Permutationsgruppen[1]

Dozent: Dr. Friedrich Martin Schneider
$\LaTeX$: rydval.jakub@gmail.com
Version: 11. November 2016
Technische Universität Dresden

[1]Math Ba ALGSTR: Permutationsgruppen, WS 2015/16

Inhaltsverzeichnis

0 Einleitung

Definition. Gruppe $\langle G, \cdot, {}^{-1}, e \rangle$, wobei G Menge

- $\cdot$ binäre Operation (Multiplikation) auf G,
- e neutrales Element,
- x^{-1} inverses Element zu $x \in G$.

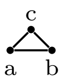
mit folgenden Axiomen:

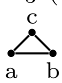
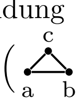
- $\forall x, y, z \in G : (xy)z = x(yz)$, (Assoziativität)
- $\forall x \in G : ex = xe = x$, (Neutrales Element)
- $\forall x \in G : x^{-1}x = xx^{-1} = e$. (Inverses Element)

Wichtige Beispiele:

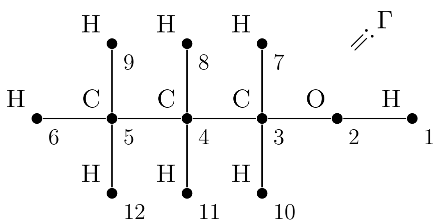
(a) Symmetrie- bzw. Isometriegruppen (geometrisch),
(b) Automorphismengruppen (algebraisch/kombinatorisch).

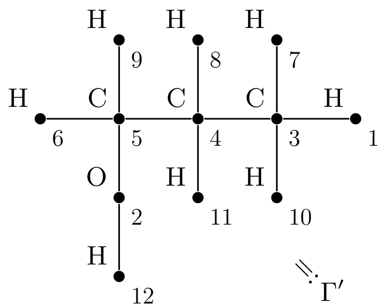
Konkret:

Zu (a): Isometrische Abbildungen der Ebene, die  in Drehung bringen: Drehungen um 0°, 120°, 240°. Spiegelungen um Achsen durch $0, 1, 2 \implies 6$ Symmetrien. Genauer: $G \cong S_3$ (volle symmetrische Gruppe).

Zu (b): Betrachte  als Graphen (Punkte & Knoten). Automorphismus ist 1-1-Abbildung auf Punkten, die Knoten in Kanten überführt $\implies$ Aut () $= S_3$.

Anderes Beispiel:





Zu (a): triviale Symmetrie & Spiegelung an der horizontalen Achse
Zu (b): Es gibt zahlreiche Automorphismen von Γ. Fixpunkte: $1, 2, 3, 4, 5$. Vertauschen der H-Nachbarn von:

3:	$7 \longleftrightarrow 10$	$\implies \operatorname{Aut}\Gamma \cong S_2 \times S_3 \times S_3$
4:	$8 \longleftrightarrow 11$	
5:	$6, 9, 12$	$\implies \lvert\operatorname{Aut}\Gamma\rvert = 24$

Beobachtung: Γ und Γ' sind „im Prinzip“ gleiche Graphen, d.h. es existiert ein Isomorphismus $f : \Gamma \to \Gamma'$.

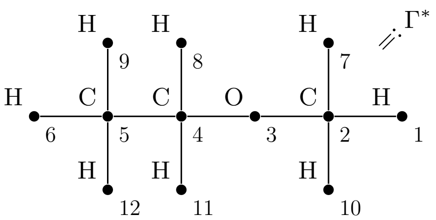
Isomorphieproblem: Wann sind zwei Strukturen im wesentlichen gleich d.h. isomorph? Bemerkung: Isomorphieproblem ist zurückführbar auf Bestimmung der Automorphismengruppe:

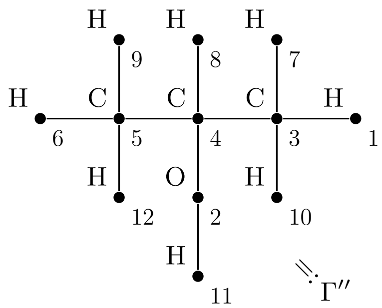
$$\left.\begin{aligned} f &: \Gamma \to \Gamma' \\ f^{-1} &: \Gamma' \to \Gamma \end{aligned}\right\} \text{ist als Automorphismus von } \Gamma \uplus \Gamma' \text{ interpretierbar}$$

Spezialität von Symmetrie-/Automorphismengruppen: ihre Elemente bilden selbst eine algebraische Struktur $\longrightarrow$ Permutationsgruppen.

Nochmal zum Beispiel: (zum Isomorphieproblem, chemische Isomere) Frage: Wie viele verschiedenen Alkohole mit Strukturformel C_3H_7OH gibt es? Antwort: Γ (siehe oben, Siedepunkt 97.1°C) und Γ'' (siehe unten, Siedepunkt 82.4°). Γ und Γ'' sind nicht isomorph! (Übungsaufgabe: Bestimmung von $\operatorname{Aut}\Gamma''$).

Bemerkung: Zur Strukturformel C_3H_8O gibt es noch einen weiteren Bindungsgraphen Γ^* (kein Alkohol):





Allgemeine Lösung: Anzahl lässt sich als Anzahl von „Bahnen“ einer Permutationsgruppe beschreiben (bestimmbar mit Lemma von Cauchy–Frobenius–Burnside)

$\longrightarrow$ Abzähltheorie (POLYA). Anderes Beispiel für POLYAsche Abzähltheorie: Wie viele wesentlich verschiedene Ketten mit 3 Sorten Perlen und fester Anzahl n_i von Perlen der Sorte $i \in \{1, 2, 3\}$ gibt es?

Einordnung:

- Permutationsgruppen sind spezielle „und trotzdem mehr als“ Gruppen (jede Gruppe ist isomorph zu einer Permutationsgruppe).
- Automorphismengruppen (z.B. algebraische Strukturen) sind besonders wichtig!
- historische Bemerkung: Gruppentheorie ist aus dem Studium von Permutationsgruppen entstanden.

Ziele der Vorlesung:

- Permutationsgruppen & Gruppenwirkungen
- Konstruktionen mit Permutationsgruppen
- POLYAsche Abzähltheorie
- Automorphismengruppen von Relationen, speziell von Graphen
- „Paradoxe“ unendliche Gruppen und paradoxe Zerlegungen bzgl. Permutationsgruppen
- „Invariantes Messen“ bzgl. (nicht–paradoxen) Permutationsgruppen

1 Permutationen und Permutationsgruppen

Permutationen einer endlichen Menge M können unterschiedlich definiert werden:

– Als lineare Anordnung der Elemente von M, z.B. für $M = a, b, c$:

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

– Als bijektive Abbildungen in *2-zeilen-Darstellung*, z.B.:

$$\pi_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \begin{array}{l} \longleftarrow \text{Argumentenzeile} \\ \longleftarrow \text{Bildzeile} \end{array}$$

$$\pi_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$\vdots$$

$$\pi_6 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

Allgemein für $M = \{a_1, ..., a_n\}$:

$$\pi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{i_1} & a_{i_2} & \cdots & a_{i_n} \end{pmatrix}$$

bezeichnet $\pi : M \to M$, $a_k \mapsto a_{i_k}$ (Reihenfolge der Spalten spielt keine Rolle).

1.1 Definition. Eine *Permutation* auf einer Menge M ist eine bijektive Abbildung $f : M \to M$. $S_M := S(M) :=$ Menge aller Permutationen auf M. Bezeichnung für Bild $f(a)$ eines Elements $a \in M$ unter $f \in S_M : a^f$.

Also ist

$$\pi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^f & a_2^f & \cdots & a_n^f \end{pmatrix}$$

für $M = \{a_1, ..., a_n\}$.

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

Beweis. Übungsaufgabe. ■

1.3 Definition. Der Graph einer Permutation $f : M \to M$:

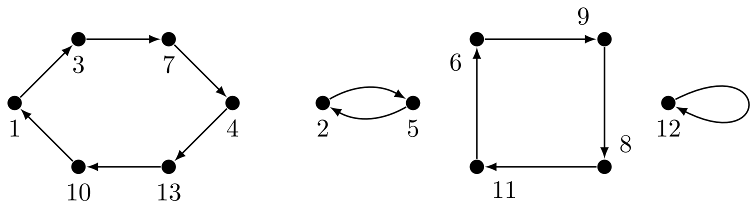
– $f^\bullet := \{(a, b) \in M \times M \mid a^f = b\}$ ist *Graph von f*.

– Die Paare $(a, b) \in f^\bullet$ sind *gerichtete Kanten* eines Graphen $(M, f^\bullet)$ mit Knotenmenge M.

Beispiel.

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

$f^\bullet$:



Fakt: Vorausgesetzt M ist endlich. Der Graph $f^\bullet$ einer Permutation f ist ein Kreis (Zyklus) oder eine Vereinigung von paarweise disjunkten Kreisen (Zyklen). (Folgt aus Bijektivität: Jeder Punkt ist Ausgangs- bzw. Endpunkt genau einer Kante.)

Ab jetzt: M endliche Grundmenge (bis auf Weiteres, falls nicht anders erwähnt).

1.4 Definition. Die *Zyklendarstellung* einer Permutation $f \approx$ „lineares Aufschreiben von f“:

$$f = \begin{pmatrix} a_1 & a_1^f & a_1^{ff} & \cdots & a_1^{f^{k_1}} \end{pmatrix} \cdots \begin{pmatrix} a_l & a_l^f & a_l^{ff} & \cdots & a_l^{f^{k_l}} \end{pmatrix},$$

wobei $(a_1^{f^{k_1}})^f = a_1, ..., (a_l^{f^{k_l}})^f = a_l$. Falls M fest, lässt man Zyklen der Länge 1 weg (*verkürzte Zyklendarstellung*).

Beispiel. Sei f wie oben, dann:

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

Zyklische Permutation := Permutation mit genau einem Zyklus in der verkürzten Zyklendarstellung.

Identische Permutation: $e : x \mapsto x$ (andere Bez.: ε, id_M), Zyklendarstellung: $\begin{pmatrix} 1 \end{pmatrix}$ für $M = \{1, ..., n\}$.

Beachte: $\begin{pmatrix} a & b & c \end{pmatrix}$, $\begin{pmatrix} b & c & a \end{pmatrix}$, $\begin{pmatrix} c & a & b \end{pmatrix}$ bezeichnen dieselbe Permutation (nur Reihenfolge ist wichtig, nicht der Anfangselement).

1.5 Definition. Multiplikation (Produkt) von Permutationen = Hintereinanderausführung (Komposition) von Abbildungen $a \xrightarrow{f} M \xrightarrow{g} M,\ a \mapsto a^f \mapsto a^{fg}$. *Produkt* fg wird definiert durch

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

(alternative Schreibweise: $f; g$, $f \cdot g$, ist wieder eine Permutation, falls $fg \in S^M$).

Beispiel zum Produkt von Permutationen:

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

Fakt: Sei f Permutation mit (verkürzten) Zyklendarstellung

$$f=(-c_1-)(-c_2-)\cdots(-c_k-)$$

(k Zyklen) und sei g_j jeweils die Permutation mit verkürzten Zyklendarstellung $(-c_j-)$, dann $f=g_1\cdot...\cdot g_k$ (d.h. jede Permutation ist Produkt von zyklischen Permutationen).

1.6 Satz. *Die Menge S_M bildet mit der Multiplikation eine Gruppe – die* volle Symmetrische Gruppe *(vom Grad $|M|$, falls M endlich ist).*

Beweis. Übungsaufgabe! ■

Bemerkung. Alle gruppentheoretische Begriffe sind daher insbesondere für Permutationsgruppen definiert, z.B. die Ordnung $\operatorname{ord}(f):=\inf\{m\in\mathbb{N}\backslash\{0\}\mid f^m=e\}$, Untergruppe (UG), Normalteiler (NT), konjugierte Elemente etc.

1.7 Definition. Eine *Permutationsgruppe* G vom Grad n ist eine Untergruppe einer vollen symmetrischen Gruppe S_M vom Grad n.

Bezeichnung: (G,M) oder $G\leq S_M$ falls G Untergruppe. (Permutationsgruppen sind also Paare bestehend aus einer Menge & Gruppe von Permutationen auf dieser).

Meist: $M=\{0,1,...,n-1\}=:n$, d.h. S_n, $M=\{1,2,...,n\}=:\underline{n}$, d.h. $S_{\underline{n}}$.

Weitere Notation: für $U,V\subseteq S_M$:

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

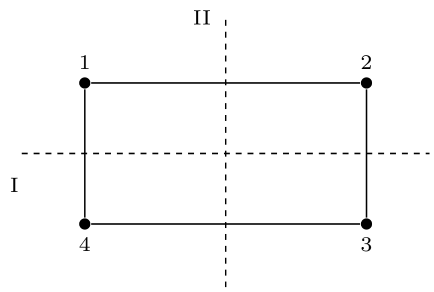
für $a\in M$, $B\subseteq M$, $g\in S_M$:

$$a^U:=\{a^u\mid u\in U\},\ B^g:=\{b^g\mid b\in B\},\ B^U:=\{b^u\mid b\in B,u\in U\}.$$

1.8 Satz (Untergruppenkriterium). *(Voraussetzung: M ist endlich) $U\subseteq S_M$ ist Gruppe gdw. $U\neq\emptyset$ und $UU\subseteq U$.*

Beweis. Übungsaufgabe! ■

1.9 Beispiel. Symmetriebildungen eines Rechtecks in der Ebene können durch Permutationen der Eckpunkte beschrieben werden.



Identische Abbildung: (1) =: e, Drehung um 180°: (1 3)(2 4) =: g_1, Spiegelung an I: (1 4)(2 3) =: g_2, Spiegelung an II: (1 2)(3 4) =: g_3. $G := \{e, g_1, g_2, g_3\}$ ist Permutationsgruppe vom Grad 4. $G \cong$ Symmetriegruppe des Rechtecks genannt die *kleinsche Vierergruppe* ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2$).

1.10 Definition. (G, M) Permutationsgruppe, $a \in M$. Dann ist:

(a) $G_a := \{g \in G \mid a^g = a\}$ *Stabilisator* von a.[2] Verallgemeinerung:

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

ist *punktweise Stabilisator* von $\{a_1, \dots, a_m\}$.

(b) $a^G := \{a^g \mid g \in G\}$ *Bahn* von a (auch 1-*Bahn*, *Orbit*), $\text{1-Orb}\,(G, M) :=$ Menge aller 1-Bahnen.

(c) $B \subseteq M$ *invariant* (bzgl. G) $:\Longleftrightarrow B^G = B$ ($\Longleftrightarrow$ $B \subseteq B$).

(d) G *transitiv* $:\Longleftrightarrow \exists a \in M : a^G = M \iff |\text{1-Orb}\,(G, M)| = 1 \iff \forall a \in M : a^G = M$.
Bedeutung: Alle Elemente von M haben gleiche „Eigenschaften" in der Struktur, falls $G = \text{Aut}\,(\text{Struktur auf } M)$.

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

(i) *G_a ist Untergruppe von G.*

(ii) *$G_{a^g} = g^{-1} G_a g$ für jedes $g \in G$.*

(iii) *Durch $a \sim b :\Longleftrightarrow a^G = b^G$ ist eine ÄR auf M definiert und $\text{1-Orb}\,(G, M) = {}^{M}/_{\sim} \implies$ die Menge $\text{1-Orb}\,(G, M)$ bildet Partition der Menge M. (Zwei Bahnen sind entweder gleich oder disjunkt, beachte: $b \in a^G \iff a \in b^G$ — Übungsaufgabe!)*

(iv) *Jede invariante Menge $B \subseteq M$ ist Vereinigung von 1-Bahnen:*

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

Beweis. Übungsaufgabe! ■

[2] D.h. Menge aller Permutationen in G für die a ein Fixpunkt ist.

Bemerkung. Ein Repräsentantensystem einer Partition (z.B. 1-Orb (G, M)) heißt auch *Transversale.*

Wiederholung Algebra:

1.12 Satz von LAGRANGE. *Die Ordnung $|U|$ jeder Untergruppe U einer endlichen Gruppe G ist Teiler der Gruppenordnung $|G|$. Es gilt:*

$$|G| = \underbrace{[G:U]}_{\text{Index v. } U \text{ in } G} \cdot |U|$$

Beweis. ${}^G/_U = \{Ug \mid g \in G\}$ ist Partition der Menge G. Nach Definition ist $k := [G : U] = |{}^G/_U| =$ Anzahl der Nebenklassen von U in G. Also $G = Ug_1 \uplus ... \uplus Ug_k$ für beliebige Transversale $g_1, ..., g_k \in G$. Da $|U| = |Ug_i|$ für jedes $i \in \{1, ..., k\}$ folgt Behauptung. ∎

1.13 Lemma. *Sei $a \in M$, $G \leq S_M$. Durch $a^G \to {}^G/_{G_a}$, $a^g \mapsto G_a g$ ist eine bijektive Abbildung zwischen Elementen der von a erzeugten Bahn und Nebenklassen des Stabilisators G gegeben. Insbesondere gilt: $|a^G| = [G : G_a] = |{}^G/_{G_a}|$.*

Beweis. Kette von Äquivalenzen:

$$a^g = a^{g^i} \iff a = a^{g^i g^{-1}} \iff g^i g^{-1} \in G_a \iff g^i \in G_a g \iff G_a g^i = G_a g.$$

Die Hinrichtungen zeigen, dass die Abbildung wohldefiniert ist, die Rückrichtungen zeigen, dass die Abbildung injektiv ist. Surjektivität klar. ∎

Aus 1.12 und 1.13 folgt:

1.14 Folgerung. *Permutationsgruppentheoretische Umformulierung des Satzes von Lagrange: Für $a \in M$, $G \leq S_M$ gilt:*

$$|G| = |G_a| \cdot |a^G|.$$

Beweis. $|G| \overset{1.12}{=} [G : G_a] \cdot |G_a| \overset{1.13}{=} |a^G||G_a|$. ∎

1.15 Beispiel. $G := S_{\underline{4}}$ (d.h. $M = \{1, 2, 3, 4\}$). $1^G = \{1, 2, 3, 4\} \implies |G_1| \overset{1.14}{=} \frac{|G|}{|1^G|} = \frac{4!}{4} = 6$. Auflistung der Elemente von G_1: $G_1 = \{(1), (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}$. Iteration führt zu: $|G_{1,2}| = \frac{|G_1|}{|2^{G_1}|} = \frac{6}{3} = 2$. Auflistung: $G_{1,2} = \{(1), (3\ 4)\}$. Ein weiterer Schritt: $|G_{1,2,3}| = \frac{|G_{1,2}|}{|3^{G_{1,2}}|} = \frac{2}{2} = 1$. Auflistung: $G_{1,2,3} = \{(1)\}$.

1.16 Definition. Zwei Permutationsgruppen (G, M), (H, N) heißen *ähnlich*, wenn eine bijektive Abbildung $f : M \to N$ und ein Gruppenisomorphismus $\varphi : G \to H$ existieren, so dass gilt:

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

d.h. $gf = f\varphi(g)$ für jedes $g \in G$. D.h.: für jedes $g \in G$ ist das Diagramm

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

kommutativ.

Bemerkung: Durch f und G ist H vollständig festgelegt. Für $g \in G$, $y \in M$ sei $a := f^{-1}(y)$. Dann $y^{\varphi(g)} = f(a)^{\varphi(g)} = f(a^g) = f(f^{-1}(y)^g) = y^{f^{-1}gf}$. Also $H = \{\varphi(g) \mid g \in G\} = \{f^{-1}gf \mid g \in G\}$. Beobachtung: Sogar φ ist durch f und G eindeutig bestimmt.

Beachte: Ähnlichkeit $\implies$ Isomorphie ($\impliedby$ gilt i.a. nicht).

1.17 Beispiel. (a) S_M ähnlich zu $S_N \iff |M| = |N|$.

(b) $(\overbrace{\{e, (1\ 2)\}}^{=:G}, \{1, 2\})$ ist ähnlich zu $(\{e, (\alpha\ \beta)\}, \{\alpha, \beta\})$, aber nicht zu $(\underbrace{\{e, (1\ 2)\}}_{=:G'}, \{1, 2, 3\})$, obwohl $G \cong G'$ (als abstrakte Gruppen).

1.18 Definition. (a) Zwei Permutationen $g_1, g_2 \in S_M$ heißen *ähnlich*, wenn in ihrer Zyklendarstellung gleich viele Zyklen gleicher Länge vorkommen. Z.B.: $g_1 = (1)(2)(3\ 4\ 5)(6\ 7)(8\ 9)$ und $g_2 = (3)(7)(1\ 4\ 9)(2\ 8)(5\ 6)$ sind ähnlich.

(b) Sei $G \leq S_M$. Dann heißt $g_2 \in S_M$ *konjugiert zu* $g_1 \in S_M$ *in* G, wenn ein $f \in G$ existiert, sodass $g_2 = f^{-1}g_1 f$. (Sprechweise: g_1 und g_2 sind konjugiert in G).

1.19 Lemma. (a) *Konjugiertheit und Ähnlichkeit sind ÄR in S_M.*

(b) *Aus der Darstellung*

$$g = (a_1\ a_2\ \cdots)(b_1\ b_2\ \cdots)(\cdots) \in S_M$$

erhält man die Zyklendarstellung von $f^{-1}gf$ für $f \in S_M$ wenn man f auf jedes Element in jedem Zyklus anwendet:

$$f^{-1}gf = (a_1^f\ a_2^f\ \cdots)(b_1^f\ b_2^f\ \cdots)(\cdots).$$

(c) *g_1 konjugiert zu g_2 in $G \implies g_1$ und g_2 sind ähnlich ($\impliedby$ gilt i.a. nicht). Aber: g_1 konjugiert zu g_2 in $S_M \iff g_1$ und g_2 sind ähnlich.*

(d) *$g_1, g_2 \in S_M$ ähnlich $\iff$ die erzeugten (zyklischen) Uuntergruppen $(\langle g_1 \rangle, M)$ und $(\langle g_2 \rangle, M)$ sind ähnlich im Sinne von 1.16.*

Beweis. Übungsaufgabe! ∎

2 Gruppenwirkungen und Darstellungen

2.1 Definition. Ein (Gruppen-)Homomorphismus $\psi : G \to S_M$ einer (abstrakten) Gruppe G in eine symmetrische Gruppe S_M heißt *Permutationsdarstellung* von G (vom Grad $|M|$).

– ψ und die dazugehörige Gruppenwirkung, vgl. unten, heißen *treu* $:\iff$ ψ ist injektiv.

Bemerkung: ψ treu $\iff$ $\operatorname{Ker}\psi = \{g \in G \mid \psi(g) = e\} = \{e_G\} \implies G \cong \psi(G) \leq S_M$ (Homomorphiesatz, eigentlich ${}^{G}/_{\operatorname{Ker}\psi}$, aber $\operatorname{Ker}\psi = \{e_G\} \implies {}^{G}/_{\operatorname{Ker}\psi} = G$).

2.2 Definition. Sei G Gruppe und M Menge. Eine Abbildung $\varphi : G \times M \to M, (x, g) \mapsto \varphi(x, g) =: xg$ heißt *Gruppenwirkung* von G auf M, falls gilt:

(i) $\underset{\varphi(x,e_G)}{\overset{\|}{xe_G}} = x \ \forall x \in M$,

(ii) $\underset{\varphi(\varphi(x,g)g')}{\overset{\|}{(xg)g'}} = \underset{\varphi(x,gg')}{\overset{\|}{x(gg')}} \ \forall x \in M, g, g' \in G$.

Sprechweise: *G wirkt* (*operiert*) auf M.
Schreibweise: (G, M) Gruppenwirkung.
Bemerkung: Jede Permutationsgruppe $G \leq S_M$ operiert in natürlicher Weise auf M: $\varphi(x, g) := x^g$ $(x \in M, g \in G)$.

2.3 Satz. *Jeder Gruppenwirkung entspricht in eindeutiger Weise eine Permutationsdarstellung $\psi : G \to S_M$ und umgekehrt. Und zwar in folgender Weise: $x^{\psi(g)} = \varphi(x, g)$. ($:=$ falls φ gegeben, $=:$ falls ψ gegeben.)*

Beweis. Übungsaufgabe! ■

Hinweis:

– Falls φ gegeben, so ist $\psi(g)$ (definiert wie oben) eine Permutation auf M (für jedes $g \in G$), und ψ ist Homomorphismus.
– Falls ψ gegeben, so erfüllt φ (i) und (ii).

2.4 Lemma. (a) *Ist G (abstrakte) Gruppe, so ist durch $h^{g^*} := hg$ (Rechtsmultiplikation mit g) für $g \in G$ eine Permutation $g^* \in S_G$ gegeben für $h \in G$.*
(b) *$\psi : G \to S_G$ ist Permutationsdarstellung (Homo.), $\psi : g \mapsto g^*$.*
(c) *$\varphi : G \times G \to G$, $(h, g) \mapsto hg$ ist zugehörige Gruppenwirkung.*
(d) *ψ oben ist treu (und heißt rechtsreguläre Darstellung v. G.*

2.5 Satz (CAYLEY). *Für beliebige Gruppe G ist $G^* := \{g^* \mid g \in G\} \leq S_G$ zu G isomorphe Permutationsgruppe, (G^*, G) heißt rechtsreguläre Darstellung von G.*

Beweis von Lemma 2.4. (a) und (b) folgen wegen 2.3 aus (c). Zu (c):

(i) $\varphi(h, e) = he = h$,
(ii) $\varphi(h, gg') = h(gg') = (hg)g' = \varphi(\varphi(h, g), g')$.

Noch zu zeigen ist (d): Seien $g_1, g_2 \in G$ mit $g_1^* = g_2^*$. Dann ist $g_1 = e^{g_1^*} = e^{g_2^*} = g_2$. ■

2.6 Bemerkungen. (a) *Ist $g \in G\backslash\{e\}$, dann hat $g^* : M \to M$ keinen Fixpunkt.*
(b) *Jedes $g*$ zerfällt in Produkt von Zyklen der Länge* $\operatorname{ord}(g)$. *(Zum Beweis: Die Zyklen von g^* sind alle von der Form $(h\ hg\ hg^2\ \cdots\ hg^{n-1})$ für $h \in G$ und $n := \operatorname{ord}(g)$.)*
(c) *G^* hat Grad $|G|$.*
(d) *G^* ist transitiv (d.h. es gibt nur eine Bahn, $G = e^{G^*}$).*
(e) *Die Eigenschaften* (a)-(d) *charakterisieren die Regularität von G^* (vgl. 5.4).*

2.7 Beispiele. (1) *Wirkung durch Konjugation*: $\varphi : G \times G \to G,\ (h, g) \mapsto g^{-1}hg$, $\psi : G \to S_G,\ g \mapsto \psi(g)$ mit $h^{\psi(g)} := g^{-1}hg$.
(2) *Wirkung auf Untergruppen*: $U \leq G$, $\varphi : \overbrace{\operatorname{Sub}(G)}^{\text{Menge aller Untergruppen von } G} \times G \to \operatorname{Sub}(G),\ (U, g) \mapsto g^{-1}Ug$.
(3) *Wirkung auf Rechtsnebenklassen*: $G/U = \{Uh \mid h \in G\}$ Faktorgruppe einer Untergruppe $U \leq G$, $\varphi : G/U \times G \to G/U,\ (Uh, g) \mapsto Uhg$.

2.8 Satz. *Wirkungen von Permutationsgruppen (G, M) auf anderen Mengen:*

(a) *Induzierte Wirkung von G auf $\mathfrak{P}(M)$: $\varphi : \mathfrak{P}(M) \times G \to \mathfrak{P}(M),\ (B, g) \mapsto B^g = \{b^g \mid b \in B\}$. Bezeichnung: $(G, \mathfrak{P}(M))$.*
(b) *(Einschränkung von* (a)*) Wirkung von G auf $\mathfrak{P}_n(M)$:= Menge aller n-elementigen Teilmengen von M: $\varphi : \mathfrak{P}_n(M) \times G \to G,\ (B, g) \mapsto B^g$. Bezeichnung: $(G^{\{n\}}, \mathfrak{P}_n(M))$.*
(b) *Induzierte Wirkung von G auf M^n: $\varphi : M^n \times G \to M^n$; $((a_1, ..., a_n, g) \mapsto (a_1^g, ..., a_n^g)$. Bezeichnung: $(G^{[n]}, M^n)$.*

3 Erzeugendensysteme & Sims-Ketten

Problem: Beschreibung von Permutationsgruppen. Aufzählung aller Elemente ist selten möglich bzw. nötig. ($S_{\underline{100}}$ hat 100! Elemente!)

Ausweg:

– Beschreibung als Automorphismengruppe (s. Kapitel 4,5)
– oder durch Erzeugendensysteme

Wiederholung aus Algebra

3.1 Definition. $U \subseteq G$ heißt *Erzeugendensystem* einer Gruppe $G :\Longleftrightarrow$ jedes $g \in G$ ist als Produkt $g = u_1 \cdots u_m$ mit $u_i \in U$ oder u_i^{-1} ($i \in \{1, ..., m\}$, $m \in \mathbb{N}$) darstellbar. Bezeichnung: $G = \langle U \rangle_G$. Für große G kennt man manchmal nur ein Erzeugendensystem U.

Probleme:

(P1) Entscheide $g \in \langle U \rangle$ für $g \in S_{\underline{n}}$ und $U \subseteq S_{\underline{n}}$.
(P2) Beschreibe Bahnen von $\langle U \rangle$, also $a^{\langle U \rangle}$ für gegebenes $a \in \underline{n}$.
(P3) Beschreibung der Untergruppen von $\langle U \rangle$.

Methode (Charles Sims)

Für „große“ Gruppen: Man benutzt Mengen T_i ($i = 1, ..., r$), sodass $G = T_r \cdot T_{r-1} \cdot ... \cdot T_1$ (Komplexprodukt) und die Darstellung $g = t_r \cdot t_{r-1} \cdot ... \cdot t_1$ (ist eindeutig!) für jedes $g \in G$ (wichtige Anwendung in der Kodierungstheorie!). „Speicheraufwand“: $\sum_{i=1}^r |T_i|$ (im Vergleich zu $|G| = \prod_{i=1}^r |T_i|$). Beispiel: $G = S_n \implies |G| = n!$. Aber $\sum_{i=1}^r |T_i| \leq n(n+1)/2$ ist möglich. Jede Permutation benötigt Speicheraufwand n, also wächst Speicherbedarf insgesamt wie n^3.

3.2 Definition. Die *Sims-Kette* einer Permutation $G \leq S_M$ mit $M = \{a_1, ..., a_n\}$: Für punktweise Stabilisatoren (vgl. 1.10)

$$U_1 = G_{a_1}, U_2 := G_{a_1,a_2}, ..., U_{n-1} = G_{a_1,...,a_{n-1}} = G_{a_1,...,a_n} = \{e\}$$

gilt $\{e\} = U_{n-1} \leq U_{n-2} \leq ... \leq U_2 \leq U_1 := G$. Sei $r := \min\{i \mid U_i = \{e\}\}$ (hängt von Reihenfolge der Elemente a_i ab). Dann heißt $(a_1, ..., a_r)$ *Sims-Basis* von G und $\{e\} = U_r \lneqq U_{r-1} \leq ... \leq U_1 \leq U_0 = G$ heißt die *Sims-Kette* von G (zur Basis $(a_1, ..., a_r)$) der Länge r.

Für Nebenklassenzerlegung ${}^{U_{i-1}}\!/_{U_i} = U_i g_{i_1} \uplus U_i g_{i_2} \uplus ... \uplus U_i g_{i_{n_i}}$ wird Repräsentantensystem (Transversale) $T_i := \{g_{i_1}, ..., g_{i_{n_i}}\} \subseteq U_{i-1}$ gewählt ($i = 1, ..., r$). (Meist $g_{i_1} = e$). Beachte: ${}^{U_{r-1}}\!/_{U_r} \cong U_{r-1} \implies T_r = U_{r-1}$.

Bemerkung: Bei Umnummerierung der Elemente von M entstehen möglicherweise kürzere Basen!

3.3 Satz. *Seien $G, T_1, ..., T_r$ wie in 3.2. Dann gilt:*

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

$$g = h_r h_{r-1} \cdots h_1$$

mit $h_i \in T_i$ ($i \in \{1, ..., r\}$) darstellen. Insbesondere gilt $G = T_1 T_{r-1} \cdots T_1$ und $|G| = \prod_{i=1}^{r} |T_i|$.

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

Bemerkung. (a) $\implies$ $T_1 \cup ... \cup T_r$ ist ein (spezielles) Erzeugendensystem für G.

Beweis. Zu (a): Sei $g \in G$

$$\begin{aligned}
&\overset{T_1 \text{ Transversale}}{\underset{\text{von } G/U_1}{\Longrightarrow}} \exists! h_1 \in T_1 : g \in U_1 h_1 &&\implies g h_1^{-1} \in U_1 \\
&\overset{T_2 \text{ Transversale}}{\underset{\text{von } U_1/U_2}{\Longrightarrow}} \exists! h_2 \in T_2 : g h_1^{-1} \in U_2 h_2 &&\implies g h_1^{-1} h_2^{-1} \in U_2 \\
&\vdots \\
& &&\implies g h_1^{-1} h_2^{-1} ... h_r^{-1} \in U_r = \{e\}.
\end{aligned}$$

$\implies$ $g = h_r h_{r-1} \cdots h_2 h_1$ (Existenz der Darstellung). Eindeutigkeit: Annahme: $g = h_r \cdots h_1 = h'_r \cdots h'_1$ mit $h_i, h'_i \in T_i$ ($i \in \{1, ..., r\}$). Es gilt $\underbrace{h_r \cdots h_2}_{\in U_1} h_1 = \underbrace{h'_r \cdots h'_2}_{\in U_1} h'_1 \implies h_1 \in U_1 h'_1$

$$\overset{T_1 \text{ Transversale}}{\underset{\text{von } G/U_1}{\Longrightarrow}} h_1 = h'_1 \implies \underbrace{h_r \cdots h_2}_{\in U_2} = \underbrace{h'_r \cdots h'_2}_{\in U_2} \implies h_2 = h'_2$$

$$\vdots$$

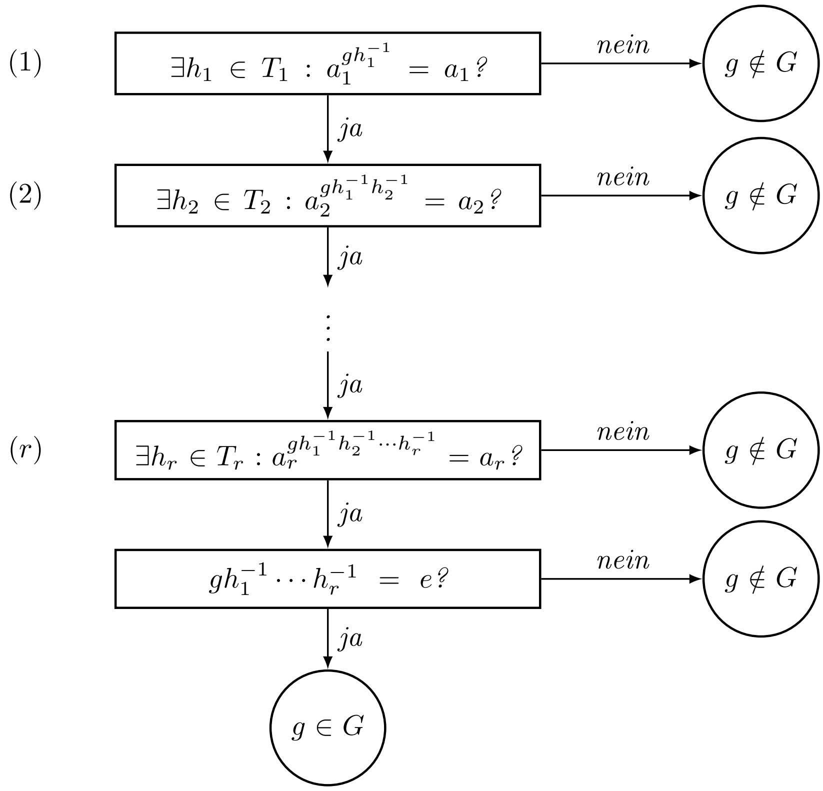
$$\implies h_i = h'_i \text{ für jedes } i \in \{1, ..., r\}.$$

Zu (b): $g, g' \in G$ mit $(a_1^g, ..., a_r^g) = (a_1^{g'}, ..., a_r^{g'}) \implies a_i^{g(g')^{-1}} = a_i$ für jedes $i \in \{1, ..., r\}$, d.h. $g(g')^{-1} \in G_{a_1, ..., a_r} = \{e\} \implies g = g'$.

■

3.4 Beispiel. $G = S_{\underline{4}}$ mit $M = \{1, 2, 3, 4\}$. Es gilt $G_1 \cong S_{\underline{3}}$, $G_{1,2} \cong S_{\underline{2}}$, $G_{1,2,3} = \{e\}$. $T_1 = \{e, g_1, g_1^2, g_1^3\}$ für $g_1 := (1\ 2\ 3\ 4)$, $T_2 = \{e, g_2, g_2^2\}$ für $g_2 := (2\ 3\ 4)$, $T_3 = \{e, g_3\}$ für $g_3 := (3\ 4)$ $\overset{3.3}{\Longrightarrow}$ Jedes $g \in S_{\underline{4}}$ ist eindeutig (!) in der Form $g = g_3^{\alpha_3} \cdot g_2^{\alpha_2} \cdot g_1^{\alpha_1}$ mit $\alpha_1 \in \{0, 1, 2, 3\}$, $\alpha_2 \in \{0, 1, 2\}$, $\alpha_3 \in \{0, 1\}$ darstellbar.

3.5 Folgerung (Testalgorithmus). *Für G seien $T_1, ..., T_r$ wie in 3.2 gegeben. Sei $g \in S_M$. Test für $g \in G$:*



Problem: Wie findet man die Repräsentantensysteme $T_1, ..., T_r$ für die Untergruppen falls nur Erzeugendensystem U für G gegeben ist? (vgl Problem 3.1 (P3)) Antwort gibt ein Resultat von SCHREIER:

3.6 Satz (SCHRIER). *Sei G Gruppe und $U = \{g_1, ..., g_m\}$ endliches Erzeugendensystem für G. Sei $V \leq G$ Untergruppe mit Nebenklassenzerlegung $G = Vh_1 \uplus Vh_2 \uplus ... \uplus Vh_s$ (oBdA $h_1 = e$), $T := \{h_1, ..., h_s\}$ Transversale für ${}^G/_V$. Für $g \in G$ sei $\varphi(g) \in T$ der Repräsentant der Nebenklasse Vg (d.h. $g \in V\varphi(g)$, $\varphi : G \to T$ Repräsentantenabb.). Dann ist*

$$X := \{h_i g_j^k \varphi(h_i g_j^k)^{-1} \mid i \in \{1, ..., s\}, j \in \{1, ..., m\}, \underbrace{k \in \{-1, 1\}}_{\substack{\textit{entfällt falls} \\ G \textit{ endlich ist}}}\}$$

ein Erzeugendensystem für die Gruppe V.

Beweis. (1) $X \subseteq V$, denn $h_i g_j^k \in V\varphi(h_i g_j^k) \implies h_j g_j^k \varphi(h_i g_j^k)^{-1} \in V$ für $j \in \{1, ..., m\}$, $i \in \{1, ..., m\}$, $k \in \{-1, 1\}$.

(2) Bemerkung: Ist G endlich, dann gilt $\forall g \in G : g^{-1} = g^{n-1}$ mit $n := \mathrm{ord}\,(g)$. Sei

$g \in V$. Dann gibt es Darstellung $g = g_{i_1}^{k_1} \cdots g_{i_t}^{k_t}$ mit $k_1, ..., k_t \in \{-1, 1\}$. Es gilt:

$$\begin{aligned} g = h_1 g_{i_1}^{k_1} \cdots g_{i_t}^{k_t} &= \underbrace{h_1 g_{i_1}^{k_1} \varphi(h_1 g_{i_1}^{k_1})^{-1}}_{\in X} \underbrace{\varphi(h_1 g_{i_1}^{k_1})}_{=:h_{j_1} \in T} g_{i_2}^{k_2} \cdots g_{i_t}^{k_t} \\ &= \underbrace{\qquad\qquad}_{\in X} \underbrace{h_{j_1} g_{i_2}^{k_2} \varphi(h_{j_1} g_{i_2}^{k_2})^{-1}}_{\in X} \underbrace{\varphi(h_{j_1} g_{i_2}^{k_2})}_{=:h_{j_2} \in T} g_{j_3}^{k_3} \cdots g_{j_t}^{k_t} \\ &\vdots \\ &= \underbrace{\qquad\qquad}_{\in X} \cdots \underbrace{\qquad\qquad}_{\in X} \underbrace{\varphi(h_{j_{t-1}} g_{i_t}^{k_t})}_{\in T} \end{aligned}$$

$\implies \varphi(h_{j_{t-1}} g_{i_t}^{k_t}) = e \implies g$ ist Produkt von Elementen aus X.

■

3.7 Satz (Erzeugendensysteme der Gruppe $S_{\underline{n}}$). *Folgende Mengen erzeugen $S_{\underline{n}}$:*

(a) $\{(i\ j) \mid i, j \in \underline{n}\}$,
(b) $\{(1\ 2), (2\ 3), (3\ 4), ..., (n-1\ n)\}$,
(c) $\{(1\ 2), (1\ 3), (1\ 4), ..., (1\ n)\}$,
(d) $\{(1\ 2), (1\ 2\ 3\ \cdots\ n)\}$.

Beweis. Zu (a): Für Zyklen gilt $(a_1\ \cdots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k)$ (ohne Beweis). Jede Permutation ist Produkt von Zyklen.
Zu (b): Sei $i < j$. Dann gilt: $(i\ j) = (i\ i+1)(i+1\ i+2)\cdots(j-1\ j)(j-2\ j-1)(j-3\ j-2)\cdots(i+1\ i+2)(i\ i+1)$.
Zu (c): $(i\ j) = (1\ i)(1\ j)(1\ i)$. Weiter mit (a).
Zu (d): $g = (1\ 2)$, $h = (1\ 2\ 3\ \cdots\ n)$, $(2\ 3) = h^{-1}gh$, $(3\ 4) = h^{-1}(2\ 3)h$,...,$(n-1\ n) = h^{-1}(n-2\ n-1)h$. Weiter mit (b).

■

Bemerkung: Zerlegung in Transpositionen ist nicht eindeutig (im Gegensatz zu Sims-Ketten-Zerlegung 3.3).

3.9 Definition. Sei $g \in S_{\underline{n}}$. Eine *Inversion* von g ist ein Paar $(i, j) \in \underline{n} \times \underline{n}$ mit $i < j$ und $i^g > j^g$. Beispiel:

– Die Permutation $(1\ 2)(3\ 4)$ hat die Inversionen $(1, 2)$, $(3, 4)$.
– Die Permutation $(1\ 3)(2)$ hat die Inversionen $(1, 3)$, $(1, 2)$, $(2, 3)$.

Definiere *Signum* von g:

$$\operatorname{sgn}(g) := \begin{cases} 1 & \text{falls die Anzahl der Inversionen von } g \text{ gerade ist,} \\ -1 & \text{falls die Anzahl der Inversionen von } g \text{ ungerade ist.} \end{cases}$$

g hei§t *gerade Permutation*, falls $\operatorname{sgn}(g) = 1$ und *ungerade Permutation*, falls $\operatorname{sgn}(g) = -1$.

Bemerkungen. Für $g \in S_{\underline{n}}$ gilt:

(1) $\operatorname{sgn}(g) = \prod_{i<j} \frac{j^g - i^g}{j-i} = \prod_{i<j} \frac{j^{gh} - i^{gh}}{j^h - i^h}$ für jedes $h \in S_{\underline{n}}$.

(2) $\operatorname{sgn}(gh) = \operatorname{sgn}(g)\operatorname{sgn}(h) \forall g, h \in G$. Begründung:

$$\operatorname{sgn}(g)\operatorname{sgn}(h) = \prod_{i<j} \frac{j^g - i^g}{j-i} \cdot \prod_{i<j} \frac{j^h - i^h}{j-i} \overset{(1)}{=} \prod_{i<j} \frac{j^{gh} - i^{gh}}{j^h - i^h} \cdot \frac{j^h - i^h}{j-i} = \operatorname{sgn}(gh).$$

(3) $\operatorname{sgn}(e) = 1$, $\operatorname{sgn}(g^{-1}) = \operatorname{sgn}(g)$. Begründung: $1 = \operatorname{sgn}(e) \overset{(2)}{=} \operatorname{sgn}(g)\operatorname{sgn}(g^{-1})$.

(4) $\operatorname{sgn} : S_{\underline{n}} \to \{-1, 1\}$ ist ein Homomorphismus auf die multiplikative Gruppe $\{-1, 1\}$.

(5) Die geraden Permutationen bilden Untergruppe von $S_{\underline{n}}$. Diese Bezeichnen wir mit $A_{\underline{n}}$, die *alternierende Gruppe.*

(6) $g \in S_{\underline{n}}$ gerade (ungerade) $\iff$ für jede Darstellung von g als Produkt von Transpositionen $g = t_1 t_2 \cdots t_q$ ist g gerade (ungerade). Begründung: $g = t_1 t_2 \cdots t_q \implies \operatorname{sgn}(g) = \operatorname{sgn}(t_1) \cdots \operatorname{sgn}(t_q) = (-1)^q$.

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

Beweis. Erster Teil gilt wegen 3.9.(b): $\operatorname{sgn} : S_{\underline{n}} \to \{-1, 1\}$ ist Homomorphismus $\implies A_{\underline{n}} = \{g \in S_{\underline{n}} \mid \operatorname{sgn}(g) = 1\} = \operatorname{Ker}(\operatorname{sgn})$ ist ein Normalteiler von $S_{\underline{n}}$. Homomorphiesatz: $S_{\underline{n}}/A_{\underline{n}} \cong \{-1, 1\}$, da sgn surjektiv ist. Also $2 = |S_{\underline{n}}/A_{\underline{n}}| \implies |A_{\underline{n}}| = |S_{\underline{n}}|/2 = n!/2$. ■

3.11 Beispiel. $G = S_{\underline{n}}$, $V = A_{\underline{n}}$. Dann $S_{\underline{n}} = \langle g_1, g_2 \rangle$ mit $g_1 := (1\ 2)$, $g_2 := (1\ 2\ \cdots\ n)$ (vgl. 3.7.(d)). $S_{\underline{n}} = Vh_1 \uplus Vh_2 = A_{\underline{n}} \underbrace{e}_{=:h_1} \uplus A_{\underline{n}} \underbrace{(1\ 2)}_{=:h_2 = g_1}$. Satz 3.6: $A_{\underline{n}}$ wird erzeugt von:

– $h_1 g_1 \varphi(h_1 g_1)^{-1} = e(1\ 2)(1\ 2) = e$.

– $h_1 g_2 \varphi(h_1 g_2)^{-1} = \begin{cases} g_2(1\ 2) & \text{falls } n \text{ ungerade,} \\ g_2 e & \text{falls } n \text{ gerade.} \end{cases}$

– $h_2 g_1 \varphi(h_2 g_1)^{-1} = (1\ 2)(1\ 2)e = e$.

– $h_2 g_2 \varphi(h_2 g_2)^{-1} = \begin{cases} (1\ 2)(1\ 2\ \cdots\ n)(1\ 2) = (2\ 1\ 3\ 4\ \cdots\ n) & \text{falls } n \text{ ungerade,} \\ (1\ 2)(1\ 2\ \cdots\ n)e = (1\ 3\ 4\ \cdots\ n) & \text{falls } n \text{ gerade.} \end{cases}$

$\implies$ Erzeugendensystem für $A_{\underline{n}}$:

falls n gerade:	falls n ungerade:
$(2\ 3\ 4\ \cdots\ n)$	$(1\ 2\ 3\ \cdots\ n)$
$(1\ 3\ 4\ \cdots\ n)$	$(2\ 1\ 3\ 4\ \cdots\ n)$

.

4 Automorphismen, invariante Relationen und die Sätze von KRASNER

Wiederholung. 2.8 (c): $g \in S_M$ induziert $\tilde{g} \in S_{M^n}$ durch

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

Bezeichnung der Wirkung $(\tilde{G}, M^n)$ auch mit (G, M^n).
2.8 (a): Wirkung von G auf $\mathfrak{P}(M^n)$ für $G \leq S_M$:

$$\Phi^{\tilde{g}} := \{\underline{a}^{\tilde{g}} \mid \underline{a} \in \Phi\}$$

für $\Phi \subset M^n$ (vgl. 1.7).

4.1 Definition. $g \in S_M$, $\Phi \subset M^n$ n-stellige Relation.

– *g bewahrt* Φ (Φ *invariant unter* g, Bezeichnung: $g \rhd \Phi$) $:\Longleftrightarrow \Phi^g \subset \Phi \overset{M \text{ endl.}}{\Longleftrightarrow} \Phi^g = \Phi \Longleftrightarrow: g$ *Automorphismus* v. Φ.
D.h. $g \rhd \Phi \iff \forall a_1, ..., a_n \in M : (a_1, ..., a_n) \in \Phi \iff (a_1^g, ..., a_n^g) \in \Phi$.
– Bezeichnung:

$$R_M := \{\Phi \mid \Phi \subset M^n,\ n = 1, 2, ...\} = \bigcup_{n=1}^{\infty} \mathfrak{P}(M^n)$$

ist *Menge aller endlich-stelligen Relationen auf* M. Setze

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

für $\Phi \in R_M$.
– Für $Q \subseteq R_M$:

$$\operatorname{Aut} Q := \bigcap_{\Phi \in Q} \operatorname{Aut}\Phi$$

Automorphismen von Q.
– Für $G \subseteq S_M$:

$$n\text{-Inv}\,(G, M) := n\text{-Inv}_M G := \{\Phi \subset M^n \mid \forall g \in G : \Phi^g = \Phi\},$$

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

Invarianten von G.

Einschub:

(1) Sei X Menge. $H : \mathfrak{P}(X) \to \mathfrak{P}(X)$ heißt *Hüllenoperator* $:\Longleftrightarrow$
  (i) H ist *monoton*, d.h. $H(A) \subset H(B)$ für alle $A \subset B \subset X$,
  (ii) H ist *extensiv*, d.h. $A \subset H(A) \forall A \subset X$

(iii) H ist *idempotent*, d.h. $H(H(A)) = H(A) \forall A \subset X$.

(2) Sei X Menge. $\mathcal{H} \subset \mathfrak{P}(X)$ ist *Hüllensystem* $:\Longleftrightarrow$

(i) $\forall \emptyset \neq \mathcal{H}_0 \subset \mathcal{H} : \bigcap \mathcal{H}_0 \in \mathcal{H}$,
(ii) $X \in \mathcal{H}$ (mit Konvention $X = \bigcap \emptyset$ kann man (ii) streichen).

– Ist $\mathcal{H}$ Hüllensystem auf X, dann ist H: $\mathfrak{P}(X) \to \mathfrak{P}(X)$ mit

$$H(A) := \bigcap \{H \in \mathcal{H} \mid A \subseteq H\}$$

Hüllenoperator auf X.

– Ist H Hüllenoperator auf X, dann ist

$$\mathcal{H} := \{H(A) \mid A \subseteq X\}$$

Hüllensystem auf X.

(3) Ist $R \subseteq X \times Y$ Relation zwischen Mengen X und Y, so heißt das Paar (φ, ψ) eine (die von R erzeugte) *Galoisverbindung*:

$$\varphi : \mathfrak{P}(X) \to \mathfrak{P}(Y), A \mapsto \{y \in Y \mid \forall x \in A : (x, y) \in R\},$$
$$\psi : \mathfrak{P}(Y) \to \mathfrak{P}(X), B \mapsto \{x \in X \mid \forall y \in B : (x, y) \in R\}.$$

Jede Relation induziert eine Galoisverbindung, also auch

$$\{(g, \Phi) \in S_M \times R_M \mid \Phi^g = \Phi\} \subseteq S_M \times R_M.$$

4.2 Fakt. Durch Aut und Inv ist eine Galoisverbindung gegeben:

$$\varphi = \operatorname{Aut} : \mathfrak{P}(R_M) \to \mathfrak{P}(S_M), Q \mapsto \operatorname{Aut}(Q),$$
$$\psi = \operatorname{Inv} : \mathfrak{P}(S_M) \to \mathfrak{P}(R_M), G \mapsto \operatorname{Inv}(G).$$

Insbesondere gelten die folgenden Eigenschaften: (für alle $G, G' \leq S_M$, $Q, Q' \subset R_M$):

(I) $G \subseteq G' \implies \operatorname{Inv} G \supseteq \operatorname{Inv} G'$.
(II) $Q \subseteq Q' \implies \operatorname{Aut} Q \supseteq \operatorname{Aut} Q'$.
(III) $G \subseteq \operatorname{Aut} \operatorname{Inv} G$.
(IV) $Q \subseteq \operatorname{Inv} \operatorname{Aut} Q$.
(V) $\operatorname{Aut} \operatorname{Inv} \operatorname{Aut} Q = \operatorname{Aut} Q$.
(VI) $\operatorname{Inv} \operatorname{Aut} \operatorname{Inv} G = \operatorname{Inv} G$.
(VII) $G \mapsto \operatorname{Aut} \operatorname{Inv} G$ ist Hüllenoperator auf S_M.
(VIII) $Q \mapsto \operatorname{Inv} \operatorname{Aut} Q$ ist Hüllenoperator auf R_M.
(IX) $G \subseteq \operatorname{Aut} Q \iff \operatorname{Inv} G \supseteq Q$.
(X) Aut und Inv induzieren Bijektionen zwischen den Mengen der *Galoishüllen*:

$$\begin{tikzcd} \{G \subseteq S_M \mid \operatorname{Aut} \operatorname{Inv} G\} \arrow[r, bend left, "\operatorname{Aut}"] & \{Q \subseteq R_M \mid \operatorname{Inv} \operatorname{Aut} Q\} \arrow[l, bend left, "\operatorname{Inv}"] \end{tikzcd}$$

(Es gilt: „Was links groß ist, wird rechts klein und umgekehrt.“)

Beweis. Übung! ■

4.3 Definition. Eine Relation der Form

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

heißt *n-Bahn* (*n-Orbit*) von $G \leq S_M$. Bezeichnung: $n\text{-Orb}\,(G, M)$:= *Menge aller n-Bahnen* von G=$\{\boldsymbol{a}^G \mid \boldsymbol{a} \in M^n\}$.

Bemerkung. Für $\Phi \subseteq M^n$:

$$\begin{aligned} \Phi \in n\text{-Orb}\,(G, M) &\iff \Phi \in 1\text{-Orb}\,(\tilde{G}, M^n), \\ \Phi \in n\text{-Inv}\,(G, M) &\iff \Phi \text{ ist invariante Menge von } (\tilde{G}, M^n), \\ &\ \text{vgl. 1.10c.} \end{aligned}$$

4.4 Satz. *Sei $G \leq S_M$. Dann gilt:*

(a) *Jede n-Bahn ist invariante Relation, d.h. $n\text{-Orb}\,(G, M) \subseteq n\text{-Inv}\,(G, M)$.*
(b) *Jede n-stellige invariante Relation von (G, M) ist (disjunkte) Vereinigung von n-Bahnen von (G, M).*
(c)

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

Beweis. Zu (a): Sei $\boldsymbol{a} \in M^n$. Z.z.: $\boldsymbol{a}^G$ ist invariant für jedes $g \in G$. Offenbar: $\left(\boldsymbol{a}^G\right)^g = \boldsymbol{a}^{Gg} = \boldsymbol{a}^G$ für alle $g \in G$.
Zu (b): Folgt aus 1.11(iv) und Bemerkung zu 4.3.
Zu (c): Folgt aus (b). (Hinweis: Nach (b) ist $f : \mathfrak{P}\,(n\text{-Orb}\,(G, M)) \to n\text{-Inv}\,(G, M), B \mapsto \bigcup B$ bijektiv).
■

Folgerung aus 1.4 (Satz von LAGRANGE für Permutationsgruppen):

4.5 Lemma. *Für $\Phi \in n\text{-Orb}\,(G, M)$ und $(a_1, ..., a_n) \in \Phi$ gilt:*

$$|\Phi| = [G : G_{a_1,...,a_n}].$$

Beweis. $\Phi = (a_1, ..., a_n)^{\tilde{G}} = \boldsymbol{a}^{\tilde{G}}$, $\tilde{G}_{\boldsymbol{a}} = G_{a_1,...,a_n}$ für Wirkung $(\tilde{G}, M^n)$. 1.14 $\implies |G| = |\tilde{G}| = |\tilde{G}_{\boldsymbol{a}}| \cdot \underbrace{|\boldsymbol{a}^{\tilde{G}}|}_{= \Phi} \implies$ Behauptung. ■

Galoisverbindung Aut-Inv (vgl. 4.2). Was sind die Galois-Hüllen?

Probleme:

– Welche (Permutations-)Gruppen sind Automorphismengruppen von geeigneten invarianten Relationen? (Z.B. Graphen)
– Welche Relationenmengen sind die Invariantenmengen für geeignete Gruppe $G \leq S_M$?

Antwort: Sätze von Marc KRASNER (hier nur für endliche Grundmenge M).

Vorbemerkung:

4.6 Satz. *Sei $Q \subseteq R_M$. Dann ist* $\operatorname{Aut} Q$ *eine Gruppe (Untergruppe von S_M).*

Beweis. Übung! ■

4.7 Theorem (1. Satz von KRASNER). *$M = \{a_1, ..., a_n\}$ endliche (!) Menge. Dann:*

(a) *Jede Permutationsgruppe $G \leq S_M$ ist Automorphismengruppe einer geeigneten Menge von Relationen. Es gilt:*

$$G = \operatorname{Aut}\operatorname{Inv} G = \operatorname{Aut}\operatorname{Orb} G = \operatorname{Aut} m\text{-}\operatorname{Orb} G = \operatorname{Aut} \boldsymbol{a}^G$$

für $\boldsymbol{a} := \{a_1, ..., a_m\}$.

(b) *Für Teilmenge $G \subseteq S_M$ gilt*

$$\underbrace{\langle G \rangle_{S_M}}_{\text{interne}} = \underbrace{\operatorname{Aut}\operatorname{Inv} G}_{\text{externe}}$$

Beschreibung der von G erzeugten Untergruppe

Beweis. Zu (a): Wir zeigen zunächst: $\operatorname{Aut}\Phi \subset G$ für $\Phi := \boldsymbol{a}^G$ (die von $\boldsymbol{a} = (a_1, ..., a_n)$) erzeugte m-Bahn). Sei $f \in \operatorname{Aut}\Phi$. Dann $\underbrace{(a_1, ..., a_m)^f}_{\substack{\| \\ (a_1^f, ..., a_m^f)}} \in \Phi = \boldsymbol{a}^G$,

ich wirke auf jedem Element $\longrightarrow$

also $\exists g \in G : (a_1, ..., a_m)^f = (a_1, ..., a_m)^g$, d.h. $f = g \in G$. Das heißt $\operatorname{Aut}\Phi \subset G$.
Rest:

$$\begin{aligned} G &\overset{4.2\ (\mathrm{III})}{\subseteq} \operatorname{Aut}\operatorname{Inv} G \overset{4.2\ (\mathrm{II})}{\subseteq} \operatorname{Aut}\operatorname{Orb} G \\ &\overset{4.2\ (\mathrm{II})}{\subseteq} \operatorname{Aut} m\text{-}\operatorname{Orb} G \overset{4.2\ (\mathrm{II})}{\subseteq} \operatorname{Aut}\Phi \subseteq G. \end{aligned}$$

Damit folgen alle Gleichungen in (a).

Zu (b): $G \subseteq \operatorname{Aut}\operatorname{Inv} G$ (vgl. 4.2 (III)) $\implies \langle G \rangle \subseteq \langle \operatorname{Aut}\operatorname{Inv} G \rangle \overset{4.6}{=} \operatorname{Aut}\operatorname{Inv} G \overset{4.2\ (\mathrm{V})}{\subseteq} \operatorname{Aut}\operatorname{Inv} \langle G \rangle \overset{(\mathrm{a})}{=} \langle G \rangle$.

■

Erinnerung: Prädikatenkalkül erster Stufe

Sei X Variablenmenge, $R_1, ..., R_n$ Prädikate, wobei R_i r_i-stellig ist mit $r_i \geq 1$ ($i = 1, ..., n$). Wir definieren die Menge $\mathcal{F} = \mathcal{F}(X, R_1, ..., R_n)$ der *Formeln des Prädikatenkalküls erster Stufe* über X und $R_1, ..., R_n$ als die kleinste Menge $\mathcal{F}$ mit folgenden Eigenschaften:

– Für je zwei $x, y \in X$ ist

freie Variablen

$$x = y \in \mathcal{F},\ \mathrm{FV}(x = y) := \{x, y\}$$

– Für jedes $i \in \{1, ..., n\}$ und $x_1, ..., x_n \in X$ ist

$$R_i(x_1, ..., x_n) \in \mathcal{F},\ \mathrm{FV}(R_i(x_1, ..., x_n)) := \{x_1, ..., x_n\}.$$

– Für $\varphi_1, \varphi_2 \in \mathcal{F}$ ist $\varphi_1 \wedge \varphi_2 \in \mathcal{F}$, $\varphi_1 \vee \varphi_2 \in \mathcal{F}$, $\neg\varphi_1 \in \mathcal{F}$, wobei $\mathrm{FV}(\varphi_1 \wedge \varphi_2) := \mathrm{FV}(\varphi_1 \vee \varphi_2) := \mathrm{FV}(\varphi_1) \cap \mathrm{FV}(\varphi_2)$ und $\mathrm{FV}(\neg\varphi_1) := \mathrm{FV}(\varphi_1)$.
– Für jedes $\varphi \in \mathcal{F}$ und $x \in \mathrm{FV}(\varphi)$ ist $\forall x, \varphi \in \mathcal{F}$, $\exists x, \varphi \in \mathcal{F}$, wobei $\mathrm{FV}(\forall x, \varphi) := \mathrm{FV}(\exists x, \varphi) := \mathrm{FV}(\varphi) \backslash \{x\}$.

4.8 Definition (Operationen auf Relationen). Jede Formel φ des Prädikatenkalküls 1. Stufe mit Relationensymbolen (Prädikaten) $R_1, ..., R_q$ (R_i sei r_i-stellig, $i = 1, ..., q$) und freien Variablen $x_1, ..., x_n$ definiert eine q-stellige Operation:

$$F_\varphi : \mathfrak{P}(M^{r_1}) \times ... \times \mathfrak{P}(M^{r_q}) \to \mathfrak{P}(M^n)$$

(genannt *logische Operation*), die q Relationen $\Phi_1 \subseteq M^{r_1}, ..., \Phi_q \subseteq M^{r_q}$ eine n-stellige Relation $F_\varphi(\Phi_1, ..., \Phi_q)$ zuordnet:

es gilt

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

4.9 Beispiele logischer Operationen. (i) $\varphi :\equiv \exists z : R_1(x, z) \wedge R_2(z, y)$,

$$\begin{aligned} F_\varphi(\Phi_1, \Phi_2) &= \{(x, y) \in M^2 \mid \exists z \in M : (x, z) \in \Phi_1 \wedge (z, y) \in \Phi_2\} \\ &=: \Phi_1 \circ \Phi_2\ (\textit{Relationenprodukt}). \end{aligned}$$

(ii) $\varphi_{\substack{1\\2}}(R_1, R_2; x, y) :\equiv R_1(x, y) \underset{\vee}{\wedge} R_2(x, y)$, $F_{\varphi_{\substack{1\\2}}} = \Phi_1 \underset{\cup}{\cap} \Phi_2$.

(iii) $\varphi(R_1; x_1, ..., x_n) :\equiv \neg R_1(x_1, ..., x_n)$,

$$F_\varphi(\Phi) = \{(a_1, ..., a_n) \in M^n \mid \neg((a_1, ..., a_n) \in \Phi)\} = M^n \backslash \Phi.$$

(iv) $\varphi(x_1, ..., x_4) :\equiv x_1 = x_2 \vee x_3 = x_4$, $F_\varphi = \{(a_1, a_2, a_3, a_4) \in M^4 \mid a_1 = a_2 \vee a_3 = a_4\}$.

(v) $\varphi(x_1, x_2) :\equiv x_1 = x_2$, $F_\varphi = \{(a_1, a_2) \in M^2 \mid a_1 = a_2\} =: \triangle_M$ (*Diagonalrelation*).

(vi) $\varphi(R_1; x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) :\equiv \exists x_i : R_1(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n)$,

$$\begin{aligned} F_\varphi(\Phi) =& \{(a_1, ..., a_{i-1}, a_{i+1}, ..., a_n) \in M^{n-1} \mid \exists a_i \in M : (a_1, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n) \in \Phi\} \\ =& \mathrm{pr}_{\underline{n} \backslash \{i\}}(\Phi) \end{aligned}$$

($\mathrm{pr}_K : M^n \to M^{|K|}$ für $K \subseteq \underline{n}$, d.h. Projektion von $\Phi \subseteq M^n$ auf die von i verschiedene Koordinaten).

4.10 Definition (Krasner-Algebren). Für $Q \subseteq R_M$ sei

$$\begin{aligned}[Q] :=& \{F_\varphi(\Phi_1, ..., \Phi_q) \mid n \in \mathbb{N} \backslash \{0\},\ q \in \mathbb{N},\ \Phi_1, ..., \Phi_q \in Q,\ \varphi \text{ Formel} \\ & \text{wie in 4.8 über } q \text{ Prädikaten und } n \text{ freien Variablen}\}\end{aligned}$$

der *Abschluss gegen logische Operationen.*

Bemerkung 1. Die Abbildung $\mathfrak{P}(R_M) \to \mathfrak{P}(R_M), Q \mapsto [Q]$ ist ein Hüllenoperator.

Bemerkung 2. Die gegen logische Operationen abgeschlossenen Mengen $Q \subset R_M$ (d.h. $[Q] = Q$) heißen auch *Krasner-Algebren.* Aus algebraischer Sicht sind dies genau die Unteralgebren von $\langle R_M, (R_\varphi)_{\varphi \text{ Formel}} \rangle$.

4.11 Satz. *Sei $G \subseteq S_M$. Dann ist $\operatorname{Inv} G$ eine Krasner-Algebra (d.h. $[\operatorname{Inv} G] = \operatorname{Inv} G$).*

Beweis. Sei $\Phi_1, ..., \Phi_q \in \operatorname{Inv} G$, d.h. $\Phi_i^g = \Phi_i$ für alle $g \in G$ und $i \in \{1, ..., q\}$. Sei φ Formel in q Prädikaten und n Variablen, $n \geq 1$. Dann gilt:

$$(F_\varphi(\Phi_1, ..., \Phi_q))^g = F_\varphi(\Phi_1^g, ..., \Phi_q^g)$$

für jedes $g \in S_M$. (Übungsaufgabe! Hinweis: Durch Induktion über den Aufbau von Formeln des Prädikatenkalküls erster Stufe.) Es folgt:

$$(F_\varphi(\Phi_1, ..., \Phi_q))^g = F_\varphi(\Phi_1^g, ..., \Phi_q^g) = F_\varphi(\Phi_1, ..., \Phi_q)$$

für alle $g \in G$. Also $F_\varphi(\Phi_1, ..., \Phi_q) \in \operatorname{Inv} G$. ■

4.12 Theorem (2. Satz von KRASNER). *Sei M endliche Menge. Dann gilt:*

(a) *Jede Krasner-Algebra $Q \subseteq R_M$ ist Invariantenmenge einer geeigneten Menge von Permutationen. Es gilt:*

$$Q = \operatorname{Inv} \operatorname{Aut} Q.$$

(b) *Für jede beliebige Teilmenge $Q \subseteq R_M$ gilt*

$$\underbrace{[Q]}_{\text{interne}} = \underbrace{\operatorname{Inv} \operatorname{Aut} Q}_{\text{externe}}$$

Beschreibung der von Q
erzeugten Krasner-Algebra

Beweis. (b) folgt aus (a) und 4.11:

$$\begin{aligned} Q \overset{4.2\ (\mathrm{IV})}{\subseteq} \operatorname{Inv} \operatorname{Aut} Q \implies [Q] &\subseteq [\operatorname{Inv} \operatorname{Aut} Q] \overset{4.11}{=} \operatorname{Inv} \operatorname{Aut} Q \\ &\subseteq \operatorname{Inv} \operatorname{Aut} [Q] \overset{(a)}{=} [Q]. \end{aligned}$$

Zu (a): Sei $M = \{a_1, ..., a_m\}$, $\boldsymbol{a} := \{a_1, ..., a_m\}$, $G := \operatorname{Aut} Q$, $[Q] = Q \subseteq R_M$.

1. Schritt: $\boldsymbol{a}^G \in Q$ (Lemma 4.13),
2. Schritt: $\operatorname{Inv} G \subseteq [\boldsymbol{a}^G]$ (Lemma 4.14).

Dann folgt:

$$Q \overset{4.2\,(\mathrm{IV})}{\subseteq} \operatorname{Inv}\operatorname{Aut} Q \implies [Q] \subseteq \operatorname{Inv}\operatorname{Aut} Q = \operatorname{Inv} G \overset{2.\,\mathrm{S.}}{\subseteq} [\boldsymbol{a}^G] \overset{1.\,\mathrm{S.}}{\subseteq} [Q] = Q.$$

■

4.13 Lemma. *Sei* $[Q] = Q \subseteq R_M$*,* $G = \operatorname{Aut} Q$*,* $M = \{a_1, ..., a_m\}$*,* $\boldsymbol{a} = (a_1, ..., a_m)$*. Dann gilt* $\boldsymbol{a}^G \in Q$*.*

Beweis. Definiere

$$\gamma := \bigcap \{\varrho \in Q \mid \boldsymbol{a} \in \varrho\}. \qquad (*)$$

Nach 4.9 (ii) ist $Q = [Q]$ gegen (endliche) Durchschnitte angeschlossen. Da M endlich ist, ist auch $Q \cap M^n$ endlich $\implies \gamma$ ist endlich. Es folgt: $\gamma \in Q$.

Plan: Wir zeigen $\boldsymbol{a}^G = \gamma$.

Beobachtung $(**)$: Alle m-Tupel aus γ bestehen aus paarweise verschiedenen Komponenten, denn

$$\boldsymbol{a} \in F_{\varphi_0} = \{(b_1, ..., b_m) \in M^m \mid \forall i, j \in \{1, ..., m\}, i \neq j, b_i \neq b_j\}$$

für $\varphi_0(x_1, ..., x_m) :\equiv \bigwedge_{i \neq j} \neg(x_i = x_j)$. Nun $\gamma \subseteq F_{\varphi_0}$ wegen $(*)$ und $F_{\varphi_0} \in [Q] = Q$.

– $\boldsymbol{a} \in \gamma \implies \boldsymbol{a}^G \subseteq \gamma^G = \gamma$ da $\gamma \in Q \subseteq \operatorname{Inv}\operatorname{Aut} Q = \operatorname{Inv} G$. Also $\boldsymbol{a}^G \subseteq \gamma$.
– Noch zu zeigen: $\gamma \subseteq \boldsymbol{a}^G$. Indirekt: Angenommen, es gibt $\boldsymbol{r} = (r_1, ..., r_m) \in \gamma$ mit $\boldsymbol{r} \notin \boldsymbol{a}^G$. Dann ist die Funktion (Permutation) $f : M \to M$, $a_i \mapsto r_i$ *kein* Element von G (wegen $(**)$, es gilt $\boldsymbol{a}^f = \boldsymbol{r}$). Also $f \notin \operatorname{Aut} Q$, d.h. $\exists \varrho_0 \in Q : f \notin \operatorname{Aut} \varrho_0$, d.h. $\exists \boldsymbol{s} \in \varrho_0 : \boldsymbol{s}^f \notin \varrho_0$. Sei ϱ_0 t-stellig. Dann gibt es $j_1, ..., j_t \in \{1, ..., m\}$ mit $\boldsymbol{s} = (a_{j_1}, ..., a_{j_t})$. Betrachte die Formel

$$\varphi(R, S; x_1, ..., x_m) := R(x_1, ..., x_m) \wedge S(x_{j_1}, ..., x_{j_t})$$

und weiter

$$\sigma := F_\varphi(\gamma, \varrho_0) = \{(x_1, ..., x_m) \in M^m \mid (x_1, ..., x_m) \in \gamma \wedge (x_{j_1}, ..., x_{j_t}) \in \varrho_0\}.$$

Also $\sigma \in [Q] = Q$ und $\sigma \subseteq \gamma$. Wegen $\boldsymbol{a} \in \gamma$ und $\boldsymbol{s} \in \varrho$ folgt $\boldsymbol{a} \in \sigma$. Aber $\boldsymbol{r} = \boldsymbol{a}^f \notin \sigma$, weil $(a_{j_1}, ..., a^f_{j_k})^f = \boldsymbol{s}^f \notin \varrho$. Das heißt: $\boldsymbol{r} \notin \gamma \backslash \sigma \implies \gamma \nsubseteq \sigma$. Anderseits: $\boldsymbol{a} \in \sigma \in Q \overset{(*)}{\implies} \gamma \subseteq \sigma \implies$ Widerspruch. Also $\boldsymbol{a}^G = \gamma \in Q$. ■

4.14 Lemma. *Sei* $M = \{a_1, ..., a_m\}$*,* $[Q] = Q \subseteq R_M$*,* $G = \operatorname{Aut} Q$*,* $\boldsymbol{a} = (a_1, ..., a_m)$*. Dann gilt:*

$$\operatorname{Inv} G \subseteq [\boldsymbol{a}^G].$$

(Bemerkung: Es gilt sogar die Gleichheit, weil $[\operatorname{Inv} G] = \operatorname{Inv} G$*.)*

Beweis. Da $Q = [Q]$ abgeschlossen gegen Vereinigungen (4.9 (ii)) und jede invariante Relation Vereinigung von Bahnen ist (4.4 (b)), ist es ausreichend Folgendes zu zeigen:

$$n\text{-}\mathrm{Orb}\, G \subseteq [\boldsymbol{a}^G] \forall n \in \mathbb{N}\backslash\{0\}.$$

(Dann folgt: $\mathrm{Inv}\, G = [\bigcup_{n=1}^{\infty} n\text{-}\mathrm{Orb}\, G] \subseteq [\boldsymbol{a}^G] \overset{4.13}{\subseteq} [Q] \subseteq [\mathrm{Inv}\, G] \overset{4.11}{=} \mathrm{Inv}\, G$.)

Also sei $\Phi \in n\text{-}\mathrm{Orb}\, G$, d.h. $\Phi = \boldsymbol{b}^G$ für ein $\boldsymbol{b} = (b_1, ..., b_n) \in M^n$. Dann gibt es eine (eindeutig bestimmte) Abbildung $\pi : \{1, ..., n\} \to \{1, ..., m\}$, sodass $b_i = a_{\pi(i)}$ für alle $i \in \{1, ..., n\}$. (*Genauer*: betrachte die Abbildungen $\boldsymbol{a} : \{1, ..., m\} \to M$, $\boldsymbol{b} : \{1, ..., n\} \to M$ und definiere π durch $\pi(i) := \boldsymbol{a}^{-1}(\boldsymbol{b}(i))$ $(i \in \{1, ..., n\})$.) Definiere nun

$$\varphi(R; x_1, ..., x_n) :\equiv \exists z_1, ..., z_m : R(z_1, ..., z_m) \bigwedge_{j=1}^{n} x_i = z_{\pi(i)}.$$

Dann:

$$\begin{aligned}
F_\phi(\boldsymbol{a}^G) =& \{(y_1, ..., y_n) \in M^n \mid \exists (c_1, ..., c_m) \in \boldsymbol{a}^G : \forall i \in \{1, ..., n\} : y_i = c_{\pi(i)}\} \\
=& \{(y_1, ..., y_n) \in M^n \mid \exists g \in G \forall i \in \{1, ..., n\} : y_i = a_\pi^g\} \\
=& \{(y_1, ..., y_n) \in M^n \mid \exists g \in G \forall i \in \{1, ..., n\} : y_i = b_i^g\} \\
=& \{(b_1^g, ..., b_n^g) \in M^n \mid g \in G\} = \boldsymbol{b}^G,
\end{aligned}$$

d.h. $\Phi = \boldsymbol{b}^G = F_\varphi(\boldsymbol{a}^G) \in [\boldsymbol{a}^G]$. ■

5 k-Abgeschlossene Permutationsgruppen, primitive Gruppen, Automorphismengruppen von Graphen

1. Satz von KRASNER: $G = \operatorname{Aut}\operatorname{Inv} G$ für $G \leq S_M$.

Frage: Wann gilt $G = \operatorname{Aut} k\text{-Inv}$ für ein vorgegebenes k?

5.1 Definition. Sei $G \leq S_M$, $k \in \mathbb{N}\backslash\{0\}$. Die Permutationsgruppe

$$G^{(k)} := \operatorname{Aut} k\text{-Inv}\, G$$

heißt *k-Abschluss* von G. G ist *k-abgeschlossen* $:\Longleftrightarrow G^{(k)} = G$.

Zwei Gruppen $G_1, G_2 \leq S_M$ heißen *k-äquivalent* (Bez. $G_1 \approx_k G_2$), wenn $k\text{-Inv}\, G_1 = k\text{-Inv}\, G_2$.

5.2 Satz. *Es gilt:*

(i) $(\operatorname{Aut}, k\text{-Inv})$ *bildet eine Galoisverbindung (induziert von der Relation*

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

wobei $R_M^{(k)} := \mathfrak{P}\left(M^k\right)$, *vgl. 4.2).*

(ii) $G_1 \approx_k G_2 \iff G_1^{(k)} = G_2^{(k)}$.

(iii) $G \approx_k G^{(k)}$. *Unter allen zu G äquivalenten Gruppen ist $G^{(k)}$ die größte* ($G \approx_k H \implies H \subseteq H^{(k)} = G^{(k)}$).

(iv) *Die Abbildung $G \mapsto G^{(k)}$ ist ein Hüllenoperator auf* $\mathfrak{P}(S_M)$.

(v) $G^{(k)} = \operatorname{Aut} k\text{-Inv}\, G = \operatorname{Aut} k\text{-Orb}\, G$.

Beweis. Übungsaufgabe! ∎

5.3 Satz. *Sei $G \leq S_M$.*

(a) *$G^{(k)}$ hat die „k-Interpolationseigenschaft“, d.h. für alle $h \in S_M$ gilt:*

$$h \in G^{(k)} \iff \forall a_1, ..., a_k \in M \exists g \in G : (a_1, ..., a_k)^h = (a_1, ..., a_k)^g \ (\text{d.h. } \boldsymbol{a}^h = \boldsymbol{a}^g).$$

(b) *k-Abschlusskriterium (hinreichend):*

$$(\exists a_1, ..., a_{k-1} \in M : G_{a_1, ..., a_{k-1}} = \{e\}) \implies G = G^{(k)}.$$

(c) *Charakterisierung:*

$$\exists Q \subseteq R_M^{(k)} : G = \operatorname{Aut} Q \iff G = G^{(k)}.$$

Beweis. Zu (a):

$$\begin{aligned} h \in G^{(k)} &\overset{5.2\,(v)}{\iff} h \in \operatorname{Aut} k\text{-Orb}\, G \\ &\iff \forall \boldsymbol{a} \in M^k : \left(\boldsymbol{a}^G\right)^h = \boldsymbol{a}^G \\ &\iff \forall \boldsymbol{a} \in M^k : \boldsymbol{a}^h \in \boldsymbol{a}^G \end{aligned}$$

(„$\Longleftarrow$“ gilt auch, denn: $\boldsymbol{b} \in \boldsymbol{a}^G \implies \exists g \in G : \boldsymbol{b} = \boldsymbol{a}^g$. Es folgt $\boldsymbol{b}^h \in \boldsymbol{b}^G = \boldsymbol{a}^G$.)

$$\Longleftrightarrow \forall a_1, ..., a_k \in M \exists g \in G : \boldsymbol{a}^h = \boldsymbol{a}^g.$$

Zu (b): Zu zeigen: $h \in G^{(k)} \implies h \in G$. Sei $h \in G^{(k)}$. Nach (a) gilt: $\forall b \in M \exists g_b \in G : (a_1, ..., a_{k-1}, b)^h = (a_1, ..., a_{k-1}, b)^{g_b}$. Sind $b, b' \in M$, dann ist $g_b g_{b'}^{-1} \in G_{a_1,...,a_{k-1}} = \{e\}$ und somit $g_b = g_{b'}$. Definiere $g := g_b$ (für irgendein $b \in M$). Nun ist $\forall c \in M : c^h = c^{g_c} = c^{g_b} = c^g \implies h = g \in G$.

Zu (c): „$\Longrightarrow$“ Sei $Q \subseteq R_M^{(k)}$ mit $G = \operatorname{Aut} Q$. Dann folgt:

$$Q \subseteq k\text{-Inv}\, G$$

$$G = \operatorname{Aut} Q \overset{4.2\ (\mathrm{II})}{\supseteq} \operatorname{Aut} k\text{-Inv}\, G = G^{(k)} \supseteq G.$$

„$\Longleftarrow$“ Setze einfach $Q := k\text{-Inv}\, G$. Dann klar.

■

Ab jetzt betrachten wir den (besonders interessanten) Spezialfall $k = 2$:

5.4 Definition. $G \leq S_M$ heißt

$$\textit{semi-regulär} \;:\Longleftrightarrow \forall a \in M : G_a = \{e\},$$
$$\textit{regulär} \;:\Longleftrightarrow G \text{ ist semi-regulär und transitiv (vgl. 1.10 (d)).}$$

Bemerkung: G regulär $\Longleftrightarrow$ G transitiv und $\exists a \in M : G_a = \{e\}$.

5.5 Satz. *Sei $G \leq S_M$ semi-regulär. Dann:*

(a) *G ist 2-abgeschlossen ($G^{(2)} = G$).*
(b) *Für jede Permutation $g \in G$ gilt: Alle Zyklen der vollständigen (d.h. der nicht-verkürzten) Zyklendarstellung von g haben die gleiche Länge.*
(c) $\forall a \in M : |a^G| = |G|$.
(d) *Ist G regulär so gilt $|G| = |M|$.*

Beweis. (a) folgt aus 5.3 (b).

Zu (b): Sei $g \in G$. Hätte g Zyklen der Länge $l_1 < l_2$, so wäre $g^{l_1} \neq e$ und g^{l_1} besäße Fixpunkte (nämlich alle Elemente aus Zyklen der Länge l_1). Widerspruch, da $G_a = \{e\}$ für alle $a \in M$.
Zu (c): $|G| \overset{1.14}{=} |G_a||a^G| = |a^G|$.
Zu (d): G transitiv, d.h. $\exists a \in M : a^G = M$. Nach (c) ist $|M| = |a^G| = |G|$.

■

5.6 Beispiele. (i) $\{e, (1\ 2)(3\ 4)\} \leq S_4$ semi-regulär, aber nicht regulär, da nicht transitiv.

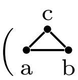
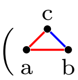
(ii) Die rechtsreguläre Darstellung $G^* \leq S_G$ jeder Gruppe G ist regulär (vgl. 2.5, Satz von CAYLEY). Für $g \in G : g^* : G \to G, x \mapsto xg$.

5.7 Definition. Ein *gerichteter Graph* ist ein Paar $\Gamma = (V, E)$, wobei V Menge (endlich)—Elemente heißen *Knoten*, $E \subseteq V \times V$ Relation—Elemente heißen *Kanten.*

- $(a, b) \in E$ heißt *gerichtete Kante* von a nach b bzw. *Schlinge* falls $a = b$.
- $(a, b) \in E$ heißt *ungerichtete Kante* von a nach b, falls $\{(a, b), (b, a)\} \subseteq E$.
- *Automorphismenmenge von* Γ:

$$\operatorname{Aut}\Gamma := \operatorname{Aut}_V E \text{ (vgl. 4.1, wobei } E \text{ binäre Relation).}$$

- Ein *gefärbter Graph* ist ein Paar (Γ, γ), wobei:
  - $\Gamma = (V, E)$ Graph,
  - $\gamma : E \to C$ Abbildung in eine Menge C (γ ist *Färbungsfunktion* und C *Menge der Farben*).
- $(a, b) \in E$ heißt *gerichtete Kante von a nach b mit Farbe $r \in C$*, wenn $\gamma((a, b)) = r$. (Häufig wird γ als surjektiv vorausgesetzt.)
- ein *Automorphismus* von (Γ, γ) ist eine Permutation $f : V \to V$, so dass:
  - $f \in \operatorname{Aut}\Gamma$,
  - für alle $(a, b) \in E$ gilt $\gamma((a, b)) = \gamma((a^f, b^f))$. (Kanten werden auf Kanten gleicher Farbe abgebildet.)
- *Automorphismengruppe von* (Γ, γ): $\operatorname{Aut}(\Gamma, \gamma)$ (ist tatsächlich eine Gruppe—Übungsaufgabe!).

Aut () $= S_3$ aber Aut () $\neq S_3$.

5.8 Satz. *Sei (Γ, γ) gefärbter Graph. Für jedes $r \in C$ definiere $\Gamma_r := (V, E_r)$ mit $E_r := \{(a, b) \in E \mid \gamma(a, b) = r\} = \gamma^{-1}(r)$. Dann:*

(a) $\operatorname{Aut}(\Gamma, \gamma) = \bigcap_{r \in C} \operatorname{Aut}(\Gamma_r)$.

(b) *Sei M Menge. Genau dann ist $G \leq S_M$ 2-abgeschlossen, wenn G die Automorphismengruppe eines gefärbten Graphen mit Knotenmenge M ist.*

Beweis. Zu (a): Behauptung folgt aus Definitionen (Übung!).

Zu (b): „$\Longleftarrow$“ Sei $G = \operatorname{Aut}(\Gamma, \gamma)$. Dann $G \overset{(a)}{=} \bigcap_{r \in C} \operatorname{Aut}(E_r) = \operatorname{Aut}\{E_r \mid r \in C\} =: Q \subseteq R_M^{(2)}$ ist 2-abgeschlossen nach 5.3(c).

„$\Longrightarrow$“ Annahme: G ist 2-abgeschlossen. Dann $G = G^{(2)} \overset{5.2(v)}{=} \operatorname{Aut} 2\text{-}\operatorname{Orb} G$. Sei $2\text{-}\operatorname{Orb} G = \{\Phi_1, ..., \Phi_q\}$. Definiere $C := \{1, ..., q\}$, $E_r := \Phi_r$, $\Gamma_r := (M, E_r)$ $(r \in \{1, ..., q\})$. Beachte: $E_r \cap E_s = \emptyset$ oder E_r für alle $r, s \in \{1, ..., q\}$ und $M \times M = \bigcup_{r=1}^{q} E_r$. Setze $\gamma : M \times M \to \{1, ..., q\}$ mit $\gamma(a, b) = r \iff (a, b) \in \Phi_r$. Dann gilt $G = \operatorname{Aut} 2\text{-}\operatorname{Orb} G = \bigcap_{r \in C} \operatorname{Aut}\Phi_r = \bigcap_{r \in C} \operatorname{Aut}\Gamma_r \overset{(a)}{=} \operatorname{Aut}(\Gamma, \gamma)$. ■

5.9 Definition. Sei G Gruppe, $U, V \leq G$ Untergruppen. Für $g \in G$ heißt

$$UgV := \{ugv \mid u \in U, v \in V\}$$

Doppelnebenklasse von g (bzgl. U und V).

$$U\backslash G/V := \{UgV \mid g \in G\}$$

ist *Menge der Doppelnebenklassen.*

Es gilt: $U\backslash G/V$ ist Partition von G.

Beweis. Offenbar $G = \bigcup U\backslash G/V$. Zwei Elemente von $U\backslash G/V$ sind entweder disjunkt oder gleich, denn:

$$\begin{aligned} h \in UgV \cap Ug'V &\iff \exists u, u' \in U,\ v, v' \in V : ugv = u'g'v' \\ &\implies g = u^{-1}u'g'v'v^{-1} \\ &\implies UgV = \underbrace{Uu^{-1}u'}_{=U}g'\underbrace{v'v^{-1}V}_{=V} = Ug'V. \end{aligned}$$ ∎

5.10 Lemma. $G \leq S_M, x \in M$. *Dann:*

(a) *Sei G transitiv. Dann enthält jede 2-Bahn von G ein Element der Form (x, x^g) für ein geeignetes $g \in G$.*

(b) $(x, x^g)^G = (x, x^{g'})^G \iff G_x g G_x = G_x g' G_x$ *für alle $g, g' \in G$.*

Beweis. Zu (a): Sei $(a, b) \in M^2$. Da G transitiv ist, existieren $g \in G$ mit $a^g = x$ und $g' \in G$ mit $x^{g'} = b^g$. Es folgt $(x, x^{g'}) = (a^g, b^g) \in (a, b)^G$.

Zu (b): $G_x g G_x = G_x g' G_x \iff g' \in G_x g G_x \iff \exists h_1, h_2 \in G_x : g' = h_1 g h_2 \boxed{\iff} (x, x^{g'}) \in (x, x^g)^G \iff (x, x^{g'})^G = (x, x^g)^G$.

$\boxed{\implies}$

$(x, x^{g'}) = (x, x^{h_1 g h_2}) \overset{h_1 \in G_x}{=} (x, x^{g h_2}) \overset{h_2 \in G_x}{=} (x^{h_2}, x^{g h_2}) = (x, x^g)^{h_2} = (x, x^g)^G$.

$\boxed{\impliedby}$ Sei $(x, x^{g'}) \in (x, x^g)^G \implies \exists h_2 \in G : (x, x^{g'}) = (x, x^g)^{h_2} = (x^{h_2}, x^{g h_2}) \implies h_2 \in G_x$. Definiere $h_1 := g' h_2^{-1} g^{-1}$. Dann $x^{h_1} = x^{g' h_2^{-1} g^{-1}} = x^{g h_2 h_2^{-1} g^{-1}} = x \implies x \in G_x$. Außerdem ist $h_1 g h_2 = g'$. ∎

5.11 Satz. *Sei $G \leq S_M$ transitiv, $x \in M$. Dann:*

(a) 2-*Bahnen* $\overset{1:1}{\longleftrightarrow}$ *Doppelnebenklassen. Die Abbildung*

$$\alpha : 2\text{-Orb}\,(G, M) \to G_x\backslash G/G_x,\ (x, x^g)^G \mapsto G_x g G_x$$

ist eine Bijektion.

(b) *Elemente von 2-Bahn* $\overset{1:1}{\longleftrightarrow}$ *Rechtsnebeklassen nach „Doppelstabilisator". Die Abbildung*

$$\alpha' : (x, x^g)^G \to G \backslash G_{x,x^g}, \ (x^h, x^{gh}) \mapsto G_{x,x^{gh}}$$

ist eine Bijektion (für jedes $g \in G$). Bemerkung: $G_{x,x^g} = G_x \cap G_{x^g} \overset{1.11(\text{ii})}{=} G_x \cap g^{-1}G_x g$.

(c) *Wirkung φ von G auf 2-Bahnen $\cong$ Wirkung φ' von G auf Rechtsnebenklassen. Die Wirkung von G auf 2-Bahnen*

$$\varphi : (x, x^g)^G \times G \to (x, x^g)^G, ((x^h, x^{gh}), f) \mapsto (x^{hf}, x^{ghf})$$

und die Wirkung von G auf den zugehörigen Nebenklassen (gemäß (b)*)*

$$\varphi' : G/G_{x,x^g} \times G \to G/G_{x,x^g}, \ (G_{x,x^{gh}}, f) \mapsto G_{x,x^g}hf$$

sind ähnlich (für jedes $g \in G$).

Beweis. Zu (a): α ist auf allen 2-Bahnen definiert wegen 5.10(a). Außerdem ist α wohldefiniert und injektiv nach 5.10(b). Surjektivität: Für jedes $g \in G$ ist $(x, x^g)^G \in 2\text{-Orb}\,(G, M)$ und $\alpha((x, x^g)^G) = G_x g G_x$.

Zu (b): Behauptung folgt aus 1.13 (Abbildung $a^G \to {}^G/_{G_a}$, $a^h \mapsto G_a h$ ist injektiv) angewendet auf induzierte Wirkung (G, M^2) (dann $G_a = G_{x,x^g}$ für $a = (x, x^g) \in M^2$).

Zu (c): φ ist Wirkung wegen 2.8(c), φ' ist Wirkung wegen 2.7(3). Ähnlichkeit von φ und φ' (vgl. 1.16):

$$\begin{tikzcd}
(x, x^g)^G \arrow[rrr, "\alpha'"'] \arrow[ddd, "f"'] & & & {}^G/_{G_{x,x^g}} \arrow[ddd, "f"] \\
& (x^h, x^{gh}) \arrow[r, mapsto] \arrow[d, mapsto] & (G_{x,x^g}h) \arrow[d, mapsto] & \\
& (x^{hf}, x^{ghf}) \arrow[r, mapsto] & G_{x,x^g}hf & \\
(x, x^g)^G \arrow[rrr, "\alpha'"] & & & {}^G/_{G_{x,x^g}}
\end{tikzcd}$$

(mit $\varphi = \text{id}$ in 1.16) kommutiert für jedes $f \in G$. ■

5.12 Satz. *$G \leq S_M$ transitiv, $x \in M$. Dann:*

(a) *Die Abbildung $\kappa : 2\text{-Orb}\,(G, M) \to 1\text{-Orb}\,(G_x, M)$, $(x, x^g)^G \mapsto (x^g)^{G_x}$ ist bijektiv. Dabei gilt:*

$$\kappa(\Phi) = \{y \in M \mid (x, y) \in \Phi\} \ (\Phi \in 2\text{-Orb}\,(G, M)),$$
$$\kappa^{-1}(B) = \{(x^h, y^h) \mid y \in B, h \in G\} \ (B \in 1\text{-Orb}\,(G_x, M)).$$

Speziell für $\triangle_M \in 2\text{-Orb}\,(G, M)$: $\kappa(\triangle_M) = \{x\}$.

(b) *Ist T Transversale (Repräsentantensystem) der Doppelnebenklassen $G_x\backslash G/G_x$, dann ist $\tilde{T} := x^T = \{x^g \mid g \in T\}$ Transversale für die Zerlegung* 1-Orb(G_x, M) *(und $\hat{T} = \{(x, x^g) \mid g \in T\}$ Transversale für* 2-Orb(G, M)*).*

Beweis. Zu (a): κ ist wohldefiniert und injektiv: $(x, x^g)^G = (x, x^{g'})^G \iff \exists h \in G : (x, x^g) = (x, x^g)^h \iff \exists h \in G_x : x^g = x^{g'h} \iff x^g \in (x^{g'})^{G_x} \iff (x^g)^{G_x} = (x^{g'})^{G_x}$. Surjektivität: für jedes $B \in$ 1-Orb(G_x, M) gibt es $y \in M$ mit $B = y^{G_x}$. Da G transitiv: $\exists g \in G : y = x^g$. Also $B = (x^g)^{G_x}$. Dann $(x, x^g)^G \in$ 2-Orb(G, M) und $\kappa((x, x^g)^G) = (x^g)^{G_x} = B$. Restliche Gleichungen: Übung!

Zu (b): T Transversale von $G_x\backslash G/G_x \overset{5.11(a)}{\Longrightarrow} \hat{T}$ Transversale von 2-Orb$(G, M) \overset{(a)}{\Longrightarrow} \tilde{T}$ Transversale von 1-Orb(G_x, M). ∎

Wichtiges Prinzip zur Reduktion von Problemen: Das *Homomorphieprinzip*:

– Vergröberung der betrachteten Struktur durch Homomorphismus,
– Problem in grober Struktur behandeln.

5.13 Definition (Homomorphismen und Wirkungen). (Speziell Permutationsgruppen, Verallg. von 1.16) Seien (G, M), (H, N) Gruppenwirkungen. Abbildungspaar (φ, f) mit $\varphi : G \to H$ Gruppenhomomorphismus, $f : M \to N$ heißt *Homomorphismus* von (G, M) nach (H, N), falls folgende Verträglichkeitsbedingung erfüllt ist:

$$\forall m \in M \forall g \in G : f(m^g) = f(m)^{\varphi(g)}, \tag{$*$}$$

d.h. das Diagramm

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

kommutiert (für jedes $g \in G$).

Häufiger Spezialfall: $G = H$, $\varphi : G \to G$ ist identische Abbildung. Dann meistens f surjektiv und oBdA $f : M \to {}^M/_\Theta$ für ÄR Θ auf M.

5.14 Lemma. *Sei $G \leq S_M, \Theta \in$* Äq(M)*. Dann ist durch*

$${}^M/_\Theta \times G \to {}^M/_\Theta, \ ([m]_\Theta, g) \mapsto [m^g]_\Theta$$

genau dann eine Gruppenwirkung von G auf ${}^M/_\Theta$ gegeben, wenn $\Theta \in$ 2-Inv(G, M)*. In diesem Fall ist (φ, f) mit $\varphi = \mathrm{id} : G \to G$ und $f : M \to {}^M/_\Theta, m \mapsto [m]_\Theta$ ein Homomorphismus von (G, M) nach $(G, {}^M/_\Theta)$.*

Beweis. Die Abbildung $([m]_\Theta, g) \mapsto [m^g]_\Theta$ ist genau dann wohldefiniert, wenn $[m]_\Theta = [m']_\Theta \implies [m^g]_\Theta = [m'^g]_\Theta$, d.h. $(m, m') \in \Theta \implies (m^g, m'^g) \in \Theta$ (d.h. Θ ist invariant für jedes $g \in G$). Die Eigenschaften 2.2(i),(ii) (Gruppenwirkung) folgen dann aus den Definitionen (Übung!). Ebenso 5.13($*$): $[m^g]_\Theta = [m]_\Theta^g$ (Übung!). ∎

5.15 Definition. Sei $G \leq S_M$.

(1) $B \subseteq M$ heißt *Block* von G, falls gilt:

$$\forall g \in G : B^g = B \text{ oder } B^g \cap B = \emptyset,$$

M und $\{a\}$ $(a \in M)$ heißen *triviale Blöcke.*

(2) Eine Partition $\mathcal{B}$ von M heißt *verträgliches Blocksystem*, wenn $\forall g \in G \forall B \in \mathcal{B} : B^g \in \mathcal{B}$.

(3) G heißt *imprimitiv*, falls G einen nichttrivialen Block besitzt. Anderenfalls heißt G *primitiv.*

Bemerkungen:

(a) *$G \leq S_M$ primitiv $\implies$ G ist transitiv oder $G = \{e\}$ (da jeder Orbit von (G, M) ein Block ist).*

(b) *Für $\Theta \in \text{Äq}(M)$ gilt:*

$$\Theta \in 2\text{-Inv}\,(G, M) \iff {}^{M}\!/_{\Theta} \textit{ ist verträgliches Blocksystem (Übung!).}$$

5.16 Folgerung. *Sei $G \leq S_M$. Die folgenden Aussagen sind äquivalent:*

(a) *G ist imprimitiv.*

(b) *Es gibt eine nichttriviale Äquivalenzrelation $\Theta \in \text{Äq}(M) \cap \text{Inv}\,(G, M)$ (d.h. $\triangle_M \neq \Theta \neq M^2$).*

(c) *Es gibt ein nichttriviales verträgliches Blocksystem für G.*

Beweis. (a) $\Longrightarrow$ (c): Sei $B \subseteq M$ nichttrivialer Block. Dann ist

$$\mathcal{B} := \{B^g \mid g \in G\} \cup \{M \setminus \bigcup_{g \in G} B^g\}$$

ein nichttriviales verträgliches Blocksystem. Für $g, h \in G$:

$$B^g \cap B^h \neq \emptyset \iff B^{gh^{-1}} \cap B \neq \emptyset \overset{B \text{ Block}}{\iff} B^{gh^{-1}} = B \iff B^g = B^h.$$

Es folgt: $\mathcal{B}$ ist Partition. Verträglichkeit:

$$B^{gh} \cap B^g \neq \emptyset \overset{(*)}{\iff} B^{gh} = B^g.$$

(c) $\Longrightarrow$ (b): Sei $\mathcal{B}$ nichttriviales Blocksystem, verträglich. Dann ist

$$\Theta := \{(x, y) \in M^2 \mid \exists B \in \mathcal{B} : \{x, y\} \subseteq B\}.$$

Außerdem:

$$\mathcal{B} \text{ verträglich} \iff {}^{M}\!/_{\Theta} \text{ verträglich} \iff \Theta \text{ invariant.}$$

Da $\mathcal{B}$ nichttrivial: $\triangle_M \neq \Theta \neq M^2$.

(b) $\Longrightarrow$ (a): $\Theta \in \text{Äq}(M)\backslash\{\triangle_M, M^2\}$ invariant. Dann gibt es $x \in M$ mit $\{x\} \neq [x]_\Theta \neq M$.
Da Θ invariant, ist $B := [x]_\Theta$ Block. Auch: $\{x\} \subsetneqq B \subsetneqq M \implies B$ nichttrivial. ■

5.17 Definition (Mengenstabilisatoren). Sei $G \leq S_M$, $B \subseteq M$. $G_{[B]} := \{g \in G \mid B^g = B\} = G \cap \text{Aut}_M B$ heißt *Mengenstabilisator* von B in G.

$G_{[B]}$ (einfacher G_B) bildet eine Gruppe (Übung!) und durch $B \times G_B \to B$, $(b, g) \mapsto b^g$ ist Gruppenwirkung (G_B, B) auf B gegeben (Übung!).

5.18 Satz. *Sei (G, M) Gruppenwirkung und $\Theta \in \text{Äq}(M)$ invariant (d.h. $\mathcal{B} := {}^M/_\Theta$ ist verträgliches Blocksystem) (Bemerkung: Dann ist (id_G, f) Homomorphismus von (G, M) nach $(G, {}^M/_\Theta)$ mit $f : M \to {}^M/_\Theta$, $x \mapsto [x]_\Theta$). Sei $\mathcal{T}$ Transversale der 1-Bahnen von $(G, {}^M/_\Theta)$ und, für jedes $B \in \mathcal{T}$, $\mathcal{T}_B$ Transversale der 1-Bahnen von (G_B, B). Dann ist $\bigcup_{B \in \mathcal{T}} \mathcal{T}_B$ Transversale der 1-Bahnen von (G, M).*

Beweis. Übung! ■

5.19 Bemerkungen. *Seien (G, M), (H, N) Gruppenwirkungen, $(\varphi, f) : (G, M) \to (H, N)$ morphismus. Dann gilt:*

(i) $\Theta := \ker f$ *ist* G-invariant, *d.h.* ${}^M/_\Theta$ *ist verträgliches Blocksystem.*
(ii) $G_{f^{-1}(b)} = \varphi^{-1}(H_b)$ *für jedes* $b \in N$.
(iii) $\forall a \in M,\ g \in G, b \in N : a, a^g \in f^{-1}(b) \implies g \in \varphi^{-1}(H_b)$ *(d.h.* $f(a) = f(a^g) = b \implies b^{\varphi(g)} = b$*).*

Beweis. Übung! ■

Vorbemerkungen zum nächsten Satz:

Sei $R \subseteq M \times M$. Setze:

- $R^{\text{ref}} := R \cup \triangle_M$ ist *reflexiver Abschluss*,
- $R^{\text{sym}} := R \cup R^{-1}$ ist *symmetrischer Abschluss*, wobei $R^{-1} = \{(b, a) \mid (a, b) \in R\}$,
- $R^{\text{trans}} := \bigcup_{n \in \mathbb{N}\backslash\{0\}} R^n$ ist *transitiver Abschluss*, wobei $R^n := R \circ ... \circ R$ für $n \geq 1$ und
$$R \circ S = \{(a, c) \in M^2 \mid \exists b \in M : (a, b) \in R,\ (b, c) \in S\},$$
- $R^{\text{äq}} := \bigcup\{S \in \text{Äq}(M) \mid R \subseteq S\}$ die von R erzeugte Äquivalenzrelation auf M (bzgl. $\subseteq$ kleinstes Element von $\text{Äq}(M)$, das R enthält).

Es gilt:
$$R^{\text{äq}} = \left((R^{\text{ref}})^{\text{sym}}\right)^{\text{trans}} \qquad (*)$$

(Übung!)

Begiffe:

- *R antireflexiv* $:\Longleftrightarrow R \cap \triangle_M = \emptyset$.

– Graph (M,R) heißt *zusammenhängend* $:\Longleftrightarrow \forall a,b\in M, a\neq b \exists a=a_0,a_1,...,a_n=b\in M : \forall i\in\{0,...,n-1\} : (a_i,a_{i+1})\in R$ oder $(a_{i+1},a_i)\in R \overset{(*)}{\Longleftrightarrow} R^{\text{äq}}=M\times M$.

5.20 Satz (Charakterisierungssatz für primitive Permutationsgruppen). *Sei (G,M) transitiv. Dann:*

(A) *(G,M) imprimitiv $\Longleftrightarrow$ $\exists a\in M\exists U\leq G : G_a \lneqq U \lneqq G$ ($\Longleftrightarrow$ $\forall a\in M\dots$ da (G,M) transitiv).*

(B) *(G,M) primitiv $\Longleftrightarrow$ $\forall a\in M : G_a = G$ oder G_a ist maximale UG von G ($\Longleftrightarrow$ $\exists a\in M\dots$ da (G,M) transitiv).*

(C) **Satz von HIGMAN**:

$$(G,M) \text{ primitiv} \Longleftrightarrow \text{Für jede antireflexive 2-Bahn } \varrho\in 2\text{-Orb}\,(G,M) \text{ ist der Graph } (M,\varrho) \text{ zusammenhängend.}$$

Beweis. (B) ist Umformulierung von (A).

Zu (A): „$\Longrightarrow$“ (G,M) imprimitiv $\overset{5.12(c)}{\Longrightarrow}$ $\exists$ nichttrivialer Block $B\subseteq M$. Sei $a\in B$ und $U:=G_{[B]}$. Dann gilt:

(i) U ist nicht transitiv ($B^U=B\subsetneqq M$), also $U\lneqq G$ (da G transitiv).

(ii) $G_a\subseteq U$, denn $g\in G_a \Longrightarrow a=a^g\in B^g \Longrightarrow B\cap B^g\neq\emptyset \overset{B\text{ Block}}{\Longrightarrow} B^g=B \Longleftrightarrow g\in G_B=U$.

(iii) $G_a\lneqq U$: G transitiv, $|B|\geq 2 \Longrightarrow \exists b\in B, a\neq b\exists h\in G : b=a^h$, d.h. $h\notin G_a$. $b=a^h\in B^h \overset{b\in B}{\Longrightarrow} B\cap B^h\neq\emptyset \overset{B\text{ Block}}{\Longrightarrow} B=B^h \Longrightarrow h\in G_B=U$.

„$\Longleftarrow$“ Sei $a\in M, U\leq G$ mit $G_a\lneqq U\lneqq G$. Behauptung: $B:=a^U$ ist ein nichttrivialer Block von G. (Damit (G,M) imprimitiv.)

– Blockeigenschaft: Sei $b\in B\cap B^g$, $g\in G \Longrightarrow \exists h,h'\in U : b=a^h$, $b=a^{h'g} \Longrightarrow h'gh^{-1}\in G_a\subseteq U \Longrightarrow g\in (h')^{-1}Uh=U \Longrightarrow B^g=a^{Ug}\overset{g\in U}{=} a^U=B$.

– B nicht trivial: $G_a\lneqq U \Longrightarrow \exists h\in U : a^h\neq a \Longrightarrow |B|=|a^U|\geq 2$. $U\lneqq G \Longrightarrow \exists g\in G\backslash U \Longrightarrow B\cap B^g=\emptyset$ (denn $B=B^g \overset{\text{s.o.}}{\Longrightarrow} g\in U$) $\Longrightarrow |B|\leq\frac{|M|}{2}$. Also $B\neq M$.

Zu (C): „$\Longrightarrow$“ Sei (G,M) primitiv. Sei $\varrho\in 2\text{-Orb}\,(G,M)$ antireflexiv (d.h. $\triangle_M\cap\varrho=\emptyset \overset{\varrho\text{ 2-Bahn}}{\Longleftrightarrow} \varrho\nsubseteq\triangle_M$). Setze:

$$\Theta := \varrho^{\text{äq}} \overset{(*)}{=} \left(\left(\varrho^{\text{ref}}\right)^{\text{sym}}\right)^{\text{trans}} = \left((\triangle_M\cup\varrho)\cup\varrho^{-1}\right)^{\text{trans}}.$$

Da $\text{Inv}\,(G,M)$ Krasneralgebra ist (vgl. 4.11) folgt $\Theta\in\text{Inv}\,(G,M)\cap\text{Äq}(M)$. Da (G,M) primitiv, ist $\Theta=\triangle_M$ oder $\Theta=M^2$ (5.16). Weil $\varrho\subseteq\Theta$ und $\varrho\nsubseteq\triangle_M$, ist $\Theta=M\times M$.

„$\Longleftarrow$“ Annahme: (G,M) imprimitiv. Dann gibt es nichttriviale Äquivalenzrelation $\Theta\in 2\text{-Inv}\,(G,M)$. Sei $(a,b)\in\Theta\backslash\triangle_M$. Dann ist $\varrho:=(a,b)^G$ antireflexive 2-Bahn. (M,ϱ) ist nicht zusammenhängend, da $\varrho^{\text{äq}}=(\underbrace{(a,b)^G}_{\subseteq\Theta})^{\text{äq}}\subseteq\Theta^{\text{äq}}=\Theta\neq M^2$ (vgl. Vorbemerkung). ■

5.21 Folgerung. *Jede 2-fach transitive Permutationsgruppe G (d.h. $2\text{-Inv}(G, M) = \{\triangle_M, M^2 \backslash \triangle_M\}$) ist primitiv.*

Beweis. 2-fach transitiv $\iff$ $2\text{-Orb}(G, M) = \{\triangle_M, M^2\backslash\triangle_M\}$ $\implies$ es gibt keine nichttriviale Äquivalenzrelation für (G, M). ■

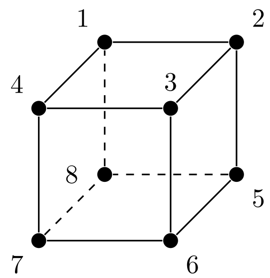
Neues Problem: Wie bestimmt man eigentlich Automorphismengruppen von Graphen?

5.22 Verfahren. Bestimmung der Automorphismengruppe $\operatorname{Aut}\Gamma$ bzw. der Anzahl $|\operatorname{Aut}\Gamma|$ für einen Graphen $\Gamma = (V, E)$. Sei $G := \operatorname{Aut}\Gamma$.

(1) Wähle $a_1 \in V$ und bestimme eine Menge $T_1 = \{g_{11}, ..., g_{1n_1}\}$ mit $a_1^G = \{a^{g_{11}}, ..., a_1^{g_{1n_1}}\}$, $n_1 = |a_1^G|$. Dann gilt $G = G_{a_1}T_1$ (und $|G| = |G_{a_1}| \cdot n_1$). Bemerkung: Die Darstellung hg_1 ($h \in G_{a_1}$, $g_1 \in T_1$) ist eindeutig!
(2) Wenn Elemente von G_{a_1} bzw. $|G_{a_1}|$ noch nicht bekannt sind, wiederhole (1) mit G_{a_1} statt G: Wähle $a_2 \in V$, $a_2 \neq a_1$, bestimme $T_2 = \{g_{21}, ..., g_{2n_2}\}$ mit $a_2^{G_{a_1}} = \{a_2^{g_{21}}, ..., a_2^{g_{2n_2}}\}$, $n_2 = |a_2^{G_{a_1}}|$. Dann gilt: $G = G_{a_1,a_2}T_2T_1$ und $|G| = |G_{a_1,a_2}|n_1n_2$.
(3) Wiederhole solange, bis Stabilisator $G_{a_1,...,a_r}$ bekannt ist (spätestens bist $G_{a_1,...,a_r} = \{e\}$).
(4) Ergebnis: $G = G_{a_1,...,a_r}T_r \cdots T_1$ bzw. $|G| = |G_{a_1,...,a_r}|n_r \cdots n_1$. Jede Permutation ist eindeutig in der Form $g = ht_r \cdots t_1$ ($h \in G_{a_1,...,a_r}$, $t_i \in T_i$ für $i \in \{1, ..., r\}$) darstellbar.

Bemerkung: Falls $G_{a_1,...,a_r} = \{e\}$, so ist $(a_1, ..., a_r)$ Sims-Basis (vgl. 3.2) und T_i sind Transversalen für die zugehörige Sims-Kette $U_i = G_{a_1,...,a_i}$, $i = 1, ..., r$. Zum Beweis siehe 3.3.

5.23 Beispiel. Automorphismengruppe des Würfelgraphen Γ_W:



Anzahl der Automorphismen:

$a_1 := 1$: $n_1 = |a_1^G| = 8$, denn $\exists$ Automorphismen (Drehungen) $f := \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}$, $g := \begin{pmatrix}1 & 8 & 7 & 4\end{pmatrix}\begin{pmatrix}2 & 5 & 6 & 3\end{pmatrix}$.

$a_2 := 2$: $n_2 = |a_2^{G_{a_1}}|$. Kandidaten $\{2, 4, 8\}$ und $\exists$ Automorphismus $h := \begin{pmatrix}2 & 8 & 4\end{pmatrix}\begin{pmatrix}5 & 7 & 3\end{pmatrix}$ (Rotation um Achse 1-6).

$a_3 := 3$: $n_3 = |a_3^{G_{a_1,a_2}}| = 2$. Kandidaten $\{3,5\}$ und $\exists$ Automorphismus $k := \big(3\ 5\big)\big(4\ 8\big)$ (Spiegelung an der Ebene durch $1,2,6,7$). Nun $G_{a_1,a_2,a_3} = \{e\} \overset{5.22}{\Longrightarrow} |G| = n_1 n_2 n_3 = 48$.

Bestimmung der Automorphismengruppe:

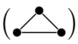
$a_1 = 1$: $a_1^G = \{1,...,8\} = \{a_1^e, a_1^f, a_1^{f^2}, a_1^{f^3}, a_1^{fg}, a_1^{fgf}, a_1^{fgf^2}, a_1^{fgf^3}\}$,
$T_1 = \{e, f, f^2, f^3, fg, fgf, fgf^2, fgf^3\}$.
$a_2 = 2$: $a_2^{G_{a_1}} = \{2,4,8\} = \{a_2^e, a_2^h, a_2^{h^2}\}$, $T_2 = \{e, h, h^2\}$.
$a_3 = 3$: $a_3^{G_{a_1,a_2}} = \{3,5\} = \{a_3^e, a_3^k\}$, $T_3 = \{e, k\}$.

Jeder Automorphismus von Γ_W ist eindeutig in der Form $t_3t_2t_1$ mit $t_3 \in T_3, t_2 \in T_2, t_1 \in T_1$ darstellbar (nach 5.22). Insbesondere: $T_1 \cup T_2 \cup T_3$ ist ein Erzeugendensystem von $G \Longrightarrow$ einfacheres Erzeugendensystem: $\{f, g, h, k\}$.

5.24 Bemerkung. *Satz von KRASNER* $\Longrightarrow$ *Jede Relation der Form* $F_\varphi(\Phi)$*, die sich aus* $\Phi \subset V \times V$ *durch logische Operation* F_φ *ergibt (*$\varphi(R, x_1, ..., x_m)$ *Formel des Prädikatenkalküls erster Stufe) ist wieder invariant bzgl.* $\mathrm{Aut}\,\Phi$ *(*$F_\varphi(\Phi) \in \mathrm{Inv}\,\mathrm{Aut}\,\Phi = [\Phi]$*).*

Folgerung: Ist φ *eine Eigenschaft von Punkten, Punktepaaren (z.B. Kanten), Punktentripeln (z.B. Dreiecke), usw. eines Graphen, die sich durch eine Formel des Prädikatenkalküls erster Stufe beschreiben lässt (ausschließlich unter Verwendung der Relation* Φ*), dann bleibt die Eigenschaft* Φ *unter Automorphismen erhalten (*$a \vDash \varrho \Longrightarrow a^g \vDash \varrho$*,* $(a,b) \vDash \varrho \Longrightarrow (a^g, b^g) \vDash \varrho$*,* $(a_1, ..., a_n) \vDash \varrho \Longrightarrow (a_1^g, ..., a_n^g) \vDash \varrho$*).*

Beispiele für ϱ:

- Knoten a hat Valenz k,
- a hat genau einen Nachbarn mit Valenz 3,
- je zwei Nachbarn von a sind nicht durch eine Kante verbunden,
- a ist in genau 2 Dreiecken () enthalten.

6 POLYAsche Abzähltheorie

6.1 Beispiele (Isomorphietypen von Graphe). Graph $\Gamma = (V, E)$ ohne Schlingen, d.h. $E \subseteq (V \times V) \backslash \triangle_M =: M$. Sei $V := \{1, ..., n\}$. Dann $E \subseteq M \iff E \in \mathfrak{P}(M) \implies$ Es gibt $|\mathfrak{P}(M)| = 2^{|M|}$ viele solcher Graphen mit fester Knotenmenge V.

Problem: Wie viele Isomorphietypen gibt es? (D.h. wie viele bis auf Isomorphie verschiedene Graphen.)

Seien $\Gamma = (V, E), \Gamma' = (V', E')$ Graphen. Dann:

$$\Gamma \cong \Gamma' :\iff \exists \text{ Bijektion } f : V \to V' \forall v_1, v_2 \in V : (v_1, v_2) \in E \iff (f(v_1), f(v_2) \in E'.$$

Umformulierung: oBdA $V = V' = \{1, ..., n\}$, d.h. $f \in S_{\underline{n}}$. Dann:

$$f : \Gamma \to \Gamma' \text{ Isomorphismus } \iff \Gamma' = (V, E^{\tilde{f}}) \text{ mit } E^{\tilde{f}} = \{(a, b)^{\hat{f}} \mid (a, b) \in E\}$$

wobei $(a, b)^{\hat{f}} = (a^f, b^f)$ (Wirkungen auf Paaren, vgl. 2.8(c) bzw. auf Potenzmenge, vgl. 2.8(a)). Also:

$$(V, E) \cong (V, E') \iff \exists f \in S_{\underline{n}} : E' = E^{\tilde{f}} \iff E' \in E^{\tilde{S}_{\underline{n}}}.$$

Dabei ist $E^{\tilde{S}_{\underline{n}}}$ 1-Bahn (von E erzeugt) der Gruppenwirkung $(\tilde{S}_{\underline{n}}, \mathfrak{P}(M))$.

$$(V, E) \cong (V, E') \iff E \text{ und } E' \text{ sind in gleicher Bahn.}$$

Das heißt:

$$\#\text{Isomorphietypen} = \overbrace{|\text{1-Orb}\,(\tilde{S}_{\underline{n}}, \mathfrak{P}(M))|}^{\text{(Anzahl der Bahnen)}}.$$

Feinere Klassifizierung möglich, z.B. für festes $k \geq 0$:

$$\begin{matrix}\#\text{Isomorphietypen von Graphen} \\ \Gamma = (V, E) \text{ mit } |E| = k\end{matrix} = |\text{1-Orb}\,(\tilde{S}_{\underline{n}}^{[k]}, \mathfrak{P}_k(M))|.$$

Einschränkung der Wirkung $(\tilde{S}_{\underline{n}}, \mathfrak{P}(M))$ auf $\mathfrak{P}_k(M)$

Menge der k-elementigen Teilmengen von M

Darstellung oft durch erzeugende Funktion (Polynom):

$$\gamma(x) = \sum_{k=0}^{|M|} t_k x^k \overset{\text{Satz von}}{\underset{\text{POLYA}}{=}} Z(\hat{S}_{\underline{n}}).$$

sog. Zyklenzeiger $Z(\hat{S}_{\underline{n}})$ (aus $Z(S_{\underline{n}})$ bestimmbar)

6.2 Definition. Sei (G, M) Gruppenwirkung. Für $g \in G$ sei $M_g := \{m \in M \mid m^g = m\}$ (Menge aller Fixpunkte). Setze $\chi(g) := |Mg|$ der *Charakter* von g.

6.3 Lemma von CAUCHY–FROBENIUS–BURNSIDE. („3-Männer–Lemma".)
Sei (G, M) Gruppenwirkung. Dann gilt:

$$\underbrace{|\text{1-Orb}\,(G, M)|}_{\#\text{1-Bahnen}} = \underbrace{\frac{1}{|G|} \sum_{g \in G} \chi(g)}_{\substack{\text{Arithmetisches Mittel} \\ \text{der Charaktere}}}$$

Beweis. Betrachte Graph $\Gamma = (M \uplus G, E)$ mit $E = \{(g, m) \in G \times M \mid m^g = m\} \overset{(*)}{=} \{(g, m) \in G \times M \mid m \in M_g\} \overset{(**)}{=} \{(g, m) \in G \times M \mid g \in G_m\}$. Nun gilt:

$$E \overset{(*)}{=} \sum_{g \in G} |Mg| = \sum_{g \in G} \chi(g).$$

Anderseits:

$$\begin{aligned} |E| &\overset{(**)}{=} \sum_{m \in M} |G_m| \underset{\text{LAGR.}}{\overset{1.14}{=}} \sum_{m \in M} \frac{|G|}{|m^G|} = |G| \sum_{m \in M} \frac{1}{|m^G|} \\ &= |G| \sum_{B \in \text{1-Orb}\,(G,M)} \sum_{m \in B} \underbrace{\frac{1}{|m^G|}}_{=\frac{1}{|B|}} = |G| \sum_{B \in \text{1-Orb}\,(G,M)} 1 \\ &= |G| \cdot |\text{1-Orb}\,(G, M)|. \end{aligned}$$

■

6.4 Definition. (a) Sei $g \in S_M$. Es sei $j_k(g)$ ($= j_k$, falls keine Verwechslungsgefahr) die Anzahl der Zyklen der Länge k in der vollständigen (also unverkürzten) Zyklendarstellung von g ($k \in \{1, ..., n\}$, $n := |M|$) Das Polynom (in unbestimmten $x_1, ..., x_n$)

$$Z(g) := x_1^{j_1(g)} \cdot x_2^{j_2(g)} \cdots x_n^{j_n(g)}$$

heißt *Zyklentyp* (*Zyklenindex*) von g. (Falls $j_k(g) = 0$, so wird $x_k^{j_k(g)} = 1$ auch weggelassen.)

(b) Für $G \leq S_M$ heißt das Polynom

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} Z(g)$$

der *Zyklenzeiger* (*Zyklenindex*) von G.

(c) *POLYA–Substitution:* Ersetzee von x_k durch $(1 + x^k)$ im Zyklentyp bzw. Zyklenzeiger ($k \in \{1, ..., n\}$). Bezeichnung für die durch Substitution entstehenden Polynome: $Z(g, 1 + x)$ bzw. $Z(G, 1 + x)$.

Bemerkung: Ähnliche Permutationen habe den gleichen Zyklentyp (vgl. 1.18). Genauer:

$$g_1, g_2 \text{ ähnlich} \iff Z(g_1) = Z(g_2).$$

Daher Zusammenfassung ähnlicher Permutationen im Zyklenzeiger möglich!
($\rightsquigarrow$ Normalform.)

6.5 Beispiele. (a)
$G := C_4 = \{g_0, g_1, g_2, g_3\} = \{e, \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}\}$ auf $\underline{4} = \{1,2,3,4\}$. $Z(G) = \frac{1}{4}(x_1^4 + x_4^1 + x_2^2 + x_4^1) = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4)$.

(b) $G := S_{\underline{3}}$ auf $\underline{3} = \{1,2,3\}$. $|S_{\underline{3}}| = 3! = 6$. Dann gilt: $Z(G) = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3)$.

(c) $G := S_{\underline{3}}^{[2]}$ induzierte Wirkung von $S_{\underline{3}}$ auf der Menge

$$M := \{(a,b) \in \underline{3} \times \underline{3} \mid a \neq b\} = (\underline{3} \times \underline{3}) \backslash \triangle_{\underline{3}}.$$

Dann gilt: (Übung!) $Z(G) = \frac{1}{6}(x_1^6 + 3x_2^3 + 2x_3^2)$. Das heißt: G besitzt 1 Permutation mit 6 Fixpunkten, 3 Permutationen mit 3 Zyklen der Länge 2, 2 Permutationen mit 2 Zyklen der Länge 3.

6.6 Bemerkung. *Wegen 6.3 erhält man die Zahl* $|1\text{-Orb}\,(G,M)|$ *aus* $Z(G)$*, wenn man alle Exponenten* $j_1(g)$ *von* x_1 *(Fixpunkte* $\approx$ *Zyklen der Länge* 1*) aufsummiert (ergibt Arithmetisches Mittel wegen Faktor* $\frac{1}{|G|}$ *in* $Z(G)$*). Formal:*

$$|1\text{-Orb}\,(G,M)| = \frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{g\in G} j_1(g).$$

Beispiel. $G = \{e, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\}$, $M = \underline{4}$. Dann: $Z(G) = \frac{1}{4}(x_1^4 + x_1^2x_2 + x_1^2x_2 + x_2^2) \implies |1\text{-Orb}\,(G,M)| = \frac{1}{4}(1\cdot 4 + 2\cdot 2) = 2$. Diese ist aber gleich dem Koeffizienten $\text{coef}_{\,1}(Z(G, 1+x))$ von x im Polynom $Z(G, 1+x)$ (vgl. POLYA–Substitution, 6.4).

Beweis. Übungsaufgabe! ∎

Definition. $\text{coef}_{\,k}\big(\sum_{i=0}^m a_i x^i\big) := a_k$ $(k \in \{0, ..., m\})$.

Beispiel. Sei G wie oben. $Z(G, 1+x) = \frac{1}{4}((1+x^4) + 2(1+x^2)(1+x^2) + (1+x^2)^2) \implies \text{coef}_{\,1}(Z(G,1+x)) = \frac{1}{4}(4 + 2\cdot 2) = \frac{8}{4} = 2$.

Für Beispiel (c) aus 6.5 ergibt die POLYA–Substitution

$$Z(S_{\underline{3}}^{[2]}, 1+x) = \frac{1}{6}((1+x)^6 + 3(1+x^2)^3 + 2(1+x^3)^2)$$

$\implies \text{coef}_{\,1}(Z(S_{\underline{3}}^{[2]}, 1+x)) = \frac{1}{6}\cdot 6 = 1$. Das heißt: $S_{\underline{3}}^{[2]}$ hat nur eine Bahn, also $S_{\underline{3}}^{[2]}$ transitiv auf M (vgl. 6.5).

6.7 Beispiel (Abzähltheorie—allgemeine Aufgabestellung). Abzählung „kombinatorischer“ Objekte durch Einteilung in Klassen ($\approx$ Eigenschaften). A Menge, $\sim$ Äquivalenzrelation auf A, $k : A \to \mathbb{N}^r$ mit $\sim\, = \ker k$. (D.h. jede Äquivalenzklasse $[a]_\sim$ (mit $a \in A$) ist eindeutig durch Zahlentupel $k(a) = (k_1(a), ..., k_r(a))$ charakterisiert.) Dann heißt das Polynom (in Variablen $x_1, ..., x_r$)

$$t(x_1, ..., x_r) = \sum_{[a]_\sim \in A/\sim} |[a]_\sim| \cdot x_1^{k_1(a)} \cdots x_r^{k_r(a)}$$

erzeugende Funktion für die Zerlegung $A/\sim$.

Problem: Bestimmung der erzeugenden Funktion.

Wiederholung: Für $f : A \to B$ ist $\ker f := \{(a,b) \in A^2 \mid f(a) = f(b)\}$ (vgl. lineare Algebra).

Die POLYAsche Abzähltheorie berechnet erzeugende Funktionen für (zunächst komplizierte) Zerlegungen, die durch Gruppenwirkungen induziert werden—und zwar aus dem Zyklenzeiger der gegebenen Gruppe.

Beispiel.

„einfach“	„kompliziert“
(G, M)	$(\tilde{G}, \mathfrak{P}(M))$ (vgl. 6.1, 2.8(a))
Zerlegung von M 1-Orb (G, M)	Zerlegung von $\mathfrak{P}(M)$ 1-Orb $(\tilde{G}, \mathfrak{P}(M))$
$\downarrow$	$\downarrow$
Anzahl aus $Z(G)$ bzw. $Z(G, 1+x)$ bestimmbar (vgl. 6.6)	auch aus $Z(G, 1+x)$ bestimmbar $\longrightarrow$ Satz von POLYA 6.9 (Auch aus $Z(G)$ bestimmbar)

6.8 Vorbereitung auf Satz von POLYA. Sei (G, M) Permutationsgruppe (bzw. allgemeiner: Gruppenwirkung), $m := |M|$.

– Induzierte Gruppenwirkung von G auf k-elementigen Teilmengen von M ($0 \leq k \leq m$): $(G^{\{k\}}, \mathfrak{P}_k(M))$, vgl. 2.8(b).
– Induzierte Gruppenwirkung von G auf Potenzmenge: $(\tilde{G}, \mathfrak{P}(M))$, vgl. 2.8(a).

$\Longrightarrow$ Zerlegung der 1-Bahnen:

$$\text{1-Orb}\,(\tilde{G}, \mathfrak{P}(M)) = \biguplus_{k=0}^{m} \text{1-Orb}\,(G^{\{k\}}, \mathfrak{P}_k(M)).$$

Erzeugende Funktion für diese Zerlegung:

$$t_G(x) := \sum_{k=0}^{m} t_k x^k \text{ mit } t_k := |\text{1-Orb}\,(G^{\{k\}}, \mathfrak{P}_k(M))|.$$

Beachte:

$$t_G(1) = \sum_{k=0}^{m} t_k = |\text{1-Orb}\,(\tilde{G}, \mathfrak{P}(M)),\ t_1 = |\text{1-Orb}\,(G, M)| \ (= |\text{1-Orb}\,(G^{\{1\}}, \mathfrak{P}_1(M))|).$$

6.9 Satz von POLYA. (Für eine Variable.) *Sei (G, M) Permutationsgruppe (bzw. Gruppenwirkung). Dann gilt*

$$t_G(x) = Z(G, 1+x).$$

Speziell erhält man $t_G(a) = |\text{1-Orb}\,(\tilde{G}, \mathfrak{P}(M))|$, wenn alle Variablen in $Z(G)$ mit dem Wert 2 belegt werden ($t_G(1) = Z(G, 1+x)(1) = Z(G)(2, ..., 2)$).

Beweis. $Z(G, 1+x) = \frac{1}{|G|}\sum_{g \in G} Z(g, 1+x)$.

$Z(g, 1+x) = (1+x)^{j_1(g)} \cdot (1+x^2)^{j_2(g)} \cdots (1+x^m)^{j_m(g)}$. Für jedes $k \in \{0, ..., m\}$ sei $c_k := \operatorname{coef}_k(Z(g, 1+x))$, d.h. $Z(g, 1+x) = \sum_{k=0}^m c_k(g)x^k$. Dann ist:

$$Z(G, 1+x) = \frac{1}{|G|}\sum_{g \in G}\left(\sum_{k=0}^m c_k(g)x^k\right) = \sum_{k=0}^m \underbrace{\boxed{\left(\frac{1}{|G|}\sum_{g \in G} c_k(g)\right)}}_{k} x^k.$$

Zu Zeigen: $\boxed{}_k \overbrace{=}^{\text{vgl. 6.8}} t_k$ für alle $k \in \{0, ..., m\}$.

Lemma. *Für alle $k \in \{0, ..., m\}$ gilt $c_k(g) = \chi(g^{\{k\}})$ mit*

$$g^{\{k\}} : \mathfrak{P}_k(M) \to \mathfrak{P}_k(M),\ B \mapsto B^g.$$

Mit obigem Lemma folgt:

$$\boxed{}_k \overset{6.10}{=} \frac{1}{|G|}\sum_{g \in G}\chi(g^{\{k\}}) = \frac{1}{|G^{\{k\}}|}\sum_{h \in G^{\{k\}}}\chi(h) \overset{6.3}{=} |\text{1-Orb}\,(G^{\{k\}}, \mathfrak{P}_k(M))| \underset{\text{Def.}}{\overset{6.8}{=}} t_k.$$

Somit:

$$Z(G, 1+x) = \sum_{k=0}^m t_k x^k = t_G(x).$$

■

6.10 Lemma. (Notation wie in 6.8 und 6.9)

(a) $c_k(g)$ ($\overset{\text{Def.}}{=} \operatorname{coef}_k(Z(g, 1+x))$) *ist die Anzahl der k-elementigen Teilmengen von M, die invariant sind unter g, d.h. $c_k(g) = |\{B \in \mathfrak{P}_k(M) \mid B^g = B\}|$.*

(b) $c_k(g) = \chi(g^{\{k\}})$ *(wobei $g^{\{k\}} : \mathfrak{P}_k(M) \to \mathfrak{P}_k(M),\ B \mapsto B^g$).*

Beweis. (b) ist nur Umformulierung von (a), denn

$$B \text{ invariant unter } g \iff B^g = B \iff B^{g^{\{k\}}} = B \iff B \text{ Fixpunkt von } g^{\{k\}}$$

für alle $B \in \mathfrak{P}_k(M)$.

Zu (a): Vorbemerkung: Für $B \subseteq M$ gilt:

$$B^g = B \overset{1.11(\text{iv})}{\iff} B \text{ ist Vereinigung von Zyklen von } g. \qquad (*)$$

Wir betrachten die (vollständige) Zyklendarstellung von g:

$$\begin{array}{lc} \text{Anzahl der Elemente in Zyklen} & M_1 \quad M_2 \qquad M_s \\ & g = (\cdots)(\cdots)\cdots(\cdots) \\ \text{Menge der Elemente in Zyklen} & m_1 \quad m_2 \qquad m_s \end{array}$$

mit $m_1 = |M_1|$, $m_2 = |M_2|$, ..., $m_s = |M_s|$, $s :=$ #Zyklen von g. Beachte: $\sum_{i=1}^s m_i = m = |M|$. Nun ist $j_l(g) := |\{i \in \{1,...,s\} \mid m_i = l\}|$ für alle $l \in \{1,...,m\}$. Es folgt:

$$\begin{aligned} Z(g, 1+x) =& (1+x)^{j_1(g)}(1+x^2)^{j_2(g)} \cdots (1+x^m)^{j_m(g)} \\ =& (1+x^{m_1})(1+x^{m^2}) \cdots (1+x^{m_s}). \end{aligned}$$

Nun gilt:

$$\begin{aligned} Z(g, 1+x) &= \prod_{l=1}^m (1+x^l)^{j_l(g)} = \prod_{i=1}^s (1+x^{m_i}) \\ &\overset{(**)}{=} \sum_{T \subseteq \{1,...,s\}} \prod_{i \in T} x^{m_i} = \sum_{T \subseteq \{1,...,s\}} x^{\sum_{i \in T} m_i}, \end{aligned}$$

wobei allgemein gilt (Übung!):

$$\prod_{i=1}^s (1+z_i) = \sum_{T \subseteq \{1,...,s\}} \prod_{i \in T} z_i. \tag{**}$$

$\implies$ $\operatorname{coef}_k(Z(g, 1+x)) = |\{T \subseteq \{1,...,s\} \mid k = \sum_{i \in T} m_i\}|$.

Bemerkung: Die Abbildung

$$\Phi : \mathfrak{P}(\{1,...,s\}) \to \mathfrak{P}(M), \ T \mapsto \biguplus_{i \in T} M_i$$

ist injektiv, und es gilt $|\Phi(T)| = \sum_{i \in T} m_i$ für alle $T \subseteq \{1,...,s\}$.

$$\begin{aligned} \operatorname{coef}_k(Z(g, 1+x)) \overset{\Phi \text{ inj.}}{=} & |\{\Phi(T) \mid T \subseteq \{1,...,s\}, \ k = \sum_{i \in T} m_i\}| \\ =& |\{\Phi(T) \mid T \subseteq \{1,...,s\}, \ k = |\Phi(T)|\}| \\ =& |\{B \in \mathfrak{P}_k(M) \mid \exists T \subseteq \{1,...,s\} : B = \Phi(T)\}| \\ =& |\{B \in \mathfrak{P}_k(M) \mid B^g = B\}|. \end{aligned}$$

■

6.11 Folgerung. *Sei $g \in S_M$, $s :=$ #Zyklen von g (in vollst. Zyklendarstelung), und sei $\tilde{g} : \mathfrak{P}(M) \to \mathfrak{P}(M)$, $B \mapsto B^g$. Dann gilt $\chi(\tilde{g}) = 2^s$.*

Beweis. Aus Beweis von 6.10: $\Phi : \mathfrak{P}(\{1,...,s\}) \to \mathfrak{P}(M)$, $T \mapsto \bigcup_{i \in T} M_i$ ist injektiv, und $\operatorname{Im}(\Phi) = \{B \subseteq M \mid B^g = M\}$. Damit folgt:

$$\chi(\tilde{g}) = |\{B \subseteq M \mid B^g = M\}| = |\operatorname{Im}(\Phi)| \overset{\Phi \text{ inj.}}{=} 2^s. \quad ■$$

6.12 Bemerkung. $\mathfrak{P}(M) \cong 2^M \rightsquigarrow$ Verallgemeinerung:

$$K^M := \{f \mid f : M \to K \text{ Abbildung}\}$$

für beliebige Menge K. Es gibt eine Version des Satzes von Polya für mehrere Variablen: beschreibt Bahnen für Wirkung von $G \leq S_M$ auf der Menge K^M.

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, shift right, "g"'] \arrow[dr, phantom, "\circlearrowleft"] & K \\ M \arrow[u, dashed, shift right, "g^{-1}"'] \arrow[ur, bend right, "f^{\tilde{g}}"'] & \end{tikzcd}$$

$f^{\tilde{g}}(x) := f(x^{g^{-1}})$,

$g \in G$, $x \in M$, $f \in K^M$. Für $K = \{1, ..., r\}$: zu $f \in K^M$ definiert man $m_i := |f^{-1}(i)|$ $(i \in \{1, ..., r\})$, $\text{Typ}(f) := z_1^{m_1} \cdots z_r^{m_r}$. Genaueres: Klein/Pöschel/Rosenbaum: Angewandte Algebra, S. 89-91.

6.13 Beispiel (Isomorphie von Graphen). (vgl. 6.1) Sei $\Gamma = (V, E)$ Graph ohne Schlingen, d.h. $E \subseteq M := (V \times V) \setminus \triangle_V$. $\Gamma \cong \Gamma' \overset{6.1}{\iff} E' \in E^{\tilde{S}_{\underline{n}}}$ $(|V| := \tilde{S}_{\underline{n}}, \Gamma' = (V, E'))$.

$\#$Isomorphietypen $= |1\text{-Orb}\,(\tilde{S}_{\underline{n}}, \mathfrak{P}(M))|$,
$\#$Isomorphietypen von Graphen mit k Kanten $= |1\text{-Orb}\,(S_{\underline{n}}^{\{k\}}, \mathfrak{P}_k(M))| = t_k$.

Gemäß Vorbereitung 6.8 ist die erzeugende Funktion von $(\tilde{S}_{\underline{n}}, \mathfrak{P}(M))$ gegeben durch $t_G(x) = \sum_{k=0}^{M} t_k x^k$, wobei (G, M) Wirkung von $S_{\underline{n}}$ auf M ist, d.h. $(G, M) := (S_{\underline{n}}^{[2]}, M)$. Berechnung von $t_G(x)$, d.h. $t_{S_{\underline{n}}^{[2]}}(x)$, mit dem Satz von POLYA (6.9):

$$t_{S_{\underline{n}}^{[2]}}(x) = Z(S_{\underline{n}}^{[2]}, 1 + x).$$

Man muss also Zyklenzeiger von $S_{\underline{n}}^{[2]}$ bestimmen (Übung für $n = 3$!).

Hier am Beispiel $n = 4$: $|S_{\underline{4}}| = 4!$, aber nur 5 Ähnlichkeitsklassen:

Repräsentanten	Anzahl der Elemente in Ähnlichkeitsklassen
$g_1 = e = (1)(2)(3)(4)$	$\# = 1$
$g_2 = (12)(3)(4)$	$\# = \binom{4}{2} = 6$
$g_3 = (12)(34)$	$\# = \frac{1}{2}\binom{4}{2} = 3$
$g_4 = (123)(4)$	$\# = 2\binom{4}{3} = 8$
$g_5 = (1234)$	$\# = 3! = 6$

Da ähnliche Permutationen den gleichen Zyklentyp haben (vgl. 6.4), ergibt sich $Z(S_{\underline{4}}) = \frac{1}{4!}(Z(e) + 6Z(g_2) + 3Z(g_3) + 8Z(g_4) + 6Z(g_5)) = \frac{1}{4!}(x_1^4 + 6x_1^2 x_2 + 3x_2^2 + 8x_1 x_3 + 6x_4)$. Nun Übergang zu $S_{\underline{4}}^{[2]}$. In $S_{\underline{4}}$: Ähnlichkeit = Konjugiertheit $\Longrightarrow$ Konjugiertheit bleibt beim Übergang zu $S_{\underline{4}}^{[2]}$ erhalten:

$$\varphi(\tilde{g}) = \varphi(h^{-1} g h) = \varphi(h)^{-1} \varphi(g) \varphi(h).$$

Also
$$Z(S_{\underline{4}}^{[2]}) = \frac{1}{4!}(Z(\hat{e}) + 6Z(\hat{g}_2) + 3Z(\hat{g}_3) + 8Z(\hat{g}_4) + 6Z(\hat{g}_5)),$$
wobei $\tilde{g} : M \to M,\ (a,b) \mapsto (a^g, b^g)$ induzierte Wirkung von $g \in S_M$ auf $M = (V \times V)\backslash\triangle_V$, $|M| = 12$. Insbesondere $\hat{e} = e \implies Z(\hat{e}) = x_1^{12}$. $g_2 = \Big(12\Big)\Big(3\Big)\Big(4\Big) \implies$
$$\hat{g}_2 = \Big((1,2)(2,1)\Big)\Big((1,3)(2,3)\Big)\Big((1,4)(2,4)\Big)\Big((3,1)(3,2)\Big)\Big((4,1)(4,2)\Big)\Big((3,4)(4,3)\Big)$$
$\implies Z(\hat{g}_2) = x_1^2 x_2^5$. Analog berechnet man: $Z(\hat{g}_3) = x_2^6$, $Z(\hat{g}_4) = x_3^4$, $Z(\hat{g}_5) = x_4^3$. Also $Z(S_{\underline{4}}^{[2]}) = \frac{1}{4!}(x_1^{12} + 6x_1^2x_2^5 + 3x_2^6 + 8x_3^4 + 6x_4^3)$. POLYA–Substitution:
$$\begin{aligned}Z(S_{\underline{4}}^{[2]}, 1+x) =& \frac{1}{4!}((1+x)^{12} + 6(1+x)^2(1+x^2)^5 + 3(1+x^2)^6 + 8(1+x^3)^4 + 6(1+x^4)^3)\\ =&1 + x + 5x^2 + 13x^3 + 27x^4 + 38x^5 + 48x^6 + 38x^7 + 27x^8 + 13x^9 + 5x^{10}\\ &+ x^{11} + x^{12}.\end{aligned}$$
Wie viel bis auf Isomorphie verschiedene Graphen mit 4 Knoten und 5 Kanten gibt es? Antwort: 38. Fun–fact: Wiederholung der Zahlen wegen Komplementbildung von Graphen.

7 Operationen auf Permutationsgruppen

7.1 Definition. Das *direkte Produkt* $(G, M) \times (H, N)$ zweier Permutationsgruppen $(G, M),\ (H, N)$ ist definiert als $(G \times H, M \times N)$ mit Wirkung

$$(a, b)^{(g,h)} := (a^g, b^h)$$

für $(a, b) \in M \times N,\ (g, h) \in G \times H$. Übung: Nachrechnen, dass dies eine Wirkung definiert!

Andere Wirkung der gleichen abstrakten Gruppe:

7.2 Definition. Die *direkte Summe* $(G, M) \oplus (H, N)$ zweier Permutationsgruppen $(G, M),\ (H, N)$ ist definiert als $(G \times H, M \uplus N)$ mit Wirkung gemäß

$$x^{(g,h)} := \begin{cases} x^g \text{ falls } x \in M, \\ x^h \text{ falls } x \in N \end{cases}$$

für $x \in M \uplus N,\ (g, h) \in G \times H$. Übung: Nachrechnen, dass dies Wirkung ist!

Bemerkung: Falls M und N nicht disjunkt sind, werden sie künstlich disjunkt gemacht mittels $M \uplus N := (M \times \{0\}) \uplus (N \times \{1\})$.

7.3 Satz und Definition. *Es sei G eine (beliebige) Gruppe und (H, N) eine Permutationsgruppe. Dann ist die Menge*

$$G^N \times H = \{(\alpha, h) \mid \alpha : N \to G,\ h \in H\}$$

zusammen mit der Operation $(\alpha', h') \cdot (\alpha'', h'')$ mit $\alpha(i) := \alpha'(i)\alpha''(i^{h'})$ $(i \in N)$ und $h := h'h''$ eine Gruppe, das sogenannte K r a n z p r o d u k t (engl. W r e a t h P r o d u c t) $G \wr (H, N)$ (auch $G \,\mathrm{Wr}\, (H, N)$, $G \wr_N H$).

Beweis. – Assoziativität von $\cdot$: Nachrechnen (Übung!)
– neutrales Element bzgl. $\cdot$: (ε, e_H) mit $\varepsilon : N \to G,\ i \mapsto e_G$
– inverses Element zu $(\alpha, h) \in G^N \times H$: $(\overline{\alpha}, h^{-1})$ mit $\overline{\alpha}(i) := \alpha(i^{h^{-1}})^{-1}$ $(i \in N)$. ■

Darstellung von $(\alpha, h) \in G^N \times H$:

$$\begin{tikzcd} N \arrow[r, "h"] \arrow[d, "\alpha"'] & N \\ G & \end{tikzcd}$$

Produkt:

$$\begin{tikzcd} N \arrow[r, "h'"'] \arrow[rr, bend left, "h"] \arrow[dr, "\alpha'"] \arrow[ddr, bend right, "\alpha"'] & N \arrow[r, "h''"'] \arrow[d, "\alpha''"] & N \\ & G\times G \arrow[d, "\text{Produkt in } G"] & \\ & G & \end{tikzcd}$$

7.4 Definition. Spezialfall: Seien G, H (abstrakte) Gruppen, (H^*, H) rechtsreguläre Darstellung von H (vgl. 2.4, 2.5) durch Rechtsmultiplikation ($h^* : H \to H, x \mapsto xh$).

$$G \wr_r H := G \wr (H^*, H)$$

heißt *reguläres Kranzprodukt* von G und H.

Bemerkung. Sei $N \trianglelefteq G$. Es gibt eine Einbettung $\Phi : G \to N \wr_r ({}^G/_N)$. Wähle dazu Abb. $f : {}^G/_N \to G$, sodass $H = Nf(H)$ für alle $H \in {}^G/_N$ (Repräsentantenauswahl). Definiere nun $\Phi : G \to N \wr_r {}^G/_N$ durch $\Phi(g) := (\alpha_g, Ng)$ $(g \in G)$, $\alpha_g := {}^G/_N \to N, H \mapsto f(H)gf(Hg)^{-1}$. Beobachtung: Nach Wahl von f ist $H = Nf(H)$, also $f(H)g \in Nf(Hg)$ für alle $H \in {}^G/_N$ und $g \in G$. Damit ist α_g wohldefiniert für jedes $g \in G$. Nachrechnen: Φ ist injektiver Gruppenhomomorphismus.

7.5 Satz. *Sei G Gruppe, $H \leq S_N$, $|N| = n$. Dann:*

(a) $|G \wr (H, N)| = |G|^{|N|} \cdot |H| = |G|^n |H|$.

(b) $D := \{\alpha, e_H\} \mid \alpha \in G^N\}$ *ist Normalteiler von $G \wr (H, N)$. Für jedes $i \in N$ ist $D_i := \{(\alpha, e_H) \mid \alpha \in G^N \forall j \in N \backslash \{i\} : \alpha(j) = e_G\}$ Untergruppe von $G \wr (H, N)$ und isomorph zu G. Isomorphismus: $G \ni g \mapsto (\alpha_{i,g}, e_H) \in D_i$ mit*

$$\alpha_{i,g}(j) := \begin{cases} g & \text{, falls } i = j, \\ e_G & \text{, sonst.} \end{cases}$$

Außerdem ist D inneres direktes Produkt der Gruppen $D_1, ..., D_n$ und $G^N \cong D$.

(c) $H^* := \{(\varepsilon, h) \mid h \in H\} \cong H$ *und es gilt $G \wr (H, N) = H^* D$ und $|D \cap H^*| = 1$.*

(d) $\Delta(G) := \{(c_g, e_H) \mid g \in G\} \leq D \leq G \wr (H, N)$ *(mit $c_g : N \to G, i \mapsto g$). Es gilt $\Delta(G) \cong G$ und $|\Delta(G) \cap H^*| = 1$ und $H^* \Delta(G) \cong H \times G$.*

7.6 Definition und Satz. *Das* K r a n z p r o d u k t $(G, N) \wr (H, N)$ *zweier Permutationsgruppen (G, M), (H, N) ist die Wirkung $(G \wr (H, N), M \times N)$ auf dem kartesischen Produkt $M \times N$ gemäß $(a, b)^{(\alpha, h)} := (a^{\alpha(b)}, b^h)$ für $(a, b) \in M \times N$, $(\alpha, h) \in G^N \times H$. Ist $M \neq \emptyset$, dann ist diese Wirkung treu (vgl. 2.1).*

Beweis. Es gilt $(a, b)^{(\varepsilon, e)} = (a^{\varepsilon(b)}, b^{e_H}) = (a, b)$,

$$\left((a, b)^{(\alpha', h')}\right)^{(\alpha'', h'')} = (a^{\alpha(b)}, b^{h'})^{(\alpha'', h'')} = (a^{\alpha'(b)\alpha''(b^{h'})}, b^{h'h''}) \overset{7.3}{=} (a^{\alpha(b)}, b^h) = (a, b)^{(\alpha, h)}$$

für $(\alpha, h) = (\alpha', h')(\alpha'', h'')$. Treue: Sei $(\alpha, h) \in G^N \times H$ mit $(\alpha, h) \neq (\varepsilon, e)$.

1. Fall: $h \neq e \implies \exists b \in N : b^h \neq b$. Wähle $a \in M \neq \emptyset$. Dann $(a, b)^{(\alpha, h)} = (a^{\alpha(b)}, b^h) \neq (a, b)$.
2. Fall: $\alpha \neq \varepsilon \implies \exists b \in N : \alpha(b) \neq e \implies \exists a \in M : a^{\alpha(b)} \neq a \implies (a, b)^{(\alpha, h)} = (a^{\alpha(b)}, b^h) \neq (a, b)$.

■

7.7 Beispiele. (a) Seien M, N (endliche) nicht-leere Mengen. Definiere Äquivalenzrelation

$$\theta := \{((a,b),(a',b')) \in (M \times N)^2 \mid b = b'\}$$

auf $M \times N$. Dann ist $(\operatorname{Aut}\theta, M \times N) \cong (S_M, M) \wr (S_N, N)$ (Ähnlichkeit, vgl. 1.6).

Beweis. Die Wirkung von $S_M \wr (S_N, N)$ auf $M \times N$ gem. 7.6 definiert Homomorphismus

$$\varphi : S_M \wr (S_N, N) \to S_{M\times N},\ (a,b)^{\varphi(\alpha,h,)} := (a,b)^{\alpha,h} \overset{7.6}{=} (a^{\alpha(b)}, b^h).$$

Da die Wirkung treu ist, ist φ injektiv (vgl. 2.1). Zu Zeigen ist: $\mathrm{Im}\varphi = \operatorname{Aut}\theta$

(1) $\mathrm{Im}\varphi \subseteq \operatorname{Aut}\theta$: Für $(\alpha, h) \in (S_M)^N \times S_N$:

$$\begin{aligned}((a,b),(a',b')) \in \theta \iff b = b' &\overset{h\in S_N}{\iff} b^h = (b')^h \\ &\iff ((a,b)^{(\alpha,h)}, (a',b')^{(\alpha,h)}) \in \theta,\end{aligned}$$

d.h. $\varphi(\alpha,h) \in \operatorname{Aut}\theta$.

(2) $\operatorname{Aut}\theta \subseteq \mathrm{Im}\varphi$: Sei $g \in \operatorname{Aut}\theta$. Betrachte

$$\mathrm{pr}_M : M \times N \to M,\ (a,b) \mapsto a,\ \mathrm{pr}_N : M \times N \to M,\ (a,b) \mapsto b.$$

Definiere $\alpha : N \to S_M$ durch

$$a^{\alpha(b)} := \mathrm{pr}_M((a,b)^g)$$

$(a \in M,\, b \in N)$. Sei $b \in N$. Dann ist $\alpha(b) : M \to M$ wirklich eine Permutation: Für $a, a' \in M$ gilt:

$$\begin{aligned} a \neq a' &\iff (a,b) \neq (a',b) \\ &\overset{g\in S_{M\times N}}{\iff} (a,b)^g \neq (a',b)^g \\ &\overset{g\in \operatorname{Aut}\theta}{\iff} \mathrm{pr}_M((a,b)^g) \neq \mathrm{pr}_M((a',b)^g)\end{aligned}$$

$\implies$ $\alpha(b)$ ist injektiv $\overset{M \text{ endlich}}{\implies}$ $\alpha(b) \in S_M$. Wähle nun $a_0 \in M \neq \emptyset$. Definiere $h : N \to N$, $b \mapsto \mathrm{pr}_N((a_0,b)^g)$. Auch h ist Permutation: Für $b, b' \in N$:

$$\begin{aligned} b \neq b' &\iff (a_0,b) \neq (a_0,b') \\ &\iff (a_0,b) \neq (a_0,b')^g \\ &\overset{g\in \operatorname{Aut}\theta}{\iff} \mathrm{pr}_N((a_0,b)^g) \neq \mathrm{pr}_N((a_0,b')^g)\end{aligned}$$

$\implies$ h ist injektiv $\overset{N \text{ endl.}}{\implies}$ $h \in S_N$. Schließlich folgt für alle $(a,b) \in M \times N$:

$$\begin{aligned}(a,b)^g &= (\mathrm{pr}_M((a,b)^g), \mathrm{pr}_N((a,b)^g)) \\ &\overset{g\in \operatorname{Aut}\theta}{=} (a^{\alpha(b)}, \mathrm{pr}_N(a_0,b)^g) \\ &= (a^{\alpha(b)}, b^h) = (a,b)^{\alpha,h}\end{aligned}$$

$\implies$ $\varphi(\alpha,h) = g$. ∎

(b) Seien $\Gamma_0 = (N, \Phi_0)$, $\Gamma_1 = (M, \Phi_1)$ endliche, nichtleere Graphen, definiere Graph $\Gamma := (M \times N, \Phi)$ mit

$$\Phi := \{((a,b),(a',b')) \in (M \times N)^2 \mid (b,b') \in \Phi_0 \vee ((a,a') \in \Phi_1 \wedge b = b')\}.$$

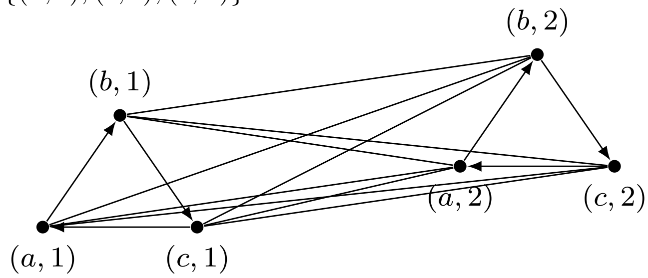
Die Wirkung aus 7.6 definiert einen (injektiven) Homomorphismus $\varphi : \operatorname{Aut}\Gamma_1 \wr (\operatorname{Aut}\Gamma_0, N) \to \operatorname{Aut}\Gamma$.

Beweis. Sei $(\alpha, h) \in (\operatorname{Aut}\Gamma_1)^N \times (\operatorname{Aut}\Gamma_0)$. Wir zeigen: $\varphi(\alpha, h) \in \operatorname{Aut}\Gamma$. Betrachte eine Kante $((a,b),(a',b')) \in \Phi$ in Γ.

– $(b,b') \in \Phi_0 \overset{h \in \operatorname{Aut}\Gamma_0}{\Longleftrightarrow} (b^h, (b')^h) \in \Phi_0 \implies ((a,b)^{(\alpha,h)}, (a',b')^{(\alpha,h)}) \in \Phi.$
– $(a,a') \in \Phi_1 \wedge b = b' \overset{\alpha(b) \in \operatorname{Aut}\Gamma_1}{\Longleftrightarrow} (a^{\alpha(b)}, (a')^{\alpha(b)}) \in \Phi_1 \wedge b^h = (b')^h$
$\implies ((a,b)^{(\alpha,h,)}, (a',b')^{(\alpha,h)}) \in \Phi.$

Also $\varphi(\alpha, h) \in \operatorname{Aut}\Gamma$. ■

Konkret: $\Gamma_0 := (N, (N \times N) \backslash \Delta_N)$ mit $N := \{1, 2\}$ und $\Gamma_1 := (M, \Phi_1)$ mit $M := \{a, b, c\}$, $\Phi_1 := \{(a,b),(b,c),(c,a)\}$. Bild:



Dann gilt: $\operatorname{Aut}\Gamma_0 = S_{\underline{2}}$, $\operatorname{Aut}\Gamma_1 \cong \mathbb{Z}_3$ und $\varphi : H := \operatorname{Aut}\Gamma_1 \wr (\operatorname{Aut}\Gamma_0, N) \to \operatorname{Aut}\Gamma =: G$ ist ein Isomorphismus. Denn:

$$\begin{aligned} |G| =& |(a,1)^G| \cdot |G_{(a,1)}| = G \cdot |(a,2)^{G_{(a,1)}}| \cdot |G_{(a,1),(a,2)}| \\ =& 6 \cdot 3 = 18 = 3^2 \cdot 2 = |\mathbb{Z}_3|^2 \cdot |S_{\underline{2}}| = |H| \end{aligned}$$

und φ ist eine Einbettung nach dem ersten Teil von (b). ■

7.8 Definition und Satz. *Die Exponentiation* $(G, M) \uparrow (H, N)$ *ist die Wirkung* $(G \wr (H, N), M^N)$ *gemäß*

$$f^{(\alpha,h)} := f(b^{h^{-1}})^{\alpha(b^{h^{-1}})}$$

(Kranzprodukt, vgl. 7.3), d.h.

$$f^{(\alpha,h)}(b^h) = f(b)^{\alpha(b)}$$

für alle $(\alpha, h) \in G^N \times H$, $f \in M^N$ *und* $b \in N$. *Diese ist treu, falls* $|M| \geq 2$.

Darstellung von $(\alpha, h) \in G^N \times H$:

$$\begin{tikzcd}
N \arrow[r, "h"] \arrow[d, "\alpha"'] & N \\
G &
\end{tikzcd}$$

Exponentiation:

$$\begin{tikzcd}
N \arrow[rrr, "h"] \arrow[ddd, bend right, "f"'] \arrow[ddd, "\alpha"] & & & N \arrow[ddd, "f^{(\alpha,h)}"] \\
& b \arrow[r, mapsto] \arrow[d, mapsto] & b^h \arrow[d, mapsto] & \\
& (f(b), \alpha(b)) \arrow[r, mapsto] & f(b)^{\alpha(b)} & \\
M \times G \arrow[rrr, "\substack{\text{Wirkung} \\ (b,g) \mapsto b^g}"'] & & & M
\end{tikzcd}$$

Beweis. Es gilt $f^{(\varepsilon,e)} = f(b^e)^{\varepsilon(b^e)} = f^b$,

$$\begin{aligned}
\left(f^{(\alpha',h')}\right)^{(\alpha'',h'')} &= f^{(\alpha',h')}\left(b^{(h'')^{-1}}\right)^{\alpha''\left(b^{(h'')^{-1}}\right)} \\
&= f\left(b^{(h'')^{-1}(g')^{-1}}\right)^{\alpha'\left(b^{(h'')^{-1}}(h')^{-1}\right)\alpha''\left(b^{(h'')^{-1}}\right)} \\
&= f\left(b^{(h'h'')^{-1}}\right)^{\alpha'\left(b^{(h'h'')^{-1}}\right)\alpha''\left(b^{(h'')^{-1}}\right)} \\
&= f\left(b^{h^{-1}}\right)^{\alpha'\left(b^{h^{-1}}\right)\alpha''\left(\left(b^{h^{-1}}\right)^{h'}\right)} \\
&= f\left(b^{h^{-1}}\right)^{\alpha\left(b^{h^{-1}}\right)} = f^{(\alpha,h)}(b)
\end{aligned}$$

für

$$(\alpha, h) \overset{\text{Def.}}{=} \underbrace{(\alpha', h')}_{\in G^N \times H}\underbrace{(\alpha'', h'')}_{\in G^N \times H}. \tag{7.3}$$

Diese Wirkung ist treu (falls $|M| \geq 2$). Denn sei $(\alpha, h) \in G^N \times H$ mit $(\alpha, h) \neq (\varepsilon, e)$.

1. Fall: $h \neq e$. Dann gibt es $b \in N$ mit $b^h \neq b$. Da $|M| \geq 2$, gibt es $f \in M^N$ mit $f(b)^{\alpha(b)} \neq f(b^h)$. Es folgt $f^{(\alpha,h)}(b^h) = f(b)^{\alpha(b)} \neq f(b^h)$ und daher $f^{(\alpha,h)} \neq f$.
2. Fall: $h = e_H$. Dann $\alpha \neq \varepsilon$. Also gibt es $b \in N$ mit $\alpha(b) \neq e_G$. Dann gibt es $a \in M$ mit $a^{\alpha(b)} \neq a$. Setze nun $f : N \to M$, $x \mapsto a$ (konstant). Dann ist $f\underbrace{(\alpha, h)}_{=e} = a^{\alpha(b)} \neq a = f(b)$ und daher $f^{(\alpha,h)} \neq f$.

■

7.9 Bemerkung. Schreibweise von $(\alpha, h) \in G^N \times H = G \wr (H, N)$ in *Tabellenform*, falls $N = \{1, ..., n\}$:

$$((g_1, ..., g_n), h) \text{ mit } g_i := \alpha(i) \in G, \; i = 1, ..., n.$$

Kranzproduktmultiplikation in dieser Schreibweise:

– Einselement: $((e_G, ..., e_G)), e_H)$,
– Inverses von $((g_1, ..., g_n), h)$: $((g_{1^h}^{-1}, ..., g_{n^h}^{-1}), h^{-1})$,

– Multiplikation:

$$((g'_1, ..., g'_n), h') \cdot ((g''_1, ..., g''_n), h'') = ((g'_1 g''_{1^{h'}}, ..., g'_n g''_{n^{h'}}), h'h'')$$

Insbesondere lässt sich jedes Element zerlegen in ein Produkt der Form

$$\begin{aligned}((g_1, ..., g_n), h) =& ((g_1, e, ..., e), e) \cdot ... \cdot ((e, ..., e, g_n), e) \cdot ((e, ..., e), h)\\ =& ((g_1, ..., g_n), e) \cdot ((e, ..., e), h),\end{aligned}$$

vgl. auch 7.5.

7.10 Bemerkung. Für $N = \{1, ..., n\}$. Schreibw. für $f \in M^N$: $f = \overbrace{(f(1), ..., f(n))}^{=:(a_1,...,a_n)} \in M^n$. Die Wirkung der Exponentiation (vgl. 7.8) lässt sich wie folgt beschreiben: Für $(\alpha, h) = ((g_1, ..., g_n), h) = ((g_1, ..., g_n), e_H) \cdot ((e_G, ..., e_G), h) \in G^N \times H$ (Zerlegung wie in 7.9) ist:

– $(a_1, ..., a_n)^{((g_1,...,g_n),e_H)} = (a_1^{g_1}, ..., a_n^{g_n})$,
– $(a_1, ..., a_n)^{((e_G,...,e_G),h)} = (a_1^{h^{-1}}, ..., a_n^{h^{-1}})$,
– $(a_1, ..., a_n)^{(\alpha,h)} = (a_{1^{h^{-1}}}^{g_1^{h^{-1}}}, ..., a_{n^{h^{-1}}}^{g_n^{h^{-1}}})$.

7.11 Beispiel (der n-dimensionale Würfel). Sei $B = \{0, 1\}$, $n \geq 1$. Der *n-dimensionale Würfel* ist der Graph $(B^n, \Phi_1(n))$ mit der Kantenmenge

$$\Phi_1(n) := \{(\boldsymbol{a}, \boldsymbol{b}) \in B^n \times B^n \mid d(\boldsymbol{a}, \boldsymbol{b}) = 1\},$$

wobei $d : B^n \times B^n \to \mathbb{N}$ *Hamming-Metrik*, d.h.

$$d(\boldsymbol{a}, \boldsymbol{b}) := \{i \in \underline{n} \mid a_i \neq b_i\} \ (\boldsymbol{a}, \boldsymbol{b} \in B^n).$$

Mengentheoretische Beschreibung: $N = \{1, ..., n\}$:

$$\begin{array}{ccc}\text{Teilmengen} & \overset{1-1}{\longleftrightarrow} & \text{Elemente von } B^n\\ A \subseteq N & \mapsto & \chi(A) = (a_1, ..., a_n) \text{ mit}\end{array}$$

$$a_i := \begin{cases} 1 & \text{falls } i \in A,\\ 0 & \text{sonst.}\end{cases}$$

Für $A, B \in \mathfrak{P}(N)$ gilt dann: $d(\chi(A), \chi(B)) = |A \Delta B|$, wobei $A \Delta B := (A \cup B) \backslash (A \cap B)$ (*symm. Differenz*). Insbesondere gilt: $d(\chi(A), \chi(B)) = 1 \iff |A \Delta B| = 1$. Für $i \in \{0, ..., n\}$ definieren wir

$$\Phi_i(n) := \{(\boldsymbol{a}, \boldsymbol{b}) \in B^n \times B^n \mid d(\boldsymbol{a}, \boldsymbol{b}) = i\}.$$

Zerlegung: $B^n \times B^n = \biguplus_{i=0}^n \Phi_i(n)$.

7.12 Satz. *Die Automorphismengruppe des n-dimensionalen Würfels:*

$$\mathrm{Aut}\,\Phi_1(n) \cong S_{\underline{2}} \uparrow S_{\underline{n}}.$$

Genauer: $(\mathrm{Aut}\,\Phi_1(n), B^n) \cong (S_{\underline{2}}, B) \uparrow (S_{\underline{n},\underline{n}})$ *(im Sinne von Ähnlichkeit).*

Beweis. Die Wirkung von $S_{\underline{2}} \wr (S_{\underline{n}}, \underline{n})$ auf B^n gemäß 7.8 definiert einen Homomorphismus $\varphi : S_{\underline{2}} \wr (S_{\underline{n}}, \underline{n}) \to S_{B^n}$. Da die Wirkung treu ist (vgl. 7.8), ist φ injektiv (vgl. 2.1). Das heißt: φ induziert einen Isomorphismus von $S_{\underline{2}} \wr (S_{\underline{n}}, \underline{n})$ auf $\varphi(S_{\underline{2}} \wr (S_{\underline{n}}, \underline{n})) = \mathrm{Im}\varphi$. Zu zeigen: $\mathrm{Im}\varphi = \mathrm{Aut}\,\Phi_1(n)$. Zunächst: $\mathrm{Im}\varphi \subseteq \mathrm{Aut}\,\Phi_1(n)$. Sei $(\alpha, h) = ((g_1, ..., g_n), h) \in S_{\underline{2}}^n \times S_{\underline{n}}$

$(\boldsymbol{a}, \boldsymbol{b}) \in \Phi_1(n) \iff \boldsymbol{a}$ und $\boldsymbol{b}$ unterscheiden sich in genau einer Koordinate.

- $\implies (a_1^{g_1}, ..., a_n^{g_n})$ und $(b_1^{g_1}, ..., b_n^{g_n})$ unterscheiden sich in genau einer Koordinate $\iff (\boldsymbol{a}^{((g_1,...,g_n),e)}, \boldsymbol{b}^{((g_1,...,g_n),e)}) \in \Phi_1(n) \implies \varphi(((g_1, ..., g_n), e)) \in \mathrm{Aut}\,\Phi_1(n)$.
- $\implies (a_{1^{h^{-1}}}, ..., a_{n^{h^{-1}}})$ und $(b_{1^{h^{-1}}}, ..., b_{n^{h^{-1}}})$ unterscheiden sich in genau einer Koordinate $\implies \varphi(((e, ..., e), h)) \in \mathrm{Aut}\,\Phi_1(n)$.

Es folgt: $\varphi(\alpha, h) \underset{\text{Hom.}}{\overset{\varphi \text{ ist}}{=}} \varphi(((g_1, ..., g_n), e))\varphi(((e, ..., e), h)) \in \mathrm{Aut}\,\Phi_1(n)$.

7.13 Zwischenbemerkungen. Für $i \in \{0, ..., n\}$ definiere

$$\Gamma_i(\boldsymbol{a}) := \{\boldsymbol{b} \in B^n \mid d(\boldsymbol{a}, \boldsymbol{b}) = i\} \ (\boldsymbol{a} \in B^n).$$

Dann gilt:

$$\Gamma_i(\boldsymbol{a})^f = \Gamma_i(\boldsymbol{a}^f) \text{ für alle } \boldsymbol{a} \in B^n,\ i \in \{0, ..., n\} \text{ und } f \in \mathrm{Aut}\,\Phi_1(n), \qquad (*)$$

$$\{\boldsymbol{b}\} = \bigcap\{\Gamma_1(\boldsymbol{a}) \mid \boldsymbol{a} \in \Gamma_1(\boldsymbol{b}) \cap \Gamma_i(\boldsymbol{0})\}. \qquad (**)$$

Beweis. Übungsaufgabe. Hinweis für $(**)$: „$\subseteq$“ ist klar, „$\supseteq$“ ist einfach für $i \in \{1, ..., n-1\}$, $\boldsymbol{b} \in \Gamma_{i+1}(\boldsymbol{0})$. ■

Nach $(*)$ folgt $\Gamma_1(\boldsymbol{0})^f = \Gamma_1(\boldsymbol{0}^f) = \Gamma_1(\boldsymbol{0})$ für alle $f \in G_{\boldsymbol{0}}$ (von jetzt an ist $G := \mathrm{Aut}\,\Phi_1(n)$), d.h. jedes $f \in G_{\boldsymbol{0}}$ permutiert die Nachbarn von $\boldsymbol{0}$. Wir erhalten eine Abbildung $\psi : G_{\boldsymbol{0}} \to S_N,\ f \mapsto f|_N$, wobei $N := \Gamma_1(\boldsymbol{0}) = \{(1, 0, ..., 0), ..., (0, ..., 0, 1)\}$. Offenbar ist ψ Homomorphismus, außerdem ist ψ surjektiv.

Sei $g \in S_N$. Da die Abbildung $\theta : \{1, ..., n\} \to N,\ i \mapsto (0, ..., 0, 1, 0, ..., 0)$ (1 an der i-ten Stelle) bijektiv ist, können wir ein $h \in S_{\underline{n}}$ durch $i^h := \theta^{-1}(\theta(i)^g)$ $(i \in \underline{n})$ definieren. Es folgt nun für jedes $i \in \underline{n}$:

$$\begin{aligned}(0, ..., 0, \overbrace{1}^{i\text{-te Stelle}}, 0, ..., 0)^g &= \theta(i)^g = \theta(i^h) = (0, ..., 0, \overbrace{1}^{i^h\text{-te Stelle}}, 0, ..., 0)\\ &\overset{7.10}{=} (0, ..., 0, \underbrace{1}_{i\text{-te Stelle}}, 0, ..., 0)^{((e,...,e),h)}.\end{aligned}$$

Also $\overbrace{\varphi(((e, ..., e), h))}^{\in G_0}|_N = g$.

Wir zeigen nun: ψ ist auch injektiv. Es genügt zu zeigen: $\ker\psi = \{e\}$. Dazu sei $f \in \mathrm{Ker}\,\psi$, d.h. $f \in G_{\boldsymbol{0}}$ und $f|_N = \mathrm{id}_N$. Wir zeigen $f|_{\Gamma_i(\boldsymbol{0})} = \mathrm{id}|_{\Gamma_i(\boldsymbol{0})}$ per Induktion über $i \in \{1, ..., n\}$.

(IA) Nach Voraussetzung.
(IS) Gelte $f|_{\Gamma_i(\mathbf{0})} = \mathrm{id}|_{\Gamma_i(\mathbf{0})}$ fur ein $i \in \{1, ..., n-1\}$. Für alle $\boldsymbol{b} \in \Gamma_{i+1}(\mathbf{0})$:

$$\begin{aligned}\{\boldsymbol{b}^f\} = \{\boldsymbol{b}\}^f &\overset{(**)}{=} \bigcap\{\Gamma_1(\boldsymbol{a})^f \mid \boldsymbol{a} \in \Gamma_1(\boldsymbol{b}) \cap \Gamma_i(\mathbf{0})\} \\ &\overset{(*)}{=} \bigcap\{\Gamma_1(\boldsymbol{a}^f) \mid \boldsymbol{a} \in \Gamma_1(\boldsymbol{b}) \cap \Gamma_i(\mathbf{0})\} \\ &\overset{(\mathrm{IV})}{=} \bigcap\{\Gamma_1(\boldsymbol{a}) \mid \boldsymbol{a} \in \Gamma_1(\boldsymbol{b}) \cap \Gamma_i(\mathbf{0})\} \\ &\overset{(**)}{=} \{\boldsymbol{b}\}, \text{ also } \boldsymbol{b}^f = \boldsymbol{b}\end{aligned}$$

$\Longrightarrow f|_{\Gamma_{i+1}(\mathbf{0})} = \mathrm{id}|_{\Gamma_{i+1}(\mathbf{0})}$.

Wegen $B^n = \bigcup_{i=0}^n \Gamma_i(\mathbf{0})$ folgt $f = \mathrm{id}_{B^n}$. Also ist ψ injektiv und damit ein Isomorphismus. Insbesondere gilt: $|G_{\mathbf{0}}| = |S_N| = n!$.

Außerdem: $\boldsymbol{a}^G = B^n$ (d.h. G ist transitiv). Für jedes $(a_1, ..., a_n) \in B^n$ gibt es $g_1, ..., g_n \in S_{\underline{2}}$ mit $a_1 = 0^{g_1}, ..., a_n = 0^{g_n}$ und es folgt $(a_1, ..., a_n) = (0^{g_1}, ..., 0^{g_n}) = (0, ..., 0)^{((g_1, ..., g_n), e)} \in \mathbf{0}^G$.

Finale: Nach 1.14 gilt $|G| = |G_{\mathbf{0}}| \cdot |\mathbf{0}^G| = n! \cdot |B^n| = n! \cdot 2^n$.

Da φ injektiv ist: $|\mathrm{Im}\varphi| = |S_{\underline{2}} \wr (S_{\underline{n}}, \underline{n})| \overset{7.5}{=} 2^n n!$. Wegen $\mathrm{Im}\varphi \subseteq G$ folgt $\mathrm{Im}\varphi = G$. Also: φ ist Isomorphismus von $S_{\underline{n}} \wr (S_{\underline{n}}, \underline{n})$ nach G. ∎

8 Die Sätze von CAUCHY und SYLOW

Erinnerung: Satz von LAGRANGE, vgl. 1.12:

$$G \text{ Gruppe (endlich)}, H \text{ Untergruppe} \implies |G| = H \cdot [G : H],$$

insbesondere $|H| \mid |G|$.

Nahliegende Frage: Gibt es für jede endliche Gruppe G und jeden Teiler $d \mid |G|$ stets eine Untergruppe $H \leq G$ mit $d = |H|$?

Antwort: Nein. Beispiel: A_4 hat keine Untergruppe der Ordnung $6 \mid |A_4| = \frac{|S_4|}{[S_4 : A_4]} = 12$ (Übung).

Bemerkung: Obige Aussage ist allerdings wahr, wenn man zusätzlich voraussetzt dass d Primzahl ist $\longrightarrow$ Satz von CAUSCHY.

Definition. Sei p Primzahl. Eine Gruppe G heißt *p-Gruppe* $:\Longleftrightarrow \exists n \in \mathbb{N} : |G| = p^n$.

Definition. Für eine Gruppenwirkung (G, M) definieren wir

$$\mathrm{Fix}\,(G, M) := \{a \in M \mid \forall g \in G : a^g = a\}$$

(*Menge aller Fixpunkte*).

8.1 Lemma. *Sei (G, M) Gruppenwirkung und G eine p-Gruppe für eine Primzahl p. Dann gilt:*

$$|M| \equiv |\mathrm{Fix}\,(G, M)| \mod p.$$

Beweis. Bemerkung: Für jedes $a \in M$ ist entweder $G_a = G$ und damit $a \in \mathrm{Fix}\,(G, M)$ oder $G_a \neq G$ und daher $p \mid \frac{|G|}{|G_a|} \overset{1.14}{=} |a^G|$. Sei nun T Transversale von 1-Orb$\,(G, M)$. Dann gilt $\mathrm{Fix}\,(G, M) \subseteq T$, und daher

$$|M| = \sum_{a \in T} |a^G| = \underbrace{\sum_{a \in \mathrm{Fix}\,(G,M)} \overbrace{|a^G|}^{=1}}_{=|\mathrm{Fix}\,(G,M)|} + \underbrace{\sum_{a \in T \setminus \mathrm{Fix}\,(G,M)} \overbrace{|a^G|}^{p|\cdot}}_{p|\cdot} \equiv |\mathrm{Fix}\,(G, M)| \mod p.$$

■

8.2 Folgerung. *Sei (G, M) Gruppenwirkung und G p-Gruppe für eine Primzahl p. Dann gilt:*

(1) $p \nmid |M| \implies \mathrm{Fix}\,(G, M) \neq \emptyset$.
(2) $p \mid |M| \implies p \mid |\mathrm{Fix}\,(G, M)|$.

8.3 Definition und Sätzchen. *Sei G Gruppe. Dann ist das Z e n t r u m*

$$Z(G) := \{g \in G \mid \forall h \in G : gh = hg\}$$

von G ein Normalteiler (insbesondere eine Untergruppe) von G.

Beweis. Übungsaufgabe! ■

8.4 Satz. *Sei G p-Gruppe für eine Primzahl p und sei $\{e\} \neq N \trianglelefteq G$. Dann gilt:*

$$p \mid |N \cap Z(G)|$$

(insbesondere $N \cap Z(G) \neq \{e\}$).

Beweis. Wir betrachten die Wirkung (G, N) gegeben durch Konjugation, d.h. $x^g := g^{-1}xg$ $(x \in N,\ g \in G)$. Dies ist tatsächlich eine Wirkung nach 2.7(1). Beobachtung:

$$\begin{aligned} \operatorname{Fix}(G, N) =& \{x \in N \mid \forall g \in G : x^g = x\} \\ =& \{x \in N \mid \forall g \in G : xg = gx\} \\ =& N \cap Z(G). \end{aligned}$$

Mit Lemma 8.1 folgt:

$$|N| \equiv |N \cap Z(G)| \mod p. \tag{$*$}$$

Weil $|N| > 1$ und $|N| \mid |G|$ nach Satz von LAGRANGE (1.12), gilt auch $p \mid |N|$. Daher $p \mid |N \cap Z(G)|$ nach $(*)$. Zur Aussage in Klammern: Da $e \in N \cap Z(G)$ ist $|N \cap Z(G)| \neq \{e\}$. ■

8.5 Folgerung. *Ist p Primzahl und G nicht–triviale p-Gruppe, dann gilt: $p \mid |Z(G)|$ (insbesondere $Z(G) \neq \{e\}$).*

Beweis. Folgt aus 8.4 für $N = G$. ■

8.6 Satz (kleine Anwendung). *Sei p Primzahl. Jede endliche Gruppe der Ordnung p^2 ist abelsch, und daher entweder isomorph zu $\mathbb{Z}_p \times \mathbb{Z}_p$ oder zu $\mathbb{Z}_{p^2}$.*

Der Beweis von 8.6 benötigt folgende Vorüberlegung:

8.7 Lemma. *Sei G Gruppe. Ist die Gruppe ${}^{G}/_{Z(G)}$ zyklisch, so ist G abelsch.*

Beweis. Sei $a \in G$, sodass ${}^{G}/_{Z(G)} = \{Z(G)a^n \mid n \in \mathbb{Z}\}$. Seien $g, h \in G$. Dann gibt es $m, n \in \mathbb{Z}$ und $x, y \in Z(G)$ mit $g = xa^m$ und $h = ya^n$. Es folgt:

$$\begin{aligned} gh \quad &= \quad xa^m ya^n \overset{x,y \in Z(G)}{=} a^m a^n xy = a^{m+n}xy \\ &\overset{x,y \in Z(G)}{=} a^n a^m yx \overset{x,y \in Z(G)}{=} ya^n xa^m = hg. \end{aligned}$$ ■

Beweis von 8.6. Sei G Gruppe mit $|G| = p^2$. Nach 8.5 gilt: $p \mid |Z(G)|$. Wegen Satz von LAGRANGE: $|Z(G)| \mid p^2$. Fallunterscheidung:

1. Fall: $|Z(G)| = p^2 \implies Z(G) = G$, d.h. G abelsch.
2. Fall: $|Z(G)| = p \implies |{}^{G}/_{Z(G)}| \overset{1.12}{=} {}^{|G|}/_{|Z(G)|} = p \implies {}^{G}/_{Z(G)}$ zyklisch $\overset{8.7}{\implies}$ G abelsch, d.h. $Z(G) = G$. Widerspruch.

Also $G = Z(G)$ zyklisch. Rest folgt nach dem Klassifikationssatz über endliche abelsche Gruppen. ■

Nun zum angekündigten Satz:

8.8 Satz (Causchy). *Sei G endliche Gruppe und p Primzahl mit $p \mid |G|$. Dann enthält G ein Element (eine Untergruppe) der Ordnung p.*

Beweis. Betrachte die Wirkung $(\mathbb{Z}_p, G^p)$ gegeben durch

$$(g_0, ..., g_{p-1})^l := (g_l, ..., g_{p-1}, g_0, ..., g_{l-1}) = (g_{l \mod p}, g_{l+1 \mod p}, ..., g_{l+p-1 \mod p})$$

für alle $g_0, ..., g_{p-1} \in G$ und $l \in \mathbb{Z}_p = \{0, ..., p-1\}$. Man sieht leicht, dass $(\mathbb{Z}_p, G^p)$ tatsächlich eine Wirkung ist (Übungsaufgabe). Die Teilmenge

$$M := \{(g_0, ..., g_{p-1}) \in G^p \mid g_0 \cdots g_{p-1} = e\}$$

ist invariant unter dieser Wirkung:

$$\begin{aligned} (g_0, ..., g_{p-1}) \in M &\iff g_0 \cdots g_{p-1} = e \\ &\iff g_l \cdots g_{p-1} = g_{l-1}^{-1} \cdots g_0^{-1} \\ &\iff g_l \cdots g_{p-1} g_0 \cdots g_{l-1} = e \\ &\iff (g_0, ..., g_{p-1})^l \in M. \end{aligned}$$

Da $\mathbb{Z}_p$ eine p-Gruppe ist, können wir Lemma 8.1 auf die (eingeschränkte) Wirkung $(\mathbb{Z}_p, M)$ anwenden und erhalten.

$$|M| = |\mathrm{Fix}\,(\mathbb{Z}_p, M)| \mod p. \tag{$*$}$$

Beobachtung 1: $$\begin{aligned} \mathrm{Fix}\,(\mathbb{Z}_p, M) &= \{(g_0, ..., g_{p-1}) \in M \mid g_0 = ... = g_{p-1}\} \\ &= \{(g, ..., g) \mid g \in G, g^p = e\} \end{aligned}$$

$\implies |\mathrm{Fix}\,(\mathbb{Z}_p, M)| = |\{g \in G \mid g^p = e\}| =: t.$

Beobachtung 2: Die Abbildung $f : G^{p-1} \to M$, $(g_0, ..., g_{p-2}) \mapsto (g_0, ..., g_{p-2}, (g_0 \cdots g_{p-2})^{-1})$ ist eine Bijektion $\implies |M| = |G|^{p-1}$.

Da $p \mid |G|$ folgt $p \mid |M|$ nach Behauptung 2, und daher $p \mid t$ nach $(*)$ und Behauptung 1. Wegen $l^p = l$ ist $t > 0$, und somit $t \geq p \geq 2$. Also enthält G ein Element $g \neq e$ mit $g^p = e$. Es folgt $\mathrm{ord}\,(G) \mid p$ (vgl. ALGZTH) und daher $\mathrm{ord}\,(g) = p$ (da p Primzahl). ∎

8.9 Satz (Anwendung). *Jede (endliche) Gruppe der Ordnung 6 ist entweder isomorph zu $\mathbb{Z}_6$ ($\cong \mathbb{Z}_2 \times \mathbb{Z}_3$) oder isomorph zu S_3.*

Beweis. Sei G Gruppe mit $|G| = 6$. Nach Satz von CAUCHY (8.8) existieren $a, b \in G$ mit $\mathrm{ord}\,(a) = 2$ und $\mathrm{ord}\,(b) = 3$. Fallunterscheidung:

1. Fall: $ab \neq ba$. Nach Satz von LAGRANGE ist $|{}^{G}/_{H}| = 3$ für $H := \langle a \rangle t\{e, a\}$. Nun ist $f : G \to S_{G/H}$ ($\cong S_3$) mit

$$(Hx)^{f(g)} := Hxg$$

$(g, x \in G)$ eine Isomorphismus.

Beweis dazu: f ist Homomorphismus (klar, vgl. 2.4). Wir zeigen, dass f injektiv ist. Sei dazu $g \in \mathrm{Ker}\, f$, d.h. $f(g) = \mathrm{id}_{G/H}$. Dann gilt:

– $Hg = H$, d.h. $g \in H = \{e, a\}$,
– $Hbg = Hb \iff Hbgb^{-1} = H \iff bgb^{-1} \in H \iff g \in b^{-1}Hb = \{e, b^{-1}ab\}$. Da $ab \neq ba$ ist auch $a \neq b^{-1}ab$. Somit: $H \cap b^{-1}Hb = \{e\} \implies g = e$. Also f injektiv $\overset{|G|=6=|S_{G/H}|}{\Longrightarrow}$ f ist Ismomorphismus.

2. Fall: $ab = ba$. Dann folgt $gh = hg$ für alle $g \in \langle a \rangle$ und $h \in \langle b \rangle \implies G$ ist abelsch

$$\underset{\substack{\text{-satz für endl.}\\ \text{abelsche Gruppen}}}{\overset{\text{Klassifikations-}}{\Longrightarrow}} G \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3.$$

■

Bemerkung: Im 2. Fall kann man auch direkt zeigen: $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \to G,\ (k, l) \mapsto a^k b^l$ ist Isomorphismus (Übung).

Wir kommen nun zu einer Verfeinerung des Satzes von CAUCHY: den (drei) Sätzen von SYLOW.

Definition. Sei G endliche Gruppe und p Primzahl. Eine Untergruppe $H \leq G$ heißt:

– *p-Untergruppe* von $G :\iff H$ p-Gruppe,
– *p-Sylow-Untergruppe* von $G :\iff |H| = p^{\nu_p(|G|)}$.

Wir bezeichnen mit:

– $\mathrm{Sub}_p(G)$ die *Menge der p-Untergruppen von G*.
– $\mathrm{Syl}_p(G)$ die *Menge der p-Sylow-Untergruppen von G*.

Wiederholung (aus elementaren Zahlentheorie (1.44) bekannt): Für $n \in \mathbb{N}\backslash\{0\}$ und Primzahl p sei

$$\nu_p(n) := \max\{m \in \mathbb{N} \mid p^m \mid n\}.$$

8.10 Definition und Sätzchen. *Sei G Gruppe und $H \leq G$. Dann heißt $N(H) := N_G(H) := \{g \in G \mid g^{-1}Hg = H\}$ der N o r m a l i s a t o r von H (in G). Es gilt:*

$$H \trianglelefteq N(H) \leq G.$$

Beweis. Übungsaufgabe! ■

8.11 Satz. *Sei G endliche Gruppe, p Primzahl und H p-Untergruppe von G, sodass $p \mid [G : H]$. Dann gilt:*

$$p \mid [N(H) : H].$$

Insbesondere ist $N(H) \neq H$.

Beweis. Betrachte die Wirkung $(H, {}^{G}\!/\!{}_{H})$ gegeben durch $(Hg)^h := Hgh$ $(g \in G,\ h \in H)$. Man sieht leicht, dass dies tatsächlich eine Wirkung ist (vgl. 2.7, Übung). Da H p-Gruppe ist, folgt nach Lemma 8.1:

$$|{}^{G}\!/\!{}_{H}| \equiv |\mathrm{Fix}\,(H, {}^{G}\!/\!{}_{H})| \mod p. \tag{$*$}$$

Beobachtung: Für alle $g \in G$ gilt:

$$\begin{aligned} Hg \in \mathrm{Fix}\,(H, {}^{G}\!/\!{}_{H}) &\iff \forall h \in H : Hgh = Hg \\ &\iff \forall h \in H : ghg^{-1} \in H \\ &\iff gHg^{-1} = H \iff g^{-1}Hg = H \\ &\iff g \in N(H). \end{aligned}$$

Daher: $|\mathrm{Fix}\,(H, {}^{G}\!/\!{}_{H})| = |\{Hg \mid g \in N(H)\}| = |{}^{N(H)}\!/\!{}_{H}| = [N(H) : H]$. Aus $(*)$ ergibt sich damit:

$$[G : H] \equiv [N(H) : H] \mod p. \tag{$**$}$$

Nach Voraussetzung des Satzes: $p \mid [G : H]$. Daher $p|[N(H) : H]$ nach $(**)$. Zur letzten Aussage:

$$p \mid [N(H) : H] > 0 \implies [N(H) : H] \geq p \geq 2 \implies N(H) \neq H.$$

■

8.12 Folgerung. *Sei G p-Gruppe für eine Primzahl p. Ist $H \leq G$ und $[G : H] = p$, dann ist $H \trianglelefteq G$.*

Wiederholung aus ALGZTH (5.32): *Ist G Gruppe und $U \leq V \leq G$, dann gilt:*

$$[G : U] = [G : V][V : U].$$

Beweis. Übungsaufgabe! ■

Beweis von Folgerung 12. Nach Formel oben:

$$[G : H] = [G : N(H)][N(H) : H].$$

Ist $[G : H] = p$, dann $p \mid [N(H) : H]$ nach Satz 8.11 und daher $[G : N(H)] = 1$, also $N(H) = G$. D.h. $H \overset{8.10}{\trianglelefteq} N(H) = G$. ■

8.13 Satz. *Sei G endliche Gruppe, p Primzahl, $H \in \mathrm{Sub}_p(G)$ mit $p \mid [G : H]$ ($\iff$ $|H| < p^{\nu_p(|G|)}$). Dann gibt es $H' \leq G$ mit $H \leq H'$ und $|H'| = |H| \cdot p$.*

Beweis. Nach 8.10 ist $H \trianglelefteq N(H)$. Betrachte die Gruppe ${}^{N(H)}\!/\!{}_{H}$. Nach Satz 8.11:

$$p \mid [N(H) : H] = |{}^{N(H)}\!/\!{}_{H}|.$$

Nach Satz von CAUCHY (8.8):

$$\exists K \leq {}^{N(H)}/_{H} : |K| = p.$$

Betrachte den Homomorphismus

$$\pi : N(H) \to {}^{N(H)}/_{H}, \; g \mapsto Hg.$$

Dann ist $H' := \pi^{-1}(K)$ Untergruppe von $N(H)$ und somit von G. Weiter:

$$|H'| = |\pi^{-1}(K)| = |\biguplus_{k \in K} \pi^{-1}(k)| = \sum_{k \in K} \underbrace{|\pi^{-1}(k)|}_{=|H|} = |K||H| = p|H|.$$

Offenbar $H = \operatorname{Ker} \pi \subseteq \pi^{-1}(K) = H'$. ■

8.14 Folgerung. *Sei G endliche Gruppe und $H \in \mathrm{Sub}_p(G)$ für eine Primzahl p. Sei $m := \nu_p(|H|)$ (d.h. $|H| = p^m$) und $n := \nu_p(|G|)$. Dann gibt es eine Kette von Untergruppen $H = H_m \leq H_{m+1} \leq ... \leq H_n \leq G$, sodass $|H_i| = p^i$ für jedes $i \in \{m, ..., n\}$.*

Beweis. Induktion Über $i \in \{m, ..., n\}$:

Induktionsanfang: Fall $i = m$ ist klar.
Induktionsschritt: Sei $i \in \{m, ..., n-1\}$ und seien $H = H_m \leq H_{m+1} \leq ... \leq H_i \leq G$, sodass $|H_j| = p^j$ für jedes $j \in \{m, ..., i\}$. Dann $|H_i| = p^i < p^n = p^{\nu_p(|G|)}$. Nach Satz 8.13 gibt es $H_{i+1} \leq G$ mit $H_i \leq H_{i+1}$ und $|H_{i+1}| = |H_i| \cdot p = p^{i+1}$. ■

8.15 Satz (SYLOW I). *Sei G endliche Gruppe und p eine Primzahl. Dann gilt:*

(a) *Jede p-Untergruppe von G ist in einer p-Sylow-Untergruppe von G enthalten. Insbesondere ist $\mathrm{Syl}_p(G) \neq \emptyset$.*
(b) *$\mathrm{Syl}_p(G) = \max(\mathrm{Sub}_p(G), \subseteq)$, d.h. die p-Sylow-Untergruppen von G sind genau die maximalen p-Untergruppen von G.*

Beweis. Zu (a): Erste Aussage folgt unmittelbar aus Folgerung 8.14. Zur zweiten Aussage in (a): Da $\{e\}$ (trivialerweise) p-Untergruppe von G ist, besitzt G nach erster Aussage von (a) eine p-Sylow-Untergruppe (die $\{e\}$ enthält).
(b) folgt direkt aus (a). ■

Definition. Sei G Gruppe. Zwei Untergruppen $U, V \leq G$ heißen *konjugiert* $:\Longleftrightarrow \exists g \in G : g^{-1}Ug = V$.

8.16 Satz (SYLOW II). *Sei G endliche Gruppe, p Primzahl. Dann sind je zwei p-Sylow-Untergruppen von G konjugiert.*

Beweis. Seien $H, K \in \mathrm{Sub}_p(G)$. Betrachte die Wirkung $(H, {}^{G}\!/\!_{K})$ gegeben durch

$$(Kg)^h := Kgh$$

$(g \in G,\ h \in H)$. Da K p-Sylow-Untergruppe von G ist:

$$p \nmid \frac{|G|}{|K|} \overset{\text{LAGR.}}{=} [G:K] = |{}^{G}\!/\!_{K}|.$$

Da H p-Gruppe ist, können wir Folgerung 8.12 anwenden, und schließen: $\mathrm{Fix}\,(H, {}^{G}\!/\!_{K}) \neq \emptyset$. Sei $g \in G$ mit $Kg \in \mathrm{Fix}\,(H, {}^{G}\!/\!_{K})$, d.h. $Kgh = Kg$ für alle $h \in H$. Dann $ghg^{-1} \in K$ für alle $h \in H$. Also $gHg^{-1} \subseteq K$. Weiter:

$$|H| = |gHg^{-1}| \leq |K| = |H| \implies gHg^{-1} = K.$$

■

8.17 Folgerung. *Sei G endliche Gruppe und p Primzahl. Dann sind folgende Aussagen äquivalent:*

(a) $|\mathrm{Syl}_p(G)| = 1$.
(b) $\exists H \in \mathrm{Syl}_p(G) : H \trianglelefteq G$.
(c) $\forall H \in \mathrm{Syl}_p(G) : H \trianglelefteq G$.

Beweis. Die Menge $\mathrm{Syl}_p(G)$ ist abgeschlossen unter Konjugation, d.h. $\forall H \in \mathrm{Syl}_p(G)$ $\forall g \in G : g^{-1}Hg \in \mathrm{Syl}_p(G)$. Daher gilt: (a) $\implies$ (c). Klar: (c) $\implies$ (b), da $\mathrm{Syl}_p(G) \neq \emptyset$ nach Satz 8.15. Außerdem: (b) $\implies$ (a) nach Satz 8.16. ■

8.18 Satz (SYLOW III). *Sei G endliche Gruppe und p Primzahl. Dann gilt:*

(a) $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$.
(b) *Ist H p-Sylow-Untergruppe von G, dann gilt:*

$$|\mathrm{Syl}_p(G)| = [G : N(H)] \mid [G : H] = \frac{|G|}{p^{\nu_p(|G|)}}.$$

Beweis. Betrachte die Wirkung $(G, \mathrm{Syl}_p(G))$ gegeben durch $H^g := g^{-1}Hg$ $(H \in \mathrm{Syl}_p(G),\ g \in G)$.

Zu (a): Sei $P \in \mathrm{Syl}_p(G)$ ($\neq \emptyset$ nach Satz 8.15, SYLOW I). Da P p-Gruppe ist, können wir Lemma 8.1 auf die eingeschränkte Wirkung $(P, \mathrm{Syl}_p(G))$ anwenden und erhalten:

$$|\mathrm{Syl}_p(G)| \equiv |\mathrm{Fix}\,(P, \mathrm{Syl}_p(G))| \mod p.$$

Wir zeigen: $\mathrm{Fix}\,(P, \mathrm{Syl}_p(G)) = \{P\}$. Offenbar: $P \in \mathrm{Fix}\,(P, \mathrm{Syl}_p(G))$, da $g^{-1}Pg = P$ für alle $g \in P$. Sei $H \in \mathrm{Fix}\,(P, \mathrm{Syl}_p(G))$. Dann $g^{-1}Hg = H$ für alle $g \in P$ und daher $P \subseteq N(H)$. Da nun $H \leq N(H) \leq G$, folgt $|H| \mid |N(H)|$ und $|N(H)| \mid |G|$ nach Satz von LAGRANGE. Somit $\nu_p(|G|) \geq \nu_p(|N(H)|) \geq \nu_p(|H|) = \nu_p(|P|) = \nu_p(|G|)$. Es folgt: $P, H \in \mathrm{Syl}_p(N(H))$. Nach Satz 8.16, SYLOW II sind P und H konjugiert in $N(H)$, d.h. es gibt $g \in N(H)$ mit $P = g^{-1}Hg \overset{g \in N(H)}{=} H$. Das zeigt die Behauptung. Aus $(*)$ folgt: $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$.

Zu (b): Nach Satz 8.16, SYLOW II ist $(G, \mathrm{Syl}_p(G))$ transitiv. Sei $H \in \mathrm{Syl}_p(G)$. Dann gilt:
$$G_H = \{g \in G \mid g^{-1}Hg = H\} = N(H).$$
Daher $|G| \overset{1.14}{=} |H^G| \cdot |G_H| = |\mathrm{Syl}_p(G)| \cdot |N(H)|$. Es folgt:
$$|\mathrm{Syl}_p(G)| = \frac{|G|}{|N(H)|} \overset{\text{LAGR.}}{[G : N(H)]}.$$
Letzte Aussage: $|\mathrm{Syl}_p(G)| \cdot [N(H) : H] = [G : N(H)] \cdot [N(H) : H] \overset{\text{ALGZTH}}{=} [G : H]$. Also $|\mathrm{Syl}_p(G)| = [G : N(H)] \mid [G : H] \overset{\text{LAGR.}}{=} \frac{|G|}{|H|} = \frac{|G|}{p^{\nu_p(|G|)}}$. ■

8.19 Satz. *Sei G endliche Gruppe und seien p und q verschiedene Primzahlen mit $|\mathrm{Syl}_p(G)| = 1 = |\mathrm{Syl}_q(G)|$. Dann kommutiert jedes Element der p-Sylow-Untergruppe von G mit jedem Element der q-Sylow-Untergruppe von G.*

Beweis. Sei P die p-Sylow-Untergruppe von G und Q die q-Sylow-Untergruppe von G. Da $P \cap Q$ sowohl Untergruppe von P als auch von Q ist, folgt $|P \cap Q| \mid |P|$ und $|P \cap Q| \mid |Q|$ nach Satz von LAGRANGE. Da $|P|$ und $|Q|$ teilerfremd sind, ist $|P \cap Q| = 1$, d.h. $P \cap Q = \{e\}$. Nach Folgerung 8.17 sind P und Q Normalteiler von G. Für $g \in P$, $h \in Q$ folgt:
$$\underbrace{g^{-1}\overbrace{h^{-1}gh}^{\in P}}_{\in Q} \in P \cap Q \implies g^{-1}h^{-1}gh = e, \text{ d.h. } gh = hg.$$
■

8.20 Satz. *Sei G endliche Gruppe, $p_1, ..., p_n$ seien die paarweise verschiedene Primteiler von $|G|$. Gilt $\mathrm{Syl}_{p_i}(G) = \{P_i\}$ für jedes $i \in \{1, ..., n\}$, dann ist die Abbildung*
$$\varphi : P_1 \times ... \times P_n \to G, \ (g_1, ..., g_n) \mapsto g_1 \cdots g_n$$
ein Gruppenisomorphismus.

Vorbemerkung zum Beweis. *Sei G endliche Gruppe und seien $g_1, ..., g_n \in G$, sodass $g_ig_j = g_jg_i$ und $\mathrm{ggT}(\mathrm{ord}(g_i), \mathrm{ord}(g_j)) = 1$ für je zwei $i, j \in \{1, ..., n\}$ mit $i \neq j$. Dann gilt:*
$$\mathrm{ord}(g_1 \cdots g_n) = \mathrm{ord}(g_1) \cdots \mathrm{ord}(g_n).$$

Beweis. Sei $m_1 := \mathrm{ord}(g_1), ..., m_n := \mathrm{ord}(g_n)$, $m := m_1 \cdots m_n$. Dann $(g_1 \cdots g_n)^m \overset{\text{komm.}}{=} g_1^m \cdots g_n^m \overset{m_i | m}{=} e$. Daher $k := \mathrm{ord}(g_1 \cdots g_n) \mid m$. Für $i \in \{1, ..., n\}$:
$$\begin{aligned} e &= (g_1 \cdots g_n)^{km_1 \cdots m_{i-1}m_{i+1} \cdots m_n} \\ &\overset{\text{komm}}{=} g_1^{km_1 \cdots m_{i-1}m_{i+1} \cdots m_n} \cdots g_n^{km_1 \cdots m_{i-1}m_{i+1} \cdots m_n} \\ &= g_i^{km_1 \cdots m_{i-1}m_{i+1} \cdots m_n} \end{aligned}$$
$\implies m_i \mid km_1 \cdots m_{i-1}m_{i+1} \cdots m_n \underset{\text{teilerfremd}}{\overset{m_1,...,m_n}{\implies}} m_i \mid k$. Nochmal Teilerfremdheit liefert: $m = m_1 \cdots m_n \mid k$. Also $m = k$. ■

Beweis von Satz 8.20. φ ist Homomorphismus:

$$\begin{aligned}\varphi((g_1,...,g_n)(h_1,...,h_n)) =& \varphi((g_1h_1,...,g_nh_n))\\ =& g_1h_1\cdots g_nh_n \overset{8.19}{=} g_1\cdots g_nh_1\cdots h_n\\ =& \varphi((g_1,...,g_n))\cdot((h_1,...,h_n))\end{aligned}$$

für alle $(g_1,...,g_n),\ (h_1,...,h_n) \in P_1 \times ... \times P_n$.

Injektivität von φ: Sei $(g_1,...,g_n) \in \operatorname{Ker}\varphi$. Für $i \in \{1,...,n\}$: $\operatorname{ord}(g_i) \mid |P_i|$ (Satz von LAGRANGE),

$$\begin{aligned}\operatorname{ord}(g_i) &\overset{g_1\cdots g_n=e}{=} \operatorname{ord}(g_1^{-1}\cdots g_{i-1}^{-1}g_{i+1}^{-1}\cdots g_n^{-1})\\ &\underset{\&\ 8.19}{\overset{\text{Vorbem.}}{=}} \operatorname{ord}(g_1^{-1})\cdots\operatorname{ord}(g_{i-1}^{-1})\operatorname{ord}(g_{i+1}^{-1})\cdots\operatorname{ord}(g_n^{-1}) \mid |P_1|\cdots|P_{i-1}||P_{i+1}|\cdots|P_n|\end{aligned}$$

(Satz von LAGRANGE) $\underset{\text{teilerfremd}}{\overset{|P_1|,...,|P_n|}{\Longrightarrow}}$ $\operatorname{ord}(g_i) = 1$, d.h. $g_i = e$. Das zeigt: $(g_1,...,g_n) = (e,...,e)$. Also ist φ injektiv.

Surjektivität von φ:

$$|P_1 \times ... \times P_n| = |P_1|\cdots|P_n| = p_1^{\nu_{p_1}(|G|)}\cdots p_n^{\nu_{p_n}(|G|)} = |G|$$

$\underset{\text{injektiv}}{\overset{\varphi\text{ ist}}{\Longrightarrow}}$ $G = \varphi(P_1 \times ... \times P_n)$.

Somit ist φ ein Isomorphismus. ■

8.21 Satz (Anwendung). *Seien p und q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede (endliche) Gruppe der Ordnung $p \cdot q$ zyklisch.*

Beweis. Sei G Gruppe mit $|G| = p \cdot q$. Nach Satz 8.18 (SYLOW III):

$$|\operatorname{Syl}_p(G)| \mid \frac{|G|}{p} = q$$

(Teil (b), 8.18). Wäre nun $|\operatorname{Syl}_p(G)| = q$, dann $q \equiv 1 \mod p$ nach Teil (a) von 8.18, also $p \mid (q-1)$. Widerspruch. Also ist $|\operatorname{Syl}_p(G)| = 1$. Analog: Nach 8.18, Teil (a): $|\operatorname{Syl}_q(G)| \mid \frac{|G|}{q} = p$. Wäre $|\operatorname{Syl}_q(G)| = p$, dann $p \equiv 1 \mod q$ nach Teil (a) von 8.18, daher $q \mid (p-1)$. Widerspruch zu $p < q$. Also $|\operatorname{Syl}_q(G)| = 1$. Sei nun $\operatorname{Syl}_p(G) = \{P\}$ und $\operatorname{Syl}_q(G) = \{Q\}$. Nach 8.20:

$$G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong Z_{pq}.$$

Daher ist G zyklisch (letzte Isomorphie wegen Teilerfremdheit von p und q). ■

8.22 Satz (Anwendung). *Seien p und q Primzahlen mit $p < q$ und $p \nmid (q-1)$. Dann ist jede Gruppe der Ordnung p^2q abelsch.*

Beweis. Sei G Gruppe mit $|G| = p^2 q$. Nach 8.18: $|\mathrm{Syl}_p(G)| \mid \frac{|G|}{p^2} = q$. Es folgt wie oben (Beweis von 8.21): $|\mathrm{Syl}_p(G)| = 1$. Nach 8.18, Teil (b): $|\mathrm{Syl}_q(G)| \mid \frac{|G|}{q} = p^2$. Fallunterscheidung:

(1) $|\mathrm{Syl}_q(G)| = p \underset{\text{Teil (a)}}{\overset{8.18}{\Longrightarrow}} p \equiv 1 \mod q \iff q \mid (p-1)$. Widerspruch.

(2) $$\begin{aligned} |\mathrm{Syl}_q(G)| = p^2 &\underset{\text{Teil (a)}}{\overset{8.18}{\Longrightarrow}} p^2 \equiv 1 \mod q \\ &\iff q \mid (p^2-1) = (p+1)(p-1) \\ &\iff q \mid (p+1) \vee q \mid (p-1). \end{aligned}$$

Widerspruch.

Also $|\mathrm{Syl}_p(G)| = 1$. Sei $\mathrm{Syl}_p(G) = \{P\}$ und $\mathrm{Syl}_q(G) = \{Q\}$. Da $|Q| = q$ Primzahl ist, ist $Q \cong \mathbb{Z}_q$ zyklisch (insbesondere abelsch). Da $|P| = p^2$, ist P abelsch nach 8.6. Nach 8.20: $G \cong P \times Q$ ist abelsch. ■

Die SYLOW-Sätze werden häufig so verwendet: Einen Satz (den man für alle endliche Gruppen beweisen möchte) zeigt man zunächst für p-Gruppen und schließt dann (mithilfe der SYLOW-Sätze) auf die allgemeine Situation. Es folgen zwei Beispiele für dieses Vorgehen.

8.23 Satz. *Sei G endliche Gruppe. Gilt $|\{H \leq G \mid |H| = d\}| \leq 1$ für jeden Teiler $d \mid |G|$, dann ist G Zyklisch.*

Beweis. Schritt 1: Sei G p-Gruppe für eine Primzahl p. Sei $g \in G$ mit $\mathrm{ord}\,(g) = \max\{\mathrm{ord}\,(h) \mid h \in G\}$. Zu zeigen: $G = \langle g \rangle$. Sei dazu $h \in G$. Nach dem Satz von LAGRANGE: $\exists m, n \in \mathbb{N} : \mathrm{ord}\,(g) = p^m$, $\mathrm{ord}\,(h) = p^n$. Maximalität: $p^n \leq p^m$, also $p^n \mid p^m = |\langle g \rangle|$. Dann hat $\langle g \rangle$ eine Untergruppe der Ordnung p^n (nämlich explizit $\langle g^{p^{m-n}} \rangle$—Übung, oder nach Folgerung 8.14). Auch $\langle h \rangle$ hat die Ordnung p^n. Also stimmen diese beiden Untergruppen nach Voraussetzung überein. Somit $\langle h \rangle \subseteq \langle g \rangle$. D.h. $h \in \langle g \rangle$.

Schritt 2: Seien $p_1, ..., p_n$ die paarweise verschiedene Primteiler von $|G|$. Nach Voraussetzung: $|\mathrm{Syl}_{p_i}(G)| = 1$ für jedes $i \in \{1, ..., n\}$. Sei $i \in \{1, ..., n\}$ und $\mathrm{Syl}_{p_i}(G) = \{P_i\}$. Nach Schritt 1: P_i ist zyklisch, d.h. $P_i = \langle g_i \rangle$ für ein $g_i \in P_i$ und daher $\mathrm{ord}\,(g_i) = |P_i| = p_i^{\nu_{p_i}}(|G|)$. Nach Satz 8.20:

$$\begin{aligned} G \cong P_1 \times ... \times P_n &\overset{\text{Schritt 1}}{\cong} \mathbb{Z}_{p_1^{\nu_{p_1}(|G|)}} \times ... \times \mathbb{Z}_{p_n^{\nu_{p_n}(|G|)}} \\ &\overset{\text{teilerfr.}}{\cong} \mathbb{Z}_{p_1^{\nu_{p_1}(|G|)} \cdots p_n^{\nu_{p_n}(|G|)}}. \end{aligned} \qquad (■)$$

Anderes Argument: Nach 8.19 ist $g_i g_j = g_j g_i$ für $i, j \in \{1, ..., n\}$, $i \neq j$. Nach Vorbemerkung zum Beweis von Satz 8.20:

$$\mathrm{ord}\,(g_1 \cdots g_n) = \mathrm{ord}\,(g_1) \cdots \mathrm{ord}\,(g_n) = p_1^{\nu_{p_1}(|G|)} \cdots p_n^{\nu_{p_n}(|G|)} = |G|$$

$\Longrightarrow$ G ist zyklisch. ■

8.24 Satz. *Sei G endliche Gruppe. Gilt $|\{x \in G \mid x^n = e\}| \leq n$ für jeden Teiler $n \mid |G|$, dann ist G zyklisch.*

Beweis. Schritt 1: Sei G p-Gruppe für eine Primzahl p. Sei $g \in G$ mit $\operatorname{ord}(g) = \max\{\operatorname{ord}(h) \mid h \in G\}$. Für alle $h \in \langle g \rangle$ ist $h^{\operatorname{ord}(g)} = e$ (da $\operatorname{ord}(h) \mid \operatorname{ord}(g)$ nach dem Satz von LAGRANGE). Nach Voraussetzung (für $n := \operatorname{ord}(g) = |\langle g \rangle|$):

$$\{x \in G \mid x^{\operatorname{ord}(g)} = e\} = \langle g \rangle. \tag{$*$}$$

Für jedes $h \in G$ ist $\operatorname{ord}(h)$ eine p-Potenz (da G eine p-Gruppe ist) und $\operatorname{ord}(h) \leq \operatorname{ord}(g)$. Daher $\operatorname{ord}(h) \mid \operatorname{ord}(g)$, also $h^{\operatorname{ord}(g)} = e \overset{(*)}{\Longrightarrow} h \in \langle g \rangle$. Also ist $H = \langle g \rangle$ zyklisch.

Schritt 2: Sei p Primteiler von $|G|$, $P \in \operatorname{Syl}_p(G)$. Dann $g^{|P|} = e$ für jedes $g \in P$. Nach Voraussetzung:

$$\{x \in G \mid x^{|P|} = e\} = P. \tag{$**$}$$

Sei $P' \in \operatorname{Syl}_p(G)$. Dann $g^{|P|} = g^{|P'|} = e$ und daher nach $(**)$: $g \in P$ für jedes $g \in P'$. Also $P' \subseteq P$ und somit $P' = P$ (da $|P'| = p^{\nu_p(|G|)} = |P|$). Das Zeigt: $|\operatorname{Syl}_p(G)| = 1$. Rest wie letzter Teil im Schritt 2 im Beweis von 8.23. Erinnerung:

$$\begin{aligned} G \overset{8.20}{\cong} P_1 \times \ldots \times P_n &\overset{\text{Schritt 1}}{\cong} \mathbb{Z}_{p_1^{\nu_{p_1}(|G|)}} \times \ldots \times \mathbb{Z}_{p_n^{\nu_{p_n}(|G|)}} \\ &\overset{\text{teilerfr.}}{\cong} \mathbb{Z}_{p_1^{\nu_{p_1}(|G|)} \cdots p_n^{\nu_{p_n}(|G|)}} = \mathbb{Z}_{|G|}. \end{aligned}$$

■

9 Einfache Gruppen

9.1 Definition und Sätzchen. *Sei G Gruppe.*

$$\begin{aligned} G \text{ ist } e\,i\,n\,f\,a\,c\,h &:\Longleftrightarrow \{e\} \text{ und } G \text{ sind die einzigen Normalteiler von } G \\ &\overset{\text{Übung}^3}{:\Longleftrightarrow} \forall H\, \text{Gruppe} \forall h : G \to H\, \text{Homomorphismus}: \\ &\qquad h \text{ ist injektiv oder konstant.} \end{aligned}$$

9.2 Bemerkungen. (1) *Für endliche abelsche Gruppe G gilt:*

$$\begin{aligned} G \text{ ist einfach } &\Longleftrightarrow \{e\} \text{ und } G \text{ sind die einzigen Untergruppen von } G \\ &\Longleftrightarrow^4 |G| = 1 \text{ oder } |G| \text{ ist eine Primzahl} \\ &\Longleftrightarrow^5 |G| = 1 \text{ oder } G \cong \mathbb{Z}_p \text{ für eine Primzahl } p. \end{aligned}$$

(2) **Klassifikationssatz.**[6] *Jede nicht-triviale endliche einfache Gruppe ist isomorph zu einer der folgenden:*

- *zyklische Gruppen $\mathbb{Z}_p$ für $p \in \mathbb{P}$,*
- *alternierende Gruppen A_n für $n \geq 5$,*
- *einfache Gruppen vom Lie-Typ über einem endlichen Körper,*
- 26 *sporadische Gruppen.*

Einfache Gruppen bilden „Bausteine" der endlichen Gruppen.

9.3 Satz. *Sei G endliche Gruppe. Dann existiert Kette von Untergruppen:*

$$\{e\} = G_0 \mathrel{\ntrianglelefteq} G_1 \mathrel{\ntrianglelefteq} ... \mathrel{\ntrianglelefteq} G_{n-1} \mathrel{\ntrianglelefteq} G_n = G,$$

sodass G_i/G_{i-1} einfach ist für jedes $i \in \{1,..,n\}$.

Beweis. Da G endlich ist, ist $n := \sup\{m \in \mathbb{N} \mid \exists \{e\} \neq G_1 \mathrel{\ntrianglelefteq} G_2 \mathrel{\ntrianglelefteq} ... \mathrel{\ntrianglelefteq} G_{m-1} \mathrel{\ntrianglelefteq} G\} < \infty$. Sei $\{e\} = G_0 \mathrel{\ntrianglelefteq} G_1 \mathrel{\ntrianglelefteq} ... \mathrel{\ntrianglelefteq} G_{n-1} \mathrel{\ntrianglelefteq} G_n = G$. Behauptung: $\forall i \in \{1,...,n\}$: G_i/G_{i-1} einfach. Sei $i \in \{1,...,n\}$. Annahme: G_i/G_{i-1} nicht einfach. Dann:

$$\exists N \mathrel{\ntrianglelefteq} G_i/G_{i-1} : N \neq \{e_{G_i/G_{i-1}}\} = \{G_{i-1}\}.$$

Dann $\pi^{-1}(N) \mathrel{\ntrianglelefteq} G_i$ (sonst $N = \pi(\pi^{-1}(N)) = \pi(G_i) = G_i/G_{i-1}$ und $G_{i-1} = \operatorname{Ker} \pi \mathrel{\ntrianglelefteq} \pi^{-1}(N)$). Also:

$$\{e\} = G_0 \mathrel{\ntrianglelefteq} G_1 \mathrel{\ntrianglelefteq} ... \mathrel{\ntrianglelefteq} G_{i-1} \mathrel{\ntrianglelefteq} \pi^{-1}(N) \mathrel{\ntrianglelefteq} G_i \mathrel{\ntrianglelefteq} ... \mathrel{\ntrianglelefteq} G_{n-1} \mathrel{\ntrianglelefteq} G_n = G.$$

Diese Kette hat ein Glied mehr als die ursprüngliche. Widerspruch zur Definition von n. Daher ist G_i/G_{i-1} einfach. ■

[3] Hinweis: Für eine Richtung den Kern anschauen, für die andere Richtung Faktorgruppe benutzen.
[4] Hinweis: Eine Richtung mit dem Satz von LAGRANGE (1.12), die andere mit dem Satz von CAUCHY (8.8.)
[5] Hinweis: Beweis mit dem Klassifikationssatz oder direkt.
[6] Fun Fact: Letzte Lücke im Beweis wurde 2002 geschlossen.

Die entstehenden Faktoren ${}^{G_i}/_{G_{i-1}}$ ($i \in \{1, ..., n\}$) sind (bis auf Isomorphie und Permutation der Reihenfolge) eindeutig bestimmt:

9.4 Satz (Jordan-Hölder). *Sei G endliche Gruppe. Sind*

$$\begin{aligned}\{e\} = & G_0 \underset{\neq}{\trianglelefteq} G_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} G_{n-1} \underset{\neq}{\trianglelefteq} G_n = G,\\ \{e\} = & H_0 \underset{\neq}{\trianglelefteq} H_1 \underset{\neq}{\trianglelefteq} ... \underset{\neq}{\trianglelefteq} H_{m-1} \underset{\neq}{\trianglelefteq} H_m = G,\end{aligned}$$

sodass $\forall i \in \{1, ..., n\}$: ${}^{G_i}/_{G_{i-1}}$ einfach und $\forall j \in \{1, ..., m\}$: ${}^{H_j}/_{H_{j-1}}$ einfach, dann gilt: $m = n$ und es gibt $\pi \in S_{\underline{n}}$ mit

$$\forall i \in \{1, ..., n\} : {}^{G_i}/_{G_{i-1}} \cong {}^{H_{i^\pi}}/_{H_{i^\pi - 1}}.$$

Beweis. Eventuell später. ∎

Nächstes Ziel: Einfachheit alternierender Gruppen.

9.5 Lemma. *Sei $n \in \mathbb{N}$ mit $n \geq 3$. Die Gruppe $A_{\underline{n}}$ wird erzeugt von der Menge*

$$E := \{(a\ b\ c) \mid a, b, c \in \underline{n},\ |\{a, b, c\}| = 3\}.$$

Beweis. Zunächst: $E \subseteq A_{\underline{n}}$. Denn: $(a\ b\ c)(b\ a) = (a)(b\ c)$, daher

$$\begin{aligned}\operatorname{sgn}((a\ b\ c)) &= \operatorname{sgn}((a\ b\ c)(b\ a)(b\ a))\\ &\underset{\text{Homom.}}{\overset{\text{sgn}}{=}} \underbrace{\operatorname{sgn}((a\ b\ c)(b\ a))}_{=-1} \cdot \underbrace{\operatorname{sgn}((b\ a))}_{=-1} = 1,\end{aligned}$$

d.h. $(a\ b\ c) \in A_{\underline{n}}$ für alle $(a\ b\ c) \in E$. Zu zeigen:

$$\forall a, b, c, d \in \underline{n},\ a \neq b,\ c \neq d : (a\ b)(c\ d) \in \langle E \rangle. \qquad (*)$$

Fallunterscheidung:

- $\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}a & b\end{pmatrix} = e \in \langle E \rangle$,
- $\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}a & c\end{pmatrix} = \begin{pmatrix}a & b & c\end{pmatrix} \in E \subseteq \langle E \rangle$,
- $\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}c & d\end{pmatrix} = \begin{pmatrix}a & b & c\end{pmatrix}\begin{pmatrix}a & d & c\end{pmatrix} \in \langle E \rangle$.

Aussage des Lemmas: Sei $g \in A_{\underline{n}}$. Dann gibt es Transpositionen $h_1, h_2, ..., h_{2t-1}, h_{2t}$ mit

$$g = \underbrace{h_1 h_2}_{\substack{\in \langle E \rangle \\ \text{nach } (*)}} \cdots \underbrace{h_{2t-1} h_{2t}}_{\substack{\in \langle E \rangle \\ \text{nach } (*)}} \in \langle E \rangle.$$

∎

9.6 Lemma. *Sei $n \in \mathbb{N}$ mit $n \geq 5$. Je zwei Elemente von*

$$E := \{\begin{pmatrix} a & b & c \end{pmatrix} \mid a,b,c \in \underline{n},\ |\{a,b,c\}| = 3\}$$

sind konjugiert in $A_{\underline{n}}$.

Beweis. Sei $\begin{pmatrix} a & b & c \end{pmatrix} \in E$. Zeige: $\begin{pmatrix} a & b & c \end{pmatrix}$ ist konjugiert zu $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ in $A_{\underline{n}}$. Aussage des Lemmas folgt dann mit 1.19 (a). Da $\begin{pmatrix} a & b & c \end{pmatrix}$ und $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ ähnlich sind, sind sie konjugiert in $S_{\underline{n}}$ (vgl. 1.19 (c)), d.h. $\exists h \in S_{\underline{n}} : \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = h \begin{pmatrix} a & b & c \end{pmatrix} h^{-1}$. Ist $h \in A_{\underline{n}}$, dann fertig. Annahme: $h \notin A_{\underline{n}}$, d.h. $\operatorname{sgn}(h) = -1$. Setze $\tilde{h} := \begin{pmatrix} 4 & 5 \end{pmatrix} h$. Dann $\operatorname{sgn}(\tilde{h}) = \operatorname{sgn}(\begin{pmatrix} 4 & 5 \end{pmatrix}) \cdot \operatorname{sgn}(h) = 1$, also $\tilde{h} \in A_{\underline{n}}$, und

$$\begin{aligned} \tilde{h} \begin{pmatrix} a & b & c \end{pmatrix} \tilde{h}^{-1} &= \begin{pmatrix} 4 & 5 \end{pmatrix} h \begin{pmatrix} a & b & c \end{pmatrix} h^{-1} \begin{pmatrix} 4 & 5 \end{pmatrix} \\ &\overset{(*)}{=} \begin{pmatrix} 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}. \end{aligned}$$

■

9.7 Folgerung. *$A_{\underline{5}}$ ist einfach.*

Erinnerung (vgl. 3.8): *Ein Zyklus ist genau dann eine gerade Permutation, wenn er ungerade Länge hat*, denn:

$$\left.\begin{aligned} \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix} &\overset{3.9}{=} \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_1 & a_3 \end{pmatrix} \cdots \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \begin{pmatrix} a_1 & a_k \end{pmatrix} \\ &= \begin{pmatrix} a_k & a_{k-1} \end{pmatrix} \begin{pmatrix} a_{k-1} & a_{k-2} \end{pmatrix} \cdots \begin{pmatrix} a_3 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_1 \end{pmatrix} \end{aligned}\right\} (k-1) \text{ Faktoren.}$$

. Beweis von 9.7 Jedes Element von $A_{\underline{5}}$ ist von einem der folgenden Typen (für $\{a,b,c,d,e\} = \{1,2,3,4,5\}$).

Maximum der Zyklenlängen in Zyklendarstellung	Typ (Zyklendarstellung)	
1	$e = \begin{pmatrix} a \end{pmatrix} \begin{pmatrix} b \end{pmatrix} \begin{pmatrix} c \end{pmatrix} \begin{pmatrix} d \end{pmatrix} \begin{pmatrix} e \end{pmatrix}$	
2	$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} \begin{pmatrix} e \end{pmatrix}$	$\longrightarrow$ Typ (I)
3	$\begin{pmatrix} a & b & c \end{pmatrix} \begin{pmatrix} d \end{pmatrix} \begin{pmatrix} e \end{pmatrix}$	$\longrightarrow$ Typ (II)
4	—	
5	$\begin{pmatrix} a & b & c & d & e \end{pmatrix}$	$\longrightarrow$ Typ (III)

Sei $\{e\} \neq N \trianglelefteq A_{\underline{5}}$.

Behauptung: *N enthält ein Element von* $E := \{\begin{pmatrix} a & b & c \end{pmatrix} \mid a,b,c \in \underline{5},\ |\{a,b,c\}| = 3\}$.

Beweis. Sei $g \in N \backslash \{e\}$. Fallunterscheidung:

Fall 1: g hat Typ (I), also $g = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix}$. Dann

$$\underbrace{(\begin{pmatrix} a & b & e \end{pmatrix} g \begin{pmatrix} a & b & e \end{pmatrix}^{-1})}_{=\begin{pmatrix} a & e & b \end{pmatrix}\begin{pmatrix} c \end{pmatrix}\begin{pmatrix} d \end{pmatrix} \in E} g \in N \text{ (da } N \trianglelefteq A_{\underline{5}}).$$

Also $N \cap E \neq \emptyset$.
Fall 2: g hat Typ (II), also $g \in E \implies N \cap E \neq \emptyset$.
Fall 3: g hat Typ (III), also $g = \begin{pmatrix} a & b & c & d & e \end{pmatrix}$. Dann

$$\underbrace{(\begin{pmatrix} a & b & e \end{pmatrix} g \begin{pmatrix} a & b & e \end{pmatrix}^{-1})}_{=\begin{pmatrix} a \end{pmatrix}\begin{pmatrix} b & c & e \end{pmatrix}\begin{pmatrix} d \end{pmatrix} \in E} g \in N \text{ (da } N \trianglelefteq A_{\underline{5}}).$$

Also $N \cap E \neq \emptyset$. ■

Nach Behauptung: $N \cap E \neq \emptyset$. Wegen Lemma 9.6 und $N \trianglelefteq A_{\underline{5}}$, folgt $E \subseteq N$. Daher $N = A_{\underline{5}}$ nach Lemma 9.5 (und da $N \leq A_{\underline{5}}$). Also ist $A_{\underline{5}}$ einfach. ■

9.8 Lemma. *Sei $n \in \mathbb{N}$, $n \geq 5$. Dann:* $\forall g \in A_{\underline{n}} : \forall A_{\underline{n}} \backslash \{e\} \exists n \in A_{\underline{n}} \backslash \{g\}$:

(i) *g und h sind konjugiert in $A_{\underline{n}}$, und*
(ii) $\exists i \in \{1, ..., n\} : i^g = i^h$.

Beweis. Sei $g \in A_{\underline{n}} \backslash \{e\}$. Sei m die maximale Länge eines Zyklus in der Zyklendarstellung von g. Klar: $m \geq 2$. Fallunterscheidung:

$m \geq 3$: Sei $g = \begin{pmatrix} a_1 & \cdots & a_m \end{pmatrix} g'$ Zyklendarstellung von g. Wähle $b, c \in \{1, ..., n\} \backslash \{a_1, a_2, a_3\}$, $b \neq c$. Dann $\begin{pmatrix} a_3 & b & c \end{pmatrix} \in A_{\underline{n}}$ (vgl. 9.5) und daher $h := \begin{pmatrix} a_3 & b & c \end{pmatrix} g \begin{pmatrix} a_3 & b & c \end{pmatrix}^{-1} \in A_{\underline{n}}$ konjugiert zu g in $A_{\underline{n}}$. Nun:

- $a_1^h = a_1^{\begin{pmatrix} a_3 & b & c \end{pmatrix} g \begin{pmatrix} a_3 & b & c \end{pmatrix}^{-1}} = a_2 = a_1^g$,
- $a_2^h = a_2^{\begin{pmatrix} a_3 & b & c \end{pmatrix} g \begin{pmatrix} a_3 & b & c \end{pmatrix}^{-1}} = c \neq a_3 = a_2^g \implies g \neq h$.

$m = 2$: Dann $h = \begin{pmatrix} a_{11} & a_{12} \end{pmatrix} \begin{pmatrix} a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} a_{31} & a_{32} \end{pmatrix} \cdots \begin{pmatrix} a_{k1} & a_{k2} \end{pmatrix}$ für paarweise verschiedene $a_{11}, a_{12}, ..., a_{k1}, a_{k2} \in \underline{n}$. Fallunterscheidung ($k \geq 2$, da g gerade Permutation ist):

$k \geq 3$: Dann $\begin{pmatrix} a_{11} & a_{12} \end{pmatrix} \begin{pmatrix} a_{21} & a_{31} \end{pmatrix} \in A_{\underline{n}}$ und daher

$$h := \begin{pmatrix} a_{11} & a_{12} \end{pmatrix} \begin{pmatrix} a_{21} & a_{31} \end{pmatrix} g \begin{pmatrix} a_{11} & a_{12} \end{pmatrix} \begin{pmatrix} a_{21} & a_{32} \end{pmatrix} \in A_{\underline{n}}$$

konjugiert zu g in $A_{\underline{n}}$. Und:
- $a_{11}^h = a_{12} = a_{11}^g$,
- $a_{21}^h = a_{32} \neq a_{22} = a_{21}^g \implies g \neq h$.

$k = 2$: Dann $g = \begin{pmatrix} a_{11} & a_{12} \end{pmatrix}\begin{pmatrix} a_{21} & a_{22} \end{pmatrix}$. Dann $\begin{pmatrix} a_{11} & a_{21} & a_{12} \end{pmatrix} \in A_{\underline{n}}$ (vgl. 9.5), also $h := \begin{pmatrix} a_{11} & a_{21} & a_{12} \end{pmatrix} h \begin{pmatrix} a_{11} & a_{12} & a_{21} \end{pmatrix} \in A_{\underline{n}}$ konjugiert zu g in $A_{\underline{n}}$. Und:

– $a_{11}^h = a_{22} \neq a_{12} = a_{11}^g \implies g \neq h$,
– $b^h = b = b^g$ für jedes $b \in \{1, ..., n\} \backslash \{a_{11}, a_{12}, a_{21}, a_{22}\}$.

■

9.9 Lemma. *Sei $n \in \mathbb{N}$ mit $n \geq 3$, und $i \in \{1, ..., n\}$. Dann gilt: $(A_{\underline{n}})_i \cong A_{\underline{n-1}}$.*

Beweis. Betrachte Injektion $f : \{1, ..., n-1\} \to \{1, ..., n\}$ mit

$$f(j) := \begin{cases} j & \text{falls } j < i, \\ j+1 & \text{falls } j \geq i \ (j \in \{1, ..., n-1\}). \end{cases}$$

Dann $\mathrm{Im}(f) = \{1, ..., n\} \backslash \{i\}$. Betrachte injektiven Homomorphismus $\Phi : S_{\underline{n-1}} \to S_{\underline{n}}$ mit

$$j^{\Phi(g)} := \begin{cases} f(f^{-1}(j)^g) & \text{falls } j \neq i, \\ i & \text{sonst,} \end{cases}$$

für $j \in \{1, ..., n\}$ und $g \in S_{\underline{n-1}}$. Dann $\mathrm{Im}(\Phi) = (S_{\underline{n}})_i$. Und: Φ bildet Transpositionen auf Transpositionen ab. Genauer:

$$\Phi(\begin{pmatrix} j & k \end{pmatrix}) = \begin{pmatrix} f(j) & f(k) \end{pmatrix}$$

für alle $j, k \in \{1, ..., n-1\}$, $j \neq k$. Folgerung:

$$\begin{aligned} g \in A_{\underline{n-1}} &\iff g \text{ ist produkt einer geraden Anzahl von Transpositionen} \\ &\implies \Phi(g) \text{ ist Produkt einer geraden Anzahl von Transpositionen} \\ &\iff \Phi(g) \in A_{\underline{n}}. \end{aligned}$$

Also $\Phi(A_{\underline{n-1}}) \subseteq A_{\underline{n}} \cap (S_{\underline{n}})_i = (A_{\underline{n}})_i$. Und:

$$|(A_{\underline{n}})| = \frac{|A_{\underline{n}}|}{|i^{A_{\underline{n}}}|} \overset{A_{\underline{n}} \text{ ist}}{\underset{\text{transitiv}}{=}} \frac{\frac{n!}{2}}{n} = \frac{(n-1)!}{2} = |A_{\underline{n-1}}|.$$

Also $\Phi(A_{\underline{n-1}}) = (A_{\underline{n}})_i$. Damit ist $A_{\underline{n-1}} \cong (A_{\underline{n}})_i$. ■

9.10 Satz. *Sei $n \in N$ mit $n \geq 5$. Dann ist $A_{\underline{n}}$ einfach.*

Beweis. Induktion über $n \geq 5$:

Induktionsanfang: Folgerung 9.7.
Induktionsschritt: Sei $n \geq 6$ und Einfachheit von $A_{\underline{n-1}}$ vorausgesetzt. Sei $\{e\} \neq N \trianglelefteq A_{\underline{n}}$. Sei $g \in N \backslash \{e\}$. Nach Lemma 9.8: $\exists h \in A_{\underline{n}} \backslash \{g\}$:

(i) g und h konjugiert in $A_{\underline{n}}$,

(ii) $\exists i \in \{1, ..., n\} : i^g = i^h$.

Wegen (i) und $N \trianglelefteq A_{\underline{n}}$ ist $h \in N$. Wegen (ii) ist $gh^{-1} \in \left(A_{\underline{n}}\right)_i =: H_i$ für ein $i \in \{1, ..., n\}$. Also: $e \neq gh^{-1} \in N \cap H_i \implies N \cap H_i \neq \{e\}$. Wegen $N \trianglelefteq A_{\underline{n}}$ ist $(N \cap H_i) \trianglelefteq H_i$ (ganz allgemein gilt $N \trianglelefteq G, H \leq G \implies N \cap H \trianglelefteq H$). Weil $H_i = \left(A_{\underline{n}}\right)_i \overset{9.9}{\cong} A_{\underline{n-1}}$ einfach nach Induktionshypothese: $N \cap H_i = H_i$, d.h. $H_i \subseteq N$. Da H_i Zyklus der Länge 3 enthält, enthält auch N einen solchen. Wegen Lemma 9.6 und $N \trianglelefteq A_{\underline{n}}$ enthält N jeden Zyklus der Länge 3. Mit Lemma 9.5 folgt: $N = A_{\underline{n}}$. Das zeigt: $A_{\underline{n}}$ ist einfach.

■