



seit 1558

Friedrich-Schiller-Universität Jena
Mathematisches Institut

Algebra und Geometrie
Sommersemester 2008

David J. Green
Stand: 4. Februar 2009

Zeichnungen: Ivo Hedtke

Inhaltsverzeichnis

1	Ein einführendes Beispiel	1
2	Untergruppen und Homomorphismen	2
2.1	Untergruppen	2
2.2	Homomorphismen	3
2.3	Permutationen	4
2.4	Die Signatur	6
3	Nebenklassen und Quotientengruppen	8
3.1	Nebenklassen: der Satz von Lagrange	8
3.2	Die Ordnung eines Gruppenelements	10
3.3	Normalteiler	10
3.4	Kern und Bild	11
3.5	Die Quotientengruppe	12
3.6	Die Symmetriegruppe eines regulären n -Ecks	13
4	Operationen und die Isomorphiesätze	16
4.1	Der Homomorphiesatz	16
4.2	Folgerungen des Homomorphiesatzes: die Isomorphiesätze	16
4.3	Gruppenoperationen	18
5	Die regulären Polyeder	22
5.1	Ein Symmetriebegriff	22
5.2	Die Isometriegruppe des Tetraeders	25
5.3	Die Isometriegruppe des Würfels	27
5.4	Das Ikosaeder	29
6	Endliche Gruppen von orthogonalen Transformationen	33
6.1	Rotationen	33
6.2	Vorüberlegungen anhand eines Beispiels	34
6.3	Die Klassifikation	36
7	Konjugation und einfache Gruppen	40
7.1	Konjugationsklassen	40
7.2	Das Zentrum und ein Satz von Cauchy	41
7.3	Die Gruppe A_5 ist einfach	43
8	Möbiustransformationen	45
8.1	Die Riemannsche Zahlenkugel	45
8.2	Die Riemannsche Zahlenkugel als ein projektiver Raum	46
8.3	Möbiustransformationen und Projektivitäten	46
8.4	Möbiustransformationen als eine Quotientengruppe	47

8.5	Drei Punkte	48
8.6	Möbiustransformationen und Kreise	49
9	Hyperbolische Geometrie	52
9.1	Konforme Abbildungen	52
9.2	Die hyperbolische Ebene: Das Halbebene-Modell	54
9.3	Das Scheiben-Modell	56
9.4	Das Doppelverhältnis	57

1 Ein einführendes Beispiel

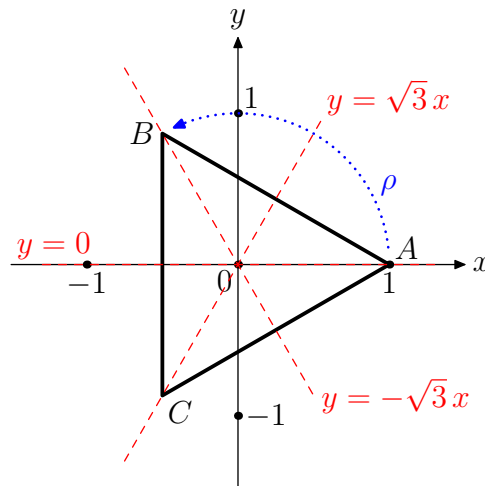
Definition Eine Gruppe G besteht aus einer Menge G und einer Abbildung $\mu: G \times G \rightarrow G, (g, h) \mapsto gh$, die folgende Axiome erfüllt:

- (G1) Assoziativität: $(gh)k = g(hk)$ für alle $g, h, k \in G$;
- (G2) Neutrales Element: Es gibt ein $e \in G$ mit: $\forall g \in G \quad eg = ge = g$;
- (G3) Existenz von Inversen: Zu jedem $g \in G$ gibt es ein $g' \in G$ mit $gg' = g'g = e$.

Gilt $gh = hg$ für alle $g, h \in G$, so heißt G *abelsch*.

Bezeichnung Meistens schreibt man x^{-1} statt x' ; manchmal schreibt man 1 statt e . Bei manchen abelschen Gruppen schreibt man $g + h$ statt gh ; dementsprechend schreibt man dann 0 für e , und $-g$ für g' . Eine solche Gruppe nennt man eine *additive* Gruppe.

Die Diedergruppe D_3 : die Symmetriegruppe des regulären Dreiecks.



Hilfssatz (Gruppentafel-Sudoku) Sei G eine Gruppe und $x \in G$. Dann sind die Abbildungen $L_x: G \rightarrow G, L_x: g \mapsto xg$ und $R_x: G \rightarrow G, R_x: g \mapsto gx$ Bijektionen. Für die Gruppentafel bedeutet dies: jedes Element kommt genau einmal in jeder Spalte und genau einmal in jeder Zeile vor.

Hilfssatz Sei G eine Gruppe.

- a) Sind $g, h \in G$ mit $gh = g$ oder mit $hg = g$, so ist $h = e$.
- b) Sind $g, h \in G$ mit $gh = e$, so ist $g = h^{-1}$ und $h = g^{-1}$.
- c) Das neutrale Element e ist eindeutig, ferner sind Inverse eindeutig.

2 Untergruppen und Homomorphismen

2.1 Untergruppen

Definition Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge. Man nennt H eine *Untergruppe* von G falls:

1. Definition: H selbst eine Gruppe ist, und zwar bezüglich der gleichen Multiplikation wie G ;
2. Definition: Für alle $h, k \in H$ ist auch $hk \in H$, und H ist selbst eine Gruppe;
3. Definition: Es ist $e \in H$; ferner ist $h^{-1}, hk \in H$ für alle $h, k \in H$.

Bezeichnung: $H \leq G$.

Beispiele $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$; $\{\text{Id}, \rho, \rho^2\} \leq D_3$; $S^1 \leq \mathbb{C}^*$; $\mathbb{C}^* \not\leq \mathbb{C}$.

Bemerkung Untergruppen sind nicht leer; $\{e\}$ und G selbst sind immer Untergruppen; ist $K \leq H$ und $H \leq G$, dann $K \leq G$; sind umgekehrt $H, K \leq G$ und $K \subseteq H$, dann $K \leq H$.

Lemma 2.1 Sei $(H_i)_{i \in I}$ eine Familie von Untergruppen von G ; dann ist auch die Schnittmenge $H := \bigcap_{i \in I} H_i$ eine Untergruppe von G .

Definition Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Nach Lemma 2.1 ist

$$\langle X \rangle := \bigcap \{H \leq G \mid X \subseteq H\}$$

eine Untergruppe von G , die man die von X erzeugte Untergruppe nennt. Dann ist $X \subseteq \langle X \rangle$ und $\langle X \rangle \leq H$ für jedes $H \leq G$ mit $X \subseteq H$, also ist $\langle X \rangle$ die kleinste Untergruppe von G , die X enthält.

Beispiel $\langle \rho \rangle = \{\text{Id}, \rho, \rho^2\}$; $\langle \sigma_A \rangle = \{\text{Id}, \sigma_A\}$.

Lemma 2.2 Sei G eine Gruppe und $X \subseteq G$. Dann ist $\langle X \rangle$ die Menge aller Wörter in den Elementen von X :

$$\langle X \rangle = \{x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} \mid r \geq 0, x_i \in X, n_i \in \mathbb{Z}\}.$$

Beweis. Das Wort mit $r = 0$ ist das neutrale Element. Einerseits ist die rechte Seite in jeder Untergruppe enthalten, die X enthält; andererseits ist die rechte Seite eine Untergruppe, die X enthält. ■

Beispiel Für $n \geq 1$ sei C_n die Gruppe

$$C_n = \left\{ \exp\left(\frac{2\pi ir}{n}\right) \mid 0 \leq r \leq n-1 \right\} \leq S^1.$$

Diese ist eine abelsche multiplikative Gruppe mit n Elementen. Für jedes r ist $\exp\left(\frac{2\pi ir}{n}\right) = x^r$ für $x := \exp\left(\frac{2\pi i}{n}\right)$, also ist $C_n = \{1, x, \dots, x^{n-1}\} = \langle x \rangle$. Also ist C_n zyklisch, im folgenden Sinne.

Definition Eine Gruppe G heißt *zyklisch*, falls es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Hilfssatz Zyklische Gruppen sind abelsch.

Beweis. Seien $x, y \in G = \langle g \rangle$. Nach Lemma 2.2 gibt es $n, m \in \mathbb{Z}$ mit $x = g^n$, $y = g^m$. Dann ist aber $xy = g^{n+m} = yx$. ■

Beispiel D_3 ist nicht zyklisch, da nicht abelsch; $\mathbb{Z} = \langle 1 \rangle$ ist zyklisch.

Bezeichnung Die Anzahl der Elemente einer Gruppe G wird mit $|G|$ bezeichnet, und heißt die *Ordnung* der Gruppe. Ist die Ordnung endlich, so heißt G eine endliche Gruppe.

Beispiel $|C_n| = n$; $|D_3| = 6 = |C_6|$, aber C_6 ist zyklisch, D_3 nicht.

Definition $G_1 \times G_2, \prod_{i \in I} G_i$

Beispiel Kleinsche Vierergruppe $C_2 \times C_2$: Ordnung 4, nicht zyklisch.

2.2 Homomorphismen

Definition Seien G, H Gruppen. Eine Abbildung $f: G \rightarrow H$ heißt ein (Gruppen) *Homomorphismus*, falls $f(g_1 g_2) = f(g_1) f(g_2)$ gilt für alle $g_1, g_2 \in G$.

Lemma 2.3 Ist $f: G \rightarrow H$ ein Homomorphismus, dann gelten $f(e_G) = e_H$ und $f(g^{-1}) = f(g)^{-1}$.

Beispiele a) $f: (\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \cdot), z \mapsto \exp(2\pi iz)$.

b) $f: D_3 \rightarrow C_2 = \{1, -1\}, \alpha \mapsto \det(\alpha)$.

c) $f: (\mathbb{Z}, +) \rightarrow (C_n, \cdot), r \mapsto \exp\left(\frac{2\pi ir}{n}\right)$.

d) Ist G eine beliebige Gruppe, so ist die Identitätsabbildung $\text{Id}: G \rightarrow G, g \mapsto g$ ein Homomorphismus. Sind $f: G \rightarrow H$ und $g: H \rightarrow K$ Homomorphismen, so ist auch $g \circ f: G \rightarrow K$ ein Homomorphismus.

e) Die Signatur einer Permutation $\varepsilon: S_n \rightarrow \{1, -1\}$. Mehr dazu unten.

Lemma 2.4 Ist $f: G \rightarrow H$ sowohl ein Homomorphismus als auch eine Bijektion, so ist auch $f^{-1}: H \rightarrow G$ ein Homomorphismus.

Bezeichnung Ein bijektiver Homomorphismus heißt ein *Isomorphismus*. Gibt es einen Isomorphismus $f: G \rightarrow H$, so heißen die Gruppen G, H *isomorph*. Isomorphie ist eine Äquivalenzrelation.

Beispiel Die Untergruppe $\langle \rho \rangle$ des D_3 ist isomorph zu C_3 , ein Isomorphismus ist $f(\rho^r) = \exp\left(\frac{2\pi ir}{3}\right)$.

2.3 Permutationen

Bereits in der LAAG1 lernten wir Permutationen erstmals kennen (Stichwort: Determinante).

Definition Sei X eine beliebige Menge. Eine Bijektion $\sigma: X \rightarrow X$ heißt eine *Permutation* von X . Die Menge aller Permutationen bildet eine Gruppe bezüglich Verknüpfung: die *symmetrische* Gruppe $S(X)$. Im wichtigen Fall $X = \{1, \dots, n\}$ schreibt man S_n für $S(X)$.

Einfache Bezeichnung Eine Schreibweise für eine Permutation $\sigma \in S_n$ ist

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}.$$

So ist etwa $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \in S_4$ die Permutation $\sigma: 1 \leftrightarrow 3, 2 \leftrightarrow 4$.

Eine bessere Schreibweise für eine Permutation ist als ein Produkt disjunkter Zykeln.

Definition Eine Permutation $\sigma \in S(X)$ heißt ein *r-Zykel*, wenn es paarweise verschiedene Elemente $x_1, \dots, x_r \in X$ gibt mit $\sigma(x_i) = x_{i+1}$ für $1 \leq i < r$, $\sigma(x_r) = x_1$, und $\sigma(x) = x$ für alle weiteren $x \in X$. In diesem Fall schreibt man $\sigma = (x_1 x_2 x_3 \dots x_r)$. Ein 2-Zykel heißt auch eine *Transposition*.

Zwei Zykeln $(x_1 x_2 x_3 \dots x_r)$ und $(y_1 y_2 \dots y_s)$ heißen *disjunkt*, falls kein x_i ein y_j ist.

Beispiele a) Die Permutation $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix} \in S_4$ ist ein 3-Zykel. Es ist

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix} = (1\ 2\ 4) = (2\ 4\ 1) = (4\ 1\ 2).$$

- b) Dagegen ist $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \in S_4$ kein Zykel, sondern das Produkt $(1\ 3)(2\ 4)$ von zwei disjunkten Transpositionen.
- c) $(1\ 2\ 3\ 4\ 5\ 6)^{-1} = (1\ 6\ 5\ 4\ 3\ 2)$.
- d) Jeder 1-Zykel ist das neutrale Element des S_n .

Bemerkung Disjunkte Zykeln kommutieren miteinander, z.B. $(1\ 3\ 5)(2\ 4) = (2\ 4)(1\ 3\ 5)$.

Satz 2.5 Jede Permutation $\sigma \in S_n$ lässt sich zerlegen als ein Produkt von disjunkten Zykeln. Lässt man 1-Zykel weg, so ist diese Zerlegung eindeutig, bis auf die (beliebige) Reihenfolge der Faktoren.

Bemerkung Für den Beweis ist es nützlich den Begriff *Träger*¹ einer Permutation einzuführen, gegeben durch $\text{supp}(\sigma) := \{x \mid \sigma(x) \neq x\}$. Dann für $r \geq 2$ ist $\{a_1, a_2, \dots, a_r\}$ der Träger des r -Zykels $(a_1\ a_2\ \dots\ a_r)$. Somit sind zwei Zykeln τ_1, τ_2 genau dann disjunkt, wenn die Schnittmenge $\text{supp}(\tau_1) \cap \text{supp}(\tau_2)$ leer ist. Dies bedeutet wiederum: ist $\sigma = \tau_1 \tau_2 \cdots \tau_\ell$ eine Zerlegung als Produkt von disjunkten Zykeln, so gilt $\text{supp}(\sigma) = \biguplus_{i=1}^{\ell} \text{supp}(\tau_i)$.

Beweis. Die Existenz zeigen wir per Induktion über die Größe vom Träger. Ist $\text{supp}(\sigma)$ leer, so ist $\sigma = \text{Id}$, ein Produkt von 0 Zykeln. Ist der Träger nicht leer, so wählen wir ein i mit $\sigma(i) \neq i$. Wir setzen $a_1 = i$ und $a_{j+1} = \sigma(a_j)$ für $j \geq 1$. Spätestens bei $r = n$ tritt die erste Wiederholung ein: a_{r+1} ist eins der bisherigen a_j . Da σ eine Bijektion ist, muss dann $a_{r+1} = a_1$ sein. Sei $\tau \in S_n$ der r -Zykel $\tau = (a_1\ a_2\ \dots\ a_r)$; da $\sigma(i) \neq i$ muss $r \geq 2$ sein. Setze $\sigma_1 := \tau^{-1}\sigma$. Dann $\sigma_1(a_j) = a_j$ für alle j ; und ist x kein a_j , dann $\sigma_1(x) = \sigma(x)$. Somit ist $\text{supp}(\sigma_1) = \text{supp}(\sigma) - \{a_1, \dots, a_r\}$. Nach der Induktionsannahme also ist σ_1 ein Produkt von disjunkten Zykeln; und aufgrund der Bemerkung oben kommt keins der a_j in diesen disjunkten Zykeln vor. Somit ist auch $\sigma = \tau\sigma_1$ ein Produkt disjunkter Zykeln.

Eindeutigkeit: Seien $\sigma = \tau_1 \cdots \tau_\ell = \rho_1 \cdots \rho_m$ zwei Zerlegungen von σ als ein Produkt von disjunkten Zykeln. Es reicht zu zeigen, dass jedes τ_i ein ρ_j ist. Sei $\tau_{i_0} = (a_1\ a_2\ \dots\ a_r)$. Da die τ_i disjunkt sind, folgt es, dass $\sigma(a_k) = a_{k+1}$, $\sigma(a_r) = a_1$. Nun, wegen $\sigma = \rho_1 \cdots \rho_m$ gibt es genau ein ρ_{j_0} mit $a_1 \in \text{supp}(\rho_{j_0})$. Da die ρ_j disjunkt sind und $\sigma(a_k) = a_{k+1}$, $\sigma(a_r) = a_1$ gelten, folgt auch $\rho_{j_0}(a_k) = a_{k+1}$, $\rho_{j_0}(a_r) = a_1$. Also $\tau_{i_0} = \rho_{j_0}$. ■

Beispiel Wir behandelten zwei zufällig gewählte Beispiele in der Vorlesung: einmal aus S_{13} , einmal aus S_{16} .

¹Auf Englisch: support

Bemerkung Nach der Eindeutigkeitsaussage in Satz 2.5 hat jede Permutation $\sigma \in S_n$ einen wohldefinierten Typ $2^{n_2} 3^{n_3} 4^{n_4} 5^{n_5} 6^{n_6} \dots$, wobei n_r die Anzahl von r -Zyklen in der Zerlegung von σ ist. Vorsicht: der Typ 4^1 von $(1\ 3\ 2\ 4)$ und der Typ 2^2 von $(1\ 4)(2\ 3)$ sind nicht gleich, d.h. der Typ ist nicht auszumultiplizieren.

Beispiel Der Typ von $(1\ 2)(3\ 4\ 5)(6\ 7)(8\ 9\ 10\ 11\ 12)$ ist $2^2 3^1 5^1$.

Bemerkung Bekanntlich ist $|S_n| = n!$.

Lemma 2.6 a) Jeder r -Zykel ist ein Produkt von $r - 1$ Transpositionen.

b) Jede Permutation $\sigma \in S_n$ ist ein Produkt von Transpositionen.

c) S_n wird durch die $n - 1$ Transpositionen $(1\ 2), (1\ 3), (1\ 4), \dots, (1\ n)$ erzeugt.

d) Die $n - 1$ Transpositionen $(1\ 2), (2\ 3), (3\ 4), \dots, (n - 1\ n)$ erzeugen auch S_n .

e) Die Transposition $(1\ 2)$ und der n -Zykel $(1\ 2\ \dots\ n)$ erzeugen S_n .

Beweis. a) Induktion über r , da $(a_1\ a_2\ \dots\ a_r) = (a_1\ a_r)(a_1\ a_2\ \dots\ a_{r-1})$.

b) Folgt aus dem ersten Teil und Satz 2.5.

c) Für $1 < a < b$ gilt $(a\ b) = (1\ a)(1\ b)(1\ a)$.

d) Für $2 \leq r \leq n - 1$ gilt $(1\ r + 1) = (r\ r + 1)(1\ r)(r\ r + 1)$.

e) Für $2 \leq r \leq n - 1$ gilt $(r\ r + 1) = (1\ 2\ \dots\ n)(r - 1\ r)(1\ 2\ \dots\ n)^{-1}$. ■

2.4 Die Signatur

Aus der LAAG1 wissen wir:

Definition Die *Signatur* $\varepsilon(\sigma)$ einer Permutation $\sigma \in S_n$ wird definiert durch

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \{1, -1\}.$$

Bemerkung 2.7 Nach Lemma 6.2 der LAAG1 ist bekannt:

$$\text{Für Permutationen } \sigma, \tau \in S_n \text{ gilt } \varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

Somit ist die Signatur ein Gruppenhomomorphismus $\varepsilon: S_n \rightarrow C_2$.

Aus Lemma 2.6 erhalten wir:

Lemma 2.8 a) Eine Transposition hat Signatur -1 .

b) Ist σ ein Produkt von N Transpositionen, so ist $\varepsilon(\sigma) = (-1)^N$. Ein r -Zykel hat Signatur $(-1)^{r-1}$.

Beweis. a) Aus der Definition sieht man, dass $\varepsilon(\tau) = -1$ gilt für die Transposition $\tau = (r \ r + 1)$. Der Beweis vom vierten Teil von Lemma 2.6 zeigt, dass $\varepsilon(\tau) = -1$ gilt für $\tau = (1 \ a)$. Somit zeigt der Beweis vom dritten Teil desselben Lemmas, dass $\varepsilon(\tau) = -1$ gilt für jede Transposition.

b) Der erste Teil folgt aus Bemerkung 2.7. Der zweite Teil folgt aus dem ersten Teil von Lemma 2.6. ■

Definition Sei σ eine Permutation. Ist $\varepsilon(\sigma) = 1$, so heißt σ *gerade*; ist $\varepsilon(\sigma) = -1$, so heißt σ *ungerade*.

Bemerkung Nach Lemma 2.6 ist jede Permutation σ ein Produkt von Transpositionen. Nach Lemm 2.8 gilt: ist σ ein Produkt von N Permutationen, so ist N gerade, falls σ gerade ist, und N ist ungerade, falls σ ungerade ist.

Beispiel S_4 besteht aus 24 Permutationen:

(1 2) und 5 weitere Transpositionen	ungerade
(1 2 3) und 7 weitere 3-Zykel	gerade
(1 2 3 4) und 5 weitere 4-Zykel	ungerade
(1 2)(3 4), (1 3)(2 4) und (1 4)(2 3) vom Typ 2^2	gerade
Die Identität	gerade

Beispiel Nach Bemerkung 2.7 ist das Produkt von zwei geraden Permutationen wieder gerade. Ferner ist das neutrale Element gerade, und mit σ ist auch σ^{-1} gerade, denn sonst wäre $\text{Id} = \sigma\sigma^{-1}$ ungerade, was nicht geht.

Also bilden die geraden Permutationen eine Untergruppe von S_n . Diese Untergruppe heißt die *alternierende Gruppe* A_n . Es ist $A_n = \{\sigma \in S_n \mid \sigma \text{ gerade}\}$.

Aus der Tabelle oben entnehmen wir, dass A_4 aus 12 Elementen besteht. Allgemein gilt $|A_n| = \frac{n!}{2} = \frac{1}{2} |S_n|$ für jedes $n \geq 2$, denn dann ist $\sigma \mapsto \sigma(1 \ 2)$ eine Bijektion zwischen den geraden und den ungeraden Permutationen: diese Abbildung ist ihre eigene Umkehrabbildung.

3 Nebenklassen und Quotientengruppen

3.1 Nebenklassen: der Satz von Lagrange

Beispiel Hier sind alle Untergruppen der Diedergruppe D_3 :

$$\begin{array}{lll} \langle \text{Id} \rangle & \langle \rho \rangle = \{ \text{Id}, \rho, \rho^2 \} & \langle \sigma_A \rangle = \{ \text{Id}, \sigma_A \} \\ \langle \sigma_B \rangle = \{ \text{Id}, \sigma_B \} & \langle \sigma_C \rangle = \{ \text{Id}, \sigma_C \} & \{ \text{Id}, \rho, \rho^2, \sigma_A, \sigma_B, \sigma_C \} \end{array}$$

Es gibt keine weiteren, im wesentlichen weil jede zyklische Gruppe $\langle g \rangle$ in dieser Liste auftaucht, und wir wissen, dass $\langle \rho, \sigma_A \rangle = \langle \sigma_A, \sigma_B \rangle = D_3$ ist.

Diese sechs Untergruppen haben Ordnungen 1, 3, 2, 2, 2 bzw. 6. Somit ist für jede Untergruppe $H \leq D_3$ die Gruppenordnung $|H|$ ein Teiler der Gruppenordnung $|D_3| = 6$. Nach dem Satz von Lagrange ist dies kein Zufall.

Der Satz von Lagrange (vorläufige Fassung) Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann ist $|G|$ durch $|H|$ teilbar.

Um diesen Satz zu beweisen, führen wir den Begriff Nebenklasse ein.

Definition Sei H eine Untergruppe von G .

a) Für $g \in G$ setzt man

$$gH := \{ gh \mid h \in H \} \subseteq G \qquad Hg := \{ hg \mid h \in H \} \subseteq G.$$

Man nennt gH eine *Linksnebenklasse* von H in G , und Hg eine *Rechtsnebenklasse*².

b) Mit G/H bzw. $H \backslash G$ bezeichnet man die Menge der Links- bzw. der Rechtsnebenklassen: $G/H = \{ gH \mid g \in G \}$.

c) Der Index $|G : H|$ von H in G definiert man als die Anzahl $|G/H|$ der Linksnebenklassen. Später sehen wir, dass auch $|G : H| = |H \backslash G|$ gilt.

Beispiel Die Untergruppe $H = \langle (1\ 2) \rangle = \{ \text{Id}, (1\ 2) \}$ hat drei Linksnebenklassen in S_3 :

$$\begin{array}{ll} \text{Id} H = (1\ 2)H = \{ \text{Id}, (1\ 2) \} & (1\ 3)H = (1\ 2\ 3)H = \{ (1\ 3), (1\ 2\ 3) \} \\ & (2\ 3)H = (1\ 3\ 2)H = \{ (2\ 3), (1\ 3\ 2) \}, \end{array}$$

weshalb $|S_3 : H| = 3$ ist. Außerdem gibt es drei Rechtsnebenklassen:

$$\begin{array}{ll} \text{Id} H = (1\ 2)H = \{ \text{Id}, (1\ 2) \} & H(1\ 3) = H(1\ 3\ 2) = \{ (1\ 3), (1\ 3\ 2) \} \\ & H(2\ 3) = H(1\ 2\ 3) = \{ (2\ 3), (1\ 2\ 3) \}. \end{array}$$

Insbesondere ist $(1\ 3)H \neq H(1\ 3)$, und mehr noch: die Rechtsnebenklasse $H(1\ 3)$ ist keine Linksnebenklasse.

²Diese Namensgebung ist vielleicht etwas willkürlich, doch aber Standard.

Bemerkung Ist G abelsch, so ist $gH = Hg$ für alle $H \leq G$ und alle $g \in G$: in einer abelschen Gruppe stimmen Links- und Rechtsnebenklassen miteinander überein.

Lemma 3.1 *Es sei $H \leq G$.*

a) *Die Relationen \sim_L und \sim_R auf G gegeben durch*

$$x \sim_L y \Leftrightarrow \exists h \in H \ y = xh \qquad x \sim_R y \Leftrightarrow \exists h \in H \ y = hx$$

sind Äquivalenzrelationen.

b) *Die Äquivalenzklassen von \sim_L sind die Linksnebenklassen von H in G . Somit liegt jedes $g \in G$ in genau einer Linksnebenklasse, und unterschiedliche Linksnebenklassen haben leeren Schnitt. Die gleiche Aussagen gelten für \sim_R und die Rechtsnebenklassen.*

c) *Alle Nebenklassen von H haben die gleiche Größe wie H .*

d) *Die Abbildung $G/H \rightarrow H \setminus G$, $gH \mapsto Hg^{-1}$ ist wohldefiniert und eine Bijektion. Somit gilt $|G : H| = |G/H| = |H \setminus G|$.*

Beweis. a) \sim_R reflexiv: $ex = x$; \sim_L symmetrisch: $y = xh \Leftrightarrow x = yh^{-1}$;
 \sim_R transitiv: ist $y = h_1x$ und $z = h_2y$, dann $z = (h_2h_1)x$.

b) Folgt aus dem ersten Teil und den Definitionen.

c) Die Abbildungen $H \rightarrow gH$, $h \mapsto gh$ und $H \rightarrow Hg$, $h \mapsto hg$ sind Bijektionen.

d) Wohldefiniert: wir müssen die Repräsentantenunabhängigkeit zeigen, d.h. ist $g_1H = g_2H$, dann $Hg_1^{-1} = Hg_2^{-1}$. Ist $g_1H = g_2H$, dann ist $g_2 = g_1h$ für ein $h \in H$, also $Hg_2^{-1} = Hh^{-1}g_1^{-1} = Hg_1^{-1}$. Bijektion: Die Umkehrabbildung ist $Hg \mapsto g^{-1}H$. ■

Der Satz von Lagrange *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann gilt $|G : H| \cdot |H| = |G|$. Insbesondere ist $|G|$ durch $|H|$ teilbar.*

Beweis. G ist eine disjunkte Vereinigung von Nebenklassen. Jede Nebenklasse enthält $|H|$ Elemente. Nach Definition ist der Index $|G : H|$ die Anzahl der Nebenklassen. ■

Beispiel Sei H eine Untergruppe des S_4 . Wegen $|S_4| = 24$ besagt Lagrange, dass $|H|$ ein Element der Liste 1, 2, 3, 4, 6, 8, 12, 24 ist. Man kann nachweisen, dass jede Ordnung vorkommt: so hat etwa $\langle (1\ 2\ 3\ 4), (1\ 4)(2\ 3) \rangle$ die Ordnung 8.

Beispiel Natürlich ist 120 durch 15 teilbar, trotzdem kann man zeigen, dass S_5 keine Untergruppe der Ordnung 15 hat.

3.2 Die Ordnung eines Gruppenelements

Definition Sei G eine Gruppe und $g \in G$. Die *Ordnung* $o(g)$ des Elements g ist per Definition die Ordnung der zyklischen Untergruppe $\langle g \rangle$:

$$o(g) = |\langle g \rangle| .$$

Beispiel Es ist $\langle (1\ 2\ 3) \rangle = \{\text{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Somit hat $(1\ 2\ 3)$ die Ordnung 3. Allgemeiner hat ein r -Zykel die Ordnung r .

Lemma 3.2 a) Ist $g \in G$ ein Element der Ordnung n , so ist $n \mid |G|$ und $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$.

b) Eine endliche Gruppe G der Ordnung n ist genau dann zyklisch, wenn es ein $g \in G$ gibt mit $o(g) = n$. In diesem Fall ist $G = \{e, g, g^2, \dots, g^{n-1}\}$.

c) Ist p eine Primzahl, so ist jede Gruppe der Ordnung p zyklisch.

Beweis. a) Wegen Lagrange ist $n \mid |G|$. Sei $r \geq 1$ die kleinste Zahl derart, dass die Liste e, g, g^2, \dots, g^r eine Wiederholung enthält: $g^r = g^s$ für ein $0 \leq s < r$. Multipliziert man mit g^{r-s} , so erhält man $e = g^{r-s}$ und deshalb $s = 0$: es ist $g^r = e$ die erste Wiederholung. Dann ist aber $g^{-1} = g^{r-1}$, weshalb $\{e, g, \dots, g^{r-1}\}$ eine Untergruppe von G ist, die kleinste Untergruppe, die g enthält. Also $r = n$ und $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$.

b) G ist zyklisch genau dann, wenn $G = \langle g \rangle$ gilt für ein $g \in G$. Jetzt benutzt man den ersten Teil sowie die Definition von $o(g)$.

c) Sei $|G| = p$ und $g \in G$ mit $g \neq e$. Nach dem ersten Teil ist $o(g) = 1$ oder p ; und $o(g) \neq 1$ wegen $g \neq e$. Also $o(g) = p$ und $G = \langle g \rangle$ nach dem zweiten Teil. ■

Beispiel So ist etwa jede Gruppe der Ordnung 7 zyklisch.

3.3 Normalteiler

In der LAAG2 definierten wir Restklassen modulo einen Untervektorraum U eines Vektorraums V . Dann definierten wir den Quotientenvektorraum V/U , und zwar so, dass die Abbildung $V \rightarrow V/U, v \mapsto v + U$ surjektiv und linear war.

Wir wollen das gleiche für Gruppen machen. Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Gerne möchten wir die Menge G/H der Links-Nebenklassen zu einer Gruppe machen, indem man ein Produkt von Nebenklassen durch $g_1H \cdot g_2H := g_1g_2H$ definiert. Diese Gruppe würde man dann die Quotientengruppe G/H nennen.

Beispiel Es geht aber nicht. Sei $H \leq S_3$ die Untergruppe $H = \langle (1\ 2) \rangle = \{\text{Id}, (1\ 2)\}$. Dann $(1\ 3)H \cdot (2\ 3)H = (1\ 3)(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\}$. Aber $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$, und $(1\ 2\ 3)H \cdot (2\ 3)H = (1\ 2\ 3)(2\ 3)H = (1\ 2)H = \{\text{Id}, (1\ 2)\}$. Das heißt, der Wert von $g_1H \cdot g_2H$ hängt davon ab, welchen Vertreter g_1 der Nebenklasse g_1H wir wählen. Zusammengefasst:

$$(1\ 3)H = (1\ 2\ 3)H \quad \text{aber} \quad (1\ 3)H \cdot (2\ 3)H \neq (1\ 2\ 3)H \cdot (2\ 3)H.$$

Das ist schlecht: die Multiplikation auf G/H ist nicht wohldefiniert.

Es stellt sich heraus, dass man nur dann die Quotientengruppe G/H bilden kann, wenn H nicht nur eine Untergruppe sondern ein Normalteiler von G ist.

Definition Sei G eine Gruppe. Eine Untergruppe $H \leq G$ heißt ein *Normalteiler* von G , Bezeichnung $H \triangleleft G$, falls die folgenden äquivalenten Aussagen gelten:

- a) Für jedes $g \in G$ ist $gH = Hg$.
- b) Für jedes $g \in G$ ist $gHg^{-1} = H$, wobei $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.
- c) Für jedes $g \in G$ ist $gHg^{-1} \subseteq H$.

Äquivalenznachweis a) \Leftrightarrow b): multipliziert man $gH = Hg$ von rechts mit g^{-1} , so erhält man $gHg^{-1} = H$. b) \Rightarrow c) ist klar. c) \Rightarrow b): Da $g^{-1} \in G$ ist, ist auch $g^{-1}H(g^{-1})^{-1} \subseteq H$ für alle g , d.h. $g^{-1}Hg \subseteq H$. Also $g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$, d.h. $(gg^{-1})H(gg^{-1}) \subseteq gHg^{-1}$, d.h. $H \subseteq gHg^{-1}$.

Beispiele Für $H = \langle (1\ 2) \rangle$ und $g = (1\ 3)$ ist $gH \neq Hg$. Deshalb ist H kein Normalteiler des S_3 . In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

Die Untergruppe $K = \langle (1\ 2\ 3) \rangle = \{\text{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$ ist ein Normalteiler $K \triangleleft S_3$, denn:

$$K = \{\text{Id}, (1\ 2\ 3), (1\ 3\ 2)\} \quad S_3 - K = \{(1\ 2), (1\ 3), (2\ 3)\};$$

also ist $gK = Kg = K$ für jedes $g \in K$ und $gK = Kg = S_3 - K$ für jedes $g \in S_3 - K$.

3.4 Kern und Bild

Definition Sei $f: G \rightarrow H$. Man setzt

$$\text{Bild}(f) = \{f(g) \mid g \in G\} \subseteq H \quad \text{Kern}(f) = \{g \in G \mid f(g) = e_H\}.$$

Lemma 3.3 *Es ist $\text{Bild}(f) \leq H$ und $\text{Kern}(f) \triangleleft G$. Die Abbildung f ist genau dann injektiv, wenn $\text{Kern}(f) = \{e_G\}$ gilt.*

Beweis. Da f ein Homomorphismus ist, ist $f(e_G) = e_H$, $f(g^{-1}) = f(g)^{-1}$ und $f(g_1)f(g_2) = f(g_1g_2)$. Also $\text{Bild}(f) \leq H$. Es ist $\text{Kern}(f) \leq G$, denn $f(e_G) = e_H$; ist $f(g) = e_H$, dann $f(g^{-1}) = f(g)^{-1} = e_H$; und aus $g_1, g_2 \in \text{Kern}(f)$ folgt $f(g_1g_2) = f(g_1)f(g_2) = e_H^2 = e_H$. Ferner ist $\text{Kern}(f) \triangleleft G$, denn ist $\gamma \in \text{Kern}(f)$ und $g \in G$, dann $f(g\gamma g^{-1}) = f(g)f(\gamma)f(g^{-1}) = f(g)e_Hf(g)^{-1} = e_H$.

Letzter Teil: ist $f(g) = f(g')$, dann $f(g^{-1}g') = e_H$, also $g^{-1}g' \in \text{Kern}(f) = \{e_G\}$, also $g = g'$. ■

Bemerkung In der linearen Algebra gehört zu einem Quotientenraum V/U auch eine surjektive lineare Abbildung $p: V \rightarrow V/U$, $v \mapsto v + U$, mit $\text{Kern } U$. In der Gruppentheorie sind Kerne immer Normalteiler. Somit erwarten wir, dass die Quotientengruppe G/H nur dann existieren kann, wenn H ein Normalteiler von G ist.

3.5 Die Quotientengruppe

Satz 3.4 *Sei $H \triangleleft G$ ein Normalteiler. Mit der Multiplikation $g_1H \cdot g_2H := g_1g_2H$ wird die Menge G/H der Links-Nebenklassen zu einer Gruppe, die Quotientengruppe G/H . Es ist $|G/H| = |G : H| = \frac{|G|}{|H|}$. Ferner ist die kanonische Projektion $p: G \rightarrow G/H$, $g \mapsto gH$ ein surjektiver Gruppenhomomorphismus mit Kern H .*

Beweis. Am wichtigsten ist der Nachweis, dass diese Multiplikation wohldefiniert d.h. repräsentantenunabhängig ist. Seien also $g_1, g'_1, g_2, g'_2 \in G$ mit $g_1H = g'_1H$ und $g_2 = g'_2H$. Zu zeigen ist $g'_1H \cdot g'_2H = g_1H \cdot g_2H$, d.h. $g'_1g'_2H = g_1g_2H$. Wegen $g_1H = g'_1H$ und $g_2 = g'_2H$ gibt es $h_1, h_2 \in H$ mit $g'_1 = g_1h_1$ und $g'_2 = g_2h_2$. Also $g'_1g'_2 = g_1h_1g_2h_2$. Wir wollen h_1, h_2 miteinander vertauschen. Es ist $h_1g_2 \in Hg_2$. Da $H \triangleleft G$ ist, ist $Hg_2 = g_2H$. Also gibt es ein $h' \in H$ mit $h_1g_2 = g_2h'$. Also $g'_1g'_2 = g_1g_2h'h_2$ und deshalb $g'_1g'_2H = g_1g_2H$. Die Multiplikation ist also wohldefiniert.

Die Gruppenaxiome folgen jetzt, da sie bereits in G gelten. Assoziativität:

$$\begin{aligned} g_1H(g_2Hg_3H) &= g_1Hg_2g_3H = g_1(g_2g_3)H \\ &= (g_1g_2)g_3H = g_1g_2Hg_3H = (g_1Hg_2H)g_3H. \end{aligned}$$

Neutrales Element eH : es ist $eHgH = egH = gH$, gleiches für $gHeH$. Inverses $(gH)^{-1} = g^{-1}H$: $gHg^{-1}H = gg^{-1}H = eH$, gleiches für $g^{-1}HgH$. Die Aussage zur Ordnung $|G/H|$ folgt aus dem Satz von Lagrange. Die Abbildung p ist offensichtlich surjektiv; ein Homomorphismus ist sie, da $p(g_1g_2) = g_1g_2H = g_1Hg_2H = p(g_1)p(g_2)$ ist; und der Kern ist H denn $p(g) = eH$ genau dann wenn $gH = eH$, d.h. $g \in H$ ist. ■

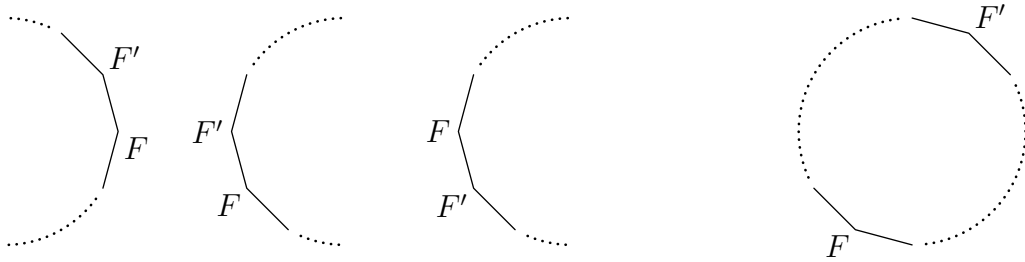
Beispiel $G = D_3 = \{\text{Id}, \rho, \rho^2, \sigma_A, \sigma_B, \sigma_C\}$. Sei $H = \langle \rho \rangle = \{\text{Id}, \rho, \rho^2\}$. Dann $H \triangleleft G$, denn H ist der Kern des Homomorphismus $G \rightarrow C_2 = \{1, -1\}$, $g \mapsto \det(g)$. Somit gibt es eine Quotientengruppe $D_3/\langle \rho \rangle$ mit $2 = \frac{6}{3}$ Elementen. Die Beiden Nebenklassen sind $\text{Id}H = \{\text{Id}, \rho, \rho^2\}$ und $\sigma_A H = \{\sigma_A, \sigma_B, \sigma_C\}$.

3.6 Die Symmetriegruppe eines regulären n -Ecks

Für $n \geq 3$ sei $X \subseteq \mathbb{R}^2$ das reguläre n -Eck mit Schwerpunkt in $(0, 0)$ und einer Ecke in $(1, 0)$. Somit liegen die Ecken in $(\cos \frac{2\pi r}{n}, \sin \frac{2\pi r}{n})$ für $0 \leq r \leq n-1$. Schreiben wir E_r für diese Ecke ($r \in \mathbb{Z}$), also ist $E_{-1} = E_{n-1}$. Wir wollen die Symmetriegruppe von X berechnen. Die Symmetriegruppe des regulären n -Ecks heißt die *Diedergruppe* D_n .

Sei ρ die Drehung durch $\frac{2\pi}{n}$ um den Mittelpunkt. Auf den Ecken operiert dies als der n -Zykel $(E_0 E_1 E_2 \dots E_{n-1})$. Sei σ die Spiegelung in der x -Achse: diese vertauscht jedes E_s mit E_{-s} .

Sei $\phi: X \rightarrow X$ eine Symmetrie. Dann gibt es genau ein $0 \leq r \leq n-1$ mit $\phi(E_0) = E_r$. Die zu E_0 benachbarten Ecken E_1, E_{-1} müssen auf den zu E_r benachbarten Ecken E_{r+1}, E_{r-1} abgebildet werden; steht umgekehrt fest, wohin E_{-1}, E_0, E_1 abgebildet werden, so ist ϕ eindeutig festgelegt.



Da ρ^r die Abbildung

$$E_{-1} \mapsto E_{r-1} \qquad E_0 \mapsto E_r \qquad E_1 \mapsto E_{r+1}$$

bewirkt und $\rho^r \sigma$ die Abbildung

$$E_{-1} \mapsto E_{r+1} \qquad E_0 \mapsto E_r \qquad E_1 \mapsto E_{r-1},$$

folgt: die Symmetriegruppe D_n des regulären n -Ecks ist die $2n$ -elementige Menge

$$D_n = \{\text{Id}, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma\}.$$

Von dieser Beschreibung liest man ab, dass $D_n = \langle \rho, \sigma \rangle$ ist. Es ist $\sigma^2 = \rho^n = \text{Id}$. Außerdem ist $\sigma\rho\sigma = \rho^{-1}$, da

$$\sigma\rho\sigma(E_{-1}) = E_{-2} \qquad \sigma\rho\sigma(E_0) = E_{-1} \qquad \sigma\rho\sigma(E_1) = E_0.$$

Aus den Relationen $\sigma^2 = \text{Id}$ und $\sigma\rho\sigma = \rho^{-1}$ erhalten wir

$$\begin{aligned} \rho^r \cdot \rho^s &= \rho^{r+s} & \rho^r \cdot \rho^s \sigma &= \rho^{r+s} \sigma & \rho^r \sigma \cdot \rho^s &= \rho^{r-s} \sigma \\ \rho^r \sigma \cdot \rho^s \sigma &= \rho^{r-s} & (\rho^r)^{-1} &= \rho^{-r} & (\rho^r \sigma)^{-1} &= \rho^r \sigma, \end{aligned}$$

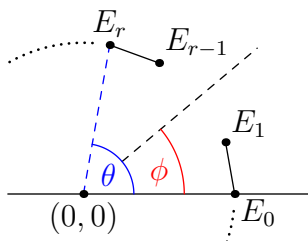
denn $\sigma = \sigma^{-1}$ und

$$ghg^{-1} \cdot gkg^{-1} = ghkg^{-1} \quad (ghg^{-1})^{-1} = gh^{-1}g^{-1} \quad (ghg^{-1})^r = gh^r g^{-1},$$

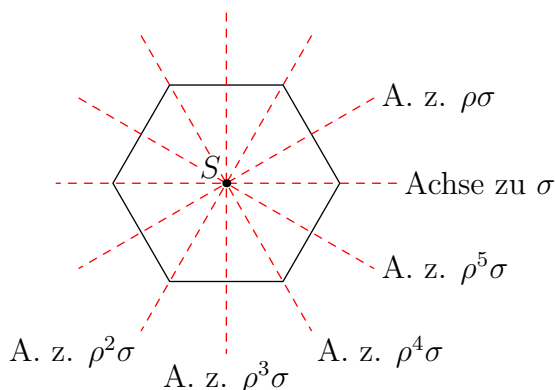
also $\sigma\rho^r\sigma = \rho^{-r}$ und $\sigma\rho^r = \rho^{-r}\sigma$. Somit folgt bereits aus den Relationen $\rho^n = \sigma^2 = \text{Id}$ und $\sigma\rho\sigma = \rho^{-1}$ und der Tatsache, dass D_n durch ρ, σ erzeugt wird, dass D_n höchstens die $2n$ Elemente $\rho^r, \rho^r\sigma$ besteht. Da D_n aber nachweislich $2n$ Elemente hat, folgert man, dass alle Relationen zwischen ρ und σ in D_n aus diesen drei Relationen $\rho^n = \sigma^2 = \text{Id}$ und $\sigma\rho\sigma = \rho^{-1}$ folgen. Man schreibt diese Tatsache so hin:

$$D_n = \langle \rho, \sigma \mid \rho^n = \sigma^2 = \text{Id}, \sigma\rho\sigma = \rho^{-1} \rangle.$$

Welche Symmetrie ist $\rho^r\sigma$?



Ein Strahl mit Winkel θ zur x -Achse wird durch σ auf $-\theta$ abgebildet, dann durch ρ^r auf $\frac{2\pi r}{n} - \theta$. Der Strahl mit Winkel $\frac{\pi r}{n}$ wird also auf sich selbst abgebildet, der Strahl mit Winkel $\frac{\pi r}{n} + \frac{\pi}{2}$ wird umgedreht. Also ist $\rho^r\sigma$ eine Spiegelung in der Gerade mit Winkel $\frac{\pi r}{n}$ zur x -Achse. Beispiel $n = 6$:



Is n ungerade, so liegt eine Ecke auf jeder Spiegelungsachse; ist n gerade, so liegt für r gerade zwei Ecken auf der Spiegelungsachse, für r ungerade liegen keine Ecken auf der Achse.

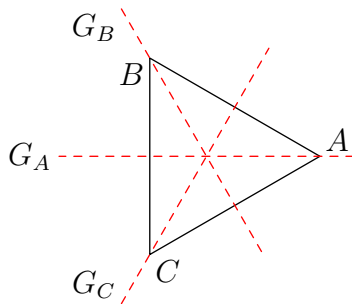
Die Untergruppe $\langle \rho \rangle$ ist ein Normalteiler, da $\sigma \rho^r \sigma^{-1} = \rho^{-r}$. Es gibt zwei Nebenklassen $\text{Id}\langle \rho \rangle$ und $\sigma \langle \rho \rangle$.

Bemerkung Die Formeln

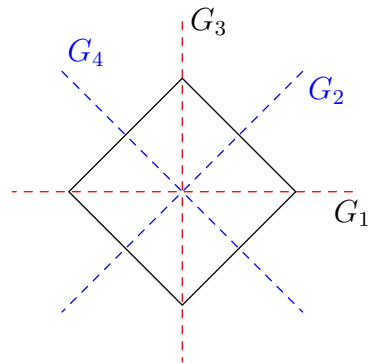
$$ghg^{-1} \cdot gkg^{-1} = ghkg^{-1} \quad (ghg^{-1})^{-1} = gh^{-1}g^{-1} \quad (ghg^{-1})^r = gh^r g^{-1}$$

sind allgemein nützlich.

Bemerkung D_3 permutiert die Symmetrieachsen des regulären Dreiecks transitiv, d.h. für zwei beliebige Achsen gibt es eine Symmetrie, die die erste Achse auf die zweite abbildet.



Dagegen ist die Operation von D_4 auf die Achsen des Quadrats nicht transitiv, da zwei Achsen keine Ecken enthalten, und zwei Achsen je zwei Ecken enthalten.



4 Operationen und die Isomorphiesätze

4.1 Der Homomorphiesatz

Dieser Satz ist der richtige Weg, Quotientengruppen zu verstehen.

Der Homomorphiesatz Ein Gruppenhomomorphismus $f: G \rightarrow H$ induziert einen Isomorphismus $\bar{f}: G/\text{Kern}(f) \rightarrow \text{Bild}(f)$. Insbesondere gilt: ist f surjektiv, so ist die Quotientengruppe $G/\text{Kern}(f)$ isomorph zu H .

Beweis. Setzen wir $K := \text{Kern}(f)$. Nach Lemma 3.3 ist $\text{Bild}(f) \leq H$ und $K \triangleleft G$. Nach Satz 3.4 existiert die Quotientengruppe G/K . Definieren wir $\bar{f}: G/K \mapsto \text{Bild}(f)$ durch $\bar{f}(gK) := f(g)$. Ist $gK = g'K$, so gibt es $k \in K$ mit $g' = gk$. Also $f(g') = f(g)f(k) = f(g)$, denn $K = \text{Kern}(f)$. Somit ist $\bar{f}(gK) = \bar{f}(g'K)$, d.h. \bar{f} ist wohldefiniert. Ferner ist \bar{f} ein Homomorphismus, denn

$$\bar{f}(gH \cdot g'H) = \bar{f}(gg'H) = f(gg') = f(g)f(g') = \bar{f}(gH)\bar{f}(g'H).$$

Für jedes $h = f(g)$ aus $\text{Bild}(f)$ ist $h = \bar{f}(gK)$, somit ist \bar{f} surjektiv. Ist $\bar{f}(gK) = e_H$, dann $f(g) = e_H$, also $g \in \text{Kern}(f)$ und $gK = eK$. Somit ist \bar{f} auch injektiv und somit ein Isomorphismus. ■

Beispiel Für $n \geq 2$ ist die Signatur $\varepsilon: S_n \rightarrow C_2 = \{1, -1\}$ ein surjektiver Homomorphismus mit Kern A_n , also ist $S_n/A_n \cong C_2$.

Für ein Körper k setzt man

$$\begin{aligned} GL_n(k) &:= \{A \in M_n(k) \mid A \text{ invertierbar}\} \\ SL_n(k) &:= \{A \in M_n(k) \mid \det(A) = 1\}. \end{aligned}$$

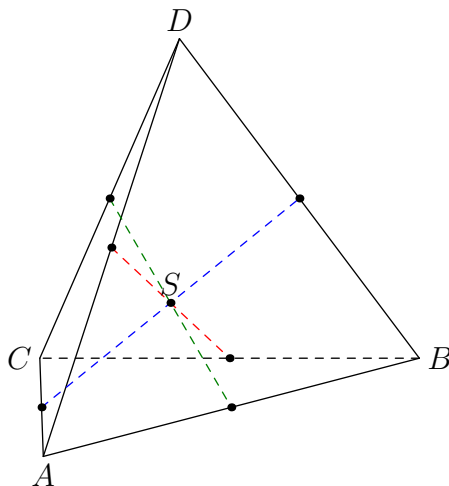
Man nennt $GL_n(k)$ die *allgemeine lineare Gruppe* (engl.: general linear group) und $SL_n(k)$ die *spezielle lineare Gruppe*. Die Determinante ist ein surjektiver Homomorphismus von $GL_n(k)$ nach der multiplikativen Gruppe $k^* = k \setminus \{0\}$, und der Kern ist $SL_n(k)$. Somit ist $GL_n(k)/SL_n(k) \cong k^*$.

4.2 Folgerungen des Homomorphiesatzes: die Isomorphiesätze

In unseren bisherigen Beispielen für Quotientengruppen G/H war meistens H groß und G/H sehr klein. Hier sind drei Beispiele, wo die Quotientengruppe nicht so einfach gestrickt ist; die Details machen wir erst später.

- a) S_3 ist eine Quotientengruppe des S_4 , der Normalteiler ist die Kleinsche Vierergruppe.

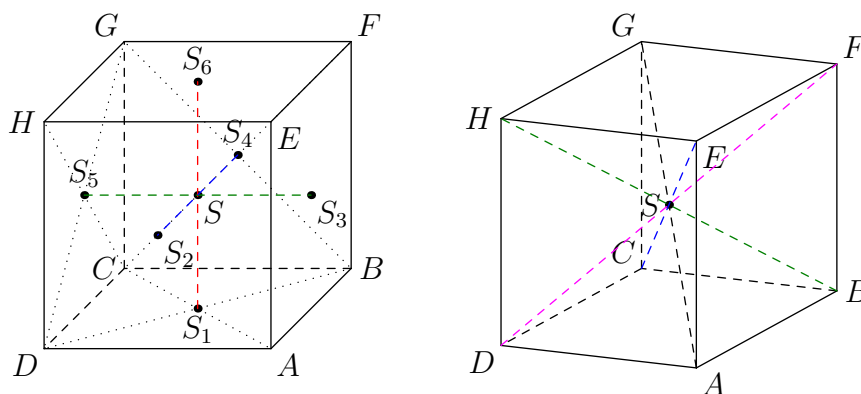
1. Begründung: S_4 ist die Symmetriegruppe des Tetraeders und permutiert die drei Achsen in diesem Bild:



2. Begründung: Algebraisch mittels des 1. Isomorphiesatzes.

- b) S_4 ist eine Quotientengruppe der Symmetriegruppe des Würfels, der Normalteiler ist C_2 .

Begründung: Die Würfelgruppe permutiert die vier Achsen im rechten Würfelbild.



- c) S_3 ist eine Quotientengruppe der Würfelgruppe. Der Normalteiler hat Ordnung 8.

1. Begründung: Die Würfelgruppe permutiert die drei Achsen im linken Würfelbild oben.

2. Begründung: Folgt aus a) und b) wegen des 2. Isomorphiesatzes.

Der 1. Isomorphiesatz Sei G eine Gruppe, $H \leq G$ eine Untergruppe und $K \triangleleft G$ ein Normalteiler. Dann ist $HK := \{hk \mid h \in H, k \in K\}$ eine Untergruppe

von G , K ist ein Normalteiler von HK , $H \cap K$ ist ein Normalteiler von H , und es gibt einen Isomorphismus $HK/K \cong H/(H \cap K)$.

Beweis. HK eine Untergruppe: $e = ee \in HK$; $(hk)(h'k') = (hh')(k''k') \in HK$ für $k'' = h'^{-1}kh' \in K$, da $K \triangleleft G$; $(hk)^{-1} = (ek^{-1})(h^{-1}e) \in (HK)^2 = HK$. Dann $K \triangleleft HK$, da $K \triangleleft G$ und $K \leq HK \leq G$. Es ist $H \cap K \leq H$ und $H \cap K \leq K$. Für $h \in H$ ist $h(H \cap K)h^{-1}$ eine Teilmenge von H , da $H \cap K \subseteq H$; und $h(H \cap K)h^{-1}$ eine Teilmenge von K , da $H \cap K \subseteq K$ und $K \triangleleft G$. Also $H \cap K \triangleleft G$.

Betrachten wir nun die Abbildung $f: H \rightarrow HK/K$, gegeben durch $f(h) = hK$. Dies ist ein Homomorphismus. Es ist surjektiv: $hkK = f(h)$. Der Kern von f ist $H \cap K$, denn $hK = eK$ genau dann, wenn $h \in K$. Nach dem Homomorphiesatz also ist $H/(H \cap K)$ isomorph zu HK/K . ■

Beispiel Sei $G = S_4$; sei $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$, eine Kopie von S_3 ; und sei $K = \{\text{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, eine Kopie der Kleinschen Vierergruppe. Wegen

$$\sigma \cdot (ab)(cd) \cdot \sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))$$

ist $K \triangleleft S_4$. Offensichtlich ist $K \cap H = \{\text{Id}\}$. Nach dem 1. Isomorphiesatz also ist $HK \leq S_4$ und $HK/K \cong H/(H \cap K)$, d.h. $HK/K \cong S_3$. Also ist $|HK| = |K| \cdot |S_3|$ wegen Lagrange, d.h. $|HK| = 4 \cdot 6 = 24 = |S_4|$. Also $HK = S_4$, und $S_4/K \cong S_3$.

Der 2. Isomorphiesatz ist eine Kürzungsregel.

Der 2. Isomorphiesatz Sei G eine Gruppe und H, K zwei Normalteiler von G mit $K \subseteq H$. Dann $K \triangleleft H$, $H/K \triangleleft G/K$ und es gibt einen Isomorphismus $(G/K)/(H/K) \cong G/H$.

Beweis. Da $K \triangleleft G$ ist, ist $hKh^{-1} = K$ für alle $h \in H$, also $K \triangleleft H$. Da H/K selbst eine Gruppe ist bzgl. der gleichen Multiplikation wie G/K , ist $H/K \leq G/K$. Sei $f: G/K \rightarrow G/H$ die Abbildung $f(gK) = gH$. Dieses f ist wohldefiniert: ist $gK = g'K$ dann gibt es ein $k \in K$ mit $g' = gk$. Da $K \subseteq H$ ist, ist $k \in H$, also $g'H = gH$. Ferner ist f ein Homomorphismus: $f(g_1K g_2K) = f(g_1 g_2 K) = g_1 g_2 H = g_1 H g_2 H = f(g_1 K) f(g_2 K)$. Außerdem ist f surjektiv, denn $gH = f(gK)$. Schließlich ist $\text{Kern}(f) = H/K$, denn $gH = eH$ genau dann, wenn $g \in H$ ist, d.h. wenn $gK \in H/K$ ist. Nach Lemma 3.3 ist also $H/K \triangleleft G/K$; und nach dem Homomorphiesatz induziert f einen Isomorphismus $(G/K)/(H/K) \rightarrow G/H$. ■

4.3 Gruppenoperationen

Definition Sei G eine Gruppe und X eine Menge. Eine (Links-)Operation von G auf X besteht aus einer Abbildung $\rho: G \times X \rightarrow X$, $(g, x) \mapsto gx$, mit den folgenden Eigenschaften:

(O1) Assoziativität: $g(hx) = (gh)x$ für alle $g, h \in G, x \in X$.

(O2) Normierung: $ex = x$ für alle $x \in X$.

Beispiele a) Die Diedergruppe D_n operiert per Definition auf dem regulären n -Eck. Sie operiert auch auf der Mengen der Ecken: diese Operation benutzen wir um die Diedergruppe zu berechnen.

b) Die natürliche Operation des $GL_n(\mathbb{R})$ auf \mathbb{R}^n , gegeben durch $\rho(A, v) = A \cdot v$.

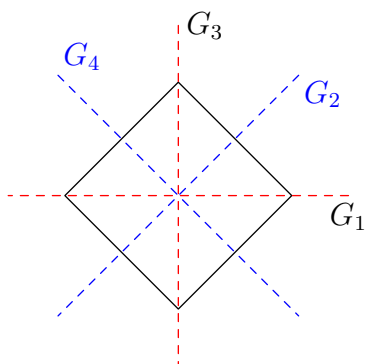
c) Jede Gruppe operiert auf sich selbst durch Linksmultiplikation: G ist beliebig, $X = G$ und $\rho(g, x) = gx$.

d) Außerdem operiert jede Gruppe auf sich selbst durch Konjugation: G ist beliebig, $X = G$ und $\rho(g, x) = gxg^{-1}$.

e) Komplexe Konjugation: $X = \mathbb{C}, G = C_2$ und $\rho(g, z) = \begin{cases} z & g = 1 \\ \bar{z} & g = -1 \end{cases}$.

f) Die natürliche Operation der symmetrischen Gruppe $S(X)$ auf X , gegeben durch $\rho(\sigma, x) := \sigma(x)$.

g) $G = D_4$ operiert auf die vier Achsen eines Quadrats.



Die Operation f) führt zu einer zweiten äquivalenten Definition des Operationsbegriffs.

Lemma 4.1 Sei G eine Gruppe und X eine Menge. Es gibt eine bijektive Korrespondenz zwischen der Menge der Operationen von G auf X und der Menge der Homomorphismen von G nach der symmetrischen Gruppe $S(X)$ aller Permutationen von X .

Beweis. Ist $\alpha: G \rightarrow S(X)$, so definieren wir $\rho: G \times X \rightarrow X$ durch $\rho(g, x) = \alpha(g)(x)$. Dann ist $\rho(e, x) = \alpha(e)(x) = \text{Id}(x) = x$; und

$$\rho(g, \rho(g', x)) = \alpha(g)(\alpha(g')(x)) = (\alpha(g) \circ \alpha(g'))(x) = \alpha(gg')(x) = \rho(gg', x).$$

Also ist ρ eine Gruppenoperation. Ist dagegen $\rho: G \times X \rightarrow X$ eine Operation, so definiert jedes $g \in G$ eine Abbildung $\sigma_g: X \rightarrow X$ durch $\sigma_g(x) = gx$. Da $g^{-1}(gx) = ex = g(g^{-1}x)$ ist, ist $\sigma_{g^{-1}} = \sigma_g^{-1}$, also ist σ_g eine Bijektion. Somit ist $g \mapsto \sigma_g$ eine Abbildung $G \rightarrow S(X)$. Diese Abbildung ist ein Homomorphismus, denn $\sigma_g \sigma_{g'}(x) = \sigma_g(g'x) = gg'x = \sigma_{gg'}(x)$. ■

Definition Die Gruppe G operiere auf der Menge X .

a) Der *Stabilisator* $G_x = \text{Stab}_G(x)$ eines Elements $x \in X$ ist

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

b) Die *Bahn* $Gx = \text{Bahn}_G(x)$ ist $Gx := \{gx \mid g \in G\}$. Die Anzahl der Elemente einer Bahn heißt die *Länge*.

c) Eine Operation heißt *transitiv*, falls es ein $x \in X$ gibt mit $Gx = X$.

Beispiel $G = D_3$ operiert auf das reguläre Dreieck. Die drei Ecken bilden eine Bahn: der Stabilisator von A ist die Untergruppe $\langle \sigma_A \rangle = \{\text{Id}, \sigma_A\}$. Der Stabilisator von B dagegen ist $\{\text{Id}, \sigma_B\}$. Die Mittelpunkte der drei Kanten bilden eine weitere Bahn; der Stabilisator des Mittelpunkts von AB ist $\{\text{Id}, \sigma_C\}$. Der Schwerpunkt bildet eine einelementige Bahn, deren Stabilisator ganz D_3 ist. Sei P ein Punkt auf der Kante AB , der zwischen A und der Mittelpunkt liegt: dann hat die Bahn von P sechs Elemente, und $\text{Stab}_G(P) = \{\text{Id}\}$. Die Operation ist nicht transitiv: wir haben bereits drei verschiedene Bahnen gesehen.

In diesem Beispiel ist der Stabilisator eine Untergruppe von G , und das Produkt der Bahnlänge mit der Ordnung des Stabilisators ist immer $|G| = 6$. Dies ist kein Zufall.

Beispiel Die symmetrische Gruppe S_n operiert auf der Menge $\{1, \dots, n\}$. Diese Operation ist transitiv, denn für jedes $r \geq 2$ liegt r in $\text{Bahn}_{S_n}(1)$ wegen der Transposition $(1 r)$. Der Stabilisator von 1 ist eine Kopie von $S(\{2, \dots, n\})$ und somit isomorph zu S_{n-1} .

Lemma 4.2 a) Für jedes $x \in X$ ist $\text{Stab}_G(x) \leq G$.

b) Die Relation $y \in \text{Bahn}_G(x)$ ist eine Äquivalenzrelation auf X , deren Äquivalenzklassen die Bahnen der Operation sind. Somit ist die Operation genau dann transitiv, wenn es nur eine Bahn gibt.

Beweis. a) Es ist $ex = x$, also $e \in \text{Stab}_G(x)$. Ist $gx = x$, dann $g^{-1}x = x$. Ist $gx = x$ und $hx = x$, dann $(gh)x = g(hx) = gx = x$.

b) Reflexiv, da $ex = x$. Symmetrisch, da $y = gx$ genau dann, wenn $x = g^{-1}y$. Transitiv, da aus $y = gx$ und $z = hy$ folgt $z = (hg)x$. ■

Lemma 4.3 (Die Bahnengleichung) Für jedes $x \in X$ gilt die Bahnengleichung:

$$|\text{Stab}_G(x)| \cdot |\text{Bahn}_G(x)| = |G| .$$

Beweis. Sei $H = \text{Stab}_G(x) \leq G$. Nach Lagrange ist $|G| = |H| \cdot |G : H|$. Wir werden also zeigen, dass es eine Bijektion gibt zwischen der Bahn von x und der Menge G/H der Linksnebenklassen. Ist $gH = g'H$, so gibt es $h \in H$ mit $g' = gh$. Also $g'x = ghx = gx$, da $hx = x$. Somit ist die Abbildung $G/H \rightarrow \text{Bahn}_G(x)$, $gH \mapsto gx$ wohldefiniert. Sie ist injektiv, denn aus $gx = g'x$ folgt $g^{-1}g'x = x$, also $g^{-1}g' \in H = \text{Stab}_G(x)$, also $gH = g'H$. Surjektiv: ist $y \in \text{Bahn}_G(x)$ dann $y = gx$ für ein $g \in G$. Somit ist y das Bild von gH . Die Abbildung ist also bijektiv. ■

Der Satz von Cayley Jede Gruppe G ist isomorph zu einer Untergruppe der symmetrischen Gruppe $S(G)$. Somit ist jede Gruppe isomorph zu einer Permutationsgruppe.

Beweis. Wir betrachten die Operation von G auf sich selbst durch Linksmultiplikation. Diese Operation entspricht einem Homomorphismus $\rho: G \rightarrow S(G)$, gegeben durch $\rho(g)(x) = gx$. Dieser Homomorphismus ist injektiv, denn ist $\rho(g) = \text{Id}$, dann $\rho(g)(e) = e$. Aber $\rho(g)(e) = ge = g$. Also $g = e$. Nach dem Homomorphiesatz also ist $G \cong \text{Bild}(\rho) \leq S(G)$. ■

5 Die regulären Polyeder

5.1 Ein Symmetriebegriff

Jedes Kind weiß, was man unter den Begriff „Symmetrie“ zu verstehen hat. Wir benötigen eine mathematisch präzise Definition.

Definition Sei $X \subseteq \mathbb{R}^n$. Eine *isometrische Symmetrie* (kurz: Symmetrie) von X ist eine Bijektion $f: X \rightarrow X$, die Abstände erhält: es ist $\|f(w) - f(v)\| = \|w - v\|$ für alle $v, w \in X$. Die Menge aller isometrischen Symmetrien ist eine Gruppe bzgl. Verknüpfung, die *Isometriegruppe* von X .

Beispiel Die Diedergruppe D_n definieren wir als die Isometriegruppe des regulären n -Ecks.

Ist $X \subseteq \mathbb{R}^3$ ein reguläres Polyeder, dessen Schwerpunkt im Koordinatenursprung liegt, dann wird jede Symmetrie von X durch eine orthogonale Transformation $A \in O(3)$ bewirkt. Diese Tatsache kann man als anschaulich klar betrachten; oder man kann sie beweisen. Allerdings haben wir den Begriff „reguläres Polyeder“ noch nicht präzisiert. Also beweisen wir ein etwas allgemeineres Ergebnis (Lemma 5.1). Zuerst benötigen wir einige Hilfsmittel.

Definition Sei $X \subseteq \mathbb{R}^m$. Eine Abbildung $f: X \rightarrow \mathbb{R}^n$ heißt eine *isometrische Einbettung* falls sie Abstände erhält, d.h. $\|f(y) - f(x)\| = \|y - x\|$ für alle $x, y \in X$.

Isometrische Einbettungen sind injektiv: ist $x \neq y$, dann $\|x - y\| \neq 0$, also $\|f(x) - f(y)\| \neq 0$, also $f(x) \neq f(y)$. Meistens sind sie nicht surjektiv.

Wir beschäftigen uns nur mit isometrischen Einbettungen $f: X \rightarrow \mathbb{R}^n$ wenn X selbst eine Teilmenge des \mathbb{R}^n ist. Solche isometrischen Einbettungen sind meistens affin oder sogar linear. Außerdem: wenn linear, dann sogar orthogonal.

Aus der LAAG1 (Lemma 9.4) wissen wir: zu jeder affinen Abbildung $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ gibt es genau eine assoziierte lineare Abbildung $g: \mathbb{R}^n \rightarrow \mathbb{R}^n$. Es ist dann $f(a + x) = f(a) + g(x)$ für alle $a, x \in \mathbb{R}^n$.

Definition Eine affine Abbildung $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ heißt eine *Bewegung* des \mathbb{R}^n , falls die assoziierte lineare Abbildung $g: \mathbb{R}^n \rightarrow \mathbb{R}^n$ orthogonal ist. Die Bewegungen bilden eine Gruppe bzgl. Verknüpfung. Bezeichnung: $AO(n)$.

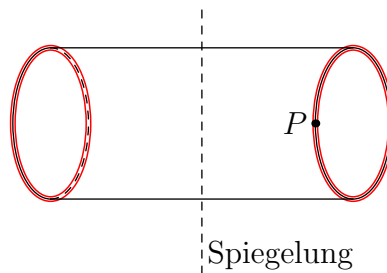
Genau dann ist also f eine Bewegung, wenn es für ein $a \in \mathbb{R}^n$ eine orthogonale Matrix $A \in O(n)$ gibt mit $f(a + x) = f(a) + A \cdot x$ für alle $x \in \mathbb{R}^n$.

Bezeichnung Für $x \in \mathbb{R}^n$ und $\varepsilon > 0$ ist $B(x, \varepsilon) := \{y \in \mathbb{R}^n \mid \|y - x\| < \varepsilon\}$, der offene Ball um x vom Radius ε .

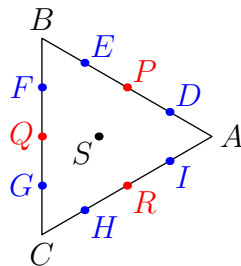
Lemma 5.1 Sei $X \subseteq \mathbb{R}^n$ eine Teilmenge, die mindestens einen inneren Punkt enthält, d.h. es gibt ein $x \in X$ und ein $\varepsilon > 0$ mit $B(x, \varepsilon) \subseteq X$. Dann:

- Jede isometrische Einbettung $f: X \rightarrow \mathbb{R}^n$ ist die Einschränkung einer Bewegung $f \in AO(n)$.
- Angenommen, es gibt ein $x \in X$ dessen Bahn bzgl. der Operation der Isometriegruppe auf X endlich ist. Dann gibt es ein $x_0 \in \mathbb{R}^n$, mit $f(x_0) = x_0$ für jede isometrische Symmetrie von X ; und wählt man den Koordinatenursprung in x_0 , so ist die Isometriegruppe von X eine Untergruppe des $O(n)$.

Bemerkung Wichtigster Fall: $X \subseteq \mathbb{R}^3$ ist ein reguläres Polyeder. Dann ist jeder Punkt, der nicht auf der Oberfläche liegt, ein innerer Punkt. Da es nur endlich viele Ecken gibt, hat jede Ecke eine endliche Bahn. Der Schwerpunkt ist dann ein solcher Punkt x_0 . Die Bedingung in Teil b) soll auch in allgemeinen Fällen die Existenz eines „Schwerpunktes“ nachzuweisen. Im Zylinder dagegen gibt es Punkte, deren Bahnlänge unendlich ist.



Auch bei endlichen Bahnen können unterschiedliche Bahnlängen auftreten:



Beweis. a) Sei also $B(x, \varepsilon) \subseteq X$. Es reicht, den Fall $x = f(x) = 0$ zu behandeln. Somit gilt nicht nur $\|f(y) - f(z)\| = \|y - z\|$ sondern auch $\|f(y)\| = \|y\|$ ($z = 0$ nehmen!). Die Abbildung f erhält also Skalarprodukte, denn

$$\begin{aligned} 2\langle f(y), f(z) \rangle &= \|f(y)\|^2 + \|f(z)\|^2 - \|f(y) - f(z)\|^2 \\ &= \|y\|^2 + \|z\|^2 - \|y - z\|^2 = 2\langle y, z \rangle. \end{aligned}$$

Für $1 \leq i \leq n$ sei $v_i = \frac{\varepsilon}{2}e_i \in B(0, \varepsilon) \subseteq X$. Sei $A \in M_n(\mathbb{R})$ die Matrix, deren i -te Spalte $\frac{2}{\varepsilon}f(v_i)$ ist. Weil f Skalarprodukten erhält, haben die Spalten

die Länge 1, und sie sind orthogonal: es ist also $A \in O(n)$. Außerdem ist $f(v_i) = A \cdot v_i$ für jedes i , und diese n Vektoren bilden eine Basis von \mathbb{R}^n . Für beliebiges $w \in X$ ist also

$$\langle f(w), A \cdot v_i \rangle = \langle f(w), f(v_i) \rangle = \langle w, v_i \rangle = \langle A \cdot w, A \cdot v_i \rangle$$

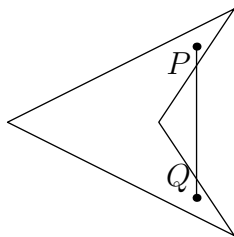
für alle i , weshalb $f(w) = A \cdot w$.

- b) Sei f eine isometrische Symmetrie und $\{x_1, \dots, x_r\}$ eine endliche Bahn der Isometriegruppe. Sei $x_0 = \frac{1}{r} \sum_{i=1}^r x_i$. Dies ist eine affine Kombination von x_1, \dots, x_r und f ist eine affine Abbildung. Also

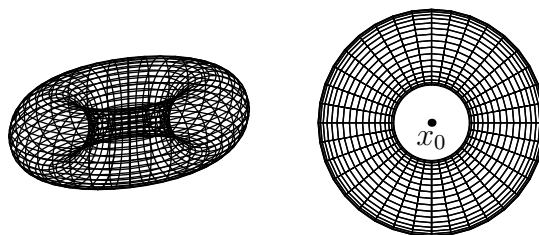
$$f(x_0) = \frac{1}{r} \sum_{i=1}^r f(x_i) = \frac{1}{r} \sum_{i=1}^r x_i = x_0,$$

denn f operiert als eine Permutation der Menge $\{x_1, \dots, x_r\}$. Wählt man den Koordinatenursprung in x_0 , so zeigt der Beweis zu a), dass jede isometrische Symmetrie orthogonal ist. ■

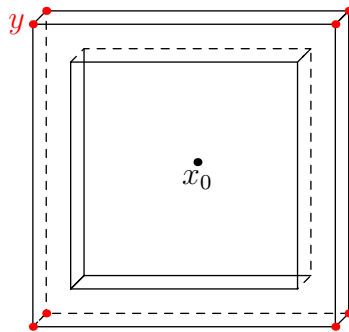
Bemerkung Eine Teilmenge X des \mathbb{R}^n heißt konvex, falls für alle P, Q die Strecke von P nach Q ganz in X liegt. Somit ist das folgende Viereck nicht konvex:



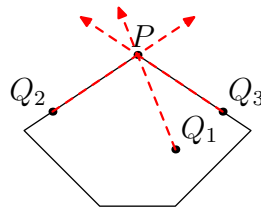
Ist X nicht konvex in Lemma 5.1 b), so kann es vorkommen, dass x_0 außerhalb von X liegt, etwa im Torus



oder im „Bilderrahmen“:



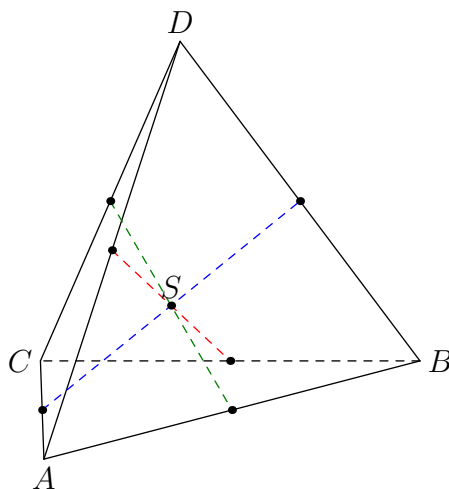
Die Ecken eines konvexen Polyeders $X \subseteq \mathbb{R}^3$ lassen sich so charakterisieren: genau dann ist $E \in X$ eine Ecke, wenn für jedes $E \neq P \in X$ die Gerade von P in Richtung E direkt hinter E aus X heraustritt.



Da jede Bewegung f umkehrbar ist, Geraden auf Geraden abbildet und Längen erhält, gilt: ist f eine isometrische Symmetrie von X , so ist auch $f(E)$ eine Ecke.

5.2 Die Isometriegruppe des Tetraeders

Das Tetraeder ist ein reguläres Polyeder mit vier Seiten, sechs Kanten und vier Ecken. Die Seiten sind reguläre Dreiecke. Nennen wir die Ecken A, B, C, D . Zu jedem Paar von Ecken gibt es eine Kante, die die beiden Ecken miteinander verbinden; zu jedem Tripel von Ecken gibt es eine Seite mit diesen Ecken.



Der Schwerpunkt S ist der Durchschnitt aller vier Ecken:

$$\vec{OS} = \frac{1}{4} (\vec{OA} + \vec{OB} + \vec{OC} + \vec{OD}) .$$

Jede isometrische Symmetrie permutiert die Ecken, also $f(S) = S$ für jede Symmetrie. Wählen wir den Koordinatenursprung in S , so ist jede Symmetrie eine orthogonale Transformation. Es sind $4! = 24$ Permutationen der Ecken denkbar. Jeder 3-Zykel kommt auch vor: eine Drehung durch $\frac{2}{3}\pi$ um die Achse DS etwa bewirkt den 3-Zykel $(A B C)$. Also kommt jede Permutation $\sigma \in A_4$ vor, denn:

Lemma 5.2 *Für jedes $n \geq 1$ wird A_n durch die Menge aller 3-Zykel erzeugt.*

Beweis. Transpositionen haben Vorzeichen -1 , und jede Permutation ist ein Produkt von Transpositionen. Also wird $A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = +1\}$ von allen Produkten von zwei Transpositionen erzeugt. Drei Fälle: $(a b)(a b) = \text{Id}$; $(a b)(a c) = (a c b)$, ein 3-Zykel; und $(a b)(c d) = (a c b)(a c d)$, ein Produkt von zwei 3-Zykeln. ■

Spiegelt man dagegen in der Ebene durch A, B und den Mittelpunkt der Kante CD , so erhält man die Transposition $(C D)$. Aber A_4 und S_4 selbst sind die einzigen Untergruppen des S_4 , die A_4 enthalten (Lagrange). Somit entsteht jede Permutation $\sigma \in S(\{A, B, C, D\})$ durch eine isometrische Symmetrie des regulären Tetraeders. Umgekehrt sei f eine isometrische Symmetrie, die im Kern des Homomorphismus nach S_4 liegt. Dann ist f linear, und $f(A) = A$, $f(B) = B$, $f(C) = C$. Da die Ortsvektoren \vec{OA} , \vec{OB} und \vec{OC} eine Basis des \mathbb{R}^3 sind, ist $f = \text{Id}$. Wir haben gezeigt:

Lemma 5.3 *Durch die Operation auf den Ecken wird die Isometriegruppe T des regulären Tetraeders zur Symmetriegruppe S_4 isomorph.* ■

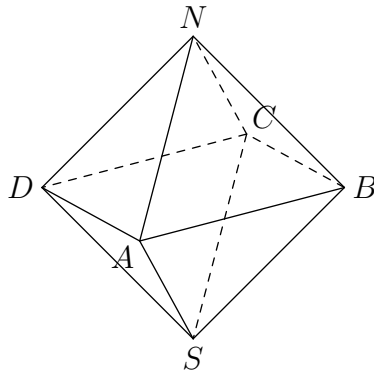
Jede Kante K des Tetraeders hat eine entgegengesetzte Kante K' , erklärt durch $\{A, B, C, D\} = \text{Endpunkte}(K) \uplus \text{Endpunkte}(K')$. Zum Beispiel ist $K' = BD$ für $K = AC$. Es sind drei solche Kantenpaare $\{K, K'\}$. Entsprechend gibt es drei Geraden, die die Mittelpunkte von entgegengesetzten Kanten miteinander verbinden. Diese drei Geraden treffen sich in deren gemeinsamen Mittelpunkt S .

Beispiel $K = AC$, $K' = BD$. Die Gerade zu diesem Paar enthält die Kantenmittelpunkte P, Q gegeben durch $\vec{OP} = \frac{1}{2}(\vec{OA} + \vec{OC})$, $\vec{OQ} = \frac{1}{2}(\vec{OB} + \vec{OD})$. Der Mittelpunkt der Gerade ist S , denn $\vec{OS} = \frac{1}{2}(\vec{OP} + \vec{OQ})$.

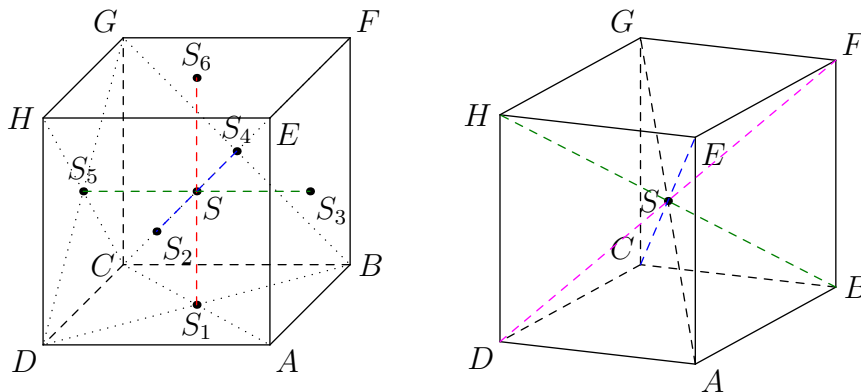
Ist f eine Symmetrie, dann $f(K') = [f(K)]'$, also operiert die Isometriegruppe T auf die Menge der drei Geraden. Eine Rotation bewirkt ein 3-Zykel, eine Spiegelung bewirkt eine Transposition, also entsteht jede Permutation $\sigma \in S_3$ auf dieser Weise. Der induzierten Homomorphismus von T nach S_3 ist also surjektiv. Nach dem Homomorphiesatz ist S_3 eine Quotientengruppe von T . Da aber $T \cong S_4$ ist, haben wir unseren 2. Beweis, dass S_3 eine Quotientengruppe von S_4 ist.

5.3 Die Isometriegruppe des Würfels

Der Würfel hat sechs Flächen, zwölf Kanten und acht Ecken. Das Oktaeder mit acht Flächen, zwölf Kanten und sechs Ecken



ist dual zum Würfel: die sechs Flächenmittelpunkte eines Würfels sind die Ecken eines Oktaeders, und die acht Flächenmittelpunkte eines Oktaeders sind die acht Ecken eines Würfels. Somit haben Würfel und Oktaeder die gleiche Isometriegruppe, die wir W nennen werden³.



Betrachten wir die Operation von W auf der Menge der Ecken. Eine Drehung um $\frac{\pi}{2}$ um die Achse durch den Schwerpunkt S und den Flächenmittelpunkt S_3 bewirkt die Permutation $(E A B F)(H D C G)$. Somit enthält $\text{Bahn}_W(E)$ mindestens E, A, B, F . Sie enthält auch H, D (um die Achse durch S und S_2 drehen). Dann ist aber $\text{Bahn}_W(E) = \text{Bahn}_W(H)$, was auch C, G enthält. Ergebnis: die Operation auf den Ecken ist transitiv. Aufgrund der Bahnengleichung ist also $|W| = 8 \cdot |W_E|$.

Betrachten wir jetzt die Operation des Stabilisators W_E . Dies permutiert die drei zu E benachbarten Ecken A, F, H . Eine Drehung um $\frac{2}{3}\pi$ um die Achse durch

³Manche Quellen nennen diese Gruppe O ; der Verwechslungsgefahr wegen vermeiden wir diese Schreibweise.

S und E permutiert liegt im Stabilisator und operiert auf $\{A, F, H\}$ als $(A F H)$. Bezeichnen wir mit $W_{E,A}$ den gemeinsamen Stabilisator von E, A : es ist also

$$W_{E,A} = \{f \in W \mid f(E) = E, f(A) = A\} = \text{Stab}_{W_E}(A).$$

Dann ist $|W_E| = 3 \cdot |W_{E,A}|$ und $|W| = 24 \cdot |W_{E,A}|$.

Bezeichnung G operiere auf X . Für $x_1, \dots, x_n \in X$ setzen wir

$$G_{x_1, x_2, \dots, x_n} := \{g \in G \mid \forall i \ g(x_i) = x_i\},$$

der gemeinsame Stabilisator von x_1, \dots, x_n . Genau wie ein gewöhnlicher Stabilisator ist G_{x_1, x_2, \dots, x_n} eine Untergruppe von G .

Dieser gemeinsame Stabilisator $W_{E,A}$ operiert wiederum auf der Menge $\{F, H\}$ der beiden anderen zu E benachbarten Ecken. Eine Spiegelung in der Ebene durch E, A, S bewirkt die Transposition $(F H)$ dieser Menge. Also $|W_{E,A}| = 2 \cdot |W_{E,A,F}|$ und $|W| = 48 \cdot |W_{E,A,F}|$. Ist aber $f \in W_{E,A,F}$ dann $f = \text{Id}$, denn $f(S) = S$ und die Ortsvektoren (bzgl. S) von E, A, F sind eine Basis des \mathbb{R}^3 . Also $W_{E,A,F} = \{\text{Id}\}$; der Homomorphismus $W \rightarrow S(\text{Ecken}(\text{Würfel}))$ ist ein Isomorphismus auf sein Bild, und $|W| = 48$.

Jetzt wollen wir die Struktur des W untersuchen. Wählen wir den Koordinatensprung in S , so ist $W \leq O(3)$.

Lemma 5.4 *Sei $G \leq O(n)$. Setze $H := SO(n) \cap G$. Dann entweder $\det(A) = 1$ für alle $A \in G$ und $H = G$; oder es gibt ein $A \in G$ mit $\det(A) = -1$, $H \triangleleft G$ und $|G : H| = 2$.*

Zusatz für n ungerade: Enthält G die so genannte Punktspiegelung $A = -E_n$, so ist $|G : H| = 2$ und $G \cong C_2 \times H$.

Beweis. $\det: G \rightarrow C_2$ ist ein Gruppenhomomorphismus. Also ist der Kern H ein Normalteiler, und $|G : H| = |\text{Bild}(\det)| \in \{1, 2\}$.

Zum Zusatz: Da n ungerade ist, ist $\det(-E_n) = (-1)^n = -1$. Also $|G : H| = 2$. Ferner ist $(-E_n)^2 = E_n$, also $\langle -E_n \rangle \cong C_2$; und für $A = -E_n$ ist $AB = BA$ für jedes $B \in O(n)$, also ist die Abbildung $\phi: C_2 \times H \rightarrow G$, $\phi(\varepsilon, B) = (-E_n)^\varepsilon B$ ein Gruppenhomomorphismus und eine Bijektion, ein Isomorphismus also. ■

Die Punktspiegelung $-E_3$ gehört zu W , also ist $W = \langle -E_3 \rangle \times R$ für $R := W \cap SO(3)$. Betrachten wir jetzt die Operation von W und von R auf die Menge $\{EC, AG, HB, FD\}$ der vier Diagonalen durch entgegengesetzten Ecken. Dreht man um EC , so erhält man den 3-Zykel $(AG FD HB)$; analog erhält man jeden 3-Zykel, und daher jede gerade Permutation. Dreht man um die Achse durch S, S_3 , so erhält man den (ungeraden) 4-Zykel $(EC AG HB FD)$. Drehungen um Achsen haben Determinante $+1$, also operiert R auf $\{EC, AG, HB, FD\}$ als die volle symmetrische Gruppe. Da $|R| = 24 = |S_4|$ ist, folgt $R \cong S_4$ und

$W \cong C_2 \times S_4$. Da auch W als die volle Symmetriegruppe operiert, ist S_4 zu einer Quotientengruppe von W isomorph.

Auch permutiert W die drei Achsen durch Flächenmittelpunkte. Dreht man um die Achse EC , so permutiert man diese 3 Achsen mit einem 3-Zykel. Spiegelt man in der Ebene EBC , so vertauscht man zwei Achsen miteinander und lässt die dritte fest. Also entsteht jede Permutation der drei Achsen. Also ist auch S_3 eine Quotientengruppe von W (1. Begründung).

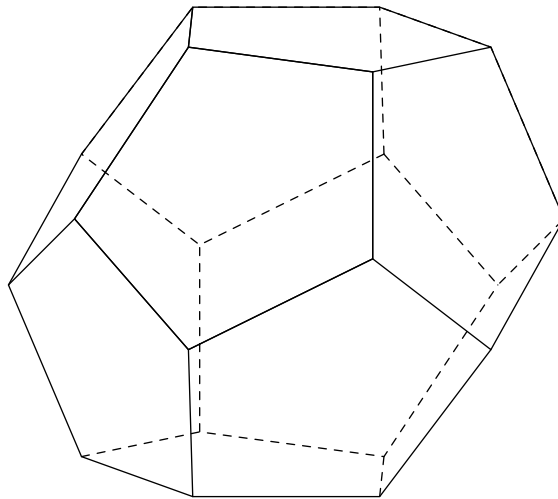
Beispiel Der 2. Isomorphiesatz $(G/K)/(H/K) \cong G/H$ ist eine Kürzungsregel. Mit $G = W$, $K = \langle -E_3 \rangle$ und $H = \text{Kern}(W \rightarrow S_3)$ erhalten wir $S_4/(H/K) \cong S_3$ (3. Begründung). Alternativ können wir aus „ S_3 Quotientengruppe von S_4 “ und „ S_4 Quotientengruppe von W “ folgern, dass S_3 eine Quotientengruppe von W ist, aufgrund des folgenden Lemmas (2. Begründung).

Lemma 5.5 Sei $f: G \rightarrow \Gamma$ surjektiv mit Kern K . Sei $N \triangleleft \Gamma$ ein Normalteiler. Dann ist $H := f^{-1}(N)$ ein Normalteiler von G , $K \leq H$, und $G/H \cong \Gamma/N$.

Beweis. Sei $p: \Gamma \rightarrow \Gamma/N$ die kanonische Projektion. Dann $H = \text{Kern}(p \circ f) \triangleleft G$ und $K \leq H$. Jetzt den 2. Isomorphiesatz anwenden. ■

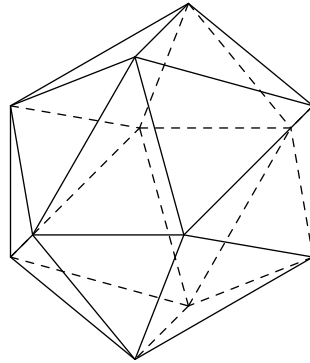
5.4 Das Ikosaeder

Das Dodekaeder mit 12 Flächen, 20 Ecken und 30 Kanten



ist dual zum Ikosaeder mit 12 Ecken, 20 Flächen und 30 Kanten: die Flächenmittelpunkte des einen sind die Ecken einer Kopie des anderen. Also haben sie die gleiche Isometriegruppe I . Wir arbeiten mit dem Ikosaeder. Die Flächen sind reguläre Dreiecke. An jeder Ecke treffen sich fünf Flächen. Jede Ecke hat eine entgegengesetzte Ecke. Betrachtet man diese Ecken als Nord- und Südpol, so hat

jeder Pol seinen Polarkreis, der aus den fünf Flächen um den Pol besteht. Die restlichen zehn Flächen bilden ein äquatorielles Band.

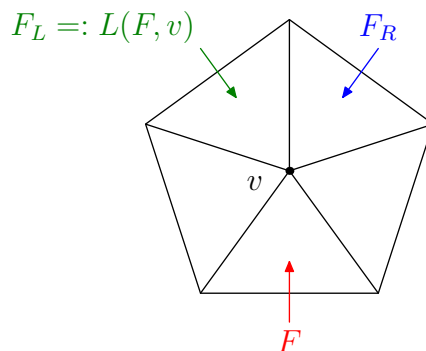


Die Isometriegruppe I enthält $-E_3$, es ist also $I \cong C_2 \times I_+$, wobei I_+ den Schnitt $I_+ = I \cap SO(3)$ bezeichnet.

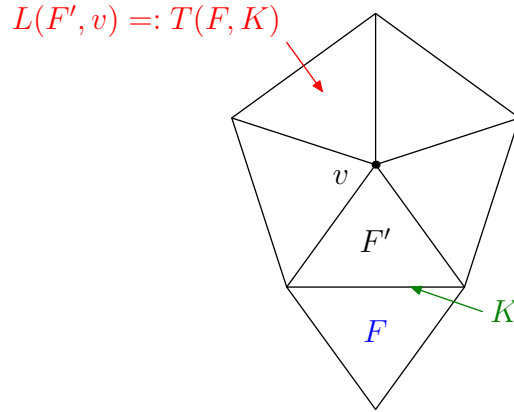
Die Operation von I_+ auf die Ecken ist transitiv. Dies kann man so sehen: Dreht man durch $\frac{2\pi}{5}$ um die Achse durch zwei entgegengesetzte Ecken, so verteilen sich die Ecken in vier Bahnen: der Nordpol und der Südpol als Bahnen mit je einem Element; und zwei fünf-elementige Bahnen, ein oberer Ring und ein unterer Ring. Dreht man um eine Ecke im oberen Ring, so verschmelzen sich die vier Bahnen in einer. Wird eine Ecke N festgehalten, so kann man um sie drehen, die fünf benachbarten Ecken bilden eine Bahn. Werden zwei benachbarten Ecken N, A festgehalten, so gibt es – außer eine Spiegelung, die nicht in I_+ liegt – keine Isometrien mehr. Es ist also $|I_+| = 60$ und $|I| = 120$.

Es stellt sich heraus, dass $I_+ \cong A_5$ ist. Hieraus folgt, dass $I \cong A_5 \times C_2$ ist. Man beachte, dass $A_5 \times C_2$ nicht zu S_5 isomorph ist, denn es gibt kein $\sigma \in S_5$, das Ordnung 2 hat und mit jedem $\tau \in S_5$ kommutiert.

Wir müssen fünf Gegenstände finden, die durch I_+ permutiert werden. Sei v eine Ecke und F eins der fünf Flächen um v . Es gibt zwei Flächen um v , die gegenüber von F liegen. Halte ich das Ikosaeder mit v mit direkt gegenüber und F ganz unten im Kreis der fünf Flächen, so sind die beiden gegenüber liegenden Flächen oben: ein links oben und ein rechts oben. Ich schreibe $L(F, v)$ für die Fläche links oben.



Nun wähle ich eine Fläche F und eine Kante K von F . Sei F' die Fläche auf der anderen Seite von K , und sei v die Ecke von F' gegenüber von K . Schreiben wir $T(F, K)$ für die Fläche $L(F', v)$.



Sei $T(F)$ die Menge

$$T(F) = \{F\} \cup \{T(F, K) \mid K \text{ eine Kante von } F\}.$$

Dann: $T(F)$ hat vier Elemente, und für alle $F' \in T(F)$ und für jede Kante K' von F' ist $T(F', K') \in T(F)$. Aufgrund dieser Symmetrie sind die Flächenmittelpunkte der vier Flächen die vier Ecken eines regulären Tetraeders, weshalb ich $T(F)$ das Tetraeder von F nenne. Außerdem ist jede Ecke des Ikosaeders Ecke von genau einer Fläche in $T(F)$. Daher werden die zwanzig Flächen des Ikosaeders in fünf vier-elementige Tetraeder aufgeteilt. Um jede Ecke ist jedes Tetraeder mit einer Fläche vertreten. Da Rotationen die rechts- und links-gegenüberliegenden Flächen an einer Ecke nicht vertauschen, induziert jedes $f \in I_+$ eine Permutation der fünf-elementigen Mengen der Tetraeder. Dreht man um eine Ecke, so muss diese Permutation ein 5-Zykel sein. Dreht man um die Achse durch den Mittelpunkt einer Fläche F^4 , so entsteht ein 3-Zykel: denn die drei Nachbarflächen zu F haben gemeinsame Ecken und entsammen so drei verschiedener Tetraeder. Diese drei werden zyklisch permutiert: und die einzige gerade Permutation von 5 Objekten, deren Zerlegung in disjunkten Zykeln ein 3-Zykel enthält, ist ein 3-Zykel. Somit ist $I_+ \cong A_5$, denn $|I_+| = 60 = A_5$, und das Bild von I_+ in der symmetrischen Gruppe der fünf Tetraeder ist A_5 :

Lemma 5.6 a) Seien $\sigma, \tau \in S_4$ zwei 3-Zykel mit $\tau \neq \sigma^{\pm 1}$. Dann $\langle \sigma, \tau \rangle = A_4$.

b) Sei $\sigma \in S_5$ ein 3-Zykel und $\tau \in S_5$ ein 5-Zykel. Dann $\langle \sigma, \tau \rangle = A_5$.

Beweis. a) Sei $\sigma = (a b c)$, $\tau = (d e f)$. Wegen $\tau \neq \sigma^{\pm 1}$ ist $\{d, e, f\} \neq \{a, b, c\}$. Da $\{a, b, c\}$ und $\{d, e, f\}$ Teilmengen von $\{1, 2, 3, 4\}$ sind, enthält

⁴Die Fläche ganz unten ist übrigens um $\frac{\pi}{3}$ verdreht.

der Schnitt $\{a, b, c\} \cap \{d, e, f\}$ genau zwei Elemente. Nummeriert man um, so sind es oBdA 1, 2, und $\sigma = (1\ 2\ 3)$. Ersetzt man dann zur Not τ durch τ^{-1} , so ist $\tau = (1\ 2\ 4)$. Sei $H = \langle \sigma, \tau \rangle$. Wegen Lagrange ist $3 \mid |H| \mid 12 = |A_4|$, und es reicht zu zeigen: $4 \mid |H|$.

Es ist $(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$ und $(1\ 2\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3)$, also enthält H die vier-elementige Untergruppe $\langle (1\ 3)(2\ 4), (1\ 4)(2\ 3) \rangle$, und $4 \mid |H|$ nach Lagrange.

- b) Sei $H = \langle \sigma, \tau \rangle$. Dann $H \leq A_5$; und es ist $3 \mid |H|$ und $5 \mid |H|$. Es reicht z.z. $4 \mid |H|$. Nummeriert man um, so ist der 3-Zykel $(1\ 2\ a)$ für $a \in \{3, 4, 5\}$. Ersetzt man dann den 5-Zykel durch eine geeignete Potenz, so ist der 5-Zykel $(1\ 2\ c\ d\ e)$. Nummeriert man $\{3, 4, 5\}$ erneut um, so ist der 5-Zykel $(1\ 2\ 3\ 4\ 5)$ und der 3-Zykel ist $(1\ 2\ 3)$, $(1\ 2\ 4)$ oder $(1\ 2\ 5)$. Wegen $(1\ 2\ 5) = (5\ 1\ 2)$ und $(1\ 2\ 3\ 4\ 5) = (5\ 1\ 2\ 3\ 4)$ ist der Fall $(1\ 2\ 5)$ der gleiche Fall wie $(1\ 2\ 3)$. Wir müssen also nur die Fälle $(1\ 2\ 3)$, $(1\ 2\ 4)$ prüfen.

Fall $(1\ 2\ 3)$: es ist $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(1\ 2\ 3\ 4\ 5)^{-1} = (2\ 3\ 4)$, also $(2\ 3\ 4) \in H$. Nach Teil a) ist $A_4 \leq H$ und daher $4 \mid |H|$.

Fall $(1\ 2\ 4)$: Diesmal ist $(1\ 2\ 3\ 4\ 5)(1\ 2\ 4)(1\ 2\ 3\ 4\ 5)^{-1} = (2\ 3\ 5)$ ein Element von H . Es ist $(1\ 2\ 4)(2\ 3\ 5) = (1\ 2\ 3\ 5\ 4)$. Mit $(1\ 2\ 3\ 5\ 4) = (4\ 1\ 2\ 3\ 5)$ und $(1\ 2\ 4) = (4\ 1\ 2)$ sind wir wieder im Fall $(1\ 2\ 3)$. ■

Wir haben also bewiesen:

Lemma 5.7 *Die Isometriegruppe des Ikosaeders ist isomorph zu $C_2 \times A_5$, aber nicht zu S_5 isomorph.* ■

6 Endliche Gruppen von orthogonalen Transformationen

6.1 Rotationen

Ist P ein reguläres Polyeder, dessen Schwerpunkt im Ursprung liegt, so ist die Isometriegruppe von P eine Untergruppe der Orthogonalgruppe $O(3)$. Diese Untergruppe ist endlich, denn der Homomorphismus von der Isometriegruppe zur symmetrischen Gruppe auf den Ecken ist injektiv, und es gibt nur endlich viele Ecken.

Isometriegruppen regulärer Polyeder sind somit endliche Untergruppen der Orthogonalgruppe $O(3)$. In diesem Kapitel untersuchen wir die endlichen Untergruppen von $O(3)$. Genauer gesagt untersuchen wir die endlichen Untergruppen von $SO(3)$ – nach Lemma 5.4 hat jede Untergruppe von $O(3)$ eine Untergruppe mit Index 1 oder 2, die in $SO(3)$ liegt.

Elemente von $SO(3)$ werden *Rotationen* genannt, da sie Drehungen um eine Achse darstellen (s. Lemma 6.1 unten). Wir werden feststellen, dass jede endliche Gruppe von Rotationen entweder zyklisch ist (Rotationen um eine gemeinsame Achse), oder die Gruppe der Rotationen eines der bekannten regulären Polyeders ist. Dies nehmen wir als Beleg dafür, dass die fünf bekannten regulären Polyeder (Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder) die einzigen sind.

Aus der LAAG1 (Lemma 8.8) ist bekannt, dass jede Matrix $A \in SO(2)$ von der Gestalt $A = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ ist und somit eine Drehung um den Ursprung durch θ darstellt. Außerdem stellt jedes $A \in O(2) \setminus SO(2)$ eine Spiegelung in einer Achse durch den Ursprung dar. Auch Elemente des $SO(3)$ stellen Drehungen dar:

Lemma 6.1 *Sei $E_3 \neq A \in SO(3)$. Dann ist 1 ein Eigenwert von A , und der Eigenraum dazu ist eindimensional. Die Matrix A stellt eine Drehung dar, und dieser Eigenraum ist die Achse der Drehung.*

Hilfssatz Ist λ ein reeller Eigenwert von $A \in O(n)$, so ist $\lambda = \pm 1$, und die geometrische und algebraische Vielfachheiten von λ stimmen miteinander überein.

Beweis. Ist v ein Eigenvektor mit Eigenwert λ , so ist $\|A \cdot v\| = \|v\|$ wegen Orthogonalität, d.h. $\|\lambda v\| = \|v\|$, d.h. $\lambda = \pm 1$. Ist $w \perp v$, dann

$$\langle A \cdot w, v \rangle = \frac{1}{\lambda} \langle A \cdot w, A \cdot v \rangle = \frac{1}{\lambda} \langle w, v \rangle = 0,$$

also ist der Unterraum v^\perp invariant bezüglich A , und A induziert eine orthogonale Transformation des $(n-1)$ -dimensionalen Unterraums v^\perp . Das Ergebnis folgt per Induktion über n . ■

Beweis des Lemmas. Das charakteristische Polynom ist ein reelles Polynom vom Grad 3 und hat somit mindestens eine reelle Nullstelle (Analysis 1). In \mathbb{C} gibt es genau drei Nullstellen, gezählt mit Vielfachheit. Das Produkt der drei Nullstellen ist $\det(A) = 1$. Sind es drei reelle Nullstellen, so sind es $1, 1, 1$ oder $1, -1, -1$. Aber $1, 1, 1$ kommt nur bei $A = E_3$ vor, wegen des Hilfssatzes. Sind es zwei komplexe Nullstellen z_1, z_2 zuzüglich zu λ , so ist $z_2 = \bar{z}_1$, da Nullstellen eines reellen Polynoms. Also $1 = \lambda |z_1|^2$, weshalb $\lambda = +1$.

Somit hat der Eigenwert $+1$ die Vielfachheit 1. Nun sei U das orthogonale Komplement des eindimensionalen Eigenraums. Dann operiert A orthogonal auf U und stellt somit eine Drehung um den Mittelpunkt dar, d.h. um die Achse, die der Eigenraum ist. ■

Lemma 6.2 Sei $G \leq O(2)$ endlich, und sei $H = G \cap SO(2)$. Dann gibt es ein $n \geq 1$ derart, dass H isomorph zu C_n ist und durch die Drehung um $\frac{2\pi}{n}$ erzeugt wird. Ferner ist entweder $G = H \cong C_n$, oder $|G : H| = 2$ und $G \cong D_n$, die Diedergruppe erzeugt durch H und eine Spiegelung.

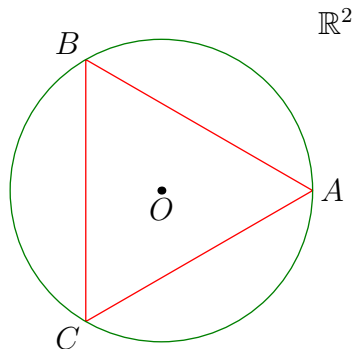
Beweis. Erste Teil: sei $\theta > 0$ der kleinste Winkel, der als eine Drehung in H vorkommt. Dann ist $\theta = \frac{2\pi}{n}$, und $H = \langle \theta \rangle$. Zweite Teil: ist $H < G$, so wähle $\alpha \in G - H = G \setminus SO(2)$. Dann ist $\det(\alpha) = -1$, d.h. α ist eine Spiegelung. Wählt man die Koordinatenachsen so, dass α die Spiegelung in die x -Achse ist, so sieht man: $G \cong D_n$. ■

Bemerkung Wir lernten D_n als Isometriegruppe eines regulären n -Ecks kennen, was $n \geq 3$ voraussetzt. Dieses Lemma liefert die richtige Interpretation für D_2 und D_1 .

6.2 Vorüberlegungen anhand eines Beispiels

Die Klassifikation der endlichen Untergruppen von $SO(3)$ erfolgt durch die Analyse einer ganz bestimmten Gruppenoperation.

Betrachten wir das reguläre Dreieck: im Kreis vom Radius 1 um O in der x, y -Ebene. Im \mathbb{R}^2 lassen sich die Symmetrien $\sigma_a, \sigma_b, \sigma_c$ nur als Spiegelungen aus $O(2) - SO(2)$ verwirklichen.



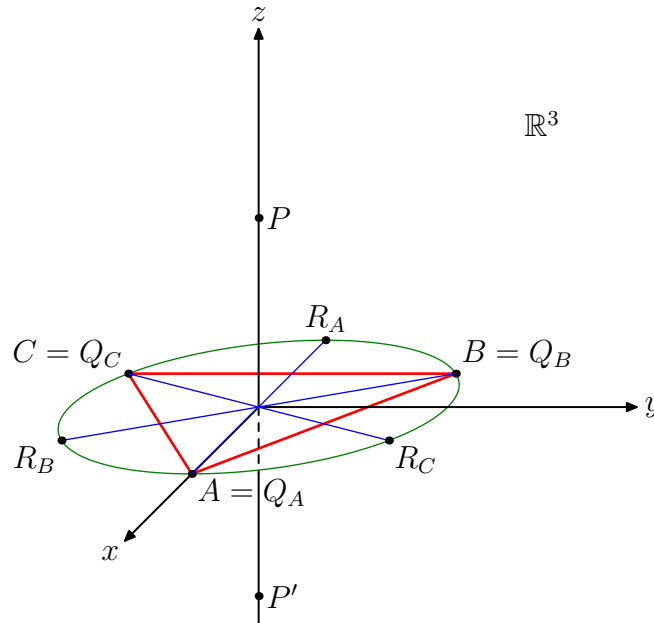
Im \mathbb{R}^3 dagegen lassen sie sich durch Rotationen um π bewirken:

ρ, ρ^2	Drehung um $\frac{2\pi}{3}$ bzw. um $\frac{4\pi}{3}$ um Achse $P'OP$
σ_a	Drehung um π um Achse R_aOQ_a
σ_b	Drehung um π um Achse R_bOQ_b
σ_c	Drehung um π um Achse R_cOQ_c

wobei

$$\begin{aligned}
 P &= (0, 0, 1) & Q_a &= (1, 0, 0) & Q_b &= \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}, 0\right) \\
 Q_c &= \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}, 0\right) & P' &= -P & R_i &= -Q_i
 \end{aligned}$$

Das heißt, wir haben die Isometriegruppe D_3 in $SO(3)$ eingebettet. Sei X die achtelementige Menge $X = \{P, P', Q_a, Q_b, Q_c, R_a, R_b, R_c\}$. Es geht um die Operation von D_3 auf X . Beachten Sie: X ist die Menge aller Vektoren, die die Länge 1 haben und auf Achsen von Rotationen in D_3 liegen.



Lemma 6.3 Sei $G \leq SO(3)$ eine endliche Untergruppe, $G \neq \{E_3\}$. Sei $X \subseteq \mathbb{R}^3$ die Menge

$$\begin{aligned}
 X &:= \{x \in \mathbb{R}^3 \mid \|x\| = 1 \text{ und } x \text{ ist Achse einer Rotation } \in G\} \\
 &\stackrel{L6.1}{=} \{x \in \mathbb{R}^3 \mid \|x\| = 1 \text{ und } \exists E_3 \neq g \in G \text{ mit } gx = x\}.
 \end{aligned}$$

Dann X ist endlich mit $2 \leq |X| \leq 2|G| - 2$; G operiert auf X , d.h. $gx \in X$ für alle $g \in G, x \in X$; und für jedes $x \in X$ ist $|G_x| \geq 2$.

Beweis. Nach der zweiten Definition trägt jedes $E_3 \neq g \in G$ zwei Elemente zu X bei, aber zwei Rotationen können die gleichen Achsenpunkte haben. Ferner enthält jedes G_x mindestens ein $g \neq E_3$, also $|G_x| \geq 2$.

Zur Operation: Sei $x \in X$ und $E_3 \neq g \in G$ mit $gx = x$. Sei $\gamma \in G$, und $y := \gamma x$. Zu zeigen ist: $y \in X$. Nun, $\gamma g \gamma^{-1} \in G$ und $\neq E_3$. Ferner ist $\gamma g \gamma^{-1} y = \gamma g x = \gamma x = y$, also $y \in X$. ■

Man beachte: in unserem Beispiel gibt es drei Bahnen in X : $\{P, P'\}$; $\{Q_a, Q_b, Q_c\}$; $\{R_a, R_b, R_c\}$. Dagegen gibt es nur zwei Bahnen von Achsen, denn Q_a, R_a liegen auf der gleichen Achse.

Als weitere Vorbereitung:

Lemma 6.4 *Sei G eine Gruppe mit vier Elementen. Dann ist G abelsch und zu genau einer der folgenden Gruppen isomorph: $C_4, C_2 \times C_2$ (Kleinsche Vierergruppe).*

Beweis. Element Ordnung 4 genau dann, wenn zyklisch. Sonst alle nicht-neutrale Elemente Ordnung 2. Ist also $g \neq e$ dann $|G : \langle g \rangle| = 2$, daher $\langle g \rangle \triangleleft G$, daher $hgh^{-1} = g$ für jedes $h \in G$: kann nur g, e sein. Also abelsch. Sind g, h zwei verschiedene Elemente $\neq e$, dann ist gh ein weiteres solche Element. Also Vierergruppe. ■

6.3 Die Klassifikation

Die 2. Bahnengleichung *Die endliche Gruppe G operiere auf der endlichen Menge X . Dann gilt*

$$\text{Anzahl der Bahnen} = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

wobei $X^g = \{x \in X \mid gx = x\}$ die Fixpunktmenge von g ist.

Beweis. Die Größe der Menge $Y := \{(g, x) \in G \times X \mid gx = x\}$ kann man auf zwei verschiedene Weisen bestimmen. Zählt man die Anzahl der $x \in X$ für ein gegebenes $g \in G$, so erhält man $|Y| = \sum_{g \in G} |X^g|$. Zählt man dagegen die Anzahl der $g \in G$ für ein gegebene $x \in X$, so erhält man

$$|Y| = \sum_{x \in X} |\text{Stab}_G(x)| = \sum_{x \in X} \frac{|G|}{|\text{Bahn}_G(x)|},$$

und deshalb $\sum_{x \in X} \frac{1}{|\text{Bahn}_G(x)|} = \frac{1}{|G|} \sum_{g \in G} |X^g|$. Andererseits ist $\sum_{x \in X} \frac{1}{|\text{Bahn}_G(x)|}$ die Anzahl der Bahnen. ■

Satz 6.5 *Sei $G \leq SO(3)$ endlich und nichttrivial. Dann tritt genau einer der folgenden Fällen ein:*

- a) $G = C_n$ für ein $n \geq 2$: Rotationen um einer gemeinsamen Achse;
- b) $G = D_n$ für ein $n \geq 2$; Diedergruppe, wie in unserem Beispiel;
- c) $G = A_4$: die Rotationsgruppe des Tetraeders;
- d) $G = S_4$: die Rotationsgruppe des Würfels;
- e) $G = A_5$: die Rotationsgruppe des Ikosaeders.

Beweis. Betrachten wir die Operation von G auf X , wie in Lemma 6.3. Sei N die Anzahl der Bahnen. Für $g \in G$ ist

$$|X^g| = \begin{cases} |X| & g = E_3 \\ 2 & \text{sonst.} \end{cases}$$

Aus der 2. Bahnengleichung folgt also $N = \frac{|X|}{|G|} + \frac{2}{|G|}(|G| - 1)$, d.h.

$$\frac{|X| - 2}{|G|} = N - 2. \quad (*)$$

Da $2 \leq |X| \leq 2|G| - 2$ gilt, ist $0 \leq$ linke Seite < 2 , also $N = 2$ oder 3 .

Schritt 1: Der Fall $N = 2$

Nach Gleichung (*) ist auch $|X| = 2$. Also ist $X = \{v, -v\}$ für ein v . Nach den Überlegungen zu $O(2)$ ist G eine zyklische Gruppe von Rotationen um die Richtung von v .

Schritt 2: Überlegungen zum Fall $N = 3$

Seien x, y, z Vertreter der drei Bahnen. Dann

$$|X| = \frac{|G|}{|G_x|} + \frac{|G|}{|G_y|} + \frac{|G|}{|G_z|}$$

nach der Bahnengleichung, also aus (*) folgt

$$\frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|} = 1 + \frac{2}{|G|}. \quad (**)$$

OBdA wählen wir x, y, z mit $|G_x| \leq |G_y| \leq |G_z|$. Es ist $|G_x| \geq 2$. Ist $|G_x| \geq 3$, dann beträgt die linke Seite von (**) höchstens $\frac{1}{3} + \frac{1}{3} + \frac{1}{3}$, ein Widerspruch. Also $|G_x| = 2$. Ist $|G_y| \geq 4$, dann beträgt die linke Seite höchstens $\frac{1}{2} + \frac{1}{4} + \frac{1}{4}$, ein Widerspruch. Also $|G_y| = 2$ oder $= 3$.

Schritt 3: Der Fall $|G_y| = 2$

Aus (**) wird $|G_z| = \frac{|G|}{2}$. Sei $n = |G_z| \geq 2$, also $|G| = 2n$. Die Bahnen von x, y haben dann Länge n , und die von z hat Länge 2.

Man beachte: für $v \in X$ ist die Bahn von $-v$ die Menge $\{-w \mid w \in \text{Bahn}_G(v)\}$.

Ist $n \geq 3$, so ist $\{z, -z\}$ die Bahn von z , denn $z, -z$ müssen in Bahnen der gleichen Länge liegen. Ist $n = 2$, so besteht jede der drei Bahnen aus 2 Elemente. Ist die Bahn von z nicht $\{z, -z\}$, so ist sie oBdA $\{z, -x\}$. Dann ist aber $\{x, -z\}$ die Bahn von $-z$, übrig bleibt $\{y, -y\}$ als die dritte Bahn. OBdA ist also $\{z, -z\}$ die Bahn von z , auch im Fall $n = 2$.

Diese Gruppe ist die Diedergruppe D_n der Isometrien eines regulären n -Ecks – bzw. für $n = 2$ eines Rechtecks – in der Ebene senkrecht zur z -Richtung, nach Lemma 6.2.

Schritt 4: Der Fall $|G_y| = 3$: nur drei mögliche Werte für $|G|$

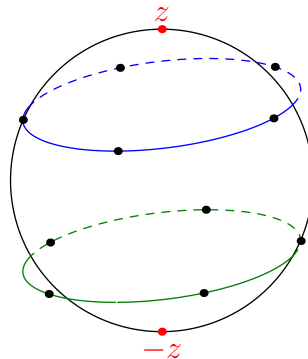
Es ist $\frac{1}{|G_z|} = \frac{1}{6} + \frac{2}{|G|}$. Hier gibt es nur drei Möglichkeiten:

$$|G_z| = 3, |G| = 12 \quad |G_z| = 4, |G| = 24 \quad |G_z| = 5, |G| = 60$$

Schritt 5: Nur die drei bekannten Isometriegruppen möglich

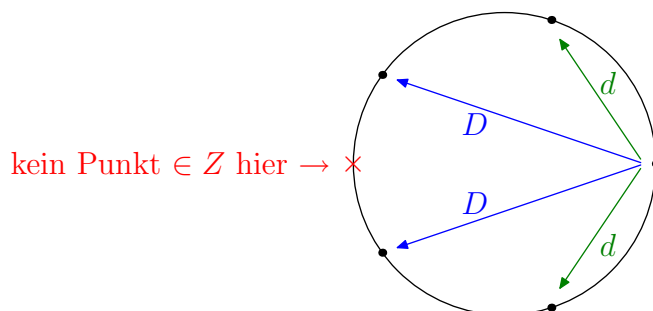
Bei jeder der drei möglichen Gruppenordnungen in Schritt 4 müssen wir zeigen, dass es sich um die bekannte Isometriegruppe handelt. Wir behandeln exemplarisch nur den Fall $|G| = 60$. Hier ist $|G_x| = 2, |G_y| = 3, |G_z| = 5$. Sei Z die Bahn von z . Es ist $|Z| = 12$. Da die drei Bahnen drei verschiedene Längen haben (30 bzw. 20 bzw. 12), gibt: für jedes $v \in X$ liegen $v, -v$ in der gleichen Bahn.

Die Gruppe G_z operiert als eine zyklische Gruppe von Rotationen um die Achse $0z$. Jede Rotation fixiert nur die Punkte auf der Achse, also haben die Bahnen von der Operation von G_z auf X Länge 1 (auf Achse) oder 5 (nicht auf Achse). Es gibt also vier Bahnen: z selbst; $-z$; und zwei 5-elementige Bahnen. Jeder Punkt einer solchen Bahn liegt auf der gleichen Höhe bzgl. dem Nordpol z , und hat auch die gleiche Entfernung von z .



Es gibt also nur drei möglichen Entfernungen von z zu einem anderen $v \in Z$: d für v im oberen Kreis; $d < D < 2$ für v im unteren Kreis; und 2 für $v = -z$. Die Elemente des oberen Kreises nennen wir die Nachbarn von z . Das gleiche mit den gleichen Entfernungen $d, D, 2$ gilt für jedes andere $z' \in Z$.

Sei v im oberen Kreis bzgl. z . Betrachten wir die anderen vier Punkte im Kreis. Die beiden Nachbarn im Kreis müssen die Entfernung d haben, die anderen beiden Punkten müssen die Entfernung D haben.



Die 5 Nachbarn von v sind also z , zwei Nachbarn im oberen z -Kreis, und zwei Punkte aus dem unteren z -Kreis. Also kommt z zwischen den beiden Nachbarn im oberen z -Kreis. Somit ist das Dreieck zwischen z und zwei benachbarte Punkte im oberen Kreis gleichseitig mit Kantenlänge d . Um jeden Punkt $v \in Z$ gibt es 5 solche gleichseitige Dreiecke. Das Ikosaeder liegt vor. Die Punkte in der Bahn von y sind die Flächenmittelpunkte; die Punkte in der Bahn von x sind die Kantenmittelpunkte. ■

Übungsaufgabe Machen Sie das gleiche für die anderen beiden Gruppen. Identifizieren Sie beim Tetraeder die drei verschiedenen Bahnen von Achsenpunkten.

7 Konjugation und einfache Gruppen

7.1 Konjugationsklassen

Zur Erinnerung Sei G eine Gruppe. Konjugation ist die Operation von G auf sich selbst gegeben durch $(g, x) \mapsto gxg^{-1}$.

Bezeichnung Bahnen bzgl. Konjugation heißen *Konjugationsklassen*.

Lemma 7.1 a) Sei G eine Gruppe und $g \in G$. Die Abbildung $c_g: G \rightarrow G$, $c_g(h) := ghg^{-1}$ ist ein Gruppenhomomorphismus. Ist $H \triangleleft G$, so ist ferner $c_g: H \rightarrow H$ ein Homomorphismus.

- b) Genau dann ist die Untergruppe $H \leq G$ ein Normalteiler in G , wenn H eine Vereinigung von Konjugationsklassen ist.
- c) Für $\sigma, \pi \in S_n$ berechnet man $\pi\sigma\pi^{-1}$ aus der disjunkten Zykel-Zerlegung von σ , indem man π auf jedem Zykeleintrag anwendet.
- d) Zwei Permutationen $\sigma, \tau \in S_n$ liegen genau dann in der gleichen Konjugationsklasse, wenn sie vom gleichen Typ sind.

Beweis. a) Wegen $G \triangleleft G$ reicht es, den zweiten Teil zu zeigen. Wegen $H \triangleleft G$ ist $c_g(h) \in H$ für alle $h \in H$, $g \in G$. Außerdem ist $c_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = c_g(h_1)c_g(h_2)$.

- b) Genau dann ist $H \triangleleft G$, wenn $ghg^{-1} \in H$ ist für alle $g \in G$, $h \in H$.
- c) Wegen Teil a) reicht es, den Fall $\sigma = (a_1 \ a_2 \ \dots \ a_r)$ ein r -Zykel zu behandeln. Ist $b \notin \{\pi(a_1), \dots, \pi(a_r)\}$, so ist $\pi^{-1}(b) \notin \{a_1, \dots, a_r\}$, daher $\sigma\pi^{-1}(b) = \pi^{-1}(b)$ und $\pi\sigma\pi^{-1}(b) = b$. Für $b = \pi(a_i)$ ist $\pi\sigma\pi^{-1}(b) = \pi\sigma(a_i) = \pi(a_{i+1})$, bzw. $\pi(a_1)$ falls $i = r$. Also $\pi\sigma\pi^{-1} = (\pi(a_1) \ \dots \ ; \ \pi(a_r))$.
- d) Wegen c) haben konjugierte Permutationen den gleichen Typ. Umgekehrt seien $\sigma, \tau \in S_n$ zwei Permutationen vom gleichen Typ. Schreiben wir die disjunkten Zykel-Zerlegungen von σ, τ hin, jeweils mit den längsten Zykeln vorne und den kleinsten Zykeln (diesmal einschl. 1-Zykeln!) hinten. Jetzt die Zykel-Klammer wegradieren. Wir erhalten zwei Zahlenreihen: eine für σ , eine für τ . Jede Reihe enthält die Zahlen $1, \dots, n$ in irgendeiner Reihenfolge. Es gibt genau eine Permutation $\pi \in S_n$, die für jedes r die r te Zahl in der σ -Reihe auf der r ten Zeile in der τ -Reihe abbildet. Dann ist $\pi\sigma\pi^{-1} = \tau$ nach Teil c) und unserer Konstruktion. ■

Beispiele Beispiele zu Teil c) und zum Beweis von Teil d).

7.2 Das Zentrum und ein Satz von Cauchy

Einfache Betrachtungen über die Länge von Konjugationsklassen führen zu einigen interessanten Ergebnissen.

Definition Das Zentrum $Z(G)$ einer Gruppe G ist die Teilmenge

$$Z(G) := \{g \in G \mid hg = gh \forall h \in G\}.$$

Lemma 7.2 $Z(G) \triangleleft G$.

Beweis. Genau dann ist $g \in Z(G)$, wenn $ghg^{-1} = h$ ist für jedes $h \in G$. Das heißt, $Z(G)$ ist der Kern des Homomorphismus $G \rightarrow S(G)$, der durch die Konjugation-Operation induziert wird (vgl. Lemma 4.1). Kerne sind Normalteiler. ■

Beispiele Ist G abelsch, so ist $Z(G) = G$. Es ist $Z(S_3) = \{\text{Id}\}$. Für $D_4 = \{\text{Id}, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ mit $\sigma^2 = \rho^4 = \text{Id}$ und $\sigma\rho\sigma = \rho^3$ ist $Z(D_4) = \{\text{Id}, \rho^2\}$.

Definition Sei p eine Primzahl. Ist G eine endliche Gruppe mit $|G| = p^n$ für ein $n \geq 0$, so heißt G eine (endliche) p -Gruppe.

Beispiele Für jede Primzahl p ist die zyklische Gruppe C_p eine p -Gruppe. Die Gruppe $S_3 \cong D_3$ ist keine p -Gruppe. Die Gruppe D_4 ist eine 2-Gruppe, denn $|D_4| = 2^3$. Es ist Geschmackssache, ob die triviale Gruppe $G = \{e\}$ als eine p -Gruppe gezählt wird oder nicht.

Lemma 7.3 Sei G eine p -Gruppe (endlich, nichttrivial). Dann ist das Zentrum $Z(G)$ nicht trivial: $Z(G) > \{e\}$.

Beweis. Es ist $|G| = p^n$ mit p prim und $n \geq 1$. Betrachten wir die Operation von G auf sich selbst durch Konjugation. Die Summe der Bahnlängen beträgt $|G| = p^n$ und ist durch p teilbar. Jede Bahnlänge teilt p^n wegen der Bahnengleichung, und ist daher entweder 1 oder durch p teilbar. Es folgt, dass die Anzahl der Bahnen, deren Länge 1 beträgt, durch p teilbar sein muss. Eine solche Bahn ist $\{e\}$. Somit gibt es mindestens $p \geq 2$ solche Bahnen. Aber $g \in Z(G)$ genau dann, wenn $\{g\}$ eine Bahn ist. ■

Augustin-Louis Cauchy (1789–1857) ist eher für seine Beiträge zur Analysis bekannt, hat aber auch in der Gruppentheorie gewirkt.

Lemma 7.4 (Der Satz von Cauchy) Sei p eine Primzahl und G eine endliche Gruppe mit $p \mid |G|$. Dann hat G mindestens eine Untergruppe, die zyklisch der Ordnung p ist.

Beweis. Induktion über $|G|$. Induktionsanfang: nach Lemma 3.2 ist jede Gruppe der Ordnung p zyklisch. Nun sei $|G| > p$, und das Lemma gelte für alle Gruppen H mit $|H| < |G|$.

Schritt 1: Der Fall $\exists g \in G$ mit $p \mid o(g)$

Angenommen es gibt ein $g \in G$ mit $p \mid m := o(g)$. Dann hat $g^{\frac{m}{p}}$ Ordnung p und erzeugt daher eine zyklische Untergruppe der Ordnung p . Fertig.

Schritt 2: Der Fall $Z(G) \neq \{e\}$ (einschl. der Fall G abelsch)

Wähle $e \neq g \in Z(G)$. Sei $m = o(g)$ und $H = \langle g \rangle$. Dann $|H| = m$ und $H \triangleleft G$. Es ist $p \nmid m$, sonst würde Schritt 1 eintreten. Also teilt p die Ordnung der Quotientengruppe G/H . Nach der Induktionsannahme gibt es $\gamma \in G$ derart, dass $\gamma H \in G/H$ eine zyklische Untergruppe der Ordnung p erzeugt. Also $\gamma \notin H$, aber $\gamma^p \in H$. Somit ist $p \mid o(\gamma) \mid pm$. Fertig nach Schritt 1.

Schritt 3: Der Fall $Z(G) = \{e\}$

Die Summe der Längen der Konjugationsklassen beträgt $|G|$ und ist daher durch p teilbar. Es gibt genau eine Konjugationsklasse der Länge 1, nämlich $\{e\}$. Da p prim ist, muss es also mindestens ein $g \in G$ geben, deren Konjugationsklasse-Länge sowohl ≥ 2 als auch durch p nicht teilbar ist. Das heißt, der Stabilisator von g ist eine echte Untergruppe von G , deren Ordnung durch p teilbar ist. Nach der Induktionsannahme enthält der Stabilisator eine zyklische Untergruppe der Ordnung p . ■

Beispiel In der Gruppe $GL_3(\mathbb{F}_2)$ gibt es ein Element der Ordnung 7, denn die Ordnung der Gruppe beträgt $7 \cdot 6 \cdot 4$. Das heißt, es gibt eine (3×3) -Matrix A mit Einträgen aus \mathbb{F}_2 derart, dass $A^7 = E_3$, $A \neq E_3$.

Lemma 7.5 Sei k ein endlicher Körper mit q Elementen.

a) Ist V ein n -dimensionaler k -Vektorraum, so hat V genau q^n Elemente.

b) Für $n \geq 0$ ist $|GL_n(k)| = \prod_{r=0}^{n-1} (q^n - q^r)$.

c) Für $n \geq 1$ ist $|SL_n(k)| = \frac{1}{q-1} \prod_{r=0}^{n-1} (q^n - q^r)$.

Bemerkung Man kann nachweisen (Übungsaufgabe!), dass q eine Primpotenz sein muss. Außerdem kann man nachweisen, dass k durch q eindeutig bestimmt ist. Daher schreibt man häufig $GL_n(q)$ für $GL_n(k)$, und $SL_n(q)$ für $SL_n(k)$.

Beweis. a) Sei v_1, \dots, v_n eine Basis von V . Jedes $v \in V$ ist auf genau einer Weise eine Linearkombination von v_1, \dots, v_n . Und es gibt genau q^n Möglichkeiten für die Koeffizienten bei einer solchen Linearkombination.

- b) Die Vektoren Av_1, \dots, Av_n bestimmen eine Matrix $A \in GL_n(k)$ eindeutig. Die einzige Bedingung auf diesen Vektoren ist, dass sie linear unabhängig sein sollten. Für Av_1 gibt es $q^n - 1$ Möglichkeiten: alles außer der Nullvektor. Sind Av_1, \dots, Av_r bereits gewählt, so gibt es $q^n - q^r$ Möglichkeiten für Av_{r+1} : alles außerhalb des r -dimensionalen Unterraums $\text{Spann}(Av_1, \dots, Av_r)$.
- c) Für $n \geq 1$ ist die Determinante ein surjektiver Homomorphismus von $GL_n(k)$ nach der multiplikativen Gruppe $k^* = k \setminus \{0\}$: surjektiv wegen $A = \text{diag}(x, 1, \dots, 1)$ für beliebiges $x \in k^*$. Der Kern ist $SL_n(k)$. ■

Bemerkung Allgemeiner besagt der Satz von Sylow, dass eine Gruppe der Ordnung $p^d m$ mit $p \nmid m$ mindestens eine Untergruppe der Ordnung p^d enthält. Somit enthält jede Gruppe der Ordnung 72 Untergruppen der Ordnungen 8 und 9.

7.3 Die Gruppe A_5 ist einfach

Lemma 7.6 *In der alternierenden Gruppe A_5 gibt es genau 5 Konjugationsklassen:*

- *Das neutrale Element;*
- *Alle 3-Zykel (20 Stück);*
- *Alle Permutationen vom Typ 2^2 , d.h. vom Typ $(a\ b)(c\ d)$ (15 Stück)*
- *Zwei verschiedene Konjugationsklassen von je zwölf 5-Zykeln. Ist σ ein 5-Zykel, so ist $\sigma \sim \sigma^{-1}$, $\sigma \not\sim \sigma^2$.*

Bezeichnung Der Zentralisator $C_G(g)$ eines Elements $g \in G$ ist $C_G(g) = \{h \in G \mid hg = gh\}$. Dies ist der Stabilisator $\text{Stab}_G(g)$ bzgl. der Konjugationsoperation. Also $C_G(g) \leq G$, und

$$|G| = |\text{Konjugationsklasse von } g| \cdot |C_G(g)| .$$

Beweis. Ist $\sigma \in A_5$ ein 3-Zykel, so gibt es $\pi \in S_5$ mit $\pi(1\ 2\ 3)\pi^{-1} = \sigma$. Das gleiche gilt, wenn man π durch $\pi(4\ 5)$ ersetzt. Eins von diesen beiden ist gerade. Das gleiche gilt mit $\sigma = (a\ b)(c\ d)$, $(1\ 2)(3\ 4)$ und $\pi(1\ 2)$.

Es gibt 24 5-Zykel in S_5 . Alle sind dort konjugiert, also ist $|C_{S_5}(\sigma)| = 5$ für $\sigma \in S_5$ ein 5-Zykel. Also $C_{S_5}(\sigma) = \langle \sigma \rangle \leq A_5$. Folglich hat die Konjugationsklasse von σ in A_5 die Länge 12.

Für $\sigma = (a\ b\ c\ d\ e)$ ist $\pi\sigma\pi^{-1} = \sigma^{-1}$ für $\pi = (b\ e)(c\ d) \in A_5$, und $\pi\sigma\pi^{-1} = (a\ c\ e\ b\ d) = \sigma^2$ für $\pi = (b\ c\ e\ d) \notin A_5$. Der Zentralisator liegt in A_5 , also ist $\sigma \not\sim \sigma^2$ in A_5 . ■

Definition Eine Gruppe G heißt *einfach*, wenn es genau zwei Normalteiler gibt: $\{e\}$ und G selbst.

Beispiel C_p

Satz 7.7 *Die Gruppe A_5 ist einfach.*

Beweis. Sei $H \triangleleft A_5$ ein Normalteiler mit $H \neq A_5$. Es ist H eine Vereinigung von Konjugationsklassen. Keine 3-Zykel dürfen vorkommen, wegen Lemma 5.2. Wegen $(1\ 2)(4\ 5) \cdot (1\ 3)(4\ 5) = (1\ 3\ 2)$ darf auch nichts von der Gestalt 2^2 vorkommen. Somit können nur Id (zwangsweise) und 5-Zykeln vorkommen. Somit ist $|H| \in \{1, 13, 25\}$. Von diesen ist nur 1 ein Teiler von $|A_5| = 60$. ■

8 Möbiustransformationen

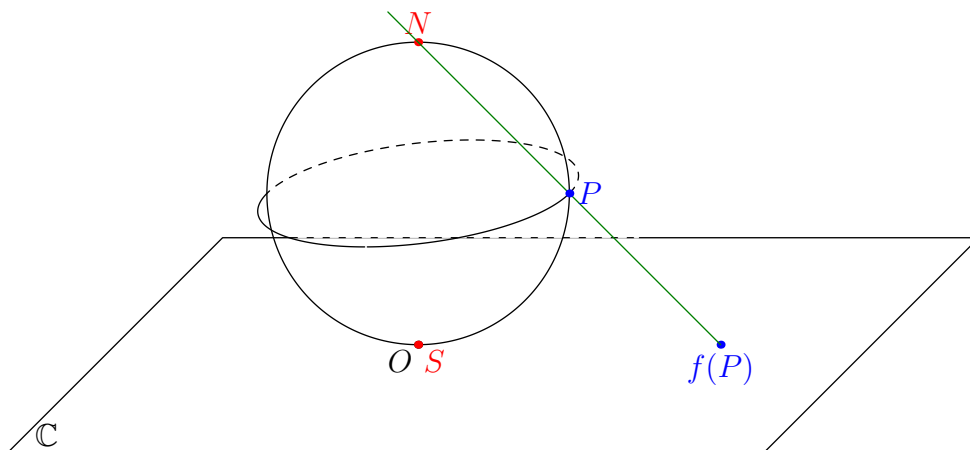
1. *Definition* Seien $a, b, c, d \in \mathbb{C}$ mit $ad - bc \neq 0$. Die Funktion

$$f(z) = \frac{az + b}{cz + d}$$

heißt eine *Möbiustransformation*. $\mathbb{C} \cup \{\infty\}$ ist Definitions- und Wertebereich. Für $c = 0$ ist $f(\infty) = \infty$; für $c \neq 0$ ist $f(-\frac{d}{c}) = \infty$, $f(\infty) = \frac{a}{c}$.

8.1 Die Riemannsche Zahlenkugel

Identifizieren wir die komplexe Ebene mit der Ebene $z = 0$ des \mathbb{R}^3 . Betrachten wir die Sphäre⁵ \mathcal{S} vom Radius 1 mit Mittelpunkt $(0, 0, 1)$.



Sei $N = (0, 0, 2)$, der „Nordpol“ der Sphäre. Nun sei $P \in \mathcal{S}$ mit $P \neq N$. Dann trifft die Gerade NP die komplexe Ebene in genau einem Punkt $=: f(P)$. So erhalten wir eine Abbildung $f: \mathcal{S} \setminus \{N\} \rightarrow \mathbb{C}$. Insbesondere ist $f(S) = 0$ für den „Südpol“ $S = (0, 0, 0)$. Diese Abbildung ist stetig: es ist

$$f(x, y, z) = \frac{2}{2 - z}(x + iy),$$

mit $z < 2$ da $P \neq N$. Sie ist eine Bijektion, und die Umkehrabbildung

$$f^{-1}(x + iy) = \frac{1}{x^2 + y^2 + 4}(4x, 4y, 2(x^2 + y^2))$$

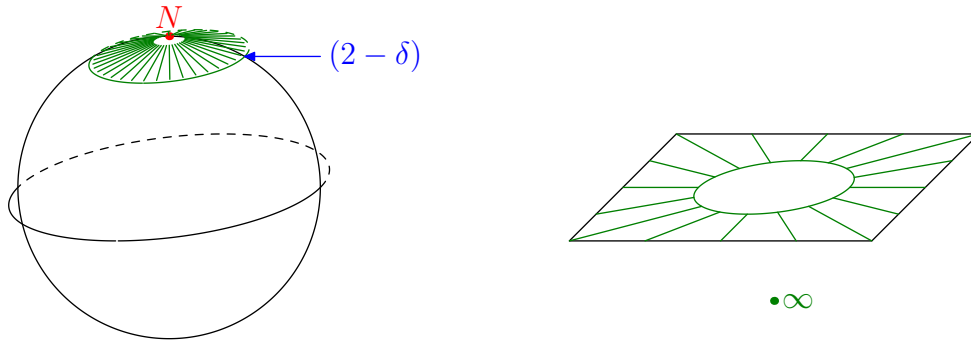
ist auch stetig. Ferner gilt: desto näher P zu N ist, desto größer ist $|f(P)|$. Also kann man \mathbb{C} mit einer Sphäre minus einem Punkt identifizieren.

Definition Aus diesem Grund kann man die Menge $\mathbb{C} \cup \{\infty\}$ als eine Sphäre betrachten. Name: die *Riemannsche Zahlenkugel*.

⁵Kugeloberfläche

Bemerkung Hier ist ∞ bloß ein Symbol, die den Punkt N entspricht wenn man $z \in \mathbb{C}$ mit $f^{-1}(z) \in \mathcal{S}$ identifiziert. Von $+\infty$ und $-\infty$ zu reden wäre in diesem Zusammenhang unangebracht, von $i\infty$ erst recht.

Bemerkung Man kann auch Analysis auf der Riemannschen Zahlenkugel treiben (Funktionentheorie). Die ε -Umgebungen von ∞ sind die Mengen $\{\infty\} \cup \{z \in \mathbb{C} \mid |z| > K\}$.



8.2 Die Riemannsche Zahlenkugel als ein projektiver Raum

Projektive Räume kennen wir aus LAAG2 §20. Sei V ein k -Vektorraum, und $v, w \in V \setminus \{0\}$. Wir setzen $v \sim w$ falls es $\lambda \in k$ gibt mit $v = \lambda w$, zwangsweise ist $\lambda \neq 0$. Dies ist eine Äquivalenzrelation, wir schreiben $[v]$ für die Äquivalenzklasse von $0 \neq v \in V$. Der projektive Raum $P(V)$ ist die Menge $P(V) = \{[v] \mid 0 \neq v \in V\}$ aller eindimensionalen Untervektorräume von V .

Für $V = k^{n+1}$ schreiben wir $(x_0 : x_1 : \dots : x_n) = [(x_0, x_1, \dots, x_n)]$ („homogene Koordinaten“). Insbesondere ist

$$P_1(k) = \{(z : 1) \mid z \in k\} \cup \{(1 : 0)\},$$

also steht $P_1(k)$ in Bijektion mit $k \cup \{\infty\}$. Insbesondere steht $P_1(\mathbb{C})$ in Bijektion mit $\mathbb{C} \cup \{\infty\}$: es ist

$$(z : w) = \begin{cases} (\frac{z}{w} : 1) & w \neq 0 \\ (1 : 0) & w = 0 \end{cases}.$$

Es gibt also eine Bijektion zwischen $P_1(\mathbb{C})$ und der Riemannschen Zahlenkugel, die z auf $(z : 1)$ und ∞ auf $(1 : 0)$ abbildet. Ab jetzt bezeichnen wir die Riemannsche Zahlenkugel mit $P_1(\mathbb{C})$.

8.3 Möbiustransformationen und Projektivitäten

Ist $F: V \rightarrow V$ ein Automorphismus (d.h. ein invertierbarer Endomorphismus), so gilt $v \sim w \Rightarrow F(v) \sim F(w)$. Durch $\bar{F}([v]) := [F(v)]$ induziert also F eine wohldefinierte Abbildung $\bar{F}: P(V) \rightarrow P(V)$.

Definition Eine solche Abbildung $\bar{F}: P(V) \rightarrow P(V)$ heißt eine *Projektivität* von $P(V)$.

Es ist $\bar{F}\bar{G} = \overline{FG}$, also $(\bar{F})^{-1} = \overline{F^{-1}}$: Projektivitäten sind invertierbar, und sie bilden eine Gruppe bzgl. Verknüpfung.

Für $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ entspricht die Möbiustransformation $f_A(z) = \frac{az+b}{cz+d}$ der Projektivität $\bar{A}(z:w) = (az+bw : cz+dw)$ des $P_1(\mathbb{C})$: denn

$$\bar{A}(z:1) = (az+b : cz+d) = \begin{cases} \left(\frac{az+b}{cz+d} : 1\right) & cz+d \neq 0 \\ (1:0) & cz+d = 0 \end{cases}$$

$$\bar{A}(1:0) = (a:c) = \begin{cases} \left(\frac{a}{c} : 1\right) & c \neq 0 \\ (1:0) & c = 0 \end{cases}$$

Die Produktregel $f_A f_B = f_{AB}$ folgt jetzt aus $\bar{A}\bar{B} = \overline{AB}$. Ohne den Umweg der Projektivitäten müssen viele Spezialfälle geprüft werden.

8.4 Möbiustransformationen als eine Quotientengruppe

2. *Definition* Eine Möbiustransformation ist eine Projektivität des $P_1(\mathbb{C})$.

Lemma 8.1 a) Jede Möbiustransformation ist eine Bijektion von der Riemannschen Zahlenkugel $P_1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ nach sich selbst.

b) Die Möbiustransformationen bilden eine Gruppe bezüglich Verknüpfung.

c) Die Gruppe der Möbiustransformationen ist isomorph zu einer Quotientengruppe von $GL_2(\mathbb{C})$ und zu einer Quotientengruppe von $SL_2(\mathbb{C})$.

Beweis. Die ersten beiden Teile haben wir oben nachgewiesen, der erste Teil von c) auch. Für $0 \leq \lambda$ erfüllt die Skalarmatrix $B_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ die Gleichungen $\det(B_\lambda) = \lambda^2$ und $f_{B_\lambda} = \text{Id}$. Mit λ eine Quadratwurzel von $\det(A)^{-1}$ ist daher $AB_\lambda \in SL_2(\mathbb{C})$ und $f_{AB_\lambda} = f_A$. ■

Lemma 8.2 a) $f_A = \text{Id}$ genau dann, wenn A eine Skalarmatrix $A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ ist.

b) Für jede der Gruppen $G = GL_2(\mathbb{C}), GL_2(\mathbb{R}), SL_2(\mathbb{C}), SL_2(\mathbb{R})$ und $O(2)$ gilt:

$$Z(G) = \{A \in G \mid A \text{ eine Skalarmatrix}\}.$$

Beweis. a) $\frac{az+b}{cz+d} = z$ ausmultiplizieren, Koeffizientenvergleich.

b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SO(2)$ kommutieren: $d = a, b = -c$. Kommutiert man dann $\begin{pmatrix} a & -c \\ c & a \end{pmatrix}$ mit $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ für $x \neq y$, so erhält man $c = 0$. Solche Matrizen sind $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O(2)$ und $\begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \in SL_2(\mathbb{R})$. ■

Definition Die projektive spezielle lineare Gruppe $PSL_n(k)$ ist per Definition die Quotientengruppe $SL_n(k)/Z(SL_n(k))$. Analog definiert man die projektive allgemeine lineare Gruppe $PGL_n(k)$ als $GL_n(k)/Z(GL_n(k))$.

Korollar 8.3 Die Gruppe der Möbiustransformationen ist isomorph zu $PSL_2(\mathbb{C})$ und zu $PGL_2(\mathbb{C})$.

Beweis. Folgt aus Lemma 8.2 und Lemma 8.1. ■

Bezeichnung Die Gruppe der Möbiustransformationen bezeichnen wir daher mit $PSL_2(\mathbb{C})$.

Bei den Möbiustransformationen geht es also um eine Operation von $PSL_2(\mathbb{C})$ auf $P_1(\mathbb{C})$.

Bemerkung $PSL_2(\mathbb{R})$ kann als eine Untergruppe von $PSL_2(\mathbb{C})$ betrachtet werden: wichtig für die hyperbolische Geometrie.

Lemma 8.4 Die Gruppe der Möbiustransformationen wird erzeugt durch Transformationen der drei Arten $f(z) = \frac{1}{z}$, $f(z) = z + b$ ($b \in \mathbb{C}$) und $f(z) = az$ ($0 \neq a \in \mathbb{C}$).

Beweis. Klar für $c = 0$. Für $c \neq 0$ ist

$$f(z) = \frac{a}{c} + \frac{bc - ad}{c(cz + d)}.$$
■

8.5 Drei Punkte

Lemma 8.5 Seien $\{P_1, P_2, P_3\}$ und $\{Q_1, Q_2, Q_3\}$ zwei dreielementige Teilmengen des $P_1(\mathbb{C})$. Dann gibt es genau eine Möbiustransformation f mit $f(P_i) = Q_i$ für alle $1 \leq i \leq 3$.

Zusatz: Sind die P_i, Q_j alle reell, d.h. der Art $(x : y)$ mit $x, y \in \mathbb{R}$, so liegt $f \in PGL_2(\mathbb{R})$.

Beweis. Seien $v_1, v_2, v_3 \in \mathbb{C}^2$ mit $P_i = [v_i]$. Da die Punkte P_i verschieden sind, sind keine zwei v_i linear abhängig: insbesondere gibt es $\alpha, \beta \neq 0$ mit $v_3 = \alpha v_1 + \beta v_2$. Ersetzen wir v_1 durch αv_2 und v_2 durch βv_2 , so ist oBdA $v_3 = v_1 + v_2$, d.h. $P_3 = [v_1 + v_2]$. Analog wählen wir $u_1, u_2 \in \mathbb{C}^2$ mit $Q_1 = [u_1]$, $Q_2 = [u_2]$ und $Q_3 = [u_3]$ für $u_3 = u_1 + u_2$. Sind die P_i alle reell, so wählen wir $v_1, v_2, v_3 \in \mathbb{R}^2$, dann sind $\alpha, \beta \in \mathbb{R}$, also oBdA $v_3 = v_1 + v_2$ und alle drei Vektoren reell. Analog wählen wir u_1, u_2 und $u_3 = u_1 + u_2$ alle reell, falls die Q_i alle reell sind.

Eine Möbiustransformation der gesuchten Sorte entspricht einem Automorphismus F des \mathbb{C}^2 derart, dass $F(v_i)$ ein Skalarvielfaches von u_i ist $\forall i$ (für $u_3 = u_1 + u_2$). Ein solcher wird mittels linearer Fortsetzung eindeutig definiert durch $F(v_1) = u_1$, $F(v_2) = u_2$. Sind die v_i und die u_i reell, so ist die Matrix von F reell, denn die Basiswechselfmatrizen zwischen der Standardmatrix und den beiden Basen v_1, v_2 und u_1, u_2 sind reell.

Ist G ein zweiter solcher Automorphismus, dann aus $[G(v_1)] = [u_1]$ folgt, dass es ein $\lambda \neq 0$ gibt mit $G(v_1) = \lambda u_1$; analog gibt es $\mu, \nu \neq 0$ mit $G(v_2) = \mu u_2$ und $G(v_1 + v_2) = \nu(u_1 + u_2)$. Also $\nu(u_1 + u_2) = \lambda u_1 + \mu u_2$, d.h. $\mu = \nu = \lambda$ und $G = \lambda F$, was die gleiche Möbiustransformation induziert. ■

Bemerkung Eine Möbiustransformation f ist also eindeutig definiert durch das Tripel $f(0), f(1), f(\infty)$; und jedes Tripel von paarweise verschiedenen Elementen von $P_1(\mathbb{C})$ kommt so vor.

Beispiel Aufgabe: man bestimme die Möbiustransformation, die $f(0) = 2i$, $f(1) = -1$ und $f(\infty) = \frac{1}{2}$ erfüllt. Welchen Wert nimmt $f(-1)$ an? Für welches z ist $f(z) = \infty$?

Lösung: Aus $f(\infty) = \frac{1}{2}$ folgt $f(z) = \frac{z+b}{2z+d}$. Aus $f(0) = 2i$ folgt dann $f(z) = \frac{z+2id}{2z+d}$. Aus $f(1) = -1$ folgt dann $\frac{1+2id}{2+d} = -1$, also $1 + 2id = -2 - d$, also $(1 + 2i)d = -3$, also $5d = -3(1 - 2i)$. Es ist also

$$f(z) = \frac{5z + 12 - 6i}{10z - 3 + 6i};$$

$$f(-1) = \frac{7-6i}{6i-13} = \frac{1}{205}(7-6i)(13+6i) = \frac{127-36i}{205}; \text{ und } f^{-1}(\infty) = -\frac{d}{2} = \frac{6i-3}{10}.$$

8.6 Möbiustransformationen und Kreise

Wir werden sehen, dass Möbiustransformationen Kreise auf Kreise abbilden. Wir benötigen aber eine Sonderregelung für den Punkt ∞ .

Beispiel Was passiert mit dem Einheitskreis $\{z \mid |z| = 1\}$ unter $f(z) = \frac{z-1}{z+1} \in PSL_2(\mathbb{C})$?

Es ist $f(1) = 0$, $f(i) = i$, $f(-i) = -i$: diese liegen alle auf der Gerade $\Re(z) = 0$. Außerdem ist $f(-1) = \infty$. Allgemeiner gilt für $z \neq -1$ mit $z\bar{z} = 1$:

$$f(z) = \frac{(z-1)(\bar{z}+1)}{(z+1)(\bar{z}+1)} = \frac{z-\bar{z}}{2+z+\bar{z}} = \frac{\Im(z)}{1+\Re(z)}i.$$

Somit bildet f den Einheitskreis auf der Gerade $\Re(z) = 0$ zzgl. ∞ bijektiv ab (Grenzwertverhalten für $z \rightarrow -1$ betrachten).

1. Definition Ein Kreis in $\mathbb{C} \cup \{\infty\}$ ist entweder ein gewöhnlicher Kreis in \mathbb{C} , oder eine Gerade in \mathbb{C} zzgl. den Punkt ∞ .

Es gibt eine zweite Definition, die (fast) ohne Fallunterscheidung auskommt. Zur Erinnerung (LAAG1, insbes. Lemma 8.2): eine Matrix $A \in M_n(\mathbb{C})$ heißt *hermitesch*, falls $A^H = A$ gilt, wobei $A^H \in M_n(\mathbb{C})$ durch $A_{ij}^H = \overline{A_{ji}}$ definiert ist. Die hermiteschen Matrizen aus $M_2(\mathbb{C})$ sind die der Gestalt $\begin{pmatrix} x & a \\ \bar{a} & y \end{pmatrix}$ mit $x, y \in \mathbb{R}$.

2. *Definition* Sei $A = \begin{pmatrix} x & a \\ \bar{a} & y \end{pmatrix}$ eine invertierbare hermitesche Matrix. Sofern die Lösungsmenge

$$K_A := \{(z : w) \in P_1(\mathbb{C}) \mid xz\bar{z} + a\bar{z}w + \bar{a}z\bar{w} + yw\bar{w} = 0\}$$

nicht leer ist, heißt sie ein *Kreis* in $P_1(\mathbb{C})$.

Beispiel $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist hermitesch und invertierbar. Diese Matrix entspricht der Gleichung $z\bar{z} + w\bar{w} = 0$, die nur für $z = w = 0$ und daher für kein $(z : w) \in P_1(\mathbb{C})$ lösbar ist.

Bemerkung Diese zweite Definition macht Sinn: Ist $(z' : w') = (z : w)$ dann gibt es $0 \neq \lambda \in \mathbb{C}$ mit $z' = \lambda z$, $w' = \lambda w$. Also

$$xz'\bar{z}' + a\bar{z}'w' + \bar{a}z'\bar{w}' + yw'\bar{w}' = |\lambda|^2 (xz\bar{z} + a\bar{z}w + \bar{a}z\bar{w} + yw\bar{w}),$$

und daher $(z : w) \in K_A \iff (z' : w') \in K_A$.

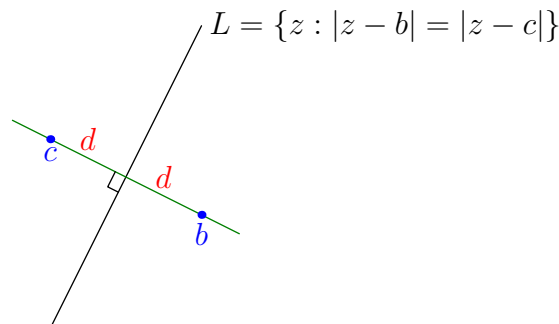
Lemma 8.6 *Beide Definitionen sind äquivalent.*

Beweis. Der Kreis mit Radius $r > 0$ und Mittelpunkt $b \in \mathbb{C}$ ist gegeben durch $|z - b| = r$, d.h. $(z - b)(\bar{z} - \bar{b}) = r^2$, d.h. $z\bar{z} - b\bar{z} - \bar{b}z + (b\bar{b} - r^2) = 0$. Wechselt man zu homogenen Koordinaten $(z : w)$, so hat man

$$z\bar{z} - b\bar{z}w - \bar{b}z\bar{w} + yw\bar{w} = 0$$

für $y = |b|^2 - r^2$: für $(z : w) = (z : 1)$ und $(1 : 0)$ prüfen! Dies ist K_A für $A = \begin{pmatrix} 1 & -b \\ -\bar{b} & |b|^2 - r^2 \end{pmatrix}$. Determinante $-r^2$, also invertierbar.

Sei $b \neq c \in \mathbb{C}$. Die Menge $\{z \mid |z - b| = |z - c|\}$ ist eine Gerade, und jede Gerade lässt sich so beschreiben.



Also $(z - b)(\bar{z} - \bar{b}) = (z - c)(\bar{z} - \bar{c})$, also $\overline{(c - b)}z + (c - b)\bar{z} + (|c|^2 - |b|^2) = 0$. Für homogene Koordinaten heißt das $\overline{(c - b)}z\bar{w} + (c - b)\bar{z}w + (|c|^2 - |b|^2)w\bar{w} = 0$, was – wie erwünscht – den Punkt $(1 : 0)$ der Lösungsmenge hinzufügt. Mit $a = c - b$ und $y = |c|^2 - |b|^2 \in \mathbb{R}$ liegt hier K_A für $A = \begin{pmatrix} 0 & a \\ \bar{a} & y \end{pmatrix}$ vor: offensichtlich hermitesch, und invertierbar wegen $b \neq c$.

Umgekehrt sei $A = \begin{pmatrix} x & a \\ \bar{a} & y \end{pmatrix}$ invertierbar und hermitesch, und K_A sei nicht leer. 1. Fall $x = 0$: Es ist $a \neq 0$. Sei $\lambda \in \mathbb{C}$ gegeben durch $(2\lambda + 1)|a|^2 = y$. Dann mit $c = (\lambda + 1)a$ und $b = \lambda a$ ist $a = c - b$, $y = |c|^2 - |b|^2$: eine Gerade liegt vor.

2. Fall $x \neq 0$: teilt man die Gleichung für K_A durch $x \in \mathbb{R}$, so ändert sich die Lösungsmenge nicht. Also oBdA $x = 1$, und die Gleichung lautet $z\bar{z} + a\bar{z}w + \bar{a}z\bar{w} + yw\bar{w} = 0$, also $|z + aw|^2 + (y - |a|^2)|w|^2 = 0$. Für $y - |a|^2 > 0$ ist dies nur für $z = w = 0$ lösbar: keine Lösungen in $P_1(\mathbb{C})$. Der Fall $y - |a|^2 = 0$ kommt nicht vor, denn A ist invertierbar. Für $y - |a|^2 < 0$ liegt der Kreis mit Mittelpunkt $-a$ und Radius $\sqrt{|a| - y}$ vor. ■

Lemma 8.7 *Ist f eine Möbiustransformation und $K \subseteq \mathbb{C} \cup \{\infty\}$ ein Kreis im oberen Sinne, so ist auch $f(K)$ ein Kreis.*

Beweis. Sei A invertierbar und hermitesch. Die Gleichung für K_A lautet

$$\begin{pmatrix} \bar{z} & \bar{w} \end{pmatrix} \cdot A \cdot \begin{pmatrix} z \\ w \end{pmatrix} = 0.$$

Sei f_B die Möbiustransformation einer invertierbaren Matrix B . Dann hat $f_B(K_A)$ die Gleichung $\begin{pmatrix} \bar{z} & \bar{w} \end{pmatrix} \cdot A' \cdot \begin{pmatrix} z \\ w \end{pmatrix} = 0$ für $A' = (B^{-1})^H A B^{-1}$. Auch A' ist also invertierbar und hermitesch, und die Lösungsmenge ist nicht leer. Also $f_B(K_A) = K_{A'}$. ■

Lemma 8.8 *Seien P_1, P_2, P_3 drei verschiedene Punkte des $P_1(\mathbb{C})$. Dann gibt es genau einen Kreis, der alle drei Punkte enthält.*

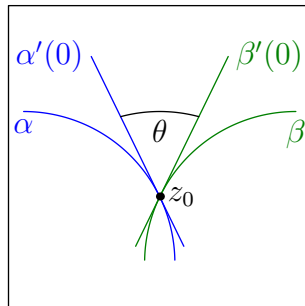
Beweis. Nach Lemma 8.5 und Lemma 8.7 reicht es, den Fall $P_1 = 0, P_2 = 1, P_3 = \infty$ zu betrachten. Kein herkömmlicher Kreis enthält ∞ . Bei den Geraden enthält nur die x -Achse (einschl. ∞) alle drei Punkte. ■

9 Hyperbolische Geometrie

9.1 Konforme Abbildungen

Lemma 9.1 *Möbiustransformationen sind konforme Abbildungen, d.h. sie erhalten Winkel.*

Beweis. Seien $\alpha, \beta: \mathbb{R} \rightarrow \mathbb{C}$ zwei differenzierbare Funktionen mit $\alpha(t) = \beta(t) = z_0$.

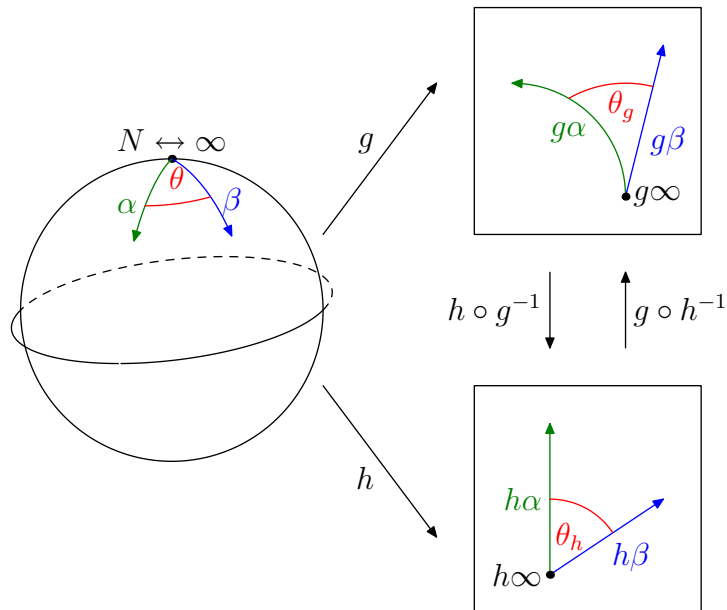


Sei $f(z) = \frac{az+b}{cz+d}$ eine Möbiustransformation mit $f(z_0) \neq \infty$. Wir berechnen $(f \circ \alpha)'(0)$. Es ist

$$(f \circ \alpha)'(t) = \frac{a\alpha'(t)(c\alpha(t) + d) - c\alpha'(t)(a\alpha(t) + b)}{(c\alpha(t) + d)^2},$$

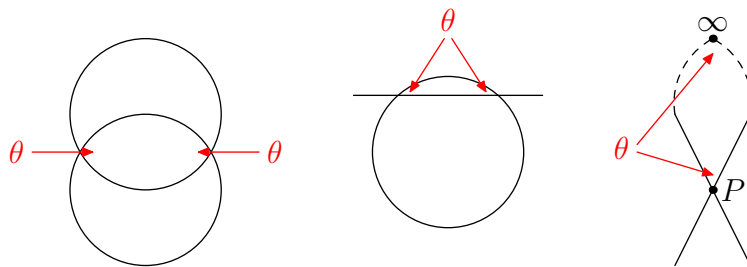
also $(f \circ \alpha)'(0) = \lambda\alpha'(0)$ für $\lambda = \frac{ad-bc}{(cz_0+d)^2} \neq 0$. Auch $(f \circ \beta)'(0) = \lambda\beta'(0)$. Somit sind die Winkel zwischen $f \circ \alpha$, $f \circ \beta$ und zwischen α , β gleich.

Bleibt der Fall zu untersuchen, wo mindestens eins aus z_0 , $f(z_0) = \infty$ ist. Nach dem aber, was wir bereits bewiesen haben, können wir sagen: Zwei Kurven α, β , die sich in ∞ schneiden, sind differenzierbar dort und schneiden sich mit Winkel θ genau dann, wenn dies gilt für den Schnittpunkt 0 der Kurven $1/\alpha(t)$, $1/\beta(t)$. Wir hätten auch jede andere Möbiustransformation mit $f(\infty) \neq \infty$ nehmen können: wegen dem bereits bewiesenen Teil bekämen wir die gleiche Antwort. ■



Beispiel K ein Kreis mit Mittelpunkt auf der x -Achse. Dann treffen sich die Kreise $f(K)$, $f(x\text{-Achse})$ in rechten Winkeln.

Beispiel Zwei nicht-parallele Geraden⁶ treffen sich einmal in der komplexen Ebene und einmal in ∞ . An beiden Stellen treffen sie sich im gleichen Winkel. Begründung: Eine Möbiustransformation anwenden, die beide Schnittpunkte nach Punkte in \mathbb{C} abbildet. Jetzt geht es um Schnittpunkte Kreis mit Kreis oder Kreis mit Gerade. Bekanntlich gibt es höchstens zwei, und wenn es zwei gibt, dann sind beide Winkel gleich.



Beispiel Zwei parallele Geraden dagegen treffen sich nur in ∞ ; dort berühren sie sich.

Bemerkung Vergleich: $P_1(\mathbb{C})$ und $P_2(\mathbb{R})$.

⁶Nicht vergessen: es geht hier um $P_1(\mathbb{C})$, nicht um $P_2(\mathbb{R})$.

9.2 Die hyperbolische Ebene: Das Halbebene-Modell

Definition Sei \mathcal{H} die obere Halbebene der komplexen Ebene:

$$\mathcal{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

Eine *hyperbolische Gerade* in \mathcal{H} ist die Menge $\mathcal{H} \cap K$ für einen Kreis K in $P_1(\mathbb{C})$, der die x -Achse (einschl. ∞) zweimal im rechten Winkel schneidet.

Bemerkung Kreise in $P_1(\mathbb{C})$ sind herkömmliche Kreise oder (euklidische) Geraden. Ein herkömmlicher Kreis schneidet die x -Achse genau dann im rechten Winkel, wenn der Mittelpunkt auf der x -Achse liegt. Nach den obigen Überlegungen ist eine euklidische Gerade genau dann eine hyperbolische Gerade, wenn sie parallel zur y -Achse ist.

Die Halbkreis-Endpunkte auf der x -Achse gehören *nicht* zur hyperbolischen Gerade.

Lemma 9.2 a) Seien $P, Q \in \mathcal{H}$ mit $P \neq Q$. Es gibt genau eine hyperbolische Gerade L , die P mit Q verbindet.

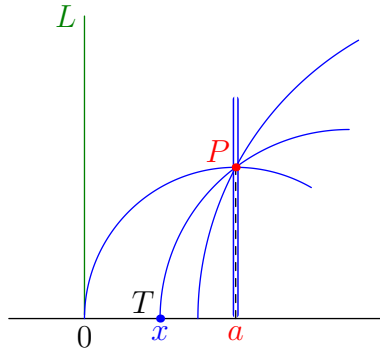
b) Zwei hyperbolische Geraden treffen sich in höchstens einem Punkt.

c) Sei L eine hyperbolische Gerade und $P \in \mathcal{H} \setminus L$. Dann gibt es unendlich viele hyperbolische Geraden durch P , die L nicht treffen.

Beweis. a) Sei R der Mittelpunkt der Strecke PQ . Sei G die Gerade durch R , die senkrecht auf PQ steht. Ist G parallel zur x -Achse, so haben P, Q die gleiche x -Koordinate: somit liegen Sie auf keinem Kreis mit Mittelpunkt auf der x -Achse; und sie liegen auf genau einer Gerade parallel zur y -Achse. Ist dagegen G nicht parallel zur x -Achse, so trifft sie die x -Achse in genau einem Punkt M . Der Kreis mit Mittelpunkt M durch P, Q ist die einzige hyperbolische Gerade.

b) Treffen sich zwei hyperbolische Geraden in $z \in \mathcal{H}$, so treffen sie sich auch in $\bar{z} \in P_1(\mathbb{C}) \setminus \mathcal{H}$. Aber zwei Kreise in $P_1(\mathbb{C})$ treffen sich höchstens zweimal.

c) Nach Lemma 9.3 unten operiert $PSL_2(\mathbb{R})$ auf \mathcal{H} und permutiert die hyperbolischen Geraden. Nach Lemma 9.4 unten werden die hyperbolischen Geraden *transitiv* permutiert. OBdA ist also L die Gerade $x = x_1$ und P der Punkt $x_2 + iy_2$, $y_2 > 0$. Es ist $x_1 \neq x_2$, oBdA $x_1 < x_2$. Die Gerade $x = x_2$ ist eine solche hyperbolische Gerade. Für jedes $x_1 \leq x_3 < x_2$ gibt es genau einen Kreis mit Mittelpunkt auf der x -Achse, die x_3 und P enthält. Dieser Kreis trifft L nicht. ■



Lemma 9.3 a) Die Gruppe $PSL_2(\mathbb{R})$ operiert auf der hyperbolischen Ebene \mathcal{H} durch Möbiustransformationen.

- b) Jede Möbiustransformation aus $PSL_2(\mathbb{R})$ bildet hyperbolische Geraden bi-jektiv auf hyperbolischen Geraden ab.
- c) Keine weitere Möbiustransformation bildet \mathcal{H} bijektiv auf sich selbst ab.
- d) Bildet $f \in PSL_2(\mathbb{C})$ den Kreis „ x -Achse zzgl. ∞ “ auf sich selbst ab, so ist $f \in PGL_2(\mathbb{R})$. Gibt es außerdem ein $P \in \mathcal{H}$ mit $f(P) \in \mathcal{H}$, so ist $f \in PSL_2(\mathbb{R})$.

Beweis. a) Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, d.h. $a, b, c, d \in \mathbb{R}$ und $ad - bc = 1$. Wegen $a, b, c, d \in \mathbb{R}$ liegen $f_A(\infty)$ und $f^{-1}(\infty)$ auf dem Kreis „ x -Achse zzgl. ∞ “.

Überlegung: Für $z \in \mathbb{C}$ ist $\Im(adz + bc\bar{z}) = \Im(z)$, denn $ad = bc + 1$, also $adz + bc\bar{z} = z + bc(z + \bar{z})$.

Sei $z \in \mathbb{C}$ mit $f(z) \neq \infty$. Wir zeigen: $\Im(z)$ und $\Im(f_A(z))$ haben das gleiche Vorzeichen. Es ist $f_A(z) = \frac{az+b}{cz+d} = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}$, also $\Im(f_A(z)) = \frac{1}{|cz+d|^2} \Im(adz + bc\bar{z}) = \frac{1}{|cz+d|^2} \Im(z)$. Also bildet f_A die hyperbolische Ebene \mathcal{H} bijektiv auf sich selbst ab.

- b) Möbiustransformationen bilden Kreise auf Kreise ab und erhalten Winkel. Also bildet f_A hyperbolische Geraden auf hyperbolische Geraden ab.
- c) Sei K der Kreis „ x -Achse zzgl. ∞ “ und f eine Möbiustransformation, die \mathcal{H} bijektiv auf sich selbst abbildet. Angenommen $f(K) \neq K$. Dann $\exists x \in \mathbb{R}$ $f(x) \notin K$. Dann $\Im(f(x)) < 0$, da $f^{-1}(z) \in \mathcal{H}$ für jedes $z \in \mathcal{H}$. Aber es gibt eine Folge (z_n) aus \mathcal{H} , die gegen x konvergiert, also konvergiert $f(z_n)$ gegen $f(x)$. Widerspruch, da $\Im(f(x)) < 0$ und $\Im(f(z_n)) > 0$ für alle n . Fazit: $f(K) = K$. Das Ergebnis folgt also aus d).

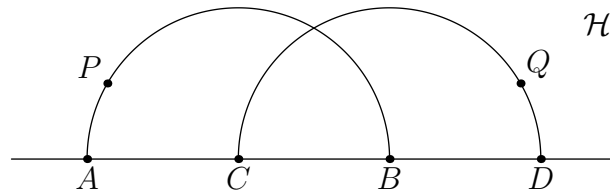
- d) $f(0)$, $f(1)$ und $f(\infty)$ sind also reell im Sinne des Zusatzes zu Lemma 8.5. Also gibt es eine Möbiustransformation f_A mit $A \in GL_2(\mathbb{R})$ und $f_A(z) = f(z)$ für $z = 0, 1, \infty$. Sind etwa $f(0) = p$, $f(1) = q$ und $f(\infty) = r$ alle in \mathbb{R} , so ist diese Möbiustransformation $\frac{(q-p)rz - p(q-r)}{(q-p)z - (q-r)}$. Also nach dem selben Lemma ist $f = f_A$ und $f \in PGL_2(\mathbb{R})$. Es ist $f_A \in PSL_2(\mathbb{R})$ genau dann, wenn $\det A > 0$. Aber $\Im(f_A(i))$ und $\det A$ haben das gleiche Vorzeichen. Also $f \in PSL_2(\mathbb{R})$. ■

Lemma 9.4 Sei T die Menge aller Paare (P, L) mit P ein Punkt der hyperbolischen Ebene und L eine hyperbolische Gerade mit $P \in L$.

- a) Durch $f * (P, L) = (f(P), f(L))$ operiert $PSL_2(\mathbb{R})$ auf T .
- b) Diese Operation ist transitiv.
- c) Der Stabilisator von (P, L) ist zyklisch der Ordnung zwei; das einzige nicht-triviale Element ist die Möbiustransformation, die P auf sich selbst abbildet und die beiden Endpunkte von L miteinander vertauscht.

Beweis. a) $PSL_2(\mathbb{R})$ operiert bekanntlich auf \mathcal{H} und auf der Menge der hyperbolischen Geraden.

- b) (P, L) und (Q, G) . Fußpunkte a, b von L und c, d von G . Sei f die Möbiustransformation mit $f(P) = Q$, $f(a) = c$ und $f(b) = d$. Dann $f(L) = G$, denn es ist eine hyperbolische Gerade und nur ein Kreis enthält c, d, Q .



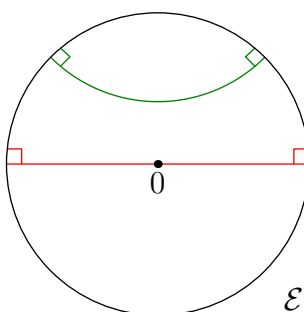
Nun, $f(x\text{-Achse})$ ist ein Kreis, der G rechtwinklig in c, d schneidet. Der einzige solche Kreis ist die x -Achse. Nach Lemma 9.3 Teil d) ist also $f \in PSL_2(\mathbb{R})$.

- c) Ist f im Stabilisator, dann $f(P) = P$ und $\{f(a), f(b)\} = \{a, b\}$. ■

9.3 Das Scheiben-Modell

Definition Sei \mathcal{E} die Scheibe $\mathcal{E} := \{z \in \mathbb{C} \mid |z| < 1\}$. Eine *hyperbolische Gerade* in \mathcal{E} ist die Menge $L \cap \mathcal{E}$ für einen Kreis L in $P_1(\mathbb{C})$, der den Einheitskreis

$|z| = 1$ zweimal im rechten Winkel schneidet.



Lemma 9.5 Vermöge der Möbiustransformation $f_0(z) = \frac{1+iz}{1-iz}$ ist das Scheiben-Modell der hyperbolischen Geometrie äquivalent zur Halbebene-Modell.

Beweis. f_0 bildet den Rand von \mathcal{H} bijektiv auf dem Rand von \mathcal{E} ab, und $f_0(i) = 0$. Wegzusammenhangskomponenten betrachten $\Rightarrow f_0(\mathcal{H}) = \mathcal{E}$. Möbiustransformationen sind konformal, also bilden f_0 und f_0^{-1} hyperbolische Geraden auf hyperbolischen Geraden ab. ■

Bemerkung Sei $g \in PSL_2(\mathbb{C})$. Es ist $g(\mathcal{E}) = \mathcal{E}$ genau dann, wenn $h(\mathcal{H}) = \mathcal{H}$ für $h = f_0^{-1}gf_0$, also genau dann, wenn $g \in f_0PSL_2(\mathbb{R})f_0^{-1}$. Nennen wir die $g \in PSL_2(\mathbb{C})$ mit $g(\mathcal{E}) = \mathcal{E}$ Transformationen von \mathcal{E} . Genau wie die Elemente von $PSL_2(\mathbb{R})$ im Halbebenenmodell sind es im Scheibenmodell die Transformationen von \mathcal{E} , die die hyperbolischen Geraden permutieren. So gilt etwa Lemma 9.4 für das Scheibenmodell, man muss nur „ $f \in PSL_2(\mathbb{R})$ “ durch „ f eine Transformationen von \mathcal{E} “ ersetzen.

9.4 Das Doppelverhältnis

Hyperbolische Abstandsmessung.

Definition Seien z_1, z_2, z_3, z_4 vier verschiedene Punkte. Das *Doppelverhältnis*

$$[z_1, z_2, z_3, z_4] := \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_2)(z_3 - z_4)}.$$

Bemerkung Manche Quellen (z.B. Wikipedia) geben andere Formeln der selben Art, die im wesentlichen die gleichen Eigenschaften haben.

Lemma 9.6 a) Das Doppelverhältnis vier verschiedener Punkte des $P_1(\mathbb{C})$ ist eine wohldefinierte komplexe Zahl.

b) Möbiustransformationen ändern das Doppelverhältnis nicht.

Beweis. a)

$$\begin{aligned} & [(z_1 : w_1), (z_2 : w_2), (z_3 : w_3), (z_4 : w_4)] \\ & = [(z_1 w_3 - w_1 z_3)(z_2 w_4 - w_2 z_4) : (z_1 w_2 - w_1 z_2)(z_3 w_4 - w_3 z_4)]. \end{aligned}$$

Da alle vier Punkte verschieden sind, ist $[z_1, z_2, z_3, z_4] = (z : w)$ mit $z, w \neq 0$, also Doppelverhältnis $\frac{z}{w} \in \mathbb{C}$.

b) Gemeint ist

$$[f(z_1), f(z_2), f(z_3), f(z_4)] = [z_1, z_2, z_3, z_4].$$

Für $f(z) = \frac{az+b}{cz+d}$ ist $f(z : w) = (z' : w')$ für $z' = az + bw$, $w' = cz + dw$. Mit $\Delta := ad - bc \neq 0$ ist $z'_i w'_j - w'_i z'_j = \Delta(z_i w_j - w_i z_j)$. ■

Lemma 9.7 a) Für feste $z_1, z_2, z_4 \in P_1(\mathbb{C})$ ist $z_3 \in P_1(\mathbb{C}) \setminus \{z_1, z_2, z_4\}$ eindeutig bestimmt durch $[z_1, z_2, z_3, z_4] \in P_1(\mathbb{C}) \setminus \{0, 1, \infty\}$.

b) Vier Punkte liegen genau dann auf dem gleichen Kreis in $P_1(\mathbb{C})$, wenn deren Doppelverhältnis reell ist.

c) $[z_4, z_3, z_2, z_1] = [z_1, z_2, z_3, z_4]$.

d) Seien P, Q zwei Punkte der hyperbolischen Ebene und A, B die Endpunkte der hyperbolischen Gerade, die die P, Q verbindet, Ordnung A, P, Q, B . Dann ist $[A, P, Q, B] > 1$.

Beweis. a) Sei f die Möbiustransformation mit $f(z_1) = 0$, $f(z_2) = 1$ und $f(z_4) = \infty$. Nach Lemma 9.6 b) ist $[z_1, z_2, z_3, z_4] = [0, 1, f(z_3), \infty]$. Nun,

$$[0, 1, z, \infty] = z,$$

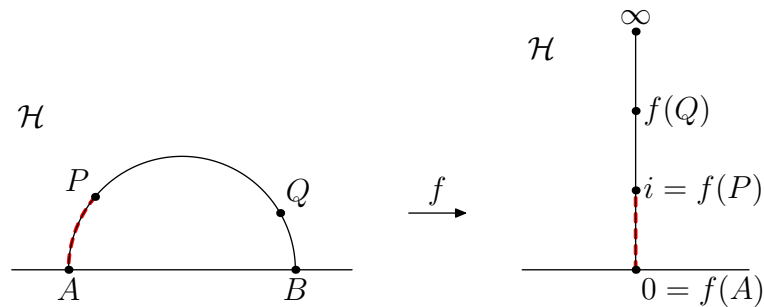
also $z_3 = f^{-1}([z_1, z_2, z_3, z_4])$. Aber f ist durch z_1, z_2, z_4 eindeutig bestimmt, nach Lemma 8.5.

b) Wie in a) ist oBdA $z_1 = 0$, $z_2 = 1$, $z_4 = \infty$. Schreibe $z = z_3$. Wegen $[0, 1, z, \infty] = z$ und $z \notin \{0, 1, \infty\}$ folgt das Ergebnis.

c) Klar.

d) Nach c) ist oBdA $A \neq \infty$. Die Möbiustransformation $f(A) = 0$, $f(P) = i$, $f(B) = \infty$ liegt in $PSL_2(\mathbb{R})$ nach dem Beweis von Lemma 9.4 b). Der kurze Kreisbogen von A nach P wird stetig abgebildet auf einem kompakten

Intervall auf der y -Achse, das $0, i$ enthält.



Da $f(Q) = yi$ in \mathcal{H} aber außerhalb dieses Intervalls liegt, ist $y > 1$. ■

Warnbeispiel Es ist i.Allg. $[A, P, Q, B] = [B, Q, P, A] \neq [A, Q, P, B]$, z.B. für $A = 0, P = i, Q = 2i, B = \infty$.

Definition Hyperbolischer Abstand $d(P, Q) = \ln[A, P, Q, B]$. Beide Modelle.

Beispiel Halbebene-Modell: für $y > x$ ist $d(xi, yi) = \ln \frac{y}{x}$.
Scheiben-Modell: für den Mittelpunkt 0 ist $[-e^{i\theta}, 0, re^{i\theta}, e^{i\theta}] = \frac{1+r}{1-r}$.

Lemma 9.8 a) $d(P, Q) = d(Q, P)$.

b) Es ist $d(f(P), f(Q)) = d(P, Q)$ für $f \in PSL_2(\mathbb{R})$ (Halbebenenmodell) bzw. für f eine Transformation von \mathcal{E} (Scheibenmodell).

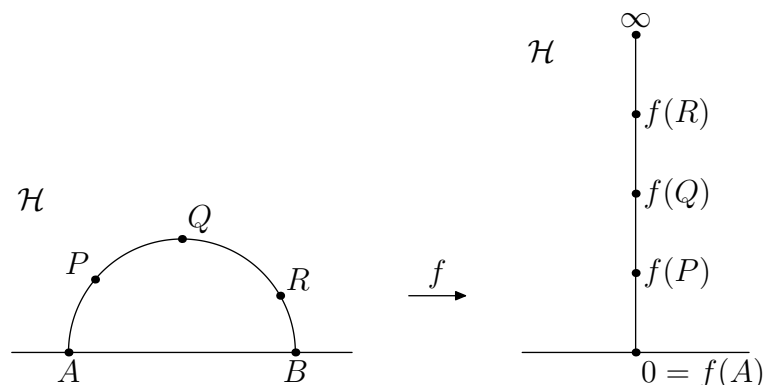
c) P, Q, R auf einer hyperbolischen Gerade, Q zwischen P und R . Dann

$$d(P, R) = d(P, Q) + d(Q, R).$$

Beweis. a) Folgt aus Lemma 9.7.

b) Möbiustransformationen ändern das Doppelverhältnis nicht. Für eine solche Transformation f sind $f(A), f(B)$ die Endpunkte der hyperbolischen Gerade durch $f(P), f(Q)$.

c) Nach Möbiustransformation: OBdA Halbebenenmodell, $P = xi, Q = yi, R = zi$ mit $z > y > x > 0$.

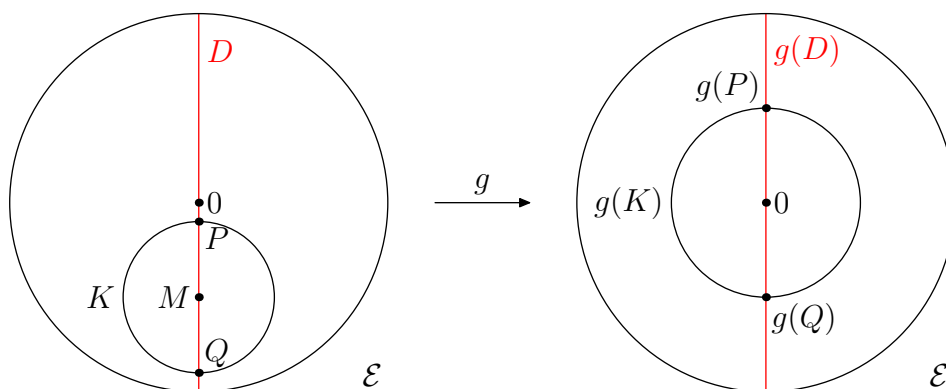


Jetzt $d(xi, yi) = \ln \frac{y}{x}$ benutzen. ■

Lemma 9.9 *Hyperbolische Kreise sind herkömmliche Kreise, und umgekehrt.*

Bemerkung Erläuterung der Begriffe. Warnung: Mittelpunkt, Radius im Allg. nicht gleich.

Beweis. Der herkömmliche Kreis mit Mittelpunkt 0 und Radius $r < 1$ ist (Scheibenmodell) der hyperbolische Kreis mit Radius $\frac{1+r}{1-r}$. Folglich ist jeder hyperbolische Kreis ein herkömmlicher Kreis (beide Modelle). Ist umgekehrt K ein herkömmlicher Kreis, dann oBdA im Scheibenmodell, Mittelpunkt $M \neq O$. Seien P, Q die zwei Punkte von K , die auf dem Durchmesser $D = OM$ liegen. Nach Lemma 9.4 gibt es eine konformale, längenerhaltende Transformation g der Scheibe, mit $g(D) = D$, $g(M) = O$. Dann ist $g(K)$ ein herkömmlicher Kreis in der Scheibe, die $g(P)$ und $g(Q)$ enthält, und dort senkrecht auf dem Durchmesser D steht.



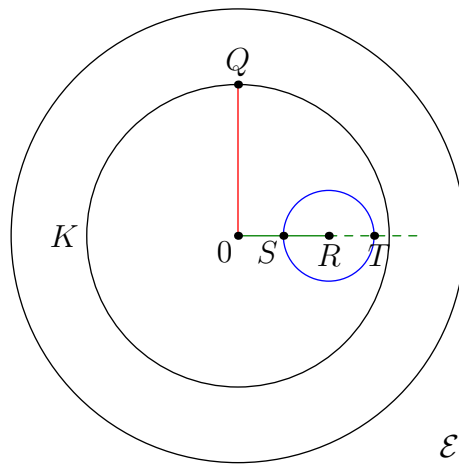
Somit hat $g(K)$ Mittelpunkt der Strecke $g(P)g(Q)$. Dies ist O . Also ist $g(K)$ und folglich auch K ein hyperbolischer Kreis. ■

Korollar 9.10 *Im Scheibenmodell sei K ein hyperbolischer Kreis mit Mittelpunkt R . Als herkömmlicher Kreis liegt der Mittelpunkt auf dem Scheibendurchmesser OR , bzw. in O falls $R = O$.*

Beweis. Den Fall $R = O$ hatten wir schon, also oBdA $R \neq O$. Sei D der Durchmesser OR . Sei g die Transformation von \mathcal{E} mit $g(D) = D$, $g(R) = O$ (existiert nach Lemma 9.4). Als hyperbolischer Kreis hat $g(K)$ den Mittelpunkt O , also ist $g(K)$ ein herkömmlicher Kreis mit Mittelpunkt O . Somit schneidet $g(K)$ den Durchmesser $D = g(D)$ zweimal im rechten Winkel. Möbiustransformationen sind konformal, also schneidet K den Durchmesser D zweimal im rechten Winkel. Also liegt das Zentrum auf D . ■

Lemma 9.11 *Dreiecksungleichung: $d(P, Q) \leq d(P, R) + d(R, Q)$. Gleichheit gilt nur dann, wenn P, Q, R auf einer hyperbolischen Gerade liegen.*

Beweis. Scheibenmodell. OBdA $d(P, Q) \geq d(P, R) \geq d(R, Q)$. OBdA $P = O$ (Lemma 9.4). Sei K der Kreis (hyperbolisch und herkömmlich) um O durch Q . Sei L der hyperbol. Kreis um R durch Q , d.h. mit Radius $d(R, Q)$. Sei D der Scheibendurchmesser OR . Sei $T \in D$ der Punkt mit $d(R, T) = d(R, Q)$ und $d(O, T) = d(O, R) + d(R, Q)$. Sei $S \in D$ der Punkt mit $d(R, S) = d(R, Q)$ und $d(O, S) = d(O, R) - d(R, Q)$. Als herkömmlicher Kreis hat L Mittelpunkt auf D (Korollar 9.10), und enthält S, T . Somit ist T der Punkt auf L , der den größten herkömmlichen Abstand zu O hat. Nun, der hyperbolische Abstand zu O ist eine streng wachsende Funktion des herkömmlichen Abstands, und umgekehrt. Ist also $d(O, R) + d(R, Q) < d(O, Q)$, dann $d(O, T) < d(O, Q)$, also liegt L vollständig innerhalb von K , was $Q \in K \cap L$ widerspricht.



Ist $d(O, R) + d(R, Q) = d(O, Q)$, dann berühren sich K, L in T und treffen sich daher sonst nirgendwo. Also $Q = T$ und O, R, Q liegen alle auf D , eine hyperbolische Gerade. ■

Bemerkung Mit Analysis kann man hyperbolische Kurvenlänge und hyperbolische Fläche berechnen. Nach dem Satz von Gauß-Bonnet gilt

$$\text{Fläche eines hyperbolischen Dreiecks} = \pi - \text{Winkelsumme},$$

woraus folgt, dass die Winkelsumme von der Größe des Dreiecks abhängt und immer $< \pi$. In der hyperbolischen Ebene kann man ein reguläres rechteckiges Achteck konstruieren: man kann sogar die hyperbolische Ebene mit solchen Rechtecken pflastern.