

Definition der Permutationsgruppen

Definition (1.2)

Sei X eine Menge. Dann ist das Paar $(\text{Per}(X), \circ)$ bestehend aus der Teilmenge $\text{Per}(X) \subseteq \text{Abb}(X)$ der **bijektiven** Abbildungen $X \rightarrow X$ und der Komposition $\circ$ von Abbildungen eine Gruppe, die man als **Permutationsgruppe** der Menge X bezeichnet. Die Elemente von $\text{Per}(X)$ nennt man auch **Permutationen** von X .

Definition (1.3)

Ist $r \in \mathbb{N}$ und sind $k_1, \dots, k_r \in \mathbb{N}$ mit $k_1 \geq \dots \geq k_r \geq 2$, dann bezeichnet man das Tupel $(k_1, \dots, k_r)$ als **Zerlegungstyp** eines Elements $\sigma \in S_n$, wenn σ als Produkt disjunkter Zyklen der Längen $(k_1, \dots, k_r)$ dargestellt werden kann.

Satz (1.4)

Die Gruppe S_n ist für $n \leq 2$ abelsch und für $n \geq 3$ **nicht abelsch**.

Beweis von Satz 14

z.zg. (i) S_n abelsch für $n \leq 2$

(ii) S_n nicht abelsch für $n \geq 3$

zu (i) für $n=1$ klar, da $S_1 = \{\text{id}\}$

$n=2$

o	id	(12)
id	id	(12)
(12)	(12)	id

$$(12) \circ (12) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \text{id}$$

An der Symmetrie der Verknüpfungstabelle bzgl. der Diagonalen sieht man, dass S_2 abelsch ist.

Erinnerung:

- Das Signum auf der symm. Gruppe S_n ist eine Abbildung $\text{sgn}: S_n \rightarrow \{\pm 1\}$.
- wichtige Eigenschaften:

$$\forall \sigma, \tau \in S_n: \text{sgn}(\sigma \circ \tau) = \text{sgn}(\sigma) \text{sgn}(\tau)$$

Ist σ ein k -Zykel ($2 \leq k \leq n$), dann gilt $\text{sgn}(\sigma) = (-1)^{k-1}$. Mit diesen Regeln kann das Signum jedes Elements schnell berechnet werden.

$$\text{Bsp: } \sigma = (1234)(57)(689)$$

$$(\sigma \in S_9) \Rightarrow \text{sgn}(\sigma) = (-1)^{4-1} \cdot (-1)^{2-1} \cdot (-1)^{3-1} \\ = (-1) \cdot (-1) \cdot 1 = 1$$

- Die Elemente der Menge

$A_n = \{ \sigma \in S_n \mid \text{sgn}(\sigma) = 1 \}$ bilden
mit $\circ$ eine Gruppe, die sog. alternierende
Gruppe

weitere nicht-kommutative Gruppen: Lineare Gruppen

- (1) Ist $n \in \mathbb{N}$ und K ein Körper, dann ist das Paar $(\mathrm{GL}_n(K), \cdot)$ bestehend aus der Menge $\mathrm{GL}_n(K)$ der invertierbaren $n \times n$ -Matrizen über K mit der Multiplikation $\cdot$ von Matrizen als Verknüpfung die sog. allgemeine lineare Gruppe über dem Körper K .
- (2) Die Teilmenge $\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) \mid \det(A) = 1\}$ bildet mit der Multiplikation von Matrizen die spezielle lineare Gruppe.
- (3) Die orthogonale Gruppe $\mathcal{O}(n)$ besteht aus den Matrizen A mit der Eigenschaft ${}^t A \cdot A = E_n$. Die Menge

$$\mathrm{SO}(n) = \mathcal{O}(n) \cap \mathrm{SL}_n(\mathbb{R})$$

bildet die spezielle orthogonale Gruppe.

- (4) Über dem Körper $K = \mathbb{C}$ gibt es entsprechend die unitäre Gruppe $\mathcal{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t \bar{A} \cdot A = E_n\}$ und die spezielle unitäre Gruppe $\mathrm{SU}(n) = \mathcal{U}(n) \cap \mathrm{SL}_n(\mathbb{C})$.

Lineare Gruppen als endliche nicht-abelsche Gruppen

- Wir werden später sehen: Für jede Primzahlpotenz q gibt es einen (im Wesentlichen eindeutig bestimmten) Körper $\mathbb{F}_q$ mit q Elementen. Ist q keine Primzahl, dann ist dies allerdings **nicht** der Restklassenring $\mathbb{Z}/q\mathbb{Z}$.
- Für jedes $n \in \mathbb{N}$ und mit $n \geq 2$ und jede Primzahlpotenz q sind $\mathrm{GL}_n(\mathbb{F}_q)$ und $\mathrm{SL}_n(\mathbb{F}_q)$ **endliche nicht-abelsche Gruppen**.
- Es gilt

$$|\mathrm{GL}_n(\mathbb{F}_q)| = q^{\frac{1}{2}n(n-1)} \prod_{k=1}^n (q^k - 1) \quad \text{und} \quad |\mathrm{SL}_n(\mathbb{F}_q)| = q^{\frac{1}{2}n(n-1)} \prod_{k=2}^n (q^k - 1).$$

Beweis der Gleichung

$$|GL_n(\mathbb{F}_q)| = q^{\frac{1}{2}n(n-1)} \prod_{k=1}^n (q^k - 1)$$

falls $n \in \mathbb{N}$, q Primzahlpotenz, $q > 1$

bekannt aus der linearen Algebra:

Eine Matrix $A \in M_{n, \mathbb{F}_q}$ ist genau dann invertierbar, wenn das Tupel $(a_{\bullet 1}, \dots, a_{\bullet n})$ der Spaltenvektoren $a_{\bullet k} \in \mathbb{F}_q^n$ eine geordnete Basis des $\mathbb{F}_q^n$ bildet. $\Rightarrow$ genügt, die Anzahl der geordneten Basen des $\mathbb{F}_q^n$ zu bestimmen.

Beh.: Ist $m \in \mathbb{N}$ und V ein m -dim

$\mathbb{F}_q$ -Vektorraum dann ist die Anzahl
der geordneten Basen von V geg. durch

$$\prod_{k=1}^m (q^m - q^{k-1})$$

bekannt aus der Linearen Alg.

(Basisergänzungssatz): Jedes linear unabh.
System von Vektoren in V kann zu einer
Basis ergänzt werden.

Beh.: Die Anzahl der linear unabh. Tupel

in V bestehend aus k Elementen ($1 \leq k \leq m$)
ist gleich $\prod_{l=1}^k (q^m - q^{l-1})$

$k=1$: Anzahl der Tupel (v) mit $v \in V \setminus \{0_V\}$
ist gleich $q^m - 1 = \prod_{l=1}^1 (q^m - q^{l-1})$

$k \mapsto k+1$: Ein Tupel $(v_1, \dots, v_k, v_{k+1})$ in V ist genau
dann lin. unabh., wenn $(v_1, \dots, v_k)$ lin. unabh. ist
und $v_{k+1} \notin \langle v_1, \dots, v_k \rangle_{\mathbb{F}_q}$ gilt.

Anzahl der Mögl. für $(v_1, \dots, v_k)$ ist $\prod_{l=1}^k (q^m - q^{l-1})$

Ein Tupel $(v_1, \dots, v_k, v_{k+1})$ in V ist genau dann lin. unabh., wenn $(v_1, \dots, v_k)$ lin. unabh. ist

nach Ind.-V. $(v_1, \dots, v_k)$ lin. unabh. $\Rightarrow$ dim $\langle v_1, \dots, v_k \rangle_{\mathbb{F}_q} = k \Rightarrow |\langle v_1, \dots, v_k \rangle_{\mathbb{F}_q}| = q^k \Rightarrow q^m - q^k$ Mögl. für die Wahl von v_{k+1} . für das Tupel $(v_1, \dots, v_k, v_{k+1})$ insg.

$$\prod_{l=1}^k (q^m - q^{l-1}) \cdot (q^m - q^k) = \prod_{l=1}^{k+1} (q^m - q^{l-1})$$

$\Rightarrow$ insbesondere: V hat $\prod_{l=1}^m (q^m - q^{l-1})$ geordnete Basen.

außerdem:

$$\begin{aligned} \prod_{l=1}^m (q^m - q^{l-1}) &= \prod_{l=0}^{m-1} (q^m - q^l) = q^{\sum_{l=0}^{m-1} l} \prod_{l=0}^{m-1} (q^{m-l} - 1) \\ &= q^{\frac{1}{2}(m-1)m} \prod_{l=1}^m (q^l - 1) \end{aligned} \quad \square$$

Erinnerung:

- Eine **Bewegung** im $\mathbb{R}^n$ ist eine Abbildung $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ mit $\|\phi(v) - \phi(w)\| = \|v - w\|$ für alle $v, w \in \mathbb{R}^n$.
- Ist ϕ eine Bewegung, dann gibt es eindeutig bestimmte $u \in \mathbb{R}^n$ und $A \in \mathcal{O}(n)$, so dass $\phi(v) = u + Av$ für alle $v \in \mathbb{R}^n$ gilt.
- Ist $\det(A) = +1$, dann spricht man von einer **orientierungserhaltenden**, im Fall $\det(A) = -1$ von einer **orientierungsumkehrenden** Bewegung.

Definition (1.5)

Die Menge der Bewegungen im $\mathbb{R}^n$ bildet zusammen mit der Komposition eine Gruppe, die wir mit $\mathcal{B}_n$ bezeichnen. Die orientierungserhaltenden Bewegungen bilden ebenso eine Gruppe; diese bezeichnen wir mit $\mathcal{B}_n^+$.

Nachweis, dass B_n eine Gruppe ist.

- Zeige zunächst: Sind $\phi, \psi: \mathbb{R}^n \rightarrow \mathbb{R}^n$ Elemente von B_n , dann gilt dasselbe für $\phi \circ \psi$.

$$\phi \in B_n \Rightarrow \exists u \in \mathbb{R}^n, A \in O(n) \text{ mit} \\ \phi(v) = u + Av \quad \forall v \in \mathbb{R}^n$$

$$\psi \in B_n \Rightarrow \exists w \in \mathbb{R}^n, B \in O(n) \text{ mit} \\ \psi(v) = w + Bv \quad \forall v \in \mathbb{R}^n$$

$\Rightarrow$ erhalte für alle $v \in \mathbb{R}^n$:

$$(\phi \circ \psi)(v) = \phi(w + Bv) = u + A(w + Bv)$$

$$\phi(v) = u + Av \quad \forall v \in \mathbb{R}^n$$

$$w \in \mathbb{R}^n$$

$= (u + Aw) + ABv$, wobei $u + Aw \in \mathbb{R}^n$ und $AB \in O(n)$ (da $O(n)$ eine Gruppe ist)

$$\Rightarrow \phi \circ \psi \in \mathbb{B}_n$$

- Da $\circ$ assoziativ auf der Menge aller Abbildungen $\mathbb{R}^n \rightarrow \mathbb{R}^n$ ist, gilt dasselbe erst recht für die Abbildungen, die in $\mathbb{B}_n$ liegen.
- Für alle $v \in \mathbb{R}^n$ gilt $\text{id}(v) = v = 0_{\mathbb{R}^n} + E_n v$, und $E_n \in O(n) \Rightarrow \text{id} \in \mathbb{B}_n$. Wegen $\text{id} \circ \phi = \phi \circ \text{id} = \phi$ $\forall \phi \in \mathbb{B}_n$ ist $\text{id} \in \mathbb{B}_n$ ein Neutralelement in $(\mathbb{B}_n, \circ)$.

• Inverse: Sei $\phi \in \mathcal{B}_n$, zeige: ϕ ist bijektiv, und $\phi^{-1} \in \mathcal{B}_n$

$$\phi \in \mathcal{B}_n \Rightarrow \exists u \in \mathbb{R}^n, A \in \mathcal{O}(n) \text{ mit} \\ \phi(v) = u + Av \quad \forall v \in \mathbb{R}^n$$

bekannt: $A \in \mathcal{O}(n) \Rightarrow A$ ist invertierbar, und $A^{-1} \in \mathcal{O}(n)$

Für alle $v, w \in \mathbb{R}^n$ gilt die Äquivalenz

$$w = \phi(v) \iff w = u + Av \iff \\ w - u = Av \iff v = A^{-1}(w - u)$$

$\Rightarrow v = -A^{-1}u + A^{-1}w$ Dies zeigt:

$\phi^{-1}(w) = -A^{-1}u + A^{-1}w$, und wegen $-A^{-1}u \in \mathbb{R}^n$, $A^{-1} \in O(n)$ gilt $\phi^{-1} \in B_n$.

Wegen $\phi^{-1} \circ \phi = \text{id}$ und $\phi \circ \phi^{-1} = \text{id}$ ist ϕ^{-1} das Inverse von ϕ in B_n . $\square$

Die Symmetriegruppe einer Menge $T \subseteq \mathbb{R}^n$

Definition (1.5)

Die Menge der Bewegungen im $\mathbb{R}^n$ bildet zusammen mit der Komposition eine Gruppe, die wir mit $\mathcal{B}_n$ bezeichnen. Die orientierungserhaltenden Bewegungen bilden ebenso eine Gruppe; diese bezeichnen wir mit $\mathcal{B}_n^+$.

Definition (1.6)

Ist $T \subseteq \mathbb{R}^n$ eine beliebige Teilmenge, dann bezeichnet man

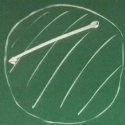
$$\text{Sym}(T) = \{\phi \in \mathcal{B}_n \mid \phi(T) = T\}$$

als **Symmetriegruppe** von T . Die Elemente von $\text{Sym}^+(T) = \text{Sym}(T) \cap \mathcal{B}_n^+$ bezeichnet man als **orientierungserhaltende Symmetrien** der Menge T .

Die konvexe Hülle einer Punktmenge

- Die **kleinste** konvexe Teilmenge des $\mathbb{R}^n$, die eine Teilmenge $X \subseteq \mathbb{R}^n$ enthält, wird die **konvexe Hülle** von X genannt und mit $\text{conv}(X)$ bezeichnet.
- Die konvexe Hülle einer endlichen Teilmenge vom $\mathbb{R}^n$ bezeichnet man als **Polytop**.
- Ist X nicht in einem echten affinen Unterraum des $\mathbb{R}^n$ enthalten, spricht man von einem **nicht ausgearteten** Polytop.

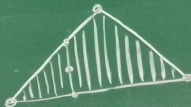
Bsp. für eine konvexe Teilmenge



nicht konvex:



konvexe Hülle



Definition (1.7)

Sei $n \in \mathbb{N}$ mit $n \geq 3$, und für $0 \leq k < n$ sei der Punkt $P_{n,k} \in \mathbb{R}^2$ gegeben durch

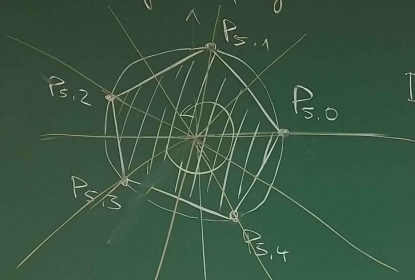
$$P_{n,k} = \left(\cos\left(\frac{2\pi k}{n}\right), \sin\left(\frac{2\pi k}{n}\right) \right).$$

Dann bezeichnen wir die konvexe Hülle der endlichen Punktmenge

$$\{P_{n,k} \mid 0 \leq k < n\}$$

als das **regelmäßiges Standard- n -Eck** Δ_n . Die Symmetriegruppe $D_n = \text{Sym}(\Delta_n)$ wird die n -te **Diedergruppe** genannt.

Beispiel: regelmäßiges Fünfeck



Elemente von

$$D_5 = \text{Sym}(A_5)$$

5 Spiegelungen

5 Drehungen

$$\text{insgesamt: } |D_5| = 10$$

Man kann zeigen:

$$D_5 = \{ \rho^k \mid 0 \leq k < 5 \} \cup \{ \rho^k \circ \tau \mid 0 \leq k < 5 \},$$

wobei $\rho = 72^\circ$ -Drehungen, τ Spiegelung an der x -Achse