Permutationsgruppen WS 20/21

Prof. Pöschel

3. Dezember 2020

Inhaltsverzeichnis

Preface

The plan is to go rather fast through the first chapter of this book(to get fast to K-Theory), take some notes, write down ideas, examples and remarks, rewrite proofs, so that i can understand them in my way. Also add sometimes reminders to concepts/definitions, so that i have a good overview about vector bundles and of course K-Theory. I will also use notation from courses i took in the past. But I will put remarks for the reader. Hope you will find these notes helpful in any way.

ScyllaHide, 3. Dezember 2020

0. Einführung

mathematische Strukturen:

$$\begin{tikzcd}
 & \text{math. Strukturen} \arrow[dl] \arrow[d] \arrow[dr] & \\
\text{alg. Struk} \arrow[d] & \text{relat./Ordstruk} & \text{top. Struk} \\
\text{Menge+Op.} \arrow[d] & & \\
\text{z.B Gruppe} & &
\end{tikzcd}$$

Definition 0.1
Gruppe $< G, \cdot, ^{-1}, e >$

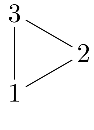
- G Gruppe
- e neutrales Element zu x
- x^{-1} inverses Element zu x
- $x \cdot y$ (meist xy) "Produkt", binäre Operation

Axiome:

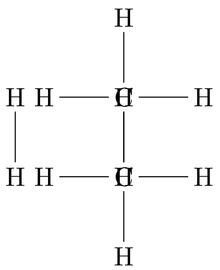
$$\begin{aligned}
\forall x \in G &: ex = xe = x \\
\forall x \in G &: xx^{-1} = x^{-1}x = e \\
\forall x, y, z \in G &: x(yz) = (xy)z
\end{aligned}$$

■ **Beispiel 0.2**

1. Symmetriegruppen (geom.): isometrische Abbildung der Ebene
   Drehungen: 0°, 120°, 240°
   Spiegelung: s_0, s_1, s_2
   Also 6 Symmetrieoperationen ($\cong$ volle symmetrische Gruppe S_3)

2. Automorphismen (algebraisch bzw. kombinatorisch): Dreieck als Graph betrachten Automorphismen (bijektive Abbdildung, die Kanten in Kanten überführen). Also Aut(Dreieck) $\cong S_3$



- Spiegelungen an horizontalen Achse
- Es gibt zahlreiche Automorphismen (Fixpunkte: 0,1,2,3,4) viele Vertauschungen

$$|S_2 \times S_2 \times S_3| = 24$$

Γ, Γ' sind "im Prinzip" das gleiche. $\exists$ Isomorphismus $f\colon \Gamma \to \Gamma'$. Das führt auf ein Isomorphieproblem: Wann sind zwei Strukturen isomorph?

► **Bemerkung 0.3**
Isomorphieproblem zurückführbar auf Bestimmung von Automorphismen:

$$\text{als Automrophismus von } \Gamma \cup \Gamma' \begin{cases} f & : \Gamma \to \Gamma' \\ f & : \Gamma' \to \Gamma \end{cases}$$

Spezialität der Symmetrien bzw. Automorphismen: haben innere Struktur sind bijektive Abbildungen (=: Permutationen) $\Rightarrow$ Permutationsgruppen.

■ **Beispiel 0.4**
zum Isomorphieproblem
chemische Isomere: Wieviel verschiedene Alkohole (Propanole, d.h. Bindungsgruppen O−H) mit Strukturformel C_3H_7OH gibt es?
Antwort: Γ siehe oben. und Γ'', wobei Γ's Siedepunkt = 97,1°C und Γ'' = 82,4°C.

► **Bemerkung 0.5**
gleiche Summenformel:

Im Allgemeinen Lösung: Anzahl lässt sich als die Anzahl der sogenannten "Bahnen" (eng. Orbit) einer Permutationsgruppe beschrieben. (bestimmbar mit Lemma von Cauchy-Frobenius-Burnside). $\Rightarrow$ Abzählbartheoreme (Polya).

■ **Beispiel 0.6**
anderes Beispiel für Polyasche Abzählbartheorie:
Wieviele wesentlich verschiedene Ketten mit 3 Sorten von Perlen gibt es? (n_i Perlen der Sorte $i = 1, 2, 3$)

- Permutationsgruppen sind spezielle Gruppen und trotzdem "mehr" als Gruppen
- Automorphismengruppen besonders wichtige (von algebraische Struktur)

Gruppentheoretisch ist aus den Permutationsgruppen entstanden (Galoistheorie) Galoisgruppe = Permutationsgruppe

■ **Beispiel 0.7**
für Permuationen

- S_n volle symmetrische aller Permutation auf n-elementiger Menge

- lin. Abbildung eines Vektorraumes

  $$x \mapsto Ax + b$$

  wobei A invertierbare Matrix ist

Vorlesungsinahlt

- Permutations- und Gruppenwirkung
- Konstruktionen mt Permutationsgruppen
- Polyasche Abzählungstheoreme
- Automorphismengruppen von Relationen

1. Permutationen und Permutationsgruppen

Permutationen können unterschiedlich definiert und dargestellt werden:

1. als Lineare Anordnung von Elementen einer Menge, z.B. $M = \{a, b, c\}$

   $$\begin{aligned} &\pi_1 : abc && \pi_2 : acb \\ &\pi_3 : bac && \pi_4 : bca \\ &\pi_5 : cab && \pi_6 : cba \end{aligned}$$

2. als bijektive Abbildung (in 2-Zeilen-Darstellung)

   $$\pi_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \pi_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \dots, \pi_6 = ...$$

   allgemein

   $$\pi = \begin{pmatrix} a_1 & \dots & a_n \\ \vdots & & \vdots \\ a_{1i} & \dots & a_{1n} \end{pmatrix}$$

   bezeichnen. Also Abbildung $\pi\colon M \to M$ mit $a_k \mapsto a_{i_k}$, wobei $M = \{a_1, \dots, a_n\}$ Reihenfolge der Spalten spielt keine Rolle.

Definition 1.1
Eine Permutation auf Menge M ist bejektiv Abbildung $f\colon M \to M$

$$S_m := S(M) := \text{Menge aller Permutationen auf } M$$

Bezeichnung: für Bild $f(a)$ eines Elementes $a \in M$ a^f also ist

$$f = \begin{pmatrix} a_1 & \dots & a_n \\ a_1^f & \dots & a_n^f \end{pmatrix}$$

Satz 1.2
Für $|M| = n$ gibt $n!$ viele Permutationen auf M.

$$|S_M| = n!$$

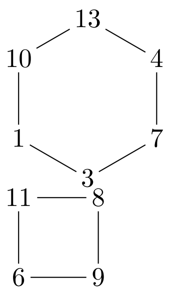
proof. Selbststudium! □

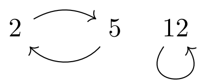
Definition 1.3
Der Graph einer Permutation

- $f\colon M \to M$
- $f^{\cdot} = \{(a,b) \in M^2 \mid a^f = b\}$ Graph von f, Paare (a,b) als gerichtete Kanten von a nach b zeichnen.
- Graph $f^{\cdot}$ (genauer: $(M, f^{\cdot})$ hat Knotenpunktmenge M und Knotenmenge $f^{\cdot}$

■ **Beispiel 1.4**

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 3 & 5 & 7 & 12 & 2 & 9 & 4 & 11 & 8 & 1 & 6 & 12 & 10 \end{pmatrix}$$





Fakt Vorraussetzung M endlich: Graph $f^{\cdot}$ einer Permutation f ist ein Kreis (Zyklus) oder die Vereinigung von paarweisen disjunkten Kreisen (Zyklen) (folgt aus Bijektivität) (Gilt nicht für unendliche Mengen $f\colon \mathbb{Z} \to \mathbb{Z}$ mit $x \mapsto x+1$)

Ab jetzt M endlich.

Definition 1.5
Die Zyklendarstellung einer Permutation f (entspricht “lineares Aufschreiben von $f^{\cdot}$”)

■ **Beispiel 1.6**
f wie oben

$$(1,3,7,4,13,10)(2,5)(6,9,8,11)(12)$$

Falls M fest, Zyklen der Menge 1 weglassen, das nennt man die verkürtzte Zyklendarstellung. zyklische Permutation := Permutation mit genau einem Zyklus in der verkürtzten Zyklendarstellung. Die identische Permutation $x \mapsto x$, Zyklendarstellung (1).
Beachte: $(abc), (bca), (cab)$ bezeichnen die selbe Permutation. (nur Reihenfolge, nicht Anfangselement wichtig)

Definition 1.7
Die Multipllikation (Produkt) von Permutationen ist die Hintereinanderausführung von Abbildungen.

$$M \xrightarrow{f} M \xrightarrow{g} M$$

$$a \xmapsto{f} a^f \xmapsto{g} a^{fg}$$

Produkt fg (oder $f;g$ oder $f \cdot g$, oder auch $g \circ g$) wird definiert durch

$$a^{fg} := (a^f)^g$$

ist wieder Permutation.

■ **Beispiel 1.8**

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

- Zykeldarstellung: $(12)(3) \cdot (13)(2) = (123)$
- verkürtzt: $(12) \cdot (13) = (123)$

Fakt: verkürtzte Zyklendarstellung k Zyklen

$$f = (- - c_1 - -)(- - c_2 - -) \dots (- - c_3 - -)$$
$$g = (- - c_i - -)$$

g also Permutation zyklisch. Also haben wir

$$f = g_1 \cdot g_2 \cdot \dots \cdot g_k$$

(Komposition)

Satz 1.9
Die Permutationen aus S_M bilden mit der Multiplikation eine Gruppe. die volle symmetrische Gruppe vom Grad $|M|$. (Einselement (1) = identische Abbildung, inverse Abbildung f^{-1} Zeilen in 2-Zeilendarstellung vertauschen. $(ab \dots xy)^{-1} = (yx \dots ba)$.

proof. SeSt.

▶ **Bemerkung 1.10**
Alle gruppentheoretische Begriffe sind auch für Permutationsgruppen definiert:Ordnung $\operatorname{ord}(f) = \min\{m \mid f^m = e\}$, Untergruppen, Normalteiler, konjugierte Elemente, usw.

Definition 1.11
Eine Permutationsgruppe G von Grad n ist eine Untergruppe der vollen symmetrischen Gruppe S_M vom Grad n.
Bezeichnung: (G, M) oder auch falls G Untergruppe ist, $G \leq S_M$. Wobei meist

$$M = \{0, 1, \dots, n-1\} =: n \Rightarrow S_n$$
$$M = \{1, 2, \dots, n\} =: \underline{n} \Rightarrow S_{\underline{n}}$$

▶ **Bemerkung 1.12**
Weitere Schreibweisen für $U, V \subseteq S_M$, dabei

$$UV = \{uv \mid u \in U, v \in V\}$$

$a \in M, B \subseteqq M, g \in S_M$

$$\begin{aligned} a^u &= \{a^u \mid u \in U\} \\ B^g &= \{b^g \mid b \in B\} \\ B^u &= \{b^u \mid b \in B, u \in U\} \end{aligned}$$

Satz 1.13 (Gruppenkriterium)
Sei M endlich. Dann ist $U \subseteqq S_M$ Gruppe genau dann, wenn $U \cdot U \subseteqq U$.

proof. SeSt.

■ **Beispiel 1.14**
Symmetrieabbildung des Rechtecks in der Ebene können durch Permutation der Eckpunkte beschrieben werden. Also

Identitätsabbildung:	$(1) =: e$
Drehung 180°:	$(13)(24) =: g_1$
Spiegelung an I:	$(14)(23) =: g_2$
Spiegelung an II:	$(12)(34) =: g_3$

Damit ist $G = \{e, g_1, g_2, g_3\}$ Permutationsgruppe und $G \cong$ Symmetriegruppe des Rechtecks in der Ebene.

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

das ist die KLEINsche Vierergruppe, die isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist.

Definition 1.15
Sei (G, M) Permutationsgruppe, $a \in M$, dann definiere

1. Den Stabilisator von a

$$G_a := \{g \in G \mid a^g = a\}$$

Allgemeiner haben wir

$$G_{a_1, a_2, \ldots, a_m} := \bigcap_{i=1}^{m} G_{a_i}.$$

2. Die Bahn (1-Bahn, Orbit)

$$a^G := \{a^g \mid g \in G\}.$$

Also ist der 1-Orb$(G, M) :=$ Menge aller 1-Bahnen (Andere Bezeichnung: $G \| M$).

3. $B \subseteq M$ invariante Menge (bezüglich G) $:\Leftrightarrow B^G \subseteqq B$
4. G transitiv $\Leftrightarrow \exists a \in M \colon a^G = M$

▶ **Bemerkung**
Äquivalent dazu sind:

$$\forall a \in M \colon a^G = M$$
$$|1 - \mathrm{Orb}(G, M)| = 1$$

Lemma 1.16
Sei $G \leq S_M, a \in M$. Es gilt:

(a) G_a ist Untergruppe von G.

(b) $G_{a^g} = g^{-1}(G_a)g \ (g \in G)$

(c) Durch $a \sim b \Leftrightarrow a^G = b^G$ ist eine Äquivalenzrelation gegeben und es gilt:

$$1 - \mathrm{Orb}(G, M) = M/\sim$$

Die menge aller 1-Bahnen bildet eine Zerlegung von M (zwei Bahnen sind gleich oder disjunkt).
Beachte:

$$b \in a^G \Leftrightarrow a \in b^G \qquad \text{Sest!}$$

(d) Jede invariante Menge $B \subseteqq M$ ist Vereinigung von 1-Bahnen

$$B = B^G = \bigcup_{b \in B} b^G$$

proof. Lemma 1.16 (a) - Lemma 1.16 (c) SeSt, Lemma 1.16 (d) klar nach Definition! □

▶ **Bemerkung 1.17**
Repräsentatensystem einer Zerlegung $1 - \mathrm{Orb}(G, M)$ heisst Transversale.

Wiederholung Algebra

Satz 1.18 (Satz von Lagrange)
Die Ordnung $|U|$ jeder Untergruppe einer endlichen Gruppe G ist Teiler der Gruppenordnung. Es gilt

$$|G| = [G \colon U] \cdot |U|$$

(wobei $[\cdot \colon \cdot]$ der Index ist).

proof. Index $[G \colon U] = |G/U| =$ Anzahl k der (rechts-)Nebenklassen Ug in der Nebenklassenzerlegung.

$$G = Ug_1 \cup Ug_2 \cup \ldots Ug_k$$

Dabei ist die Nebenklasse durch $Ug := \{u \cdot g \mid u \in U\}$ und $G/U := \{Ug \mid g \in G\}$ und wegen $|U| = |Ug|$ folgt satz 1.18. □

Lemma 1.19
Sei $a \in M, G \leq S_M$.

$$\begin{cases} a^G & \to G/G_a \\ a^g & \mapsto G_a g \end{cases}$$

ist eine bijektive Abbildung zwischen Elementen der von a erzeugten Bahn un den Nebenklassen nach dem Stabilisator G_a gegeben. Insbesondere gilt:

$$\left|a^G\right| = [G\colon G_a] = |G/G_a|$$

proof.

$$\begin{aligned} a^g = a^{g'} &\overset{\Leftarrow}{\Rightarrow} a = a^{g'g^{-1}} \overset{\Leftarrow}{\Rightarrow} g'g^{-1} \in G_a \\ &\overset{\Leftarrow}{\Rightarrow} g' \in G_a g \overset{\Leftarrow}{\Rightarrow} G_a g' = G_a g \end{aligned}$$

(letzte $\Rightarrow$ benutzt Nebenklassen gleich oder disjunkt)

- $\Rightarrow$ zeigt, dass $a^g \mapsto G_a g$ wohldefiniert ist
- $\Leftarrow$ zeigt, dass $a^g \mapsto G_a g$ injektiv ist.
- Surjektivität ist klar, da g beliebig gewählt werden kann. □

Nun formulieren wie eine Folgerung, die satz 1.18 und Lemma 1.19.

Corollary 1.20 (Permutationsgruppentheoretische Umformulierung des satz 1.18)
Für $a \in M$, $G \leq S_M$ gilt:

$$|G| = |G_a| \cdot \left|a^G\right|$$

proof.

$$\begin{aligned} |G| &\overset{satz\ 1.18}{=} [G\colon U] \cdot |U| = [G\colon G_a] \cdot [G_a] \\ &= |G/G_a| \cdot |G_a| \overset{Lemma\ 1.19}{=} \left|a^G\right| \cdot |G_a| \end{aligned}$$

□

■ **Beispiel 1.21**
Sei $G := S_{\underline{4}}$, $1^G = \{1,2,3,4\}$ und $M = \underline{4} = \{1,2,3,4\}$, dann

$$|G_1| \overset{Folgerung\ 1.20}{=} |G|/\left|1^G\right| = 4!/4 = 3! = 6$$

"Raten" der Permutationen aus G_1 führt zu

$$G_1 = \{(1),(23),(24),(34),(234),(243)\}$$

(mehr als 6 gibt es nicht!)
Iteration führt zu

$$\begin{aligned} |G_{1,2}| &= |G_1| : \left|2^{G_1}\right| = 6 : 3 = 2 \\ G_{1,2} &= \{(1),(34)\} \\ |G_{1,2,3}| &= |G_{1,2}| : \left|3^{G_{1,2}}\right| = 2 : 2 = 1 \\ G_{1,2,3} &= \{(1)\} \end{aligned}$$

Definition 1.22
Zwei Permutationsgruppen (bzw. Wirkungen, siehe 2.2) (G, M) und (H, N) heißen ähnlich, wenn eine bijektive Abbildung

$$f\colon M \to N$$

und ein Gruppenisomorphismus

$$\varphi\colon G \to H$$

existieren, so dass gilt:

$$\forall a \in M, \forall g \in G \quad f(a^g) = f(a)^{\varphi(g)}$$

d.h. das Diagramm

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "g"] & N \arrow[d, "\varphi(g)"] \\ M \arrow[r, "f"] & N \end{tikzcd}$$

ist kommutativ.

▶ **Bemerkung**
Durch f und G ist φ und H vollständig festgelegt (folgt aus Diagramm)

$$y \in N \quad y^{\varphi(g)} = g^{f^{-1}gf}$$
$$H = \{\varphi(g) \mid g \in G\} = \left\{f^{-1}gf \mid g \in G\right\}$$

Beachte: Ähnlichkeit impliziert Isomorphie, Äquivalenz gilt im Allgemeinen nicht!

■ **Beispiel 1.23**
1. S_M ähnlich zu $S_N \Rightarrow |M| = |N|$
2. $(G, M) = (\{e, (12)\}, \{(1, 2)\})$ ähnlich zu $(\{e, (\alpha, \beta)\}, \{\alpha, \beta\}) = (H, N)$ aber nicht ähnlich zu $(\{e, (1, 2)\}, \{1, 2, 3, 4\}) = (G', M')$, obwohl $G \cong G'$ (als Gruppen).

Definition 1.24
Ähnlichkeit und Konjugiertheit von Permutationen

1. zwei Permutationen $g_1, g_2 \in S_M$ heißen ähnlich, wenn in ihren Zyklendarstellungen gleich viele Zyklen, gleicher Länge vorkommen, z.B.

$$\begin{aligned} g_1 =& (1)(2)(345)(67)(89) \\ g_2 =& (3)(7)(149)(28)(56) \\ & (\cdot)(\cdot)(\cdots)(\cdot\cdot)(\cdot\cdot) \end{aligned}$$

2. Sei $G \leq S_M$, $g_2 \in S_M$ heißt konjugiert zu $g_1 \in G$, wenn ein $f \in G \neq S_M$ existiert, so dass $g_2 = f^{-1}g_1f$.
Sprechweise: g_1 und g_2 sind konjugiert.

Lemma 1.25

1. Konjugiertheit und Ähnlichkeit sind Äquivalenzrelation (in $S_{\underline{n}}$).
2. Aus der Zyklendarstellung
$$g = (a_1, a_2, \dots)(b_1, b_2, \dots)(\dots)\dots$$
erhält man die Zyklendarstellung von $f^{-1}gf$ (für $f \in S_{\underline{n}}$), wenn f auf jedes Element im Zyklus angewendet wird
$$f^{-1}gf = (a_1^f, a_2^f, \dots)(b_1^f, b_2^f, \dots)(\dots)\dots$$
3. g_1 und g_2 konjugiert $\Rightarrow g_1, g_2$ ähnlich ($\Leftarrow$ im Allgemeinen nicht!), aber, wenn $g_1 \vee g_2$ konjugiert in $S_{\underline{n}} \Leftrightarrow g_1, g_2$ ähnlich
4. $g_1, g_2 \in S_{\underline{n}}$ ähnlich $\Leftrightarrow$ die erzeugte zyklische Untergruppe $(\langle g_1\rangle, M)$ und $(\langle g_2\rangle, M)$ sind ähnlich im Sinne von der Definition der Untergruppe (Definition 1.22).

2. Gruppenwirkungen und Darstellungen (Satz von Cayley)

Definition 2.1 (Permutationsdarstellung)

(i) Ein Homomorphismus
$$\psi\colon G \to S_M$$
einer (abstrakten) Gruppe G in eine symmetrische Gruppe S_M heisst Permutationsdarstellung von G. (vom Grad $|M|$)

(ii) ψ true, falls ψ injektiv.

▶ **Bemerkung**

ψ ist treu $\Leftrightarrow \ker\psi = \{g \mid \psi(g) = e\} = \{e\}$, mithilfe des Homomorphiesatz folgt $G \cong \mathfrak{Im}\psi(G) = \psi[G] \leq S_M$. ($G$ ist "praktisch" Permutationsgruppe.)

Definition 2.2

Sei $G = \langle G, \cdot, ^{-1}, e\rangle$ Gruppe, M Menge. Eine Abbildung
$$\varphi\colon \begin{cases} M \times G & \to M \\ (x, g) & \mapsto xg = \varphi(x, g) \end{cases}$$
heisst Gruppenwirkung(alt: Gruppenoperation, eng. group action) von G auf Menge M, falls folgendes gilt:

1. $\varphi(x, e) = xe_G = x \quad \forall x \in M$
2. $$\begin{aligned} (xg)g' &= x(g \cdot_G g') \\ \varphi(\varphi(x, g), g') &= \varphi(x, g \cdot_G g') \end{aligned}$$

Sprechweise: G wirkt (operiert, eng. acts) auf M
Schreibweise: (G, M)

▶ **Bemerkung**
Jede Permutationsgruppe $G \leq S_M$ operiert auf natürliche Weise auf M

$$xg = \varphi(x, g) = x^g$$

(oft Schreibweise x^g statt $\varphi(x, g) \wedge xg$)

Satz 2.3
Jeder Gruppenwirkung

$$\varphi\colon M \times G \to M$$

entspricht in ein-eindeutiger Weise einer Permutationsdarstellung.
$\psi\colon G \to S_M$ und umgekehrt, und zwar gemäß

$$\begin{array}{rl} x^{\psi(g)} = xg & (= \varphi(x, g) \\ (x \in M, g \in G) := & \text{falls } \varphi \text{ gegeben} \\ := & \text{falls } \psi \text{ gegeben} \end{array}$$

proof. SeSt.. (Hinweis: Es muss gezeigt werden, dass ψ ein Gruppenhomomorphismus ist.) □

Lemma 2.4
(a) Ist G (abstrakte) Gruppe, so ist durch

$$h \in G \quad h^{g^*}$$

(rechts-multiplikation mit g) für jedes $g \in G$ eine Permutation: $g^* \in S_G$ gegeben.

(b) $\psi\colon G \to S_G$ mit $g \mapsto g^*$ ist Permutationsdarstellung

(c) $\varphi\colon (G \times G) \to G$ mit $(h, g) \mapsto hg$ (Produkt in Gruppe G) zugehörige Gruppenwirkung

(d) φ ist treu (und heißt rechtsreguläre Darstellung von G)

Folgerung aus Lemma 2.4 (d) (vergleiche Bemerkung zu Definition 2.1) ist

Corollary 2.5 (Satz von Cayley)
Für eine beliebige Gruppe G ist

$$G^* = \{g^* \mid g \in G\} \subset S_G$$

eine zu G isomorphe (da treu) Permutationsgruppe (G^*, G) heißt rechtsreguläre Darstellung von G.

proof (**??**).
- Lemma 2.4 (a) und Lemma 2.4 (b) folgen wegen satz 2.3 aus 3)
- zu zeigen satz 2.3 für φ
  1. $\varphi(h, g) = he = h$
  2. $(hg)g^{-1} = h(gg^{-1})$ (assoziativ Gruppen der Gruppenmultiplikation)
- noch zu zeigen Lemma 2.4 (c): Sei $g_1^* = g_2^*$ (gilt unter ψ). Dann $h^{g_1^*} = h^{g_2^*}$ impliziert $\xRightarrow{h^{-1}} g_1 = g_2$. (Da $h^{-1} \cdot h = e$ gilt.) □

■ **Beispiel 2.6**
Sei $G = S_3 = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ mit $M = \{1, 2, 3\}$

$$g_1 = e = (1) \quad g_2 = (12) \quad g_3 = (13)$$
$$g_4 = (23) \quad g_5 = (123) \quad g_6 = (132)$$

Multiplikationstafel (Cayley table) then we have: $g_i^* g \to gg_i$ wird durch die 3. Spalte des Cayleytafel beschrieben, d.h.

$$g_3^* = \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_3 & g_5 & g_1 & g_6 & g_2 & g_4 \end{pmatrix} = (g_1 g_3)(g_2 g_5)(g_3 g_1)$$

Zyklenschreibweise.

▶ **Bemerkung**

1. G wirkt $S_{\underline{3}}$ auf $M = \{1, 2, 3\}$
2. $G^* = S_{\underline{3}}^*$ wirkt auf der Menge $S_{\underline{3}} = \{g_1, \ldots, g_6\}$ d.h. ist Untergruppe der S_G, SeSt kein $g^* \neq e$ hat eine Fixpunkt
3. Jedes g^* zerfällt in ein Produkt von Zyklen gleicher Menge $\mathrm{ord}(g)$, vgl. vorheriges Beispiel: $\mathrm{ord}(g_2) = 2$
4. G^* hat Grad $|G|$.
5. G^* ist transitiv (d.h. gibt nur eine Bahn $e^{G^*} = G$)
6. Die EGS 2. und 5. charakterisieren die Regularität von G^* (vgl 5.4)

■ **Beispiel 2.7 (Weitere Beispiele von Gruppenwirkungen einer (abstrakten) Gruppe G)**

1. Wirkung durch Konjugation (siehe Geometrie Kurs)

$$\varphi\colon \begin{cases} G \times G & \to G \\ (h, g) & \mapsto g^{-1}hg \end{cases}$$

zugehörige Permutationsdarstellung:

$$\psi\colon \begin{cases} G & \to S_G \\ g & \to \psi(g) \end{cases}$$
$$h^g = h^{\psi(g)} = g^{-1}hg$$

2. Wirkung auf Untergruppen $U \subseteq G$ ($\mathrm{Sub}(G)$ Menge der Untergruppen von G)

$$\psi\colon \begin{cases} \mathrm{Sub}(G) \times G & \to \mathrm{Sub}(G) \\ (U, g) & \to g^{-1}Ug \end{cases}$$

zugehörige Permutationsdarstellung

$$\varphi\colon G \to S_{\mathrm{Sub}(G)}$$

3. Wirkung auf rechte-Cosets G/U

$$U \subseteq G, G/U = \{Uh \mid h \in G\}$$
$$\varphi\colon \begin{cases} G/U \times G & \to G/U \\ (Uh, g) & \mapsto Uhg \end{cases}$$
$$\varphi\colon G \to S_{G/U}$$

■ **Beispiel 2.8 (Wirkungen von Permutationsgruppen (G, M) auf andere Mengen)**

(a) induzierte Wirkung $(G, \mathcal{P}(M))$ auf Potenzmenge $\mathcal{P}(M)$

$$\mathcal{P}(M) \times G \to \mathcal{P}(M)$$
$$(B, g) \mapsto B^g = \{h^g \mid h \in B\}$$

(b) Einschränkung: induzierte Wirkung $(G, \mathcal{P}_m(M))$ auf m-elementige Teilmenge

$$\varphi\colon \begin{cases} \mathcal{P}_m(M) \times G & \to \mathcal{P}_m(M) \\ (B, g) & \mapsto B^g \quad |B| = m \end{cases}$$

Bezeichnung dieser Wirkung auch $(G^m, \mathcal{P}_m(M))$

(c) induzierte Wirkung von (G, M^m) auf m-Tupel d.h. auf M^m

$$\varphi\colon \begin{cases} M^m \times G & \to M^m \\ (a_1, \ldots, a_m)^g & \mapsto (a_1^g, \ldots, a_m^g) \end{cases}$$

Bezeichnung: $(G^{[m]}, M^m)$.

3. Erzeugendensysteme und Sims-Ketten

Problem: Beschreibung von Permutationsgruppen, Aufzählung aller Elemente ist nur selben möglich ($\underline{S_{100}} = 100 \Rightarrow 10^{100} \ldots 10^{200}$)
Aufzählung: Beschreibung als Automorphismusgruppen (siehe Kapitel 4 und 5) oder durch EZS.
Wiederholung:

Definition 3.1
$U \subseteq G$ heißt Erzeugendensystem einer Gruppe $G :\Leftrightarrow$ jedes $g \in G$ ist als endliches Produkt $u_1, \ldots, u_m$ mit $u_i \in U$ oder $u_i^{-1} \in U$ darstellbar.
Bezeichunung: $G = \langle u_i \rangle_G$.

Probleme:

(P1) Entscheide $g \in \langle U \rangle$ für $g \in S_n, U \subseteq S_n$?

(P2) Bestimme Bahnen von $\langle U \rangle$, spezielle Bahnen $a^{\langle U \rangle}$ für spezielle $a \in G$.

(P3) Beschreibung der Untergruppen von $\langle U \rangle$, benutze Methode von SIMS für große G. Man benutzt Menge T_i für $i = \{1, \ldots, r\}$, sodass

$$G = T_r \cdot T_{r-1} \cdots T_1$$

und Darstellung

$$g = t_r \cdot t_{r-1} \cdot t_{r-2} \cdots t_1$$

ist Eindeuting.

Damit wäre die Speicherformel: $\sum_{i=1}^{r}|T_i|$

■ **Beispiel**
$G = S_{\underline{n}}$ impliziert $|G| = n!$ oder $\sum|T_i| \leq \frac{n(n+1)}{2}$ möglich, also ist der Speicherbedarf $\sim n^2$.

Definition 3.2 (Sims-Kette, Sims-Basis, Transversale)
Die Sims-Kette einer Permutationsgruppe $G \subseteq S_M$, $M = \{a_1, \ldots, a_n\}$ speziell $M = \underline{n} = \{1, \ldots, n\}$ für punktweise Stabilisatoren:

$$U_1 = G_{n_1} \quad U_2 = G_{n_1,n_2} \quad \ldots \quad U_i = G_{n_1,\ldots,n_i} \quad U_n = G_{n_1,\ldots,n_n} = \{e\}$$

Also haben wir

$$\{e\} = U_1 \subseteq U_2 \subseteq \cdots \subseteq U_i \subseteq \cdots \subseteq U = G$$

Sei $r := \min\{i \mid U_i = \{e\}\}$ (hängt von der Reihenfolge der Elemente n_i ab). Die Menge der $\{a_1, \ldots, a_r\}$ genauer $(a_1, \ldots, a_r)$ heißt <u>SIMS-Basis</u> von G und

$$\{e\} = U_r \subsetneqq U_{r-1} \leqq \cdots \leqq U_1 \leqq U_0 = 0$$

ist die <u>SIMS-Kette</u> von G der Länge r (zur Basis $(a_1, \ldots, a_r)$). Für

$$U_{i-1}/U_i = U_i g_{i_1} \dot\cup U_i g_{i_2} \dot\cup U_i g \dot\cup \ldots \dot\cup U_i g_{i_{n_i}} \quad \text{meist } g_{i_1} = e$$

wird Repräsentatensystem (<u>Transversale</u>) $T_i := \left\{g_{i_1}, \ldots, g_{i_{n_i}}\right\}$ gewählt $(i = 1, \ldots, r)$.
Beachte:

$$U_{r-1}/U_r \cong U_{r-1}\text{,also } T_r = U_{r-1}$$

Bei Umnummerierung der Elemente entstehen möglicherweise kürzere Base. (Fixpunkte in Basis weggelassen)

Satz 3.3
Seien G, T_i wie in Definition 3.2. Dann gilt

(i) Jede Permutation $g \in G$ lässt sich eindeutig in der Form

$$g = h_r h_{r-1} \cdots h_1 \text{ mit } h_i \in T_i \ (i \in \{1, \ldots, r\})$$

darstellen. Insbesondere gilt dann

$$G = T_r T_{r-1} \cdot \cdots \cdot T_1 \text{ and } |G| = \prod_{i=1}^{r} n_i.$$

(ii) Jede Permutation $g \in G$ ist eindeutig durch die Bilder der Basis festgelegt, d.h. durch $(a_1^g, \ldots, a_r^g)$.

▶ **Bemerkung**
Definition 3.3 (i) impliziert $T_1 \cup \cdots \cup T_r$ ist ein (spezielles) Erzeugendensystem für G.

proof.

- zu Definition 3.3 (i):

$$\begin{aligned} g \in G \Rightarrow \exists! h_1 \in T_1 \colon g \in U_1 h_1 \\ \Rightarrow g h_1^{-1} \in U_1 \Rightarrow \exists! h_2 \in T_2 \colon g h_1^{-1} \in U_2 h_2 \\ \Rightarrow g h_1^{-1} h_2^{-1} \in U_2 \Rightarrow \exists! h_3 \ldots \\ \Rightarrow g h_1^{-1} h_2^{-1} \ldots h_r^{-1} \in U_r = \{e\} \\ \Rightarrow g = h_r h_{r-1} \cdot \cdots \cdot h_2 \cdot h_1 \end{aligned}$$

  Eindeutigkeit der Darstellung folgt aus der Eindeutigkeit der Repäsentaten (der Nebenklassen).

- zu Definition 3.3 (ii):

$$(a_1^g, \ldots, a_r^g) = (a_1^{g'}, \ldots, a_r^{g'}) \Rightarrow a_i^{gg^{-1}} = a_i \qquad \text{Fixpunkte}$$

  d.h.

$$gg^{-1} \in G_{a_1 a_2 \ldots a_r} = \{e\} \Rightarrow g = g'$$

□

■ Beispiel 3.4
Sei $G = S_{\underline{4}}, M = \{a_1, a_2, a_3, a_4\} = \{1, 2, 3, 4\}$, $G_1 \cong S_3$, $G_{1,2} \cong S_2$ und $G_{1,2,3} = \{e\}$, dann muss man etwas rechnen und bekommt

$$\begin{aligned} T_1 &= \left\{e, g_1, g_1^2, g_1^3\right\} && \text{für } g_1 = (1234) \\ T_2 &= \left\{e, g_2, g_2^2\right\} && \text{für } g_2 = (234) \\ T_1 &= \{e, g_3\} && \text{für } g_3 = (34) \end{aligned}$$

Dann folgt mit Definition 3.3 (i): Jedes $g \in S_{\underline{4}}$ ist eindeutig in der Form

$$g = g_3^{\alpha_3} g_2^{\alpha_2} g_1 \alpha_1$$

wobei $\alpha_3 \in \{0, 1\}$, $\alpha_2 \in \{0, 1, 2\}$, $\alpha_1 = \{0, 1, 2, 3\}$ und $g_0 = e$.

▶ Bemerkung
Speicheraufwand (in Bit):

$$\begin{aligned} |T_1| &= 4 \Rightarrow 2 \text{ Bit} \\ |T_2| &= 3 \Rightarrow 2 \text{ Bit} \\ |T_3| &= 2 \Rightarrow 1 \text{ Bit} \\ &\Rightarrow 5 \text{ Bit} \end{aligned}$$

ist optimal, da wir $2^4(16) \lneqq 4!(24) \leq 2^5(32)$ haben.

Corollary 3.5 (Test $g \in G$, vergleiche Probleme (P1) vom Anfang des Kapitels)
Für $G \leq S_M$ seinen eine SIMS-Basis $(a_1, \ldots, a_r)$ and $T_1, \ldots, T_r$ bekannt (vergleiche Definition 3.2), $g \in S_M$ gegeben.

Algorithmus zum Testen, ob $g \in G$:

$$\begin{array}{ccc}
\exists h_1 \in T_1\colon a_1^{gh_1^{-1}} = a_1? & \xrightarrow{\text{nein}} & g \notin G \\
\downarrow \text{ ja} & & \\
\exists h_2 \in T_2\colon a_2^{gh_1^{-1}h_2^{-1}} = a_2? & \xrightarrow{\text{nein}} & g \notin G \\
\downarrow \text{ ja} & & \\
\dots & & \\
\exists h_r \in T_r\colon a_r^{gh_1^{-1}h_2^{-1}\cdots h_r^{-1}} = a_r? & \xrightarrow{\text{nein}} & g \notin G \\
\downarrow \text{ ja} & & \\
\exists g h_1^{-1} h_2^{-1} \dots h_r^{-1} = e? & \xrightarrow{\text{nein}} & g \notin G \\
\downarrow \text{ ja} & & \\
g \in G & &
\end{array}$$

proof. 1. Schritt: Wegen $G = \bigcup_{h \in T_1} G_{a_1} h$ folgt

$$g \in G \Leftrightarrow \exists h \in T_1\colon g \in G_{a_1} h \Leftrightarrow \exists h \in T_1\colon gh^{-1} \in G_{a_1}$$
$$\Leftrightarrow \exists h \in T_1\colon a_1^{gh^{-1}} = a_1 \wedge gh^{-1} \in G \Rightarrow \exists h \in T_1\colon a_1^{gh^{-1}} = a_1.$$

Also führt der ($\xrightarrow{\text{nein}}$)-Zweig zu $g \notin G$. (Die weiteren Schritte sind analog.) □

Problem: Wie findet man das Repräsentatensystem $T_1, \dots, T_r$ für die Untergruppen $U_1, \dots, U_r$, falls Erzeugendensystem U gegeben

$$G = \langle U \rangle \qquad \text{vergleiche (P3) unter Definition 3.1}$$

(beachte, dass $T_1 \dot\cup \dots T_r$ ist Erzeugendensystem für $U_{1\dots r}$)
Antwort: Resultat von SCHREIER (Otto Schreier 1901 -1929)

Satz 3.6 (Schreier-Lemma)
Sei $G = \langle U \rangle$ mit $U = \{g_1, \dots, g_n\}$ (bzw. für endlich erzeugbare Gruppen G, also $|G| = \infty$ sein.) $V \leq G$ Untergruppe mit

$$G = Vh_1 \cup Vh_2 \cup \dots \cup Vh_s \quad s\text{-cosets und oBdA } h_1 = e$$

$T = \{h_1, \dots, h_s\}$ Repräsentatensystem für G/V. Für $g \in G$ sei $\varphi(g) \in T$ der Repräsentant der Nebenklasse Vg (d.h. $g \in Vg = V_{\varphi(g)}$) Dann ist

$$X := \left\{ h_i g_j^k \varphi(h_i g_j^k)^{-1} \mid i \in \{1, \dots, s\}, g \in \{1, \dots, m\} \right\}$$

($k \in \{1, -1\}$ bei unendlichen Gruppen) ein Erzeugendensystem für die Untergruppe V.

▶ **Bemerkung**

$$k = \{1, -1\} \quad {}^{-1} \text{ ist Inverse} \tag{1}$$

proof. 1. $X \subsetneqq V$, dann

$$h_i g_j \in V\varphi(h_i g_j) \Rightarrow h_i g_j \cdot \varphi(h_i g_j)^{-1}$$

2. X ist Erzeugendensystem von V. Sei $g \in V \leq G = \langle U \rangle$. Dann existiert Darstellung $g = g_{i_1} \cdots g_{i_t}$ (bei

unendlichen Gruppen braucht man wieder g^{-1} vergleiche (1))

$$\Rightarrow g = h_1 g_{i_1} \cdots g_{i_t} = \underbrace{h_1 g \varphi(h_1 g_j)^{-1}}_{\ni X} \underbrace{\varphi(h_1 g_1)}_{\exists \varphi(g_1) h_{i_1}} g_{i_1} \dots g_{i_t}$$

$$= \underbrace{\cdots}_{\in X} \underbrace{h_{j_1} g_{i_2} \varphi(h_{j_1} g_{i_2})^{-1}}_{\in X} \quad \underbrace{\varphi(h_{j_1} g_{i_2})}_{\exists j_2:\ \varphi(h_{j_2} g_{i_2}) = h_{j_2}} \quad g_{i_3} \cdots g_{i_t}$$

$$\overset{\text{usw.}}{=} \underbrace{}_{\in X} \underbrace{}_{\in X} \cdots \underbrace{}_{\in X} \underbrace{\varphi \dots \varphi^{-1}}_{\in X} \quad g \in V$$

Sest noch einen Schritt

$$\Rightarrow \varphi(hg) \in V$$

konkret folgt also, dass $g \in \langle X \rangle$. □

■ **Beispiel 3.7**
Sei $G := S_{\underline{n}}, V := A_{\underline{n}}$ (alternierende Gruppe der geraden Permutationen). Erzeugendensystem $g_1 := (12), g_2 := (12 \dots n)$ (vergleiche Bemerkung 3.8 (d)):

$$G = \langle g_1, g_2 \rangle_{S_{\underline{n}}}$$

Nebenklassenzerlegung mit Repräsentaten $h_1 := e = (1), h_2 := (12)$:

$$S_{\underline{n}} = V h_1 \dot\cup V h_2 = A_{\underline{n}} \dot\cup A_{\underline{n}}(12)$$

$\xRightarrow{\textit{satz } 3.6}$ $A_{\underline{n}}$ wird erzeugt von

$$\begin{aligned}
h_1 g_1 \varphi(h_1 g_1)^{-1} &= e \cdot (12) \cdot (12) = e \\
h_1 g_2 \varphi(h_1 g_2)^{-1} &= \begin{cases} e \cdot (12 \dots n) \cdot (12) = (23 \dots n) & \text{falls } n \text{ gerade} \\ e \cdot (12 \dots n) \cdot e = (213 \dots n) & \text{falls } n \text{ ungerade} \end{cases} \\
h_2 g_1 \varphi(h_2 g_1)^{-1} &= (12) \cdot (12) \cdot e = e \\
h_2 g_2 \varphi(h_2 g_2)^{-1} &= \begin{cases} (12) \cdot (12 \dots n) \cdot (12) = (213 \dots n) & \text{falls } n-1 \text{ gerade} \\ (12) \cdot (12 \dots n) \cdot e = (134 \dots n) & \text{falls } n-1 \text{ ungerade} \end{cases}
\end{aligned}$$

(wobei $(12) \cdot (12 \dots n) = (134 \dots n)$). Also erhält man folgendes Erzeugendensystem für $A_{\underline{n}}$:

$$A_{\underline{n}} = \begin{cases} \langle (234 \dots n), (134 \dots n) \rangle_{S_{\underline{n}}} & \text{falls } n \text{ gerade} \\ \langle (123 \dots n), (213 \dots n) \rangle_{S_{\underline{n}}} & \text{falls } n \text{ ungerade} \end{cases}$$

▶ **Bemerkung 3.8**
Erzeugendensysteme der $S_{\underline{m}}$: folgende Mengen erzeugen $S_{\underline{m}}$:

(a) $\{(ij) \mid i, j \in N\}$ alle Transpositionen

(b) $\{(12), (23), \dots, (n-1, n)\}$ spezielle Transposotionen

(c) $\{(12), (13), (14), \dots, (1n)\}$ spezielle Transpositionen

(d) $\{(12), (12 \dots n)\}$

proof (Bemerkung 3.8).

zu Bemerkung 3.8 (a): Für Zyklen gilt:

$$(a_1 \dots a_k) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_k) \quad \text{SeSt!}$$

Jede Permutation ist Produkt von Zyklen (siehe Geometrie Fehm).

Bemerkung 3.8 (b) - Bemerkung 3.8 (b) SeSt! □

▶ **Bemerkung**
Zerlegung in Transpositionen nicht eindeutig (im Gegensatz zu SIMS-Ketten-Zerlegung satz 3.3), aber es gibt gewisse Invarianten

Definition 3.9 (gerade und ungerade Permutationen)
Sei $g \in S_{\underline{n}}$. Eine Inversion von g ist ein Paar (i, j) mit $1 \leq j \leq n$ und $i^g > j^g$. zum Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

hat zwei Inversionen: $1 < 2$, $3 < 4$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)(2)$$

hat die Inversionen: $1 < 2$, $2 < 3$, $1 < 3$. (=Anzahl der Vertauschungen von Nachbarn in der zweiten Zeile, um daraus 1. Zeile zu bekommen) Definiere Signum:

$$\operatorname{sgn}(g) := \begin{cases} 1 & \text{falls \# Inversionen gerade} \\ -1 & \text{falls \# Inversionen ungerade} \end{cases}$$

g heißt dann gerade bzw. ungerade Permutation.
Es gilt:

(i)

$$\operatorname{sgn}(g) = \prod_{\substack{i<j \\ i,j \in \underline{n}}} \frac{j^g - i^g}{j - 1} = \prod_{i<j} \frac{j^{gh} - i^{gh}}{j^h - i^h}$$

(für beliebige Permutation h)

proof. Jede Inversion liefert (-1) im Zähler. Beim Aufsetzen einer Permutation h wird genau dann im Produkt der Zähler ein Vorzeichen geändert, wenn auch Änderung im Nenner. □

(ii) $\operatorname{sgn}(gh) = \operatorname{sgn}(g) \cdot \operatorname{sgn}(h)$, denn

$$\begin{aligned} \operatorname{sgn}(g) \cdot \operatorname{sgn}(h) &= \prod_{i<j} \frac{j^g - i^g}{j - i} \prod_{i<j} \frac{j^h - i^h}{j - i} \\ &= \frac{j^{gh} - i^{gh}}{j^h - i^h} \cdot \frac{j^h - i^h}{j - 1} \\ &= \frac{j^{gh} - i^{gh}}{j - 1} \\ &= \operatorname{sgn}(gh) \end{aligned}$$

(iii) $\operatorname{sgn}(e) = 1, \operatorname{sgn}(g^{-1}) = \operatorname{sgn}(g)$ (denn $1 = \operatorname{sgn}(g \cdot g^1) = \operatorname{sgn}(g) \cdot \operatorname{sgn}(g^{-1})$)

(iv) $\operatorname{sgn}\colon S_{\underline{n}} \to \{1, -1\}$ ist Homomorphismus auf der multiplikativen Gruppe $\langle \{1, -1\}, \cdot \rangle$

(v) Die geraden Permutationen bilden Untergruppe (wegen Definition 3.9 (ii), Definition 3.9 (iii) =: die alternierende Gruppe $A_{\underline{n}}$ von $S_{\underline{n}}$)

(vi) $g \in S_{\underline{n}}$ gerade (bzw. ungerade) $\Leftrightarrow$ Für jede Darstellung $g = t_1, \dots, t_q$ als Produkt von Transpositionen ist g gerade (bzw. ungerade)

proof (Definition 3.9 (vi)).

$$
\begin{aligned}
&g = t_1 \dots t_q \\
&e = t_1 \dots t_q \dots t_1 = s \cdot t_1 \dots t_q \\
&e = s \cdot t_1 \dots t_q = s(-1) \cdot t_{q-1} \dots t_1 \\
&e = s(-1) \cdot t_{q-1} \dots t_1 = s(-1)^q = 1
\end{aligned}
$$

□

Daraus folgt:

Satz 3.10
Die alternierende Gruppe $A_{\underline{n}} \leq S_{\underline{n}}$ besteht aus allen Permutation, die sich als Produkt einer geraden Anzahl von Transpositionen darstellen lassen.
$A_{\underline{n}}$ ist Normalteiler in $S_{\underline{n}}$ und enthält $n!/2$ Elemente.

proof.
- erster Teil: Definition 3.9 (vi)
- zweiter Teil: Homorphiesatz für sgn: $S_{\underline{n}} \to \{1, -1\}$ (vergleiche Definition 3.9 (v))

$$
\begin{aligned}
&\ker(\mathrm{sgn}) = \{g \mid \mathrm{sgn}(g) = 1\} = A_{\underline{n}} \\
&\left|S_{\underline{n}/A_{\underline{n}}}\right| = \frac{\left|S_{\underline{n}}\right|}{\left|A_{\underline{n}}\right|} = 2
\end{aligned}
$$

□

▶ **Bemerkung 3.11**
$A_{\underline{n}}$ ist einfach für $n \leq 5$ (keine Normalteiler). Daraus folgt direkt S_n ist für $n \geq 5$ nicht auflösbar. (siehe Fehm Geometrie Skript)

4. Automorphismen, invariante Relationen und die Sätze von Krasner

algebraisch haben wir folgende Sachen

kombinatorische Strukturen	$\leftrightarrow$	Gruppe der “Symmetrien”
Relationen gegeben	$\rightarrow$	Automorphismen
Invariante Relation	$\leftarrow$	G gegeben

▶ **Erinnerung (Beispiel 2.8 (c))**
$g \in S_M$ induziert $\tilde{g} \in S_{M^n}$ durch

$$(a_1, \dots, a_n)^g := (a_1, \dots, a_n)^{\tilde{g}} := (a_1^g, \dots, a_n^g)$$

Bezeichnung der $(\tilde{G}, M^n)$ auch mit (G, M^n) oder $(G^{[n]}, M^n)$.
Beispiel 2.8 (a) $\Rightarrow$ Wirkung auf $\mathcal{P}(M^n)$
Bezeichnung $(G, \mathcal{P}(M^n))$ (für $G \leqq S_M$:

$$\Phi^g := \left\{\underline{a}^{\tilde{g}} \mid \underline{a} \in \Phi\right\} \quad \text{vergleiche Definition 1.7 für } \Phi \subseteqq M^n$$

Definition 4.1
$g \in S_M, \Phi \subseteqq M^n$ n-stellige Relation (Elemente (n-Tupel) als Spalten einer "Matrix"). g bewahrt Φ (Bezeichnung $g \rhd \Phi$), also Φ invariant für g, bzw g Automorphismus von Φ

$$:\Leftrightarrow \Phi^g \subseteqq \Phi \text{ bzw. } \Phi^g = \Phi$$

d.h. $\forall a_1, \ldots, a_n \in M\colon (a_1, \ldots, a_n) \in \Phi \overset{\Leftrightarrow}{\Rightarrow} a_1^g, \ldots a_n^g \in \Phi$
(M endlich: $g \rhd \Phi \Leftrightarrow g$ Automorphismus)

Notation
Bezeichne die Menge der endlich-stelligen Relation mit

$$R_M := \{\Phi \mid\subseteq M^n \mid n = 1, 2, 3, \ldots\}$$

$$\operatorname{Aut}\Phi = \operatorname{Aut}_M \Phi := \{g \in S_M \mid \Phi^g = \Phi\}$$

Für $\mathcal{Q} \subseteq R_M$:

$$\operatorname{Aut}\mathcal{Q} := \bigcap_{\Phi \in \mathcal{Q}} \operatorname{Aut}\Phi \quad (\text{Automorphismen von } \mathcal{Q})$$

$$\begin{aligned} n - \operatorname{Inv}(G, M) &:= n - \operatorname{Inv}_M G \; (n - \operatorname{Inv} G) \\ &= \{\Phi \subseteq M^n \mid \forall g \in G\colon g \rhd \Phi\} \end{aligned}$$

n-stellige Invarianten von G:

$$\operatorname{Inv}_M G := \bigcup_{n=1}^{\infty} n - \operatorname{Inv} G \quad (\text{Invarianten von } G)$$

Jede binäre Relation, also auch

$$\{(g, \Phi) \mid \Phi^g = \Phi\} \subseteqq S_M \times R_M$$

induziert eine Galoisverbindung (φ, ψ).

Definition 4.2
Durch Aut und Inv ist eine Galoisverbindung gegeben:

$$\varphi\colon \operatorname{Aut}\begin{cases} \mathcal{P}(R_M) & \to \mathcal{P}(S_M) \\ \mathcal{Q} & \mapsto \operatorname{Aut}\mathcal{Q} \end{cases}$$

$$\psi\colon \operatorname{Inv}\begin{cases} \mathcal{P}(S_M) & \to \mathcal{P}(R_M) \\ G & \mapsto \operatorname{Inv} G \end{cases}$$

insbesondere gelten die folgenden Eigenschaften ($G, G' \subseteq S_M, \mathcal{Q}, Q' \subseteq R_M$):

(i) $G \subseteqq G' \Rightarrow \operatorname{Inv} G \supseteqq \operatorname{Inv} G'$

(ii) $G \subseteqq Q' \Rightarrow \operatorname{Aut}\mathcal{Q} \supseteqq \operatorname{Aut} Q'$

(iii) $G \subseteqq \operatorname{Aut}\operatorname{Inv} G$

(iv) $U \subseteq \operatorname{Inv}\operatorname{Aut} U$ What is U here? :o

(v) $\operatorname{Aut}\operatorname{Inv}\operatorname{Aut}\mathcal{Q} = \operatorname{Aut}\mathcal{Q}$

(vi) $\operatorname{Inv}\operatorname{Aut}\operatorname{Inv} G = \operatorname{Inv} G$

(vii) $G \mapsto \operatorname{Aut}\operatorname{Inv} G$ ist Hüllenoperator What is a Hüllenoperator?

(viii) $\mathcal{Q} \mapsto \operatorname{Inv}\operatorname{Aut}\mathcal{Q}$ ist Hüllenoperator

(ix) $G \subseteqq \operatorname{Aut}\mathcal{Q} \Leftrightarrow \operatorname{Inv} G \supseteqq \mathcal{Q}$

(x) Aut und Inv sind Bijektionen auf den Galoishüllen

$$G = \operatorname{Aut}\operatorname{Inv} G \quad \mathcal{Q} = \operatorname{Inv}\operatorname{Aut}\mathcal{Q}$$

▶ **Bemerkung**

- Definition 4.2 (i)-Definition 4.2 (iv) definieren bereits die Galoisverbindung.
- Definition 4.2 (v) - Definition 4.2 (x) sind Folgerungen aus Definition 4.2 (i)-Definition 4.2 (iv)

▶ **Erinnerung (Hüllenoperator)**
content...

Definition 4.3
Eine Relation der Form

$$(a_1, \ldots, a_n)^G = \{(a_1, \ldots, a_n)^g \mid g \in G\}$$

heißt <u>n-Bahn</u> (n-Orbit) von $G \leqq S_M$.
Notation:

$$\begin{aligned} n - \operatorname{Orb}(G, M) = & \text{ Menge der } n\text{-Bahnen} \\ = & \left\{\underline{a}^G \mid \underline{a} \in M^n\right\} \end{aligned}$$

▶ **Bemerkung**

1. $\Phi \in n - \operatorname{Orb}(G, M) \Leftrightarrow \Phi \in 1 - \operatorname{Orb}(G^{[n]}, M^n)$
2. $\Phi \in \operatorname{Inv}(G, M) \Leftrightarrow \Phi$ invariante Menge von $(G^{[n]}, M^n)$ (vergleiche Punkt 1)

Satz 4.4
Sei $G \leq S_M$.

(a) Jede n-Bahn ist eine invariante Relation:

$$n - \operatorname{Orb}(G, M) \subseteqq n - \operatorname{Inv}(G, M)$$

(b) Jede n-stellige invariante Relation ist (disjunkte) Vereinigung von n-Bahnen

(c) $|n - \operatorname{Inv}(G, M)| = 2^{|n - \operatorname{Orb}(G, M)|}$

proof. 1. $\underline{a}^{G \cdot G} = \underline{a}^G$ für beliebige $\underline{a} \in M^n$ (wobei $\underline{a}^G$ n-Bahn ist)

2. folgt aus Lemma 1.16 (d) (satz 4.4 (b) für n-Bahnen) und Bemerkung zu Definition 4.3 □

Folgerung aus satz 1.18.

Lemma 4.5
Für $\Phi \in n - \mathrm{Orb}(G, M)$ und $\underline{a} = (a_1, \dots, a_n) \in \Phi$, gilt:

$$|\Phi| = [G \colon G_{a_1,\dots,a_n}] = \frac{|G|}{|(a_1, \dots, a_n)|}.$$

($G_{a_1,\dots,a_n}$ ist Stabilisator und $\mathcal{Q} = G^{[n]}$, letzteres gilt nach Beispiel 2.8)

proof.

$$\begin{aligned} \Phi &= (a_1, \dots, a_n)^G =: \underline{a}^{\tilde{G}} \\ \tilde{G}_{\underline{a}} &= G_{a_1 \dots a_n} \text{für Wirkung } (\tilde{G}, M^n) \\ &\xRightarrow{satz\ 1.18} \left|\tilde{G}\right| = |G| = \left|\tilde{G}_{\underline{a}}\right| \cdot \left|\underline{a}^{\tilde{G}}\right| \end{aligned}$$

□

Galoisverbindung Aut – Inv (vergleiche **??**)

- Was sind die Galoishüllen? (d.h. Aut $\mathcal{Q}$ bzw. Inv G?)
- Probleme:
  - Welche (Permutations)Gruppen sind Automorphismengruppen von geeigneten invarianten Relation?
  - Welche Relationsmengen sind die invarianten Relationen für eine geeignete Gruppe $G \leqq S_M$?
- Setze von MAIRE KRASNER (1912-1985) (hier nur für endliche Grundmengen M)

Vorbemerkung:

Satz 4.6
Sei $\mathcal{Q} \subseteq R_M$. Dann ist $\mathrm{Aut}_M\, \mathcal{Q}$ eine (Permutations)Gruppe ($\leq S_M$).

proof. SeSt! □

Theorem 4.7 (1. Satz von Krasner)
Sei $M = \{a_1, \dots, a_m\}$ endlich!

(i) Jede Permutationsgruppe (G, M) ist Automorphismengruppe einer geeigneten Menge von Relationen. Insbesondere gilt:

$$\begin{aligned} G &= \mathrm{Aut}\,\mathrm{Inv}\, G \\ &= \mathrm{Aut}\,\mathrm{Orb}\, G \text{ Orb alle } n\text{-Bahn}, n \in \{1, 2, 3, \dots\} \\ &= \mathrm{Aut}\, m - \mathrm{Orb}\, G \\ &= \mathrm{Aut}\, \underline{a}G \quad (\underline{a} := (a_1, \dots, a_m)) \end{aligned}$$

(Es reicht eine einzige m-stellige Relation)

(ii) Für beliebige Teilmenge $G \subseteqq S_M$ gilt:

$$\langle G \rangle = \mathrm{Aut}\,\mathrm{Inv}\, G$$

($\langle G \rangle$ interne Beschreibung der von G erzeugten Untergruppe, Aut Inv G externe Beschreibung der von G erzeugten Untergruppe (als Galoishülle))

Definition 4.8

1. zu Theorem 4.7 (i) Wir zeigen zunächst

$$\operatorname{Aut}\Phi \subsetneqq G$$

für die von $\underline{a} = (a_1, \dots, a_m)$ erzeugte m-Bahn $\Phi = aG$. Sei $f \in \operatorname{Aut}\Phi \Rightarrow \underbrace{(a_1, \dots, a_m)}_{\in\Phi}^{f} = \underline{a}^{\underline{G}}$, also $\exists g \in G\colon (a_1, \dots, a_m)^f = (a_1, \dots, a_m)^g \in \underline{a}^{\underline{G}}$, d.h. $f = g \in G$, also $\operatorname{Aut}\Phi \subseteq G$.
Die angegebenen Gleichungen folgen nun unmittelbar:

$$G \overset{Definition\ 4.2\ (iii)}{\subsetneqq} \operatorname{Aut}\operatorname{Inv}G \overset{Definition\ 4.2\ (ii)}{\subsetneqq} \operatorname{Aut}\operatorname{Orb}G$$
$$\operatorname{Aut} m - \operatorname{Orb}G \subsetneqq \operatorname{Aut}\{\Phi\} \subsetneqq G.$$

2. zu Theorem 4.7 (ii)

$$G \subsetneqq \operatorname{Aut}\operatorname{Inv}G \quad Definition\ 4.2\ (iii)$$
$$\Rightarrow \langle G\rangle \subsetneqq \langle \operatorname{Aut}\operatorname{Inv}G\rangle \overset{satz\ 4.6}{=} \operatorname{Aut}\operatorname{Inv}G \subseteq \operatorname{Aut}\operatorname{Inv}\langle G\rangle \overset{Theorem\ 4.7\ (i)}{=} \langle G\rangle.$$

▶ **Bemerkung 4.9 (Operationen auf Relationen)**
Jede Formel $\varphi(M, \dots, R_q, a_1, \dots, x_n)$ des Prädikantenkalküls 1. Stufe $(\exists, \forall, \vee, \wedge, \neg, =)$ und Relationssymbole (Prädikate) $R_1, \dots, R_q$ (R_i sind i-stellig, $i = 1, \dots, q$) und freie Variablen $x_1, \dots, x_n$ definiert eine q-stellige Operation

$$Fq : \mathcal{P}(M^{r_i}) \times \dots \mathcal{P}(M^{r_i}) \to \mathcal{P}(M^n)$$

(genau er logische Operation), die q vielen Relationen $\Phi_1 \subseteq M^{r_1}, \dots, \Phi_g \subseteq M^{r_q}$ eine n-stellige Relation $F_\varphi(\Phi_1, \dots, \Phi_q)$ zuordnet:

$$F_\varphi(\Phi_1, \dots, \Phi_q) := \{(a_1, \dots, a_q) \in M^n \mid\models \varphi(\Phi_1, \dots, \Phi_q, a_1, \dots, a_n)\}$$

(wobei $\models$ "es gilt" heisst.)

■ **Beispiel 4.10 (logische Operationen)**

(a) $\varphi(R_1, R_2, x, y) :\equiv \exists z\colon R_1(x, y) \vee R_2(z, y)$

$$F_\varphi(\Phi_1, \Phi_2) = \big\{(x, y) \in M^2 \mid \exists z\colon \Phi_1(x, z) \vee \Phi_2(z, y)\big\} = \varphi_1 \circ \Phi_2 \qquad \text{Relationenprodukt}$$

(b)

$$\varphi_{12}(R_1, R_2, x, y) :\equiv R_1(x, y) \vee \wedge R_2(x, y)$$
$$F_{\varphi_1, \varphi_2}(\Phi_1, \Phi_2) = \Phi_1 \cap \cup \Phi_2$$

(c) $\varphi(R_1, x_1, \dots, x_n) :\equiv \neg R_1(x_1, \dots, x_n)$

$$F_\varphi(\Phi_1) = \neg\Phi_1 \quad (= M^n \setminus \Phi \text{ Komplement})$$

(d) $\varphi(x_1, \dots, x_4) \vee x_1 = x_2 \vee x_3 = x_4$ (keine Prädikate für $q = 0$) $\Rightarrow$ konstante Operation,

$$F_\varphi = \big\{(a_1, a_2, a_3, a_4) \in M^4 \mid a_1 = a_2 \vee a_3 = a_4 \subseteq M^4\big\}$$

(e) $\varphi(x_1, x_2) := x_1 = x_2 \Rightarrow$ Konstante

$$F_\varphi = \big\{(a_1, a_2) \in M^2 \mid a_2 = a_1\big\} = \Delta_M \quad \text{Gleichheitsrelation}$$

(f) $\varphi(R_1, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) := \exists x_i \colon R_1(x_1, \ldots, x_i, \ldots, x_n)$

$$\begin{aligned} F_\varphi(\Phi_1) &= \big\{(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in M^{n-1} \mid \exists a_i \colon (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in \Phi_1\big\} \\ &=: \pi_{n\setminus\{i\}}(\Phi_1) \text{ Projektion von } \Phi_1 \text{ auf die } (\underline{n} \setminus \{i\})\text{-ten Koordinaten.} \end{aligned}$$

Streichen der i-ten Zeile (Bei Darstellung von Relationen durch “Matrix”, Elemente (n-Tupel) als Spalten)

Definition 4.11 (Krasner-Algebra)
Für $\mathcal{Q} \subseteq R_M$ sei

$$[\mathcal{Q}] := \{F_\varphi(\Phi_1, \ldots, \Phi_q) \mid \Phi_1, \ldots, \Phi_q \in \mathcal{Q}, \varphi(R_1, \ldots, R_q, x_1, \ldots, x_n)\}$$

formal wie in Bemerkung 4.9 mit $q \in \{0, 1, 2, \ldots\}$, $n \in \{1, 2, \ldots\}$

Anhang

Index