Gruppen & ihre Darstellungen

WS 2020/2021 SoSe 2024

M. Baake / (N. Mañibo) J. Mazáč

- etwas Gruppentheorie
  - Struktur
  - Permutationen
  - abelsche Gruppen

- Darstellungstheorie (über $\mathbb{C}$)
  - lineare Darstellungen
  - Darstellungen & Charaktere
  - Beispiele
  - Tensorprodukte

- kompakte Gruppen
  - Lie-Gruppen, Haar-Maß
  - Matrix-Gruppen
  - Peter-Weyl-Theorem
  - Charakterformel

Ausblick: Symmetrien in der Physik

Literatur:

- M. Hall, The Theory of Groups, reprint, Chelsea (1959)
- B. Simon, Representations of Finite and Compact Groups, AMS (1996)

H. Boseck, Grundlagen der Darstellungstheorie, VEB/DVdW (1973)

H. Boerner, Darstellungen von Gruppen, 2. Aufl., Springer (1967)

J.-P. Serre, Linear Representations of Finite Groups, Springer (1977)

M. Hamermesh, Group Theory and its Application to Physical Problems, Dover (1989)

W. Lucha & F.F. Schöberl, Gruppentheorie, BI (Spektrum) (1993)

- G. James & M. Liebeck, Representations and Characters of Groups, 2. Aufl., CUP (2001)

(weitere Lit. im Laufe der VL)

Warum Gruppentheorie?

"The miracle of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor deserve."

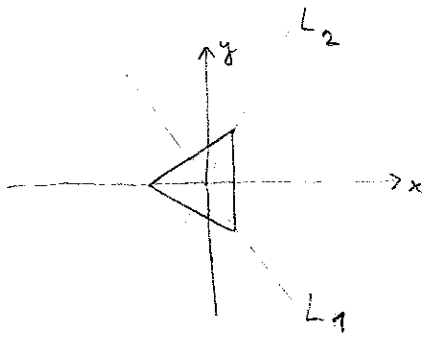
E. P. Wigner, in: The unreasonable effectiveness of mathematics", Commun. Pure Appl. Math. 13 (1969) 1 – 14.

Gruppen und ihre Darstellungen treten auf in:

- klass. Mechanik (→ Symm., Noether-Theorem)
- Kristallographie (→ Punkt-, Raumgruppen)
- Relativitätstheorie (→ Lorentzgruppe)
- Quantenmechanik (→ Spin, SU(2), Entartung)
- Feldtheorie (→ Eichtheorie)
- Euklidische Geometrie (→ "Symmetrie")

u. v. a. m. !

(Ex.)



Symm. des gleichs. Δ

$\mathbb{R}^2 \simeq \mathbb{C}$

1) <u>Drehungen:</u> $R(z) = e^{2\pi i/3} \cdot z \quad \left(\hat{=} \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix} \right)$

$\mathbb{1}, R, R^2, R^3 = \mathbb{1} \quad \curvearrowright \quad \langle R \rangle \simeq C_3$ <u>Gruppe</u>

2) <u>Spiegelungen:</u> $(S : \mathbb{C} \to \mathbb{C}, \; z \mapsto S(z) = \bar{z})$

S (Spiegelung an der x-Achse) $\quad z \mapsto \bar{z}$

RSR^{-1} (Spiegelung an L_1) $\quad z \mapsto e^{4\pi i/3}\bar{z}$

R^2SR^{-2} (Spiegelung an L_2) $\quad z \mapsto e^{2\pi i/3}\bar{z}$

$S^2 = \mathbb{1}$

<u>Also:</u> $\text{Symm}(\Delta) = \{1, R, R^2, S, RSR^{-1}, R^2SR^{-2}\}$

<u>Bem.:</u> $R^{-1} = R^2, \; R^{-2} = R, \; RS = SR^2 = SR^{-1}$

<u>Bew.:</u> 1. & 2. Beh. klar. 3. Beh. kann man "sehen", aber ein Bew. geht so:

$$RS(z) = R(S(z)) = R(\bar{z}) = e^{2\pi i/3}\bar{z}$$

$$= \overline{e^{-2\pi i/3}}\,\bar{z} = S(e^{-2\pi i/3}z) = S(R^{-1}(z))$$

$$= S(e^{4\pi i/3}z) = S(R^2(z))$$

□

$\Rightarrow$ (allgemeiner) $\boxed{R^m S = SR^{-m}} \quad (m \in \mathbb{Z})$

Also: $\mathrm{Symm}(\Delta) = \{ R^m S^n \mid 0 \le m \le 2,\ 0 \le n \le 1 \}$

Nun ist:

- $R^m S^n R^k S^l = R^m R^{(-1)^n k} S^n S^l = R^{m+(-1)^n k} S^{n+l}$
  $= R^{(m+(-1)^n k \bmod 3)} S^{(n+l) \bmod 2}$
- Es gilt (klar!) das Assoziativgesetz
- Es gibt ein Einselement, $\mathbb{1} = R^0 \cdot S^0$
- $R^m S^n \cdot R^{m'} S^n = R^{m+(-1)^n m'} S^{2n} = R^0 S^0 = \mathbb{1}$
  für $m' = (-1)^{n+1} m$
- Regeln: $R^3 = S^2 = (RS)^2 = \mathbb{1}$

<u>Satz:</u> $\mathrm{Symm}(\Delta) = \{ R^m S^n \mid R^3 = S^2 = (RS)^2 = \mathbb{1} \}$ ist eine <u>Gruppe</u> (wie in LA def.) bzgl. $\circ$ als Gruppenmultiplikation.

<u>Bew.:</u> $RSRS = \mathbb{1}$

$S^2 = \mathbb{1} \Rightarrow RSR = S \quad \overset{R^3 = \mathbb{1}}{\Rightarrow} \quad RS = SR^2 = SR^{-1}$

$\Rightarrow R^m S \overset{\circledast}{=} S R^{-m}$ für $m \in \mathbb{N}$ per Induktion

Außerdem: $RSRS = \mathbb{1}$

$R^3 = \mathbb{1} \Rightarrow SRS = R^2 \Rightarrow SR = R^{-1} S \Rightarrow \circledast$ für $m \in \mathbb{Z}$

$\Rightarrow$ Regeln legen $\mathrm{Symm}(\Delta)$ fest! Rest klar. □

<u>Abstrakt:</u>

$D_3 := \{ r^m s^n \mid r^3 = s^2 = (rs)^2 = e \}$

"dihedrale Gruppe"

(Ex) $S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

abelsche Gruppe, aber nicht endlich!

Die Abstraktion führt auf das Konzept der Gruppe aus der LA, mit einer Ergänzung:

Def.: Eine top. Gruppe ist eine Gruppe G, versehen mit einer Topologie (hausdorffsch), so daß die Gruppenoperationen stetig sind:
↳ erläutern!

$$P: \quad G \times G \longrightarrow G, \quad (g,h) \longmapsto g \circ h$$

$$I: \quad G \longrightarrow G, \quad g \longmapsto g^{-1}$$

(erläutern!)

Bem.:
- Bei endl. Gruppen nimmt man die diskrete Top., was dann nichts hinzufügt.
- Kompakte Gruppen sind "fast" so gut wie endl. Gruppen, wegen Heine-Borel (erläutern!)

Lit.: Topologie ↷ B. v. Querenburg, Mengentheor. Topologie

FAPP: Top. durch offene Mengen mittels Metrik erzeugt ("metr. Top.")

Def.: Sei X eine Menge. Ein System $\mathcal{O}$ von Teilmengen von X heißt **Topologie von X**, wenn:

(a) $O_i \in \mathcal{O},\ i \in I \Rightarrow \bigcup_{i \in I} O_i \in \mathcal{O}$ (I bel.)

(b) $O_1, \dots, O_n \in \mathcal{O} \Rightarrow \bigcap_{i=1}^{n} O_i \in \mathcal{O}$ ($n \geq 1$)

(c) $\emptyset, X \in \mathcal{O}$

Damit heißt $(X, \mathcal{O})$ **top. Raum**. Die Elemente von $\mathcal{O}$ sind die **offenen Mengen**, ihre Komplemente **abgeschlossen**. $\emptyset$ und X sind "**clopen**".

(Ex) • X endl. $\curvearrowright$ $\mathcal{O} = \mathcal{P}(X)$ (Potenzmenge)
diskrete Top.

• $X = \mathbb{R}$, $\mathcal{O}$: alle Vereinigungen von (a,b) mit $a, b \in \mathbb{R}$ $(a \leq b)$

Def.: $(X, \mathcal{O}_1)$, $(Y, \mathcal{O}_2)$ seien top. Räume.

$f: X \to Y$ heißt **stetig**, wenn die Urbilder offener Mengen offen sind; also wenn gilt:

$$\forall\, O \in \mathcal{O}_2 : f^{-1}(O) \in \mathcal{O}_1$$

Bem.: • Dies verallgemeinert den bekannten Stetigkeitsbegriff des $\mathbb{R}^d$ (→ Übung)

• kompakt $:\Leftrightarrow$ jede Überdeckung besitzt endl. Teilüberdeckung, & hausdorffsch

Def.: Ein Raum (eine Gruppe) heißt **lokal kompakt**, wenn jeder Punkt eine kompakte Umgebung besitzt.

(Ex) • Jede komp. Gruppe ist lokal kompakt

• $(\mathbb{R}^d, +)$ ist LCAG, und das wichtigste Beispiel für die Physik

Bem.: Fourier-Analysis geht besonders gut auf LCAGs !

(Ex) $\mathcal{S}(\mathbb{R}^n)$, $\mathcal{S}'(\mathbb{R}^n)$: Distributionen

L. Schwartz, Théorie des Distributions, Hermann, Paris (3. Aufl. 1998)

Ab jetzt schauen wir Gruppen etwas "abstrakter" an, also $G = (\text{Menge}, \circ)$, und schreiben e_G (oder e) für das neutrale Element.

Nun brauchen wir ein Konzept für einen **Vergleich**. Wir beschränken uns dafür zunächst auf **endl.** Gruppen (Top. trivial).

(G, H seien endl. Gruppen)

Def.: Eine Abb. $\varphi: G \to H$ heißt **Homomorphismus** wenn gilt: $\varphi(xy) = \varphi(x)\varphi(y)$.

Insbesondere ist $\varphi(e_G) = e_{\varphi(G)}$ und $\varphi(x^{-1}) = \varphi(x)^{-1}$, denn mit $x' = \varphi(x)$ folgt:

$$\varphi(e_G) \cdot x' = \varphi(e_G) \cdot \varphi(x) = \varphi(e_G x) = \varphi(x) = x' = e_{\varphi(G)} \cdot x'$$

+ kürzen

und:

$$\varphi(x^{-1}) \cdot x' = \varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1} x) = \varphi(e_G) = e_{\varphi(G)}$$

Auch die Assoziativität wird vererbt, und $\varphi(G) \subseteq H$ ist eine **Gruppe**.

Ist φ surjektiv und injektiv, heißt φ **Isomorphismus** und $G \simeq H$ bedeutet: G und H sind isomorph.

(Ex.) $(S^1, \cdot) \simeq ([0,1), +_{\text{mod } 1})$

$$e^{2\pi i x} \quad \overset{\varphi}{\longleftrightarrow} \quad x_{\text{mod } 1}$$

[Bem.: Hier zus. Stetigkeit fordern!]

Es genügt offensichtlich, Gruppen bis auf Isomorphie zu kennen! Dazu später mehr.

Def.: $\mathrm{Aut}(G) = \{\varphi \mid \varphi: G \to G \text{ ist Isomorph.}\}$

$\mathrm{Aut}(G)$ ist eine **Gruppe**, mit $\varphi\psi := \varphi \circ \psi$; $e_{\mathrm{Aut}(G)} = \mathrm{id}$

eine wichtige Untergruppe bilden die **inneren Automorphismen:**

$$i_x: G \to G$$
$$g \mapsto i_x(g) = x g x^{-1}$$

Def.: Eine Untergruppe $N \leq G$ heißt **Normalteiler**
$:\Leftrightarrow \; i_x(N) = xNx^{-1} = N, \quad \forall x \in G$ ("normal subgroup")

(Ex.) $\{e\}$, G sind (triviale) Normalteiler von G.
Jede Untergruppe einer abelschen Gruppe ist NT.

Def.: Eine Gruppe (G) heißt **einfach**, wenn es nur die beiden trivialen Normalteiler gibt.

Bem.: Einfache Gruppen sind so etwas wie die "Primzahlen" der Gruppentheorie.
→ klassifiziere die endl. einfachen Gruppen!
Es ist nicht klar, ob das Ziel momentan schon erreicht ist ∇
↷ Aschbacher
Conway / Sloane
Gorenstein: "The enormous theorem"
Borcherds: "Monsters and Moonshine"
Lange Geschichte, inzwischen wohl gesichert

(Ex.) $Y \simeq A_5$ ist einfach

⇒ Polynome vom Grad ≥ 5 lassen i.a. keine Nullstellenformel mit Radikalen zu!
↷ Galois-Theorie, vgl. Fraleigh, kap. 8.

Um das besser zu verstehen, müssen wir uns mit Permutationsgruppen beschäftigen.

Notation: $\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$

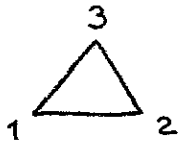
(Ex.) S_3:

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Geometrisch:



Symmetrien: 3 Drehungen, 3 Spiegelungen

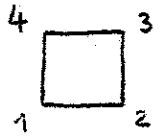
Algebraisch (abstrakt):

$$D_3 = \{ g^n h^m \mid g^3 = h^2 = (gh)^2 = e \}$$

"dihedrale Gruppe"

Übung: Studiere die 3 Versionen, zeige Isomorphie.

(Ex.)



$\leftrightarrow$ D_4 $\leftrightarrow$ $G \subset S_4$

Übung: (a) Vergleiche und zeige Isomorphie.

(b) Stelle vollständiges Gruppen-Untergruppen-Diagramm von D_4 auf ("Verband").

Prop.: $\varphi : G \to H$ sei Gruppenhomomorphismus. Dann ist $\mathrm{Im}(\varphi) = \{ \varphi(x) \mid x \in G \}$ Untergruppe von H und $\ker(\varphi) = \{ x \in G \mid \varphi(x) = e_H \}$ Normalteiler von G.

Bew.: Teil 1 hatten wir schon.

Also $\ker(\varphi)$:

$x, y \in \ker(\varphi) \Rightarrow \varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H \cdot e_H^{-1} = e_H$

$\Rightarrow xy^{-1} \in \ker(\varphi)$, also Untergruppe.

$g \in G,\ x \in \ker(\varphi) \Rightarrow gxg^{-1} \in \ker(\varphi)$, denn:

$$\varphi(gxg^{-1}) = \varphi(g)\, e_H\, \varphi(g)^{-1} = e_H$$

$\Rightarrow g \ker(\varphi) g^{-1} \subseteq \ker(\varphi)$, also NT. □

Def.: Eine bijektive Abb. $\tau : A \to A$ heißt Permutation von A. $A \xrightarrow{\tau} A \xrightarrow{\sigma} A$ ist durch Komposition erklärt:

$\sigma\tau(a) := (\sigma \circ \tau)(a) = \sigma(\tau(a))$.

Sätzchen: Sei S_A die Menge der Perm. von A. Dann ist $(S_A, \circ)$ eine Gruppe, die Perm.gr. von A.

Bew.: Übung in Axiomatik – anschaulich klar!

Def.: Ist $A = \{1, \dots, n\}$, so heißt $S_n = S_A$ die symmetrische Gruppe von n Symbolen.

Prop.: $|S_n| = n!$

Bew.: Es gibt $n!$ versch. Anordnungen von n Symbolen. □

S_n besitzt interessante Untergruppen!

① $\operatorname{sgn}: S_n \to (\mathbb{Z}_2 \cong) C_2 \qquad C_2 = \{e, g\} : g^2 = e$

$\pi \mapsto \operatorname{sgn}(\pi) = (-1)^{\pi}$

Vandermonde Polynom:

$$V(x_1, \dots, x_n) = \prod_{i<j} (x_j - x_i)$$

$$\curvearrowright \quad V(x_{\pi(1)}, \dots, x_{\pi(n)}) = \pm V(x_1, \dots, x_n)$$

$$\curvearrowright \quad \boxed{\operatorname{sgn}(\pi) := \frac{V(x_{\pi(1)}, \dots, x_{\pi(n)})}{V(x_1, \dots, x_n)}}$$

Beh.: sgn ist Gruppenhomomorphismus.

Bew.: Übung!

Ⓔx $\pi = (12) = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix} \Rightarrow \operatorname{sgn}(\pi) = -1.$

π ist eine sog. Transposition.

Def.: $A_n = \{\pi \in S_n \mid \operatorname{sgn}(\pi) = 1\} = \ker(\operatorname{sgn})$ heißt alternierende Gruppe.

Sätzchen: A_n ist Normalteiler von S_n, $|A_n| \overset{(n \geq 2)}{=} \frac{n!}{2}$

Bew.: $A_n = \ker(\operatorname{sgn})$; $S_n = A_n \cup (12) \cdot A_n \quad (n \geq 2)$ □

Folgerung: S_n ist einfach $\Leftrightarrow n \in \{1, 2\}$.

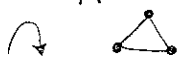
Bew.: Für $n \geq 3$ ist $|\{e\}| = 1 < \frac{n!}{2} = |A_n| < n! = |S_n|$.

$n=1$: $A_1 = S_1$; $n=2$: $A_2 = \{e\}$; Rest klar! □

(Ex.)

$A_2 \simeq \{e\}$ (triviale Gruppe)

$A_3 \simeq C_3$ (zykl. Gruppe der Ordnung 3)



$A_4 \simeq T$ (Tetraedergruppe !)

↷ 4 Ecken des Tetraeders

$A_5 \simeq Y$ (Ikosaedergruppe !)

↷ $Y = \langle \tau, u \mid \tau^3 = u^2 = (\tau u)^5 = e \rangle$

$u \hat{=} (24)(35)$, $\tau \hat{=} (143)$, $\tau u \tau \hat{=} (12345)$

Satz: A_n ist einfach für $n \geq 5$, sowie (trivialerweise) für $n = 2$ und $n = 3$.

(ohne Beweis)

$\simeq C_p = \langle x \mid x^p = e \rangle$

Satz: $\mathbb{Z}_p$, p eine Primzahl, ist einfach.
Weitere endl. abelsche Gruppen, die einfach sind, gibt es nicht!

Bew.: $\mathbb{Z}_p = C_p$ besitzt überhaupt nur die trivialen Untergruppen, also insbesondere keine nicht-triv. Normalteiler. s. u.

Andere abelsche Gruppen besitzen aber stets weitere Untergruppen (→ kommt später noch einmal!), die dann automatisch Normalteiler sind (!) □

Satz: Jede endl. einfache nicht-abelsche Gruppe besitzt gerade Ordnung!

(Vers. von Burnside, Bew.: Thompson & Feit, '64)

(Ex.) "Monster": $|M_{\text{Griess}}| = 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000.$

Nachtrag:

$x, x^2, \dots, x^p = e \quad \curvearrowright \quad |C_p| \leq p$

Falls $\{x, x^2, \dots, x^p\}$ paarw. versch., ist $|C_p| = p$;
sonst $x^m = x^n$ für $1 \leq m < n \leq p$,
also $x^{n-m} = e$ mit $1 \leq n-m \leq p-1 < p$ ↯

Sei $H \subseteq C_p$ Untergruppe, $y \in H$, $|H| \leq p$
$\Rightarrow \{y, y^2, \dots\} \subseteq H$.
Nun ist $y = e$ (triv. Fall) oder $y = x^r$, $1 \leq r \leq p-1$,
$\Rightarrow x^r, x^{2r}, \dots$ in H und $x^{kr} = x^{lr}$ für $k \neq l$
nach Dirichlet'schem Schubfachschluss
$\Rightarrow x^{(l-k)r} = e \quad \Rightarrow \quad p \mid (l-k) \cdot r$, mit $1 \leq k < l \leq p+1$

p prim, $p \nmid r$ $\Rightarrow$ $p \mid (l-k)$ $\overset{l \neq k}{\Rightarrow}$ $l = k + p$ $\Rightarrow$ $x^{pr} = e$, p min.

$\Rightarrow$ Beh. □