Skript zur Vorlesung

Lineare Algebra 2 (4std.)

Sommersemester 2026

Prof. Dr. Martin Möller

Frankfurt am Main, 8. Juli 2026

Inhaltsverzeichnis

1 Skalarprodukte 2
1.1 Euklidische Vektorräume 2
1.2 Unitäre Vektorräume 3
1.3 Matrixdarstellung eines Skalarprodukts 4
1.4 Normierte Vektorräume 5
1.5 Winkel und Orthogonalität 8
1.6 Orthogonales Komplement 10
1.7 Ein Definitheitskriterium 12
1.8 Nichtausgeartete Bilinearformen 13
2 Orthogonale, unitäre und normale Abbildungen 15
2.1 Die adjungierte Abbildung 15
2.2 Normale Endomorphismen, Isometrien 17
2.3 Normalformen im unitären Fall 20
2.4 Normalformen im euklidischen Fall 22
3 Affine Räume 30
3.1 Affine Unterräume 31
3.2 Etwas ebene affine Geometrie 34
3.3 Affine Abbildungen 35
4 Euklidische affine Räume 39
4.1 Bewegungen 41
5 Axiomatische Geometrie 45
6 Projektive Räume 54
6.1 Projektive Unterräume 55
6.2 Projektive Vervollständigung von affinen Räumen 58
6.3 Projektive Abbildungen 61
7 Gruppen und Untergruppen 66
7.1 Ordnung von Elementen und Untergruppen 67
7.2 Untergruppen und Erzeuger 68
7.3 Gruppenhomomorphismen und der Homomorphiesatz 70
7.4 Semidirekte Produkte 73
8 Gruppenoperationen 75
8.1 Die Bahnbilanz 77

8.2 Zentrum, Zentralisator, Normalisator 80
8.3 Fixpunktaussagen und Gruppen mit wenig Primteilern 82
9 Etwas Ringtheorie 84
9.1 Ideale 84
9.2 Hauptidealringe 86
Literatur 93

Einleitung

Die Vorlesung "Lineare Algebra 2" baut auf der Vorlesung "Lineare Algebra 1" auf und setzt den Inhalt des Skripts [LA1] voraus. Sie besteht aus zwei Teilgebieten.

Der erste Teil der Vorlesung behandelt Geometrie. Darin werde wir wichtige Begriffe der Geometrie kennenlernen, wie z.B. Parallelität, Schneiden, Abstand, Winkel. Insbesondere die letztgenannten Begriffe setzen voraus, dass wir in den Räumen messen können und deswegen startet die Vorlesung mit Skalarprodukten auf Vektorräumen und dem daraus resultierenden Normbegriff. Anschließend werden wir den Begriff der "affine Geometrieäbstrahieren und etwas abstrakte Geometrie behandeln, in der Begriffe wie "schneiden" und "parallel" axiomatisch behandelt werden. Die Tatsache, dass Parallelen sich nicht schneiden ist ein Defekt, der in der "projektiven Geometrie" behoben wird.

Der zweite Teil der Vorlesung vertieft die Grundbegriffe der Algebra, Gruppen und Ringe, aus der Vorlesung Lineare Algebra 1. Wir werden insbesondere die Struktur von Untergruppen und Gruppenwirkungen genauer untersuchen, d.h. die Situation dass Gruppen strukturerhaltenden Mengen transformieren.

Wenn diese Mengen Vektorräume oder affine Räume, oder die allgemeinen Geometrien aus dem ersten Teil sind, dann können wir die Konzepte aus beiden Teilen nützlich miteinander kombinieren.

Dieses Skript wird laufend parallel zur Vorlesung aktualisiert. Prüfen Sie regelmäßig, ob auf der Homepage eine neue Version des Skripts vorliegt.

Im Sommersemester 2026 wurden die folgenden Kapitel des Skripts behandelt: 1. Skalarprodukte, 2. Orthogonale, unitäre und normale Abbildungen, 7. Gruppen und Untergruppen, 8. Gruppenoperationen, 3. Affine Räume (unter Auslassung von Desargues und Pappus, aber mit Strahlensatz). 4. Euklidische affine Räume. 5. Axiomatische Geometrie (Beweise zu Satz 5.10 und Satz 5.12 nur teilweise). 6. Projektive Räume (nur Anriss, von Beginn bis einschließlich Korollar 6.5). 9. Ringtheorie (nicht gefordert für die Klausur im Juli).

Quellen und Literatur: Zahlreiche Bücher, zumeist mit dem Titel „Lineare Algebra", umfassen den ersten Teil dieser Vorlesung, zum Beispiel das Buch von S. Bosch. Ebenso viele Skripten, z.B. Lineare Algebra I von A. Werner (Frankfurt) oder F. Herrlich und S. Kühnlein (Karlsruhe), sowie H.Kuhnle, G.Aumann und K.Schober (Karlsruhe) decken diesen Stoff ab und sind zum größten Teil Grundlage dieses Skripts. Das Kapitel zur projektiven Geometrie basiert auf dem fünften Kapitel des Lehrbuchs „Geometry" von Michèle Audin.

1 Skalarprodukte

Wir wollen Vektorräume mit einem Abstandsbegriff versehen und der Abstand zweier Vektoren soll stets nicht-negativ sein. Dies zwingt uns, $\mathbb{R}-$Vektorräume und $\mathbb{C}-$Vektorräume (leicht) unterschiedlich zu behandeln. Wir schreiben K für einen beliebigen Körper. Sei V ein $K-$Vektorraum. Wir wiederholen den Begriff einer Multilinearform im Spezialfall von zwei Argumenten.

Definition 1.1 *Eine* Bilinearform *über V ist eine Abbildung*

$$F\colon V \times V \longrightarrow K, \quad (v,w) \mapsto F(v,w),$$

die in beiden Argumenten linear ist, d.h. es gilt für alle $v_1, v_2, w_1, w_2 \in V,\ \alpha, \beta \in K$:

$$\begin{aligned} F(\alpha v_1 + \beta v_2, w_1) &= \alpha\, F(v_1, w_1) + \beta\, F(v_2, w_1) \\ F(v_1, \alpha w_1 + \beta w_2) &= \alpha\, F(v_1, w_1) + \beta\, F(v_1, w_2). \end{aligned}$$

Die Bilinearform heißt symmetrisch, *falls für alle $v, w \in V$ gilt: $F(v,w) = F(w,v)$.*

1.1 Euklidische Vektorräume

Wir nennen eine Bilinearform F *positiv definit*, wenn $F(v,v) > 0$ für alle $v \in V \setminus \{0\}$ gilt. Für $K = \mathbb{R}$ ist dies die gewünschte Zusatzeigenschaft, die Geometrie auf dem $\mathbb{R}-$Vektorraum möglich macht.

Definition 1.2 *Eine positiv definite, symmetrische Bilinearform F auf dem $\mathbb{R}-$Vektorraum V heißt* Skalarprodukt. *Das Paar (V,F) wird* euklidischer Vektorraum *genannt.*

Beispiel 1.3 Das erste der Beispiele, die Abbildung F_0 wird *Standardskalarprodukt* genannt.

i) Auf $V = \mathbb{R}^n$ ist

$$\begin{aligned} F_0\colon \mathbb{R}^n \times \mathbb{R}^n &\longrightarrow \mathbb{R} \\ \big((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)\big) &\longmapsto \sum_{j=1}^{n} \alpha_j \beta_j \end{aligned}$$

ein Skalarprodukt: Bilinearität und Symmetrie prüfe der Leser direkt nach. Zur positiven Definitheit zeigt man zuerst, dass für alle $v = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$

$$F_0(v,v) = \sum_{j=1}^{n} \alpha_j^2 \geq 0$$

gilt und dass $\sum_{j=1}^{n} \alpha_j^2 = 0$ genau dann, wenn $\alpha_1 = \ldots = \alpha_n = 0$ ist, also wenn $v = 0$ ist.

ii) Die Abbildung $F_1 \colon \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$ gegeben durch

$$\big((\alpha_1,\alpha_2,\alpha_3),(\beta_1,\beta_2,\beta_3)\big) \mapsto \alpha_1\beta_1 + 2\alpha_2\beta_2 - \alpha_2\beta_3 - \alpha_3\beta_2 + \alpha_3\beta_3,$$

ist ebenfalls ein Skalarprodukt, denn es gilt $F_1(v,v) = \alpha_1^2+\alpha_2^2+(\alpha_2-\alpha_3)^2$ für beliebiges $v = (\alpha_1,\alpha_2,\alpha_3)$.

iii) Die Abbildung $F_2 \colon \mathbb{R}^2\times\mathbb{R}^2 \longrightarrow \mathbb{R}$, $\big((\alpha_1,\alpha_2),(\beta_1,\beta_2)\big) \longrightarrow \alpha_1\beta_1$ ist eine symmetrische Bilinearform, aber kein Skalarprodukt, denn $F_2\big((0,1),(0,1)\big) = 0$.

1.2 Unitäre Vektorräume

Auch für einen $\mathbb{C}-$Vektorraum könnte man nach positiv definiten, symmetrischen Bilinearformen suchen. Das Problem ist nur, dass es einfach keine gibt, wenn der Vektorraum V nicht der Nullraum ist. Denn angenommen, F sei positiv definit und linear und $v \in V$, so ist

$$F(ia,ia) = i^2F(a,a) = -F(a,a)$$

und es können nicht $F(a,a)$ und $F(ia,ia)$ positiv sein.

Wenn man sich daran erinnert, dass der komplexe Betrag $|z| = \sqrt{z\cdot\overline{z}}$ immer positive ist und unter der Wurzel das Produkt mit der komplex Konjugierten von z multipliziert, ist folgende Definition naheliegend.

Definition 1.4 *Sei V ein $\mathbb{C}-$Vektorraum. Eine* Hermitesche Form *(oder* Sesquilinearform*) ist eine Abbildung*

$$H \colon V \times V \longrightarrow \mathbb{C},\ (v,w) \mapsto H(v,w)$$

mit der Eigenschaft, dass für alle $v_1, v_2, v, w \in V$ und $\lambda_1, \lambda_2 \in \mathbb{C}$ gilt:

$$\begin{aligned} H(\lambda_1v_1 + \lambda_2v_2, w) &= \lambda_1H(v_1,w) + \lambda_2H(v_2,w) \\ H(v,w) &= \overline{H(w,v).} \end{aligned}$$

Unmittelbare Konsequenz aus der Definition sind die Eigenschaften

$$H(v,v) \in \mathbb{R} \quad \text{und} \quad H(v,\mu_1w_1+\mu_2w_2) = \overline{\mu_1}H(v,w_1) + \overline{\mu_2}H(v,w_2)$$

für alle $v, w_1, w_2 \in V$ und alle $\mu_1, \mu_2 \in \mathbb{C}$. Wir rechnen die zweite Eigenschaft nach:

$$\begin{aligned} H(v,\mu_1w_1+\mu_2w_2) &= \overline{H(\mu_1w_1+\mu_2w_2,v)} \ = \ \overline{\mu_1}\overline{H(w_1,v)} + \overline{\mu_2}\overline{H(w_2,v)} \\ &= \overline{\mu_1}H(v,w_1) + \overline{\mu_2}H(v,w_2). \end{aligned}$$

Definition 1.5 *Analog zum reellen Fall heißt eine Hermitesche Form* positiv definit, *falls für alle* $v \in V\backslash\{0\}$ *gilt* $H(v,v) > 0$.*Ein* Skalarprodukt *auf einem* $\mathbb{C}-$*Vektorraum* V *ist eine positiv definite Hermitesche Form* H*. Das Paar* (V,H) *wird* unitärer Vektorraum *genannt.*

Beispiel 1.6 Die Abbildung

$$H_0 \colon \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}, \qquad \big((\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n)\big) \mapsto \sum_{j=1}^{n} \alpha_j \cdot \overline{\beta_j}$$

ist ein Skalarprodukt. Wir prüfen nur positive Definitheit und überlassen die Verifikation der Hermite-Eigenschaft dem Leser. Es ist

$$H_0\big((\alpha_1,\ldots,\alpha_n),(\alpha_1,\ldots,\alpha_n)\big) = \sum_{j=1}^{n} \alpha_j \cdot \overline{\alpha_j} = \sum_{j=1}^{n} |\alpha_j|^2 > 0.$$

für alle $(\alpha_1,\ldots,\alpha_n) \neq (0,\ldots,0)$. Das Skalarprodukt H_0 wird *Standardskalarprodukt* genannt.

Wenn klar ist, welches Skalarprodukt auf V gemeint ist, werden wir oft die Schreibweise $\langle v,w\rangle$ statt $F(v,w)$ bzw. $H(v,w)$ im reellen bzw. im komplexen Fall verwenden.

1.3 Matrixdarstellung eines Skalarprodukts

Sei $B = \{b_1,\ldots,b_n\}$ eine Basis des Vektorraums V. Wir wollen den Wert eines Skalarprodukts $F(v,w)$ bzw. $H(v,w)$ bestimmen, wenn wir nur die Werte $F(b_i,b_j)$ bzw. $H(b_i,b_j)$ kennen. Dies gelingt immer und wir führen dabei die zum Rechnen angenehme Matrixdarstellung ein. Wir behandeln den Fall eines unitären Vektorraums ausführlich. Wir schreiben die Vektoren $v = \sum_{j=1}^{n} \alpha_j b_j$ und $w = \sum_{j=1}^{n} \beta_j b_j$ in ihrer Basisdarstellung und es sei G die Matrix

$$G = (g_{jk})_{j,k=1\ldots n} \quad , \quad g_{jk} = H(b_j,b_k).$$

Dann gilt aufgrund der Hermite-Eigenschaft

$$\begin{aligned} H(v,w) &= \sum_{j,k=1}^{n} \alpha_j g_{jk} \overline{\beta_k} = (\alpha_1,\ldots,\alpha_n) \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{n1} & \cdots & g_{nn} \end{pmatrix} \begin{pmatrix} \overline{\beta_1} \\ \vdots \\ \overline{\beta_n} \end{pmatrix} \\ &= (\overrightarrow{v})^{\top} G\, \overline{w}, \end{aligned}$$

wobei $\overrightarrow{v} := \overrightarrow{v_B} := (\alpha_1,\ldots,\alpha_n)^T$ und $\overrightarrow{w} := \overrightarrow{w_B} := (\beta_1,\ldots,\beta_n)^T$ den Koordinatenvektor von v bzw. w in der Basis B bezeichnet.

Definition 1.7 *Für eine Matrix* $\mathbb{A} \in \mathbb{C}^{n\times n}$ *sei* $A^* = \overline{A}^{\top}$ *die konjugiert transponierte Matrix. Eine Matrix mit der Eigenschaft* $A^* = A$ *wird* hermitesch *genannt, eine Matrix mit der Eigenschaft* $A^{\top} = A$ *wird* symmetrisch *genannt.*

Wir fassen also zusammen: Die Matrix $G = (g_{jk})$ mit Einträgen $g_{jk} = H(b_j, b_k)$ im unitären Fall bzw. $g_{jk} = F(b_j, b_k)$ im reellen Fall wird *Fundamentalmatrix* des Skalarprodukts in der Basis B genannt. Sie ist hermitesch bzw. symmetrisch (Übungsaufgabe!).

Schließlich untersuchen wir das Verhalten der Fundamentalmatrix $G = G_B$ unter Basiswechsel. Sei $C = \{c_1, \ldots, c_n\}$ eine weitere Basis, die aus B durch

$$\begin{array}{rcccc} c_1 & = & \lambda_{11}b_1+ & \cdots & +\lambda_{n1}b_n \\ \vdots & & \vdots & & \vdots \\ c_n & = & \lambda_{1n}b_1+ & \cdots & +\lambda_{nn}b_n \end{array}$$

hervorgeht. Die Transformationsmatrix

$$\theta_{C,B} = \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1n} \\ \vdots & & \vdots \\ \lambda_{n1} & \cdots & \lambda_{nn} \end{pmatrix},$$

in deren Spalten (!) die Koeffizienten von c_i in der Basis B stehen, führt den Koordinatenvektor $\overrightarrow{v_C}$ von v in der Basis C in den Koordinatenvektor $\overrightarrow{v_B}$ von v in der Basis B über.
(Man überprüft leicht die Richtigkeit des Verfahrens, indem man die Wirkung auf die Koordinateneinheitsvektoren in der Basis C verifiziert.) Sei G_C die Fundamentalmatrix von H in der Basis C, d.h. $G_C = (a_{ij})_{i,j=1\ldots n}$ mit $a_{ij} = H(c_i, c_j)$. Dann gilt

$$\begin{aligned} a_{ij} &= H(c_i, c_j) = H\big(\sum_{s=1}^{n} \lambda_{si} \cdot b_s, \sum_{t=1}^{n} \lambda_{tj} b_t\big) \\ &= \sum_{s,t=1}^{n} \lambda_{si}\overline{\lambda_{tj}} H(b_s, b_t) = \sum_{s,t=1}^{n} \lambda_{si} \cdot g_{st} \cdot \overline{\lambda_{tj}}, \end{aligned}$$

also

$$G_C = \theta_{C,B}^{\top}\, G\, \overline{\theta_{C,B}}. \tag{1.1}$$

Der Leser prüft im Fall eines euklidischen Vektorraums (V, F) die entsprechende Beziehung

$$G_C = \theta_{C,B}^{\top}\, G\, \theta_{C,B}$$

leicht selbst nach.

1.4 Normierte Vektorräume

In diesem Abschnitt wollen wir euklidische und unitäre Vektorräume parallel behandeln. Wir sprechen, beide Fälle zusammenfassend, von einem *metrischen Vektorraum* V mit Skalarprodukt $\langle \cdot, \cdot \rangle$. Wir führen zunächst den Begriff einer Norm ein und leiten daraus später einen Abstandsbegriff (eine Metrik) ab — woraus sich die Bezeichnung rechtfertigt. Wir schreiben K für den Körper, um beide Fälle $K = \mathbb{R}$ und $K = \mathbb{C}$ gemeinsam zu behandeln.

Definition 1.8 *Sei V ein metrischer Vektorraum. Dann heißt*

$$\|v\| = \sqrt{\langle v, v\rangle}$$

die Norm *des Vektors $v \in V$.*

Hierbei verwenden wir stets die nicht-negative Wurzel, d.h. $\|v\| \in \mathbb{R}_{\geq 0}$.

Satz 1.9 *(Cauchy-Schwarz-Ungleichung). In einem metrischen Vektorraum V gilt für alle $v, w \in V$ die Abschätzung*

$$|\langle v, w\rangle| \leq \|v\| \cdot \|w\|.$$

Es gilt Gleichheit genau dann, wenn v und w linear abhängig sind.

Beweis : Wir nehmen an, dass V ein unitärer Vektorraum ist, und überlassen dem Leser die Anpassung an den Fall des euklidischen Vektorraums.
Ist $v = 0$, so gilt offenbar Gleichheit. Sind v, w linear abhängig und $v \neq 0$, so gibt es $\lambda \in \mathbb{C}$ mit $w = \lambda \cdot v$, also ist $\langle v, w\rangle = \overline{\lambda}\langle v, v\rangle$ und $\overline{\langle v, w\rangle} = \lambda\overline{\langle v, v\rangle} = \lambda\langle v, v\rangle$. Zusammen multipliziert erhält man also

$$|\langle v, w\rangle|^2 = \langle v, w\rangle\overline{\langle v, w\rangle} = \lambda\overline{\lambda}\|v\|^2 \cdot \langle v, v\rangle = \|v\|^2\|w\|^2$$

und durch Quadratwurzelziehen die Gleichheit in der Cauchy-Schwarz-Ungleichung.
Sind v, w linear unabhängig, so ist $v - \lambda w \neq 0$ für alle $\lambda \in \mathbb{C}$ und $\langle w, w\rangle > 0$, da $w \neq 0$. Also

$$0 < \langle v - \lambda w, v - \lambda w\rangle = \langle v, v\rangle - \lambda\langle w, v\rangle - \overline{\lambda}\langle v, w\rangle + \lambda\overline{\lambda}\langle w, w\rangle.$$

Nimmt man speziell $\lambda = \frac{\langle v,w\rangle}{\langle w,w\rangle}$, so erhält man

$$0 < \langle v, v\rangle - \frac{\langle v, w\rangle\overline{\langle v, w\rangle}}{\langle w, w\rangle} - \frac{\overline{\langle v, w\rangle}\langle v, w\rangle}{\langle w, w\rangle} + \frac{\langle v, w\rangle\overline{\langle v, w\rangle}}{\langle w, w\rangle^2}\langle w, w\rangle.$$

Durchmultiplizieren mit $\langle w, w\rangle$ ergibt

$$0 < \langle v, v\rangle \cdot \langle w, w\rangle - \langle v, w\rangle\overline{\langle v, w\rangle} = \|v\|^2 \cdot \|w\|^2 - |\langle v, w\rangle|^2$$

und damit die Behauptung. □

Wir halten nun einige Eigenschaften der Norm fest, die sich aus den Eigenschaften eines Skalarprodukts ergeben.

Proposition 1.10 *Für alle $v, w \in V$ und $\lambda \in K$ gilt*

(Definitheit)	$\|v\| \geq 0 \quad$ und $\quad \|v\| = 0 \Leftrightarrow v = 0,$
(Homogenität)	$\|\lambda v\| = \|\lambda\| \cdot \|v\|,$
(Dreiecksungleichung)	$\|v + w\| \leq \|v\| + \|w\|.$

Beweis : Die erste Bedingung folgt aus der positiven Definitheit. Die Homogenität folgt aus

$$\|\lambda v\| = \sqrt{\langle \lambda v, \lambda v\rangle} = \sqrt{\lambda\overline{\lambda}\langle v, v\rangle} = \sqrt{|\lambda|^2 \|v\|^2} = |\lambda| \cdot \|v\|.$$

Für die Dreiecksungleichung berechnen wir

$$\begin{aligned}\|v+w\|^2 &= \langle v+w, v+w\rangle \\ &= \|v\|^2 + \langle v, w\rangle + \langle w, v\rangle + \|w\|^2 \\ &= \|v\|^2 + \langle v, w\rangle + \overline{\langle v, w\rangle} + \|w\|^2 \\ &= \|v\|^2 + 2\,\mathrm{Re}(\langle v, w\rangle) + \|w\|^2.\end{aligned}$$

Setzen wir $\langle v, w\rangle = \alpha + i\beta$ mit $\alpha, \beta \in \mathbb{R}$, so ist

$$\mathrm{Re}(\langle v, w\rangle) = \alpha \leqslant \sqrt{\alpha^2 + \beta^2} = |\langle v, w\rangle|\,.$$

Nach Einsetzen erhalten wir die gewünschte Ungleichung durch

$$\begin{aligned}\|v+w\|^2 &\leqslant \|v\|^2 + 2\,|\langle v, w\rangle| + \|w\|^2 \\ &\leqslant \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 = (\|v\| + \|w\|)^2\,.\end{aligned}$$

mit Hilfe der Cauchy-Schwarz-Ungleichung. □

Definition 1.11 *Sei V ein reeller oder komplexer Vektorraum. Eine Abbildung*

$$\|\cdot\| : V \longrightarrow \mathbb{R}, \quad v \longmapsto \|v\|,$$

welche die Axiome von Proposition 1.10, also Definitheit, Homogenität und Dreiecksungleichung erfüllt, heißt Norm. *Dann heißt das Paar $(V, \|\cdot\|)$ ein* normierter Vektorraum.

Jeder euklidsche oder unitäre Vektorraum ist also auch ein normierter Vektorraum. Wir untersuchen die Umkehrung. Jede Norm, die von einem Skalarprodukt herkommt, erfüllt die Parallelogrammidentität

$$\|v+w\|^2 + \|v-w\|^2 = 2\|v\|^2 + 2\|w\|^2,$$

denn

$$\begin{aligned}&\langle v+w, v+w\rangle + \langle v-w, v-w\rangle = \\ &= \langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle + \langle w, w\rangle + \langle v, v\rangle - \langle v, w\rangle - \langle w, v\rangle + \langle w, w\rangle \\ &= 2\langle v, v\rangle + 2\langle w, w\rangle.\end{aligned}$$

Proposition 1.12 *Auf einem normierten Vektorraum V gibt es ein Skalarprodukt $\langle\ ,\ \rangle$ mit $\|v\| = \sqrt{\langle v, v\rangle}$ genau dann, wenn die Norm die Parallelogrammidentität erfüllt. In diesem Fall ist das Skalarprodukt gegeben durch*

$$\langle v, w\rangle = \frac{1}{4}(\|v + w\|^2 - \|v - w\|^2)$$

im reellen Fall bzw. durch

$$\langle v, w\rangle = \frac{1}{4}(\|v + w\|^2 - \|v - w\|^2) + \frac{i}{4}(\|v + iw\|^2 - \|v - iw\|^2)$$

im komplexen Fall.

Beweis : Übungsaufgabe □

1.5 Winkel und Orthogonalität

Nehmen wir an $V = \mathbb{R}^n$ und zwei Vektoren v, w seien durch „Pfeile“ („Richtungsvektoren“) im Nullpunkt beginnend repräsentiert. Der geometrischen Figur, ein Winkel mit Schenkeln v und w, wollen wir eine Zahl zuordnen. Diese bezeichnen wir auch mit Winkel, (obwohl vielleicht „Winkelmaß“ zur Unterscheidung der Begriffe genauer wäre). Aufgrund der Cauchy-Schwarz-Ungleichung ist

$$-1 \leqslant \frac{\langle v, w\rangle}{\|v\| \cdot \|w\|} \leqslant 1$$

und aus der Analysis ist bekannt, dass

$$\begin{array}{rccc} & [0, \pi] & \longmapsto & [-1, 1] \\ \cos: & \alpha & \longmapsto & \cos(\alpha) \end{array}$$

bijektiv und streng monoton fallend. Also ist folgender Begriff wohldefiniert:

Definition 1.13 *Sei V euklidischer Vektorraum und $v, w \in V \setminus \{o\}$. Die Zahl $\alpha \in [o, \pi]$ mit*

$$\cos\alpha = \frac{\langle v, w\rangle}{\|v\| \cdot \|w\|}$$

heißt Winkel *zwischen den Vektoren v und w. Wir schreiben auch $\alpha = \omega(v, w)$ für den Winkel.*

Bei diesem Zugang wirkt (und ist) die Skalierung des Winkels mit $\cos(\cdot)$ willkürlich. Man hätte alle Informationen über die geometrische Figur „Winkel“ auch durch das Wissen von $\frac{\langle v,w\rangle}{\|v\|\cdot\|w\|}$. Hingegen ist „Null“ in jedem Körper ein ausgezeichnetes Element. Wir geben daher dem Fall des Skalarprodukts $\langle v, w\rangle = 0$ (d.h. des Winkels $\omega(v, w) = \pi/2$) gesondert einen Namen.

Definition 1.14 *Sei V ein metrischer Vektorraum. Zwei Vektoren $v, w \in V$ mit $\langle v, w\rangle = 0$ heißen* orthogonal.

Orthogonale Vektoren sind nützlich zum effizienten Ausrechnen von Skalarprodukten. Wir beschreiben daher im Folgenden ein Verfahren, das aus einer beliebigen Basis eine Basis mit paarweise orthogonalen Vektoren erstellt.

Definition 1.15 *Eine Menge $M \subseteq V$ eines metrischen Vektorraums heißt* Orthogonalsystem, *falls $M \neq \emptyset$, falls $0 \notin M$ und falls $\langle v, w\rangle = 0$ für alle $v \neq w \in M$ gilt. Ist M zudem eine Basis von V, so heißt M* Orthogonalbasis. *Gilt zudem $\|v\| = 1$ für alle $v \in M$, so sprechen wir von einem* Orthonormalsystem *bzw. falls es sich um eine Basis handelt um eine* Orthonormalbasis.

Satz 1.16 (Gram-Schmidt) *Sei V ein metrischer Vektorraum. Jedes Orthogonalsystem M von V ist linear unabhängig. Zu jeder Basis $B = \{b_1, \ldots, b_n\}$ von V gibt es eine Orthogonalbasis $\{c_1, \ldots, c_n\}$ mit*

$$[c_1, \ldots, c_r] = [b_1, \ldots, b_r] \quad \textit{für alle} \quad r = 1, \ldots, n.$$

Beweis : Für die erste Aussage nehmen wir an, es gäbe $\{v_1, \ldots, v_k\} \subseteq M$ und $\alpha_i \in K$ mit $\sum_{i=1}^k \alpha_i v_i = 0$. Dann ist $\langle \sum_{i=1}^k \alpha_i v_i, v_j\rangle = 0$ für alle j, also $\alpha_i \langle v_i, v_j\rangle = 0$. Wegen der positiven Definitheit des Skalarprodukts folgt $\alpha_j = 0$ für alle $j = 1, \ldots, k$.
Die zweite Aussage beweisen wir durch Induktion nach r. Für $r = 1$ nehmen wir $c_1 = b_1$. Zum Induktionsschritt setzen wir voraus, dass $c_1, \ldots, c_{r-1}$ bereits die geforderte Eigenschaft besitzt. Aus dem Ansatz $c_r = b_r + \lambda_1 c_1 + \ldots + \lambda_{r-1} c_{r-1}$ und der Forderung $\langle c_r, c_k\rangle = 0$ für alle $k = 1, \ldots, r-1$ folgt

$$\langle b_r, c_k\rangle + \lambda_k \langle c_k, c_k\rangle = 0$$

Also setzen wir $\lambda_k = -\frac{\langle b_r, c_k\rangle}{\langle c_k, c_k\rangle}$ und somit

$$c_r = b_r - \sum_{k=1}^{r-1} \frac{\langle b_r, c_k\rangle}{\langle c_k, c_k\rangle} \cdot c_k.$$

Damit sind alle Orthogonalbedingungen erfüllt und es gilt $[c_1, \ldots, c_r] = [b_1, \ldots, b_r]$. Zudem ist $c_r \neq 0$, denn sonst wäre $b_r \in [c_1, \ldots, c_{r-1}] = [b_1, \ldots, b_r]$ im Widerspruch zur linearen Unabhängigkeit von B. □

Bemerkung 1.17 Ist $M \subset V$ ein Orthogonalsystem, so ist $N = \{\frac{m}{\|m\|}, m \in M\}$ ein Orthonormalsystem. Auf gleiche Weise erhält man aus einer Orthogonalbasis eine Orthonormalbasis.

Proposition 1.18 *Die Fundamentalmatrix eines Skalarprodukts bezüglich einer Orthonormalbasis ist die Einheitsmatrix. Umgekehrt ist die Fundamentalmatrix eines Skalarprodukts in einer Basis B die Einheitsmatrix, so ist B eine Orthonormalbasis.*

Beweis : B ist Orthonormalbasis genau dann, wenn der Eintrag g_{ij} der Fundamentalmatrix

$$g_{ij} = \langle b_i, b_j \rangle = \delta_{ij}$$

ist, also G_B die Einheitsmatrix ist. □

1.6 Orthogonales Komplement

Zu jedem Untervektorraum W eines Vektorraums V gibt es einen Untervektorraum U, sodass $V = W \oplus U$ ist, wie in [LA1] bewiesen wurde. Der Raum U, genannt ein *Komplement* von W ist keineswegs eindeutig, man kann bei der Konstruktion viele Wahlen treffen. Ein eindeutiges Komplement mit guten Eigenschaften zu haben ist oft nützlich. Dieses gibt es, falls ein Skalarprodukt vorhanden ist. Sei also nun V ein metrischer Vektorraum und W ein Untervektorraum.

Definition 1.19 *Die Menge* $W^\perp = \{v \in V : \langle v, w \rangle = 0 \,\forall\, w \in W\}$ *heißt* orthogonales Komplement *zu* W *in* V.

Der Leser überzeugt sich leicht davon, dass $W^\perp$ ein Untervektorraum von V ist. Wir fassen weitere Eigenschaften, die unmittelbar aus der Definition folgen, zusammen.

Proposition 1.20 *Es ist* $W \cap W^\perp = \{0\}$ *und* $W \subseteq (W^\perp)^\perp$. *Ist* $\dim V = n < \infty$, *so ist* $\dim W^\perp = n - \dim W$ *und es gilt* $W = (W^\perp)^\perp$.

Beweis : Ist $w \in W \cap W^\perp$, so ist $\langle w, w \rangle = 0$, also $w = 0$. Es gilt

$$(W^\perp)^\perp = \{v \in V : \forall x \in W^\perp : \langle v, x \rangle = 0\}.$$

Ist also $w \in W$, so ist $\langle w, x \rangle = 0$ für alle $x \in W^\perp$, und daher $w \in (W^\perp)^\perp$. Sei nun $\dim V = n$. Die zweite Aussage der Proposition ist trivialerweise richtig für $W = \{0\}$ oder $W = V$. In den anderen Fällen sei $B_W = \{b_1, \ldots, b_k\}$ eine Basis von W und $B = \{b_1, \ldots, b_n\}$ eine Ergänzung zu einer Basis von V. Das Gram-Schmidt-Verfahren liefert eine Orthogonalbasis $C = \{c_1, \ldots, c_n\}$ von V, derart, dass

$$[c_1, \ldots, c_k] = [b_1, \ldots, b_k] = W$$

ist. Offenbar ist $W^\perp \supseteq [c_{k+1}, \ldots, c_n]$. Ist $x = \sum_{i=1}^{n} \lambda_i c_i$ ein beliebiges Element von $W^\perp$, so ist für $j = 1, \ldots, k$

$$0 = \langle x, c_j \rangle = \Big\langle \sum_{i=1}^{n} \lambda_i c_i, c_j \Big\rangle = \lambda_j \langle c_j, c_j \rangle,$$

also $\lambda_j = 0$. Daraus folgt $W^\perp = [c_{k+1}, \ldots, c_n]$. Mit dem gleichen Argument folgt nun

$$(W^\perp)^\perp = [c_1, \ldots, c_k] = W$$

und auch die Dimensionsaussage. □

Der Beweis dieser Proposition gibt eine Strategie dafür, wie man das orthogonale Komplement in der Praxis findet. Wir illustrieren an einem Beispiel:

Beispiel 1.21 Sei $V = \mathbb{R}^3, W = \left[\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right]$. Diese Basis wird durch $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ zu einer Basis von V ergänzt. Nach Gram-Schmidt ist $\left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 1 \\ -1/2 \end{pmatrix} \right\}$ eine Orthogonalbasis von W und

$$c_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} - \frac{1}{3} \begin{pmatrix} 1/2 \\ 1 \\ -1/2 \end{pmatrix} = \begin{pmatrix} 1/3 \\ -1/3 \\ -1/3 \end{pmatrix}.$$

Also ist $W^\perp = [c_3]$.

Wir betrachten weiterhin die Situation $\dim V = n$. Dann ist $V = W \oplus W^\perp$. Oftmals ist es nützlich einen beliebigen Vektor $v \in V$ als $v = w + x$ mit $w \in W$ und $x \in W^\perp$ zu schreiben. Insbesondere ist eine solche Summenschreibweise eindeutig. Die Abbildung

$$\pi : \begin{cases} V & = W \oplus W^\perp & \longrightarrow V \\ v & = w + x & \longmapsto w \end{cases}$$

ist linear. Sie wird *orthogonale Projektion* auf W genannt. Wir fassen ihre wesentlichen Eigenschaften zusammen.

Proposition 1.22 *Ist π die orthogonale Projektion auf W, so ist Bild $(\pi) = W$, $\mathrm{Ker}(\pi) = W^\perp$ und $\pi^2 = \pi$. Es gilt $\|\pi(v)\| \leq \|v\|$ und, falls $C_W = \{c_1, \ldots, c_k\}$ eine Orthonormalbasis von W ist, so gilt für alle $v \in V$*

$$\pi(v) = \sum_{j=1}^{k} \langle v, c_j \rangle \cdot c_j.$$

Als Slogan für die zweite Eigenschaft sagt man, dass orthogonale Projektionen *kontrahierend* sind.

Beweis : Die Aussagen über Bild und Kern sind klar. Ist $v \in \text{Bild}(\pi) = W$, so ist $\pi(v) = v$, also ist $\pi^2 = \pi$. Es gilt aufgrund der Orthogonalität

$$\langle v, v \rangle = \langle w + x, w + x \rangle = \langle w, w \rangle + \langle x, x \rangle \geqslant \langle w, w \rangle$$

und daher $\quad \|\pi(v)\| \leqslant \|v\|$.

Für die letzte Aussage ergänzen wir C_W zu einer Orthonormalbasis $C = \{c_1, \ldots, c_n\}$ von ganz V. Ist $v = \sum_{i=1}^n \lambda_i c_i$, so ist $w = \sum_{i=1}^k \lambda_i c_i$ und $x = \sum_{i=k+1}^n \lambda_i c_i$. Es gilt $\langle v, c_j \rangle = \lambda_j$ und daher $\pi(v) = w = \sum_{j=1}^k \langle v, c_j \rangle \cdot c_j$. □

1.7 Ein Definitheitskriterium

Sei $G = G_B$ die Fundamentalmatrix einer symmetrischen Bilinearform bzw. hermitschen Form. Die Eigenschaften symmetrisch oder hermitsch können wir $G \in \mathrm{Mat}(n,n)$ schnell ansehen. Gesucht ist ein einfaches Kriterium, das entscheidet, ob die Form, die G darstellt, positiv definit ist. Dies ist offenbar äquivalent dazu, dass $v^\top G\,\overline{v} > 0$ für alle $v \in \mathbb{R}^n \setminus \{0\}$ ist. Wir nennen eine solche Matrix *positiv definit*.

Lemma 1.23 *Ist G positiv definit, so ist $\det G$ reell und positiv.*

Beweis : Nach dem Satz von Gram-Schmidt besitzt V eine Orthonormalbasis C. Bezüglich dieser ist die Fundamentalmatrix G_C die Einheitsmatrix. Wir hatten in (1.1) die Basiswechseleigenschaft

$$G_C = \theta_{C,B}^\top G_B \overline{\theta_{C,B}}$$

gezeigt. Also gilt

$$1 = \det G_C = \det \theta_{C,B}^\top \cdot \det G_B \cdot \det \overline{\theta_{C,B}} = |\det \theta_{C,B}|^2 \cdot \det G_B.$$

Das Betragsquadrat $|\det \theta_{C,B}|^2$ ist reell und positiv, da $\theta_{C,B}$ als Basiswechselmatrix regulär ist. Daraus folgt die Behauptung. □

Die Umkehrung des Lemmas ist bereits ab Dimension zwei nicht mehr richtig. (Der Leser konstruiere selbst ein Gegenbeispiel). Zur richtigen Formulierung einer Umkehrung benötigen wir die *Hauptunterdeterminanten* (auch *Hauptminoren*) einer Matrix G definiert durch

$$\Delta_k(G) = \det \begin{vmatrix} g_{11} & \cdots & g_{1k} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kk} \end{vmatrix}.$$

Satz 1.24 (Hurwitzsches Definitheitskriterium) *Sei V ein n-dimensionaler K-Vektorraum. Sei $\langle\cdot,\cdot\rangle$ eine symmetrische Bilinearform (falls $K = \mathbb{R}$) oder hermitsche Form (falls $K = \mathbb{C}$) auf V und sei G die Fundamentalmatrix bzgl. einer Basis $B = \{b_1, \ldots, b_n\}$. Dann ist G positiv definit (und damit $\langle\cdot,\cdot\rangle$ ein Skalarprodukt) genau dann, wenn alle Hauptminoren Δ_k von G positiv sind.*

Beweis : Sei G positiv definit. Dann ist die Einschränkung von $\langle\cdot,\cdot\rangle$ auf $W = [b_1, \ldots, b_k]$ für $k \in \{1, \ldots, n\}$ ein Skalarprodukt auf W. Insbesondere ist die Fundamentalmatrix dieser Einschränkung

$$G|_W = \begin{pmatrix} g_{11} & \cdots & g_{1k} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kk} \end{pmatrix}$$

positiv definit. Nach dem Lemma ist $\det(G|_W) = \Delta_k > 0$. Dies beweist die erste Implikation. Die Umkehrung beweisen wir durch Induktion nach n. Für $n = 1$ ist $G = (g_{11})$ mit $g_{11} > 0$. Also ist für alle $v = (v_1) \in V \setminus \{0\}$ das Skalarprodukt $\langle v, v\rangle = (v_1)^\top G(\overline{v_1}) = |v_1|^2 \cdot g_{11} > 0$.
Wir nehmen nun an, dass für alle $(n-1)$-dimensionalen Vektorräume und für jede Basiswahl darin die Aussage richtig ist.
Wir wenden dies auf $W = [b_1, \ldots, b_{n-1}]$ an. Die Fundamentalmatrix der Einschränkung von $\langle\cdot,\cdot\rangle$ auf W ist $G|_W = (\langle b_i, b_j\rangle)_{i,j=1,\ldots,n-1}$. Die Hauptminoren dieser Matrix sind die ersten $n-1$ Hauptminoren von G, also positiv. Also ist $\langle\cdot,\cdot\rangle|_W$ ein Skalarprodukt. Nach Gram-Schmidt gibt es eine Orthonormalbasis $C_W = \{c_1, \ldots, c_{n-1}\}$ von W und bezüglich dieser ist die Fundamentalmatrix die Einheitsmatrix.

In Analogie zu Gram-Schmidt setzen wir

$$c_n = b_n - \sum_{j=1}^{n-1} \langle b_n, c_j\rangle \cdot c_j.$$

Dann ist $C = \{c_1, \ldots, c_n\}$ eine Basis von V, denn andernfalls wäre $c_n \in W$ und dann $[b_1, \ldots, b_n] = [b_1, \ldots, b_{n-1}] = W$, im Widerspruch zur Basiseigenschaft von B. Außerdem ist $\langle c_n, c_j\rangle = \langle b_n, c_j\rangle - \langle b_n, c_j\rangle\langle c_j, c_j\rangle = 0$ für $j < n$. Also ist die Fundamentalmatrix von $\langle\cdot,\cdot\rangle$ bzgl. C gegeben durch

$$G_C = \left(\begin{array}{ccc:c} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \\ \hdashline 0 & \cdots & 0 & \langle c_n, c_n\rangle \end{array}\right).$$

Ist $\theta_{C,B}$ die Basiswechselmatrix, so ist $G_C = \theta_{C,B}^\top G_B \overline{\theta_{C,B}}$, also

$$\langle c_n, c_n\rangle = \det G_C = |\det \theta_{C,B}|^2 \cdot \det G_B > 0$$

nach Voraussetzung und da $\theta_{C,B}$ regulär ist. Schreiben wir nun $0 \neq v = (v_1, \ldots, v_n)^\top$ als Koordinatenvektor in der Basis C, so ist

$$\langle v, v\rangle = |v_1|^2 + \ldots + |v_{n-1}|^2 + \langle c_n, c_n\rangle \cdot |v_n|^2 > 0.$$

□

1.8 Nichtausgeartete Bilinearformen

Vieles aus den vorigen Unterabschnitten kann man auch über anderen Körpern und unter schwächeren Voraussetzungen an die Bilinearform beweisen.

Ab jetzt sei K ein Körper und V ein endlichdimensionaler K-Vektorraum mit symmetrischer Bilinearform $\langle \cdot, \cdot \rangle$.

Sei $W \subseteq V$ ein Untervektorraum. Wir definieren $W^{\perp} := \{v \in V \mid \forall w \in W : \langle v, w \rangle = 0\}$ das orthogonale Komplement von W.

Definition 1.25 *Wir nennen eine symmetrische Bilinearform $\langle \cdot, \cdot \rangle : V \times V \to K$*

- *nichtausgeartet, wenn gilt*

$$\langle x, y \rangle = 0 \text{ für alle } y \in V \Rightarrow x = 0,$$

- *ausgeartet, wenn sie nicht nichtausgeartet ist, und*
- *anisotrop, wenn für alle $v \in V \backslash \{0\}$ gilt, dass $\langle v, v \rangle \neq 0$.*
- *für $K = \mathbb{R}$ positiv-definit (analog. negativ-definit), falls $\langle v, v \rangle > 0$ (analog $\langle v, v \rangle < 0$) für alle $v \in V \backslash \{0\}$.*

Man zeige als Übung:

Proposition 1.26 *i) Es gelten folgende Implikationen*

$$\langle \cdot, \cdot \rangle \text{ ist ein Skalarprodukt} \Rightarrow \langle \cdot, \cdot \rangle \text{ ist anisotrop} \Rightarrow \langle \cdot, \cdot \rangle \text{ ist nichtausgeartet}$$

ii) Sei $K = \mathbb{R}$. Dann ist eine symmetrische Bilinearform anisotrop ist genau dann, wenn Sie entweder positiv oder negativ definit ist.

Aus den vorherigen Unterabschnitten wissen wir, dass es für jeden Unterraum $U \subset V$ gilt, dass $V = U \oplus U^{\perp}$, falls $\langle \cdot, \cdot \rangle$ ein Skalarprodukt ist. Es stellt sich heraus dass die Eigenschaft, die das realisiert genau die Anisotropie ist.

Proposition 1.27 *Eine symmetrische Bilinearform $\langle \cdot, \cdot \rangle$ ist anisotrop, genau dann wenn für beliebigen Unterraum $U \subset V$ gilt, dass $V = U \oplus U^{\perp}$.*

Auch für das Gram-Schmidt-Verfahren reicht schon Anisotropie.

Proposition 1.28 (Gram-Schmidt) *Sei V ein Vektorraum mit anisotroper Bilinearform $\langle \cdot, \cdot \rangle$. Zu jeder Basis $B = \{b_1, ..., b_n\}$ von V gibt es eine Orthogonalbasis $\{c_1, ..., c_n\}$ mit*

$$[c_1, ..., c_r] = [b_1, ..., b_r]$$

für alle $r = 1, ..., n$.

2 Orthogonale, unitäre und normale Abbildungen

Wir untersuchen nun Abbildungen zwischen Vektorräumen mit Skalarprodukt. Wir erinnern daran, dass es im zwischen zwei Vektorräumen viele Abbildungen gibt, da man die Bilder einer Basis beliebig vorschreiben kann. Liegen Skalarprodukte vor, so ist die adjungierte Abbildung eine natürliche Abbildung 'in der umgekehrten Richtung', die mit dem Skalarprodukt verträgtich ist.

2.1 Die adjungierte Abbildung

Sei V, W zwei euklidsche oder zwei unitäre Vektorräume und $f\colon V \longrightarrow W$ eine lineare Abbildung. Wir suchen nach einer Abbildung $f^*\colon W \longrightarrow V$, die (grob gesagt) den Effekt von f auf das Skalarprodukt kompensiert. Genauer:

Definition 2.1 *Die Abbildung $f^*\colon W \longrightarrow V$ heißt* zu f adjungierte Abbildung *(oder kurz:* Adjungierte*), falls für alle $v \in V$ und alle $w \in W$ gilt:*

$$\langle f(v), w\rangle = \langle v, f^*(w)\rangle.$$

Der Spezialfall $W = V$ wird natürlich im Folgenden eine wichtige Rolle spielen. Der Leser möge sich die Definition des Begriffs stets am allgemeinen Fall klarmachen, denn auf der linken Seite der Gleichung steht das Skalarprodukt in W, rechts das in V. Dementsprechend können auch nur Elemente von W bzw. von V in das Skalarprodukt eingesetzt werden. Mit dieser Plausibilitätsprüfung kann man überprüfen, ob man sich in der Definition des Begriffes nicht irrt.

Satz 2.2 *Zu einer linearen Abbildung f gibt es höchstens eine Adjungierte. Ist der Vektorraum V endlichdimensional, so gibt es stets eine Adjungierte.*

Seienx $B = \{b_1, \ldots, b_n\}$ und $C = \{c_1, \ldots, c_p\}$ Orthonormalbasen von V bzw. von W und A die Abbildungs-Matrix von f bzgl. B und C, so ist $A^\top$ (bzw. im unitären Fall A^*) die Abbildungsmatrix von f^* bzgl. der Basen C im Definitionsbereich und B im Bildbereich von f^*.

Beweis : Sind f_1^* und f_2^* zwei Adjungierte zu f, so gibt für alle $v \in V$ und alle $w \in W$

$$\langle f(v), w\rangle = \langle v, f_1^*(w)\rangle = \langle v, f_2^*(w)\rangle,$$

also $\langle v, f_1^*(w) - f_2^*(w)\rangle = 0$. Daraus folgt $f_1^*(w) - f_2^*(w) = 0$ für alle $w \in W$, also $f_1^* = f_2^*$.

Für die zweite Aussage sei $B = \{b_1, \ldots, b_n\}$ eine Orthonormalbasis von V. Wir definieren

$$f^*(w) \;=\; \sum_{j=1}^{n} \langle w, f(b_j)\rangle \cdot b_j\,. \tag{2.1}$$

Offenbar ist f^* linear und es gilt für $v = \sum_{i=1}^{n} \lambda_i b_i$

$$\langle f(v), w\rangle = \sum_{i=1}^{n} \lambda_i \cdot \langle f(b_i), w\rangle.$$

Andererseits berechnen wir

$$\begin{aligned}\langle v, f^*(w)\rangle &= \left\langle \sum_{i=1}^{n} \lambda_i b_i, \sum_{j=1} \langle w, f(b_j)\rangle \cdot b_j \right\rangle \\ &= \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{n} \overline{\langle w, f(b_j)\rangle} \cdot \langle b_i, b_j\rangle \right) \\ &= \sum_{i=1}^{n} \lambda_i \cdot \overline{\langle w, f(b_i)\rangle} = \sum_{i=1}^{n} \lambda_i \langle f(b_i), w\rangle \\ &= \langle f(v), w\rangle\end{aligned}$$

un haben so verifiziert, dass diese Abbildung f^* wirklich die Adjungierte ist.

Für die letzte Aussage des Satzes schreiben wir

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{p1} & \cdots & \alpha_{pn} \end{pmatrix}$$

und daher $f(b_i) = \sum_{k=1}^{p} \alpha_{ki} \cdot c_k$. Die Definition der Adjungierten oben ergibt

$$\begin{aligned}f^*(c_j) &= \sum_{i=1}^{n} \langle c_j, f(b_i)\rangle b_i = \sum_{i=1}^{n} \langle c_j, \sum_{k=1}^{p} \alpha_{ki} \cdot c_k\rangle \cdot b_i \\ &= \sum_{i=1}^{n} \overline{\alpha_{ji}} \cdot b_i\end{aligned}$$

In Matrixschreibweise übertragen, ist das genau die Behauptung. □

Für die Adjungierten gelten folgende Rechenregeln (Übung):

$$(f+g)^* = f^* + g^*, \quad (\lambda f)^* = \overline{\lambda} f^*, \quad (f \circ g)^* = g^* \circ f^* \quad \text{und} \quad f^{**} = f.$$

Proposition 2.3 *Sei $f : V \to W$ linear, so dass die adjungierte Abbildung $f^* : W \to V$ existiert, und $U \subset V$ ein Untervektorraum. Dann gilt*

$$f^*(f(U)^\perp) \subset U^\perp.$$

Beweis : Wir müssen zeigen, dass für alle $w \in f(U)^\perp$ der Vektor $f^*(w)$ orthogonal zu allen $u \in U$ steht. Das folgt direkt aus der Definition der adjungierten Abbildung denn

$$\langle u, f^*(w)\rangle = \langle f(u), w\rangle = 0$$

für $w \in f(U)^\perp$. □

2.2 Normale Endomorphismen, Isometrien

Wir schränken uns von nun an auf den Fall $\dim V < \infty$ ein und untersuchen verschiedene, sukzessive restriktivere Bedingungen auf f und seine Adjungierte f^*. In all diesen Fällen wollen wir eine orthonormale Basis von V suchen, sodass die Abbildungsmatrix von f (und von f^*) eine besonders einfache Gestalt hat.

Definition 2.4

- *Ein Endomorphismus $f\colon V \longrightarrow V$ heißt* normal, *falls $f \circ f^* = f^* \circ f$ gilt.*
- *Ein Endomorphismus $f\colon V \longrightarrow V$ heißt* selbstadjungiert, *falls $f^* = f$ gilt.*
- *Eine lineare Abbildung $f\colon V \longrightarrow W$ heißt* Isometrie, *falls für alle $v \in V$ gilt:*

$$\|f(v)\| = \|v\|.$$

Offenbar sind Isometrien injektiv, denn aus $f(v) = f(w)$ folgt

$$0 = \|f(v) - f(w)\| = \|f(v - w)\| = \|v - w\|$$

und aufgrund der Definitheit folgt $v = w$.

Proposition 2.5 *Eine lineare Abbildung $f\colon V \longrightarrow W$ ist genau dann eine Isometrie, wenn für alle $v_1, v_2 \in V$ gilt*

$$\langle f(v_1), f(v_2)\rangle = \langle v_1, v_2\rangle.$$

Beweis : Für eine Richtung genügt es $v_1 = v_2$ zu setzen. Sei im Fall von euklidischen Vektorräumen umgekehrt f eine Isometrie. Dann ist

$$\begin{aligned}\langle f(v_1 + v_2), f(v_1 + v_2)\rangle &= \langle v_1 + v_2, v_1 + v_2\rangle = \langle v_1, v_1\rangle + 2\langle v_1, v_2\rangle + \langle v_2, v_2\rangle \\ &= \langle f(v_1), f(v_1)\rangle + 2\langle f(v_1), f(v_2)\rangle + \langle f(v_2), f(v_2)\rangle.\end{aligned}$$

Da $\langle f(v_i), f(v_i)\rangle = \langle v_i, v_i\rangle$ für $i = 1, 2$ verbleiben die mittleren Terme in beiden Zeilen und das ist die Behauptung.

Im Fall von unitären Vektorräumen folgt aus dieser Rechnung

$$\mathrm{Re}\langle f(v_1), f(v_2)\rangle \;=\; \mathrm{Re}\langle (v_1), (v_2)\rangle\,.$$

Wendet man die gleiche Rechnung auf $v_1 + iv_2$ an, so folgt auch die Gleichheit der Imaginärteile und somit die Behauptung. □

Unmittelbare Folge hieraus ist, dass eine Isometrie Winkel invariant lässt.

Satz 2.6 *Ist $V = W$, so ist f eine Isometrie genau dann, wenn $f^* \circ f = \mathrm{id}_V$ gilt. Insbesondere ist f normal und $f^* = f^{-1}$.*

Beweis : Ist f Isometrie, so folgt aus dem vorigen Satz für alle $v, w \in V$:

$$\langle v, (f^* \circ f)(w)\rangle = \langle f(v), f(w)\rangle = \langle v, w\rangle,$$

also $\langle v, (f^* \circ f)(w) - w\rangle = 0$ für alle v, w und damit $f^* \circ f = \mathrm{id}_v$. Gilt umgekehrt $f^* \circ f = \mathrm{id}_V$, so ist

$$\langle v, w\rangle = \langle v, (f^* \circ f)(w)\rangle = \langle f(v), f(w)\rangle$$

und damit f eine Isometrie. Die weiteren Behauptungen folgen aus der Injektivität von f und $f^{**} = f$. □

Wir leiten ab sofort die Matrixdarstellungen von f für das allgemeinere Konzept von normalen Endomorphismen her.

Proposition 2.7 *Ist f normal, so gilt für alle $v \in V$:*

$$\|f(v)\| = \|f^*(v)\|.$$

Hat f den Eigenvektor v zum Eigenwert λ, so ist v auch Eigenvektor von f^* zum Eigenwert $\overline{\lambda}$.

Im euklidischen Fall kann auf die komplexe Konjugation in der zweiten Aussage verzichtet werden.

Beweis : Wir berechnen allgemeiner für alle $v, w \in V$:

$$\langle f(v), f(w)\rangle = \langle v, (f^* \circ f)(w)\rangle = \langle v, (f \circ f^*)(w)\rangle = \langle f^*(v), f^*(w)\,,$$

woraus die erste Behauptung ím Spezialfall $v = w$ folgt. Ist f normal, so ist auch $(f - \lambda\mathrm{id})$ normal, denn

$$\begin{aligned}
&(f - \lambda\mathrm{id}) \circ (f - \lambda\mathrm{id})^* = (f - \lambda\mathrm{id}) \circ (f^* - \overline{\lambda}\mathrm{id}) \\
&= f \circ f^* - \lambda f^* - \overline{\lambda} f + \lambda\overline{\lambda}\mathrm{id} = f^* \circ f - \overline{\lambda} f - \lambda f^* + \overline{\lambda}\lambda\mathrm{id} \\
&= (f^* - \overline{\lambda}\mathrm{id}) \circ (f - \lambda\mathrm{id}) = (f - \lambda\mathrm{id})^* \circ (f - \lambda\mathrm{id}).
\end{aligned}$$

Nach der ersten Aussage gilt daher $\|(f - \lambda\mathrm{id})(v)\| = \|(f^* - \overline{\lambda}\mathrm{id})(v)\|$ und daraus folgt die Behauptung. □

Normale Endomorphismen erkennt man oft durch die folgende Charakterisierung.

Korollar 2.8 *Ein Endomorphismus f is normal, genau dann wenn*

$$\langle f(v), f(w)\rangle \;=\; \langle f^*(v), f^*(w)\rangle \tag{2.2}$$

für alle $v, w \in V$ gilt.

Beweis : Eine Implikation haben wir im vorigen Beweis miterledigt. Für die andere nehmen wir (2.2) an. Dann gilt

$$\langle v, f^* \circ f(w)\rangle \;=\; \langle v, f \circ f^*(w)\rangle$$

also $\langle v, f^* \circ f - f \circ f^*(w)\rangle = 0$ für alle $v, w \in V$. Also ist $f^* \circ f - f \circ f^*(w) \in V^\perp = \{0\}$ nach Proposition 1.20 und das ist die Behauptung. □

Korollar 2.9 *Selbstadjungierte Endomorphismen von unitären Vektorräumen haben reelle Eigenwerte.*

Beweis : Ist λ ein Eigenwert eines selbstadjungierten Endomorphismus f eines unitären Vektorraums und v ein dazugehöriger Eigenvektor, so ist v auch Eigenvektor von $f^* = f$ zum Eigenwert $\overline{\lambda}$ nach der vorhergehenden Proposition (man beachte, dass selbstadjungierte Endomorphismen normal sind). Darum muss $\lambda = \overline{\lambda}$ gelten, der Eigenwert λ ist also reell. □

Wir beenden diesen Abschnitt mit den entsprechenden Begriffen für Matrizen.

Definition 2.10 *Eine $(n \times n)$-Matrix A heißt* normal, *falls $A \cdot A^* = A^* \cdot A$ gilt. Sie heißt* unitär, *falls $A \cdot A^* = I_n$ gilt. Ist A reell, so heißt A orthogonal, falls $A \cdot A^\top = I_n$ gilt.*

Satz 2.11 *Ein Endomorphismus ϕ eines euklidischen (bzw. unitären) Vektorraumes ist normal genau dann, wenn die Abbildungsmatrix A von ϕ bzgl. einer Orthonormalbasis normal ist. Ein Endomorphismus ϕ ist eine Isometrie genau dann, wenn A orthogonal (bzw. unitär) ist, und selbstadjungiert genau dann, wenn A symmetrisch (bzw. hermitesch) ist.*

Beweis : Das folgt direkt aus den entsprechenden Definitionen, weil die Adjungierte ϕ^* bzgl. der gewählten Orthonormalbasis durch die Abbildungsmatrix $A^\top$ (bzw. A^*) beschrieben wird. □

2.3 Normalformen im unitären Fall

Beim Beweis von Normalformen behandeln wir den euklidischen und unitären Fall getrennt. Wir führen im nächsten Abschnitt den euklidischen auf den unitären Fall zurück. Sei nun also V endlichdimensional und unitär.

Satz 2.12 *Ein Endomorphismus $f: V \longrightarrow V$ ist normal genau dann, wenn es eine Orthonormalbasis aus Eigenvektoren gibt.*

Beweis : Sei $B = \{b_1, \ldots, b_n\}$ eine Orthonormalbasis aus Eigenvektoren, d.h. $f(b_i) = \lambda_i b_i$. Dann gilt nach der Formel (2.1) für die Adjungierte, dass $f^*(b_i) = \overline{\lambda_i} b_i$. Die Abbildungsmatrizen A und A^* von f und f^* in der Basis B sind also

$$A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \qquad A^* = \begin{pmatrix} \overline{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\lambda_n} \end{pmatrix}$$

und es gilt

$$A \cdot A^* = \begin{pmatrix} |\lambda_1|^2 & & 0 \\ & \ddots & \\ 0 & & |\lambda_n|^2 \end{pmatrix} = A^* \cdot A.$$

Also ist f normal.
Die Umkehrung beweisen wir durch Induktion nach $n = \dim V$. Für $n = 1$ ist jede Basis eine Orthogonalbasis (da nur einelementig) und kann normiert werden. Sie besteht immer aus einem Eigenvektor von f. Die Behauptung gelte nun für alle $(n-1)$-dimensionalen Vektorräume. Da wir über $\mathbb{C}$ arbeiten, hat f nach dem Fundamentalsatz der Algebra einen Eigenwert λ_1 mit Eigenvektor v_1, ohne Einschränkung normiert. Wir schreiben $V = [v_1] \oplus [v_1]^\perp$. Um die Induktionshypothese anzuwenden, behaupten wir, dass f den Untervektorraum $W = [v_1]^\perp$ auf sich abbildet. In der Tat gilt $f^*(v_1) = \overline{\lambda}_1(v_1)$ nach Proposition 2.7, was die Voraussetzung 'f normal' braucht, und nun ist für alle $w \in W$

$$\langle f(w), v_1 \rangle \;=\; \langle w, f^*(v_1) \rangle \;=\; \lambda_1 \langle w, v_1 \rangle \;=\; 0\,, \tag{2.3}$$

wie behauptet. Für $w_1, w_2 \in W$ gilt

$$\langle f|_W(w_1), w_2 \rangle = \langle f(w_1), w_2 \rangle = \langle w_1, f^*(w_2) \rangle = \langle w_1, f^*|_W(w_2) \rangle.$$

Also ist die Einschränkung $f^*|_W$ die Adjungierte zur Einschränkung $f|_W$. Aus $f \circ f^* = f^* \circ f$ folgt $f|_W \circ f^*|_W = f^*|_W \circ f|_W$ und daher, dass $f|_W$ wieder ein normaler Endomorphismus ist. Sei also $B_W = \{b_2, \ldots, b_n\}$ die Orthonormalbasis aus Eigenvektoren von W, die die Induktionshypothese liefert. Dann ist

$$B = \{v_1, b_2, \ldots, b_n\}$$

die gewünschte Orthonormalbasis aus Eigenvektoren. □

Die *Normalform* eines normalen Endomorphismus f eines unitären Vektorraumes ist also eine Diagonalmatrix aus den Eigenwerten von f. Die zugrundeliegende Basis von V kann als Orthonormalbasis gewählt werden. Die Normalform ist, bis auf Vertauschung der Diagonalelemente, eindeutig. Der obige Satz hat folgende Konsequenz für Matrizen:

Korollar 2.13 *Sei $A \in \mathbb{C}^{n\times n}$ eine normale Matrix. Dann gibt es eine unitäre Matrix $S \in \mathbb{C}^{n\times n}$, so dass SAS^* eine Diagonalmatrix ist.*

Beweis : Wir wenden Satz 2.12 auf den Endomorphismus $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ an, der bzgl. der Standardbasis B durch A beschrieben wird. Nach dem Satz gibt es eine orthonormale Basis C von $\mathbb{C}^n$, die aus Eigenvektoren von f besteht. Nach der aus der linearen Algebra 1 bekannten Basiswechseleigenschaft ist daher $\theta_{B,C} A \theta_{B,C}^{-1}$ eine Diagonalmatrix, wobei $\theta_{B,C}$ die Transformationsmatrix von der Standardbasis B nach C bezeichnet. Aus dem folgenden Lemma folgt, dass $\theta_{B,C}$ eine unitäre Matrix ist, also $\theta_{B,C}^{-1} = \theta_{B,C}^*$ erfüllt. Somit können wir $S := \theta_{B,C}$ setzen. □

Lemma 2.14 *Sei V ein euklidischer (bzw. unitärer) Vektorraum mit zwei Orthonormalbasen $B = (b_1, \ldots, b_n)$ und $C = (c_1, \ldots, c_n)$. Dann ist die Transformationsmatrix $\theta_{B,C}$ von B nach C orthogonal (bzw. unitär).*

Beweis : Seien t_{ij} die Einträge der Transformationsmatrix $\theta_{B,C}$. Nach Definition von $\theta_{B,C}$ gilt

$$b_i = \sum_{k=1}^{n} t_{ki} c_k$$

für $i = 1, \ldots, n$. Im unitären Fall haben wir für $i, j = 1, \ldots, n$

$$\begin{aligned} \delta_{ij} &= \langle b_i, b_j \rangle = \left\langle \sum_{k=1}^{n} t_{ki} c_k, \sum_{l=1}^{n} t_{lj} c_l \right\rangle = \sum_{k,l=1}^{n} t_{ki} \overline{t_{lj}} \langle c_k, c_l \rangle \\ &= \sum_{k,l=1}^{n} t_{ki} \overline{t_{lj}} \delta_{kl} = \sum_{k=1}^{n} t_{ki} \overline{t_{kj}} = (\theta_{B,C}^* \theta_{B,C})_{ji}. \end{aligned}$$

Somit gilt $\theta_{B,C}^* \theta_{B,C} = I_n$, die Transformationsmatrix ist also unitär. Im euklidischen Fall finden wir analog $\theta_{B,C}^T \theta_{B,C} = I_n$, dann ist also $\theta_{B,C}$ orthogonal. □

Wir spezialisieren nun auf Isometrien und selbstadjungierte Endomorphismen.

Satz 2.15 *Ein normaler Endomorphismus f eines unitären Vektorraumes ist genau dann eine Isometrie, wenn für alle Eigenwerte λ von f die Zusatzbedingung $|\lambda| = 1$ gilt.*

Beweis : Ist f eine Isometrie, so ist f normal und daher jeder Eigenvektor v zum Eigenwert λ auch ein Eigenvektor von f^* zum Eigenwert $\overline{\lambda}$. Daher ist

$$v = (f^* \circ f)(v) = f^*(\lambda v) = \overline{\lambda}\lambda v$$

und daher $|\lambda| = 1$. Umgekehrt schreiben wir den normalen Endomorphismus in Normalform. Dann ist seine Abbildungsmatrix

$$A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

und die von f^* ist A^*. Ist $|\lambda_i| = 1$ für alle i, so ist $A \cdot A^* = 1$, also $f \circ f^* = f^* \circ f = id$ und f eine Isometrie. □

Satz 2.16 *Ein normaler Endomorphismus f eines unitären Vektorraumes ist genau dann selbstadjungiert, wenn alle Eigenwerte von f reell sind.*

Beweis : Ist f selbstadjungiert, so sind alle Eigenwerte nach Korollar 2.9 reell.

Umgekehrt können wir einen normalen Endomorphismus f mit reellen Eigenwerten bezüglich einer geeigneten orthonormalen Basis durch eine diagonale Abbildungsmatrix A mit reellen Diagonaleinträgen darstellen (Normalform). Eine solche Matrix ist hermitesch ($A = A^*$). Daher ist f selbstadjungiert. □

2.4 Normalformen im euklidischen Fall

Sei $(V, \langle \cdot, \cdot \rangle)$ ein euklidischer Vektorraum der Dimension n. Ziel des Abschnittes ist es, einen unitären Vektorraum Z zu bauen, der (als $\mathbb{C}$-Vektorraum) ebenfalls die Dimension n hat und V als $\mathbb{R}$-Untervektorraum enthält. Dabei erinnern wir an die Einbettung von $\mathbb{R}$ nach $\mathbb{C}$, gegeben durch $\mathbb{R} \ni v \longmapsto v + 0 \cdot i \in \mathbb{C}$. Komplexe Zahlen können wir als $\alpha + \beta i$ schreiben (und $i^2 = -1$ beachten) oder als Tupel (α, β) und die Multiplikation

$$(\alpha, \beta) \cdot (v, w) = (\alpha v - \beta w, \alpha w + \beta v)$$

entsprechend definieren. Wir verwenden hier beide Schreibweisen auch für den Vektorraum Z.

Sei $Z = V \times V = \{(v_1, v_2) \mid v_1, v_2 \in V\}$. Wir definieren die Addition

$$(v_1, v_2) + (w_1, w_2) := (v_1 + w_1, v_2 + w_2)$$

und Skalarmultiplikation für $(\alpha, \beta) = \alpha + i\beta \in \mathbb{C}$:

$$(\alpha, \beta)(v_1, v_2) = (\alpha v_1 - \beta v_2, \alpha v_2 + \beta v_1).$$

Dann ist Z ein $\mathbb{C}$-Vektorraum (und damit natürlich auch $\mathbb{R}$-Vektorraum) und

$$\iota \colon V \longrightarrow Z, \quad v \longmapsto (v, 0)$$

ist eine injektive lineare Abbildung von $\mathbb{R}$-Vektorräumen. Man beachte, dass gegeben eine Basis $\{b_1, \ldots, b_n\}$ von V die Menge $\{(b_1, 0), \ldots, (b_n, 0)\}$ eine Basis (als $\mathbb{C}$-Vektorraum) von Z ist, also $\dim_{\mathbb{C}-VR} Z = \dim_{\mathbb{R}-VR} V = n$. Als $\mathbb{R}$-Vektorraum ist z.B. die Menge $\{(b_1, 0), (0, b_1), \ldots (b_n, 0), (0, b_n)\}$ eine Basis (Übung!) und folglich ist $\dim_{\mathbb{R}-VR} V = 2 \cdot n$. Oft ist die Schreibweise $(v_1, v_2) =: v_1 + iv_2$ für Elemente von Z schöner. Wir schreiben auch $i \cdot V$ für den Unterraum der Paare, deren erste Koordinate Null ist. (Man verwechsle $i \cdot V$ und $\iota(V)$ nicht!) Genauer gesagt, fassen wir V via der Abbildung ι als Teilraum von Z auf. Dann ist $Z = V \oplus iV$. Die Skalarmultiplikation mit $\alpha + i\beta \in \mathbb{C}$ liest sich dann als

$$(\alpha + i\beta)(v_1 + iv_2) = (\alpha v_1 - \beta v_2) + i \cdot (\beta v_1 + \alpha v_2).$$

Satz 2.17 *Es gibt genau eine hermitsche Form H auf Z, sodass die Einschränkung von H auf $\iota(V) \subseteq Z$ gerade die vorgegebene Bilinearform $\langle \cdot, \cdot \rangle =: F(\cdot, \cdot)$ ist. Ist F positiv definit, so ist auch H positiv definit.*

Beweis : Wir beginnen mit der Eindeutigkeit. Wenn H eine solche Form ist, dann gilt

$$\begin{aligned} H(v_1 + iw_1, v_2 + iw_2) &= H(v_1, v_2) + H(w_1, w_2) + iH(w_1, v_2) - iH(v_1, w_2) \\ &= F(v_1, v_2) + F(w_1, w_2) + iF(w_1, v_2) - iF(v_1, w_2). \end{aligned}$$

Alle Terme der rechten Seite sind durch die Vorgabe von F festgelegt und H somit eindeutig. Andererseits kann man diese Gleichung auch zur Definition von H verwenden. Dann sieht man, dass

$$H(v_2 + iw_2, v_1 + iw_1) = \overline{H(v_1 + iw_1, v_2 + iw_2)}$$

ist und dass H linear im ersten Argument ist, da F dies ist. Also ist H eine hermitsche Form. Weiter ist, falls F positiv definit ist,

$$H(v_1 + iw_1, v_1 + iw_1) = F(v_1, v_1) + F(w_1, w_1) \geqslant 0$$

und Gleichheit gilt genau dann, wenn $v_1 = w_1 = 0$ ist. Also ist auch H positiv definit. □

Der metrische Raum (Z, H) heißt *unitäre Erweiterung* von (V, F). Als nächstes untersuchen wir, wie sich lineare Abbildungen von V auf die unitäre Erweiterung fortsetzen.

Satz 2.18 *Ist $f\colon V \longrightarrow V$ ein Endomorphismus, so ist*

$$\widetilde{f}(v+iw) := f(v) + if(w)$$

ein Endomorphismus von Z. Diese Abbildung ist der einzige Endomorphismus von Z, dessen Einschränkung auf V gerade f ist. Die Adjungierte von $\widetilde{f}$ ist $\widetilde{(f^*)}$. Ist f normal, so ist auch $\widetilde{f}$ normal.

Beweis : Ist $z_1 = v_1 + iw_1,\ z_2 = v_2 + iw_2 \in Z$ und $\alpha + i\beta \in \mathbb{C}$, so ist

$$\begin{aligned}\widetilde{f}(z_1+z_2) &= \widetilde{f}((v_1+v_2)+i(w_1+w_2)) = f(v_1+v_2)+if(w_1+w_2)\\ &= f(v_1)+if(w_1)+f(v_2)+if(w_2)\\ &= \widetilde{f}(v_1+iw_1)+\widetilde{f}(v_2+iw_2)\end{aligned}$$

und

$$\begin{aligned}\widetilde{f}((\alpha+i\beta)z_1) &= \widetilde{f}\left((\alpha v_1-\beta w_1)+i(\beta v_1+\alpha w_1)\right)\\ &= f(\alpha v_1-\beta w_1)+if(\beta v_1+\alpha w_1)\\ &= (\alpha+i\beta)\left(f(v_1)+if(w_1)\right) = (\alpha+i\beta)\widetilde{f}(z_1).\end{aligned}$$

Also ist $\widetilde{f}$ linear. Ist φ eine lineare Fortsetzung von f nach Z, so gilt

$$\varphi(v_1+iw_1) = \varphi(v_1)+i\varphi(w_1) = f(v_1)+if(w_1),$$

was die Eindeutigkeit von $\widetilde{f}$ beweist. Zur Bestimmung der Adjungierten berechnen wir

$$\begin{aligned}&H\big(\widetilde{f}(v_1+iw_1), v_2+iw_2\big) = H\big(f(v_1)+if(w_1), v_2+iw_2\big)\\ &= H\big(f(v_1),v_2\big)+iH\big(f(w_1),v_2\big)+H\big(f(w_1),w_2\big)-iH\big(f(v_1),w_2\big)\\ &= H\big(v_1,f^*(v_2)\big)+iH\big(w_1,f^*(v_2)\big)+H\big(w_1,f^*(w_2)\big)-iH\big(v_1,f^*(w_2)\big)\\ &= H\big(v_1+iw_1, f^*(v_2)+if^*(w_2)\big)\end{aligned}$$

Also ist $\widetilde{(f^*)}(v_2+iw_2) = f^*(v_2)+if^*(w_2)$ eine Adjungierte. Wegen der Eindeutigkeit der Adjungierten ist der bestimmte Artikel in der dritten Aussage des Satzes gerechtfertigt. Außerdem können wir ab sofort gefahrlos Klammern weglassen und nur $\widetilde{f^*}$ schreiben. Ist f normal, so gilt

$$\begin{aligned}&(f\circ f^*)(v+iw) = f(f^*(v)+if^*(w)) = f(f^*(v))+if(f^*(w))\\ &= f^*(f(v))+if^*if(w) \quad = \quad f^*(f(v+iw)) \quad = \quad (f^*\circ f)(v+iw)\end{aligned}$$

für alle $v+iw \in Z$. □

Ziel dieser Vorarbeiten ist ein Satz über die Normalform von normalen Endomorphismen im euklidischen Fall. Noch eine Vorbemerkung dazu:

Lemma 2.19 *Sei f ein normaler Endomorphismus des euklidischen Vektorraumes V. Ist $z = v + iw \in Z$ ein auf 1 normierter Eigenvektor von $\widetilde{f}$ zum nicht-reellen Eigenwert $\alpha + i\beta$ mit $\alpha \in \mathbb{R}$ und $\beta \in \mathbb{R}^*$, so ist $\overline{z} = v - iw$ ein auf 1 normierter Eigenvektor von $\widetilde{f}$ zum Eigenwert $\alpha - i\beta$. Weiter gilt $H(z, \overline{z}) = 0$.*

Der Vektor $\overline{z}$ heißt der zu z komplex konjugierte Vektor.

Beweis : Die Eigenschaft Eigenvektor für $\widetilde{f}$ zu sein, übersetzt sich in Eigenschaften von f wie folgt:

$$f(v) + if(w) = \widetilde{f}(v + iw) = (\alpha + i\beta)(v + iw) = (\alpha v - \beta w) + i(\beta v + \alpha w).$$

Da f reellwertig ist, folgt daraus $f(v) = \alpha v - \beta w$ und $f(w) = \beta v + \alpha w$. Also ist

$$\begin{aligned}\widetilde{f}(\overline{z}) = \widetilde{f}(v - iw) = f(v) - if(w) &= (\alpha v - \beta w) - i(\beta v + \alpha w) \\ &= (\alpha - i\beta)(v - iw) = (\alpha - i\beta) \cdot \overline{z}.\end{aligned}$$

Also ist $\overline{z}$ Eigenvektor von $\widetilde{f}$ zum Eigenwert $(\alpha - i\beta)$. Offenbar ist $\langle \overline{z}, \overline{z} \rangle = \langle v, v \rangle + (-1)^2 \langle w, w \rangle = \langle z, z \rangle = 1$, was die Normiertheit zeigt. Die Eigenschaft $\langle z, \overline{z} \rangle = 0$ folgt, weil z und $\overline{z}$ Eigenvektoren zu verschiedenen Eigenwerten des normalen Endomorphismus f sind (siehe Übungen). □

Satz 2.20 (Normalform für normale Endomorphismen euklidischer Vektorräume) *Sei V ein endlichdimensionaler euklidischer Vektorraum und f ein Endomorphismus von V. Dann ist f genau dann normal, wenn es eine Orthonormalbasis von V gibt, sodass die Abbildungsmatrix von f die Gestalt*

$$A = \begin{pmatrix} \lambda_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & \lambda_k & & & & \\ & & & \boxed{\begin{matrix} \lambda'_{k+1} & -\lambda''_{k+1} \\ \lambda''_{k+1} & \lambda'_{k+1} \end{matrix}} & & & \\ & & & & \ddots & & \\ & & & & & \boxed{\begin{matrix} \lambda'_{k+r} & -\lambda''_{k+r} \\ \lambda''_{k+r} & \lambda'_{k+r} \end{matrix}} & \\ 0 & & & & & & \end{pmatrix}$$

hat. Dabei sind $\lambda_1, \ldots, \lambda_k$ die reellen Nullstellen des charakteristischen Polynoms χ_f von f und $\lambda_{k+1}, \overline{\lambda_{k+1}}, \ldots, \lambda_{k+r}, \overline{\lambda_{k+r}}$ die Paare komplex konjugierter Eigenwerte von χ_f. Weiterhin ist dabei

$$\begin{aligned}\lambda_{k+j} &= \lambda'_{k+j} + i\lambda''_{k+j} \\ \overline{\lambda_{k+j}} &= \lambda'_{k+j} - i\lambda''_{k+j}\end{aligned}$$

für alle $1 \leq j \leq r$ mit $\lambda'_{k+j} \in \mathbb{R}$ und $\lambda''_{k+j} \in \mathbb{R}_{>0}$. Außerdem sind die Nullstellen von χ_f genau die Eigenwerte der Fortsetzung $\widetilde{f}$ von f.

Beweis : Sei f normal. Wir beweisen die Existenz einer Abbildungsmatrix A per Induktion nach $n = \dim(V)$. Für $n = 1$ ist $V = \langle v \rangle$ und v ein Eigenvektor von f, den wir zudem normiert wählen können. Alle Behauptungen sind in diesem Fall offensichtlich. Wir nehmen an, dass die Aussage für alle Vektorräume der Dimension höchstens $n - 1$ gilt. Wir unterscheiden zwei Fälle.

1.) Der Endomorphismus f hat einen reellen Eigenwert v_1. Wie im Beweis von Satz 2.12 sieht man, dass man die Induktionsvoraussetzung auf $U = [v_1^\perp]$ anwenden kann. Sei A_U die Abbildungsmatrix der Einschränkung bzgl. der Basis $\{v_2, \ldots, v_n\}$ von U. Dann hat die Abbildungsmatrix bzgl. der Basis $\{v_1, \ldots, v_n\}$ von V die Gestalt

$$A = \left(\begin{array}{c|ccc} \lambda_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A_U & \\ 0 & & & \end{array}\right)$$

und ist von der gewünschten Form.

2.) Der Endomorphismu f hat keinen reellen Eigenwert. Wir wollen die Normalform aus Satz 2.12 der unitären Erweiterung $\widetilde{f}$ von f anwenden. Nach Satz 2.18 ist diese auch normal. Wir vergleichen die Minimalpolynome $\chi_{\widetilde{f}}$ und χ_f von $\widetilde{f}$ und f. Sei $B = \{b_1, \ldots, b_n\}$ eine Basis von V. Dann ist, wie zu Beginn des Abschnittes 2.4 erklärt, B auch eine Basis des $\mathbb{C}$-Vektorraums Z. Ist $f(b_i) = \sum_{i=1}^n \alpha_{ij} b_j$, so ist nach Definition der Fortsetzung auch $\widetilde{f}(b_i) = \sum_{i=1}^n \alpha_{ij} b_j$. Also stimmen die Abbildungsmatrizen von $\widetilde{f}$ und f in dieser Basis überein. Folglich ist $\chi_f = \chi_{\widetilde{f}}$ und $\chi_{\widetilde{f}}$ hat keine reelle Nullstelle. Also hat $\chi_{\widetilde{f}}$ eine komplexe Nullstelle $\lambda = \lambda' + i\lambda''$ und $\widetilde{f}$ einen Eigenvektor $z = v + iw$ zum Eigenwert λ. Wir können $z \in Z$ auf 1 normiert wählen. Nach dem vorangehenden Lemma hat $\widetilde{f}$ auch den Eigenvektor $\overline{z} = v - iw$ zum Eigenwert $\overline{\lambda} = \lambda' - i\lambda''$. Wir können gegebenenfalls die Rollen von v und $\overline{v}$ vertauschen und $\lambda'' > 0$ annehmen. Der Unterraum $U = [z, \overline{z}] \subseteq Z$ ist $\widetilde{f}$-invariant. Wir suchen nach Vektoren in $V \subseteq Z$ die $U \cap V$ aufspannen. Es liegen $b_1 = \sqrt{2} \cdot w = \frac{1}{\sqrt{2} \cdot i}(z - \overline{z})$ und $b_2 = \sqrt{2} \cdot v = \frac{1}{\sqrt{2}}(z + \overline{z})$ in $U \cap V =: V_U$. Es gilt

$$\begin{aligned} \langle b_2, b_2 \rangle &= \frac{1}{2}\langle z + \overline{z}, z + \overline{z} \rangle = 1 \\ \langle b_1, b_2 \rangle &= \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}i}\langle z - \overline{z}, z + \overline{z} \rangle = \frac{1}{2i}(1 - 1) = 0 \\ \langle b_1, b_1 \rangle &= \frac{1}{\sqrt{2}i} \cdot \frac{-1}{\sqrt{2}i}\langle z - \overline{z}, z - \overline{z} \rangle = \frac{1}{2}\left(\langle z, z \rangle + \langle \overline{z}, \overline{z} \rangle\right) = 1 \end{aligned}$$

Damit ist also $\{b_1, b_2\}$ eine Orthonormalbasis von V_U. Es ist

$$\begin{aligned} f(b_1) = \widetilde{f}(b_1) &= \frac{1}{\sqrt{2}i}\left(\widetilde{f}(z) - \widetilde{f}(\overline{z})\right) = \frac{1}{\sqrt{2}i}\big((\lambda' + i\lambda'')z - (\lambda' - i\lambda'')\overline{z}\big) \\ &= \lambda' b_1 + \lambda'' b_2 \\ f(b_2) = \widetilde{f}(b_2) &= \frac{1}{\sqrt{2}}\left(\widetilde{f}(z) + \widetilde{f}(\overline{z})\right) = \frac{1}{\sqrt{2}}\big((\lambda' + i\lambda'')z + (\lambda' - i\lambda'')\overline{z}\big) \\ &= -\lambda'' b_1 + \lambda' b_2. \end{aligned}$$

Also ist $V_U \subseteq V$ ein f-invariater Unterraum und f hat bzgl. $\{b_1, b_2\}$ auf diesem die Abbildungsmatrix

$$A_{V_U} = \begin{pmatrix} \lambda' & \lambda'' \\ -\lambda'' & \lambda' \end{pmatrix}.$$

Sobald wir gezeigt haben, dass $V_U^\perp$ invariant unter f ist, können wir die Induktionsannahme auf $V_U^\perp$ anwenden. Die Einschränkung von f auf $V_U^\perp$ hat die Normalform $A_{V_U^\perp}$ bzgl. einer Basis $\{b_3, \ldots, b_n\}$ und die Abbildungsmatrix von f bzgl. $B = \{b_1, \ldots, b_n\}$ ist

$$\left(\begin{array}{cc:c} \lambda' & \lambda'' & 0 \\ -\lambda'' & \lambda' & \\ \hdashline 0 & & A_{V_U^\perp} \end{array}\right).$$

Es genügt die Reihenfolge der Basiselemente zu vertauschen, um die Eigenwerte und (2×2)-Blöcke in die richtige Reihenfolge zu bekommen.
Damit ist die erste Implikation bewiesen. Sei umgekehrt A wie im Satz die Abbildungsmatrix von f bezüglich einer Orthonormalbasis. Dann ist $A^\top$ die Abbildungsmatrix der

Adjungierten und es gilt

$$A \cdot A^\top = \begin{pmatrix} \lambda_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & \lambda_k & & & & \\ & & & \boxed{\begin{matrix} \lambda'_{k+1} & -\lambda''_{k+1} \\ \lambda''_{k+1} & \lambda'_{k+1} \end{matrix}} & & & \\ & & & & \ddots & & \\ & & & & & \boxed{\begin{matrix} \lambda'_{k+r} & -\lambda''_{k+r} \\ \lambda''_{k+r} & \lambda'_{k+r} \end{matrix}} & \\ 0 & & & & & & \end{pmatrix}$$

$$\cdot \begin{pmatrix} \lambda_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & \lambda_k & & & & \\ & & & \boxed{\begin{matrix} \lambda'_{k+1} & \lambda''_{k+1} \\ -\lambda''_{k+1} & \lambda'_{k+1} \end{matrix}} & & & \\ & & & & \ddots & & \\ & & & & & \boxed{\begin{matrix} \lambda'_{k+r} & \lambda''_{k+r} \\ -\lambda''_{k+r} & \lambda'_{k+r} \end{matrix}} & \\ 0 & & & & & & \end{pmatrix}$$

$$= \begin{pmatrix} \lambda_1^2 & & & & & & 0 \\ & \ddots & & & & & \\ & & \lambda_k^2 & & & & \\ & & & \boxed{\begin{matrix} |\lambda_{k+1}| & 0 \\ 0 & |\lambda_{k+1}| \end{matrix}} & & & \\ & & & & \ddots & & \\ & & & & & \boxed{\begin{matrix} |\lambda_{k+r}| & 0 \\ 0 & |\lambda_{k+r}| \end{matrix}} & \\ 0 & & & & & & \end{pmatrix} = A^\top \cdot A.$$

Also ist A normal und damit f normal. □

Wir spezialisieren nun auf Isometrien.

Satz 2.21 *Zu jeder Isometrie f eines n-dimensionalen euklidischen Vektorraumes V gibt es eine Orthonormalbasis, in der f die Abbildungsmatrix*

$$A = \begin{pmatrix} \boxed{\begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix}} & & & & \\ & \boxed{\begin{matrix} -1 & & 0 \\ & \ddots & \\ 0 & & -1 \end{matrix}} & & & \\ & & \boxed{\begin{matrix} \cos\omega_1 & -\sin\omega_1 \\ \sin\omega_1 & \cos\omega_1 \end{matrix}} & & \\ & & & \ddots & \\ & & & & \boxed{\begin{matrix} \cos\omega_r & -\sin\omega_r \\ \sin\omega_r & \cos\omega_r \end{matrix}} \end{pmatrix}$$

hat. Die Matrix A ist bis auf die Reihenfolge der Blöcke eindeutig durch f bestimmt. Hat umgekehrt ein Endomorphismus f von V eine Abbildungsmatrix der Gestalt von A bezüglich einer Orthonormalbasis, so ist f eine Isometrie. Die Matrix A heißt Normalform der Isometrie.

Beweis : Jede Isometrie ist normal und wir können daher Satz 2.20 anwenden. Die 2×2 Blöcke enthalten als Einträge λ'_{k+j} und $\pm\lambda''_{k+j}$, wobei $\lambda_{k+j} = \lambda'_{k+j} \pm i\lambda''_{k+j}$ die komplexen Eigenwerte der unitären Fortsetzung $\widetilde{f}$ von f sind. Da $\widetilde{f}$ auch eine Isometrie ist, ist $|\lambda_{k+j}| = 1$, d.h. $(\lambda'_{k+j})^2 + (\lambda''_{k+j})^2 = 1$. Wegen $\lambda''_{k+j} > 0$ gibt es genau eine reelle Zahl $\omega_j \in (0, \pi)$ mit

$$\cos(\omega_j) = \lambda'_{k+j} \quad \text{und} \quad \sin(\omega_j) = \lambda''_{k+j} \quad \text{für} \quad j = 1, \ldots, r.$$

Daraus folgt, dass A die angegebene Gestalt hat. Die übrigen Aussagen folgen nun leicht. □

Beispiel 2.22 Für die Isometrie eines zweidimensionalen euklidischen Vektorraumes gibt es 4 Typen der Normalform:

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad B_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad B_3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad B_4 = \begin{pmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{pmatrix}$$

mit $0 < \omega < \pi$. Geometrisch beschrieben werden diese als die Identität, die Geradenspiegelung an $[e_1]$, die Punktspiegelung an Ursprung und als die Drehung um den Winkel ω.

Abschließend betrachten wir selbstadjungierte Endomorphismen von euklidischen Vektorräumen.

Satz 2.23 *Ein Endomorphismus f eines endlichdimensionalen euklidischen Vektorraums V ist genau dann selbstadjungiert, wenn es eine Orthonormalbasis von V aus Eigenvektoren von f gibt.*

Beweis : Ist f selbstadjungiert, so ist auch die unitäre Erweiterung $\widetilde{f}$ von f selbstadjungiert, weil $\widetilde{f}^* = \widetilde{(f^*)} = \widetilde{f}$ gilt. Daher hat das charakteristische Polynom $\chi_f = \chi_{\widetilde{f}}$ nach Korollar 2.9 nur reelle Nullstellen. Nach Satz 2.20 hat daher f eine diagonale Normalform bzgl. einer geeigneten Orthonormalbasis (in der Normalform treten keine (2×2)-Blöcke auf). Diese Orthonormalbasis besteht daher aus Eigenvektoren von f.

Gibt es umgekehrt eine Orthonormalbasis von V aus Eigenvektoren von f, so ist die Abbildungsmatrix A von f bezüglich dieser Basis diagonal. Insbesondere ist A symmetrisch und daher f selbstadjungiert. □

Dieser Satz hat folgende Bedeutung für Matrizen:

Korollar 2.24 *Sei $A \in \mathbb{R}^{n\times n}$ eine symmetrische Matrix. Dann gibt es eine orthogonale Matrix $S \in \mathbb{R}^{n\times n}$, so dass $SAS^\top$ eine Diagonalmatrix ist.*

Beweis : Wir wenden den vorigen Satz auf den Endomorphismus $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ an, der bzgl. der Standardbasis B durch A beschrieben wird. Nach dem Satz gibt es eine orthonormale Basis C von $\mathbb{R}^n$, die aus Eigenvektoren von f besteht. Nach der aus der linearen Algebra bekannten Basiswechseleigenschaft ist daher $\theta_{B,C} A \theta_{B,C}^{-1}$ eine Diagonalmatrix, wobei $T_{B,C}$ die Transformationsmatrix von B nach C bezeichnet. Aus Lemma 2.14 folgt, dass $\theta_{B,C}$ eine orthogonale Matrix ist. Somit stimmt die Aussage für $S := \theta_{B,C}$. □

3 Affine Räume

Affine Räume sollen ein Modell des Anschauungsraumes der „Welt, in der wir leben " sein. Wie in einem Vektorraum wollen wir zu zwei Punkten einen „Verbindungsvektor " zuordnen und diese Verbindungsvektoren erfüllen die Axiome, die in einem (reellen) Vektorraum gelten. Aber im Gegensatz zu einem Vektorraum gibt es keine natürliche Wahl eines „Ursprungs ", eines „Nullpunktes ". Dies motiviert folgende Definition. Sei K ein beliebiger Körper.

Definition 3.1 *Sei V ein Vektorraum über einem Körper K. Eine nichtleere Menge $\mathbb{A}$ zusammen mit einer Abbildung „Verbindungsvektor "*

$$\Phi\colon \mathbb{A} \times \mathbb{A} \longrightarrow V$$

heißt affiner Raum *zu V, falls folgende Axiome gelten:*

i) Für alle $P \in \mathbb{A}$ und $v \in V$ gibt es genau ein $Q \in \mathbb{A}$, sodass $\Phi(P,Q) = v$.

ii) Für alle $P, Q, R \in \mathbb{A}$ gilt $\Phi(P,Q) + \Phi(Q,R) = \Phi(P,R)$.

Ist $\dim V = n < \infty$, so schreiben wir $\mathbb{A}^n$ oder auch $\mathbb{A}^n_k$, wenn wir den zugrundeliegenden Körper betonen wollen. Statt $\Phi(P,Q)$ schreiben wir auch $\overrightarrow{PQ}$.

Wir halten zwei unmittelbare Konsequenzen der Definition fest. Das Axiom i) bedeutet, dass für alle $P \in \mathbb{A}$ die Abbildung

$$\Phi_P : \mathbb{A} \to V, \;\; Q \mapsto \overrightarrow{PQ}$$

bijektiv ist. Dabei ist $\Phi_P(P) = \overrightarrow{PP} = 0$, denn nach Axiom ii) gilt $\overrightarrow{PP} + \overrightarrow{PP} = \overrightarrow{PP}$. Man halt also Bijektionen von einem affinen Raum zu einem Vektorraum, aber nicht nur eine, sondern viele. Man muss einen Punkt P auswählen um eine solche Bijektion festzulegen.

Proposition 3.2 *Sei $\mathbb{A}$ ein affiner Raum. Dann gilt für alle $P, Q \in \mathbb{A}$:*

$$\overrightarrow{PQ} = 0 \iff P = Q \quad \textit{und} \quad \overrightarrow{PQ} = -\overrightarrow{QP}.$$

Beweis : Die erste Aussage folgt unmittelbar aus der obigen Bemerkung mit $\Phi_P(Q) = \overrightarrow{PQ}$. Die zweite Aussage folgt aus Axiom ii): $\overrightarrow{PQ} + \overrightarrow{QP} = \overrightarrow{PP} = 0$. □

Beispiel 3.3 Ist V ein Vektorraum, so ist $\mathbb{A} = V$ mit $\Phi(v,w) = w - v$ ein affiner Raum über V. Ist $\mathbb{A} = \mathbb{R}^2, V = \mathbb{R}$ und $\Phi\big((v_1,v_2),(w_1,w_2)\big) = w_1 - v_1$, so ist $\mathbb{A}$ kein affiner Raum über V, denn die Eindeutigkeitsaussage in Axiom i) ist verletzt.

Beispiel 3.4 Sei $Ax = b$ ein inhomogenes lineares Gleichungssystem, d.h. $b \neq 0$ und $V = \mathrm{Ker}(A)$ die Lösungsmenge des zugehörigen homogenen Gleichungssystems. Dann gibt es für $\mathbb{L} = \mathbb{L}_{A,b}$ keinen ausgezeichnetes Nullelement x_0. Wir können aber ein solches wählen. Wir hatte dies in [LA1] eine spezielle Lösung genannt. Dann gibt die Abbildung $\Phi_{x_0} : V \to \mathbb{L}$, die $v \mapsto x_0 + v$ schickt, eine Bijektion von V und der Lösungsmenge. Andersherum haben wir eine Abbildung $\Phi : \mathbb{L} \times \mathbb{L} \to V$, die $(x_1, x_2) \mapsto x_2 - x_1$ abbildet. Diese erfüllt alle Axiome eines affinen Raumes.

3.1 Affine Unterräume

Viele natürliche Beispiele von affinen Räumen, die nicht wie in Beispiel 3.3 einen Nullpunkt haben, entstehen, indem man die Verbindungsvektoren eines Unterraumes $U \subset V$ von einem Aufpunkt P aus abträgt.

Definition 3.5 *Sei $\mathbb{A}$ ein affiner Raum zu V. Eine Teilmenge $\mathbb{B} \subset \mathbb{A}$ heißt* affiner Unterraum, *falls es ein $P \in \mathbb{B}$ gibt, so dass*

$$U := \Phi_P(\mathbb{B}) = \{\overrightarrow{PQ} \colon Q \in \mathbb{B}\}$$

ein Unterraum von V ist.

Der Aufpunkt P in dieser Definition ist in keiner Weise besonders. Aber der Unterraum U ist eindeutig durch $\mathbb{B}$ bestimmt:

Proposition 3.6 *Ist $\mathbb{B} \subseteq \mathbb{A}$ ein affiner Unterraum, so gibt es einen eindeutigen Unterraum U von V, so dass*

$$U = \Phi_R(\mathbb{B}) = \{\overrightarrow{RQ} \colon Q \in \mathbb{B}\}$$

für alle $R \in \mathbb{B}$ gilt. Zudem ist $\mathbb{B}$ zusammen mit der Einschränkung von Φ auf $\mathbb{B} \times \mathbb{B}$ ein affiner Raum zu U.

Der Unterraum U heißt der zu $\mathbb{B}$ gehörige Unterraum.

Beweis : Nach der obigen Definition gibt es ein $P \in \mathbb{B}$, so dass $U := \Phi_P(\mathbb{B})$ ein Unterraum von V ist. Wir zeigen, dass für alle anderen $R \in \mathbb{B}$ ebenfalls $U = \Phi_R(\mathbb{B})$ gilt. In der Tat gilt für $Q \in \mathbb{B}$

$$\overrightarrow{RQ} = \overrightarrow{RP} + \overrightarrow{PQ} = \overrightarrow{PQ} - \overrightarrow{PR},$$

wir haben also $\Phi_R(\mathbb{B}) = \Phi_P(\mathbb{B}) - \overrightarrow{PR} = U - \overrightarrow{PR} = U$ wegen $\overrightarrow{PR} \in \Phi_P(\mathbb{B}) = U$. Das zeigt die Existenz des offensichtlich eindeutigen Unterraums U.

Die nichtleere Menge $\mathbb{B}$ zusammen mit der Einschränkung von Φ auf $\mathbb{B} \times \mathbb{B}$ ist ein affiner Unterraum zu U, denn das Axiom ii) folgt aus dessen Gültigkeit in $\mathbb{A}$ und i) folgt, da sich für alle $R \in \mathbb{B}$ die Bijektion $\Phi_R : \mathbb{A} \to V$ wegen $\Phi_R(\mathbb{B}) = U$ zu einer Bijektion $\mathbb{B} \to U$ einschränkt. □

Satz 3.7 *Sind $\mathbb{B}_j$ (für j in einer Indexmenge J) affine Unterräume des affinen Raumes $\mathbb{A}$ mit zugehörigen Untervektorräumen U_j und ist $\mathbb{B} = \bigcap\limits_{j \in J} \mathbb{B}_j$ nicht leer, so ist $\mathbb{B}$ ein affiner Unterraum von A mit $U = \bigcap\limits_{j \in J} U_j$ als zugehörigem Vektorraum.*

Beweis : Sei $P \in \mathbb{B}$. Dann liegt P in allen $\mathbb{B}_j$, nach Proposition 3.1 gilt also

$$\Phi_P(\mathbb{B}) = \Phi_P\Big(\bigcap_{j \in J} \mathbb{B}_j\Big) = \bigcap_{j \in J} \Phi_P(\mathbb{B}_j) = \bigcap_{j \in J} U_j,$$

wobei die zweite Gleichheit aus der Bijektivität von Φ_P folgt. Somit ist $\mathbb{B}$ ein affiner Unterraum mit $\bigcap_{j \in J} U_j$ als zugehörigem Unterraum. □

Definition 3.8 *Sei $M \subseteq \mathbb{A}$ nicht leer und $\mathcal{B}_M$ die Menge aller affinen Unterräume von $\mathbb{A}$, die M enthalten. Dann heißt $[M] := \bigcap_{\mathbb{B} \in \mathcal{B}_M} \mathbb{B}$ die* affine Hülle *von M. Sind $\mathbb{B}_1, \mathbb{B}_2$ zwei affine Unterräume von $\mathbb{A}$, so heißt $\mathbb{B}_1 + \mathbb{B}_2 := [\mathbb{B}_1 \cup \mathbb{B}_2]$ der* Verbindungsraum *von $\mathbb{B}_1$ und $\mathbb{B}_2$.*

Nach dem vorherigen Satz ist $[M]$ ein affiner Unterraum von $\mathbb{A}$. Es ist der kleinste affine Unterraum von $\mathbb{A}$, der M enthält.

Lemma 3.9 *Sei $M \subseteq \mathbb{A}$ nicht leer und $P \in M$. Dann ist der zum affinen Unterraum $[M] \subseteq \mathbb{A}$ gehörige Unterraum gleich dem von $\Phi_P(M) \subset V$ aufgespannten Unterraum $[\Phi_P(M)]$.*

Beweis : Eine Teilmenge $\mathbb{B} \subset \mathbb{A}$ mit $P \in \mathbb{B}$ ist genau dann ein affiner Unterraum, der M enthält, wenn $\Phi_P(\mathbb{B})$ ein Unterraum von V ist, der $\Phi_P(M)$ enthält. Wegen der Bijektivität von $\Phi_P : \mathbb{A} \to V$ ist somit $\Phi_P([M])$ gleich dem Durchschnitt aller Unterräume von V, die $\Phi_P(M)$ enthalten. Dieser Durchschnitt ist genau der von $\Phi_P(M)$ aufgespannte Unterraum $[\Phi_P(M)]$. Der zu $[M]$ gehörige Unterraum $\Phi_P([M]) \subset V$ ist also $[\Phi_P(M)]$. □

Beispiel 3.10 Sind P, Q zwei Punkte in $\mathbb{A}^2$, so ist $[\{P, Q\}]$ die Verbindungsgerade von P und Q mit zugehörigem Unterraum $[\Phi_P(\{P, Q\})] = [\overrightarrow{PQ}]$.

Dieses Beispiel zeigt, dass, im Unterschied zur entsprechenden Aussage für Vektorräume, der Vektorraum zu $\mathbb{B}_1 + \mathbb{B}_2$ nicht $U_1 + U_2$ ist, denn die Vektorräume zu $\{P\}$ und $\{Q\}$ sind jeweils der Nullraum, aber der Vektorraum zur Verbindungsgeraden ist eindimensional.

Definition 3.11 *Zwei affine Unterräume $\mathbb{B}_1$ und $\mathbb{B}_2$ von $\mathbb{A}$ mit zugehörigen Vektorräumen U_1 und U_2 heißen* parallel, *falls $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ gilt.*

Als Übung zeigt man leicht:

Proposition 3.12 *Sind $\mathbb{B}_1$ und $\mathbb{B}_2$ parallel, so ist $\mathbb{B} := \mathbb{B}_1 \cap \mathbb{B}_2$ leer oder $\mathbb{B}_1$ ein affiner Unterraum von $\mathbb{B}_2$ oder $\mathbb{B}_2$ ein affiner Unterraum von $\mathbb{B}_1$.*

Dabei ist es natürlich möglich, dass die beiden letztgenannten Fälle gleichzeitig auftreten, d.h., dass $\mathbb{B} = \mathbb{B}_1 = \mathbb{B}_2$ ist.

Beispiel 3.13 Für zwei eindimensionale affine Unterräume $\mathbb{B}_1, \mathbb{B}_2$ (im Folgenden *Geraden* genannt) von $\mathbb{A}^3$ tritt genau einer der folgenden Fälle auf:

i) $\mathbb{B}_1 = \mathbb{B}_2$

ii) $\mathbb{B}_1 \cap \mathbb{B}_2$ haben einen Punkt gemeinsam.

iii) $\mathbb{B}_1 \cap \mathbb{B}_2 = \emptyset$ und $\mathbb{B}_1$ und $\mathbb{B}_2$ sind parallel.

iv) $\mathbb{B}_1$ und $\mathbb{B}_2$ sind *windschief*, d.h. es gibt keinen affinen zweidimensionalen Unterraum von $\mathbb{A}^3$, der $\mathbb{B}_1$ und $\mathbb{B}_2$ enthält.

Diese Behauptung zeigt man, indem man alle möglichen Fälle für $\dim(\mathbb{B}_1 + \mathbb{B}_2)$ durchgeht.

3.2 Etwas ebene affine Geometrie

In diesem Abschnitt formulieren wir einige Sätze über Punkte und Geraden in der Ebene, die sich nur mit den Begriffen 'schneiden' und 'parallel sein' formulieren lassen. Der Grund für diese Sätze wird im Abschnitt über axiomatische Geometrie klar.

Definition 3.14 *Drei Punkte $P, Q, X \in \mathbb{A}^n$ heißen* kollinear, *falls $[\{X, P, Q\}]$ eine Gerade ist. Ist zudem $X \neq Q$, so heißt die Zahl λ mit $\overrightarrow{XP} = \lambda \overrightarrow{XQ}$ das* Teilverhältnis *von X, P, Q und wird mit $\tau(X, P, Q)$ bezeichnet.*

Offenbar hängt τ von der Reihenfolge der Argumente ab, z.B. gilt $\tau(X, Q, P) = 1/\tau(X, P, Q)$. Mit diesem Begriff beweisen wir einige klassische Sätze der ebenen affinen Geometrie.

Satz 3.15 (Desargues) *Seien $g, h, k \in \mathbb{A}^2$ drei paarweise verschiedene Geraden, die sich in O schneiden, und $A, A' \in g$, $B, B' \in h$ und $C, C' \in k$ von O verschiedene Punkte. Ist $[\{A, B\}]$ parallel zu $[\{A', B'\}]$ und $[\{B, C\}]$ parallel zu $[\{B', C'\}]$, so ist auch $[\{A, C\}]$ parallel zu $[\{A', C'\}]$.*

Wir zeigen zunächst:

Lemma 3.16 (Strahlensatz) *In obiger Situation gilt: $[\{A', B'\}]$ ist parallel zu $[\{A, B\}]$ genau dann, wenn $\tau(O, A, A') = \tau(O, B, B')$ erfüllt ist.*

Beweis : Es gilt die Parallelität genau dann, wenn $\overrightarrow{AB}$ und $\overrightarrow{A'B'}$ linear abhängig sind. Wegen

$$\begin{array}{lll} \overrightarrow{OB} = \tau(O, B, B')\, \overrightarrow{OB'} & \text{und} & \overrightarrow{OA} = \tau(O, A, A')\, \overrightarrow{OA'} \\ \text{sind } \overrightarrow{A'B'} = \overrightarrow{OB'} - \overrightarrow{OA'} & \text{und} & \overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA} = \tau(O, B, B')\, \overrightarrow{OB'} - \tau(O, A, A')\, \overrightarrow{OA'} \end{array}$$

linear abhängig genau dann, wenn

$$\det \begin{pmatrix} 1 & -1 \\ \tau(O, B, B') & -\tau(O, A, A') \end{pmatrix} = 0$$

ist, also wenn $\tau(O, A, A') = \tau(O, B, B')$ gilt. □

Beweis (Desargues) : Nach Voraussetzung und dem Strahlensatz ist $\tau(O, A, A') = \tau(O, B, B')$ und $\tau(O, B, B') = \tau(O, C, C')$, daher $\tau(O, A, A') = \tau(O, C, C')$ und damit folgt wieder nach dem Strahlensatz die Behauptung. □

Satz 3.17 (Pappus) *Seien g, h zwei verschiedene Geraden, die sich in O schneiden, $P_1, P_2, P_3 \in g$ und $Q_1, Q_2, Q_3 \in h$ paarweise verschieden und von O verschieden. Sind $[\{P_1, Q_2\}]$ und $[\{P_2, Q_1\}]$ parallel sowie $[\{Q_2, P_3\}]$ und $[\{P_2, Q_3\}]$ parallel, so sind auch $[\{P_1, Q_3\}]$ und $[\{Q_1, P_3\}]$ parallel.*

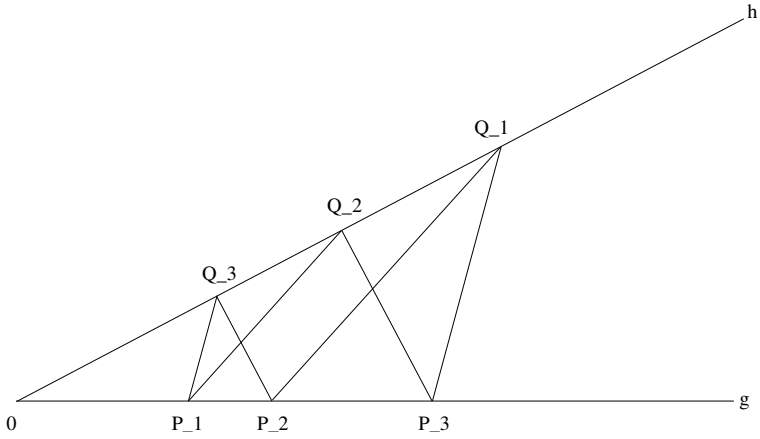

Abbildung 3.1: Satz von Pappus

Beweis : Sei $a = \overrightarrow{OP_1}$ und $b = \overrightarrow{OQ_3}$. Diese beiden Vektoren bilden eine Basis von $\mathbb{R}^2$. Wir schreiben $p_i = \overrightarrow{OP_i}$ und $q_i = \overrightarrow{OQ_i}$. Dann ist $p_i = \lambda_i a$ und $q_i = \mu_i b$ und die λ_i und μ_i sind alle von Null verschieden. Die Voraussetzung ist äquivalent dazu, dass $\overrightarrow{P_1Q_2}$ und $\overrightarrow{P_2Q_1}$ linear abhängig sind, sowie dass $\overrightarrow{P_2Q_3}$ und $\overrightarrow{P_3Q_2}$ linear abhängig sind. Es gilt $\overrightarrow{P_iQ_j} = \overrightarrow{OQ_j} - \overrightarrow{OP_i} = \mu_j b - \lambda_i a$. Wir wissen also, dass $\mu_2 b - \lambda_1 a$ und $\mu_1 b - \lambda_2 a$ linear abhängig sind, sowie dass $\mu_3 b - \lambda_2 a$ und $\mu_2 b - \lambda_3 a$ linear abhängig sind. Da a und b linear unabhängig sind, folgt daraus, dass $\lambda_1\mu_1 = \lambda_2\mu_2$ und $\lambda_2\mu_2 = \lambda_3\mu_3$. Daraus folgt $\lambda_1\mu_1 = \lambda_3\mu_3$ und weiter, dass $\mu_3 b - \lambda_1 a = \overrightarrow{P_1Q_3}$ und $\mu_1 b - \lambda_3 a = \overrightarrow{P_3Q_1}$ linear abhängig sind. Dies impliziert die Behauptung. □

3.3 Affine Abbildungen

Die folgende Definition ist so konzipiert, dass alle wesentlichen Begriffe der affinen Geometrie (Parallelität, Teilverhältnisse, ...) unter affinen Abbildungen erhalten bleiben.

Definition 3.18 *Seien $\mathbb{A}^n$ und $\mathbb{B}^p$ zwei affine Räume über dem selben Grundkörper K. Eine Abbildung $F : \mathbb{A}^n \to \mathbb{B}^p$ heißt affin, wenn für alle $P, Q, R, T \in \mathbb{A}^n$ und alle $\lambda \in K$ gilt:*

$$\textit{Aus} \quad \overrightarrow{PQ} = \lambda \cdot \overrightarrow{RT} \quad \textit{folgt} \quad \overrightarrow{F(P)F(Q)} = \lambda \overrightarrow{F(R)F(T)}.$$

Seien V und W die zugrundeliegenden Vektorräume von $\mathbb{A}^n$ bzw. $\mathbb{B}^p$.

Beispiel 3.19 i) Als *Translation* um $v \in V$ bezeichnet man die affine Abbildung $T_v : \mathbb{A}^n \to \mathbb{A}^n$ mit $\overrightarrow{PT_v(P)} = v$ für alle $P \in \mathbb{A}^n$. Diese hat die Eigenschaft

$$\begin{aligned}\overrightarrow{T_v(P)T_v(Q)} &= \overrightarrow{T_v(P)P} + \overrightarrow{PQ} + \overrightarrow{QT_v(Q)} \\ &= -v + \overrightarrow{PQ} + v = \overrightarrow{PQ}.\end{aligned}$$

ii) Als *Streckung* mit Zentrum Z und Streckfaktor $\lambda \in K$ bezeichnet man die Abbildung $\sigma_\lambda : \mathbb{A}^n \to \mathbb{A}^n$ mit $\overrightarrow{Z\sigma_\lambda(P)} = \lambda\overrightarrow{ZP}$ für alle $P \in \mathbb{A}^n$.

iii) Als *Scherung* $S_g : \mathbb{A}^2 \to \mathbb{A}^2$ entlang der Gerade g bezeichnet man folgende affine Abbildung. Sei $[v_1] \subset V$ der zu g gehörige Unterraum und $\{v_1, v_2\}$ eine Basis von V. Sei $A = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ die Abbildungsmatrix einer linearen Abbildung $f : V \to V$.

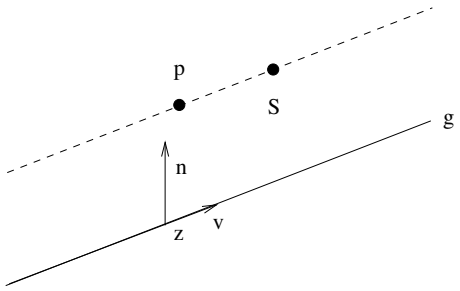

Abbildung 3.2: Scherung entlang einer Geraden

Dann gelte für alle $P \in \mathbb{A}^2$ und $Z \in g$:

$$\overrightarrow{ZS_g(P)} = f(\overrightarrow{ZP}).$$

Die Streckung hängt von der Basiswahl in V und $t \in K$ ab.

Satz 3.20 *Zu jeder affinen Abbildung $F : \mathbb{A}^n \to \mathbb{B}^p$ gibt es genau eine lineare Abbildung $f : V \to W$ mit*

$$f(\overrightarrow{PQ}) = \overrightarrow{F(P)F(Q)} \qquad \textit{für alle } P, Q \in \mathbb{A}^n. \tag{3.1}$$

Beweis : Zunächst bestimmt (3.1) eindeutig eine Abbildung $f : V \to W$. Ist $v \in V$, so wähle $P \in \mathbb{A}^n$ und dann $Q \in \mathbb{A}^n$ mit $\overrightarrow{PQ} = v$. Dann ist $f(v) = \overrightarrow{F(P)F(Q)}$ und somit f eindeutig festgelegt. Hat man statt P einen anderen "Aufpunkt" R gewählt und S mit $\overrightarrow{RS} = v$, so folgt aus der Definition einer affinen Abbildung, dass $f(v) = \overrightarrow{F(P)F(Q)} = \overrightarrow{F(R)F(S)}$.

Wir weisen noch Linearität der oben definierten Abbildung f nach. Seien $v, w \in V$ mit $\overrightarrow{PQ} = v$ und $\overrightarrow{QR} = w$. Dann ist

$$\begin{aligned} f(v+w) &= f(\overrightarrow{PQ} + \overrightarrow{QR}) = f(\overrightarrow{PR}) = \overrightarrow{F(P)F(R)} \\ &= \overrightarrow{F(P)F(Q)} + \overrightarrow{F(Q)F(R)} = f(\overrightarrow{PQ}) + f(\overrightarrow{QR}) \\ &= f(v) + f(w). \end{aligned}$$

Ist $\lambda \cdot v = \overrightarrow{PR}$, so folgt $f(\lambda v) = f(\overrightarrow{PR}) = \overrightarrow{F(P)F(R)} = \lambda\overrightarrow{F(P)F(Q)} = \lambda f(\overrightarrow{PQ}) = \lambda f(v)$. □

Umgekehrt ist eine affine Abbildung durch Vorgabe eines Aufpunkts, dessen Bild und einer linearen Abbildung gegeben.

Satz 3.21 *Sei $f : V \to W$ linear, $Z \in \mathbb{A}^n, Z' \in \mathbb{B}^p$ beliebig. Dann ist*

$$F : \left\{ \begin{array}{ccc} \mathbb{A}^n & \to & \mathbb{B}^p \\ P & \mapsto & F(P) \end{array} \right. \quad \textit{mit } f(\overrightarrow{ZP}) = \overrightarrow{Z'F(P)}$$

die einzige affine Abbildung, deren zugehörige lineare Abbildung f ist und die Z auf Z' abbildet.

Beweis : Wir prüfen, dass F eine affine Abbildung definiert. Es ist

$$\begin{aligned} f(\overrightarrow{PQ}) &= f(\overrightarrow{ZQ} - \overrightarrow{ZP}) = f(\overrightarrow{ZQ}) - f(\overrightarrow{ZP}) \\ &= \overrightarrow{Z'F(Q)} - \overrightarrow{Z'F(P)} = \overrightarrow{F(P)F(Q)}. \end{aligned}$$

Da f linear ist, folgt aus $\overrightarrow{PQ} = \lambda\overrightarrow{RT}$ die Gleichung $f(\overrightarrow{PQ}) = \lambda f(\overrightarrow{RT})$ und aus obiger Rechnung $\overrightarrow{F(P)F(Q)} = \lambda\overrightarrow{F(R)F(T)}$, was zu zeigen war. Offenbar gehört zu F die lineare Abbildung f. Sind F und G zwei affine Abbildungen mit $F(Z) = Z' = G(Z)$ und zugehöriger linearer Abbildung f, so ist

$$\overrightarrow{Z'F(X)} = f(\overrightarrow{ZX}) = \overrightarrow{Z'G(X)}$$

und nach der Eindeutigkeit in Axiom i) eines affinen Raumes folgt $F = G$. □

Damit können wir einige Objekte und Eigenschaften auflisten, die unter einer affinen Abbildung invariant sind.

Satz 3.22 *Sei $F : \mathbb{A}^n \to \mathbb{B}^p$ affin. Dann gilt*

i) Ist $\mathbb{D} \subseteq \mathbb{A}^n$ ein affiner Unterraum mit zugehörigem Vektorraum U, so ist $F(\mathbb{D})$ ein affiner Unterraum von $\mathbb{B}^p$ mit zugehörigem Unterraum $f(U)$, wobei f die lineare Abbildung zu F aus Satz 3.20 ist.

ii) Sind $\mathbb{D}_1, \mathbb{D}_2 \subseteq \mathbb{A}^n$ parallele affine Unterräume, so sind auch $F(\mathbb{D}_1)$ und $F(\mathbb{D}_2)$ parallel.

iii) F lässt Teilverhältnisse unverändert, d.h. für drei kollineare Punkte $X, P, Q \in \mathbb{A}^n$ mit $Q \neq X$ gilt:

$$\tau(X, P, Q) = \tau\big(F(X), F(P), F(Q)\big),$$

falls $F(Q) \neq F(X)$.

Beweis : Sei $P \in \mathbb{D}$. Nach Proposition 3.1 gilt

$$U = \Phi_P(\mathbb{D}) = \{\overrightarrow{PQ} : Q \in \mathbb{D}\}.$$

Nach Satz 3.20 folgt

$$f(U) = \{f(\overrightarrow{PQ}) : Q \in \mathbb{D}\} = \{\overrightarrow{F(P)F(Q)} : Q \in \mathbb{D}\} = \Phi_{F(P)}(F(\mathbb{D})).$$

Daher ist $F(\mathbb{D})$ ein affiner Unterraum von $\mathbb{B}^p$ mit zugehörigem Unterraum $f(U)$. Das zeigt i). Die Eigenschaft ii) folgt aus i) und der Definition von Parallelität direkt. Zum Beweis von iii) sei $\tau(X, P, Q) = \lambda$, also $\overrightarrow{XP} = \lambda\overrightarrow{XQ}$. Nach Definition einer affinen Abbildung folgt direkt

$$\overrightarrow{F(X)F(P)} = \lambda\overrightarrow{F(X)F(Q)}$$

und damit die Behauptung. □

Unter allen affinen Abbildungen haben wir bereits in den einführenden Beispielen zumeist affine Selbstabbildungen $F\colon \mathbb{A}^n \longrightarrow \mathbb{A}^n$ untersucht. Unter diesen sind die bijektiven Selbstabbildungen, genannt *Affinitäten*, besonders wichtig.

Satz 3.23 *Die Menge* $\mathrm{Aff}(\mathbb{A}^n)$ *der Affinitäten von* $\mathbb{A}^n$ *bildet eine Gruppe, die* affine Gruppe *von* $\mathbb{A}^n$.

Beweis : Das Verknüpfen affiner Abbildungen ist offenbar eine affine Abbildung, wie man an der Definition direkt abliest. Neutrales Element ist die Identitätsabbildung. Sei F bijektiv und affin. Wir rechnen nach, dass F^{-1} affin ist. Sei

$$\overrightarrow{PQ} = \lambda\overrightarrow{RT}$$

und $Z \in \mathbb{A}^n$ der eindeutig bestimmte Punkt, sodass

$$\overrightarrow{F^{-1}(P)Z} = \lambda\overrightarrow{F^{-1}(R)F^{-1}(T)}.$$

Anwendung von F ergibt $\overrightarrow{PF(Z)} = \lambda\overrightarrow{RT}$ und nach der Eindeutigkeit folgt $Q = F(Z)$ oder $Z = F^{-1}(Q)$, was zu zeigen war. □

Aufgrund von Satz 3.23 können wir affine Abbildungen $F\colon \mathbb{A}^n \longrightarrow \mathbb{B}^p$ in Koordinaten darstellen. Seien dazu $O \in \mathbb{A}^n$, $O' \in \mathbb{B}^p$ und $\{b_1, \ldots, b_n\}$ bzw. $\{c_1, \ldots, c_p\}$ Basen von V bzw. W. Sei A die Abbildungsmatrix der zu F gehörigen linearen Abbildung und $a = \overrightarrow{O'F(O)}$. Ist $X \in \mathbb{A}^n$ und $\overrightarrow{x} \in K^n$ der zu $\overrightarrow{OX}$ gehörige Koordinatenvektor bzgl. $\{b_1, \ldots, b_n\}$ sowie $\overrightarrow{x'} \in K^p$, der zu $\overrightarrow{O'F(X)}$ gehörige Koordinatenvektor, so gilt

$$\begin{aligned}\overrightarrow{O'F(X)} &= \overrightarrow{O'F(O)} + \overrightarrow{F(O)F(X)} \\ &= a + f(\overrightarrow{OX}),\end{aligned}$$

also haben wir Koordinaten

$$\overrightarrow{x'} = \overrightarrow{a} + A \cdot \overrightarrow{x}, \tag{3.2}$$

wobei $\overrightarrow{a}$ der Koordinatenvektor von a bzgl. $\{c_1, \ldots, c_p\}$ ist. Umgekehrt prüft man mit Hilfe von Satz 3.21 leicht nach, dass jede Abbildung, die in Koordinaten durch (3.2) gegeben ist, eine affine Abbildung ist.

4 Euklidische affine Räume

Dieser Abschnitt ist auf das Verständnis unseres Anschauungsraumes, der „Welt, in der wir leben“ ausgerichtet und beinhaltet im Vergleich zum vorigen Abschnitt zusätzlich einen Abstandsbegriff. Wir wählen daher hier den Grundkörper $K = \mathbb{R}$. In fortgeschritteneren Vorlesungen (Differentialgeometrie, komplexe Algebraische Geometrie) wird zusätzlich der Begriff der Krümmung von Räumen mit Abstandsbegriffen eingeführt. Dann erkennt man, dass euklidische affine Räume der relativ einfach Fall ohne Krümmung ist.

Definition 4.1 *Ein euklidischer affiner Raum $\mathbb{E}$ ist ein affiner Raum $(\mathbb{E}, \phi)$, dessen zugrundeliegender Vektorraum ein euklidischer Vektorraum $(V, \langle\ ,\ \rangle)$ ist.*

Ist $\dim \mathbb{E} = n$, so schreiben wir wieder $\mathbb{E}^n$. Das Skalarprodukt erlaubt die Definition einer Abstandsfunktion

$$\begin{aligned}d\colon \mathbb{E} \times \mathbb{E} &\longrightarrow \mathbb{R} \\ (P, Q) &\longmapsto \|\phi(P, Q)\| = \|\overrightarrow{PQ}\|.\end{aligned}$$

Aus den Eigenschaften der Norm folgt sofort:

Proposition 4.2 *Die Abstandsfunktion eines euklidischen affinen Raumes erfüllt*

$d(P, Q) \geqslant 0 \quad \textit{und} \quad d(P, Q) = 0 \Longleftrightarrow P = Q$	*(Definitheit)*
$d(P, Q) = d(Q, P)$	*(Symmetrie)*
$d(P, R) \leq d(P, Q) + d(Q, R)$	*(Dreiecksungleichung)*

für alle $P, Q, R \in \mathbb{E}$.

Definition 4.3 *Ein Tupel $(O, e_1, \ldots, e_n)$ mit $O \in \mathbb{E}^n$ und einer Orthonormalbasis $\{e_1, \ldots, e_n\}$ von V heißt* kartesisches Koordinatensystem.

Ist $P \in \mathbb{E}^n$ ein beliebiger Punkt, so können wir

$$\overrightarrow{OP} = \sum_{i=1}^{n} \lambda_i e_i$$

schreiben. Wir nennen $(\lambda_1, \ldots, \lambda_n)$ die Koordinaten des Punktes P bzgl. des kartesischen Koordinatensystems $(O, e_1, \ldots, e_n)$. Umgekehrt gibt es zu $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ genau einen Punkt $P \in \mathbb{E}^n$ mit diesen vorgegebenen Koordinaten, nämlich den Punkt P mit $\overrightarrow{OP} = \sum_{i=1}^{n} \lambda_i e_i$. Der Vorteil eines kartesischen Koordinatensystems (d.h. der Eigenschaft, dass die e_i orthonormiert sind) besteht darin, dass sich Abstände leicht ausrechnen lassen. Sind $P = (\lambda_1, \ldots, \lambda_n)$ und $Q = (\mu_1, \ldots, \mu_n)$, so ist

$$d(P, Q) = \|\overrightarrow{PQ}\| = \|\sum_{i=1}^{n} (\mu_i - \lambda_i) e_i\| = \sqrt{\sum_{i=1}^{n} (\mu_i - \lambda_i)^2}.$$

Die naheliegendste Abstandsfolge ist die zweier affiner Unterräume $\mathbb{B}, \mathbb{B}'$ in $\mathbb{A}$. Dabei wollen wir als *Abstand* das Infimum der Abstände von Punkten in $\mathbb{B}$ bzw. $\mathbb{B}'$ definieren, in Zeichen

$$d(\mathbb{B}, \mathbb{B}') = \inf\{d(X, X') \ : \ X \in \mathbb{B}, X' \in \mathbb{B}'\}.$$

Wir zeigen, dass das Infimum angenommen wird und wie man es berechnet. Dazu verwenden wir die Orthogonalprojektion π aus Abschnitt 1.6.

Satz 4.4 *Sind $\mathbb{B}, \mathbb{B}'$ affine Unterräume von $\mathbb{E}^n$ mit zugehörigen Unterräumen W und W' sowie $P \in \mathbb{B}$ und $P' \in \mathbb{B}'$ gegeben, so gilt*

$$d(\mathbb{B}, \mathbb{B}') = \|\overrightarrow{PP'} - \pi(\overrightarrow{PP'})\|,$$

wobei π die orthogonale Projektion auf den Unterraum $W + W'$ ist.

Beweis : Wir schreiben die orthogonale Projektion π als

$$\pi : \left\{ \begin{array}{ccccccc} V & = & (W + W') & \oplus & (W + W')^{\perp} & \longrightarrow & V \\ v & = & y & + & z & \longrightarrow & y = w + w', \end{array} \right.$$

mit $w \in W$ und $w' \in W'$, wobei diese Zerlegung im Gegensatz zur Zerlegung $v = y + z$ nicht eindeutig ist. Insbesondere können wir $\pi(\overrightarrow{PP'}) = w_0 + w_0'$ schreiben, wobei $w_0 \in W, w_0' \in W'$ ist. Daher gibt es Punkte $L \in \mathbb{B}$ und $L' \in \mathbb{B}'$ („Lotfußpunkte“) mit $\overrightarrow{PL} = w_0$ und $\overrightarrow{L'P'} = w_0'$. Außerdem gilt $\overrightarrow{PP'} - \pi(\overrightarrow{PP'}) = \overrightarrow{LL'} \in (W + W')^{\perp}$. Mit diesen Bezeichnungen müssen wir also zeigen, dass

$$d(\mathbb{B}, \mathbb{B}') = \|\overrightarrow{LL'}\|$$

gilt. Das Infimum ist sicher durch $\|\overrightarrow{LL'}\|$ beschränkt, also $d(\mathbb{B},\mathbb{B}') \leq \|\overrightarrow{LL'}\|$. Andererseits gilt für alle $X \in \mathbb{B}$ und $X' \in \mathbb{B}'$:

$$\begin{aligned}\|\overrightarrow{XX'}\|^2 &= \| \underbrace{\overrightarrow{LL'}}_{\in (W+W')^\perp} + \underbrace{\left(\overrightarrow{XP} + \overrightarrow{P'X'} + \pi(\overrightarrow{PP'})\right)}_{\in (W+W')} \|^2 \\ &= \|\overrightarrow{LL'}\|^2 + \|\overrightarrow{XP} + \overrightarrow{P'X'} + \pi(\overrightarrow{PP'})\|^2 \geqslant \|LL'\|^2.\end{aligned}$$

Insbesondere gilt diese Ungleichung auch für das Infimum und daraus folgt die Behauptung. □

Aus diesem Beweis ergibt sich ein Algorithmus zur Bestimmung von $d(\mathbb{B},\mathbb{B}')$. Gesucht ist ein Punktepaar $L \in \mathbb{B}$ und $L' \in \mathbb{B}'$, sodass $\overrightarrow{LL'} \perp W$ und $\overrightarrow{LL'} \perp W'$. Denn für so ein Punktepaar ist $\mathbb{B} = \{X \in \mathbb{E}^n : \overrightarrow{LX} \in W\}$ und $\mathbb{B}' = \{X' \in \mathbb{E}^n : \overrightarrow{L'X'} \in W'\}$ und $d(\mathbb{B},\mathbb{B}') = \|\overrightarrow{LL'} - \pi(\overrightarrow{LL'})\| = \|\overrightarrow{LL'}\|$. Um so ein Punktepaar zu finden, wählt man eine Basis $\{b_1,\ldots,b_r\}$ von W und eine Basis $\{b'_1,\ldots,b'_s\}$ von W'. Man macht den Ansatz

$$\overrightarrow{OL} = \ell = p + \sum_{i=1}^{r} \lambda_i b_i, \quad \overrightarrow{OL'} = \ell' = p' + \sum_{k=1}^{s} \mu_k b'_k,$$

wobei $p = \overrightarrow{OP}$ und $p' = \overrightarrow{OP'}$. Die Unbekannten $\lambda_1,\ldots,\lambda_r$ und $\mu_1,\ldots,\mu_s$ bestimmt man aus dem Gleichungssystem.

$$\begin{aligned}\langle \ell - \ell', b_i\rangle &= 0 \quad \text{für} \quad i = 1,\ldots,r \\ \langle \ell - \ell', b'_k\rangle &= 0 \quad \text{für} \quad k = 1,\ldots,s.\end{aligned}$$

Dieses homogene Gleichungssystem hat $r+s$ Gleichungen für $r+s$ Unbestimmte. Es hat also stets eine Lösung, welche im Allgemeinen nicht eindeutig ist.

4.1 Bewegungen

Definition 4.5 *Eine affine Selbstabbildung des $\mathbb{E}^n$, deren zugehörige lineare Abbildung eine Isometrie ist, heißt* Bewegung.

Ist F eine Bewegung, so läßt F Abstände unverändert, denn es gilt

$$d\big(F(X),F(Y)\big) = \|\overrightarrow{F(X)F(Y)}\| = \|f(\overrightarrow{XY})\| = \|\overrightarrow{XY}\| = d(X,Y).$$

Überraschend ist, dass auch die Umkehrung dieser Aussage gilt.

Satz 4.6 *Ist $F : \mathbb{E}^n \longrightarrow \mathbb{E}^n$ eine Selbstabbildung, die alle Abstände invariant läßt, ist eine Bewegung.*

Wir bemerken, dass a priori noch nicht einmal vorausgesetzt ist, dass F affin ist. Zum Beweis verwenden wir folgendes Lemma.

Lemma 4.7 *Vier Punkte $A, B, C, D \in \mathbb{E}^n$ sind genau dann (in dieser Reihenfolge) Ecken eines Parallelogramms (d.h. es gilt $\overrightarrow{AB} = \overrightarrow{DC}$), wenn gilt:*

$$d^2(A,B) + d^2(B,C) + d^2(C,D) + d^2(D,A) = d^2(A,C) + d^2(B,D). \tag{4.1}$$

Sei V der Vektorraum, der $\mathbb{E}^n$ zugrundeliegt.

Beweis des Satzes : Wir definieren eine Abbildung

$$f\colon V \longrightarrow V \quad \text{durch} \quad f(\overrightarrow{AB}) = \overrightarrow{F(A)F(B)}$$

und zeigen sukzessive, dass f wohldefiniert, linear und schließlich eine Isometrie ist. Ist $\overrightarrow{AB} = \overrightarrow{DC}$, so gilt nach dem Lemma und der Voraussetzung über F, dass

$$\begin{aligned} d^2\big(F(A),F(B)\big) + d^2\big(F(B),F(C)\big) + d^2\big(F(C),F(D)\big) + d^2\big(F(D),F(A)\big) \\ = d^2\big(F(A),F(C)\big) + d^2\big(F(B),F(D)\big). \end{aligned}$$

Die umgekehrte Implikation des Lemmas besagt, dass $\overrightarrow{F(A)F(B)} = \overrightarrow{F(D)F(C)}$ und damit, dass f wohldefiniert ist. Weiter ist

$$\|f(x)\| \;=\; \|f(\overrightarrow{AB})\| \;=\; \|\overrightarrow{F(A)F(B)}\| \;=\; \|\overrightarrow{AB}\| \;=\; \|x\|, \tag{4.2}$$

wobei wir A und B in $\mathbb{E}^n$ mit $\|x\| = \|\overrightarrow{AB}\|$ gewählt haben. Sind $x, y \in V$ gegeben, so wählen wir $A, B \in \mathbb{E}^n$ mit $\overrightarrow{AB} = x$ und sodann $C \in \mathbb{E}^n$, sodass $\overrightarrow{BC} = y$. Also ist

$$\begin{aligned} f(x+y) &= f(\overrightarrow{AB} + \overrightarrow{BC}) = f(\overrightarrow{AC}) = \overrightarrow{F(A)F(C)} \\ &= \overrightarrow{F(A)F(B)} + \overrightarrow{F(B)F(C)} = f(\overrightarrow{AB}) + f(\overrightarrow{BC}) = f(x) + f(y) \end{aligned}$$

Aus der Additivität folgt für $k \in \mathbb{Z}$, das $f(k \cdot x) = k \cdot f(x)$ ist. Angewandt auf $y = \frac{1}{k}x$ folgt $f(y) = k \cdot f(\frac{1}{k}x)$, also $f(qx) = q \cdot f(x)$ für alle $q \in \mathbb{Q}$ und alle $x \in V$. Da F Abstände bewahrt, ist F und somit auch f stetig. Also gilt $f(rx) = rf(x)$ für alle $r \in \mathbb{R}$ und f ist linear. Aus (4.2) folgt, dass f in der Tat eine Isometrie ist.

Die Eigenschaft 'F affin' folgt jetzt auch aus der Linearität von f, und der Wohldefiniertheit, alos: Falls $\overrightarrow{PQ} = \lambda\overrightarrow{RS}$ mit $\lambda \in \mathbb{R}$, so haben wir im Wesentlichen schon gesehen, dass

$$\overrightarrow{F(P)F(Q)} \;=\; f(\overrightarrow{PQ}) \;=\; f(\lambda\overrightarrow{RS}) \;=\; \lambda f(\overrightarrow{RS}) \;=\; \lambda\overrightarrow{F(R)F(S)}\,.$$

□

Beweis des Lemmas : Wir verwenden, dass ein Viereck $ABCD$ ein Parallelogramm ist, genau dann wenn sich die Diagonalen in ihren Mittelpunkten schneiden. (Übung!)

Es sei $a = \overrightarrow{AB}, b = \overrightarrow{BC}, c = \overrightarrow{CD}$ und $d = \overrightarrow{DA}$. Ferner sei $e = \overrightarrow{AC}$ und $f = \overrightarrow{BD}$. Der Verbindungsvektor x der Mittelpunkte der Diagonalen ist also

$$x = a + \frac{f}{2} - \frac{e}{2} = a - \frac{a+d}{2} - \frac{a+b}{2} = -\frac{b+d}{2} = \frac{a+c}{2}.$$

Außerdem gilt natürlich $a + b + c + d = 0$. Aus der Rechnung

$$\begin{aligned}
&\|a\|^2 + \|b\|^2 + \|c\|^2 + \|d\|^2 - \|e\|^2 - \|f\|^2 \\
&= \langle a, a\rangle + \langle b, b\rangle + \langle c, c\rangle + \langle d, d\rangle - \langle a+b, a+b\rangle - \langle a+d, a+d\rangle \\
&= \langle c, c\rangle - \langle a, a\rangle - 2\langle a, b\rangle - 2\langle a, d\rangle = \langle c, c\rangle + \langle a, a\rangle + 2\langle a, c\rangle \\
&= \langle a+c, a+c\rangle = 4\|x\|^2.
\end{aligned}$$

folgt, dass die Gleichung (4.1) genau dann gilt, wenn $x = 0$. □

Beispiel 4.8 2011 fand die Frauenfußballweltmeisterschaft in Deutschland statt. Zu Beginn des Eröffnungsspiels Deutschland - Kanada und zu Beginn der 2. Halbzeit lag der Ball auf dem Anstoßpunkt des Berliner Stadions. Zeigen Sie, dass zu diesen zwei Zeitpunkten mindestens 2 Punkte an der Oberfläche des Balles auf dem gleichen Punkt lagen.
Die Bewegungen des Balles während der ersten Halbzeit sind eine affine Abbildung F, dessen zugehörige lineare Abbildung eine Isometrie ist. Außerdem wird der Mittelpunkt M un die Orientierung des Balles unter F festgelassen. Ist $\{b_1, b_2, b_3\}$ eine ONB des $\mathbb{R}^3$, so wird F bzgl. dem kartesischen Koordinatensystem $(M, \{b_1, b_2, b_3\})$ beschrieben als

$$F\colon x \longmapsto x' = A \cdot x,$$

wobei A die Abbildungsmatrix einer Isometrie mit $\det(A) = +1$ ist. Wir können die Basis $\{b_1, b_2, b_3\}$ so wählen, dass A in Normalform ist. Da $\dim \mathbb{R}^3 = 3$ ungerade ist, hat diese Normalform möglicherweise ein Drehkästchen, sicher aber die Gestalt

$$A = \begin{pmatrix} +1 & 0 & 0 \\ 0 & ? & ? \\ 0 & ? & ? \end{pmatrix}.$$

Ist r der Radius des Balles, so werden also die Punkte $(\pm r, 0, 0)^T$ auf der Oberfläche von F fixiert.

Wir nehmen das Beispiel als Anlass und wollen die Bewegungen des $\mathbb{R}^n$ klassifizieren. Im Beispiel war es sehr angenehm, dass F einen Fixpunkt hat.

Lemma 4.9 *Wenn F keinen Fixpunkt hat, so hat die zugehörige Isometrie den Eigenwert $+1$.*

Beweis : Sei $F(x) = A \cdot x + a$ die Darstellung von F in einem Koordinatensystem. Falls A nicht den Eigenwert $+1$ hat, so ist $(A - E)$ regulär, also hat $(A - E) \cdot x = -a$ eine Lösung $x \neq 0$. Diese ist ein Fixpunkt von F. □

Bewegungen mit Fixpunkt: Hat F einen Fixpunkt, so wählen wir diesen als Ursprung eines kartesischen Koordinatensystems. Wir wählen die ONB wiederum so, dass die Isometrie in Normalform ist, also

$$x' = A \cdot x \quad \text{mit}$$

$$A = \begin{pmatrix} \boxed{\begin{matrix} +1 & & \\ & \ddots & \\ & & +1 \end{matrix}} & & & & 0 \\ & \boxed{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}} & & & \\ & & \boxed{\begin{matrix} \cos w_1 & -\sin w_1 \\ \sin w_1 & \cos w_1 \end{matrix}} & & \\ & & & \ddots & \\ 0 & & & & \boxed{\begin{matrix} \cos w_r & -\sin w_r \\ \sin w_r & \cos w_r \end{matrix}} \end{pmatrix}.$$

Bewegungen ohne Fixpunkt: Wir wählen zunächst einen beliebigen Ursprung O, aber zumindest eine ONB von $\mathbb{R}^n$, sodass die Isometrie Normalform hat. Seien $\{b_1, \ldots, b_k\}$ für $k \leqslant n$ die Eigenvektoren zum Eigenwert $+1$ und

$$F\colon x \longmapsto x' = A \cdot x + a.$$

Wir wollen a durch $\widetilde{a}$ ersetzen, das zwar nicht Null, aber zumindest relativ einfach ist. Ist O' ein anderer Ursprung und $F(x) = Ax + \widetilde{a}$ die Darstellung von F bzgl. dem kartesischen Koordinatensystem $(O', b_1, \ldots, b_n)$, so gilt mit $c = \overrightarrow{O'O}$

$$\widetilde{a} = \overrightarrow{O'F(O')} = \overrightarrow{O'O} + \overrightarrow{OF(O)} + \overrightarrow{F(O)F(O')} = c + a - A \cdot c,$$

also $\widetilde{a} = a - (A - E) \cdot c$. Sei $U = [b_1, \ldots, b_k]$. Dann gilt $\pi_U(\widetilde{a}) = \pi_U(a)$ und die Einschränkung der linearen Abbildung $f(x) = A \cdot x$ auf $U^\perp$ hat keinen Eigenwert $+1$. Also ist $(f - id)_{U^\perp}$

invertierbar und wir können c so wählen, dass $\pi_{U^\perp}(a) = (f - id)|_{U^\perp}(c)$ ist, also $\pi_{U^\perp}(\widetilde{a}) = 0$. In Koordinaten haben wir dann $F(x) = A \cdot x + \widetilde{a}$ mit

$$A = \begin{pmatrix} \boxed{\begin{matrix} +1 & & \\ & \ddots & \\ & & +1 \end{matrix}} & & & & 0 \\ & \boxed{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}} & & & \\ & & \boxed{\begin{matrix} \cos w_1 & -\sin w_1 \\ \sin w_1 & \cos w_1 \end{matrix}} & & \\ & & & \ddots & \\ 0 & & & & \boxed{\begin{matrix} \cos w_r & -\sin w_r \\ \sin w_r & \cos w_r \end{matrix}} \end{pmatrix}$$

und $\widetilde{a} = (a_1, \ldots, a_k, 0, \ldots, 0)^T$.

Beispiel 4.10 Wir spezialisieren auf Dimension zwei. Die Bewegungen mit Fixpunkt wurden nach obigen Überlegungen im Kapitel über Isometrienormalformen klassifiziert. Es sind dies Identität, Geradenspiegelung, Punktspiegelung und Drehung um einen Fixpunkt. Es gibt zwei Normalformen mit Eigenwert $+1$, nämlich

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Zu A_1 gehören Translationen, wobei a beliebig ist. Im Fall von A_2 können wir die erste Komponente von a gleich Null erreichen. Wir erhalten damit *Schubspiegelungen*, wobei die Verschiebung in Richtung der Fixachse stattfindet.

5 Axiomatische Geometrie

Man kann ebene affine Geometrie auch axiomatisch beginnen, indem man die Eigenschaften von Geraden hinsichtlich Schnitt und Parallelität axiomatisch formuliert. Damit wird der affine Raum $\mathbb{A}^2$ aus Abschnitt 3 ein Beispiel von folgender Definition. Wir verwenden dabei folgende Begriffe. Gegeben zwei Geraden g, h nennen wir die Menge aller Punkte P mit $P \in g$ und $P \in h$ die *Schnittpunkte* von g und h und schreiben hierfür $g \cap h$. Wir nennen eine Menge M von Punkten *kollinear*, falls es eine Gerade g gibt mit $P \in g$ für alle $P \in M$. Wir nennen zwei Geraden $g, h \in \mathcal{G}$ *parallel*, falls $g = h$ oder $g \cap h = \emptyset$. Wir schreiben dafür $g||h$.

Definition 5.1 *Eine* ebene affine Geometrie *besteht aus einer Menge $\mathcal{P}$ von* Punkten, *einer Menge $\mathcal{G}$ von* Gerade *und einer Relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{G}$ mit folgenden Eigenschaften, in denen wir statt $(P, g) \in \mathcal{I}$ auch P* liegt auf g oder $P \in g$ *sagen.*

(V) Durch je zwei Punkte geht genau eine Gerade, d.h. zu $P, Q \in \mathcal{P}$ mit $P \neq Q$ gibt es genau ein $g \in \mathcal{G}$ mit $P \in g$ und $Q \in g$.
(G) Auf jeder Geraden liegen mindestens zwei Punkte.
(R) Es gibt vier Punkte, von denen je drei nicht kollinear sind.
(P) Zu $g \in \mathcal{G}$ und $P \in \mathcal{P}$ mit $P \notin g$ gibt es genau eine Gerade $h \in \mathcal{G}$ mit $P \in h$ und $g||h$.

Zu $P, Q \in \mathcal{P}$ bezeichnen wir mit $\overline{PQ}$ die eindeutige *Verbindungsgerade* nach Axiom (V). Die Axiome werden demzufolge auch als *Verbindungsaxiom*, *Geradenaxion*, *Reichhaltigkeitsaxiom* und *Parallelenaxiom* bezeichnet.

Eine Gerade wird durch die Punkte festgelegt, die auf ihr liegen:

Lemma 5.2 *Die Abbildung $\iota : \mathcal{G} \to \{M : M \subset \mathcal{P}\}$ definiert durch $\iota(g) = \{P : P \in g\}$ ist injektiv und es gilt zudem*

$$\iota(g) \subset \iota(h) \quad \textit{impliziert} \quad g = h$$

für $g, h \in \mathcal{G}$.

Beweis : Wir betrachten zwei Geraden mit der Eigenschaft $\iota(g) \subset \iota(h)$. Nach Axiom (G) gibt es zwei Punkte P, Q auf g und somit nach (V) genau eine Verbindungsgerade dieser zwei Punkte. Da h auch eine Verbindungsgerade dieser Punkte ist, besagt die Eindeutigkeit in (V), dass $g = h$. □

Das einfachste Beispiel ist die sogenannte *affine Ebene der Ordnung* 2 bestehend aus den Punkten $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ und

$$\mathcal{G} \;=\; \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}\,.$$

Manchmal wird das Reichhaltigkeitsaxiom nur in der abgeschwächten Version gefordert, dass es eine Gerade g und einen Punkt P gibt mit $P \notin G$. In diesem Axiomensystem gibt es dann auch eine ebene Geometrie mit drei Punkten. Die Frage, ob das Parallelenaxiom unabhängig von den anderen Axiomen ist, war lange Gegenstand von Diskussionen. Die hyperbolische Ebene ist ein Beispiel einer Geometrie, bei der die Eindeutigkeit im Parallelaxiom nicht erfüllt ist.

Aus dem Axiom (V) folgt auch sofort, dass zwei Geraden sich schneiden oder parallel sind. Direkt aus der Definition folgt auch:

Lemma 5.3 *Parallelität ist eine Äquivalenzrelation.*

Die Äquivalenzklasse von g unter dieser Relation wird die zugehörige *Parallelenschar* $P(g) = \{h \in \mathcal{G} : h||g\}$ genannt. Zwei verschiedene Parallelenscharen sind disjunkt und aus (R) folgt, dass es mindesten 3 verschiedene Parallelenscharen gibt.

Wir diskutieren im folgenden etwas die Struktur von *endlichen* ebenen Geometrien. In diesem Fall ist bereits interessant für welche (n, m) es Geometrien mit $|\mathcal{P}| = n$ und $|\mathcal{G}| = m$ gibt. Der folgende Satz setzt Endlichkeit nicht voraus, gibt aber im endlichen Fall eine Beziehung zwischen m und n.

Satz 5.4 *Auf jeder Parallelenschar π liegen gleich viele Geraden. Ihre Anzahl ist gleich der Anzahl der Punkte auf jeder Geraden. Diese Anzahl wird* Ordnung der affinen Ebene *genannt.*

Beweis : Seien $P(g_1)$ und $P(g_2)$ zwei verschiedene Parallelscharen. Dann ist $g_1 \nparallel g_2$ und für jeden Punkt $P \in g_1$ gibt es genau eine Gerade h mit $h \parallel g_2$ und $P \in h$. Andererseits existiert für $h \parallel g_2$ genau ein Schnittpunkt $P \in h \cap g_1$ (da wir oben festgestellt haben, das Doppelschnittpunkte nicht-paralleler Geraden unmöglich sind). Wir erhalten also eine Bijektion $g_1 \longleftrightarrow P(g_2)$ zwischen Punkten auf g_1 und Parallelen zu g_2. Das heißt insbesondere, dass g_1 und $P(g_2)$ gleich viele Elemente haben.

Es folgt, dass auf jeder Parallelenschar gleich viele Elemente liegen, denn für Parallenscharen $P(g_1)$ und $P(g_2)$, die verschieden sind, existiert (wie oben gezeigt) eine dritte Parallelenschar $P(g_3)$ mit $P(g_3) \neq P(g_1)$ und $P(g_3) \neq P(g_2)$. Also gibt es zwei Bijektionen

$$P(g_1) \longleftrightarrow g_3 \longleftrightarrow P(g_2)$$

und daraus folgt die Behauptung.

Ebenso liegen auf jeder Geraden gleich viele Punkte. Denn zu zwei Geraden g_1, g_2 gibt es eine Gerade g_3 mit $g_3 \nparallel g_1$ und $g_3 \nparallel g_2$ und dann zwei Bijektionen

$$g_1 \longleftrightarrow P(g_3) \longleftrightarrow g_2 \,.$$

Wir haben also gezeigt, dass die Anzahl der Punkte auf einer Geraden gleich der Anzahl der Geraden h einer Parallelenschar ist. □

Satz 5.5 *Sei $(\mathcal{P}, \mathcal{G})$ eine affine Ebene der Ordnung $n < \infty$. Dann hat $(\mathcal{P}, \mathcal{G})$ genau n^2 Punkte und $n^2 + n$ Geraden.*

Beweis : Sei $P(g)$ eine Parallelenschar. Dann liegen n Geraden in $P(g)$ und auf jeder dieser Geraden liegen n Punkte. Es gibt also insgesamt n^2 Punkte, weil alle Punkte der affinen Ebene auf einer Geraden in $P(g)$ liegen (Parallelenaxiom). Sei nun $P \in \mathcal{P}$ ein fester Punkt. Man zeigt leicht, dass durch P genau $n + 1$ Geraden gehen (Übung!). Außerdem geht von jeder Parallelenschar genau eine Gerade durch P (Parallelenaxiom). Es gibt also $n + 1$ Parallelenscharen und in jeder Parallelenschar liegen n Geraden. Insgesamt sind das $n(n+1) = n^2 + n$ Geraden. □

Es ist ein offenes Problem, welche natürlichen Zahlen n als Ordnungen von affinen Ebenen auftreten. Es ist nur bekannt, dass alle Primzahlpotenzen, d.h. $n = p^r$ mit p prim und $r \in \mathbb{N}$ auftreten. Es ist auch bekannt, dass keine affinen Ebenen der Ordnungen 6 und 10 existieren. Bereits für Ordnung 12 ist die Existenzfrage bis heute ungelöst.

Das genannte Axiomensystem reicht bei Weitem nicht aus, um alle Sätze der ebenen affinen Geometrie in diesem Skript herzuleiten. Insbesondere die Sätze von Desargues und Pappos folgen nicht daraus. D.h. es gibt ebene affine Geometrien wie die **Moulton-Ebene**, in der der Satz von Desargues nicht gilt!

Die Punkte der **Moulton-Ebene** sind die Punkte der reellen Ebene $\mathbb{R}^2$ und die Geraden sind die Geraden der reellen Ebene mit der Ausnahme, dass Geraden mit negativer Steigung an der y-Achse einen Knick haben: In der rechten Halbebene ist die Steigung doppelt so groß wie in der linken Halbebene. Die Geraden mit Steigung ∞, also die Parallelen zur y-Achse, sind auch Geraden in der Moulton-Ebene, ohne Knick. Formaler ist

$$\begin{aligned} \mathcal{P} &= \mathbb{R}^2 \\ \mathcal{G} &= (\mathbb{R} \cup \infty) \times \mathbb{R} \end{aligned}$$

wobei das Tupel eine Gerade durch ihre Steigung in der linken Halbebene und den Schnittpunkt mit der y-Achse (bzw. mit der x-Achse, falls die Steigung ∞ ist) angibt. D.h. die Indizenz ist gegeben durch

$$(x,y) \in (m,b) \leftrightarrow \begin{cases} x = b & \text{falls } m = \infty \\ y = mx + b & \text{falls } 0 \leq m \neq \infty \\ y = mx + b & \text{falls } m \leq 0, x \leq 0 \\ y = 2mx + b & \text{falls } m \leq 0, x \geq 0 \end{cases}$$

Satz 5.6 *Die Moulton-Ebene ist eine affine Ebene, in der der Satz von Desargues nicht gilt.*

Beweis : Die Existenz einer Geraden durch zwei Punkte (x_i, y_i), je einer davon in der linken und einer in der rechten Halbebene (also $x_1 \leq 0 < x_2$), ist nicht offensichtlich, falls $y_2 < y_1$ ist. Man rechnet direkt die Gleichung einer solchen Geraden (sowie deren Eindeutigkeit) nach (Übung). Die Axiome (G) und (R) sind offensichtlich und für (P) genügt es zu beobachten, dass sich auch in der Moulton-Ebene Geraden mit gleichem m und verschiedenem y nicht schneiden.

Zum Nachweis, dass der Satz von Desargues nicht erfüllt ist, arrangiere man eine Desargues-Konfiguration (Geraden g, h, k, die sich in O schneiden, sowie die Punkte $A, \ldots, C'$) so, dass sich alle Punkte bis auf C' in der linken Halbebene befinden. Dann ist die euklidische Gerade AC parallel zu $A'C'$ (nach dem Satz von Desargues für die euklidische affine Eben), aber die Moulton-Geraden durch diese Punkte schneiden sich bei geeigneter Wahl der Punkte (Übung). □

Wie Ebenen kann man auch die Struktur des $\mathbb{A}^n$ für $n \geq 2$ axiomatisch aufbauen, indem man zusätzliche einen Begriff von Ebenen einführt. Diese axiomatische Geometrie geht auf Hilbert [Hil99] (Erstauflage 1899) zurück. Hilbert wird auch nachgesagt, man könne statt „Punkte, Geraden und Ebenen" jederzeit auch „Tische, Stühle und Bierseidel" sagen; es komme nur darauf an, dass die Axiome erfüllt sind.

In affinen ebenen Geometrien argumentieren wir ständig mit der Fallunterscheidung 'schneiden sich oder sind parallel'. Eine der Motivationen zur Einführung von projektiver Geometrie ist dies Fallunterscheidung abzuschaffen und ein Axiomensystem zu verwenden, bei dem Punkte und Geraden völlig dual zueinander sind, siehe Satz 5.12.

Definition 5.7 *Eine* ebene projektive Geometrie *besteht aus einer Menge $\mathcal{P}$ von* Punkten*, einer Menge $\mathcal{G}$ von* Gerade *und einer Relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{G}$ mit folgenden Eigenschaften, in denen wir statt $(P, g) \in I$ auch P* liegt auf g oder $P \in g$ *sagen.*

(V) Durch je zwei Punkte geht genau eine Gerade, d.h. zu $P, Q \in \mathcal{P}$ mit $P \neq Q$ gibt es genau ein $g \in \mathcal{G}$ mit $P \in g$ und $Q \in g$.
(G) Auf jeder Geraden liegen mindestens drei Punkte.
(R) Es gibt vier Punkte, von denen je drei nicht kollinear sind.
(S) Zu je zwei Geraden $g, h \in \mathcal{G}$ mit $g \neq h$ existiert genau ein Schnittpunkt $P \in g \cap h$.

Beispiele 5.8 i) Eine Kugel $S \subset \mathbb{R}^n$, bei der zwei gegenüberliegende Punkte als ein Punkt aufgefasst werden, definiert wie folgt eine projektive Ebene: d.h.

$$\begin{aligned} \mathcal{P} &= \{\{P, Q\} \mid P, Q \in S; \quad P, Q \text{ liegen gegenüber}\} \\ \mathcal{G} &= \{\text{Großkreise}\} \end{aligned}$$

Zwischen zwei verschiedenen (nicht gegenüberliegenden) Punkten existiert genau ein Großkreis. Zwei verschiedene Großkreise sich genau in zwei gegenüberliegenden Punkten schneiden, also in einem Element in $\mathcal{P}$. Das Reichhaltigkeitsaxiom ist auch erfüllt (wähle vier Punkte auf einer Halbkugel, die nicht gemeinsam auf einem Großkreis liegen). Es sind also alle Axiome einer projektiven Geometrie erfüllt.

ii) Man macht aus der affinen „Minimalebene" eine projektive „Minimalebene", indem man zu jeder Parallelenschar einen Schnittpunkt hinzunimmt. Die neuen Punkte werden mit $\circ$ gekennzeichnet (vgl. Abbildung 5.1).
Eine neue Gerade, in der Abbildung gestrichelt eingezeichnet, wird ebenso benötigt, damit auch für die neuen Punkte Axiom (V) erfüllt ist. Somit hat die Ebene jetzt 7 Punkte und 7 Geraden und ist projektiv. Dies ist das kleinste Beispiel, weil nach dem Reichhaltigkeitsaxiom vier Punkte wie im affinen Minimalbeispiel existieren müssen.

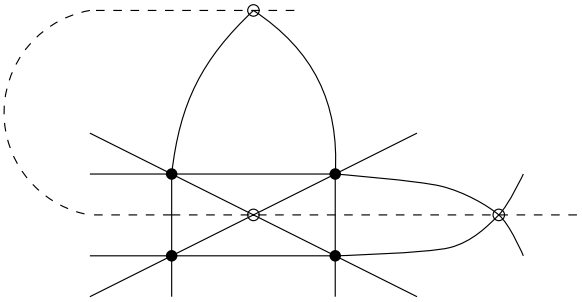

Abbildung 5.1: Projektive Ebene mit 7 Punkten und 7 Geraden

iii) Wie kann man allgemein aus einer affinen Ebene eine projektive Ebene machen? Sei $(\mathcal{P}, \mathcal{G})$ eine affine Ebene. Wir wissen, dass $\mathcal{G}$ Vereinigung von Parallelscharen ist. Für jede Parallelenschar π fügt man einen neuen Punkt P_π hinzu, d.h.

$$\mathcal{P}' := \mathcal{P} \cup \{P_\pi \mid \pi \text{ Parallelenschar in } (\mathcal{P}, \mathcal{G})\}$$

Jeder der neuen Punkte P_π wird zu jeder Geraden g in der Parallelenschar π hinzugefügt, aber nicht zu Geraden die nicht in π liegen. Weiterhin wird eine neue Gerade u hinzugefügt, die alle neuen Punkte P_π enthält, (vgl. Abbildung 5.2). Man definiert also

$$\mathcal{G}' := \bigcup_\pi \Big\{ g \cup \{P_\pi\} \mid g \in \pi \Big\} \cup \Big\{ \underbrace{\{P_\pi\}_\pi}_{=:u} \Big\}$$

Die Punkte P_π heißen *Punkte im Unendlichen* und die Gerade u heißt *unendlich ferne Gerade*. Wir zeigen jetzt, dass $(\mathcal{P}', \mathcal{G}')$ die Axiome einer projektiven Geometrie erfüllt.

i) Das Verbindungsaxiom ist klar für $P \neq Q$ in der ursprünglichen Punktmenge $\mathcal{P}$. Für $P \in \mathcal{P}$ und $Q = P_\pi$ gibt es genau eine Gerade g in der Parallelenschar π, die durch P geht. Daher ist $g \cup \{P_\pi\}$ die eindeutige Gerade durch P und P_π. Für zwei beliebige Punkte im Unendlichen ist u die einzige Gerade, die die beiden Punkte verbindet.

ii) Das Schnittaxiom stimmt, weil zwei ursprünglich parallele Geraden jetzt einen Schnittpunkt haben und jede ursprüngliche Gerade die Gerade u in genau einem Punkt schneidet.

iii) Das Reichhaltigkeitsaxiom ist ohnehin erfüllt, weil es bereits in der affinen Ebene erfüllt war.

Man nennt $(\mathcal{P}', \mathcal{G}')$ auch *projektiven Abschluss von* $(\mathcal{P}, \mathcal{G})$. Wenn $(\mathcal{P}, \mathcal{G})$ eine affine Ebene der endlichen Ordnung n war, dann hat $(\mathcal{P}, \mathcal{G})$ genau n^2 Punkte und $n+1$ Parallelenscharen. Folglich hat der projektive Abschluß n^2+n+1 Punkte und n^2+n+1 Geraden. Auf jeder Geraden liegen $n+1$ Punkte.

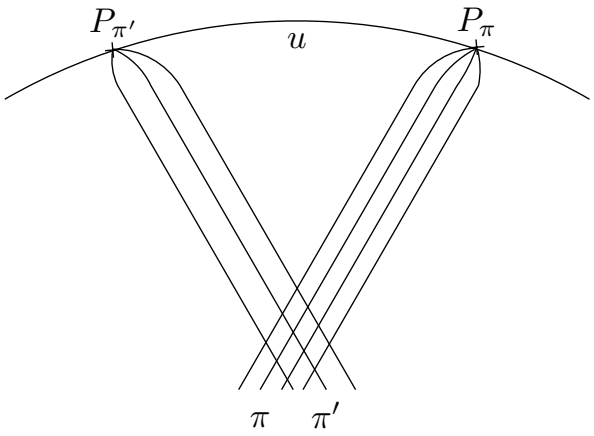

Abbildung 5.2: Neue Punkte bei der Konstruktion einer projektiven Ebene

Beispiel 5.9 Die affine Ebene der Ordnung 3 wird zu einer projektiven Ebene mit $3^2+3+1 = 13$ Punkten und 13 Geraden. Jede Gerade hat 4 Punkte.

Projektive Ebenen haben Anwendungen auch in der Kombinatorik, beispielsweise bei der Organisation eines Doppelkopfturniers mit 13 Spielern. Doppelkopf wird in Runden zu 4 Spielern gespielt. Es korrespondieren

$$\begin{aligned} \text{Spieler} &\longleftrightarrow \text{ Punkte einer projektiven Ebene der Ordnung } 3 \\ \text{Runden} &\longleftrightarrow \text{Geraden in dieser Ebene.} \end{aligned}$$

Nach Axiom 1 treffen je zwei Spieler in genau einer Runde aufeinander. Es kann also ein genau 13-rundiges Turnier organisiert werden.

Satz 5.10 *Sei $\mathbb{P} = (\mathcal{P}, \mathcal{G})$ eine projektive Ebene und $u \in \mathcal{G}$ eine beliebige Gerade. Entfernt man u und alle Punkte auf u, so entsteht eine affine Ebene. Dies bedeutet, dass $(\mathcal{P}', \mathcal{G}')$ mit*

$$\begin{aligned} \mathcal{P}' &:= \mathcal{P} \setminus u \\ \mathcal{G}' &:= \{g \setminus u \mid g \in \mathcal{G} \setminus \{u\}\} \end{aligned}$$

eine affine Ebene ist. Außerdem ist $(\mathcal{P}, \mathcal{G})$ der projektive Abschluss dieser Ebene.

Beweis : Wir überprüfen die Axiome der affinen Ebene für $(\mathcal{P}', \mathcal{G}')$

i) Wir prüfen (V). Seien $P \neq Q \in \mathcal{P}'$. Es gibt genau eine Gerade $g \in \mathcal{G}$ mit $P, Q \in g$. Diese Gerade ist nach Voraussetzung über die Lage von P und Q nicht u. Daher ist $g \setminus u$ die einzige Gerade in $\mathcal{G}'$, die P mit Q verbindet.

ii) Wir prüfen (P). Sei $g' := g \setminus u$ eine Gerade in $\mathcal{G}'$ und $P \in \mathcal{P}'$. Ist $P \in g \setminus u$, so ist $g \setminus u$ eine Parallele zu g durch P, und die einzige Parallele nach dem Axiom (V) einer

projektiven Ebene. Also können wir ab sofort annehmen, dass $P \notin g \setminus u$. Sei $Q := g \cap u$ der Schnittpunkt von g und u in $\mathcal{P}$. Eine Gerade h durch P ist in $(\mathcal{P}', \mathcal{G}')$ parallel zu g genau dann, wenn der eindeutige Schnittpunkt von h und g in u liegt (sonst gibt es einen Schnittpunkt in $\mathcal{P}'$), d.h. wenn $h \cap g = \{Q\}$. Unter den Geraden, die ausserdem durch Q gehen ist das nach Axiom (V) nur für genau eine Gerade h erfüllt und dies ist die gesuchte Parallele.

iii) Wir prüfen (R). Seien $P_1, P_2, P_3, P_4 \in \mathcal{P}$, so dass je drei von diesen Punkten auf keiner Geraden liegen. Falls die vier Punkte alle nicht in u liegen, erfüllen diese Punkte das Reichhaltigkeitsaxiom für $(\mathcal{P}', \mathcal{G}')$. Andernfalls liegen maximal zwei dieser Punkte auf u. Wir können also annehmen, dass $P_1, P_2 \notin u$ und $P_4 \in u$ liegt. Der Punkt P_3 kann, muss aber nicht auf u liegen. Wir definieren $P_4' := P_1P_4 \cap P_2P_3$. Dann gilt $P_4' \notin u$, denn

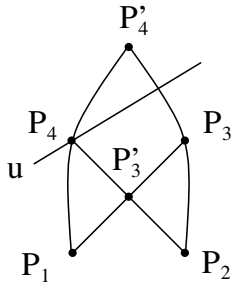

Abbildung 5.3: Schnittverhalten im Nachweis der Reichhaltigkeit

wegen $P_1 \notin u$ und $P_4 \in u$ ist $P_1P_4 \neq u$ und wegen $P_4 \notin P_2P_3$ (vgl. Abbildung 5.3) würde $P_4' \in u$ den Widerspruch $P_1P_4 = u$ ergeben. Darüber hinaus definieren wir noch $P_3' := P_1P_3 \cap P_2P_4$. Wegen $P_2 \notin u$, aber $P_4 \in u$ und $P_2 \notin P_1P_3$ gilt dann $P_3' \notin u$. Wir behaupten, dass $P_1, P_2, P_3', P_4' \in \mathcal{P}'$ das Reichhaltigkeitsaxiom für $(\mathcal{P}', \mathcal{G}')$ erfüllen. Dazu muss noch überprüft werden, dass keine drei dieser Punkte auf einer Geraden liegen. Falls z.B. P_1, P_3', P_4' auf einer Gerade g liegen würden, dann wäre dies einerseits die eindeutige Gerade von P_1 nach P_4', was $P_4 \in g$ impliziert, und andererseits die eindeutige Gerade von P_1 noch P_3', was $P_3 \in g$ impliziert. Also $P_1, P_3, P_4 \in g$ im Widerspruch zur Annahme. Analog argumentiert man für die anderen Kombinationen. Also ist $(\mathcal{P}', \mathcal{G}')$ eine affine Ebene.

Schließlich gilt:

$$\begin{array}{lcl} \text{Parallelenscharen von } (\mathcal{P}', \mathcal{G}') & \overset{1:1}{\longleftrightarrow} & \text{Punkte auf } u \\ \text{Parallelenschar von } g \setminus u & \longmapsto & g \cap u \\ \text{Geraden } g \setminus u \text{ mit } g \cap u = Q & \leftarrow & Q \end{array}$$

Deswegen ist der projektive Abschluss von $(\mathcal{P}', \mathcal{G}')$ genau $(\mathcal{P}, \mathcal{G})$. □

Folgerung 5.11 *Für jede endliche projektive Ebene $\mathbb{P}$ gibt es ein eindeutiges $n \in \mathbb{N}$, so dass $\mathbb{P}$ genau n^2+n+1 Punkte und n^2+n+1 Geraden hat und auf jeder Geraden $n+1$ Punkte liegen. Die Zahl n heißt die* Ordnung der projektiven Ebene $\mathbb{P}$.

Zum Abschluss formulieren wir noch das Dualitätsprinzip in projektiven Ebenen. Zur jeder Aussage über Punkte und Geraden in einer projektiven Ebene (beispielsweise: „Zwei Geraden haben genau einen Schnittpunkt“) kann man in eine duale Aussage über Geraden und Punkte übersetzen (im Beispiel: „Durch zwei Punkte geht genau eine Gerade“). Ein weiteres Beispiel ist „Drei Geraden gehen durch einen Punkt“, was sich zu „Drei Punkte liegen auf einer Geraden“dualisiert.

Satz 5.12 (Dualitätsprinzip in projektiven Ebenen) *Zu jeder Aussage über projektive Ebenen, die aus den Axiomen hergeleitet werden kann, gibt es eine duale Aussage, die ebenfalls aus den Axiomen hergeleitet werden kann. Dabei müssen folgende Ersetzungen vorgenommen werden*

Punkte	$\longmapsto$	*Geraden*
Geraden	$\longmapsto$	*Punkte*
Schnittpunkt	$\longmapsto$	*Verbindungsgerade*
Verbindungsgerade	$\longmapsto$	*Schnittpunkt*

Beweis : Die Axiome (V) und (R) sind dual zueinander. Das Axiom (R) ist zu sich selbst dual, denn die folgenden Aussagen sind äquivalent:

a) Es gibt vier Punkte, von denen keine drei auf einer Geraden liegen.

b) Es gibt vier Geraden von denen keine drei durch einen Punkt gehen.

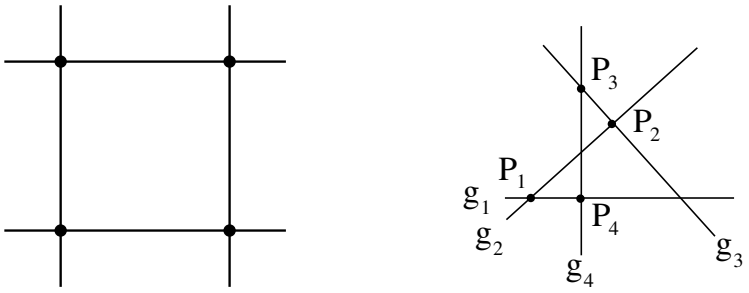

Abbildung 5.4: Zur Dualität des Reichhaltigkeitsaxioms

Zum Beweis der Implikation a) $\Rightarrow$ b) seien vier Punkte gegeben, von denen keine drei auf einer Geraden liegen. Von den Geraden aus Abbildung 5.4 gehen keine drei durch einen Punkt.

Zum Beweis der umgekehrten Implikation b) $\Rightarrow$ a) seien vier Geraden g_1, g_2, g_3, g_4 gegeben, von denen keine drei durch einen Punkt gehen. Wir definiere $P_1 := g_1 \cap g_2$, $P_2 := g_2 \cap g_3$,

$P_3 := g_3 \cap g_4$ und $P_4 := g_1 \cap g_4$, vgl. Abbildung 5.4. Dann liegen von diesen Punkten keine drei auf einer Geraden.

Es bleibt zu zeigen, dass das Dual von (G) gilt, also dass durch jeden Punkt P mindestens drei Geraden gehen. Dazu nimmt man eine Gerade g, die nicht durch P geht, welche nach (R) existiert. Auf g liegen mindestens drei Punkte Q_i, und die Verbindungsgeraden h_i von P mit Q_i leisten das Verlangte. □

6 Projektive Räume

Projektive Räume sollen eine „Vervollständigung“ von affinen Räumen darstellen, in der es keine parallelen Unterräume gibt. In Abschnitt 6.2 werden wir sehen, dass ein projektiver Raum so konstruiert ist, dass er als Erweiterung eines affinen Raums angesehen werden kann, zu dem Punkte im „Unendlichen“ hinzugefügt werden. Parallele Unterräume des ursprünglichen affinen Raums schneiden sich dabei im „Unendlichen“.

Definition 6.1 *Sei $V \neq \{0\}$ ein Vektorraum über einem Körper K. Die Menge aller 1-dimensionalen Unterräume von V heißt* projektiver Raum *$P(V)$ zu V. Im Fall $\dim V < \infty$ definieren wir $\dim P(V) := \dim V - 1$.*

Bemerkungen:

- Ein projektiver Raum $P(V)$ kann mit der Menge der Äquivalenzklassen der durch

  $$v \sim w \iff \exists \lambda \in K^\times : v = \lambda w$$

  definierten Äquivalenzrelation auf $V \setminus \{0\}$ identifiziert werden. Dabei entspricht die Äquivalenzklasse von einem Element $v \in V \setminus \{0\}$ dem 1-dimensionalen Unterraum $Kv \subset V$ in $P(V)$.

- Wir werden die Abbildung

  $$p : \begin{array}{ccc} V \setminus \{0\} & \to & P(V) \\ v & \longmapsto & Kv \end{array}$$

  als *kanonische Projektion* bezeichnen.

- Falls V eindimensional ist, besteht $P(V)$ nur aus einem Element.

- Wir nennen $P(V)$ eine *projektive Gerade*, falls $\dim V = 2$ gilt, und eine *projektive Ebene*, falls $\dim V = 3$ gilt.

- Für den projektiven Raum $P(K^{n+1})$ schreiben wir auch $\mathbb{P}^n(K)$ und nennen ihn den n-dimensionalen projektiven Standardraum über K.

6.1 Projektive Unterräume

Jeder nicht-triviale Unterraum eines Vektorraums V definiert einen projektiven Unterraum des projektiven Raums $P(V)$.

Definition 6.2 *Eine Teilmenge Y eines projektiven Raums $P(V)$ heißt* projektiver Unterraum, *falls es einen Untervektorraum $U \subset V$ gibt, so dass*

$$Y = p(U \setminus \{0\}) = \{Kv \in P(V) \,:\, v \in U \setminus \{0\}\}$$

gilt, also Y aus allen 1-dimensionalen Unterräumen von U besteht.

In dieser Situation können wir Y mit dem projektiven Raum $P(U)$ identifizieren, daher schreiben wir $Y = P(U) \subset P(V)$. Der Unterraum $U \subset V$ heißt der zu Y gehörige Unterraum. Falls Y eindimensional ist (d.h. $\dim U = 2$), so nennen wir Y eine *Gerade* in $P(V)$.

Beispiel 6.3 Jeder Punkt $P = Kv$ eines projektiven Raums $P(V)$ bildet einen 0-dimensionalen projektiven Unterraum, denn es gilt $\{P\} = P(Kv) \subset P(V)$.

Proposition 6.4 *Seien Y und Z zwei projektive Unterräume eines endlich-dimensionalen projektiven Raums $P(V)$ mit $\dim Y + \dim Z \geq \dim P(V)$. Dann ist der Durchschnitt $Y \cap Z$ nicht leer.*

Diese Proposition zeigt insbesondere, dass sich zwei Geraden in einer projektiven Ebene immer schneiden. Im Unterschied zur affinen Geometrie gibt es also in einer projektiven Ebene keine parallelen Geraden.

Beweis : Es gelte $Y = P(U)$ und $Z = P(W)$ für Unterräume $U, W \subset V$. Mit der Dimensionsformel

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

folgt

$$\begin{aligned} \dim(U \cap W) &= \dim U + \dim W - \dim(U + W) \\ &\geq (\dim Y + 1) + (\dim Z + 1) - \dim V \geq \dim P(V) + 2 - \dim V = 1. \end{aligned}$$

Dabei haben wir $U + W \subset V$ und die Voraussetzung $\dim Y + \dim Z \geq \dim P(V)$ verwendet. Der Durchschnitt $Y \subset Z$ ist die Menge aller 1-dimensionalen Unterräume von V, die in $U \cap W$ enthalten sind. Wegen $\dim(U \cap W) \geq 1$ ist diese Menge nicht-leer. □

Korollar 6.5 *Sei Y ein projektiver Unterraum in einem endlich-dimensionalen projektiven Raums $P(V)$ mit $\dim Y = \dim P(V) - 1$ (ein solches Y wird* Hyperebene *genannt) und P ein Punkt von $P(V)$, der nicht in Y liegt. Dann schneidet jede Gerade durch P die Hyperebene Y in genau einem Punkt.*

Nach diesem Korollar gibt es also in projektiven Räumen keine Geraden, die parallel zu einer Hyperebene liegen.

Beweis : Sei g eine Gerade durch P. Mit der vorangegangenen Proposition können wir $g \cap Y \neq \emptyset$ folgern, weil $\dim Y + \dim g = \dim P(V)$ gilt. Sei nun $Y = P(U)$ und $g = P(W)$ für Unterräume U und W von V mit $\dim U = \dim V - 1$ und $\dim W = 2$. Weil P nicht in Y liegt, ist g nicht in Y enthalten. Daher ist W nicht in U enthalten, es gilt also $U + W \supsetneq U$. Aus Dimensionsgründen muss daher $U + W$ ganz V sein. Die Dimensionsformel für $U + W$ ergibt also

$$\dim(U \cap W) = \dim U + \dim W - \dim(U + W) = \dim V - 1 + 2 - \dim V = 1.$$

Die Gerade g schneidet somit die Hyperebene Y genau im Punkt von $P(V)$, der dem 1-dimensionalen Unterraum $U \cap W \subset V$ entspricht. □

Wie im affinen Fall ist der Durchschnitt von projektiven Unterräumen wieder ein projektiver Unterraum, sofern er nicht leer ist.

Proposition 6.6 *Seien $(Y_i)_{i\in I}$ (für eine beliebige Indexmenge I) projektive Unterräume von $P(V)$ mit zugehörigen Unterräumen $U_i \subset V$. Dann ist $\bigcap_{i\in I} Y_i$ genau dann nicht leer, wenn $U := \bigcap_{i\in I} U_i$ nicht gleich $\{0\}$ ist. In diesem Fall ist $\bigcap_{i\in I} Y_i$ ein projektiver Unterraum von $P(V)$ und es gilt $\bigcap_{i\in I} Y_i = P(U)$.*

Beweis : Das folgt direkt aus den Definitionen, weil die Punkte von $\bigcap_{i\in I} Y_i$ genau die 1-dimensionalen Unterräume von V sind, die in $\bigcap_{i\in I} U_i$ enthalten sind. □

Definition 6.7 *Sei M eine nicht leere Teilmenge eines projektiven Raums $P(V)$ und $\mathcal{B}$ die Menge aller projektiven Unterräume von $P(V)$, die M enthalten. Dann heißt $[M] := \bigcap_{Y\in\mathcal{B}} Y$ die* projektive Hülle *von M. Sind Y_1, Y_2 zwei projektive Unterräume von $P(V)$, so heißt $Y_1 + Y_2 := [Y_1 \cup Y_2]$ der* Verbindungsraum *von Y_1 und Y_2.*

Wie im affinen Fall ist $[M]$ nach der vorherigen Proposition ein projektiver Unterraum von $P(V)$. Es ist der kleinste projektive Unterraum von $P(V)$, der M enthält.

Proposition 6.8 *Sei $M \subset P(V)$ nicht leer. Dann ist der zum projektiven Unterraum $[M] \subset P(V)$ gehörige Unterraum gleich dem von $p^{-1}(M)$ aufgespannten Unterraum $[p^{-1}(M)] \subset V$, wobei $p : V \setminus \{0\} \to P(V)$ die kanonische Projektion bezeichnet.*

Beweis : Nach der vorangegangenen Proposition ist der zu $[M] = \bigcap_{Y\in\mathcal{B}} Y$ gehörige Unterraum gleich dem Durchschnitt aller Unterräume $U \subset V$ mit $M \subset P(U)$. Ein Unterraum $U \subset V$ erfüllt genau dann $M \subset P(U)$, wenn $p^{-1}(M)$ in U enthalten ist, denn $p^{-1}(M)$ ist

genau die Vereinigung der 1-dimensionalen Unterräume von V, die zu den Punkten in M korrespondieren. Somit ist der zu $[M]$ gehörige Unterraum gleich dem Durchschnitt aller Unterräume von V, die $p^{-1}(M)$ enthalten. Dies ist genau der von $p^{-1}(M)$ aufgespannte Unterraum $[p^{-1}(M)] \subset V$. □

Beispiel 6.9 Für zwei projektive Unterräume $Y_1 = P(U_1)$ und $Y_2 = P(U_2)$ von $P(V)$ gilt $Y_1 + Y_2 = P(U_1 + U_2)$, denn nach der Proposition gehört zu $Y_1 + Y_2 = [Y_1 \cup Y_2]$ der Unterraum

$$[p^{-1}(Y_1 \cup Y_2)] = [p^{-1}(Y_1) \cup p^{-1}(Y_2)] = [U_1 \cup U_2] = U_1 + U_2.$$

Korollar 6.10 *Für zwei projektive Unterräume Y_1, Y_2 eines endlich-dimensionalen projektiven Raums $P(V)$ gilt die Dimensionsformel*

$$\dim(Y_1 + Y_2) = \begin{cases} \dim Y_1 + \dim Y_2 - \dim(Y_1 \cap Y_2) & , \text{ falls } Y_1 \cap Y_2 \neq \emptyset \\ \dim Y_1 + \dim Y_2 + 1 & , \text{ falls } Y_1 \cap Y_2 = \emptyset \end{cases}.$$

Beweis : Sei $Y_1 = P(U_1)$ und $Y_2 = P(U_2)$ für Unterräume U_1, U_2 von V. Dann gilt $Y_1 + Y_2 = P(U_1 + U_2)$ nach dem obigen Beispiel. Daher haben wir

$$\begin{aligned} \dim(Y_1 + Y_2) &= \dim(U_1 + U_2) - 1 = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2) - 1 \\ &= (\dim Y_1 + 1) + (\dim Y_2 + 1) - \dim(U_1 \cap U_2) - 1 \\ &= \dim Y_1 + \dim Y_2 - \dim(U_1 \cap U_2) + 1. \end{aligned}$$

Die behauptete Formel folgt, da $Y_1 \cap Y_2$ genau dann nicht leer ist, wenn $U_1 \cap U_2 \neq \{0\}$ gilt und in diesem Fall $\dim(Y_1 \cap Y_2) = \dim(U_1 \cap U_2) - 1$ ist. □

Beispiel 6.11 Sei $P(V)$ ein dreidimensionaler projektiver Raum und g_1, g_2 zwei Geraden in $P(V)$. Dann gibt es drei Fälle für die gegenseitige Lage von g_1, g_2:

i) $\dim(g_1 + g_2) = 1$: Aus Dimensionsgründen kann das nur gelten, wenn die beiden Geraden gleich sind.

ii) $\dim(g_1 + g_2) = 2$: In diesem Fall schneiden sich die Geraden nach der Dimensionsformel in einem 0-dimensionalen projektiven Unterraum, also in genau einem Punkt.

iii) $\dim(g_1 + g_2) = 3$: In diesem Fall schneiden sich die Geraden gemäß Dimensionsformel nicht. Es handelt sich um windschiefe Geraden, weil die beiden Geraden nicht in einer Ebene liegen.

Man beachte, dass der Fall von zwei parallelen Geraden im Gegensatz zur affinen Geometrie nicht auftritt. In der projektiven Geometrie gibt es also insgesamt weniger Möglichkeiten für die gegenseitige Lage von zwei Unterräumen.

6.2 Projektive Vervollständigung von affinen Räumen

In diesem Abschnitt erklären wir, inwiefern projektive Räume als „Vervollständigung“ von affinen Räumen aufgefasst werden können. Wir veranschaulichen die allgemeine Situation zuerst anhand der Beispiele einer Geraden und einer Ebene.

Beispiel 6.12 Sei $P(V)$ eine projektive Gerade (V ist also ein zweidimensionaler K-Vektorraum). Nach Wahl einer Basis können wir V mit K^2 identifizieren und $P(V)$ als die Menge der Geraden durch den Ursprung in der Ebene K^2 auffassen. Mit Ausnahme der x-Achse $K \cdot (1,0)$ schneiden all diese Geraden die horizontale Gerade $\{y = 1\} \subset K^2$ in einem eindeutigen Punkt. Daher können wir $P(V) \setminus \{K \cdot (1,0)\}$ mit der affinen Gerade $\{y = 1\} \subset K^2$ identifizieren. Wir erhalten also den projektiven Raum $P(V)$, indem wir zur affinen Gerade $\{y = 1\}$ einen zusätzlichen Punkt, der der x-Achse in K^2 entspricht, hinzufügen. Diesen zusätzlichen Punkt nennen wir *unendlichfernen Punkt*.

Häufig werden die Punkte auf der Geraden $\{y = 1\}$ mit K identifiziert, wobei $\lambda \in K$ dem Punkt $(\lambda, 1)$ entspricht, und der unendlichferne Punkt als ∞ bezeichnet. Somit können wir insgesamt $\mathbb{P}^1(K) = P(K^2)$ mit $K \cup \{\infty\}$ identifizieren, wobei $\lambda \in K$ dem Punkt $K \cdot (\lambda, 1)$ und ∞ dem Punkt $K \cdot (1,0)$ entspricht.

Beispiel 6.13 Analog können wir $\mathbb{P}^2(K) = P(K^3)$ als “Vervollständigung” der affinen Ebene $\{z = 1\} \subset K^3$ auffassen. In der Tat besteht $P(K^3)$ aus den Geraden durch den Ursprung im Raum K^3. Mit Ausnahme der Geraden, die in der xy-Ebene liegen, schneiden all diese Geraden die horizontale Ebene $\{z = 1\}$ in einem eindeutigen Punkt. Die Menge der Geraden durch den Urpsrung, die in der xy-Ebene liegen, können wir mit $P(K^2)$ identifizieren. Wir erhalten also den projektiven Raum $P(K^3)$, indem wir eine projektive Gerade $P(K^2)$ (deren Punkte wir als Geraden durch den Ursprung, die in der xy-Ebene liegen, auffassen) zur affinen Ebene $\{z = 1\} \subset K^3$ hinzufügen. Die zusätzliche projektive Gerade nennen wir *unendlichferne Gerade*.

Ganz allgemein können wir einen affinen Raum $\mathbb{A}$ zum Vektorraum V zu einem projektiven Raum $\mathbb{P}$ vervollständigen, indem wir die Punkte des projektiven Raums $P(V)$ zu $\mathbb{A}$ hinzufügen. Dazu wählen wir einen festen Punkt $Q \in \mathbb{A}$ und betrachten die Verknüpfung der Abbildungen

$$\begin{array}{ccccc} \mathbb{A} & \longrightarrow & V \times K & \xrightarrow{p} & P(V \times K) \\ R & \longmapsto & (\overrightarrow{QR}, 1) & \longmapsto & K \cdot (\overrightarrow{QR}, 1) \end{array} .$$

Diese ist injektiv mit Bild $P(V \times K) \setminus P(V \times \{0\})$, weil jeder eindimensionale Unterraum von $V \times K$, der nicht in $V \times \{0\}$ enthalten ist, den affinen Unterraum $V \times \{1\}$ in genau einem Punkt schneidet und $R \mapsto \overrightarrow{QR}$ eine bijektive Abbildung $\mathbb{A} \longmapsto V$ ist. Daher können wir $\mathbb{A}$ mit $P(V \times K) \setminus P(V \times \{0\})$ identifizieren. Wir erhalten also den projektiven Raum

$\mathbb{P} := P(V \times K)$, wenn wir zu $\mathbb{A}$ die Punkte von $P(V \times \{0\}) \cong P(V)$ hinzufügen. Wir nennen $\mathbb{P}$ eine *projektive Vervollständigung* von $\mathbb{A}$ und die projektive Hyperebene $H := P(V \times \{0\}) \subset \mathbb{P}$ die *unendlichferne Hyperebene*.

Der folgende Satz erklärt den Zusammenhang zwischen den affinen Unterräumen von $\mathbb{A}$ und den projektiven Unterräumen einer projektiven Vervollständigung $\mathbb{P}$. Der Einfachheit halber nehmen wir im Folgenden an, dass $\mathbb{A}$ endlich-dimensional ist.

Satz 6.14 *Sei $\mathbb{A}$ ein endlich-dimensionaler affiner Raum zum Vektorraum V und $\mathbb{P}$ eine projektive Vervollständigung von $\mathbb{A}$ mit unendlichferner Hyperebene $H := \mathbb{P} \setminus \mathbb{A}$. Dann stehen die affinen Unterräume von $\mathbb{A}$ in Bijektion zu den projektiven Unterräumen von $\mathbb{P}$, die nicht in der unendlichfernen Hyperebene H enthalten sind. Eine Bijektion ist gegeben durch*

$$\mathbb{B} \subset \mathbb{A} \mapsto [\mathbb{B}] \subset \mathbb{P},$$

wobei $[\mathbb{B}]$ die projektive Hülle von $\mathbb{B}$ in $\mathbb{P}$ bezeichnet, und eine Umkehrabbildung durch

$$Y \subset \mathbb{P} \mapsto Y \cap \mathbb{A} \subset \mathbb{A}.$$

Diese Bijektion erhält die Dimension von Unterräumen, d.h. für jeden affinen Unterraum $\mathbb{B} \subset \mathbb{A}$ gilt $\dim \mathbb{B} = \dim[\mathbb{B}]$.

Beweis : Sei zunächst $\mathbb{B}$ ein affiner Unterraum von $\mathbb{A}$ mit zugehörigem Unterraum $U \subset V$ und $P \in \mathbb{B}$. Nach Konstruktion von $\mathbb{P}$ identifizieren wir die Punkte von $\mathbb{B}$ mit $\{K \cdot (\overrightarrow{QR}, 1) : R \in \mathbb{B}\} \subset \mathbb{P} = P(V \times K)$, wobei $Q \in \mathbb{A}$ der in der Konstruktion von $\mathbb{P}$ fest gewählte Punkt ist. Nach Proposition 6.8 ist die projektive Hülle $[\mathbb{B}]$ ein projektiver Unterraum von $\mathbb{P}$ mit zugehörigem Unterraum $W := [\{(\overrightarrow{QR}, 1) \,:\, R \in \mathbb{B}\}] \subset V \times K$. Weil $\mathbb{B}$ ein affiner Unterraum zu U ist, können wir W wie folgt umschreiben:

$$W = [\{(\overrightarrow{QP} + x, 1) \,:\, x \in U\}] = K \cdot (\overrightarrow{QP}, 1) + U \times \{0\}.$$

Es gilt somit

$$\dim[\mathbb{B}] = \dim W - 1 = (1 + \dim U) - 1 = \dim U = \dim \mathbb{B}.$$

Weiter ist $[\mathbb{B}]$ nicht in $H = \mathbb{P} \setminus \mathbb{A}$ enthalten, weil $\mathbb{B}$ in $[\mathbb{B}]$ enthalten ist.

Es bleibt zu zeigen, dass die Zuordnung $Y \mapsto Y \cap \mathbb{A}$ invers zur Abbildung $\mathbb{B} \mapsto [\mathbb{B}]$ ist. Sei also $Y = P(W)$ ein projektiver Unterraum von $\mathbb{P} = P(V \times K)$, der nicht in $H = P(V \times \{0\})$ enthalten ist. Der zu Y gehörige Unterraum $W \subset V \times K$ ist nach Voraussetzung nicht in $V \times \{0\}$ enthalten. Daher ist die Einschränkung $\pi_2|_W$ der Projektion auf den zweiten Faktor eine surjektive lineare Abbildung $W \to K$. Deren Kern $W \cap (V \times \{0\})$ ist darum nach der Dimensionsformel für lineare Abbildungen von der Form $U \times \{0\}$ für einen Unterraum $U \subset V$ mit $\dim U = \dim W - 1$.

Der Durchschnitt $Y \cap \mathbb{A}$ besteht aus den Punkten $R \in \mathbb{A}$, für die $(\overrightarrow{QR}, 1)$ in $W \cap (V \times \{1\})$ liegt. Da Y nicht in H enthalten ist, gibt es einen Punkt $P \in Y \cap \mathbb{A}$. Wegen $(\overrightarrow{QR}, 1) = (\overrightarrow{QP}, 1) + (\overrightarrow{PR}, 0)$ liegt $(\overrightarrow{QR}, 1)$ genau dann in $W \cap (V \times \{1\})$, wenn $(\overrightarrow{PR}, 0)$ in $W \cap (V \times \{0\}) = U \times \{0\}$ liegt. Somit besteht $Y \cap \mathbb{A}$ genau aus den Punkten $R \in \mathbb{A}$ mit $\overrightarrow{PR} \in U$. Daher ist $Y \cap \mathbb{A}$ ein affiner Unterraum von $\mathbb{A}$ zum Unterraum U und es gilt

$$\dim Y \cap \mathbb{A} = \dim U = \dim W - 1 = \dim Y.$$

Weiter gilt $[Y \cap \mathbb{A}] \subset Y$ für die projektive Hülle $[Y \cap \mathbb{A}]$, weil Y ein projektiver Unterraum von $\mathbb{P}$ ist, und $\dim[Y \cap \mathbb{A}] = \dim Y \cap \mathbb{A} = \dim Y$. Weil $[Y \cap \mathbb{A}]$ und Y beides projektive Unterräume von $\mathbb{P}$ sind, folgt somit $[Y \cap \mathbb{A}] = Y$.

Analog schließen wir $[\mathbb{B}] \cap \mathbb{A} = \mathbb{B}$ für einen affinen Unterraum $\mathbb{B}$ von $\mathbb{A}$, denn es gilt $\mathbb{B} \subset [\mathbb{B}] \cap \mathbb{A}$ und $\dim[\mathbb{B}] \cap \mathbb{A} = \dim[\mathbb{B}] = \dim \mathbb{B}$.

Somit ist gezeigt, dass $\mathbb{B} \mapsto [\mathbb{B}]$ und $Y \mapsto Y \cap \mathbb{A}$ zueinander inverse Bijektionen sind, die die Dimension der Unterräume erhalten. □

Korollar 6.15 *Seien $\mathbb{B}_1$ und $\mathbb{B}_2$ zwei parallele verschiedene affine Unterräume eines endlich-dimensionalen affinen Raums $\mathbb{A}$ mit $\dim \mathbb{B}_1 = \dim \mathbb{B}_2 = k$. Dann schneiden sich die projektiven Hüllen $[\mathbb{B}_1]$ und $[\mathbb{B}_2]$ in einer projektiven Vervollständigung $\mathbb{P}$ in einem $(k-1)$-dimensionalen projektiven Unterraum, der in der unendlichfernen Hyperebene $H = \mathbb{P} \setminus \mathbb{A}$ enthalten ist.*

Dieses Korollar besagt, dass sich parallele affine Unterräume eines affinen Raums im „Unendlichen“ schneiden. Insbesondere schneiden sich parallele Geraden in genau einem Punkt im Unendlichen.

Beweis : Seien U_1 und U_2 die zu $\mathbb{B}_1$ und $\mathbb{B}_2$ gehörigen Unterräume und $P_1 \in \mathbb{B}_1$ sowie $P_2 \in \mathbb{B}_2$. Weil $\mathbb{B}_1$ und $\mathbb{B}_2$ parallel und von der gleichen Dimension sind, gilt $U_1 = U_2 =: U$. Nach dem Beweis des vorangegangenen Satzes gilt

$$\begin{aligned} [\mathbb{B}_1] &= P(K(\overrightarrow{QP_1}, 1) + U \times \{0\}), \\ [\mathbb{B}_2] &= P(K(\overrightarrow{QP_2}, 1) + U \times \{0\}), \end{aligned}$$

wobei $Q \in \mathbb{A}$ der in der Konstruktion von $\mathbb{P}$ fest gewählte Punkt ist. Es gilt $P_1 \neq P_2$, weil $\mathbb{B}_1$ und $\mathbb{B}_2$ als verschiedene affine Unterräume mit gleichem zugehörigen Unterraum disjunkt sind. Der Schnitt der 1-dimensionalen Unterräume $K(\overrightarrow{QP_1}, 1)$ und $K(\overrightarrow{QP_2}, 1)$ ist daher trivial und es gilt

$$[\mathbb{B}_1] \cap [\mathbb{B}_2] = P(U \times \{0\}) \subset P(V \times \{0\}) = H$$

und somit $\dim([\mathbb{B}_1] \cap [\mathbb{B}_2]) = \dim U - 1 = k - 1$. □

Ist $\mathbb{P} = P(V)$ ein beliebiger endlich-dimensionaler projektiver Raum, ist in diesem keine unendlichferne Hyperebene festgelegt. Der folgende Satz zeigt jedoch, dass jede beliebige Hyperebene $H \subset \mathbb{P}$ zur unendlichfernen Hyperebene „gemacht" werden kann.

Satz 6.16 *Sei $\mathbb{P} = P(V)$ ein endlich-dimensionaler projektiver Raum und $H \subset \mathbb{P}$ eine Hyperebene, d.h. ein projektiver Unterraum mit $\dim H = \dim \mathbb{P} - 1$. Dann kann $\mathbb{A} := \mathbb{P} \setminus H$ als affiner Raum aufgefasst werden und $\mathbb{P}$ ist eine projektive Vervollständigung von $\mathbb{A}$ mit unendlichferner Hyperebene H.*

Beweis : Sei $H = P(U)$ für einen Unterraum $U \subset V$. Wegen $\dim U = \dim H + 1 = \dim P(V) = \dim V - 1$ gibt es einen Isomorphismus $\phi : V \to U \times K$ mit $\phi(U) = U \times \{0\}$. Wir identifizieren V mit $U \times K$ via diesen Isomorphismus. Unter dieser Identifikation gilt $H = P(U \times \{0\})$. Jeder Punkt z in $\mathbb{A} := \mathbb{P} \setminus H$ ist ein 1-dimensionaler Unterraum von $U \times K$, der nicht in $U \times \{0\}$ enthalten ist und daher $U \times \{1\}$ in genau einem Punkt $(w_z, 1)$ schneidet. Die Funktion $z \mapsto w_z$ ist eine Bijektion $\mathbb{A} \to U$. Daher ist $\mathbb{A}$ ein affiner Raum zu U vermöge

$$\overrightarrow{xy} := w_y - w_x.$$

Sei nun Q der eindeutige Punkt in $\mathbb{A}$ mit $w_Q = 0$. Dann gilt für alle $R \in \mathbb{A}$

$$K \cdot (\overrightarrow{QR}, 1) = K \cdot (w_R - w_Q, 1) = K \cdot (w_R, 1) = R.$$

Daher ist $\mathbb{P}$ eine projektive Vervollständigung von $\mathbb{A}$ mit unendlichferner Hyperebene $\mathbb{P} \setminus \mathbb{A} = H$. □

6.3 Projektive Abbildungen

Jede injektive lineare Abbildung $f : V \to V'$ induziert eine Abbildung $P(f) : P(V) \to P(V')$ zwischen den dazugehörigen projektiven Räumen vermöge

$$P(f)(Kv) := Kf(v),\ v \in V \setminus \{0\},$$

denn diese Definition ist unabhängig von der Wahl des Repräsentanten $v \in V \setminus \{0\}$, weil $f(\lambda v) = \lambda f(v)$ für $\lambda \in K^\times$ gilt, und es gilt $f(v) \in V' \setminus \{0\}$ wegen der Injektivität von f. Die Abbildung $P(f)$ ist so definiert, dass das Diagramm

$$\begin{array}{ccc} V \setminus \{0\} & \xrightarrow{f} & V' \setminus \{0\} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ P(V) & \xrightarrow{P(f)} & P(V') \end{array}$$

kommutiert, wobei $p : V \setminus \{0\} \to P(V)$ and $p' : V' \setminus \{0\} \to P(V')$ die kanonischen Projektionen sind.

Definition 6.17 *Eine Abbildung $g : P(V) \to P(V')$ zwischen projektiven Räumen heißt* projektive Abbildung, *falls eine injektive lineare Abbildung $f : V \to V'$ mit $g = P(f)$ existiert. Eine bijektive projektive Abbildung heißt* Projektivität.

Unmittelbar aus der obigen Definition folgt, dass

$$P(f' \circ f) = P(f') \circ P(f) \tag{6.1}$$

für zwei injektive Abbildungen $f : V \to V'$ und $f' : V' \to V''$ gilt.

Lemma 6.18 *Eine projektive Abbildung $P(f) : P(V) \to P(V')$ ist genau dann eine Projektivität, wenn $f : V \to V'$ ein Isomorphismus ist.*

Beweis : Nach Definition von $P(f)$ gilt $P(f)(P(V)) = P(f(V)) \subset P(V')$. Wenn $P(f)$ eine Projektivität ist, gilt daher $f(V) = V'$. In diesem Fall ist also f sowohl injektiv wie auch surjektiv und somit ein Isomorphismus.

Falls umgekehrt f ein Isomorphismus ist, so gilt

$$\begin{aligned} P(f) \circ P(f^{-1}) &= P(f \circ f^{-1}) = P(\mathrm{id}_{V'}) = \mathrm{id}_{P(V')}, \\ P(f^{-1}) \circ P(f) &= P(f^{-1} \circ f) = P(\mathrm{id}_{V}) = \mathrm{id}_{P(V)}. \end{aligned}$$

Daher ist in diesem Fall $P(f)$ bijektiv mit $P(f)^{-1} = P(f^{-1})$ und somit eine Projektivität. □

Insbesondere gibt es im endlich-dimensionalen Fall nur Projektivitäten zwischen projektiven Räumen der gleichen Dimension.

Proposition 6.19 *Die Menge der Projektivitäten $g : P(V) \to P(V)$ eines projektiven Raums $P(V)$ bildet eine Gruppe $GP(V)$ bezüglich der Verknüpfung von Abbildungen.*

Beweis : Dies folgt unmittelbar aus den vorangegangenen Ausführungen, denn die Menge $GP(V)$ der Projektivitäten von $P(V)$ ist abgeschlossen unter Verknüpfung nach Gleichung (6.1), die Identität $\mathrm{id}_{P(V)} = P(\mathrm{id}_V)$ ist eine Projektivität und für $P(f) \in GP(V)$ gilt $P(f)^{-1} = P(f^{-1}) \in GP(V)$. □

Im Folgenden betrachten wir nur Projektivitäten $P(V) \to P(V')$ zwischen endlich-dimensionalen projektiven Räumen der Dimension n. Falls $(b_0, \ldots, b_n)$ bzw. $(b'_0, \ldots, b'_n)$ Basen von V bzw. V' sind, so gibt es genau einen Isomorphismus $f : V \to V'$ mit $f(b_i) = b'_i$ für $i = 0, \ldots, n$. Die dadurch definierte Projektivität $P(f) : P(V) \to P(V')$ erfüllt

$$P(f)(Kb_i) = Kb'_i,\ i = 0, \ldots, n.$$

Es gibt jedoch weitere Projektivitäten $P(h) : P(V) \to P(V')$ mit dieser Eigenschaft, denn diese Eigenschaft ist für alle $P(h) : P(V) \to P(V')$ mit $h(b_i) \in Kb_i',\ i = 0, \ldots, n$ erfüllt. Die Bilder der $n+1$ Punkte $Kb_0, \ldots, Kb_n$ legen also keine eindeutige Projektivität $P(h) : P(V) \to P(V')$ fest. Vielmehr ist die Projektivität $P(h)$ erst durch das Bild eines weiteren geeigneten Punktes eindeutig bestimmt, wie wir im nächsten Satz sehen werden. Dadurch ist die nachfolgende Definition motiviert.

Definition 6.20 *Sei $P(V)$ ein endlich-dimensionaler projektiver Raum der Dimension n. Ein Tupel $(Kb_0, \ldots, Kb_{n+1}) \in P(V)^{n+2}$ mit $b_0, \ldots, b_{n+1} \in V \setminus \{0\}$ heißt* projektive Basis *von $P(V)$, wenn für alle $i = 0, \ldots, n+1$ die $n+1$ Vektoren $\{b_0, \ldots, b_{n+1}\} \setminus \{b_i\}$ linear unabhängig in V sind.*

Bemerkungen:

- Wegen $\dim V = n+1$ bilden die $n+1$ Vektoren $\{b_0, \ldots, b_{n+1}\} \setminus \{b_i\}$ in der obigen Defintion eine Basis von V.
- Die Definition ist unabhängig von der Wahl der Repräsentanten $b_0, \ldots, b_{n+1} \in V \setminus \{0\}$ der gegebenen $n+2$ Punkte von $P(V)$.

Beispiel 6.21 Drei beliebige paarweise verschiedene Punkte (Kb_0, Kb_1, Kb_2) einer projektiven Geraden $P(V)$ bilden eine projektive Basis, denn $\{b_0, b_1\}$, $\{b_0, b_2\}$, $\{b_1, b_2\}$ sind linear unabhängig, weil die Geraden Kb_0, Kb_1, Kb_2 in V nach Voraussetzung paarweise verschieden sind.

Satz 6.22 *Sei $P(V)$ ein endlich-dimensionaler projektiver Raum mit projektiver Basis $(p_0, \ldots, p_{n+1})$.*

i) Falls $g : P(V) \to P(V')$ eine Projektivität ist, so ist $(g(p_0), \ldots, g(p_{n+1}))$ eine projektive Basis von $P(V')$.

ii) Ist $P(V')$ ein projektiver Raum mit $\dim P(V) = \dim P(V')$ und projektiver Basis $(q_0, \ldots, q_{n+1})$, so gibt es genau eine Projektivität $g : P(V) \to P(V')$ mit $g(p_i) = q_i$ für alle $i = 0, \ldots, n+1$.

Beweis : Sei $p_i = Kv_i$ für $i = 0, \ldots, n+1$ mit $v_i \in V \setminus \{0\}$.

Für Teil (i) bemerken wir, dass für eine Projektivität $g = P(f) : P(V) \to P(V')$ die Bilder der Punkte p_i der gegebenen projektiven Basis durch $P(f)(p_i) = Kf(v_i),\ i = 0, \ldots, n+1$ gegeben sind. Da f ein Isomorphismus ist, erfüllt das Tupel $(Kf(v_0), \ldots, Kf(v_n)) \in P(V')^{n+2}$ ebenfalls die obige Definition einer projektiven Basis. Somit ist $(g(p_0), \ldots, g(p_{n+1}))$ eine projektive Basis von $P(V')$.

Für Teil (ii) bemerken wir zunächst, dass nach der Definition einer projektiven Basis $(v_0, \ldots, v_n)$ eine Basis von V ist. Daher gibt es $\lambda_0, \ldots, \lambda_n \in K$ mit

$$v_{n+1} = \lambda_0 v_0 + \cdots + \lambda_n v_n.$$

Dabei sind alle $\lambda_i \neq 0$, denn falls ein i mit $\lambda_i = 0$ existieren würde, so wären $\{v_0, \ldots, v_{n+1}\} \setminus \{v_i\}$ linear abhängig im Widerspruch zur Definition einer projektiven Basis. Analog gilt $q_i = Kw_i$ für $i = 0, \ldots, n+1$ mit $w_i \in V' \setminus \{0\}$ und

$$w_{n+1} = \mu_0 w_0 + \cdots + \mu_n w_n$$

mit $\mu_0, \ldots, \mu_n \in K \setminus \{0\}$. Da $\left(\frac{\mu_0}{\lambda_0} w_0, \ldots, \frac{\mu_n}{\lambda_n} w_n\right)$ eine Basis von V' ist, gibt es genau einen Isomorphismus $f : V \to V'$ mit $f(v_i) = \frac{\mu_i}{\lambda_i} w_i$ für alle $i = 0, \ldots, n$. Die durch f induzierte Projektivität $P(f)$ erfüllt nach Konstruktion $P(f)(p_i) = q_i$ für alle $i = 0, \ldots, n$. Außerdem gilt

$$\begin{aligned} P(f)(p_{n+1}) &= Kf(v_{n+1}) = K(\lambda_0 f(v_0) + \cdots + \lambda_n f(v_n)) = K(\mu_0 w_0 + \cdots + \mu_n w_n) \\ &= Kw_{n+1} = q_{n+1}. \end{aligned}$$

Somit erfüllt $g := P(f)$ die geforderten Bedingungen und es bleibt zu zeigen, dass g die einzige solche Projektivität ist.

Sei also $g' = P(f')$ eine weitere Projektivität $P(V) \to P(V')$ mit $g'(p_i) = q_i$ für alle $i = 0, \ldots, n+1$. Dann gibt es $\xi_0, \ldots, \xi_{n+1} \in K \setminus \{0\}$ mit

$$f'(v_i) = \xi_i w_i$$

für alle $i = 0, \ldots, n+1$. Insbesondere gilt dann

$$\begin{aligned} \xi_{n+1}(\mu_0 w_0 + \cdots + \mu_n w_n) &= \xi_{n+1} w_{n+1} = f'(v_{n+1}) = f'(\lambda_0 v_0 + \cdots + \lambda_n v_n) \\ \lambda_0 \xi_0 w_0 + \cdots + \lambda_n \xi_n w_n. \end{aligned}$$

Da $(w_0, \ldots, w_n)$ eine Basis von V' ist, folgt daraus für alle $i = 0, \ldots, n$

$$\xi_i = \xi_{n+1} \frac{\mu_i}{\lambda_i}$$

und somit $f'(v_i) = \xi_{n+1} f(v_i)$ für alle $i = 0, \ldots, n$. Es folgt $f' = \xi_{n+1} f$, weil $(v_0, \ldots, v_n)$ eine Basis von V ist. Also gilt $g' = P(\xi_{n+1} f) = P(f) = g$, was die Eindeutigkeit von g zeigt. □

Wir wenden nun diesen Satz auf projektive Geraden an. Drei beliebige verschiedene Punkte (a, b, c) einer projektiven Gerade g bilden eine projektive Basis (Beispiel 6.21). Es gibt daher eine eindeutige Projektivität $\phi : g \to \mathbb{P}^1(K)$ mit

$$\phi(a) = \infty,\ \phi(b) = 0,\ \phi(c) = 1,$$

wobei $\mathbb{P}^1(K) = P(K^2)$ wie in Beispiel 6.12 mit $K \cup \{\infty\}$ identifiziert ist.

Definition 6.23 *Seien a, b, c, d vier Punkte auf einer projektiven Gerade g, so dass a, b, c paarweise verschieden sind, und $\phi : g \to \mathbb{P}^1(K)$ wie oben. Dann heißt $\phi(d) \in K \cup \{\infty\}$ das* Doppelverhältnis *von a, b, c, d und wird mit $[a, b, c, d]$ bezeichnet.*

Der Name „Doppelverhältnis“ wird durch die folgende Proposition gerechtfertigt.

Proposition 6.24 *Seien A, B, C, D vier Punkte auf einer affinen Gerade g, so dass A, B, C paarweise verschieden sind. Dann gilt für das Doppelverhältnis von A, B, C, D in einer projektiven Vervollständigung $\overline{g} := g \cup \{\infty\}$ von g die Beziehung*

$$[A, B, C, D] = \begin{cases} \frac{\tau(D,B,A)}{\tau(C,B,A)} & , D \neq A \\ \infty & , D = A \end{cases},$$

wobei $\tau(D, B, A)$ bzw. $\tau(C, B, A)$ das Teilverhältnis aus Definition 3.14 bezeichnet.

Beweis : Nach Wahl eines Koordinatensystems können wir g mit K und $\overline{g}$ wie in Beispiel 6.12 mit $P(K^2) = \mathbb{P}^1(K) = K \cup \{\infty\}$ identifizieren. Die gegebenen Punkte $A, B, C, D \in g$ sind daher als Punkte des projektiven Raums $P(K^2)$ von der Form

$$\begin{aligned} A &= K \cdot (a, 1), \\ B &= K \cdot (b, 1), \\ C &= K \cdot (c, 1), \\ D &= K \cdot (d, 1) \end{aligned}$$

für gewisse $a, b, c, d \in K$ und der unendlichferne Punkt $\{\infty\}$ entspricht dem Punkt $K \cdot (1, 0)$ in $P(K^2)$. Wir rechnen nun nach, dass die eindeutige Projektivität $\phi : P(K^2) \to P(K^2)$ mit $\phi(A) = \infty$, $\phi(B) = 0$ und $\phi(C) = 1$ durch $\phi = P(f)$ gegeben ist, wobei

$$f(z, \lambda) = ((c - a)(z - \lambda b), (c - b)(z - \lambda a)).$$

In der Tat gilt

$$\begin{aligned} \phi(A) &= K \cdot f(a, 1) = K \cdot ((c - a)(a - b), 0) = K \cdot (1, 0) = \infty, \\ \phi(B) &= K \cdot f(b, 1) = K \cdot (0, (c - b)(b - a)) = K \cdot (0, 1) = 0, \\ \phi(C) &= K \cdot f(c, 1) = K \cdot ((c - a)(c - b), (c - b)(c - a)) = K \cdot (1, 1) = 1. \end{aligned}$$

Die behauptete Formel für das Doppelverhältnis folgt nun durch Nachrechnen: Im Fall $D = A$ gilt $[A, B, C, D] = \phi(D) = \infty$. Im Fall $D \neq A$ ist

$$\phi(D) = K \cdot f(d, 1) = K \cdot ((c - a)(d - b), (c - b)(d - a)) = \frac{(c - a)(d - b)}{(c - b)(d - a)}$$

und es gilt nach Defintion des Teilverhältnisses von drei Punkten $\tau(D, B, A) = \frac{b-d}{a-d}$ sowie $\tau(C, B, A) = \frac{b-c}{a-c}$, es gilt also in der Tat

$$[A, B, C, D] = \phi(D) = \frac{\tau(D, B, A)}{\tau(C, B, A)}$$

wie behauptet. □

Proposition 6.25 *Seien g und g' zwei projektive Geraden und A, B, C, D bzw. A', B', C', D' vier Punkte auf g bzw. g', wovon jeweils die ersten drei paarweise verschieden sind. Dann gilt: Es gibt genau dann eine Projektivität $\phi : g \to g'$ mit*

$$\phi(A) = A',\ \phi(B) = B',\ \phi(C) = C',\ \phi(D) = D', \tag{6.2}$$

wenn die Doppelverhältnisse $[A, B, C, D]$ und $[A', B', C', D']$ gleich sind.

Diese Proposition zeigt insbesondere, dass projektive Abbildungen das Doppelverhältnis von vier Punkten erhalten. Diese Aussage ist analog dazu, dass affine Abbildungen das Teilverhältnis von drei Punkten erhalten.

Beweis : Nach Beispiel 6.21 und Satz 6.22 gibt es eindeutige Projektivitäten $\phi : g \to g'$, $\psi : g \to \mathbb{P}^1(K)$ und $\psi' : g' \to \mathbb{P}^1(K)$ mit

$$\begin{aligned} \phi(A) &= A',\ \phi(B) = B',\ \phi(C) = C', \\ \psi(A) &= \infty,\ \psi(B) = 0,\ \psi(C) = 1, \\ \psi'(A') &= \infty,\ \psi'(B') = 0,\ \psi'(C') = 1. \end{aligned}$$

Wegen der Eindeutigkeitsaussage in Satz 6.22 gilt $\psi' \circ \phi = \psi$ und es gibt genau dann eine Projektivität mit den Eigenschaften (6.2), wenn $\phi(D) = D'$ gilt. Letzteres ist äquivalent zu $\psi'(D') = \psi'(\phi(D)) = \psi(D)$, also zur Gleichheit der Doppelverhältnisse $[A, B, C, D]$ und $[A', B', C', D']$. □

7 Gruppen und Untergruppen

Den Begriff einer Gruppe haben wir in [LA1] kennengelernt, zusammen mit den Begriffen von Untergruppe sowie Gruppenhomomorphismus.

Als wichtigstes Beispiel wurde dort die *symmetrische Gruppe* zu einer beliebige Menge M definiert als

$$S_M = \{f \colon M \longrightarrow M \mid f \text{ ist bijektiv}\}.$$

Wir haben als günstige Schreibweise die Zykeldarstellung eingeführt und gezeigt, dass jedes Element von S_M sich als Produkt von Transpositionen schreiben lässt. Das *Signum* war ein wichtiges Beispiel für einen Gruppenhomomorphismus $(S_M, \circ) \to (\{\pm 1\}, \cdot)$. Diese Gruppe ist *endlich*, d.h. sie besteht aus endlich vielen Elementen, genau dann wenn M eine endliche Menge ist.

Ein weiteres Beispiel für eine Gruppe aus der Vorlesung [LA1] ist die Gruppe der linearen Abbildungen $\mathrm{GL}(V)$ eines Vektorraums V oder konkreter die Gruppe $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$-Matrizen mit Einträgen in einem Körper K.

7.1 Ordnung von Elementen und Untergruppen

Wenn nicht anders bezeichnet, so schreiben wir die Gruppenverknüpfung hier multiplikativ. Mehrfahres Hintereinanderausführung schreiben wir daher als Potenzen, also $g^n = g \circ \cdots \circ g$ mit n Faktoren, falls $n \in \mathbb{N}$ ist, $g^0 = e$ ist das neutrale Element per Definition und $g^{-n} = g^{-1} \circ \cdots \circ g^{-1}$ ist die n-fache Verknüpfung des inversen Elements zu g. Mit dieser Schreibweise gelten die üblichen Potenzgesetze. Man beachte, dass im Allgemeinen $(gh)^n \neq g^n h^n$ gilt, aber dass in abelschen Gruppen hier Gleichheit gilt.

Viele Beispiele von Gruppen in diesem Abschnitt werden endliche Gruppen sein, aber die Definition sind nicht auf diesen Fall beschränkt.

Definition 7.1 *Die* Ordnung *eines Elements $g \in G$ ist das kleinste $n \in \mathbb{N}_{>0}$ mit $g^n = e$, falls es so ein n gibt. In diesem Fall schreiben wir $\mathrm{ord}(g) = n$. Andernfalls hat g* unendliche Ordnung, *in Zeichen $\mathrm{ord}(g) = \infty$.*

Es ist auch üblich die Mächtigkeit einer Gruppe G als deren *Ordnung* zu bezeichnen und das Symbole $\mathrm{ord}(G)$ zu verwenden. Diese beiden Begriffe hängen wie folgt zusammen. Für $g \in G$ schreiben wir

$$\langle g \rangle = \{g^z, z \in \mathbb{Z}\}$$

und nennen diese die von g *erzeugte* Untergruppe. Wir können auch den Gruppenhomomorphismus

$$\varphi_g : \mathbb{Z} \to G, \qquad z \mapsto g^z$$

betrachten. Dann ist $\langle g \rangle = \mathrm{Bild}(\varphi_g)$ und damit ist klar, dass dies wirklich eine Untergruppe von G ist.

Proposition 7.2 *Für jedes $g \in G$ ist $\mathrm{ord}(g) = \mathrm{ord}(\langle g \rangle)$ und falls $\mathrm{ord}(g) = n < \infty$, so ist*

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}\,.$$

Falls $\mathrm{ord}(g) = \infty$ so impliziert $g^a = g^b$, dass $a = b$.

Beweis : Wir schreiben $a = qn + r$ mit $0 \leq r < n$. Dann ist $g^a = (g^n)^q \cdot g^r = g^r$ und somit sind alle Potenzen von g in der genannten Menge. Die genannten Elemente sind zudem verschieden, denn wäre $g^a = g^b$ mit $0 \leq a < b < n$, so ist $g^{b-a} = e$, im Widerspruch zur Definition der Ordnung.

Für die zweite Aussage schließen wir analog, dass aus $g^a = g^b$ wieder $g^{b-a} = e$ folgt, und wenn $b \neq a$, so hätte g endliche Ordnung. □

Beispiel 7.3 Sei P_n ein regelmässiges n-Eck, desse Punkte auf dem Einheitskreis im $\mathbb{R}^2$ liegen und sodass ein Punkt bei 1 ist. Die Ecken sind also die sogenannten n-ten Einheitswurzeln, die wir als komplexe Zahlen $e^{2\pi ik/n}$ for $k = 0, 1, \ldots, n$ auffassen können. Wir untersuchen die Symmetriegruppe von P_n, die affinen Abbildungen, die P_n wieder in sich überführen. Zu diesen gehört die Drehungen um den Winkel φ, die Abbildungen

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto D_\varphi \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{7.1}$$

falls φ von der Form $2\pi ik/n$ für $k \in \mathbb{Z}$ ist. Für $k = 1$ hat die Drehung die Ordnung n.

Ebenfalls eine Symmetrie von P_n ist die Achsenspiegelung S an der x-Achse. Diese Spiegelung hat offensichtlich Ordnung 2.

Beispiel 7.4 Für jeden Körper K ist die Gruppe

$$\mathrm{SL}_n(K) \;=\; \{A \in \mathrm{GL}_n(K) \,:\, \det(A) = 1\} \tag{7.2}$$

eine Untergruppe von $\mathrm{GL}_n(K)$, die *spezielle lineare Gruppe*. Wir betrachten nun $K = \mathbb{Q}$. Dann ist

$$\mathrm{SL}_n(\mathbb{Z}) \;=\; \{A \in \mathrm{SL}_n(\mathbb{Q}) \,:\, A \in \mathrm{Mat}^{2\times 2}(\mathbb{Z})\} \tag{7.3}$$

eine Untergruppe von $\mathrm{SL}_n(K)$. (Warum? Formel für die Inverse mit Hilfe der Adjunkten!) Es ist

$$\mathrm{ord}(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) \;=\; \infty, \quad \mathrm{ord}(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}) \;=\; 2, \quad \mathrm{ord}(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}) \;=\; 4,$$

Finden Sie eine Matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ mit $\mathrm{ord}(U) = 3$!

7.2 Untergruppen und Erzeuger

Bei Vektorräumen hatten wir den Schnitt und die Summe von Vektorräumen definiert und in diesem Zusammenhang den Begriff der Linearkombination eingeführt. Darauf hatten wir die Begriffe Erzeugendensystem und Basis aufgebaut. Der Begriff 'Summe' ist bei Untergruppen im Allgemeinen nicht erklärt, lediglich 'direkte Summe' kann man definieren. Wir starten daher etwas anders.

Proposition 7.5 *Sei G eine Gruppe und U_i für $i \in I$ Untergruppen. Dann ist $\cap_{i\in I} U_i$ auch eine Untergruppe, der* Schnitt der Untergruppen.

Beweis : Wie beim Schnitt von Untervektorräumen. □

Ist die Indexmenge I angeordnet (z.B. $I = \mathbb{N}$) und hat man die starke Zusatzvoraussetzung $U_i \subseteq U_j$ falls $i \leq j$, so ist auch $\cup_{i\in I} U_i$ eine Untergruppe. (Die Situation und das Argument ist wie beim Beweis der Existenz einer Basis.) Diese Voraussetzung ist selten gegeben. Stattdessen betrachten wir folgende Konstruktion. Sei $S \subset G$ eine nichtleere Teilmenge und $T = S \cup S^{-1}$ die Teilmenge, die auch alle Inversen von S enthält. Dann definiert man $T^0 = \{e\}$ und

$$T^n \;=\; \underbrace{T \cdots T}_{n}$$

als die Menge der *Worte der Länge n in den Symbolen S*. Da T^n unter Inversenbildung abgeschlossen ist, ist offenbar

$$\langle S\rangle \;=\; \bigcup_{n\geq 0} T^n \tag{7.4}$$

eine Untergruppe von G, die *von S erzeugte Untergruppe*. Wir geben noch eine andere Charakterisierung dieser Gruppe.

Proposition 7.6 *Die Untergruppe $\langle S\rangle$ ist der Schnitt aller Untergruppen, die S enthalten, in Zeichen*

$$\langle S\rangle \;=\; \bigcap_{S\subset U} U\,.$$

Beweis : Ist U eine Untergruppe mit $S \subset U$, so ist auch $T \subset U$ und $T^n \subset U$ für alle n aufgrund der Untergruppeneigenschaften. Damit ist die linke Seite in der rechten Seite enthalten. Da $\langle S\rangle$ eine Untergruppe ist, die S enthält, ist die andere Inklusion offensichtlich. □

Eine Menge S mit $\langle S\rangle = G$ nennen wir ein *Erzeugendensystem* von G. Aus der Definition folgt, dass wir ein beliebiges Element von G (nicht als Linearkombination sondern) als Wort in $S \cup S^{-1}$ schreiben können, wobei die Wortlänge a priori unbeschränkt ist. Jede Gruppe hat offenbar $S = G$ als Erzeugendensystem und in der Praxis wollen wir möglichst kleine Erzeugendensysteme finden. Aus der Definition folgt direkt, dass wenn S ein Erzeugendensystem von G ist und $f : G \to H$ ein Gruppenhomomorphismus, dann ist die Bildmenge $f(S)$ ein Erzeugendensystem von H.

Beispiel 7.7 Ein Erzeugendensystem für die Gruppe $\mathrm{GL}_n(K)$ ist gegeben durch die Elementarmatrizen $M_i(\lambda), E_{ij}(\lambda), V_{ij}$ wie in [LA1] definiert. Der Beweis hiervon ist konstruktiv, gegeben durch den Gauß-Algorithmus.

Ebenfalls in [LA1] haben wir gezeigt, dass die Tranpositionen ein Erzeugendensystem für die symmetrische Gruppe S_n für $n \geq 2$ bilden.

Zeigen Sie, dass die Drehung um den Winkel $2\pi/n$ und die Achsenspiegelung S die Symmetriegruppe des regulären n-Ecks P_n erzeugen.

7.3 Gruppenhomomorphismen und der Homomorphiesatz

Die Begriffe Gruppenhomomorphismus und Vektorraumhomomorphismus hatten wir in [LA1] eingeführt. Ist f ein solcher Homomorphismus, so wird in beiden Fällen der *Kern* als das Urbild der Null $\mathrm{Ker}(f) = f^{-1}(0)$ definiert. Wir hatten nachgewiesen, dass der Kern eines Vektorraumhomomorphismus ein Untervektorraum ist und der gleiche Beweis zeigt, dass der Kern eines Gruppenhomomorphismus eine Untergruppe ist. Welche Untergruppen bzw. welche Untervektorräume können als Kerne auftreten? Hier zeigt sich, dass die Gruppentheorie wesentlich subtiler ist.

Ist $h \in G$ und $g \in G$ ein weiteres Element, so nennen wir das Elment hgh^{-1} ein *zu h konjugiertes Element*. Ist $U \subset G$ eine Teilmenge, so schreiben wir

$$gUg^{-1} \;=\; \{ghg^{-1} \,:\, h \in U\}\,.$$

Falls U eine Untergruppe ist, so nennen wir gUg^{-1} eine zu U konjugierte Gruppe. Eine Untergruppe N mit der Eigenschaft $gNg^{-1} = N$ für alle $g \in G$ heißt ein *Normalteiler* von G. Offenbar sind die Untergruppen $\{e\}$ und ganz G Normalteiler. Die Untergruppe erzeugt von der Transposition (12) in S_3 ist kein Normalteiler. In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler, wie man direkt anhand der Definition sieht.

Die folgende Eigenschaft motiviert diesen Begriff:

Proposition 7.8 *Ist $f : G \to H$ ein Gruppenhomomorphismus und $N = \mathrm{Ker}(f)$, so ist N ein Normalteiler von G.*

Beweis : Ist $n \in N$ und $g \in G$, so ist

$$f(gng^{-1}) \;=\; f(g)e_H f(g^{-1}) \;=\; f(g)f(g)^{-1} \;=\; e_H$$

also $gng^{-1} \in N$. Damit ist $gNg^{-1} \subset N$. Da Multiplikation von links mit g^{-1} eine Bijektion ist folgt auch $Ng^{-1} \subset g^{-1}N$ und da Multiplikation von rechts mit g auch eine Bijektion ist, folgt $N \subset g^{-1}Ng$. Da g ein beliebiges Gruppenelement war und wir es in diesem Argument mit dem Inversen ersetzen können, folgt hiermit die umgekehrte Inklusion. □

Das Argument aus dem Beweis sagt, dass wir für einen Normalteiler immer nur die Inklusion $gNg^{-1} \subset N$ für alle g nachweisen müssen.

Es bleibt also die Frage, ob alle Normalteiler Kerne von Homomorphismen sind. Dies ist eine Gelegenheit einen allgemeines Konzept von mathematischen Objekten einzuführen, eine universelle Abbildungseigenschaft. Diese charakterisiert das Objekt durch Existenz und Eindeutigkeit einer Abbildung. Die Frage, ob ein Objekt mit diesen Wünschen existiert, ist im Einzelfall zu entscheiden und bedarf einer speziellen Konstruktion.

Definition 7.9 *Sei $N \subset G$ ein Normalteiler. Ein* Quotient Q (von G nach N) *ist eine Gruppe zusammen mit einem Gruppenhomomorphismus $q : G \to Q$ sodass $N \subset \mathrm{Ker}(q)$ gilt, und sodass der Gruppenhomomorphismus universell in folgendem Sinne ist: Für jeden anderen Gruppenhomomorphismus $f : G \to H$, der auch N im Kern hat, gibt es genau eine Abbildung $\overline{f} : Q \to H$, sodass $\overline{f} \circ q = f$ gilt.*

Objekte, die durch eine Solche universelle Abbildungseigenschaft definiert sind, sind eindeutig bestimmt in folgendem Sinne. Man beachte, dass die Eindeutigkeit der Abbildung hierbei wesentlich verwendet wird.

Lemma 7.10 *Sind $q : G \to Q$ und $q' : G \to Q'$ beides Quotienten von G nach N so gibt es genau einen Gruppenhomomorphismus $\varphi : Q \to Q'$ und genau eine Gruppenhomomorphismus $\varphi' : Q' \to Q$ sodass $\varphi \circ q = q'$ und $\varphi' \circ q' = q$. Die beiden Abbildungen φ und φ' sind zueinander invers, also Gruppenisomorphismen.*

Zeichnen Sie sich die Gruppen und Abbildungen im folgenden Beweis in einem Diagramm auf!

Beweis : Da $q : G \to Q$ ein Quotient ist, können wir die Definition mit $f = q'$ anwenden und erhalten φ' mit $\varphi' \circ q' = q$. Da $q' : G \to Q'$ ein Quotient ist, können wir die Definition mit $f = q$ anwenden und erhalten φ mit $\varphi \circ q = q'$. Die Abbildung ist ein beiden eindeutig, wie gefordert.

Nun betrachten wir nochmal den Quotient $q : G \to Q$ und wenden die Definition auf die Abbildung q selbst an. Dann erfüllt sicher id_Q die Gleichung $\mathrm{id}_Q \circ q = q$. Es ist aber auch $\varphi' \circ \varphi \circ q = \varphi' \circ q' = q$. Wegen der Eindeutigkeit in der Definition folgt $\varphi' \circ \varphi = \mathrm{id}_Q$. In diesem Argument können wir an jeder Stelle die Rollen von Q und Q' vertauschen und erhalten auch $\varphi \circ \varphi' = \mathrm{id}_{Q'}$. Damit sind die Abbildungen zueinander invers. □

Für die Existenz von Quotienten benötigen wir den Begriff der Faktorgruppe. Dazu definieren wir für eine Untergruppe $N \subset G$ die Relation

$$g \sim g' \quad \text{falls es } n \in N \text{ gibt, sodass } gn = g' \tag{7.5}$$

Dies ist eine Äquivalenzrelation (Übung, ganz analog zur Äquivalenzrelation, die wir bei der Definition des Faktorraums in [LA1] eingeführt hatten). Die Äquivalenzklasse von g ist

$$gN = \{gn : n \in N\}\,.$$

Man beachte, dass bei Gruppen, die nicht kommutativ sind, es relevant ist ob wir in der Definition der Äquivalenzrelation von rechts oder links mit n multiplizieren. Oben haben wir von rechts multipliziert und nennen daher gN eine *Rechtsnebenklasse von N*. Ganz analog

können wir eine Äquivalenzrelation durch Multiplikation von links definieren und daher nennen wir $Ng = \{ng : n \in N\}$ eine Linksnebenklasse. Die Äquivalenrelation sowie die Begriffe der Rechts- und Linksnebenklassen benötigen nur, dass N eine Untergruppe ist!

Sei nun wieder N ein Normalteiler, also $gNg^{-1} = N$ oder $gN = Ng$ für alle $g \in G$. Normalteiler zu sein ist also äquivalent dazu, dass jede Rechtnebenklasse von g auch gleich der Linksnebenklasse von g ist. Dies verwenden wir wie folgt:

Proposition 7.11 *Sei $N \subseteq G$ ein Normalteiler. Auf der Menge G/N der Rechtsnebenklassen ist die Abbildung*

$$\cdot : G/N \times G/N \to G/N, \quad (gN, hN) \mapsto ghN$$

wohldefiniert und macht die Menge mit der Inversenabbildung $i(gN) = g^{-1}N$ zu einer Gruppe, genannt die Faktorgruppe *von G nach N.*

Beweis : In der Definition der Abbilung haben wir die Rechtsnebenklassen durch Vertreter benannt. Wir zeigen, dass diese Abbildung von dieser Wahl unabhängig ist, denn die Abbildung ist auch das (elementweise) Produkt von Teilmengen, wie

$$(gN) \cdot (hN) = g \cdot (Nh) \cdot N = g \cdot (hN) \cdot N \; = \; gh \cdot N$$

zeigt. Die Assoziativität prüft man genauso und verwendet wiederum, dass N ein Normalteiler ist. Die Nebenklasse $N = eN$ ist das neutrale Element. □

Satz 7.12 *Die Faktorgruppe G/N is ein Quotient von G nach N.*

Beweis : Zunächst benötigen wir die Quotientabbildung $q : G \to G/N$, welche einfach durch $g \mapsto gN$ gegeben ist. Dies ist in der Tat ein Gruppenhomomorphismus, denn

$$q(gh) = ghN = gN \cdot hN = q(g) \cdot q(h)\,,$$

wobei wir die Rechnung aus dem vorigen Beweis rückwärts gelesen haben. Offenbar ist $N \subset \mathrm{Ker}(q)$, womit eine Bedingung des Quotienten erfüllt ist.

Sei nun $f : G \to H$ mit $N \subset \mathrm{Ker}(f)$ gegeben. Die gesuchte Abbildung $\overline{f}$ muss die Rechtsnebenklasse $gN = q(g)$ auf $f(g)$ schicken. Also prüfen wir, ob die Definition $\overline{f}(gN) = f(g)$ eine wohldefinierte Abbildung ergibt. Ist $h = gn$ ein weiterer Vertreter der Nebenklasse, so ist $\overline{f}(hN) = f(h) = f(gn) = f(g)$, da $n \in \mathrm{Ker}(f)$. Man prüfe nach, dass $\overline{f}$ in der Tat ein Gruppenhomomorphismus ist. Damit haben wir alle geforderten Eigenschaften mitgeprüft, nämlich die Verkettungseigenschaft $\overline{f} \circ q = f$ und die Eindeutigkeit, denn diese stecken beide in der Aussage "muss ... schicken". □

Die universelle Eigenschaft des Quotienten ist der erste Schritt im Beweis des Homomorphiesatzes. Dessen Korollare zum Abzählen von Gruppenordnungen werden in dieser Vorlesung hauptsächlich angewandt werden.

Satz 7.13 (Homomorphiesatz) *Sei $f : G \to H$ ein Gruppenhomomorphismus. Denn gibt es einen Gruppenisomorphismus*

$$\varphi : G/\operatorname{Ker}(f) \to \operatorname{Im}(f)\,.$$

Beweis : Nach Proposition 7.8 is $\operatorname{Ker}(f)$ ein Normalteiler von G und somit $G/\operatorname{Ker}(f)$ eine Gruppe. Aufgrund der Eigenschaften des Quotienten gibt es eine Abbildung $G/\operatorname{Ker}(f) \to H$, welche per Definition des Bildes die Verkettung der gesuchten Abbildung $\varphi : G/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ und der Inklusion $\operatorname{Im}(f) \to H$ ist. Offensichtlich ist φ surjektiv.

Sei nun $g \in \operatorname{Ker}(\varphi)$. Dann ist $g \in \operatorname{Ker}(\varphi \circ q) = \operatorname{Ker}(f)$, also $g \in N$. Damit ist aber $gN = N$ die Nebenklasse des neutralen Elements und φ injektiv, was noch zu zeigen war. □

Korollar 7.14 *Sei $f : G \to H$ ein Gruppenhomomorphismus und G endlich. Dann gilt*

$$|G/\operatorname{Ker}(f)| \;=\; |\operatorname{Im}(f)| \quad \textit{und} \quad |G| = |\operatorname{Ker}(f)| \cdot |\operatorname{Im}(f)|\,.$$

Die erste Aussage ist unmittelbare Konsequenz des Homomorphiesatzes. Die zweite Aussage werden wir im nächsten Kapitel mitbeweisen.

7.4 Semidirekte Produkte

Das semidirekte Produkt ist eine Konstruktion um nicht-kommutative Gruppen aus zwei gegebenen (möglicherweise, aber nicht notwendig kommutativen) Gruppen zu konstruieren. Es ist eine Variante des Produkts von Gruppen. Wir werden erst die Konstruktion einführen und dann analysieren, welche uns bekannten Gruppen semidirekte Produkte sind.

Proposition 7.15 *Seien N, H zwei Gruppen und $\Psi : H \to \operatorname{Aut}(N)$ ein Gruppenhomomorphismus. Dann ist die Menge $G = N \times H$ mit der Gruppenverknüfung Dann wird die Menge $G = N \times H$ zusammen mit der Verknüpfung*

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \Psi(h_1)(n_2), h_1 h_2)$$

zu einer Gruppe. Via der Abbildungen $n \longmapsto (n, 1)$ und $h \longmapsto (1, h)$ kann man N und H als Untergruppen von G auffassen. Dabei ist N ein Normalteiler.

Eine Merkregel für die Verknüfung lautet: Will man h_1 nach rechts an n_2 vorbeiziehen, so muss man n_2 um $\Psi(h_1)$ abändern. Beispiele für einen solchen Homomorphismus Ψ sind die offensichtliche Inklusion im Fall

$$H = \mathrm{GL}_n(K), \quad , N = K^n, \quad \Psi : \mathrm{GL}_n(K) \to \mathrm{Aut}(K^n) \tag{7.6}$$

wobei man beachten soll, dass K^n einfach als Gruppe aufgefasst wird und es daher a priori mehr Gruppenautomorphismen $\mathrm{Aut}(K^n)$ als lineare Abbildungen $\mathrm{GL}_n(K)$ geben könnte. Ein anderes Beispiel ist

$$H = \mathbb{Z}/2b\mathbb{Z}, \quad N = \mathbb{Z}/n\mathbb{Z}, \quad \Psi : -1 \mapsto (x \mapsto -x)\,. \tag{7.7}$$

Natürlich ist für Ψ auch der Homomorphismus erlaubt, der alles auf $id \in \mathrm{Aut}(N)$ schickt. Damit vereinfacht sich die Gruppenverknüpfung und wir erhalten das direkte Produkt zurück.

Beweis : Wir prüfen die Assoziativität:

$$\begin{aligned}
\Big((n_1,h_1)\cdot(n_2,h_2)\Big)\cdot(n_3,h_3) &= \Big(n_1\Psi(h_1)(n_2),h_1h_2\Big)\cdot(n_3,h_3)\\
&= \Big(n_1\Psi(h_1)(n_2)\Psi(h_1h_2)(n_3),h_1h_2h_3\Big)\\
(n_1,h_1)\cdot\Big((n_2,h_2)\cdot(n_3,h_3)\Big) &= (n_1,h_1)\cdot\Big(n_2\Psi(h_2)(n_3),h_2h_3\Big)\\
&= \Big(n_1\Psi(h_1)\big(n_2\Psi(h_2)(n_3)\big),h_1h_2h_3\Big)\\
&= \Big(n_1\Psi(h_1)(n_2)\Psi(h_1h_2)(n_3),h_1h_2h_3\Big).
\end{aligned}$$

Neutrales Element ist offenbar $(1,1)$ und das Inverse zu (n,h) ist $\Big(\big(\Psi(h^{-1})(n)\big)^{-1},h^{-1}\Big)$. Die Untergruppenaussagen sind klar. Für die Normalteilereigenschaft rechnet man

$$\begin{aligned}
(n_2,h_2)\cdot(n_1,1)\cdot(n_2,h_2)^{-1} &= \Big(n_2\Psi(h_2)(n_1),h_2\Big)\Big(\Psi(h_2^{-1})(n_2)^{-1},h_2^{-1}\Big)\\
&= \Big(n_2\Psi(h_2)(n_1)n_2^{-1},1\Big)\in N.
\end{aligned}$$

nach. □

Die Normalteilereigenschaft gibt ein Hinweis darauf, welche Gruppen als semidirekte Produkte identifiziert werden können. Die genaue Aussage ist der folgende Satz

Satz 7.16 *Ist G eine Gruppe, die einen Normalteiler N und eine weitere Untergruppe H mit $N \cap H = \{1\}$ und $G = N \cdot H$ enthält, so ist G zu einem semidirekten Produkt $N \rtimes H$ isomorph.*

Beweis : Für jedes $h \in H$ ist die Abbildung $n \longmapsto hnh^{-1} \in N$ ein Automorphismus von N. Die damit erhaltene Abbildung $\Psi\colon H \longrightarrow \mathrm{Aut}(N)$ ist wegen

$$\Psi(gh)(n) = ghnh^{-1}g^{-1} = \Psi(g)\Big(\Psi(h)(n)\Big)$$

ein Homomorphismus. Wir betrachten die Abbildung

$$\varphi\colon N \times H \longrightarrow G, \quad (n,h) \longmapsto n \cdot h$$

und behaupten, dass die Abbildung φ ein Homomorphismus ist, falls $N \times H$ mit der Verknüpfung eines semidirekten Produkts bezüglich obigem Ψ versehen wird. Wegen $N \cap H = \{1\}$ und $G = N \cdot H$ ist φ dann sogar ein Isomorphismus. Wir müssen also noch nachrechnen

$$\varphi(n_1,h_1) \cdot \varphi(n_2,h_2) = n_1 h_1 n_2 h_2$$

und

$$\begin{aligned}\varphi\Big((n_1,h_1)\cdot(n_2,h_2)\Big) &= \varphi\Big(n_1\Psi(h_1)(n_2), h_1h_2\Big)\\ &= \varphi(n_1h_1n_2h_1^{-1}, h_1h_2) = n_1h_1n_2h_2,\end{aligned}$$

womit die Homomorphie von φ gezeigt ist. □

Wir kennen folgende Beispiele von semidirekten Produkten:

- Die Diedergruppen, die Symmetriegruppen des regelmässigen n-Ecks aus Beispiel 7.3 sind isomorph zum semidirekten Produkt aus (7.7)
- Die affine Gruppe $\mathrm{Aff}(\mathbb{A}^n)$ aus Satz 3.23 ist isomorph zum semidirekten Produkt in (7.6).

8 Gruppenoperationen

Definition 8.1 *Eine* Operation *der Gruppe G auf der Menge X ist eine Abbildung $G \times X \to X$, die wir üblichweise als $(g,x) \mapsto g \cdot x$ oder einfach $(g,x) \mapsto gx$ schreiben, und welche folgenden Eigenschaften genügt.*

i) Es gilt die formale Assoziativität $g \cdot (h \cdot x) = (gh) \cdot x$ *für alle $g,h \in G$ und alle $x \in X$.*

ii) Das neutrale Element operiert als Identität, d.h. $e \cdot x = x$ für alle $x \in G$.

Statt (Gruppen)operation sind auch (Gruppen)wirkung und (Gruppen)aktion übliche synonyme Bezeichnungen. Genauer gesagt haben wir eine Linksoperation definiert. Analog ist eine Rechtsoperation eine Abbildung $X \times G \to X$, bei der nun die formale Assoziativität die Gestalt

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

annimmt. Man prüfe, dass bei einer gegebenen Linksoperation die Abbildung $(x,g) \mapsto g^{-1}x$ eine Rechtsoperation definiert. Die sorgfältige Trennung der Begriffe ist unter anderem dann wichtig, wenn eine Menge zwei Operationen, eine von links und eine von rechts, hat. Eine Menge mit G-Operation nennt man auch *G-Menge*.

Wir geben einige Beispiele von Gruppenoperationen.

- Die Gruppe $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ operiert auf $\mathbb{C}$ durch $(\lambda, x) \mapsto \lambda x$.
- Die Gruppe $\mathrm{GL}_n(K)$ operiert auf K^n durch Linksmultiplikation $(A, x) \mapsto A \cdot x$.
- Die Gruppe S_n operiert auf $\{1, \ldots, n\}$ durch $(f, k) \mapsto f(k)$.
- Die Gruppe $\mathrm{SL}_2(\mathbb{R})$ operiert auf $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ durch (Übung!)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}\,. \tag{8.1}$$

Diese Beispiele kombinieren eine Gruppe, die auf und einer Menge ohne Gruppenstruktur operiert. Wenn wir nur eine Gruppe gegeben haben, dann gibt es zwei Operationen, die in der Folge wichtig sind, in der jeweils die Gruppe auf sich selbst operiert. Die Operation

$$G \times G \to G, \quad (g, x) \mapsto gx \qquad g, x \in G \tag{8.2}$$

wird *Linksmultiplikation* oder manchmal auch *Linkstranslation* genannt. Der zweite Begriff ist anschaulich, wenn wir $G = (\mathbb{R}, +)$ oder auch $G = (\mathbb{R}^2, +)$ nehmen. Die Operation

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1} \qquad g, x \in G$$

wird *(Operation durch) Konjugation* genannt. Wie unterschiedlich die beiden Operationen sind, wird anhand der folgenden Begriff deutlich:

Definition 8.2 *Die Gruppe G operiere auf der Menge X. Die* Bahn *von $x \in X$ (oder auch der G-*Orbit *von x) ist die Menge*

$$Gx := G \cdot x := \{y \in X \,:\, \textit{es gibt } g \in G : y = gx\}\,.$$

Der Stabilisator *von $x \in X$ ist die Untergruppe*

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

Der Bahnenraum *ist die Menge der Teilmengen*

$$G\backslash X := \{B \subset X, B = G \cdot x \textit{ für ein } x \in X\}\,.$$

Man beachte, dass der kleine Symbolunterschied von Gx zu G_x einen drastischen Bedeutungsunterschied nach sich zieht.

Wir analysieren einige der Beispiele oben, beginnend mit der Operation von $\mathbb{C}^*$ auf $\mathbb{C}$. Die Bahn von 0 ist einelementig, bestehend nur aus der Null. Die Bahn von jedem anderen Element $\lambda \in \mathbb{C} \setminus \{0\}$ ist gleich $\mathbb{C} \setminus \{0\}$, denn zu jedem $\mu \in \mathbb{C} \setminus \{0\}$ gibt es ein $g \in \mathbb{C}^*$ mit $g\mu = \lambda$. Also ist hier der Bahnenraum $\mathbb{C}^*\backslash\mathbb{C}$ zweielementig. Der Stabilisator von 0 ist

$G_0 = \mathbb{C}^*$, aber von jedem anderen Element $\lambda \in \mathbb{C} \setminus \{0\}$ ist der Stabilisator $G_\lambda = \{1\}$, die triviale Gruppe. Man sieht hier schon die Faustregel "je kleiner der Stabilisator, desto größer die Bahn", welche wir noch präziser machen werden.

Die Operation von $\mathrm{GL}_n(K)$ auf K^n ist eine Verallgemeinerung hiervon: Es gibt wieder nur zwei Bahnen, die Bahn der Null und die Bahn des ersten Einheitsvektors, die alle anderen Elemente enthält. (Übung! Basisergänzungssatz!)

Bei der Operation von S_n auf $\{1, \ldots, n\}$ gibt es nur eine Bahn. Man sagt in diesem Fall die Operation ist *transitiv*. Auch die Operation von $\mathrm{SL}_2(\mathbb{R})$ auf $\mathbb{H}$ ist transitiv. Wir bestimen den Stabilisator von $i \in \mathbb{H}$. Ist $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i)$, so gilt

$$\frac{ai+b}{ci+d} = i, \quad \text{also} \quad ai + b = -c + di\,.$$

Es gilt also $a = d$ und $b = -c$. Aus $1 = \det(A) = ad - bc = a^2 + b^2$ folgt, dass wir $a = \cos(\varphi)$ und $b = -\sin(\varphi)$ schreiben können. Die Umkehrung dieses Schlusses ist offenbar auch richtig und wir fassen zusammen

$$\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i) = \left\{ \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \right\}.$$

Proposition 8.3 *Die Gruppe G operiere auf der Menge X. Dann ist die Relation $x \sim y$ genau dann wenn es ein $g \in G$ gibt mit $gx = y$ eine Äquivalenzrelation. Die Äquivalenzklassen sind genau die Bahnen von G.*

Beweis : Reflexivität wird durch das Einselement und Symmetrie durch Verwendung des inversen Elements zertifiziert. Ist $x \sim y$ und $y \sim z$ so gibt es $g_1, g_2 \in G$ mit $g_1 x = y$ und $g_2 y = z$. Dann ist $g_2 g_1 x = z$, also $x \sim z$ und somit gilt Transitivität. Die zweite Behauptung ist offensichtlich. □

8.1 Die Bahnbilanz

Wir machen nun die Faustregel von oben präsize:

Satz 8.4 (Bahnbilanz) *Die endliche Gruppe G operiere auf der Menge X. Dann gilt*

$$|G| \;=\; |G_x| \cdot |G \cdot x| \qquad \textit{für jedes } x \in X\,.$$

Außerdem gilt

$$|X| \;=\; \sum_{B \in G\backslash X} |G|/|G_{x_B}|\,,$$

wobei x_B ein beliebiges Element der Bahn B ist.

Beweis : Für die erste Aussage fixieren wir ein $x \in X$ und betrachen die Linksmultiplikation $\ell : G \to X$, die $g \mapsto gx$ abbildet. Das Bild dieser Abbildung ist die Bahn B von x per Definition. Das Urbild $\ell^{-1}(x)$ ist per Definition gleich G_x. Wir behaupten, dass

i) jedes Urbild $\ell^{-1}(y)$ für $y \in B$ hat $|G_x|$ Elemente, und
ii) diese Urbilder sind disjunkt.

Aus den beiden Behauptungen folgt die erste Formel des Satzes offensichtlich. Zum Beweis von i) geben wir explizit eine Bijektion an. Sei $g \in G$ so gewählt, dass $gx = y$. Dann ordnen wir $h \in \ell^{-1}(x)$ das Element gh zu, was wegen

$$ghx \;=\; gx \;=\; y \tag{8.3}$$

in der Tat in $\ell^{-1}(y)$ liegt. Ist umgekehrt $u \in \ell^{-1}(y)$, so liegt $g^{-1}u \in \ell^{-1}(y)$. Da diese Zuordnungen zueinander invers sind, zeigt das die Bijektion und somit habe alle diese Urbilder $|G_x|$ Elemente. Die Behauptung ii) gilt für jede Abbildung.

Für die zweite Formel summieren wir die erste über alle Bahnen von X. Es gilt also

$$|X| \;=\; \sum_{B \in G\backslash X} |B| \;=\; \sum_{B \in G\backslash X} |G|/|G_{x_B}|\,.$$

Dass der Ausdruck auf der rechten Seite unabhängig von der Wahl des Elements $x(B)$ in der Bahn ist, haben wir durch die erste Formel bereits beweisen. □

Wir verwenden die Bahnbilanz auf projektive Räumen um die Anzahl der Elemente in $\mathrm{GL}_2(\mathbb{F}_p)$ für den endlichen Körper $\mathbb{F}_p$ mit p Elementen zu bestimmen. Sei $\mathbb{P}^1 = \mathbb{P}^1(\mathbb{F}_p) = P(\mathbb{F}_p^2)$ die Menge aller 1-dimensionalen Unterräume von $\mathbb{F}_p^2$ wie in Abschnitt 6. Wir schreiben den vom Vektor $(x, y)^T \in \mathbb{F}_p^2$ aufgespannten eindimensionalen Unterraum hier mit Doppelpunkt $(x : y)$ (statt mit dem sonst für den Spann üblichen Symbol). Man beachte, dass $(x : y) = (cx : cy) \in \mathbb{P}^1(\mathbb{F}_p)$ für jedes $c \in \mathbb{F}_p^1 \setminus \{0\}$. Es gilt

$$|\mathbb{P}^1(\mathbb{F}_p)| \;=\; (|\mathbb{F}_p^2| - 1)/(|\mathbb{F}_p - 1|) \;=\; (p^2 - 1)/(p - 1) \;=\; p + 1\,.$$

Die Gruppe $\mathrm{GL}_2(K)$ operiert für einen beliebigen Körper auf $\mathbb{P}^1(K)$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x : y) \;=\; (ax + by : cx + dy)\,.$$

Die Transitivität der Operation folgt aus der Transitivität aus der Operation auf K^2.

Der Stabilisator von $(1 : 0)$ ist die ("Borel")-Untergruppe $B_2(\mathbb{F}_p) \subset \mathrm{GL}_2(\mathbb{F}_p)$ der oberen Dreiecksmatrizen (mit beliebigen Elementen auf der Diagonalen). Diese Gruppe hat $p(p-1)^2$ Elemente. Aufgrund des Satzes gilt also

$$|\,\mathrm{GL}_2(\mathbb{F}_p)| = |B_2(\mathbb{F}_p)| \cdot |\mathbb{P}^1(\mathbb{F}_p)| \;=\; p(p-1)^2(p+1) \;=\; (p^2-1)(p^2-p)\,.$$

Das Ergebnis hätten wir auch schneller erhalten können: In der ersten Spalten steht ein Vektor ungleich Null. Dafür gibt es $p^2 - 1$ Möglichkeiten. Bei gegebener ersten Spalte ist die zweite Spalte in Vektor, der nicht Vielfaches der ersten Spalte ist (denn sonst ist die Determinante Null), der aber sonst keinen Einschränkungen unterliegt. Dafür gibt es $p^2 - p$ Möglichkeiten.

Wir wenden jetzt die Bahnbilanz auf die Operation durch Linkstranslation an.

Proposition 8.5 *Es gibt eine Bijektion $U\backslash G \cong G/U$ zwischen Linksnebenklassen und Rechtsnebenklassen. Die Anzahl dieser Nebenklassen wir als* Index *bezeichnet und mit $(G : U) = |G/U|$ abgekürzt. Es gilt*

$$(G : U) \;=\; |G|/|U|\,.$$

Beweis : Für die erste Aussage ordnen wir gU die Menge $(gU)^{-1} = Ug^{-1}$ zu. Aus der ersten Schreibweise dieser Menge sieht man dass die inverse Zuordnung auch durch Invertieren gegeben ist und dass dies somit eine Bijektion ist.

Die zweite Aussage folgt aus der Operation von G auf G/U. □

Zum Beispiel ist $\mathrm{SL}_2(\mathbb{F}_p)$ in $\mathrm{GL}_2(\mathbb{F}_p)$ eine Untergruppe vom Index $|\mathbb{F}_p^*| := |\mathbb{F}_p \backslash \{0\}| = p-1$, denn die Abbildung $\det : \mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^*$ ist offenbar surjektiv, hat Kern $\mathrm{SL}_2(\mathbb{F}_p)$ und nach dem Homomorphiesatz ist

$$|\,\mathrm{GL}_2(\mathbb{F}_p)/\,\mathrm{SL}_2(\mathbb{F}_p)| \;=\; |\mathbb{F}_p^*|\,.$$

Satz 8.6 (Lagrange) *Sei U eine Untergruppe der endlichen Gruppe G. Dann gilt $|G| = |G/U| \cdot |U|$.*

Hiermit haben wir offenbar auch den Beweis von Korollar 7.14 vervollständigt.

Beweis : Auf der Menge G/U haben wir eine Operation von G durch Linksmultiplikation, d.h. $h \cdot gU \mapsto hgU$. (Man prüfe kurz die Wohldefiniertheit!) Diese Operation ist offensichtlich transitiv, d.h. es gibt nur eine Bahn. Der Stabilisator der Nebenklasse $U = eU$ ist die Untergruppe U. Die Aussage des Satzes ist also genau die erste Formel der Bahnbilanz angewandt auf $X = G/U$ und $x = eU$. □

Dieser Satz hat die folgenden offensichtlichen, aber extrem nützlichen Konsequenzen.

Korollar 8.7 *Ist U eine Untergruppe von G, so ist $|U|$ ein Teiler von $|G|$. Ist g ein Element von G, so ist $\mathrm{ord}(g)$ ein Teiler von $|G|$.*

Beispielsweise ist in der Gruppe S_6 mit $6! = 720$ Elementen kein Platz für ein Element der Ordnung 7. Bestimmen Sie alle Elementordnungen von Elementen in S_6 (Zykelzerlegung!).

Satz 8.8 *Jede Gruppe G, deren Ordnung eine Primzahl p ist, ist eine* zyklische Gruppe, *d.h. sie ist von einem Element erzeugt. Genauer gesagt ist jedes Element in $G \setminus \{e\}$ ein Erzeuger. Die Gruppe G ist isomorph zur Gruppe $\mathbb{Z}/p\mathbb{Z}$.*

Beweis : Ist $g \in G \setminus \{e\}$, so ist $1 \neq \mathrm{ord}(g)$ ein Teiler von p und somit $\mathrm{ord}(g) = p$, da p Primzahl. Damit folgen die ersten zwei Behauptungen. Für die letzte Aussage fixieren wir wieder ein $g \in G \setminus \{e\}$ und betrachten die Abbildung

$$\varphi : \mathbb{Z} \to G, \qquad n \mapsto g^n \,.$$

Diese Abbildung ist surjektiv, da g ein Erzeuger ist. Der Kern der Abbildung enhält offenbar die Untergruppe $p\mathbb{Z}$. Gäbe es ein $n \in \mathrm{Ker}(\varphi) \setminus p\mathbb{Z}$, so gäbe es nach Division mit Rest auch ein $n \in \mathrm{Ker}(\varphi)$ mit $0 \leq n < p$. Das ist ein Widerspruch und somit ist $\mathrm{Ker}(\varphi) = p\mathbb{Z}$. Nach dem Homomorphiesatz folgt die Behauptung. □

8.2 Zentrum, Zentralisator, Normalisator

Wir betrachten nun einige Untergruppen, die durch Eigenschaften der Operation durch Konjugation entstehen. Wir nennen wir zwei Untergruppen U_1 und U_2 *konjugiert*, falls es ein $g \in G$ gibt, sodass $gU_1g^{-1} = U_2$ ist. Dieser Begriff definiert offenbar eine Äquivalenzrelation auf der Menge aller Untergruppen.[1]

Lemma 8.9 *Konjugierte Untergruppen sind zueinander isomorph*

Beweis : Die Abbildung $u \mapsto gug^{-1}$ definiert offenbar eine Bijektion von U_1 nach U_2, denn die umgekehrte Bijektion wird durch Konjugation mit g^{-1} gegeben. Man rechnet jetzt noch nach, dass diese Abbildung ein Gruppenhomomorphismus ist. □

Beispielsweise sind in der S_n alle Untergruppen der Form $\{e, \tau\}$, wobei τ eine Transposition ist, zueinander konjugiert. Um dies zu zeigen, seien $U_1 = \langle (ij) \rangle$ und $U_2 = \langle k\ell \rangle$ zwei solche Untergruppen. Wir nehmen eine Bijektion $g \in S_n$ her, welche $g(i) = k$ und $g(j) = \ell$ erfüllt und ansonsten beliebig ist. Dann ist $gU_1g^{-1} = U_2$.

Für ein weiteres Beispiel betrachten wir die Isometriegruppe des regelmässigen n-Ecks mit n ungerade. Darin sind alle Untergruppen, die von einer Achsenspiegelung erzeugt werden, zueinander konjugiert. (Übung! Das konjugierende Element ist eine Drehung.) Gilt das auch für n gerade? Machen Sie sich an diesem Beispiel klar, dass in einer endlichen Gruppe nicht alle Untergruppen einer gegeben Ordnung zueinander konjugiert sind. Dies gilt nicht einmal dann, wenn die Gruppen dir Ordnung zwei haben, und somit zueinander isomorph sind!

[1] Man beachte, dass die Operation durch Linkstranslation kein Pendant dieser Aussage hat: das Linkstranslat gU einer Untergruppe ist im Allgemeinen keine Untergruppe.

Definition 8.10 *Das* Zentrum $Z(G)$ *einer Gruppe* G *ist die Untergruppe bestehend aus den Elementen* z*, sodass* $zgz^{-1} = g$ *für alle* $g \in G$*.*

Die Elemente im Zentrum "kommutieren" mit allen Elementen der Gruppe G, d.h. es gilt $zg = gz$ für alle $g \in G$, wie man die definierende Bedinung auch äquivalent umschreiben kann. Das Zentrum besteht also genau aus den Fixpunkten bei der Operation durch Konjugation der Gruppe G auf der Menge G (der Gruppe selbst). Aus der Definition folgt auch direkt:

Proposition 8.11 *Das Zentrum einer Gruppe* G *ist ein Normalteiler von* G*.*

Ist G eine abelsche Gruppe, so ist $Z(G) = G$ per Definition. Ist $G = \mathrm{GL}_n(K)$ so sind die Diagonalmatrizen D_λ, bei denen alle Diagonaleinträge gleich $\lambda \in K$ sind, offensichtlich im Zentrum. Man kann zeigen, dass dies das gesamte Zentrum ist, also dass

$$Z(\mathrm{GL}_n(K)) \;=\; \{D_\lambda, \lambda \in K\}$$

gilt. (Übung! Gegeben eine Matrix A, die nicht von der Gestalt D_λ ist, suche man eine geeignete Elementarmatrix $E_{ij}(\mu)$, sodass $E_{ij}(\mu)A \neq AE_{ij}(\mu)$ ist.)

Proposition 8.12 *Das Zentrum der symmetrischen Gruppe* S_n *ist* S_n *für* $n \leq 2$ *und die triviale Gruppe für* $n \geq 3$*.*

Beweis : Die Aussage für $n \leq 2$ ist klar. Sei $n \geq 3$ und $\sigma \in S_n$ ein nichttriviales Element. Es enhält also einen nichttrivialen Zykel, sagen wir der Länge k. Wir können die Elemente von S_n so umbenennen, dass $\sigma = (12\cdots k)\sigma'$ ist, wobei σ' alle anderen Zykel von σ umfasst. Ist $k \geq 3$ so berechnen wir, dass

$$\sigma \circ (12) : 1 \mapsto 3, \quad (12) \circ \sigma : 1 \mapsto 1.$$

Ist $k = 2$, so berechnen wir, dass

$$\sigma \circ (123) : 1 \mapsto 1, \quad (123) \circ \sigma : 1 \mapsto 3.$$

In beiden Fällen haben wir ein Element gefunden, dass belegt, dass $\sigma \notin Z(S_n)$ ist. □

Die beiden folgenen Begriffe werden in dieser Vorlesung keine Rolle mehr spielen. Beides sind natürliche Konstruktionen, wie man aus einer Untergruppe durch Konjugation neue Untergruppen gewinnen kann. Die erste Definition sollte man mit der des Zentrums vergleichen.

Der *Zentralisator* $Z_G(U)$ einer Untergruppe U in G ist

$$Z_G(U) \;=\; \{g \in G : gu = ug \quad \text{für alle } u \in U\}\,.$$

Der *Normalisator* $N_G(U)$ einer Untergruppe ist

$$N_G(U) \;=\; \{g \in G : gUg^{-1} = U\}\,.$$

Aus der Definition folgt, dass das Zentrum der Zentralistor von ganz G ist, also $Z(G) = Z_G(G)$. Ebenfalls folgt aus der Definition direkt

$$Z(G) \subseteq Z_G(U) \subseteq N_G(U) \subseteq G\,. \tag{8.4}$$

8.3 Fixpunktaussagen und Gruppen mit wenig Primteilern

Wir werden nun mit Fixpunktaussagen und der Struktur des Zentrums die Struktur von Gruppen, deren Ordnung wenige Primteiler hat verstehen.

Proposition 8.13 *Ist G eine Gruppe der Ordnung p^n für eine Primzahl p, so hat G nichttriviales Zentrum.*

Dies gibt noch einen Beweis dafür, dass Gruppen der Ordnung p abelsch sind, was wir bereits oben bewiesen haben.

Beweis : Wir betrachten Bahnbilanz für die Operation durch Konjugation von G auf G selbst. Die Bahnen sind entweder Fixpunkte der Operation, oder die Bahn hat die Länge einer nichttrivialen Untergruppe. Da p die Ordnung von so einer Gruppe teilt, folgt

$$|G| \cong |\mathrm{Fix}(G)| \mod p \tag{8.5}$$

Da die Fixpunkte der Konjugationsoperation gerade die Elemente des Zentrums sind, führt die Annahme $Z(G) = \{e\}$ zu einem Widerspruch, und das beweist die Proposition. □

Als Übung beweise man:

Lemma 8.14 *Ist G eine Gruppe, sodass $G/Z(G)$ zyklisch ist, so ist G abelsch.*

Lemma 8.15 *Ist G eine Gruppe der Ordnung pq, wobei p und q Primzahlen sind, so ist G abelsch, oder $Z(G) = \{e\}$.*

Lemma 8.16 *Ist G eine Gruppe der Ordnung p^2, so ist G abelsch. Genauer gesagt ist $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Eine Gruppe der Ordnung p^3 ist nicht notwendigerweise abelsch, die Argumentation oben lässt sich also nicht 'per Induktion' fortsetzen. Ein Beispiel hierfür ist die Heisenberggruppe H über einen endlichen Körper, also die Gruppe der echten oberen Dreicksmatrizen

$$H \;=\; \left\{ M_{a,b,c} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}) \right\} \tag{8.6}$$

Diese Gruppe hat offenbar p^3 Elemente und es gilt

$$M_{1,0,0}M_{0,0,1} \;=\; M_{1,1,1} \;\neq\; M_{1,0,1} \;=\; M_{0,0,1}M_{1,0,0} \tag{8.7}$$

Zum Abschlußdieses Kapitels wollen wir eine 'Umkehrung' des Satzes von Lagrange beweisen. Dieser Satz gibt durch eine Teilbarkeitsaussage Einschränkungen, wann eine Untergruppe einer gewissen Ordnung existieren könnte. Der folgende Satz gibt eine Aussage, dass eine Untergruppe einer tatsächlich existiert.

Satz 8.17 *Sei G eine endliche Gruppe und die Primzahl p sei ein Teiler der Gruppenordnung von G. Dann gibt es eine Untergruppe U von G mit $|U| = p$.*

Die Sätze von Sylow geben noch präzisere Aussages, wann Gruppen von Ordnung eines gegebenen Teilers von G existieren. Vermutlich werden wir im Laufe der Vorlesung diese nicht mehr ansprechen können. Für interessierte Leser sei dazu ein Buch über Algebra, z.B. [Bos20] empfohlen.

Beweis : Wir lassen die zyklische Gruppe $Z = \mathbb{Z}/p\mathbb{Z}$ auf der Menge

$$X \;=\; \{(g_0, \ldots, g_{p-1}) \in G^p \;:\; g_0 \ldots g_{p-1} = 1\}$$

durch zyklische Vertauschung operieren, d.h. das Element $a \in Z$ operiert auf X durch

$$a \cdot (g_0, \ldots, g_{p-1}) = (g_a, \ldots, g_{a+p-1}),$$

wobei die Indizes in dieser Gleichung modulo p zu rechnen sind. Wir müssen nachweisen, dass dies wirklich eine Operation ist. Dazu ist zu zeigen, dass das Bild wirklich in X und nicht nur in G^p liegt. (Die Axiome einer Operation sind offensichtlich erfüllt.) Dazu stellen wir fest, dass Multiplikation mit von g_0^{-1} von links und anschließend Multiplikation mit von g_0 von rechts aus $g_0 \ldots g_{p-1} = 1$ die Gleichung $g_1 \ldots g_{p-1} g_0 = 1$. Wenn man das Argument a-fach anwendet, erhält man die Behauptung.

Wir zählen nun wieder Fixpunkte der Operation von Z auf X, denn dies sind Tupel der Form $(g, \ldots, g)$ mit $g^p = 1$. Also sind dies die Elemente, die die gesuchten Untergruppen

erzeugen, sowie der triviale Fixpunkt $(e, \ldots, e)$, der natürlich keine solche Untergruppe erzeugt. Es gilt nach der Bahnbilanz

$$|\mathrm{Fix}(Z, X)| \cong |X| \cong 0 \mod p$$

da alle anderen Bahnen die Länge $p = |Z|$ haben und da $|X| = G^{p-1}$ ein Vielfaches von p ist. (Man kann die ersten $p-1$ Elemente eines Tupels frei wählen und der letzte Eintrag ist dann eindeutig festgelegt.) Da es offensichtlich den trivialen Fixpunkt gibt, erzwingt die Kongruenz mindestens p Fixpunkte, also auch den gesuchten nichttrivialen Fixpunkt. □

9 Etwas Ringtheorie

Wir verweisen auf [LA1] für die Definition eines Rings, der bei uns immer ein Einselement hat, aber bei dem die Multiplikation nicht notwendigerweise kommutativ ist. Beispiele von Ringen sind die ganzen Zahlen $\mathbb{Z}$, die Ringe von $n \times n$-Matrizen, die Polynomringe und natürlich Körper. (Kartesische) Produkte von Ringen sind wieder Ringe.

Wir starten mit einigen fundamentalen Konzepten, wie dem der Quotienten. Dabei sehen wir Parallelen zur Gruppentheorie. Das faszinierende an Ringen ist das Konzept der Primfaktorenzerlergung, bzw. wann und wie sich dies von den ganzen Zahlen auf andere Ringe verallgemeinert. Wir werden dies für spezielle Ringe beantworten. Das Thema wird in den Vorlesungen Algebra, elementarer Zahlentheorie und algebraischer Zahlentheorie vertieft.

Sei $(R, +, \cdot)$ ein Ring. Ein Element $0 \neq a \in R$ ist *Nullteiler*, falls es ein $b \in R \setminus \{0\}$ gibt, mit $ab = 0$ und ein Element b' mit b' mit $b'a = 0$.[2] Ein Element $e \in R$ heißt *Einheit*, falls es ein Element $f \in R$ gibt mit $ef = 1$. Die Menge aller Einheiten bezeichnen wir mit $R^\times$. In dieser Schreibweise ist R ein Körper genau dann wenn $R^\times = R \setminus \{0\}$ ist. Ein Körper hat keine Nullteiler, auch ein Polynomring über einem Körper hat keine Nullteiler, aber das Kartesische Produkt von zwei Ringen hat stets Nullteiler, z.B. $(1, 0)$.

9.1 Ideale

Ein *Unterring* U von R ist eine nichtleere Teilmenge, die unter den beiden Ringverknüpfungen abgeschlossen ist. Ist S ein weiterer Ring, so ist ein *Ringhomomorphismus* eine Abbildung $f : R \to S$ mit $f(xy) = f(x)f(y)$ und $f(x + y) = f(x) + f(y)$ für alle $x, y \in R$. Hier passiert die erste Überraschung im Vergleich zu Vektorräumen, man vergleiche mit den analogen Aussagen zu Gruppen und Normalteilern.

[2] Gilt nur eine der beiden Bedingungen so spricht man von einem Rechtsnullteiler bzw. Linksnullteiler. In einem kommutativen Ring fallen die drei Begriffe offenbar zusammen.

Proposition 9.1 *Ist $f : R \to S$ ein Ringhomomorphismus, so ist* $\mathrm{Bild}(f)$ *ein Unterring von S. Der Kern* $\mathrm{Ker}(f)$ *ist ein Unterring $\mathcal{I} \subset R$, der zudem die Eigenschaft $r \cdot x \in \mathcal{I}$ und $x \cdot r \in \mathcal{I}$ für alle $r \in R$ und alle $x \in \mathcal{I}$ hat.*

Eine solchen Unterring $\mathcal{I}$ nennt man ein *Ideal* von R.[3] Die Menge aller Polynome in X^2 bilden zum Beispiel einen Unterring von $K[X]$, aber sie bilden kein Ideal, denn Multiplikation mit X bildet den Unterring nicht in sich ab.

Beweis : Die Unterringeigenschaften rechnet man direkt nach. Ist $x \in \mathrm{Ker}(f)$ und $r \in R$ so ist $f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$, also ist $rx \in \mathrm{Ker}(f)$. Analog ist $f(xr) = f(x)f(r) = 0 \cdot f(r) = 0$, also ist $xr \in \mathrm{Ker}(f)$ und das zeigt, dass der Kern ein Ideal ist. □

Im Abschnitt über Gruppentheorie haben wir den Begriff eines Quotienten (nach einem Normalteiler) definiert und gezeigt, dass es einen solchen Quotienten gibt. Genau so gehen wir hier vor, die Analogien mit dem Gruppentheorie-Abschnitt sind beabsichtigt.

Definition 9.2 *Sei $\mathcal{I} \subset R$ ein Ideal. Ein* Quotient Q (von R nach $\mathcal{I}$) *ist ein Ring zusammen mit einem Ringhomomorphismus $q : R \to Q$ sodass $\mathcal{I} \subset \mathrm{Ker}(q)$ gilt, und sodass der Ringhomomorphismus universell in folgendem Sinne ist: Für jeden anderen Ringhomomorphismus $f : R \to S$, der auch $\mathcal{I}$ im Kern hat, gibt es genau eine Abbildung $\overline{f} : Q \to S$, sodass $\overline{f} \circ q = f$ gilt.*

Die Eindeutigkeit eines Quotienten zeigt man wörtlich genau wie bei Gruppen. Für die Existenz wollen wir das Konzept der Faktorgruppe nachbauen. Sei also $\mathcal{I} \subset R$ ein Ideal. Dann definiert

$$x \sim_{\mathcal{I}} y \qquad \text{falls } x - y \in \mathcal{I} \tag{9.1}$$

eine Äquivalenzrelation auf R und wir schreiben $[x]$ für die Äquivalenzklasse von x (bzw. $[x]_{\mathcal{I}}$, falls wir das Ideal klarstellen müssen). Wir sagen in diesem Fall dass *x kongruent zu y modulo $\mathcal{I}$* ist.

Proposition 9.3 *Sei $\mathcal{I} \subset R$ ein Ideal. Auf der Menge $R/\mathcal{I}$ der Äquivalenzklassen sind die Abbildungen*

$$+ : R/\mathcal{I} \times R/\mathcal{I} \to R/\mathcal{I}, \quad ([x],[y]) \mapsto [x+y]$$
$$\cdot : R/\mathcal{I} \times R/\mathcal{I} \to R/\mathcal{I}, \quad ([x],[y]) \mapsto [xy]$$

wohldefiniert und machen $R/\mathcal{I}$ zu einem Ring, genannt der Faktorring *von R nach $\mathcal{I}$.*

[3] Genauer gesagt ist dies ein *zweiseitiges Ideal*. Gilt nur $r \cdot x \in \mathcal{I}$ für alle $r \in R$, so ist es ein *Linksideal*, gilt $x \cdot r \in \mathcal{I}$ für alle $r \in R$, so ist $\mathcal{I}$ ein *Rechtsideal*. Für kommutative Ringe, also für die wichtigen Beispiele $\mathbb{Z}$ und Polynomringe, auch in mehreren Variablen, fallen all diese Begriffe zusammmen. Matrixringe sind ein wichtiges Beispiel eines nicht-kommutativen Rings und man muss die Begriffe unterscheiden und aufpassen von welcher Seite man multipliziert, also beide definierenden Eigeschaften des zweiseitigen Ideals nachprüfen.

Beweis : Wir prüfen Wohldefiniertheit der Multiplikation und überlassen die Addition dem Leser. Sei $[x'] = [x]$ und $[y'] = [y']$, also $x' - x = a$ und $y' - y = b$ mit $a, b \in \mathcal{I}$. Dann ist

$$x'y' - xy \;=\; (x' - x)y' + x(y' - y) \;=\; ay' + xb \in \mathcal{I}. \tag{9.2}$$

Das additive Inverse von $[x]$ ist $[-x]$. Die Ringaxiome von $R/\mathcal{I}$ folgen direkt aus denen von R. □

Satz 9.4 *Der Faktorring $R/\mathcal{I}$ ist ein Quotient von R nach $\mathcal{I}$.*

Beweis : Die Quotientabbildung ist $q : x \mapsto [x]$. Der Rest ist wie in Satz 7.12. □

Ein wichtiges Beispiel für $R = \mathbb{Z}$ haben wir schon lange verwendet. Für $n \in \mathbb{N}$ ist die Menge $n\mathbb{Z} = \{z \in \mathbb{Z} : n \text{ teilt } z\}$ ein Ideal. Der Quotientenring $\mathbb{Z}/n\mathbb{Z}$ ist für $n = p$ prim ein Körper. Das Beispiel verallgemeinert sich wie folgt.

Sei R ein beliebiger kommutativer Ring und $a \in R$ ein beliebiges Element. Dann ist $Ra = \{ra : r \in R\} =: \langle a \rangle$ ein Ideal, genannt das von a erzeugte *Hauptideal*.

9.2 Hauptidealringe

Der Begriff Ideal leitet sich von 'idealen Zahlen' ab. Dieses Konzept stammt vom Satz über die Primfaktorenzerlegung, welcher im Ring der ganzen Zahlen gut bekannt ist. In anderen Ringen, zum Beispiel den Ganzzahligen von Körpererweiterungen, die in der Vorlesung Zahlentheorie behandelt weren, gilt dies nicht mehr. Man muss Faktorisierung in Zahlen durch Faktorisierung in 'idealen Zahlen' ersetzen. In Hauptidealringen entsprechen Zahlen (also Ringelemente) den Idealen und diese Problem tritt nicht auf. Wir werden also als Ziel dieses Abschnitts die Primfaktorenzerlegung in Hauptidealringen beweisen.

Definition 9.5 *Ein kommutativer, nullteilerfreier Ring R heißt* Hauptidealring, *falls jedes Ideal in R ein Hauptideal ist, d.h. falls es zu jedem Ideal $\mathcal{I} \subset R$ ein $r \in R$ gibt, sodass $\mathcal{I} = Rr$.*

Körper sind offensichtlich Hauptidealringe, denn dort gibt es nur das Nullideal und das Einsideal. In Körpern ist die Primfaktorenzerlegung nicht spannend und wir suchen zunächst ein gutes Kriterium für Hauptidealringe.

Definition 9.6 *Ein kommutativer, nullteilerfreier Ring R heißt* euklidisch, *falls es eine Gradabbildung $\deg : R \setminus \{0\} \to \mathbb{N}_{\geq 0}$ gibt, sodass es zu jedem $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ gibt mit*

$$a \;=\; qb + r \quad \textit{und} \quad \deg(r) \leq \deg(b) \quad \textit{oder } r = 0. \tag{9.3}$$

Ein Ring ist also euklidsch, falls es eine Division mit Rest gibt, also falls der Euklidische Algorithmus (zur Bestimmung des ggT) funktioniert. Die Ringe $\mathbb{Z}$ und $K[X]$ sind also nach [LA1] euklidisch. Ein weiteres Beispiel ist (Übung !)

$$\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}\,. \tag{9.4}$$

Satz 9.7 *Ist R euklidisch, so ist R ein Hauptidealring.*

Beweis : Sei $\mathcal{I} \subset R$ ein Ideal. Ist $\mathcal{I} = \{0\}$ das Nullideal, so liegt offenbar ein Hauptideal vor. Andernfalls gibt es Element ungleich Null in $\mathcal{I}$. Sei b ein solches Element, und zwar eines von minimalem Grad. Wir wollen zeigen, dass $\mathcal{I} = Rb$ ist. Sei also $a \in \mathcal{I}$ ein weiteres Element. Dann können wir (9.3) anwenden. Wegen der Gradminimalität von b muss $r = 0$ sein und damit ist $a = qb \in \mathcal{I}$, was zu zeigen war. □

Wir übersetzen nun die bekannten Begriffe der Teilbarkeit in die Sprache von Idealen. Sei R ein kommutativer, nullteilerfreier Ring und $a, b \in R$. Wir sagen a *teilt* b (in Zeichen $a|b$), falls es ein $x \in R$ gibt mit $xa = b$. Wir sagen, dass a und b *assoziiert* sind, falls es eine Einheit $r \in R^\times$ gibt, mit $a = rb$. Assoziiert sein ist offenbar eine Äquivalenzrelation.

Lemma 9.8 *Sei R nullteilerfrei und $a, b \in R \setminus \{0\}$. Es gilt $a|b$ genau dann wenn $\langle a\rangle \supset \langle b\rangle$.*

Beweis : Wenn $a|b$, also $xa = b$, so ist ein Element von $rb \in Rb$ gleich $r(xa) = (rx)a$ und somit in Ra. Umgekehrt folgt aus der Idealinklusion, dass $a \in Rb$ ist, also, dass es ein $x \in R$ gibt mit $xa = b$. □

Lemma 9.9 *Die Elemente a und b sind assoziiert genau dann, wenn die davon erzeugten Ideale gleich sind und dies gilt genau dann, wenn zugleich $a|b$ und $b|a$.*

Beweis : Zweimaliges Anwenden der ersten Aussage gibt die zweite Äquivalenz in der zweiten Aussage. Wenn $a = rb$ mit $r \in R^\times$, so gilt $b|a$ offensichtlich und es gibt ein $s \in R$ mit $rs = 1$, also $sa = b$. Daraus folgt $b|a$. Die umgekehrte Inklusion startet mit der Voraussetzung $a = rb$ und $b = sa$ für $r, s \in R$. Von diesen Elementen r, s müssen wir noch zeigen, dass es Einheiten sind. Kombination der Gleichungen gibt $b = srb$, also $b(sr - 1) = 0$. Jetzt nutzen wir die Nullteilerfreiheit und schließen $sr - 1 = 0$, also $sr = 1$. □

In der Umgangssprach wir der Begriff 'prim' für zwei Eigenschaften verwendet, von denen wir letztendlich sehen, dass sie in Hauptidealringen zusammenfallen, im Allgemeinen aber nicht äquivalent sind. Wir trennen die Begriff also sorgfältig.

Definition 9.10 *Sei R ein kommutativer, nullteilerfreier Ring und $p \in R$ ein Element, das weder Null noch eine Einheit ist. Das Element p heißt* irreduzibel, *wenn $p = ab$ folgt, dass $a \in R^\times$ oder $b \in R^\times$ ist. Andernfalls heißt p* reduzibel. *Das Element p heißt* prim, *falls aus $p|ab$ bereits $p|a$ oder $p|b$ folgt.*

Proposition 9.11 *Sei R ein kommutativer, nullteilerfreier Ring. Ist p prim, so ist p irreduzibel.*

Beweis : Sei p prim und $p = ab$. Dann folgt $p|a$ oder $p|b$, wobei wir den ersten Fall annehmen können indem wir gegebenenfalls die Rollen vertauschen. Also gibt es $x \in R$ mit $px = a$. Damit gilt $a = px = abx$, also $a(bx - 1) = 0$. Da $p \neq 0$ ist $a \neq 0$ und damit ist $b \in R^\times$. □

Proposition 9.12 *Ist R ein Hauptidealring und $p \in R$ irreduzibel, so ist p prim. In Hauptidealringen fallen also die Begriffe prim und irreduzibel zusammen.*

Beweis : Sei p irreduzibel und $p = ab$. Wir nehmen an, dass $p \not| a$ und wollen zeigen, dass dann $p|b$ gilten muss. Wir betrachten das Ideal kleinste Ideal $\mathcal{I}$, das a und p enhält. Nach Voraussetzung ist es von einem Element $y \in R$ erzeugt. Es gilt also $y|p$ und $y|a$. Es gibt also $c, d \in R$ mit $yc = p$ (und $yd = a$). Auf die erste Gleichung wenden wir die Voraussetzung 'irreduzibel' an. Ist c eine Einheit, so gilt $pc^{-1} = y$, also $pdc^{-1} = a$ im Widerspruch zur Annahme. Also ist y eine Einheit. Dann ist $(y) = R = \langle a, p\rangle$. Also gibt es $u, v \in R$ mit $ua + vp = 1$. Durchmultiplizieren mit b ergibt

$$b \;=\; uab + vpb \;=\; up + vpb \;=\; p(u + vb)$$

und daraus folgt $p|b$. □

Als ein Beispiel für einen Ring, in dem irreduzibel nicht prim impliziert, nehmen wir

$$\mathbb{Z}[\sqrt{10}] \;=\; \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}\,. \tag{9.5}$$

und betrachten das Element $p = 2$. Wir zeigen, dass p keine Einheit und irreduzibel ist. Dazu ist es nützlich die Abbildung

$$\sigma : \mathbb{Z}[\sqrt{10}] \to \mathbb{Z}[\sqrt{10}], \qquad a + b\sqrt{10} \mapsto a - b\sqrt{10}$$

zu betrachten. Sie ist ein Ringhomomorphismus (nachrechnen!) und hat die Eigenschaft, dass für jedes Element $x = a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ das Element $N(x) := x\sigma(x) = a^2 - 10b^2 \in \mathbb{Z}$ liegt. Wäre p eine Einheit, also $ps = 1$, so ist $N(p)N(s) = N(1) = 1$, aber $N(p) = 4$ und wir haben ein Widerspruch zur Teilbarkeit in $\mathbb{Z}$. Die gleiche Idee zeigt, dass p irreduzibel ist: Angenommen $p = xy$, so ist

$$4 \;=\; N(p) \;=\; N(x)N(y),$$

also $N(x), N(y) \in \{\pm 1, \pm 2, \pm 4\}$. Die einzige Faktorisierung, bei der weder x noch y eine Einheit ± 1 sind, ist $N(x) = N(y) = \pm 2$. Dies impliziert $a^2 - 10b^2 = \pm 2$. Da Quadratzahlen modulo 10 immer die Reste 1,4,5,6,9 haben, ist dies ein Widerspruch. Schließlich wollen wir noch zeigen, dass p nicht prim ist. Dazu beobachten wir, dass

$$p|(4 + \sqrt{10})(4 - \sqrt{10}) \; = \; 6,$$

aber man prüfe, dass weder $p|(4 + \sqrt{10})$ noch $p|(4 - \sqrt{10})$ gilt. (Angenommen doch, also $p(a + b\sqrt{10}) = 4 \pm \sqrt{10}$ für $a, b \in \mathbb{Z}$. Dann gilt $2a = 4$ und $2b = \pm 1$, was ein Widerspruch ist.)

Wir formalisieren jetzt den Begriff der Primfaktorenzerlegung.

Definition 9.13 *Sei R ein kommutativer, nullteilerfreier Ring. Der Ring ist* faktoriell, *falls sich jedes Element a, das nicht Null und keine Einheit ist, schreiben lässt als*

$$a \; = \; p_1 \cdots p_r \, , \tag{9.6}$$

wobei die p_i Primelemente in R sind.

Die Eindeutigkeit der Zerlegung (bis auf die offensichtlichen Änderungen in Reihenfolge und durch Einheiten) gilt ohne weitere Voraussetzungen.

Lemma 9.14 *Sei R ein kommutativer, nullteilerfreier Ring und*

$$p_1 \cdots p_r \; = \; q_1 \cdots q_s \tag{9.7}$$

für Primelemente p_i und q_j. Dann gilt $r = s$ und nach geeigneter Umnumerierung gilt $p_i = e_i q_i$ mit $e_i \in R^\times$ Einheiten.

Beweis : Nach etwaigem Vertauschen der Rollen können wir $r \leq s$ annehmen. Es gibt also ein Index j, sodass $p_1 | q_j$ da p_1 prim. Da aber auch q_j prim ist, folgt $p_1 = e_1 q_j$. Wir numerieren um, sodass $j = 1$ ist und teilen beide Seiten durch $p_1 = e_1 q_1$. Durch mehrfaches Anwenden des Arguments ist $r = 0$, also haben wir eine Gleichung

$$e = q_{r+1} \cdots q_s \tag{9.8}$$

für eine Einheit e. Indem wir dieses Produkt als Produkt von einem q_i mit allen anderen Faktoren auffassen sehen wir, dass dann die q_i für $i \geq r + 1$ Einheiten sein müssten, im Widerspruch dazu, dass Primelemente Einheiten ausschließt. □

Satz 9.15 *Ein Hauptidealring ist faktoriell.*

Beweis : In einen Widerspruchsbeweis nehmen wir an, dass wir einen Hauptidealring R vorliegen haben und ein Element $a \in R$, das keine Zerlegung wie in (9.6) zulässt. Dann ist nach Proposition 9.12 das Element a nicht prim, also nicht irreduzibel. Also $a = a_1 b_1$ mit $a_i, b_i \in R \setminus R^\times$, wobei mindestens eines der Elemente a_1 oder b_1 auch keine Zerlegung wie in (9.6) besitzt, denn sonst hätte das Produkt so eine Zerlegung. Wir nehmen an, dass a_1 keine solche Zerlegung besitzt und iterieren dieses Argument. Im n-ten Schritt ist $a := a_0 = a_1 a_2 \cdots a_n b_n$. Wir finden also eine Folge a_i von Ringelementen mit $a_{i+1} | a_i$, aber a_{i+1} ist nicht assoziiert zu a_i (da $b_i \notin R^\times$). Übersetzt mit Lemma 9.8 finden wir also eine Kette von Idealen

$$\langle a \rangle \;=\; \langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots \tag{9.9}$$

Die Vereinigung $\mathcal{I} = \bigcup_{i=1}^{\infty} \langle a_i \rangle$ ist wieder ein Ideal (Übung!), als nach Voraussetzung ein Hauptideal, sagen wir erzeugt von b. Dann gibt es aber ein Index i_0, sodass $b \in a_{i_0}$. Dann aber ist

$$\mathcal{I} = \langle b \rangle \subseteq \langle a_{i_0} \rangle \subseteq \bigcup_{i=1}^{\infty} \langle a_i \rangle \;=\; \mathcal{I}\,, \tag{9.10}$$

also sind alle Inklusionen Gleichheiten. Das aber widerspricht den strikten Inklusion in (9.9). □

Damit können wir auch den Rest der üblichen Teilbarkeitstheorie der ganzen Zahlen verallgemeinern. Man beachte, dass es in allgemeinen Ringen keine Ordnungsrelation (wie in $\mathbb{Z}$) gibt. Daher muss man mit Begriffen wie 'größter' aufpassen und die übliche Definition wie folgt abändern:

Definition 9.16 *Sei R kommutativ und nullteilerfrei und $a, b \in R \setminus \{0\}$. Ein* größter gemeinsamter Teiler von a und b, *in Zeichen* $\mathrm{ggT}(a, b)$, *ist ein Element $d \in R$ mit $d|a$ und $d|b$ und folgender Maximalitätseigenschaft: Ist $f \in R$ ein weiteres Element mit $f|a$ und $f|b$, so gilt $f|d$.*

Ein kleinstes gemeinsames Vielfaches von a und b, *in Zeichen* $\mathrm{kgV}(a, b)$, *ist ein Element $d \in R$ mit $a|d$ und $b|d$ und folgender Minimalitätseigenschaft: Ist $f \in R$ ein weiteres Element mit $a|f$ und $b|f$, so gilt $d|f$.*

Satz 9.17 *Ist R faktoriell, so gibt es für jedes Paar $a, b \in R \setminus \{0\}$ einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches.*

Beweis : Wir wählen ein Vertretersystem der Primzahlen in R, sodass die Vertreter paarweise nicht assoziiert sind. Seien diese Primzahlen als p_j mit $j \in J$ aufgelistet. Dann können wir die gegebenen Zahlen als

$$a \;=\; e_a \prod_{j \in J} p_j^{m_j} \quad \text{and} \quad b \;=\; e_b \prod_{j \in J} p_j^{n_j}$$

schreiben, wobei $e_a, e_b \in R^\times$ und $m_i \geq 0$ und $n_i \geq 0$ und zudem fast alle (d.h. alle bis auf endlich viele) m_i und n_i Null sind. Da Teilbarkeit aus der Primfaktorzerlegung direkt ablesbar ist, erfüllen

$$\begin{aligned} \mathrm{ggT}(a,b) &= \prod_{j\in J} p_j^{\min(m_j,n_j)} \\ \mathrm{kgV}(a,b) &= \prod_{j\in J} p_j^{\max(m_j,n_j)} \end{aligned}$$

offenbar die Bedingungen. □

Man kann den ggT und den kgV auch mit Hilfe von Idealen charackterisieren. Das liefert (beim ggT) die Darstellbarkeit als Linearkombination.

Proposition 9.18 *Seien $a, b \in R \setminus \{0\}$. Ist das Ideal $\langle a, b\rangle$ ein Hauptideal, erzeugt von $d \in R$, so ist $d = \mathrm{ggT}(a, b)$. Insbesondere gibt es $r, s \in R$ mit $ar + bs = \mathrm{ggT}(a, b)$.*

Die Voraussetzung in dieser Proposition ist in einem Hauptidealring natürlich immer erfüllt.

Beweis : Da $a, b \in \langle d\rangle = \langle a, b\rangle$ gilt $d|a$ und $d|b$ nach Lemma 9.8. Aus der Gleichheit dieser Idealerzeugnisse folgern wir auch sofort, dass es $r, s \in R$ gibt mit $ar + bs = d$. Sei $f \in R$ ein weiterer Teiler von a und b. Dieser ist Teiler von $ar + bs$, also auch von d und somit $d = \mathrm{ggT}(a, b)$. □

Als Übung überlege man sich, dass der Durchschnitt von Idealen auch stets in Ideal ist. Dann erhält man folgendes Pendant der Proposition: Ist das Ideal $\langle a\rangle \cap \langle b\rangle$ ein Hauptideal, erzeugt von $f \in R$, so ist $f = \mathrm{kgV}(a, b)$.

Und was ersetzt die Primfaktorzerlegung in Ringen, die kein Hauptidealring sind, wie z.B. $\mathbb{Z}[\sqrt{10}]$? Die Primidealzerlegung! Das Folgende ist eine Zusammenfassung des Materials, das in den Vorlesungen Algebra und dann in der Algebraischen Zahlentheorie genauer untersucht wird:
Statt Vektorräumen, bei denen die Skalare in einem Körper sind, untersucht man *R-Moduln*, die man auch "Ring-Vektorräume" nennen könnte. Alles, wo man nicht dividieren musste, klappt dann wie in der LA1. Aber Achtung, bereits der Gauß-Algorithmus beinhaltet Division in Form von der Elementarmatrizen M_λ. Ideale sind R-Moduln, aber man kann den Begriff erweitern: Statt in $R = \mathbb{Z}[\sqrt{10}]$ arbeitet man in $K = \mathbb{Q}[\sqrt{10}]$, was ein Körper ist, ein Teilkörper der reellen Zahlen. In K betrachtet man alle R-Moduln (nicht nur die Ideale, die auch in R enthalten sind) und nennt diese Menge *gebrochene Ideale*, da gewisse Nenner zugelassen sind. Außerdem läßt sich der Begriff des Primelements wörtlich auf Ideale verallgemeinern, indem man die Definition von Teilbarkeit mit Lemma 9.8 in Idealinklusion

übersetzt. Man erhält so den Begriff von *Primidealen*. Ausserdem ist das Produkt von Idealen wieder ein Ideal, und allgemeiner ist das Produkt von gebrochenen Idealen wieder ein gebrochenes Ideal. So definiert man *invertierbare gebrochene Ideale* als diejenigen, für die es einen Partner gibt, sodass das Produkt das Einsideal ist. Diese invertierbaren gebrochenen Ideale spielen die Rolle der Einheiten. Schließlich charakterisiert man die Ringe, die sich wie $R = \mathbb{Z}[\sqrt{10}] \subset K = \mathbb{Q}[\sqrt{10}]$ verhalten: sie sind 'lokal' Hauptidealringe und werden *Dedekindringe* genannt. Damit haben wir alle Vokabeln in der Hand für den folgenden Satz:

Satz 9.19 *In einem Dedekindring hat jedes gebrochene Ideal ungleich dem Nullideal eine eindeutige Faktorisierung in Primideale.*

Literatur

[Bos20] S. Bosch. *Algebra*. Ninth Edition. Springer Spektrum, Berlin, [2020] ©2020, S. x+490. URL: https://doi.org/10.1007/978-3-662-61649-9.

[Hil99] D. Hilbert. *Grundlagen der Geometrie*. Fourteenth Edition. Bd. 6. Teubner-Archiv zur Mathematik. Supplement. B. G. Teubner Verlagsgesellschaft mbH, Stuttgart, 1999, S. xxiv+408.

[LA1] M. Möller. *Lineare Algebra 1*. 2021. eprint: Vorlesungsskript, Frankfurt/Main.