ANALYTISCHE GEOMETRIE

und

LINEARE ALGEBRA

Teil II:
Anschauliche Geometrie
und Gruppentheorie

Samuel J. Patterson
Mathematisches Institut Göttingen

Inhaltsverzeichnis

Einleitung

Dieses Skript ist eine Neufassung eines Skripts, das ich vor fast 20 Jahren vorbereitet und mehrmals als Begleittext zu der Vorlesung "Analytische Geometrie und Lineare Algebra, Teil II" verwendet habe. Diese Fassung ist gegenüber der alten lediglich leicht überarbeitet; sie ist aber jetzt in elektronischer Form verfügbar.

Die Grundgedanken hinter dieser Vorlesung sind, dass neben der linearen Algebra (AGLA I) die Gruppentheorie zur Grundausbildung in Algebra gehört und dass die Geometrie ebenbürtig mit der Algebra ist. Durch die vielfältigen Wechselwirkungen zwischen Geometrie und Gruppentheorie ergänzen sich diese Ziele gegenseitig. Sie tragen auch der seit 1998 geltenden LehrPVO Rechnung, in der für das Lehramt "Geometrie vom höheren Standpunkt aus" vorgeschrieben wird. Der Geist von Felix Klein ist in dieser Vorlesung allgegenwärtig.

Bei der ersten Fassung hat Frau Christa Mirgel mir bei der Vorbereitung des Manuskripts geholfen; Frau Christiane Gieseking hat es in dem finsteren Zeitalter der elektromechanischen Schreibmaschinen getippt und die Zeichnungen gefertigt. Diese Fassung wurde von Frau Claudia Gabler geTeXt; sie hat die Zeichnungen neu erstellt. Allen gebührt mein herzlicher Dank.

S.J. Patterson

Kapitel 1

Allgemeine Gruppentheorie

1. Einleitende Bemerkungen

Gruppentheorie befaßt sich mit Symmetrien. Fast alle Gruppen beschrieben die Symmetrien irgendeines Objektes. Auch wenn die zugehörigen Gruppen gleich sind, können diese Objekte sehr unterschiedlicher Natur sein. In der Vorlesung werden wir mehrere Beispiele studieren, und es wäre voreilig, jetzt viele aufzuzählen. Die einfachste Symmetrie, die aus einem Element zweiter Ordnung besteht, tritt überall auf, man denkt: Links/rechts, positiv/negativ, Bild/Spiegelbild, ja/nein, schwarz/weiß, männlich/weiblich, und sogar ganze Philosophien stützen sich auf solche Dichotomien.

In diesem Kapitel werden zuerst Gruppen definiert (schon in diesem Abschnitt), danach wird eine Abstrahierung der konkreten Gegenstände, die die Symmetrien besitzen, in Kapitel I. 2. eingeführt. Diese Objekte heißen *G-Mengen*. Angesichts der Tatsache, dass fast alle Gruppen als Symmetriegruppen auftreten, ist es angebracht, nicht nur Gruppen, sondern auch die entsprechend G-Mengen von Anfang an zu untersuchen.

In Kapitel I. 3. werden die Beziehungen zwischen verschiedenen Gruppen und ihrer G-Mengen beschrieben.

Obwohl die ganze Vorlesung dazu dient, Beispiele für die in diesem Kapitel eingeführten Begriffe zu liefern, wird in Kapitel I. 4. eine Liste von häufig vorkommenden Gruppen und G-Mengen angegeben. Der in diesem Kapitel behandelte Stoff mag aber ziemlich trocken erscheinen, und die Zuhörer(innen) und Leser(innen) werden gebeten, etwas Geduld zu haben, weil die Beispiele erst "nachher" ausführlich behandelt werden.

Nun kommen wir zur Definition einer Gruppe.

Definition. Eine Menge G mit einem ausgezeichneten Element e (die "Identität") und einer Abbildung (die "Multiplikation")

$$G \times G \to G,$$

geschrieben $(g_1, g_2) \longmapsto g_1 \cdot g_2$, heißt *eine Gruppe*, wenn die folgenden Axiome erfüllt sind:
GR 1: $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3) \quad (g_1, g_2, g_3 \in G)$
GR 2: $e \cdot g = g, g \cdot e = g \quad (g \in G)$
GR 3: Seien $g_1, g_2 \in G$; es gibt $g \in G$ (bzw. $g' \in G$), so dass gilt

$$g \cdot g_1 = g_2 \quad (\text{bzw. } g_1 \cdot g' = g_2).$$

Lemma. *Sei G eine Gruppe. Zu jedem $g \in G$ kann man ein Element $g^{-1} \in G$ zuordnen, so dass gilt*

$$g \cdot g^{-1} = e, g^{-1} \cdot g = e.$$

Darüber hinaus gilt für $g_1, g_2 \in G$

$$(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}.$$

Bemerkung. Es wäre möglich, Axiom GR 3 durch den Schluß dieses Lemma zu ersetzen. Es wäre auch möglich, GR 2 durch eine von den beiden Gleichungen zu ersetzen.

Das Element g^{-1} heißt das *Inverse* zu g.

Beweis. In GR 3 wählen wir $g_2 = e$; es gibt daher $g', g'' \in G$, so dass gelten

$$g' \cdot g_1 = e \quad , \quad g_1 \cdot g'' = e.$$

Wir schreiben jetzt schlicht g statt g_1. Nun -nach GR 1- gilt

$$(g' \cdot g) \cdot g'' = g' \cdot (g \cdot g'').$$

Es folgt

$$e \cdot g'' = g' \cdot e,$$

oder -nach GR 2-

$$g'' = g'.$$

Deswegen sind g' und g'' beide gleich und daher eindeutig bestimmt. Wir definieren $g^{-1} := g'$. Damit ist die erste Behauptung bewiesen.

Nach GR 1 gelten

$$\begin{aligned} \left(g_2^{-1} \cdot g_1^{-1}\right) \cdot (g_1 \cdot g_2) &= g_2^{-1} \cdot \left(g_1^{-1} \cdot (g_2 \cdot g_2)\right) \\ &= g_2^{-1} \cdot \left(\left(g_1^{-1} \cdot g_1\right) \cdot g_2\right) \\ &= g_2^{-1} \cdot (e \cdot g_2). \end{aligned}$$

Nach GR 2 ist dieses $g_2^{-1} \cdot g_2 = e$. Wir haben bewiesen, dass gilt

$$\left(g_2^{-1} \cdot g_1^{-1}\right) \cdot (g_1 \cdot g_2) = e.$$

Ähnlich gilt

$$(g_1 \cdot g_2) \cdot \left(g_2^{-1} \cdot g_1^{-1}\right) = e.$$

Deshalb, weil $(g_1 g_2)^{-1}$ eindeutig durch diese Eigenschaften bestimmt ist, gilt

$$g_2^{-1} \cdot g_1^{-1} = (g_1 \cdot g_2)^{-1}.$$

Korollar. 1. *Sei G eine Gruppe, und seien $g_1, g_2 \in G$. Das einzige Element $g \in G$, das der Bedingung*

$$g_1 \cdot g = g_2 \quad (\text{bzw. } g \cdot g_1 = g_2)$$

genügt, ist $g_1^{-1} g_2$ (bzw. $g_2 g_1^{-1}$). Insbesondere ist g^{-1} durch die Gleichung $g^{-1} \cdot g = e$ (oder $g \cdot g^{-1} = 2$) völlig bestimmt.

2. *Es gilt $(g^{-1})^{-1} = g\,(g \in G)$.*

Beweis. Von $g_1 \cdot g = g_2$ haben wir

$$g_1^{-1} \cdot (g_1 \cdot g) = g_1^{-1} \cdot g_2.$$

Nach GR 1 folgt

$$\begin{aligned} \left(g_1^{-1} \cdot g_1\right) \cdot g &= g_1^{-1} \cdot g_2 \\ \text{oder} \\ e \cdot g = g &= g_1^{-1} \cdot g_2. \end{aligned}$$

Damit ist g eindeutig bestimmt. Die andere Aussage von 1 läuft analog.

Nun liefern

$$\begin{aligned} g^{-1} \cdot \left(g^{-1}\right)^{-1} &= e \\ \text{und} \\ g^{-1} \cdot g &= e \\ g &= \left(g^{-1}\right)^{-1}. \end{aligned}$$

Damit ist das Korollar bewiesen.

Fortan werden wir den Punkt in $g_1 \cdot g_2$ normalerweise weglassen.

Eine besonders wichtige Klasse von Gruppen sind die *abelschen* (oder *kommutativen*) *Gruppen*; sie werden durch das zusätzliche Axiom
AB:
Für

$$g_1, g_2 \in G$$

gilt

$$g_1 g_2 = g_2 g_1$$

definiert.

Definition. Sei G eine Gruppe. Eine Untergruppe H von G ist eine Untermenge von G, die e enthält, und die auch eine Gruppe bezüglich der von G übertragenen Multiplikation bildet.

Lemma. *Eine nicht-leere Untermenge H von G ist eine Untergruppe, wenn, und nur wenn die folgende Bedingung erfüllt ist:*
UG: *Für $h_1, h_2 \in H$ gilt auch $h_1^{-1}h_2 \in H$.*

Beweis. Dass diese Bedingung notwendig ist, ist klar, weil erstens $h_1^{-1} \in H$ und dann zweitens $h_1^{-1}h_2 \in H$ gelten, da H eine Gruppe ist.

Umgekehrt, von der UG mit $h_1 = h_2 = h$ erhalten wir zuerst $e \in H$. Dann erhalten wir mit $h_2 = e, h_1 = h \in H$, dass, wenn $h \in H$ gilt, $h^{-1} \in H$ folgt $h^1 \in H$. Schließlich folgt für $h_1, h_2 \in H$

$$h_1 h_2 = \left(h_1^{-1}\right)^{-1} h_2 \in H.$$

Deswegen ist die von G übertragene Multiplikation auf H definiert. Axiome GR 1, GR 2 sind offensichtlich erfüllt. Dass Axiom GR 3 erfüllt ist, folgt aus dem Korollar zu dem ersten Lemma.

Bemerkung. Eine Untergruppe einer abelschen Gruppe ist auch eine abelsche Gruppe.

2. G-Mengen

Eine G-Menge ist ein Objekt, das durch G entstehende Symmetrien aufweist. Sei dann G eine Gruppe.

Definition. Eine *G-Menge* X ist eine Menge X und eine Abbildung

$$G \times X \to X; \quad \text{geschrieben } (g, x) \to gx,$$

so dass gelten
GM 1: $g_1(g_2x) = (g_1g_2)x \quad (g_1, g_2 \in G, x \in X)$,
GM 2: $ex = x \quad (x \in X)$.

Man erinnere sich an die Definition eines affinen Raumen aus AGLA I.

Wir machen jetzt zwei weitere Definitionen von Begriffen, die sich in der Analysis von G-Räumen nützlich erweisen.

Definition. Sei X ein G-Raum, $x \in X$; die *Stabilisatorgruppe*; $\mathrm{Stab}_G(x)$, ist die folgende Untergruppe von G:

$$\mathrm{Stab}_G(x) = \{g \in G : gx = x\}.$$

Wir definieren die *Bahn* $O_G(x) = \{gx \in X : g \in G\}$. Hier bedeutet O "orbit" (englisch) und "orbite" (französisch). Weil jede G-Menge auch eine H-Menge ist, wobei H eine Untergruppe von G sei, ist es sinnvoll, $\mathrm{Stab}_H(x), O_H(x)$ zu bilden.

Lemma. 1. *Seien G, X wie oben. Seien $x, x' \in X$; dann gilt entweder*

$$O_G(x) \cap O_G(x') = \emptyset$$

oder

$$O_G(x) = O_G(x').$$

2. *Sei $x \in X, y \in O_G(x)$. Gelte $y = g_1x$, dann gelten*

$$\begin{aligned} \{g \in G : gx = y\} &= g_1\mathrm{Stab}_G(x) \\ &(= \{g_1\gamma : \gamma \in \mathrm{Stab}_G(x)\}) \end{aligned}$$

und

$$\begin{aligned} \mathrm{Stab}_G(y) &= g_1\mathrm{Stab}_G(x)g_1^{-1} \\ &(= \{g_1\gamma g_1^{-1} : \gamma \in \mathrm{Stab}_G(x)\}). \end{aligned}$$

Beweis. 1. Wir nehmen an, dass $O_G(x) \cap O_G(x') \neq \emptyset$ gilt. Sei $y \in O_G(x) \cap O_G(x')$. Dann gibt es $g, g' \in G$, so dass gelten

$$y = gx,$$

und

$$y = g'x'.$$

Es folgt von GM 1

$$x' = g'^{-1}(gx) = (g'^{-1}g)x.$$

Deshalb folgt mit $\gamma \in G$

$$\gamma x' = \Big(\gamma\Big(g'^{-1}g\Big)\Big)\, x \in O_G(x);$$

deshalb gilt

$$O_G(x') \subset O_G(x).$$

Analog gilt

$$O_G(x) \subset O_G(x');$$

deshalb

$$O_G(x) = O_G(x').$$

Damit ist der erste Teil bewiesen.

Nun beweisen wir den zweiten Teil. Von GM 1, 2 folgt

$$\begin{aligned}
\{g \in G : gx = g_1 x\} &= \{g \in G : \Big(g_1^{-1}g\Big)x = \Big(g_1^{-1}g_1\Big)x\} \\
&= \{g \in G : \Big(g_1^{-1}g\Big)x = x\} \\
&= \{g \in G : g_1^{-1}g \in \mathrm{Stab}_G(x)\} \\
&= g_1 \mathrm{Stab}_G(x).
\end{aligned}$$

Auch hat man

$$\begin{aligned}
\mathrm{Stab}_G(y) &= \{g \in G : gy = y\} \\
&= \{g \in G : g(g_1 x) = g_1 x\} \\
&= \{g \in G : \Big(g_1^{-1}gg_1\Big)x = x\} \\
&= \{g \in G : g_1^{-1}gg_1 \in \mathrm{Stab}_G(x)\} \\
&= g_1 \mathrm{Stab}_G(x) g_1^{-1}.
\end{aligned}$$

Damit ist das Lemma bewiesen.

Definition. Nun definieren wir eine *transitive G-Menge* als eine nichtleere G-Menge X, so dass für jedes $x \in X$ gilt $0_G(x) = X$.

Sei $\mathrm{Men}(G)$ die Menge aller G-Mengen. Wir können alle mengentheoretischen Begriffe auf $\mathrm{Men}(G)$ übertragen. So bildet man

$$X \cup Y, X \cap Y, X - Y, X \times Y (X, Y \in \mathrm{Men}(G)),$$

wenn diese sinnvoll sind. Auch kann man die Beziehungen $X \subset Y$ und $X \supset Y$ benutzen.

Ist X eine G-Menge, so sind die Bahnen $O_G(x)$ auch G-Mengen, die sogar transitiv sind. Die Menge X ist nach dem Lemma die disjunkte Vereinigung der verschiedenen Bahnen. Außerdem folgt aus dem Lemma, eine transitive G-Menge Y hat keine echten Untermengen, die auch G-Mengen sind. Bei den üblichen

Mengen besitzen genau die Mengen, die aus einem Punkt bestehen, diese Eigenschaft. Auf diese Weise kann man die transitiven G-Mengen als das Analogon zu Punkten betrachten.

Wir können eine Art G-Mengen bilden, die eine große Rolle spielen.

Definition. Sei $H \subset G$ eine Untergruppe. Auf G definieren wir die Äquivalenzrelation $x \underset{H}{\sim} m$ durch

$$x \underset{H}{\sim} y \overset{\text{Def}}{\Longleftrightarrow} y^{-1}x \in H \quad y, x \in G$$

(bzw. $x \underset{H}{\approx} Y$ durch

$$x \underset{H}{\approx} y \overset{\text{Def}}{\Longleftrightarrow} xy^{-1} \in H).$$

Es ist leicht nachzuweisen, dass $\underset{H}{\sim}$ und $\underset{H}{\approx}$ Äquivalenzrelationen sind und dass die Äquivalenzklasse von x unter $\underset{H}{\sim}$ (bzw. unter $\underset{H}{\approx}$) $xH := \{h \in H\}$ (bzw. $Hx := \{hx : h \in H\}$) ist. Der Quotientenraum $G/\underset{H}{\sim}$ (bzw. $G/\underset{H}{\approx}$) wird mit G/H (bzw. $H \setminus G$) bezeichnet. Mengen der Form xH (bzw. Hx) heißen Links- (bzw. Rechts-)nebenklassen.

Wir machen G/H (bzw. $H \setminus G$) jetzt zu einem G-Raum. Wir fassen die Elemente von G/H (bzw. $H \setminus G$) als Nebenklassen xH (bzw. Hx) auf. Dann definieren wir

$$g(xH) := (gx)H$$

bzw.

$$g(Hx) := H\left(xg^{-1}\right).$$

Wir bemerken, dass, wenn gilt $x_1 \underset{H}{\sim} x_2$ (bzw. $x_1 \underset{H}{\approx} x_2$), dann folgt

$$gx_1 \underset{H}{\sim} gx_2$$

bzw.

$$x_1 g^{-1} \underset{H}{\approx} x_2 g^{-1}.$$

Dies ist durch die folgenden Rechnungen gerechtfertigt:

$$\begin{aligned}(gx_2)^{-1}(gx_1) &= \left(x_2^{-1}g^{-1}\right)(gx_1)\\ &= x_2^{-1}\left(g^{-1}(gx_1)\right)\\ &= x_2^{-1}\left(\left(g^{-1}g\right)x_1\right)\\ &= x_2^{-1}(ex_1)\\ &= x_2^{-1}x_1 \in H\end{aligned}$$

und

$$\begin{aligned}\left(x_1g^{-1}\right)\left(x_2g^{-1}\right)^{-1} &= \left(x_1g^{-1}\right)\left(gx_2^{-1}\right)\\ &= x_1\left(g^{-1}g\right)x_2^{-1}\\ &= x_1x_2^{-1} \in H.\end{aligned}$$

Deswegen ist die Definition möglich. Auch GM 2 ist offensichtlich richtig. Bei GM 1 gehen wir folgendermaßen vor:

$$\begin{aligned} g_1\Big(g_2(xH)\Big) &= g_1(g_2xH) \\ &= (g_1g_2x)H \\ &= g_1g_2(xH), \end{aligned}$$

und

$$\begin{aligned} g_1\Big(g_2(Hx)\Big) &= g_1\Big(Hxg_2^{-1}\Big) \\ &= Hxg_2^{-1}g_1^{-1} \\ &= Hx(g_1g_2)^{-1} \\ &= g_1g_2(Hx). \end{aligned}$$

Die beiden G-Mengen G/H und $H\setminus G$ sind nur auf den ersten Blick unterschiedlich. Wir bemerken, dass

$$\begin{aligned} x_1 \underset{H}{\approx} x_2 &\Leftrightarrow x_1x_2^{-1} \in H \\ &\Leftrightarrow \Big(x_1^{-1}\Big)^{-1}\Big(x_2^{-1}\Big) \in H \\ &\Leftrightarrow x_1^{-1} \underset{H}{\sim} x_2^{-1}. \end{aligned}$$

Deswegen ist die Abbildung

$$I : G/H \to H\setminus G \quad ; \quad xH \to Hx^{-1}$$

wohldefiniert. Es gilt auch

$$\begin{aligned} I\Big(g(xH)\Big) &= I(gxH) \\ &= H(gx)^{-1} \\ &= Hx^{-1}g^{-1} \\ &= gI(xH). \end{aligned}$$

Wir brauchen fortan nur G/H in Betracht zu ziehen.

Satz 1.1. *Sei X eine transitive G-Menge. Sei $x \in X$ und $H = \mathrm{Stab}_G(x)$. Dann ist die Abbildung*

$$F : G/H \to X \quad ; \quad g\cdot H \longmapsto gx$$

eine Bijektion. Es gilt

$$F(g\alpha) = gF(\alpha) \quad (\alpha \in G/H).$$

Beweis. Nehmen wir an, dass $g' \underset{H}{\sim} g$, d.h. $g' \in gH$. Von ${g'}^{-1}g \in H$ erhalten wir

$$\Big({g'}^{-1}g\Big)x = x;$$

daher

$$gx = g'x.$$

Die Abbildung F ist also wohldefiniert. Sie ist surjektiv, weil X transitiv ist. Wir zeigen, dass sie injektiv ist. Gilt $F(gH) = F(g'H)$, so haben wir

$$gx = g'x,$$

oder

$$(g')^{-1}gx = x$$

oder

$$(g')^{-1}g \in \mathrm{Stab}_G(x) = H$$

oder

$$g' \underset{H}{\sim} g.$$

Deshalb gilt

$$g'H = gH$$

und F ist injektiv.

Endlich sei $\alpha = \gamma H (\gamma \in G)$. Es folgt

$$\begin{aligned} F\big(g \cdot (\gamma H)\big) &= F(g\gamma H) \\ &= g\gamma x \\ &= g(\gamma x) \\ &= gF(\gamma H), \end{aligned}$$

wie behauptet. Damit ist der Satz bewiesen.

Wir sagen auch, wenn X eine G-Menge ist, dass G auf X *operiert* oder *wirkt*. Wenn für jedes $x \in X$ gilt

$$\mathrm{Stab}_G(x) = \{e\},$$

sagen wir, dass G *fixpunktfrei* auf X operiert. Nach Satz 1.1 ist in diesem Fall für jedes $x \in X$ die Abbildung

$$G \to O_G(x) \quad ; \quad g \longmapsto gx$$

eine Bijektion.

Zum Abschluß dieses Abschnitts führen wir eine spezielle G-Menge ein, die später von großer Wichtigkeit sein wird. Die Menge selbst ist G, die Operation von G auf G wird durch

$$G \times G \to G \quad ; \quad (g, g') \longmapsto gg'g^{-1}$$

definiert. Wir schreiben

$${}^{g}g' := gg'g^{-1}.$$

Dann gilt

$${}^{e}g' = eg'e^{-1} = g$$

und

$$\begin{aligned} {}^{g_1 g_2}(g') &= g_1 g_2 g' (g_1 g_2)^{-1} \\ &= g_1 g_2 g' g_2^{-1} g_1^{-1} \\ &= g_1 \left({}^{g_2} g'\right) g_1^{-1} \\ &= {}^{g_1}\left({}^{g_2} g'\right). \end{aligned}$$

Deshalb sind GM 1 und GM 2 erfüllt. Die Operation heißt *Konjugation*, und die Bahnen heißen *Konjugationsklassen*.

3. Morphismen

Um Gruppen zu untersuchen, ist es notwendig, Beziehungen zwischen verschiedenen Gruppen beschreiben zu können. Dieses erreicht man mit Morphismen.

Wir definieren zuerst einen *Homomorphismus* $f : G_1 \to G_2$, wobei G_1 und G_2 Gruppen sind, also eine Abbildung, die die folgende Eigenschaft besitzt:

HM: Seien $g, g' \in G_1$; dann gilt

$$f(gg') = f(g)f(g').$$

Lemma. *Seien G_1, G_2 Gruppen, $f : G_1 \to G_2$ ein Homomorphismus. Dann gelten*

$$f(e_1) = e_2 \quad (e_j \text{ die Identität von } g_j, j = 1, 2)$$

und

$$f\left(g^{-1}\right) = f(g)^{-1}.$$

Beweis. Nach der Definition gilt

$$f(g) = f(e_1 g) = f(e_1)f(g).$$

Deswegen folgt

$$f(e_1) = f(g)f(g)^{-1} = e_2.$$

wie behauptet.

Zunächst

$$e_2 = f\left(gg^{-1}\right) = f(g)f\left(g^{-1}\right);$$

davon folgt unmittelbar

$$f\left(g^{-1}\right) = f(g)^{-1}.$$

Beispiele. 1. Sei H eine Untergruppe von G. Dann ist die *Einbettung*

$$i : H \to G \quad ; \quad h \longmapsto h$$

ein Homomorphismus.

2. Seien G_1 und G_2 Gruppen. Dann wird $G_1 \times G_2$ eine Gruppe mit Idendität von $G_j (f = 1, 2)$ ist, wenn wir die Multiplikation folgenderweise definieren:

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2').$$

Die *Projektionen*

$$\begin{array}{rcccccc} p_1 & : & G_1 \times G_2 & \to & G_1; & (g_1, g_2) & \longmapsto & g_1 \\ p_2 & : & G_1 \times G_2 & \to & G_2; & (g_1, g_2) & \longmapsto & g_2 \end{array}$$

sind Homomorphismen.

Ein injektiver Homomorphismus heißt ein *Monomorphismus* oder eine *Injektion.*
Ein surjektiver Homomorphismus heißt ein *Epimorphismus* oder eine *Surjektion.*
Ein bijektiver Homomorphismus heißt ein *Isomorphimus* oder eine *Bijektion.*
Falls es ein Isomorphimus zwischen G_1 und G_2 gibt, schreiben wir

$$G_1 \cong G_2 \quad (''G_1 \text{ ist isomorph zu } G_2'').$$

Sei nun $f : G_1 \to G_2$ ein Homomorphismus. Der Kern, $\mathrm{Ker}(f)$, von f ist so definiert:

$$\mathrm{Ker}(f) = \{g \in G_1 : f(g) = e_2\}$$

Satz. *Seien f, G_1, G_2 wie oben. Dann ist $\mathrm{Ker}(f)$ eine Untergruppe von G_1. Für $g \in \mathrm{Ker}(f), \gamma \in G_1$ gilt*

$$\gamma g \gamma^{-1} \in \mathrm{Ker}(f).$$

Beweis. Seien $g_1, g_2 \in \mathrm{Ker}(f)$. Dann gilt

$$\begin{aligned} f\left(g_1^{-1} g_2\right) &= f(g_1)^{-1} f(g_2) \quad (f \text{ Homomorphismus}) \\ &= e_2^{-1} e_2 \\ &= e_2. \end{aligned}$$

Deswegen gilt $g_1^{-1} g_2 \in \mathrm{Ker}(f)$; deshalb ist $\mathrm{Ker}(f)$ eine Untergruppe.

Außerdem gilt mit $g \in \mathrm{Ker}(f)$

$$\begin{aligned} f\left(\gamma g \gamma^{-1}\right) &= f(\gamma) f(g) f(\gamma)^{-1} \\ &= f(\gamma) f(\gamma)^{-1} \\ &= e_2. \end{aligned}$$

Es folgt, dass gilt

$$\gamma g \gamma^{-1} \in \mathrm{Ker}(f).$$

Damit ist der Satz bewiesen.

Definition. Sei G eine Gruppe. Eine Untergruppe N von G heißt *Normalteiler* von G, wenn die folgende Bedingung erfüllt ist:
NT: Für $\gamma \in N$, $g \in G$ gilt

$$g \gamma g^{-1} \in N.$$

Damit ist der Kern eines Homomorphismus ein Normalteiler.

Lemma. *Eine Untergruppe H von G ist ein Normalteiler dann, und nur dann, wenn die Relationen $\underset{H}{\sim}$ und $\underset{H}{\approx}$ gleichbedeutend sind. In diesem Fall folgt mit $x_1 \underset{H}{\sim} x_2$ und $x_1' \underset{H}{\sim} x_2'$ auch*

$$x_1^{-1} x_1' \underset{H}{\sim} x_2^{-1} x_2'.$$

Beweis. Wir nehmen an, dass $\underset{H}{\sim}$ und $\underset{H}{\approx}$ gleichbedeutend sind. Sei $h \in H$. Dann gilt $h \underset{H}{\sim} e$ und -für $g \in G$- auch $gh \underset{H}{\sim} g$. Es folgt $gh \underset{H}{\approx} g$. Daher $ghg^{-1} \underset{H}{\approx} gg^{-1} = e$. Mit anderen Worten: $ghg^{-1} \in H$. Deshalb ist H ein Normalteiler.

Wir nehmen jetzt an, dass H ein Normalteiler ist. Dann ist

$$\begin{aligned} g_1 \underset{H}{\sim} g_2 &\Leftrightarrow g_2^{-1} g_1 \in H \\ &\Leftrightarrow g_2 \left(g_2^{-1} g_1\right) g_2^{-1} \in H \quad (H \text{ Normalteiler}) \\ &\Leftrightarrow g_1 g_2^{-1} \in H \\ &\Leftrightarrow g_1 \underset{H}{\approx} g_2. \end{aligned}$$

Deshalb sind $\underset{H}{\sim}$ und $\underset{H}{\approx}$ gleichbedeutend.

Zuletzt seien x_1, x_2, x_1', x_2' wie in der Aussage des Lemmas. Dann gelten

$$x_2^{-1} x_1 \in H$$

und

$$x'^{-1}_2 x_1' \in H.$$

$$\begin{aligned} \left(x_2^{-1} x_2'\right)^{-1} \left(x_1^{-1} x_1'\right) &= x'^{-1}_2 \left(x_2 x_1^{-1}\right) x_1' \\ &= x'^{-1}_2 \left(x_2 x_1^{-1}\right) x_2' x'^{-1}_2 x_1' \end{aligned}$$

Weil gilt

$$x_1 \underset{H}{\approx} x_2,$$

gilt

$$x_2 x_1^{-1} \in H$$

und -da H ein Normalteiler ist- sogar

$$x'^{-1}_2 \left(x_2 x_1^{-1}\right) x_2' \in H.$$

Weil $x_1' \underset{H}{\sim} x_2'$ gilt, hat man auch $x'^{-1}_2 x_1' \in H$. Da H eine Untergruppe ist, gilt

$$\left(x_2^{-1} x_2'\right)^{-1} \left(x_1^{-1} x_1'\right) = \left(x'^{-1}_2 \left(x_2 x_1^{-1}\right) x_2'\right) \left(x'^{-1}_2 x_1'\right) \in H,$$

was wir zeigen wollten. Damit ist das Lemma bewiesen.

Sei N ein Normalteiler von G. Wir definieren eine Multiplikation auf G/N durch

$$\text{Klasse von } x_1 \cdot \text{ Klasse von } x_2 := \text{ Klasse von } x_1 x_2,$$

wobei "Klasse" die Äquivalenzklasse bezüglich $\underset{N}{\sim}$ oder $\underset{N}{\approx}$ bedeutet. Ist $x_1 \underset{N}{\sim} x_2$, folgt aus dem Lemma $x_1^{-1} \underset{N}{\sim} x_2^{-1}$. Daher hat man für $x_1, x_1', x_2' \in G, x_1 \underset{N}{\sim} x_1', x_2 \underset{N}{\sim} x_2'$ auch $x_1 x_2 \underset{N}{\sim} x_1' x_2'$. Deswegen ist die Definition sinnvoll. Die Identität von G/N soll die Klasse von e sein. Mit diesen Definitionen ist es leichter nachzuweisen, dass G/N eine Gruppe wird. Nämlich:

GR 1: diese folgt von

$$\begin{aligned} \mathrm{Kl}(x_1)\left(\mathrm{Kl}(x_2)\mathrm{Kl}(x_3)\right) &= \mathrm{Kl}(x_1)\mathrm{Kl}(x_2 x_3) \\ &= \mathrm{Kl}\left(x_1(x_2 x_3)\right) \\ &= \mathrm{Kl}\left((x_1 x_2) x_3\right) \\ &= \mathrm{Kl}(x_1 x_2)\mathrm{Kl}(x_3) \\ &= \left(\mathrm{Kl}(x_1)\mathrm{Kl}(x_2)\right)\mathrm{Kl}(x_3). \end{aligned}$$

GR 2:

$$\begin{array}{rcccl} \mathrm{Kl}(x)\mathrm{Kl}(e) & = & \mathrm{Kl}(xe) & = & \mathrm{Kl}(x) \\ \mathrm{Kl}(e)\mathrm{Kl}(x) & = & \mathrm{Kl}(ex) & = & \mathrm{Kl}(x) \end{array}$$

GR 3:

$$\begin{array}{rll} & \mathrm{Kl}(x)\mathrm{Kl}(x_1) & = \mathrm{Kl}(x_2) \\ \Leftrightarrow & \mathrm{Kl}(x)\left(\mathrm{Kl}(x_1)\mathrm{Kl}\left(x_1^{-1}\right)\right) & = \mathrm{Kl}(x_2)\mathrm{Kl}\left(x_1^{-1}\right) \\ \Leftrightarrow & \mathrm{Kl}(x)\mathrm{Kl}(e) & = \mathrm{Kl}\left(x_2x_1^{-1}\right) \\ \Leftrightarrow & \mathrm{Kl}(x) & = \mathrm{Kl}\left(x_2x_1^{-1}\right). \end{array}$$

Auch

$$\begin{array}{rll} & \mathrm{Kl}(x_1)\mathrm{Kl}(x) & = \mathrm{Kl}(x_2) \\ \Leftrightarrow & \mathrm{Kl}(x) & = \mathrm{Kl}\left(x_1^{-1}x_2\right). \end{array}$$

Hier bedeutet $\mathrm{Kl}(x)$ die Klasse von x, wie sie oben definiert wurde.

Definition. Die Gruppe G/N heißt die *Quotientengruppe* von G durch N. Wir nennen die Abbildung

$$p : G \to G/N \quad ; \quad x \longmapsto \text{ Klasse von } x$$

die *kanonische Projektion.* (Kanonisch wird hier als die Bezeichnung für diese Abbildung verstanden. Es hat keine weitere Bedeutung.)

Satz 1.2.

1. *Sei G eine Gruppe, N ein Normalteiler von G. Dann ist die kanonische Projektion $p : G \to G/N$ ein Homomorphismus mit*

$$\mathrm{Ker}(p) = N.$$

2. *Sei $f : G \to G'$ ein Homomorphimus. Sei $N = \mathrm{Ker}(f)$. Dann gibt es einen Monomorphimus $\bar{f} : G/N \to G'$, so dass f die Verknüpfung*

$$G \xrightarrow{\ p\ } G/N \xrightarrow{\ \bar{f}\ } G'$$

ist, wobei p die kanonische Projektion ist.

Dieser Satz bringt ein Wechselspiel zwischen Homomorphismen und Normalteiler ans Licht. Dieses Wechselspiel wird sehr wichtig sein.

Beweis. Zu 1.:

$$\begin{array}{rcl} p(x_1x_2) & = & \text{Klasse von } (x_1x_2) \\ & = & \text{Klasse von } (x_1) \text{ Klasse von } (x_2) \\ & = & p(x_1)p(x_2). \end{array}$$

Der Kern von p ist

$$\begin{array}{rl} & \{g \in G \ : \ p(g) = \text{Klasse von } e\} \\ = & \{g \in G \ : \ \text{Klasse von } g = \text{ Klasse von } e\} \\ = & \{g \in G \ : \ g \in N\} \\ = & N. \end{array}$$

Damit ist der erste Teil bewiesen.
Zu 2.: Wir definieren $\bar{f}$ durch

$$\bar{f}\ (\text{Klasse von } x) := f(x).$$

Wir müssen zeigen, dass $\bar{f}$ tatsächlich wohldefiniert ist. Nun gelten

$$\begin{array}{rrcl} & \text{Klasse von } x & = & \text{Klasse von } x' \\ \Leftrightarrow & xx'^{-1} & \in & N \\ \Leftrightarrow & f\left(xx'^{-1}\right) & = & e \\ \Leftrightarrow & f(x) & = & f(x'). \end{array}$$

Deshalb ist $\bar{f}$ wohldefiniert und sogar injektiv. Dass $f = \bar{f} \circ p$ gilt, folgt vor der Definition.

Nun

$$\begin{array}{rcl} \bar{f}\Big(\text{Klasse } (x)\text{Klasse } (x')\Big) & = & \bar{f}\Big(\text{Klasse } (xx')\Big) \\ & = & f(xx') \\ & = & f(x) \cdot f(x') \\ & = & \bar{f}\Big(\text{Klasse } (x)\Big) \cdot \bar{f}\Big(\text{Klasse } (x')\Big). \end{array}$$

Deshalb ist $\bar{f}$ ein Homomorphismus. Der Beweis des Satzes ist jetzt fertig.

Es bleibt noch, etwas über Abbildungen zwischen G-Mengen zu sagen. Der am häufigsten vorkommende Begriff ist der eines G-Morphismus oder einer G-Abbildung zwischen zwei G-Mengen. Seien X, Y G-Mengen; eine Abbildung $f : X \to Y$ heißt ein *G-Morphismus* (oder eine *G-Abbildung*), wenn die folgende Bedingung erfüllt ist:

MM: Für $x \in X, g \in G$ gilt $f(gx) = gf(x)$.
Die Abbildung

$$I : G/H \to H/G$$

von Kapitel I., 2. ist ein G-Monomorphismus.

Es gibt aber auch noch andere Beziehungen zwischen G-Mengen. Zum Beispiel betrachten wir einen Homomorphismus $f : G_1 \to G_2$ und eine G_2-Menge X. Diese G_2-Menge wird eine G_1-Menge durch

$$G_1 \times X \to X \quad ; \quad (g, x) \longmapsto f(g)x.$$

Auf diese Weise erhalten wir eine Abbildung, die mit f^* bezeichnet wird,

$$f^* : \text{Men}(G_2) \to \text{Men}(G_1).$$

Es ist bemerkenswert, dass f^* "in der entgegengesetzten Richtung zu f" geht. Es ist auch möglich, eine Abbildung

$$f_* : \text{Men}(G_1) \to \text{Men}(G_2)$$

zu definieren. Obwohl diese Definition hier kaum benutzt wird, wird sie der Gründlichkeit halber angegeben. Sei X eine G_1-Menge. Man bildet die Menge $G_2 \times X$. Auf dieser Menge konstruiert man die Äquivalenzrelation $\sim$ durch:

$$(h, x) \sim (h', x'),$$

wenn es ein $\gamma \in G_1$ gibt, so dass gilt

$$h' = hf(\gamma)^{-1} \quad , \quad x' = \gamma x.$$

Wir definieren $f_*(X)$ als den Quotientenraum $(G_2 \times X)/\sim$. Sei $[h, x]$ die Klasse von (h, x). Dann wird $(G_2 \times X)/\sim$ eine G_2-Menge durch

$$\begin{array}{rcl} G_2 \times \Big((G_2 \times X)/\sim\Big) & \to & (G_2 \times X)/\sim; \\ (g, [h, x]) & \longmapsto & [gh, x]. \end{array}$$

Diese Konstruktion hat mehrere interessante Eigenschaften, wovon einige als Aufgaben erscheinen werden.

4. Beispiele

Folgendes sind Beispiele von Gruppen:

1. $\mathbb{Z}$ Identität = 0 "Multiplikation" = Addition

   Sei K ein Körper.
2. K Identität = 0 "Multiplikation" = Addition
3. $K^\times := K - \{0\}$ Identität = 1 "Multiplikation" = Multiplikation

   Sei V ein über K definierter Vektorraum.
4. V Identität = 0 "Multiplikation" = Addition

Die nächsten Beispiele sind solche, wo nicht nur eine Gruppe G, sondern auch eine G-Menge X gleich von Anfang an definiert wird.

5. Sei X eine Menge, $S(X)$ die Menge von allen Bijektionen $\alpha : X \to X$. In $S(X)$ nimmt man als Identität die Abbildung $e : e(x) = x$. Mit der Verknüpfung als "Multiplikation" wird $S(X)$ eine Gruppe.

   Im Spezialfall $X = \{1, 2, \ldots, n\}$ schreibt man Σ_n statt $S(\{1, \ldots, n\})$. Die ist die "symmetrische Gruppe" und wird eine große Rolle spielen.
   (Man kann die Konstruktion von $S(X)$ verallgemeinern, wenn man eine G-Menge X nimmt und statt $S(X)$ die Menge $S_G(X)$ der G-Morphismen $\alpha : X \to X$ in Betracht zieht. Die Gruppe $S_G(X)$ ist einer Untergruppe von $S(X)$.)

6. Sei V ein über K definierter Vektorraum. Sei $GL(V)$ die Menge aller bijektiven, *linearen* Abbildungen $\alpha : V \to V$. In $GL(V)$ nimmt man als Identität die Abbildung $E : E(x) = x$. Mit der Verknüpfung als "Multiplikation" wird $GL(V)$ eine Gruppe. V ist ein $GL(V)$-Raum.

   Im Fall, dass V endlich dimensional ist, ist die Abbildung

   $$\det : GL(V) \to K^\times \quad ; \quad \alpha \longmapsto \det(\alpha),$$

   ein Homomorphismus. Der Kern von det wird mit $SL(V)$ bezeichnet.

   Man schreibt $GL_n(K)$, $SL_n(K)$ statt $GL(K^n), SL(K^n)$.
   (Hier bedeutet GL "general linear" (= allgemein linear) und SL "special linear" (= speziell linear).)

7. Sei V ein über K definierter Vektorraum, $b : V \times V \to K$ eine Bilinearform. Dann bildet man

   $$O(V, b) = \{\alpha \in GL(V) : b(\alpha x, \alpha y) = b(x, y)(x, y \in V)\}.$$

(Meistens wird die Bezeichnung nur für den Fall, dass b symmetrisch ist, angewandt.)

Dann ist $O(V, b)$ eine Untergruppe von $GL(V)$. Darüber hinaus ist V auch eine $O(V, b)$-Menge.

Im Falle, dass $V = \mathbb{R}^n$ und $b = \langle , \rangle$ (das euklidische innere Produkt) genommen werden, schreibt man gewöhnlich $O_n(\mathbb{R})$ (oder O_n) statt $O(\mathbb{R}^n, \langle , \rangle)$.

Zum Schluß sollte es betont werden, dass die hier angeführten Beispiele großen, allgemeinen Klassen angehören. Viele der interessantesten Gruppen sind "Einzelgänger". Sie haben Eigenschaften, die durch "Zufälle" entstehen und sehr lohnenswert zu studieren sind. Beispiele sind die Symmetriegruppen der regulären Polyeder (Tetraeden, Würfel, Oktaeder, Ikosaeder, Dodekaeder), die wir später kennenlernen werden. Oder die Kleinsche Gruppe der 168 Elementen.

Kapitel 2

Gruppentheorie und Geometrie

1. Über Euklidische Geoemtrie

Es ist auf den ersten Blick gar nicht klar, dass die klassische Geometrie überhaupt etwas mit Gruppentheorie zu tun hat. Man braucht aber nur die Grundlagen mit anderen Augen zu sehen, um den Zusammenahng zu erkennen.

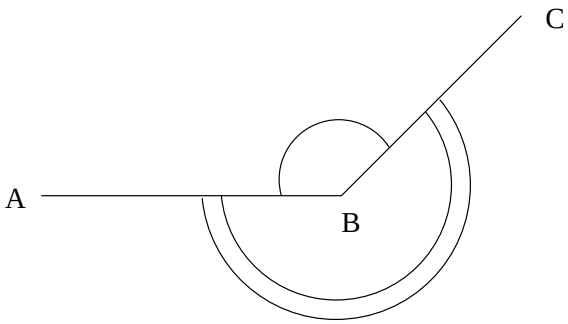
In der Geometrie ist die Möglichkeit, zwei Gegenstände zu vergleichen, die wichtigeste Sache. Zwei Strecken haben dieselbe Länge, wenn wir die eine genau auf die andere legen können. Mit demselben Verfahren können wir *definieren*, ob eine Strecke länger oder kürzer als eine andere ist. Die Möglichkeit, Länge von Strecken und Abstände zu vergleichen haben wir, wenn wir sie in eine günstige Lage bewegen können und wenn das Ergebnis nicht von der gewählten Lage abhängt.

Man sollte bemerken, dass es noch nicht in Frage gekommen ist, Längen und Abstände zu *messen*; bis jetzt kann man "nur" Aussagen der Art

$$AB > CD \quad , \quad AB = CD$$

machen. Um Längen zu *messen*, braucht man eine *Standardlänge* und die Eudoxossche Proportionalitätslehre, wovon später die Rede sein wird.

Ähnlich kann man Winkel vergleichen. Hier wird ein System von drei Punkten, geschrieben $\sphericalangle ABC$, gegeben; man kann durch verschiedene Regeln solche vergleichen. Es ist in diesem Fall schwieriger, die Regeln aufs Papier zu bringen, weil man zwischen äußerem und innerem Winkel unterscheiden muß. Normalerweise benutzt man Bilder und Vernunft.



Wenn man soviel festgelegt hat, fängt man an, Dreiecke zu vergleichen. Ein Dreieck ist auch durch drei Punkte (die drei Ecken) anzugeben; es wird $\triangle ABC$ geschrieben, wobei $\triangle ABC, \triangle BAC, \triangle BCA$, usw. nicht unterscheidbar sind. Wenn von zwei Dreiecken eins durch eine Bewegung (vielleicht auch eine Spiegelung) genau auf das andere gelegt werden kann, sagt man, dass die Dreiecke *kongruent* sind.

Fast die ganze euklidische Geometrie stützt sich auf die folgenden Kriterien dafür, dass zwei Dreiecke, $\triangle ABC$ und $\triangle A'B'C'$, kongruent sind:

1. Gelten $AB = A'B', BC = B'C', C'A' = CA$, dann sind $\triangle ABC$ und $\triangle A'B'C'$ kongruent.
2. Gelten $AB = A'B', BC = B'C', \sphericalangle ABC = \sphericalangle A'B'C'$, dann sind $\triangle ABC$ und $\triangle A'B'C'$ kongruent.
3. Gelten $AB = A'B', \sphericalangle CAB = \sphericalangle C'A'B', \sphericalangle ABC = \sphericalangle A'B'C'$, dann sind $\triangle ABC$ und $\triangle A'B'C'$ kongruent.

Genauer ausgedrückt, kann $\triangle A'B'C'$ ind $\triangle ABC$ so bewegt werden, dass A' auf A, B' auf B und C' auf C liegen. ("Bewegen" schließt hier auch Spiegelungen ein.)

Von diesen Kriterien kann sehr viel aufgebaut werden. Sie müssen aber vorausgesetzt werden, da sie sich nicht aus etwas Einfacherem herleiten lassen. Natürlich entsprechen sie unserer Anschauung. (Eigentlich können die drei Kriterien auf eines reduziert werden; diese Tatsache ist aber für uns nicht wichtig.)

In der euklidischen Geometrie hat man auch den Begriff paralleler Strecken oder Geraden. Man kann diesen Begriff so erkären: alle Strecken durch A, die in einem gegebenen Strahl (oder einer Halbgeraden) liegen, definieren eine *Richtung*.

Es ist nun möglich, Richtungen in verschiedenen Punkten zu vergleichen. Dieses geht jedenfalls aus unseren alltäglichen Erfahrungen hervor. Um dies auszudrücken, nehmen wir an, dass wenn zwei Punkte A und A' gegeben sind, es eine ausgezeichnete und eindeutig bestimmte Bewegung gibt, die A in A' schickt. Mit dieser Bewegung können wir die Richtungen in A und A' vergleichen. Diese Bewegung sollte die durch A und A' laufenden Geraden in sich schicken; diese Eigenschaft -nimmt man an- definiert die Bewegung völlig. Weiter werden vorausgesetzt:

1. Wenn die Richtung von AB nicht mit der von AA' oder der entgegengesetzten Richtung übereinstimmt, dann haben AB und das Bild von AB keine gemeinsamen Punkte.

2. Die Verknüpfung von der eben definierten Bewegung von A nach A' und von A' nach A'' ist die von A nach A''.

Eine Bewegung dieser Art heißt eine *Parallelverschiebung* oder eine *Translation*.

Wir können jetzt alles zusammenfassen, obwohl wir nochmal zu Euklid zurückkehren müssen. In der Geometrie wird eine Menge $\mathbb{A}$ (die affine Ebene) vorausgesetzt. Paare von Punkten aus $\mathbb{A}$ definieren Strecken. Es gibt eine Gruppe von Bewegungen von $\mathbb{A}$, die wir mit $\mathbb{E}$ (nach Euklid) bezeichnen werden. Auf diese Weise wird $\mathbb{A}$ eine $\mathbb{E}$-Menge. Die Gruppe $\mathbb{E}$ ist groß genug, um Strecken miteinander vergleichen zu können. Auch können Winkel verglichen werden. Darüberhinaus liefern die Kriterien, ob zwei Dreiecke kongruent werden, die Existenz von geeigneten Elementen von $\mathbb{E}$.

Innerhalb von $\mathbb{E}$ gibt es eine Untergruppe, die aus Translationen besteht. Diese bezeichnen wir mit $\mathbb{T}$. Zu jedem Paar A, A' von Punkten aus $\mathbb{A}$ gibt es genau ein $t \in T$, so dass gilt $t(A) = A'$. Es wird auch angenommen, dass $\mathbb{T}$ ein Normalteiler von $\mathbb{E}$ ist. Dies entspricht auch der geometrischen Intuition.

Es sollte hier auch erwähnt werden, dass Kreise jetzt ganz natürlich entstehen. Sei $P \in \mathbb{A}$. Sei $\mathbb{E}_P$ die Stabilisatorgruppe von P, d.h.

$$\mathbb{E}_P = \{g \in \mathbb{E} : g(P) = P\}.$$

Sei $Q \in A$. Dann ist die Bahn von Q unter $\mathbb{E}_P$ ein Kreis, wovon P der Mittelpunkt ist.

Sollten wir eine Länge *messen* wollen, müssen wir eien gegebene Strecke mit einer Standardstrecke vergleichen. Das heißt, dass wir von dem Verhältnis $AB : CD$ reden können müssen. Es ist dann möglich, Gleichheit von zwei Verhältnissen zu definieren. Diese Gleichheit wird

$$AB : CD :: A'B' : C'D'$$

geschrieben. Es ist auch möglich, "größer" oder "kleiner" zu definieren.

Es liegt dann nahe, alle Transformationen von der Ebene zu betrachten, die die Verhältnisse gleichlassen. Diese heißen in der klassischen Geometrie *Ähnlichkeitstransformationen*, man redet von ähnlichen Dreiecken und anderen Gebilden. Diese wurden auch von Euklid gründlich untersucht. Sei $\tilde{\mathbb{E}}$ die Menge aller Ähnlichkeitstransformationen. Sie ist auch eine Gruppe, $\tilde{\mathbb{E}} \supset \mathbb{E}$.

Diese Skizze der klassischen Geometrie sollte klarmachen, dass hinter der herkömmlichen Sprache der Gruppenbegriff liegt. Zu Euklids Zeit studierte man die Gebilde und nicht die Bewegungen, die uns erlauben, verschiedene Gebilde zu vergleichen. Die Bewegungsgruppe in den Vorgrund zu stellen ist ein viel

abstrakteres Vorgehen. Es ist dadurch gerechtfertigt, dass dieselben Ideen auf andere Gebiete angewendet werden können und umgekehrt, dass Ideen von jenen anderen Gebieten neues Licht auf alte Probleme der Geomtrie werden. Zum Beispiel wird es viel anschaulicher, was die Unabhängigkeit des Parallelenaxioms anbetrifft. Davon wird in Kapitel II, 3. wieder die Rede sein.

2. Die kontinuierlichen Gruppen der Geometrie

Die Grundzüge der Geometrie, die eben beschrieben worden sind, haben nichts mit der Identifizierung der Ebene mit $\mathbb{R}^2$ zu tun gehabt. Dass eine solche Identifizierung gemacht wurde, war eine große Entdeckung Descartes, die einen bisher ungeahnten Zusammenhang zwischen Geometrie und Arithmetik herstellte. Dieser Zusammenhang ist jetzt natürlich zentral in der Behandlung geometrischer Probleme.

Wir sollten uns daran erinnern, wie dieser Zusammenhang zustande kam. Die Gruppe $\mathbb{T}$ ist abelsch. Die "Multiplikation" (d.h. Verknüpfung) in $\mathbb{T}$ wird mit "+" bezeichnet. Die betrachten $\mathbb{R}$ als die Menge aller möglichen Verhältnisse $AB : CD (C \neq D)$. Aus der Eudoxosschen Proportionalitätslehre geht hervor, dass für $\lambda \in \mathbb{R}, t \in \mathbb{T}$ ein Element λt von $\mathbb{T}$ definiert werden kann. Es ist dann nicht schwierig einzusehen, dass $\mathbb{T}$ ein $\mathbb{R}$-Vektorraum wird. $\mathbb{T}$ hat sogar die Dimension 2.

Nach den im letzten Abschnitt gemachten Bemerkungen ist A ein $\mathbb{T}$-affiner Raum. Bis jetzt ist es nicht nötig gewesen, überhaupt eine Wahl ausgezeichneter Punkte zu treffen. Wir können einen *Ursprung* U von $\mathbb{A}$ und eine *Basis* e_1, e_2 von $\mathbb{T}$ wählen. Dann kann jeder Punkt von $\mathbb{A}$ in der Form $\big(x_1 e_1 + x_2 e_2\big)(U)$ $\big(x_1, x_2 \in \mathbb{R}\big)$ geschrieben werden. Dies ist die kartesische Darstellung von A.

Sei U ein Punkt aus $\mathbb{A}$ und $\mathbb{E}_U$ die Stabilisatorgruppe von U in $\mathbb{E}$. Sei g ein willkürlich gewähltes Element von $\mathbb{E}$. Dann ist $g(U)$ von der Form $t_g(U)$, wobei t_g ein eindeutig bestimmtes Element aus $\mathbb{T}$ ist. ann gilt

$$g(U) = t_g(U)$$

und auch

$$\big(t_g\big)^{-1} g(U) = U.$$

Deswegen gilt

$$\big(t_g\big)^{-1} g \in \mathbb{E}_U$$

und g kann eindeutig als $t_g r_g$ geschrieben werden, wobei $t_g \in \mathbb{T}, r_g \in \mathbb{E}_U$ liegen. (Hier bedeutet "t_g" Translation, "r_g" Rotation = Drehung.)

Wir erinnern uns daran, dass $\mathbb{T}$ ein Normalteiler von $\mathbb{E}$ sein sollte. Deshalb gilt

$$rtr^{-1} \in \mathbb{T} \quad (t \in \mathbb{T}, r \in \mathbb{E}_U).$$

Die Abbildung

$$t \longmapsto rtr^{-1}$$

ist linear, wir schreiben $t \longmapsto {}^r t$.

Wir können dann jedes Element von $\mathbb{E}$ als (t, r) schreiben und

$$\begin{aligned} (r,t) \cdot (t', r') &= t \cdot r \cdot t' \cdot r' \\ &= t \cdot rt'r^{-1} \cdot r \cdot r' \\ &= \big(t +^r t', rr'\big) \qquad (*) \end{aligned}$$

(Wenn wir $\mathbb{T}$ betrachen, schreiben wir die Verknüpfung als $+$; dagegen, wenn wir $\mathbb{T}$ als eine Untergruppe von $\mathbb{E}$ betrachten, schreiben wir sie als "$\cdot$".)

Es folgt, wenn wir $\mathbb{T}, \mathbb{E}_U$ und die Operation von $\mathbb{E}_U$ auf $\mathbb{T}$, die jetzt eine $\mathbb{E}_U$-Menge geworden ist, kennen, können wir durch $(*)$ die Gruppe $\mathbb{E}$ rekonstruieren.

Wir können dies alles "konkreter" machen. Zuerst können wir $\mathbb{E}_U$ mit

$$O_2(\mathbb{R}) = \{g \in M(2 \times 2, \mathbb{R}); \langle gx, gx' \rangle = \langle x, x' \rangle\}$$

identifizieren, wobei $\langle , \rangle$ das übliche Skalarprodukt bezeichnet. Diese Aussage ist im Grunde genommen äquivalent zum Pythagoras'schen Lehrsatz. Sie kommt zustande, weil $\mathbb{E}_U$ Winkel nicht ändert.

Wenn wir $\mathbb{A}$ mit $\mathbb{R}^2$ identifizieren, dann ist $\mathbb{E}$ die Gruppe aller Bewegungen der Form

$$\underline{x} \longmapsto g(\underline{x}) + \underline{y} \qquad \left(g \in O_2(\mathbb{R}), \underline{y} \in \mathbb{R}^2\right).$$

Die Untergruppe von Bewegungen der Form

$$\underline{x} \longmapsto \underline{x} + \underline{y} \qquad \left(\underline{y} \in \mathbb{R}^2\right)$$

ist $\mathbb{T}$.

Wir können diese Gruppe mit 3×3 Matrizen darstellen. Wir ordnen $\underline{x} \to g(\underline{x}) + \underline{y}$ die Matrix

$$\begin{array}{cc} & \\ 2 & \\ 1 & \end{array} \begin{pmatrix} g & \underline{y} \\ 0 & 1 \end{pmatrix} \begin{array}{cc} & \\ & \\ 2 & 1 \end{array}$$

zu. Dann gilt mit Matrizenmultiplikation

$$\begin{pmatrix} g & \underline{y} \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} \underline{x} \\ 1 \end{pmatrix} \quad = \quad \begin{pmatrix} g\underline{x} + y \\ 1 \end{pmatrix},$$

wobei $\begin{pmatrix} \underline{x} \\ 1 \end{pmatrix}$ den Spaltenvektor $\begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix}$ bedeutet, wenn $\underline{x}$ der Spaltenvektor $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ ist. Auf diese Weise erhalten eine "analytische" Darstellung der Gruppe $\mathbb{E}$. Ähnlich kann man $\widetilde{\mathbb{E}}$ darstellen. Man braucht nur $O_2(\mathbb{R})$ durch die Gruppe

$$\widetilde{O}_2(\mathbb{R}) = \{g \in M(2 \times 2; \mathbb{R}) : \text{es gibt } \lambda_g \in \mathbb{R} - \{0\}, \\ \text{so dass gilt } \langle gx, gx' \rangle = \lambda_g \langle x, x' \rangle\}$$

zu ersetzen. Diese ist die Gruppe *konformer* Transformationen. Weil darunter die Funktion

$$\frac{\langle \underline{x}, \underline{x'} \rangle}{\langle \underline{x}, \underline{x} \rangle^{\frac{1}{2}} \langle \underline{x'}, \underline{x'} \rangle^{\frac{1}{2}}}$$

erhalten bleibt, bleiben auch Winkel erhalten. Längen werden aber durch einen Faktor von λ_g geändert.

Ähnliche Definitionen können für Geometrien höherer Dimensionen angegeben werden. Für unserer Zwecke reicht es vollkommen aus, nur 2-dimensionale Geometrien in Betracht zu ziehen.

Eine solche Darstellung der Geometrie ist eine Zusammenfassung der bisherigen Errungenschaften. Natürlich ist es viel einfacher, praktische Probleme mit analytischen Methoden zu lösen. Es gibt aber auch andere Entwicklungen der Geometrie, die sie wiederrum in ein neues Licht setzen.

3. Axiomatik und Geometrie

In Kapitel II, 1. wurde die euklidische Geometrie knapp zusammengefaßt. Wir werden jettz die euklidische Methodik etwas genauer anschauen.

Das Wesentliche, das man in der Geometrie nie vergessen sollte, liegt darin, dass die Geometrie eine Abstrahierung unserer Wahrnehmung der physikalischen Welt darstellt. Die räumliche Wahrnehmung ist eine charakteristische menschliche Fähigkeit, die unserem logischen Denken zu Grunde liegt. Es ist dann nicht verwunderlich, dass die Geometrie eine der ältesten Wissenschaften ist. Man sollte aber nicht durch dieses Alter dazu verführt werden, den physikalischen Ursprung der Geometrie zu vergessen und sie als ein logisches Spiel aufzufassen.

Zu Euklids Zeit hatte man schon erkannt, dass -ausgehend von einigen offensichtlichen geometrischen Eigenschaften- man durch eine Kette logischer Schlüsse zu geometrischen Eigenschaften gelangen könnte, die gar nicht offensichtlich sind. Das klassische Beispiel dafür ist der Pythagoras'sche Lehrsatz. Vielleicht genauso auffallend ist die Konstruktion des Ikosaeders oder Dodekaeders und der Nachweis, dass diese die "kompliziertesten" regulären Körper sind.

Euklid stellte deshalb am Anfang eine Liste von Axiomen auf. Diese sollte geometrischen "Tatsachen" sein, die niemand anzweifeln könnte. Das Wort "Axiom" stammt von dem Wort "axios" = richtig. Es ist aber von großer Tragweite, dass viele Mathematiker das Parallelenaxiom nicht als anschaulich empfunden hatten und (vergeblich) versucht haben, es von den anderen (sicheren) Axiomen herzuleiten.

Nachdem er die Axiome aufgestellt hatte, leitete Euklid daraus Sätze ab. Diese sind von zunehmender "Tiefe"; viele sind jedenfalls gar nicht anschaulich, was vom Pythagoras'schen Lehrsatz belegt wurde. Eigentlich führte Euklid sein Vorhaben nicht rigoros durch. Es kann aber gemacht werden und wurde ca. 1900 von D. Hilbert vollendet.

Heutzutage wird die Axiomatik anders aufgefaßt. Man erkennt, dass es eine große Freiheit bei der Auswahl der Axiome gibt. Ganz allgemein benutzt man die Axiomatik, um die Struktur eines Arguments darzulegen. Zum Beispiel haben wir sie angewendet, um Vektorräume zu definieren (Teil I). Die dabei gewonnenen Sätze hatten die größtmögliche Allgemeinheit.

Wie in diesem Beispiel kann es leicht passieren, dass mehr als ein Objekt die Axiome erfüllen. Die Menge von allen Objekten, die ein Axiomsystem erfüllen, heißt eine *Kategorie*, wenn wir auch die zwischen den verschiedenen Objekten bestehenden Beziehungen in Betracht ziehen. Davon wird hier nicht weiter die Rede sein.

Ein Objekt, das ein Axiomensystem erfüllt, heißt *ein Modell* für das System. So ist z.B. jede Gruppe ein Modell für die Gruppenaxiome.

Es kann auch passieren, dass es in der Geometrie mehrere Modelle für ein Axiomensystem gibt. Die unerwarteten (sog. nichtstandarden) Modelle können auch von großem Interesse sein.

Wir können auch Axiomensysteme abändern, wenn wir einige Eigenschaften als unwichtig betrachten. Wir könnten z.B. ein Dreieck nur als Dreieck ohne Berücksichtigung der Seitenlängen und Winkel betrachten.

Um die in den letzten zwei Abschnitten erwähnten Punkte zu erläutern, schauen wir uns das Beispiel der projektiven Geometrie an.

In dieser Geometrie gehen wir von zwei Mengen E_P und E_G aus. die zugehörigen Elemente heißen *Punkte* und *Geraden*. Wir haben eine Relation $\vdash$ zwischen E_P und E_G. $''a \vdash L''(a \in E_P, L \in E_G)$ bedeutet: a ist ein Punkt von L. Wir schreiben auch $''L \vdash a''$, ausgesprochen $''L$ geht durch a''.

Die Grundaxiome sind

PG 1: Seien $a_1, a_2 \in E_P, a_1 \neq a_2$. Dann gibt es genau $L \in E_G$, so dass gilt

$$a_j \vdash L \qquad (j = 1, 2).$$

PG 2: Seien $L_1, L_2 \in E_G, L_1 \neq L_2$. Dann gibt es genau ein $a \in E_P$, so dass gilt

$$L_j \dashv a \qquad (j = 1, 2).$$

Wir könnten auch ein weiteres Axiom hinzufügen, nämlich

PG 3: Es gibt eine Gruppe G, so dass

(i) E_P, E_G G-Mengen sind,

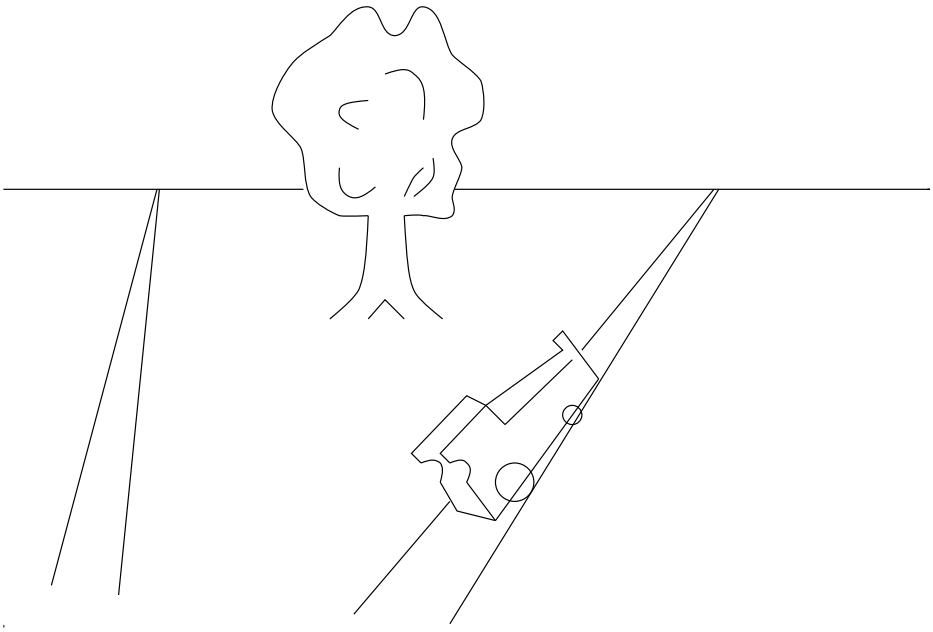
(ii) $g(a) \vdash g(L) \Leftrightarrow a \vdash L$ für $g \in G$ gilt
und

(iii) wenn $a_1, a_2, a_3, b_1, b_2, b_3 \in E_P$ (a_1, a_2, a_3 (bzw. b_1, b_2, b_3) nicht alle auf einer Gerade) gegeben werden, dann gibt es ein $g \in G$, so dass gilt:

$$g(a_1) = b_1, \quad g(a_2) = b_2, \quad g(a_3) = b_3.$$

Mit anderen Worten: jedes Dreieck kann in jedes andere geschickt werden. Wie wir gesehen haben, ist PG 3 nicht eine Folgerung von PG 1 und PG 2.

Wir stellen einige Modelle vor. Man könnte den Einwand erheben, dass PG 1 und PG 2 nicht unserer Institution entsprechen, weil zwei parallele Geraden sich nicht schneiden. Doch ist die projektive Geometrie aus der Praxis der Malerei entstanden. Wir stellen uns die Ebene als Landschaft vor, worüber wir 2 Meter (ungefähr) stehen. Dann sehen Eisenbahnschienen bekanntlich so aus:



Dasselbe passiert hinter unseren Köpfen. Wir werden zu der Ebene eine ideale Gerade $\mathcal{T}$ hinzufügen - den Horizont. Wir müssen das, was sich hinter unseren Köpfen abspielt, und das, was vor unseren Augen sichtbar ist, "identifizieren" - sonst würden sich zwei parallele Geraden in zwei Punkten schneiden.

In der Ebene selbst können wir die Punkte der neuen Gerade $\mathcal{T}$ mit Scharen paralleler Geraden identifizieren. Genauer: sei $\mathcal{T}$ die Menge der Äquivalenzklassen der Geraden in der Ebene unter der Äquivalenzrelation "parallel". Mit diesen Vorbereitungen können wir das erste Modell beschreiben:

1. Modell:
$E_P := \mathbb{A} \cup \mathcal{T}$
$E_G := \{G : G \text{ eine Gerade in } \mathbb{A}\} \cup \{\mathcal{T}\}$

(i) Seien G_1 und G_2 nicht-parallele Geraden. Dann scheiden sich G_1 und G_2 wie üblich in $\mathbb{A}$.

(ii) Sei G eine in $\mathbb{A}$ liegende Gerade. Dann schneiden sich G und $\mathcal{T}$ in einem Punkt, der mit $I(G)$ bezeichnet wird. Hier stellt $I(G)$ die Äquivalenzklasse von G in $\mathcal{T}$ dar. Ist G' zu G parallel, dann gilt $I(G') = I(G)$; G und G' schneiden sich in $I(G)$.

(iii) Jeder Punkt von $\mathcal{T}$ ist von der Form $I(G)$ für irgendeine Gerade G, $G \neq \mathcal{T}$. Sei a ein Punkt von $\mathbb{A}$. Dann ist die durch a und $I(G)$ laufende Gerade diejenige, die durch a läuft und parallel zu G ist.

2. Modell:
In diesem Modell spielt sich alles im $\mathbb{R}^3$ ab.

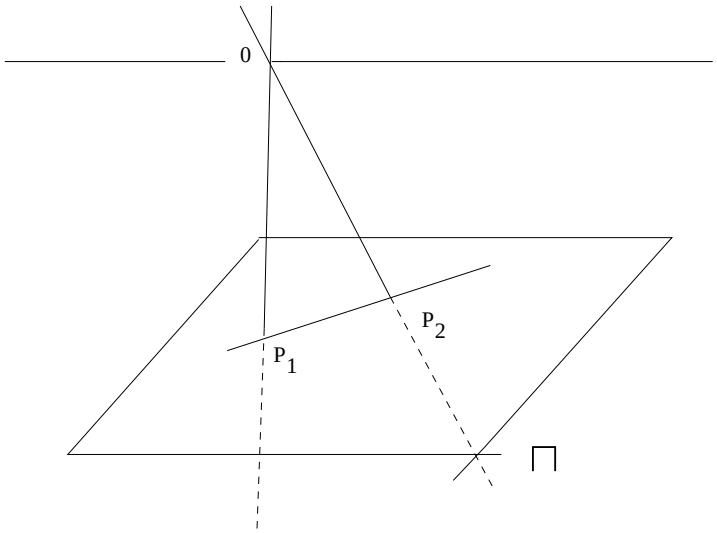
E_P = Menge der durch den Ursprung laufenden Geraden.
E_G = Menge der durch den Ursprung laufenden Ebene.

Es ist leicht einzusehen, dass die Axiome erfüllt sind.

Diese beiden Modelle hängen eng zusammen.

Sei Π eine im $\mathbb{R}^3$ liegende Ebene, die nicht durch den Ursprung läuft. Zu jedem $e \in E_G$, e nicht zu Π parallel, erhalten wir eine Gerade in Π durch Bildung von $\Pi \cap e$. Das einzige $e_\Pi \in E_G$, das zu Π parallel ist, entspricht $\mathcal{T}$ (für Π). Dieses Verfahren können wir genauso mit den Geraden durch den Ursprung fortsetzen, weil diese Punkte von Π oder $\mathcal{T}$ erzeugen.

Von drei Dimensionen auf zwei zu gehen, ist genau das, was die Maler machen.



Die Bezeichnung "projektive Geometrie" erhält dadurch ihre Rechtfertigung; wir projezieren den Raum auf eine Ebene, die Leinwand.

Da es sich im zweiten Modell um lineare Unterräume von $\mathbb{R}^3$ handelt, sieht man sofort, dass die ganze Gruppe $GL_3(\mathbb{R})$, der linearen Abbildung auf E_P und E_G operiert und dass PG 3 dadaurch erfüllt ist. Dies war beim ersten Modell nicht ersichtlich. Man kann diese Gruppe auch anwenden, um festzustellen, was passiert, wenn man die oben gewählte Ebene Π durch eine andere ersetzt, weil $GL_3(\mathbb{R})$ auf der Menge solcher Ebenen transitiv operiert.

Für das dritte Modell nehmen wir die Sphäre

$$S = \left\{ \underline{x} \in \mathbb{R}^3 : \| \underline{x} \|^2 = 1 \right\}.$$

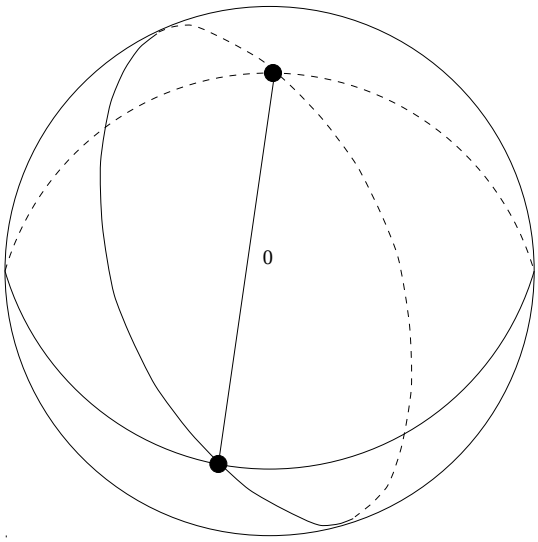
Auf S stellen wir eine Äquivalenzrelation auf;

$$\underline{x} \sim \underline{y} \Leftrightarrow \underline{x} = \underline{y} \text{ oder } -\underline{y}.$$

Dann ist E_P der Quotientenraum; E_P besteht aus Paaren von Antipoden (gegenüberliegende Punkte). Eine Gerade entspricht dem von S mit einer druch den Ursprung laufenden Ebene gebildeten Schnitt - einem *Großkreis*.

3. Modell:
Sei E_P wie oben. Sei E_G die Menge aller Großkreise, als Untermengen von E_P aufgefaßt. Dann ist E_P, E_G eine projektive Geometrie.

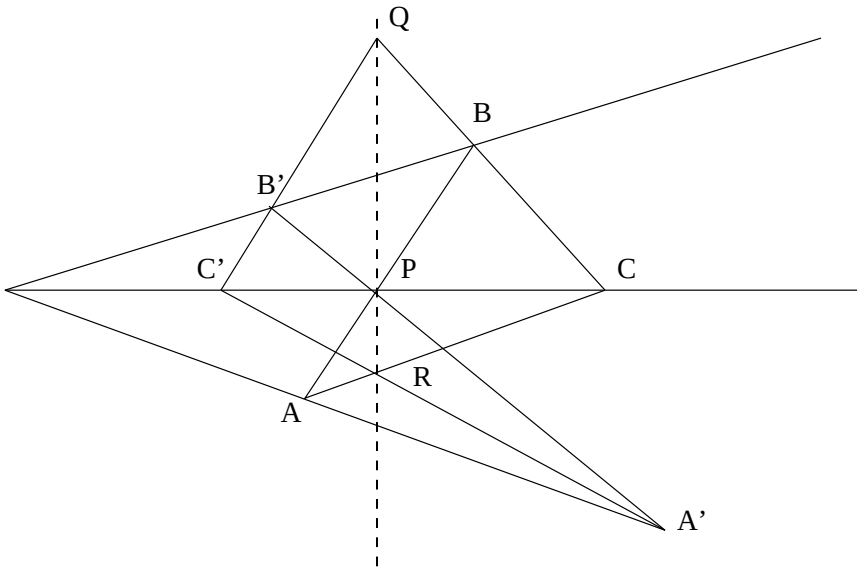
Sogar diese läßt sich auch von dem zweiten Modell herleiten. Der Schnitt von S mit einer durch 0 laufenden Gerade besteht aus zwei Antipoden. Der Schnitt von S mit einer durch 0 laufenden Ebene ist ein Großkreis.



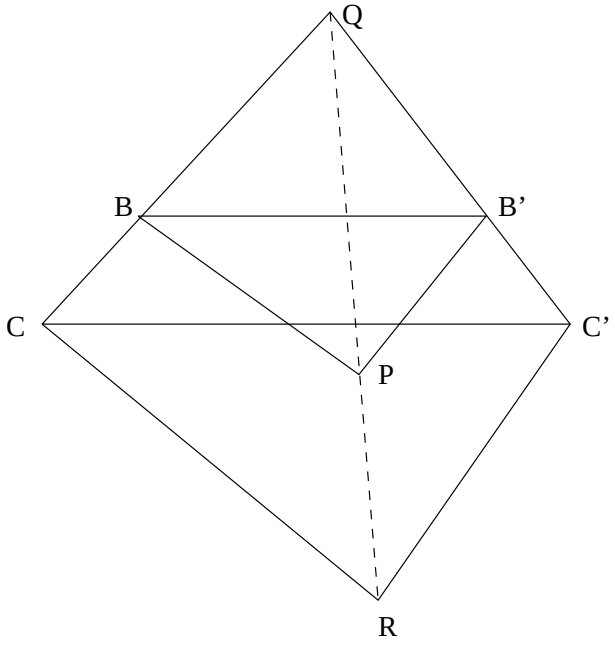
Bevor wir zu anderen Beispielen übergehen, sollten wir bemerken, dass die Axiome in E_G und E_P symmetrisch sind. Deshalb können wir ihre Rollen vertauschen. Jedem Satz entspricht ein "Dualsatz", worin wir Punkte und Geraden vertauscht haben. Dieses Phänomen heißt *Dualität.*

Wir betrachten als Beispiel -etwas oberflächlich, weil wir später dahin zurückkehren werden- den Satz von Desargues.

Satz. *Seien ABC und $A'B'C'$ zwei Dreiecke, so dass sich die Verlängerungen von AA', BB' und CC' in einem Punkt treffen. Sei P (bzw. Q, R) der Schnitt von den Verlängerungen von AB (bzw. BC, CA) und $A'B'$ (bzw. $B'C', C'A'$). Dann liegen P, Q, R alle auf einer Geraden.*



Der Dualsatz ist die Umkehrung davon. Für den *Beweis* kann man aus dem 2. Modell annehmen, dass PG 3 gilt. Dann dürfen wir annehmen, dass die Gerade AA' auf $\mathcal{T}$ liegt und sich deshalb die Verlängerungen von AA', BB' und CC' auf $\mathcal{T}$ schneiden, da BB' und CC' parallel zu AA' sind. Dann sieht das Bild so aus:



Hier sind BB' und CC', BP und CR, PB' und RC' parallel. Wir müssen zeigen, dass PQR auf einer Geraden liegen. Stattdessen definieren wir R als den Schnitt von CR und der Verlängerung von QP, wobei CR parallel zu BP ist. Wir müssen dann zeigen, dass RC' zu PB' parallel ist.

Um dieses zu tun, können wir Betrachtungen aufwenden, die nicht zur projektiven Geometrie gehören. Wegen Parallelität gilt

$$\sphericalangle PBB' \quad = \quad \sphericalangle RCC'.$$

Aus demselben Grund gilt

$$BP : CR :: BQ : CQ :: BB' : CC'.$$

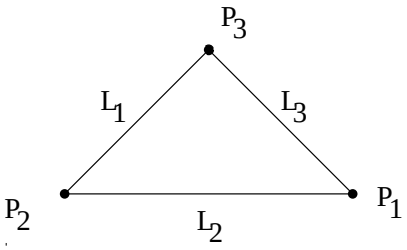
Deshalb sind $\triangle PBB'$ und $\triangle RCC'$ ähnlich. Es gilt daher

$$\sphericalangle BB'P \quad = \quad \sphericalangle CC'R;$$

deshalb sind PB' und RC' parallel wie behauptet. Durch dieses Beispiel wird es klar, wie nützlich es sein kann, wenn eine größere Gruppe vorhanden ist. Dann kan man ein Problem auf ein einfacheres reduzieren und dort zusätzlich Methoden anwenden.

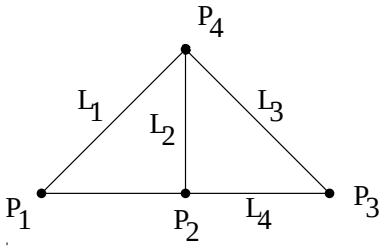
Nun stellen wir einige Modelle auf, worin E_P und E_G endlich sind.

4. Modell:
$E_P = \{P_1, P_2, P_3\}, E_G = \{L_1, L_2, L_3\}$.
P_1 liegt auf L_2 und L_3 usw. Dieses Modell können wir folgendermaßen graphisch darstellen:

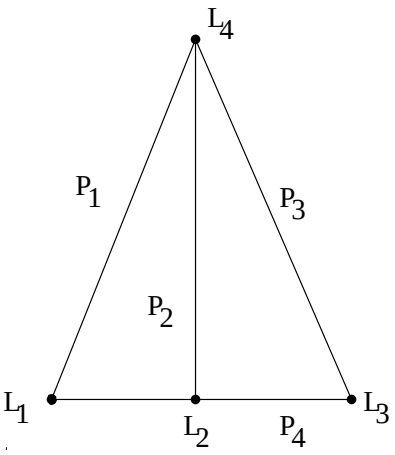


Hier genügt die Geometrie PG 3 (warum?). Wie die oben angegebenen Modelle ist dieses auch "gleich" seinem Dualmodell.

5. Modell:
$E_P = \{P_1, P_2, P_3, P_4\}, E_G = \{L_1, L_2, L_3, L_4\}$.

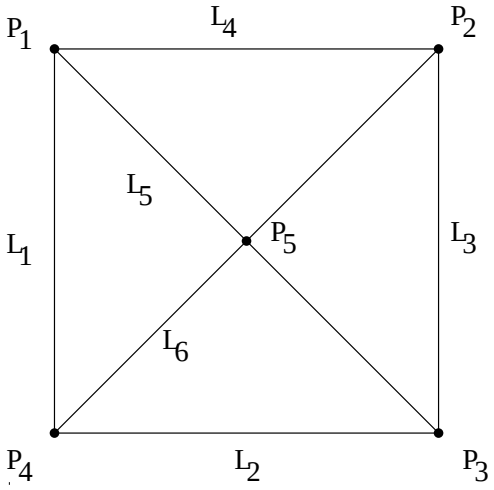


Das Dualmodell ist

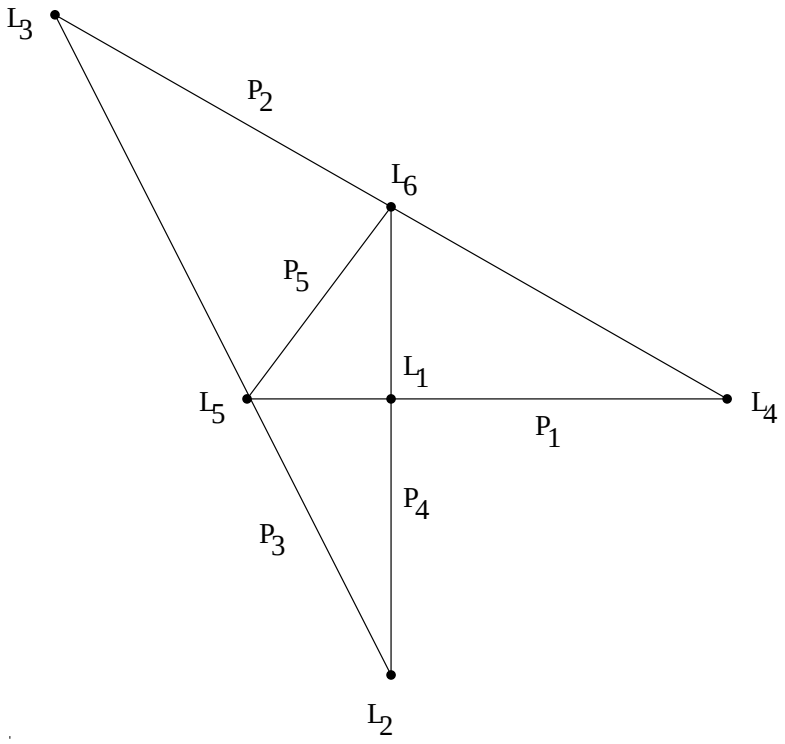


wieder dasselbe.

6. "Modell":
$E_P = \{P_1, P_2, P_3, P_4, P_5\}, E_G = \{L_1, L_2, L_3, L_4, L_5, L_6\}$.



Das Dualmodell dazu ist aber



endlich was anderes. In diesem Fall, weil P_5 der einzige Punkt ist, der auf zwei, aus drei Punkten bestehenden Geraden liegt, muß P_5 durch jede Gruppe festgelassen werden. Deshalb kann PG 3 nicht gelten.

Nun erhalten wir als **Korollar** dieser Konstruktion:
Es ist nicht möglich, PG3 von PG 1 und PG 2 zu folgern.

Dieses Beispiel zeigt, wie man die Unabhängigkeit eines Axioms von anderen zeigen kann; man findet ein Modell, in dem alle, außer des bezweifelten Axioms erfüllt sind, das übrige aber nicht.

Kapitel 3

Endliche Gruppen

1. Der Satz von Lagrange

Da man die Elemente einer endlichen Gruppe zählen kann, ist es möglich, Einsicht in ihre Struktur zu gewinnen. In diesem Kapitel werden wir fast ausschliesslich mit endlichen Gruppen und G-Mengen zu tun haben. (Dass eine Gruppe G endlich ist, bedeutet nicht, dass alle ihre G-Mengen endlich sind. Die transitiven G-Mengen sind aber endlich.)

Der Ausgangspunkt für die Theorie endlicher Gruppen ist der Satz von Lagrange. Um diesen zu formulieren, brauchen wir einige Bezeichnungen.

Ist A eine endliche Menge, schreiben wir $|A|$ statt $\mathrm{Card}(A)$, für die Anzahl von Elementen von A.

Ist G eine Gruppe, H eine Untergruppe von G, so haben wir G/H schon definiert (Kapitel I, 2.). Wir schreiben $[G : H]$ statt $|G/H|$.

Satz 3.1 (Lagrange). *Sei G eine endliche Gruppe, H eine Untergruppe von G. Dann gilt*

$$|G| = [G : H] \cdot [H].$$

Insbesondere ist $|H|$ ein Teiler von $|G|$.

Beweis. Wir haben G/H dadurch definiert, dass wir eine Äquivalenzrelation $\underset{H}{\sim}$ auf G konstruierten und bezeichneten den Quotientenraum $G/\underset{H}{\sim}$ als G/H. Die Äquivalenzrelation wurde wie folgt definiert:

$$x \underset{H}{\sim} y \Leftrightarrow y^{-1}x \in H (\Leftrightarrow x^{-1}y \in H).$$

Die Äquivalenzklasse von x ist

$$\begin{aligned} \{y : x^{-1}y \in H\} &= \{y : x^{-1}x = h, h \in H\} \\ &= \{xh : h \in H\}. \end{aligned}$$

Deshalb hat jede Äquivalenzklasse $|H|$ Elemente. Es gibt aber nach Definition $[G:H]$ Äquivalenzklassen. Da G die disjunkte Vereinigung von Äquivalenzklassen ist, gilt nun

$$|G| = [G:H]|H|,$$

wie behauptet. Damit ist der Satz bewiesen.

Wir werden $|G|$ die *Ordnung* von G nennen.

Sei nun $g \in G$, wobei G eine nicht notwendige endliche Gruppe ist. Wir definieren $g^m (m \in \mathbb{Z})$ induktiv, wie folgt:

$$\begin{aligned} g^m &= g^{m-1} \cdot g \quad (m > 0) \\ g^o &= e \\ g^m &= g^{m+1} g^{-1} \quad (m < 0). \end{aligned}$$

Lemma 3.2. *Es gelten*

$$\begin{aligned} g^m \cdot g^n &= g^{m+n} \\ (g^{-1})^m &= g^{-m} \end{aligned}$$

Beweis. Die zweite Aussage folgt induktiv aus der Definition. Deshalb brauchen wir in der ersten nur den Fall $n \geq 0$ zu beweisen, weil wir sonst g durch g^{-1} ersetzen können. Wir beweisen die Aussage induktiv. Wir nehmen deshalb an, dass sie für alle $n' < n$ schon bewiesen ist. Wir müssen auch den Fall $n = 1$ beweisen, und den behandeln wir zuerst. Sei $m < 0$; dann gilt

$$g^m g = \left(g^{m+1} g^{-1}\right) g = g^{m+1}.$$

Dasselbe gilt für $m \geq 0$. Deshalb ist die Aussage für $n = 1$ bewiesen. Nun gelten

$$\begin{aligned} g^m g^n &= g^m \cdot \left(g^1 gn - 1\right) && \text{(Induktion)} \\ &= g^{m+1} \cdot g^{n-1} && \text{(Assoziativität)} \\ &= g^{(m+1)+(n-1)} && \text{(Induktion)} \\ &= g^{m+n}. \end{aligned}$$

Damit ist das Lemma bewiesen.

Deshalb ist $\{g^m : m \in \mathbb{Z}\}$ eine Untergruppe von G. Sie wird mit $\langle g \rangle$ bezeichnet. Die Ordnung der Gruppe $\langle g \rangle$, falls diese Gruppe endlich ist, wird auch die *Ordnung* des Elementes g genannt und mit $o(g)$ bezeichnet.

Definiere

$$\mathbb{Z} \to G \quad ; \quad m \longmapsto g^m.$$

Das Bild dieser Abbildung wird mit $\langle g \rangle$ bezeichnet. Das Lemma besagt, dass die Abbildung ein Homomorphismus ist. Wir brauchen jetzt:

Satz 3.3 (Euklid). *Jede Untergruppe von $\mathbb{Z}$ ist von der Form $N\mathbb{Z}(:= Nn; n \in \mathbb{Z})$ mit $N \geq 0, N \in \mathbb{Z}$.*

Beweis. Sei $H \subset \mathbb{Z}$ eine Untergruppe. Gilt $H = \{0\}$, dann nehmen wir ein $N = 0$ und alles wird damit erledigt. Deshalb können wir annehmen, dass $H \neq \{0\}$. Weil gilt

$$m \in H \Leftrightarrow -m \in H,$$

gibt es mindestens ein positives Element in H. Sei $N = \text{Min}\{m \in H, m > 0\}$. Dieses existiert. Sei nun $m \in H, m > 0$. Nach dem Restsatz (für gewöhnliche Division) gilt

$$m = q \cdot N + r$$

mit $0 \leq r \leq N$. Aber $N \in H$; und weil $qN = N + N + \ldots + N$ (q-mal), folgt $qN \in H$. Deshalb: $r = m - q \cdot N \in H$. Nach der Definition von N und $0 \leq r < N$ kann nur gelten: $r = 0$. Deswegen gilt

$$m = qN.$$

Umgekehrt liegt qN in H. Ist $m \in H$ eine negative Zahl, dann ist $-m (\in H)$ der Form $q'N$; deshalb gilt $m = -q' \cdot N$. Deshalb gilt

$$H = N\mathbb{Z},$$

und die Behauptung ist bewiesen. □

Nun kehren wir zu $\langle g \rangle$ zurück. Wir nehmen an, dass $\langle g \rangle$ endlich ist. Dann ist der Kern von $\mathbb{Z} \to G; m \longmapsto g^m$ die Menge der Vielfachen von N, wobei N die Ordnung von g bezeichnet, weil $\mathbb{Z}/N\mathbb{Z}$ von Ordnung N ist. (Die Klassen in $\mathbb{Z}/N\mathbb{Z}$ sind $0 + N\mathbb{Z}, 1 + N\mathbb{Z}, \ldots, (n-1) + N\mathbb{Z}$.) Es folgt, dass $e = g^o, g^1, g^2, \ldots, g^{N-1}$ verschieden sind und es gilt

$$g^N = e.$$

Deshalb erhalten wir:

Korollar 3.4. *Sei G eine endliche Gruppe. Die Ordnung $o(G)$ von einem Element $g \in G$ ist*

$$o(g) = \text{Min}\{m > 0 : g^m = e\}.$$

Diese Zahl teilt $|G|$.

Die letzte Behauptung folgt von Satz 3.1 mit $H = \langle g \rangle$.

Bemerkung.

1. Obwohl wir im allgemeinen die Gruppenmultiplikation als ein Produkt schreiben, werden wir für $\mathbb{Z}$ "+" benutzen. Vielleicht ist das Vorgehen nicht konsequent, aber ...

2. Weil $\mathbb{Z}$ abelsch ist, ist $N\mathbb{Z}$ ein Normalteiler von $\mathbb{Z}$. Deshalb ist $\mathbb{Z}/N\mathbb{Z}$ nach Kapitel I, 3. eine Gruppe.

2. Beispiele von endlichen Gruppen

1. Die zyklischen Gruppen
Sei $N > 0$. Wir haben in Kapitel III, 1. die Gruppe $\mathbb{Z}/N\mathbb{Z}$ gebildet. Sie heißt "*die zyklische Gruppe N-ter Ordnung*" und wird mit C_N bezeichnet. Die Multiplikation wird meistens als Produkt geschrieben, gelegentlich aber auch als Addition. Wie schon bemerkt wurde, ist die Gruppe abelsch. Sie besitzt eine Element der Ordnung N. Umgekehrt sei G eine Gruppe von Ordnung N mit einem Element g der Ordnung N. Dann gilt

$$|\langle g\rangle| = |G|;$$

weil $\langle g\rangle \subset G$ gilt, folgt $\langle g\rangle = G$. Von der in Kapitel III, 1. diskutierten Abbildung hat man

$$\langle g\rangle \cong C_N.$$

Deshalb:

$$G \cong C_N.$$

Jedes Element g von C_N, für welches gilt

$$\langle g\rangle = C_N,$$

heißt ein *Erzeugendes* von C_N.

Eine Gruppe G, die C_N isomorph ist, heißt *zyklisch*; ein Element $g \in G$ mit der Eigenschaft $\langle g\rangle = G$ heißt ein *Erzeugendes* von G.

Zum Beispiel ist jedes Element (außer e) der Gruppe $C_2 \times C_2$ von der Ordnung 2. Dagegen hat C_4 ein Element (sogar zwei Elemente) von Ordnung 4. Deshalb sind $C_2 \times C_2$ und C_4 nicht isomorph. $C_2 \times C_2$ ist die "kleinste" nicht zyklische Gruppe; sie heißt die "Kleinsche Vierergruppe".

2. Die Diedergruppen
Sei G eine abelsche Gruppe. Die Abbildung

$$\iota : G \to G; g \longmapsto g^{-1}$$

ist ein Homomorphismus, weil gelten

$$\begin{aligned} \iota(g_1g_2) &= \iota(g_2g_1) && (g \text{ abelsch}) \\ &= (g_2g_1)^{-1} \\ &= g_1^{-1}g_2^{-1} \\ &= \iota(g_1)\cdot\iota(g_2). \end{aligned}$$

Außerdem gilt

$$\iota^2 = \mathrm{Id}.$$

Wir bilden nun eine Gruppe $\widetilde{G}$, die mengentheoretisch $G \times \{e, \iota\}$ ist. Nun ist die Multiplikation folgendermaßen definiert:

$$\begin{aligned}
(g_1, e) \cdot (g_2, e) &= (g_1 g_2, e) \\
(g_1, e) \cdot (g_2, \iota) &= (g g_2, \iota) \\
(g_1, \iota) \cdot (g_2, e) &= \Big(g_1 \iota(g_2), \iota\Big) \\
(g_1, \iota) \cdot (g_2, \iota) &= \Big(g_1 \iota(g_2), e\Big).
\end{aligned}$$

Die Identität soll (e, e) sein. Es ist etwas mühsam, aber nicht schwierig, nachzuweisen, dass $\widetilde{G}$ eine Gruppe ist.

Im Falle $G = C_N$ schreiben wir D_{2N} statt $\widetilde{C}_N$. Dies ist die Diedergruppe von Ordnung $2N$. Wir betrachten C_N als Untergruppe von D_{2N}, $C_N = \{(g, e) : g \in C_N\}$. Sei $\mathcal{T} = (e, \iota)$. Dann ist jedes Element von D_{2N} entweder von der Form (g, e), d.h. in C_N, oder von der Form $(g, e)(e, \iota)$, d.h. von der Form $g\mathcal{T}$ mit $g \in C_N$. Es gelten

$$\begin{aligned}
& \mathcal{T}^2 = e, \mathcal{T} g \mathcal{T} = g^{-1} \quad (g \in C_N) \\
\Leftrightarrow \quad & \mathcal{T} g \mathcal{T}^{-1} = g^{-1}
\end{aligned}$$

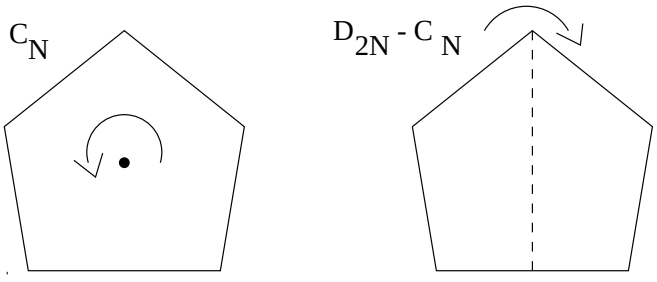
Jedes Element von $D_{2N} - C_N$ ist von der Ordnung 2, weil

$$\begin{aligned}
(g\mathcal{T})^3 &= g\mathcal{T} g\mathcal{T} \\
&= g g^{-1} \\
&= e.
\end{aligned}$$

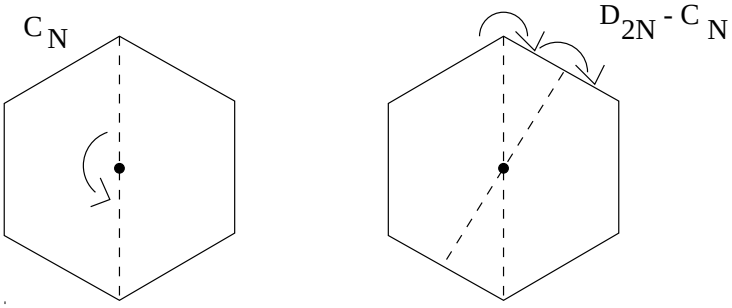
Es folgt, dass D_4 wieder die Kleinsche Vierergruppe $C_2 \times C_2$ ist.

Wir stellen uns C_N als die Drehung eines regulären N-Ecks vor und D_{2N} als die Drehung und Spiegelungen dieses Polygons.

<u>N ungerade</u>



N gerade



Die symmetrischen Gruppen

Die symmetrische Gruppe S_n ist die Menge der bijektiven Abbildungen von $\{1, \ldots, n\}$ auf sich. Die Gruppenmultiplikation ist die Verknüpfung. Sei $\sigma \in S_n$. Es wird sich als nützlich erweisen, einige Schreibweisen für σ tz entwickeln. Zuerst werden wir $\begin{pmatrix} 1 & 2 & & n \\ & & \ldots & \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$ schreiben. Zum Beispiel wird in S_4:

$$\sigma: \begin{array}{l} \sigma(1)=2 \\ \sigma(2)=3 \\ \sigma(3)=1 \\ \sigma(4)=4 \end{array} \quad \text{als} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \text{bezeichnet.}$$

Die obere Zeile besteht aus den Argumenten von σ, die untere aus den Werten.

Zunächst führen wir die *Zyklusdarstellung* ein. Wir fangen mit 1 an, dann schreiben wir

$$1, \sigma(1), \sigma^2(1), \sigma^3(1), \ldots$$

bis wir wieder bei 1 sind. Dann wählt man ein i, das nicht in dieser Liste steht und verfährt mit diesem genauso wie mit der 1; man erhält

$$i, \sigma(i), \sigma^2(i), \ldots$$

u.s.w., bis es keine nicht-aufgezählten Elemente mehr gibt. Man schreibt σ als

$$\big(1, \sigma(1), \sigma^2(1), \ldots\big)\big(i, \sigma(i), \sigma^2(i), \ldots\big)\big(i', \sigma(i'), \sigma^2(i'), \ldots\big) \ldots .$$

Zum Beispiel erhält man von $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ die Darstellung

$$(1,2,3) \cdot (4).$$

Als ein komplizierteres Beispiel nehmen wir

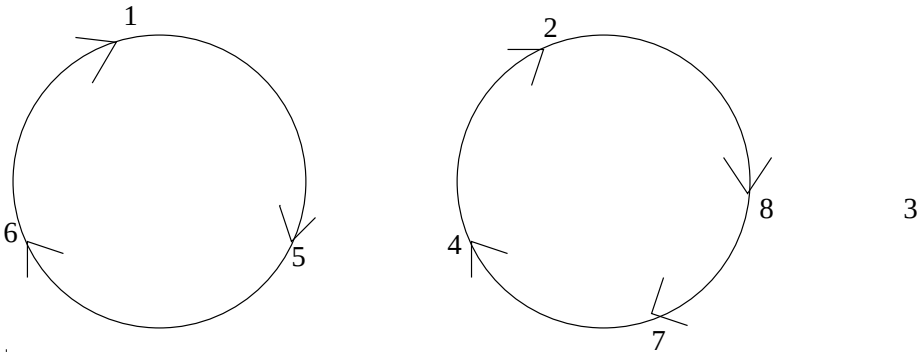
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 3 & 2 & 6 & 1 & 4 & 7 \end{pmatrix} \in S_8.$$

Wir erhalten

$$(1,5,6)(2,8,7,4)(3).$$

$$\big((3) \text{ z.B. wird im folgenden weggelassen}\big)$$

Wir sollten uns diese so vorstellen



N.B. Zyklus wird von dem griechischen "kuklos" = "der Kreis" hergeleitet. Um zu sehen, welche Wirkung $(1,5,6)(2,8,7,4)(3)$ auf ein Element, z.B. 8, ausübt, brauchen wir nur das folgende Element zu nehmen, d.h. 7. Da dies Zyklen sind, folgt 1 der 6, 2 folgt der 4. Es ist üblich, Zyklen, die aus einem Element bestehen, nicht zu schreiben.

Als Beispiel nehmen wir jetzt

$$(1,3,5,9)(2,8)(7,6) \in S_{10}.$$

Nach der ersten Schreibweise wird dieses so geschrieben:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 8 & 5 & 4 & 9 & 7 & 6 & 2 & 1 & 10 \end{pmatrix}.$$

Sei $\sigma \in \Sigma_n$. Der Typ von σ ist die Folge

$$k_1 \geq k_2 \geq k_3 \geq k_4 \ldots \geq k_r,$$

wobei in der Zyklusdarstellung σ aus r Zyklen besteht, deren Längen $k_1, k_2, \ldots, k_r$ sind. In dem Beispiel ist der Typ von

$$(1,3,5,9)(2,8)(7,6)$$
$$4,2,2,1,1.$$

Da in S_n die Summe der Zyklenlängen n ist, haben wir immer

$$k_1 + k_2 + \ldots, k_r = n.$$

Eine solche Folge heißt eine *Partition* von n.

Wir bemerken hier, wenn σ als ein Produkt $C_1 \dots C_r$ von Zyklen geschrieben wird, so sind $C_1, \dots, C_r$ Elemente von S_r, mindestens wenn sie mit zusätzlichen Zyklen der Länge 1 versehen werden. Da die Ordnung keine Rolle spielt, gilt

$$C_i C_j = C_j C_i$$

und $\sigma = C_1 \dots C_r$ als Produkt in S_n.

Wir bemerken auch, dass die Zyklen genau die Bahnen von $\{1, \dots, n\}$ unter $\langle\sigma\rangle$ sind. Das Element C_i hat nur bei einer Bahn eine nicht-triviale Wirkung; "es permutiert diese Bahn zyklisch". Das Element C_i ist der Ordnung k_i, wenn es von der Länge k_i ist, da erst bei $l = k_i C_i^l$ eine triviale Wirkung auf jene Bahn hat.

Zwei Elemente von Σ_n, die in Zyklusdarstellung angegeben werden, zu multiplizieren, ist nicht schwierig. In Σ_4 multiplizieren wir (13)(24) mit (123).

$$\Big((13)\cdot(24)\Big)\cdot(123)$$

Auf 1: $1 \to 2 \to 4$
Auf 4: $4 \to 4 \to 2$
Auf 2: $2 \to 3 \to 1$

Damit wird eine Zyklus geschlossen: Wir erhalten

$$(1\ 4\ 2).$$

Es bleibt nun 3 übrig. Aus Sicherheitsgründen überprüfen wir, dass 3 wirklich in 3 geschickt wird; $3 \to 1 \to 3$.$\surd$
In diesen Rechnungen beschreibt der erste Pfeil, welche Wirkung (123) hat; der zweite, welche Wirkung (13)(24) hat.

Jetzt brauchen wir eine Rechnung.

Sei $C = (i_1, \dots, i_k)$ ein Zyklus der Länge k in Σ_n. Sei $\sigma \in \Sigma_n$. Wir definieren

$$\sigma_C = \Big(\sigma(i_1), \dots, \sigma(i_k)\Big).$$

Lemma 3.5. *Es gilt:*

$$\sigma_C = \sigma \cdot C \cdot \sigma^{-1}.$$

Beweis. Sei j ein Element von $\{1, \dots, n\}$, das von der Form $\sigma(i_a)$ ist. Dann gilt

$$\begin{array}{lcll} \sigma_C \cdot j & = & j' & \text{wobei } j' = \sigma(i_{a+1}) \\ & & & (k+1=1) \\ \sigma C \sigma^{-1}(j) & = & \sigma C i_a & \\ & = & \sigma\Big(i_{a+1}\Big) & \\ & = & j'. & \end{array}$$

Ist j nicht der Form $\sigma(i_a)$, dann gilt

$$^{\sigma}Cj = j$$

und

$$C \cdot \left(\sigma^{-1} j\right) = \sigma^{-1} j, \quad \text{oder} \quad \sigma C \sigma^{-1}(j) = j.$$

Deshalb haben $^{\sigma}C$ und $\sigma C \sigma^{-1}$ dieselbe Wirkung, sind also gleich. Damit ist das Lemma bewiesen.

Satz 3.6. *Seien $g_1, g_2 \in \Sigma_n$ Elemente des gleichen Typs. Dann gibt es ein $\sigma \in S_n$, so dass gilt*

$$\sigma g_1 \sigma^{-1} = g_2.$$

Bweis. Sei der Typ von g_1 und g_2 $k_1 \geq k_2 \geq \ldots \geq k_r$. Wir schreiben

$$\begin{aligned} g_1 &= C_1^{(1)} \ldots C_r^{(1)} \\ g_2 &= C_1^{(2)} \ldots C_r^{(2)}. \end{aligned}$$

Damit ist

$$C_j^{(i)} = \left(c_1^{i,j}, \ldots, c_{k_j}^{i,j}\right).$$

Dann sehen die obigen Gleichungen so aus:

$$\begin{aligned} g_1 &= \left(c_1^{1,1}, \ldots, c_{k_1}^{1,1}\right)\left(c_1^{1,2}, \ldots, c_{k_2}^{1,2}\right)\ldots \\ g_2 &= \left(c_1^{2,1}, \ldots, c_{k_1}^{2,1}\right)\left(c_1^{2,2}, \ldots, c_{k_2}^{2,2}\right)\ldots \end{aligned}$$

In diesen Darstellungen haben wir, wenn wir die Klammern vergessen würden, in beiden Fällen die Zahl 1 bis n in irgendeiner Reihenfolge. Deswegen können wir σ folgendermaßen definieren:

$$\sigma\left(c_j^{1,i}\right) = c_j^{2,i} (1 \leq j \leq k_i, 1 \leq i \leq r).$$

Mit anderen Worten: σ schickt ein Element aus der ersten Zeile in das entsprechende Element der zweiten Zeile.

Nach Lemma 3.5 gilt

$$C_i^{(2)} =^{\sigma} \left(C_i^{(1)}\right) = \sigma C_i^{(1)} \sigma^{-1}.$$

Es folgt

$$g_2 = \sigma\left(C_i^{(1)}\sigma^{-1} \cdot \sigma C_2^{(1)}\sigma^{-1} \cdot \sigma C_3^{(1)}\sigma^{-1} \ldots \sigma C_r^{(1)}\sigma^{-1}\right).$$

Die inneren σ's kürzen sich weg. Wir erhalten

$$\begin{aligned} g_2 &= \sigma C_1^{(1)} \ldots C_r^{(1)} \sigma^{-1} \\ &= \sigma g_1 \sigma^{-1}. \end{aligned}$$

Damit ist der Satz bewiesen.

Um zu zeigen, wie man dieses Verfahren durchführt, nehmen wir als Beispiel

$$\begin{aligned} n &= 6 \\ g_1 &= (12)(365) \\ g_2 &= (246)(35). \end{aligned}$$

Wir schreiben die Elemente so:

$$\begin{aligned} g_1 &= (3\ 6\ 5)(1\ 2)(4) \\ g_2 &= (2\ 4\ 6)(3\ 5)(1). \end{aligned}$$

Nun nehmen wir

$$\begin{aligned} \sigma \ : \ & 3 \to 2 \\ & 6 \to 4 \\ & 5 \to 6 \qquad \text{u.s.w.} \end{aligned}$$

Wir erhalten

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix} = (1\ 3\ 2\ 5\ 6\ 4)$$

BEACHTE: σ ist nicht eindeutig bestimmt!!

Dann gilt

$$\sigma g_1 \sigma^{-1} = g_2.$$

Dieser Satz ist häufig für die Konstruktion von Elementen aus Σ_n nützlich.

Ein Element der Form $(ij)(i \neq j)$, ein Zweier-Zyklus, heißt eine *Transposition*. Wir haben schon in AGLA I bei der Konstruktion von Determinanten gesehen, dass jedes $\sigma \in \Sigma_n$ in der Form

$$\tau_1 \dots \tau_s$$

geschrieben werden kann, wobei die τ_j Transpositionen sind. Man kann diese Tatsache auch von der folgenden Gleichung herleiten:

$$(1, 2, \dots, n) = (1, 2)(2, 3) \dots \left(n^{-1}, n\right),$$

da jeder Zyklus dann als ein Produkt von Transpositionen geschrieben werden kann.

Wir hatten in AGLA I auch gesehen, dass es eine Abbildung

$$\operatorname{sgn} : \Sigma_n \to \{\pm 1\}$$

gibt, die

$$\operatorname{sgn}(\sigma_1 \sigma_2) = \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2)$$

genügt.

Wenn wir Unbestimmte $x_1, \ldots, x_n$ einführen, können wir sgn so definieren:

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \left(x_{\sigma(i)} - x_{\sigma(j)}\right) / \prod_{i<j} \left(x_i - x_j\right).$$

Hier treten in Zähler und Nenner diesselben Faktoren auf; sie können aber verschiedene Vorzeichen haben. Wir hatten $\operatorname{sgn}(\sigma)$ dadurch definiert:

$$L\left(v_{\sigma(1)}, \ldots, v_{\sigma(n)}\right) = \operatorname{sgn}(\sigma) L\left(v_1, \ldots, v_n\right),$$

wobei $L \in \operatorname{Alt}(V, n), n = \dim(V), v_1, \ldots, v_n \in V$ angenommen wurden.

Offensichtlich ist sgn ein Homomorphismus. Wir wissen auch, wenn τ eine Transposition ist, dann gilt

$$\operatorname{sgn}(\tau) = -1.$$

4. Die alternierende Gruppe

Die Gruppe Σ_n hat $n!$ Elemente. Der Kern von sgn heißt die *alternierende Gruppe* A_n. Sie hat $\frac{1}{2}(n!)$ Elemente. Ein Zyklus der Länge k liegt in A_n dann und nur dann, wenn k ungerade ist. Diese Aussage folgt aus der Darstellung

$$(1, 2, \ldots, k) = (1, 2)(2, 3) \ldots (k-1, k),$$

d.h. ein Zyklus der Länge k kann als ein Produkt von $k-1$ Transpositionen geschrieben werden. Deshalb erkennen wir vom Typ von $g \in \Sigma_n$, ob dieses Element in A_n liegt; es muß nämlich eine gerade Anzahl von Zyklen mit gerade Länge haben.

Als Beispiele nehmen wir $n = 3$ und 4.

$n = 3$ $\quad \Sigma_3 = \{e, (12), (23), (13), (123), (132)\}$
$\quad A_3 = \{e, (123), (132)\}.$

Diese Gruppe ist zu der zyklischen Gruppe mit 3 Elementen isomorph.

$n = 4$ $\quad \Sigma_4 = \{e, (12), (13), (14), (23), (24), (34), (123), (213),$
$(124), (214), (134), (143), (234), (243),$
$(12)(34), (13)(24), (14)(23), (1234), (1243)$
$(1324), (1342), (1423)(1432)\}$

$A_4 = \{e, (123), (213), (124), (214), (134), (143), (234),$
$(243), (12)(34), (13)(24); (14)(23)\}$

Deshalb hat A_4

1 Element von Ordnung 1
8 Elemente von Ordnung 3
3 Elemente von Ordnung 2.

(123) ist in A_4 zu

$$(123), (243), (134), (214)$$

konjugiert; genau die Hälfte der Menge der Elemente dritter Ordnung. Deshalb ist das Analogen von Satz 3.6 für A_n nicht richtig.

Die Gruppe Σ_4 hat eine Eigenart, die wir jetzt erwähnen werden. Wegen

$$\begin{aligned}(12)(34)\cdot(13)(24) &= (14)(23)\\ (12)(34)\cdot(14)(23) &= (13)(24) \qquad \text{u.s.w.}\end{aligned}$$

ist

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

eine Untergruppe von S_4, die zu der Kleinschen Vierergruppe $C_2 \times C_2$ isomorph ist. V kann auch folgendermaßen beschrieben werden:

$$V = \{g \in \Sigma_4 : g^2 = e, \operatorname{sgn}(g) = 1\},$$

wie man leicht nachprüft. Für $\sigma \in \Sigma_4, g \in \Sigma_4$ haben wir

$$\begin{aligned}\left(\sigma g \sigma^{-1}\right)^2 &= \sigma g \sigma^{-1} \sigma g \sigma^{-1}\\ &= \sigma g^2 \sigma^{-1}\\ &= \sigma\sigma^{-1}\\ &= e\end{aligned}$$

und

$$\operatorname{sgn}\left(\sigma g \sigma^{-1}\right) = \operatorname{sgn}(g) = 1.$$

Deshalb folgt $\sigma g \sigma^{-1} \in V$; V ist deswegen ein Normalteiler von Σ_4.

Sei

$$\begin{aligned}V_0 &= \{(12)(34), (13)(24), (14)(23)\}.\\ \left(\right. &= V - \{e\}\left.\right).\end{aligned}$$

Dann ist V_0 eine S_4-Menge durch

$$\sigma(x) = \sigma x \sigma^{-1}.$$

Wir erhalten dadurch einen Homomorphismus

$$\theta : \Sigma_4 \to \Sigma_3.$$

Der Kern von θ ist

$$\begin{aligned}K &= \{\alpha \in \Sigma_4 : \alpha x \alpha^{-1} = x (x \in V_0)\}\\ &= \{\alpha \in \Sigma_4 : x^{-1}\alpha x = \alpha\}.\end{aligned}$$

Weil V abelsch ist, gilt

$$K \supset V.$$

Weil θ surjektiv ist, wie man leicht nachrechnen kann, gilt

$$[\Sigma_4 : K] = |\Sigma_3| = 6;$$

so

$$|K| = 4.$$

Deshalb gilt $V = K$ und $\Sigma_4/V \cong \Sigma_3$. Es ist auch leicht zu zeigen, dass gilt

$$A_3/V \cong C_3.$$

3. Abelsche Gruppen

Um abelsche Gruppen zu untersuchen, benötigt man Kenntnisse der Struktur von $\mathbb{Z}$.

Wir sagen, dass a ein *Teiler* von b ist, wobei a, b ganze Zahlen sind, $a \neq 0$, wenn es eine ganze Zahl q gibt, so dass gilt

$$b = aq.$$

Wir schreiben $a|b$ (gesprochen "a teilt b"). Eine natürliche Zahl $p(\neq 1)$ heißt eine *Primzahl*, wenn die sämtlichen Teiler von p die Menge $\{\pm 1, \pm p\}$ bilden. Beispiele sind $2, 3, 5, 7, 11, 13, \ldots$. Um nachzuweisen, dass eine natürliche Zahl keine Teiler außer $\pm 1, \pm p$ besitzt, genüt es auszuprobieren, ob eine Zahl aus der Menge $\{2, 3, \ldots, p-1\}$ teilt, weil aus $a|b$

$$|a| = |b/q| \leq |b|$$

folgt.

Satz 3.7. *Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ nicht alle Null. Es gibt eine natürliche Zahl d, die die folgenden Eigenschaften hat:*

1. $d|a_i \qquad (1 \leq i \leq n)$
2. *es gibt $m_1, m_2, \ldots, m_n$, so dass gilt*

$$d = a_1 m_1 + a_2 m_2 + \ldots + a_n m_n,$$

Die Zahl d heißt der größte gemeinsame Teiler von $a_1, \ldots, a_n$, geschrieben

$$d = ggT(a_1, \ldots, a_n).$$

Beweis. Die Menge

$$\{a_1 s_1 + \ldots + a_n s_n : s_1, \ldots, s_n \in \mathbb{Z}\}$$

ist eine Untergruppe von $\mathbb{Z}$, weil die Differenz

$$\Big(a_1 s_1 + \ldots + a_n s_n\Big) - \Big(a_1 s_1' + \ldots + a_n s_n'\Big) = \Big(a_1(s_1 - s_1') + \ldots + a_n(s_n - s_n')\Big)$$

auch in der Menge liegt (s. Kapitel I, 1.). Nach Satz 3.3 ist diese Menge der Form $d\mathbb{Z}, d \geq 0$. Weil $d \in \mathbb{Z}$ gilt, muß es $m_1, \ldots, m_n$ geben, so dass gilt

$$d = a_1 m_1 + \ldots + a_n m_n.$$

Damit hat d die zweite Eigenschaft. Da a_i in $d\mathbb{Z}$ liegt, gibt es b_i, so dass gilt

$$a_i = d b_i;$$

d.h.

$$d|a_i.$$

Damit hat d auch die erste Eigenschaft.

Korollar. *Sei p eine natürliche Zahl, $p \neq 0, 1$; dann sind die beiden folgenden Eigenschaften gleichbedeutend:*

1. *p ist eine Primzahl,*
2. *wenn p ein Produkt ab von zwei natürlichen Zahlen teilt, dann teilt p mindestens eine von den beiden.*

Beweis. 1. $\Rightarrow$ 2. Sei p eine Primzahl. Wir nehmen an, dass gilt $p|ab$ aber nicht $p|a$ oder $p|b$. Da $ggT(p,a)$ (bzw. $ggT(p,b)$) ein Teiler von p ist, gilt

$$ggT(p,a) \in \{1,p\} \quad (\text{bzw.} ggT(p,b) \in \{1,p\}).$$

Von $ggT(p,a) = p$ würde folgen, dass a durch p teilbar wäre. Deshalb gelten

$$ggT(p,a) = 1, \quad ggT(p,b) = 1.$$

Es existieren m, n, m', n', so dass gelten

$$pm + an = 1, pm' + bn' = 1.$$

Multipliziere diese Gleichungen:

$$p^2mm' + pmbn' + pm'an + ab \cdot nn' = 1.$$

Jedes auf der linken Seite stehende Glied ist durch p teilbar. Es existiert daher eine natürliche Zahl N, so dass gilt:

$$Np = 1,$$

was unmöglich ist. Damit ist die Behauptung bewiesen.

2. $\Rightarrow$ 1. Sei p eine Zahl, die die zweite Eigenschaft hat, aber keine Primzahl ist. Dann hat p einen Teiler a, der weder 1 noch p ist. Sei $b = p/a$; dieses ist ebenfalls eine natürliche Zahl. Dann gilt

$$p = ab.$$

Deshalb ist ab durch p teilbar; es folgt, dass mindestens eine von a und b durch p teilbar ist. Wir dürfen annehmen, dass a durch p teilbar ist. Das heißt:

$$a = pq \quad (q \in \mathbb{N}).$$

Es folgt

$$p = ab = p \cdot (qb).$$

Deshalb

$$qb = 1$$

oder

$$q = 1, b = 1.$$

Diesem widerspricht der Bedingung, dass a weder 1 noch q sei.

Satz 3.8 (Fundamentalsatz der Arithmetik). *Sei n eine natürliche Zahl. Dann gibt es Primzahlen $p_1, \dots, p_m$ und natürliche Zahlen $e_1, \dots, e_m$, so dass n durch*

$$n = p_1^{e_1} \dots p_m^{e_m}$$

dargestellt werden kann. Diese Darstellung ist sogar bis auf Anordnung eindeutig.

Beweis. Ist n schon eine Primzahl, dann ist der Satz richtig. Wenn n keine Primzahl ist, können wir zwei Teiler a, b finden,

$$n = ab, a \neq 1, n, b \neq 1, n.$$

Es gilt

$$a < n, b < n.$$

Induktionsannahme

Der Satz sei für alle Zahlen kleiner n gültig. Dann können a und b als Produkte von Primzahlpotenzen dargestellt werden. Nach der Gliederung $n = ab$ gilt dasselbe von n selbst. Daher folgt die Darstellbarkeit von n im allgemeinen.

Wir müssen noch zeigen, dass die Darstellung eindeutig ist. Sei n die kleinste Zahl, die mehr als eine Darstellung hat. Seien zwei davon

$$n = p_1^{e_1} \dots p_m^{e_m}, n = q_1^{f_1} \dots q_n^{f_n}.$$

Von der ersten folgt $p_1 | n$. Es folgt

$$p_1 | q_1^{f_1} \dots q_n^{f_n}.$$

Aus dem Korollar folgt: p_1 teilt eine von den Zahlen $q_1^{f_1}, \dots q_n^{f_n}$. Deshalb kommt p_1 unter den Primzahlen $q_1, \dots, q_n$ vor. Wir dürfen annehmen, dass $q_1 = p_1$. Daher

$$n/p_1 = p_1^{e_1 - 1} p_2^{e_2} \dots p_m^{e_m}; n/p_1 = q_1^{f_1 - 1} q_2^{f_2} \dots q_n^{f_n}.$$

Nach Induktionsannahme sind diese Darstellungen von n/p_1 gleich. Deshalb ist die Darstellung von n selbst eindeutig.

Wir brauchen folgendes

Korollar. *Sei*

$$n = p_1^{e_1} \dots p_m^{e_m},$$

eine Darstellung von n als ein Produkt von Primzahlpotenzen. Die Zahlen

$$n/p_1^{e_1}, n/p_2^{e_2}, \dots, n/p_m^{e_m}$$

sind ganz; es gilt

$$ggT\left(n/p_1^{e_1}, \dots, n/p_m^{e_m}\right) = 1.$$

Beweis. Die erste Aussage ist klar. Für die zweites sei

$$d = ggT\left(n/p_1^{e_1}, \dots, n/p_m^{e_m}\right).$$

Wir nehmen an, dass gilt $d \neq 1$. Dann gibt es nach dem Satz eine Primzahl p, so dass p ein Teiler von d ist. Es gilt

$$p | \frac{n}{p_1^{e_1}} = p_2^{e_2} p_3^{e_3} \dots p_m^{e_m}. \qquad \text{u.s.w.}$$

Deshalb ist p eine von den Primzahlen $p_2, \dots, p_m$. Genauso ist p eine von $p_1, p_3, \dots, p_m$, u.s.w. Es gibt aber kein gemeinsames Element in allen diesen Mengen; p kann deswegen nicht existieren. Es folgt, dass $d = 1$ gilt.

Nun sei A eine endliche abelsche Gruppe, wobei die "Multiplikation" als Produkt geschrieben wird. Sei n die Ordnung von A. Sei

$$n = p_1^{e_1} \dots p_m^{e_m}$$

die Darstellung von n als Produkt von Primzahlpotenzen.

Wir machen eine Bemerkung. Sei N eine ganze Zahl. Wir definieren induktiv für $a \in A$ a^N durch

$$\begin{array}{rcll} a^N & = & a^{N-1} \cdot a & (N > 0) \\ & = & e & (N = 0) \\ & = & a^{N+1} \cdot a^{-1} & (N < 0). \\ & & \text{(vgl. Kapitel 3, 1.)} & \end{array}$$

Lemma. *Es gilt*

$$(ab)^N = a^N \cdot b^N.$$

Beweis. Sie $N > 0$. Wir nehmen an, dass die Aussage schon für $N - 1$ bewiesen worden ist. Dann

$$\begin{array}{rcll} (ab)^N & = & (ab)^{N-1} \cdot ab & \\ & = & a^{N-1} \cdot b^{N-1} \cdot a \cdot b & \\ & = & a^{N-1} \cdot a \cdot b^{N-1} \cdot b & (A \text{ abelsch}) \\ & = & a^N \cdot b^N. & \end{array}$$

Da

$$a^{-N} = \left(a^N\right)^{-1} \qquad \text{(Kapitel 3, 1.)}$$

folgt auch die Richtigkeit für negatives N. Für $N = 0$ ist die Aussage trivial.

Wir fassen dieses Lemma als die folgende Aussage auf:

$$a \longmapsto a^N \text{ ist ein Homomorphismus.}$$

Sei A nun eine endliche abelsche Gruppe; sei $n = |G|$. Sei $n = p_1^{e_1} - p_m^{e_m}$ die Primzahlzerlegung von n.
Sei nun A_i die folgende Untergruppe von A:

$$A_i = \{a \in A : a^{p_i^{e_i}} = e\}.$$

Satz 3.9. *Die Gruppe A ist zu*

$$A_1 \times A_2 \times \ldots \times A_m$$

isomorph. Die Ordnung von A_i ist $p_i^{e_i}$.

Dieser Satz ist fundamental bei der Untersuchung der abelschen Gruppen. Die Zerlegung heißt *"die primäre Zerlegung"* von A.

Beweis. Seien

$$\begin{aligned} n_i &= n/p_i^{e_i} \\ q_i &= p_i^{e_i}. \end{aligned}$$

Wir wissen schon, dass gilt

$$ggT\Big(n_1, n_2, \ldots, n_m\Big) = 1$$

(Kor. zu Satz 3.8). Nach Satz 3.7. gibt es ganze Zahlen $s_1, \ldots, s_m$, so dass gilt

$$n_1 s_1 + n_2 s_2 + \ldots + n_m s_m = 1.$$

Nach Korollar 3.4 gilt für jedes $a \in A$

$$e = a^n = a^{n_i \cdot q_i}.$$

Daher folgt

$$a^{n_i} \in A_i$$

Wir bilden

$$\varphi = A \to A_i \times A_2 \times A_m; a \longmapsto \Big(a^{n_1}, a^{n_2}, \ldots a^{n_m}\Big).$$

Wir zeigen, dass diese Abbildung ein Isomorphismus ist. Nach dem obigen Lemma ist sie ein Homomorphismus.

Sei $a \in \mathrm{Ker}(\varphi)$. Dann gelten

$$a^{n_1} = e, a^{n_2} = e, \ldots, a^{n_m} = e,$$

und daher

$$a = a^{n_1 s_1 + n_2 s_2 + \ldots + n_m s_m} = e.$$

Deshalb ist a injektiv.

Wir betrachten nun die Einschränkung von φ auf A_i. Für $j \neq i$ gilt $q_i | n_j$ und für $a \in A_i$ gilt daher

$$a^{n_j} = e \qquad (j \neq i).$$

Das Bild von A_i liegt in $A_i \subset A_1 \times A_2 \times \ldots \times A_m$. Da $\varphi | A_i$ auch injektiv ist, muß $\varphi | A_i$ surjektiv sein. Deshalb

$$A_i \subset \varphi(A).$$

Deshalb gilt

$$\varphi(A) = A_1 \times \dots A_m;$$

m.a.W. φ ist surjektiv.

Man hat

$$|A| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_m|. \qquad (*)$$

Um die letzte Aussage des Satzes zu beweisen, reicht es aus, folgendes zu zeigen:

Sei B eine endliche, abelsche Gruppe, p eine Primzahl, $f \geq 1$ eine ganze Zahl, so dass für jedes $x \in B$ gilt

$$x^{p^f} = e.$$

Dann ist $|B|$ eine Potenz von p.

Nach dieser Aussage ist $|A_i|$ eine Potenz von p_i. Wegen der Gleichung $(*)$ kann $|A_i|$ nur

$$p_i^{e_i}$$

sein.

Wir müssen diese Aussage noch beweisen.

Sei B derart, dass B die Voraussetzungen erfüllt und dass $|B|$ für gegebenes p^f minimal ist, wenn $|B|$ nicht eine Potenz von p ist. Sei $x \in B, x \neq e$. Dann ist die Ordnung von $\langle x \rangle$ von der Form $p^h (h \geq 1)$. Die Gruppe $\langle x \rangle$ ist ein Normalteiler von B, weil B abelsch ist. Da $B/\langle x \rangle$ auch die Voraussetzung erfüllt und weil

$$\left|B/\langle x \rangle\right| < \left|B\right|$$

gilt, ist $\left|B/\langle x \rangle\right|$ eine Potenz von p. Dann ist aber

$$\left|B\right| = \left|B/\langle x \rangle\right| \cdot \left|\langle x \rangle\right|$$

auch eine Potenz von p. Aus diesem Widerspruch folgt die Behauptung. Damit ist der Satz bewiesen.

Man kann auch die Gruppen A_i näher klassifizieren. Diese Klassifikation hängt eng mit der Jordan-Normalform zusammen. Wir werden sie in dieser Vorlesung nicht gebrauchen.

4. Aufzählung von Konjugationsklassen

Eine der effektivsten Methoden, eine gegebene Gruppe zu untersuchen, besteht in der Untersuchung der Konjugationsklassen. Wir erinnern uns daran, dass durch

$$\begin{aligned} G \times G &\to G; \\ (\gamma, g) &\to \gamma g = \gamma g \gamma^{-1} \end{aligned}$$

G selbst eine G-Menge wird. Die Bahnen sind die Konjugationsklassen. Der Stabilisator von G heißt hier der *Zentralisator* von g

$$\begin{aligned} Z_G(g) &= \{\gamma \in G : \gamma g \gamma^{-1} = g\} \\ &= \{\gamma \in G : \gamma g = g\gamma\}. \end{aligned}$$

Man bemerke:

$$\langle g \rangle \subset Z_G(g).$$

Das *Zentrum* einer Gruppe ist

$$Z_G := \bigcap_g Z_G(g) = \{\gamma \in G : \gamma g = g\gamma \text{ für alle } g \in G\}.$$

Wenn gilt

$$g_1 g_2 = g_2 g_1$$

sagt man, dass g_1 und g_2 *"kommutieren"*. Das Zentrum ist die Menge aller Gruppenelemente, die mit allen Gruppenelementen kommutieren. Dabei sind $Z_G(g), Z_G$ Untergruppen von $g, Z_G(g) \supset Z_G$.

Wir machen jetzt eine allgemeine Bemerkung:

Satz 3.10. *Sei G eine endliche Gruppe, X eine transitive G-Menge. Sei $x \in X, H = \mathrm{Stab}_G(x)$. Dann gilt*

$$|X| = |G|/|H|.$$

Beweis. Nach Satz 1.1 kann X mit G/H identifiziert werden. Die Behauptung folgt dann von Satz 3.1.

Wir werden

$$\{g\}_G$$

für die Konjugationsklasse von g schreiben. Sie besteht aus

$$|G|/|Z_G(g)|$$

Elementen. Da G aus $|G|$ Elementen besteht, gilt

$$\sum \frac{|G|}{|Z_G(g)|} = |G|$$

oder

$$\sum \frac{1}{|Z_G(g)|} = 1,$$

wobei die Summe über je ein Element aus jeder Konjugationsklasse gebildet wird. Man hat

$$Z_G(e) = G;$$

deshalb ist ein Glied der Summe $1/|G|$.

Wir werden jetzt den folgenden Satz beweisen, um zu zeigen, wie solche Überlegungen benutzt werden können.

Satz 3.11 *Sei G eine endliche Gruppe von Ordnung p^l, wobei p eine Primzahl ist. Dann gilt:*

$$Z_G \neq \{e\}.$$

(Natürlich ist G nicht notwendigerweise abelsch).

Beweis. In der Summe

$$\sum \frac{1}{|Z_G(g)|}$$

ist jedes Glied von der Form

$$\frac{1}{p^j} \qquad (j \leq l).$$

Das Glied p^{-l} kommt mindestens einmal vor. Die Summe ist eine ganze Zahl; käme p^{-l} nur einmal vor, hätte sie p^l als Nenner. Das ist unmöglich; deshalb gibt es andere $g \in G$, so dass $|Z_G(g)| = p^l$ gilt. Diese Aussage ist aber gleichbedeutend damit

$$Z_G(g) = G,$$

oder -umgesetzt- $g \in Z_G$. Damit wird der Satz bewiesen.

Mit derselben Idee kann man auch den folgenden Satz beweisen:

Satz 3.12. *Sei G eine endliche Gruppe, p eine Primzahl, $p|\,|G|$. Dann gibt es in G ein Element g von Ordnung p.*

Beweis. Der Beweis erfolgt nach Induktion nach $|G|$, als Ausgangspunkt nehmen wir an, dass die Aussage für alle G' mit $|G'| < |G|$ richtig ist. In der Summe

$$\sum \frac{1}{|Z_G(g)|} = 1$$

kommt ein $\frac{1}{p^l}$ im Glied mit $g = e$ vor, dies enthält den Faktor $1/p$. Wie vorher gibt es dann ein anderes $g \in G$, so dass $|Z_G(g)|$ durch p teilbar ist. Es gibt zwei Möglichkeiten

1. $|Z_G(g)| < |G|$. Dann können wir die Induktionsannahme benutzen, um zu schließen, dass $Z_G(g)$ ein Element von Ordnung p enthält.

2. $|Z_G(g)| = |G|$. Dann liegt g in Z_G, wie wir schon gesehen haben. In der Summe
$$\sum \frac{1}{|Z_G(g)|}$$
tragen die $g \in Z_G$ (von denen die Konjugationsklassen aus g selbst bestehen) insgesamt
$$\frac{|Z_G|}{|G|}$$
bei.

Wir dürfen annehmen, dass der erste Fall gar nicht vorkommt, weil wir sonst unser Problem schon erledigt haben. Deswegen sind die einzigen Glieder in der Summe, die ein p im Nenner haben, genau die Elemente $|Z_G| \cdot |G|^{-1}$. Weil die Summe ganz ist, muß $|Z_G|$ durch dieselbe Potenz von p teilbar sein, wie $|G|$ selbst. In jedem Fall ist $|Z_G|$ durch p teilbar. Die Gruppe $|Z_G|$ ist aber abelsch; der Schluß ist dann eine Folgerung von Satz 3.9.

$*$ Als letztes Beispiel betrachten wir Gruppen von Ordnung pq, wobei p und q zwei verschiedene Primzahlen sind.

Satz 3.13. *Sei G eine Gruppe von Ordnung pq, wobei p und q zwei verschiedene Primzahlen sind. Es wird angenommen, dass gilt*

$$p > q.$$

Dann gelten entweder

A. $G \cong C_{pq}$

oder

B. *G besitzt einen Normalteiler H mit $H \cong C_p$ und $G/H \cong C_q$. Jedes Element in $G - H$ ist von Ordnung q, und*

$$q|(p-1).$$

Wir wählen Elemente γ, von der Ordnung p und δ, von Ordnung q. Es gibt eine ganze Zahl $a, 1 \leq a < p$, mit der folgenden Eigenschaft. Jedes Element von G kann in der Form $\gamma^x \delta^y (0 \leq x < p, 0 \leq y < q)$ geschrieben werden. Die Multiplikation wird durch

$$(\gamma^x \cdot \delta^y)\left(\gamma^{x'} \cdot \delta^{y'}\right) = \gamma^{x+a^y x'} \delta^{y+y'}$$

gegeben.

Es ist übrigens nicht schwierig, eine Liste aller Gruppen der Ordnung pq aufzustellen.

Beweis. Nach Satz 3.9 ist jede abelsche Gruppe zu $C_1 \times C_2 \times \ldots \times C_m$ isomorph, unter anderem $C_{pq} \cong C_p \times C_q$. Deshalb können wir uns auf den Fall beschränken, in dem G nicht abelsch ist. Außer e hat jedes Element von G entweder Ordnung

p oder q. Denn, wenn es ein Element pq gäbe, würde G zu C_{pq} isomorph sein. Es kann nicht passieren, dass $Z_G(g) = G \ (g \neq e)$ gilt. Um dieses einzusehen, nehmen wir an, dass die Ordnung von g, p ist. Sei h von Ordnung q; nach Satz 3.12 gibt es solch ein h. Dann kommutieren g und h. Die Elemente $g^x h^y (0 \leq x < p, 0 \leq y < q)$ sind alle verschieden, wie gleich bewiesen wird. Es gibt $p \cdot q$ solche Elemente. Deshalb kommt jedes Element von G vor. Diese Elemente kommutieren; d.h. dass G abelsch ist, also etwas, das wir gerade ausgeschlossen haben. Um zu zeigen, dass diese Elemente verschieden sind, nehmen wir an

$$g^x \cdot h^y = g^{x'} \cdot h^{y'};$$

es folgt

$$g^{x-x'} = h^{y'-y}.$$

Die linke Seite ist von Orndung 1 oder p, die rechte von Ordnung 1 oder q. Deswegen sind beide gleich e; was behauptet wurde.

Anders ausgedrückt gilt

$$Z_G(g) = \langle g \rangle \qquad (g \neq e).$$

Wir nehmen an, dass es in G N_p Elemente von Ordnung p, N_q von Ordnung q gibt. Die N_p (bzw. N_q) Elemente von Ordnung p (bzw. q) werden auf N_p/q (bzw. N_q/p) Konjugationsklassen verteilt, wovon jede $q = pq/p$ (bzw. $p = pq/q$) Elemente hat. Es folgt, dass $p|N_q, q|N_p$ gelten.

Weil auch jede Untergruppe von Ordnung p (bzw. q), $p-1$ (bzw. $q-1$) Elemente von Ordnung p (bzw. q) enthält, gelten

$$(p-1)|N_p$$

und

$$(q-1)|N_q.$$

Da $p > q$ vorausgesetzt wurde, ist $q-1$ <u>nicht</u> durch p teilbar. Deswegen ist N_q durch $p(q-1)$ teilbar.

Nun gilt

$$pq = 1 + N_p + N_q.$$

Es folgt, dass gilt

$$N_q \leq p(q-1)$$

und folglich

$$N_p \leq pq - 1 - p(q-1) = p - 1.$$

Da N_p durch $p-1$ teilbar und nicht Null ist, folgt schließlich

$$\begin{aligned} N_p &= p-1 \\ N_q &= p(q-1). \end{aligned}$$

Die erste Gleichung bedeutet, dass die Menge von Ordnung p mit e eine zyklische Gruppe bildet. Diese sei H. Weil sie eindeutig ist, ist sie ein Normalteiler von G. Es folgt

$$G/H \cong C_q,$$

jedes Element von $G-H$ ist von Ordnung q. Sei δ von Ordnung q, γ von Ordnung p. Jedes Element von G kann, wie oben, als

$$\gamma^x \delta^y (0 \leq x < p, 0 \leq y < q)$$

dargestellt werden. Da H ein Normalteiler von G ist, muß $\delta\gamma\delta^{-1}$, welches ebenfalls von Ordnung p ist, von der Form $\gamma^a (1 \leq a \leq p-1)$ sein. Die Gleichung

$$(\gamma^x \cdot \delta^y) \cdot \left(\gamma^{x'} \cdot \delta^{y'}\right) = \gamma^{x+a^y x'} \delta^{y+y'}$$

folgt. Damit ist der Satz bewiesen.

Wir bemerken zusätzlich, dass aus

$$N_q = p(q-1)$$

folgt, dass es p Untergruppen $?_1, \ldots, ?_p$ von Ordnung q gibt. Für jedes j gibt es ein eindeutiges $\gamma \in H$, so dass gilt

$$?_j = \gamma ?_1 \gamma^{-1}.$$

5. Die Sylow-Sätze

Die Ideen, die wir in Kapitel III, 4. verwendet haben, können etwas weiter getrieben werden. In diesem Abschnitt werden die Sylow-Sätze bewiesen, die einen Grundstein für alle weiteren Untersuchungen in der Theorie endlicher Gruppen darstellen.

Zuerst führen wir einige Bezeichnungen ein. Wir schreiben $n \not| m$, wenn n nicht m teilt. Sei p eine Primzahl, f eine natürliche Zahl. Wir schreiben

$$p^f \parallel n \quad \text{(gesprochen " } p^f \text{ teilt } n \text{ genau")}$$

wenn

$$p^f | n \quad \text{aber } p^{f+1} \not| n.$$

So, z.B., $4 \parallel 12$, $3 \parallel 12$.

Die Sylow-Sätze sind im folgenden Satz enthalten:

Satz 3.14. *Sei G eine endliche Gruppe; sei n die Ordnung von G und p^f eine Primzahlpotenz, so dass gilt*

$$p^f \parallel n.$$

Es gibt mindestens eine Untergruppe von G mit der Ordnung p^f. Sei $\mathrm{Syl}_p(G)$ die Menge aller Untergruppen von G von Ordnung p^f. Dann gelten:

1. *Seien $H_1, H_2 \in \mathrm{Syl}_p(G)$; dann gibt es ein $g \in G$, so dass gilt*

$$H_1 = gH_2g^{-1}$$

2. *Sei $N = \mathrm{Card}\left(\mathrm{Syl}_p(G)\right)$. Dann hat man*

$$\begin{aligned} p|(N-1) \\ N|(n/p^f) \end{aligned}$$

Bezeichnung. Ein $H \in \mathrm{Syl}_p(G)$ heißt eine p-Sylow-Gruppe von G.

Beweis. Wir werden eine besondere G-Menge X benutzen. Die Elemente von X sind Untermengen $S \subset X$, wobei verlangt wird

$$\mathrm{Card}(S) = p^f.$$

Wir definieren

$$gS = \{gs : s \in S\}.$$

Auf diese Weise wird X eine G-Menge. Die Menge X hat

$$\left(\begin{array}{c} n \\ p^f \end{array} \right) = \frac{n(n-1)(n-2)\dots(n-p^f+1)}{p^f \cdot (p^f-1)\dots \cdot 1}$$

Elemente.

Weil die entsprechenden Glieder des Zählers und des Nenners durch dieselbe Potenz von p teilbar sind, ist $\left(\begin{array}{c} n \\ p^f \end{array} \right)$ nicht durch p teilbar. Deshalb gibt es eine Bahn $\mathcal{O}_G(S) \subset X$, so dass Card $\mathcal{O}_G(S)$ auch nicht durch p teilbar ist. Sei

$$H = \mathrm{Stab}_G(S).$$

Weil gilt (s. Satz 3.10)

$$\mathrm{Card}\ \mathcal{O}_G(S) = |G|/|H|$$

muß weiter gelten

$$p^f \,|\, |H|.$$

Andererseits halten wir $s_0 \in S$ fest.

$$\begin{array}{rcl} \mathrm{Stab}_G(S) & \subset & \{g : gs_0 \in S\} \\ & = & \{g : g = ss_0^{-1}, s \in S\} \\ & = & \{ss_0^{-1} : s \in S\}. \end{array}$$

Deshalb hat $\mathrm{Stab}_G(S) = H$ höchstens $p^f (= \mathrm{Card}(S))$ Elemente. Diese zwei Aussagen sind nur vereinbar, wenn gilt

$$|H| = p^f.$$

Deswegen haben wir gezeigt, dass $\mathrm{Syl}_p(G)$ nicht leer ist.

Sei nun $? \subset G$ eine Gruppe mit p^α Elementen ($\alpha \leq f$). $?$ operiert auf der G-Menge G/H, wobei $H \in \mathrm{Syl}_p(G)$ gewählt wird. Wegen

$$[G : H] = n/p^f$$

ist die Anzahl von Elementen von G/H nicht durch p teilbar. Deshalb gibt es eine Bahn unter $?$, deren Anzahl von Elementen auch nicht durch p teilbar ist. Wegen Satz 3.10 hat diese Bahn nur ein Element. Sei dieses eine Elemente die Klasse von g in G/H. Für jedes $\gamma \in ?$ gibt es dann $g_\gamma \in H$, so dass

$$\gamma g = g \cdot h_\gamma;$$

oder

$$g^{-1}\gamma g \in H$$

oder

$$g^{-1} ?\, g \subset H.$$

Wenden wir dies auf ein $? \in \mathrm{Syl}_p(G)$ an, erhalten wir die erste Eigenschaft.

Die Menge $\mathrm{Syl}_p(G)$ wird durch

$$(g, H) \longmapsto gHg^{-1}$$

eine transitive G-Menge. Der Stabilisator von H enthält H; deswegen gilt

$$N = \mathrm{Card}\Big(\mathrm{Syl}_p(G)\Big) = |G|/|\mathrm{Stab}_G(H)|.$$

Der letzte Ausdruck teilt $|G|/|H| = n/p^f$. Dies ist ein Teil der zweiten Aussage.

Für die einzige übriggebliebene Aussage betrachten wir $\mathrm{Syl}_p(G)$ als H_0-Menge, wobei H_0 ein festgewähltes Element von $\mathrm{Syl}_p(G)$ ist. Da $|H_0| = p^f$ gilt, hat jede Bahn entweder ein Element, oder die Anzahl von Elementen ist durch p teilbar. Wir zeigen, dass es nur eine Bahn gibt (nämlich $\{H_0\}$ selbst), die aus einem Element besteht. Daraus folgt, dass $N - 1$ durch p teilbar sein muß.

Sei $\{H_1\}$ eine zweite Bahn, die aus einem Element besteht. Nach Definition gilt

$$hH_1h^{-1} = H_1. \qquad (h \in H_0)$$

Deswegen ist die Untermenge $H_0H_1 = \{h_0h_1 : h_0 \in H_0, h_1 \in H_1\}$ von G auch eine Untergruppe. H_0 und H_1 sind in H_0H_1 konjugiert (weil sie es in $\mathrm{Syl}_p(H_0H_1)$ sind). Es gibt dann $h_0h_1 \in H_0H_1$, so dass

$$H_0 = h_0h_1H_1(h_0h_1)^{-1}.$$

Aber die rechte Seite hier ist

$$\begin{aligned} h_0\Big(h_1H_1h_1^{-1}\Big)h_0^{-1} &= h_0H_1h_0^{-1} \\ &= H_1 \end{aligned}$$

Deshalb folgt $H_0 = H_1$. Damit ist die Behauptung bewiesen.

Wir bemerken, dass wir im Laufe des Beweises noch etwas mehr bewiesen haben, nämlich

Korollar 3.15. *Seien G, p^f wie in Satz 3.14. Sei $? \subset G$ eine Untergruppe mit*

$$\mathrm{Card}(?) = p^\alpha.$$

Dann gibt es $H \in \mathrm{Syl}_p(G)$, so dass gilt

$$? \subset H.$$

Als Beispiel nehmen wir die alternierende Gruppe A_5. Sie ist von Ordnung $60 = 2^2 \cdot 3 \cdot 5$. Dann sind die folgenden Sylow-Untergruppen

$$\begin{array}{ll} \{e, (12)(23), (13)(24), (14)(23)\} & (p = 2) \\ \{e, (123), (132)\} & (p = 3) \\ \{(12345)^j : 0 \le j < 5\} & (p = 5). \end{array}$$

Insgesamt hat man

$$\begin{aligned} \mathrm{Card}\ \mathrm{Syl}_2(A_5) &= 5 \\ \mathrm{Card}\ \mathrm{Syl}_3(A_5) &= 10 \\ \mathrm{Card}\ \mathrm{Syl}_5(A_5) &= 6. \end{aligned}$$

Jedes Element von A_5 ist entweder von Ordnung $1, 2, 3$ oder 5. Alle Elemente von Ordnung 2 (bzw. 3) sind miteinander konjugiert. Die $6 \times 4 = 24$ Elemente von Ordnung 5 bilden 2 Konjugationsklassen.

In dieser Gruppe ist A_4 eine Untergruppe

$$\begin{aligned} \{H \subset A_4 : H \in \mathrm{Syl}_2(A_5)\} &= \mathrm{Syl}_2(A_4) \\ &= \{e, (12)(34), (13)(24), (14)(23)\} \\ \{H \subset A_4 : H \in \mathrm{Syl}_3(A_5)\} &= \mathrm{Syl}_3(A_4) \\ &= \{e, (123), (132)\}. \end{aligned}$$

Die Elemente

$$\{(12345)^j, (14)(23)(12345)^j : 0 \leq j < 5\}$$

bilden eine Diedergruppe.

Wir zeigen jetzt, dass es keine Untergruppe $? \subset A_5$ gibt, die Ordnung 20 hat. Weil $\mathrm{Syl}_5(?) \neq \emptyset, \mathrm{Syl}_2(?) \neq \emptyset$ können wir annehmen, dass

$$? \supset \{(12345)^j : 0 \leq j < 5\}.$$

Darüber hinaus hat man von den an $\mathrm{Card}\ \mathrm{Syl}_p(G)$ gestellten Bedingungen, dass

$$\mathrm{Card}\Big(\mathrm{Syl}_5(?)\Big) | 4, 5 | \mathrm{Card}\Big(\mathrm{Syl}_5(?) - 1\Big).$$

Deswegen

$$\mathrm{Card}\ \mathrm{Syl}_5(?) = 1.$$

Die übrigen Elemente aus $?$ müssen von Ordnung 2 sein. Es gibt 15 davon, die in sich nichtüberschneidenden Sylow-Gruppe vierter Ordnung verteilt sind. Deswegen gilt

$$\mathrm{Card}\ \mathrm{Syl}_2(?) = 5.$$

Deshalb liegen alle Elemente von Ordnung 2 in $?$. Unter denen befindet sich $(12)(34)$. Aber $\Big((12)(34)\Big) \cdot (12345) = (245)$. In $?$ kann es aber keine Elemente dritter Ordnung geben. Deswegen existiert $?$ nicht.

Ein anderer *Beweis* ist der folgende:
Weil $A_5/?$ eine A_5-Menge ist, erhalten wir einen Homomorphismus $A_5 \to \Sigma_3$. Da das Bild transitiv operiert, hat das Bild 3 oder 6 Elemente. Der Kern ist ein Normalteiler von Ordnung 20 oder 10. Dieser muß ein Element von $\mathrm{Syl}_5(A_5)$ enthalten - und damit alle. Eine solche Gruppe ist aber A_5 selbst.

Dieses Beispiel zeigt, wie man die Sylow-Sätze anwenden kann, um die Struktur einer Gruppe zu untersuchen. Insbesondere kann man Gruppen klassifizieren, wenn die Ordnung aus wenigen Primzahlen besteht (vgl. Satz 3.13 oben).

Kapitel 4

Die regulären Polyeder

1. Die regulären Polyeder und ihre Gruppen

Ein regulärer Polyeder ist ein Polyeder, dessen Flächen (bzw. Kanten, Ecken) kongruent sind. Für uns wird ein Polyeder ein konvexer Körper sein, dessen Oberflächen aus endlich vielen Vielecken besteht. Es gibt genau fünf, die in drei Gruppen verteilt sind:

1. Die Tetraeder,
2. der Würfel und Oktaeder,
3. der Ikosaeder und Dodekaeder.

Diesen Körpern werden die folgenden Symmetriegruppen zugeordnet:

1. A_4 (oder S_4),
2. S_4 (oder $S_4 \times C_2$),
3. A_5 (oder $A_5 \times C_2$).

Die ersten Gruppen sind die Symmetrien, die aus Drehungen bestehen, die zweiten setzen sich aus Transformationen zusammen, die orthogonal, aber nicht notwendigerweise orientierungstreu sind.

In diesem Abschnitt werden die Gebilde beschrieben. Im nächsten wird gezeigt, dass diese Liste vollständig ist.

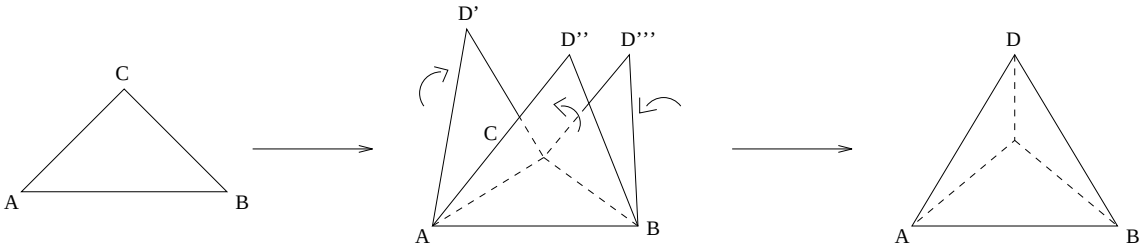
1. Der Tetraeder
Hier fängt man mit einem gleichschenkeligen Dreieck $\triangle ABC$ an. Auf jeder Seite klebt man ein ebenfalls gleichschenkeliges Dreieck (s. Abb., $\triangle ACD', \triangle ABD'', \triangle BCD'''$). Nun faltet man $\triangle ACD'$ und $\triangle ABD''$ zusammen. Weil AD' (bzw. AD'') einen Kegel um AC (bzw. AB) beschreibt, kommen diese nur auf den beiden Schnittgeraden der Kegel zusammen. Wir wählen eine solche Richtung. Da nun $D' = D''$ zutrifft, ist $\triangle D'BC$ gleichschenkelig. Deshalb können wir dieses mit $\triangle D'''BC$ bedecken; d.h. wir falten $\triangle D'''BC$ auf $\triangle D'BC$. Damit haben wir einen Tetraeder konstruiert.

Wichtig daran ist, dass die Dreiecke nur auf eine Weise (oder genauer auf zwei Weisen, die durch eine Spiegelung in der Ebene von $\triangle ABC$ verwandt sind)

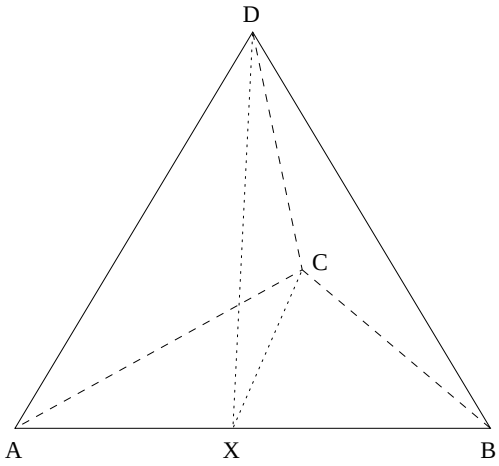
zusammengeklebt werden können. Daher folgt es, dass wenn wir den Tetraeder $ABCD$ so drehen würden, dass ein anderes Dreieck, z.B. $\triangle BCD$ auf die alte Lage von $\triangle ABC$ kommt, auch A zu der alten Lage von D geschickt wird.

Tetraeder

Konstruktion:



Spiegelung:



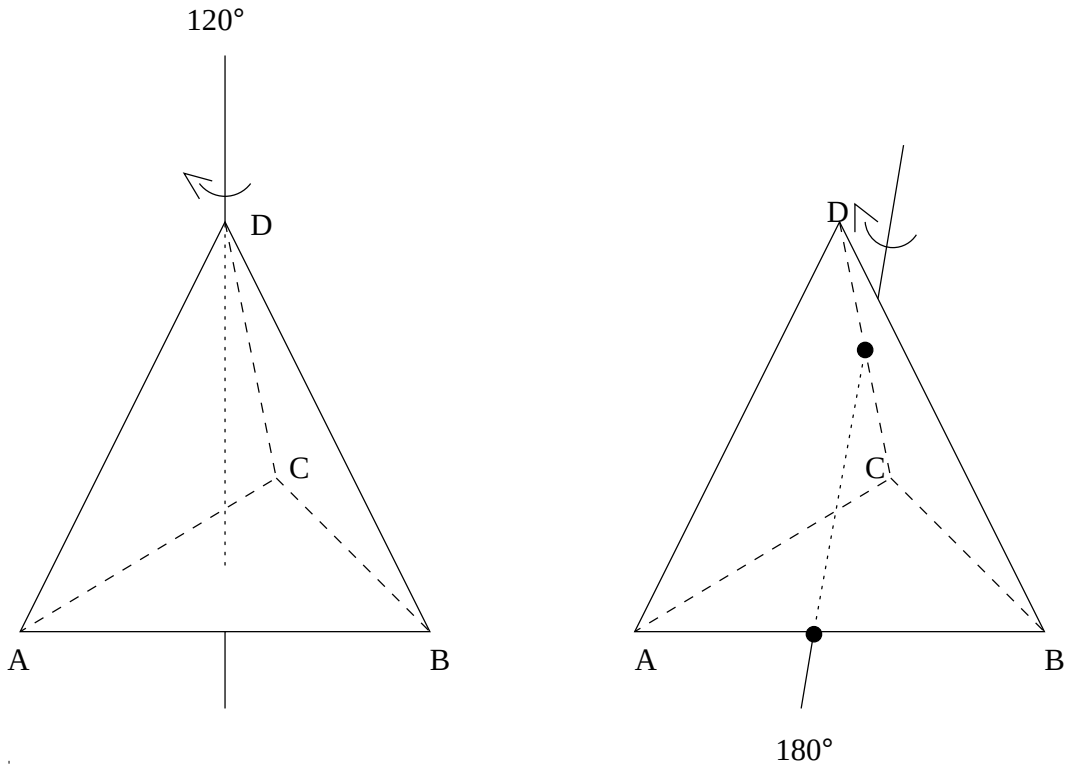
Nun bemerken wird, dass eine Spiegelung in der Ebene CDX, wobei X der Mittelpunkt von AB ist, die Punkte AB vertauscht, die anderen beiden C, D aber festläßt. Se G nun die Gruppe aller orthogonalen Transformationen, die den Tetraeder in sich schicken. Damit ist G eine Gruppe von Transformationen im $\mathbb{R}^3$, die Abstände bewahren. Wir können diese Gruppe als Permutationsgruppe auf den Ecken auffassen. Wir haben gesehen, dass es ein $g \in G$ gibt, so dass gilt

$$g = (BD), (BD), (AC), (AD), (BD).$$

Nach der geläufigen Schreibweise der Theorie der Permutationensgruppen schreiben wir g als (AB). Genauso können wir Spiegelungen finden, so dass jedes andere Paar vertauscht wird.

$$g = (BC), (BD), (AC), (AD), (BD).$$

Drehungen:



Diese Elemente erzeugen die ganze Gruppe S_4. Die sechs Spiegelungsebenen schneiden sich in jedem Punkt $\mathcal{O}$, der den gleichen Abstand von A, B, C und D hat. Wir wählen $\mathcal{O}$ als den Ursprung. Da G Abstände bewahrt, dürfen wir G mit einer Untergruppe von $\mathcal{O}_3(\mathbb{R})$ identifizieren. Hier setzen wir wie früher

$$\mathcal{O}_3(\mathbb{R}) = \{A \in GL_3(\mathbb{R}) : \langle Ax, Ay\rangle = \langle x, y\rangle\},$$

wobei $GL_3(\mathbb{R})$ aus den invertierbaren Matrizen besteht. Wir brauchen von AGLA I den Satz:

Satz 4.1. *Sei $A \in \mathcal{O}_3(\mathbb{R})$. Dann gilt entweder*

$$\det(A) = 1$$

oder

$$\det(A) = -1.$$

Wenn $\det(A) = -1$ *gilt, folgt* $\det(-A) = 1$. *Im Fall*

$$\det(A) = +1$$

gibt es $B \in SO_3(\mathbb{R})$, so dass

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

für irgendwelche θ. Diese Matrix stellt eine Drehung um die "z-Achse" von θ dar.

Beweis. Zur ersten Aussage. Aus

$$^tAA = E_3$$

folgt

$$\det(^tA)\det(A) = 1,$$

oder

$$\det(A^2) = 1.$$

Deswegen

$$\det(A) = \pm 1.$$

Aus $\det(-E_3) = -1$ folgt

$$\det(-A) = -\det(A).$$

Sei $A \in SO_3$; dann ist das charakteristische Polynom von A von Grad 3. Die Eigenwerte sind entweder von der Form $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ oder $\lambda_1 \in \mathbb{R}, \lambda_2, \overline{\lambda_2}$ mit $\lambda_2 \in \mathbb{C} - \mathbb{R}$. Da $\langle A\underline{x}, A\underline{x}\rangle = \langle \underline{x}, \underline{x}\rangle$ folgt für einen Eigenvektor v_1 zum Eigenwert λ_1, dass gilt $\lambda^2\langle v_1, v_1\rangle = \langle v_1, v_1\rangle$. Deswegen gilt $\lambda^2 = 1$ oder $\lambda = \pm 1$. Wir wählen v_1 mit $\| v_1 \| = 1$. Im Falle, dass A lauter reelle Eigenwerte hat, gilt $\lambda_1\lambda_2\lambda_3 = 1$, so dass zwei Möglichkeiten vorkommen (bis auf die Reihenfolge); diese sind $\lambda_1 = 1, \lambda_2 = 1, \lambda_3 = 1$ oder $\lambda_1 = 1, \lambda_2 = -1, \lambda_3 = -1$. Da A den Raum $\langle v_1\rangle^-$ in sich selbst schickt, hat die Einschränkung von A auf $\langle v_1\rangle^-$ die Eigenwerte $+1, +1$ oder $-1, -1$ und die Abbildung ist orthogonal. Man folgert, dass die Einschränkung $\pm$ (Identität) ist.

Falls die Eigenwerte $\lambda_1, \lambda_2, \overline{\lambda_2}$ sind, dann gilt $\lambda_1 \cdot |\lambda_2|^2 = 1$. Deshalb ist λ_1 positiv; es folgt $\lambda_1 = 1$. Die Einschränkung von A auf $\langle v_1\rangle^-$ ist wieder orthogonal. Bezüglich einer orthonomalen Basis hat die Abbildung die Matrix

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

Zusammengefasst gibt es eine Matrix (sogar eine orthogonale Matrix) B_1, so dass gilt

$$B_1AB_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

Wir können jetzt die Koordinaten umnumerieren, so dass wir eine Matrix B_2 haben,

$$B_2AB_2^{-1} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Falls B_2 orthogonal gewählt wurde, gilt

$$\det(B_2) = \pm 1.$$

Falls $\det(B_2) = \pm 1$, setzen wir $B = B_2$, sonst $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} B_2$. Dann haben wir die letzte Aussage von Satz 4.1 bewiesen.

Durch diesen Satz sind die Drehungen von G durch die Eigenschaft

$$\det(A) = +1$$

gekennzeichnet. Wir können sie jetzt bestimmen. Die Abbildung det liefert einen Homomorphismus

$$G \to \{\pm 1\}$$

genauso wie *signum* (sgn).

Nun kehren wir zum Tetraeder zurück. Auf den Spiegelungen, die wir schon beschrieben haben und die die Gruppe G erzeugen, stimmen diese beiden Homomorphismen überein. Sie sind daher gleich, und die Untergruppe der Drehungen ist dann A_4.

Wir können dieses explizit einsehen. Eine Drehung um eine Achse, die senkrecht zur Ebene ABC durch D läuft, wird von der Form (ABC) oder (ACB) sein. Wenn wir zwei gegenüberstehende Seiten AB und CD wählen, die Gerade durch ihren Mittelpunkt bilden und darum eine Drehung von 180° machen, erhalten wir ein Element von G von der Form

$$(AB)(CD).$$

Jedes Element von A_4 ist von einer dieser beiden Formen. Deswegen könne nwir A_4 als die Gruppe der Drehungen darstellen.

Es gibt drei Paare von gegenüberstehenden Kanten, nämlich

$$AB, CD \quad ; \quad AC, BD \quad ; \quad AD, BC \quad .$$

Die Gruppe G permutiert diese. Auf diese Weise erhalten wir die Abbildung

$$\Sigma_4 \to \Sigma_3,$$

die wir schon in Kapitel III, 2. kennengelernt haben.

Übrignes: Der Name "Tetraeder" stammt vom griechischen "tetros" = die Zahl vier, "hedra" = Sitz, Fläche.

2. Der Würfel und Oktaeder

Der Name "Würfel" stammt vom althochdeutschen "wurfil" = Spielwürfel und der Name Oktaeder vom griechischen "oktō" = acht. Dass das Wort "Würfel"

einheimischer Herkunft ist, zeigt deutlich, dass der Würfel der alltäglichste der fünf regulären Körper ist. Es wird hier unnötig sein, dessen Konstruktion zu wiederholen.

Ein Oktaeder kann auf ähnliche Weise wie eine Tetraeder konstruiert werden. Man wählt ein Quadrat, A, B, C, D. Auf jeder Seite klebt man zwei gleichschenkelige Dreiecke

$$\triangle ABE', \triangle ABF', \triangle BCE'', \triangle BCF'', \triangle CDE''', \triangle CDF''', \triangle DAE'''', \triangle DAF''''.$$

Dann faltet man die Dreiecke $\triangle ABE', \triangle BCE'', \triangle CDE''', \triangle DAE''''$ nach oben zusammen und $\triangle ABF', \triangle BCF'', \triangle CDF''', \triangle DAF''''$ nach unten. Daraus entsteht ein Oktaeder. Wenn wir die Mittelpunkt der Flächen eines Würfels anschauen, bilden sie die Ecken eines Oktaeders. Umgekehrt bilden die Mittelöunkte der Flächen eines Oktaeders einen Würfel. Um die erste Aussage zu beweisen, bemerken wir, dass die Mittelpunkte der vier senkrechten Seiten ein Quadrat bilden. Das Übrige ist klar.

Die Umkehrung kann man folgenderweise beweisen: Zu jeder Ecke eines Würfels, in dem wir einen Oktaeder wie oben konstruiert haben, ziehen wir die Strecke zum Mittelpunkt des Würfels. Diese schneidet den Oktaeder. Dass dieser Punkte den gleichen Abstand von den Mittelpunkten der drei Flächen des Würfels, die sich in der Ecke schneiden, hat, ist klar. Diese drei Mittelpunkte sind aber die Ecken einer Fläche des Oktaeders. Alle Mittelpunkte der Flächen des Oktaeders liegen dann auch auf solchen "Radien". Das Verhältnis zum gesamten "Radius" ist für alle Ecken dasselbe. Deshalb bilden die Mittelpunkte der Flächen des Oktaeders einen neuen Würfel, der eine Verkleinerung des ursprünglichen ist (das Verhältnis ist übrigens 1:3).

Wir nennen nun die Ecken eines Würfels $ABCD$ und $A'B'C'D'$, so dass AA', BB', CC', DD' Hauptdiagonale sind (siehe Zeichnung). Sei nun g eine Abbildung $\mathbb{R}^3 \to \mathbb{R}^3$, die Abstände, Geraden und Flächen bewahrt und die den Würfel in sich schickt. Sei G die Menge aller solchen g.

Wir betrachten die $g \in G$, die die Eigenschaft

$$\begin{aligned} g(AA') &= AA' \\ g(BB') &= BB' \\ g(CC') &= CC' \\ g(DD') &= DD' \end{aligned}$$

haben. Dann gilt entweder

$$g(A) = A \quad \text{oder} \quad g(A) = A'.$$

Da B, C', D auf von A ausgehenden Kanten liegen, müssen wir im ersten Fall die folgenden Zuordnungen haben:

$$g(B) = B, g(C') = C', g(D) = D$$

und daher auch

$$g(B') = B', g(C) = C, g(D') = D'.$$

Deshalb schickt g jede Ecke in sich selbst. Es ist leicht zu folgern, dass g selbst die Identität haben muß.

Im zweiten Fall erhalten dagegen

$$g(D) = B', g(C') = C, g(D) = D'$$

und

$$g(B') = B, g(C) = C', g(D') = D.$$

Sei $-I$ die Abbildung

$$\underline{x} \longmapsto -\underline{x},$$

wobei der Mittelpunkt des Würfels als Ursprung gewählt wurde. Dann ist $(-I)\cdot g$ die Identität auf den Ecken und daher die Identitätsabbildung.

Wir schreiben das gerade bewiesene formell hin:

Lemma. *Sei G wie oben. Sei G_1 die Untergruppe aller Drehungen aus G, d.h.*

$$G_1 = \{g \in G : \det(g) = 1\}.$$

Die Untergruppe von G (bzw. G_1), die aus denjenigen Elementen g besteht, die

$$g(AA') = AA', g(BB') = BB', g(CC') = CC', g(DD') = DD'$$

genügen, ist $\{I, -I\}$ (bzw. $\{I\}$).

Nun schauen wir uns G_1 an. Jedes Element $g \in G_1$ permutiert $(AA'), (BB'), (CC'), (DD')$. Nennen wir diese $1, 2, 3, 4$ erhalten wir eine Abbildung $G_1 \to \Sigma_4$. Der Kern ist $\{I\}$ (nach dem Lemma). Da G_1 und Σ_4 beide 24 Elemente besitzen, ist diese Abbildung ein Isomorphismus. Wir haben also einen Isomormphismus

$$G_1 \cong \Sigma_4$$

realisiert.

Sei nun $g \in G$. Dann liegt $(-I)g$ in G_1. Die Abbildung

$$G_1 \times \{\pm I\} \to G; (g, a) \longmapsto ga$$

ist daher ein Isomorphismus, und wir haben eine Abbildung

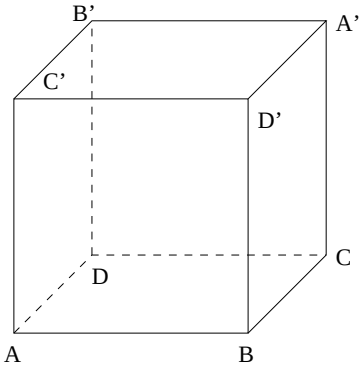
$$G \cong S_4 \times C_2.$$

Wir bemerken zuletzt, dass G und G_1 auf der Menge von gegenüberstehenden Flächen operiert. Dann gibt es drei; die entsprechende Abbildung (Homomorphismus)

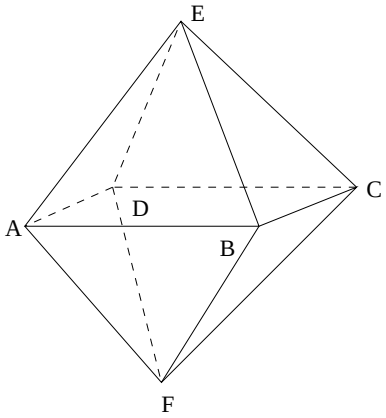
$$\Sigma_4 \to \Sigma_3$$

ist wieder die von Kapitel III, 2.

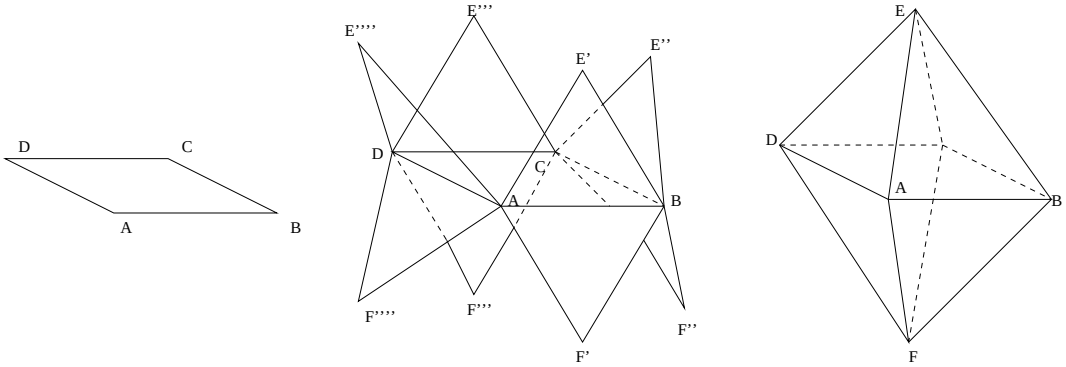
Würfel

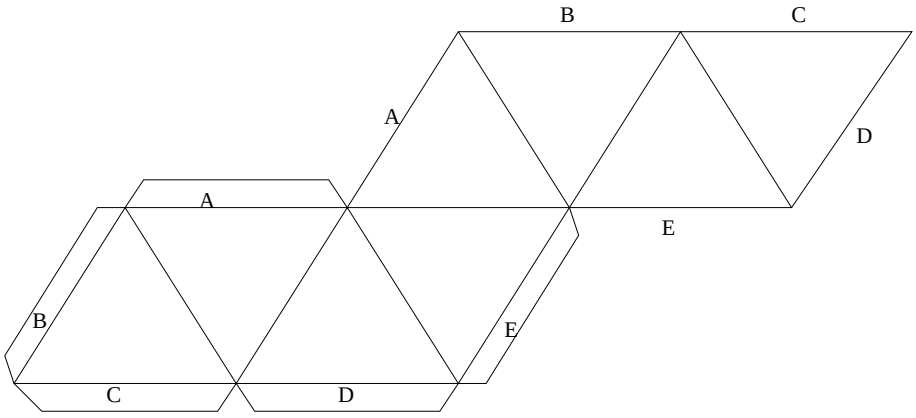


Oktaeder



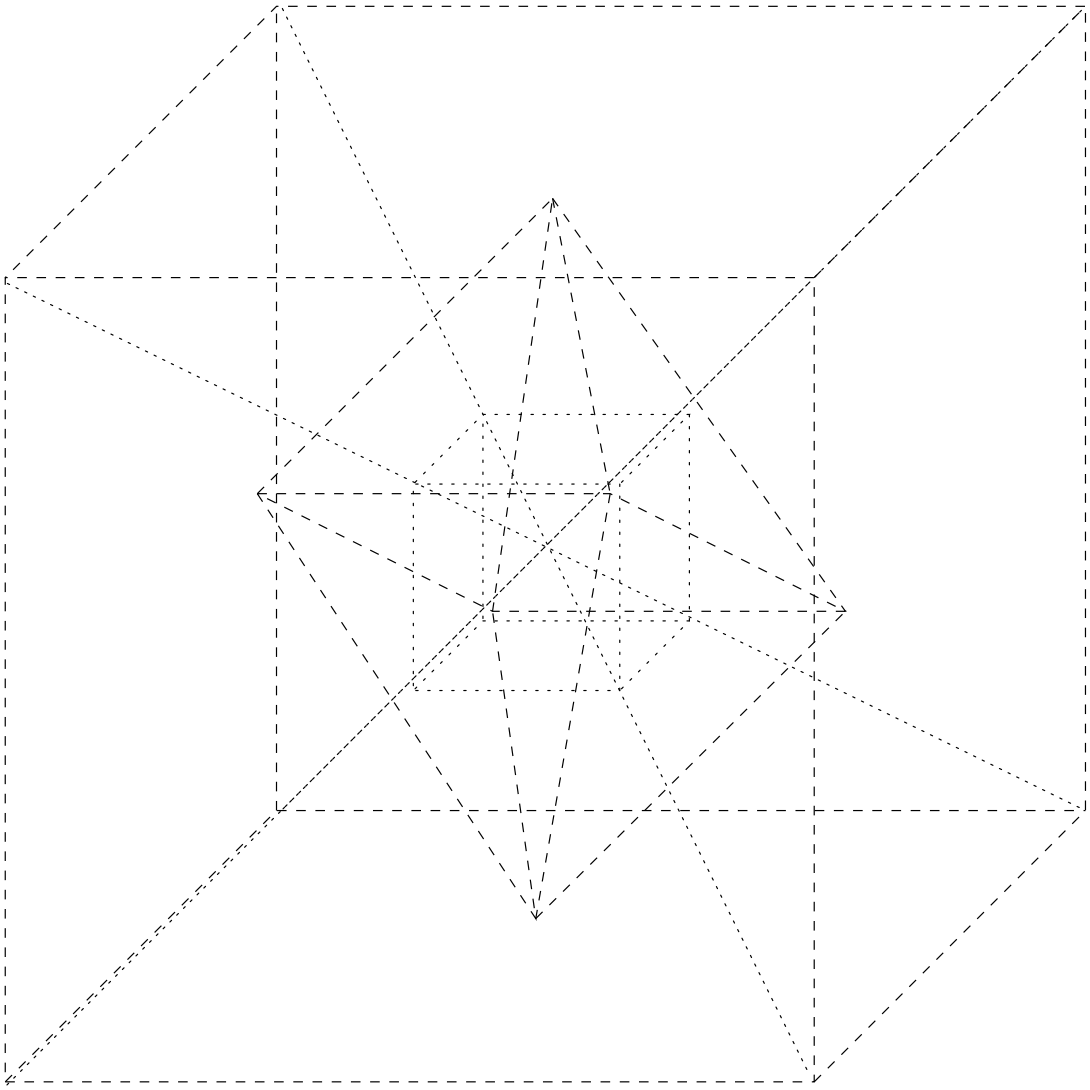
Konstruktion des Oktaeders





Beziehung zwischen Würfel und Oktaeder

Die Ecken des Oktaeders sind die Mittelpunkte der Flächen des größeren Würfels. Die Ecken des kleineren Würfels sind die Mittelpunkte der Flächen des Oktaeders.
Die Seitenlänge des kleineren Würfels beträgt ein Drittel der Seitenlänge des größeren.

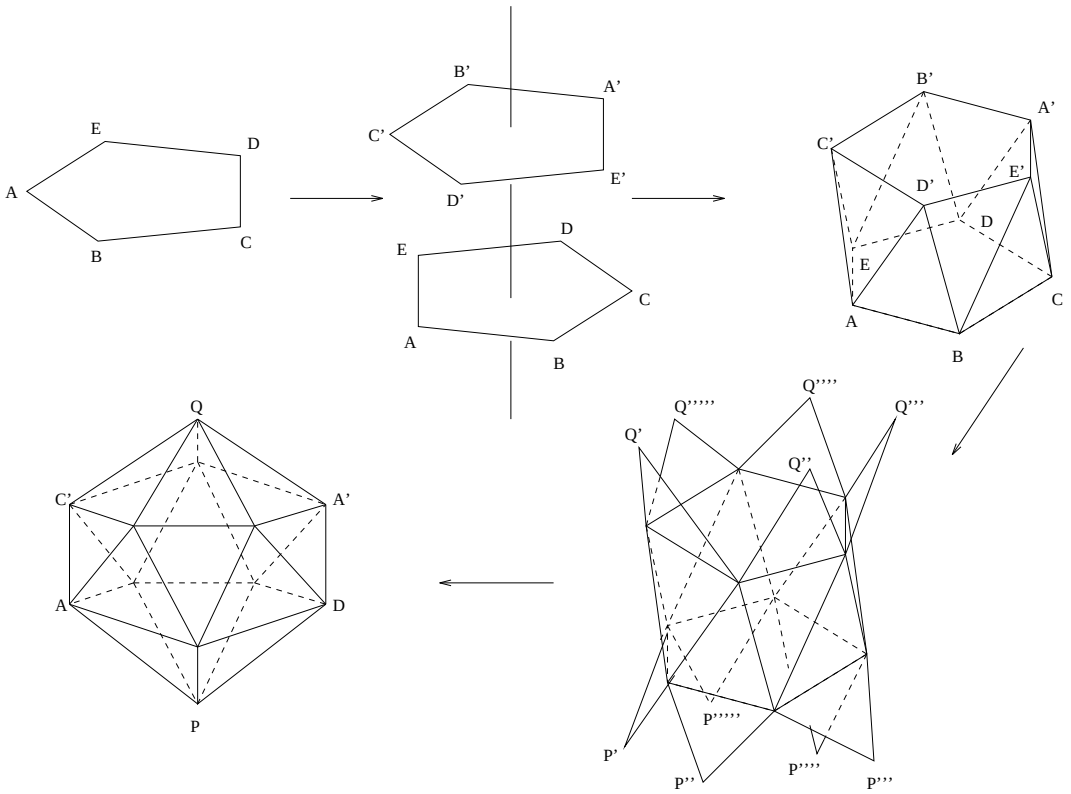


3. Der Dodekaeder und Ikosaeder

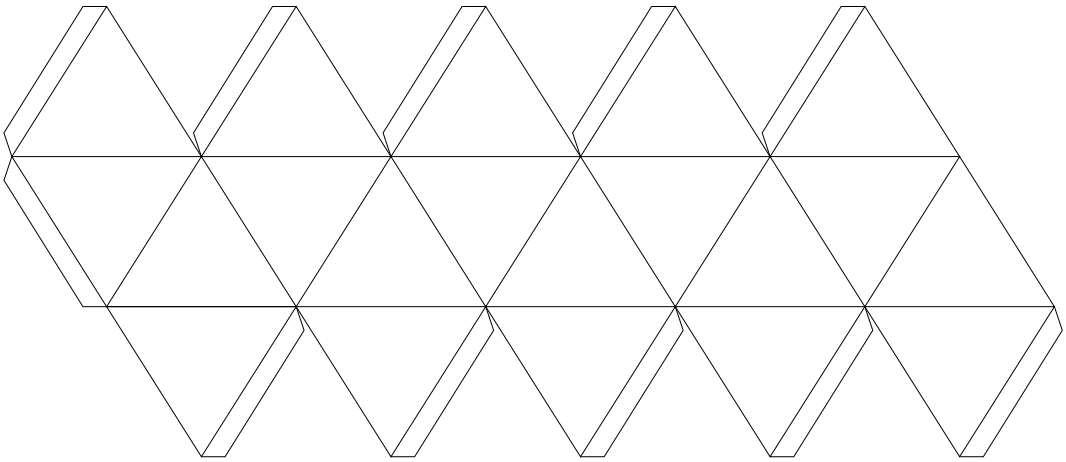
Diese sind die interessantesten und kompliziertesten regulären Körper. Der Dodekaeder hat 12 Flächen (griechisch "dō deka" = zwölf); der Ikosaeder hat 20 Flächen (griechisch "heikosi" = zwanzig). Umgekehrt hat der Dodekaeder 20 Ecken, der Ikosaeder 12. Beide haben 30 Kanten.

Um den Ikosaeder zu konstruieren, gehen wir von zwei übereinanderliegenden regulären Fünfecken aus. Diese liegen in parallelen Ebenen, haben Zentren, die übereinander liegen und sind um einen Winkel von 36° (oder 180°) gegeneinander gedreht. Seien diese $ABCDE$ und $A'B'C'D'E'$. Wir verbinden A mit $C'D'$, B mit $D'E'$, C mit $E'A'$, D mit $A'B'$, E mit $B'C'$. Wir wählen den Abstand zwischen den Ebenen so, dass AC', AD' usw. gleich AB, BC usw. Nun kleben wir auf AB, BC, CD, DE, EA, $A'B'$, $B'C'$, $C'D'$, $D'E'$, $E'A'$ gleichschenkelige Dreiecke, $\triangle ABP'$, $\triangle BCP''$, $\triangle CDP'''$, $\triangle DEP''''$, $\triangle EAP'''''$ und $\triangle A'B'Q'$, $\triangle C'D'Q'''$, $\triangle D'E'Q''''$, $\triangle E'A'Q'''''$. Diese falten wir zusammen und erhalten einen Ikosaeder.

Konstruktion des Ikosaeders



Ein Bastel-Ikosaeder



Man kann auch mit dem gezeichneten Gebilde von gleichschenkeligen Dreiecken durch die angedeuteten Faltungen einen Ikosaeder konstruieren.

Um einen Dodekaeder zu konstruieren, gehen wir von einem regulären Fünfeck aus. Auf jede Seite kleben wir ein reguläres Fünfeck. Nun falten wir diese nach oben, so dass die benachbarten Seiten zusammenkommmen. Diese erfolgt nun auf eine Weise. Wir erhalten eine Schüssel. Nun nehmen wir zwei von diesen Schüsseln, kippen eine um und kleben die beiden zusammen. Wir müssen uns aber überzeugen, dass diese wirklich zusammenpassen.

Dazu betrachten wir eine Schüssel. Die Geraden, die senkrecht zu den Flächen durch deren Zentren laufen, müssen sich in einem Punkt treffen (Symmetrie). Die Ecken sind alle gleich weit von diesem "Mittelpunkt" entfernt. Wir bilden die Sphäre, die diesen Mittelpunkt hat und durch die Ecken läuft. Nun projezieren wir die Seiten auf diese Sphäre. Wir erhalten sechs reguläre Fünfecke, deren Seiten Strecken von Großkreisen sind.

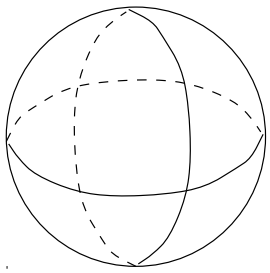
Dass an den inneren Ecken drei Fünfecke zusammenkommen, bedeutet: die inneren Winkel der Fünfecke sind 120°. Deshalb sind auch die Außenwinkel der Projektion der Schüssel auf der Sphäre 120° ($= 360° - 2 \times 120°$). Dass diese Projektionen zusammenpassen, ist nun klar. Damit existiert der Dodekaeder.

Wir bemerken noch, dass die Mittelpunkte der Flächen eines Dodekaeders die Ecken eines Ikosaeders bilden und umgekehrt. Dieses weist man durch Aufzählung nach. Es folgt auch daraus, dass es nur einen Weg gibt, den Ikosaeder zu bauen.

Wir bestimmen jetzt die zugehörigen Rotationsgruppen. Wir bemerken, wenn wir den Mittelpunkt als Ursprung wählen, schickt die Abbildung $\underline{x} \longmapsto -\underline{x}$ den Ikosaeder und den Dodekaeder in sich selbst. Das wurde auch schon beim Würfel und Oktaeder bemerkt. Wir brauchen dann nur die eigentlichen Drehungen ($\det = 1$) anzusehen. Weil man den Dodekaeder um die Achse drehen kann,

die durch die Mittelpunkte zweier gegenüberliegender Flächen läuft, erhält man fünf Drehungen. Jede Fläche kann aber auch in jede andere. Dadurch erhalten wir $60 = 5 \times 12$ Drehungen. Es wird jetzt bewiesen, dass die dadurch gebildete Gruppe die alternierende Gruppe A_5 ist.

Es ist nötig, irgendwas zu finden, das aus einer Zusammensetzung von fünf Objekten besteht, so dass wir die Drehungsgruppe als eine Permutationsgruppe von 5 Objekten auffassen dürfen. Dazu betrachten wir zuerst eine Seite des Ikosaeders, den wir wieder auf eine Kugel projezieren. Wir setzen diese Seite zu einem vollständigen Großkreis fort; dieser enthält dann eine zweite Seite und schneidet zwei andere Seiten senkrecht. Diese liegen wiederum auf einem Großkreis, der zwei andere Seiten schneidet, die wir ebenfalls zu einem Großkreis fortsetzen. Wir erhalten daraus ein System von drei senkrechten, sich schneidenen Kreisen, die so aussehen:



Dieses Gebilde enthält 6 Kanten. Es gibt aber 30 Kanten und dadurch 5 solcher Systeme. Wir stellen uns vor, dass eine Elefant auf unseren Ikosaeder getreten hat. Wir erhalten ein ebenes Bild, das aus Punkte und Verbindungsstrecken besteht. Wir färben die Seiten mit rot, blau, grün, purpur, orange ein (r, b, g, p, o). Das zustandekommende Bild folgt. Jede Drehung permutiert diese Seiten. Beim Ikosaeder kommt jede Kombination von drei Farben zweimal vor (es gibt $\binom{5}{3} = 10$ solche Kombinationen und 20 Seiten). Nun bemerken wir, dass die Orientierung nur einmal vorkommt. Der Grund dafür liegt darin, dass die Flächen, die gleich gefärbt sind, gegenüber liegen und die Abbildung $\underline{x} \to -\underline{x}$, also eine nichtorientierungsfähige Abbildung, den Vergleich der beiden Flächen verschafft.

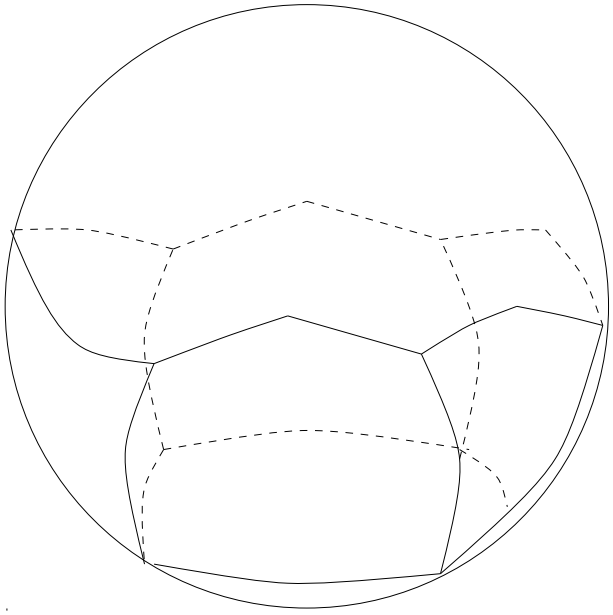
Deswegen ist die einzige Drehung, die keine Wirkung auf die Farben ausübt, die Identität, weil alle Flächen fest bleiben. Auf diese Weise erhalten wir eine Abbildung

$$G_1 \to \Sigma_5,$$

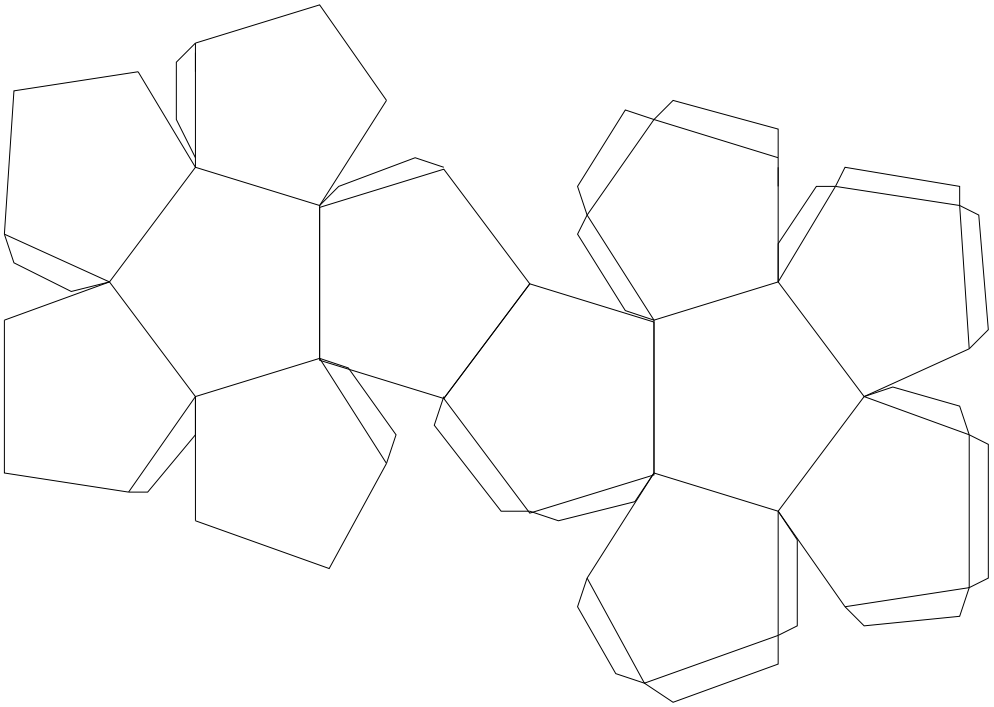
wobei G_1 die Gruppe der Drehungen bezeichnet. Das Bild hat 60 Elemente. Wir können aber jede Fläche in jede andere bringen, wenn wir eine Folge von Drehungen um Ecken anwenden, die eine Fläche in eine Nachbarfläche schickt. Wir bemerken, dass eine solche durch einen 5er-Zyklus in Σ_5 dargestellt wird, weil alle fünf Farben an jeder Ecke zusammenkommen. Diese liegen in A_5. Wenn wir eine festgewählte Fläche in eine andere gebracht haben, bleiben nur drei Möglichkeiten. Wie man leicht feststellt, werden die Drehungen einer Seite durch 3er-Zyklen

dargestellt, die auch in A_5 liegen. Deswegen liegt das Bild des Homomorphismus in A_5. Da G_1 und A_5 beide 60 Elemente besitzen, ist dieser Homomorphismus ein Isomorphismus. Damit ist die Identifikation hergestellt.

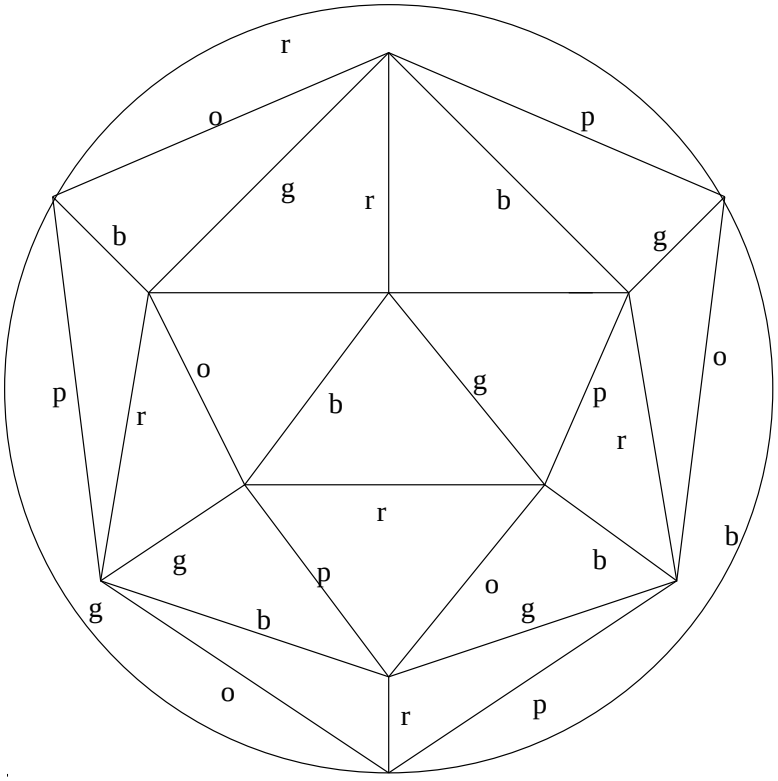
Projektion der Schüssel auf die Sphäre



Ein Basteldodekaeder



Plattgedrückter Ikosaeder



r = rot
b = blau
g = grün
p = purpur
o = orange

(Nachfärben empfohlen!)

2. Es gibt keinen anderen regulären Polyeder

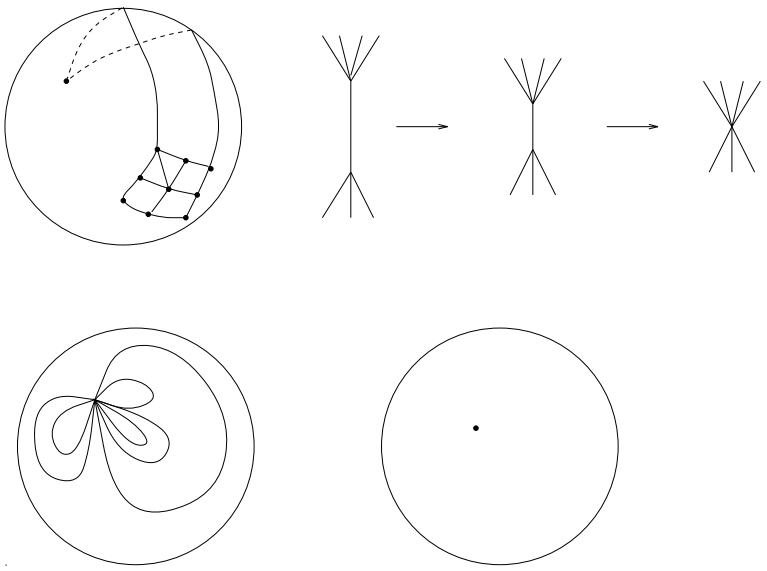
Die fünf regulären Polyeder wurden von den Griechen entdeckt. Sie haben auch bewiesen, dass es keine anderen gibt. Diese Aussage kann in mehreren Weisen gezeigt werden, und in diesem Abschnitt wird ein Beweis angegeben. Mittelpunkt dieses Beweises ist eine allgemeine Eigenschaft der Polyeder, die Eulersche Formel, die eigentlich zur "Topologie" gehört.

Satz (Eulersche Formel). *Sei P ein Polyeder mit e_0 Ecken, e_1 Kanten und e_2 Flächen. Dann gilt*

$$e_0 - e_1 + e_2 = 2.$$

Beweis. Wir nehmen einen inneren Punkt $\mathcal{O}$ von P und eine Sphäre mit Zentrum $\mathcal{O}$. Wir projezieren P auf die Sphäre und erhalten dadurch ein System von Wegen auf der Sphäre, die die Sphäre in getrennte Gebiete zerlegen (diese Wege brauche keine Großkreise zu sein). Wir betrachten diese Wegen als Schnüre, die zusammengeknotet werden. Wenn wir an eine Schnur denken, können wir diese immer kürzer machen, bis endlich die beiden Endpunkte verschmelzen (angenommen, dass sie vorher nicht gleich waren). Dabei verschwindet eine "Kante", und zwei Ecken werden zu einer. Dabei aber bleibt $e_0 - e_1 + e_2$ erhalten. Wir wiederholen dieses Verfahren, bis alle "Kanten" nur einen Endpunkt haben.

Nun betrachten wir zwei Kanten des ursprünglichen Gebildes. Wenn wir auf der Sphäre von einem Punkt auf einer Kante zu einem Punkt auf der anderen laufen wollten, könnten wir immer "auf dem Weg" bleiben, also statt ein Feld zu überqueren, könnten wir auf dem Rand bleiben (bei P hat jede Fläche nur ein Randstück). Wenn mehr als eine Ecke übrigbleibt, müssten zwei davon verbunden sein; wir hätten das Verfahren noch nicht zu Ende geführt. Deshalb bleibt nur eine Ecke übrig.



Wenn wir einen Weg (eine Kante) wegwischen würden, würden zwei Flächen vereinigt. Es gäbe eine Fläche und eine Kante weniger; $e_0 - e_1 + e_2$ bliebe aber wieder erhalten. Wir wiederholen dieses Verfahren, bis es keine Kanten mehr gibt. Es bleiben eine Fläche (die Sphäre selbst) und ein Punkt übrig. Daher erhalten wir für $e_0 - e_1 + e_2 = 1 - 0 + 1 = 2$. Damit ist der Satz bewiesen.

Dieser Satz ist sehr allgemein; wir brauchten nicht etwa "Regularität" anzunehmen, sondern nur, dass der Polyeder auf eine Sphäre bijektiv abgebildet werden konnte und dass die Flächen nur ein Randstück hatten.

Nun betrachten wir einen regulären Polyeder P. Wir nehmen an, dass an jeder Ecke m Kanten zusammentreffen, jede Fläche n Seiten (=Kanten) hat und dass es insgesamt N Flächen gibt.

Da jede Kante auf dem Ran von zwei Flächen liegt, gibt es

$$\frac{N \cdot m}{2}$$

Kanten. Da jede Kante zwei Endpunkte hat, die Ecken sind, gibt es

$$\left(\frac{Nm}{2}2\right)/n = \frac{Nm}{n}$$

Ecken.

Darüber hinaus gelten

$$n \geq 3, m \geq 3,$$

weil eine Fläche mindestens drei Seiten hat und mindestens drei Flächen an einer Ecke zusammenkommen.

Nun wenden wir die Eulersche Formel an. Es glten

$$\begin{aligned} e_0 &= \frac{Nm}{n} \\ e_1 &= \frac{Nm}{2} \\ e_2 &= N \end{aligned}$$

und daher

$$2 = e_0 - e_1 + e_2 = \frac{Nm}{n} - \frac{Nm}{2} + N.$$

Wir teilen durch mN und erhalten

$$\frac{2}{m} + \frac{1}{2} = \frac{1}{m} + \frac{1}{n}.$$

Insbesondere

$$\frac{1}{m} + \frac{1}{n} > \frac{1}{2}.$$

Da $\frac{1}{m} \leq \frac{1}{3}$ erhalten wir

$$\frac{1}{n} > \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$$

oder

$$n < 6$$

oder

$$n \leq 5.$$

Genauso erhalten wir

$$m \leq 5.$$

Die einzigen (m, n) mit $\frac{1}{m} + \frac{1}{n} > \frac{1}{2}$ sind

$$\begin{gathered}(3,3), (3,4), (3,5) \\ (4,3), (5,3).\end{gathered}$$

Schon 5 Lösungen. Wir bilden Paare

$$\begin{gathered}(3,3) \qquad \text{(Einzelgänger)} \\ (3,4), (4,3) \\ (3,5), (5,3).\end{gathered}$$

Dann gilt (wegen $\frac{2}{Nm} + \frac{1}{2} = \frac{1}{m} + \frac{1}{n}$)

$$\begin{aligned} N &= 4 \quad \text{für } (3,3) \\ &= 8 \quad \text{für } (3,4) \\ &= 6 \quad \text{für } (4,3) \\ &= 20 \quad \text{für } (3,5) \\ &= 12 \quad \text{für } (5,3) \end{aligned}$$

P wird aus N m-Ecken konstruiert. Wir erkennen in dieser Liste Tetraeder, Oktaeder, Würfel, Ikosaeder und Dodekaeder. Bei jeder Ecke kommen n Flächen zusammen. Wie wir bei den Konstruktionen in Kapitel IV, 1. gesehen haben, gelingt uns diese Konstruktion nur auf einer eindeutig bestimmten Weise. Deshalb gibt es keine weiteren regulären Polyeder als die, die in Kapitel IV, 1. aufgezählt wurden.

Kapitel 5

Ornamente, Kristalle und Heiratsregeln

1. Tapetenmuster und Kristalle

Wir wissen alle vom Kunstunterricht, wie man reguläre Muster mit Hilfe von Kartoffeldrucken herstellt. Man bereitet die Kartoffel vor, druckt eine Reihe des Motivs, geht zurück zum Anfang der Reihe und fängt darunter nochmals an. Es entstehen Reihen von Abdrücken, die eventuelle gegeneinander verschoben sind.

Wenn wir etwas phantasievoller an die Arbeit gehen, könnten wir die Kartoffel regelmäßig drehen, so dass das Muster nicht immer in derselben Richtung liegt. Wir erfahren aber, dass die Wirkung dieselbe ist, als ob wir mit einer viel größeren Kartoffel angefangen hätten, worauf mehrer Kopien des Musters in allen vorkommenden Richtungen sind und wir diese ohne sie zu drehen verwendet hätten. Genauso kann man Spiegelungen statt Drehungen anwenden. Ein Beispiel für das allereinfachste Muster ist auf Abb. 1 zu sehen. Ein anderes mit Drehung wird in Abb. 2 gezeigt, wobei ein interessantes Muster hier einfach durch ein (ersetzt wurde.

Solche Muster wurden in früheren Jahren für geblümte Tapeten verwendet, insbesondere für geblümte Tapeten verwendet, insbesondere für diejenigen von William Morris und seinen Nachfolgern. Sie wurden auch in der arabischen Kunst sehr häufig verwandt, da die islamische Religion die Darstellung lebendiger Wesen verbietet; s. dazu H. Weyl: Symmetrien.

Solche Muster heißen *Tapetenmuster*. Die Abbildungen zeigen die verschiedenen Möglichkeiten. In diesem Abschnitt wird erklärt werden, wie diese mathematisch aufzufassen sind.

Abb . 1

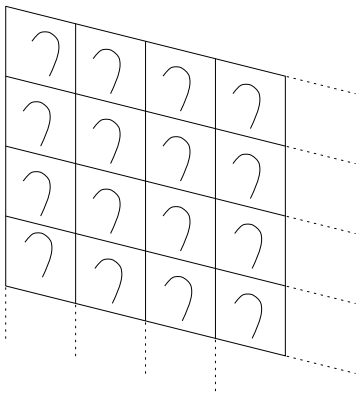
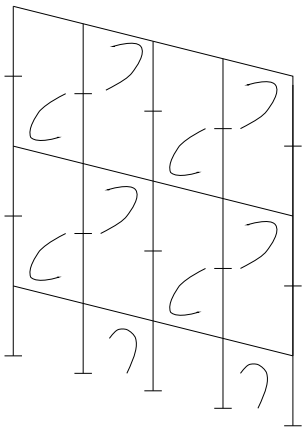
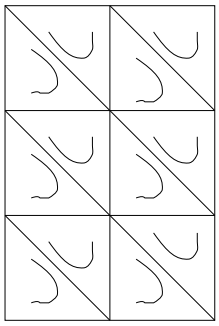
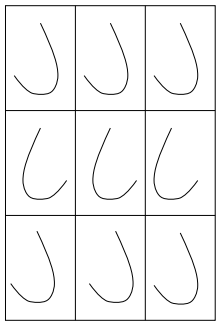
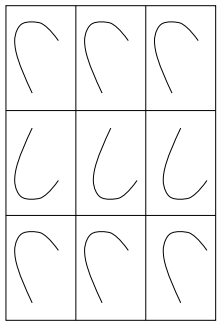


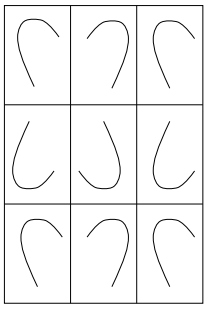
Abb. 2

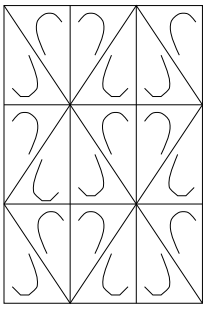


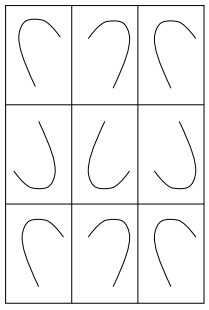


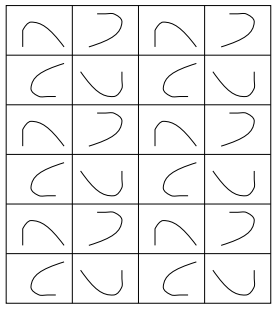


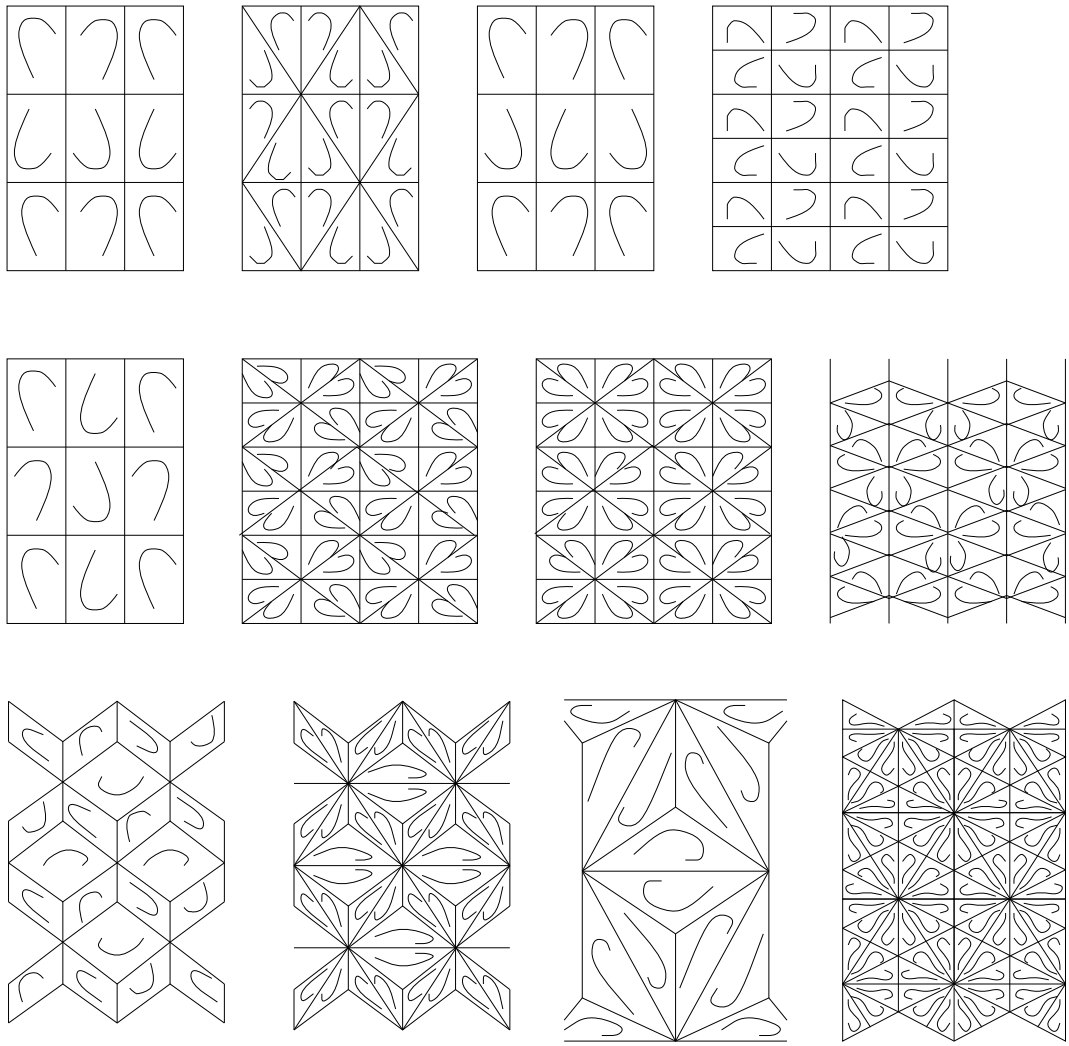












Zuerst ist aber eine Bemerkung angebracht. Die Überlegungen, die hier in der ebenen Geometrie durchgeführt werden, können auch auf andere Dimensionen erweitert werden. Dabei ist die Dimension 3 besonders wichtig, weil diese in der Kristallographie Anwendungen findet. In diesem Kristall sitzen die Atome in einem regelmäßigen Gitter, das besonders stabil ist (vgl. K. Vonnegut "Cat's Cradle"). Makroskopisch wird dies durch die äußere Form des Kristalls sichtbar. Die inere Struktur ist auch mit Röntgenspektroskopie feststellbar. Wenn mehrere Elemente vorhanden sind, kann das Kristall interessant und kompliziert sein; diejenigen, die in der Mineralogie bei Edelsteinen und Halbedelsteinen gefunden werden, belegen diese These. Wie gut diese Struktur zur Geltung kommt, hängt von der Kunst des Diamantenschleifers ab. Insgesamt gibt es im Dreidimensionalen 230 verschiedene Möglichkeiten. Deswegen ist die Kristallographie schon mathematisch interessant (aber nicht nur von diesem Gesichtspunkt).

Zunächst wird skizziert, wie diese Objekte mathematisch beschrieben werden können. Wir erinnern uns, dass wir die Ebene mit $\mathbb{A}$ un die Gruppe der euklidischen Bewegungen mit $\mathbb{E}$ bezeichnet haben.

Definition. Eine Untergruppe G von $\mathbb{E}$ heißt eine *Tapetengruppe*, wenn die folgenden Bedingungen erfüllt sind:

TG 1: Es gibt eine beschränkte Menge $B \subset A$, so dass gilt

$$\bigcup_{g \in G} g(B) = \mathbb{A}.$$

TG 2: Sei $P \in \mathbb{A}$. Dann ist die Menge

$$\{g(P) : g \in G\}$$

diskret, d.h. wenn $Q = gP(g \in G), Q \neq P$ gelten, dann gibt es ein $c > o$, so dass der Abstand zwischen P und Q mindestens c ist.

Mit anderen Worten: Bei TG 1 wird verlangt, dass es einen "Kartoffeldruck" gibt, dessen Wiederholungen nach dem Muster von G die ganze Ebene bedecken.

Bei TG 2 muß man etwas aufpassen. Die Stabilisatorgruppe von P braucht nicht trivial zu sein. Wir werden sehen, dass sie aber immer endlich ist (sogar höchstens von Ordnung 6). Dann bedeutet TG 2, dass die "Kartoffelabdrucke" sauber getrennt voneinander sein sollten.

Im dreidimensionalen Fall bedeutet TG 1, dass das Kristall eine räumliche Ausdehnung hat. TG 2 besagt, dass die Atome wirlich voneinander getrennt sind. (In diesem Fall müssen $\mathbb{A}$ und $\mathbb{E}$ durch ihre dreidimensionalen Analogien ersetzt werden; davon wird hier nicht die Rede sein.)

Sei -wie früher- $\mathbb{T}$ die Gruppe der Translationen; $\mathbb{T}$ ist ein Normalteiler von $\mathbb{E}$. Die Quotientengruppe $\mathbb{E}/\mathbb{T}$ wird mit $\mathbb{D}$ bezeichnet; sie ist zu $\mathcal{O}_2$ isomorph. Sei

$$d : \mathbb{E} \to \mathbb{D}$$

die zugehörige Abbildung. Diese Tatsachen gehen aus den Überlegungen von Kapitel II, 2. hervor.

Der zentral Satz in diesem Abschnitt ist folgender:

Satz 5.1. *Sei G eine Tapetengruppe. Seien*

$$\begin{aligned} ?(G) &= d(G) \subseteq \mathbb{D} \\ L(G) &= G \cap \mathbb{T}. \end{aligned}$$

Dann ist $L(G)$ ein Normalteiler von G, der auch TG 1 *und* TG 2 *genügt und die Quotientengruppe*

$$G/L(G) \cong ?(G)$$

ist endlich.

Beweis. Dieser Beweis wird unter der folgenden Voraussetzung geführt:
In B (vgl. TG 1) gibt es nur endlich viele Punkte P, so dass gilt

$$\mathrm{Stab}_G(P) \neq \{e\}.$$

Diese Voraussetzung kann aus TG 1 und TG 2 gefolgert werden. Zuerst bemerken wir, dass es genügt, die Endlichkeit von $?\,(G)$ zu zeigen. Denn dann ist der Kern der Einschränkung von d auf G, also der Kern von $?\,(G)$, genau

$$G \cap \mathbb{T} = L(G).$$

Seien $g_1, \ldots, g_N \in G$ Elemente, so dass

$$?\,(G) = \{d(g_i) | 1 \leq i \leq N\}$$

ist. In TG 1 sei

$$B^* = \bigcup_i g_i(B).$$

Nun kann $g \in G$ als $lg_i (l \in L(G), 1 \leq i \leq N)$ geschrieben werden, denn es muß ein i geben, so dass gilt

$$d(g) = d(g_i).$$

Daher:

$$d(gg_i^{-1}) = e$$

also

$$gg_i^{-1} \in \operatorname{Kern} d = L(G)$$

d.h.

$$l := gg_i^{-1} \in L(G),$$

oder

$$g = lg_i.$$

Nun

$$\begin{aligned} \mathbb{A} = \bigcup_{g \in G} g(B) &\subset \bigcup_{l \in L(G)} \bigcup_i l\Big(g_i(B)\Big) \\ &= \bigcup_{l \in L(G)} l(B^*). \end{aligned}$$

Deshalb ist TG 1 erfüllt. TG 2 ist automatisch erfüllt. Deswegen ist auch $L(G)$ eine Tapetengruppe. Jetzt zur Endlichkeit von $?\,(G)$ mit einem Umweg über $\operatorname{Stab}_G(P)$. Wegen Satz 1.2 gilt

$$?\,(G) = G/L(G),$$

weil $L(G)$ der Kern des Homomorphismusses $d|G$ ist.

Wir zeigen, dass

$$\operatorname{Stab}_G(P)$$

endlich ist und sogar, dass es ein N gibt, so dass die Ordnung von $\operatorname{Stab}_G(P)$ kleiner als N ist, wobei N unabhängig von P ist. Sei R der maximale Durchmesser von B. Es muß ein $g(P)$ geben, so dass $g(P) \neq P$ und der Abstand von P nach $g(P)$ kleiner als $2R$ ist. Sonst wäre TG 1 nicht erfüllt, da es eine Lücke im Muster gäbe.

Sei $Q = g(P)$. Dann liegt die Menge

$$hQ \quad \Big(h \in \mathrm{Stab}_G(P)\Big)$$

auf einem, Kreis, dessen Radius kleiner als $2R$ ist. Die Abstände zwischen den einzelnen hQ sind nach TG 2 aber minestens c; es liegen dann höchstens $\frac{4\pi R}{c}$ Punkte auf dem Kreis. Deshalb hat die Drehungsgruppe um P höchstens die Ordnung $\frac{4\pi R}{c}$, die volle Gruppe (d.h. einschließlich Spiegelungen) höchstens $\frac{8\pi R}{c}$. Nach der weiteren Voraussetzung gibt es ein N, so dass jedes Element von $\mathrm{Stab}_G(P)$ höchstens die Ordnung N hat (für alle P), wobei N nur von G abhängt.

Sei nun $g \in G, d(g) \neq e, \det\Big(d(g)\Big) = 1$. Dann kann g als Abbildung der Form

$$x \longmapsto Ax + b$$

geschrieben werden ($A \in \mathcal{O}_2, b \in \mathbb{R}^2$). Da $d(g) \neq e$ gilt, folgt $A \neq E$. Wir suchen einen Fixpunkt von g; dieser wird durch

$$Ax + b = x$$

bestimmt. Oder

$$(E - A)\underline{x} = \underline{b}.$$

Weil $\det(A) = +1$ folgt, dass $E - A$ nicht singular ist. Deshalb gibt es einen Fixpunkt und $d(g)$, die dieselbe Ordnung wie A hat, hat höchstens Ordnung N.

Deshalb hat auch

$$?_1(G) = \{\gamma \in ?(G) : \det(\gamma) = 1\}$$

höchstens die Ordnung N, weil $?_1(G)$ einfach aus Drehungen besteht. Aber $?_1(G)$ ist ein Normaltieler von $?(G)$ (da $?_1(G)$ der Kern der Abbildung det ist) und

$$?(G)/?_1(G) \cong \{1\} \quad \text{oder} \quad \{\pm 1\}.$$

Deswegen ist $?(G)$ auch endlich, denn $\mathrm{ord}\,?(G)$ höchstens $2N$ und damit ist der Satz bewiesen.

Satz 5.2. *Sei $\gamma \in ?(G)$. Dann hat γ die Ordnung $1, 2, 3, 4$ oder 6.*

Beweis. Wir fassen $?(G)$ als die Menge aller A auf, die in G vorkommen, wenn wir $G \subset \mathbb{E}$ in der Form

$$\underline{x} \longmapsto A\underline{x} + \underline{b}$$

darstellen. Ein Element aus $L(G)$ ist von der Form

$$\underline{x} \longmapsto \underline{x} + \underline{b'}.$$

Nun berechnen wir $g_1^{-1} g_2 g_1$, wobei

$$\begin{aligned} g_1 : \underline{x} &\longmapsto A\underline{x} + \underline{b} \\ g_2 : \underline{x} &\longmapsto \underline{x} + \underline{b'} \end{aligned}$$

sind. Wir finden

$$\begin{aligned} g_1^{-1}g_2g_1(x) &= g_1^{-1}(Ax+b+b') \\ &= A^{-1}(Ax+b+b')-A^{-1}b \\ &= x+A^{-1}b'. \end{aligned}$$

Deshalb, fassen wir $L(G)$ als die Menge aller solchen $b's$ auf, sehen wir, dass aus $b' \in L(G)$

$$A^{-1}b' \in L(G)$$

folgt.
Natürlich erhält man bei der Verknüpfung

$$b'_1, b'_2 \in L(G) \Rightarrow b'_1 + b'_2 \in L(G).$$

Wir wissen von AGLA I:

$$A^2 - \mathrm{Tr}(A)A + \det(A)E = 0. \qquad (*)$$

Da aus $\det(A) = -1$, $A^2 = E$ folgt, dürfen wir annehmen, dass gilt

$$\det(A) = +1.$$

Multiplizieren wir $(*)$ mit A^{-1}, folgt

$$A + A^{-1} = \mathrm{Tr}(A)E.$$

Wenden wir dies auf $b' \in L(G)$ an, so erhalten wir

$$\left(A + A^{-1}\right)(b') = \mathrm{Tr}(A)b'.$$

Die linke Seite liegt in $L(G)$. Es folgt

$$\mathrm{Tr}(A)b' \in L(G);$$

wir wählen nun b' so, dass b' nicht ein Vielfaches von einem anderen Element aus $L(G)$ ist und folgern:

$$\mathrm{Tr}(A) \in \mathbb{Z}.$$

Aber es gilt auch

$$\mathrm{Tr}(A) = 2\cos\theta,$$

wenn A eine Drehung um θ ist. Deshalb

$$|\mathrm{Tr}(A)| \leq 2.$$

Die Möglichkeiten sind nun

$$\mathrm{Tr}(A) = -2, -1, 0, 1, 2$$

mit

$$\theta = \pi, \frac{2\pi}{3}, \frac{\pi}{2}, \frac{\pi}{3}, 0.$$

In diesem Fall ist A von Ordnung $2, 3, 4, 6$ und 1. Damit ist der Satz bewiesen.

Man kann zeigen, dass $L(G)$ von der Form

$$\{m'\underline{e}' + m''\underline{e}''|m', m'' \in \mathbb{Z}\}$$

ist, wobei $e', e'' \in L(G)$ linear unabhängig sind.

Eine solche Gruppe heißt *ein Gitter*. Hier wird eine Skizze des für uns nicht ausschlaggebenden Beweises angegeben. Man wählt $\underline{e}' \in L(G)$, so dass $\underline{e}'$ nicht ein Vielfaches eines anderen Elementes ist. Dann nehmen wir $\underline{f} \in L(G)$, $\underline{f}$ kein Vielfaches von $\underline{e}'$. Wir erhalten von TG 1, dass ein solches $\underline{f}$ existiert. Im Parallelogramm mit den Ecken $\underline{+e}*, \underline{+f}$ liegen nur endlich viele Elemente von $L(G)$, (TG 2). Davon wählen wir eines, $\underline{e}''$, so dass kein weiteres Element von $L(G)$ innerhalb des Parallelogramms mit den Ecken $\underline{+e}', \underline{+e}''$ liegt; wir haben das Parallelogramm so klein wie möglich gemacht. Wir nehmen als Basis von $\mathbb{R}^2$ $\underline{e}', \underline{e}'' - \underline{e}'$. Dann liegen

$$(1, 0), (1, 1)$$

in $L(G)$. Andererseits gilt

$$L(G) \cap \{(x_1, x_2)||x_1| < 1, \quad |x_2| < 1\} = \{0\}.$$

Hiervon kann man leicht beweisen (der Beweis läuft wie der von Satz 3.3), dass gilt

$$L(G) = \{(m_1, m_2)|m_1, m_2 \in \mathbb{Z}\}.$$

Wenn man so weit gekommen ist, muß man die verschiedenen $L(G)$ und $?(G)$ klassifizieren. (Hat $?(G)$ ein Element von Ordnung $3, 4$ oder 6, ist $L(G)$ schon bestimmt.) Die Arbeit ist von diesem Punkt an recht fummelig; die wesentlichen Ideen stecken aber in den beidne obigen Sätzen. Mit dieser Schilderung sollte es klar sein, wie es überhaupt möglich ist, solche Gruppen zu klassifizieren. Die entsprechende Arbeit im Falle von drei Dimensionen ist etwas schwerer, folgt aber demselben Muster.

2. Heiratsregeln einiger Stämme

"Früher war es klar: Wenn der Vater Bäcker war, wurde die Tochter natürlich Schneiderin." Zitat eines 15jähriger Schülers aus "Professor Mammuts gesammelte Stilblüten".

Völker, die entweder als Jäger und Sammler oder von einer einfachen Landwirtschaft leben, müssen sich zwangsläufig ausbreiten, weil sie sich nur so ernähren können. Solcher Völker leben in Stämmen, die evtl. sehr groß sind. Man braucht nur an die vorkolumbischen Stämme Nordamerikas zu denken. In der Regel bestehen solche Stämme aus mehreren Tausend Leuten, wobei die Bevölkerungsdichte sehr gering ist (bei den Uraustraliern vor der Ankunft der Europäer etwa 0,04 Menschen pro Quadratkilometer - man vergleiche mit 240 Einw./qkm in Deutschland). Die Stämme leben in kleineren Gruppen, Sippen, die aus ein paar Hundert Menschen bestehen. Die Mitglieder eines Stammes verhalten sich in der Regel rücksichtsvoll gegeneinander und versuchen, Konflikte auf friedliche Weise zu lösen, was nicht immer gelingt. Da die Sippen oft über ein großes Gebiet vertreut sind, kann es passieren, dass verschiedene Sippen sich nicht als Mitglieder desselben Stammes fühlen. Es kommt tatsächlich vor, dass sich ein Stamm in zwei neue spaltet, nachdem er sein Gebiet übermäßig ausgedehnt hat. (Vielleicht sollte man dieses Verhalten mit dem von Cliquen vergleichen.) In solchen Fällen ist es nötig, den Zusammenhalt des Stammes durch gesellschaftliche Einrichtungen zu sichern. Denn bei ritualisierten Kämpfen können möglicherweise Aggressionen abgebaut werden, die sonst zu Stammesfehden geführt hätten. Eine andere Möglichkeit ist es, Geschenke auszutauschen. Das bekannteste Beispiel dafür ist der Potlatsch der Kwakiutl, wobei die Gegner versuchen, sich durch Großzügigkeit gegenseitig zu beschämen.

Eine weitere Sitte bei solchen Völkern ist die Exogamie. Mitglieder einer Sippe heiraten nicht untereinander; es würde als Inzest empfunden. Dadurch bleiben die verschiedenen Sippen miteinander verwandt. Um zu vermeiden, dass sich ein Stamm zufällig spaltet, weil die Mitglieder innerhalb kleinerer Gruppen von Sippen heiraten, haben sich Regeln entwickelt, die so etwas vermeiden. Anthropologen berichten, dass die alten Leute solche Regeln mit Diagrammen in Sand erklären und haben bemerkt, dass die Klarheit dieser Erklärungen, die ähnlicher Ausführungen von europäischen Professoren übertrifft. Die Diagramme machen es klar, dass es sich um eine Art Mathematik handelt. Leider haben die meisten Anthropologen keine Vorliebe für Mathematik; es wäre zu hoffen, dass man dadurch Einsicht in die kulturgeschichtliche Entwicklung der Mathematik gewinnen könnte. Der einzige, der sich mit diesem Aspekt auseinandergesetzt hat, ist Cl. Lévi-Strauss. Er versucht, den Inhalt von Sippen und Mythen durch ihre Struktur zu verstehen. Das Beispiel, dass hier diskutiert wird, stammt von einer Überarbeitung seiner Beschreibung des Murngin-Stammes in Australien. Die Übersetzung in mathematische Sprache hat A. Weil, einer der größten Mathematiker seiner Zeit und ein Freund von Lévi-Strauss, gemacht.

Das folgende wird aus

Cl. Lévi-Strauss: Les structures élémentaires de la parenté

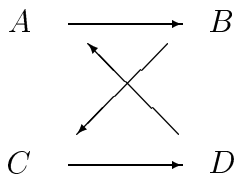
entnommen.

In diesem System wird jeder einer Klasse (hier wird das Wort Klasse in seinem mathematischen und nicht im soziologischen Sinn verwendet) zugeordnet. Es gibt dann Heiratstypen, ein Mann aus einer Klasse darf eine Frau aus einer bestimmten anderen Klasse heiraten.

Ein Heiratstyp ist eine dieser zugelassenen Verheiratungen.

Beispiel 1
Wir stellen uns vor, dass der Stamm aus vier Klassen besteht; diese seien A, B, C, D.

Dann bezeichnen wir einen möglichen Heiratstyp mit einem Pfeil, wobei $A \to B$ bedeutet: ein Mann aus A heiratet eine Frau aus B. Eine Möglichkeit wäre dann



Dann sind die Heiratstypen

$$(A, B), (B, C), (C, D), (D, A).$$

Wir bemerken, dass die verschiedenen Klassen durch die Heiratstypen ersetzt werden können. Somit gehört ein Mann aus Klasse A zum Heiratstyp (A, B) und eine Frau aus Klasse A zum Heiratstyp (D, A). Nun müssen aber auch die Kinder einem Heiratstyp zugeordnet werden.

Seien nun $M_1, M_2, \ldots, M_N$ die verschiedenen Heiratstypen. Zu jedem wir der Heiratstyp eines Sohnes, $s(M_j)$, oder einer Tochter, $t(M_j)$, zugeordnet. Soll eine Klasse nicht sofort aussterben, müssen s und t Permutationen von $\{M_1, \ldots, M_N\}$ sein. Deshalb können wir s, t als Element von Σ_N auffassen. Sei G die kleinste Untergruppe von Σ_N, die s und t enthält. Wir dürfen annehmen, dass diese Gruppe *transitiv* auf $M_1, \ldots, M_N$ (oder einfach auf $1, \ldots, N$) operiert; sonst würde sich der Stamm in "Bahnen" zerlegen und danach vermutlich in verschiedene Stämme aueinandergehen.

Folgende Regel kommt erstaunlicherweise vor:

Ein Mann darf die Tochter des Bruders seiner Mutter heiraten.

Symbolisch ausgedrückt sieht der Stammbaum dann so aus:

$$\begin{array}{ccccccc} & & & & \overbrace{\qquad\qquad\qquad\qquad} & & \\ ? & = & t(M) & & & s(M) & = & ? \\ & & \Big| & & & \Big| & & \\ & & st(M) & = & & ts(M) & & \end{array}$$

Deswegen erhalten wir, wenn wir "=" in die Mathematik übertragen

$$st = ts;$$

diese Regel bedeutet, dass die Gruppe aus Beispiel 1 auch *abelsch* ist.

Wir untersuchen jetzt, wie eine abelsche transitive Untergruppe von Σ_n auszusehen hat.

Dazu schreiben wir t als Produkt von Zyklen

$$t = C_1 C_2 \dots C_k.$$

Dann gilt

$$t = sts^{-1} = {}^sC_1 \cdot {}^sC_2 \cdot \dots \cdot {}^sC_k.$$

Deswegen sind ${}^sC_1$, ${}^sC_2, \dots$, ${}^sC_k$ Permutationen von $C_1, \dots, C_k$.

Sei nun $g \in G$. Wir können g in der Form schreiben

$$g = s^A t^B.$$

Dann gilt mit

$$\begin{aligned} gC_j g^{-1} &= s^A t^B C_j t^{-B} s^{-A} \\ &= s^A\, C_j \end{aligned}$$

weil die Potenzen von t mit jedem C_j vertauschbar sind und sich dadurch gegenseitig aufheben. Seien nun C_j, C_k zwei Zyklen, $C_j = (r_1, r_2, \dots), C_k = (q_1, q_2, \dots)$. Weil G transitiv operiert, gibt es ein $g \in G$, so dass gilt:

$$g(r_1) = q_1.$$

Da aber C_k dadurch charakterisiert ist, dass C_k der Zyklus von t ist, der q_1 enthält, folgt

$$gC_j g^{-1} = C_k,$$

oder auch mit $g = s^A t^B$

$$s^A C_j (s^A)^{-1} = C_k.$$

Deswegen sind alle C_j gleichen Typs (siehe Satz 3.6), haben also dieselbe Länge und es gilt, wenn wir die C_j passen ordnen:

$$\begin{aligned} sC_1 s^{-1} &= C_2 \\ sC_2 s^{-1} &= C_3 \\ &\vdots \\ sC_{k-1} s^{-1} &= C_k \\ sC_k s^{-1} &= C_1. \end{aligned}$$

Es folgt

$$s^k C_j (s^k)^{-1} = C_j.$$

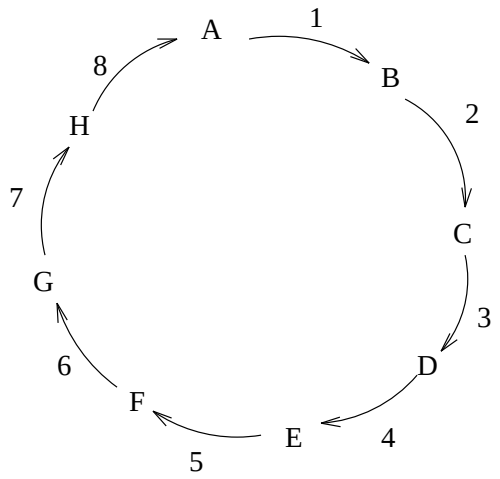
Dieses bedeutet aber nicht, dass s^k die Identität ist, sondern nur, dass es ein L gibt mit

$$s^k = t^L.$$

Als zweites Beispiel nehmen wir mit $N = 8$

$$\begin{aligned} s &= (1234)(5678) \\ t &= (1537)(2648). \end{aligned}$$

Das heißt, mit



folgt

$$\begin{array}{lllllll} s(AB) & = & (BC) & t(AB) & = & (EF) & \\ s(BC) & = & (CD) & t(EF) & = & (CD) & \\ s(CD) & = & (DE) & t(CD) & = & (GH) & \\ s(DE) & = & (AB) & t(GH) & = & (AB). & \text{u.s.w.} \end{array}$$

Dann gelten

$$\begin{aligned} st &= (1234)(5678)(1537)(2648) \\ &= (16)(27)(38)(45) \\ ts &= (1537)(2648)(1234)(5678) \\ &= (16)(27)(38)(45) \\ s^2 = t^2 &= (13)(57)(24)(68) \\ s^4 &= e. \end{aligned}$$

Die Gruppe G ist dann

$$\begin{aligned} & \{e, s, s^2, s^3, t, t^3, st, s^3 t\} \\ = \; & \{e, s, s^2, s^3, (st), s \cdot (st), s^2 \cdot (st), s^3 \cdot (st)\}, \end{aligned}$$

die wir als

$$C_4 \times C_2$$

erkennen.

In diesem Beispiel gilt:

$$s^2 = t^2,$$

oder
Ein Mann darf die Tochter der Schwester seines Vaters heiraten.

Als ein drittes Beispiel betrachten wir wieder eine Gesamtheit von 8 Klassen

$$A1, A2, B1, B2, C1, C2, D1, D2.$$

Alternierende Generationen heiraten nach den beiden Regeln

$$\begin{array}{cccc} A1 & \rightleftarrows & B1 & \qquad A1 \qquad\qquad B1 \\ & & & \qquad\quad \times \\ A2 & \rightleftarrows & B2 & \qquad A2 \qquad\qquad B2 \\ C1 & \rightleftarrows & D1 & \qquad C1 \qquad\qquad D1 \\ & & & \qquad\quad \times \\ C2 & \rightleftarrows & D2 & \qquad C2 \qquad\qquad D2 \quad ; \end{array}$$

d.h., wenn die Eltern nach der rechten Regel heiraten, heiraten die Kinder nach der linken und umgekehrt.

Es gibt dann 16 Heiratstypen (Mann, Frau),

$$\begin{array}{cc} (A1, B1)(B1, A1) & (A2, B2)(B2, A2) \\ (C1, D1)(D1, C1) & (C2, D2)(D2, C2) \end{array}$$

und

$$\begin{array}{cc} (A1, B2)(B2, A1) & (A2, B1)(B1, A2) \\ (C1, D2)(D2, C1) & (C2, D1)(D1, C2). \end{array}$$

Deise bezeichnen wir mit

$$\begin{array}{cccc} M_1 & M_2 & M_3 & M_4 \\ M_5 & M_6 & M_7 & M_8 \\ M_9 & M_{10} & M_{11} & M_{12} \\ M_{13} & M_{14} & M_{15} & M_{16}. \end{array}$$

Die Kinder gehören nun zu einer Klasse, die nur von der der Mutter abhängt und zwar nach der Regel

Klasse der Mutter:	$A1, A2, B1, B2, C1, C2, D1, D2$
Klasse des Kindes:	$C2, C1, D2, D1, A1, A2, B1, B2.$

Wir rechnen nun nach:

$$\begin{aligned} s &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 14 & 15 & 16 & 13 & 12 & 9 & 10 & 11 & 6 & 7 & 8 & 5 & 4 & 1 & 2 & 3 \end{pmatrix} \\ &= (1,14)(2,15)(3,16)(4,13)(5,12)(6,9)(7,10)(8,11) \end{aligned}$$

$$\begin{aligned} t &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 13 & 16 & 15 & 14 & 11 & 10 & 9 & 12 & 5 & 8 & 7 & 6 & 3 & 2 & 1 & 4 \end{pmatrix} \\ &= (1,13,3,15)(2,16,4,14)(5,11,7,9)(6,10,8,12). \end{aligned}$$

In diesem Fall genügen s und t den Gleichungen:

$$s^2 = e; sts^{-1} = t^{-1}, t^4 = 2.$$

Hier operiert G nicht transitiv aus $\{1, 2, \ldots, 16\}$. Die zwei Bahnen sind

$$\{1, 2, 3, 4, 13, 14, 15, 16\}$$

und

$$\{5, 6, 7, 8, 9, 10, 11, 12\}.$$

Die Gruppe selbst ist zu D_8 isomorph.

Die Interpretation dieser Heiratsregel ist etwas eigentümlich. Man bemerkt, dass jede Klasse in jeder Bahn vertreten ist. Durch die wechselnden Generationen kommt es aber zustande, dass dieser Stamm aus zwei untereinander heiratenden Gruppen besteht. Diese werden durch die Mitgliedschaft in den verschiedenen Heiratsklassen zusammengehalten. Diese Klassen haben verschiedene Bedeutungen für Eltern und Kinder, aber dieselbe für Großeltern und Enkel.

Übrigens, in diesem Beispiel gelten

$$\begin{aligned} s^2 &= e \\ t^2 &= (1,3)(13,15)(2,4)(14,16)(5,7)(11,9)(6,8)(10,12), \end{aligned}$$

so dass folgt

$$s^2(j) \neq t^2(j). \quad (\text{alle } j)$$

In dieser Gesellschaft darf ein Mann nicht die Tochter der Schwester seines Vaters heiraten; das wäre Inzest.

Dass Geschwister nicht heiraten dürfen, bedeutet

$$s(M) \neq t(M) \quad (\text{für alle } M);$$

diese Regel ist in allen oben erwähnten Beispielen gültig.

Kapitel 6

Quadriken, Geometrie und Gruppen

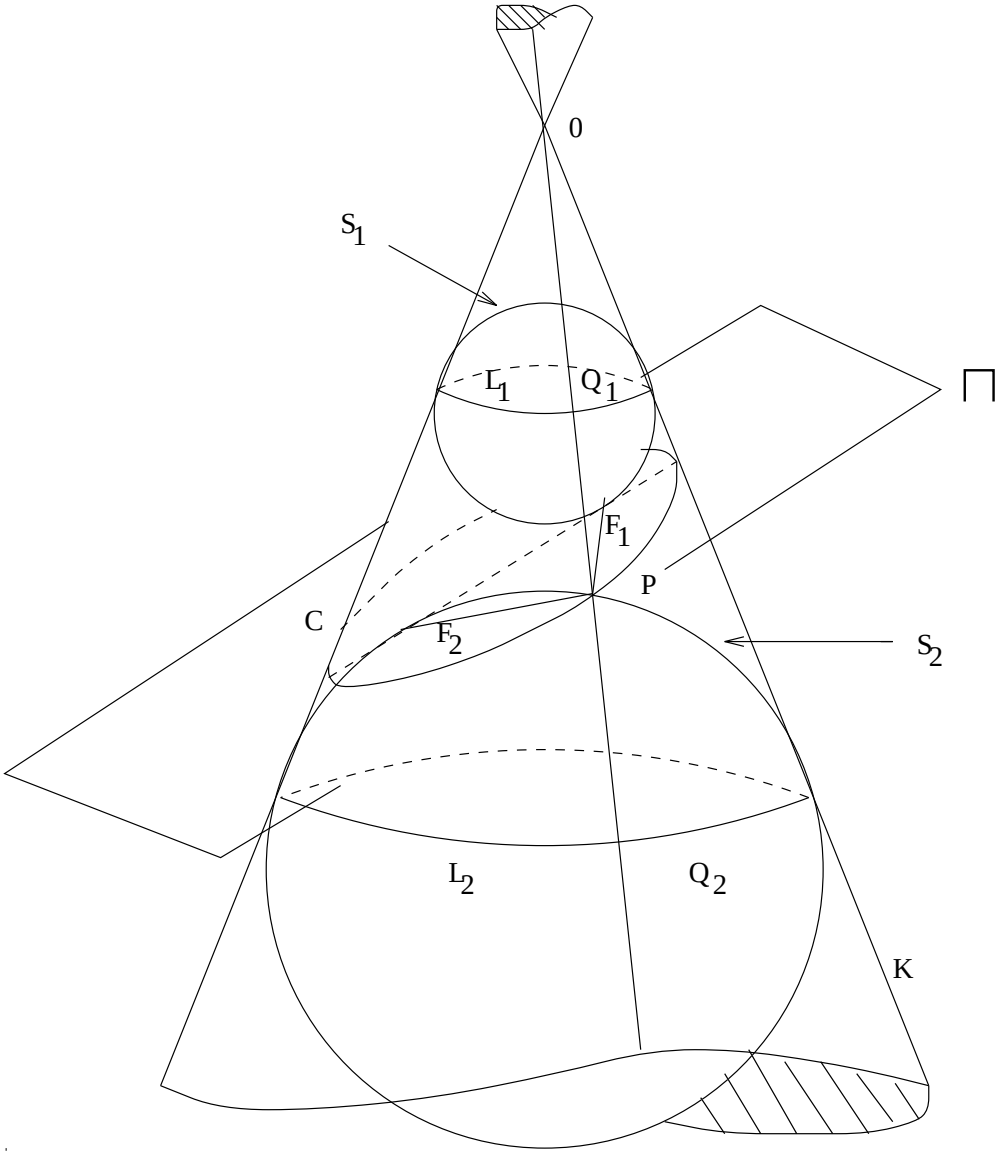
1. Die Sphären von Dandelin

Kegelschnitte heißen Kegelschnitte, weil sie Kegelschnitte sind. Um dieses zu verstehen, betrachten wir einen Kegel K und eine Ebene Π, die K dann schneiden muß. Sei C der Schnitt. Wir zeigen, dass C tatsächlich ein Kegelschnitt ist.

Der Beweis wird mittels einer schönen Konstruktion des Mathematikers Dandelin geführt. Es gibt zwei Sphären S_1, S_2, die gleichzeitig tangential zu K und Π sind (siehe Abbildung). Diese sind die Sphären von Apollonius. S_1 und S_2 berühren K entlang der Kreise L_1 und L_2. Auch S_1 (bzw. S_2) und Π berühren einander an einem Punkt F_1 (bzw. F_2). Sei O die Spitze des Kegels.

Die Sphären von Dandelin

Ellipse



Sei nun P ein Punkt auf C. Wir verbinden 0 und P und erhalten eine Strecke, deren Verlängerunge L_1 und L_2 schneidet. Seien Q_1 und Q_2 die Schnittpunkte.

Weil Q_1P und F_1P tangential zu S_1 sind, sind sie gleich lang:

$$Q_1P = F_1P.$$

Genauso erhalten wir

$$Q_2P = F_2P.$$

Es gilt aber

$$|Q_1P \pm Q_2P| = Q_1Q_2 = \text{const},$$

wobei + gewählt werden muß, falls P zwischen Q_1 und Q_2 liegt, $-$ sonst.

Daraus folgt

$$F_1P \pm F_2P = \text{const}.$$

Wie wir in Kapitel 6, 2 sehen werden, charakterisiert diese Gleichung einen Kegelschnitt im Sinne der analytischen Geometrie.

Bevor wir dieses nachweisen, sollten wir eine andere Folgerung notieren. Sei C ein Kegelschnitt -z.B. eine Ellipse. Sie P ein Punkt auf C und sei T_P die Gerade, die durch P geht und für welche die Winkel zwischen T_P und F_1P und zwischen T_P und F_2P gleich sind. Wir zeigen, dass T_P die Tangente zu C bei P ist.

Sei X ein anderer Punkt auf T_P. Dann gilt

$$F_1X + F_2X > F_1P + F_2P.$$

Zum Beweis betrachtet man die Spiegelung F_2' von F_2 an T_P. Dann liegen F_1, P, F_2' auf einer Geraden, F_1, X, F_2' nicht. Da eine Gerade die kürzeste Verbindung zwischen zwei Punkten ist, folgern wir

$$F_1X + F_2'X > F_1P + F_2'P.$$

Außerdem gilt wegen der Spiegelung

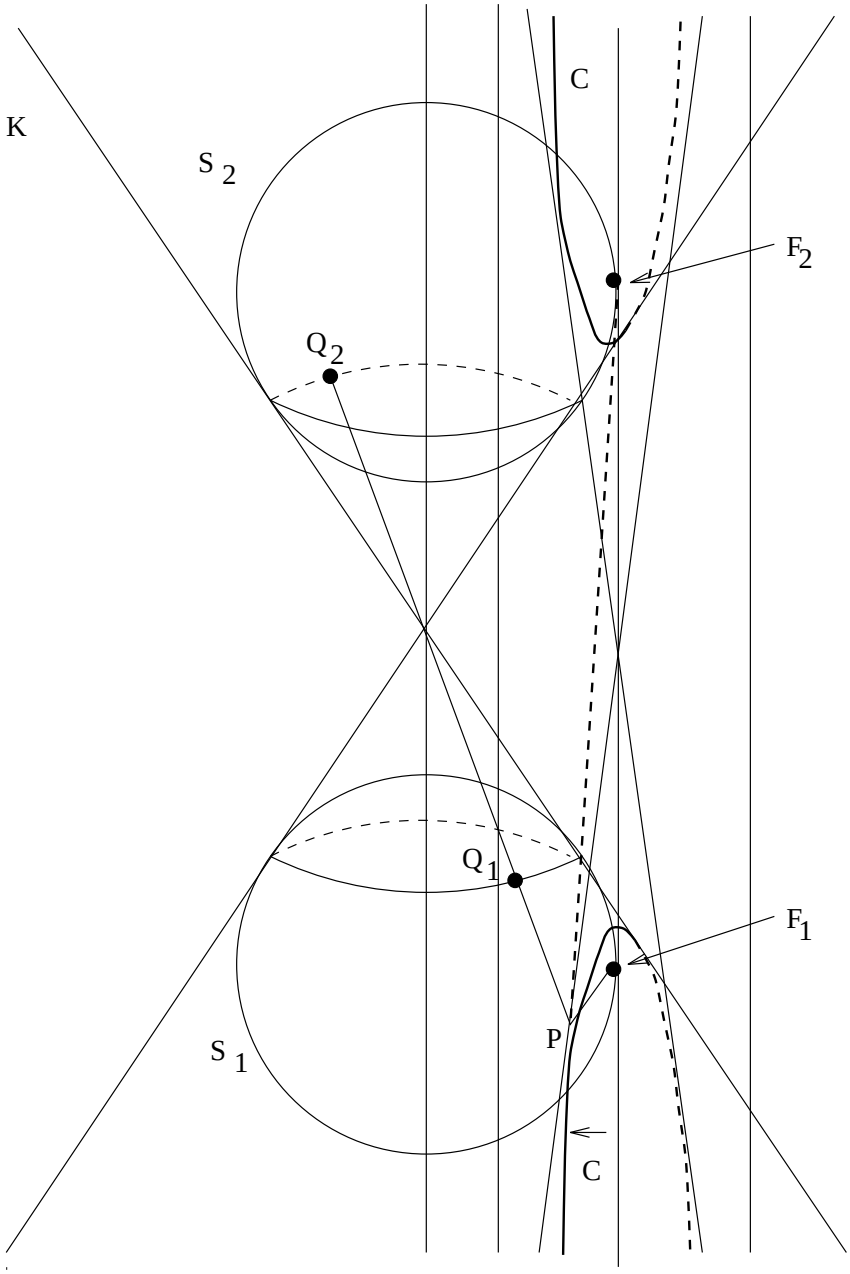
$$F_2'X = F_2X$$

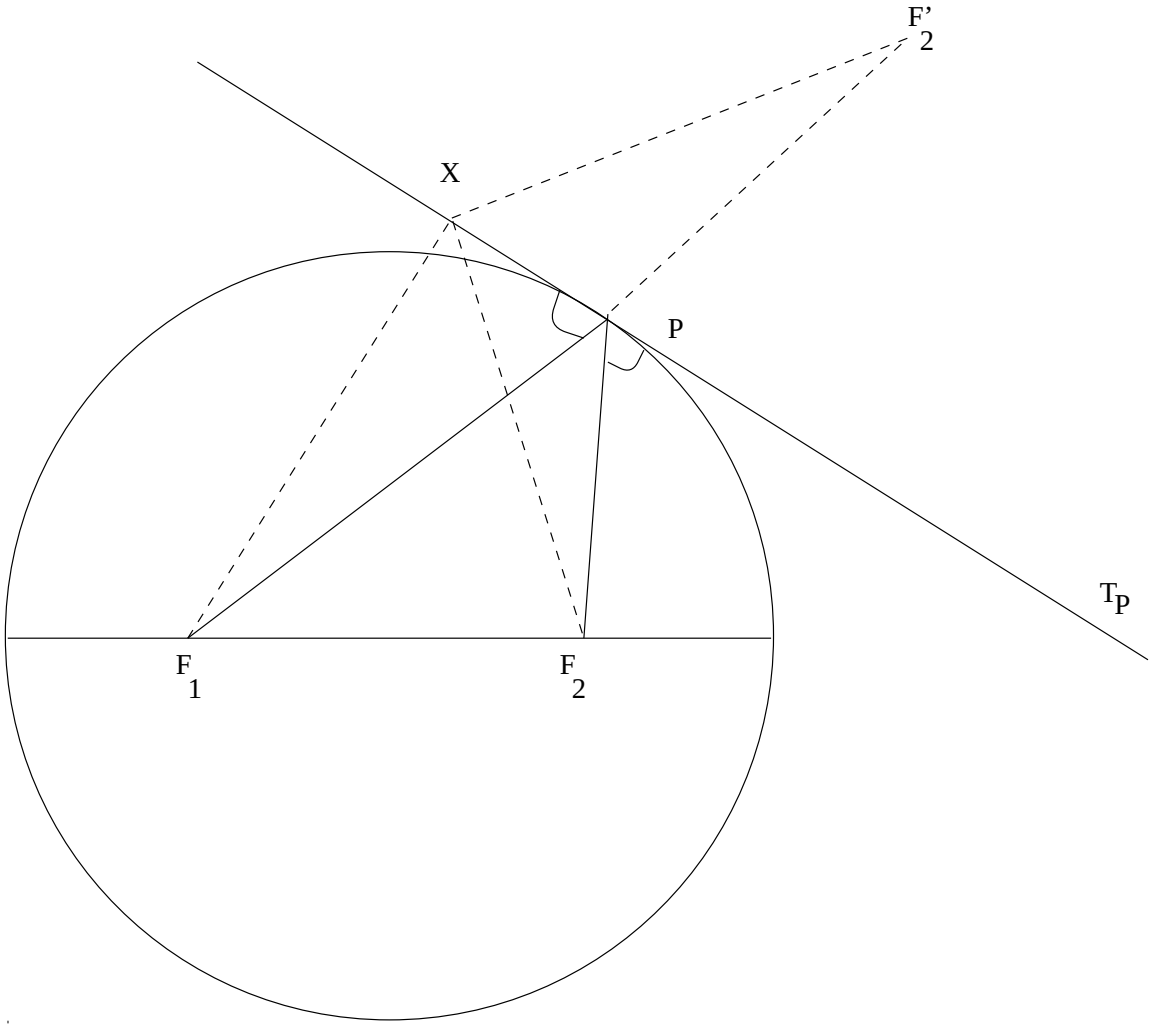
und

$$F_2P = F_2'P.$$

Damit ist die Behauptung bewiesen. Es folgt, dass X außerhalb von C liegt.

Die Sphären von Dandelin
Hyperbel




F’
2
X
P
T
P
F
1
F
2

Anders formuliert: T_P ist die Tangentialgerade zu C bei P. Diese Gerade ist gerade dadurch charakterisiert, dass

$$\sphericalangle(T_P, F_1P) = \sphericalangle(T_P, F_2P).$$

Diese Tatsache kann wie folgt interpretiert werden. Wir stellen uns vor, dass wir eine Kerze bei F_1 aufgestellt haben. Dann werden alle Lichtstrahlen an der Kurve C zum Punkt F_2 reflektiert.

Aus diesem Grund heißen F_1 und F_2 die *Brennpunkte* von C. (In anderen Sprachen Focus (Mehrzahl: Foci) nach dem lateinischen focus = Herd). Der Name "Focus" stammt von J. Kepler.

Um die analytische Beschreibung von C zu bestimmen, verwenden wir Polarkoordianten. Sei F_1 das Zentrum und F_1F_2 die Grundrichtung.

Seien

$$\begin{aligned} d &= F_1F_2 \\ e &= F_1P + F_2P. \end{aligned}$$

Sei $r = F_1P$ und θ der Winkel zwischen F_1F_2 und F_1P.

Nach der Kosinusregel erhalten wir

$$F_2P^2 = F_1P^2 + F_1F_2^2 - 2F_1P\,F_1F_2 \cdot \cos\theta$$

oder

$$(l-r)^2 = r^2 + d^2 - 2rd\cos\theta.$$

Diese Gleichung läßt sich vereinfachen; und wir erhalten die Gleichung für eine Ellipse mit

$$\left(l^2 - d^2\right) = 2(l - d\cos\theta)r.$$

Nun schreiben wir dieses als

$$\frac{l^2 - d^2}{2} + d \cdot r \cdot \cos\theta = l \cdot r.$$

Diese ist die Gleichung einer Ellipse in Polarkoordinaten. Diese quadrieren wir und führen kartesische Koordinaten

$$\begin{aligned} X &= r\cos\theta \\ Y &= r\sin\theta \end{aligned}$$

ein. Es folgt

$$\left(\frac{l^2 - d^2}{2} + d \cdot X\right)^2 = l^2\left(X^2 - Y^2\right).$$

Diese kann zunächst ausmultipliziert werden; etwas umgeformt sieht die Gleichung dann so aus:

$$\left(l^2 - d^2\right)X^2 - d\left(l^2 - d^2\right)X + l^2Y^2 = \left(\frac{l^2 - d^2}{2}\right)^2.$$

Wenn wir nun das Quadrat vervollständigen, erhalten wir

$$\begin{aligned}\left(l^2-d^2\right)\left(X-\frac{d}{2}\right)^2+l^2Y^2 &= \left(\frac{l^2-d^2}{2}\right)^2+\frac{\left(l^2-d^2\right)d^2}{4}\\ &= l^2\left(l^2-d^2\right)/4.\end{aligned}$$

Diese Gleichung entspricht der Ellipse in kartesischen Koordinaten. Setzt man $X_1 = X - \frac{d}{2}$ und $Y_1 = Y$, entspricht das der Transformation des Ursprungs von F_1 zum Mittelpunkt von F_1F_2. Die längere Hauptachse hat Länge 1, die kürzere $\sqrt{l^2-d^2}$. Diese folgen von der obigen Gleichung, denn setzt man $Y = 0$, dann folgt

$$\left(X-\frac{d}{2}\right) = \sqrt{l^2/4}.$$

Deshalb sind die Endpunkte der längeren Achse

$$\left(\frac{d}{2}\pm\frac{l}{2},0\right);$$

der Abstand zwischen diesen Punkten ist l. Ähnlich bestimmt man die Länge der kürzeren Achse, indem man $X = \frac{d}{2}$ setzt.

Eine letzte Bemerkung zur Formel

$$F_1P + F_2P = \text{const.}$$

Diese kann verwendet werden, um Ellipsen zu zeichnen. Man wählt zwei Punkte (F_1, F_2) und verbindet sie mit einer Schnur, die länger als F_1F_2 ist. Dann nimmt man einen Stift, drückt ihn gegen den Faden und bewegt ihn so, dass der Faden straff bleibt. Der Stift beschreibt dann eine Ellipse.

2. Quadriken und Projektive Geometrie

Sei $P(x_1, x_2)$ eine Funktion folgender Gestalt

$$P(x_1, x_2) = A_{11}x_1^2 + 2A_{12}x_1x_2 + A_{22}x_2^2 + 2A_{01}x_1 + 2A_{02}x_2 + A_{00}.$$

Eine solche Funktion heißt eine Funktion *zweiter Ordnung*. Es ist angebracht, diese Funktion etwas anders zu schreiben.

Sei

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{01} \\ A_{12} & A_{22} & A_{02} \\ A_{01} & A_{02} & A_{00} \end{pmatrix};$$

also eine symmetrische Matrix aus $M(3 \times 3; \mathbb{R})$.

Sei

$$\underline{\tilde{x}} = \begin{pmatrix} x_1 \\ x_1 \\ 1 \end{pmatrix}.$$

Sei

$$\underline{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Dann ist

$$P(\underline{x}) = {}^t\tilde{x}A\underline{\tilde{x}}.$$

Auf diese Weise fassen wir die Ebene $\{(x_1x_2) : x_1, x_2 \in \mathbb{R}\}$ als die Ebene $\Pi_0 = \{(x_1, x_2, 1) | (x_1, x_2) \in \mathbb{R}^2\}$ in $\mathbb{R}^3$ auf.

Die zu A (oder P) gehörende Quadrik Q_A ist die Menge

$$\{\underline{x} \in \mathbb{R}^2 : P(\underline{x}) = 0\}.$$

Sei

$$Q_A^0 = \{\underline{y} \in \mathbb{R}^3 :^t \underline{y}A\underline{y} = 0\}.$$

Dann kann man Q_A als den Schnitt von Q_A^0 und Π_0 auffassen.

Diese Konstruktion kann leicht in zwei Richtungen verallgemeinert werden. Es ist nämlich möglich, $\mathbb{R}$ durch andere Körper zu ersetzen oder die Dimensionszahl zu erhöhen. Für uns aber wird der obige Fall genug Inhalt haben.

Wir wissen, dass es eine nicht-singuläre Matrix S gibt, so dass ${}^tSAS$ diagonal ist. Es wäre sogar möglich, $S \in O_3$ zu wählen (Hauptachsensatz); diese Annahme ist im Augenblick nicht nötig. Was wir nun haben, ist

$$B = {}^tSAS = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}.$$

Wir definieren Q_B^0 wie oben. Dann haben wir für $u \in Q_B^0$

$$ {}^t u {}^t S A S u = 0. $$

Es folgt

$$ {}^t(Su) A (Su) = 0 $$

oder

$$ Su \in Q_A^0. $$

Da auch die Umkehrung richtig ist, können wir schreiben

$$ Q_A^0 = S\big(Q_B^0\big). $$

Weil Q_A als $Q_A^0 \cap \Pi_0$ definiert wurde, gilt

$$ Q_A = S\big(Q_B^0 \cap S^{-1}\Pi_0\big). $$

Hier ist $S^{-1}\Pi_0$ eine nicht durch den Ursprung laufende Ebene.

Wir brauchen jetzt ein algebraisches Hilfsmittel. Wir erinnern uns daran, dass wir die euklidische Gruppe $\mathbb{E}$ mit der Untergruppe von $GL_3(\mathbb{R})$

$$ \left\{ \begin{array}{cc} & \begin{array}{cc} 2 & 1 \end{array} \\ 2 & \begin{pmatrix} A & y \\ 0 & 1 \end{pmatrix} \\ 1 & \end{array} \;\middle|\; A \in 0_2(\mathbb{R}), y \in \mathbb{R}^2 \right\} $$

identifiziert hatten. Diese Gruppe schickt Π_0 in sich selbst. Wir schreiben fortan $\mathbb{E}$ für diese Untergruppe von $GL_3(\mathbb{R})$.

Satz 6.1. *Sei $A \in M(3\times 3;\mathbb{R})$ eine symmetrische Matrix. Es gibt ein $S \in \mathbb{E}$, so dass ${}^t SAS$ entweder von der Form*

$$ \begin{pmatrix} a & 0 & 0 \\ 0 & a' & 0 \\ 0 & 0 & a'' \end{pmatrix} \quad \textit{oder} \quad \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & b & 0 \end{pmatrix} \quad (b \neq 0) $$

ist.

Beweis. Wir betrachten die Untermatrix $\begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{22} \end{pmatrix}$ von A. Nach dem Hauptachsensatz gibt es ein $R \in 0_2(\mathbb{R})$, so dass gilt

$$ {}^t R \begin{pmatrix} A_{11} & A_{12} \\ A_{12} & A_{22} \end{pmatrix} R = \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix}. $$

Es könnte sein, dass a oder a' Null ist. Wenn $A' \neq 0$ ist, dürfen wir aber annehmen, dass auch $A \neq 0$ richtig ist. Wir wenden dann $\begin{pmatrix} R & 0 \\ 0 & 1 \end{pmatrix}$ auf A an und erhalten

$$ A' = \begin{pmatrix} a & 0 & * \\ 0 & a' & * \\ * & * & * \end{pmatrix} $$

wobei die Sternchen unbekannte sind. Wir unterscheiden drei Fälle:

(i) $a \neq 0, a' \neq 0$. Wir schreiben A' in $(2+1) \times (2+1)$ Blockform

$$A' = \begin{pmatrix} A'_{11} & A'_{12} \\ {}^tA'_{12} & A'_{22} \end{pmatrix},$$

wobei $A'_{11} = \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix}$, A'_{12} ein Spaltenvektor und $A'_{22} \in \mathbb{R}$ ist. Es gilt

$${}^t\begin{pmatrix} E & \underline{x} \\ 0 & 1 \end{pmatrix} A' \begin{pmatrix} E & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A'_{11} & (A'_{11}x + A'_{12}) \\ {}^tA'_{11}\underline{x} + A'_{12} & * \end{pmatrix}.$$

Wir wählen

$$x = -{A'_{11}}^{-1} A'_{12}$$

(möglich, weil A'_{11} nicht singulär ist). Dann ist diese Matrix von der Form

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a' & 0 \\ 0 & 0 & * \end{pmatrix},$$

wie behauptet.

(ii) $a \neq 0, a' = 0$. Wie im Fall (i) mit einem geeigneten $\underline{x} \left(= \begin{pmatrix} -u/a \\ 0 \end{pmatrix}, \text{falls } A'_{12} = \begin{pmatrix} u \\ 0 \end{pmatrix} \text{ist} \right)$ kann man die Matrix auf die Form bringen

$$\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & b & c \end{pmatrix}$$

bringen. Wir dürfen annehmen, dass $b \neq 0$ gilt, weil die Matrix sonst schon in gewünschter Gestalt wäre. Es gilt aber mit beliebigem y:

$${}^t\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & b & c \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & b & c + 2by \end{pmatrix}$$

Wir wählen

$$y = -c/2b$$

und haben eine Matrix in der gewünschten Form.

(iii) $a = 0, a' = 0$. Wir wählen ein $R \in \mathcal{O}_2(\mathbb{R})$, so dass gilt

$${}^tR\, A'_{12} = \begin{pmatrix} 0 \\ u \end{pmatrix},$$

d.h. A'_{12} wird durch ${}^tR$ senkrecht zur x-Achse gedreht.
Dann gilt:

$${}^t\begin{pmatrix} R & 0 \\ 0 & 1 \end{pmatrix} \cdot A' \cdot \begin{pmatrix} R & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & u \\ 0 & u & e \end{pmatrix}$$

für irgendwelches c. Nun können wir vorgehen, wie wir es in Fall (ii) gemacht haben und erhalten die gewünschte Form.

Damit ist der Satz bewiesen.

Die Bedeutung dieses Satzes liegt darin, dass wir jede Quadrik durch eine geeignete euklidische Transformation auf eine der Normalformen

$$ax_1^2 + a'x_2^2 + a'' = 0$$

oder

$$ax_1^2 + 2bx_2 = 0 \quad (b \neq 0)$$

bringen können.

Wir erkennen diese als die üblichen Kegelschnitte. Wir sollten jetzt die geometrischen Gebilde aufzählen, die entstehen, wenn die Vorzeichen irgendwie gewählt werden oder einige Koeffizienten Null sind. Wir nehmen an, dass A nicht 0 ist. Von der ersten Gleichung erhalten wir:

1. eine Ellipse: falls $a > 0, a' > 0, a'' < 0$ oder $a < 0, a' < 0, a'' > 0$
2. eine Hyperbel: falls $aa' < 0, a'' \neq 0$
3. $\emptyset$ falls $a > 0, a' > 0, a'' > 0$ oder $a < 0, a' < 0, a'' < 0$ $a = 0, aa'' > 0$ $a' = 0, aa'' > 0$
4. zwei Geraden: falls $a'' = 0, aa' < 0$
5. eine Gerade: falls $a' = 0, a'' = 0; a = 0', a'' = 0$
6. zwei parallele Geraden: falls $a = 0, a'a'' < 0; a' = 0, aa'' < 0$
7. einen Punkt: falls $a'' = 0, aa' > 0$.

Von der zweiten Gleichung erhalten wir

8. eine Parable: falls $a \neq 0$
9. eine Gerade: falls $a = 0$.

Wir betrachten den 3., 4., 5., 6., 7. und 9. Fall als entartet.

Sei P eine Funktion zweiter Ordnung und $S \in GL_2(\mathbb{R})$. Dann ist

$$x \longmapsto P(S\underline{x})$$

auch eine Funktion zweiter Ordnung. Wenn Q_A die zu P entsprechende Quadrik ist, ist $S^{-1}Q_A$ die zu dieser neuen Funktion entsprechende Quadrik. Deswegen bleibt die Gesamtheit aller Quadriken oder Kegelschnitte unter der Gruppe aller linearen Transformationen erhalten.

Jetzt wird es angebracht sein, anzunehmen, dass A nicht ausgeartet ist.

Wir werden jetzt sehen, dass die Menge aller Quadriken unter der Gruppe aller projektiven Transformationen erhalten bleibt.

Wir erinnern uns daran, dass in der projektiven Geometrie die "Punkte" die durch 0 laufenden Geraden waren, mindestens in einem der Modelle. Ein zweites Modell erhielten wir, indem sich eine nicht durch O laufende Ebene Π mit

einer durch 0 laufenden Gerade schnitt und wir diesen Schnittpunkt der Gerade zuordneten.

Dieses ist aber genau das Verfahren von Kapitel 6, 1.

Ein Kegel ist eine Vereinigung von durch O laufende Geraden, also in der projektiven Geometrie eine Vereinigung von Punkten. Diese haben wir auf eine Ebene Π "projeziert". Wir dürfen dann einen Kegel als "Kegelschnitt" oder "Quadrik" in der projektiven Geometrie auffassen.

Ähnlich betrachten wir Q_A^0. Sei $y \in Q_A^0$; dann gilt ${}^t yAy = 0$. Sei $\lambda \in \mathbb{R}^\times$, wegen

$$ {}^t(\lambda y)A(\lambda y) = \lambda^2 \cdot ({}^t yAy) $$

folgt, dass $\lambda y \in Q_A^0$ dann und nur dann gilt, wenn $y \in Q_A^0$ gilt. Dies ist auch eine Vereinigung von durch 0 laufenden Geraden. Auch war Q_A die "Projektion" auf Π_0.

Auf diese Weise können wir Q_A^0 als ein Objekt in der projektiven Geometrie interpretieren.

Wir sahen, dass $GL_3(\mathbb{R})$ auf der projektiven Geometrie wirkte. Sei $S \in GL_3(\mathbb{R})$; dann

$$ \begin{aligned} S\left(Q_A^0\right) &= \{Sy = {}^t yAy = 0\} \\ &= \{y' : {}^t\left(s^{-1}y'\right)A\left(s^{-1}y'\right) = 0\} \\ &= \{y' : {}^t y' \cdot {}^t S^{-1}AS^{-1} \cdot y' = 0\} \\ &= Q_B^0 \end{aligned} $$

mit

$$ B = {}^t S^{-1}AS^{-1}. $$

Wir hatten angenommen, dass A nicht entartet war. Deswegen gibt es ein S, so dass

$$ B = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}. $$

Wären alle $d_j > 0$ oder alle $d_j < 0$, würde folgen, dass $Q_B^0 = \{0\}$ gilt. Deshalb sind zwei d_j's positiv und eines negativ oder umgekehrt. Dann gilt

$$ Q_{-B}^0 = Q_B^0, $$

dürfen wir annehmen, dass zwei d_j's positiv sind; ohne Beschränkung der Allgemeinheit seien $d_1, d_2 > 0, d_3 < 0$. Wenn wir statt S

$$ \begin{pmatrix} \sqrt{d_1} & 0 & 0 \\ 0 & \sqrt{d_2} & 0 \\ 0 & 0 & \sqrt{|d_3|} \end{pmatrix} \cdot S $$

anwenden, erhalten wir

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

Wir schreiben nun

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

Wir haben jetzt gezeigt, dass alle Quadriken von der Form $S\left(Q_H^0\right)$ sind, $S \in GL_1(\mathbb{R})$.

In der projektiven Geometrie gibt es dann sozusagen nur einen Kegelschnitt; dadurch wird die Theorie viel leichter.

Man kann sagen, dass

1. eine Ellipse ein Kegelschnitt ist, der die imaginäre Gerade J nicht schneidet,
   (Ebene nicht parallel zu einer Geraden aus der Geradenschar durch 0)
2. eine Parabel ein Kegelschnitt ist, der die imaginäre Gerade J berührt,
   (Ebene parallel zu einer Geraden des Kegels)
3. eine Hyperbel ein Kegelschnitt ist, der die imaginäre Gerade J in zwei Punkte schneidet; diese zwei Punkte stellen die Richtungen der beiden Asymptoten dar.
   (Ebene parallel zu 2 Geraden des Kegels)

Zuletzt identifizieren wir Q_H^0. Dies ist

$$\left\{\left(x_1, x_2, x_3\right) | x_1^2 + x_2^2 - x_3^2 = 0\right\}.$$

Der Schnitt davon mit der Ebene $x_3 = z$ ist ein Kreis, dessen Radius $|z|$ ist. Das sieht man, wenn man die Gleichung in der Form

$$x_1^2 + x_2^2 = z^2$$

schreibt. Anders formuliert ist dieses Gebilde ein Kegel.

3. Der Satz von Pascal

Der Satz von Pascal ist eine Satz aus der projektiven Geometrie über Quadriken. Er wurde von Pascal ca. 1640 entdeckt, obwohl er den griechischen Mathematikern zugänglich gewesen wäre. Pascal hat die Konstruktion das "hexagramme mystique" genannt.

Die Aussage ist:

Satz 6.2. *Sei Q eine Quadrik. Seien $A_1, \ldots, A_6$ auf Q die Ecken eines Sechsecks. Sei*

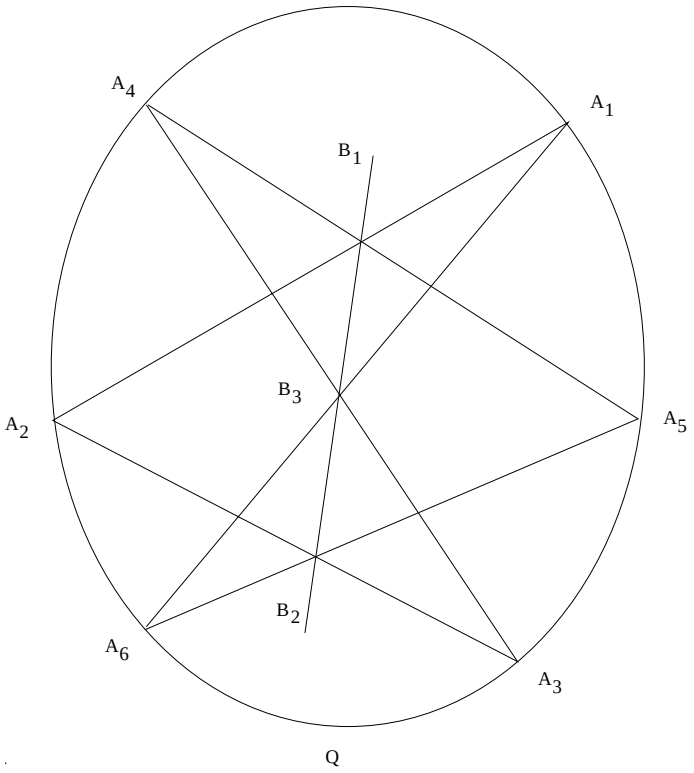
B_1 *der Schnittpunkt von* A_1A_2 *und* A_4A_5
B_2 *der Schnittpunkt von* A_2A_3 *und* A_5A_6
B_3 *der Schnittpunkt von* A_3A_4 *und* A_6A_1.

Dann liegen B_1, B_2, B_3 auf einer Gerade.

Wir werden hier den Satz im Falle einer nicht ausgearteten Quadrik beweisen. Der Satz gilt auch, wenn Q eine Vereinigung von zwei Geraden ist; diese Aussage ar den Griechen bekannt und heißt der Satz von Pappos. Er kann mit ähnlichen Mittel bewiesen werden.

In diesem Fall ist der Dualsatz wesentlich verschieden vom ursprünglichen. Er wurde ca. 1815 vom Gründer der Dualitätslehre Brianchon entdeckt. Sogar der Dualsatz des Pappos'schen Satzes wurde von Brianchon gefunden; das war 1500 Jahre nach Pappos. Hier schaffte man wirklich neue Erkenntnisse mit der Dualitätslehre.

Satz von Pascal



Beweis. Der Satz ist aus der projektiven Geometrie. Wir dürfen deshalb projektive Transformationen anwenden. Wir tun es so: die Gerade A_1A_2 soll die imaginäre Gerade J sein (siehe Zeichnung); dann wird Q eine Hyperbel. Wir wählen als Achsen die Symptoten von Q. Wir können dann annehmen, dass Q die Hyperbel

$$x_1x_2 = 1$$

ist. Wir nehmen an, dass A_1 (bzw. A_2) in der Richtung der 1-Achse (2-Achse) ist.

Seien

$$\begin{aligned} A_3 &= (s, s^{-1}) \\ A_4 &= (t, t^{-1}) \\ A_5 &= (u, u^{-1}) \\ A_6 &= (v, v^{-1}). \end{aligned}$$

Dann ist B_1 der Punkt auf J, der durch die Richtung von A_4A_5 bestimmt ist. Das heißt, wir müssen zeigen, dass A_4A_5 und B_2B_3 parallel sind (denn zwei parallele Geraden schneiden J im gleichen Punkt).

Nun ist B_2 der Schnitt von der durch A_3 laufenden Gerade, die parallel zur 2-Achse ist und der Gerade A_5A_6. Die Steigung der Geraden A_5A_6 ist aber

$$\frac{x_2 - u^{-1}}{x_1 - u} = \frac{v^{-1} - u^{-1}}{v - u} = -\frac{1}{vu}.$$

Die durch A_3 laufende Gerade ist durch $x_1 = s$ charakterisiert. Deswegen ist

$$B_2 = \left(s, u^{-1} - \frac{s-u}{uv}\right) = \left(s, u^{-1} + v^{-1} - s/uv\right).$$

B_3 ist der Schnitt von der durch A_6 laufenden Gerade, die parallel zur 1-Achse ist und der Geraden A_3A_4. Die Steigung ist

$$\frac{x_2 - s^-1}{x_1 - s} = -\frac{1}{st};$$

die durch A_6 laufende Gerade wird durch $x_2 = v^{-1}$ beschrieben. Wir erhalten für B_3

$$B_3 = \left(s - t - \frac{st}{v}, v^{-1}\right).$$

Die Steigung von B_2B_3 ist daher

$$\frac{\left(u^-1 + v^{-1} - s/uv\right) - \left(v^{-1}\right)}{s - (s + t - st/v)} = \frac{v^{-1}u^{-1}(v-s)}{tv^{-1}(s-v)}.$$

Man bemerke, dass Zähler und Nenner nicht Null sind. Dieser Ausdruck läßt sich zu

$$-\frac{u^{-1}}{t} = -\frac{1}{ut}$$

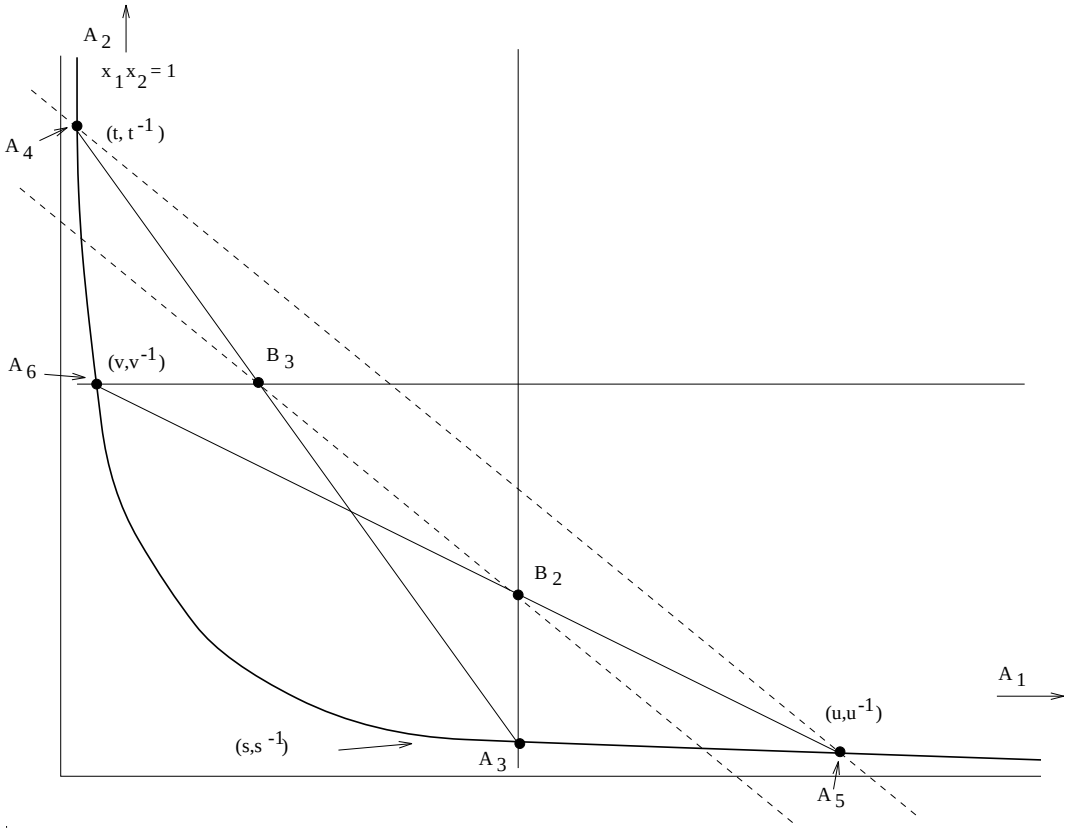
vereinfachen.

Die Steigung von A_4A_5 ist

$$\frac{t^{-1} - u^{-1}}{t - u} = \frac{1}{tu}.$$

Aus der Gleichheit der beiden Steigungen folgt, dass A_4A_5 und B_2B_3 parallel sind. Damit ist der Satz bewiesen.

Durch diesen Satz wird es möglich, Quadriken in der projektiven Geometrie zu definieren.



Wir werden zeigen:

1. Seien $P_1, \ldots, P_5$ fünf Punkte in der projektiven Ebene. Dann gibt es eine Quadrik Q, so dass $P_1, \ldots, P_5$ auf Q liegen.

2. Liegen keine drei Punkte $P_1, \ldots, P_5$ auf einer Geraden, so ist Q nicht ausgeartet und eindeutig bestimmt.

3. Sind $P_1, \ldots, P_5$ wie in 2., kann Q so konstruiert werden:
Verbinde P_1P_2 und P_3P_4; sei R der Schnittpunkt. Sei L eine beliebige, durch R laufende Gerade.

Sei A_L der Schnittpunkt von L und P_3P_5.
Sei B_L der Schnittpunkt von L und P_1P_5.
Sei M_L der Schnittpunkt von P_4B_L und P_2A_L.

Dann liegt M_L auf Q und jeder Punkt M auf Q (außer P_1, P_2, P_3, P_4, P_5) kann als ein M_L für geeignetes L konstruiert werden.

Diese Konstruktion ist nicht ohne Bedeutung für die Bestimmung von Kometenbahnen in der Astronomie.

Zu 1.: Wir nehmen an, dass P_j durch $\underline{x}_j \neq 0$ dargestellt wird. Dass $x_1, \ldots, x_5$ auf Q_A^0 liegen, ist gleichbedeutend damit, dass gilt

$$ {}^t\underline{x}_j A \underline{x}_j = 0. $$

Diese bilden fünf lineare Gleichungen in den sechs Veränderlichen $(A_{11}, A_{22}, A_{33}, A_{12}, A_{23}, A_{31})$. Da $6 > 5$ gilt, gibt es eine Lösung und damit eine geeignete Matrix A.

Zu 2.: Wäre Q ausgeartet, würde sie aus höchstens zwei Geraden bestehen. Auf einer davon müssen dann mindestens drei Punkte sein. Es wurde aber vorausgesetzt, dass keine drei Punkte auf einer Geraden liegen. Deshalb kann Q nicht ausgeartet sein. Außerdem folgt aus 2.: $P_1, \ldots, P_5$ sind verschieden.

Um zu beweisen, dass Q eindeutig bestimmt ist, genügt es zu zeigen, dass zwei verschiedene nicht ausgeartete Quadriken Q, Q' sich in höchstens vier Punkten schneiden.

Es seien A_1, A_2 zwei solche Schnittpunkte. Wir machen A_1A_2 zur imaginären Gerade J. Wie im Beweis des Pascalschen Satzes können wir annehmen, dass Q die Form $x_1x_2 = 1$ annimmt. Da Q' parallele Asymptoten zu denen von Q hat, muß die Gleichung für Q'

$$ \big(x_1 - a\big)\big(x_2 - b\big) = c $$

sein. Diese zwei Gleichungen haben entweder keine oder zwei gemeinsame Lösungen.

Zu 3.: Liegt M auf Q, ist $P_1P_2MP_4P_3P_5$ ein Sechseck, wie im Pascalschen Satz. Deshalb entsteht nach diesem Satz jedes M als ein M_L. Wir müssen noch zeigen, dass keine zusätzlichen Punkte außerhalb von C vorkommen können.

Anders ausgedrückt heißt das, wir zeigen, dass jedes L (außer P_1P_2 oder P_3P_4) vorkommen darf.

Dafür wählen wir eine ebenes Modell der projektiven Geometrie so, dass der Schnitt von P_1P_2 und P_3P_5 auf J liegt. Die möglichen L's, außer P_1P_2 bzw. P_3P_4 werden durch A_L charakterisiert. Sei $A = A_L$; wir wissen, dass die Gerade P_2A die Quadrik in zwei Punkten schniedet oder tangential zu Q ist (projektiv gesehen, müssen wir diese Aussage nur für einen Kreis beweisen; das entspricht der Aussage: eine Gerade schneidet einen Kreis in $0, 1$ oder 2 Punkten; falls sie ihn in einem Punkt schneidet, ist sie tangential).
Sei N der zweite Schnittpunkt (oder P_2, falls P_2A zu Q tangential ist). Sei B der Schnittpunkt von P_4N und P_1P_5. Nach dem Pascalschen Satz liegt B auf L; B ist deswegen B_L.

Damit haben wir für jede Gerade L einen Punkt N auf Q zugeordnet, so dass gilt

$$M_L = N.$$

Damit ist die dritte Behauptung bewiesen.

4. Orthogonale Gruppen

Sei V ein Vektorraum und $Q : V \to \mathbb{R}$ eine nicht ausgeartete quadratische Form. Ebenso schreiben wir Q für die bilineare Form

$$Q : V \times V \to \mathbb{R},$$

die von Q hergeleitet wurde. Das einfachste Beispiel dafür, nämlich die euklidische Form, erhalten wir mit

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2.$$

Dann ist $Q(x,x) = \| x \|^2 = \langle x, x \rangle$, denn

$$Q(x) = {}^t x E_2 x = x_1^2 + x_2^2.$$

Es ist allgemein

$$\begin{aligned} Q(x,x) &= Q(x) \\ Q(x,y) &= \frac{1}{2}\Big(Q(x+y) - Q(x) - Q(y)\Big). \end{aligned}$$

Definition. Die orthogonale Gruppe $O(V,Q)$ ist die Gruppe aller linearen Abbildungen

$$a : V \to V,$$

so dass gilt

$$Q\Big(a(x)\Big) = Q(x).$$

Diese ist eine Untergruppe von $GL(V)$, denn:

1. wenn a, b in $O(V,Q)$ sind, fann folgt

$$Q\left(a\Big(b(x)\Big)\right) = Q\Big(b(x)\Big) = Q(x);$$

   deshalb ist auch ab in $O(V,Q)$.
2. wenn a in $O(V,Q)$ ist, folgt

$$Q(x) = Q\Big(a \cdot a^{-1}(x)\Big) = Q\Big(a^{-1}(x)\Big);$$

   deshalb liegt auch a^{-1} in $O(V,Q)$.

Man bemerke:

$$\begin{aligned} Q\Big(a(x), a(y)\Big) &= \frac{1}{2}\left(Q\Big(a(x+y)\Big) - Q\Big(a(x)\Big) - Q\Big(a(y)\Big)\right) \\ &= \frac{1}{2}\Big(Q(x+y) - Q(x) - Q(y)\Big) \\ &= Q(x,y). \end{aligned}$$

Sei V endlich dimensional; wir identifizieren V mit Hilfe einer Basis mit $\mathbb{R}^N$. Dann wird Q durch eine symmetrische Matrix $S \in M(N \times N; \mathbb{R})$ dargestellt, nämlich

$$\begin{aligned} Q(x) &= {}^t x S x \\ Q(x,y) &= {}^t x S y, \end{aligned}$$

wobei x, y als Spaltenvektoren aufgefaßt werden und $Q(x)$ statt $Q(x,x)$ geschrieben wird. Wir können dann $O(V,Q)$ auch mit der Untergruppe

$$O_N(X) = \{A \in GL_N(\mathbb{R}) |\, {}^t A S A = S\}$$

von $GL_N(\mathbb{R})$ identifizieren. Das alles haben wir schon in AGLA I gesehen.

Außer der euklidischen Form werden noch andere wichtig sein; wähle $p, q \geq 0$ mit $p + q = N$. Setze

$$Q(x) = x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_N^2;$$

hier sind p Quadrate mit positivem Vorzeichen, q mit negativem Vorzeichen. Die orthogonale Gruppe wird mit

$$O_{p,q}$$

bezeichnet.

Ein Spezialfall ist $O_{3,1}$, die orthogonale Gruppe von $x_1^2 + x_2^2 + x_3^2 - x_4^2$, die Minkowski-Metrik der speziellen Relativitätstheorie. Die Lorenz-Transformation $(|v|) < 1)$

$$\begin{aligned} x_1 &\longmapsto \frac{x_1 - v x_4}{\sqrt{1 - v^2}} \\ x_2 &\longmapsto x_2 \\ x_3 &\longmapsto x_3 \\ x_4 &\longmapsto \frac{x_4 - v x_1}{\sqrt{1 - v^2}} \end{aligned}$$

liegen in $O_{3,1}$. Deswegen heißt $O_{3,1}$ auch die Lorenz-Gruppe.

Die quadratische Form $x_1^2 + x_2^2 - x_3^2$ wurde in Kapitel 6, 2. verwendet, um einen Kegel zu beschreiben. Aus diesem Grund spielt $O_{2,1}$ eine wichtige Rolle in der Theorie der Quadriken.

Im allgemeinen gibt es keine "Formel" für orthogonale Gruppen, und es ist schwierig, einen Überblick über die ganze Gruppe zu schaffen. In diesem Abschnitt wird gezeigt, wie man in $O(V,Q)$ einige Elemente explizit konstruieren kann.

Zuerst sei $x \in V, Q(x) \neq 0$. Solche Elemente gibt es; sonst wäre $Q(x,y)$ auch immer Null und Q wäre ausgeartet.

Dann definieren wir die lineare Abbildung

$$\sigma_x : V \longmapsto V; v \longmapsto v - 2Q(x,v)Q(x)^{-1}x.$$

Diese Abbildung hat die Eigenschaften

$$\begin{aligned} \sigma_x(x) &= x - 2Q(x)Q(x)^{-1}x \\ &= -x \end{aligned}$$

und

$$\sigma_x(y) = y \quad \text{falls} \quad Q(x,y) = 0.$$

Im Falle von der euklidischen Metrik Q kann man dies als Spiegelung in der "Ebene" $\{u : Q(x,u) = 0\}$ interpretieren. Deswegen heißt σ_x auch eine *Spiegelung.*

Wir weisen jetzt nach, dass σ_x in $O(V,Q)$ liegt. Man hat

$$\begin{aligned} Q\Big(\sigma_x(v)\Big) &= Q\left(v + \Big(-2Q(x,v)Q(x)^{-1}\Big)x\right) \\ &= {}^t\left(v - 2Q(x,v)Q(x)^{-1}\right) \cdot A\left(v \cdot 2Q(x,v)Q(x)^{-1}x\right) \\ &= Q(v) + 4\Big(Q(x,v)Q(x)^{-1}\Big)^2 Q(x,x) + 2 \cdot 2\left(-Q(x,v)Q(x)^{-1}Q(x,v)\right) \\ &= Q(v) + 2Q(x,v)^2Q(x)^{-1} - 4Q(x,v)^2Q(x)^{-1} \\ &= Q(v). \end{aligned}$$

Damit erhalten wir

$$\sigma_x \in O(V,Q).$$

Wir benutzen die σ's jetzt, um das folgende Lemma zu beweisen:

Lemma. *Seien $x, y \in V, Q(x) = Q(y) \neq 0$. Dann gibt es $a \in O(V,Q)$ mit*

$$a(x) = y.$$

Beweis. Wegen der Gleichung von Ptolemäus

$$\begin{aligned} Q(x+y) + Q(x-y) &= 2\Big(Q(x) + Q(x)\Big) \\ &= 4Q(x) \neq 0 \end{aligned}$$

folgert man, dass entweder

$$Q(x+y) \neq 0$$

oder

$$Q(x-y) \neq 0$$

gilt.

Nehmen wir an

$$Q(x-y) \neq 0,$$

so folgt daraus

$$\sigma_{x-y}(x) = x - 2Q(x-y,x)Q(x-y)^{-1}(x-y).$$

Mit

$$\begin{aligned} Q(x-y,x-y) &= Q(x)+Q(y)-2Q(x,y) \\ &= 2Q(x)-2Q(x,y) \\ &= 2Q(x,x-y) \end{aligned}$$

gilt

$$\begin{aligned} \sigma_{x-y}(x) &= x-(x-y) \\ &= y \end{aligned}$$

wie erwünscht.

Gilt aber $Q(x-y)=0$, so erhalten wir

$$Q(x+y) \neq 0.$$

Wird y durch $-y$ ersetzt, erhalten wir von der obigen Gleichung

$$\sigma_{x-y}(x) = -y.$$

Folglich ist wegen $\sigma_x(x) = -x$

$$\sigma_y\Big(\sigma_{x-y}(x)\Big) = y.$$

Deshalb existiert in beiden Fällen ein geeignetes Element von $O(V,Q)$.

Wir benutzen dieses Lemma nun, um eine allgemeinere Aussage machen zu können:

Satz 6.3. *Wir behalten die obige Bezeichnung bei. Seien W_1, W_2 Unterräume von V, so dass die Einschränkungen von Q auf W_1 und W_2 nicht ausgeartet sind. Wir nehmen an, dass eine bijektive lineare Abbildung*

$$a : W_1 \to W_2$$

existiert, so dass gilt

$$Q\Big(a(x)\Big) = Q(x).$$

Dann gibt es ein $\tilde{a} \in O(V,Q)$, so dass die Einschränkung $\tilde{a}|W_1$ wieder a ist;

$$\tilde{a}|W_1 = a.$$

Beweis. Dieser Beweis macht von der Induktion nach $\dim(W_1)$ Gebrauch. Im Falle von $\dim(W_1)=1$ ist die Aussage genau die des Lemmas. Für $\dim(W_1)>1$

dürfen wir annehmen, dass sie schon für niedrigere Dimensionen als $\dim(W_1)$ bewiesen worden ist.

Da Q auf W_1 nicht ausgeartet ist, gibt es ein $x_1 \in W_1$, so dass $Q(x_1) \neq 0$ gilt. Sei $y_1 = a(x_1)$. Dann gilt $Q(y_1) = Q(x_1)$. Nach dem Lemma gibt es ein $b \in O(V,Q)$, so dass $b(y_1) = x_1$ gilt. Wir ersetzen W_2 durch $W_2' = bW_2$ und a durch ba. Es gilt $ba : W_1 \to W_2'$ und

$$\begin{aligned} Q\Big(ba(x)\Big) &= Q\left(b\Big(a(x)\Big)\right) \\ &= Q\Big(a(x)\Big) \\ &= Q(x) \end{aligned}$$

für $x \in W_1$. Deshalb genügen W_1, W_2', ba denselben Voraussetzungen wie W_1, W_2, a. Wir werden zeigen, dass es ein $c \in O(V,Q)$ gibt, so dass gilt

$$c|W_1 = ba|W_1.$$

Denn dann liegt auch

$$\tilde{a} := b^{-1}a$$

in $O(V,Q)$ und genügt

$$\tilde{a}|W_1 = b^{-1}c|W_1 = a|W_1,$$

wie im Satz verlangt wurde.

Wir haben aber auch $ba(x_1) = x_1$. Sei

$$\begin{aligned} U &= \langle x_1 \rangle \\ &= \{y \in V : Q(x_1, y) = 0\}. \end{aligned}$$

Da $Q(x_1) \neq 0$ gilt, folgt $x_1 \notin U$. Man hat

$$U \cap \langle x_1 \rangle = \{0\}$$

und folgert:

$$V = U \oplus \langle x_1 \rangle.$$

Sei

$$\begin{aligned} W_1^* &= W_1 \cap U \\ W_2^* &= W_2' \cap U. \end{aligned}$$

Da $x_1 \in W_1, x_1 \in W_2'$ gelten und Q auf W_1 und W_2' nicht ausgeartet ist, folgt

$$\begin{aligned} W_1 &= W_1^* \oplus \langle x_1 \rangle \\ W_2' &= W_2^* \oplus \langle x_1 \rangle. \end{aligned}$$

Die Summanden sind senkrecht zueinander. Deswegen ist Q auf W_1^*, W_2^* und U nicht ausgeartet. Sei auch $w \in W_1^*$. Dann ist

$$\begin{aligned} Q\Big(ba(w), x_1\Big) &= Q\Big(ba(w), ba(x_1)\Big) \\ &= Q(w, x_1) \\ &= 0; \end{aligned}$$

deshalb gilt

$$ba\Big(W_1^*\Big) = W_2^*.$$

Dabei ist ba surjektiv, weil ba immer injektiv bleibt und zusätzlich gilt:

$$\begin{aligned} \dim\Big(W_1^*\Big) &= \dim(W_1) - 1 \\ &= \dim(W_2') - 1 \\ &= \dim(W_2^*). \end{aligned}$$

Für $x \in W_1^*$ hat man

$$Q\Big(ba(x)\Big) = Q(x).$$

Deswegen sind die Voraussetzungen des Satzes erfüllt, wenn V, W_1, W_2 durch U, W_1^*, W_2^* ersetzt sind. Nach der Induktionsannahme gibt es ein $c_1 : U \to U$, so dass

$$c_1|W_1^* = ba|W_1^*.$$

Wir definieren nun c auf $V = U \oplus \langle x_1 \rangle$ durch

$$c\Big(u, \lambda x_1\Big) = \Big(c_1 u, \lambda x_1\Big) \quad (\lambda \in \mathbb{R}).$$

Es folgt

$$\begin{aligned} c|\langle x_1 \rangle &= \text{Identität} \\ c|W_1^* &= ba|W_1^*. \end{aligned}$$

Deswegen ist

$$c|W_1^* \oplus \langle x_1 \rangle = ba|W_1^* \oplus \langle x_1 \rangle.$$

Weil U und $\langle x_1 \rangle$ zueinander senkrecht sind, hat man

$$\begin{aligned} Q\Big(c(u, \lambda x_1)\Big) &= Q(c_1 u, \lambda x_1) \\ &= Q(c_1 u, o) + Q(o, \lambda x_1) \\ &= Q(u, o) + Q(o, \lambda x_1) \\ &= Q(u, \lambda x_1). \end{aligned}$$

Deswegen liegt c in $O(V, Q)$. Wir haben gezeigt, dass c die notwendigen Eigenschaften hat. Damit ist der Satz bewiesen.

Es sichert die Existenz von vielen Elementen von $O(V, Q)$. Eine Anwendung werden wir im nächsten Abschnitt sehen.

5. Das Sylvestersche Trägheitsgesetz

Wir haben gesheen, dass für eine nicht ausgeartete quadratische Form Q auf einem endlich dimensionalen Vektorraum V eine Basis $e_1, \ldots, e_N$ von V existiert, so dass gilt

$$Q(e_i, e_j) = 0 \quad (i \neq j).$$

Anders ausgedrückt ist die zugehörige Matrix diagonal. Wenn der Körper $\mathbb{R}$ ist, wie er es in unseren Beispielen auch sein wird, können wir es schaffen, dass die Diagonalelemente $Q(e_i, e_j)$ entweder $+1$ oder -1 sind.

Das können wir auch wie folgt formulieren: Sei $S \in M(N \times N; \mathbb{R})$ eine symmetrische nicht-singuläre Matrix. Dann gibt es ein $A \in GL_N(\mathbb{R})$, so dass gilt

$${}^tASA = \begin{pmatrix} \underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{p} & & \\ & \underbrace{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}}_{q} & \\ & & 0 \end{pmatrix}$$

Dies kann man auf mehreren Wegen erreichen. Zum Beispiel

$$\begin{aligned} x^2 + 6xy + 4y^2 &= (x+3y)^2 - \left(\sqrt{5}y\right)^2 \\ \text{aber auch} \qquad &= -\left(\tfrac{\sqrt{5}x}{2}\right)^2 + \left(\tfrac{3}{2}x + 2y\right)^2. \end{aligned}$$

Wir lassen allgemein $A \in GL_N(\mathbb{R})$ zu. Im Hauptachsensatz betrachtet man ausschließlich $A \in O_N$; davon ist hier aber nicht die Rede.

Das Sylvestersche Trägheitsgesetz besagt, dass die Anzahl von positiven Gliedern (bzw. negativen Gliedern) in einer solchen Diagonalisierung unabhängig von der Diagonalisierung ist.

Zum Beispiel gibt es kein $A \in GL_5(\mathbb{R})$, so dass gilt

$${}^tA \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \cdot A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

gilt. Man definiert dann die Signatur von Q als

$$\begin{array}{rl} & \text{Anzahl von positiven Gliedern} \\ - & \text{Anzahl von negativen Gliedern} \end{array}$$

in einer Diagonalisierung von Q. Wegen des Hauptachsensatzes kann diese Zahl mit der

Anzahl von positiven Eigenwerten
\- Anzahl von negativen Eigenwerten

gleichsetzen, weil die Eigenwerte die diagonalen Glieder in der Hauptachsendiagonalisierung sind. Deswegen kann der Index vom charakteristischen Polynom ausgerechnet werden. Die Hilfsmittel sind die Descartessche Vorzeichenregel oder die Sturmsche Kette, die Methoden anbieten, die Anzahl von Nullstellen eines Poylnoms in einem gegebenen Intervall durch Betrachtung der Koeffizienten auszurechnen.

Es ist auch üblich, statt $p - q$ anzugeben,

$$(\underbrace{+, +, \ldots, +}_{p}, \underbrace{-, \ldots, -}_{q})$$

als Signatur zu schreiben.

Satz 6.4 (Sylvestersches Trägheitsgesetz). *Sei Q eine nicht ausgeartete quadratische Form auf einem Vektorraum V. Seien $e_1, \ldots, e_N$ und $e'_1, \ldots, e'_N$ Basen von V, so dass $Q(e_i, e_j) = 0, Q(e'_i, e'_j) = 0$ $(i \neq j)$ gelten. Dann gilt:*

$$\mathrm{Card}\{i : Q(e_i) > o\} = \mathrm{Card}\{i : Q(e'_i) > 0\}.$$

Es werden hier zwei Beweise angegeben. Sie sind grundverschieden. Der erste ist einfacher; beim zweiten werden weitere Hilfsmittel benutzt.

Erster Beweis. Seien

$$\begin{array}{rclcrcl} V_+ & = & \langle e_i | Q(e_i) > 0 \rangle & ; & V_- & = & \langle e_i | Q(e_i) < 0 \rangle \\ V'_+ & = & \langle e'_i | Q(e'_i) > 0 \rangle & ; & V'_- & = & \langle e'_i | Q(e'_i) < 0 \rangle. \end{array}$$

Nach Voraussetzung gelten

$$V = V_+ \oplus V_- \quad , \quad V = V'_+ \oplus V'_-,$$

weil für jedes i entweder $Q(e_i) > 0$ oder $Q(e_i) < 0$ (bzw. $Q(e'_i) > 0$ oder $Q(e'_i) < 0$) zutrifft. Darüber hinaus folgt für i mit $Q(e_i) > 0$, j mit $Q(e_j) < 0$

$$i \neq j$$

und daher

$$Q(e_i, e_j) = 0.$$

Deswegen sind V_+ und V_- bezüglich Q senkrecht; d.h. für $x \in V_+, y \in V_-$ gilt immer

$$Q(x, y) = 0.$$

$Q|V_+$ ist positiv definit, $Q|V_-$ ist negativ definit.

Analoge Aussagen gelten für V'_+, V'_-.

Wir nehmen jetzt an, dass der Satz nicht richtig ist, d.h.

$$\dim(V_+) \neq \dim(V'_+).$$

Wir dürfen annehmen, dass gilt

$$\dim(V_+) > \dim(V'_+).$$

Sei

$$r = \dim(V'_+).$$

Wir wählen $x_1, \ldots, x_{r+1} \in V_+, x_1, \ldots, x_{r+1}$ linear unabhängig. In der Zerlegung

$$V = V'_+ \oplus V'_-$$

schreiben wir

$$x_j = y_j + z_j.$$

Da $\dim(V'_+) = r$ gilt, sind $y_1, \ldots y_{r+1}$ linear abhängig. Sei

$$\sum_{j=1}^{r+1} \lambda_j y_j = 0$$

eine Relation, wobei nicht alle λ_j Null sind. Dann sei

$$x = \lambda_1 x_1 + \ldots + \lambda_{r+1} x_{r+1}$$

weil $x_1, \ldots, x_{r+1}$ linear abhängig gewählt worden sind, folgt

$$x \in V_+, x \neq 0;$$

und folglich

$$Q(x) > 0.$$

Aber auch

$$\begin{aligned} x &= \lambda_1\Big(y_1 + z_1\Big) + \ldots + \lambda_{r+1}\Big(y_{r+1} + z_{r+1}\Big) \\ &= \Big(\lambda_1 y_1 + \ldots + \lambda_{r+1} y_{r+1}\Big) + \Big(\lambda_1 z_1 + \ldots + \lambda_{r+1} z_{r+1}\Big) \\ &= 0 + \Big(\lambda_r z_1 + \ldots + \lambda_{r+1} z_{r+1}\Big) \\ &\in V'_-. \end{aligned}$$

Deswegen

$$Q(x) \leq 0.$$

Das ist unmöglich. Deshalb ist die Annahme, dass $\dim(V_+)$ und $\dim(V'_+)$ ungleich waren, falsch. Damit ist der Satz bewiesen.

Zweiter Beweis. Wir bemerken zuerst, dass es nichts zu beweisen gibt, falls Q positiv definit ist.

Seien

$$\begin{array}{rclcrcl} p & = & \mathrm{Card}\{i : Q(e_i) > 0\} & , & q & = & \mathrm{Card}\{i : Q(e_i) < 0\} \\ p' & = & \mathrm{Card}\{i : Q(e'_i) > 0\} & , & q' & = & \mathrm{Card}\{i : Q(e'_i) < 0\}. \end{array}$$

Wir nehmen auch an, dass $Q(e_i) = \pm 1, Q(e'_i) = \pm 1$ gelten. Wir dürfen annehmen, dass

$$|p - q| \geq |p' - q'|$$

gilt. Da wir Q durch $-Q$ ersetzen dürfen, können wir auch $p > q$ annehmen.

Nach Umnummierung der Basiselemente hat die Matrix die Form

$$\begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & & & & \\ & & & & & & -1 & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & -1 & \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \end{matrix}\right\} p-q \\ \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} q \\ \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} q \end{matrix}$$

bezüglich der ersten Basis und

$$\begin{pmatrix} \pm 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & \pm 1 & & & & & & & \\ & & & 1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & & & & \\ & & & & & & -1 & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & -1 & \end{pmatrix} \begin{matrix} \\ \\ \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} q \\ \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} q \end{matrix}$$

bezüglich der zweiten Basis. Die zweite Aussage folgt, weil gelten

$$\begin{aligned} q &= \frac{1}{2}\big(p + q - (p - q)\big) \\ &= \frac{1}{2}\big(N - |p - q|\big) \\ &\leq \frac{1}{2}\big(N - |p' - q'|\big) \\ &= \frac{1}{2}\big((p' + q') - |p' - q'|\big) \end{aligned}$$

und

$$\begin{aligned} |p' - q'| &\geq p' - q' \\ |p' - q'| &\geq q' - p' \end{aligned}$$

und daher

$$\begin{aligned} q &\leq \frac{1}{2}\Big((p'+q')-(p'-q')\Big) &&= q' \\ q &\leq \frac{1}{2}\Big((p'+q')-(q'-p')\Big) &&= p'. \end{aligned}$$

Weil $p' \geq q' \geq q$ gelten, gibt es mindestens q-mal $+1$ und q-mal -1, für die noch unbekannten Elemente steht ± 1. Es ist zu zeigen, dass diese alle $+1$ sind.

Sei $U_1 \subset V$ von den letzten $2q$ Basiselementen der ersten Basis erzeugte Unterraum. Sei $U_1 \subset V$ der von der letzten $2q$ Basiselementen der zweiten Basis erzeugte Unterraum. Da die Einschränkung von Q auf U_1 und U_2 dieselbe Form aufweisen, gibt es $a : U_1 \to U_2$ mit

$$Q\Big(a(x)\Big) = Q(x).$$

Nach Satz 6.3 gibt es ein $\tilde{a} \in O(V,Q)$ mit

$$\tilde{a}|U_1 = a.$$

Nun ist U_1^- (bzw. U_2^-) von den ersten $p-q$ Elementen der ersten Basis (bzw. der zweiten Basis) erzeugte Unterraum von V. Es gilt auch

$$\tilde{a}\Big(U_1^-\Big) = U_2^-,$$

denn

$$x \in U_1^-, a(y) \in U_2 \quad (\text{wobei } y \in U_1)$$

liefert

$$\begin{aligned} Q\Big(\tilde{a}(x), a(y)\Big) &= Q\Big(\tilde{a}(x), \tilde{a}(y)\Big) \\ &= Q(x,y) \\ &= 0. \end{aligned}$$

Deswegen hat man

$$\tilde{a}\Big(U_1^-\Big) \subset U_2^-.$$

Um die andere Richtung zu zeigen, benutzen wir

$$\begin{aligned} \dim\Big(U_1^-\Big) &= \dim(V) - \dim(U_1) \\ &= p - q \\ &= \dim(V) - \dim(U_2) \\ &= \dim\Big(U_2^-\Big). \end{aligned}$$

Da $\tilde{a}$ bijektiv ist, gilt

$$\tilde{a}\Big(U_1^-\Big) = U_2^-,$$

weil die zwei Räume dieselbe Dimension haben.

Sei nun $x \in U_2^-$. Dann gibt es ein $y \in U_1^-$ mit $\tilde{a}(y) = x$. Es folgt

$$\begin{aligned} Q(x) &= Q\big(\tilde{a}(x)\big) \\ &= Q(y) \\ &> 0. \end{aligned}$$

Deswegen ist $Q|U_2^-$ auch positiv definit. Die Matrix von Q bezüglich der zweiten Basis kann dann nur

$$\begin{pmatrix} \underbrace{\begin{matrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{matrix}}_{p-q} & & & & 0 \\ & & \underbrace{\begin{matrix} 1 & \\ & 1 \end{matrix}}_{q} & & \\ & & & \underbrace{\begin{matrix} 1 & \\ & 1 \end{matrix}}_{q} & \\ 0 & & & & \end{pmatrix}$$

sein. Das ist aber genau das, was bewiesen werden mußte.

6. Einige orthogonale Gruppe

Es wurde oben betont, dass es in der Regel keine "Formel" für die orthogonalen Gruppen gibt. Nichtsdestoweniger kann man bei kleinen Dimensionen alle orthogonalen Gruppen durch andere -besser bekannte Gruppen- ausdrücken.

Die Lister der in Frage kommenden Gruppen ist

$$\begin{aligned}
\dim(V) &= 2, \quad \text{Signatur } = (+,+) \\
&= 2, \quad \text{Signatur } = (+,-) \\
&= 3, \quad \text{Signatur } = (+,+,+) \\
&= 3, \quad \text{Signatur } = (+,+,-) \\
&= 4, \quad \text{Signatur } = (+,+,+,+) \\
&= 4, \quad \text{Signatur } = (+,+,+,-) \\
&= 4, \quad \text{Signatur } = (+,+,-,-).
\end{aligned}$$

Hiermit sind alle Fälle mit $\dim(V) \leq 4$ abgedeckt, weil $O(V,Q) = O(V,-Q)$ gilt.

Die zweidimensionalen Fälle sind aus der Schulmathematik bekannt. Der Fall $(+,+,+)$ ist für die Geometrie realer Gegenstände von großem Interesse. Für Besserwissende ist $(+,+,+,-)$ noch von größerer Bedeutung, weil damit die Lorentzgruppe der speziellen Relativitätstheorie behandelt wird. Die hier angegebene Beschreibung dieser Gruppe spielt heutzutage eine wichtige Rolle in der theoretischen Physik.

Die ähnliche Signatur $(+,+,-)$ kommt, wie wir schon gesehen haben, in der Geometrie der Quadriken vor. Wir werden sehen, dass diese Gruppe in der hyperbolischen Geometrie entscheidend sein wird.

Hier werden die Konstruktionen der Gruppen beschrieben. Es wird aber nicht nachgewiesen, dass damit alle Gruppenelemente erfaßt werden. Um dies zu zeigen, muß man beweisen, dass alle Spiegelungen schon dargestellt worden sind. Dann muß gezeigt werden, dass ein beliebiges $g \in O(V,Q)$ in der Form $S_1 \dots S_k$ geschrieben werden kann, wobei die S_j sämtlich Spiegelungen sind.
Um das zu beweisen, sei $e_1, \dots, e_n$ eine Basis, so dass

$$\begin{aligned}
Q(e_i, e_j) &= 0 \quad (i \neq j) \\
&= 1 \quad (i = j \leq p) \\
&= -1 \quad (p < i = j \leq n).
\end{aligned}$$

Dann genügen $f_1 = g(e_1), \dots, f_n = g(e_n)$ denselben Bedingungen. Nach dem Lemma von Kapitel 6, 3. gibt es eine Spiegelung oder das Produkt zweier Spiegelungen S_1; so dass $S_1 e_1 = f_1$. Wir ersetzen g durch $S_1^{-1} g$. Nun sind $f_1, \dots, f_n$ derart, dass $f_1 = e_1$ gilt. Deswegen ist

$$\begin{aligned}
\langle e_2, \dots, e_n \rangle = \langle e_1 \rangle^- &= \langle f_1 \rangle^- \\
&= \langle f_1, \dots, f_n \rangle.
\end{aligned}$$

D.h., das neue g schickt den Raum $\langle e_2, \dots, e_n\rangle$ in sich selbst. Es gibt dann ein Produkt von Spiegelungen, das g auf $\langle e_1, \dots e_n\rangle$ darstellt. Weil die Spiegelungen in $\langle e_2, \dots, e_n\rangle$ definiert sind und weil σ_v auf $\langle v\rangle^-$ trivial operiert, lassen sich auf $\langle e_1\rangle \oplus \langle e_2, \dots, e_n\rangle$ fortsetzen. Auf diese Weise haben wir $S_1^{-1}g$ als ein Produkt von Spiegelungen dargestellt und damit auch g.

Nach diesen Bemerkungen beschreiben wir die orthogonalen Gruppen der oben angegebenen Liste.

1. $\underline{\dim(V) = 2, \text{ Signatur } = (+,+).}$
Hier ist

$$Q(x) = x_1^2 + x_2^2$$

und

$$O(V,Q) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \Big| \theta \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix} \Big| O \in \mathbb{R} \right\}$$

wie schon in AGLA I bewiesen worden ist.

2. $\underline{\dim(V) = 2, \text{ Signatur } = (+,-).}$
Hier ist

$$\begin{aligned} Q(x) &= x_1^2 - x_2^2 \\ &= \big(x_1 + x_2\big)\big(x_1 - x_2\big). \end{aligned}$$

Wir führen neue Koordinaten ein:

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= x_1 - x_2. \end{aligned}$$

Dann wird

$$Q'(y) = y_1 y_2$$

und

$$O(V,Q') = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} : t \in \mathbb{R}^\times \right\} \cup \left\{ \begin{pmatrix} 0 & -t \\ t^{-1} & 0 \end{pmatrix} \Big| t \in \mathbb{R}^\times \right\}.$$

Beweis. Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O(V,Q')$. Daraus folgt, dass

$$Q\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) = Q \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

sein muß, also

$$\big(ay_1 + by_2\big)\big(cy_1 + dy_2\big) = y_1 y_2;$$

oder

$$ac = 0, bd = 0, ad + bc = 1.$$

Löst man diese Gleichungen, so kommt man auf die angegebene Form.

3. $\underline{\dim(V) = 3, \text{ Signatur } = (+,+,-).}$
Die quadratische Form ist

$$x_1^2 + x_2^2 - x_3^2.$$

Wir führen neue Koordinaten ein

$$\begin{aligned} y_1 &= x_1 \\ y_2 &= x_2 + x_3 \\ y_3 &= x_2 - x_3. \end{aligned}$$

Die quadratische Form ist jetzt

$$y_1^2 + y_2 y_3.$$

Das Wichtigste ist nun, diesen Ausdruck mit

$$-\det \begin{pmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{pmatrix}$$

zu identifizieren.

Diese Matrix hat die Spur =0. Umgekehrt kann jedes 2×2-Matrix mit verschwindender Spur in dieser Form geschrieben werden.

Wir schreiben dann

$$\begin{aligned} V &= \left\{ a \in M(2 \times 2; \mathbb{R}) | Tr(A) = 0 \right\} \\ Q(A) &= -det(A). \end{aligned}$$

Wir erhalten Elemente aus $O(V,Q)$ von $GL_N(\mathbb{R})$ durch das folgende Verfahren: $g \in GL_2(\mathbb{R})$ liefert die lineare Abbildung

$$A \longmapsto gAg^{-1}$$

auf V. Es gilt auch

$$\begin{aligned} Q(gAg^{-1}) &= -\det(gAg^{-1}) \\ &= -\det(g)\det(A)\det(g)^{-1} \\ &= -\det(A) \\ &= Q(A). \end{aligned}$$

Deshalb liegt diese lineare Abbildung in $O(V,Q)$.

Es kann natürlich passieren, dass zwei Elemente $g_1, g_2 \in GL_2(\mathbb{R})$ dieselbe lineare Abbildung liefern. Das würde bedeuten:

$$g_1 A g_1^{-1} = g_2 A g_2^{-1}$$

für alle A. Das heißt (da V eine $GL_2(\mathbb{R})$-Menge ist)

$$\left(g_2^{-1}g_1\right)\cdot A = A\left(g_2^{-1}g_1\right).$$

Die Spur von A war Null. Jedes $B \in M(2\times 2;\mathbb{R})$ kann aber als $\left(B-\frac{1}{2}Tr(B)E_2\right)+\frac{1}{2}Tr(B)E_2$ geschrieben werden. Da $g_2^{-1}g_1$ mit allen $A \in V$ und auch mit E_2 kommutiert und $B-\frac{1}{2}Tr(B)E_2$ in V liegt, folgt

$$\left(g_2^{-1}g_1\right)B = B\left(g_1g_2^{-1}\right)$$

für alle B. Deswegen muß (nach AGLA I) $g_2^{-1}g_1$ von der Form $\lambda E_2\left(\lambda \in \mathbb{R}^\times\right)$ sein. Man kann dann $O(V,Q)$ mit

$$GL_2(\mathbb{R})/\left\{\lambda E_2 : \lambda \in \mathbb{R}^\times\right\}$$

identifizieren. Man bemerke, dass die Untergruppe ein Normalteiler ist.

Die eben durchgeführte Idee liegt auch den anderen Beispielen zugrunde. Wichtig ist, dass bei 2×2-Matrizen die Determinante eine quadratische Form ist.

Der nächste Fall wird ähnlich behandelt.

4. $\underline{\dim(V)=4\text{ , Signatur }=(+,+,-,-).}$
Die quadratische Form ist

$$x_1^2+x_2^2-x_3^2-x_4^2.$$

Wir führen neue Koordinaten ein

$$\begin{aligned} y_1 &= x_1-x_3\\ y_2 &= x_1+x_3\\ y_3 &= x_2+x_4\\ y_4 &= x_4-x_2. \end{aligned}$$

Dann wird die quadratische Form

$$y_1y_2-y_3y_4 = \det\begin{pmatrix} y_1 & y_3\\ y_4 & y_2\end{pmatrix}.$$

Wir nehmen

$$\begin{aligned} V &= M(2\times 2,\mathbb{R})\\ Q &: Q(A)=\det(A). \end{aligned}$$

Wir betrachten V als $GL_2(\mathbb{R})\times GL_2(\mathbb{R})$-Menge

$$\begin{aligned} \left(GL_2(\mathbb{R})\times GL_2(\mathbb{R})\right)\times V &\to V\\ \left((g_1,g_2),A\right) &\longmapsto g_1Ag_2^{-1}. \end{aligned}$$

Nun gilt

$$\begin{aligned} Q\left(g_1 A g^{-1}\right) &= \det\left(g_1 A g_2^{-1}\right) \\ &= \det(g_1)\det(A)\det(g_2)^{-1} \\ &= \det(g_1)\det(g_2)^{-1} Q(A). \end{aligned}$$

Wir betrachten deswegen die Untergruppe

$$G = \left\{(g_1, g_2) \in GL_2(\mathbb{R}) \times GL_2(\mathbb{R}) | \det(g_1) = \det(g_2)\right\}.$$

Für $(g_1, g_2) \in G$ hat man dann

$$Q\left(g_1 A g_2^{-1}\right) = Q(A).$$

Die Untergruppe $\left\{(\lambda E_2, \lambda E_2) | \lambda \mathbb{R}^\times\right\}$ wirkt trivial, so dass man kann $O(V, Q)$ mit

$$G/\left\{(\lambda E_2, \lambda E_2) | \lambda \in \mathbb{R}^x\right\}$$

identifizieren kann.

Um die anderen drei Beispiele zu behandeln, braucht man Matrizen aus $M(2 \times 2, \mathbb{C})$.

5. $\underline{\dim(V) = 3, \text{ Signatur } = (+,+,+).}$
Hier ist die quadratische Form

$$x_1^2 + x_2^2 + x_3^2.$$

Wir führen neue (komplexe) Koordinaten ein:

$$\begin{aligned} y_1 &= x_1 + ix_2 \\ \bar{y}_1 &= x_1 - ix_2 \\ y_3 &= x_3. \end{aligned}$$

Dann ist die quadratische Form

$$y_1 \bar{y}_1 + y_3^2 = -\det \begin{pmatrix} y_3 & y_1 \\ \bar{y}_1 & -y_3 \end{pmatrix}.$$

Die Matrix stellt dann eine *Hermitesche Form* mit Spur Null dar. $GL_2(\mathbb{C})$ operiert auf der Menge aller

$$\left\{A \in M(2 \times 2, \mathbb{C}) : {}^tA = A\right\}$$

durch

$$A \longmapsto g A^t \bar{g}.$$

Sei

$$A = \begin{pmatrix} u & v \\ \bar{v} & -u \end{pmatrix} (u \in \mathbb{R}, v \in \mathbb{C}),$$

eine solche Matrix. Dann ist die Spur von $gA^t\bar{g}$

$$\Big(|a|^2 + |c|^2 - |b|^2 - |d|^2\Big)u + 2Re\Big((a\bar{b} + c\bar{d})v\Big).$$

Da die Spur gleich Null sein soll, verlangen wir

$$\begin{aligned} |a|^2 + |c|^2 &= |b|^2 + |d|^2 \\ a\bar{d} + c\bar{d} &= 0. \end{aligned}$$

Diese Bedingungen bestimmen eine Untergruppe von $GL_2(\mathbb{C})$, da sie Elemente festlegen, die alle dieselbe Eigenschaft haben. Da Q erhalten bleiben soll, muß eine weitere Forderung an g gestellt werden, nämlich $|\det(g)|^2 = 1$ (vgl. Fall 6 unten). Man kann sich überlegen, dass die folgende Menge zwar nicht alle Lösungen darstellt, aber ausreichend ist:

$$G = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \Big| \, |\alpha|^2 + |\beta|^2 = 1 \right\} \cup \left\{ \begin{pmatrix} \alpha & \beta \\ \bar{\beta} & -\bar{\alpha} \end{pmatrix} \Big| \, |\alpha|^2 + |\beta|^2 = 1 \right\},$$

womit die obigen Bedingungen offensichtlich erfüllt sind. Die Gruppe $O(V, Q)$ ist zu

$$G/\{\pm E_2\}$$

isomorph.

6. $\underline{\dim(V) = 4, \text{ Signatur} = (+,+,+,-).}$
Hier ist die quadratische Form gleich

$$x_1^2 + x_2^2 + x_3^2 - x_4^2.$$

Wir führen wieder neue Koordinaten ein

$$\begin{aligned} y_1 &= x_3 + x_4 \\ y_2 &= x_4 - x_3 \\ y_3 &= x_1 + ix_2 \\ \bar{y}_3 &= x_1 - ix_2. \end{aligned}$$

Dann ist die quadratische Form

$$|y_3|^2 - y_1 y_2 = -\det \begin{pmatrix} y_1 & y_3 \\ \bar{y}_3 & y_2 \end{pmatrix}.$$

Diese Matrix stellt eine allgemeine Hermitesche Form dar. Die Gruppe $GL_2(\mathbb{C})$ operiert auf

$$\{A \in M(2 \times 2; \mathbb{C}) | \, {}^t\bar{A} = A\}$$

durch

$$A \longmapsto gA^t\bar{g}.$$

Wir erhalten

$$\begin{aligned} Q\big(gA^t\bar{g}\big) &= \det(g)Q(A)\det(\bar{g}) \\ &= |\det(g)|^2 Q(A). \end{aligned}$$

Wir müssen mindestens verlangen, dass

$$|\det(g)|^2 = 1.$$

Weil aber für $\zeta \in \mathbb{C}$ mit $|\zeta|^2 = 1$ gilt

$$(\zeta E_2)A^t(\overline{\zeta E_2}) = A$$

können wir uns auf diejenigen g mit

$$\det(g) = 1$$

beschränken. Deswegen operiert $SL_2(\mathbb{C})$ als orthogonale Gruppe. Man stellt wieder fest, dass $SL_2(\mathbb{C})/\{\pm E_2\}$ zu einer Untergruppe von $O(V,Q)$ vom Index 2 isomorph ist. Die Spiegelung $(y_1, y_2, y_3) \longmapsto (y_2, y_1, y_3)$ ist nicht dargestellt.

7. $\underline{\dim(V) = 4, \text{ Signatur} = (+,+,+,+).}$
Hier ist die quadratische Form

$$x_1^2 + x_2^2 + x_3^2 + x_4^2$$

gegeben.

Wir führen jetzt die neuen Koordinaten ein

$$\begin{aligned} y_1 &= x_1 + ix_2 \\ y_2 &= x_3 + ix_4 \\ \bar{y}_1 &= x_1 - ix_2 \\ \bar{y}_2 &= x_3 - ix_4. \end{aligned}$$

Dann wird die quadratische Form

$$|y_1|^2 + |y_2|^2 = \det \begin{pmatrix} y_1 & y_2 \\ -\bar{y}_2 & \bar{y}_1 \end{pmatrix}.$$

Wir bemerken zunächst, dass

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \cdot \begin{pmatrix} u' & v' \\ -\bar{v}' & \bar{u}' \end{pmatrix} = \begin{pmatrix} uu' - v\bar{v}' & uv' + v\bar{u}' \\ -\bar{v}u' - \bar{u}\bar{v}' & \bar{u}\bar{u}' - \bar{v}\bar{v}' \end{pmatrix};$$

deshalb ist ein Produkt zweier Matrizen der Form $\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ wieder von derselben Form. Die Menge aller solchen nicht verschwindenden Matrizen bilden deswegen eine Untergruppe G von $GL_2(\mathbb{C})$. Sei

$$V = \left\{ \begin{pmatrix} y_1 & y_2 \\ -\bar{y}_2 & \bar{y}_1 \end{pmatrix} \in M(2 \times 2; \mathbb{C}) \right\}.$$

Dann wird V eine $G \times G$-Menge durch

$$\Big((g_1, g_2), A\Big) \longmapsto g_1 A g_2^{-1}.$$

Auf diese Weise erhält man ein Element aus $O(V, Q)$. Die orthogonale Gruppe wird hier

$$G \times G / \Big\{(E_2, E_2), (-E_2, -E_2)\Big\}.$$

Schlußbemerkung. Der Grund dafür, dass viele dieser Gruppen aus zwei Teilen bestehen, ist folgender:
Auf $O(V, Q)$ kann man die Determinante definieren. Wie wir schon gesehen haben (vgl. Beweis zu Satz 4.1), gilt für $A \in O(V, Q)$

$$\det(A) = \pm 1.$$

Man kann nachrechnen, dass

$$\det(S) = -1$$

gilt, falls S eine Spiegelung ist. (Hier und auch in anderen Zusammenhängen benehmen sich orthogonale Gruppen wie symmetrische Gruppen, Spiegelungen wie Transpositionen.)
Deshalb haben wir eine Abbildung

$$\det : O(V, Q) \to \{\pm 1\}.$$

Der Kern wird $SO(V, Q)$. Diese Untergruppe ist ein Teil. Da man

$$O(V, Q) = SO(V, Q) \cup S\, SO(V, Q)$$

hat, wobei S irgendeine Spiegelung ist, ist die zu beobachtende Zerlegung erklärt.

Im sechsten Fall ($\dim(V) = 4$, Signatur = (+,+,+,-)) ist $SO(V, Q)$ zu $SL_2(\mathbb{C})/\{\pm E_2\}$ isomorph.

7. Die hyperbolische Geometrie

Wir betrachten hier die äquivalenten quadratischen Formen

$$x_1^2 + x_2^2 - x_2^3$$

oder

$$y_1^2 + y_2 y_3.$$

Geometrisch ist es etwas leichter

$$x_1^2 + x_2^2 - x_3^2$$

zu betrachten, algebraisch kann man besser mit

$$y_1^2 + y_2 y_3$$

arbeiten. Wir werden aber immer die Relationen

$$\begin{array}{rclcrcl} y_1 & = & x_1 & & x_1 & = & y_1 \\ y_2 & = & x_2 + x_3 & \text{oder} & x_2 & = & \frac{1}{2}(y_2 + y_3) \\ y_3 & = & x_2 - x_3 & & x_3 & = & \frac{1}{2}(y_2 - y_3) \end{array}$$

im Auge behalten.

Zuerst betrachten wir die Quadriken

$$Q_R : x_1^2 + x_2^2 - x_3^2 = R.$$

Es gibt drei Fälle:

1. $R = 0$. Wir sahen in Kapitel 6, 2., dass Q_R ein Kegel ist. Der Schnitt von Q_0 mit $x_3 = z$ ist ein Kreis mit Radius z.

2. $R > 0$. Der Schnitt von Q_R mit $x_3 = z$ ist ein Kreis mit Radius $\sqrt{R + z^2}$. Wir erhalten ein einschaliges Hyperboloid. Die "Taille" hat Radius R.

3. $R < 0$. Der Schnitt von Q_R mit $x_3 = z$ ist wieder ein Kreis mit Radius $\sqrt{z^2 + R}$. Dieser existiert nur, wenn gilt

$$z^2 > (-R).$$

Deswegen spaltet sich Q_R in zwei Teile, nämlich dem mit $x_3 > \sqrt{|R|}$. Wir erhalten hier ein zweischaliges Hyperboloid.

Wie in Kapitel 6, 6. ordnen wir (y_1, y_2, y_3) die Matrix $Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{pmatrix}$ zu. Dann gilt

$$-\det \begin{pmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{pmatrix} = y_1^2 + y_2 y_3.$$

Wie wir schon gesehen haben, wirkt $GL_2(\mathbb{R})$ durch

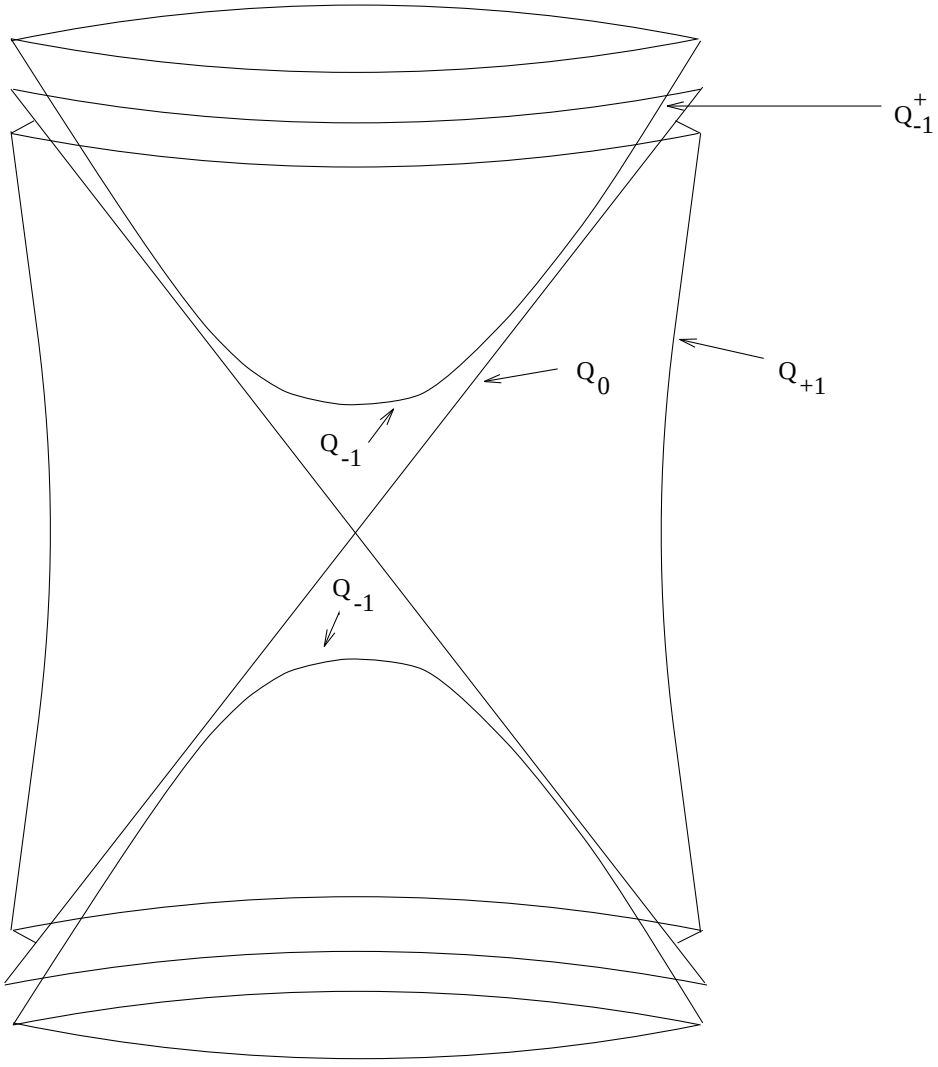
$$g : Y \longmapsto gYg^{-1}.$$

Die quadratische Form $-\det(Y)$ bleibt erhalten, und damit wird

$$Q_R = \{Y | -\det(Y) = R\}$$

zu einer $GL_2(\mathbb{R})$-Menge.

Für uns ist es bequemer, statt $GL_2(\mathbb{R})$ nur die Gruppe $SL_2(\mathbb{R})$ zu betrachten.



Wir untersuchen jetzt, wie $SL_2(\mathbb{R})$ auf die Q_R's operiert.

1. $R = 0$. $SL_2(\mathbb{R})$ läßt 0 fest; wir betrachten deswegen $Q_0 - \{0\}$. Ein Punkt auf Q_0 ist $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, ein anderer $\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$, also $(x_1, x_2, x_3) = \left(0, \frac{1}{2}, \frac{1}{2}\right)$ bzw. $\left(0, -\frac{1}{2}, -\frac{1}{2}\right)$. Wir zeigen, dass $Q_0 - \{0\}$ die Vereinigung der Bahnen dieser zwei Elemente ist, dass sie disjunkt sind und dass gilt

$$\mathrm{Stab}_{SL_2(\mathbb{R})}\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = \mathrm{Stab}_{SL_2(\mathbb{R})}\left(\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\right) = \left\{\pm\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R}\right\}.$$

Um diese Aussage zu beweisen, berechnen wir

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -ac & a^2 \\ -c^2 & ac \end{pmatrix}.$$

Sei $Y \in Q_0 - \{0\}$. Ist y_2 positiv, so müßte gelten

$$\begin{aligned} y_3 &= -y_1^2/y_2 < 0, \\ y_1 &= \pm\sqrt{-y_2 y_3}. \end{aligned}$$

Deswegen definieren wir $a = \sqrt{y_2}, c = -y_1/a$ und b, d, so dass $ad - bc = 1$. Damit haben wir ein geeignetes $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gefunden, so dass

$$g\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}g^{-1} = Y.$$

Gilt aber $y_2 = 0$, dann wählen wir

$$c = \sqrt{-y_3}; \quad a = 0$$

und b, d, so dass

$$ad - bc = 1.$$

Es folgt wieder $g\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}g^{-1} = Y$.

In den anderen Fällen $y_2 < 0$ oder $y_2 = 0\, y_3 > 0$ brauchen wir nur Y durch $-Y$ zu ersetzen. Aus der Rechnung oben sehen wir, dass es $g \in SL_2(\mathbb{R})$ gibt, so dass

$$g\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}g^{-1} = Y.$$

Gilt aber $y_2 = 0$, dann wählen wir

$$c = \sqrt{-y_3}; \quad a = 0$$

und b, d, so dass

$$ab - bc = 1.$$

Es folgt wieder $g \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} g^{-1} = Y$.

In den anderen Fällen $y_2 < 0$ oder $y_2 = 0\ y_3 > 0$ brauchen wir nur Y durch $-Y$ zu ersetzen. Aus der Rechnung oben sehen wir, dass es $g \in SL_2(\mathbb{R})$ gibt, so dass

$$g \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} g^{-1} = Y.$$

D.h. $Q_0 - \{0\}$ läßt sich als Vereinigung der Bahnen von $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$ darstellen.

Es ist aber nicht möglich, dass

$$\begin{pmatrix} -ac & a^2 \\ -c^2 & ac \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$$

weil $a^2 > 0$ gilt. Deswegen sind die beiden Bahnen disjunkt.

Für den letzten Teil der Behauptung benötigen wir die Lösung von $\begin{pmatrix} -ac & a^2 \\ -c^2 & ac \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$$a = \pm 1, c = 0.$$

Dann ist der Stabilisator die oben angegebene Gruppe, da von $ad - bc = 1$ folgt

$$\begin{aligned} a &= d = \pm 1 \\ b &= \text{willkürlich.} \end{aligned}$$

2. $R > 0$. Wir wissen, dass gilt

$$\begin{aligned} \lambda Q_R &= \{\lambda Y \,|\, \det(Y) = R\} \\ &= \{\lambda Y \,|\, \det(\lambda Y) = \lambda^2 R\} \\ &= Q_{\lambda R}. \end{aligned}$$

Deswegen können wir unsere Überlegungen auf den Fall $R = 1$ beschränken.

Damit folgt

$$\begin{aligned} Y^2 &= \begin{pmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{pmatrix} \begin{pmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{pmatrix} \\ &= \begin{pmatrix} y_1^2 + y_2 y_3 & 0 \\ 0 & y_1^2 + y_2 y_3 \end{pmatrix} \\ &= \begin{pmatrix} R & 0 \\ 0 & R \end{pmatrix} \\ &= +E_2. \end{aligned}$$

Die Eigenwerte von Y sind daher ± 1, weil ihre Quadrate 1 sind. Da $\det(Y) = -1$ gilt, ist ein Eigenwert $+1$, der andere -1. Da sie verschieden sind, gibt es ein $g \in GL_2(\mathbb{R})$, so dass gilt

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

Wir können g mit $\begin{pmatrix} 1 & 0 \\ 0 & 1/\det(g) \end{pmatrix} g$ ersetzen. Dieses Element liegt aber in $SL_2(\mathbb{R})$ und deshalb gibt es $g \in SL_2(\mathbb{R})$ mit

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

Deshalb besteht Q_1 aus einer Bahn, nämlich der von $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In diesem Fall ist die Stabilisatorgruppe

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{R}^\times \right\}.$$

Das beweist man, indem man die Gleichung

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

in der Form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

betrachtet. Es folgt: $b = 0, c = 0$ und mit $ad = 1$ die Behauptung.

3. $R < 0$. Hier können wir $R = -1$ nehmen. Es gibt hier wieder zwei Bahnen, die von $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und die von $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; die Stabilisatorgruppe ist

$$\left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

In diesem Fall hat man

$$Y^2 = -E_2;$$

woran man sieht, dass Y Eigenwerte $\pm i$ hat. Da $\det(Y) = 1$ gilt, ist i der eine Eigenwert, $-i$ der andere. In AGLA I wurde gezeigt, dass es dann ein $g \in GL_2(\mathbb{R})$ gibt, so dass

$$g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g^{-1} = Y.$$

Wir können g durch $\sqrt{|\det(g)|}^{-1} g$ ersetzen; deswegen dürfen wir annehmen, dass gilt

$$\det(g) = \pm 1.$$

Wir bemerken, dass $\det \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -1$ und

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \frac{1}{-1} \begin{pmatrix} 0 & -1 \\ +1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

gelten.

Wir rechnen nun nach: für $g \in SL_2(\mathbb{R})$ gilt

$$(*) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} ac+bd & -(a^2+b^2) \\ (c^2+d^2) & -(ac+bd) \end{pmatrix}.$$

Deswegen gibt es in der $SL_2(\mathbb{R})$-Bahn von $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ nur solche Y mit $y_2 < 0, y_3 > 0$. In der $SL_2(\mathbb{R})$-Bahn von $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ sind die Y mit $y_2 > 0, y_3 < 0$. Da $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ die beiden Bahnen vertauscht, folgt, dass <u>alle</u> Y mit $y_2 < 0, y_3 > 0$ in der Bahn von $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ vorkommen.

Aus der Gleichung $(*)$ folgt auch, dass der Stabilisator durch

$$\begin{aligned} ac+bd &= 0 \\ a^2+b^2 &= 1 \\ c^2+d^2 &= 1 \\ ad-bc &= 1 \quad (\text{wegen } g \in SL_2(\mathbb{R})) \end{aligned}$$

angegeben wird. Diese Gleichungen können leicht gelöst werden -es wurde in AGLA I durchgeführt- und man erhält die oben angegebene Gruppe.

Wir können $Q^+_{-1} = \{Y \in Q_{-1} | y_2 > 0\}$ als eine Art Geometrie betrachten. Sie ist die hyperbolische und Lobatschewskijsche Geometrie. Die "Ebene" ist Q^+_{-1}; die "Bewegungsgruppe" ist $SL_2(\mathbb{R})$. Wir werden jetzt einen Abstand auf Q^+_{-1} definieren. Dazu brauchen wir einige vorhergehende Überlegungen.

Seien nun $Y_1, Y_2 \in Q^+_{-1}$. Dann liegt für $s : 0 \leq s \leq 1$ ein $sY_1 + (1-s)Y_2$ auf einem $Q_{R(s)}$ mit $R(s) \leq -1$. Das heißt

$$Q\Big(Y_1 \cdot s + Y_2(1-s)\Big) \leq -1$$

und deshalb folgt für $s : 0 \leq s \leq 1$ nach Ausmultiplizieren von ${}^t\Big(y_1 + y_2(1-s)\Big) A \Big(y_1 s + y_2(1-s)\Big) \leq 1$

$$-s^2 + 2s(1-s)Q(Y_1, Y_2) - (1-s)^2 \leq -1.$$

Wir erhalten

$$2s(1-s)Q(Y_1,Y_2) \leq s^2 + (1-s)^2 - 1 = -2s(1-s)$$

und daher

$$Q(Y_1,Y_2) \leq -1.$$

Vom Bild sieht man auch, dass $sY_1 + (1-s)Y_2$ gerade dann in Q^+_{-1} liegt, wenn $s = 0, 1$ oder $Y_1 = Y_2$ gilt. Deswegen gilt

$$-Q(Y_1,Y_2) > 1$$

falls $Y_1 \neq Y_2$. (Von Q_{+1} kann man eine solche Folgerung nicht ziehen, weil es Geraden gibt, die in Q_{+1} liegen, eine Gegebenheit, die für die moderne Architektur wichtig ist.)

Es ist auch möglich, diese Ungleichung algebraisch zu beweisen. Wir benutzen die $\underline{x}$-Koordinaten; Q^+_{-1} ist dann das Gebilde

$$x_1^2 + x_2^2 - x_3^2 = -1, x_3 > 0.$$

Sei $\underline{x}_0 = (0,0,1)$. Für jeden anderen Punkt $\underline{x}$ gilt $x_3 > 1$ und deswegen

$$Q\left(\underline{x}_0, \underline{x}\right) = \frac{1}{2} Q\left(Q\left(\underline{x}_0 + \underline{x}\right) - Q\left(\underline{x}_0\right) - Q\left(\underline{x}\right)\right) = -x_3 < -1.$$

Für $g \in SL_2(\mathbb{R})$ hat man $\left(\underline{x}_0 \neq \underline{x}\right)$

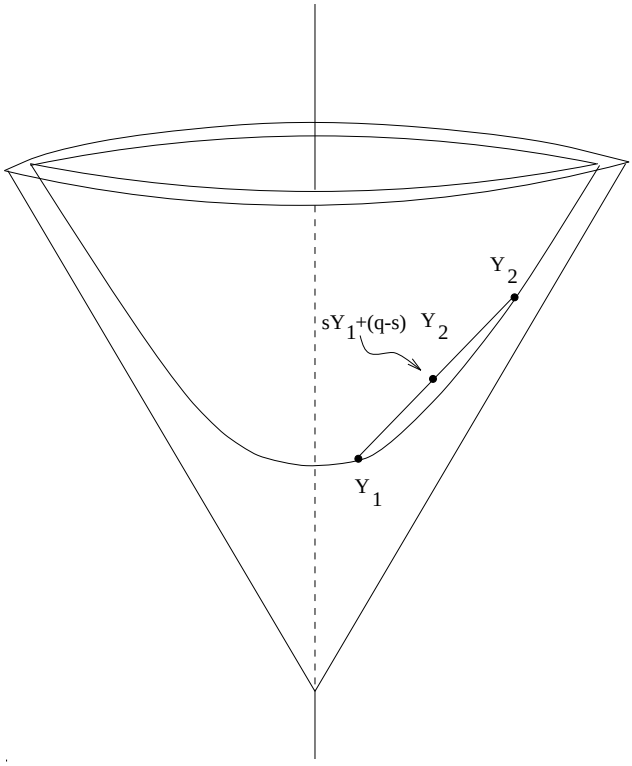
$$Q\left(g\left(\underline{x}_0\right), g\left(\underline{x}\right)\right) < -1.$$

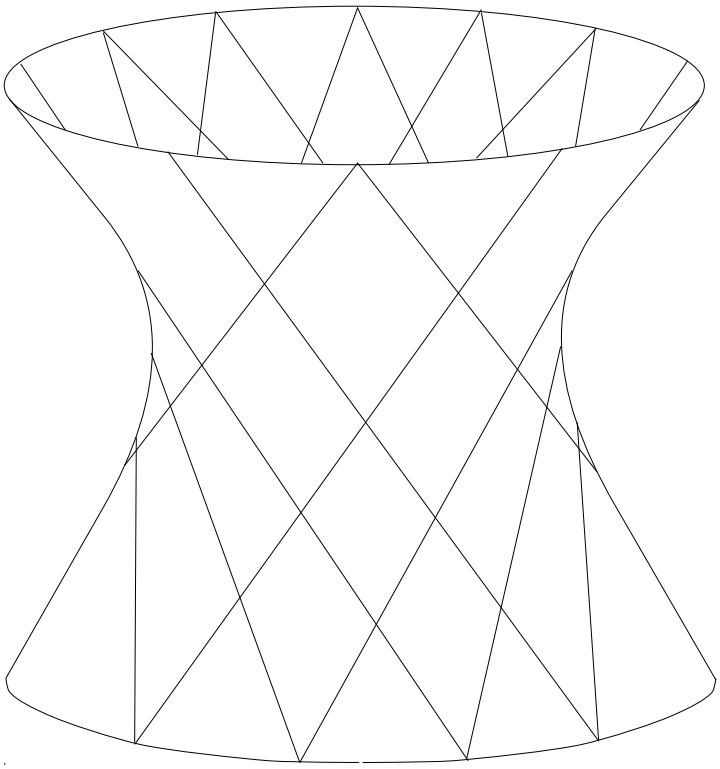
Weil $SL_2(\mathbb{R})$ transitiv auf Q^+_{-1} operiert, folgt

$$Q(y,y') < -1 \quad (y, y' \in Q^+_{-1}, y \neq y').$$

Mit derselben Idee betrachten wir

$$Q(x_0,x), Q(x_0,x') \quad \text{und} \quad Q(x,x').$$


Y 2
sY 1+(q-s) Y 2
Y 1



Seien

$$\begin{aligned} x &= (x_1, x_2, x_3) &\in Q^+_{-1} \\ x' &= (x'_1, x'_2, x'_3) &\in Q^+_{-1}. \end{aligned}$$

Dann ist

$$\begin{aligned} Q(x_0, x) &= -x_3 \\ Q(x_0, x') &= -x'_3 \end{aligned}$$

und

$$Q(x, x') = x_1 x'_1 + x_2 x'_2 - x_3 x'_3.$$

Nun ist $x_1 x'_1 + x_2 x'_2$ das innere Produkt zwischen (x_1, x_2) und (x'_1, x'_2); dieses ist wiederum

$$\sqrt{x_1^2 + x_2^2} \cdot \sqrt{x'^2_1 + x'^2_2} \cdot \cos\theta,$$

wobei θ der Winkel zwischen (x_1, x_2) und (x'_1, x'_2) sei. Dies ist

$$\sqrt{x_3^2 - 1} \cdot \sqrt{x'^2_3 - 1} \cdot \cos\theta.$$

Deswegen hat man

$$Q(x, x') = \sqrt{x_3^2 - 1} \cdot \sqrt{x'^2_3 - 1} \cdot \cos\theta - x_3 x'_3.$$

Dieser Ausdruck hat einen negativen Wert. Daher hat $-Q(x, x')$ den größten Wert, wenn $\cos\theta = -1$ gesetzt wird; es folgt

$$-Q(x, x') \leq x_3 x'_3 + \sqrt{x_3^2 - 1}\sqrt{x'^2_3 - 1}$$

mit Gleichheit, wenn $\theta = \pi$ zutrifft. Geometrisch bedeutet das, dass $\underline{x}, \underline{x}'$ auf einen durch die x_3-Achse laufende Ebene liegen. Es folgt

$$-Q(x, x') \leq Q(x, x_0)Q(x', x_0) + \sqrt{\big(Q(x, x_0)\big)^2 - 1}\sqrt{\big(Q(x', x_0)\big)^2 - 1}.$$

Wir schreiben nun

$$-Q(x, x') = \cosh d(x, x').$$

Da

$$-Q(x, x') \geq 1,$$

folgt

$$\begin{aligned} d(x, x') &\geq 0 \\ d(x, x') &= 0 \end{aligned}$$

dann, und nur dann, wenn $x = x'$ ist.

Die obige Ungleichung wird

$$\begin{aligned}\cosh d(x,x') &\leq \cosh d(x,x_0)\cosh d(x',x_0) + \sqrt{\cosh^2 d(x,x_0)-1}\sqrt{\cosh^2 d(x',x_0)-1}\\ &= \cosh d(x,x_0)\cosh d(x',x_0) + \sinh d(x,x_0)\sinh d(x',x_0)\\ &= \cosh\Big(d(x,x_0)+d(x',x_0)\Big).\end{aligned}$$

Es folgt:

$$d(x_1,x_3) \leq d(x_1,x_2) + d(x_2,x_3).$$

Wir definieren nun *eine "Gerade"* in Q^+_{-1} als den Schnitt von Q^+_{-1} mit einer durch 0 laufenden Ebene. Die Ebenen bleiben unter $SL_2(\mathbb{R})$ erhalten, weil $SL_2(\mathbb{R})$ auf $\mathbb{R}^3$ durch lineare Abbildungen operiert.

Nun sehen wir

$$d(x,x_3) = d(x_1,x_2) + d(x_2,x_3),$$

dann und nur dann, wenn x_2 auf der Verbindungsstrecke zwischen x_1 und x_3 liegt. Das hatten wir im Spezialfall bewiesen.

Deswegen verhält sich $d(x,y)$ genau wie ein Abstand. Es ist auch möglich, einen Winkel in dieser Geometrie zu definieren; er kann sogar als euklidischer Winkel auf Q^+_{-1} verstanden werden.

In jedem Fall ist Q^+_{-1} eine Geometrie mit allen Eigenschaften, die man sich wünschen könnte, außer dem Parallelenaxiom.

Sei nun Π die durch $x_3 = 1$ definierte Ebene. Wir projezieren Q^+_{-1} auf Π;

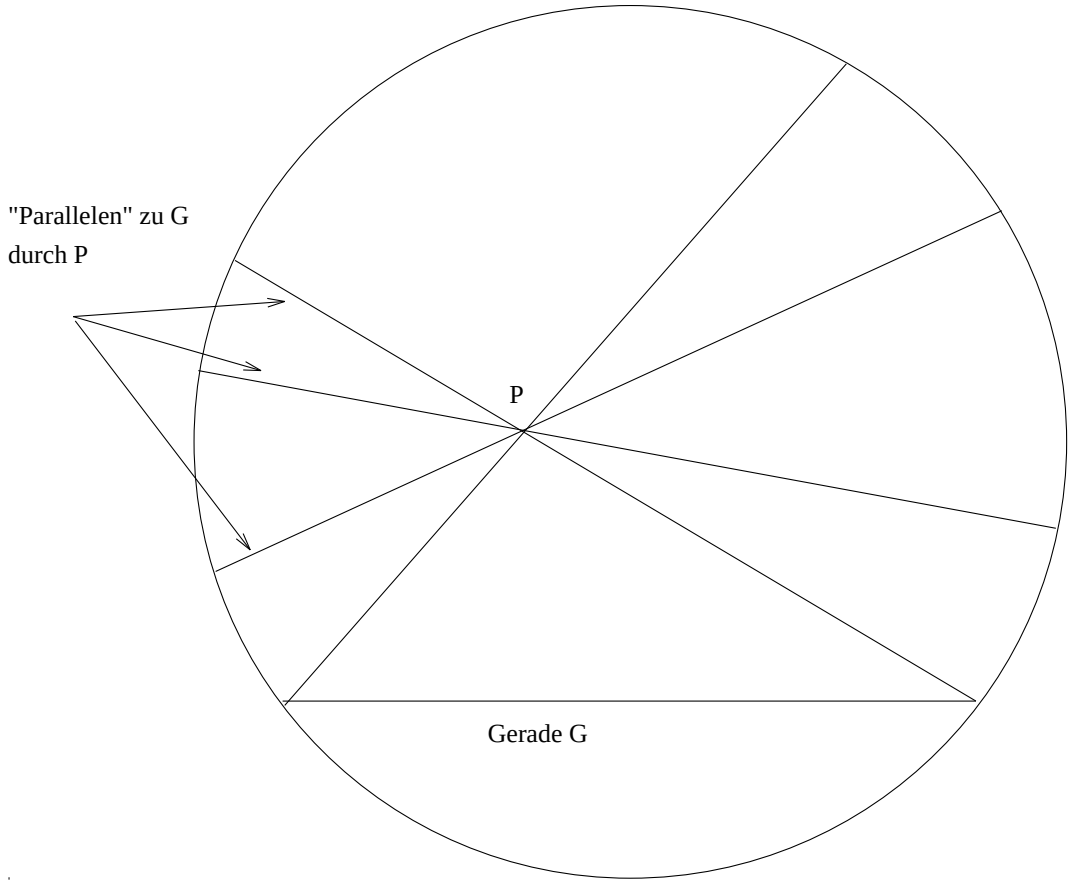
$$(x_1,x_2,x_3) \longmapsto \left(\frac{x_1}{x_3},\frac{x_2}{x_3},1\right).$$

Das Bild ist

$$\Big\{(y_1,y_2,1) : y_1^2+y_2^2<1\Big\},$$

also eine Kreisscheibe. Die Geometrie hat diese *Kreisscheibe* als Modell. Die Geraden sind die Schnitte von dieser Kreisscheibe mit durch 0 laufenden Ebenen, ebenso bestimmen die Geraden Punkte. Es ist ungewöhnlich, dass $SL_2(\mathbb{R})$ auf der Kreisscheibe und den Geraden operiert. Eine Formel kann angegeben werden; sie ist aber nicht sehr einleuchtend. Es ist auch nicht besonders einleuchtend, die Formel für den Abstand d in diesem Modell zu definieren. Wichtig ist aber die Existenz der Operation von $SL_2(\mathbb{R})$ und von d.

Kleinsches Modell der hyperbolischen Geometrie



Man bemerke hier, dass die Stabilisatorgruppe eines Punktes dieselbe Gruppe ist, die in der euklidischen Geometrie auftritt.

In diesem Modell, welches man F. Klein verdankt, ist es klar, dass es unendlich viele "Parallelen" durch einen gegebenen Punkt zu einer gegebenen Geraden, die den Punkt nicht enthält, gibt, da sich diese Geraden im endlichen nicht schneiden (siehe Bild).

Mit dieser Geometrie, die durch eine strenge Herleitung aus einem Axiomensystem von Lobatschewskij ca. 1835 zuerst entdeckt worden ist, erfährt man, dass das Parallelaxiom keine Konsequenz der anderen Axiome der euklidischen Geometrie ist.

Index