Schulmathematik vom höheren Standpunkt aus

Vorlesungszusammenfassung

(fast) finale Version

1. Geometrie und Symmetriegruppen

1.1. Grundlegende geometrische Objekte

Welche mathematische Voraussetzungen benötigt man um Punkte, Geraden und Ebenen definieren zu können? Welche Zusatzinformationen braucht man um Abstände, Längen und Winkel zu definieren?

Um Geraden sowie Ebenen definieren zu können, muss die Grundmenge V eine reelle Vektorraumstruktur (oder zumindest eine affine Struktur) haben.

Definition 1.1.1. Eine *Gerade* in einem Vektorraum V nennt man jeden eindimensionalen Untervektorraum und deren Bilder unter Translationen. Eine *Ebene* in V nennt man jeden zweidimensionalen Untervektorraum und deren Bilder unter Translationen. Punkte sind einfach die Elemente (Vektoren) aus V.

Eine Translation $T_v : V \to V$ um v ist die Abbildung $T_v(x) := v + x$ für ein beliebiges aber festes $v \in V$.

Ein typisches Beispiel eines n-dimensionalen Vektorraumes ist $\mathbb{R}^n$, die Menge aller n-Tupeln reeller Zahlen. Vereinbarungsgemäß schreiben wir diese Tupel als Spaltenvektoren. Allerdings ist $\mathbb{R}^n$ mehr als ein bloßer n-dimensionaler Vektorraum, denn es gibt in $\mathbb{R}^n$ eine ausgezeichnete Basis und einen ausgezeichneten Skalarprodukt: die kanonische Basis $e_1 = (1, 0, \dots, 0)^T, \dots, e_n = (0, \dots, 0, 1)^T$ sowie $\langle x, y\rangle_{\text{kan}} = x^T \cdot y$.

In jedem Vektorraum gibt es einen ausgezeichneten Punkt: den Nullpunkt, d.h. das neutrale Element der Gruppe $(V, +)$. Für viele geometrische Überlegungen ist jedoch die Hervorhebung von 0 nicht nötigt. Daher führt man den Begriff eines n-dimensionalen affinen Raumes ein, in dem alle Punkte gleichberechtigt sind. Grob gesagt, ein affiner Raum ist ein Vektorraum (besser gesagt die darunter liegende Menge V) der vollkommen homogen ist, d.h., in dem kein Punkt (z.B. der Nullpunkt) besonders auszeichnet ist. Aber wie formuliert man diesen Sachverhalt mathematisch korrekt? Dazu kann man den Begriff einer Gruppenwirkung benutzen.

Definition 1.1.2. Es sei $(G, \circ)$ eine Gruppe (mit dem neutralen Element e) und X eine Menge. Eine *Gruppenoperation* (oder *Gruppenwirkung*) von G auf X ist eine Abbildung $\mu : G \times X \to X$ mit den folgenden Eigenschaften:

O1 $\mu(e, x) = x$ für alle $x \in X$.

O2 Für alle $g, h \in G$ und $x \in X$ gilt: $\mu(g, \mu(h, x)) = \mu(g \circ h, x)$

Eine Gruppenoperation heißt *transitiv*, falls für jedes Paar (x, y) von Elementen aus X es ein $g \in G$ mit $\mu(g, x) = y$ gibt.

Eine Gruppenoperation heißt *einfach transitiv*, falls für jedes Paar (x, y) von Elementen aus X es genau ein $g = g_{x,y} \in G$ mit $\mu(g, x) = y$ gibt.
Oft benutzen wir von Anfang an die "Verknüpfungsschreibweise" und schreiben z.B. $\diamond : G \times X \to X$ statt $\mu : G \times X \to X$ sowie $g \diamond x$ statt $\mu(g, x)$.
Gegeben sie die Operation $\cdot : G \times X \to X$. Jedes Element $g \in G$ induziert eine Abbildung $X \to X$, $x \mapsto g \cdot x$. Diese Abbildung ist eine Bijektion, da $x \mapsto g^{-1} \cdot x$ deren Umkehrabbildung ist: $g^{-1} \cdot (g \cdot x) = (g^{-1} g) \cdot x = e \cdot x = x$ und $g \cdot (g^{-1} \cdot x) = (g g^{-1}) \cdot x = e \cdot x = x$ gilt für alle $x \in X$. Von nun an für jedes $g \in G$ schreiben wir $g : X \to X$ für die Abbildung $x \mapsto g \cdot x$, falls aus dem Kontext ersichtlich ist, welche Gruppenoperation $\cdot : G \times X \to X$ gemeint ist.

Definition 1.1.3. Es sei $\cdot : G \times X \to X$ eine Gruppenoperation. Einen *G-Orbit* [eine *G-Bahn*] durch $x \in X$ nennt man die Teilmenge:

$$G(x) := G \cdot x := \{g \cdot x : g \in G\}$$

Die Relation $x \sim y \overset{\text{Def}}{\iff} \exists\, g \in G,\ g \cdot x = y$ ist eine Äquivalenzrelation. Deren Äquivalenzklassen sind genau die (paarweise disjunkten!) G-Bahnen.

Beispiele.
(a) Die Operation $\mathrm{SL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$ (Multiplikation von $n \times n$ und $n \times 1$ Matrizen) hat genau zwei $\mathrm{SL}_n(\mathbb{R})$-Bahnen: $\{0\}$ und $\mathbb{R}^n \setminus \{0\}$.
(b) Die Operation $\mathrm{SO}(2, \mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2$ hat unendlich viele $\mathrm{SO}(2, \mathbb{R})$-Bahnen, die sich durch den Halbstrahl $\mathbb{R}_{\geq 0}$ parametrisieren lassen: Eine $\mathrm{SO}(2, \mathbb{R})$-Bahn ist entweder eine Kreislinie um den Nullpunkt mit Radius $\rho > 0$ oder der Nullpunkt selbst (der Fall $\rho = 0$). Hier bezeichnet

$$\mathrm{SO}(2, \mathbb{R}) = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} : \alpha \in \mathbb{R} \right\} = \{A \in \mathbb{R}^{2\times 2} : A \cdot A^T = E_2 \text{ und } \det A = 1\}$$

die orthogonale Drehgruppe der Ebene.
(c) Die $(\mathbb{R}, +)$-Bahnen bzgl der Operation

$$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n, \qquad (\lambda, (x_1, \ldots, x_n)^T) \mapsto (x_1 + \lambda a_1, x_2 + \lambda a_2, \ldots, x_n + \lambda a_n)^T$$

sind alle zu $\mathbb{R} \cdot (a_1, \ldots, a_n)^T$ parallele Geraden in $\mathbb{R}^n$.
(d) Die $(\mathbb{R}, \cdot)$-Bahnen bzgl der Operation

$$\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n, \qquad (\lambda, (x_1, \ldots, x_n)^T) \mapsto (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)^T$$

sind alle Geraden in $\mathbb{R}$ durch den Ursprung ohne den Punkt $\{0\}$ und die einpunktige Menge $\{0\}$.

Definition 1.1.4. Ein reeller *affiner n-dimensionaler* Raum besteht aus einer Menge $\mathbb{A}$, zusammen mit einer einfach transitiven Operation $+ : V \times \mathbb{A} \to \mathbb{A}$ eines n-dimensionalen Vektorraumes V (hierbei wird die abelsche Gruppe $(V, +)$) als wirkende Gruppe betrachtet). Wir schreiben manchmal $V_{\mathbb{A}}$ um hervorzuheben, dass V der dem affinen Raum $\mathbb{A}$ zugeordnete Vektorraum ist und $\mathbb{A}^n$ statt $\mathbb{A}$ um die Dimension zu kennzeichen.

Aus der Definition folgt, dass für je zwei Punkte $A, B \in \mathbb{A}$ es genau einen Vektor $v \in V$ mit $v + A = B$ gibt. Durch das Fehlen eines ausgezeichneten Bezugspunktes (Nullpunktes) in $\mathbb{A}$ können zwar einzelne Punkte aus $\mathbb{A}$ nicht als Vektoren angesehen werden, dafür aber deren Differenzen, und wir erhalten die Differenzenabbildung $- : \mathbb{A} \times \mathbb{A} \to V$, $(Q, P) \mapsto v$ (mit dem durch $v + P = Q$ eindeutig bestimmten v; wir schreiben auch $Q - P$ für diesen Vektor v).
Jeder Vektorraum V trägt auch eine affine Struktur: Die definitionsgemäß gegebene Addition $+ : V \times V \to V$, $(v, w) \mapsto v + w$ liefert die (einfach transitive!) Operation von V auf sich selbst.

Es sei $\mathbb{A}$ ein affiner Raum und $\dotplus : V \times \mathbb{A} \to \mathbb{A}$ die einfach transitive Operation. Für jeden Untervektorraum $W \subset V$ ist die Einschränkung $W \times \mathbb{A} \to \mathbb{A}$ wieder eine Gruppenoperation von $(W, +)$ auf $\mathbb{A}$ (die nicht transitiv ist wenn $W \neq V$). Geraden und Ebenen im affinen Raum $\mathbb{A}$ sind dann spezielle Beispiele von Bahnen solcher Unterräume W. Genauer:

Definition 1.1.5. Wir verwenden die vorhergehende Notation.
- Ein affiner k-dimensionaler Unterraum $\mathbb{B} \subset \mathbb{A}$ ist eine Bahn $W(A)$ eines Unterrvektorraumes $W \subset V$ mit $\dim W = k$.
- Eine Gerade in $\mathbb{A}$ ist ein eindimensionaler affiner Unterraum.
- Eine Ebene in $\mathbb{A}$ ist ein zweidimensionaler affiner Unterraum.

Definition 1.1.6. Es seien $\mathbb{A}$, $\mathbb{B}$ zwei affine Räume, mit den definitionsgemäß zugeordneten einfach transitiven Operationen der Vektorräume $V_{\mathbb{A}}$ und $V_{\mathbb{B}}$ Eine *affine Abbildung* $F : \mathbb{A} \to \mathbb{B}$ ist eine (mengentheoretische) Abbildung, für die es eine lineare Abbildung $L_F : V_{\mathbb{A}} \to V_{\mathbb{B}}$ gibt, so dass für alle $A, A' \in \mathbb{A}$

$$L_F(A - A') = F(A) - F(A')$$

gilt.

1.1.7. Identifizierung von $\mathbb{A}$ mit $V_{\mathbb{A}}$. Nach der Wahl eines Punktes $O \in \mathbb{A}$ haben wir die Bijektion $\beta = \beta_O : V \to \mathbb{A}$, $v \mapsto v \dotplus O$. Bezüglich dieser Identifikation entspricht $0 \in V$ dem Punkt $O \in \mathbb{A}$.

Für eine gegebene affine Abbildung $F : \mathbb{A} \to \mathbb{A}$ sei L_F wie in 1.1.6, $O \in \mathbb{A}$ beliebig und $\widetilde{F} := \beta_O^{-1} \circ F \circ \beta_O : V \to V$. Dann gilt $\widetilde{F}(v) = L_F(v) + w$, wobei $w \in V$ dem Punkt $F(O)$ bzgl. der obigen Identifikation β_O entspricht, d.h., $w = F(O) - O$. Jede affine Abbildung (betrachtet als eine Abbildung $V \to V$) ist daher eine Verkettung einer linearen Abbildung und einer Translation.

Die Menge aller invertierbaren affinen Abbildungen, d.h., die Menge aller Affinitäten bilden eine Gruppe, die wir mit $\mathrm{Aff}(\mathbb{A})$ bezeichnen werden. Die Darstellung eines Elements aus $\mathrm{Aff}(\mathbb{A})$ als die Verkettung $T_w \circ L_F$ hängt von der Wahl der Identifizierung $\beta : V \to \mathbb{A}$ ab. Für $\beta_P^{-1} \circ F \circ \beta_P = T_v \circ L$ und $\beta_O^{-1} \circ F \circ \beta_O = T_w \circ L$ wird die Beziehung zwischen v und w in dem untenstehenden Diagramm beschrieben.

$$\begin{array}{ccc} V & \xrightarrow{T_v \circ L} & V \\ & \searrow^{\beta_P} \quad \swarrow_{\beta_P} & \\ T_{P-O} \downarrow & \mathbb{A} \xrightarrow{F} \mathbb{A} & \downarrow T_{P-O} \\ & \nearrow_{\beta_O} \quad \nwarrow^{\beta_O} & \\ V & \xrightarrow[T_w \circ L]{} & V \end{array} \qquad w = v + (P - O) - L(P - O)$$

Je nach Identifizierung bleibt zwar der lineare Anteil L invariant, der Translationsanteil hängt aber von L sowie von den Identifizierungsmittelpunkten P und O ab.

Definition 1.1.8. Es sei $\mathbb{A}$ ein n-dimensionaler Vektorraum. Die Punkte $A_0, A_1, \ldots, A_m \in \mathbb{A}$ befinden sich in *allgemeiner Lage*, falls die Vektoren $A_1 - A_0, \ldots, A_m - A_0$ linear unabhängig in $V_{\mathbb{A}}$ sind.

Es gibt genau einen k-dimensionalen affinen Unterraum $\mathbb{B} \subset A$, der die vorgegebenen $k + 1$ Punkte $B_0, \ldots, B_k$ in allgemeiner Lage enthält. Sind diese Punkte nicht in allgemeiner Lage, so gibt es unendlich viele k-dimensionale affine Unterräume, die diese Punkte enthalten.

Eine Vektorraumstruktur oder eine affine Struktur reicht nicht aus um Abstände messen zu können. Dazu benötigt man ein entsprechendes "Messgerät": eine Abstandsfunktion oder Metrik:

Definition 1.1.9. Eine Abbildung $d : V \times V \to [0,\infty) \subset \mathbb{R}$ heißt eine *Metrik* oder eine *Abstandsfunktion*, falls für alle $x, y, z \in V$ die folgenden Bedingungen erfüllt sind:
(M1) $d(x,y) = 0. \iff x = y$
(M2) (Symmetrie) $d(x,y) = d(y,x)$
(M3) (Dreiecksungleichung) $d(x,y) + d(y,z) \geq d(x,z)$

Für die Definition einer Abstandsfunktion benötigt man keine Vektorraumstruktur; man kann also in der obigen Definition statt V eine beliege Menge X verwenden. Eine Menge X zusammen mit einer Metrik d nennt man einen *metrischen Raum*.

Beispiele. Es sei $N := \{1,\dots,n\}$ oder $N = \mathbb{N}$.

(a) Es sei X eine beliebige Menge. Dann ist $d_\delta(x,y) := \begin{cases} 0 & \text{falls } x = y \\ 1 & \text{falls } x \neq y \end{cases}$ die sog. *diskrete* Metrik auf X.

(b) Abkürzend schreiben wir hier $N := \{1,\dots,n\}$ oder $N = \mathbb{N}$. Für jede reelle Zahl $p \in (0,\infty)$ ist die Menge der N-Tupeln (äquivalent: Die Menge aller Abbildungen $N \to \mathbb{R}$)

$$\ell^p(N) := \{(x(k))_{k\in N} : \sum_{k\in N} |x(k)|^p < \infty\} ,$$

versehen mit der komponentenweise Addition und Skalarmultiplikation, ein $\mathbb{R}$-Vektorraum. Für $p \in [1,\infty)$ macht $\|(x(k))\|_p := \left(\sum_{k\in N} |x(k)|^p\right)^{1/p}$ aus $\ell^p(N)$ einen normierten Raum und $d_p(x,y) := \|x - y\|_p$ die zugehörige Abstandsfunktion. Falls $N = \{1,\dots,n\}$, so gilt für alle $p \in [1,\infty)$: $\ell^p(N) = \mathbb{R}^n$.

(c) Besonders wichtig ist der Spezialfall $p = 2$. In diesem Fall $d(x,y) := d_2(x,y) = \sqrt{\sum_{j=1}^n (x_j - y_j)^2}$ wir von einem Skalarprodukt (vgl. 1.1.10) induziert, d.h., für

$$\langle\ ,\ \rangle : \ell^2(N) \times \ell^2(N) \to \mathbb{R}, \quad \langle (x(k)), (y(k)) \rangle := \sum_N x(k) \cdot y(k)$$

gilt $d(x,y) = \sqrt{\langle y - x\ ,\ y - x\rangle}$. (Die Summe auf der rechten Seite ist auch für unedliches N wohldefiniert.) Diese Abstandsfunktion nennt man *euklidisch*.

Die Länge einer Kurve $\gamma : [0,1] \to (V,d)$, wobei (V,d) ein metrischer Raum ist, läßt sich wie folgt berechnen:

$$\text{Länge}(\gamma) := \sup\{\sum_{j=0}^{k} d(\gamma(x_{j+1}), \gamma(x_j)) : 0 = x_0 \leq x_1 \leq \cdots \leq x_k \leq x_{k+1} = 1\} .$$

Allerdings für besonders komplizierte Kurven kann diese Größe unendlich sein. Man nennt eine Kurve γ d-rektifizierbar, falls das obige Supremum endlich ist. Falls $V = \mathbb{R}^n$, d die euklidische Abstandsfunktion und die Kurve γ stückweise differenzierbar ist, so gilt $\text{Länge}(\gamma) < \infty$.
Sind $A, B \subset V$ zwei beliebige Teilmengen eines metrischen Raumes (V,d), so definieren wir deren Abstand durch

$$d(A,B) := \inf\{d(P,Q) : P \in A,\ Q \in B\} .$$

I.A. gibt es keine Punkte $P_A \in A$ und $P_B \in B$ mit $d(A,B) = d(P_A, P_B)$. Existieren aber solche Punkte, so müssen sie nicht eindeutig bestimmt sein (der Fall zwei parallelen Geraden).

Um einen Winkel zwischen zwei Vektoren oder zwei sich schneidenden Geraden in V messen zu können, benötigt man i.A. mehr als eine bloße Abstandsfunktion:

Definition 1.1.10. (Skalarprodukt) Es sei V ein $\mathbb{R}$-Vektorraum. Ein Skalarprodukt auf V ist eine Abbildung $h : V \times V \to \mathbb{R}$ mit den folgenden Eigenschaften:
(SP1) h ist $\mathbb{R}$-bilinear und symmetrisch
(SP2) (positive Definitheit) Für alle $x \in V$ gilt $h(x,x) \geq 0$
(SP3) (keine Entartung) $h(x,x) = 0 \iff x = 0$

Ein (reeller) Vektorraum zusammen mit einem Skalarprodukt nennt man einen *euklidischen Raum*. Analog nennt man einen affinen Raum $\mathbb{A}$ euklidisch, falls der zugrunde liegende Vektorraum $V_{\mathbb{A}}$ mit einem Skalarprodukt ausgestattet ist. Wir schreiben oft $\langle x,y\rangle$ statt $h(x,y)$ und $\|v\|$ für $\sqrt{\langle v,v\rangle}$. Sind $M,N \subset V$ zwei Teilmengen mit $\langle m,n\rangle = 0$ für alle $m \in M, n \in N$ so sagen wir, dass M und N *orthogonal* zueinander sind. Ferner schreiben wir $M^{\perp} := \{v \in V : \langle v,m\rangle = 0 \ \forall m \in m\}$. Ist $W \subset V$ ein Untervektorraum (endlichdimensional) so gilt immer $V = W \oplus W^{\perp}$. Das Skalarprodukt definiert ferner eine Normfunktion $\|v\| := \sqrt{\langle v,v\rangle}$ und eine (euklidische) Abstandsfunktion $d_{\|\ \|}(v,w) := \|v - w\| = \sqrt{\langle w-v, w-v\rangle}$.

1.1.11. Orthogonale Komplemente in affinen Räumen. Ist $\mathbb{A}$ ein affiner Raum, so dass der zugehörige Vektorraum $V_{\mathbb{A}}$ ($+ : V_{\mathbb{A}} \times \mathbb{A} \to \mathbb{A}$ einfach transitiv) euklidisch ist, so kann man das Skalarprodukt auf $V_{\mathbb{A}}$ dazu nutzen um für jeden affinen Unterraum $\mathbb{B} \subset \mathbb{A}$ und einen ausgewählten Punkt $S \in B$ einen komplementären orthogonalen affinen Unterraum $\mathbb{E}$ durch S angeben: $\mathbb{E} = W^{\perp} + S$ wobei $\mathbb{E} = W + S$ und $W \subset V_{\mathbb{A}}$ der Untervektorraum ist, deren Bahn durch S den affinen Unterraum $\mathbb{B}$ definiert.

Definition 1.1.12. Es seien $v,w \in (V, \langle\ ,\ \rangle)$ zwei Vektoren. Der Winkel zwischen v und w, in Zeichen $\varphi := \angle(v,w) = \angle(w,v)$, wird durch die Formel

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

Sind $A,B,C \in V$ beliebige Punkte und $\overline{AB}$ und $\overline{AC}$ die entsprechenden Strecken, so schreiben wir für den Winkel zwischen $\overline{AB}$ und $\overline{AC}$ einfach $\angle BAC$. Definitionsgemäß ist dieser Winkel gleich $\angle((B-A),(C-A))$.

Skalarprodukt und seine Eigenschaften. Es sei $(V, \langle\ ,\ \rangle)$ eine euklidischer Vektorraum. Wir geben einigte fundamentale Eigenschaften des Skalarprodukts an:

1.1.13. Cauchy-Schwartzsche Ungleichung:

$$|\langle v,w\rangle| \leq \|v\|\cdot\|w\| \qquad \text{für alle } v,w \in \mathbb{H}.$$

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

1.1.14. Pythagoreische Gleichung. Es seien $v,w \in V$. Interpretiert man $\|v\|$, $\|w\|$ und $\|v+w\|$ als die Längen der Seiten des Dreiecks mit den Eckpunkten $0, v$ und $v+w$, so folgt unter der Voraussetzung, dass v,w orthogonal sind, d.h., $\langle v,w\rangle = 0$,

$$\|v+w\|^2 = \langle v+w, v+w\rangle = \langle v,v\rangle + 2\langle v,w\rangle + \langle w,w\rangle = \|v\|^2 + \|w\|^2 .$$

Dies ist die klassische Pythagoreische Identität für rechtwinklige Dreiecke. Es gibt die folgende Verallgemeinerung dieser Aussage: Es sei $e_1,..,e_N$ eine orthonormale Familie von Vektoren aus V, d.h., für alle $1 \leq j,k \leq N$ gilt: $\langle e_j, e_k\rangle = \delta_{jk}$ (Kronecker-Delta). Dann gilt für einen beliebigen Vektor $v \in V$:

$$\|v\|^2 = \sum_{k=1}^{N} |\langle v, e_k\rangle|^2 + \Big\|v - \sum_{k=1}^{N} \langle e_k, v\rangle\, e_k\Big\|^2 . \tag{1.1.15}$$

In dem Abschnitt über Projektionen geben wir eine Interpretation beider Summanden auf der rechten Seite. Insbesondere folgt daraus das folgende

Korollar 1.1.16. Besselsche Ungleichung. *Unter den obigen Voraussetzungen gilt*

$$\|v\|^2 \geq \sum_{k=1}^{N} |\langle v, e_k\rangle|^2 = \| \sum_{k=1}^{N} |\langle v, e_k\rangle e_k \|^2.$$

Eine charakterisierende Eigenschaft des Skalarprodukt ist die
1.1.17. Parallelogrammgleichung. Für alle Vektoren $v, w \in V$ gilt

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

Projektionen. Eine (Parallel-)Projektion eines affinen Raumes $\mathbb{A}$ ist eine affine Abbildung $\pi : \mathbb{A} \to \mathbb{A}$ mit $\pi \circ \pi = \pi$.

Der affiner Unterraum $\mathbb{B} := \pi(\mathbb{A}) = \text{Bild}(\pi)$ bleibt punktweise invariant unter dieser Abbildung, d.h., $\pi(X) = X$ für alle $X \in \mathbb{B}$. Nach Wahl eines Punktes $O \in \mathbb{B}$ und der Identifikation $\beta_O : V \cong \mathbb{A}$ (wie in 1.1.7) ist dann entsprechend $\pi : V \to V$ eine lineare Abbildung (ohne einen Translationsanteil) und es gilt $V = \ker\pi \oplus \text{Bild}(\pi)$. Umgekehrt, zu jeder Zerlegung von V in die direkte Summe $W_1 \oplus W_2$ ist die Abbildung

$$W_1 \oplus W_2 \to W_1 \oplus W_2, \qquad w_1 + w_2 \mapsto w_2 \tag{1.1.18}$$

eine Projektion. Ist $\langle\ ,\ \rangle$ ein Skalarprodukt auf V und $\ker(\pi) \perp \text{Bild}(\pi)$, so nennt man die Projektion π *orthogonal* [oder *normal*]. Es sei jetzt $W \subset V$ eine Untervektorraum des euklidischen Raumes V. Dann gilt $V = W \oplus W^\perp$ und die orthogonale Projektion auf W ist durch die Abbildung $v = w_1 + w_2 \to w_1$ gegeben, wobei $v = w_1 + w_2$ ist die eindeutig bestimmte Zerlegung von $v \in V$ bzgl. $V = W \oplus W^\perp$ (d.h., $w_1 \in W$ und $w_2 \in W^\perp$). Es sei jetzt $e_1, \ldots, e_k$ eine orthonormale Basis von W. Dann gilt für die orthogonale Projektion π auf W:

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

Damit läßt sich die Pythagoreische Gleichung 1.1.15 folgendermaßen umformulieren:

$$\|v\|^2 = \|\pi(v)\|^2 + \|v - \pi(v)\|^2$$

wobei π die orthogonale Projektion von V auf den durch die Vektoren $e_1, \ldots, e_N$ erzeugten Unterraum W ist.

Die nächste Aussage beschreibt unter welchen Voraussetzungen sich der Abstand $d(P, M)$ eines Punktes P und einer Teilmenge $M \subset V$ in der Form $d(P, Q),\ Q \in M$ realisieren läßt.
Zur Erinnerung: Eine Teilmenge $C \subset V$ des Vektorraumes V heißt *konvex*, falls für je zwei Punkte $v, w \in C$ auch die Verbindungsstrecke $\overline{vw} = \{tv + (1-t)w, t \in [0,1]\}$ in C enthalten ist. Die kleineste konvexe Teilmenge, die die Teilmenge $M \subset V$ enthält, heißt die *konvexe Hülle* von M und wird mit $\text{conv}(M)$ bezeichnet.

Proposition 1.1.19. *Es sei V ein euklidischer Raum, $C \subset V$ eine beliebige abgeschlossene konvexe Teilmenge und $z \in V$. Dann gibt es genau einen Punkt $x_z \in C$ mit $d(z, C) = d(z, x_z)$.*

Bemerkung: Dieser Satz bleibt richtig auch in dem unendlichdimensionalen Fall, falls man noch voraussetzt, dass jede Cauchyfolge bzgl $d_{\|\ \|}$ in V konvergiert. Diese Eigenschaft ist automatisch in dem endlichdimensionalen Fall gegeben.

Beweis: Da Translationen abstandserhaltende Abbildungen sind, können wir nach Anwendung von T_{-z} o.B.d.A $z = 0$ annehmen. Dann gilt $d(y, z) = d(y, 0) = \|y\|$ für ale $y \in C$. Es sei nun $\rho := d(C, 0)$ und $(x_n)_{n\in\mathbb{N}}$ ein Folge aus C mit $\lim_{n\to\infty} d(x_n, 0) = \lim_{n\to\infty} \|x_n\| = \rho$. Wir zeigen nun, dass (x_n) ein Cauchy-Folge ist und damit gegen ein $x_z \in C$ konvergiert. (C ist abgeschlossen!). 1.1.17 impliziert nämlich

$$0 \leq \left\| \frac{x_n - x_m}{2} \right\|^2 = \frac{\|x_n\|^2}{2} + \frac{\|x_m\|^2}{2} - \Big\| \underbrace{\frac{x_n + x_m}{2}}_{\in C} \Big\|^2 \longrightarrow \frac{\rho^2}{2} + \frac{\rho^2}{2} - \lim_{m,n\to\infty} \left\| \frac{x_n + x_m}{2} \right\|^2 \leq 0$$

womit bewiesen ist, dass (x_n) eine Cauchy-Folge ist. Da V vollständig ist, konvergiert sie in V gegen x_z. Es gilt dann auch $d(z, x_z) = \rho$ (wäre $d(z, x_z) = \rho + \varepsilon$ für ein $\varepsilon > 0$, so gelte für hinreichend große n $d(z, x_n) < \rho + \varepsilon/3$ sowie $d(x_n, x_z) < \varepsilon/3$; die Dreiecksungleichung impliziert dann $d(z, x_z) \leq d(z, x_n) + d(x_n, x_z) < \rho + \frac{2}{3}\varepsilon$ im Widerspruch zu unser Annahme).Damit ist die Existenz bewiesen. Die Eindeutigkeit von x_z folgt ebenfalls aus der Parallelogrammgleichung: Sind $x, y \in C$ zwei Elemente mit $\rho := d(x, z) = d(y, z) = d(C, z)$ ($z = 0$), so haben wir

$$0 \leq \left\| \frac{x - y}{2} \right\|^2 = \frac{\|x\|^2}{2} + \frac{\|y\|^2}{2} - \underbrace{\left\| \frac{x + y}{2} \right\|^2}_{\geq\rho} \leq 0 \qquad \text{und damit } x = y\ .$$

□

Die obige Proposition steht im engen Zusammenhang mit orthogonalen Projektionen auf (abgeschlossene) Untervektorräume W. Setzt man $C = W \subset V$ (ein UVR ist eine konvexe Teilmenge), so gilt für die orthogonale Projektion π_W auf W:

$$\pi_W(z) = x_z\ ,$$

wobei $x_z \in W$ der eindeutig bestimmte Punkt mit dem kleinsten Abstand zu z ist (wie in 1.1.19).

Man kann jetzt die Definition 1.1.12 verallgemeinern und den Winkel zwischen beliebigen positivdimensionalen affinen Unterräumen $\mathbb{E}, \mathbb{E}' \subset \mathbb{A}$, die mindestens einen gemeinsamen Punkt $S \in \mathbb{E} \cap \mathbb{E}'$ haben, definieren:

• Fall 1: für zwei affine Geraden $\ell = \mathbb{R}v + S, \ell' = \mathbb{R}v' + S$ d.h. $S \in \ell \cap \ell'$. Dann definieren wir den Winkel $\angle\ell, \ell'$ durch $\min\{\angle(v, v'), \angle(v, -v')\}$.

• Fall 2: Gilt $\mathbb{E} \cap \mathbb{E}' = \{S\}$, so definiert man

$$\angle\mathbb{E}, \mathbb{E}' := \min\{\angle\ell, \ell' : \ell \subseteq \mathbb{E}, \ell' \subseteq \mathbb{E}' \text{ Geraden durch } S\}$$

• Allgemeiner Fall: Für $\mathbb{F} := \mathbb{E} \cap \mathbb{E}'$ wähle man ein beliebiges $S \in \mathbb{F}$ und $\mathbb{F}^\perp$ sei das orthogonale affine Komplement durch S, vgl. 1.1.11. Dann definieren wir

$$\angle\mathbb{E}, \mathbb{E}' := \angle\ \mathbb{E} \cap \mathbb{F}^\perp, \mathbb{E}' \cap \mathbb{F}^\perp$$

Man beachte, dass der Durchschnitt von den affinen Unterräumen $\mathbb{E} \cap \mathbb{F}^\perp$ und $\mathbb{E}' \cap \mathbb{F}^\perp$ genau $\{S\}$ ist.

Verwandt mit den Projektionen sind die Spiegelungsabbildungen: Ist $V = W_1 \oplus W_2$ so definiert man jetzt die Spiegelung an W_2 als die Abbildung

$$S : W_1 \oplus W_2 \longrightarrow W_1 \oplus W_2, \qquad v_1 + v_2 \longmapsto -v_1 + v_2\ .$$

Anders als bei einer Projektion (vgl. 1.1.18) ist jede Spiegelung eine invertierbare Abbildung. Ist eine solche Spiegelung S sogar orthogonal, d.h., $W_1 \perp W_2$ sowie $\dim W_1 = 1$ und $W_2 = w^\perp$ so gilt

$$S(v) = v - 2\frac{\langle v, w\rangle}{\langle w, w\rangle} w \qquad \forall\, v \in V\,.$$

1.2. Isometriegruppen

Es sei $\mathbb{A}$ ein euklidischer affiner Raum und (X, d) ein beliebiger metrischer Raum, z.B. $X = \mathbb{A}$ und $d = d_e$.

Definition 1.2.1.

(a) Mit $\mathrm{Aff}(\mathbb{A})$ bezeichnen wir die Menge aller Affinitäten $\mathbb{A} \to \mathbb{A}$, d.h., aller invertierbaren affinen Abbildungen.

(b) Mit $\mathrm{Isom}(\mathbb{A}, d_e) := \{F \in \mathrm{Aff}(\mathbb{A}) : d_e(F(P), F(Q)) = d_e(P, Q)\ \forall\, P, Q \in \mathbb{A}\}$ bezeichnen wir die Menge aller Isometrien des euklidischen (affinen) Raumes $\mathbb{A}$.

(c) Mit $\mathbf{B}(X, d) := \{F : X \to X : F \text{ surjektiv}, d(F(P), F(Q)) = d(P, Q)\ \forall\, P, Q \in \mathbb{A}\}$ bezeichnen wir die Menge aller Bewegungen des metrischen Raumes X.

(d) Mit $\mathbf{S}(X, d) := \{F : X \to X : F \text{ bijektiv}, \forall\, P_1, P_2, Q_1, Q_2 \in A \text{ mit } d(P_1, Q_1) = d(P_2, Q_2) \implies d(F(P_1), F(Q_1)) = d(F(P_2), F(Q_2))\}$ bezeichnen wir die Menge aller Ähnlichkeiten (oder Similaritäten) des metrischen Raumes X.

(e) Mit $\mathbf{T}(\mathbb{A}) = \{T_v : v \in V_A\} \cong (V_A, +)$ bezeichnen wir die (kommutative) Gruppe aller Translationen von A. Sie ist ein Normalteiler in $\mathrm{Isom}(\mathbb{A}, d_e)$, d.h., $\psi \circ \mathbf{T}(\mathbb{A}) \circ \psi^{-1} = \mathbf{T}(\mathbb{A})\ \forall \psi \in \mathrm{Isom}(\mathbb{A}, d_e)$.

Zusammen mit der Verkettung von Abbildungen als Verknüpfung sind alle 5 obigen Mengen Gruppen. Nach Wahl einer Identifizierung $\beta : V_{\mathbb{A}} \to \mathbb{A}$ gilt dann

$$\begin{aligned} \mathrm{Aff}(\mathbb{A}) &= \{T_v \circ L : v \in V,\ L \in \mathrm{GL}(V)\} \\ \mathrm{Isom}(\mathbb{A}, d_e) &= \{T_v \circ R : v \in V,\ R \in \mathrm{O}(V, \langle\ ,\ \rangle)\} \end{aligned} \tag{1.2.2}$$

Diese Produktdarstellung ist eindeutig, gilt also $T_v \circ R = T_w \circ S$ in $\mathrm{Aff}(\mathbb{A})$ oder in $\mathrm{Isom}(\mathbb{A}, d_e)$ (mit $T_v, T_w \in \mathbf{T}$ und $R, S \in \mathrm{GL}(V_{\mathbb{A}})$ oder $\mathrm{O}(V, \langle\ ,\ \rangle)$), so folgt $v = w$ und $R = S$. Ferner gilt

$$(T_v \circ R) \circ (T_w \circ S) = T_v \circ R \circ T_w \circ R^{-1} \circ R \circ S = T_v \circ T_{R(w)} \circ (R \circ S) = T_{v+R(w)} \circ (R \circ S)$$

Dabei schreiben wir

$$\mathrm{O}(V, \langle\ ,\ \rangle) := \{R \in \mathrm{GL}(V) : \langle R(v), R(w)\rangle = \langle v, w\rangle\ \forall\, v, w \in V\} \overset{!}{\cong} \mathrm{O}(n) = \{A \in \mathbb{R}^{n\times n} : A \cdot A^T = E_n\}$$

für die Gruppe der linearen orthogonalen Transformationen (bzgl des gegebenen Skalarproduktes $\langle\ ,\ \rangle$). Der Isomorphismus auf der rechten Seite gilt in dem Fall $\dim V = n$. Ist $\mathbb{A}$ ein affiner Raum, so schreiben wir O_P für $\beta_P \circ \mathrm{O}(\mathrm{V}_{\mathbb{A}}, \langle\ ,\ \rangle) \circ \beta_P^{-1}$ (welche eine zu $\mathrm{O}(n)$ isomorphe Gruppe ist). Es gilt

$$\mathrm{O}_P = \{F \in \mathrm{Isom}(\mathbb{A}, d_e) : F(P) = P\}\,.$$

Die Elemente aus O_P nennt man *Punktisometrien* mit Fixpunkt P. Diese Menge ist eine Untergruppe von $\mathrm{Isom}(\mathbb{A}, d_e)$ und es gilt $\mathrm{O}_Q = T_{Q-P} \circ \mathrm{O}_P \circ T_{Q-P}^{-1}$. Für jedes $P \in \mathbb{A}$ ist die Abbildung

$$\mathbf{T}(\mathbb{A}) \times \mathrm{O}_P \longrightarrow \mathrm{Isom}(\mathbb{A}, d_e), \qquad (T_v, R) \longmapsto T_v \circ R$$

eine Bijektion. Man kann auf der Produkt*menge* $\mathbf{T}(\mathbb{A}) \times \mathrm{O}_P$ eine Gruppenstruktur definieren (vgl 1.2.6), so dass die obige Abbildung zu einem Gruppenisomorphismus wird. (Diese Gruppenstruktur ist jedoch nicht die Produktstruktur.)

Jede Bewegung $F : X \to X$ eines metrischen Raumes ist automatisch injektiv, d.h., eine Bijektion: Falls $x, y \in X$, $x \neq y$ so auch $d(F(x), F(y)) = d(x, y) \neq 0$ und damit $F(x) \neq F(y)$.
In dem Fall $(X, d) = (\mathbb{A}, d_e)$ habe wir die Inklusionen

$$\mathrm{Isom}(\mathbb{A}, d_e) \subset \mathbf{B}(\mathbb{A}, d_e) \subset S(\mathbb{A}, d_e) \ .$$

Überraschenderweise ist jede Bewegung eines euklidischen Raumes automatisch affin:

Theorem 1.2.3. *Es sei $(\mathbb{A}, d_e)$ ein euklidischer affiner Raum. Dann gilt für jedes $P \in \mathbb{A}$*

$$\mathrm{Isom}(\mathbb{A}, d_e) = \mathbf{B}(\mathbb{A}, d_e) \cong \{T_v \circ R : v \in V_{\mathbb{A}}, R \in \mathrm{O}_P\}$$

Beweis: Es sei $F \in \mathbf{B}(\mathbb{A}, d_e)$. Nach Wahl einer Identifizierung $\beta_P : V_{\mathbb{A}} \to \mathbb{A}$ betrachten wir F als eine Abbildung $V \to V$. ($V := V_{\mathbb{A}}$) Dann ist $\widetilde{F} := T_{-F(0)} \circ F$ ein Element in $\mathbf{B}$ mit $\widetilde{F}(0) = 0$. Dann gilt aber für beliebiges $x \in V$:

$$(\ddagger) \qquad \|x\| = d_e(0, x) = d_e(\widetilde{F}(0), \widetilde{F}(x)) = d_e(0, \widetilde{F}(x)) = \|F(x)\| \ .$$

Aus

$$\|\widetilde{F}(v) - \widetilde{F}(w)\|^2 = d_e(\widetilde{F}(v), \widetilde{F}(w))^2 = d_e(v, w)^2 = \|v - w\|^2$$

und $(\ddagger)$ folgert man

$$(*) \qquad \langle \widetilde{F}(v), \widetilde{F}(w) \rangle = \langle v, w \rangle \qquad \forall\, v, w \in V$$

(Wir können noch nicht daraus schließen, dass $\widetilde{F}$ eine orthogonale Transformation ist, da wir (noch) nicht wissen, ob $\widetilde{F}$ linear ist.) Es sei jetzt $v_1, \ldots, v_m$ eine beliebige orthonormale Basis von V. Dann impliziert $(*)$, dass $F(v_1), \ldots, F(v_m)$ auch eine orthonormale Basis von V ist. Es gibt daher ein (lineares) $R \in \mathrm{O}(V, \langle\ ,\ \rangle)$ mit $R(v_j) = F(v_j))$ für alle $j = 1, \ldots, m$. Es sei jetzt

$$G := R^{-1} \circ \widetilde{F} = R \circ T_{-F(0)} \circ F \ .$$

Dann gilt $G \in \mathbf{B}(\mathbb{A})$, $G(0) = 0$ und $G(v_j) = v_j$ für alle $j = 1, \ldots, m$.
Beh.: $G = \mathrm{Id}$.
Beweis der Beh.: Wir zeigen, dass $G(x) = x$ für jedes $x \in V$ gilt. Dazu betrachte man für jedes $j \in \{1, \ldots, m\}$

$$\begin{aligned} \langle G(x) - x, v_j \rangle &= \langle G(x), v_j \rangle - \langle x, v_j \rangle = \\ &\overset{(*)}{=} \langle G^{-1} \circ G(x), G^{-1}(v_j) \rangle - \langle x, v_j \rangle = \\ &= \langle x, v_j \rangle - \langle x, v_j \rangle = 0 \end{aligned}$$

Wir haben also $\langle G(x) - x, y \rangle = 0$ für jedes $y \in V$ und das impliziert $G(x) = x$ für alle $x \in V$ und die Behauptung ist beweisen.
Zusammenfassend gilt nun $G = \mathrm{Id} = R^{-1} \circ T_{-F(0)} \circ F$ oder äquivalent: $F = T_{F(0)} \circ R \in \mathrm{Isom}(\mathbb{A}, d_e)$.
□

Ein kleiner Exkurs über Gruppen. Wir erinnern an einige Grundbegriffe der Gruppentheorie. Es sei $(G, \cdot)$ eine Gruppe,

$$\mathrm{Aut}(G) = \{\Phi : G \to G : \psi \text{ bijektiv}, \Phi(g \cdot h) = \Phi(g) \cdot \Phi(h)\ \forall g, h \in G\}$$

die Automorphismengruppe von G und $H < G$ eine Untergruppe. Für ein $x \in G$ ist $xHx^{-1} = \{x \cdot h \cdot x^{-1} : h \in H\}$ zwar wieder eine Untergruppe von G aber i.A. $xHx^{-1} \neq H$. Gilt $xHx^{-1} = H$ für alle $x \in G$, so heißt H ein Normalteiler in G und wir schreiben $H \lhd G$ dafür. Für eine beliebige Untergruppe $H < G$ sei

$$N_G(H) := \{x \in G : xHx^{-1} = H\}$$

der *Normalisator* von H in G. Es ist eine Untergruppe von G und es gilt $N_G(H) = G$ genau dann wenn H ein Normalteiler in G ist. Zwei Elemente $g, h \in G$ heißen *konjugiert*, falls es ein $x \in G$ mit $h = x \cdot g \cdot x^{-1}$ gibt. Analog nennt man zwei Untergruppe $H_1, H_2 < G$ *konjugiert*, falls es ein $x \in G$ gibt mit $H_2 = xH_1x^{-1}$. "Konjugiert zu sein" definiert eine Äquivalenzrelation auf G wie auch auf der Menge aller Untergruppen von G, und die entsprechende Äquivalenzklasse eines Elements $g \in G$ bezeichnen wir mit

$$C\ell_G(g) = C\ell(g) = \{x \cdot g \cdot x^{-1} : x \in G\} .$$

Die Konjugationsklassen von Untergruppen tauchen in Zusammenhang mit der Aufteilung der G-Bahnen einer Operation in geeignete Klassen.
Für jede Untergruppe $H < G$ definiert die Relation $x \sim_H y \overset{\text{Def}}{\iff} x^{-1} \cdot y \in H$ auf G ebenfalls eine Äquivalenzrelation. Die Äquivalenzklassen sind dann genau die Linksnebenklassen xH, wobei $x \in G$. Die Menge aller Äquivalenzklassen bezeichnet man mit G/H und nennt den *Quotientenraum* von G nach H. Solche Quotientenräume treten ganz natürlich als Bahnen von Gruppenwirkungen auf:

Definition 1.2.4. Es sei $\bullet : G \times X \to X$ eine Gruppenoperation auf der Menge X. Für ein $x \in X$ nennt man

$$G_x := \{g \in G : g \bullet x = x\}$$

die *Isotropieuntergruppe* (oder den *Stabilisator*) von x in G. Gilt für einen Punkt $y \in X$ $G_y = G$, so heißt y ein *Fixpunkt* der gegebenen Operation. Noch allgemeiner, sei $M \subset X$ eine beliebige Teilmenge. Dann ist die Menge

$$G_M := \{g \in G : g \bullet M = M\}$$

eine Untergruppe von G, der sog. Stabilisator von M.

Für jede Orbit $G(x) \subset X$ ist die Abbildung

$$G/G_x \to G(x), \qquad gG_x \mapsto g \bullet x$$

eine Bijektion. Damit können wir die Quotienten G/G_x mit den entsprechenden Orbiten in X identifizieren. Im Rahmen dieser Vorlesung werden wir uns vorwiegend mit der Operation $\mathbf{B} \times \mathbb{A} \to \mathbb{A}$ der Bewegungsgruppe $\mathbf{B} = \mathbf{B}(\mathbb{A}, d_e)$ sowie der diversen Untergruppen $G \subset \mathbf{B}$ auf dem affinen Raum $X = \mathbb{A}$ befassen.

Beispiele: Die Operation $\mathrm{GL}(V) \times V \to V$, $(L, v) \mapsto L(v)$ hat genau einen Fixpunkt: 0. Die Operation der affinen Gruppe $\mathrm{Aff}(\mathbb{A}) \times \mathbb{A} \to \mathbb{A}$, $(\Psi, P) \mapsto \Psi(P)$ ist transitiv und hat keine Fixpunkte. Die Isotropiegruppe $\mathrm{Aff}(\mathbb{A})_Q$ eines Punktes $Q \in \mathbb{A}$ ist isomorph zu der vollen linearen Gruppe $\mathrm{GL}(V_{\mathbb{A}})$. Für je zwei verschiedene Punkte P, Q sind $\mathrm{Aff}(\mathbb{A})_Q$ und $\mathrm{Aff}(\mathbb{A})_P$ zwei verschiedene, zueinander konjugierte Untergruppen von $\mathrm{Aff}(\mathbb{A})$.

Es sei jetzt N ein Normalteiler von G. Der Quotient G/N zusammen mit der Verknüpfung $(xN, yN) \mapsto (x \cdot y)N$ ist eine Gruppe, die sog. *Faktorgruppe* (nach N). (Die obige Verknüpfung ist nicht wohldefiniert, falls N bloß eine Untergruppe, nicht aber ein Normalteiler ist.) Beispiele für Faktoregruppen: $\mathbb{Z}_n = (\mathbb{Z}, +)/n\mathbb{Z}$ oder $\mathrm{GL}(n, \mathbb{R}) = \mathrm{Aff}(\mathbb{R}^n)/\mathbf{T}$.

Jeder Normalteiler $N \lhd G$ erlaubt uns die Struktur von G auf die (i.A. einfacheren) Gruppen N und G/N zurückzuführen. (I.A. jedoch gibt es nichtisomorphe Gruppen G_j mit $N_1 \cong N_2$ und $G_1/N_1 \cong$

G_2/N_2.) Eine Gruppe G, die keine Normalteiler außer $\{e\}$ und G hat, sich also nicht in echt kleinere Gruppen "zerlegen" läßt, nennt man eine *einfache* Gruppe. Die Inklusion $N \subset G$ und die Projektion $G \to G/N$ fasst man oft zusammen zu der folgenden (kurzen) Sequenz von Abbildungen:

$$N \xrightarrow{\alpha} G \xrightarrow{\beta} G/N \ .$$

Gibt es einen Homomorphismus $\gamma : G/N \to G$ mit $\beta \circ \gamma = \mathrm{Id}_{G/N}$, so ist G ein semidirektes Produkt $G = N \rtimes_\psi (G/N)$. Ein solcher Homomorphismus γ existiert allerdings nicht immer.

Der Normalisator $N = N_G(H)$ operiert auf H durch Gruppenautomorphismen:

$$\diamond : N_G(H) \times H \to H, \qquad (n,h) \longmapsto n \cdot h \cdot n^{-1} \ , \tag{1.2.5}$$

die wir als die *Konjugationsoperation* von $N(H)$ auf H nennen. So z.B. sind die Bahnen bzgl. der Konjugationsoperation $\diamond : G \times G \to G$ exact die Konjugationsklassen $C\ell(x)$, $x \in X$. Die Operation 1.2.5 induziert den Gruppenhomomorphismus $\psi : N \to \mathrm{Aut}(H)$, $\psi(n)(x) = n \cdot x \cdot n^{-1}$. Solche Gruppenhomomorphismen spielen eine fundamentale Rolle bei der Verallgemeinerung des direkten Gruppenproduktes.

Definition 1.2.6. Es seien $(H,\cdot),(N,\bullet)$ zwei Gruppen und $\psi : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Die Verknüpfung

$$(N \times H) \ \times \ (N \times H) \to N \times H, \qquad ((n_1,h_1),(n_2,h_2)) \longmapsto (n_1 \bullet \psi(h_1)(n_2) \ , \ h_1 \cdot h_2)$$

definiert auf $N \times H$ eine Gruppenstruktur. Das Produkt $N \times G$ mit dieser Verknüpfung nennt man das *semidirekte* Produkt von N und H. Wir schreiben $N \rtimes_\psi H$ für diese Gruppe. Die beiden Gruppe N und N können als Untergruppen von $N \rtimes_\psi H$ betrachtet werden: Die Abbildungen $\alpha : N \to N \rtimes_\psi H$, $n \mapsto (n, e_H)$, $\quad \beta : N \rtimes_\psi H \to H$, $(n,h) \mapsto h$ und $\gamma : H \to N \rtimes_\psi H$, $h \mapsto (e_N, h)$ sind Gruppenhomomorphismen (α, γ injektiv, β surjektiv, $\mathrm{Bild}(\alpha) = \ker(\beta)$)

$$N \xrightarrow{\alpha} N \rtimes_\psi H \underset{\gamma}{\overset{\beta}{\rightleftarrows}} H$$

Damit wird N mit $\alpha(N)$ sowie H mit $\gamma(H)$ identifiziert. $\alpha(N)$ und $\gamma(H)$ sind Untergruppen von $N \rtimes_\psi H$ ($\alpha(N)$ sogar ein Normalteiler) und es gilt $\alpha(H) \cap \gamma(N) = \{e\}$. Das semidirekte Produkt kann als eine Verallgemeinerung des gewöhnlichen Gruppenproduktes angesehen werden: Für die triviale Abbildung $\psi : H \to \{\mathrm{Id}\} \subset \mathrm{Aut}(N)$ gilt $N \rtimes_\psi H = N \times H$.

Lemma 1.2.7. *Es sei G eine Gruppe und $H, N < G$ zwei Untergruppen. Falls*
(i) N eine Normalteiler ist,
(ii) $NH = \{n \cdot h : n \in N, h \in H\} = G$ und
(iii) $N \cap H = \{e\}$ gilt,
so gibt es einen Homomorphismus $\psi : H \to \mathrm{Aut}(N)$, so dass das entsprechende semidirekte Produkt $N \rtimes_\psi H$ isomorph zu G ist.

1.2.8. Beispiel. Es sei $(V, \langle\ ,\ \rangle)$ ein euklidischer Vektorraum, $\mathbf{T}(V) \subset \mathbf{B}(V, d_e)$ die Untergruppe aller Translationen und $\mathrm{O}(V, \langle\ ,\ \rangle) = \mathrm{O}_0$ die orthogonale Gruppe. Es sei $\psi : \mathrm{O}_0 \to \mathrm{Aut}(\mathbf{T}(V)) = \mathrm{Aut}(V,+)$ die Abbildung $\psi(R) = R$ (d.h., $\psi(R)(T_v) = T_{R(v)}$). Das semidirekte Produkt $\mathbf{T}(V) \rtimes_\psi \mathrm{O}_0$ ist isomorph zu $\mathbf{B}(V, d_e)$ vermöge des Isomorphismus

$$\mathbf{T}(V) \rtimes_\psi \mathrm{O}_0 \longrightarrow \mathbf{B}(V, d_e), \quad (T_v, R) \longmapsto T_v \circ R$$

Ist $M \subset G$ eine Teilmenge einer Gruppe $(G, \cdot)$, so bezeichen wir mit $\langle M \rangle$ die kleinste Untergruppe von G, die alle Elemente von M enthält. $\langle M \rangle$ ist dann der Durschnitt aller Untergruppen $H_j \subset G$, die M enthalten. M heißt ein *Erzeugendensystem* der Untergruppe $\langle M \rangle$. I.A. gibt es verschiedene Erzeugendensysteme für dieselbe Untergruppe H. Jede Untergruppe hat ein Erzeugendensystem, z.B. sich selbst. Jede Untergruppe $H < G$ hat dann auch ein minimales Erzeugendensystem $\mathcal{M}$, d.h., $H = \langle \mathcal{M} \rangle$ aber $H \supsetneq \langle \mathcal{M} \smallsetminus \{z\} \rangle$ für jedes $z \in \mathcal{M}$. Je zwei minimale Erzeugendensysteme einer Gruppe müssen nicht einmal die gleiche Anzahl der Elementen haben.
Gibt es ein Erzegendensystem einer Gruppe G, das aus einem Element besteht, d.h.,

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = G,$$

so nennen wir G die von g erzeugte *zyklische* Gruppe. Für ein $x \in G$ nennt man $|\langle x \rangle|$ die *Ordnung von* x. Hierbei ist $g^0 := e$ und $g^{-k} := (g^k)^{-1} = (g^{-1})^k$ für alle $k \in \mathbb{N}$.

1.2.9. Beispiele.
• $(\mathbb{Z}, +)$ ist eine unendliche zyklische Gruppe mit $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
• $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ist eine endliche zyklische Gruppe mit $\mathbb{Z}_n = \langle \underline{1} \rangle = \langle \underline{n-1} \rangle$. Hier schreiben wir $\underline{k}$ für die Nebenklasse $k + \mathbb{Z}$.

Lemma 1.2.10. *Ist H eine zyklische Gruppe, so gilt $H \cong \mathbb{Z}$ oder $H \cong \mathbb{Z}_n$ für ein $n \in \mathbb{N}$.*

Bewegungsgruppen für kleine n. Falls $\dim \mathbb{A} = \dim V_{\mathbb{A}} = 1$ und $P \in \mathbb{A}$, so gilt $\mathrm{O}_P = \{\mathrm{Id}, s_P\}$ wobei $s_P(Q) = 2(P - Q) \dotplus Q$ die Punktspiegelung am $P \in \mathbb{A}$ bezeichnet. Ein Element von $\mathbf{B}(V) = \mathbf{T}(V) \rtimes_\psi \mathrm{O}_P$ ist entweder eine Translationen T_a oder eine Spiegelung $S_Q = T_b \circ s_P$ an einem Punkt $Q \in \mathbb{A}$: $S_Q(X) = 2(Q - X) \dotplus Q$.

Falls $\dim \mathbb{A} = \dim V_{\mathbb{A}} = 2$, so führen wie die folgenden Transformationen auf $\mathbb{A} \cong V$ ein:
Orientierungserhaltende Transformationen:
(a) *Drehungen* $D_\theta(P) : \mathbb{A} \to \mathbb{A}$ um den Punkt P gegen den Uhrzeigersinn um den Winkel $\theta \in [0, 2\pi)$. Nach Wahl einer orthonormalen Basis in $V_{\mathbb{A}}$ und der Identifizierung $\beta_P : V \to \mathbb{A}$ kann D_θ durch die Matrix

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

beschrieben. Diese Matrix beschreibt auch die (lineare) Drehung um den Winkel θ in $\mathbb{R}^2$ um den Nullpunkt $P = 0$.
(b) *Translationen* T_v, $v \in V_{\mathbb{A}} \smallsetminus \{0\}$.

Orientierungsumkehrende Transformationen: Es sei $\ell \subset \mathbb{A}$ eine beliebige affine Gerade.
(c) *Spiegelungen* $S_\ell : \mathbb{A} \to \mathbb{A}$ an ℓ. Nach Wahl einer orthonormalen Basis v_1, v_2 von $V_{\mathbb{A}}$ und der Identifizierung $\beta_P : V \to \mathbb{A}$ mit $P \in \ell$ wird S_ℓ durch die Matrix

$$\begin{pmatrix} \cos 2\beta & \sin 2\beta \\ \sin 2\beta & -\cos 2\beta \end{pmatrix}$$

beschrieben, wobei β der Winkel zwischen ℓ und der Koordinatenachse $\mathbb{R}v_1 \dotplus P$ ist.
(d) *Gleitspiegelungen* $T_v \circ S_\ell$ mit $v \in V_{\mathbb{A}} \smallsetminus \{0\}$, so dass $T_v(\ell) = \ell$ gilt. Die beschreibende Matrix und der Translationsvektor lauten (unter den gleichen Voraussetzungen wie bei den Spiegelungen):

$$\begin{pmatrix} \cos 2\beta & -\sin 2\beta \\ \sin 2\beta & \cos 2\beta \end{pmatrix} + c \begin{pmatrix} \cos\beta \\ \sin\beta \end{pmatrix} \qquad c \neq 0\,.$$

Diese Schreibweise beschreibt die Abbildung $\mathbb{R}^2 \to \mathbb{R}^2$, $\binom{x_1}{x_2} \longmapsto \left(\begin{smallmatrix} \cos 2\beta & -\sin 2\beta \\ \sin 2\beta & \cos 2\beta \end{smallmatrix}\right)\binom{x_1}{x_2} + c\binom{\cos\beta}{\sin\beta}$.

Lemma 1.2.11. *Es sei $\mathbb{A}$ ein 2-dimensionaler affiner euklidischer Raum und $R \in \mathbf{B}(\mathbb{A}, d_e)$. Dann ist R genau eine von den vier oben definierten Transformationen* (a)-(d).

1.3. Endliche und diskrete Gruppen

Es sei $(G, \cdot)$ eine endliche Gruppe. Wir bezeichnen mit $|M|$ die Anzahl der Elemente einer endlichen Menge M. Die Anzahl $|G|$ nennt man auch die Ordnung der Gruppe G. Ist $H < G$ eine Untergruppe, so bezeichnet man mit $[G : H]$ die Anzahl der verschiedenen Linksnebenklassen xH, $x \in G$, d.h., $[G : H] = |G/H|$. teilt $|H|$ die Zahl $|G|$. Die Anzahl $|H|$ teilt dann die Ordnung von G: Das ist eine direkte Konsequenz aus der

Lagrange-Formel: $$|G| = |H| \cdot [G : H] \, .$$

Wir schreiben $\mathfrak{S}_n$ für die Permutationsgruppe von n Elementen und $\mathfrak{A}_n < \mathfrak{S}_n$ für die Untergruppe aller geraden Permutationen. Auch wenn auf dem ersten Blick die Permutationsgruppen recht speziell erscheinen, enthalten sie jede beliebige endliche Gruppe als eine Untergruppe. Es gilt nämlich der

Theorem von Cayley 1.3.1. *Jede endliche Gruppe G ist isomorph zu einer Untergruppe einer Permutationsgruppe $\mathfrak{S}_n$ für ein geeignetes $n \in \mathbb{N}$.*

Ein solcher Isomorphismus wird z.B. durch die Abbildung $G \to \mathfrak{S}_{|G|}$, $g \mapsto L^g$, wobei $L^g : G \to G$ die Linkstranslation $x \mapsto gx$ ist, gegeben.

Ist $G \times X \to X$ eine Gruppenoperation auf einer endlichen Menge X, so gilt $X = \bigcup_{\text{Bahnen}} G(x_j)$, (wobei $\bigcup$ für die disjunkte Vereinigung steht) und daher $|X| = \sum_{\text{Bahnen}} |G(x_j)|$. Angewendet auf die Konjugationsoperation $\diamond : G \times G \to G$ erhalten wir die

1.3.2. Klassengleichung. $$|G| = \sum_{\text{Konjugationsklassen}} |C\ell_G(x_j)| \, .$$

Wir kehren jetzt zurück zu Untergruppen der Bewegungsgruppe.

Fixpunktsatz 1.3.3. *Es sei $G \subset \mathbf{B}(\mathbb{A}, d_e)$ eine beliebige endliche Untergruppe. Die Operation $\cdot : G \times \mathbb{A} \to \mathbb{A}$, $(g, P) \mapsto g(P)$ hat mindestens einen Fixpunkt Q in $\mathbb{A}$.*

Beweis: Man wähle eine Identifizierung $\beta_P : V \to \mathbb{A}$ und betrachte die entsprechende Operation $G \times V \to V$. Es sei $x \in V$ beliebig. Man konstruiert den folgenden Kandidaten für einen Fixpunkt:

$$y := \frac{\sum_{g \in G} g \cdot x}{|G|} \, .$$

Beh.: Es gilt $G \cdot y = y$: Für jedes $h = T_a \circ R \in G \subset \mathbf{B}(V) = \mathbf{T}(V) \rtimes \mathrm{O}_0$ gilt nämlich

$$\begin{aligned} h \cdot y = (T_a \circ R) \cdot \frac{\sum_{g \in G} g \cdot x}{|G|} = T_a\Big(\frac{\sum_{g \in G} R(g \cdot x)}{|G|}\Big) = \frac{\sum_{g \in G} R(g \cdot x)}{|G|} + a = \\ = \frac{\sum_{g \in G} (R(g \cdot x) + a)}{|G|} = \frac{\sum_{g \in G} h \cdot (g \cdot x)}{|G|} = \\ = \frac{\sum_{g \in G} (h \cdot g) \cdot x}{|G|} = \frac{\sum_{g \in G} g \cdot x}{|G|} = y \end{aligned}$$

□

Wir können daher annehemen, dass eine endliche Untergruppe $G \subset \mathbf{B}$ in einer Gruppe der Punktisometrien $\mathrm{O}_Q \cong \mathrm{O}(n, \mathbb{R})$ enthalten ist.

Beispiele.
• Die Drehung $D_{2\pi/k} \in \mathrm{SO}(2, \mathbb{R})$ erzeugt die zyklische Untergruppe $\mathcal{C}_k = \langle D_{2\pi/k} \rangle$ mit $|\mathcal{C}_k| = k$.
• Es sei jetzt $S \in \mathrm{O}(2, \mathbb{R})$ eine beliebigen Spiegelung. Es gilt dann $S D_{2\pi/k} S = D_{2\pi/k}^{-1} = D_{-2\pi/k}$. Die von $D_{2\pi/k}$ und S erzeugte Untergruppe $\mathcal{D}_k$ von $\mathrm{O}(2, \mathbb{R})$ heißt die *Diedergruppe* und es gilt

$$\mathcal{D}_k = \{D_0, D_{2\pi/k}, , D_{2\pi/k}^2, \dots, D_{2\pi/k}^{k-1},\ S,\ S D_{2\pi/k}, \dots,\ S D_{2\pi/k}^{k-1}\}, \qquad |\mathcal{D}_k| = 2k.$$

Je zwei solche Diedergruppen, $\langle D_{2\pi/k}, S \rangle$ und $\langle D_{2\pi/k}, S' \rangle$ sind konjugiert

Klassifikationssatz 1.3.4. (in zwei Dimensionen) *Es sei* $\dim \mathbb{A} = 2$ *und* $G \subset \mathbf{B}(\mathbb{A}, d_e)$ *eine endliche Untergruppe. Dann ist* $G \subset \mathrm{O}(P) \cong \mathrm{O}(2, \mathbb{R})$ *für ein* $P \in \mathbb{A}$ *und ist entweder*
• *die zyklische Gruppe* $\mathcal{C}_n$ *der Ordnung* n*, erzeugt von der Drehung* $D_\theta(P)$ *mit* $\theta = 2\pi/n$*, oder*
• *die Diedergruppe* $\mathcal{D}_n$*, die von zwei Elementen erzeugt wird: der Drehung* $D_\theta(P)$ *mit* $\theta = 2\pi/n$ *und einer Spiegelung* S_ℓ *an einer Gerade* ℓ *durch den Fixpunkt* P*, so dass* $S_\ell \langle D_\theta(P) \rangle S_\ell = \langle D_\theta(P) \rangle$*. Es gilt dann* $\mathcal{D}_n = \mathcal{C}_n \rtimes \langle S_\ell \rangle$*. Für* $n > 1$ *sind Diedergruppen nicht abelsch.* $\mathcal{D}_1 = \{\mathrm{Id}, S\}$ *ist zyklisch.*

Es sei $M \subset \mathbb{A}^2$ ein k-Eck, d.h., die durch Ihre endlich vielen Ecken erzeugte konvexe Menge (ganz allgemein nennt man die von endlich vielen Punkten erzeugten (abgeschlossenen) konvexen Teilmengen des n-dimensionalen affinen Raumes *(konvexe) Polytope*) und

$$\mathbf{B}_M = \mathrm{Isom}(M) = \{\varphi \in \mathbf{B}(\mathbb{A}^2) : \varphi(M) = m\}$$

die Isometriegruppe dieser Menge. Jede Bewegung $\psi \in \mathbf{B}_M$ permutiert die Menge der Ecken $\mathcal{E}(M)$ und der Kanten $\mathcal{K}(M)$ von M. Insbesondere werden benachbarte Kanten auf benachbarte Kanten abgebildet, jeweils nur die Ecken, die die Spitzen von gleichen Winkeln sind, und Kanten, die gleiche Länge haben, permutiert.

Identitätssatz 1.3.5. *Es seien* $A_0, A_1, A_2, \dots, A_n \in \mathbb{A}^n$ $(n+1)$*-Punkte in allgemeiner Lage und* $\psi, \phi \in \mathrm{Aff}(\mathbb{A}^n)$ *zwei affine Abbildungen, mit* $\psi(A_j) = \phi(A_j)$ *für* $j = 0, 1, \dots, n$*. Dann gilt* $\psi = \phi$*.*

Folgerungen. Es sei $M \subset \mathbb{A}^2$ ein k-Eck und $\mathcal{E}(M)$ die (k-elementige) Menge seiner Ecken.
• Die Abbildung $\mathbf{B}_M \to \mathfrak{S}(\mathcal{E}(M))$, $\psi \mapsto \psi|_{\mathcal{E}(M)}$, ist ein injektiver Homomorphismus. Insbesondere ist $\mathbf{B}_M$ endlich.
• Gilt $\mathcal{E}(M) = \{E_0, \dots, E_m\}$, so ist

$$Q = \Big(\frac{1}{1+m} \sum_{j=0}^{m} (E_j - E_0)\Big) \dotplus E_0$$

ein Fixpunkt von $\mathbf{B}_M$. Insbesondere $\mathbf{B}_M \subset \mathrm{O}_Q \cong \mathrm{O}(2)$.
• Jede der endlichen Untergruppen aus 1.3.4 ist die volle Isometriegruppe eines geeigneten k-Ecks. Die Isometriegruppe eines regulären k-Ecks (alle Kantenlängen und Eckwinkel gleich) ist die Diedergruppe $\mathcal{D}_k$.

Die volle lineare Gruppe $\mathrm{GL}(V)$ eines n-dimensionalen Vektorraumes kann mit der Menge aller invertierbaren $n \times n$ Matrizen, $\mathrm{GL}(n, \mathbb{R}) \subset \mathbb{R}^{n^2}$ identifiziert werden. Die topologische oder metrische Struktur auf $\mathbb{R}^{n^2}$ erlaubt daher von Abständen sowie offenen und abgeschlossenen Teilmengen in $\mathrm{GL}(n, \mathbb{R}) \cong \mathrm{GL}(V)$ zu sprechen.
Die affine Gruppe $\mathrm{Aff}(\mathbb{A}^n)$ kann ebenfalls als eine Untergruppe von $\mathrm{GL}(n+1, \mathbb{R})$ betrachtet werden: Nach Wahl einer Identifizierung $\beta : \mathbb{R}^n \to \mathbb{A}^n$ haben wir die semidirekte Zerlegung und die Abbildung

$$\mathrm{Aff}(\mathbb{A}^n) \cong \mathbb{R}^n \rtimes \mathrm{GL}(n, \mathbb{R}) \longrightarrow \mathrm{GL}(n+1, \mathbb{R}), \qquad (x, A) \longmapsto \begin{pmatrix} A & x \\ 0 & 1 \end{pmatrix}$$

ist ein Isomorphismus auf die Untergruppe der Blockmatrizen $\{\left(\begin{smallmatrix} A & x \\ 0 & 1 \end{smallmatrix}\right) : A \in \mathrm{GL}(n,\mathbb{R}), x \in \mathbb{R}^n\}$ in $\mathrm{GL}(n+1,\mathbb{R})$.

Definition 1.3.6. Eine Teilmenge $\Gamma \subset \mathbb{R}^N$ (oder eines metrische Raumes (X,d)) heißt *diskret*, falls für jedes $x \in \Gamma$ es eine offene Umgebung U (Kugel $B_\varepsilon(x)$) mit $U \cap \Gamma = \{x\}$ gibt.

Eine Untergruppe $\Gamma \subset \mathrm{GL}(N,\mathbb{R})$ heißt diskret, falls Γ diskret als eine Teilmenge von $\mathbb{R}^{N^2}$ ist.

Beispiele. Die Teilmengen $\mathbb{Z} \subset \mathbb{R}$ und $\{1/n : n \in \mathbb{N}\} \subset \mathbb{R}$ sind diskret. $\{1/n : n \in \mathbb{N}\} \cup \{0\} \subset \mathbb{R}$ ist nicht diskret. Diskrete Teilmengen müssen also nicht abgeschlossen sein. Es gilt aber:

Lemma 1.3.7. *Jede diskrete Untergruppe $\Gamma \subset \mathrm{GL}(n,\mathbb{R})$ ist abgeschlossen.*

Betrachtet man Gruppenoperationen (statt abstrakter Gruppen), so ist in dem Zusammenhang der folgende Typ von Gruppenoperationen von großer Wichtigkeit:

Definition 1.3.8. Eine Gruppenoperation $\cdot : G \times X \to X$ (X metrischer Raum) heißt *eigentlich diskontinuierlich*, falls für jede kompakte Teilmenge $K \subset X$ die Menge $K_G := \{g \in G : g(K) \cap K \neq \varnothing\}$ endlich ist.

Lemma 1.3.9. *Es sei $\Gamma \subset \mathbf{B}(\mathbb{A}^n)$ eine diskrete Untergruppe. Dann ist die induzierte Operation $\Gamma \times \mathbb{A}^n \to \mathbb{A}^n$ eigentlich diskontinuierlich.*

Die Translationsgruppe $\mathbf{T} \cong \mathbb{R}^n$ ist eine wichtige Untergruppe der Bewegungen. Der folgende Satz beschreibt die diskreten Untergruppen von $(\mathbb{R}^n, +)$:

Theorem 1.3.10. *Es sei $\Gamma \subset \mathbb{R}^n$ eine diskrete Untergruppe. Dann gibt es $\mathbb{R}$-linear unabhängige Vektoren $v_1, \dots, v_k \in \mathbb{R}^n$ mit $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_k$*

Die Untergruppe $\Gamma \subset \mathbb{R}^n$ operiert auf $\mathbb{R}^n$ durch Translationen. Es sei

$$\mathcal{P} := \mathcal{P}(v_1, \dots, v_k) = \{\sum_{j=1}^{k} t_j v_j : 0 \leq t_j \leq 1 \ \forall\ j = 1, \dots, k\}$$

der durch die Vektoren $v_1, \dots, v_k$ erzeugte k-dimensionale abgeschlossene Parallelotop (k-dim Spat). Dann ist $\Omega := \mathcal{P} \times \langle v_1, \dots, v_k \rangle_{\mathbb{R}}^{\perp}$ eine *Fundamentalzelle* für die Operation $\Gamma \times \mathbb{R}^n \to \mathbb{R}^n$, Dabei heißt eine Teilmenge $\Omega \subset \mathbb{R}^n$ für eine (stetige) Operation $\cdot : G \times \mathbb{R}^n \to \mathbb{R}^n$ eine Fundamentalzelle, falls gilt:

- Ω ist eine abgeschlossene Teilmenge mit einem stückweise glatten Rand, so dass $\mathrm{int}(\Omega)$ homöomorph zu einer offenen Kugel ist.
- Jede G-Bahn $G \cdot x$ schneidet Ω in höchstens endlich vielen Punkten.
- Jede G-Bahn $G \cdot y$ durch einen Punkt $y \in \mathrm{int}(\Omega)$ aus dem offenen Kern $\mathrm{int}(\Omega)$ von Ω schneidet Ω in exakt einem Punkt (nämlich $\{y\}$).

Zur Erinnerung: Der offene Kern $\mathrm{int}(M)$ einer Teilmenge $M \subset \mathbb{R}^n$ ist die Menge aller inneren Punkte, d.h., die größte, noch in M enthaltene offene Teilmenge.

Bemerkungen: Ist $\Omega \subset \mathbb{R}^n$ eine Fundamentalzelle, so gilt $\mathbb{R}^n = \bigcup_{g \in G} g \cdot \Omega$. Ferner ist die Vereinigung $\bigcup_{g \in G} g \cdot \mathrm{int}(\Omega)$ disjunkt und eine offene und dicht Teilmenge in $\mathbb{R}^n$. Nicht jede Operation besitzt eine Fundamentalzelle, und wenn ja, so ist diese Zelle nicht eindeutig bestimmt. Jede eigentlich diskontinuierliche Operation $\Gamma \times \mathbb{R}^n \to \mathbb{R}^n$ einer Untergruppe von Bewegungen, $\Gamma \subset \mathbf{B}(\mathbb{R}^n)$, besitzt eine Fundamentalzelle.

Eine *Pflasterung* (*Parkettierung*) von $\mathbb{A}^2$ (oder allgemeiner von einer Teilmenge $\mathcal{A} \subset \mathbb{A}^2$, z.B., eines unendlichen Streifens) ist eine abzählbare Familie von abgeschlossenen Teilmengen $A_j \subset \mathbb{A}^2$ (*Pflastersteinen*), so dass
- $\bigcup_{j\in\mathbb{N}} A_j = \mathbb{A}^2$;
- jedes A_j homöomorph zu einer abgeschlossenen Kugel $B_1 \subset \mathbb{A}^2$ ist;
- $\mathrm{int}(A_j)$, $j \in \mathbb{N}$, paarweise disjunkt sind.

Ist Ω eine Fundamentalzelle für eine Operation $\Gamma \times \mathbb{R}^2 \to \mathbb{R}^2$, so ist $(g \cdot \Omega)_{g\in\Gamma}$ ein Beispiel einer Pflasterung, vorausgesetzt, Ω ist eine beschränkte Menge.
Die Mengen A_j können alle unterschiedlich (nicht kongruent) sein; man kann aber ebenso gut Pflasterungen mit einem, oder endlich vielen Kongruenztypen der A_j-s betrachten. Statt bloßer Pflastersteine A_j in einer Pflasterung kann man jeden Stein mit einer Markierung (einem Muster) versehen. Pflasterungen weisen unterschiedliche Grade von "Regularität" auf: Es gibt Pflasterungen, die zwar aus einigen wenigen Kongruenzklassen von Steinen bestehen (Markierungen inbegriffen), die aber global je nach Lage der einzelnen Steine alle Möglichkeiten zwischen "völlig chaotisch" und "hochgradig symmetrisch" ausschöpfen. Für eine ausfürliche Behandlung dieses Themas, mit einer Fülle von nichttrivialen Resultaten und vielen immer noch ungelösten Problemen verweisen wir auf die Monographie *Tilings and Patterns* von B. Grünbaum und G. C. Shephard. Wir werden uns im Rahmen dieser Vorlesungen mit einigen wenigen periodischen Pflasterungen beschäftigen, d.h. Pflasterungen, deren Isometriegruppe eine nichttriviale Untergruppe der Translationen enthält. Solche Pflasterungen (mit oder ohne Markierungen) treten z.B. als (idealisierte) periodische Mosaiken, (geeignet verklebten) Tapetenmuster, periodische Friese, etc.

Wir wenden uns der Klassifikation von diskreten Untergruppen der Bewegungsgruppe zu. Um solches $\Gamma \subset \mathbf{B}(\mathbb{R}^n)$ zu analysieren, betrachten wir zwei Gruppen, die auf natürliche Weise mit Γ assoziiert sind. Zunächst erinnern wir an die semidirekte Zerlegung $\mathbf{B}(\mathbb{R}^n) = \mathbf{T} \rtimes \mathrm{O}_P \cong \mathbb{R}^n \rtimes \mathrm{O}(n)$ und die zugehörige Sequenz von Homomorphismen

$$
\begin{array}{ccccc}
 & & (T_v, R) & \longmapsto & R \\
 & & \psi & \longmapsto & T_{-\psi(0)} \circ \psi \\
\mathbf{T} & \xrightarrow{\iota} & \mathbf{B}(\mathbb{R}^n) & \xrightarrow{\mathrm{pr}} & \mathrm{O}(n) = \mathbf{B}(\mathbb{R}^n)/_{\iota(\mathbb{R}^n)} \\
\cup & & \cup & & \cup \\
\mathbf{T}_\Gamma & \xrightarrow{\iota} & \Gamma & \xrightarrow{\mathrm{pr}} & \overline{\Gamma}
\end{array}
\tag{1.3.11}
$$

Für jede Untergruppe $\Gamma \subset \mathbf{B}(\mathbb{R}^n)$ ist dann $\mathbf{T}_\Gamma := \Gamma \cap \mathbf{T}$ eine Normalteiler und $\overline{\Gamma} := \mathrm{pr}(\Gamma) \subset \mathrm{O}(n)$ die der Gruppe Γ zugeordnete Punktgruppe der orthogonalen Transformationen. Im Gegensatz zu der vollen Bewegungsgruppe $\mathbf{B}$, in der jedes Element aus $\overline{\mathbf{B}} = \mathrm{pr}(\mathbf{B}) = \mathrm{O}(n)$ auch in $\mathbf{B}$ liegt, gibt es Beispiele von Untergruppen mit $R \in \mathrm{pr}(\Gamma)$ aber $\mathrm{pr}^{-1}(R)$ nur Elemente $T_{v_j} \circ R$ mit nichttrivialen v_j enthält.

Lemma 1.3.12. *Es sei $\Gamma \subset \mathbf{B}(\mathbb{R}^n)$ eine Untergruppe und $\mathbf{T}_\Gamma = \Gamma \cap \mathbf{T} \subset \mathbb{R}^n$, $\overline{\Gamma} = \mathrm{pr}(\Gamma) \subset \mathrm{O}(n)$ die assoziierte Untergruppen. Man betrachte $\mathbf{T}_\Gamma$ als eine Teilmenge von $\mathbb{R}^n$, auf dem $\mathrm{O}(n)$ durch orthogonale Transformationen operiert. Dann gilt*

$$\overline{\Gamma} \cdot \mathbf{T}_\Gamma = \mathbf{T}_\Gamma$$

Beweis: Ist nämlich $g = T_v \circ R \in \Gamma$, so gilt wegen $\mathbf{T}_\Gamma \lhd \Gamma$ für jedes $T_w \in \mathbf{T}_\Gamma$

$$g \circ T_w \circ g^{-1} = T_v \circ R \circ T_w \circ R^{-1} \circ T_{-v} = T_{R(w)} = T_{\mathrm{pr}(g)(w)} \in \mathbf{T}_\Gamma \,,$$

d.h. $R(\mathbf{T}_\Gamma) = \mathbf{T}_\Gamma$ für jedes $R = \mathrm{pr}(g) \in \overline{\Gamma}$. □

.

Ist nun $\Gamma \subset \mathbf{B}(\mathbb{R}^n)$, so ist $\mathbf{T}_\Gamma$ eine diskrete Untergruppe von $\mathbb{R}^n$ und damit ist $\overline{\Gamma}$ als eine Untergruppe von $\{R \in \mathrm{O}(n) : R(\mathbf{T}_\Gamma)) = \mathbf{T}_\Gamma\}$ ebenfalls eine diskrete Untergruppe.

Die Möglichkeiten für $\overline{\Gamma}$ sind allerdings stark eingeschränkt, falls $\mathbf{T}_\Gamma$ ein volles Gitter in $\mathbb{R}^n$, d.h., $\mathbf{T}_\Gamma$ von einer Basis von $\mathbb{R}^n$ erzeugt wird. Aus der Tatsache, dass die Operation $\overline{\Gamma} \times \mathbb{R}^2 \to \mathbb{R}^2$ die Teilmenge $\mathbf{T}_\Gamma \subset \mathbb{R}^3$ invariant läßt , folgt die

1.3.13. Kristallographische Einschränkung. *Gilt $\mathbf{T}_\Gamma = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2$ mit linear unabhängigen $v_1, v_2 \in \mathbb{R}^2$ und ist D_φ eine Drehung in der (endlichen) Gruppe $\overline{\Gamma}$ so gilt*

$$\varphi \in \{\mathbb{Z}\frac{2\pi}{1}, \mathbb{Z}\frac{2\pi}{2}, \mathbb{Z}\frac{2\pi}{3}, \mathbb{Z}\frac{2\pi}{4}, \mathbb{Z}\frac{2\pi}{6}\} .$$

Analoge Aussage gilt auch in höheren Dimensionen.

Die beiden Gruppe $\mathbf{T}_\Gamma$ und $\overline{\Gamma}$ erlauben Rückschlüsse auf die Struktur von Γ. In dem folgenden Satz wollen wir nicht zwischen mengentheoretisch verschiedenen aber isomorphen Untergruppen unterscheiden und sprechen daher von Isomorphieklassen statt von einzelnen Untergruppen.

1.3.14. Klassifikationssatz für diskrete Bewegungsgruppen der Ebene. *Es sei $\Gamma \subset \mathbf{B}(\mathbb{R}^2)$ eine diskrete Untergruppe.*

(0) Gilt $\mathbf{T}_\Gamma = \{0\}$, so ist Γ isomorph zu einer endlichen Untergruppe von $\mathrm{O}(2)$.

(1) Gilt $\mathbf{T}_\Gamma = \mathbb{Z}v$ für ein $v \in \mathbb{R}^2 \setminus \{0\}$ und sei $\ell := \mathbb{R}v$ so ist Γ isomorph zu einer der folgenden 7 Untergruppen:

$$\langle T_v\rangle, \quad \langle T_v, D_\pi\rangle, \quad \langle T_v, S_{\ell^\perp}\rangle, \quad \begin{matrix}\langle T_v, S_\ell\rangle \\ \langle T_v, T_{1/2v} \circ S_\ell\rangle\end{matrix}, \quad \begin{matrix}\langle T_v, S_\ell, D_\pi\rangle \\ \langle T_v, T_{1/2v} \circ S_\ell, D_\pi\rangle\end{matrix}$$

In diesem Fall $\overline{\Gamma} \in \{\{e\}, \langle D_\pi\rangle, \langle S_\ell\rangle, \langle S_{\ell^\perp}\rangle, \langle S_\ell, S_{\ell^\perp}\rangle\}$.

(2) Gilt $\mathbf{T}_\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2$ für $\mathbb{R}$-linear unabhängige Vektoren $v_1, v_2 \in \mathbb{R}^2$, so gibt es 17 Isomorphieklassen von diskreten Untergruppen Γ der ebenen Bewegungsgruppe. In diesem Fall $\overline{\Gamma}$ ist isomorph zu einer der folgenden Gruppen: $\mathcal{C}_n$ oder $\mathcal{D}_n$ mit $n \in \{1, 2, 3, 4, 6\}$.

Diese Klassifikation von diskreten Gruppen erlaubt z.B. die scheinbar unendliche Vielfalt möglicher Muster, Mosaiken oder Friese nach Ihren Symmetriegraden zu ordnen. Es gibt für jede in (1) oder (2) aufgelistete diskrete Untergruppe einen Fries oder ein Mosaik, dessen volle Isometriegruppe exakt eine der im Satz 1.3.14 genannten Gruppen ist. Bereits in alten Ägypten gab es Muster zu allen 17 Isomorphieklassen diskrete Gruppen.

1.4. Kristallographische Untergruppen in Dimension 3

Die orthogonale Gruppe des n-dimensionalen Raumes hat zwei Zusammenhangskomponenten:

$$\mathrm{O}(n) = \{A \in \mathrm{O}(n) : \det A = 1\} \dot\cup \{A \in \mathrm{O}(n) : \det A = -1\} = \mathrm{SO}(n) \dot\cup S \cdot \mathrm{SO}(n), \quad \det S = -1$$

Speziell für $n = 3$ hat jedes $A \in \mathrm{SO}(3)$ 1 als Eigenwert und damit eine Fixpunktgerade $\mathbb{R}v$. Da $A(v^\perp) = v^\perp$, so ist die Einschränkung $A|_{v^\perp}$ eine Drehung in der Ebene $v^\perp$ um einen gewissen Winkel θ. Wir führen die folgende Bezeichnung für Elemente aus SO(3) ein: Für $v \in \mathbb{R}^3$ bezeichnet D_v die Drehung mit der punktweise fixierten Drehachse $\mathbb{R}v$ um den Winkel $\|v\|$ in der orthogonalen Ebene $v^\perp$ (gegen den Uhrzeigersinn nach der rechte-Hand-Regel). So z.B. bezeichnet $D_{(0,0,\pi/2)}$ die Drehung

der x_1, x_2-Ebene um den Winkel $\pi/2$ gegen den Uhrzeigersinn, während $D_{(0,0,-\pi/2)}$ die Drehung der x_1, x_2-Ebene um den Winkel $\pi/2$ im Uhrzeigersinn bezeichnet. Da $\{A \in \mathrm{O}(3) : \det A = -1\} = -E_3 \cdot \mathrm{SO}(3)$, ist jedes Element aus dieser Komponente eine Drehspiegelung, d.h., eine orthogonale Spiegelung an der Ebene $E \subset \mathbb{R}^3$ mit einer anschließenden Drehung der Ebene E um einen gewissen Winkel.

Unser Ziel ist es die endlichen Untergruppen von O(3) zu klassifizieren. Wir beginnen mit dem Fall $G < \mathrm{SO}(3)$ endlich. Die kanonische Operation $\mathrm{SO}(3) \times \mathbb{R}^3 \to \mathbb{R}^3$ induziert die Opertation $\mathrm{SO}(3) \times S^2 \to S^2$ wobei S^2 für die Einheitssphäre in $\mathbb{R}^3$ steht. Jedes $g \in G < \mathrm{SO}(3)$ hat dann genau zwei Fixpunkte in S^2, (es sei denn $g = \mathrm{Id}$), nämlich die beiden Schnittpunkte der Drehachse von g mit S^2. Die Klassifikation von endlichen $G < \mathrm{SO}(3)$ beruht auf einer geschickten Zählung aller solcher Fixpunkte samt der zugehörigen Gruppenoperation. Diese Idee läßt sich sehr allgemein formulieren als die Kombinatorik einer gewissen

Doppelfaserung. Es sei G eine endliche Gruppe, die auf einer Menge S operiert: $\cdot : G \times S \to S$. Man definiere auf $\mathcal{S} := G \times S$ die folgende Gruppenoperation:

$$\diamond : G \times (G \times S) \to (G \times S) \qquad (g, (x, z)) \mapsto (gxg^{-1}, g \cdot z) \tag{1.4.1}$$

Um die Struktur der (nichttrivialen) Isotropieuntergruppen in Punkten aus S adäquat zu beschreiben, betrachte man die folgende Teilmenge $Y := \{(g, z) \in G \times S : g \cdot z = z\}$, sowie $Y^\times := Y \smallsetminus (\{e\} \times S)$. Y und $Y^\times$ sind stabil unter der Operation (1.4.1). Die folgende (G-äquivariante) Faserung ist ein wichtiges Hilfsmittel für die Untersuchung der endlichen Untergruppen von $\mathrm{Aut}(S)$:

$$\begin{array}{ccc} G \times S & & \\ \cup & & \\ Y^\times & \xrightarrow{\pi_S} & S \\ \downarrow{\scriptstyle \pi_G} & & \\ G & & \end{array}$$

Es sei $F := \{z \in S : \exists\, g \in G \smallsetminus \{e\} \text{ mit } g \cdot z = z\} = \{z \in S : G_z \neq e\}$. Diese Teilmenge ist G-stabil (und daher ist die Einschränkung $G \times F \to F$ von $G \times S \to S$ eine Gruppenoperation aud F) und es gilt $\pi_S(Y^\times) = F$. Die Abbildung $\pi_S : Y^\times \to F$ is t G-äquivariant, d.h., $\pi_S(g \diamond y) = g \cdot \pi_S(y)$ für alle $y \in \mathbb{F}^\times$ und $g \in G$. Wir nehmen jetzt an, dass jedes $g \in G \smallsetminus \{e\}$ nur endlich viele Fixpunkte in S besitzt. (Das trifft z.B. auf $G \subset \mathrm{SO}(3)$ und $S = S^2$ zu.) Dann ist auch F endlich und durch das Abzählen der Fasern in der obigen Doppelfaserung erhält mat die folgende Formel ($\mathrm{Fix}(g)$ ist die endliche Menge der Fixpunkte von g in S):

$$\sum_{g \in G \smallsetminus e} |\,\mathrm{Fix}(g)| = \sum_{\substack{\text{Orbits} \\ \text{in F}}} \frac{|G|}{|G_{z_j}|}(|G_{z_j}| - 1) \tag{1.4.2}$$

Definition 1.4.3. Ein *Platonischer Körper* ist ein konvexes Polytop, dessen Seiten(flächen) kongruent zu einem festen regulären n-Eck sind und in jeder Ecke die gleich Anzahl von Kanten zusammenläuft.

Damit sind je zwei Ecken eines Platonischen Körpers lokal kongruent. Es gilt sogar viel mehr. Je zwei Fahnen, d.h. Konstellationen $f_j \supset k_j \supset e_j$, wobei f_j eine Seitenfläche (abg. n-Eck), k_j eine Ihrer Kanten und e_j eins der Enden von k_j ist, lassen sich durch eine geeignete globale Isometrie des Platonischen Körpers aufeinander abbilden. Platonische Körper gehören zu der Klasse der Polytope mit höchster möglicher Symmetrie.

Da mindesten 3 n-Ecke nötig sind, um eine Raumecke zu bilden, der Eckwinkel in einem regulären n-Eck $\frac{n-2}{n}\pi$ beträgt und die Summe der Winkel der anliegenden n-Ecken $< 2\pi$ sein muss, folgt nun $n \in \{3,4,5\}$. Die *lokale* Klassifizierung von möglichen Raumecken aus regulären n-Ecken für ein festes n ergibt die folgenden fünf Möglichkeiten: 3, 4 oder 5 reguläre 3-Ecke, 3 Quadrate oder 3 reguläre 5-Ecke. Diese Kongruenztypen korrespondieren zu den entsprechenden *global* existierenden 5 Platonischen Körpern: dem Tetraeder, dem Okaeder, dem Ikosaeder, dem Würfel und dem Dodekaeder. Das sind alle möglichen Körper, deren Oberfläche aus regulären k-Ecken einer Sorte besteht. Man kann sogar die Voraussetzung der Regularität bei den Seitenflächen fallen lassen und die folgende allgemeine Aussage beweisen:

Lemma 1.4.4. *Es sei $\mathcal{P}$ ein 3-dimensionales (konvexes) Polytop, $e = e_{\mathcal{P}}$ die Anzahl seiner Ecken, $k = k_{\mathcal{P}}$ die Anzahl seriner Kanten und $f = f_{\mathcal{P}}$ die Anzahl seiner Seitenflächen. Es seinen ferner $m_f, m_e \in \mathbb{N}$ zwei Zahlen, so dass gilt:*
- *Jede Seitenfläche von $\mathcal{P}$ ist ein m_f-Eck.*
- *In jeder Ecke laufen m_e Kanten zusammen.*

Dann gilt $(m_e, m_f) \in \{(3,3),\ (3,4),\ (4,3),\ (3,5),\ (5,3)\}$. Die Anzahl der Ecken, Kanten und Seitenflächen wird durch (m_e, m_f) eindeutig bestimmt:

(m_e, m_f)	$(e,\ k,\ f)$
$(3,3)$	$(4,\ 6,\ 4)$
$(3,4)$	$(8, 12, 6)$
$(4,3)$	$(6, 12, 8)$
$(3,5)$	$(20, 30, 12)$
$(5,3)$	$(12, 30, 20)$

Beweis: Grundlegend ist hier die

1.4.5. Eulersche Polyederformel für konvexe Körper $\mathcal{P}$ [Euler, Gauss-Bonet]:

$$\chi(P) := e_{\mathcal{P}} - k_{\mathcal{P}} + f_{\mathcal{P}} = 2$$

Da noch trivialerweise

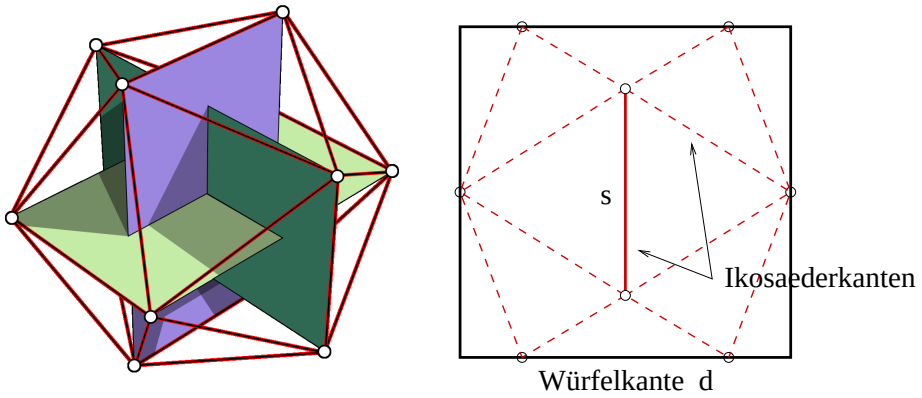
$$(*) \qquad f m_f = 2k = e m_e$$

gilt, so erhalten wir die folgende Kette von Gleichungen

$$\begin{aligned} 0 < 2 \cdot 2m_e &= 2em_e - 2km_e + 2fm_e = \\ &= 2fm_f - fm_f m_e + 2fm_e = \\ &= -f[(m_f - 2)(m_e - 2) - 4] \end{aligned}$$

Und damit folgt aus $(m_f - 2)(m_e - 2) < 4$ und der Tatsache, dass $m_e \geq 3,\ m_f \geq 3$ sein muss, dass die obigen Möglichkeiten die einzigen Möglichkeiten für die Werte der Paare (m_e, m_f). Aus den 3 Gleichungen, $(*)$ und (1.4.5), lassen sich dann die Werte e, k, f explizit berechnen. Sie ensprechen genau den 5 Konstellationen, die wir bereit von den Platonischen Körpern kennen. □

Während die explizite Konstruktion eines Tetraeders, eines Würfels und eines dazu dualen Oktaeders ziemlich offensichtlich ist, ist es schwieriger ein Dodekaeder und ein (dazu duales) Ikosaeder zu konstruieren. Eine Konstruktion des Ikosaeders baut auf dem Würfel auf: Ein Ikosaeder läßt sich so in einen Würfel einschreiben, dass jeweils 3 Paare von gegenüberliegenden Kanten des Ikosaeders auf den 6 Seitenquadraten eines Würfels liegen, siehe das linke, unten stehende Bild. Ist s die Kantenlänge des Ikosaeders, so ist $d = \frac{1+\sqrt{5}}{2} \cdot s$ die Kantenlänge des umschreibenden Würfels.



Damit sind die 12 Endpunkte der 6 Geradensegmente auf den 6 Seiten eines Würfels (siehe Zeichnung oben rechts) die Ecken eines Ikosaeders.

Theorem 1.4.6. *Jede endliche Untergruppe G von* SO(3) *ist eine von den unten aufgelisteten Untergruppen:*

(1) Die zyklische Gruppe $\mathcal{C}_k \cong \mathbb{Z}_k$ der Rotationen um vielfache Werte von $2\pi/k$ um eine beliebige feste Drehachse.

(2) Die Diedergruppe $\mathcal{D}_k$, in der die k Spiegelungen der Drehebene von $\mathcal{C}_k \lhd \mathcal{D}_k$ durch Elemente aus SO(3) *mit den in der Drehebene liegenden Drehachsen erzeugt sind;*
(in (1) und (iii) ist $k \in \mathbb{N}$ beliebig).

(3) Die Tetraedergruppe $\mathcal{T}$, d.h., die Drehgruppe eines regulären Tetraeders.

(4) Die Würfelgruppe $\mathcal{O}$, d.h., die Drehgruppe eines (regulären) Würfels

(5) Die Ikosaedergruppe $\mathcal{I}$, d.h., die Drehgruppe eines regulären Ikosaeders.

Beweisskizze. Wir lassen $G \subset$ SO(3) auf die Einheitssphäre $S := \{x \in \mathbb{R}^3 : \|x\| = 1\}$ operieren. Jedes $g \in \text{SO}(3) \setminus \{e\}$ hat genau zwei Fixpunkte in S. Es seien $F_1, \ldots, F_r$ die G-Bahnen in F und G_j entsprechend die Isotropiegruppen in den beliebig gewählten Punkten $z_j \in F_j$. Die Ordnung $|G_j|$ (≥ 2) hängt dabei nur von F_j (und nicht von der Wahl eines Punktes $z_j \in F_j$) ab. Sie wird im Folgenden mit n_j bezeichnet. Es sei $N := |G|$. In diesem Spezialfall lautet die Formel (1.4.2)

$$(*) \qquad 2(N-1) = |Y^\times| = \sum_{j=1}^{r} \frac{N}{n_j}(n_j - 1)$$

oder äquivalent: $2 - 2/N = r - \sum_{j=1}^{r} 1/n_j$
Daraus ergeben sich folgende Einschränkungen für die numerischen Werte von r, N und n_j:

(i) $2 \leq r \leq 3$ (wegen $2 > 2 - 2/N = r - \sum_{j=1}^{r} 1/n_j \geq r - r/2 = r/2$) Wir ordnen dann n_j der Größe nach: $n_1 \leq n_2 \leq n_3$

(ii) In dem Fall $r = 2$ lautet $(*)$ $2/N = 1/n_1 + 1/n_2$. Das ist nur möglich wenn $N = n_1 = n_2$, d.h. $G \subset$ SO(3) hat genau zwei Fixpunkte (F_1, F_2 sind 1-elementig).

Es bleibt der Fall $r = 3$.

(iii) $n_1 = 2$ (wenn $n_1 \geq 3$ dann gelte $2 > 2 - 2/N = 3 - \sum^{3} 1/n_j \geq 2$:Widerspruch). Analog gilt die Einschränkung $n_2 \leq 3$ ($n_2 \geq 4$ führt wie oben zum Widerspruch).

(iv) Wir betrachten jetzt die Situation $n_1 = n_2 = 2$. Dann ist $m := n_3 \geq 2$ beliebig und es gilt

$$(n_1, n_2, n_3; N) = (2, 2, m; 2m).$$

Jede Untergruppe von SO(3), die diese numerische Invariante besitzt, ist isomorph zu der Diedergruppe $\mathcal{D}_m$ und ist erzeugt durch zwei Drehungen $D_v, D_w \in$ SO(3), $G = \langle D_v, D_w \rangle$, so dass gilt:

• D_v erzeugt die zyklische Untergruppe $\mathcal{C}_m < \mathcal{D}_m$ der Ordnung m (der einzige Normalteiler vom Index 2 in der Diedergruppe).
• D_w ist eine weitere Drehung um 180 Grad, allerdings ist deren Drehachse senkrecht zu $\mathbb{R}v$.
Es sei an dieser Stelle angemerkt, dass es in der vollen Punktgruppe O(3) weitere Untergruppen existieren, die ebenfalls zu einer Diedergruppe isomorph sind, jedoch nicht nur aus Elementen aus SO(3) bestehen. Diese Beispiele zeigen, dass es in O(3) isomorphe aber nicht konjugierte endliche Untergruppen gibt.

(v) Es bleibt der Fall $n_2 = 2, n_3 = 3$. Dann führt die Gleichung $1 + 2/N = 1/2 + 1/3 + 1/n_3$ zu der Abschätzung $n_3 \leq 5$. Es bleiben also für (n_1, n_2, n_3, N) nur noch die Möglichkeiten

$$(2,3,3;12), \qquad (2,3,4;24), \qquad (2,3,5;60)$$

In der Tat gibt es zu jedem der drei Zahlensätze genau eine (bis auf Isomorphie) endliche Untergruppe G von SO(3): Dazu untersuchen wir die entsprechenden Fixpunktmengen $F \subset S = S^2$, die in allen drei Fällen in 3 G-Bahnen

$$F_1 = G(x_1) \cong G/G_1,\ F_2 = G(x_1) \cong G_2 \quad \text{und} \quad F_3 = G(x_3) \cong G/G_3$$

zerfällt. Im Folgenden untersuchen wir diese 3 Möglichkeiten.

• Für $(n_1, n_2, n_3; N) = (2,3,3;12)$ gilt es $|F_1| = 6,\ |F_2| = |F_3| = 4$. Wir werden jetzt die Menge (Bahn) F_2 (oder analog F_3) genauer beschreiben. Da $|G_2| = 3$, gilt $G_2 = \langle D_v \rangle$, wobei D_v eine Drehung um $2\pi/3$ ist und deren Achse $\mathbb{R}v$ durch den Punkt $z_2 \in S$ geht. Da insbesondere G_2 auf F_2 operiert, permutiert G_2 die 3 Punkte in $F_2 \setminus \{z_2\}$. Da aber die Elemente in G_2 Drehungen um die Achse durch z_2 sind, sind die Abstände $d(x,y)$ für alle Punktenpaare $x, y \in F_2 \setminus \{z_2\}$ gleich. Da das Gleiche für die Isotropieuntergruppen G_y und die Elemente der Menge $F_2 \setminus \{y\}$ für jedes $y \in F_2$ gilt, folgern wir, dass die Elemente aus F_2 die Ecken eines Tetraeders bilden. Die Gruppe $\mathcal{T}$ aller Drehungen dieses Tetraeders ist dann genau die Gruppe mit der nummerischen Invariante (2,3,3;12): $\mathcal{T}$ enthält 4 zyklische Gruppen von Ordnung 3 (Isotropieuntergruppen der Punkte in F_2 oder F_3), wobei die zugehörigen Achsen durch eine der Ecken aus F_2 und den Mittelpunkt der gegenüber liegenden (Dreiecks)Seite geht. Die Menge aller Durchschnitte der zugehörigen 4 Drehachsen mit S stimmt mit $F_2 \cup F_3$ überein. Die Elemente in F_1 sind dann die 6 Schnittpunkte der Drehachsen der 3 zyklischen Untergruppen von G der Ordnung 2. Da auch diese zyklischen Untergruppen die Ecken $F_2 = G(x_2)$ unseres Tetraeders invariant lassen, müssen (aus geometrischer Überlegung) diese Drehachsen durch die Mittelpunkte der 3 Paare von gegenüber liegenden Kanten des Tetraeders $T(F_2)$ gehen. Mehr Drehungen kann die Isometriegruppe des Tetraeders nicht enthalten. Zählt man alle diese Drehungen zusammen, so bekommt man $1 + 4 \cdot 2 + 3 \cdot 1 = 12$. Die Gruppe aller Drehungen des (durch F_2 erzeugten) Tetraeders hat also, wie vorausgesagt, 12 Elemente. Es gilt $\mathcal{T} \cong \mathfrak{A}_4$.

• Analog gehen wir in dem Fall $(n_1, n_2, n_3; N) = (2,3,4;24)$ vor. Wir zeigen, dass die kleinste der G-Bahnen in F, nämlich F_3 mit $|F_3| = 6$, die Ecken eines Oktaeders sind. Die Isotropieuntergruppe G_3 eines Punktes $z_3 \in F_3$ zyklisch von Ordnung $n_3 = 4$: $G_3 = \langle D_w \rangle$. Die Operation von solchem G_3 auf $F_3 \setminus \{z_3\}$ zeigt, dass $F_3 \setminus \{z_3\}$ eine G_3-Fixpunkt y_3 und 4 weitere äquidistante Punkte x_j enthält, die dann auf Grund von geometrischen Überlegungen genau auf dem Schnitt der zu $\overline{z_3 y_3}$ orthogonalen Ebene mit S liegen muss (andernfalls würden die Isotropieuntergruppen G_{x_j} nicht die Punkte in $F_3 \setminus \{x_j\}$ invariant lassen). Untersucht man die Operation von G_{x_j} auf F_3 folgern wir, dass die Abstände von je zwei nicht gegenüber liegenden Punkten aus F_3 alle gleich sind. Damit ist bewiesen, dass F_3 die Menge der Ecken eines Oktaeders ist. Die Menge aller Drehungen dieses Oktaeders hat die nummerische Invariante $(2,3,4;24)$ was sich direkt bestätigen läßt . (F_2 besteht aus den Ecken eines Würfels und F_1, der Durschnitt aller 6 Drehgeraden, die durch die Mittelpunkten von gegenüberliegenden Kanten des Würfels $W(F_2)$ laufen, die Ecken eines Archimedischen Körpers sind). Es gilt $\mathcal{O} \cong \mathfrak{S}_4$.

• Für $(n_1, n_2, n_3; N) = (2, 3, 5; 60)$ schließlich läßt sich zeigen, dass die kleinste G-Bahn in F, F_3, genau aus den 12 Ecken eines Ikosaeders besteht (und F_2 aus den 20 Ecken eines Dodekaeders) Die Gruppe aller Drehungen dieses Ikosaeders stimmt mit der Gruppe aller Drehungen des Dodekaeders $D(F_2)$. Die Berechnung der Ordnungen der entsprechenden Isotropieuntergruppen bestätigt, dass die nummerische Invariante dieser Gruppe (2,3,5;60) ist. Es gilt $\mathcal{I} \cong \mathfrak{A}_5$.

Die Klassifikation der endlichen Untergruppen von SO(3) ist der Hauptschritt in der Klassifikation der endlichen Untergruppen von $\mathbf{B}(\mathbb{A}^3)$. Der Fixpunktsatz 1.3.3 besagt, dass eine solche endliche $G < \mathbf{B}(\mathbb{A}^3)$ dann schon die Untergruppe einer Punktgruppe $\mathrm{O}_P \cong \mathrm{O}(3)$ ist. Die Zerlegung $\mathrm{O}(3) = \mathrm{SO}(3) \dot\cup (-\mathrm{Id})\cdot \mathrm{SO}(3)$ in Drehungen und (Dreh)Spiegelungen liefert einen Hinweis auf möglich Konstruktion von endlichen Untergruppe, die nicht ganz in SO(3) liegen: Für jede endliche Untergruppe $N < \mathrm{SO}(3)$ ist $\widehat{N} := N \cup (-\mathrm{Id})\cdot N$ eine endliche Untergruppe von O(3), die nicht in SO(3) enthalten ist. Für jede Untergruppe $G \subset \mathrm{O}(3)$ ist $G_{\mathrm{SO}} := G \cap \mathrm{SO}(3)$ ein Normalteiler in G, der entweder mit G übereinstimmt (falls $G \subset \mathrm{SO}(3)$) oder es gilt $[G, G_{\mathrm{SO}}] = 2$ (falls $G \not\subset \mathrm{SO}(3)$). Leider sind nicht alle (endlichen) Untergruppen von O(3) dieser Gestalt: Es existieren Gruppen $G \subset \mathrm{O}(3)$, $G \not\subset \mathrm{SO}(3)$, so dass $-\mathrm{Id} \notin G$. Zu jeder solchen Gruppe konstruieren wir jetzt die folgende Untergruppe $G^\vee$ von SO(3):

$$G^\vee = G_{\mathrm{SO}} \quad \cup \quad (-\mathrm{Id})\cdot(G \smallsetminus G_{\mathrm{SO}})$$

Umgekehrt, zu jeder Untergruppe $H < \mathrm{SO}(3)$, die einen Normalteiler $N \lhd H$ vom Index 2 enthält, ist

$$H^\wedge := N \quad \cup \quad (-\mathrm{Id})\cdot(H \smallsetminus N)$$

eine Untergruppe von O(3), die nicht in SO(3) enthalten ist, und $-\mathrm{Id} \notin H^\wedge$. Diese beiden Konstruktionen sind dual zueinander in dem folgenden Sinne: Die Abbildungen

$$\begin{array}{ccc} G & \xrightarrow{\ \alpha\ } & G^\wedge \\ \left\{ \begin{array}{c} G < \mathrm{SO}(3) \text{ endlich,} \\ \text{enthält } N \lhd G \text{ mit } [G:N] = 2 \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} G < \mathrm{O}(3),\ G \not\subset \mathrm{SO}(3) \\ \text{endlich;}\ \ -\mathrm{Id} \notin G \end{array} \right\} \\ H^\vee & \xleftarrow{\ \beta\ } & H \end{array}$$

sind Bijektionen mit $\alpha \circ \beta = \mathrm{Id}$, $\beta \circ \alpha = \mathrm{Id}$.

Theorem 1.4.7. *Es sei G eine endliche Untergruppe von* O(3). *Dann ist G entweder bereits eine Untergruppe von* SO(3) *(siehe dann* 1.4.6*) oder $G \not\subset$ SO(3). In dem letzten Fall sind genau zwei Fälle möglich:*

(i) $-\mathrm{Id} \in G$. *Dann gilt $G = H \cup (-\mathrm{Id})H$ wobei $H \subset$ SO(3) eine beliebige Untergruppe aus der Liste in* 1.4.6 *sein kann.*

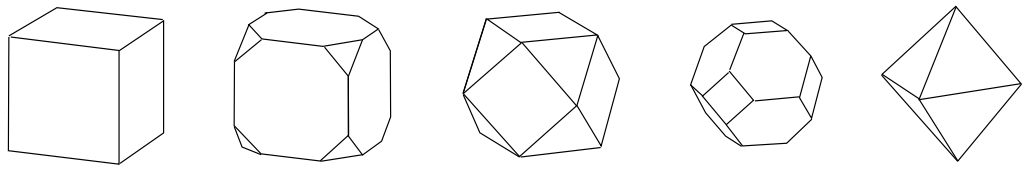
(ii) $-\mathrm{Id} \notin G$. *Dann gilt $G = H^\wedge$ wobei $H \subset$ SO(3) und $H \in \{\mathbb{Z}_{2k}, \mathcal{D}_k, \mathcal{O}\}$ ($k \in \mathbb{N}$ beliebig).*

Für eine Klassifizierung aller diskreten Untergruppen von $\mathbf{B}(\mathbb{R}^3)$ benutzt man dieselben Methoden wie bereits in dem 2-dimensionalen Fall. Die Zerlegung 1.3.11 liefert uns für ein $\Gamma \subset \mathbf{B}(\mathbb{R}^3)$ die diskrete Untergruppe $\mathbf{T}_\Gamma \subset \mathbb{R}^3$ und die Punktgruppe $\overline{\Gamma} = \mathrm{pr}(\Gamma) \subset \mathrm{O}(3)$. Anders als in dem 2-dimensionalen Fall kann es ab $\dim \mathbb{A} \geq 3$ passieren, dass das Bild $\overline{\Gamma}$ einer diskreten Untergruppe $\Gamma < \mathbb{B}(\mathbb{R}^n)$ nicht mehr diskret in $\mathrm{O}(n)$ ist. Den wichtigsten Speziallfall von diskreten Unterhruppen bilden die sog. *kristallographischen Gruppen*, d.h., diskrete Untergruppen Γ mit $\mathbf{T}_\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \mathbb{Z}v_3$. In diesem Fall ist $\overline{\Gamma}$ automatisch diskret und daher endlich. Solche Gruppen Γ treten als Isometriegruppen von (idealen) Kristalen auf und $\overline{\Gamma}$ ist sehr hilfreich un die sog. Form eines Kristalls zu charakterisieren:

Ein gutes Näherungsmodell eines Kristalls ist das Kästchenmodell, in dem man sich ein Kristall aus den sich in 3 (linear unabhängigen) Richtungen wiederholenden identischen Elementarzellen aufgebaut

denkt. Jede solche Elementarzelle ist ein Spat, der noch eine gewisse Konstellation von Atomen, die die gegebene kristalline Substanz konstituieren, beinhaltet. Mathematisch gesehen haben wir hier also mit einer 3-dimensionalen Parkettierung $\bigcup M_j$ zu tun, wobei alle M_j-s kongruente Spate, die noch zusätzlich mit einer Markierung (Atomstruktur) versehen sind. Genauso wie die diskreten Untergruppen von $\mathbf{B}(\mathbb{R}^2)$ Isometriegruppen von (periodischen) Friesen und Mosaiken sind, so sind die kristallographischen Untergruppen Isometriegruppen von (idealen, unendlich ausgedehnten) Kristallen.

Es sei $\Gamma \subset \mathbf{B}(\mathbb{R}^3)$ die Isometriegruppe eines solchen idealen Kristalls und $\overline{\Gamma} \subset \mathrm{O}(3)$ die zugehörige Punktgruppe. Mit Hilfe dieser endlichen Gruppe lassen sich verschiedene Formen von Kristallen und deren Symmetrien sehr effizient beschreiben. Das werde wir im Folgenden näher erläutern:
Die in der Natur vorkommenden Kristalle sind beschränkte Teilmengen und haben in ihrer reinen Form oft die Gestalt eines relativ komplizierten, meist konvexen Polyeders. So unterschiedlich auch die einzelnen Kristalle einer Substanz aussehen mögen, die Winkel zwischen den verschiedenen Wänden des Kristalls bleiben jedoch immer gleich. Das ist ein von Huygens und Steno entdecktes kristallographisches Gesetz. Statt die Winkel zwischen den Wänden zu betrachten, geht man äquivalent zu dem Normalenbild über, d.h., man betrachtet den normalen Halbstrahl zu jeder Seitenfläche und deren Durchschnitt mit der Einheitssphäre S^2. Die zu einem Kristall auf diese Weise assoziierte endliche Punktmenge $F \subset S^2$ läßt sich auch als die Bahn einer endlichen Gruppe $\overline{\Gamma} < \mathrm{O}(3)$ beschreiben. Das wollen wir an dem folgenden
Beispiel illustrieren. Das Kochsalz NaCl kristallisiert unter Laborbedingungen in Form eines perfekten Würfels, z.B. mit den Ecken in den Punkten $(\pm 1, \pm 1, \pm 1)^T$. Die Normalenbilder der Seitenflächen konstituieren dann die Menge $F_1 = \{(\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)\}$. Die Elementarzellen von NaCl sind ebenfalls Würfel, aus denen das ganze Kristall aufgebaut ist. Die Gruppe aller Isometrien des Würfels ist die 48-elementige Gruppe $\mathcal{O}_h$ und F_1 ist die $\mathcal{O}_h$-Bahn eines ihrer Punkte. NaCl kristallisiert auch in anderer Gestalt: Nach Beigabe von kleinen Mengen von Harnstoff erscheinen in den Ecken der würfelartigen NaCl-Kristallen kleine reguläre Dreiecke. Als immer mehr Harnstoff beigegeben wird, werden die Dreiecke immer größer und öffnen sich zu 6-Ecken bis schließlich ein Oktaeder entsteht, siehe Zeichnung.



Die Normalenbilder bestehen dann für die mittleren 3 Mischformen aus den beiden Bahnen F_1 und $F_2 = \{\frac{1}{\text{Länge}}(\pm 1, \pm 1, \pm 1)^T\} = \mathcal{O}_h \cdot \frac{1}{\text{Länge}}(1, 1, 1)^T$ während die "reine" Form des Oktaeders F_2 als das Normalenbild hat.

Es gibt natürlich noch andere $\mathcal{O}_h$-Bahnen auf der Einheitssphre S^2. Abhängig von den entsprechenden Isotropieuntergruppen $(\mathcal{O}_h)_{(x,y,z)}$ lassen sich all diese Bahnen in endlich viele Typen unterteilen, (je nach Konjugationsklasse der Isotropieuntergruppe). Z.B. wenn die Komponenten in $(x, y, z)^T$ paarweise verschieden und $\neq 0$ sind, erhält man die (sog. generischen) $\mathcal{O}_h$-Bahnen mit trivialer Isotropiegruppe: Jede solche Bahn besteht dann aus 48 Punkten. Nicht jede solche theoretisch mögliche Bahn $\mathcal{O}_h \cdot (x, y, z)^T$ erscheint auch als das Normalenbild von Seitenflächen eines Kristalls: Das von Haüy entdeckte Gesetz der rationalen Verhältnisse besagt, dass die tatsächlich auftretende $\mathcal{O}_h$-Bahnen Basispunkte der Gestalt $\frac{1}{\text{Länge}}(x, y, z)^T$ haben, wobei x, y, z nur kleine ganze Zahlen sein können. Diese Rationalität der Verhältnisse x/y, x/z etc. folgt direkt aus dem Kästchenmodell.

Außer der Gruppen $\mathcal{O}$ und $\mathcal{O}_h$ gibt es noch weitere Untergruppen $\overline{\Gamma}$, die als Punktgruppen von kristallographischen Gruppen Γ auftauchen. Da auch in dem dreidimensionalen Fall die Gruppen $\overline{\Gamma}$ der kristallographischen Einschränkung 1.3.13 unterliegen, kann man zeigen, dass es
• genau 32 Konjugationsklassen von endlichen Untergruppe $H < \mathrm{O}(3)$ mit $H = \overline{\Gamma}$ (Γ kristallographisch) gibt, vgl. auch 1.4.7.

Bei den eigentlichen kristallographischen Gruppen ist die Lage komplizierter. Man kan beweisen, dass es

• 230 Konjugationsklassen von $\Gamma < \mathbf{B}(\mathbb{R}^3)$ gibt, wobei hier nur mit orientierungserhaltenden Elementen von $\mathbf{B}(\mathbb{R}^3)$ konjugiert wird. Immerhin gibt es

• 219 Konjugationsklassen von kristallographischen $\Gamma < \mathbf{B}(\mathbb{R}^3)$, wenn man mit beliebigen Elementen aus $\mathbf{B}(\mathbb{R}^3)$ konjugieren darf.

Man betrachte zum Vergleich die Situation in $\mathbb{R}^2$. Die zweidimensionalen kristallographischen Gruppen bilden 17 Isomorphieklassen, die auch mit den Konjugationsklassen übereinstimmen. In dem vorliegenden dreidimensionalem Fall gibt es isomorphe, jedoch nicht konjugierte kristalographische Untergruppen in $\mathbf{B}(\mathbb{R}^3)$.

2. Zahlbereiche und die Galoistheorie

2.1. Elementare Zahlbereiche

Natürliche Zahlen. Die Zahlen 1,2,3,... sind ein fester Bestandteil unseres täglichen Lebens. Sie sind so selbstverständlich und elementar, dass sie in der Mathematik nicht aus anderen Objekten hergeleitet werden, sondern deren Existenz axiomatische postuliert wird. Eine mögliche axiomatische Definition der natürlichen Zahlen benutzt das Induktionsprinzip und die Anordnung $1 \to 2 \to 3 \to \cdots$

Peanosche Axiome 2.1.1. *Es sei $\mathcal{N}$ eine Menge zusammen mit einer Abbildung $\nu : \mathcal{N} \to \mathcal{N}$. Wir nennen $\nu(x)$ den Nachfolger von $x \in \mathcal{N}$. Es gelte weiter*

P1. Es existier ein Element $1 \in \mathcal{N}$, so dass $1 \notin \nu(\mathcal{N})$

P2. Gilt $\nu(x) = \nu(y)$ so folgt $x = y$

P3. **(Induktionsprinzip)** *Es sei $\mathcal{M} \subset \mathcal{N}$ eine Teilmenge, die die folgenden Bedingungen erfüllt:*

- *$1 \in \mathcal{M}$*
- *Falls $z \in \mathcal{M}$. so auch $\nu(z) \in \mathcal{M}$.*

Dann gilt $\mathcal{M} = \mathcal{N}$.

Je zwei solche Mengen sind isomorph. Die Existenz solcher Menge wird postuliert. Es bezeichne $\mathbb{N}$ eine Menge, die die Peanosche Axiome erfüllt. Eine mögliche mengentheoretische Konstruktion von $\mathbb{N}$ baut auf der leeren Menge auf und konstruiert iterativ neue Mengen:

$$1 = \{\varnothing\},\ \{\varnothing,\ \{\varnothing\}\},\ \{\varnothing,\ \{\varnothing\},\ \{\varnothing,\ \{\varnothing\}\}\},\ \{\varnothing,\ \{\varnothing\},\ \{\varnothing,\ \{\varnothing\}\},\ \{\varnothing,\ \{\varnothing\},\ \{\varnothing,\ \{\varnothing\}\}\}\},\ldots$$

wobei die Nachfolgerbildung die Operation $\nu(M) = M \cup \{M\}$ ist. Aus den Peano-Axiomen folgt auch, dass jedes Element $n \in \mathcal{N} \setminus \{1\}$ die Gestalt $\nu \circ \nu \circ \vdots \circ \nu(1)$ hat (endlich viele iterierte Anwendungen von ν)

Auf einer solchen Menge läßt sich eine Addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ und eine Multiplikation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ wie folgt rekursiv definieren.

Definition 2.1.2. (Addition)

A1 $x + 1 := \nu(x)$ für jedes $x \in \mathbb{N}$.

A2 $x + \nu(y) := \nu(x + y)$ für alle $x, y \in \mathbb{N}$.

Definition 2.1.3. (Multiplikation)

M1 $x \cdot 1 := x$ für jedes $x \in \mathbb{N}$.

M2 $x \cdot \nu(y) := x \cdot y + x$ für alle $x, y \in \mathbb{N}$.

Man kann zeigen, dass die durch die obige rekursive Definition festgelegte Addition sowie Multiplikation auf $\mathbb{N}$ wohldefiniert und eindeutig bestimmt sind.

Definition 2.1.4. (Ordnungsrelation) Für zwei Elemente $x, y \in \mathbb{N}$ wird die folgende Relation festgesetzt:

$$x < y \overset{\text{Def}}{\iff} \exists\, n \in \mathbb{N} \text{ mit } y = x + n$$

Man definiere weiter die Relation "$x \leq y$" wenn entweder $x = y$ oder $x < y$ gilt.

Bem. "$\leq$" ist eine Ordnungsrelation auf $\mathbb{N}$.

Dabei heißt eine Relation "$\preceq$" auf einer Menge $\mathcal{M}$ eine *partielle Ordnungsrelation* oder *Halbordnung*, falls für alle $x, y, z \in \mathcal{M}$ die folgenden Bedingungen erfüllt sind:

O1 $x \preceq x$.
O2 $x \preceq y$ und $y \preceq x$ impliziert $x = y$.
O3 $x \preceq y$ und $y \preceq z$ impliziert $x \preceq z$.

Eine Halbordnung heißt *total,* falls für jedes Paar $x, y \in \mathcal{M}$ entweder $x \preceq y$ oder $y \preceq x$ gilt. Ein Element $m \in \mathcal{A} \subset \mathcal{M}$ heißt *maximal* [minimal] in $\mathcal{A}$, falls für alle $a \in \mathcal{A}$ $a \preceq m$ [bzw. $m \preceq a$] gilt. Eine Teilmenge $\mathcal{A}$ einer geordneten Menge $\mathcal{M}$ muss keine maximale oder minimale Elemente besitzen. Gibt es ein Maximum [ein Minimum] in $\mathcal{A}$, so ist es eindeutig bestimmt (Folgerung aus der Antisymmetrie von $\preceq$). Gilt für ein $c \in \mathcal{M}$ $a \preceq c$ für alle $a \in \mathcal{A}$, so heißt c eine *obere Schranke* von $\mathcal{A}$. (Analoge Def. für eine "untere Schranke"). Besitzt die Menge aller oberen Schranken von $\mathcal{A}$ ein *Minimum* M, so heißt solches $M \in \mathcal{M}$ das *Supremum* von $\mathcal{A}$. Analog heißt das Maximum m aller unteren Schranken von $\mathcal{A}$ (falls existent) ein *Infimum* von $\mathcal{A}$.

Beispiele.
• Es sei X eine Menge und $M := 2^X$ deren Potenzmenge (d.h., die Menge aller Teilmengen). Auf M ist durch die Vorschrift $A \preceq B \overset{\text{Def}}{\iff} A \subset B$ eine partielle Ordnungsrelation definiert, die nicht total ist, falls $|X| \geq 2$ gilt.
• Auf $\mathbb{N} = (\mathcal{N}, \nu)$ ist durch die Vorschrift $x \preceq y \overset{\text{Def}}{\iff} x = y$ oder $\exists z \in \mathcal{N}$ mit $x + z = y$ eine totale Ordnung auf $\mathbb{N}$ definiert.
• Die Menge $\{q \in \mathbb{Q} : q < \sqrt{2}\}$ besitzt weder ein Maximum noch ein Supremum in $(\mathbb{Q}, <)$. Die Teilmenge $(0, 1] \subset (\mathbb{R}, <)$ hat ein Supremum (1), ein Maximum (1) und ein Infimum (0) aber kein Minimum in $\mathbb{R}$.

A priori ist es nicht klar, dass die in 2.1.2 und 2.1.3 definierte Verknüpfungen assoziativ oder kommutativ sind. Das läßt sich aber direkt aus den Peanoschen Axiomen und unseren Verknüpfungsdefinitionen herleiten:

2.1.5. $+$ *aus* 2.1.2 *ist assoziativ*, d.h. $(x + y) + z = x + (y + z)$ für alle $x, y, z \in \mathbb{N}$.
Um das zu zeigen, betrachten wir die Menge $\mathcal{M}$ aller $z \in \mathcal{N}$, für die die obige Gleichung für beliebige $x, y \in \mathbb{N}$ gilt.
• $1 \in \mathcal{M}$, da $x + (y + 1) \overset{A1}{=} x + \nu(y) \overset{A2}{=} \nu(x + y) \overset{A1}{=} (x + y) + 1$.
• Angenommen, $m \in \mathcal{M}$. Das ist unsere Induktionsvoraussetzung IV. Wir zeigen, dass dann auch $\nu(m) \in \mathcal{M}$ gilt:

$$x + (y + \nu(m)) \overset{A2}{=} x + \nu(y + m) \overset{A2}{=} \nu(x + (y + m)) \overset{\text{IV}}{=} \nu((x + y) + m) = \overset{A2}{=} (x + y) + \nu(m)$$

Damit gilt nach P3 $\mathcal{M} = \mathcal{N}$ und die Identität $(x + y) + z = x + (y + z)$ gilt für alle $x, y, z \in \mathbb{N}$.

2.1.6. $+$ *aus* 2.1.2 *ist kommutativ*,
Zunächt beweise man, dass $x + 1 = 1 + x$ für alle $x \in \mathbb{N}$ gilt. Das kann man entweder mit Hilfe der Induktion beweisen, oder die Tatsache benutzen, dass $x = \nu \circ \cdots \circ \nu(1) =: \nu^k(1)$ gilt. Dann gilt:

$$\begin{aligned} 1 + x = 1 + \nu^k(1) &\overset{A2}{=} \nu(1 + \nu^{k-1}(1)) \overset{A2}{=} \nu^2(1 + \nu^{k-2}(1)) = \cdots \\ &= \nu^k(1 + 1) \overset{A1}{=} \nu^{k+1}(1) = \nu \circ (\nu^k(1)) \overset{A1}{=} \nu^k(1) + 1 = x + 1 \end{aligned}$$

Wir nutzen hier die Assioziativität von Abbildungsverknüpfungen. Jetzt beweisen wir durch Induktion, dass auch $x + y = y + x$ für alle $x, y \in \mathbb{N}$: Es sei dazu $\mathcal{M} = \{y \in \mathcal{N} : x + y = y + x \ \forall x \in \mathbb{N}\}$, Wie bereits gezeigt $1 \in \mathcal{M}$. Die Induktionsvoraussetzung ist nun $x + y = y + x$ für alle $x \in \mathbb{N}$ und ein $y \in \mathbb{N}$. Dann folgt

$$x + \nu(y) \overset{A2}{=} \nu(x + y) \overset{[\text{IV}]}{=} \nu(y + x) \overset{A2}{=} y + \nu(x) \overset{A1}{=} y + (x + 1) \overset{\text{Teil 1}}{=} y + (1 + x) \overset{2.1.5}{=} (y + 1) + x \overset{A1}{=} \nu(y) + x$$

uns somit nach P3 $\mathcal{M} = \mathbb{N}$, d.h., $+$ ist eine assoziative und kommutative Verknüpfung.

Analog beweist man die Assoziativität und Kommutativität von "$\cdot$".

Kardinalzahlen. In der Klasse aller Mengen (der Begriff "Menge aller Mengen" führt zu Widersprüchen) definieren wir die folgende Relationen:

$$A \text{ gleichmächtig mit } B \overset{\text{Def}}{\iff} \exists \text{ Bijektion } \psi : A \to B$$

Diese Relation ist eine Äquivalenzrelation und die Äquivalenzklasse $[A]_{\text{glchmtig}}$ wird mit $|A|$ bezeichnet und heißt die *Kardinalzahl* von A. Ferner definiere man die folgende Relation auf der Klasse aller Kardinalzahlen:

$$A \preceq B \overset{\text{Def}}{\iff} \exists \text{ Injektion } \psi : A \to B$$

Diese Relation ist eine Ordnungsrelation. Die Reflexivität und die Transitivität folgen sofort aus der Def. Viel schwieriger ist es die Antisymmetrie O2 nachzuweisen. Das ist der Inhalt des Satzes von Bernstein-Schröder.

Wir schreiben n (aus $\mathbb{N}$) für die Kardinalzahl der Menge $\{x \in \mathbb{N} : x \leq n\}$ und nennen es endlich. Ist $A \neq \varnothing$ und $|A| \neq n$ für alle $n \in \mathbb{N}$, so heißt A unendlich. Eine Menge A ist genau dann unendlich wenn es eine echte Teilmenge $B \subsetneq A$ und eine Injektion $\psi : A \to B$ gibt. $\aleph_0 := |\mathbb{N}|$.

Weder $(\mathbb{N}, +)$ noch $(\mathbb{N}, \cdot)$ ist eine Gruppe. Man fügt daher zunächst ein neues Element, genannt 0, hinzu und definiert für alle $n \in \mathbb{N} \cup \{0\}$:

$0 + n := n + 0 := n$

$0 \cdot n := n \cdot 0 := 0$

Um 0 zu einem neutralen Element in einer Gruppe zu machen, fügt man zu jedem $n \in \mathbb{N}$ noch ein inverses Element, genannt $-n$, hinzu, d.h., man fordert $n + (-n) := (-n) + n = 0$. Dann definiert man für alle $m, n \in \mathbb{N}$

$$(-m) + (-n) := -(m + n)$$

sowie
$$m + (-n) := (-n) + m = \begin{cases} k & \text{falls } m = n + k \\ -k & \text{falls } n = m + k \\ 0 & \text{falls } m = n \end{cases}$$

$$(-m) \cdot (-n) := m \cdot n$$

$$(-m) \cdot n := n \cdot (-m) := -(m \cdot n)$$

Bem. Die Menge $\mathbb{Z} := \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$ zusammen mit den beiden oben definierten Verknüpfungen ist ein kommutativer Ring mit 1, d.h., $(\mathbb{Z}, +)$ ist eine abelsche Gruppe, $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ist eine kommutative Verknüpfung (genannt Multiplikation), so dass $(+, \cdot)$ das Distributivgesetz erfüllen und die Multiplikation noch ein neutrales Element (nämlich 1) hat.

Der Quotientenkörper. Ein kommutativer Ring $(A, +, \cdot)$ heißt *nullteilerfrei* oder ein *Integritätsbereich*, falls jede Gleichung $a \cdot b = 0$ entweder $a = 0$ oder $b = 0$ nach sich zieht.

Lemma 2.1.7. *Zu jedem nullteilerfreien Ring A mit 1 gibt es einen Körper $Q = Q(A)$, den sog. Quotientenkörper von A, der die folgenden Eigenschaften hat:*
Q1. Es gibt einen injektiven Ringhomomorphismus $\psi : A \to Q$ mot $\psi(1_R) = 1_Q$
Q2. Jedes $r \in A \setminus \{0\}$ hat ein Inverses r^{-1} in Q (d.h., $r \cdot r^{-1} = r^{-1} \cdot r = 1_Q$).
Q3. Jedes Element x in Q hat die Gestalt $r \cdot s^{-1}$ für gewisse $r, s \in R$.

Der Körper $Q(A)$ ist durch die obigen Bedingungen bis auf Isomorphie eindeutig bestimmt und läßt sich wie folgt konstruieren: Auf der Menge aller Paare aus $A \times (A \setminus \{0\})$ definiert man die folgende Äquivalenzrelation

$$(a, b) \sim (c, d) \overset{\text{Def}}{\iff} ad = bc$$

Auf der Grundmenge $Q(A) := \big(A \times (A \setminus \{0\})\big)/_\sim$ definert man die folgenden Operationen

$$+ : Q \times Q \to Q, \quad (a,b) + (c,d) := (ad + bc, bd); \qquad \cdot : Q \times Q \to Q, \quad (a,b) \cdot (c,d) := (ac, bd)$$

Man überprüft leicht, dass + und · zwei Verknüpfungen sind, die $Q(A)$ zu einem Körper machen. Schreibt man $\frac{a}{b}$ für die Äquivalenzklasse des Paares (a,b) so ist $\frac{0}{1}$ das neutrale Element der Addition "+" und $\frac{1}{1}$ das neutrale Element der Multiplikation "·". Die Abbildung $\psi : A \to Q$, $a \mapsto \frac{a}{1}$ ist ein injektiver Ringhomomorphismus, $\frac{1}{r}$ ist das zu $r \in A$ inverses Element und jedes $q \in Q$ hat die Gestalt

$$q = \frac{r}{s} = r \cdot \frac{1}{s} = r \cdot s^{-1} \qquad r, s \in A$$

Hat noch A eine mit den Verknüpfungen kompatible Ordnung $<$ so gilt das auch für den Quotientenkörper von A: Man definiere $Q_+ := \{\frac{a}{b} : a > 0, b > 0\}$ und $\frac{a}{b} < \frac{c}{d} \overset{\text{Def}}{\iff} \frac{c}{d} - \frac{a}{b} \in Q_+$ gilt. Diese Ordnungsrelation ($\leq$) ist total und macht den Quotientenkörper zu einem geordneten Körper, d.h., es gilt

GK1 $\forall x, a, b \in Q \ \wedge \ a < b$ folgt $a + x < b + x$.

GK1 $\forall a, b \in Q$ mit $0 < a, \ 0 < b$ folgt $0 < ab$.

Reelle Zahlen. Nicht alle natürlich auftretenden Größen, wie etwa Diagonalen eines Quadrats oder eines Würfels mit rationaler Kantenlänge, Nullstellen von Polynomen mit rationalen Koeffizienten etc. sind rational. Es war daher notwendig den Zahlbereich weiter zu erweitern und führte zur Konstruktion von reellen Zahlen. Axiomatisch lassen sich die reelle Zahlen folgendermaßen charakterisieren:

Definition 2.1.8. Ein *Dedekindscher Schnitt* $(A|B)$ in einer total geordneten Menge $\mathcal{R}$ besteht aus zwei nichtleeren Teilmengen A, B, so dass $A \cup B = \mathcal{R}$, $A \cap B = \varnothing$ $\forall\, a \in A, b \in B$ $a < b$. Eine *Trennungszahl* (*Schnittzahl*) $t = t(A|B)$ eines dedekindschen Schnittes ist ein Element $t \in \mathcal{R}$ mit $a \leq t \leq b$ für alle $a \in A, \ b \in B$.

2.1.9. Axiomatische Charakterisierung reeller Zahlen. Die reellen Zahlen sind eine Menge $\mathcal{R}$ zusammen mit zwei Verknüpfungen $+ : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$ (genannt Addition) und $\cdot : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$ (genannt Multiplikation) und einer ausgezeichneten Teilmenge $\mathcal{R}_+$ (deren Elemente 'positive Zahlen' heißen und auch mit $\{x > 0\}$ bezeichnet werden), so dass gilt:

RA1 $(\mathcal{R}, +)$ und $(\mathcal{R} \setminus \{0), \cdot)$ sind abelsche Gruppen.

RA2 **Distributivgesetz.**

$$\forall\, x, y, z \in \mathcal{R} \qquad x \cdot (y + z) = x \cdot y + x \cdot z$$

RA3 **Trichotomiegesetz.** Für jede reelle Zahl $x \in \mathcal{R}$ gilt genau eine der folgenden Relationen:

$$x \in \mathcal{R}_+, \qquad x = 0, \qquad -x \in \mathcal{R}_+ \, .$$

Wir schreiben hierfür abkürzend: $x > 0, \qquad x = 0, \qquad x < 0$

RA4 **Monotoniegesetze.** Für alle $x, y > 0$ gilt

$$x + y > 0, \qquad x \cdot y > 0$$

RA5 **Das Dedekindsche Schnittaxiom.** Jeder Dedekindsche Schnitt $(A|B)$ der Menge $\mathcal{R}$ besitzt eine Trennungszahl $t = t(A|B) \in \mathcal{R}$.

Die in einem angeordneten Körper $\mathcal{R}$ zu RA5 äquivalenten Bedingungen sind:

RA5' **Existenz von Suprema.** Jede nach oben beschränkte Teilmenge $M \subset \mathcal{R}$ hat ein Supremum $\sup(M) \in \mathcal{R}$.

RA5" Jede Cauchyfolge (x_n) aus $\mathcal{R}$ besitzt einen Grenzwert $\lim\limits_{n\to\infty} x_n \in \mathcal{R}$.

Je zwei Mengen $\mathbb{R}$ und $\mathcal{R}$, die die Axiome RA1–RA5 erfüllen, sind isomorph und der Körperisomorphismus $\varphi : \mathbb{R} \to \mathcal{R}$ erhält die Ordnungsrelation. $\mathbb{R}$ enthält einen zu $\mathbb{Z}$ isomorphen Unterring, nämlich

$$\{0, 1, 1+1, 1+1+1, \ldots\} \cup \{-1, -1+(-1), -1+(-1)+(-1), \ldots\}$$

und daher auch deren Quotientenkörper $\mathbb{Q}$.

In jedem vollständigen und angeordneten Körper $(\mathcal{R}, +, \cdot, \leq)$ gilt das
2.1.10. Archimedisches Axiom. Für jedes $x > 0$ gibt es ein $n \in \mathbb{N} \subset \mathcal{R}$ mit $n > x$.
(Äquivalent dazu gilt: $\forall\, \varepsilon \in \mathcal{R}_+\ \exists\, n \in \mathbb{N}$ mit $\frac{1}{n} < \varepsilon$.)

Konstruktion der reellen Zahlen. Auf der Menge $\mathcal{C}(\mathbb{Q})$ aller Cauchyfolgen $(q_n)_{n\in\mathbb{N}}$ rationaler Zahlen definiere man die folgende Äquivalenzrelation:

$$(q_n) \sim (p_n) \overset{\text{Def}}{\iff} \lim_{n\to\infty} (q_n - p_n) = 0$$

Es sei jetzt $\mathcal{R} := \mathcal{C}(\mathbb{Q})/\!\sim$. Dann definieren die unten stehenden Abbildungen

$$+ : \mathcal{R} \times \mathcal{R} \to \mathcal{R}, \quad ([(q_n)], [(p_n)]) \mapsto [(q_n + p_n)], \qquad \cdot : \mathcal{R} \times \mathcal{R} \to \mathcal{R}, \quad ([(q_n)], [(p_n)]) \mapsto [(q_n p_n)]$$

wohldefinierte assoziative Verknüpfungen auf $\mathcal{C}(\mathbb{Q})/\!\sim$.

Lemma 2.1.11. *Die Menge $\mathbb{R} := \mathcal{C}(\mathbb{Q})/\!\sim$, zusammen mit den beiden obigen Verknüpfungen "$+$" und "$\cdot$" sowie mit der Ordnungsrelation $\leq$, die durch die Teilmenge*

$$\mathbb{R}_+ := \{[x_n] : \exists\, N = N_{(x_n)} \in \mathbb{N} \textit{ mit } x_n \geq 0\ \forall\, n \geq N\ \wedge \lim_{n\to\infty} x_n \neq 0\}$$

festgelegt wird, ist ein Körper, der alle Axiome RA1-RA5 aus 2.1.9 *erfüllt, und damit bis auf Isometrie eindeutig bestimmt.*

Jeden, zu $\mathcal{C}(\mathbb{Q})/\!\sim$ isomorphen angeordneten Körper nennen wir einen Körper der reellen Zahlen.

Der Quotient $\mathcal{C}(\mathbb{Q})/\!\sim$ enthält den Körper der rationalen Zahlen: Die Abbildung $\jmath : \mathbb{Q} \to \mathcal{C}(\mathbb{Q})/\!\sim$, $q \mapsto [(q, q, q, ...)]$ ist ein injektiver Körperhomomorphismus.

Konstruktion der komplexen Zahlen. Der Wunsch eine "Zahl" i zur Verfügung zu haben, die die seltsame Eigenschaft $i^2 = -1$ besitzt, führte zu dem Körper der komplexen Zahlen. Eine solche Konstruktion, die von der Existenz des Körpers der reellen Zahlen ausgeht und ihn "verdoppelt" lautet: Es sei $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ die Grundmenge, auf der die folgenden Operationen eingeführt werden:

$$\oplus : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad (a_1, a_2) \oplus (b_1, b_2) := (a_1 + b_1\ ,\ a_2 + b_2)$$
$$\odot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad (a_1, a_2) \odot (b_1, b_2) := (a_1 b_1 - a_2 b_2\ ,\ a_1 b_2 + a_2 b_1)\ .$$

$\mathbb{C}$ zusammen mit den beiden Operationen ist ein Körper und die Abbildung $\jmath : (\mathbb{R}, +, \cdot) \to (\mathbb{C}, \oplus, \odot)$, $x \mapsto (x, 0)$ ist ein injektiver Körperhomomorphismus. Da $\oplus$ und $\oplus$ die gewöhnliche Addition bzw. Multiplikation in $\mathbb{R}$ aud $\mathbb{C}$ fortsetzen, werden wir ab jetzt diese Operationen in $\mathbb{C}$ auch mit "$+$" und "$\cdot$" bezeichnen.

Es gibt eine viel allgemeinere Konstruktion, in der $\mathbb{C}$ als ein Quotient des Polynomringes $\mathbb{R}[X]$ nach einem gewissen Teilraum $I \subset \mathbb{R}[X]$ entsteht. Wir wollen diesen Sachverhalt genauer klären.

2.2. Division in Euklidischen Ringen. Polynomringe.

Definitionen 2.2.1. Es sei R ein kommutativer Ring mit 1 und $q, r, s \in R$.
• $u \in \mathbb{R}$ heißt eine *Einheit*, falls u in $(R \setminus \{0\}, \cdot)$ invertierbar ist. Wir werden mit $R^\times$ die Menge aller (multiplikativen) Einheiten bezeichnen.
• Zwei Elemente $r, s \in R$ heißen *(zueinander) assoziiert*, falls es ein $u \in R^\times$, so dass $s = ur$ gilt.
• r heißt ein *Teiler* von s in R (in Zeichen $r|s$), falls es ein $q \in R$ mit $s = r \cdot q$ gilt.
• Es seien $r_1, .., , r_k \in R$. Ein Element $s \in R$ heißt *größter geminsamer Teiler* (in Zeichen $s = \mathrm{ggT}(r_1, \dots, r_k)$), falls $s|r_1, \dots, s|r_k$ und für jedes weitere $t \in R$ mit $t|r_1$, $t|r_2, \dots, t|r_k$ auch noch $t|s$ gilt. Es gibt Ringe, in denen kein ggT von beliebig vorgegebenen Elementen zu existieren braucht.
• r heißt *irreduzibel*, falls r keine Einheit ist und die einzigen Teiler von r die Einheiten, oder die zu r assoziierte Elemente sind.
• p heißt *prim*, falls p keine Einheit ist und für alle $q, s \in R$ mit $p|qs$ entweder $p|q$ oder $p|s$ folgt. Jedes Primelement ist irreduzibel. Es gibt aber Ringe, in denen irreduzible Elemente nicht prim sind.
• Ein *Euklidischer Ring* ist ein nullteilerfreier kommutativer Ring, zusammen mit einer Abbildung $\nu : R \setminus \{0\} \to \mathbb{N}_0$, so dass für alle $p \in R, q \in R \setminus \{0\}$ es Elemente $r, s \in R$ mit der folgenden Eigenschaften gibt:

$$p = sq + r \qquad \text{und } \nu(r) < \nu(q)$$

Definition 2.2.2. Es sei R ein kommutativer Ring. Es sei $I \subset R$ ein Unterring, d.h., eine Teilmenge, die eine Untergruppe von $(R, +)$ ist und abgeschlossen bzgl. der Multiplikation "$\cdot$" in R ist. I heißt ein *Ideal* in R (in Zeichen $I \lhd R$), falls für alle $r \in R$, $s \in I$ auch noch $r \cdot s \in I$ gilt.

Bem. Ist $I \lhd R$ ein Ideal in R so hat der Quotient R/I eine Ringstruktur: Die unten stehenden Abbildungen, Addition und Multiplikation,

$$\begin{array}{rccc} +: & R/I & \times & R/I \longrightarrow R/I \\ & (r+I & , & s+I) \mapsto r+s+I \end{array} \qquad \begin{array}{rccc} \cdot: & R/I & \times & R/I \longrightarrow R/I \\ & (r+I & , & s+I) \mapsto r\cdot s+I \end{array}$$

sind wohldefiniert und definieren die beiden Verknüpfungen auf R/I, die diesen Quotienten zu einem Ring machen.
• Ein Ring heißt ein Hauptidealring, falls jedes Ideal J in R ein Hauptideal ist, d.h., ein Ideal, das durch nur ein Element erzeugt ist ($J = R \cdot s = ((s))$).

Beispiel: Polynomring über R. Es sei R ein kommutativer Ring mit 1. Ein Polynomring über R besteht aus allen Folgen $(r_0, r_1, r_2, ...)$ der Elemente aus R, von denen höchstens endlich viele $\neq 0$ sind. Jede solche Folge nennen wir ein *Polynom* in/über R. Die Menge aller Polynome hat eine Ringstruktur: Die Verknüpfungen sind dann folgendermaßen definierT:

$$(r_0, r_1.r_2, \dots) + (s_0, s_1.s_2, \dots) := (r_0 + s_0, r_1 + s_1.r_2 + s_2, \dots)$$

sowie

$$(r_0, r_1.r_2, \dots) \cdot (s_0, s_1.s_2, \dots) := (t_0, t_1, t_2, \dots) \qquad \text{mit} \quad t_k = \sum_{j=0}^{k} r_j s_{k-j} \, .$$

So ist $(1, 0, 0, ...)$ das Einselement in diesem Ring und es gilt $(0, 1, 0, 0, ...)^k = (0, \dots, 0, 1, 0, ...)$ (1 an der k-ten Stelle). Man benutzt daher die Abkürzung $X := (0, 1, 0, 0, ...)$. Jedes Polynom kann dann in der folgenden Gestalt geschrieben werden:

$$(r_0, r_1, r_2, ...) = r_0 + r_1 X + r_2 X^2 + \cdots + r_n X^n \, .$$

Die ganze Zahl $\mathrm{Grad}(P) := n := \max\{j \in \mathbb{N}_0 : r_j \neq 0\}$ nennt man den *Grad* des Polynomes $P = (r_0, r_1, r_2, ...)$. Vereinbarungsgemäß definieren wir $\mathrm{Grad}(0) = -\infty$. Den obigen Polynomring bezeichnen wir mit $R[X]$. (Natürlich kann man für das Element $(0, 1, 0, 0, \ldots)$ auch jeden anderen Buchstaben verwenden und z.B. $R[Y], R[Z], R[T]$ etc. schreiben.) Es gilt für beliebige Polynome über einen nullteilerfreien Ring:

$$\mathrm{Grad}(P \cdot Q) = \mathrm{Grad}(P) + \mathrm{Grad}(Q) \qquad \mathrm{Grad}(P + Q) \leq \max\{\mathrm{Grad}(P), \mathrm{Grad}(Q)\}$$

Ist der Leitkoeffizient $a_n = 1$ des Polynomes Q mit $\mathrm{Grad}(Q) = n$, so heißt das Polynom Q *normiert*.

Es sei jetzt R ein kommutativer Ring und A eine R-Algebra, d.h., ein (nicht notwendigerweise kommutativer) Ring $(A, +, \circ)$ mit einer "Skalarmultiplikation" $\cdot : R \times A \to A$, so dass $\forall\, r, s \in R,\ a, b \in A$ gilt:

$$r{\cdot}(a + b) = r{\cdot}a + r{\cdot}b, \quad (r + s){\cdot}a = r{\cdot}a + s{\cdot}a \quad \text{und} \quad r(a \circ b) = (r{\cdot}a) \circ b = a \circ (r{\cdot}b), \quad 1_R{\cdot}1_A = 1_A\ .$$

Beispiel einer R-Algebra ist jeder Körper $\mathbb{F}$, der eine $\mathbb{K}$-Algebra für jeden Unterkörper $\mathbb{K} \subset \mathbb{F}$ ist, oder die $\mathbb{F}$-Algebra aller $n \times n$ Matrizen mit Koeffizienten aus $\mathbb{F}$. Für jedes $a \in A$ definiert man den Einsetzhomomorphismus

$$\varepsilon_a : R[X] \longrightarrow A, \quad P = \sum r_j X^j \longmapsto \sum_j r_j a^j \tag{2.2.3}$$

Man sagt, dass $a \in A$ eine Nullstelle von $P \in R[X]$ ist, falls $\varepsilon_a(P) = 0$ gilt. Manchmal schreiben wir der Einfachheit halber $P(a)$ statt $\varepsilon_a(P)$. Ist z.B. A die $\mathbb{F}$-Algebra aller $n \times n$-Matrizen mit Koeffizienten in $\mathbb{F}$, so besagt der Satz von Cayley-Hamilton, dass jedes $\Phi \in A = \mathbb{F}^{n\times n}$ eine Nullstelle in A des charakteristischen Polynomes $P_\Phi \in \mathbb{F}[T]$ ist: $\varepsilon_\Phi(P_\Phi) = 0$.
Jedes Polynom $P \in R[X]$ definiert auch die polynomiale Funktion $\widetilde{P} : A \to A$, $a \mapsto \varepsilon_a(P)$. Wie das Beispiel $R := \mathbb{F}_2 := (\mathbb{Z}_2, +, \cdot)$ zeigt, ist die dem nicht trivialen Polynom $F := X^2 - X$ zugeordnete Funktion $\widetilde{F} : R \to R$ die Nullfunktion.

Jeder Ringhomomorphismus $\psi : R \to S$ induziert einen Ringhomomorphismus

$$\overline{\psi} : R[X] \to S[X], \quad \overline{\psi}(r_0 + r_1 X + \cdots + r_n X^n) = \psi(r_0) + \psi(r_1)X + \cdots + \psi(r_n)X^n \tag{2.2.4}$$

So z.B. definiert der kanonische Projektionshomomorphismus $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ einen Homomorphismus $\pi_p : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$. Einige Eigenschaften von Polynomen P in $\mathbb{Z}[X]$ lassen sich dann leicht aus den Eigenschaften von $\overline{\psi}(P) \in \mathbb{Z}_p[X]$ herleiten. So z.B. die Irreduzibilität von $\overline{\psi} \in \mathbb{Z}_p[X]$ impliziert die Irreduzibilität von $P \in \mathbb{Z}[X]$ falls $\mathrm{Grad}(P) = \mathrm{Grad}(\overline{\psi}(P))$ gilt, vgl. 2.2.7.

Satz 2.2.5. *Es sei $\mathbb{F}$ ein Körper. Dann gilt:*

(i) $\mathbb{F}[X]$ *ist ein Hauptidealring.*

(ii) $\forall\, P, Q \in \mathbb{F}[X]$ *existiert deren größter gemeinsamer Teiler* $\mathrm{ggT}(P, Q) \in \mathbb{F}[X]$.

(iii) Es sei $D = \mathrm{ggT}(P, Q)$. *Dann gibt es* $U, V \in \mathbb{F}[X]$ *mit* $D = UP + VQ$.

(iv) $z \in \mathbb{F}$ *ist eine Nullstelle von* $P \in \mathbb{F}[X]$ *genau dann wenn es ein Polynom* $Q \in F[X]$ *mit* $P = (X - z) \cdot Q$ *gibt.*

(v) **(Euklidisches Lemma)** *Es sei* $P \in \mathbb{F}[X]$ *irreduzibel und* $Q_j \in \mathbb{F}[X]$ *beliebig. Gilt* $P|(Q_1 \cdot Q_2 \cdots Q_k)$, *so gibt es ein* $\ell \in \{1, \ldots, k\}$ *mit* $P|Q_\ell$

(vi) **(Faktorisierungslemma)** $\mathbb{F}[X]$ *ist ein ZPF-Ring* (*man sagt auch, dass* $\mathbb{F}[X]$ *faktoriell ist*): *Jedes* $Q \in \mathbb{F}[X]$ *ist ein Produkt von irreduziblen Elementen* P_j, *d.h.,* $Q = P_1 P_2 \cdots P_k$; *dabei sind alle Faktoren* P_j *(bis auf die Reihenfolge und Multiplikationen mit Einheiten) eindeutig bestimmt.*

Die Aussagen (i)-(iii) sowie (v)-(vi) gelten analog für einen beliebigen Euklidischen Ring R an Stelle von $\mathbb{F}[X]$.

Beweis: (Skizze)
Zu (i): Für $I \neq 0, R$ sei $D \in I$ ein Polynom mit der Bedingung $\deg D = \min\{\deg Q : Q \in I \setminus 0\}$. Unter Verwendung des Euklidischen Algorithmus zeigt man dann $I = (D)$.
Zu (ii): Definiere $I := (P, Q) = \mathbb{F}[X]\cdot P + \mathbb{F}[X]\cdot Q$. Nach (i) $I = (D)$ für ein $D \in \mathbb{F}[X]$. Es gilt dann aber $D = \mathrm{ggT}(P, Q)$. Da nun $D \in (P, Q)$, gibt es $U, V \in \mathbb{F}[X]$ mit $D = UP + VQ$. Damit ist auch (iii) bewiesen.
Zu (iv): Die nichttriviale Richtung ist "$P(a) = 0 \implies P = (X - a)\cdot B$" für ein $B \in \mathbb{F}[X]$. Der Eukl. Algorithmus impliziert die Existenz von $B, R \in \mathbb{F}[X]$ mit $\deg R \leq 0$, so dass $P = B\cdot(X - a) + R$. Dann aber $0 = P(a) = B(a)(a - a) + R = R$, also $P = B\cdot(X - a)$.
Zu (v): Durch ein Induktionsargument über die Anzahl der Faktoren in $Q_1 \cdots Q_k$ reduziert sich die Aussage zu "$P|(Q_1 Q_1) \;\Rightarrow\; P|Q_1$ oder $P|Q_2$". Da P irreduzibel ist, $\mathrm{ggT}(P, Q_1) = 1$ oder $= P$. Gilt $\mathrm{ggT}(P, Q_1) = 1$, so folgt wegen (iii) $UP + VQ_1 = 1$, und dann $Q_2 = 1\cdot Q_2 = (UP + VQ_1)Q_2 = UPQ_2 + VQ_1Q_2$. Da die beiden letzten Summanden durch P teilbar sind, folgt $P|Q_2$.
Zu (vi): Es sei $Q \in \mathbb{K}[X]$. Dann ist Q ein Produkt von irreduziblen Elementen $P_j \in \mathbb{K}[X]$, deren Anzahl durch $\deg Q$ nach oben begrenzt ist. Es seien nun $Q = P_1 \cdots P_k = R_1 \cdots R_\ell$ zwei Zerlegungen in irreduzible Faktoren. Die Eindeutigkeit wird durch Induktion über k (Anzahl der Faktoren in $P_1 \cdots P_k$) bewiesen: Der Fall $k = 1$ ist klar: Es muss $\ell = 1$ und $R_1 = P_1$. Der Induktionsschritt $k = n \to n+1$: Falls $P_1 \cdots P_{n+1} = R_1 \cdots R_\ell$ so wegen $P_{n+1}|R_1 \cdots R_\ell$ und (v) gibt es ein R_k mit $P_{n+1}|R_k$. Wegen der Irreduzibilität von P_{n+1}, $P_{n+1} = uR_k$ mit einer Einheit $u \in \mathbb{F}[X]$. Nach Umnummerierung der Faktoren können wir annehmen, dass $k = \ell$. Kürzt man die beiden Produkte um den Faktor R_ℓ,so gilt $uP_1 \cdots P_n = R_1 \cdots R_{\ell-1}$. Nach der Induktionsvoraussetzung (und eventueller Umordnung der Faktoren) folgern wir $\ell = n + 1$ und $P_i = R_i\cdot u_i$ für alle $i \in \{1, \ldots, n\}$. □

$\mathbb{Z}[X]$ ist ein Beispiel eines Ringes, welcher kein Euklidischer Ring und auch kein Hauptidealring ist. Dennoch ist $\mathbb{Z}[X]$ *faktoriell*, d.h., jedes Element in $\mathbb{Z}[X]$ ist ein bis auf die Reihenfolge und Einheiten eindeutig bestimmtes Produkt von irreduziblen Elementen. Die irreduzible Elemente in $\mathbb{Z}[X]$ sind entweder Primelemente in $\mathbb{Z}$ oder Polynome $S = b_0 + b_1X + \cdots b_nX^n \in \mathbb{Z}[X]$ mit $\mathrm{Grad}(S) = n \geq 1$, die irreduzibel in $\mathbb{Q}[Z]$ sind und $\mathrm{ggT}(b_0, b_1, \ldots, b_n) = 1$. Ein Polynom $c_0 + c_1X + \cdots + c_mX^m$ in $\mathbb{Z}[X]$, das die Bedingung $\mathrm{ggT}(c_0, c_1, \ldots, c_m) = 1$ erfüllt, nennt man *primitiv*. Damit gilt für jedes $Q \in \mathbb{Z}[X]$

$$Q = p_1 \cdots p_k \cdot S_1 \cdots S_\ell, \quad p_j \text{ Primzahlen, } S_j \text{ primitive, in } \mathbb{Q}[X] \text{ irreducible Polynome.}$$

Der Vollständigkeit halber geben wir zwei Irreduzibilitätskriteria für Polynome über $\mathbb{Z}$ und $\mathbb{Q}$ an.

Lemma 2.2.6. *Es sei $F = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ ein Polynom.*
(i) Ist F irreduzibel in $\mathbb{Z}[X]$, so ist auch F irreduzibel in $\mathbb{Q}[X]$. Die Umkehrung gilt unter der zusätzlichen Voraussetzung, dass F primitiv ist.
(ii) **(Eisensteinsches Kriterium)** *Gibt es ein Primzahl p, mit der folgenden Eigenschaft*

$$p \not| a_n, \quad \text{aber} \quad p|a_{n-1}, p|a_{n-2}, \ldots, p|a_0 \quad \text{und} \quad p^2 \not| a_0$$

so ist F irreduzibel in $\mathbb{Q}[X]$.

Anwendung: Ist p eine Primzahl, so ist das (primitive) Polynom $X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbb{Z}[X]$ irreduzibel.

Für jede Primzahl p induziert die Projektionsabbildung $\pi_p : \mathbb{Z} \to \mathbb{Z}_p$ auch den Ringhomomorphismus $\overline{\pi}_p : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$: $\overline{\pi}_p(\sum_{j=0}^n a_jX^j) = \sum_{j=0}^n \pi_p(a_j)X^j$. Es kann passieren, dass $\overline{\pi}_p(Q) = 0$ obwohl $Q \neq 0$, z.B., $\overline{\pi}_3(3X^3 - 6X + 3) = 0$. Es gilt jedoch:

Lemma 2.2.7. *Ist p eine Primzahl, die den Leitkoeffizienten a_n von $F = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ nicht teilt und ist $\overline{\pi}_p(F)$ irreduzibel in $\mathbb{Z}_p[X]$ so ist F irreduzibel in $\mathbb{Q}[X]$.*

So z.B. ist das primitive Polynom $R := X^3 - 3X + 4$ irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$: Wäre nämlich R reduzibel, so müsste ein der Faktoren L linear sein. Ferner liegen solche Faktoren, a priori mit Koeffizienten aus $\mathbb{Q}$, sogar in $\mathbb{Z}[X]$ (Folgerung aus 2.2.6.i) und sind primitiv. Also müsste auch $\overline{\pi}_p(R)$ einen linearen Faktor $\overline{\pi}_p(L)$ in $\mathbb{Z}_p[X]$ besitzen oder gleichbedeutend $\widetilde{\overline{\pi}_p(R)} : \mathbb{Z}_p \to \mathbb{Z}_p$ besäße eine Nullstelle in $\mathbb{Z}_p$. Man muss nun ausprobieren, für welche Primzahl (wenn überhaupt) das Polynom $\overline{\pi}_p(R)$ irreduzibel ist. Während $\overline{\pi}_3(R) = X^3 + \underline{1}$ tatsächlich eine Nullstelle in $\mathbb{Z}_3$ besitzt, nämlich $\underline{2}$, (Notation wie in 1.2.9) so hat $\overline{\pi}_5(R) = X^3 - \underline{3}X + \underline{4}$ keine Nullstelle in $\mathbb{Z}_5$:

$$\overline{\pi}_5(R)(\underline{0}) = \underline{4}, \quad \overline{\pi}_5(R)(\underline{1}) = \underline{2}, \quad \overline{\pi}_5(R)(\underline{2}) = \underline{1}, \quad \overline{\pi}_5(R)(\underline{3}) = \underline{2}, \quad \overline{\pi}_5(R)(\underline{4}) = \underline{1}$$

Damit ist $\overline{\pi}_5(R)$ irreduzibel in $\mathbb{Z}_5[X]$ und folglich wegen 2.2.7 ist R irreduzibel sowohl in $\mathbb{Q}[X]$ als auch in $\mathbb{Z}[X]$.

2.3. Körpererweiterungen und Nullstellen von Polynomen

Jeder Körper $\mathbb{K}$ enthält den kleinsten Unterkörper $\mathbb{F}$, der durch die Elemente $0_{\mathbb{K}}$ und $1_{\mathbb{K}}$ erzeugt wird, oder äquivalent, $\mathbb{F}$ ist der Durschnitt aller nicht trivialen Unterkörper von $\mathbb{K}$. Wie nennen $\mathbb{F}$ den *Primkörper* von $\mathbb{K}$. Insbesondere gibt es den Ringhomomorphismus

$$\jmath : \mathbb{Z} \to \mathbb{K} \qquad n \mapsto \begin{cases} 1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}} \quad (n\text{-Mal}) & \text{falls } n \geq 0 \\ -(1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}}) \ ((-n)\text{-Mal}) & \text{falls } n < 0 \end{cases}$$

Entweder ist $\jmath(\mathbb{Z}) \subset \mathbb{K}$ endlich, dann ist $\jmath(\mathbb{Z}) = \mathbb{F} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ der endlicher Körper $\mathbb{F}_p$ mit p Elementen oder $\jmath(\mathbb{Z}) \cong \mathbb{Z}$ ist unendlich. Dann ist $\mathbb{F} \cong \mathbb{Q}$, d.h., $\mathbb{F}$ ist der Quotientenkörper $Q(\jmath(\mathbb{Z}))$.

Definition 2.3.1. Ein Körper $\mathbb{K}$ hat entweder die *Charakteristik* p (p ist eine Primzahl), falls $\jmath(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ oder die *Charakteristik* 0 falls $\jmath(\mathbb{Z}) \cong \mathbb{Z}$. Wir schreiben dann $\mathrm{char}(\mathbb{K}) = p$ oder $\mathrm{char}(\mathbb{K}) = 0$.

Es sei $\mathbb{K} \subset \mathbb{L}$ eine Körpererweiterung von $\mathbb{K}$ (in Zeichen $\mathbb{L}/K$), d.h., $\mathbb{L}$ ist ein Körper, der $\mathbb{K}$ als einen Unterkörper enthält.

Definition 2.3.2. Ein Element $a \in \mathbb{L}$ heißt *algebraisch über* $\mathbb{K}$, falls es ein nicht triviales Polynom $P \in \mathbb{K}[X]$ mit $\varepsilon_a(P) = P(a) = 0$ gibt. Gibt es kein solches Polynom in $\mathbb{K}[X] \setminus \{0\}$, so heißt a *transzendent* über $\mathbb{K}$. Ist jedes Element in $\mathbb{L}$ algebraisch über $\mathbb{K}$, so heißt die Körpererweiterung $\mathbb{L}/\mathbb{K}$ algebraisch. Gibt es in $\mathbb{L}$ mindestens einen transzendenten Element, so heißt die Körpererweiterung transzendent.

Es sei $\mathbb{K} \subset \mathbb{L}$ eine Körpererweiterung. Ist $a \in \mathbb{L}$ beliebig, so bezeichnen wir mit $\mathbb{K}(a)$ den kleinsten Unterkörper von $\mathbb{L}$, der $\mathbb{K}$ und a enthält. Es gibt dann die folgenden Inklusionen:

$$\begin{array}{ccc} \mathbb{K} & & \\ \cap & & \\ \mathbb{K}[a] & = & \{Q(a) : Q \in \mathbb{K}[X]\} = \mathrm{Bild}(\varepsilon_a) \cong \mathbb{K}[X]/\ker(\varepsilon_a) \\ \cap & & \\ \mathbb{K}(a) & = & \{\dfrac{Q(a)}{R(a)} : Q, R \in \mathbb{K}[X],\ R(a) \neq 0\} \\ \cap & & \\ \mathbb{L} & & \end{array}$$

wobei $\ker \varepsilon_a =: I(a) = \{P \in \mathbb{K}[X] : P(a) = 0\}$ ein Ideal in $\mathbb{K}[X]$, das von einem normierten Polynom P_a erzeugt ist ($\mathbb{K}[X]$ ist ein Hauptidealring). Man nennt das $P_a \in \mathbb{K}[X]$ das *Minimalpolynom* von a über $\mathbb{K}$.

Bem.
• Das Minimalpolynom P_a eines algebraischen Elements a ist irreduzibel über $\mathbb{K}$ und damit ist das Ideal $((P_a))$ maximal in $\mathbb{K}[X]$. Daraus folgt, dass der Quotientring $\mathbb{K}[X]/((P_a))$ ein Körper ist und daher $\mathbb{K}[a] = \mathbb{K}(a)$.
• Das Element a ist genau dann algebraisch (über $\mathbb{K}$) wenn das Ideal $I(a)$ nicht trivial ist und transzendent, falls $I(a) = 0$ gilt. Im letzten Fall gilt $\mathbb{K}[X] \cong \mathbb{K}[a] \neq \mathbb{K}(a) \cong Q(\mathbb{K}[X]) =: \mathbb{K}(X)$.

Wir sagen, dass der Körper $\mathbb{K}(a)$ durch die *Adjunktion* des Elements a zu $\mathbb{K}$ entsteht. Analog schreiben wir $\mathbb{K}(a_1, \dots, a_k)$ für den kleinsten Unterkörper von $\mathbb{L}$, der $\mathbb{K}$ und $a_1, \dots, a_k$ enthält.

Die Isomorphieklasse des Körpers $\mathbb{K}(a)$, der durch Adjunktion eines Elements a entsteht, häng nicht von dem Oberkörper $\mathbb{L}$ ab, sondern nur vom Minimalpolynom $P_a \in \mathbb{K}[X]$ ab: Es gilt nämlich

Lemma 2.3.3. *Es seien $\mathbb{L}, \mathbb{L}'$ zwei Körpererweiterungen von $\mathbb{K}$ und $a \in \mathbb{L}$, $a' \in \mathbb{L}'$ zwei Elemente. Die Unterkörper $\mathbb{K}(a) \subset \mathbb{L}$ und $\mathbb{K}(a') \subset \mathbb{L}'$ sind genau dann isomorph, wenn die (normierten!) Minimalpolynome $P_a, P'_{a'} \in \mathbb{K}[X]$ gleich sind.*

Um Körpererweiterungen "messen" zu können, betrachtet man den Oberkörper als einen Vektorraum über den Unterkörper:

Definition 2.3.4. Es sei $\mathbb{K} \subset \mathbb{L}$ eine Körpererweiterung. Dann heißt $[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{L}$ der *Grad* der Körpererweiterung.

Bem. Entsteht $\mathbb{K}(a)$ durch Adjunktion von a, so gilt $[\mathbb{K}(a) : \mathbb{K}] = \mathrm{Grad}(P_a)$. $1, a, a^2, \dots, a^{n-1}$ ist nämlich eine Basis von $\mathbb{K}(a)$ über $\mathbb{K}$ mit $n = \mathrm{Grad}(P_a)$. Ferner ist $a \in \mathbb{L}$ genau dann algebraisch über $\mathbb{K}$, falls $[\mathbb{K}(a) : \mathbb{K}] < \infty$ gilt.

Gradsatz 2.3.5. *Es seien $\mathbb{K} \subset \mathbb{L}$ und $\mathbb{L} \subset \mathbb{F}$ zwei Körpererweiterungen. Dann gilt*

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}]$$

Definition 2.3.6. Eine Körpererweiterung $\mathbb{K} \subset \mathbb{L}$ heißt quadratisch, wenn $[\mathbb{L} : \mathbb{K}] = 2$.

Wir haben schon einige Beispiele kennen gelernt: $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ für beliebige $d \in \mathbb{Q}$. Es ist nicht allzu überraschend, dass jede quadratische Körpererweiterung von dieser Art ist. Es gilt nämlich

Lemma 2.3.7. *Es sei $\mathbb{K}$ eine Körper mit $\mathrm{char}(\mathbb{K}) \neq 2$ und $\mathbb{L}$ eine Körpererweiterung mit $[\mathbb{L} : \mathbb{K}] = 2$. Dann gibt es ein $\delta \in \mathbb{L}$ mit $\delta^2 \in \mathbb{K}$ und $\mathbb{L} = \mathbb{K}(\delta)$.*

Das Beispiel $P = X^2 + 1 \in \mathbb{Q}[X]$ zeigt, dass ein Polynom, das keine Nullstelle über einen Körper $\mathbb{K} = \mathbb{Q}$ hat, eine Zerlegung in Linearfaktoren über einen Erweiterungskörper $\mathbb{L} = \mathbb{C}$ haben kann: $P = (X - i)(X + i)$. Insbesondere gibt es für P einen Erweiterungskörper, z.B. $\mathbb{C}$, in dem P Nullstellen hat.

Man kann nun für jeden Körper $\mathbb{K}$ und jedes Polynom $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ einen Erweiterungskörper $\mathbb{L}$ finden, so dass P eine Nullstelle in $\mathbb{L}$ hat. Die Konstruktion von $\mathbb{L}$ beruht auf der formalen Adjunktion einer Nullstelle: Es sei $P \in \mathbb{K}[X]$ ein irreduzibles Polynom. Insbesondere hat die polynomiale Abbildung $\widetilde{P} : \mathbb{K} \to \mathbb{K}$ keine Nullstelle. Man definiere jetzt $\mathbb{L} := \mathbb{K}[X]/((P))$. Da

$((P)) = \mathbb{K}[X] \cdot P \lhd \mathbb{K}[X]$ maximal ist, ist dieser Quotient ein Körper, der $\mathbb{K}$ als Unterkörper enthält. Die Äquivalenzklasse $\underline{X} = X + ((P))$ von $X = (0, 1, 0, 0, \ldots) \in \mathbb{K}[X]$ ist dann eine Nullstelle von P:

$$\varepsilon_{\underline{X}} P = a_0 + a_1\underline{X} + \cdots + a_n\underline{X}^n = \underline{a_0 + a_1 X + \cdots + a_n X^n} = \underline{0} \in \mathbb{K}[X]/((P)) =: \mathbb{L}$$

Es bezeichne jetzt Z das Element $(0, 1, 0, \ldots)$ in dem Polynomring $\mathbb{L}[Z]$. Dann gilt $P = (Z - \underline{X}) \cdot Q$ für ein $Q \in \mathbb{L}[Z]$ mit $\mathrm{Grad}(Q) < \mathrm{Grad}(P)$. Zerlegt man Q in irreduzible Faktoren $Q_1 \cdots Q_\ell$ in $\mathbb{L}[Z]$ und iteriert man weiter das obige Verfahren in dem man etwa $\mathbb{L}_2 := \mathbb{L}[Z]/((Q_1))$, etc. betrachtet, so beweist man den folgenden

Satz 2.3.8. *Es seien $\mathbb{K}$ ein Körper und $P \in \mathbb{K}[X]$ ein beliebiges Polynom mit $n := \mathrm{Grad}(P)$. Dann gibt es einen Erweiterungskörper $\mathbb{L} \supset \mathbb{K}$, über den P in Linearfaktoren zerfällt:*

$$P = b \cdot (Z - \lambda_1) \cdots (Z - \lambda_n) \qquad b, \lambda_j \in \mathbb{L}$$

Definition 2.3.9. Es sei $P \in \mathbb{K}[X]$ ein Polynom. Jeder Körper $\mathbb{L}$ wie in Satz 2.3.8, der minimal in dem Sinne ist, dass er von den Nullstellen von P in $\mathbb{L}$ erzeugt wird, d.h., $\mathbb{L} = \mathbb{K}(\lambda_1, \ldots, \lambda_n)$ heißt ein *Zerfällungskörper* von P. Für einen solchen Zerfällungskörper von P gilt: $[\mathbb{L} : \mathbb{K}] \leq \mathrm{Grad}(P)!$. Man kann zeigen, dass je zwei Zerfällungskörper von P isomorph sind. Um die Abhängigkeit von P zu unterstreichen, schreiben wir $\mathbb{L}_P$ für den Zerfällungskörper von $P \in \mathbb{K}[X]$.

Endliche Körper. Es sei jetzt $\mathbb{F}$ ein endlicher Körper der Charakteristik p. Dann gilt $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}$, da $\mathbb{F}$ ein Vektorraum über den Primkörper $\mathbb{F}_p$ ist. Gibt es aber für jede Primzahl p und $n \in \mathbb{N}$ einen endlichen Körper mit p^n Elementen?

Satz 2.3.10. *Für jede Primzahl p und $n \in \mathbb{N}$ gibt es einen Körper $\mathbb{F}$ mit $|\mathbb{F}| = p^n$ und je zwei solche Körper sind isomorph.*

Wir schreiben $GF(p^n)$ (Galois field) für den Körper mit p^n Elementen. So z.B. ist $\mathbb{Z}/4\mathbb{Z}$ kein Körper, da er nichttriviale Nullteiler enthält. Dagegen ist $GF(4) \cong \mathbb{F}_2[X]/((X^2 + X + 1))$ ein Körper mit 4 Elementen.

Beispiel. Mit der "Siebmethode" des Eratosthenes kann man zeigen, dass die irreduziblen Polynome in $\mathbb{F}_2[X]$ vom Grad ≤ 5 die Folgenden sind:

$$\begin{matrix} X \\ X+1 \end{matrix}, \quad \begin{matrix} X^2 + X + 1 \\ X^3 + X^2 + 1 \\ X^3 + X + 1 \end{matrix}, \quad \begin{matrix} X^4 + X^3 + 1 \\ X^4 + X + 1 \\ X^4 + X^3 + X^2 + X + 1 \end{matrix}, \quad \begin{matrix} X^5 + X^3 + 1 \\ X^3 + X^2 + 1 \\ X^5 + X^4 + X^3 + X^2 + 1 \\ X^5 + X^4 + X^3 + X + 1 \\ X^5 + X^4 + X^2 + X + 1 \\ X^5 + X^3 + X^2 + X + 1 \end{matrix}$$

So, z.B. alle Quotienten $\mathbb{F}_2[X]/((P_j))$, wobei P_j eins der irreduziblen Polynome vom Grad 5 ist, sind isomorph zu dem Körper $GF(2^5)$ mit 32 Elementen.

2.4. Konstruktionen mit Zirkel und Lineal.

Wir legen zunächst fest, unter welchen Bedingungen sich welcher geometrische Objekte in der affinen Ebene $\mathbb{A}^2$ unter Verwendung von Zirkel und Lineal konstruieren lassen:

Konstruktionsregeln.

(i) Es werden zwei Punkte P_0, P_1 der Ebene vorgegeben, die wir als konstruierbar betrachten. Die Länge der Strecke $\overline{P_0P_1}$ wird als 1 definiert.

(ii) Durch je zwei konstruierte Punkte Q_1, Q_2 kann man (mit Hilfe des Lineals) eine Gerade ziehen oder (mit Hilfe des Zirkels) einen Kreis schlagen deren Mittelpunkt ein konstruierbare Punkt ist und deren Radius gleicht dem Abstand zwei bereits konstruierten Punkten. Solche Geraden oder Kreise sind per Definitionen konstruierbar.

(iii) Die Durchschnittspunkte von konstruierbaren Geraden und Kreisen deklarieren wir ebenfalls für konstruierbar.

Durch wiederholte Anwendung von (ii) kann aus den Anfangspunkten P_0 und P_1 immer mehr Punkte konstruiert werden. Da in jedem Konstruktionsschritt (iii) immer neue Punkte entstehen, und man (ii) und (iii) beliebig oft wiederholen kann, ist es nicht so klar, welche Punkte der Ebene sich überhaupt konstruieren lassen. Überraschenderweise läßt sich dennoch mit Hilfe der Körpertheorie entscheiden, welche Punkte der Ebene konstruierbar sind.

Man kann z.B. zu einer vorgegebenen (konstruierbaren) Gerade ℓ und *durch* einen beliebig vorgegebenen Punkt Q eine zu ℓ senkrechte Gerade ℓ_1 oder zu ℓ parallele Gerade ℓ_2 konstruieren. Insbesondere wird durch die Anfangspunkte P_0 und P_1 ein kartesisches Koordinatensystem $\{(x,y)\}$ in der affinen Ebene festgelegt (P_0 ist der Nullpunkt, die x-Achse geht durch P_0 und P_1, die y-Achse steht senkrecht zu der x-Achse und geht durch P_0 sowie P_1 hat die Koordinaten $(1,0)$).

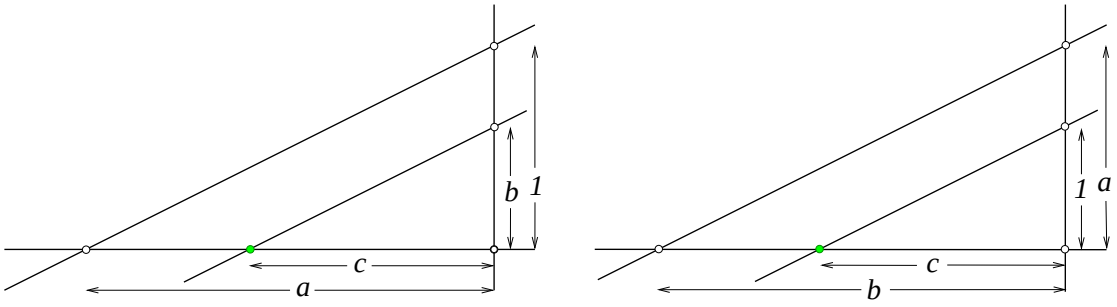
Definition 2.4.1. Eine reelle Zahl $r \in \mathbb{R}$ heißt *konstruierbar*, falls r der Abstand zweier konstruierbaren Punkte S_1, S_2 ist.

Bem. Die affine Ebene $\mathbb{A}^2$ sei mit dem oben konstruierten kartesischen Koordinatensystem versehen. Dann ist ein Punkt $Q \in \mathbb{A}^2$ genau dann konstruierbar, wenn seine Koordinaten $x(Q), y(Q)$ konstruierbare reelle Zahlen sind.

Die Verbindung zu der Körpertheorie liefert der folgende

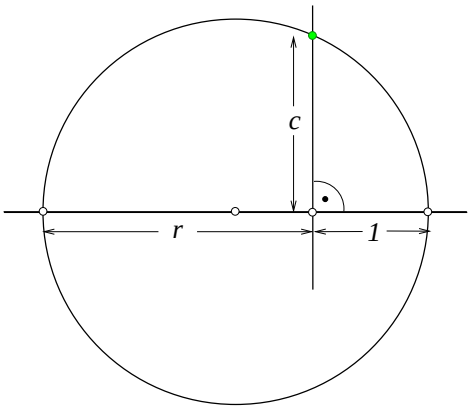
Satz 2.4.2. *Die Menge aller konstruierbaren Zahlen bildet einen Unterkörper von* $\mathbb{R}$.

Beweis: Es sei $\mathcal{K} \subset \mathbb{R}$ die Menge aller konstruierbaren Zahlen. Man muss nachweisen, dass für beliebige $a, b \in \mathcal{K}$ auch $a \pm b$ sowie ab und a/b $(b \neq 0)$ in $\mathcal{K}$ liegen. Sind zwei konstruierbare Strecken mit den Längen a, b vorgegeben, so lassen sich durch das entsprechende Abtragen der Längen auf eine (konstruierbare) Gerade $a+b$ und $a-b$ sofort konstruieren. Die Konstruierbarkeit von $c := ab$ (linke Zeichnung) sowie $c := a/b$ (rechte Zeichnung) ist zeichnerisch erklärt:



Lemma 2.4.3. *Ist $r > 0$ eine konstruierbare Zahl, so ist auch $\sqrt{r}$ konstruierbar.*

Hierbei wird zunächst die Strecke $1+r$ auf einer kostruierbaren Gerade ℓ (z.B der x-Achse) abgetragen, anschließend der Mittelpunkt dieser Strecke bestimmt, um den dann der Kreis mit Radius $(1+r)/2$ konstruiert wird. Der Durchschnittspunkt zwischen dem Kreis und der zu ℓ senkrechten Gerade liefert den gewünschten Punkt mit $c = \sqrt{r}$.



Lemma 2.4.4. *Angenommen, die Koordinaten der Punkte $Q_1, .., Q_4$ liegen in dem Körper $\mathbb{K} \subset \mathbb{R}$. Dann sind die Koordinaten der Punkte, die als Durchschnitte von*
- *zwei Geraden oder*
- *einer Gerade und eines Kreises oder*
- *zwei Kreise,*

die jeweils durch irgendwelche der Punkte $Q_1, \dots, Q_4$ festgelegt werden, liegen entweder in $\mathbb{K}$ oder in der quadratischen Körpererweiterung $\mathbb{K}(\sqrt{d})$ mit einem geeigneten $d > 0$ aus $\mathbb{K}$.

Zusammenfassend erhalten wir schließlich den folgenden

Hauptsatz 2.4.5.. *Ein Punkt $Q = (x(Q), y(Q)) \in \mathbb{R}^2$ ist genau dann konstruierbar mit Zirkel und Lineal, falls es eine Kette von Körpererweiterungen $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m$ gibt, so dass für jedes j $[\mathbb{K}_{j+1} : \mathbb{K}_j] = 2$ und $x(Q), y(Q) \in \mathbb{K}_m$. Insbesondere muss der Grad der Minimalpolynome $p_x, p_y \in \mathbb{Q}[X]$ von $x(Q)$ und $y(Q)$ eine Potenz von 2 sein.*

Anwendungen: Dreiteilung eines beliebig vorgegebenen Winkels. Einen Winkel zwischen zwei Geraden ℓ_1, ℓ_2 nennen wir konstruierbar, falls die beiden Geraden konstruierbar sind. Nimmt man die x-Achse als die Gerade ℓ_1, so ist ℓ_2 durch den Koordinatenursprung genau dann konstruierbar, wenn ihr Durchschnitt S mit dem Einheitskreis um 0 konstruierbar ist, d.h., $x(S) = \cos\varphi$ und $y(S) = \sin\varphi$ konstruierbare Zahlen sind. Es sei jetzt $\theta := \varphi/3$. Dann folgt aus dem trigonometrischen Additionstheoremen

$$\cos\varphi = 4(\cos\theta)^4 - 3\cos\theta$$

Wäre der Winkel θ konstruierbar, so muss insbesondere $\cos\theta$ eine konstruierbare Zahl sein. Da aber $\cos\theta$ eine Nullstelle des Polynomes $M = 4X^3 - 3X - \cos\varphi$ ist, das für die meisten Werte von $\cos\varphi \in \mathbb{Q}$, z.B. für $\varphi = \pi/3$ (d.h. $\cos\theta = 1/2$) irreduzibel ist, ist M das Minimalpolynom von $\cos\theta$. Deren Grad ist aber <u>keine</u> zweier Potenz. Also kann $\theta = \varphi/3$ für $\varphi = \pi/3$ nach 2.4.5 nicht mit Zirkel und Lineal konstruiert werden.

Konstruktion eines regulären p-Ecks. Es sei p eine Primzahl. Ein reguäres n-Eck mit vorgegebenen Kantenlänge d läßt sich genau dann mit Zirkel und Lineal konstruieren, wenn der Winkel $2\pi/n$ konstruierbar ist, d.h., $\cos(2\pi/n)$ und $\sin(2\pi/n)$ konstruierbare reelle Zahlen sind. Es sei jetzt $\omega := \cos(2\pi/p) + i\sin(2\pi/p)$ die komplexe Zahl, die in $\mathbb{R}^2 = \mathbb{C}$ eine Ecke des in dem Einheitskrien eingeschriebenen p-Ecks beschreibt. Dann sind $\omega, \omega^2, \dots, \omega^{p-1}, \omega^p = 1$ alle Ecken unseres p-Ecks und es gilt $0 = 1+\omega+\omega^2+\cdots+\omega^{p-1}$. Wir haben bereits gesehen, dass $1+X+X^2+\cdots+X^{p-1} \in \mathbb{Q}[X]$ ein irreduzibles Polynom ist. Liegen $\cos(2\pi/p)$ und $\sin(2\pi/p)$ in dem Körper $\mathbb{K} \subset \mathbb{R}$, so liegt ω in

der quadratischen Erweiterung $\mathbb{K}(i) \subset \mathbb{C}$. Ist $\mathbb{K}$ konstruierbar, so gilt wegen

$$[\mathbb{K}(i) : \mathbb{Q}] = [\mathbb{K}(i) : \mathbb{K}] \cdot [\mathbb{K}, \mathbb{Q}] = 2[\mathbb{K}, \mathbb{Q}] = 2^\ell \ ,$$

Insbesondere muss der Grad des Minimalpolynomes $P_\omega = 1 + X + \cdots + X^{p-1}$ eine zweier Potenz sein, d.h., $p - 1 = 2^k$. Damit haben wir gezeigt, dass wenn ein reguläres p-Eck, p Primzahl, mit Zirkel und Lineal konstruierbar ist, so muss $p = 2^k + 1$ für ein $k \in \mathbb{N}$ gelten. Man kann auch die Umkehrung zeigen, dass nämlich jedes p-Eck mit $p = 2^k + 1$ auch konstruierbar ist. Damit ist z.B. das 7-Eck, 11-Eck und 13-Eck nicht konstruierbar, dagegen läßt sich das 17-Eck oder das 257-Eck mit Zirkel und Lineal konstruieren.

2.5. Galoistheorie und die Bestimmung von polynomialen Nullstellen

In diesem Abschnitt betrachten wir nur Körper von Charakteristik 0.

Einheitswurzeln. In $\mathbb{C}$ kann man eine beliebige Wurzel aus einer beliebigen komplexen Zahl ziehen. Einen besonderen Stellenwert hat die Menge aller Einheitswurzeln: $\{\omega \in \mathbb{C} : \omega^n = 1\} = \{e^{ik\frac{2\pi}{n}} : k = 0, 1, \ldots, n-1\}$. Die n-ten Einheitswurzeln bilden eine zyklische Untergruppe der Ordnung n von $(\mathbb{C} \setminus \{0\}, \cdot)$. Nicht jedes Element $\zeta \in \{\omega \in \mathbb{C} : \omega^n = 1\} \cong (\mathbb{Z}_n, +)$ erzeugt die ganze zyklische Gruppe. Diejenigen n-ten Einheitswurzeln, die die ganze Gruppe erzeugen nennen wir *primitiv*. Allgemeiner, in jedem Körper $\mathbb{K}$, deren Charakteristik char($\mathbb{K}$) die ganze Zahl n nicht teilt, bildet die Menge $\{\omega \in \mathbb{L}_{(X^n-1)} : \omega^n = 1\}$ in dem Zerfällungkörper $\mathbb{L}$ von $X^n - 1$ eine zu $\mathbb{Z}_n$ isomorphe Gruppe. Dagegen ist jeder Körper der Charakteristik p, z.B., $\mathbb{F}_p$ bereits der Zerfällungskörper von $X^p - 1 = (X - 1)^p$ und die p-ten Wurzeln bilden die triviale Gruppe $\{1\}$.

Ist etwa $z = x + iy = re^{i\psi} \in \mathbb{C} \setminus \{0\}$, so existieren in $\mathbb{C}$ genau n verschiedene n-te Wurzeln aus z, nämlich

$$\alpha, \quad \alpha\omega, \quad \alpha\omega^2 \ , \ \ldots \ , \ \alpha\omega^{n-1} \ ,$$

wobei $\alpha := \sqrt[n]{r}\, e^{i\psi/n}$ und ω eine primitive n-te Wurzel ist. Wir schreiben einfach $\sqrt[n]{z}$ für jede solche Wurzel.

Klassische Formeln. Jedes Polynom $P = Z^n + a_{n-1}Z^n + \cdots + a_0 \in \mathbb{C}[Z]$ zerfällt in Linearfaktoren: $P = (Z - \lambda_1) \cdots (Z - \lambda_n)$. Lassen sich die Nullstellen λ_j als algebraische Ausdrücke in den Koeffizienten $a_0, \ldots, a_{n-1}$ bestimmen? Solche Formel gibt es z.B. für quadratische Gleichungen:

- $Z^2 + a_1 Z + a_0$. Dann gilt für die Nullstellen $\lambda_{1/2} = -\dfrac{a_1}{2} \pm \sqrt{\left(\dfrac{a_1}{2}\right)^2 - a_0}$
- $Z^3 + a_2 Z^2 + a_1 Z + a_0$. (Scipio del Ferro, Tartaglia, ca 1515) Durch die Substitution $Z = Y - \frac{a_2}{3}$ erhalten wir das zu dem Ursprungspolynom äquivalente Polynom $Q := Y^3 + qY + r$ mit $q, r \in \mathbb{Q}(a_0, a_1, a_2) \subset \mathbb{C}$. Um die Nullstellen von Q zu bestimmen, machen wir den Ansatz $\lambda = u + v$ und erhalten die Gleichung

$$0 = (u + v)^3 + q(u + v) + r = \left(u^3 + v^3 + r\right) + (u + v)(3uv + q) \ .$$

$u+v$ ist sicherlich eine Nullstelle von Q falls $u^3 + v^3 + r = 0$ sowie $3uv + q = 0$. O.B.d.A können wir $q \neq 0$ annehmen (sonst ist die Bestimmung der Nullstellen trivial). Dann auch $u \neq 0 \neq v$ und $v = q/(3u)$ folgt aus der zweiten Gleichung. Eingesetzt in die erste Gleichung erhalten wir $u^3 + \left(\dfrac{q}{3}\right)^3 \dfrac{1}{u^3} + r = 0$, oder äquivalent

$$\left(u^3\right)^2 + ru^3 + \left(\frac{q}{3}\right)^3 = 0 \qquad \text{und damit} \qquad \begin{aligned} u^3 &= -\frac{r}{2} + \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3} \\ v^3 &= -\frac{r}{2} - \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3} \end{aligned}$$

Sind jetzt u_0, v_0 irgendwelche komplexe dritte Wurzeln

$$u_0 := \sqrt[3]{-\frac{r}{2} + \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3}}, \qquad v_0 := \sqrt[3]{-\frac{r}{2} - \sqrt{\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3}}$$

so hat jede Nullstelle $\lambda_{1/2/3}$ von Q die Gestalt

$$u_0\omega^j + v_0\omega^k,$$

wobei ω eine primitive dritte Einheitswurzel ist und $j, k \in \{0, 1, 2\}$ so gewählt sind, dass $3u_0v_0\omega^{j+k} = -q$ gilt.

• $Z^4 + a_3Z^3 + a_2Z^2 + a_1Z + a_0$ (Luigi Ferrari, ca 1550). Nach der Substitution $X = Y - a_3/4$ erhalten wir das äquivalente Polynom

$$Z^4 + qZ^2 + rZ + s = (Z^2 + \alpha Z + \beta)(Z^2 - \alpha Z + \gamma)$$

wobei α, β, γ sich aus dem Gleichungssystem

$$\begin{array}{rcl} q &=& \beta + \gamma - \alpha^2 \\ r &=& \alpha(\beta - \gamma) \\ s &=& \beta\gamma \end{array} \qquad \Longleftrightarrow \qquad \begin{array}{rcl} 2\gamma &=& \alpha^2 + q + r/\alpha \\ 2\beta &=& \alpha^2 + q - r/\alpha \\ s &=& \beta\gamma \end{array}$$

als algebraische Ausdrücke in q, r, s bestimmen lassen: O.B.d.A $r \neq 0 \neq \alpha$ (sonst reduziert sich die Bestimmung der Nullstellen auf die quadratische Formel). Aus dem GLS auf der rechten Seite folgt

$$(\alpha^2)^3 + 2q(\alpha^2)^2 + (q^2 - 4s)\alpha^2 - r^2 = 0\,.$$

Damit lassen sich α, β und γ unter Verwendung der Nullstellenformel für kubische Polynome bestimmen und dann auch die Nullstellen der beiden quadraischen Faktoren in der Zerlegung von Q.

Analysiert man die obigen Formeln vom Standpunkt der Körpertheorie, so erhält man einen Turm von gewissen Körpererweiterungen von $\mathbb{K}_0 = \mathbb{Q}(a_0, a_1, \ldots, a_n)$. Die Nullstellen einer quadratischen Gleichung fanden wir in der Körpererweiterung

$$\mathbb{K}_0\Big(\sqrt{(\tfrac{a_1}{2})^2 - a_0}\Big) \quad \text{von} \quad \mathbb{K}_0 = \mathbb{Q}(a_0, a_1).$$

Die Nullstellen einer kubischen Gleichung lagen in der Körpererweiterung $\mathbb{K}_4$, wobei

$$\mathbb{K}_0 \subset \underbrace{\mathbb{K}_0(\sqrt{(r/2)^2 + (q/3)^3})}_{=\mathbb{K}_1} \subset \underbrace{\mathbb{K}_1(\sqrt[3]{u^3})}_{=\mathbb{K}_2} \subset \underbrace{\mathbb{K}_2(\sqrt[3]{v^3})}_{=\mathbb{K}_3} \subset \mathbb{K}_3(\omega) =: \mathbb{K}_4\,,$$

d.h., jeder Zwischenkörper entsteht hier durch Adjunktion eines geeigneten k-ten Wurzels. Das motiviert die folgende

Definition 2.5.1. Es sei $Q = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbb{K}[X]$ ein Polynom. Wir sagen, dass sich die Nullstellen von Q durch algebraische Ausdrücke mit Radikalen über $\mathbb{K}$ (bzw. aus den Koeffizienten von Q, falls $\mathbb{K} = \mathbb{Q}(a_0, \ldots, a_{n-1})$) bestimmen lassen, falls der Zerfällungskörper $\mathbb{L}_Q$ (der insbesonders alle Nullstellen von Q enthält) in einer Körpererweiterung $\mathbb{K}_r$ von $\mathbb{K}_0 = \mathbb{K}$ liegt, die sich folgendermaßen charakterisieren läßt :
• Es gibt einen Turm von Körpererweiterungen $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r$, so dass für jedes $j \in \{0, 1, \ldots, r-1\}$ $\mathbb{K}_{j+1} = \mathbb{K}_j(\sqrt[n_j]{d_j})$ für ein geeignetes $d_j \in \mathbb{K}_j$ gilt.

Wie lassen sich solche Körpererweiterungen $\mathbb{K}_r/\mathbb{K}_0$ bequemer charakterisieren, die die obige "Turmbedingung" erfüllen? Dazu brauchen wir eine weitere Invariante von Körpererweiterungen.

Die Galoisgruppe einer Körpererweiterung. Als Motivation überlegt man sich, dass jedes reelle Polynom $Q = a_0 + a_1X + \cdots + a_nX^n$ über $\mathbb{R}$ in lineare und/oder quadratische irreduzible Faktoren zerfällt. Insbesonders ist jedes reelle Polynom vom Grad ≥ 3 reduzibel. In dem Beweis dieser Tatsache spielt die komplexe Konjugation $\overline{\ }: \mathbb{C} \to \mathbb{C}$ eine entscheidende Rolle. Über $\mathbb{C}$ zerfällt Q in Linearfaktoren: $Q = \mu \cdot (Z - \lambda_1) \cdots (Z - \lambda_n)$, $\lambda_j \in \mathbb{C}$ und $n = \mathrm{Grad}(Q)$. Da Q ein reelles Polynom ist, gilt $Q = \overline{Q}$. Ist also λ eine Nullstelle von Q, so gilt dasselbe für $\overline{\lambda}$, denn

$$Q(\overline{\lambda}) = \sum a_j \overline{\lambda}^j = \sum \overline{a}_j \overline{\lambda}^j = \overline{\sum a_j \lambda^j} = \overline{0} = 0$$

Die komplexe Konjugation ist ein Körperautomorphismus $\mathbb{C} \to \mathbb{C}$, welcher den Unterkörper $\mathbb{R}$ punktweise festläßt. Gleichzeitig permutiert $\overline{\ }$ die komplexen Nullstellen von Q. Fasst man je zwei Linearfaktoren mit komplex konjugierten Nullstellen zusammen, so enthällt man ein *reelles* quadratisches Polynom: $(X - \lambda)(X - \overline{\lambda}) = X^2 - (\lambda + \overline{\lambda})X + |\lambda|^2$ Dieses Polynom ist irreduzibel in $\mathbb{R}[X]$ falls $\lambda \in \mathbb{C} \smallsetminus \mathbb{R}$ gilt. Das ist die Motivation für die Untersuchung der Menge aller solcher Körperautomorphismen in allgemeinen Situationen.

Definition 2.5.2. Es sei $\mathbb{K} \subset \mathbb{L}$ eine Körpererweiterung. Die Gruppe der Körperautomorphismen

$$\mathrm{Gal}(\mathbb{L}/K) := \left\{ \psi : \mathbb{L} \to \mathbb{L} : \begin{array}{c} \psi \text{ Körperisomorphismus} \\ \psi(k) = k \ \ \forall\, k \in \mathbb{K} \end{array} \right\}$$

mit der Abbildungsverkettung als Gruppenverknüpfung heißt die *Galoisgruppe* der Körpererweiterung $\mathbb{L}/\mathbb{K}$. Die folgenden Aussagen beschreiben den Zusammenhang zwischen solchen Gruppen und den Körpererweiterungen. Im Rahmen dieser Vorlesung verzichten wir auf deren Beweise und verweisen dazu auf die Lehrbücher zu Galoistheorie.

Satz 2.5.3. *Es sei $\mathbb{K} \subset \mathbb{L}$ eine endliche Körpererweterung und* Gal()$\mathbb{L}/K$) *deren Galoisgruppe. Dann teilt die Ordnung* $|\mathrm{Gal}(\mathbb{L}/K)|$ *den Grad* $[\mathbb{L} : \mathbb{K}]$ *der Körpererweiterung.*

Die Körpererweiterungen, für die $|\mathrm{Gal}(\mathbb{L}/K)| = [\mathbb{L} : K]$ gilt, nennt man *galoissch* oder *Galoiserweiterungen*. Sie spielen eine besondere Rolle:

Satz 2.5.4. *Eine Körpererweiterung $\mathbb{K} \subset \mathbb{L}$ (*$\mathrm{char}(\mathbb{K}) = 0$*) ist genau dann galoissch, wenn $\mathbb{L}$ der Zerfällungskörper $\mathbb{L}_Q$ eines Polynoms $Q \in \mathbb{K}[X]$ ist.*

Lemma 2.5.5. *Es sei $Q \in \mathbb{K}[X]$ mit $n = \mathrm{Grad}(Q)$.*

(i) Hat Q m verschiedene Nullstellen $\lambda_1, \ldots, \lambda_m$ in seinem Zerfällungskörper $\mathbb{L}_Q$, so gibt es einen injektiven Homomorphismus $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{K}) \to \mathfrak{S}\{\lambda_1, \ldots, \lambda_m\} \cong \mathfrak{S}_m$. *Insbesonders ist* $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{K})$ *isomorph zu einer Untergruppe der symmetrischen Gruppe $\mathfrak{S}_m$.*

(ii) Ist Q irreduzibel, so operiert $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{K})$ *transitiv auf der Menge der Nullstellen $\{\lambda_1, \ldots, \lambda_n\}$.*

Die Zwischenkörper eine Galoiserweiterung $\mathbb{K} \subset \mathbb{L}$ und die Untergruppen von $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ stehen in enger Beziehung:

Satz 2.5.6. *Es sei $\mathbb{K} \subset \mathbb{L}$ eine Galoiserweiterung.*

(i) $\mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = \{x \in \mathbb{L} : \psi(x) = x \ \forall\, \psi \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})\} = \mathbb{K}$.

(ii) Es gibt eine Bijektion zwischen der Menge aller Untergruppen $H <$ $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *und der Menge aller Zwischenkörper $\mathbb{F}$ mit $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$. Sie ist durch die Relation $H \longleftrightarrow \mathbb{L}^H$ gegeben.*

Beispiel. Es sei ω eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\omega)/\mathbb{Q}$ eine Galoiserweiterung und $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ ist isomorph zu der Gruppe der Einheiten $(\mathbb{Z}_n, \cdot)^\times$ in dem Ring $\mathbb{Z}_n$.

Wir kommen nun zu dem Hauptpunkt dieser Untersuchung.

Definition 2.5.7. (**und Lemma.**) Eine Gruppe heißt auflösbar, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) Die Kommutatorreihe $G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(r)} = \{e\}$ bricht nach endlich vielen Schritten ab. Dabei definiert man rekursiv $G^{(j+1)} = [G^{(j)} : G^{(j)}] = \langle aba^{-1}b^{-1} : a, b \in G^{(j)} \rangle$ und $\langle M \rangle$ bezeichnet die kleinste, von den Elementen der Teilmenge $M \subset G$ erzeugte Untergruppe von G.

(ii) Es gibt eine absteigende Reihe von Normalteilern in G:

$$G =: N_0 \rhd N_1 \rhd N_2 \rhd \cdots \rhd N_s = \{e\} ,$$

so dass für jedes $j \in \{0, 1, \ldots, s-1\}$ der Quotient N_j/N_{j+1} abelsch ist.

So z.B. ist jede abelsche Gruppe, sowie $\mathfrak{S}_2, \mathfrak{S}_3$ und $\mathfrak{S}_4$ auflösbar. Dagegen sind $\mathfrak{S}_n$ für jedes $n \geq 5$, $\mathrm{SL}_\ell(\mathbb{K})$ oder $\mathrm{SO}(\ell, \mathbb{R})$ nicht auflösbar.

Hauptsatz 2.5.8. *Es sei $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r$ ein Turm von Körpererweiterungen, so dass für jedes j $\mathbb{K}_{j+1}$ durch Adjunktion von $\sqrt[n_j]{d_j}$, $d_j \in \mathbb{K}_j$ entsteht und $\mathbb{L}_Q$, der Zerfällungskörper eines Polynomes $Q \in \mathbb{K}_0[X]$, in $\mathbb{K}_r$ enthalten ist. Dann ist* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *eine auflösbare Gruppe.*

Wir zeigen, wie sich die obigen Aussagen benutzen lassen um Existenz von Polynomen zu zeigen, deren Nullstellen sich nicht durch Formeln angeben lassen, die bloß algebraische Ausdrücke in den Koeffizienten des Polynomes sowie das sukzessive Wurzelziehen beinhalten.

Beispiel. Die Quintik $Q = X^5 - 4X + 2$ ist ein irreduzibles Polynom in $\mathbb{Q}[X]$. Es sei $\mathbb{L}_Q$ sein Zerfällungkörper. Wir zeigen, dass $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q}) = \mathfrak{S}_5$ und damit nicht auflösbar ist:

• Da Q irreduzibel ist, besitzt Q fünf verschiedene Nullstellen $\lambda_1, \ldots, \lambda_5$ in seinem Zerfällungskörper $\mathbb{Q} \subset \mathbb{L}_Q = \mathbb{Q}(\lambda_1, \ldots, \lambda_5) \subset \mathbb{C}$.

• Eine genauere Analyse von der Ableitung Q' der polynomialen Funktion Q zeigt, dass Q genau zwei kritische Punkte hat. Damit sind genau 3 der Nullstellen von Q rein reell und zwei Nullstellen (sagen wir λ_4, λ_5) liegen in $\mathbb{C} \setminus \mathbb{R}$.

• Q ist das Minimalpolynom jeder der Nullstellen λ_j von Q. Damit ist nach 2.3.3 jeder der Zwischenkörper $\mathbb{Q}(\lambda_j)$ (d.h., $\mathbb{Q} \subset \mathbb{Q}(\lambda_j) \subset \mathbb{L}_Q$ ($\subset \mathbb{C}$)) isomorph zu $\mathbb{Q}[X]/((Q))$. I.A. sind jedoch die fünf Zwischenkörper verschieden als Teilmengen von $\mathbb{C}$. Aus dem Gradsatz 2.3.5 folgt dann, dass

$$[\mathbb{L}_Q : \mathbb{Q}] = [\mathbb{L}_Q : \mathbb{Q}(\lambda_1)] \cdot [\mathbb{Q}(\lambda_1) : \mathbb{Q}] = [\mathbb{L}_Q : \mathbb{Q}(\lambda_1)] \cdot 5$$

durch 5 teilbar ist. Einerseits gilt nach Satz 2.5.4, dass dann auch $|\mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q})| = [\mathbb{L}_Q : \mathbb{Q}]$ durch 5 teilbar ist und daher ein Element $\sigma \in \mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q})$ der Ordnung 5 enthält. Da aber nach Lemma 2.5.5 $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q})$ isomorph zu einer Untergruppe von $\mathfrak{S}_5$ ist und die einzigen Element der Ordnung 5 in $\mathfrak{S}_5$ die zyklischen Permutationen (12345) sind, so enthält $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q})$, als Untergruppe von $\mathfrak{S}_5$ betrachtet, ein solches Element σ.

• Es gibt noch mindestens ein weiteres Element in $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q})$: Da die komplexe Konjugation $\overline{\ }: \mathbb{C} \to \mathbb{C}$ die Nullstellen $\lambda_1, \ldots, \lambda_5$ permutiert, induziert sie einen Körperautomorphismus von $\mathbb{L}_Q = \mathbb{Q}(\lambda_1, \ldots, \lambda_5)$ und ist daher auch ein Element τ in $\mathrm{Gal}(\mathbb{L}_Q/\mathbb{Q})$. τ operiert als Transposition auf $\{\lambda_1, \ldots \lambda_5\}$ da τ die 3 reellen Nullstellen $\lambda_1, \lambda_2, \lambda_3$ punktweise festläßt und λ_4 mit λ_5 vertauscht.

• Jede Untergruppe $\langle \sigma, \tau \rangle \subset \mathfrak{S}_5$, die von einer Transposition τ und einer zyklischen Permutation $(k_1k_2k_3k_4k_5)$ der Ordnung 5 erzeugt ist, stimmt bereits mit der ganzen Gruppe $\mathfrak{S}_5$ überein.(Das ist eine schöne Übungsaufgabe!)

• Wie bereits erwähnt, ist $\mathfrak{S}_5$ keine auflösbare Gruppe. Ein Grund dafür ist der Folgende: Man kan zeigen, dass der Normalteiler $\mathfrak{A}_5 \lhd \mathfrak{S}_5$ aller geraden Permutationen von 5 Elementen eine einfache Gruppe ist, d.h., die einzigen Normalteiler von $\mathfrak{A}_5$ sind $\{e\}$ und $\mathfrak{A}_5$ selbst. Da $\mathfrak{A}_5$ nicht abelsch ist, gibt es keine absteigende Kette von Normalteilern, die die Bedingung aus der Definition 2.5.7 erfüllen.

Wären nun die Nullstellen $\lambda_1, \ldots, \lambda_5$ von Q als algebraische Ausdrücke darstellbar, die sukzessiv aus $\mathbb{Q}$ durch Hinzuname beliebiger Wurzel entstehen, so müssten $\lambda_1, \ldots, \lambda_5$ und damit der ganze Zerfällungskörper $\mathbb{L}_Q$ in einem Körper $\mathbb{K}_r$ enthalten sein, für den die "Turmbedingung" aus 2.5.1 gilt. Nach dem Hauptsatz von 2.5.8 müsste dann aber auch die Galoisgruppe $\mathrm{Gal}(\mathbb{L}_Q : \mathbb{Q})$ auflösbar sein. Da aber in unserem Fall $\mathrm{Gal}(\mathbb{L}_Q : \mathbb{Q}) \cong \mathfrak{S}_5$ nicht auflösbar ist haben wir ein Bespiel eines Polynomes vom Grade 5 gefunden, deren Nullstellen sich nicht durch algebraische Ausdrücke und Radikale aus den Koeffizienten darstellen läßt , wie das für alle Polynome vom Grad ≤ 4 der Fall ist.