Definition der Permutationsgruppen

Definition (1.2)

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

Definition (1.3)

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

Satz (1.4)

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

Sei $n \in \mathbb{N}$, $M_n = \{1, 2, \ldots, n\}$.

Symmetrische Gruppe in n Elementen

$$S_n = \mathrm{Bij}(M_n)$$

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Tabellenschreibweise

$\{a_1, \ldots, a_n\} = \{1, \ldots, n\}$

i) $|S_n| = n!$

ii) k-Zykel in S_n (wobei $2 \leq k \leq n$) = Element σ aus S_n, für das eine k-elementige Teilmenge $\{m_1, \ldots, m_k\} \subseteq M_n$ existiert, so dass σ gegeben ist durch

$$\sigma(x) = \begin{cases} m_{\tau+1} & \text{falls } x = m_\tau \text{ mit } \tau \in \{1, \ldots, k-1\} \\ m_1 & \text{falls } x = m_k \\ x & \text{sonst} \end{cases}$$

für alle $x \in M_n$. Schreibweise: $\sigma = (m_1\ m_2 \ldots m_k)$

Bsp.: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ 4)$

bekannt: Jedes Element aus S_n ungleich id ist als Produkt von endl. vielen disjunkten Zyklen darstellbar. (wobei disj. = kein gemeinsames Element in je zwei Zyklen des Produkts).

Anm: Die disjunkte Zykelzerlegung kann dazu genutzt werden, alle Elemente von S_n aufzuzählen.

Bsp: $n=3$ mögliche Zerlegungstypen id (+), (2) (−), (3) (+)
2-Zykel, 3-Zykel

$S_3 = \{ id, (12), (13), (23), (123), (132) \}$

beachte: $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$

$n=4$ mögliche Zerlegungstypen

$+$ $-$ $+$ $-$ $+$

id, (2), (3), (4), (2,2)

$S_4 = \{$ id, (12), (13), (14), (23), (24), (34),
(123), (132), (124), (142), (134), (143),
(234), (243), (1234), (1324), (1432),
(1243), (1342), (1423), (12)(34),
(13)(24), (14)(23) $\}$

Doppeltranspositionen

$n=5$ mögliche Zerlegungstypen

id, (2), (3), (4), (5), (2,2), (3,2)

Bem. Je zwei disjunkte Zykel sind vertauschbar, z.B. $(123)\circ(45) = (45)\circ(123)$

(ir) Erinnerung. Das Signum eines Elements $\sigma \in S_n$ ist definiert durch $\operatorname{sgn}(\sigma) = (-1)^r$, wobei r die Anzahl der Fehlstände von σ bezeichnet. (Fehlstand von σ = 2-elem. Teilmenge $\{i,j\}$ von M_n mit $i<j$ und $\sigma(i) > \sigma(j)$)

Regeln: (1) $\operatorname{sgn}(\sigma) = (-1)^{k-1}$ falls σ ein k-Zykel ist ($k \in \{2,\dots,n\}$)

(2) $\operatorname{sgn}(\sigma\circ\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ $\forall \sigma,\tau \in S_n$

4 3 2),

uschn-

lements

$(-1)^n$

d

lem.

und

ein

T)

$\tau \in S_n$

bekannt: Die Menge $A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ bildet mit $\circ$ ebenfalls eine Gruppe, die sog. alternierende Gruppe. Es gilt $|A_n| = \frac{1}{2} n!$ für $n \geq 2$. ($S_1 = A_1 = \{id\}$)

Bsp. $n=3$ $A_3 = \{id, (123), (132)\}$

$n=4$ $A_4 = \{id, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

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 ${}^{\mathrm{t}}A \cdot A = E_n$. 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 $\mathcal{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid {}^{\mathrm{t}}\bar{A} \cdot A = E_n\}$ 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 $q > 1$ 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 $q > 1$ 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 $|GL_n(\mathbb{F}_q)| = q^{\frac{1}{2}n(n-1)} \prod_{k=1}^{n} (q^k - 1)$

- Eine Matrix $A \in M_{n,\mathbb{F}_q}$ ist genau dann invertierbar, wenn das Tupel $(v_1, \dots, v_n)$ der Spalten von A ($v_k = a_{\cdot k}$, $1 \le k \le n$) linear unabh. ist $\rightarrow$ genügt, die Anzahl dieser Tupel zu bestimmen
- Erinnerung Basisergänzungssatz: Jedes linear unabh. Tupel aus Elt. von $\mathbb{F}_q^n$ kann zu einer (geordn.) Basis (= n-elem lin. unabh. Tupel) ergänzt werden.

$\Rightarrow$ Jede geordnete Basis $(v_1, \dots, v_n)$ kann durch sukzessive

Wahl der Vektoren $v_1, \dots, v_n$ geschieht wie folgt.

- Mögl. für die Wahl von v_1 : $q^n - 1$
  (alle Vektoren aus $\mathbb{F}_q^n \setminus \{0_{\mathbb{F}_q^n}\}$)
- Möglichkeiten für die Wahl von v_2 : $q^n - q$
  (alle Vektoren aus $\mathbb{F}_q^n \setminus \langle v_1 \rangle_{\mathbb{F}_q}$)
- Möglichkeiten für v_3 : $q^n - q^2$
  (alle Vektoren aus $\mathbb{F}_q^n \setminus \langle v_1, v_2 \rangle_{\mathbb{F}_q}$)
- allgemein: Sind $v_1, \dots, v_{k-1}$ schon gewählt, gibt es noch $q^n - q^{k-1}$ Möglichkeiten für die Wahl von v_k

$$\Rightarrow |GL_n(\mathbb{F}_q)| = \prod_{k=1}^{n} (q^n - q^{k-1}) = \prod_{k=0}^{n-1} (q^n - q^k) =$$

$$q^{0+1+\cdots+n-1} \prod_{k=0}^{n-1} \left(q^{n-k}-1\right) = q^{\frac{1}{2}(n-1)n} \prod_{k=1}^{n} \left(q^{k}-1\right)$$

Die Bewegungsgruppen

Erinnerung:

- Eine Bewegung im $\mathbb{R}^n$ ist eine Abbildung $\phi : \mathbb{R}^n \to \mathbb{R}^n$ 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 $\mathcal{B}_n^+$.

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

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

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

zu Definition 1.5:

Nachweis der Gruppeneigenschaft von B_n:

- zeige: Für alle $\phi, \psi \in B_n$ gilt $\psi \circ \phi \in B_n$.
  ($\Rightarrow \circ$ ist eine Verknüpfung auf B_n)

Seien $\phi, \psi \in B_n \Rightarrow \exists\, u, v \in \mathbb{R}^n,\ A, B \in O(n)$
mit $\phi(x) = u + Ax$, $\psi(x) = v + Bx$ $\forall x \in \mathbb{R}^n$

$\Rightarrow$ Für jedes $x \in \mathbb{R}^n$ gilt $(\psi \circ \phi)(x) =$
$\psi(\phi(x)) = \psi(u + Ax) = v + B(u + Ax)$
$= v + Bu + BAx$. ($v + Bu \in \mathbb{R}^n$, $BA \in O(n)$) $\Rightarrow \psi \circ \phi \in B_n$

- Für alle $\varphi, \phi, \psi \in B_n$ gilt $(\varphi \circ \phi) \circ \psi = \varphi \circ (\phi \circ \psi)$,
da diese Gl. sogar für Bel. Abb. $\varphi, \phi, \psi : \mathbb{R}^n \to \mathbb{R}^n$

1) gültig ist.

- Neutralelement: Für alle $\phi \in B_n$ gilt $\phi \circ id_{\mathbb{R}^n} = id_{\mathbb{R}^n} \circ \phi = \phi$, und $id_{\mathbb{R}^n}$ liegt in B_n wg. $\| id_{\mathbb{R}^n}(v) - id_{\mathbb{R}^n}(w) \| = \|v - w\|$ für alle $v, w \in \mathbb{R}^n$
- Inverse: bekannt: Jedes $\phi \in B_n$ ist Bijektiv, besitzt also eine Umkehrabb. ϕ^{-1}. Für diese gilt $\phi^{-1} \circ \phi = \phi \circ \phi^{-1} = id_{\mathbb{R}^n}$. genügt z.zg.: Für jedes $\phi \in B_n$ gilt $\phi^{-1} \in B_n$. Sei also $\phi \in B_n$
$\Rightarrow \exists u \in \mathbb{R}^n, A \in O(n)$ mit $\phi(x) = u + Ax$
$\forall x \in \mathbb{R}^n \quad \forall x, y \in \mathbb{R}^n : y = u + Ax \Longrightarrow$

$y - u = Ax \iff A^{-1}(y-u) = x \iff$

$x = (-A^{-1}u) + A^{-1}y$

$(-A^{-1}u) + A^{-1}y \quad \forall y \in \mathbb{R}^n$

also: $\phi^{-1}(y) =$

$-A^{-1}u \in \mathbb{R}^n \quad \phi^{-1} \in B_n$

$\Rightarrow$

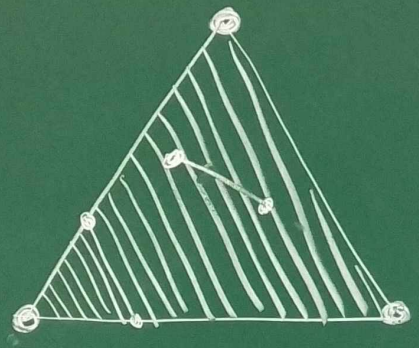
$A^{-1} \in O(n)$

□

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 $\mathrm{conv}(X)$ 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.

Beispiel: konvexe Hülle von drei Punkten



Die Diedergruppen

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

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

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 $D_n = \mathrm{Sym}(\Delta_n)$ wird die n-te Diedergruppe genannt.

Beispiel: $\mathrm{Sym}(T)$ für T = regelmäßiges 5-Eck



ρ = 72° - Drehung

τ = Spiegelung (bzgl. der ang. Achse)

$\tau \circ \rho \circ \tau = \rho^{-1} \iff$

$\tau \circ \rho = \rho^{-1} \circ \tau \neq \rho \circ \tau$ (da $\rho \neq \rho^{-1}$)

- 5 Drehungen (Drehwinkel 0°, 72°, 144°, 216°, 288°)
- 5 Spiegelungen (jeweils durch eine Seite und die gegenüberliegende Ecke)

insgesamt: Die Symmetriegruppe des regelmäßigen 5-Ecks, die Diedergruppe, ist eine 10-elementige (nicht-abelsche) Gruppe