G \\ (g, g') &\mapsto g \end{aligned}$$

und

$$\begin{aligned} p' : G \times G' &\to G' \\ (g, g') &\mapsto g' \end{aligned}$$

Homomorphismen.
Allgemeiner definiert man für jede Familie $(G_i)_{i \in I}$ von Gruppen, wobei I eine beliebige Indexmenge ist, die Produktgruppe $\prod_{i \in I} G_i$ als die Produktmenge $\prod_{i \in I} G_i = \{(g_i)_{i \in I} : g_i \in G_i\}$ zusammen mit der Verknüpfung

$$(g_i)_{i \in I} (h_i)_{i \in I} = (g_i h_i)_{i \in I}.$$

Das Produkt hat folgende universelle Eigenschaft.

**Satz 3.24** Es sei $H$ eine Gruppe. Die Homomorphismen $\Phi : H \to G \times G'$ entsprechen bijektiv den Paaren $(\varphi, \varphi')$ von Homomorphismen $\varphi : H \to G$ und $\varphi' \to G'$. Bei dieser Zuordnung ist $\mathrm{Kern}\Phi = \mathrm{Kern}\varphi \cap \mathrm{Kern}\varphi'$.

**Beweis :** Ist $\Phi : H \to G \times G'$ ein Homomorphismus, so sind $\varphi := p \circ \Phi : H \to G$ und $\varphi' := p' \circ \Phi : H \to G'$ Homomorphismen, wobei $p : G \times G' \to G$ und $p' : G \times G' \to G'$ die Projektionen sind. Sind umgekehrt $\varphi : H \to G$ und $\varphi' : H \to G'$ Homomorphismen, so ist auch

$$\begin{aligned} \Phi : H &\to G \times G' \\ h &\mapsto (\varphi(g), \varphi(g')) \end{aligned}$$

ein Homomorphismus mit Kern $\Phi = \text{Kern}\varphi \cap \text{Kern}\varphi'$.
Man rechnet leicht nach, dass diese Konstruktionen invers zueinander sind. □

Eine analoge Aussage gilt für ein Produkt der Form $\prod_{i \in I} G_i$.

**Proposition 3.25** Es seien $r, s \in \mathbb{N}$ teilerfremd und $G$ eine zyklische Gruppe der Ordnung $rs$. Dann gibt es eine Untergruppe $H_1$ von $G$ der Ordnung $r$ und eine Untergruppe $H_2$ der Ordnung $s$, so dass gilt

$$G \simeq H_1 \times H_2.$$

**Beweis :** Es sei $g$ ein Erzeuger von $G$, also $G = \langle g \rangle$. Dann ist $\text{ord}(g) = rs$. Wir zeigen nun, dass $\text{ord}(g^r) = s$ gilt. Ist nämlich $(g^r)^k = g^{rk} = 1$ für ein $k \in \mathbb{N}$, so folgt $rs \mid rk$, also $s \mid k$. Daher gilt in der Tat $\text{ord}(g^r) = s$. Genauso zeigt man $\text{ord}(g^s) = r$. Also ist $H_1 = \langle g^s \rangle$ eine Untergruppe der Ordnung $r$ und $H_2 = \langle g^r \rangle$ eine Untergruppe der Ordnung $s$. Wir betrachten den Homomorphismus

$$\begin{aligned} \Phi : G &\to H_1 \times H_2 \\ g^m &\mapsto (g^{sm}, g^{rm}) \end{aligned}$$

Ist $g^m \in \text{Kern}\Phi$, so gilt $g^{sm} = 1$ und $g^{rm} = 1$, also $rs \mid sm$ und $rs| \ rm$, d.h. $r \mid m$ und $s \mid n$. Da $r$ und $s$ teilerfremd sind, folgt $rs \mid m$ und somit $g^m = 1$. Also ist $\Phi$ injektiv. Da $G$ und $H_1 \times H_2$ dieselbe Anzahl $rs$ von Elementen haben, ist $\Phi$ nach dem Schubfachprinzip auch surjektiv, also ein Isomorphismus. □

Jetzt wollen wir noch einen wichtigen Satz über die simultane Erfüllbarkeit von Kongruenzen zeigen:

**Satz 3.26 (Chinesischer Restsatz)** Es seien $n_1, \ldots, n_r$ paarweise teilerfremde natürliche Zahlen und $n = \prod_{i=I}^{r} n_i$. Mit $\beta_i$ bezeichnen wir die natürliche Abbildung

$$\begin{aligned} \beta_i : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n_i\mathbb{Z} \\ a + n\mathbb{Z} &\mapsto a + n_i\mathbb{Z}. \end{aligned}$$

Dann ist

$$\begin{aligned} \beta = (\beta_1, \ldots, \beta_r) : \mathbb{Z}/n\mathbb{Z} &\rightarrow \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \\ a + n\mathbb{Z} &\mapsto (a + n_1\mathbb{Z}, \ldots, a + n_r\mathbb{Z}) \end{aligned}$$

ein Isomorphismus von Gruppen. Für beliebig vorgegebene Restklassen $(a_1 + n_1\mathbb{Z}, \ldots, a_r + n_r\mathbb{Z})$ gibt es also genau eine Restklasse $a + n\mathbb{Z}$ mit $a \equiv a_i \mod n_i$ für alle $i = 1, \ldots, r$.

**Beweis :** Da $n\mathbb{Z} \subset n_i\mathbb{Z}$ ist, ist $\beta_i$ wohldefiniert. Offenbar ist $\beta_i$ ein Gruppenhomomorphismus. Also ist auch die Produktabbildung $\beta$ ein Homomorphismus.
Ist $a + n\mathbb{Z} \in$ Kern$\beta$, so ist $a \in n_1\mathbb{Z} \cap \cdots \cap n_r\mathbb{Z}$, d.h. $n_i \mid a$ für alle $i = 1, \ldots, r$. Da $n_1, \ldots, n_r$ paarweise teilerfremd sind, folgt $n \mid a$, also $a + n\mathbb{Z} = 0$ in $\mathbb{Z}/n\mathbb{Z}$. Daher ist $\beta$ injektiv.
Nun setzen wir $\mathcal{N}_i = \prod_{k \neq i} n_k$. Da $n_1, \ldots, n_r$ paarweise teilerfremd sind, haben $\mathcal{N}, \ldots, \mathcal{N}_r$ keinen gemeinsamen Teiler $\neq 1$. Wir betrachten die Untergruppe $\mathcal{N}_1\mathbb{Z} + \cdots + \mathcal{N}_r\mathbb{Z}$ von $\mathbb{Z}$. Diese ist von der Form $d\mathbb{Z}$ für ein $d \in \mathbb{Z}$, also folgt $\mathcal{N}_i\mathbb{Z} \subset d\mathbb{Z}$, und daher $d \mid \mathcal{N}_i$ für alle $i = 1, \ldots, r$. Da $\mathcal{N}_1 \ldots, \mathcal{N}_r$ keinen gemeinsamen Teiler $\neq 1$ haben, folgt $d = 1$, d.h.

$$N_1\mathbb{Z} + \cdots + \mathcal{N}_r\mathbb{Z} = \mathbb{Z}.$$

Somit gibt es ganze Zahlen $q_1, \ldots, q_r$ mit $\mathcal{N}_1 q_1 + \cdots + \mathcal{N}_r q_r = 1$. Für $i \neq k$ ist $n_k$ ein Teiler von $\mathcal{N}_i$, woraus

$$1 + n_k\mathbb{Z} = \sum_{i=I}^{r} \mathcal{N}_i q_i + n_k\mathbb{Z} = \mathcal{N}_k q_k + n_k\mathbb{Z}$$

folgt. Nun können wir zeigen, dass $\beta$ surjektiv ist. Es sei $(a_1 + n_1\mathbb{Z}, \ldots, a_r + n_r\mathbb{Z}) \in \prod_{i=I}^{r} \mathbb{Z}/n_i\mathbb{Z}$. Wir setzen

$$a = \prod_{i=I}^{r} a_i \mathcal{N}_i q_i.$$

Dann ist $a + n_k\mathbb{Z} = a_k\mathcal{N}_k q_k + n_k\mathbb{Z}$, denn $n_k \mid \mathcal{N}_i$ für $i \neq k$. Da $\mathcal{N}_k q_k \equiv 1 \mod n_k$ ist, folgt $a + n_k\mathbb{Z} = a_k + n_k\mathbb{Z}$ für alle $k = 1, \ldots, r$. Somit ist $\beta(a + n\mathbb{Z}) = (a + n_1\mathbb{Z}, \ldots, a + n_r\mathbb{Z}) = (a_1 + n\mathbb{Z}, \ldots, a_r + n_r\mathbb{Z})$. Daher ist $\beta$ ein Isomorphismus. □

Wir wollen jetzt noch zwei Isomorphiesätze für Gruppen beweisen.

**Satz 3.27 (1. Isomorphiesatz)** Es sei $G$ eine Gruppe, $H \subset G$ eine Untergruppe und $N \subset G$ ein Normalteiler. Dann ist $HN$ eine Untergruppe von $G$, $N$ ist ein Normalteiler von $HN$ und $H \cap N$ ist ein Normalteiler von $H$. Die Inklusion $H \subset HN$ induziert einen Isomorphismus

$$H/H \cap N \xrightarrow{\sim} HN/N.$$

**Beweis :** Da $N$ ein Normalteiler in $G$ ist, gilt $HN = NH$. Nach Übungsaufgabe 3 (Blatt 6) ist $HN$ daher eine Untergruppe von $G$. Da $N$ normal in $G$ ist, ist $N$ erst recht normal in $HN$. Der Homomorphismus

$$\begin{array}{ccccc} \alpha : H & \hookrightarrow & HN & \to & HN/N \\ h & \mapsto & h & \mapsto & hN \end{array}$$

ist surjektiv, denn es gilt für $h \in H$ und $n \in N$ die Gleichung $hnN = hN$, also ist $\alpha(h) = hnN \in HN/N$. Es gilt

$$\begin{aligned} \text{Kern}\alpha &= \{h \in H : hN = 1\} \\ &= \{h \in H : h \in N\} \\ &= H \cap N. \end{aligned}$$

Somit ist $H \cap N$ ein Normalteiler in $H$. Mit Korollar 3.15 folgt

$$H/H \cap N \xrightarrow{\sim} HN/N.$$

□

**Satz 3.28 (2. Isomorphiesatz)** Es sei $G$ eine Gruppe und $H$ und $N$ seien zwei Normalteiler in $G$ mit $N \subset H$. Dann ist $N$ auch ein Normalteiler in $H$, und man kann $H/N$ als Normalteiler von $G/N$ auffassen. Der kanonische Gruppenhomomorphismus

$$(G/N)/(H/N) \simeq G/H$$

ist ein Isomorphismus.

**Beweis :** $N$ ist normal in $G$, also erst recht in $H$. Die Inklusion $H \subset G$ vermittelt einen Homomorphismus

$$\alpha : H \hookrightarrow G \xrightarrow{\pi} G/N.$$

Es ist Kern$\alpha = \{h \in H : h \in N\} = H \cap N = N$. Nach Satz 3.14 gibt es einen Gruppenhomomorphismus

$$\overline{\alpha} : H/N \to G/N$$

mit Kern$\overline{\alpha} = \pi_H(\text{Kern}\alpha) = \pi_H(N) = 1$, wobei $\pi_H : H \to H/N$ die Quotientenabbildung ist. Also ist $\overline{\alpha}$ injektiv und erlaubt uns, $H/N$ als Untergruppe von $G/N$ aufzufassen. Wir identifizieren also $H/N$ mit $\overline{\alpha}(H/N) \subset (G/N)$.
Ferner induziert der Epimorphismus

$$G \to G/H$$

wegen $N \subset H$ nach Satz 3.14 einen Epimorphismus

$$\beta : G/N \to G/H,$$

dessen Kern mit dem Bild von $H$ unter der Quotientenabbildung $G \to G/N$ übereinstimmt. Also ist Kern$\beta$ = Bild$(\alpha)$ = Bild$(\overline{\alpha})$, d.h. wir können Kern$\beta$ mit $H/N$ identifizieren. Aus Korollar 3.15 folgt daher

$$(G/N)/(H/N) \simeq G/H.$$

□

Zum Abschluss unserer Betrachtungen über Gruppen wollen wir noch die Struktur der endlich erzeugten abelschen Gruppen bestimmen. Dazu definieren wir zunächst die direkte Summe von Gruppen. **Ab sofort schreiben wir die Verknüpfung in den betrachteten Gruppen additiv**.

**Definition 3.29** Es sei $I$ eine Indexmenge und für alle $i \in I$ sei eine Gruppe $G_i$ gegeben. Dann heißt die Menge

$$\bigoplus_{i\in I} G_i = \{(g_i)_{i\in I} : \text{ alle bis auf endlich viele } g_i \text{ sind gleich } 0\},$$

zusammen mit der komponentenweisen Verknüpfung $(g_i)_{i\in I} + (g_i')_{i\in I} = (g_i + g_i')_{i\in I}$ die direkte Summe der Gruppen $G_i, i \in I$.

Ist $I$ eine endliche Menge, so stimmt die direkte Summe $\bigoplus_{i\in I} G_i$ mit dem direkten Produkt $\prod G_i$ überein.

**Definition 3.30** Eine Gruppe $G$, die isomorph ist zu $\bigoplus_{i\in I} \mathbb{Z}$ für eine Indexmenge $I$ heißt **freie abelsche Gruppe**.

Ist $\varphi : \bigoplus_{i\in I} \mathbb{Z} \xrightarrow{\sim} G$, so sei $e_i$ der $i$-te Einheitsvektor in $\bigoplus_{i\in I} \mathbb{Z}$ und $g_i = \varphi(e_i) \in G$. Dann hat jedes $g \in G$ eine eindeutige Darstellung der Form $g = \sum_{i\in I} m_i g_i$, wobei fast alle

ganzen Zahlen $m_i$ Null sind. Das System der Vektoren $(g_i)_{i\in I}$ heißt dann auch **Basis** der Gruppe $G$. Ist $\bigoplus_{i=1}^{n} \mathbb{Z} \simeq G$ für ein $n \in \mathbb{N}$, so heißt $G$ **endlich erzeugte freie abelsche Gruppe**. In diesem Fall hat jedes $g \in G$ eine eindeutige Darstellung der Form

$$g = \sum_{i=1}^{n} m_i g_i$$

mit $m_1, \ldots, m_n \in \mathbb{Z}$ für die Basis $(g_1, \ldots, g_n)$, wobei $g_i$ das Bild des $i$-ten Einheitsvektors in $\bigoplus_{i=1}^{n} \mathbb{Z}$ ist.

**Lemma 3.31** Ist $G \simeq \bigoplus_{i=1}^{n} \mathbb{Z}$ eine endlich erzeugte freie abelsche Gruppe und $\psi : \bigoplus_{i\in I} \mathbb{Z} \to G$ ein weiterer Isomorphismus, so ist $I$ endlich mit $\#I = n$. Jede Basis von $G$ hat also $n$ Elemente. Wir nennen $n = \text{rang}(G)$ den Rang von $G$.

**Beweis :** Es sei $p$ eine Primzahl. Dann ist $pG = \{pg : g \in G\}$ eine Untergruppe von $G$, also auch ein Normalteiler. Es gilt $G/pG \simeq \bigoplus_{i=I}^{n} \mathbb{Z}/p\mathbb{Z}$. Diese Gruppe hat $p^n$ Elemente. Es sei $\psi : \bigoplus_{i\in I} \mathbb{Z} \to G$ ein beliebiger Isomorphismus, und $r$ eine beliebige natürliche Zahl kleiner oder gleich der Ordnung von $I$. (Falls $I$ unendlich ist, ist $r$ also eine beliebige natürliche Zahl). Dann ist $\bigoplus_{i=1}^{r} \mathbb{Z}$ eine Untergruppe von $\bigoplus_{i\in 1} \mathbb{Z}$, also ist $\bigoplus_{i=1}^{r} \mathbb{Z}/p\mathbb{Z}$ isomorph zu einer Untergruppe von $G/pG$, woraus $p^r = \#(\bigoplus_{i=1}^{r} \mathbb{Z}/p\mathbb{Z}) \leq p^n$, also $r \leq n$ folgt. Daher gilt $\#I \leq n$. Dasselbe Argument mit vertauschten Rollen zeigt $n \leq \#I$, also $n = \#I$. □

**Proposition 3.32** Es sei $G'$ eine endlich erzeugte freie abelsche Gruppe und $f : G \to G'$ ein Epimorphismus abelscher Gruppen. Dann gibt es eine Untergruppe $H$ von $G$, so dass $f_{|_H} : H \to G'$ ein Isomorphismus ist und so dass die natürliche Abbildung

$$\begin{aligned} \Phi : H \oplus \text{Kern} f &\to G \\ (h, l) &\mapsto h + l \end{aligned}$$

ein Isomorphismus ist.

**Beweis :** Es sei $(g'_1, \ldots, g'_n)$ eine Basis der endlich erzeugten freien abelschen Gruppe $G'$. Wir wählen für jedes $g'_i$ ein $g_i \in G$ mit $f(g_i) = g'_i$ und setzen $H = \langle g_1, \ldots, g_n \rangle \subset G$. Dann ist die Einschränkung

$$f_{|_H} : H \to G'$$

ein surjektiver Gruppenhomomorphismus. Ist $h \in H$ in Kern$(f_{|_H})$, so können wir $h$ schreiben als $h = \sum_{i=1}^{n} k_i g_i$ mit $k_1, \ldots, k_n \in \mathbb{Z}$, da $G$ abelsch ist. Also gilt

$$0 = f(h) = \sum_{i=1}^{n} k_i f(g_i) = \sum_{i=1}^{n} k_i g_i'.$$

Da $(g_i', \ldots, g_n')$ eine Basis von $G'$ ist, folgt $k_1 = \cdots = k_n = 0$. Daher ist Kern$(f_{|_H}) = 0$, und $f_{|_H}$ ein Isomorphismus $H \to G$. Nun betrachten wir die Abbildung

$$\begin{aligned} \Phi : H \oplus \text{Kern} f &\to G \\ (h, l) &\mapsto h + l. \end{aligned}$$

Da $G$ abelsch ist, ist diese Abbildung ein Homomorphismus. Da Kern$(f_{|_H}) = 0$ ist, ist $\Phi$ injektiv. Sei $g \in G$. Dann ist $f(g) = \sum_{i=1}^{n} k_i g_i'$ für $k_1, \ldots, k_n \in \mathbb{Z}$. Also gilt $f(g) = f(h)$ für das Element $h = \sum_{i=1}^{n} k_i g_i \in H$, woraus $(g - h) \in$ Kern$f$ folgt.
Also ist $g = \Phi(h, g - h)$. Somit ist $\Phi$ surjektiv, also ein Isomorphismus. □

**Korollar 3.33** Ist $G$ eine endlich erzeugte freie abelsche Gruppe und $H \subset G$ eine Untergruppe, so ist auch $H$ eine endlich erzeugte freie abelsche Gruppe, und es gilt

$$\text{rang}(H) \leq \text{ rang}(G).$$

**Beweis :** mit Induktion nach rang$(G)$. Ist rang$(G) = 1$, so ist $G \simeq \mathbb{Z}$. Da jede Untergruppe von $\mathbb{Z}$ von der Form $d\mathbb{Z}$ für ein $d \in \mathbb{Z}$ ist, stimmt die Behauptung
Angenommen, die Behauptung gilt für alle Gruppen vom Rang $<$ rang$(G)$. Dann sei $g_1, \ldots, g_n$ eine Basis von $G$. Wir schränken den Homomorphismus

$$\begin{aligned} f : G &\to \mathbb{Z} \\ \sum_{i=1}^{n} k_i g_i &\mapsto k_1 \end{aligned}$$

auf die Untergruppe $H$ ein. Kern$(f_{|_H})$ ist eine Untergruppe der freien abelschen Gruppe $\langle g_2, \ldots, g_n \rangle$. Nach Induktionsvoraussetzung ist Kern$(f_{|_H})$ also eine freie abelsche Gruppe vom Rang $\leq n - 1$. Bild$(f_{|_H})$ ist eine Untergruppe von $\mathbb{Z}$, also eine freie abelsche Gruppe vom Rang 0 oder 1. Wir wenden Proposition 3.32 auf $f_{|_H} : H \to$ Bild$(f_{|_H})$ an und erhalten $H \simeq$ Kern$(f_{|_H}) \oplus H'$, wobei $H' \subset H$ eine Untergruppe mit $H' \simeq$ Bild$(f_{|_H})$ ist. Also ist $H$ als direkte Summe einer freien abelschen Gruppe vom Rang $\leq n - 1$ und einer freien abelschen Gruppe vom Rang $\leq 1$ eine freie abelsche Gruppe vom Rang $\leq n$. □

**Definition 3.34** Sei $G$ eine abelsche Gruppe

i) Ein $g \in G$ heißt **Torsionselement**, falls $g$ endliche Ordnung hat.

ii) Die Menge $G_{\text{tors}} = \{g \in G : g \text{ Torsionselement}\}$ heißt **Torsionsuntergruppe** von $G$.

iii) $G$ heißt **torsionsfrei**, falls $G_{\text{tors}} = 0$. In einer torsionsfreien abelschen Gruppe hat also jedes Element $\neq 1$ unendliche Ordnung.

Man rechnet leicht nach, dass die Teilmenge $G_{\text{tors}} \subset G$ wirklich eine Untergruppe ist.

**Satz 3.35** Jede endliche erzeugte torsionsfreie abelsche Gruppe ist frei.

**Beweis :** Es sei $G = \langle g_1, \ldots, g_n \rangle \neq 0$. Wir betrachten alle Teilmengen $M \subset \{g_1, \ldots, g_n\}$ für die $\langle M \rangle$ eine freie abelsche Gruppe ist. Da $G$ torsionsfrei ist, ist jede zyklische Untergruppe der Form $\langle g_i \rangle$ nach Satz 3.19 eine freie abelsche Gruppe. Daher gibt es Teilmengen $M \subset \{g_1, \ldots, g_n\}$, für die $\langle M \rangle$ frei ist, und wir können ein maximales $M$ unter ihnen auswählen. Nach Umnummerieren gilt $M = \{g_1, \ldots, g_r\}$ für ein $1 \leq r \leq n$. Ist $r = n$, so ist $G$ frei. Angenommen, $r < n$. Dann ist $\langle g_1, \ldots, g_r, g_{r+1} \rangle$ nicht frei, d.h. es gibt eine Gleichung der Form $k_1 g_1 + \cdots + k_r g_r + k_{r+1} g_{r+1} = 0$ mit $k_1, \ldots, k_{r+1} \in \mathbb{Z}$, nicht alle $k_i = 0$. Da es eine solche Gleichung in der freien Gruppe $\langle g_1, \ldots, g_r \rangle$ nicht gibt, gilt $k_{r+1} \neq 0$. Somit ist $k_{r+1} g_{r+1} \in \langle g_1, \ldots, g_r \rangle$.
Dasselbe Argument zeigt, dass für alle $i \in \{r+1, \ldots, n\}$ geeignete Vielfache von $g_i$ in $\langle g_1, \ldots, g_r \rangle$ liegen. Somit existiert ein $k \in \mathbb{N}$ mit

$$k g_{r+1}, \ldots, k g_n \in \langle g_1, \ldots, g_r \rangle.$$

Wir betrachten die Abbildung

$$\begin{array}{rcl} \varphi : G & \to & \langle g_1, \ldots, g_r \rangle \\ g & \mapsto & kg \end{array}$$

Da $G$ torsionsfrei ist, folgt Kern$\varphi = 0$. Daher ist $G$ isomorph zu einer Untergruppe der freien abelschen Gruppe $\langle g_1, \ldots, g_r \rangle$, nach Lemma 3.31 also ebenfalls frei. □

Ist $G$ eine beliebige endlich erzeugte abelsche Gruppe, so ist die Faktorgruppe $G/G_{\text{tors}}$ torsionsfrei, nach Korollar 3.33 also eine endlich erzeugte freie abelsche Gruppe. $G_{\text{tors}}$ ist als endlich erzeugte abelsche Torsionsgruppe eine endliche abelsche Gruppe. Nach Definition 3.30 gilt sogar

$$G \simeq G_{\text{tors}} \oplus H,$$

wobei $H \subset G$ eine freie abelsche Untergruppe isomorph zu $G/G_{\text{tors}}$ ist.
Um die Struktur einer beliebigen endlich erzeugten abelschen Gruppe zu verstehen, müssen wir also nur noch die endlichen abelschen Gruppen studieren.

**Definition 3.36** Ist $G$ eine endliche abelsche Gruppe, so heißt die kleinste positive Zahl $e$ mit $eg = 0$ für alle $g \in G$ der **Exponent** von $G$. Ist der Exponent von $G$ eine Primzahlpotenz $p^k$, so heißt $G$ $p$-Gruppe. Ist $G$ eine abelsche Gruppe und $p$ eine Primzahl, so definieren wir

$$G(p) = \{g \in G : \text{ord}(g) \text{ ist eine } p\text{-Potenz}\}.$$

Offenbar ist $G(p) \subset G$ eine Untergruppe.

**Satz 3.37** Jede endliche abelsche Gruppe $G$ ist die direkte Summe aller $G(p)$ mit $G(p) \neq \{0\}$.

**Beweis :** Es sei $e$ der Exponent von $G$. Offenbar ist $G(p) \neq 0$ genau dann, wenn $p \mid e$ gilt. Wir zeigen die Behauptung mit Induktion nach der Anzahl der Primteiler von $e$. Ist $e$ eine Primzahlpotenz $p^k$, d.h. $G$ eine $p$-Gruppe, so gilt $G = G(p)$. Für den Induktionsschritt betrachten wir $e = mm'$ mit natürlichen Zahlen $m, m' > 1$ und $\text{ggT}(m, m') = 1$. Also existieren $r, s \in \mathbb{Z}$ mit

$$1 = rm + sm'.$$

Es sei nun $G_m = \{g \in G : mg = 0\}$ und $G_{m'} = \{g \in G : m'g = 0\}$. $G_m$ und $G_{m'}$ sind Untergruppen von $G$. Der Exponent von $G_m$ teilt $m$, der Exponent von $G_{m'}$ teilt $m'$ (Übungsaufgabe 1, Blatt 9), also haben beide weniger Primteiler als $e$. Nach Induktionsvoraussetzung gilt daher

$$G_m = \bigoplus_{p|m} G_m(p) \text{ und } G_{m'} = \bigoplus_{p|m'} G_{m'}(p).$$

Ferner ist $G_m(p) = G(p)$ für alle $p|m$ und $G_{m'}(p) = G(p)$ für alle $p|m'$, da $m$ und $m'$ teilerfremd sind. Unsere Behauptung folgt also, wenn wir zeigen können, dass die Abbildung

$$\begin{aligned} \varphi : G_m \oplus G_{m'} &\to G \\ (h, h') &\mapsto h + h' \end{aligned}$$

ein Isomorphismus ist. Da $G$ abelsch ist, ist $\varphi$ ein Homomorphismus. Ist $h + h' = 0$, so ist $h = -h' \in G_m \cap G_{m'}$. Daher folgt $\text{ord}(h)|m$ und $\text{ord}(h')|m'$, also $\text{ord}(h) = 1$, da $m$ und $m'$ teilerfremd sind. Also gilt $h = 0$ und daher $h' = 0$, d.h. $\varphi$ ist injektiv.

Ist $g \in G$ ein beliebiges Element, so gilt $g = 1g = rmg + sm'g$. Aus $e = mm'$ ergibt sich $0 = e(rg) = mm'rg$, also $rmg \in G_{m'}$. Analog schließt man $sm'g \in G_m$. Somit ist $\varphi$ surjektiv, also ein Isomorphismus. □

Um die Struktur einer endlichen abelschen Gruppe $G$ zu verstehen, müssen wir also nur die Struktur der endlichen abelschen $p$-Gruppen $G(p)$ verstehen. Das leistet der folgende Satz.

**Satz 3.38** Jede endliche abelsche $p$-Gruppe $G \neq 0$ ist isomorph zu einer direkten Summe zyklischer $p$-Gruppen, d.h. es gilt

$$G \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{r_s}\mathbb{Z}$$

mit $r_1 \geq r_2 \geq \ldots \geq r_s \geq 1$.
Die Folge $(r_1 \ldots, r_s)$ ist eindeutig bestimmt.

**Beweis :** Es sei $G \neq 0$ eine endliche abelsche $p$-Gruppe.

i) Zunächst halten wir folgende Beobachtung fest: Ist $0 \neq a \in G$ und $p^k a \neq 0$ ein Element der Ordnung $p^m$, so gilt $\text{ord}(a) = p^{k+m}$. Da $G$ eine $p$-Gruppe ist, ist die Ordnung von $a$ eine $p$-Potenz, d.h. $\text{ord}(a) = p^n$. Aus $p^n a = 0$ folgt $n \geq k$, da $p^k a \neq 0$ ist. Also ist $p^{n-k}p^k a = 0$, woraus $m \leq n-k$, also $m+k \leq n$ folgt. Somit ist $p^{m+k} \leq \text{ord}(a)$. Da $p^{k+m}a = 0$ ist, gilt sogar Gleichheit.

ii) Wir beweisen die Behauptung mit Induktion nach $\text{ord}(G)$. Da $G \neq 0$ ist, gibt es ein Element $a \in G$, dessen Ordnung eine echte Primzahlpotenz ist. Also gilt $p \mid \text{ord}(G)$. Ist $\text{ord}(G) = p$, so ist $G$ nach Korollar 3.23 zyklisch, d.h.$G \simeq \mathbb{Z}/p\mathbb{Z}$.

   Wir können also annehmen, dass jede $p$-Gruppe der Ordnung $< \text{ord}(G)$ direkte Summe zyklischer $p$-Gruppen ist.

   Es sei $a_1 \in G$ ein Element maximaler Ordnung und $G_1 = \langle a_1 \rangle \subset G$ die von $a_1$ erzeugte zyklische Untergruppe von $G$ mit $p^{r_1} = \text{ord}(G_1)$. Ist $G = G_1$, so sind wir fertig. Ansonsten betrachten wir die $p$-Gruppe $G/G_1$. Nach Induktionsvoraussetzung gilt

   $$G/G_1 \simeq \mathbb{Z}/p^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{r_s}\mathbb{Z}$$

   mit $r_2 \geq \cdots \geq r_s \geq 1$.

   Für alle $2 \leq i \leq s$ sei $c_i \in G/G_1$ das Element, das dem $(i-1)$-ten Einheitsvektor auf der rechten Seite entspricht. Dann ist $\text{ord}(c_i) = p^{r_i}$. Wir bezeichnen die Quotientenabbildung $G \to G/G_1$ mit $a \mapsto \overline{a}$ und zeigen zunächst:

iii) Ist $c \in G/G_1$ ein Element der Ordnung $p^r$, so existiert ein $b \in G$ mit ord$(a) = p^r$ und $\overline{b} = c$.

Das zeigen wir folgendermaßen: Es sei $b' \in G$ ein beliebiges Element mit $\overline{b}' = c$. Dann ist $p^r\overline{b}' = 0$, d.h. $p^r b' \in G_1 = \langle a_1 \rangle$, also gilt $p^r b' = na_1$ für ein $n \geq 0$. Wir schreiben $n = p^k m$ mit ggT$(p, m) = 1$. Dann ist auch $ma_1$ ein Erzeuger von $G_1$, d.h. ord$(ma_1) =$ ord$G_1 = p^{r_1}$. Wir können $n$ um Potenzen von $p^{r_1}$ abändern, ohne die Gleichung $p^r b' = na_1 = p^k ma_1$ zu zerstören. Also gilt ohne Einschränkung $k < r_1$.

Aus ord$(ma_1) = p^{r_1}$ folgt ord$(p^r b') =$ ord$(p^k ma_1) = p^{r_1-k}$. Daher hat mit i) das Element $b'$ die Ordnung $p^{r+r_1-k}$. Da $a_1$ so gewählt wurde, dass ord$(a_1)$ maximal ist, folgt $r + r_1 - k \leq r_1$, also $r \leq k$. Daher gilt

$$p^r b' = p^k ma_1 = p^r(p^{k-r}ma_1) = p^r a'$$

für $a' = p^{k-r}ma_1 \in G_1$. Das Element $b = b' - a' \in G$ erfüllt $\overline{b} = \overline{b}' = c$ und ord$(b) \mid p^r$. Da andererseits ord$(b)$ ein Teiler von ord$(\overline{b}) =$ ord$(c)$, also ein Teiler von $p^r$ ist, folgt ord$(b) = p^r$.

iv) Nun fahren wir in der Induktion fort. Wir wählen Urbilder $a_2, \ldots, a_s$ in $G$ von $c_2, \ldots, c_s$ in $G/G_1$ der Ordnungen $p^{r_2}, \ldots, p^{r_s}$ und betrachten den Gruppenhomomorphismus:

$$\begin{aligned} \Phi : \langle a_1 \rangle \oplus \cdots \oplus \langle a_s \rangle &\to G \\ (b_1, \ldots, b_s) &\mapsto b_1 + \cdots + b_s. \end{aligned}$$

Ist $(b_1, \ldots, b_s) \in$ Kern$\Phi$, so gilt

$$b_i = m_i a_i \text{ für } m_1, \ldots, m_s \in \mathbb{Z} \text{ mit } m_i < p^{r_i}$$

und

$$m_1 a_1 + \cdots + m_s a_s = 0 \text{ in } G.$$

Also folgt nach Übergang zu $G/G_1$.

$$m_2\overline{a}_2 + \cdots + m_s\overline{a}_s = 0.$$

Da $G/G_1 \simeq \mathbb{Z}/p^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{r_s}\mathbb{Z}$ ist, folgt $m_2 = \cdots = m_s = 0$. Daher ist $m_1 a_1 = 0$, also auch $m_1 = 0$. Somit ist $\Phi$ injektiv. Ist $b \in G$ ein beliebiges Element, so schreiben wir $\overline{b} \in G/G_1$ als

$$\overline{b} = m_2\overline{a}_2 + \cdots + m_s\overline{a}_s$$

mit $m_2, \ldots, m_n \in \mathbb{Z}$. Daher ist $b - m_2a_2 - \cdots - m_sa_s \in G_1$, d.h. von der Form $m_1a_1$. Somit folgt

$$b = m_1a_1 + \cdots + m_sa_s,$$

d.h. $\Phi$ ist surjektiv, also ein Isomorphismus.

Somit haben wir gezeigt, dass $G$ direkte Summe zyklischer $p$-Gruppen ist.

v) Wir müssen noch die Eindeutigkeit von $(r_1, \ldots, r_s)$ nachweisen.

Angenommen, $G \simeq \mathbb{Z}/p^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{r_s}\mathbb{Z}$ für $r_1 \geq \cdots \geq r_s$ und $G \simeq \mathbb{Z}/p^{k_1}\mathbb{Z} \oplus \cdots \oplus p^{k_t}\mathbb{Z}$ für $k_1 \geq \cdots \geq k_t$.

Wir argumentieren mit Induktion nach $\mathrm{ord}(G)$. Ist $\mathrm{ord}(G) = p$, so ist $G \simeq \mathbb{Z}/p\mathbb{Z}$ die einzig mögliche Zerlegung von $G$ in zyklische Gruppen. Im allgemeinen Fall betrachten wir $pG$. Es gilt $pG \simeq \mathbb{Z}/p^{r_1-1} \oplus \cdots \oplus \mathbb{Z}/p^{r_i-1}\mathbb{Z}$ und $pG \simeq \mathbb{Z}p^{k_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{k_j-1}\mathbb{Z}$, wobei $i \leq r$ und $j \leq s$ so gewählt sind, dass $r_i > 1$ und $r_{i+1} = \cdots = r_s = 1$ bzw. $k_j > 1$ und $k_{j+1} = \cdots = k_t = 1$ gilt, denn die Faktoren der Form $\mathbb{Z}/p\mathbb{Z}$ verschwinden ja in $pG$.

Nach Induktionsvoraussetzung ist

$$(r_1 - 1), \ldots, r_i - 1) = (k_1 - 1, \ldots, k_j - 1),$$

also $i = j$ und $r_1 = k_1, \ldots, r_i = k_i$.

Nun hat $G$ mit Hilfe der ersten Zerlegung $p^{r_1+\cdots+r_s}$, mit Hilfe der zweiten Zerlegung $p^{k_1+\cdots+k_t}$ viele Elemente. Daher ist $p^{s-i} = p^{r_{i+1}+\cdots+r_s} = p^{k_{i+1}+\cdots+k_t} = p^{t-i}$, woraus $s = t$ und somit $r_{i+1} = k_{i+1} = 1, \ldots, r_s = s_s = 1$ folgt.

□

**Korollar 3.39** Jede endlich erzeugte abelsche Gruppe $G$ ist isomorph zu einer direkten Summe der Form $\bigoplus_{p|\,\mathrm{ord}(G)} (\mathbb{Z}/p^{r_1(p)}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{r_{s_p}(p)}\mathbb{Z}) \oplus \bigoplus_{i=1}^{r} \mathbb{Z}$ mit $r_1(p) \geq \cdots \geq r_{s_p}(p) \geq 1$ und $r \geq 0$.

# 4 Exkurs: Anwendungen in der Kryptographie

Wir wollen nun das RSA-Verfahren zum Verschlüsseln von Nachrichten kennen lernen. Klassische (sogenannte symmetrische) Verschlüsselungsverfahren beruhen darauf, dass Sender und Empfänger einen gemeinsamen geheimen Schlüssel besitzen, der zum Ver- und Entschlüsseln dient. Im einfachsten Fall könnte so ein geheimer Schlüssel etwa in einer Vorschrift zum Permutieren des Alphabetes bestehen. Bei solchen symmetrischen Verfahren ist ein großes Problem die Vereinbarung

des geheimen Schlüssels zwischen Sender und Empfänger. Bei diplomatischen Verschlüsselungsproblemen mag dieses Problem noch in den Griff zu bekommen sein. In der heutigen Informationsgesellschaft möchte aber eine Vielzahl von Individuen Online-banking betreiben, über sichere Internetverbindungen einkaufen und vielleicht sogar mit einer digitalen Signatur unterschreiben.
Wie ist es dabei möglich, über einen abhörbaren Kanal verschlüsselte Nachrichten zu senden, ohne vorher über einen sicheren Kanal einen geheimen Schlüssel auszutauschen? Die Antwort darauf geben die sogenannte „Public Key"-Verschlüsselungsverfahren. Hier hat jeder Nutzer zwei Schlüssel, einen geheimen, den er selbst erzeugt und nicht weitergibt, und einen öffentlichen, den er allgemein zugänglich macht. Zum Verschlüsseln benutzt man den öffentlichen Schüssel, zum Entschlüsseln den privaten. Dazu benötigt man ein geeignetes mathematisches Verfahren. Ein Beispiel ist das RSA-Verfahren, das von Rivest, Shamir und Adleman entwickelt wurde.

**RSA-Verfahren:** $A$ (Alice) möchte die geheime Nachricht $m$, auch Klartext genannt, an $B$ (Bob) schicken.

**Vorbereitung:** $B$ wählt zwei (große) Primzahlen $p$ und $q$ und berechnet

$$n = pq \text{ und } \varphi(n) = (p-1)(q-1).$$

Ferner wählt $B$ eine Zahl $e$ mit

$$\text{ggT } (e, \varphi(n)) = 1$$

und berechnet (etwa mit dem euklidischen Algorithmus) ein Inverses von $e$ in $(\mathbb{Z}/\varphi(n)\mathbb{Z})^\times$, d.h eine Zahl $d$ mit $de \equiv 1 \bmod \varphi(n)$.

Es gibt zwei Schlüssel:

1) $B$s privater Schlüssel $d$ (der bleibt geheim)

2) $B$s öffentlicher Schlüssel $(n, e)$ (den soll jeder wissen).

Wir nehmen an, der Klartext $m$ ist eine Zahl zwischen 1 und $n$.

- $A$ schaut $B$s öffentlichen Schlüssel $(n, e)$ nach.
- $A$ berechnet $m^e + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ (den Schlüsseltext) und schickt diese Zahl an $B$.
- $B$ benutzt seinen privaten Schlüssel $d$, um $(m^e)^d + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ zu berechnen.

Wieso funktioniert dieses Verfahren? Um das zu verstehen, brauchen wir folgenden Satz:

**Satz 4.1** Ist $n = pq$ mit verschiedenen Primzahlen $p$ und $q$ und $m \in \mathbb{Z}$, so gilt $m^{\varphi(n)+1} \equiv m \bmod n$.

**Beweis :** Gilt $p \nmid m$, so ist $m + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Nach dem kleinen Satz von Fermat gilt also $m^{p-1} \equiv 1 \bmod p$, also auch $m^{\varphi(n)} = m^{(p-1)(q-1)} \equiv 1 \bmod p$, woraus $m^{\varphi(n)+1} \equiv m \bmod p$ folgt. Gilt $p \mid m$, so ist $m^{\varphi(n)+1} \equiv m \equiv 0 \bmod p$.
Genauso zeigt man $m^{\varphi(n)+1} \equiv m \bmod q$. Da $p$ und $q$ teilerfremd sind mit $n = pq$, folgt aus

$$m^{\varphi(n)+1} \equiv m \bmod p \text{ und } m^{\varphi(n)+1} \equiv m \bmod q$$

die Kongruenz $m^{\varphi(n)+1} \equiv m \bmod n$. □

Aus Satz 4.1 folgt, dass Bob mit $(m^e)^d = m^{ed} \equiv m^{\varphi(n)+1} \equiv m \bmod n$ wirklich die Nachricht $m$ berechnet hat.
Wie sicher ist das RSA-Verfahren? Wir nehmen an, dass $E$ (Eva) den Schlüsseltext $m^e \bmod n$, den Alice an Bob geschickt hat, abgehört hat. Außerdem kennt Eva natürlich Bobs öffentlichen Schlüssel $(n, e)$. Kann Eva aus diesen Daten die Zerlegung $n = pq$ in Primfaktoren berechnen (d.h. das Faktorisierungsproplem für $n$ lösen), so kann sie $\varphi(n)$ berechnen und damit das Inverse $d$ von $e$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Dann erhält $E$ aus $m^e$ den Klartext $m \equiv (m^e)^d \bmod n$ zurück.
Interessanterweise ist es genauso schwierig, $B$s privaten Schlüssel $d$ aus $(n, e)$ zu berechnen wie $n$ in Primfaktoren zu zerlegen. Um das zu zeigen, setzen wir

$$s = \max\{k \in \mathbb{N} : 2^k \mid ed - 1\}.$$

und

$$m = \frac{\text{ed} - 1}{2^s}.$$

Ist dann $a$ eine ganze Zahl mit $\text{ggT}(a, n) = 1$, so gilt $a^{\varphi(n)} = a^{\text{ed}-1} \equiv 1 \bmod n$. Also ist $(a^m)^{2^s} = a^{\text{ed}-1} \equiv 1 \mod n$, d.h. die Ordnung von $a^m + n\mathbb{Z}$ teilt $2^s$.

**Lemma 4.2** Sei $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$. Wenn die Ordnungen von $a^m + p\mathbb{Z}$ und $a^m + q\mathbb{Z}$ verschieden sind, dann ist

$$1 < \text{ggT}(a^{2^t m} - 1, n) < n$$

für ein $t \in \{0, 1, 2, \ldots, s - 1\}$.

**Beweis :** Wir haben oben gesehen, dass ord$(a^m + n\mathbb{Z})$ die Zahl $2^s$ teilt. Also gilt dies auch für ord$(a^m+p\mathbb{Z})$ und ord$(a^m+q\mathbb{Z})$. Angenommen, ord$(a^m+q\mathbb{Z}) >$ ord$(a^m+p\mathbb{Z})$. Es gilt ord$(a^m + p\mathbb{Z}) = 2^t$ für ein $t$ mit $0 \leq t \leq s-1$. Dann gilt $a^{2^t m} \not\equiv 1 \bmod q$, aber $a^{2^t m} \equiv 1 \bmod p$, also ggT$(a^{2^t m} - 1, n) = p$. Den Fall ord$(a^m + p\mathbb{Z}) >$ ord$(a^m + q\mathbb{Z})$ zeigt man analog. □

Um $n$ zu faktorisieren, gehen wir nun folgendermaßen vor:

- Wir wählen ein $a \in \{1, \ldots, n-1\}$ und berechnen $g =$ ggT$(a, n)$. Ist $g > 1$, so haben wir $n$ bereits faktorisiert.
- Ist $g = 1$, so berechnen wir $h =$ ggT$(a^{2^t m} - 1, n)$ für $t = s-1, \ldots, 0$. Ist $h > 1$, so sind wir wieder fertig.
- Ist $h = 1$, so wählen wir ein neues $a \in \{1, \ldots, n-1\}$ und wiederholen das Verfahren.

Dieses Verfahren ist erfolgreich, da das folgende Resultat zeigt, dass die Wahrscheinlichkeit dafür, nach $r$ Iterationen einen Primfaktor zu finden, größer als $1 - \frac{1}{2^r}$ ist:

**Satz 4.3** In der Menge $\{1, \ldots, n-1\}$ gibt es mindestens $\frac{(p-1)(q-1)}{2}$-viele Zahlen $a$ mit ggT$(a, n) = 1$, für die ord$(a^m + p\mathbb{Z}) \neq$ ord$(a^m + q\mathbb{Z})$ ist.
Also ist die Erfolgswahrscheinlichkeit des oben beschriebenen Verfahrens in jeder Iteration mindestens $\frac{1}{2}$.

**Beweis :** Ein Beweis findet sich in J. Buchmann: Einführung in die Kryptographie, § 7.2.4. □

Somit ist die Berechnung des privaten Schlüssels $d$ mathematisch genauso aufwändig wie die Zerlegung von $n$ in seine Primfaktoren. Dieses Faktorisierungsproblem ist ein intensiv studiertes mathematisches Problem.
Es ist allerdings nicht bekannt, ob es nicht eine Möglichkeit gibt, den Klartext $m$ aus dem Chiffretext $m^e + n\mathbb{Z}$ zu berechnen, ohne erst den privaten Schlüssel $d$ zu bestimmen.

# 5 Sylowsätze

Wir wiederholen zunächst einige Begriffe zur Operation von Gruppen auf Mengen. Hier schreiben wir die Gruppen wieder multiplikativ.

**Definition 5.1** Es sei $G$ eine Gruppe und $X$ eine Menge. Eine Abbildung

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

heißt **Operation** von $G$ auf $X$, falls

i) $1x = x$ für alle $x \in X$ und

ii) $(gh)x = g(hx)$ für alle $g, h \in G$ und $x \in X$

gilt.

**Beispiel:**

1) Die Abbildung

$$\begin{aligned} \mathcal{B}_2 \times \mathbb{R}^2 &\to \mathbb{R}^2 \\ (\beta, x) &\mapsto \beta x \end{aligned}$$

ist eine Operation der euklidischen Bewegungsgruppe $\mathcal{B}_2$ auf $\mathbb{R}^2$.

2) $G$ operiert auf sich selbst durch Konjugation:

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto ghg^{-1}. \end{aligned}$$

Ist $G$ abelsch, so ist dies die triviale Operation $(g, h) \mapsto h$.

Operiert $G$ auf der Menge $X$, so definieren wir für jedes $x \in X$ die **Bahn** von $x$ als

$$B_x = \{y \in X : \text{ es gibt ein } g \in G \text{ mit } gx = y\}$$

Manchmal liest man auch die Bezeichnung $Gx$ statt $B_x$, das verwechselt man allerdings leicht mit dem Stabilisator $G_x$ (s.u.). Die Bahn $B_x$ ist gerade die Äquivalenzklasse von $x$ bezüglich der Äquivalenzrelation $y \sim z \Leftrightarrow gy = z$ für ein $g \in G$.

**Lemma 5.2**

i) Zwei Bahnen $B_x$ und $B_y$ sind entweder disjunkt oder gleich.

ii) $X$ ist disjunkte Vereinigung von Bahnen.

**Beweis :** Das folgt aus der Tatsache, dass die Bahnen Äquivalenzklassen sind. Man kann es natürlich auch direkt beweisen:

i) Ist $z \in \mathcal{B}_x \cap \mathcal{B}_y$, so ist $z = gx = hy$ für $g, h \in G$. Also ist $x = g^{-1}hy \in \mathcal{B}y$, woraus $\mathcal{B}_x = \mathcal{B}_y$ folgt.

ii) Jedes Element $x \in X$ ist in der Bahn $B_x$, also folgt die Behauptung mit i).

□

Die Gruppe $G$ operiert auf $X$, indem sie auf jeder Bahn getrennt operiert. Ein Element $g \in G$ permutiert also die Elemente jeder Bahn und transportiert kein Element einer Bahn in eine andere Bahn.
Besteht $X$ nur aus einer einzigen Bahn, so sagt man, $G$ operiert **transitiv** auf $X$. Das bedeutet, dass es für beliebige $x, y \in X$ ein $g \in G$ mit $gx = y$ gibt.

**Definition 5.3** Der **Stabilisator** (auch Standuntergruppe oder Isotropiegruppe) eines Elementes $x \in X$ ist definiert als

$$G_x = \{g \in G : gx = x\}.$$

Man prüft leicht nach, dass $G_x$ eine Untergruppe von $G$ ist. Definitionsgemäß ist $gx = hx$ genau dann, wenn $g^{-1}h \in G_x$ ist.

**Beispiel:** Betrachten wir die Operation von $\mathcal{B}_2$ auf $\mathbb{R}^2$, so ist der Stabilisator der 0 gerade die Untergruppe der linearen Isometrien.

**Lemma 5.4** Es sei $G \times X \to X$ eine Operation von $G$ auf der Menge $X$. Für jedes $x \in X$ induziert die Abbildung

$$\begin{array}{ccc} G & \to & X \\ g & \mapsto & gx \end{array}$$

eine Bijektion $\varphi_x : G/G_x \to B_x$, wobei $G/G_x$ die Menge der Linksnebenklassen bezeichnet. Ist $B_x$ endlich, so folgt $\text{ord}(B_x) = (G : G_x)$, wobei ord $B_x$ die Anzahl der Elemente in der Menge $B_x$ bezeichnet.

**Beweis :** Es gilt

$$\varphi_x(g) = \varphi_x(h) \Leftrightarrow gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x$$

Also ist $\varphi_x$ wohldefiniert und injektiv. Ist $y$ ein beliebiges Element in $B_x$, so gilt $y = gx = \varphi_x(g)$ für ein $g \in G$. Also ist $\varphi_x$ auch surjektiv. □

Es sei $X$ eine endliche Menge, auf der $G$ operiert. Wir nennen $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen von $X$, falls $X$ die disjunkte Vereinigung der Bahnen $B_{x_1}, \ldots, B_{x_r}$ ist.

**Beispiel:** Wir betrachten die natürliche Operation von $GL_2(\mathbb{F}_2)$ auf $\mathbb{F}_2^2 = \{\binom{0}{0}, \binom{1}{0}, \binom{0}{1}, \binom{1}{1}\}$. Die Bahnen sind $\{\binom{0}{0}\}$ und $\{\binom{1}{0}, \binom{0}{1}, \binom{1}{1}\}$. Also ist $\binom{0}{0}, \binom{1}{0}$ oder auch $\binom{0}{0}, \binom{1}{1}$ ein Vertretersystem der Bahnen.

**Satz 5.5 (Bahnengleichung)** Es sei $X$ eine endliche Menge, auf der $G$ operiert, und $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen. Dann gilt

$$\text{ord}(X) = \sum_{i=1}^{r} \text{ord}(B_{x_i}) = \sum_{i=1}^{r} (G : G_{x_i}).$$

**Beweis :** $X$ ist die disjunkte Vereinigung von $B_{x_1}, \ldots, B_{x_r}$. Also gilt die erste Gleichung. Die zweite Gleichung folgt aus Lemma 5.4. □

**Beispiel:** Im Falle der Operation von $GL_2(\mathbb{F}_2)$ auf $\mathbb{F}_2^2$ gilt für das Vertretersystem $\binom{0}{0}, \binom{1}{0}$:

$$G_{\binom{0}{0}} = GL_2(\mathbb{F}_2) \text{ und } G_{\binom{1}{0}} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Da $GL_2(\mathbb{F}_2)$ sechs Elemente hat, stimmt die Formel aus Satz 5.5.

Nun wollen wir die Bahnengleichung auf die Operation von $G$ auf sich selbst durch Konjugation anwenden.

**Definition 5.6** Es sei $G$ eine Gruppe und $S \subset G$ eine beliebige Teilmenge.

i) $Z_S = \{g \in G : gsg^{-1} = s \text{ für alle } s \in S\}$ heißt **Zentralisator** von $S$.

ii) $\mathcal{N}_S = \{g \in G : gSg^{-1} = S\}$ heißt **Normalisator** von $S$.

$Z_S$ und $\mathcal{N}_S$ sind Untergruppen von $G$. Das Zentrum $Z(G)$ von $G$ ist gerade der Zentralisator der Teilmenge $G$.

**Beispiel:** Wir betrachten die Konjugationsoperationen von

$$GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

auf sich selbst. Es ist

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

und

$$Z_{\{\left(\begin{smallmatrix} 01 \\ 10 \end{smallmatrix}\right)\}} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

sowie

$$Z_{\{\left(\begin{smallmatrix} 01 \\ 11 \end{smallmatrix}\right)\}} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

**Satz 5.7 (Klassengleichung)** Es sei $G$ eine endliche Gruppe und $x_1, \ldots, x_r$ ein Vertretersystem der Bahnen von $G \setminus Z(G)$ unter der Konjugationsoperation.
Dann gilt

$$\text{ord}(G) = \text{ord}(Z(G)) + \sum_{i=1}^{r} (G : Z_{\{x_i\}})$$

**Beweis :** Für jedes $z \in Z(G)$ gilt $gzg^{-1} = z$ für alle $g \in G$, also ist die Bahn von $z$ unter der Konjugationsoperation einfach $\{z\}$.
Daher operiert $G$ auch auf dem Komplement $G \setminus Z(G)$ durch Konjugation:

$$\begin{array}{rcl} G \times (G \setminus Z(G)) & \to & G \setminus Z(G) \\ (g, h) & \mapsto & ghg^{-1} \end{array}$$

Die Bahnen dieser Operation sind nach Voraussetzung $B_{x_i}, \ldots, B_{x_r}$. Der Stabilisator von $x_i$ ist

$$\begin{array}{rcl} G_{x_i} & = & \{g \in G : gx_ig^{-1} = x_i\} \\ & = & Z_{\{x_i\}}. \end{array}$$

Also folgt die Behauptung aus der Bahnengleichung Satz 5.5. □

**Beispiel:** Für $G = GL_2(\mathbb{F}_2)$ ist $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ ein Vertretersystem der Bahnen von $G \setminus Z(G) = G \setminus \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. Also stimmt die Klassengleichung hier nach den obigen Berechnungen.

**Definition 5.8** Es sei $G$ eine endliche Gruppe und $p$ eine Primzahl,

i) $G$ heißt $p$-Gruppe, falls $\text{ord}(G)$ eine $p$-Potenz $p^k, k \geq 0$, ist.

ii) Eine Untergruppe $H \subset G$ heißt $p$-Sylowgruppe, wenn $H$ eine $p$-Gruppe ist, für die $p \nmid (G : H)$ gilt.

Eine $p$-Sylowgruppe ist also eine maximale $p$-Untergruppe von $G$. Falls $p \nmid \text{ord}(G)$, so ist $\{1\}$ eine $p$-Sylowgruppe von $G$.
In Satz 3.24 haben wir eine $p$-Gruppe $G$ über die Eigenschaft, dass der Exponent von $G$ eine $p$-Potenz ist, definiert. Für abelsche Gruppen wissen wir schon, dass beide Begriffe übereinstimmen. Für beliebige Gruppen werden wir das später sehen.

**Beispiel:**

i) Die Untergruppe $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ ist eine 2-Sylowgruppe in $GL_2(\mathbb{F}_2)$. Jedes Element der Ordnung 2 in $GL_2(\mathbb{F}_2)$ liefert eine 2-Sylowgruppe. Es gibt also drei 2-Sylowgruppen in $GL_2(\mathbb{F}_2)$. Jede 3-Sylowgruppe in $GL_2(\mathbb{F}_2)$ hat die Ordnung 3, von diesen gibt es also nur eine, nämlich

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

ii) In einer endlichen abelschen Gruppe $G$ gibt es nach Satz 3.37 für jedes $p$ genau eine $p$-Sylowgruppe.

**Satz 5.9** Sei $p$ eine Primzahl und $G$ eine Gruppe der Ordnung $p^k$ für ein $k \geq 1$. Dann gilt $p \mid \text{ord}(Z(G))$, insbesondere ist $Z(G) \neq \{1\}$.

**Beweis :** Nach Satz 5.7 gilt

$$p^k = \text{ord}(G) = \text{ord}(Z(G)) + \sum_{i=1}^{r} (G : Z_{\{x_i\}})$$

für ein Vertretersystem $x_1, \ldots, x_r$ der Bahnen von $G \setminus Z(G)$ unter der Konjugationsoperation. Nach dem Satz von Lagrange gilt

$$(G : Z_{\{x_i\}}) \mid p^k.$$

Ferner ist $(G : Z_{\{x_i\}}) \neq 1$, da sonst $Z_{\{x_i\}} = G$, also $x_i \in Z(G)$ gelten würde. Also sind alle $(G : Z_{\{x_i\}})$ Vielfache von $p$, und somit ist $\text{ord}(Z(G))$ ein Vielfaches von $p$. $\square$

Das folgende Korollar ist uns für abelsche Gruppen schon bekannt.

**Korollar 5.10** Es sei $p$ eine Primzahl und $G$ eine Gruppe der Ordnung $p^k, k \geq 1$. Dann gibt es Untergruppen

$$G = G_k \supset G_{k-1} \supset \cdots \supset G_0 = \{1\}.$$

von $G$, so dass $\text{ord}(G_l) = p^l$ und $G_{l-1}$ ein Normalteiler in $G_l$ ist für alle $l \in \{1, \ldots, k\}$. Also gibt es für jedes $l \in \{1, \ldots, k\}$ eine Untergruppe von $G$ der Ordnung $p^l$, insbesondere existiert ein Element der Ordnung $p$ in $G$.

**Beweis :** (mit Induktion nach $k$) Der Fall $k = 1$ ist klar. Also sei $k > 1$. Nach Satz 5.9 ist $Z(G) \neq 1$, also existiert ein $a \in Z(G)$ mit $a \neq 1$. Aus $\text{ord}(a) \mid p^k$ folgt $\text{ord}(a) = p^r$ für ein $r \geq 1$. Daher gilt $\text{ord}(a^{p^{r-1}}) = p$. Das Element $b := a^{p^{r-1}}$ liegt in $Z(G)$, also ist $\langle b \rangle \subset G$ ein Normalteiler der Ordnung $p$.
Die Faktorgruppe $\overline{G} = G/\langle b \rangle$ hat somit die Ordnung $p^{k-1}$. Nach Induktionsvoraussetzung gibt es Untergruppen

$$\overline{G} = \overline{G}_{k-1} \supset \overline{G}_{k-2} \supset \cdots \supset \overline{G}_0 = \{1\}$$

mit ord $\overline{G}_l = p^l$, so dass $\overline{G}_{l-1} \subset \overline{G}_l$ ein Normalteiler ist. Für die Projektion $\pi : G \to \overline{G}$ setzen wir $G_l := \pi^{-1}(\overline{G}_{l-1})$. Da $\overline{G}_{l-1} \simeq G_l/\langle b \rangle$ ist, gilt ord $(G_l) = p$ ord$(\overline{G}_{l-1}) = p^l$. Nach Übungsblatt 11 ist $G_{l-1}$ ein Normalteiler in $G_l$. Also haben wir eine Kette

$$G = G_k \supset \cdots \supset G_2 \supset G_1 = \langle b \rangle \supset \{1\}$$

mit den gewünschten Eigenschaften gefunden. □

Jetzt können wir die Sylowsätze beweisen. Dazu brauchen wir folgendes technisches Lemma:

**Lemma 5.11** Es sei $G$ eine Gruppe der Ordnung $n = p^k m$ mit einer Primzahl $p$. Dann gilt für die Anzahl $s$ der Untergruppen $H$ von $G$ mit $\text{ord}(H) = p^k$:

$$s \equiv \binom{n-1}{p^k - 1} = \frac{1}{m}\binom{n}{p^k} \mod p.$$

**Beweis :** Sei $X$ die Menge aller $p^k$-elementigen Teilmengen von $G$. Dann ist $\text{ord}(X) = \binom{n}{p^k}$. Die Abbildung

$$\begin{aligned} G \times X &\to X \\ (g, U) &\mapsto gU \end{aligned}$$

ist eine Operation von $G$ auf $X$. Sei $U \in X$ eine $p^k$-elementige Teilmenge von $G$. Dann operiert die Isotropiegruppe

$$G_U = \{g \in G : gU = U\}$$

auf $U$. Die Bahnen dieser Operation sind die Mengen $\{gu : g \in G_U\}$ für $u \in U$, das sind also gewisse Rechtsnebenklassen der Untergruppe $G_U \subset G$. Daher sind diese Bahnen paarweise disjunkte Mengen der Ordnung $\text{ord}(G_U)$, deren Vereinigung $U$ ist. Also teilt $\text{ord}(G_U)$ die Zahl $p^k = \text{ord}(U)$, d.h. $\text{ord}(G_U) = p^{k'}$ für ein $k' \leq k$.
Nun betrachten wir wieder die Operation von $G$ auf $X$. Nach Satz 5.5 gilt für ein Vertretersystem $U_1, \ldots, U_r$ der Bahnen

$$\binom{n}{p^k} = \text{ord}(X) = \sum_{i=1}^{r} \text{ord}(B_{U_i}) = \sum_{i=1}^{r} (G : G_{U_i})$$

Ist $\text{ord}(G_{U_i}) = p^{k_i}$, so ist nach dem Satz von Lagrange $(G : G_{U_i}) = mp^{k-k_i}$.
Nun sammeln wir alle Vertreter $U_i$ auf, für die $k_i = k$, also ord $B_{U_i} = (G : G_{U_i}) = m$ ist, indem wir

$$I := \{i \in \{1, \ldots, r\} : k_i = k\}$$

setzen. Dann ist

$$\begin{aligned} m \,\text{ord}(I) &= \sum_{i \in I} (G : G_{U_i}) \\ &= \binom{n}{p^k} - \sum_{i \notin I} (G : G_{U_i}) \\ &\equiv \binom{n}{p^k} \bmod mp, \end{aligned}$$

da für alle $i \notin I$ der Index $(G : G_{U_i})$ ein Vielfaches von $mp$ ist.
Somit genügt es zu zeigen, dass $\text{ord}(I)$ mit der Anzahl aller Untergruppen $H$ der Ordnung $p^k$ übereinstimmt.
Sei $H \subset G$ eine solche Untergruppe. Dann ist $(G : H) = m$. Die Bahn von $H$ unter der Operation von $G$ auf $X$ ist die Menge $B_H = \{gH : g \in G\}$, sie besteht also genau aus den Linksnebenklassen von $H$ in $G$. Somit ist $\text{ord}(B_H) = m$. Daher ist $B_H = B_{U_i}$ für ein $i \in I$.
Ist $B_{H_1} = B_{H_2}$ für zwei Untergruppen $H_1, H_2$ der Ordnung $p^k$, so folgt $gH_1 = H_2$ für ein $g \in G$, also $gh = 1$ für ein $h \in H_1$ und daher $g = h^{-1} \in H_1$. Es folgt also $H_1 = H_2$. Die Untergruppen $H$ der Ordnung $p^k$ liefern also verschiedene Bahnen der Ordnung $m$, daher ist $s \leq \text{ord}(I)$.

Wir fixieren ein $i \in I$ und lassen wie oben $G_{U_i}$ auf $U_i$ operieren. Da die Bahnen dieser Operation alle die Ordnung ord $G_{U_i} = p^k = \text{ord}\, U_i$ haben, kann es nur eine Bahn geben. Also ist $U_i = G_{U_i} u_i$ für ein $u_i \in U_i$. Daraus folgt

$$\begin{aligned} B_{U_i} &= \{gU_i : g \in G\} \\ &= \{gG_{U_i}u_i : g \in G\} \\ &= \{g(u_i^{-1}G_{U_i}u_i) : g \in G\} \\ &= B_H \end{aligned}$$

für die Untergruppe $H = u_i^{-1} G_{U_i} u_i$ von $G$ der Ordnung

$$\text{ord}(H) = \text{ord}(G_{U_i}) = \frac{n}{(G : G_{U_i})} = p^k.$$

Daher gilt in der Tat $s = \text{ord}(I)$. □

**Satz 5.12 (Sylowsätze)** Es sei $G$ eine endliche Gruppe und $p$ eine Primzahl.

i) Zu jeder $p$-Untergruppe $H$ von $G$ existiert eine $p$-Sylowgruppe $S \subset G$ mit $H \subset S$. Insbesondere enthält $G$ eine $p$-Sylowgruppe.

ii) Ist $S \subset G$ eine $p$-Sylowgruppe, so auch $gSg^{-1}$ für jedes $g \in G$. Umgekehrt sind je zwei $p$-Sylowgruppen $S_1$ und $S_2$ konjugiert zueinander, d.h. es gibt ein $g \in G$ mit $gS_1g^{-1} = S_2$.

iii) Ist $s_p$ die Anzahl der $p$-Sylowgruppen in $G$, so gilt

$$s_p \mid G$$

und

$$s_p \equiv 1 \bmod p.$$

**Beweis :**

i) Es sei $n = \text{ord}(G)$. Wir schreiben $n = mp^k$ mit ggT$(m, p) = 1$ und $k \geq 0$. Dann sind die $p$-Sylowgruppen in $G$ genau die Untergruppen von $G$ der Ordnung $p^k$. Also gilt nach Lemma 5.11

$$s_p \equiv \binom{n-1}{p^k-1} = \frac{1}{m}\binom{n}{p^k} \bmod p.$$

Um diese Restklasse modulo $p$ zu berechnen, wenden wir Lemma 5.11 auf die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ an. Diese enthält für jeden Teiler $d$ von $\mathbb{Z}$ genau eine Untergruppe der Ordnung $d$, nämlich $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$. Also gilt

$$1 \equiv \binom{n-1}{p^k-1} \bmod p,$$

und somit auch $s_p \equiv 1 \bmod p$.

Insbesondere ist $s_p \neq 1$, d.h. $G$ enthält eine $p$-Sylowgruppe $S$.

Ist $H \subset G$ eine beliebige $p$-Untergruppe, so betrachten wir die natürliche Operation von $H$ auf der Menge der Linksnebenklassen $G/S$

$$\begin{aligned} H \times G/S &\to G/S \\ (h, gS) &\mapsto hgS. \end{aligned}$$

Nach der Bahnengleichung Satz 5.5 gilt für ein Vertretersystem $x_1, \ldots, x_r$ der Bahnen dieser Operation.

$$\text{ord}(G/S) = \sum_{i=1}^{r} \text{ord}(B_{x_i}).$$

Es gilt $\text{ord}(G/S) = \text{ord}(G)/\text{ord}(S) = m$. Nach Lemma 5.4 ist $\text{ord}(B_{x_i}) = (H : H_{x_i})$ für den Stabilisator $H_{x_i}$ der Nebenklasse $x_i$. Also ist $\text{ord}(B_{x_i})$ als Teiler von $\text{ord}(H)$ eine $p$-Potenz. Da $p$ nicht $\text{ord}(G/S) = m$ teilt, muss mindestens für ein $x_i$ die Bahn $B_{x_i}$ die Ordnung $p^0 = 1$ haben. Ist $x_i$ die Nebenklasse $g_iS$ von $S$ in $G$, so gilt also $hg_iS = g_iS$ für alle $h \in H$. Somit folgt $H \subset g_iSg^{-1}$. Wegen $\text{ord}(g_iSg_i^{-1}) = \text{ord}\ (S) = p^k$ ist auch $g_iSg_i^{-1}$ eine $p$-Sylowgruppe von $G$.

ii) Wir haben gerade gesehen, dass mit $S$ auch $gSg^{-1}$ eine $p$-Sylowgruppe ist. Ist $S'$ eine weitere $p$-Sylowgruppe in $G$, so existiert nach dem Beweis von i), angewandt auf $H = S'$, ein $g \in G$ mit $S' \subset gSg^{-1}$. Da $\text{ord}(S') = p^k = \text{ ord}\ (gSg^{-1})$ gilt, folgt $S' = gSg^{-1}$.

iii) Wir haben im Beweis von i) schon gesehen, dass $s_p \equiv 1 \bmod p$ gilt. Sei $X$ die Menge der $p$-Sylowgruppen in $G$. Nach ii) sind je zwei von ihnen konjugiert, d.h. die Konjugationsoperation $G \times X \to X$, $(g, S) \mapsto gSg^{-1}$ hat nur eine Bahn. Daher gilt nach Lemma 5.4

$$\text{ord}\ (X) = (G : G_S)$$

für den Stabilisator $G_S = \{g \in G : gSg^{-1} = S\} = \mathcal{N}_S$. Somit ist $s_p = \text{ord}(X) = (G : G_S)$ ein Teiler von $\text{ord}(G)$.

□

**Korollar 5.13 (Satz von Cayley)**

i) Für jeden Teiler $p$ der Gruppenordnung enthält $G$ ein Element der Ordnung $p$.

ii) Eine $p$-Sylowgruppe $S$ von $G$ ist genau dann ein Normalteiler, wenn $S$ die einzige $p$-Sylowgruppe ist, d.h. wenn $s_p = 1$ gilt.

**Beweis :**

i) $G$ enthält nach Satz 5.12 eine $p$-Sylowgruppe $S$, diese ist $\neq 1$, da $p$ die Gruppenordnung teilt. Nach Korollar 5.10 enthält $S$ ein Element der Ordnung $p$.

ii) $S$ ist ein Normalteiler in $G \Leftrightarrow gSg^{-1} = S$ für alle $g \in G \overset{5.12ii)}{\Leftrightarrow} S$ ist die einzige $p$-Sylowgruppe in $G$.

□

**Korollar 5.14** Ist $G$ eine beliebige endliche Gruppe, so teilt der Exponent von $G$ die Gruppenordnung. Beide Zahlen haben dieselben Primteiler.

**Beweis :** Die erste Behauptung haben wir in Blatt 9, Aufgabe 1 gezeigt.
Ist $p$ ein Teiler von ord$(G)$, so gibt es nach Korollar 5.13 ein $g \in G$ mit ord$(g) = p$. Also teilt $p$ den Exponenten von $G$. □

Insbesondere stimmen unsere beiden Definitionen von $p$-Gruppen in Satz 3.24 und Definition 5.8 überein.
Wir wollen jetzt noch einige Konsequenzen aus den Sylowsätzen 5.12 und dem Satz über $p$-Gruppen 5.10 ziehen.

**Satz 5.15** Sei $p$ eine Primzahl. Jede Gruppe der Ordnung $p^2$ ist abelsch.

**Beweis :** Angenommen, $G$ ist eine nicht-abelsche Gruppe der Ordnung $p^2$. Dann ist $Z(G) \neq G$, nach Satz 5.9 gilt also ord$(Z(G)) = p$. Ist $x \in G \setminus Z(G)$, so sei $Z_{\{x\}} = \{g : gxg^{-1} = x\}$ der Zentralisator von $x$. Dies ist eine Untergruppe von $G$, die $Z(G)$ enthält. Da $x \in Z_{\{x\}} \setminus Z(G)$ ist, gilt $Z(G) \subsetneq Z_{\{x\}}$. Da ord$Z_{\{x\}}$ ein Teiler von ord$(G) = p^2$ ist, folgt ord$Z_{\{x\}} = p^2$, also $Z_{\{x\}} = G$. Das bedeutet aber $x \in Z(G)$, was ein Widerspruch ist. Daher ist $G$ abelsch. □

**Korollar 5.16** Es seien $p$ und $q$ Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede Gruppe $G$ der Ordnung $pq$ zyklisch.

**Beweis :** Es sei $s_p$ die Anzahl der $p$-Sylowgruppen in $G$. Dann gilt nach Satz 5.12 $s_p \mid pq$ und $s_p \equiv 1 \bmod p$. Daher gilt $p \nmid s_p$, d.h. $s_p \mid q$. Wäre $s_p = q$, so folgte $q \equiv 1 \bmod p$ im Widerspruch zur Voraussetzung. Also ist $s_p = 1$, d.h. es existiert genau eine $p$-Sylowgruppe $S_p \subset G$. Nach Korollar 5.13 ii) ist $S_p$ dann ein Normalteiler in $G$. Es sei ferner $s_q$ die Anzahl der $q$-Sylowgruppen in $G$. Nach Satz 5.12 gilt $s_q \mid pq$ und $s_q \equiv 1 \bmod q$, also wie oben $s_q \mid p$. Da $p < q$ ist, kann $s_q$ nicht gleich $p$ sein, also folgt $s_q = 1$. Also ist die einzige $q$-Sylowgruppe $S_q \subset G$ ein Normalteiler. Die Ordnung der Untergruppe $S_p \cap S_q$ teilt $p$ und $q$, also folgt $S_p \cap S_q = \{1\}$. Wir zeigen nun, dass die Abbildung

$$\begin{aligned} \varphi : S_p \times S_q &\to G \\ (a, b) &\mapsto ab. \end{aligned}$$

ein Isomorphismus ist.
Zunächst müssen wir zeigen, dass $\varphi$ ein Homomorphismus ist. Ist $a \in S_p$ und $b \in S_q$, so gilt $aba^{-1} \in S_q$, also $(aba^{-1})b^{-1} \in S_q$ und $bab^{-1} \in S_p$, also $a(bab^{-1}) \in S_p$, woraus $aba^{-1}b^{-1} \in S_p \cap S_q = \{1\}$ folgt. Daher kommutieren $a$ und $b$, und es gilt für $a, a' \in S_p$ und $b, b' \in S_q$:

$$\begin{aligned} \varphi(a, b)\varphi(a', b') &= aba'b' \\ &= aa'bb' \\ &= \varphi(aa', bb'). \end{aligned}$$

Somit ist $\varphi$ ein Homomorphismus. Da Kern$\varphi = S_p \cap S_q = \{1\}$ gilt, ist $\varphi$ injektiv, und da beide Seiten die Ordnung $pq$ haben, auch surjektiv. Daher ist $G$ isomorph zu dem Produkt $S_p \times S_q$ zweier zyklischer Gruppen teilerfremder Ordnung. Nach dem chinesischen Restsatz 3.26 ist $G$ dann ebenfalls zyklisch. □

Als Anwendung sieht man, dass jede Gruppe der Ordnung 15 zyklisch ist, vgl. Blatt 8, Aufgabe 3.

In § 3 haben wir die Struktur aller endlichen abelschen Gruppen bestimmt. Jede endliche abelsche Gruppe ist Produkt zyklischer Gruppen. Was weiß man über die Struktur beliebiger endlicher Gruppen?

**Definition 5.17** Eine Gruppe $G$ heißt **einfach**, wenn $G$ nur die trivialen Normalteiler 1 und $G$ besitzt.

Ist $G$ abelsch, so ist $G$ genau dann einfach, wenn $G$ eine zyklische Gruppe von Primzahlordnung ist. Hat eine Gruppe $G$ einen nicht-trivialen Normalteiler $N$, so sitzt $G$ in einer exakten Sequenz von Gruppen

$$0 \to N \to G \to G/N \to 0.$$

Sukzessive kann man $G$ so durch Gruppen kleinerer Ordnung „auflösen".
Es bleibt das Problem, die Struktur endlicher einfacher Gruppen (bis auf Isomorphie) zu bestimmen. Das ist das sogenannte **„Klassifikationsproblem endlicher einfacher Gruppen"**. Dieses Problem wurde in mehreren Hundert Arbeiten von über 100 Autoren in der Zeit von 1955 - 1983 gelöst. In diesen Beweisen sind immer wieder Lücken aufgetaucht, so dass einige Experten bezweifeln, dass die Klassifikation vollständig bewiesen ist.

**Klassifikationssatz für endliche einfache Gruppen:**
Jede endliche einfache Gruppe ist isomorph zu einer der folgenden Gruppen:

I) eine (zyklische) Gruppe von Primzahlordnung

II) eine alternierende Gruppe $A_n$ für $n \geq 5$

III) eine Gruppe von Lie Typ

IV) eine von 26 sporadischen Gruppen (die meist nach ihren Entdeckern heißen).

Die alternierende Gruppe $A_n$ ist definiert als der Kern der Signumabbildung

$$\text{sgn} : \mathcal{S}_n \to \{\pm|\}.$$

auf der symmetrischen Gruppe $\mathcal{S}_n$. In LAAG I haben wir gesehen, dass $\text{sgn}(\sigma) = \det P_\sigma$ für die Permutationsmatrix $P_\sigma$ zu $\sigma$ gilt. $A_n$ ist also ein Normalteiler in $\mathcal{S}_n$ der Ordnung $\frac{n!}{2}$.
Da nach Blatt 11 die einzigen einfachen Gruppen der Ordnung $< 60$ diejenigen vom Typ I) im Klassifikationssatz sind, kann man frühestens für $n = 5$ erwarten, dass die Gruppe $A_n$ einfach ist. In der Tat ist die Gruppe $A_5$ der Ordnung $\frac{5!}{2} = 60$ die kleinste einfache Gruppe, die nicht vom Typ I) ist.
Die Gruppen $G$ von Lie Typ III) lassen sich alle als Untergruppen der Gruppe $GL_n(\mathbb{F}_p)$ für einen endlichen Körper $\mathbb{F}_p$ beschreiben. Genauer gesagt heißt eine Gruppe $G$ von Lie Typ, falls sie von der Form $G = \underline{G}(K)$ für eine lineare algebraische Gruppe $\underline{G}$ ist. Diese Definition können wir hier nicht näher erklären. Beispiele für endliche einfache Gruppen von Lie Typ sind

i) $\mathrm{PSL}(n,\mathbb{F}_p) = \mathrm{SL}(n,\mathbb{F}_p)/Z(\mathrm{SL}(n,\mathbb{F}_p))$ mit

$$\mathrm{SL}(n,\mathbb{F}_p) = \{A \in \mathbb{F}_p^{n\times n} : \det A = 1\}$$

und Zentrum

$$Z(\mathrm{SL}(n,\mathbb{F}_p)) = \left\{ \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} : a \in \mathbb{F}_p^\times, a^n = 1 \right\}$$

ii) $\mathrm{SO}(n,\mathbb{F}_p)/Z(\mathrm{SO}(n,\mathbb{F}_p))$ mit der speziellen orthogonalen Gruppe

$$\mathrm{SO}(n,\mathbb{F}_p) = \{A \in O(n,\mathbb{F}_p) : \det A = 1\},$$

wobei die orthogonale Gruppe natürlich

$$O(n,\mathbb{F}_p) = \{A \in \mathbb{F}_p^{n\times n} : AA^t = E_n\}$$

ist. Das Zentrum von $Z(\mathrm{SO}(n,\mathbb{F}_p))$ ist

$$\begin{aligned} Z(\mathrm{SO}(n,\mathbb{F}_p)) &= \left\{ \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} : a^2 = 1, a^n = 1 \right\} \\ &= \begin{cases} \{\pm E_n\}, \text{ falls } n \text{ gerade} \\ \{E_n\}, \text{ falls } n \text{ ungerade} \end{cases} \end{aligned}$$

iii) $Sp(2n,\mathbb{F}_p)/Z(Sp(2n,\mathbb{F}_p))$ mit der symplektischen Gruppe $Sp(2n,\mathbb{F}_p)$, die folgendermaßen definiert ist:

$$Sp(2n,\mathbb{F}_p) = \{A \in \mathrm{GL}(2n,\mathbb{F}_p) : A^t J A = J\}$$

für die $2n \times 2n$-Matrix

$$J = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$$

Man kann zeigen, dass $Sp(2n,\mathbb{F}_p) \subset \mathrm{SL}(2n,\mathbb{F}_p)$ gilt. Das Zentrum der symplektischen Gruppe ist

$$\begin{aligned} Z(Sp(2n,\mathbb{F}_p)) &= Sp(2n,\mathbb{F}_p) \cap \left\{ \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} : a^{2n} = 1 \right\} \\ &= \{\pm E_n\} \end{aligned}$$

Die symplektische Gruppe

$$Sp(2n, K) = \{A \in \mathrm{GL}(2n, K) : A^t J A = J\}$$

lässt sich über jedem Körper $K$ definieren.
Die Matrix $J$ ist die Koordinatenmatrix der folgenden Bilinearform $\beta$ bezüglich der kanonischen Basis $e_1, \ldots, e_n, e_{n+1}, \ldots, e_{2n}$:

$$\beta(e_i, e_j) = \begin{cases} 1, j = i + n \\ -1, j = i - n \\ 0, \text{ sonst.} \end{cases}$$

Es gilt also $\beta(e_i, e_{i+n}) = 1 = -\beta(e_{i+n}, e_i)$ für $i = 1, \ldots, n$. Die Form $\beta$ ist schiefsymmetrisch und nicht-ausgeartet.
Ist $A \in \mathrm{GL}(2n, K)$ eine invertierbare Matrix, so ist die Matrix $A^t J A$ schiefsymmetrisch. Auf diese Weise operiert $\mathrm{GL}(2n, K)$ auf der Menge der schiefsymmetrischen Matrizen in $K^{2n \times 2n}$. Die Gruppe $Sp(2n, K)$ ist der Stabilisator der Matrix $J$ unter dieser Operation.
Außer diesen drei „klassischen“ Gruppen I) - III) von Lie Typ gibt es noch einige sogenannte exzeptionelle Gruppen von Lie Typ.

Die Gruppen von Typ I), II), III) tauchen alle in „Reihen“ auf, sie lassen sich alle als Automorphismengruppe einer recht natürlichen mathematischen Struktur beschreiben. Die sporadischen Gruppen (Typ IV) sind Ausnahmeerscheinungen. Die kleinste sporadische Gruppe ist die sogenannte Matthieu-Gruppe der Ordnung 7920. Die größte sporadische Gruppe heißt Monstergruppe, sie hat etwa $10^{53}$ Elemente.

# 6 Die Gruppe SU (2 C)

Wir wollen jetzt einige geometrische Eigenschaften der speziellen unitären Gruppe SU(2,$\mathbb{C}$) beschreiben. Dabei besteht SU(2, $\mathbb{C}$) aus den Matrizen der unitären Gruppe $U(2, \mathbb{C})$, die Determinante 1 haben, d.h.

$$\mathrm{SU}(2, \mathbb{C}) = \{A \in \mathbb{C}^{2\times 2} : A^* A = E_n, \det A = 1\}$$

mit $A^* = \overline{A}^t$.
Ist $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SU}(2, \mathbb{C})$, so gilt nach der Cramer'schen Regel für die Matrixversion

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

aus $A^* = A^{-1}$ folgt also

$$\begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

d.h. $\overline{a} = d$ und $\overline{b} = -c$.
Also gilt $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$. Die Bedingung det $A$ =1 liefert außerdem die Gleichung

$$|a|^2 + |b|^2 = 1.$$

Umgekehrt liefert jedes Paar $(a, b)$ komplexer Zahlen mit $|a|^2 + |b|^2 = 1$ eine Matrix $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{SU}(2, \mathbb{C})$. Also gilt

$$\mathrm{SU}(2, \mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \text{ mit } |a|^2 + |b|^2 = 1 \right\}.$$

Wir haben also „zwei Freiheitsgrade“, nämlich die komplexen Zahlen $a$ und $b$. In der Tat gibt es einen Begriff von Dimension für klassische Gruppen wie die $\mathrm{SU}(2, \mathbb{C})$, der in diesem Fall auch die komplexe Dimension 2 liefert.
Zerlegen wir $a$ und $b$ in Real- und Imaginärteil, also

$$a = x_1 + ix_2 \text{ und } b = x_3 + ix_4,$$

so übersetzt sich die Gleichung $|a|^2 + |b|^2 = 1$ in $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$.
Also ist die Abbildung

$$\theta : S_3 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\} \to \mathrm{SU}(2, \mathbb{C}),$$

gegeben durch

$$(x_1, x_2, x_3, x_4) \mapsto \begin{pmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{pmatrix},$$

eine Bijektion.
Die Menge $S_3 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\}$ wird die Einheitssphäre in $\mathbb{R}^4$ oder auch 3-Sphäre genannt. $S_3$ ist eine Verallgemeinerung des Einheitskreises

$$S_1 = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}$$

im $\mathbb{R}^2$ und der Einheitskugel

$$S_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}$$

im $\mathbb{R}^3$.
Die 3-Sphäre $S_3$ erbt als Teilmenge des $\mathbb{R}^4$ eine Topologie. Die Gruppe $\mathrm{SU}(2,\mathbb{C})$ erbt als Teilmenge der $\mathbb{C}^{2\times 2}$ ebenfalls eine Topologie. Offenbar ist sowohl $\theta$ als auch die Umkehrabbildung $\theta^{-1}$ stetig. Eine stetige bijektive Abbildung, deren Umkehrabbildung ebenfalls stetig ist, heißt Homöomorphismus. Somit ist $\mathrm{SU}(2,\mathbb{C})$ homöomorph zur Einheitssphäre in $\mathbb{R}^4$.
Es ist bemerkenswert, dass die 3-Sphäre $S_3$ über den Isomorphismus $\theta$ eine Gruppenstruktur erbt. Auf der 2-Sphäre lässt sich nämlich keine Gruppenstruktur mit stetiger Gruppenverknüpfung definieren.
Wir werden ab jetzt einfach $\mathrm{SU}(2,\mathbb{C})$ vermöge der Abbildung $\theta$ mit der 3-Sphäre identifizieren. Nun wollen wir die Breitenkreise und die Meridiane auf $\mathrm{SU}(2,\mathbb{C})$ beschreiben. Der Punkt $(1,0,0,0)$ heißt **Nordpol** der $S_3$, er entspricht der Matrix $E \in \mathrm{SU}(2,\mathbb{C})$. Der Punkt (-1,0,0,0) heißt **Südpol** der $S_3$, er entspricht der Matrix $-E \in \mathrm{SU}(2,\mathbb{C})$.

**Definition 6.1** Ist $c \in \mathbb{R}$ eine Zahl mit $-1 < c < 1$, so heißt

$$\begin{aligned} B_c &= \{(x_1,x_2,x_3,x_4) \in S_3 : x_1 = c\} \\ &= \{(c,x_2,x_3,x_4) : x_2^2 + x_3^2 + x_4^2 + c^2 = 1\} \end{aligned}$$

Breitengrad auf $S_3$ zu $c$. Der Breitengrad $B_c$ entspricht der Teilmenge

$$\theta(B_c) = \left\{ \begin{pmatrix} c+ix_2 & x_3+ix_4 \\ -x_3+ix_4 & c-ix_2 \end{pmatrix} \right\}$$

von $\mathrm{SU}(2,\mathbb{C})$. Diese bezeichnen wir als Breitengrad zu $c$ auf $\mathrm{SU}(2,\mathbb{C})$.

**Satz 6.2**

i) Der Breitengrad zu $c$ auf $\mathrm{SU}(2,\mathbb{C})$ lässt sich beschreiben als

$$\theta(B_c) = \{A \in \mathrm{SU}(2,\mathbb{C}) : \mathrm{Spur}A = 2c\}$$

ii) Die Bahnen der Operation von $\mathrm{SU}(2,\mathbb{C})$ auf sich durch Konjugation sind gerade die einelementigen Mengen $\{E\}$, $\{-E\}$ sowie alle Breitengrade $\theta(B_c)$ für $-1 < c < 1$.

Zum Beweis dieses Satzes brauchen wir das folgende Lemma.

**Lemma 6.3** Sei $A \in \mathrm{SU}(2,\mathbb{C})$ eine Matrix mit den Eigenwerten $\lambda$ und $\mu$. Dann ist $\mu = \overline{\lambda}$ und $A$ ist in $\mathrm{SU}(2,\mathbb{C})$ konjugiert zu der Matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$.

**Beweis :** Für $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{SU}(2,\mathbb{C})$ gilt

$$\begin{aligned} \chi_A(X) &= \det(XE_2 - A) = \det(\begin{pmatrix} X-a & -b \\ \overline{b} & X-\overline{a} \end{pmatrix} \\ &= X^2 - (a+\overline{a})X + |a|^2 + |b|^2 = X^2 - 2(\mathrm{Re}(a))X + 1. \end{aligned}$$

Also ist Spur$A = 2\mathrm{Re}(a)$.
Da $A$ unitär ist, gibt es nach dem Spektralsatz für normale Matrizen ein $P \in U(2,\mathbb{C})$ mit

$$PAP^* = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \text{ oder } PAP^* = \begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix}.$$

Nun ist Spur $(A) = \mathrm{Spur}(PAP^{-1}) = \lambda + \mu$, woraus $\lambda + \mu \in \mathbb{R}$ folgt. Also ist $\mathrm{Im}(\mu) = -\mathrm{Im}(\lambda)$. Da mit $A$ auch $PAP^*$ unitär ist, gilt ferner $|\mu|^2 = |\lambda|^2 = 1$ und $1 = \det A = \lambda\mu$. Daraus folgt $\lambda = \overline{\mu}$.
Es bleibt zu zeigen, dass wir ein $Q \in \mathrm{SU}(2,\mathbb{C})$ finden, für das $QAQ^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$ gilt.
Wir setzen $\delta = \det P$. Aus $P^*P = 1$ folgt $\det P^* \det P = \overline{\delta}\delta = |\delta|^2 = 1$. Es sei $\varepsilon \in \mathbb{C}$ eine Zahl mit $\varepsilon^2 = \delta$. Dann ist auch $|\varepsilon|^2 = 1$. Die Matrix $Q = \varepsilon^{-1}P$ liegt also in $\mathrm{SU}(2,\mathbb{C})$. Sie erfüllt wegen $|\varepsilon^{-1}|^2 = 1$ die Gleichung

$$\begin{aligned} QAQ^* &= \varepsilon^{-1}PAP^*\overline{\varepsilon}^{-1} \\ &= \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} \text{ oder } \begin{pmatrix} \overline{\lambda} & 0 \\ 0 & \lambda \end{pmatrix}. \end{aligned}$$

Im zweiten Fall konjugieren wir $QAQ^*$ noch mit der Matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SU}(2,\mathbb{C})$, das vertauscht die Reihenfolge der Eigenwerte auf der Diagonalen. □

Jetzt können wir Satz 6.2 zeigen.

**Beweis :** (von Satz 6.2)

i) Wir zeigen

$$\theta(B_c) = \{A \in \mathrm{SU}(2,\mathbb{C}) : \mathrm{Spur}A = 2c\}.$$

Ist $A \in \theta(B_c)$, so gilt $A = \begin{pmatrix} c + ix_2 & x_3 + ix_4 \\ x_3 + ix_4 & c - ix_2 \end{pmatrix}$, also ist $\mathrm{Spur}(A) = 2c$.
Ist umgekehrt $A \in \mathrm{SU}(2,\mathbb{C})$ eine Matrix mit $\mathrm{Spur}(A) = 2c$, so schreiben wir

$$A = \begin{pmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{pmatrix} = \theta(x_1, x_2, x_3, x_4)$$

und erhalten $2c = \text{Spur}A = 2x_1$, also $c = x_1$. Somit liegt $A$ in $\theta(B_c)$.

ii) Offenbar liegen $E$ und $-E$ im Zentrum von $\text{SU}(2,\mathbb{C})$, die zugehörigen Bahnen unter der Konjugationsoperation sind also die Mengen $\{E\}, \{-E\}$.

Es sei $A \in \text{SU}(2,\mathbb{C})$ eine Matrix ungleich $\pm E$. Dann ist $A = \theta(x_1, x_2, x_3, x_4)$ für einen Punkt $(x_1, x_2, x_3, x_4) \in S_3$ mit $x_1 \neq \pm 1$. Liegt $A' \in \text{SU}(2,\mathbb{C})$ in derselben Konjugationsklasse von $\text{SU}(2,\mathbb{C})$ wie $A$, so gilt $\text{Spur}A' = \text{Spur}A = 2x_1$. Somit liegt $A'$ nach i) im Breitengrad $\theta(B_c)$ für $c = x_1$. Aus $x_1 \neq \pm 1$ folgt $-1 < c < 1$.

Es sei umgekehrt $A' \in \theta(B_c)$ gegeben. Dann ist $\text{Spur}(A') = 2c = \text{Spur}A$. Es seien $\lambda', \overline{\lambda}'$ die Eigenwerte von $A'$ und $\lambda, \overline{\lambda}$ die Eigenwerte von $A$ (vgl. Lemma 6.3). Dann ist $2\text{Re}\lambda = 2\text{Re}\lambda' = 2c$. Außerdem gilt $|\lambda|^2 = |\lambda'|^2 = 1$, woraus $\text{Re}\lambda = \text{Re}\lambda'$ und $\text{Im}\lambda = \pm\text{Im}\lambda'$ folgt. Also gilt $\lambda = \lambda'$ oder $\lambda = \overline{\lambda}'$. In beiden Fällen sind nach Lemma 6.3 sowohl $A$ als auch $A'$ konjugiert zu $\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$, also liegt $A'$ in derselben Konjugationsklasse wie $A$. Daher sind die nicht-trivialen Konjugationsklassen wirklich genau die Breitengrade.

□

Als nächstes wollen wir auf der $\text{SU}(2,\mathbb{C})$ Meridiane, also Längengrade, einführen. Einen Meridian der 2-Sphäre $S_2$ kann man als Schnitt der Sphäre mit einem zweidimensionalen Unterraum $W \subset \mathbb{R}^3$, der durch die beiden Pole $(\pm 1, 0, 0)$ geht, beschreiben. Daher definieren wir:

**Definition 6.4**

i) Ein Meridian in $S_3$ ist der Durchschnitt von $S_3$ mit einem zweidimensionalen Unterraum $W \subset \mathbb{R}^4$, der beide Pole $(\pm 1, 0, 0, 0)$ enthält.

ii) Eine Teilmenge von $\text{SU}(2,\mathbb{C})$ der Form $\theta(M)$ für einen Meridian $M \subset S_3$ heißt **Meridian** in $\text{SU}(2,\mathbb{C})$.

**Beispiel:** Für $W = \{(x_1, x_2, 0, 0) : x_1, x_2 \in \mathbb{R}\}$ ist

$$M = W \cap S_3 = \{(x_1, x_2, 0, 0) : x_1^2 + x_2^2 = 1\}$$

ein Meridian in $S_3$. Der zugehörige Meridian ist $\text{SU}(2,\mathbb{C})$ ist

$$\begin{aligned} T = \theta(M) &= \left\{ \begin{pmatrix} x_1 + ix_2 & 0 \\ 0 & x_1 - ix_2 \end{pmatrix} : x_1^2 + x_2^2 = 1 \right\} \\ &= \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} : \lambda \in \mathbb{C} \text{ mit } |\lambda|^2 = 1 \right\}. \end{aligned}$$

Die Meridiane in $S_3$ sind „Kreise“ durch die Pole, also „eindimensionale“ Objekte, während die Breitengrade „zweidimensionale“ Objekte sind.
Jetzt können wir alle Meridiane in $\mathrm{SU}(2,\mathbb{C})$ beschreiben.

**Satz 6.5** Die Meridiane in $\mathrm{SU}(2,\mathbb{C})$ sind genau die zu $T$ konjugierten Untergruppen $QTQ^{-1}$ für $Q \in \mathrm{SU}(2,\mathbb{C})$.

**Beweis :** Wir haben oben gesehen, dass $T = \theta(M)$ für den Meridian $M = W \cap S_3$ mit $W = \{(x_1, x_2, 0, 0) : x_1, x_2 \in \mathbb{R}\}$ gilt. Wir zeigen zunächst, dass für beliebiges $Q = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{SU}(2,\mathbb{C})$ die zu T konjugierte Untergruppe $QTQ^{-1}$ ebenfalls ein Meridian ist. Es gilt $QTQ^{-1} = \left\{ Q \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} Q^{-1} : \lambda \in \mathbb{C}, |\lambda|^2 = 1 \right\}$, und wir berechnen

$$\begin{aligned} Q \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} Q^{-1} &= \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} \\ &= \begin{pmatrix} \lambda a\overline{a} + \overline{\lambda} b\overline{b} & ab(\overline{\lambda} - \lambda) \\ -\overline{a}\overline{b}(\lambda - \overline{\lambda}) & \overline{\lambda}\overline{a}a + \lambda\overline{b}b \end{pmatrix} \end{aligned}$$

Da $Q \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} Q^{-1}$ in $\mathrm{SU}(2,\mathbb{C})$ liegt, brauchen wir nur die obere Reihe zu berechnen.

Ist $\lambda = w_1 + iw_2$, d.h. $\begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} = \theta(w_1, w_2, 0, 0)$ und $a = x_1 + ix_2, b = x_3 + x_4$, also $Q = \theta(x_1, x_2, x_3, x_4)$, so gilt

$$\begin{aligned} Q \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} Q^{-1} &= \begin{pmatrix} w_1 + iw_2(x_1^2 + x_2^2 - x_3^2 - x_4^2) & 2w_2(x_1x_4 + x_2x_3 + 2iw_2(x_2x_4 - x_1x_3) \\ * & * \end{pmatrix} \\ &= \theta(w_1, w_2(x_1^2 + x_2^2 - x_3^2 - x_4^2), 2w_2(x_1x_4 + x_2x_3), 2w_2(x_2x_4 - x_1x_3)). \end{aligned}$$

Die lineare Abbildung $f : \mathbb{R}^4 \to \mathbb{R}^4$, gegeben durch Multiplikation mit der Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x_1^2 + x_2^2 - x_3^2 - x_4^2 & 0 & 0 \\ 0 & 2(x_1x_4 + x_2x_3) & 1 & 0 \\ 0 & 2(x_2x_4 - x_1x_3) & 0 & 1 \end{pmatrix},$$

bildet den Unterraum $W \subset \mathbb{R}^2$ auf einen zweidimensionalen Unterraum $W' \subset \mathbb{R}^2$ ab, der natürlich von $Q$ abhängt. Da $\pm E$ in $QTQ^{-1}$ enthalten ist, enthält $W'$ die Pole $(\pm 1, 0, 0, 0)$. Somit ist $QTQ^{-1}$ im Meridian $\theta(W' \cap S_3)$ enthalten. Ist andererseits ein

Punkt $\theta(w') \in \theta(W' \cap S_3)$ gegeben, so gibt es $w_1, w_2 \in \mathbb{R}$ mit $f(w_1, w_2, 0, 0) = w'$. Man rechnet leicht nach, dass $f$ die Sphäre $S_3$ in sich selbst abbildet. Daher liegt mit $w'$ auch $w$ in $S_3$, d.h. $w_1^2 + w_2^2 = 1$. Nach der obigen Rechnung gilt dann für $\lambda = w_1 + iw_2$ die Gleichung $Q \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} Q^{-1} = \theta(w')$, also ist $\theta(w') \in QTQ^{-1}$. Somit ist für jedes $Q \in \mathrm{SU}(2, \mathbb{C})$ die zu $T$ konjugierte Untergruppe $QTQ^{-1}$ ein Meridian.
Sei nun $P \neq \pm E \in \mathrm{SU}(2, \mathbb{C})$ mit $P = \theta(y_1, y_2, y_3, y_4)$. Dann sind $(y_1, y_2, y_3, y_4)$ und $(1, 0, 0, 0)$ linear unabhängig und spannen daher einen zweidimensionalen Unterraum $V$ von $\mathbb{R}^4$ auf. $P$ ist im Meridian $\theta(V \cap S_3)$ enthalten. Jeder andere Meridian $\theta(V' \cap S_3)$, der $P$ enthält, erfüllt $(1, 0, 0, 0) \in V'$ und $(y_1, y_2, y_3, y_4) \in V'$, also folgt $V = V'$. Daher ist jedes $P \neq \pm E$ in genau einem Meridian enthalten.

Sei nun ein beliebiger Meridian $\theta(M)$ gegeben, und $P \neq \pm E \in \theta(M)$. Dann gibt es nach Lemma 6.3 ein $Q = \mathrm{SU}(2, \mathbb{C})$ mit $QPQ^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}$ für die Eigenwerte $\lambda, \overline{\lambda}$ von $P$. Also liegt $P$ im Meridian $Q^{-1}TQ$, woraus wegen der soeben gezeigten Eindeutigkeit bereits $\theta(M) = Q^{-1}TQ$ folgt. Somit ist jeder Meridian eine zu $T$ konjugierte Untergruppe. □

# 7 Lie Gruppen und Lie Algebren

Wir haben bereits einige interessante Matrixgruppen wie $\mathrm{GL}(n, K)$, $\mathrm{SL}(n, K)$, $\mathrm{PGL}(n, K)$, $\mathrm{SO}(n, K)$ und $\mathrm{Sp}(n, K)$ kennengelernt. Ist der Grundkörper $K = \mathbb{R}$ oder $\mathbb{C}$, so tragen diese Gruppen zusätzlich die Struktur einer reellen bzw. komplexen Mannigfaltigkeit, und die Gruppenverknüpfungen sind beliebig oft differenzierbar.
Solche Objekte bezeichnet man als Lie Gruppen. Wir können hier keine allgemeine Einführung in dieses Gebiet geben, aber wir können einige Phänomene der Lie-Theorie an den uns bekannten Beispielen untersuchen.
In LAAG II, Basiskurs, § 12, haben wir die Exponentialfunktion $e^A$ für reelle oder komplexe Matrizen durch die Reihe

$$e^A = E + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \dots$$

definiert. Es gilt $e^{A+B} = e^A e^B$, falls $AB = BA$ ist. Wir haben gezeigt, dass die Funktion $\mathbb{R} \to \mathrm{GL}(n, \mathbb{C}), t \mapsto e^{tA}$ differenzierbar ist und die Ableitung

$$\frac{d}{dt} e^{tA} = Ae^{tA}$$

besitzt. Dabei nennen wir eine Abbildung $\alpha : \mathbb{R} \to \mathrm{GL}(n, \mathbb{C})$ differenzierbar in $t$, falls der Differenzenquotient

$$\lim_{h \to 0} \frac{\alpha(t+h) - \alpha(t)}{h}$$

in $\mathbb{C}^{n \times n}$ existiert. Das ist gleichbedeutend damit, dass die Abbildung $\alpha : \mathbb{R} \to \mathrm{GL}(n, \mathbb{C})$ in jeder Koordinate differenzierbar ist.

**Definition 7.1** Es sei $K$ der Körper $\mathbb{R}$ oder $\mathbb{C}$ und $G$ eine Untergruppe von $\mathrm{GL}(n, K)$. Dann heißt ein Homomorphismus

$$\alpha : \mathbb{R} \to G,$$

der in allen $t \in \mathbb{R}$ differenzierbar ist, **Einparameteruntergruppe von** $G$.

Dies ist eine eingebürgerte, aber etwas irreführende Bezeichnung. Korrekter sollte das Bild von $\alpha$ **Einparameteruntergruppe** heißen.
**Beispiel:** Sei $K = \mathbb{R}$ oder $K = \mathbb{C}$ und $A \in K^{n \times n}$. Dann ist die Abbildung

$$\begin{array}{rcl} \alpha : \mathbb{R} & \to & \mathrm{GL}(n, K) \\ t & \mapsto & e^{tA} \end{array}$$

eine Einparameteruntergruppe von $\mathrm{GL}(n, K)$. Die Abbildung $\alpha$ ist nämlich differenzierbar in allen $t \in \mathbb{R}$ und wegen $\alpha(t + t') = e^{(t+t')A} = e^{tA} e^{t'A} = \alpha(t)\alpha(t')$ (da $tA$ und $t'A$ vertauschen) auch ein Gruppenhomomorphismus. Der folgende Satz besagt, dass diese Abbildungen die einzigen Einparameteruntergruppen von $\mathrm{GL}(n, K)$ sind:

**Satz 7.2** Es sei $K = \mathbb{R}$ oder $K = \mathbb{C}$ und $\alpha : \mathbb{R} \to \mathrm{GL}(n, K)$,

$$\alpha(t) = \begin{pmatrix} \alpha_{11}(t) & \dots & a_{1n}(t) \\ \vdots & & \vdots \\ a_{n1}(t) & \dots & a_{nn}(t) \end{pmatrix},$$

eine Einparameteruntergruppe. Dann gilt für

$$A = \frac{d}{dt}\alpha(0) = \begin{pmatrix} \frac{d}{dt}\alpha_{11}(0) & \dots & \frac{d}{dt}\alpha_{1n}(0) \\ \vdots & & \vdots \\ \frac{d}{dt}\alpha_{n1}(0) & \dots & \frac{d}{dt}\alpha_{nn}(0) \end{pmatrix} \in K^{n \times n},$$

dass $\alpha(t) = e^{tA}$ ist.

**Beweis :** Die Einparameteruntergruppe $\alpha$ ist definitionsgemäß ein differenzierbarer Gruppenhomomorphismus. Also gilt für alle $t \in \mathbb{R}$ die Gleichung $\alpha(t) = \alpha(t+0) = \alpha(t)\alpha(0)$ und $\alpha(t+h) = \alpha(t)\alpha(h)$. Somit ist

$$\frac{\alpha(t+h)-\alpha(t)}{h} = \frac{\alpha(t)\alpha(h)-\alpha(t)\alpha(0)}{h} = \frac{\alpha(h)-\alpha(0)}{h}\alpha(t) \overset{h\to 0}{\longrightarrow} \frac{d}{dt}\alpha(0)\alpha(t) = A\alpha(t).$$

Somit erfüllt $\alpha$ die Differentialgleichung $\frac{d}{dt}\alpha(t) = A\alpha(t)$ und die Anfangsbedingung $\alpha(0) = E_n$. Nach LAAG II, Basiskurs, 12.11, folgt daraus $\alpha(t) = e^{tA}$. □

Die Einparameteruntergruppen in $\mathrm{GL}(n,K)$ entsprechen also bijektiv den $n \times n$-Matrizen über $K$. Sei jetzt eine Untergruppe $G$ von $\mathrm{GL}(n,K)$ gegeben. Jede Einparametergruppe von $G$ ist auch eine Einparameteruntergruppe von $\mathrm{GL}(n,K)$, also von der Form $e^{tA}$ für ein $A \in K^{n\times n}$. Es stellt sich also die Frage, welche Matrizen $A$ die Einparametergruppen von $G$ liefern.

**Beispiele:**

i) $G = U(1,\mathbb{C}) = \{\alpha \in \mathbb{C} : |\alpha| = 1\} \subset \mathbb{C}^\times = \mathrm{GL}(1,\mathbb{C})$. Dann ist $\alpha : t \mapsto e^{it} = \cos t + i \sin t$ eine surjektive Einparameteruntergruppe von $G$.

ii) $G = \mathrm{SO}(2,\mathbb{R})$. Für $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SO}(2,\mathbb{R})$ ist $\alpha : t \mapsto e^{tA} = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$ eine surjektive Einparametergruppe von $G$.

iii) $G = \mathrm{SU}(2,\mathbb{C})$. Dann ist

$$\alpha(t) = e^{t\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)} = \begin{pmatrix} e^{it} & 0 \\ 0 & e^{-it} \end{pmatrix}$$

eine Einparameteruntergruppe von $G$. Ihr Bild ist die Gruppe

$$T = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix} : |\lambda| = 1 \right\}.$$

Für jedes $P \in \mathrm{SU}(2,\mathbb{C})$ ist dann $t \mapsto P\alpha(t)P^{-1}$ ebenfalls eine Einparameteruntergruppe mit Bild $PTP^{-1}$. Die zu $T$ konjugierten Untergruppen entsprechen nach Satz 7.2 den Meridianen in $\mathrm{SU}(2,\mathbb{C})$. Alle Meridiane in $\mathrm{SU}(2,\mathbb{C})$ sind also Bilder von Einparameteruntergruppen. Da jedes $B \neq \pm E$ aus $\mathrm{SU}(2,\mathbb{C})$ in genau einem Meridian liegt, gibt es keine weiteren Bilder von Einparameteruntergruppen.

Wir nennen eine Teilmenge $V \subset \mathbb{R}^m$ **offen**, wenn für jedes $x \in V$ auch ein offener Ball um $x$ der Form $\{y \in \mathbb{R}^m : ||x-y|| < \varepsilon\}$ für ein $\varepsilon > 0$ in $V$ liegt.
Ist $M \subset \mathbb{R}^m$ eine beliebige Teilmenge und $V \subset M$, so heißt $V$ **offen in *M*** („bezüglich der Relativtopologie"), wenn für jedes $x \in V$ auch eine Menge der Form

$$\{y \in \mathbb{R}^m : ||x-y|| < \varepsilon\} \cap M$$

für ein $\varepsilon > 0$ in $V$ liegt. Auf diese Weise können wir für jede Untergruppe $G \subset \mathrm{GL}(n,\mathbb{R}) \subset \mathbb{R}^{n\times n}$ offene Teilmengen definieren.

**Satz 7.3** Es gibt eine offene Teilmenge $U \in \mathbb{R}^{n\times n}$ mit $0 \in U$ und eine offene Teilmenge $V \subset \mathrm{GL}(n,\mathbb{R})$ mit $E_n \in V$, so dass die Abbildung $A \mapsto e^A$ einen Homöomorphismus exp: $U \mapsto V$ induziert (Das heißt folgendes: $A \mapsto e^A$ ist stetig auf $U$, bildet $U$ bijektiv auf $V$ ab, und die Umkehrabbildung $V \to U$ ist ebenfalls stetig.)

**Beweis :** Dazu benötigen wir folgenden Satz über inverse Funktionen aus der Analysis: Sei $W \subset \mathbb{R}^m$ offen und $f : W \to \mathbb{R}^m$ stetig differenzierbar. Ist dann $a \in W$ ein Punkt, so dass die Jacobi-Determinante

$$\det \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{pmatrix}(a) \neq 0$$

ist, so existiert eine offene Umgebung $U \subset W$ von $a$, auf der $f$ eine stetig differenzierbare Umkehrfunktion hat.
Insbesondere gibt es also eine offene Umgebung $V \subset \mathbb{R}^m$ von $f(a)$, so dass $f : U \to V$ ein Homöomorphismus ist. Wir wenden diesen Satz auf die Abbildung

$$\begin{array}{rcl} \mathbb{R}^{n^2} & \to & \mathrm{GL}(n,\mathbb{R})) \subset \mathbb{R}^{n^2} \\ A & \mapsto & e^A \end{array}$$

und den Nullpunkt an. Die Jacobi-Matrix ist die $(n^2 \times n^2)$-Matrix mit dem Eintrag $\left(\frac{\partial (e^X)\alpha\beta}{\partial X_{ij}}\right)$ an der Stelle $((\alpha,\beta),(i,j))$. (Wir müssen die Funktionen und Variablen hier mit Doppelindizes aus $\{1,\ldots,n\} \times \{1,\ldots,n\}$ aufzählen). Nun gilt

$$\frac{\partial e^X}{\partial X_{ij}}|_{X=0} = \frac{d}{dt} e^{tE_{ij}}|_{t=0} = E_{ij},$$

wobei die Matrix $E_{ij}$ diejenige $n \times n$-Matrix bezeichnet, deren Eintrag in der $i$-ten Zeile und $j$-ten Spalte eine 1 ist und die sonst nur Nullen enthält. Also ist $\frac{\partial (e^X)\alpha\beta}{\partial X_{ij}} = 0$, falls $(\alpha,\beta) \neq (i,j)$ und $\frac{\partial (e^X)\alpha\beta}{\partial X_{ij}} = 1$, falls $(\alpha,\beta) = (i,j)$ gilt.
Daher ist die Jacobi-Matrix im Nullpunkt die Einheitsmatrix $E_{n^2}$, und wir können den obigen Satz über inverse Funktionen anwenden. □

**Lemma 7.4** Ist $A \in \mathbb{R}$ schiefsymmetrisch, so ist $e^A$ orthogonal. Umgekehrt gibt es eine offene Umgebung $U$ von 0 in $\mathbb{R}^{n\times n}$, so dass jede Matrix $A \in U$, für die $e^A$ orthogonal ist, schiefsymmetrisch ist.

**Beweis :** Ist $A$ schiefsymmetrisch, gilt also $A^t = -A$, so folgt $e^{A^t} = e^{-A}$. Aus der Definition der Exponentialreihe ergibt sich aber $e^{A^t} = \sum \frac{(A^t)^k}{k!} = (e^A)^t$. Also gilt $(e^A)^t = e^{A^t} = e^{-A} = (e^A)^{-1}$, d.h. $e^A$ ist orthogonal. Nach Satz 7.3 gibt es eine offene Umgebung $U \subset \mathbb{R}^{n\times n}$ von 0 und eine offene Teilmenge $V \subset \mathrm{GL}(n,\mathbb{R})$, so dass $A \mapsto e^A$ einen Homöomorphismus $U \to V$ vermittelt. Nach Verkleinern von $U$ können wir annehmen, dass für jedes $A \in U$ auch $-A$ und $A^t$ in $U$ liegen. Ist nun $A \in U$ und $e^A$ orthogonal, so gilt $e^{A^t} = (e^A)^t = (e^A)^{-1} = e^{-A}$. Da die Exponentialfunktion auf $U$ bijektiv ist, folgt $A^t = -A$, d.h. $A$ ist schiefsymmetrisch. □

**Satz 7.5** Für $K = \mathbb{R}$ oder $\mathbb{C}$ und $A \in K^{n\times n}$ gilt $\det e^A = e^{\mathrm{Spur}A}$.

**Beweis :** Wir betrachten $A$ als komplexe Matrix. Dann ist $A$ trigonalisierbar, d.h. es existiert ein $P \in \mathrm{GL}(n,K)$, so dass $PAP^{-1} = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ eine obere Dreiecksmatrix ist. Auf der Diagonalen stehen die Eigenwerte $\lambda_1, \ldots, \lambda_n$ von $A$ (mit algebraischen Vielfachheiten gezählt). Daher ist $\mathrm{Spur}A = \mathrm{Spur}PAP^{-1} = \lambda_1 + \cdots + \lambda_n$. Ferner ist $Pe^AP^{-1} = e^{PAP^{-1}} = e^{\left(\begin{smallmatrix} \lambda_1 & * \\ 0 & \lambda_n \end{smallmatrix}\right)} = \sum_{k=0}^{\infty} \frac{1}{k!} \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}^k$.

Nun ist

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}^k = \begin{pmatrix} \lambda_1^k & & * \\ & \ddots & \\ 0 & & \lambda_n^k \end{pmatrix},$$

wobei $*$ immer Einträge bezeichnet, die uns nicht interessieren.
Also folgt

$$Pe^AP^{-1} = \begin{pmatrix} e^{\lambda_1} & & * \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix},$$

und daher

$$\det e^A = \det(Pe^AP^{-1}) = e^{\lambda_1} \ldots e^{\lambda_n} = e^{\lambda_1+\cdots+\lambda_n} = e^{\mathrm{Spur}A}.$$

□

**Korollar 7.6** Die Einparameteruntergruppen der Gruppe $\mathrm{SL}(n,\mathbb{R})$ sind genau die Homomorphismen $t \mapsto e^{tA}$, wobei $A \in \mathbb{R}^{n\times n}$ eine Matrix mit $\mathrm{Spur}(A) = 0$ ist.

**Beweis :** Ist Spur $A = 0$, so ist auch Spur $tA = 0$, also gilt nach Satz 7.5 $e^{tA} \in \mathrm{SL}(n,\mathbb{R})$. Daher ist $t \mapsto e^{tA}$ eine Einparameteruntergruppe von $\mathrm{SL}(n,\mathbb{R})$. Ist $t \mapsto e^{tA}$ mit $A \in \mathbb{R}^{n\times n}$ eine beliebige Einparameteruntergruppe von $\mathrm{SL}(n,\mathbb{R})$, so ist $1 = \det e^A = e^{\mathrm{Spur}A}$ nach Satz 7.5. Da Spur $A \in \mathbb{R}$ ist, folgt Spur$A = 0$. □

Wir nehmen ab jetzt $K = \mathbb{R}$ an. (Über $\mathbb{C}$ gelten jeweils ähnliche Resultate.)

**Definition 7.7** Es seien $r$ Polynome $f_1, \ldots, f_r \in K[x_1, \ldots, x_s]$ in $s$ Variablen gegeben. Dann nennen wir die Menge

$$M = \{(a_1, \ldots, a_s) \in \mathbb{R}^s : f_1(a_1, \ldots, a_s) = \cdots = f_r(a_1, \ldots, a_s) = 0\}$$

**reelle algebraische Menge.**
Eine reelle algebraische Menge ist also die Menge der gemeinsamen reellen Nullstellen endlich vieler Polynome.

**Beispiele:**

i) Da die Determinante ein Polynom in den Matrixeinträgen ist, ist $\mathrm{SL}(n,\mathbb{R}) = \{(a_{ij})_{i,j} \in \mathbb{R}^{n\times n} : \det(a_{ij}) - 1 = 0\}$ eine reelle algebraische Menge, die durch ein einziges Polynom gegeben ist.

ii) $O(n,\mathbb{R}) = \{(a_{ij})_{i,j} \in \mathbb{R}^{n\times n} : \sum_k a_{ik}a_{jk} - \delta_{ij} = 0$ für alle $i,j \in \{1,\ldots,n\}\}$ ist ebenfalls eine algebraische Gruppe. Die oben angegebenen Polynome drücken die Gleichung $AA^t = E_n$ aus.

iii) Auch $\mathrm{GL}(n,\mathbb{R})$ ist eine reelle algebraische Menge, wenn auch die Polynomgleichungen den Trick einer zusätzlichen Variablen benötigen:

$$\mathrm{GL}(n,\mathbb{R}) = \{(a_{11}, a_{12}, \ldots, a_{nn}, b) \in \mathbb{R}^{n^2+1} : \det(a_{ij})_{i,j} b = 1\}.$$

**Definition 7.8** Ist $M \subset \mathbb{R}^s$ eine beliebige Teilmenge, so heißt ein Vektor $v \in \mathbb{R}^s$ **tangential zu $M$ im Punkt** $x \in M$, wenn es eine differenzierbare Abbildung (auch Weg genannt)

$$\varphi : \mathbb{R} \to \mathbb{R}^s$$

mit $\varphi(\mathbb{R}) \subset M$ gibt, so dass $\varphi(0) = x$ und $\frac{\partial\varphi}{\partial t}(0) = v$ ist. Die Menge $T_xM$ der Tangentialvektoren in $x \in M$ heißt **Tangentialraum** von $M$ in $x$.

**Lemma 7.9** Sei $M = \{x = (x_1, \ldots, x_s) \in \mathbb{R}^s : f_1(x) = \cdots = f_r(x) = 0\}$ eine reelle algebraische Menge. Dann stehen alle Tangentialvektoren von $M$ in $x \in M$ senkrecht auf allen Gradienten

$$Df_j(x) = \left\{ \frac{\partial f_j}{\partial x_1}(x), \ldots, \frac{\partial f_j}{\partial x_s}(x) \right\}$$

für $j = 1, \ldots, r$.

**Beweis :** Sei $v$ ein Tangentialvektor zu $M$ in $x$ und $\varphi : \mathbb{R} \to \mathbb{R}^s$ der zugehörige differenzierbare Weg. Da $\varphi(\mathbb{R}) \subset M$ ist, gilt $f_1(\varphi(t)) = \cdots = f_s(\varphi(t)) = 0$ für alle $t \in \mathbb{R}$. Also folgt für alle $j = 1, \ldots, r$

$$0 = \frac{\partial f_j(\varphi(t))}{\partial t} = \left( \frac{\partial f_j}{\partial x_1}(\varphi(t)), \ldots, \frac{\partial f_j}{\partial x_s}(\varphi(t)) \right) \begin{pmatrix} \frac{\partial \varphi_1}{\partial t}(t) \\ \vdots \\ \frac{\partial \varphi_s}{\partial t}(t) \end{pmatrix}$$

Für $t = 0$ folgt die Behauptung, da $\varphi(0) = x$ und $\frac{\partial \varphi}{\partial t}(0) = v$ ist. □

**Beispiel:** Der Einheitskreis $M = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 + x_2^2 = 1\}$ ist eine reelle algebraische Menge. Jeder Tangentialvektor $v$ im Punkt $(1, 0) \in M$ steht nach Lemma 7.9 senkrecht auf $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Wir haben Tangentialvektoren mit differenzierbaren Wegen berechnet. Es gibt viele Wege mit demselben zugehörigen Tangentialvektor, d.h. mit derselben Ableitung. Daher können wir von einem Weg alle Terme $\geq$ zweiter Ordnung in der Taylorentwicklung ignorieren. Um das genau zu formulieren, definieren wir

**Definition 7.10** Sei $D = \{a + b\varepsilon : a, b \in \mathbb{R}\}$ der zweidimensionale reelle Vektorraum mit Basis $1, \varepsilon$. Wir definieren eine Multiplikation auf $D$ durch

$$(a + b\varepsilon)(c + d\varepsilon) = ac + (bc + ad)\varepsilon.$$

In $D$ gilt also $\varepsilon^2 = 0$ und $a\varepsilon = \varepsilon a$. $D$ ist ein Ring (aber kein Körper).
Für $x \in \mathbb{R}^s$ und $v \in \mathbb{R}^s$ ist $x + v\varepsilon$ ein $s$-dimensionaler Vektor mit Einträgen in $D$. Wir können ein Polynom $f(x_1, \ldots, x_s)$ auch in $x + v\varepsilon$ auswerten, wenn wir die Taylorentwicklung benutzen. Wir definieren einfach

$$\begin{aligned} f(x + v\varepsilon) &= f(x) + \left( \frac{\partial f}{\partial x_1}(x)v_1 + \cdots + \frac{\partial f}{\partial x_s}(x)v_s \right) \varepsilon \\ &= f(x) + \langle Df(x), v \rangle \varepsilon, \end{aligned}$$

wobei $\langle , \rangle$ das kanonische Skalarprodukt bezeichnet. Dieser Ausdruck ergibt sich, wenn wir $x + v\varepsilon$ formal in die Taylorentwicklung von $f$ um $x$ einsetzen und $\varepsilon^2 = 0$ benutzen.

**Definition 7.11** Sei $M \subset \mathbb{R}^s$ eine reelle algebraische Menge, gegeben durch Polynome $f_1, \ldots, f_r$. Ein Vektor $v \in \mathbb{R}^s$ heißt **infinitesimal tangential** zu $M$ in $x$, wenn

$$f_1(x + v\varepsilon) = \cdots = f_s(x + v\varepsilon) = 0$$

gilt.

**Satz 7.12** Sei $x$ ein Punkt der reellen algebraischen Menge $M$. Dann ist jeder Tangentialvektor $v$ zu $M$ in $x$ auch infinitesimal tangential.

**Beweis :** Es sei $M = \{x \in \mathbb{R}^s : f_1(x) = \cdots = f_r(x) = c$. Ist $v$ ein Tangentialvektor zu $M$ in $x$, so gilt für alle $j$ nach Lemma 7.9 $\langle Df_j(x), v\rangle = 0$, also ist

$$\begin{aligned} f_j(x + v\varepsilon) &= f_j(x) + \langle Df_j(x), v\rangle\varepsilon \\ &= f_j(x) = 0. \end{aligned}$$

□

Wir müssen hier allerdings etwas aufpassen. Unsere Definition von infinitesimal tangential hängt nicht nur von $M$, sondern auch von der Wahl der Polynome $f_1, \ldots, f_r$ ab. Ist $M$ „genügend glatt“ und sind die Gleichungen $f_1, \ldots, f_r$ geeignet gewählt, so gilt auch die Umkehrung von Satz 7.12. In folgendem Beispiel gilt sie allerdings nicht.

**Beispiel:** sei $M = \{x = (x_1, x_2) \in \mathbb{R}^2 : x_1x_2 = 0\}$ die Vereinigung der beiden Koordinatenachsen. Für das definierende Polynom $f(x_1, x_2) = x_1x_2$ gilt $Df(x_1, x_2) = (x_2, x_1)$. Für $x = 0$ ist das der Nullvektor, also ist jedes $v \in \mathbb{R}^2$ infinitesimal tangential zu $M$ in 0, während nur Vektoren auf den Koordinatenachsen tangential zu $M$ in 0 sind.

Jetzt untersuchen wir wieder Matrixgruppen.

**Definition 7.13** Eine **reelle algebraische Gruppe** ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{R})$, die gleichzeitig eine reelle algebraische Menge ist.

Wir haben oben gesehen, dass $\mathrm{GL}(n, \mathbb{R})$, $\mathrm{SL}(n, \mathbb{R})$ und $O(n, \mathbb{R})$ reelle algebraische Gruppen sind. Jede algebraische Gruppe ist auch eine Lie Gruppe.

**Definition 7.14** Ist $G$ eine reelle algebraische Gruppe, so heißt der Tangentialraum von $G$ in $E$ (der Einheitsmatrix) **Lie Algebra** von $G$. Wir bezeichnen die Lie Algebra von $G$ als Lie $G$.

Jetzt wollen wir die Liealgebren von $\mathrm{SL}(n,\mathbb{R})$ und $O(n,\mathbb{R})$ bestimmen. Dazu brauchen wir folgendes Lemma:

**Lemma 7.15** Es sei $A = (a_{ij}) \in \mathbb{R}^{n\times n}$ und $E + A\varepsilon$ die Matrix mit den Einträgen $\partial_{ij} + a_{ij}\varepsilon \in D$. Dann gilt $\det(E + A\varepsilon) = 1 + (\mathrm{Spur}A)\varepsilon$.

**Beweis :** Nach der Leibnizformel ist

$$\begin{aligned} & \det(E + A\varepsilon) = \sum_{\sigma} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} (\delta_{i\sigma(i)} + a_{i\sigma(i)}\varepsilon) \\ \overset{\varepsilon^2=0}{=} & \sum_{\sigma} \mathrm{sgn}(\sigma) \left( \prod_{i=1}^{n} \delta_{i\sigma(i)} + \sum_{j=1}^{n} \prod_{i\neq j} (\delta_{i\sigma(i)} a_{j\sigma(j)}\varepsilon) \right) \\ = & \quad 1 + \left( \sum_{i=1}^{n} a_{ii} \right) \varepsilon = 1 + (\mathrm{Spur}A)\varepsilon. \end{aligned}$$

□

**Satz 7.16** Für $A \in \mathbb{R}^{n\times n}$ sind äquivalent

i) $\mathrm{Spur}A = 0$

ii) $t \mapsto e^{tA}$ ist eine Einparameteruntergruppe von $\mathrm{SL}(n,\mathbb{R})$

iii) $A \in$ Lie SL $(n,\mathbb{R})$

iv) $A$ ist infinitesimal tangential zu $\mathrm{SL}(n,\mathbb{R})$.

**Beweis :**

i) $\Rightarrow$ ii) gilt nach Korollar 7.6

ii) $\Rightarrow$iii) ist klar, da $\frac{d}{dt}(e^{tA})|_{t=0} = A$ ist

iii) $\Rightarrow$ iv) gilt nach Satz 7.12

iv) $\Rightarrow$ i) $\mathrm{SL}(n,\mathbb{R})$ ist die Nullstellenmenge von $\det X - 1 = 0$ in $\mathbb{R}^{n^2}$. Also ist $A \in \mathbb{R}^{n^2}$ genau dann infinitesimal tangential zu $\mathrm{SL}(n,\mathbb{R})$ in $E$, wenn $\det(E + A\varepsilon) = 1$ ist. Mit Lemma 7.15 folgt daraus $\mathrm{Spur}A = 0$.

□

Die Lie Algebra von $\mathrm{SL}(n,\mathbb{R})$ lässt sich also identifizieren mit der Menge der Einparameteruntergruppen von $\mathrm{SL}(n,\mathbb{R})$ und mit der Menge der infinitesimal tangentialen Vektoren. Ein analoges Resultat gilt für die orthogonale Gruppe.

**Satz 7.17** Für $A \in \mathbb{R}^{n\times n}$ sind äquivalent:

i) $A$ ist schiefsymmetrisch

ii) $t \mapsto e^{tA}$ ist eine Einparameteruntergruppe von $O(n,\mathbb{R})$

iii) $A \in$ Lie $O(n,\mathbb{R})$

iv) $A$ ist infinitesimal tangential zu $O(n,\mathbb{R})$ in $E$.

**Beweis :**

i) $\Rightarrow$ ii) folgt aus Lemma 7.4

ii) $\Rightarrow$ iii) ist klar

iii) $\Rightarrow$ iv) gilt nach Satz 7.12

iv) $\Rightarrow$ i) $O(n,\mathbb{R})$ ist die Nullstellenmenge der Polynome, die $PP^t = E$ ausdrücken. Ist $A \in \mathbb{R}^{n\times n}$ infinitesimal tangential zu $O(n,\mathbb{R})$ in $E$, so folgt also

$$(E + A\varepsilon)(E + A\varepsilon)^t = E$$

und somit $E + A^t\varepsilon + A\varepsilon = E$. Also gilt $A^t + A = 0$, d.h. $A$ ist schiefsymmetrisch. □

Ist $G$ eine reelle algebraische Gruppe, so trägt der $\mathbb{R}$-Vektorraum Lie$G$ eine zusätzliche Verknüpfung, die Lieklammer

$$[\ ,\ ] : \text{Lie } G \times \text{ Lie } G \to \text{ Lie } G.$$

Für $G = \mathrm{SL}(n,\mathbb{R})$ und $G = O(n,\mathbb{R})$ ist diese definiert als

$$[A,B] = AB - BA.$$

Gilt Spur$A = 0$ und Spur$B = 0$ (bzw. $A$ schiefsymmetrisch und $B$ schiefsymmetrisch), so ist auch Spur$(AB - BA) = 0$ (bzw. $AB - BA$ schiefsymmetrisch). Im ersten Fall folgt dies aus Spur$AB =$ Spur$BA$, im zweiten aus

$$(AB - BA)^t = B^tA^t - A^tB^t = (-B)(-A) - (-A)(-B) = -(AB - BA).$$

Also sind Lie SL$(n, \mathbb{R})$ und Lie $O(n, \mathbb{R})$ abgeschlossen unter der Lieklammer. Die Lieklammer $[A, B] = AB - BA$ ist offenbar bilinear und erfüllt $[A, A] = 0$. Ferner gilt die sogenannte Jacobi-Identität

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0,$$

wie man leicht nachrechnet. Das motiviert folgende Definition:

**Definition 7.18** Eine **Liealgebra** $V$ über einem Körper $K$ ist ein $K$-Vektorraum zusammen mit einer Verknüpfung

$$\begin{array}{rcl} V \times V & \to & V \\ (v, w) & \mapsto & [v, w], \end{array}$$

so dass gilt

i) $[\ ,\ ]$ ist bilinear

ii) $[v, v] = 0$ für alle $v \in V$ (d.h. $[\ ,\ ]$ ist schiefsymmetrisch)

iii) es gilt die Jacobi-Identität

$$[u, [v, w]] + [v, [w, u]] + [w, [u, v]]$$

für alle $u, v, w \in V$.

Liealgebren sind deshalb so wichtig, weil sie einen Großteil der Struktur von Liegruppen und reellen algebraischen Gruppen bestimmen, andererseits aber von ihrer Struktur her einfachere Objekte sind.