Aufgabe 1: Sei f eine Isometrie des $\mathbb{R}^n$, d.h. eine bijektive Abbildung $f : \mathbb{R}^n \to \mathbb{R}^n$, sodass

$$(f(x) - f(y))^t (f(x) - f(y)) = (x - y)^t (x - y)$$

für alle x, y gilt. Es gelte $f(0) = 0$. Beweisen Sie, dass f linear ist. Hinweis: Bezeichnet b_i $(1 \leq i \leq n)$ eine Orthonormalbasis des $\mathbb{R}^n$, so kann man jedes $x \in \mathbb{R}^n$ in der Form $x = \sum_{i=1}^n (x^t b_i)\, b_i$ schreiben.

Wir müssen zwei Eigenschaften nachweisen:

1. $f(\lambda\vec{v}) = \lambda f(\vec{v})$ für alle $\lambda \in \mathbb{R}$ und alle $\vec{v} \in \mathbb{R}^n$
2. $f(\vec{v} + \vec{u}) = f(\vec{v}) + f(\vec{u})$ für alle $\vec{v}, \vec{u} \in \mathbb{R}^n$

Zwecks einfacherer Schreibweise definieren wir $\langle \vec{v} | \vec{u} \rangle := (\vec{v})^t (\vec{u})$. Wir werden ständig $\langle f(x) | f(x) \rangle = \langle x | x \rangle$ benutzen, das folgt aus der Aufgabenstellung mit $\vec{y} = \vec{0}$ wegen $f(\vec{0}) = \vec{0}$.

Zuerst betrachten wir Identitäten, die allgemein gelten:

$$\langle u + v | u + v \rangle - \langle u - v | u - v \rangle = \langle u | u \rangle + \langle v | v \rangle + - \langle u | u \rangle - \langle v | v \rangle + 4 \langle u | v \rangle$$

$$\Rightarrow \langle u | v \rangle = \frac{1}{4}\Big(\langle u + v | u + v \rangle - \langle u - v | u - v \rangle \Big) \tag{1}$$

$$\langle u + v | u + v \rangle + \langle u - v | u - v \rangle = 2 \langle u | u \rangle + 2 \langle v | v \rangle$$

$$\Rightarrow \langle u + v | u + v \rangle = 2 \langle u | u \rangle + 2 \langle v | v \rangle - \langle u - v | u - v \rangle \tag{2}$$

Nun zeigen wir, dass $\langle f(u) | f(v) \rangle = \langle u | v \rangle$ gilt. Die erste Zeile folgt aus (1), die zweite Zeile folgt aus (2).

$$\begin{aligned}
\langle f(u) | f(v) \rangle &= \frac{1}{4}\Big(\langle f(u) + f(v) | f(u) + f(v) \rangle - \langle f(u) - f(v) | f(u) - f(v) \rangle \Big) \\
&= \frac{1}{4}\Big(2(\langle f(u) | f(u) \rangle + \langle f(v) | f(v) \rangle - \langle f(u) - f(v) | f(u) - f(v) \rangle) \Big) \\
&= \frac{1}{2}\Big((\langle u | u \rangle + \langle v | v \rangle - \langle u - v | u - v \rangle) \Big) \\
&= \frac{1}{2}\Big((\langle u | u \rangle + \langle v | v \rangle - \langle u | u \rangle - \langle v | v \rangle + 2 \langle u | v \rangle \Big) = \langle u | v \rangle
\end{aligned}$$

Nachdem wir $\langle f(u) | f(v) \rangle = \langle u | v \rangle$ gezeigt haben, folgt der Rest durch Ausmultiplizieren der Skalarprodukte.

1. Wir zeigen nun $\langle f(\lambda\vec{v}) - \lambda f(\vec{v}) | f(\lambda\vec{v}) - \lambda f(\vec{v})\rangle = 0$. Da das Skalarprodukt positiv definit ist, haben wir dann $f(\lambda\vec{v}) - \lambda f(\vec{v}) = \vec{0}$ bzw. $f(\lambda\vec{v}) = \lambda f(\vec{v})$ gezeigt.

$$\begin{aligned}\langle f(\lambda\vec{v}) &-\lambda f(\vec{v}) | f(\lambda\vec{v}) - \lambda f(\vec{v})\rangle \\ &= \langle f(\lambda\vec{v}) | f(\lambda\vec{v})\rangle - 2\lambda \langle f(\lambda\vec{v}) | f(\vec{v})\rangle + \lambda^2 \langle f(\vec{v}) | f(\vec{v})\rangle \\ &= \langle \lambda\vec{v} | \lambda\vec{v}\rangle - 2\lambda \langle f(\lambda\vec{v}) | f(\vec{v})\rangle + \lambda^2 \langle \vec{v} | \vec{v}\rangle \\ &= \langle \lambda\vec{v} | \lambda\vec{v}\rangle - 2\lambda \langle \lambda\vec{v} | \vec{v}\rangle + \lambda^2 \langle \vec{v} | \vec{v}\rangle \\ &= \lambda^2 \langle \vec{v} | \vec{v}\rangle - 2\lambda^2 \langle \vec{v} | \vec{v}\rangle + \lambda^2 \langle \vec{v} | \vec{v}\rangle \\ &= 0\end{aligned}$$

2. Wir zeigen nun, dass $f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$ gilt, indem wir $\langle f(\vec{u} + \vec{v}) - (f(\vec{u}) + f(\vec{v})) | f(\vec{u} + \vec{v}) - (f(\vec{u}) + f(\vec{v}))\rangle = 0$ zeigen.

$$\begin{aligned}\langle f(\vec{u} + \vec{v}) &- (f(\vec{u}) + f(\vec{v})) | f(\vec{u} + \vec{v}) - (f(\vec{u}) + f(\vec{v}))\rangle \\ &= \langle f(\vec{u} + \vec{v}) | f(\vec{u} + \vec{v})\rangle - 2 \langle f(\vec{u} + \vec{v}) | f(\vec{u}) + f(\vec{v})\rangle + \\ &\quad \langle f(\vec{u}) + f(\vec{v}) | f(\vec{u}) + f(\vec{v})\rangle \\ &= \langle \vec{u} + \vec{v} | \vec{u} + \vec{v}\rangle - 2(\langle f(\vec{u} + \vec{v}) | f(\vec{u})\rangle + \langle f(\vec{u} + \vec{v}) | f(\vec{v})\rangle) + \\ &\quad \langle f(\vec{u}) | f(\vec{u})\rangle + 2 \langle f(\vec{u}) | f(\vec{v})\rangle + \langle f(\vec{v}) | f(\vec{v})\rangle \\ &= \langle \vec{u} + \vec{v} | \vec{u} + \vec{v}\rangle - 2(\langle \vec{u} + \vec{v} | \vec{u}\rangle + \langle \vec{u} + \vec{v} | \vec{v}\rangle) + \\ &\quad \langle \vec{u} | \vec{u}\rangle + 2 \langle \vec{u} | \vec{v}\rangle + \langle \vec{v} | \vec{v}\rangle \\ &= \langle \vec{u} + \vec{v} | \vec{u} + \vec{v}\rangle - 2(\langle \vec{u} + \vec{v} | \vec{u} + \vec{v}\rangle) + \langle \vec{u} + \vec{v} | \vec{u} + \vec{v}\rangle \\ &= 0\end{aligned}$$

Aufgabe 2: Für eine positive ganze Zahl N bezeiche D_{2N} die von den Matrizen $R(N) := \begin{pmatrix} \cos\frac{2\pi}{N} & -\sin\frac{2\pi}{N} \\ \sin\frac{2\pi}{N} & \cos\frac{2\pi}{N} \end{pmatrix}$ und $S := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ erzeugte Untergruppe von $\mathrm{GL}(2, \mathbb{R})$. Zeigen Sie, dass D_{2N} eine nicht-kommutative Gruppe der Ordnung $2N$ ist. Zeigen Sie ferner, dass D_6 isomorph zur symmetrischen Gruppe S_3 ist.

1. Nicht kommutativ: Es ist z.B. $R(N) \cdot S \neq S \cdot R(N)$.
2. $\mathrm{ord}(D_{2N}) = 2N$: Das Element S hat Ordnung 2, $M := R(N)$ hat Ordnung N.

Wir bestimmen nun die Ordnung von SM: dazu berechnen wir $(SM)(SM)$ über die Zwischenschritte SM und MSM:

$$SM = \begin{pmatrix} \cos\frac{2\pi}{N} & -\sin\frac{2\pi}{N} \\ -\sin\frac{2\pi}{N} & -\cos\frac{2\pi}{N} \end{pmatrix}$$

$$MSM = \begin{pmatrix} \left(\sin\left(\frac{2\pi}{N}\right)\right)^2+\left(\cos\left(\frac{2\pi}{N}\right)\right)^2 & 0 \\ 0 & -\left(\sin\left(\frac{2\pi}{N}\right)\right)^2-\left(\cos\left(\frac{2\pi}{N}\right)\right)^2 \end{pmatrix}$$

$$SMSM = \begin{pmatrix} \left(\sin\left(\frac{2\pi}{N}\right)\right)^2+\left(\cos\left(\frac{2\pi}{N}\right)\right)^2 & 0 \\ 0 & \left(\sin\left(\frac{2\pi}{N}\right)\right)^2+\left(\cos\left(\frac{2\pi}{N}\right)\right)^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Damit hat auch das Element SM die Ordnung 2. ($SM = (SM)^{-1} = M^{-1}S^{-1} = M^{-1}S$.) Das gleiche Argument gilt auch für SM^k, da M^k wieder eine Rotationsmatrix ist (siehe letzte Übungsblatt).

Die Gruppe D_{2N} besteht aus den Elementen $1, S, M, \ldots, M^{N-1}$ und $SM, \ldots, SM^{N-1}$. $1, S, M^k$ sind offensichtlich voneinander verschieden. Die Annahme $M^j = SM^k$ führt auf $S = M^{j-k}$. Das würde bedeuten der Kosinus ist gleichzeitig 1 und -1. Widerspruch.

Damit besteht D_{2N} aus $2N$ Elementen.

3. $D_6 \cong S_3$: Wir geben einen Homomorphismus auf den Erzeugern der Gruppen an: $\varphi : D_6 \to S_3$, $\varphi(M) \mapsto (1,2,3)$ und $\varphi(S) \mapsto (2,3)$. Es ist $\varphi(S^jM^k) = \varphi(S)^j \circ \varphi(M)^j$ und da φ auf den Erzeugern definiert wurde, ist φ eine Bijektion.

Aufgabe 3: Sei p eine rationale Primzahl.Bestimmen Sie die Bahn und den Stabilisator von $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ unter der natürlichen Operation von $G = \mathrm{GL}(2, \mathbb{F}_p)$ auf $\mathbb{F}_p^2$. Folgern Sie Formeln für die Anzahl der Elemente von G und für die Anzahl der Elemente von $\mathrm{SL}(2, \mathbb{F}_p)$.

Wir bestimmen zunächst die Anzahl der Elemente der Bahn von $\vec{v} := \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. In $\mathbb{F}_p^2$ sind p^2 verschiedene Elemente. Eine Matrix $M := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}(2, \mathbb{F}_p)$ bildet $\vec{v}$ auf $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ ab. Weil M invertierbar ist gilt $\det M = ad - bc \not\equiv 0 \pmod p$. Einzig der Vektor $\left(\begin{smallmatrix} p \\ p \end{smallmatrix}\right)$ kommt nicht als Bild von $M\vec{v}$ in Frage, da dann $a = c = p$ und die Determinante gleich 0 wäre.

Wir halten fest: Die Bahn von $\vec{v}$ ist $\mathbb{F}_p^2 \setminus \left\{\vec{0}\right\}$, das sind $p^2 - 1$ Elemente.

Für den Stabilisator von $\vec{v}$ gilt: $\mathrm{Stab}_{\vec{v}} = \{M \in \mathrm{GL}(2, \mathbb{F}_p) \mid M\vec{v} = \vec{v} = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)\}$. Das sind diejenigen Matrizen $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}(2, \mathbb{F}_p)$ mit $a = 1, c = 0$ und $ad -$

$bc \not\equiv 0 \pmod p$, also $1 \cdot d - 0 \cdot b \not\equiv 0 \pmod p$. Davon gibt es aber genau $p(p-1) = p^2 - p$ Stück.

Fazit: Nach der Abzählformel besteht G aus $(p^2 - p)(p^2 - 1) = p^4 - p^3 - p^2 + p$ Matrizen.

Zur Bestimmung der Elemente von $\mathrm{SL}(2, F_p^2)$ benutzen wir den Homoorphismus $\varphi : \mathrm{GL}(2, \mathbb{F}_p^2) \to {\mathbb{F}_p}^*$, der durch $\varphi(M) = \det M$ gegeben ist. Aufgrund der Determinatenmultiplikationsformel ist das ein Homomorphismus (rechts steht die multiplikative Gruppe). Da alle Matrizen in $\mathrm{GL}(2, \mathbb{F}_p^2)$ invertierbar sind, sind alle Determinanten ungleich 0. Wir bilden in die invertierbaren Elemente von $\mathbb{F}_p$ ab. Der Kern sind diejenigen Matrizen, die auf 1 abgebildet werden, das ist gerade $\mathrm{SL}(2, \mathbb{F}_p^2)$.

Nach dem Isomorphiesatz gilt $\mathrm{GL}(2, \mathbb{F}_p^2) / \mathrm{SL}(2, \mathbb{F}_p^2) = {\mathbb{F}_p}^*$. Die Gruppe auf der rechten Seite besteht aus $p - 1$ Elementen, daraus folgt, dass $\mathrm{SL}(2, \mathbb{F}_p^2)$ aus $(p^2 - p)(p^2 - 1)/(p - 1) = (p^2 - p)(p + 1) = p^3 - p$ Elementen besteht.